# Resolving Tactical Network Management Interoperability by Using Ontology

*John R. Schneider*

## ABSTRACT

*In the tactical domain, there are many instances in which disparate or geographically dispersed network management systems are unable to share network information electronically. When information exchanges do exist, they often rely mostly on person-to-person communications or on specific point-to-point electronic interfaces between network management systems. There is no common implementation of network management systems across the tactical domain. Each system performs network management functions by using its own information semantics and structures. Because each system is implemented independently, it is difficult to exchange information among systems. Ontology technology and mediation and transformation processing are known techniques that can significantly improve interoperability among network management systems. Ontology technology enables a common and universal exchange of network information while allowing each system to continue doing its usual business. Ontology technology is implemented by wrapping native network management systems, thereby allowing information to be exchanged with any participating management system. Ontology is widely used in the commercial environment and could enhance interoperability within the tactical domain. The Johns Hopkins University Applied Physics Laboratory (APL) is developing an ontology-based network management model for use in the tactical domain and is building a reference implementation demonstrating the interoperability that can be achieved with ontology.*

## INTRODUCTION

In a tactical environment, each armed service (e.g., Army, Navy, Marines, and Air Force) typically plans, acquires, implements, and operates various communication systems to meet its specific needs. At the communications level (as opposed to the management level), many tactical communication systems can directly interoperate with each other or can indirectly interoperate via gateways designed to interconnect disparate systems. Management systems used to plan, provision, deploy, configure, operate, control, and monitor these communication systems are typically provided with the communication systems. In general, each network management system (NMS) is tailored for the specific underlying communication system. That is, the business functions and information semantics for performing network management are unique to the communica-

tion system being managed; although the communication systems may be interoperable, the NMSs are not. For communications to cross from one system to another or to cross multiple systems, effective overall, or end-to-end, network management is required. In the tactical domain, network management among the various communication systems is typically achieved via human interaction, with little to no electronic interoperability. This lack of interoperability exists primarily because each NMS performs its management by using the business functions and information semantics for the system it manages, without regard for the need to share or exchange network information with other NMSs.

The interoperability of NMSs is negatively impacted further when joint task forces are established to perform joint operations. A joint operations area consists of land, sea, and airspace defined by a geographic combatant command or a subordinate unified command conducting military operations to accomplish a specific mission. A typical joint tactical operational mission begins with sea forces transitioning to land-based operations. The forces' communication systems are interconnected via the Joint Aerial Layer Network, a communication satellite, or both. The deployed environment has access to several applications, data stores, and computing resources and interconnects with coalition forces. The deployed environment also interconnects with the strategic enