Acknowledgement

The MNWG would like to acknowledge the contribution from FMV, the Swedish Defense Materiel Administration. They have contributed generously with the results from their project LedSystT. LedSystT is the FMV process of creating a set of design rules and guidelines which are to be used as the base for future Command & Control development projects. Some of this material was used to enhance the IP and Mobility Tenets. We also thank the United States Department of Defense Offices of the Secretary of Defense and Defense Information Services Agency (DISA) for sharing their input and guidance on IP architecture via the GIG Architecture.
General Issue Summary

The Network Centric Operations Industry Consortium (NCOIC™) Mobile Networking Working Group (MNWG) is responsible for evaluating and recommending mobile networking solutions for network-centric systems. MNWG is a distributed and collaborative forum providing solutions for today’s mobility problems and addressing new problems as they emerge. In particular, MNWG examines mobile systems, network of systems or devices that provide operational functionality while in motion at a given velocity. The objective of this MNWG Mobile Networking Evaluation (MNE) Issue publication is to evaluate and recommend existing and future commercial mobile networking technologies that may be applicable for customer missions, tasks and applications, and to identify technology gaps.

In the previously released Mobility Networking Overview (MNO)\textsuperscript{EXS-1} the MNWG defined the ten major technology problem areas faced by mobile networking: 1) Quality of Service (QoS); 2) Network Planning and Management (NPM); 3) Network and Node Mobility (NNM); 4) Routing (ROU); 5) Physical and Data Link Layer Constraints (P\&DL); 6) Information Assurance (IA); 7) Ad Hoc Networks (AHN); 8) Transport Layer Protocols (TLP); 9) Multicast (MC); and 10) Applications Interaction (AI). In this MNE, the MNWG will evaluate technologies specifically related to these defined problem areas and evaluate their applicability to the classes of mobile networking in network centric environments, including use cases defined in this document.

The MNE will be released in a series of Issues, collected as a publication volume. This document is the initial Issue of Volume 1. While much groundwork has been done to define architecture tenets, identify criteria for evaluation of standards, and specify content for the network-centricity filters, further work remains to be done to provide the foundation and intellectual endowment for globally interoperable mobile networks. Future MNE Issues will provide sections on the ten technical problem areas as they become developed.

The Mobile Networking Working Group has identified an initial set of generally agreed upon principles or tenets. The members of the MNWG concur that these tenets should drive architectural design of mobile networks. One of the purposes in identifying these principles is to minimize the potential for disruptions based on the introduction of new technologies. When new technologies are to be introduced, they will be reviewed relative to these principles. If no reasonable solution consistent with the list is identified, a flag is raised that indicates a need to violate the specific tenet. In these cases, a description of the issue is to be provided, including impact of the proposed solution on existing networks and recommended standards, and the reason this solution is more desirable than others that do not violate the tenet.

The initial categories of tenets are Internet Protocol (IP) Architecture, and Mobility. The networking principles considered basic to successful network architecture design are the IP Architecture Tenets. In addition, the Mobile Networking Working Group has identified a set of tenets that are specific to mobile nodes and networks. Any mobile node or network architecture being considered should be measured against all three sets of tenets.

The MNWG recommends standards to provide capabilities needed by our customers in mobile network centric environments. These capabilities are critical to meeting operational
needs, and are identified through typical use cases. For these use cases the three classes of mobility are defined as ad hoc mobility; connected mobility, and disconnected mobility.

A wide range of use cases exist, including humanitarian disasters ranging from Hurricane Katrina to severe drought conditions in Africa, to joint and coalition military situations, and Homeland Security Department events such as terrorist attacks, demonstrating many levels of operational and technical interoperability effecting currently deployed and future systems. The emphasis of the MNE will be on emergency “first responders” and coalition military events.

The MNWG Identified and Recommended Communications Standards section includes 1) foundational standards based on MNWG tenets, 2) standards for specific operational scenarios determined by NCOIC Integrated Product Teams (IPTs), and 3) MNWG problem area specific standards, which are the result of the MNE work performed for that problem area. For Issue 1 of the MNE, foundational standards and recommended standards from the Mobile Emergency Communication Interoperability (MECI) Phase 1 report^EXS-2 are included. No problem area specific standards are included in this Issue. As the problem area work matures, standards will complete the evaluation process and be added to the table of recommended standards. Recommended standards are current industry standards ratified by the appropriate Standards organization.

The approach planned for use by MNWG to evaluate the ability of proposed standards to support network-centricity begins with the standards evaluated against requirements and use cases from multiple environments, such as MECI, NATO, Sense and Respond Logistics, and other communities of interest. Proposed standards will then be evaluated against the IP architecture, Mobility, and IA tenets. While we utilize System Capability Operation Program Enterprise (SCOPE) Model and Network Centric Analysis Tool (NCAT™) to perform network centric evaluation, the results of our evaluation may likely provide new inputs to these models. The evaluation tools developed by NATO and the US Department of Defense (DoD) will be used to enable our proposed standards to be consistent with guidelines from our customers. To determine if a standard is supportive of network-centricity from non-technical viewpoints, the proposed standards will be also evaluated against programmatic issues.

This MNE endeavors to establish the process by which commercial standards that serve the Mobile Networking community can be consistently identified and evaluated for technical sufficiency and ultimate implementation. The MNWG will exercise the MNE process to align, inform and assist in developing, managing, and providing guidance and oversight for information technology standards management associated with mobile wireless networking. The MNE will document the evaluation of networking technologies for applicability in a network-centric mobile environment.

The document is being developed using a spiral approach. It is released to document work to date and obtain feedback from our customers and the wider community. We welcome feedback from all interested parties to suggest additions and deletions as well as volunteers to help continue the work.
Foreword

This document is being submitted as a deliverable of the Mobile Network Working Group (global-mobile-net@lists.ncoic.org), a chartered working group of the NCOIC. The NCOIC has the following mission and vision that is supported by this work:

- **Mission**: The mission of the Consortium is to help accelerate the achievement of increased levels of interoperability in a network-centric environment within, and amongst, all levels of government of the United States and its allies involved in Joint, Interagency and Multinational operations.

- **Vision**: Industry working together with our customers to provide a network-centric environment where all classes of information systems interoperate by integrating existing and emerging open standards into a common evolving global framework that employs a common set of principles and processes.

The MNWG will use the network-centricity objectives proposed within the Network-centric Checklist as a starting guideline supplemented by the technical direction of the Net Centric Implementation Directives (NCID)s, experienced inputs from NATO, (DISA), Joint Forces Command (JFCOM), Space and Naval Warfare (SPAWAR), and knowledgeable inputs from industry. The list will incorporate inputs from global organizations, such as NATO, to better reflect the international scope of the recommendations. The NCOIC process recommends NCO industry providers, adopters and users to collectively agree upon the objectives and how to achieve them. NCOIC Technical Council Functional Teams are responsible for developing this process which promises to deliver guidelines to the technical WGs to coordinate their work. The Network-centric Checklist identifies the following objectives for the Communications area which will be used as the starting point for the MNWG:

- IPv6
- Packet Switched Infrastructure
- Layering, Modularity
- Communications’ Integration
- Network Connectivity
- The Concurrent Transport of Information Flows
- Differentiated Management of Quality-of-Service (QoS)
- Inter-Network Connectivity
- Department of Defense Information Technology Standards Registry online (DISR online)
- RF Acquisition
- Joint Network-centric Capabilities
- Operations and Management of Communications and Services

The essential Net Centricity principles as connectivity, interoperability, discovery, security need to be met end to end. They apply to all the MN work areas.

The other checklist areas include Data, Services and Information Assurance (IA) which are addressed by NCOIC’s SII-WG, Services Oriented Architecture (SOA) forum and IA-WG, respectively. MNWG effort will support the Network Interoperability Framework (NIFTM).
Functional Team to propose Network Centric Operations (NCO) interoperability frameworks and help to ensure consistency and interoperability between working groups’ deliverables.
Table of Contents

Acknowledgement............................................................................................................. i
General Issue Summary....................................................................................................... ii
Foreword............................................................................................................................... 1
Table of Contents .................................................................................................................. 3
Table of Tables ...................................................................................................................... 3
Table of Figures ................................................................................................................... 3
1 Introduction ......................................................................................................................... 5
  1.1 Objective ....................................................................................................................... 6
  1.2 Scope ............................................................................................................................ 6
  1.3 Approach ...................................................................................................................... 7
2 MNE Process ...................................................................................................................... 9
  2.1 Motivation ................................................................................................................... 9
  2.2 Process ......................................................................................................................... 9
  2.3 Strategy ....................................................................................................................... 13
  2.4 Guidance Statement ................................................................................................... 14
3 Tenets ............................................................................................................................... 16
  3.1 IP Architecture Tenets ............................................................................................. 16
  3.2 Mobility Tenets .......................................................................................................... 22
4 Use Cases ......................................................................................................................... 25
  4.1 Coalition Defense use cases ...................................................................................... 25
  4.2 Mobile Emergency Communications Interoperability (MECI) use cases ................. 31
5 Evaluation of Standards ................................................................................................. 34
  5.1 Evaluation Methods ................................................................................................. 34
  5.2 Foundational Standards ......................................................................................... 35
6 Appendix .......................................................................................................................... 36
  6.1 Appendix A: Acronyms ........................................................................................... 36
  6.2 Appendix B: Glossary .............................................................................................. 38
  6.3 Appendix C: Contributors ....................................................................................... 44
  6.4 Appendix D: References ........................................................................................ 44

Table of Tables

TABLE 5.1-1. APPROACHES TO EVALUATE PROPOSED STANDARDS FOR NET CENTRICITY .......... 34
TABLE 6.4-1. REFERENCES .................................................................................................. 44

Table of Figures

FIGURE 2-1 MNE PROCESS ................................................................................................. 13
FIGURE 4-1: AD HOC MOBILITY .............................................................. 26
FIGURE 4-11: UNPLANNED SWITCH BETWEEN DUPLICATED CP ............ 29
FIGURE 4-12: DUPLICATED CP MOVING ............................................ 29
FIGURE 4-14: TYPICAL MECI ARCHITECTURE ....................................... 31
FIGURE 4-15: MECI HIERARCHICAL SCHEME ....................................... 32
FIGURE 4-16: MECI ENHANCED SCHEME ........................................... 33
1 Introduction

Today, commercially available handheld wireless devices are used to get high-speed Internet access, e-mail, video, and streaming audio services from network providers. As capabilities continue to improve, those handheld wireless devices will be able to provide more capabilities with greater speed. The challenge is to provide those same services, often with strict requirements on quality and security, to deployed war fighters or emergency response personnel who are often located in remote areas with little or no infrastructure.

Creating a fully functional mobile networking environment presents many challenges. The reliable transport of data across multiple network domain boundaries in a mobile, bandwidth constrained, lossy environment is not a simple matter. Documenting the technologies that could make such a network possible presents yet another set of challenges.

The potential existence of multiple network domains is challenging for all problem areas that require cooperation between domains. These areas specifically include QoS, Network Planning and Management (NPM), Routing (ROU), Multicast (MC), and IA.

A mobile network domain is often thought of as the set of mobile nodes and networks that are interconnected, with connectivity to a fixed-infrastructure at a number of access points. It is assumed that a mobile network domain uses the same network management mechanism, otherwise it can be seen as two separate domains. The initial challenge of creating a fully functional mobile network is making the mobile nodes interoperate with each other properly. This intra-domain communication is essential to success. Following that success, it becomes apparent that inter-domain communication is necessary if any information is to enter or leave the mobile domain. As the mobile domain becomes more heterogeneous, and as different owners interconnect their own mobile domains, the boundaries between domains often become less distinct. Are the boundaries of these domains defined by the edges of homogenous implementation clusters or by the owners? If the technologies are the same and the owners are cooperative, can the interconnecting domains use the same management techniques? Inter-domain communication becomes far more challenging and is a strong motivation for the adoption of standards in a variety of areas.

Another significant challenge is introduced if the requirement is levied that each node not only has connectivity to the greater network, but that it be directly accessible and addressable from outside the mobile domain. This seemingly trivial requirement introduces a derived requirement that the network address be maintained separately from the identity of the user. Connection oriented protocols are often dependent on the two addresses used for establishing the original connection. As the node or network moves from attachment point to attachment point, its network address may be required to change. The user, however does not change, thus creating a problem for systems that make the assumption that the address is associated with the user rather than with the current network topology.
1.1 Objective

The challenge of evaluating mobile networking problem areas with the intent of providing guidance and best practices for NCO environments is the focus of the NCOIC Mobile Networking Working Group. The Mobile Networking Overview (MNO) document established the process and defined the scope for meeting this challenge. This document has been formally reviewed by the NCOIC organization and is available for public access. The Mobile Networking Evaluation (MNE) suite of documents, released as a set of publication issues, is a foundational step toward accomplishing the objectives set forth in the MNO. The purpose of the MNE is to evaluate and recommend existing and future commercial mobile networking technologies that may be applicable for customer missions, tasks and applications, and to identify technology gaps.

In the MNO, we defined ten problem areas that constitute the major technology areas faced by mobile networking: 1) QoS; 2) Network Planning and Management (NPM); 3) Network and Node Mobility (NNM); 4) Routing (ROU); 5) Physical and Data Link Layer Constraints (P&DL); 6) Information Assurance (IA); 7) Ad Hoc Networks (AHN); 8) Transport Layer Protocols (TLP); 9) Multicast (MC); and 10) Applications Interaction (AI). It is the objective of the MNE to evaluate technologies specifically related to these defined problem areas and evaluate their applicability to the classes of mobile networking in network centric environments including use cases defined in this document and future MNE Issues.

1.2 Scope

This work covers the commercial off-the-shelf (COTS) mobile networking technologies that are currently available or will be available in the near future. Customer needs require technologies providing agile, adaptive, and transforming capabilities at both core and edge networks and devices. The technologies will apply to small, light, and durable devices that users will carry with them to remote areas as well as to moving vehicles such as automobiles, trucks, aircraft, and ships. The MNWG will exercise the MNE process to align, inform and assist in developing, managing, and providing guidance and oversight for information technology standards management associated with mobile wireless networking. The MNE will document the evaluation of networking technologies for applicability in a network-centric mobile environment. This evaluation will follow the MNE process described in Section 2. Technologies pertinent to each of the problem areas will be evaluated relative to the various “use cases” (see Section 4), “mobility classes” (see Section 4), architecture tenets (see Section 2) and initial Industry Standards (see Section 6).

The MNE will focus on the IP Reference Model Transport and Network layers, known as the network communication layers including interfaces to lower (Physical and Data Link) and higher (Applications and Services) layers. While we recognize that the Network and Transport layers are affected by the behavior of the Physical and Data Link layers, and there is a need for intercommunications between the Applications and Services Layer and the lower communications layers, our focus is on the network communications layers.

The MNE is intended for a diverse audience. Its initial purpose is to serve as MNWG evaluation input to the NIFTM. Beyond that, we hope that it will serve as a reference to network professionals and customers. The stakeholders that have been specifically
1.3 Approach

The MNE endeavors to establish the process by which commercial standards that serve the Mobile Networking community can be consistently identified and evaluated for technical sufficiency to support Network-centricity and ultimate implementation. The NCOIC MNWG intends that mobile components will be interoperable for joint military and emergency response operations, and all COTS technologies considered are based on a consistent set of commercial standards. This requires a mandated or approved set of Information Technology (IT) and network security standards that are determined via a disciplined and repeatable evaluation process. The MNE process evaluates applicable COTS wireless technologies and emerging technologies to determine whether these technologies and standards meet the needs of mobile networking. If they do not, the process identifies the shortcomings and suggests needed development and/or modifications. Based upon detailed market research to collect all the mobile networking technical data, requirements and use cases, analysis against known scenarios, trends and options will identify promising technology solutions that will provide a set of recommendations based on the results of the evaluation.

Accomplishment of this has required defining Tenets (Section 2), Use Cases (Section 4), and mobility classes (Section 4). All of these serve as bases for defining “network-centric filters” to be used as part of the evaluation of proposed technologies.

The MNE will be released in publication issues in a volume collection. This is the first of those spirals packaged as Issue-1. While much groundwork has been done to define architecture tenets, identify criteria for evaluation of standards, and specify content for network-centricity filters, further work remains to be done to recommend standards for globally interoperable mobile networks. Work has been performed in some problem areas and little or none in others. In future MNE issues spirals, we intend to address the MNO identified problem areas, add more “use cases”, evaluate more technologies, and provide a more complete evaluation of the technologies whose evaluation has begun. The document is being developed using a spiral approach. This document is being released to document work to-date and to get feedback from our customers and the wider community.

We are specifically soliciting feedback on the following:

- Are the Use cases sufficient to identify the needs of network-centricity?
- Are the Tenets appropriate?

For each problem area

- Have we identified the correct set of operational needs to prioritize our technical work for that problem area?
- Is this the appropriate survey space? What additional technologies should be considered?
- Have we identified appropriate network-centricity filters? Are there operational needs that should have been included as Use Cases?
• Have we identified appropriate end products?
• Are there emerging standards that should be considered?

We hope to receive feedback from all interested parties. Feedback to suggest both additions and deletions is welcomed as are volunteers to help continue the work.

Section 1 is the Introduction. Section 2 refines the MNE process defined in the MNO. Section 3 defines three sets of “tenets”. These tenets are provided to lay the groundwork for defining the “Network-centricity filters” required by the MNE process. Section 4 defines the Use Cases that are to be used when evaluating technologies. Section 5 clarifies the methods used for evaluation of standards. Appendices provide references, a glossary, a list of Acronyms and a list of contributors. Some technical evaluation background or supporting reference has also been included as appendices.
2 MNE Process

2.1 Motivation

The MNWG developed within the MNO document ten key mobility problem areas for advancing NCO. The document also proposes a common process for addressing the problems areas. The objective is to achieve consistent presentation of the work across all problem areas. The process provides a baseline for further discussion how we, working a particular problem area, identify and evaluate standards and patterns important to Network Mobility. The process begins to identify the interactions with other WGs both how they may impact MNE and how MNE might impact their output. The disciplined development of the problems and the evaluation process will make it easier for the NCO customer interested in multiple problem areas to absorb and act on the results helping ensure that NCOIC successfully addresses the objectives identified in its vision:

- Identify existing and emerging open standards
- Identify global framework
- Identify common set of principles and processes.
- These objectives will help the consortium and its customers develop and field network-centric systems. It is important to carefully formulate the problems being addressed and to develop and formalize the NCOIC process for addressing the problem areas in terms of the above NCOIC objectives. A common process that enforces a discipline in developing individual problem areas is especially important across highly distributed team efforts like MNWG.

2.2 Process

The MNE process is organized into multiple analysis and decomposition phases for each MNO Technology Area component:

1. Phase 1 - Develop Mobility Deployment Requirements and Domains
   a. Technology NCO Tenets, which identify the key overarching principles to be verified within the MNE. These include IPRM Tenets, Mobility Tenets, and IA Tenets.
   b. Customer Requirements Analysis, which include the Driving Requirements, Operational Use Cases, Technical Use Cases, and applying the base knowledge from the MNWG MNO specification. This work assumes MNWG working with the REQUIREMENTS VALIDATION FT to gather Driving Requirements and the SIIWG to scope the Operational Use Cases.

2. Phase 2 - Develop Network Mobility Functional Models and Technology Standards/Survey
a. Functional Requirements and Domains for an MNE functional area are identified to perform the following functions:
   i. Identify Driving Requirements
   ii. Identify User Operational Scenarios
      1. Identify Tactical Use Case Scenarios
      2. Identify Strategic Use Case Directions
   iii. Identify new MNE areas not determined within the MNO specification (change control for MNO)

b. Determine if new or enhanced technology or standard if yes go-to Phase 2a.

c. Functional Models and Technology Surveys for MNE Functional Area are identified to perform the following functions:
   i. Identify Overarching Technology Models for specific MNE Functional Areas from MNO specification
   ii. Identify organizations influencing the technical specification of the technology
   iii. Identify particular standards of interest and decipher components technically in depth
   iv. Evaluate against Functional Requirements and Domains from Phase 2a

d. Go-To Phase 2b

3. Phase 2a - Addressing New or Enhanced Technology and Standards Requirements
   a. Motivation for New Technology Focus or Standards Development to determine if MNE process should proceed:
      i. Identify technology gap
      ii. Justify requirement for the technology gap to be filled using results from Phase 1
   b. If the Gap is not justified, remove determined Technology or Standard from MNE process as work item
   c. If the Gap is justified:
      i. Identify to the Specialty Frameworks Team Chair and Technical Council this Gap needs to be filled.
      ii. Today, NCOIC or MNWG has no process or methods to enhance or introduce new technology into External Standards Forums, and these would be need to developed for each Gap identified working with the NCOIC Technical Council
   d. Await resolution with NCOIC Technical Council to determine if MNE Phase 3 should proceed for this Gap and how we input to External Forums if required.
4. Phase 2b - Delivery of MNE Phase 2 Interim Paper is a decision as an interim step to determine if MNWG wants to deliver an interim paper on Phase 2 to be verified by the NCOIC Technical Council process.

5. Phase 3 - Perform NCO Filter and Evaluation Process
   a. NCO Filter Process for the Technology or Standard of Interest are identified by the following functions:
      i. Identify whether any technology components from Phase 3 are a new requirement for NCO
      ii. Apply the IP, Mobility, and IA Tenets to the technology components from Phase 3
      iii. Identify whether the networking principles of NCO are compliant to the NCO Checklist supporting connectivity, interoperability, security, discovery, and end-to-end
      iv. Identify NCO and deployment gaps in the technology components from Phase 3
      v. Identify technology requirements to support transition forward from legacy technology for this identified technology or standard
      vi. Identify requirements from other NCOIC Specialty Framework Teams (e.g. NIF, IA, SII).
      vii. Identify whether this is new MNE area not previously determined within the MNO specification and has MNWG consensus to proceed
   b. Have the requirements for the NCO Filter passed the requirements
      i. If no, then Report reasons to NCOIC Specialty Frameworks Teams Chair and Technical Council, enter hiatus state until further discussion
      ii. If yes, then go-to Phase 3a

6. Phase 3b - Decision on MNE Phase 3 Interim Paper is a decision as an interim step to determine whether MNWG wants to deliver an interim paper on Phase 3 to be verified by the NCOIC Technical Council process.

7. Phase 4 - Develop MNE End Product
   a. Develop MNE End Product per the following functions:
      i. Identify technical interfaces and impact to NCOIC Building Code/Block functions and to other NCOIC Specialty Framework Teams (e.g. NIF, SII, IA) for this technology component
      ii. Identify technology pattern changes that will impact deployment of this technology component
      iii. Identify recommended standards for this technology component
      iv. Identify best practices and requirements for deployment of this technology component
v. Identify performance, scalability, and reliability of this technology component, as best understood from an MNWG analysis. (done as Phase 4 activity).

vi. Identify training requirements

vii. Develop MNE deployment analysis white paper and recommendations for this technology component

b. Put the MNE End Product deliverable through the NCOIC release processes
   i. if it does not pass, MNWG re-work the MNE Phase Processes to determine next steps
   ii. If it does pass, provide MNE End Product publicly as NCOIC deliverable
2.3 Strategy

The MNE strategy is to (1) solicit appropriate expertise for each problem area and (2) orchestrate the interaction between MNE and the NCOIC vision, processes and products,
e.g., Network Interoperability Framework (NIF), Network Centric Analysis Tool (NCAT), etc. and (3) develop an effective process. This is uncharted territory for a complex endeavor. This MNE framework will be used as a guideline to develop the level of detail required to allow the WG to proceed with the first iteration of the MNE.

A successful MNE process maintains an optimum balance between enabling locally speedy problem-specific process and larger emergent discipline, consistency and integration across problem areas. A one-size process will not fit all perfectly. It is expected that not all elements of the process will be applicable to all problem areas. The MNE described herein is expected to be revisited for “fine-tuning” using experience obtained during or after each iteration.

The interactions between MNE and the larger process must be loosely coupled due to the complexity of the mission and diverse maturity levels across NCOIC developments. When there are mature inputs affecting a MNE activity, they will be incorporated, but should not significantly impact MNE product delivery schedule. It will be up to the discretion of specific problem area teams as to whether their schedule should be gated by results from other problem areas or WGs.

Other NCOIC FTs are expected to provide the motivating problems and use cases and requirements. These inputs should be delivered initially to help orchestrate the first iteration of the MNE. If the NCOIC inputs impact a particular MNO problem area, then the MNE team responsible for the problem area will develop (multiple) functional model(s) potentially satisfying multiple classes of usage. If no relevant inputs are received, the MNE team will use their best judgment to develop the necessary functional model(s), tenets and assumptions. The top-down input will increase the probability that the MNE work has maximum effectiveness and consistency between problem areas, i.e., they are resolving similar classes of use cases.

The practitioner of MNE is expected to take advantage of both top-down and bottoms-up viewpoints to successfully complete their work. The exact balance will be dependent on the problem area, and the nature of the input provided from other teams. The participants experience with the “bottom/network plumbing” technology will help them effectively filter the irrelevant high-level motivating requirements and vice versa. Finally a MNWG focal point will be identified for each interaction within the MNE process. The steps in the workflow provided herein are only to be used as guidelines. Problem area investigators are expected to make reasonable effort to address each task during their investigation. If they decide that they cannot use a particular step for their problem area, they should document this rationale in lessons-learned. This input will be used to help fine-tune the MNE framework during next design iteration to address the next series of problem areas as the current ones are resolved.

2.4 Guidance Statement

This proposed process provides guidelines and directions to MNWG for development of the MNE. This ensures that MNWG’s multiple teams will proceed with similar bearing with respect to NCOIC mission as they develop products for their particular problem areas. The process proposed in the MNO has been updated during the early stage of the MNE to include improved understanding on the task flow and desired deliverables. Further process improvement is expected over time as the WG gains experience executing the MNE.
Tenets

The Mobile Networks Working Group has identified three sets of generally agreed upon principles: IP Architecture Tenets, IA Tenets, and Mobility Tenets. We have chosen to present these principles as tenets. We believe that these tenets should drive architectural design of mobile networks. One of the purposes in identifying these principles is to minimize the potential for disruptions based on the introduction of new technologies. As new technologies are introduced, they should be reviewed relative to these principles.

3.1  IP Architecture Tenets

The Mobile Networks Working Group has identified several networking principles that we consider basic to successful network architecture design. We refer to these principles as IP Architecture Tenets. We intend this list to be used as work in the problem areas is performed. Potential solutions are to be measured against the list to determine whether or not they are consistent. If no reasonable solution that is consistent with the list is identified, an indication that a need to violate the specific tenet is noted. In these cases, a description of the issue is to be provided and a note on the implications of the solutions recommended. We now provide a list of these tenets along with our view of the meaning:

3.1.1  The network should be transparent to users. This means users can use the network without needing to know technical and operational details of network infrastructure.

A primary goal in network design is to isolate the users from network implementation. Users should not have to understand the details of the network in order to use it.

3.1.2  Any host in the network can send packets to any other host in the network (unless prohibited by policy), without signaling for session establishment required between host and the network infrastructure. “Always On” paradigm.

A primary goal of networks is to provide the capability for all connected users to communicate with each other. There will be times when such communication will not be allowed. Many networks may have “receive only” nodes, – these nodes are not considered to be hosts. Protocols that do require signaling for specified capability are excluded from this tenet.

3.1.3  The network shall facilitate end-to-end interoperability.

Though the inter-network will consist of many independent networks, it must be designed to allow cooperation between these networks. Interoperability requires cooperation and coordination.
Cooperation and coordination are necessary to support global routing.

Cooperation and coordination are necessary to support end-to-end packet delivery (e.g. bi-lateral agreements, service level agreements, and trust agreements).

In order to achieve this interoperability the network shall support
- Common packet format
- Common global address scheme
- Cooperative global routing and network flow control procedures

3.1.4 **The network shall be IP-based** – The network architecture shall employ standardized interfaces between applications and transport services.

IP is the common glue that allows diverse networks to interoperate. There are several features that make IP the obvious choice for use as the Network Layer of a robust packetized network.
- It is widely accepted
- It provides a common packet format
- It supports common global addressing
- It minimizes the number of service interfaces
- It maximizes interoperability

This means that non-IP systems must interoperate with the network via gateways.

3.1.5 **The target architectural environment is a network of cooperative, but essentially autonomous networks. The network of networks should not, by design, require centralized administration and control.**

It is important for networks established by different parties to be able to be interconnected. While each of these networks may be essentially autonomous, they must cooperate to allow such things as global addressing to be used across the wider inter-network.

3.1.6 **The Network should be robust (minimize single-points of failure, protect itself against malicious attacks, and maximize availability).**

These networks will be used in crisis situations. It is crucial that they be reliable. In order to achieve the desired performance and reliability, it is important to minimize the scope of failures to prevent the network from being rendered inoperable. Graceful degradation of the network in the face of various events and failures is essential. Mobile ad hoc networks need to be self-healing and self-organizing.

3.1.7 **The network architecture shall employ a layered protocol model.**

Most modern protocol models employ a layered model. This allows the layers to be independent of layers above and below, as long as they comply with the interfaces defined between the layers. Each layer is required to be aware of only two interfaces—those to the adjacent layers.
Arguments have been made that performance increases can be achieved if adjacent layers can share information beyond the immediate data itself. RFC 817 suggests that this should be done cautiously: “The way to achieve this goal of packet sharing is to break down the barrier between the layers of the protocols, in a very restrained and careful manner, so that a limited amount of information can leak across the barrier to enable one layer to optimise its behaviour with respect to the desires of the layers above and below it”. If such “leakage” is performed via a documented interface between adjacent layers, the layered model is not violated.

3.1.8 Any use of Cross-Layer Design should be reviewed, weighing the benefits against the costs of increased complexity.

By-passing normal inter-layer interfaces to allow cross-layer design can lead to unforeseen interlayer dependencies. Industry experience has shown that such dependencies frequently lead to increased dependencies, which violate the Simplicity Principle.

Separation of concerns at each layer in the communications protocol world is a well accepted concept and ensures that the services offered by each layer to higher layer has a bounded, functional scope within the network architecture. Once the layering is broken, the luxury of designing a protocol in isolation is lost, and the cascade effect of any single design choice on the whole system needs to be considered.

Cross-layer design can create loops, and it is well known from Control Theory that stability then becomes a paramount issue. Compounding this is the fact that some interactions are not easily foreseen. Cross-layer design can thus potentially work at cross-purposes; the “law of unintended consequences” can take over if one is not careful, and a negative effect on system performance is possible.

In some circumstances the added complexity may be justifiable. This tenet expressly identifies the need to make sure the benefit outweighs the risk.

3.1.9 The network architecture should use modular constructs.

By using modular constructs, changes in one area of the architecture are isolated from changes in other areas. Modular design is generally considered a best commercial practice.

3.1.10 The core network architecture should be simple.

It is generally agreed that network complexity causes inefficiencies in interactions and data flow. We desire to improve the likelihood of network stability and reasonable performance by keeping things as simple as possible. The tenet of simplicity implies a number of things that we have elected to list as sub-tenets:

3.1.10.1 Tight coupling should be avoided

Tightly coupled systems have typically been designed for a specific set of end-to-end hardware. They optimise the performance of that hardware. They are systems of a monolithic nature rather than systems defined by standard interfaces. Such systems are often referred to as “stovepipes”. They have many interdependencies and severely limit choices. Changes in one component must often be reflected in many others. Such
systems tend to be the antithesis of “Open” systems. They are hard to understand and expensive to maintain.

3.1.10.2 The complexity of the network should be migrated to the edges – the transport should remain as simple as possible. Any function that can be accomplished in an end node should be left to that node.

Core functions exist in any network, even though there may not be a core wire line network. e.g. in a stub network, the radio contains the router which performs layer 3 functions. Other radio components have link and physical layer functions. Layer 4 and above functions are in the end device that accesses the radio.

We feel that it is inappropriate to require all core nodes to assume complexity that relates specifically to particular data types. Rather than create a core that is capable of dealing with many complexities, we believe it is more appropriate to push the data complexities to the edges where the particular data types meet the network. This avoids huge complexity in each core node by requiring each edge node to have sufficient complexity to deal with the problems for which it is responsible.

3.1.10.3 Per-flow state information should be kept in the end nodes.

Any connection/state-related protocols should be end-to-end related. The core network should not have per-flow state information complexity remembered by the network core.

When per-flow state information is kept within the network core, rather than at the ends, any change in topology can cause those flows to be interrupted and corrupted. Simplicity suggests that the nodes that care about it most keep this information – the end nodes.

The assumption that network core should not keep per flow information state and be simple and fast (by pushing complexity to edge nodes) implies that core should be dimensioned for the most demanding traffic conditions (e.g. by Capacity Over-provisioning).

3.1.10.4 The need for Gateways should be minimized – They should be pushed to the edge when they are necessary

Gateways provide the interface between the protocol requirements of the core and dedicated systems. Simplicity suggests that such interfaces should occur where the dedicated system meets the core (at the edge) rather than requiring all core nodes to have such capability.

3.1.10.5 Inter-working functions should be limited to encapsulation – done at the edge of the network

NCOIC has determined that it is important to address data-related complexities as close to the source as possible. This means keeping the core simple, and making the edge-nodes that know details about the data responsible for dealing with those details.
When non-IP data is to traverse the network, it should be encapsulated at the edge of the network and forwarded to the destination as encapsulated IP data.

3.1.10.6 **Intervention (modifying packets traversing the network in a manner that requires state information to follow the packet) should be avoided.**

We believe that added complexity is the primary mechanism that impedes efficient scaling, and is the primary driver of increases in both capital and operational expenditures. If intermediate nodes fail, or change, it is likely that state information will be lost. The loss of state information at intermediate points in the network will guarantee failure of the transport, and hence the usefulness of the network. State should only be maintained at end points so its destruction is only tied to the end point itself.

3.1.10.7 **Interaction between edge node and network core states should be minimized – The states should be orthogonal.**

This interaction violates the transparency of the network to the users – requiring knowledge of the network in order to make use of it.

3.1.11 **The network shall employ separate Control, Management, and Data Planes.**

Separation of Control, Management, and Data Planes minimizes the interaction between the edges and the network core. We believe that this is important because it conforms to the concept of modular design (previously advocated) and it tends to keep the architecture simple (another previously espoused goal).

In the Control Plane, devices communicate with each other to provide real-time control. In the Management Plane an external entity communicates with the devices in non-real-time. It may or may not have a person in the loop.

3.1.12 **The network should be capable of supporting a wide variety of applications and services, and not just be dedicated to a single application.**

The key to global connectivity is the inter-networking layer. The IP protocol was designed to be independent of any transmission medium or hardware addressing. This approach allows the network to exploit any new digital transmission technology of any kind, and to decouple its addressing mechanisms from that technology. It allows an IP network to be the easy way to interconnect fundamentally different transmission media, and to offer a single platform for a wide variety of Information Infrastructure applications and services.

This does not imply that network designers be unaware of the requirements of the applications/application classes that their networks are intended to support. It does imply that the underlying networks should be capable of supporting a wide variety of application classes – i.e. we are not addressing a single-application-dedicated network.
3.1.13 The network architecture should provide for a scalable network of networks, even though there may be limited scalability subset networks within it.

Scalability is generally desired. NCOIC advocates decisions that allow networks to grow to support more users, and to provide enough bandwidth for continual growth. We must design networks to grow into the networks we need in the future, rather than constrain us to live with networks of the past.

A network can be designed for a limited number of nodes due to network need, but this desire is to be explicit. It is important to identify the scalability limits of each network and the rationale for those limits.

Different types of networks have different types of scalability, i.e. Local Area Networks (LAN), Mobile Ad hoc Networks (MANET), Wide Area Networks (WAN). Both architects and requirements need to account for this.

3.1.14 The network should transparently protect information from malicious actions in transit.

Security impacts all three planes and is an overarching entity. Security is an integral part of the network that must be designed in rather than added on.

3.1.15 Local Optimization should depend only on local information.

We feel that the more events that simultaneously occur, the greater the likelihood that two or more will interact to produce an “unforeseen feature interaction.” We believe that small changes propagated across complex systems can result in unpredictable amplified interactions.

3.1.16 Any deviation from architectural principles should be reviewed, weighing the benefits against the costs of reduced interoperability.

We believe that there is always a fundamental tension between performance and architecture, and taking an architectural shortcut can often lead to a performance gain. Hence there always exists a temptation to violate the architecture. However, deviation from architectural principles introduces complexity and tighter coupling between components and layers and reduces interoperability. All such deviations should be considered carefully, with great weight given to the espoused architectural principles.

3.1.17 Implicit Assumptions should be avoided

The history of networking is replete with problems caused by implicit assumptions. Often these assumptions applied perfectly to the situation the designer was addressing, but not to the scenario in which it is later employed. When TCP was designed, it was assumed that any packet loss was due to network congestion, because the media was extremely reliable. When wireless networks are employed, the reliability of the media is changed by orders of magnitude and the assumption is no longer valid.
We know that follow-on users are often unaware of the original assumptions, and make assumptions of their own that compound the problem. This tenet simply states that assumptions we make in defining network architectures should be made explicit (and documented), so that they can be remembered, reviewed, and evaluated by future users of the recommendations.

3.2 Mobility Tenets

In addition to the standard IP architecture and Information Assurance tenets, the Mobile Networks Working Group has identified a set of tenets that are specific to mobile nodes and networks. Any mobile node or network architecture being considered should be measured against all three sets of tenets described in the MNE.

3.2.1 Network Architecture(s) with mobility must support both mobile and fixed infrastructures.

Mobility includes cases where mobile nodes attaching to fixed as well as cases where the infrastructure itself is moving. Any architecture claiming to be suitable for use as a mobile framework must be compatible with both fixed and moving network infrastructures.

3.2.2 Overarching mobility requirements and architecture(s) must be compatible with heterogeneous sub-networks. The overarching requirements must, therefore, be technology independent.

It is clear that within large mobile networks there is a significant likelihood that not all participants will have the same technology available. The overall architecture encompassing these diverse pockets must be designed to accommodate the diverse nature of such heterogeneous networks.

3.2.3 The mobility architecture(s) must support a broad range of network node kinematics. It must support mobile nodes moving over a wide range of speeds.

The potential use cases for mobile networks dictate that the network is able to deal with nodes that have very different dynamic behavior. Handheld nodes being carried by users will move at very different rates from airborne nodes. Mobile networks must be able to accommodate both sets of users.

3.2.4 Mobile networks can be self-forming. In this case, their dynamic configuration behavior must be autonomous and follow policy.

All networks require some initial configuration to set up the policies under which the networks will operate. Some classes of mobile networks may be able to be pre-configured, but many classes of mobile networks will require dynamic configuration. It is very important that this dynamic behavior of truly mobile networks not require manual
intervention. It must be handled within the mobile network in an autonomous way. This includes formation of the network and management of its potentially changing physical and logical topology. Such autonomous behaviour must follow the policies established during configuration.

3.2.5 The mobility architecture(s) must support a broad class of potential connectivity, including environments with links of varying capacity and potentially intermittent connectivity.

Mobile nodes will have varying capabilities. The links that interconnect these nodes will also have widely varying capacities and capabilities. There is significant potential that within the mobile infrastructure there will be intermittent connectivity with some nodes. The overall mobile architecture must support all of these.

3.2.6 Network management (overhead) traffic must be designed to maximize network availability for user traffic.

In many mobile environments, there is a need for significant network management traffic. It is important that this traffic not tie up all the resources and prevent user traffic from flowing. The goal in designing management traffic should be to maximize resources available for use by users, not to just minimize overhead traffic. If increasing the overhead traffic will result in an increase in resource availability for user traffic, this solution is preferred over the lower overhead solution.

3.2.7 Management of mobile networks and sub-networks must be complementary to and compatible with management and planning in the larger inter-network

Within a large network supporting mobility, there may be sub-networks using different technologies. Within these sub-networks, technology specific management techniques may be required. We feel that within technologies, common standards must be adopted. In the context of the larger inter-network, these sub-networks must be compatible with the standards for management and planning defined for the larger inter-network.

3.2.8 Users, nodes, networks, services, and information may move about freely with minimum impacts to functions and services during and after movement. Users and devices can be expected to move and interact both individually and as groups

Mobility can occur at all layers of the IP Reference model.

3.2.9 The underlying structure of the network should not be a limitation to mobility

3.2.10 Identity and address must be independent. Identity is associated, with a mobile node. Address is associated with a mobile node’s network attachment point

In fixed-infrastructure settings, it has become common to assume that the address of a workstation defines that workstation or is equivalent to its identity. In the mobile world,
it is likely that a node will assume different IP addresses, depending on its point of connectivity to the inter-network. It is this very assumption that allows the current routing architectures to scale beyond a few tens to hundreds of nodes in mobile networking environments. Hence, it is important that the concepts of address and identity be separated. It is necessary, however, that the current address and the identity be bound, either by dynamic or static means. Dynamic bindings are necessary in mobile networking environment to ensure this binding is current.

3.2.11 Mobile architecture(s) should provide services such as QoS, Information Assurance, and Network Management to mobile nodes and networks that are required

Network architectures that include mobile systems and/ mobile networks for mission deployments that provide merging network data solutions (i.e. real-time and non-real-time traffic) manifests criteria to prioritize traffic flows, secured traffic transactions, and managed traffic (i.e. FCAPS) for required network nodes.
4  Use Cases

The Mobile Networks Working Group will identify the mobility capabilities required by our customers and propose standards to provide these capabilities.

These capabilities will cover operational needs. These operational needs will be identified through typical use cases, which highlight elementary services to be provided in order to cover these operational needs.

Scenarios and uses cases are defined by the NCOIC FTs, by MN members, by organizations such as NATO, and by Integrated Project Teams. They are specifically defined in close cooperation with the NIF Architecture Concepts FT, as patterns are field proven canonical solutions to problems linked to scenarios in which the pattern is relevant. Net centric patterns using and adhering to net centric tenets (for example MN tenets) and principles can be then tailored and reused in different situations.

4.1  Coalition Defense use cases

Defense use cases will help to identify specific needs for defense missions, especially in the tactical environment.

Several general use cases related to defense mobility can be identified:

- Ad hoc mobility: moving nodes without predefined linkages
- Connected mobility: a group of nodes are moving together
- Disconnected mobility: a node or a network is changing its connections to other nodes or network.
- Service mobility: a service is moving from one location to another.

4.1.1  Mobility use cases

Each of the use cases involves all the communication layers, from physical to service layer. The initial state is “unconnected.” Two entities (generally networks, but could be individual nodes) will establish a connection and be able to interoperate at all levels.

This connection will take place in several steps:

1. Physical connection: manual setup (management action) or automatic discovery
2. Network connection: Agreement on parameters needed to exchange data (addressing plan, addresses of servers, routers…) and routing advertisement
3. Service connection: services of each entity are available to the other entity
4.1.1.1 Ad hoc mobility

In ad hoc mobility, the moving nodes and networks don’t need any external predefined infrastructure to communicate and have no particular dependence on any particular node. Nodes are able to join and leave the network or sub-network at will.

4.1.1.1.1 Sensor Field

A particular case of Ad hoc mobility is the sensor field, especially the micro-sensors that are spread over an area, also called “smart dust”. After being spread, the sensors have to organize into a network and must be able to establish a link to an entity that can collect the information. The entity is not necessarily continually present and generally mobile. The illustration could be an example of sensors attached to soldiers who are moving.
4.1.1.2 Connected Mobility

In connected mobility, nodes or networks move within the larger inter-network while remaining connected with a predefined network infrastructure.
4.1.1.3 **Disconnected mobility**

In disconnected mobility, the mobile nodes or networks do not preserve connectivity while moving; rather they are turned off and disconnected while moving to a new fixed location where they are then attached to a network with or without a predefined infrastructure.

![Disconnected Mobility Diagram]

**Figure 4-4: Disconnected mobility**

4.1.1.4 **Service mobility**

If users are mobile, services can also be mobile. This mobility must be transparent to the user, which means that the user doesn’t need to know where the service is located to use it.

Services can be of several types:

- Services offered by an entity (sensors, fire, information
- Services offered by people, especially Command Post (CP) services. Technically, it can be a simple phone number or mail address, or more complex software.

The three figures below show scenarios involving service mobility. Service mobility needs to accommodate unplanned changes of service location as well as service disruption due to changes of service location as illustrated in the figures below.

The first figure describes the unplanned switch between main and backup Command Posts (CP) after a severe problem preventing the main CP to continue its work. In this case, all the functions are transferred from the out of service main CP to the backup CP.
Figure 4-2: Unplanned switch between duplicated CP

The second figure describes the mobility of a duplicated CP. The goal is to change the CP location without service interruption, despite the fact that the CP mobility is a disconnected mobility. The principle is to move alternatively each CP while the other CP provides all the services.

To spare resources, the CP are not always full duplicated: in this case, only a part of the CP, called the “kernel” will be duplicated; when the functions are transferred to the alternate CP, the functions that are not duplicated must move physically to the other CP. During this move, the functions are not available,

Figure 4-3: Duplicated CP moving
4.1.2 IA use cases

The MNWG believe it is important to define IA Use Cases, but are not included in this section of MNE Issue-1. The content that follows is concepts that will be important for the Use Cases.

Defense applications have strong requirements concerning confidentiality of information. Different security domains are defined, and strongly partitioned. At least two criteria are used to define the security domains:

- Level of confidentiality (unclassified, restricted, confidential, secret, top secret),
- Ownership of information: nation, NATO, mission...

In order to access information in a security domain, a user must have the **right to know**. Inside a security domain, additional partitioning is generally defined, and right to know must be completed by a **need to know**.

Information exchanges between security domains are controlled. Exchange rules between levels of confidentiality are defined in the Bell-LaPadula document (MITRE). These rules are not sufficient to define allowed exchanges between nations: information must be explicitly tagged as “releasable to” in order to be transmitted from a nation to another.

4.1.3 QoS use cases

The MNWG believe it is important to define QoS Use Cases, but are not included in this section of MNE Issue-1. The content that follows are concepts that will be important for the Use Cases, yet they need further description.

The first need in defense networks is the voice service, and also possibly multimedia exchanges (video).

Other defense applications need also strong QoS:

- Collaborative actions, including Time Sensitive Targeting (TST),
- Sensor information, especially radar

In these use-cases it is often essential to have low delay, low jitter and that the required bandwidth is available. A resource constrained network will not be able to provide all services to all users. Mechanisms must then exist to assure that the appropriate services and flows of information are expedited in the best way possible.

The Mobile Network needs to be able to distinguish between different types of Quality of Service required by the Applications for the data transmitted: real time (latency constrain) or non real time data, prioritized data, data rate guaranteed, reliability...

**Specific QoS use cases**
Voice exchange (and other constrained data) is required inside a group of vehicles. This QoS should remain stable when the topology of the ad hoc network changes rapidly due to the movement of the vehicles.

### 4.2 Mobile Emergency Communications Interoperability (MECI) use cases

The MECI (also called Network Enabled Emergency Response (NEER)) use cases are quite similar to the tactical use cases, although some requirements are not so strong:

- Fewer IA requirements
  - No hostile people expected, at least for the first 72 hours:
  - No jamming expected

- Need to integrate existing local resources into communications network

MECI use cases cover short and middle-term scenarios:

- Emergency response in the first 72 hours after the disaster (report done)
- Emergency response post-72 hours after the disaster (to do)

#### 4.2.1 Deployment Architecture Example

The figure below illustrates a typical MECI architecture:

![Typical MECI Architecture](image)

**Figure 4-4: Typical MECI Architecture**
The first network scheme is a hierarchical scheme, with vehicles and people attached to one vehicle that provide them the connection to the network with Mobile Routers (MR) and Mobile Nodes and Networks (MNN)

This scheme can be enhanced to suppress the constraints:
- People don’t need direct connection to a vehicle,
- People are not attached to a unique vehicle,
- Vehicles organize themselves in a backbone network.
4.2.2 QoS Use Case

The MNWG believe it is important to define QoS Use Cases, but are not included in this section of MNE Issue-1. The content that follows are concepts that will be important for the Use Cases, yet they need further description.

The first operational need in a MECI deployment is the Voice communication, and possibly some multimedia communication (video).

Other applications requiring QoS could be:

- Remote medical applications (including electrocardiograms, remote surgery),
- Unmanned vehicles…

Users communicating are from different Communities of Interest (COI) like Emergency teams, Police, Army, Fire fighters…., with different organizations, procedures and hierarchy. So information transmission QoS requirements are similar to the requirements in tactical scenarios in terms of priority, reliability, real/non real time,
5 Evaluation of Standards

This section discusses approaches to evaluate proposed standards for their ability to support net centricity.

5.1 Evaluation Methods

The approaches planned for use by MNWG to evaluate the ability of proposed standards to support net-centricity include those specified in Table 5.1-1

<table>
<thead>
<tr>
<th>Approach</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use cases and requirements</td>
<td>Net centricity requirements and scenarios</td>
</tr>
<tr>
<td>IP Architecture tenets</td>
<td>Compiled / Developed by MNWG as guidance for IP architectures</td>
</tr>
<tr>
<td>Mobility tenets</td>
<td>Compiled / Developed by MNWG as guidance for mobile architectures</td>
</tr>
<tr>
<td>IA tenets</td>
<td>Compiled / Developed by MNWG as guidance for considering IA in system architectures</td>
</tr>
<tr>
<td>NCAT</td>
<td>NCOIC developed evaluation tool being used in joint NATO/NCOIC work</td>
</tr>
<tr>
<td>SCOPE</td>
<td>NCOIC developed tool</td>
</tr>
<tr>
<td>Net centric maturity levels</td>
<td>Developed by NATO</td>
</tr>
<tr>
<td>Net centric checklist</td>
<td>US Dept of Defense generated material</td>
</tr>
<tr>
<td>Support for legacy systems</td>
<td>Evaluate for ability to accommodate legacy systems and/or be compatible for legacy systems integration approaches</td>
</tr>
<tr>
<td>Programmatic Issues</td>
<td>Non-technical barriers to net-centricity</td>
</tr>
</tbody>
</table>

First the proposed standards will be evaluated against requirements and use cases from multiple environments, such as MECI, NATO, Sense and Respond Logistics, and other communities of interest. Supporting multiple scenarios and communities of interest are desired. However a standard may be more supportive of certain specialized environments. This does not exclude a candidate standard; however the specialized applicability must be noted.

Proposed standards will then be evaluated against the IP architecture, Mobility, and IA tenets. While the goal is to comply with the tenets, there may be some situations where a tenet is violated to provide needed capability. Tenet violations are to be supported with rigorous analysis and justification.
While we will use SCOPE and NCAT to perform standards evaluation, the results of our evaluation may likely provide new inputs to these models. The evaluation tools developed by NATO and the US DoD will be used to enable our proposed standards to be consistent with guidelines from our customers. Since there is a large investment in legacy non-IP based systems, the proposed standard needs to be evaluated for the ability to accommodate legacy systems and/or be compatible with legacy systems integration approaches.

The output of the above mentioned evaluations should provide insight into the proposed standard’s ability to support network-centricity from a technical standpoint. To determine if a standard is supportive of network-centricity from non-technical viewpoints, the proposed standards will be evaluated against the programmatic issues. This list may grow over time as other options are matured, our problem area work matures, and we gain experience performing evaluations. Potential future evaluation methods include Joint Force Command (JFCOM) Capabilities Portfolio Management, the ITU-T End User experience performance categories, and Swedish Defense Materiel Administration (FMV) results.

5.2 Foundational Standards

This section includes 1) foundational standards based on MNWG tenets, 2) standards for specific operational scenarios determined by NCOIC IPTs, and 3) MNWG problem area specific standards which are the result of the MNE work performed for that problem area. This section will evolve with additional spirals of the MNE work. For this spiral of the MNE, foundational standards and recommended standards from the MECI Phase 1 report are included. None of the standards have gone through the entire evaluation process as described in section 2.2. As the problem area work matures, standards will complete the evaluation process and be added to the table of recommended standards. Recommended standards are current standards; emerging standards will be listed separately as standards of interest.

In order to determine all three types of standards listed in the above paragraph, the capabilities to be provided are determined and then the standards for those capabilities are researched. A standard may be recommended because of common usage (empirical method), or based on evaluation (analysis, modeling & simulation, demonstration, or testing).

The recommended standards are NOT a minimum subset that all network devices must contain or support. Some legacy devices will not be IP-based. Some devices may not have sufficient size, weight, and power to support all the protocols. Some do not need the capabilities of those standards since their missions do not require them. If the device must provide the capability, then the recommended standard should be used, in order to promote interoperability.

Much work remains to be done in the identification, selection, and widespread adoption of communications interoperability standards. NCOIC and MNWG position is that interoperability is based on an IP-based inter-network, as indicated in our IP Architecture Tenets. These basic IP protocols make up the foundational standards.
# Appendix

## 6.1 Appendix A: Acronyms

This section defines acronyms used in this document.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AHN</td>
<td>Ad Hoc Network</td>
</tr>
<tr>
<td>AS</td>
<td>Autonomous System</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial Off the Shelf</td>
</tr>
<tr>
<td>DISA</td>
<td>Defense Information System Agency</td>
</tr>
<tr>
<td>DISRonline</td>
<td>Department of Defense (DoD) Information Technology Standards Registry, formerly Joint Technical Architecture (JTA)</td>
</tr>
<tr>
<td>FMV</td>
<td>Swedish Defense Materiel Administration</td>
</tr>
<tr>
<td>GIG</td>
<td>Global Information Grid</td>
</tr>
<tr>
<td>IA</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>INFOSEC</td>
<td>Information Security</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPT</td>
<td>Integrated Product Team</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>MANET</td>
<td>Mobile Ad Hoc Network</td>
</tr>
<tr>
<td>MECI</td>
<td>Mobile Emergency Communications Interoperability</td>
</tr>
<tr>
<td>MNE</td>
<td>Mobile Networking Evaluation</td>
</tr>
<tr>
<td>MNWG</td>
<td>Mobile Networking Working Group (NCOIC)</td>
</tr>
<tr>
<td>MNO</td>
<td>Mobile Networking Overview</td>
</tr>
<tr>
<td>MNN</td>
<td>Mobile Node and Network</td>
</tr>
<tr>
<td>MR</td>
<td>Mobile Router</td>
</tr>
<tr>
<td>NATO</td>
<td>North Atlantic Treaty Organization</td>
</tr>
<tr>
<td>NCAT</td>
<td>Network Centric Analysis Tool</td>
</tr>
<tr>
<td>NCID</td>
<td>Network-Centric Implementation Document/Directive (US DoD)</td>
</tr>
<tr>
<td>NCO</td>
<td>Network-Centric Operations</td>
</tr>
<tr>
<td>NCOIC</td>
<td>Network-Centric Operations Industry Consortium</td>
</tr>
<tr>
<td>NEER</td>
<td>Network Enabled Emergency Response</td>
</tr>
<tr>
<td>NIF</td>
<td>Network Interoperability Framework</td>
</tr>
<tr>
<td>NNM</td>
<td>Network and Node Mobility</td>
</tr>
<tr>
<td>NPM</td>
<td>Network Planning and Management</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>RFC</td>
<td>Request For Comments</td>
</tr>
<tr>
<td>ROU</td>
<td>Routing (MNWG problem area)</td>
</tr>
<tr>
<td>RT</td>
<td>Real Time</td>
</tr>
<tr>
<td>SCOPE</td>
<td>System Capability Operation Program Enterprise (NCOIC)</td>
</tr>
<tr>
<td>SOA</td>
<td>Service Oriented Architecture</td>
</tr>
<tr>
<td>SPAWAR</td>
<td>Space and Naval Warfare</td>
</tr>
<tr>
<td>STANAG</td>
<td>Standardization Agreement (NATO)</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TLP</td>
<td>Transport Layer Protocols</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over IP (Internet Protocol)</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>WG</td>
<td>Working Group</td>
</tr>
</tbody>
</table>
6.2 Appendix B: Glossary

This section defines terms used in this document. Standard definitions, where available, were used.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad hoc network</td>
<td>A self organizing network that is formed without external support, in which the devices are a part of the network for a temporary period, and there is no assumed infrastructure</td>
</tr>
<tr>
<td>Admission Control</td>
<td>It is responsible for comparing the resource requirement arising from the requested QoS levels against the available resources in the system. The decision as to whether a new request can be accommodated generally depends on system-wise resource management policies and resource availability</td>
</tr>
<tr>
<td>Authentication</td>
<td>It is a security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.</td>
</tr>
<tr>
<td>Availability (of information)</td>
<td>Timely and reliable access to information</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>The total width of the frequency band available to or used by a communications channel. Usually measured in Hertz (Hz). The bandwidth of a channel limits the available channel capacity.</td>
</tr>
<tr>
<td>Bandwidth utilization</td>
<td>The actual rate of information transfer achieved over a link, expressed as a percentage of the theoretical maximum channel capacity on that link, according to Shannon’s Law.</td>
</tr>
<tr>
<td>Buffer Management</td>
<td>The control of buffer/queue sizes and deciding which packets to drop when overloads occur</td>
</tr>
<tr>
<td>Call Control</td>
<td>Establishes, modifies, and terminates sessions (e.g., multimedia conferences). It can also invite participants to existing sessions, such as multicast conferences. [Referred to as Application Layer Control Protocol in RFC 3261]</td>
</tr>
<tr>
<td>Communications Layers</td>
<td>Layers 1-4 of the Internet Reference Model. This includes the Physical Layer, Data Link Layer, Network Layer, and the Transport Layer</td>
</tr>
<tr>
<td>Confidentiality (of information)</td>
<td>The property that information possesses when it is only made available to, or shared with, authorized individuals, processes, or devices</td>
</tr>
<tr>
<td>Control plane</td>
<td>Provides for signaling and set-up functions for the system. Example functions include call set-up, call termination.</td>
</tr>
<tr>
<td>Core</td>
<td>Major arterial networks carrying high volumes of traffic. A core network typically interconnects multiple lower-speed networks together. This usually involves very high-speed connections and geographically long links. (Reference Cisco Routing Glossary)</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Core routing</td>
<td>Forwarding of packets through the core, which is a network or group of networks that provide transit services. See Core</td>
</tr>
<tr>
<td>Data Plane</td>
<td>Defines the Configuration, Startup Conditions, and Instability Conditions of the data traffic including the traffic, collection of network elements, links between network elements, and interface profile. The purpose of this plane is to provide the ability to forward data packets</td>
</tr>
<tr>
<td>Datagram</td>
<td>A packet which contains enough information in the header to allow the network to forward it to the destination independently of previous or future datagrams</td>
</tr>
<tr>
<td>Domain</td>
<td>1) A set of network resources for a group of users; 2) a sphere of knowledge; 3) a set of network addresses; 4) network(s) under the control of a single administrative authority. (Ref. WhatIs.com)</td>
</tr>
<tr>
<td>Edge Network</td>
<td>An edge network is where users are directly connected and their data aggregated into the network core. This is where user-specific services and policies are enabled such as quality of service. (Reference Cisco Routing Glossary)</td>
</tr>
<tr>
<td>Edge routing</td>
<td>Forwarding of packets through an edge network, i.e. from a border router to the nodes within a local network</td>
</tr>
<tr>
<td>End-to-end</td>
<td>From the source host to the destination host</td>
</tr>
<tr>
<td>First responders</td>
<td>Those emergency workers who are first on the scene after a natural or man-made disaster or emergency situation has occurred</td>
</tr>
<tr>
<td>Fixed infrastructure</td>
<td>Interconnected fundamental structural elements of a network that are not capable of mobility which provide the framework for transporting information</td>
</tr>
<tr>
<td>Functional Model</td>
<td>A functional model is the management tool for grasping the entirety of &quot;what we do&quot;, eliminating redundant or superfluous work, anticipating what the enterprise will need to do in the future, and defining/designing changes of &quot;what we do&quot;.</td>
</tr>
<tr>
<td>Global Mobility:</td>
<td>Global mobility includes the movement of nodes or an entire network from one Internet IP address space to another IP address space while maintaining connectivity to nodes with which it is communicating.</td>
</tr>
<tr>
<td>Heterogeneous Network</td>
<td>A collection of nodes of different manufacturer’s products or technologies that can exchange data</td>
</tr>
<tr>
<td>Information Assurance</td>
<td>All aspects of safeguarding and protecting information, networks, and data</td>
</tr>
<tr>
<td>Integrity (of information)</td>
<td>The property that information possesses when it is current, accurate, and complete (e.g., is not accidentally or maliciously modified or destroyed)</td>
</tr>
<tr>
<td>Inter-domain</td>
<td>Between domains</td>
</tr>
<tr>
<td>Intra-domain</td>
<td>Within a domain</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
- Application Layer  
- Transport Layer  
- Internet Protocol Layer  
- Link Layer  
- Physical Layer |
<p>| Local Mobility:              | Local mobility references the movement of nodes within a local area network or within a mobile Ad hoc network and the peer-2-peer topology changes for node-to-node communications within that local network. Local Mobility can impact layers 1-5 and applications and these impacts must be part of the analysis for Local Mobility operations. |
| Management plane             | Performs management functions for the system, and also coordinates the other planes (data, control, services). The following are example workflows for the MP: login/logout, configure network elements, generate billing details. (Ref. “Security and the Management Plane Part 2”, Stephen Davis) |
| Mesh Network                 | A network where all the nodes can connect to each other. This rich connectivity allows inexpensive peer network nodes to supply back haul services to other nodes in the same network. It effectively extends a network by sharing access to higher cost network infrastructure. Mesh networks are self-healing: the network can still operate even when a node breaks down or a connection goes bad. As a result, a very reliable network is formed. This concept is applicable to wireless networks, wired networks, and software interaction. (Ref. Wikipedia) |
| Mobile Ad hoc Network (MANET) | Self-configuring network of mobile nodes connected by wireless links, not dependent on any infrastructure, that form an arbitrary, changing, and unpredictable topology. |
| Mobile Network               | An entire network, moving as a unit, which dynamically changes its point of attachment to a serving network, and thus its reachability in the topology. A mobile network may be composed of fixed and/or mobile nodes |</p>
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Node</td>
<td>A simple or complex device whose location and point of attachment to the network may change</td>
</tr>
<tr>
<td>Mobility:</td>
<td>A quality or capability of nodes, which permits them to move from place to place while retaining the ability to fulfill their primary mission. Users must be continuously connected to the network while on the move, in any terrain, throughout the three dimensions of space, in all environmental conditions, and through all phases of the operational continuum. The network will seamlessly maintain connectivity during “hand-off” from one layer to another, utilizing the most efficient communications path while on the move.</td>
</tr>
<tr>
<td>Multicast</td>
<td>Communication between a single sender and multiple receivers on a network (Reference WhatIs.com)</td>
</tr>
<tr>
<td>Multi-homing</td>
<td>With heterogeneous nature of networks in a wireless mobile network, multi-homing is necessary with connection capability of satellite, UAV, MANET, legacy waveforms</td>
</tr>
<tr>
<td>Murky</td>
<td>Fluid, indistinct</td>
</tr>
<tr>
<td>Network</td>
<td>A group of computing devices connected together to share information or resources.</td>
</tr>
<tr>
<td>Network centric</td>
<td>Capability of a node, system, component to easily and seamlessly connect with other nodes, systems, components to share information leading to increased situational awareness and easier accomplishment of individual and group goals</td>
</tr>
<tr>
<td>Network Core</td>
<td>Core functions exist in any network, even though there may not be a core wireline network. e.g. in a stub network, the radio contains the router which performs layer 3 functions. Other radio components have link and physical layer functions. Layer 4 and above functions are in the end device that accesses the radio.</td>
</tr>
<tr>
<td>Network Infrastructure</td>
<td>The physical hardware used to interconnect computers and users. This includes transmission media, such as telephone lines, cable television lines, satellites and antennas, and also the routers, aggregators, repeaters, and other devices that control transmission paths. Infrastructure also includes the software used to send, receive, and manage the signals that are transmitted (Ref WhatIs.com)</td>
</tr>
<tr>
<td>Network Planning and</td>
<td>Execution of the set of functions required for controlling, planning, allocating, deploying, coordinating, and monitoring the resources of a network. This includes such functions as initial network planning, frequency allocation, cryptographic key distribution, configuration management, fault management, security management, accounting management, performance management. A large number of protocols exist to support network and network device management. Common protocols include SNMP and NETCONF. (Ref Wikipedia)</td>
</tr>
<tr>
<td>Management</td>
<td>Node</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>It is an assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.</td>
</tr>
<tr>
<td>Packet</td>
<td>Fundamental unit of information organized in a standard way with a header followed by the data.</td>
</tr>
<tr>
<td>Policy based management</td>
<td>An administrative approach that is used to simplify the management of a network by establishing operating rules (i.e. policies) to deal with situations those are likely to occur. These operating rules can be used to control access to and priorities for the use of network resources (Ref. WhatIs.com)</td>
</tr>
<tr>
<td>Provisioning</td>
<td>Set up, allocation, and configuration of hardware, software, and services in order to provide capability to customers.</td>
</tr>
<tr>
<td>Quality of Service (QoS)</td>
<td>The collective effect of service performances which determine the degree of satisfaction of a user of the service (Reference: ITU-T Y.101 Global Information Infrastructure terminology: Terms and definitions) Characteristics such as bandwidth, latency, and jitter that describe a network's ability to customize the treatment of specific classes of data. For example, QoS can be used to prioritize video transmissions over Web-browsing traffic. Advanced networks can offer greater control over how data traffic is classified into classes and greater flexibility as to how the treatment of that traffic is differentiated from other traffic. (Reference WhatIS.com)</td>
</tr>
<tr>
<td>Routing</td>
<td>Selecting of paths in a computer network along which to send data. Routing directs forwarding, the passing of logically addressed packets from their source toward their destination through intermediary nodes, i.e. routers. (Ref Wikipedia)</td>
</tr>
<tr>
<td>Scalability</td>
<td>The ability of a network to operate properly with an arbitrarily large number of participants.</td>
</tr>
<tr>
<td>Self-forming</td>
<td>For a network to be self-forming, it must autonomously perform all of the functions necessary to establish the connectivity between nodes and to establish routes within the formed network and possibly to the wider network through points of attachment.</td>
</tr>
<tr>
<td>Self-healing</td>
<td>Self-healing implies that packets within the network will find their way to their destination (if a path exists) even in the face of changing network topologies. It also implies that if a network requires a special set of services to maintain itself, there is a mechanism to continue those services even if the original provider is unexpectedly removed from the network.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Service oriented architecture</td>
<td>A methodology and framework for documenting enterprise capabilities. SOAs comprise loosely coupled, highly interoperable application services. These services interoperate based on a formal definition independent of the underlying platform and programming language. (Ref. Wikipedia)</td>
</tr>
<tr>
<td>Topology</td>
<td>The notion of an internetwork’s physical structure, e.g. who is connected to whom.</td>
</tr>
<tr>
<td>Transport</td>
<td>Movement of data through one or more networks</td>
</tr>
<tr>
<td>Use case</td>
<td>A technique for capturing requirements. Each use case provides one or more scenarios that convey how the system should interact with the end user or another system to achieve a specific goal. Use cases are typically in the language of the end user. (Ref. Wikipedia)</td>
</tr>
<tr>
<td>Wireless Network</td>
<td>A collection of nodes connected through wireless (RF) links</td>
</tr>
</tbody>
</table>
6.3 Appendix C: Contributors

The following have contributed to the development and production of this document.

Barry Hobbs – DataPath
Bonnie Gorsic – The Boeing Company
Carl Renmarker – Saab
Dave Brown – DISA, US DoD
Dennis Pulsipher – L3 Communications
Dimitrios Hatzipapafotiou – Lockheed Martin Corporation
Hans Åkermark – Saab
Harold Zheng – John Hopkins University (Applied Physics Laboratory)
Herve Jamet – Thales
Jim Bound – Hewlett Packard
Marty Egan – Lockheed Martin Corporation
Paul Schweitzer – Lockheed Martin Corporation
Randy Yates – Northrop Grumman Corporation
Sherry Wang – John Hopkins University (Applied Physics Laboratory)
Torsten Griem – The Boeing Company
Walter Legrand – EADS
Xi Jiang – John Hopkins University (Applied Physics Laboratory)

6.4 Appendix D: References

The references in this document listed below use a convention as follows. Each section or problem area providing references uses a three letter abbreviation, such as NNM for Network and Node Mobility, appropriate for the section. References in that section are then incrementally referred to as NNM-1, NNM-2, etc. References are grouped according to the abbreviation.

<table>
<thead>
<tr>
<th>Document ID</th>
<th>Document Information</th>
<th>Author</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>TEN-1</td>
<td>University of Illinois ay Urbana – Champaign, IEEE Wireless Communications: A CAUTIONARY PERSPECTIVE ON CROSS-LAYER DESIGN</td>
<td>Vikas Kawadia, BBN Technologies, P. R. Kumar</td>
<td>2005-02</td>
</tr>
</tbody>
</table>
---|---|---
TEN-4 | RFC 3439: Some Internet Architectural Guidelines and Philosophy | RFC | 2002-12
TEN-6 | IETF-66, Montréal, Canada [tsvarea-6.pdf]: Improving the Interactions Between Transport & Network Mechanisms | Lars Eggert, Magnus Westerlund and Jari Arkko
TEN-7 | ACIRI/ICSI [handley-wireless.pdf]: On Interlayer Assumptions (A View from the Transport Area) | Mark Handley
TEN-8 | IPAM Tutorial USC Information Sciences Institute Marina del Rey, CA [cntut_1494.pdf]: Architectural Principles of the Internet | Bob Braden | 2002-03
TEN-10 | RFC 817, MIT Laboratory for Computer Science, Computer Systems and Communications Group: MODULARITY AND EFFICIENCY IN PROTOCOL IMPLEMENTATION | David D. Clark | 1982-07
STD-1 | [MECI-P1]: Findings and Recommendations for Mobile Emergency Communications Interoperability | NCOIC | 2007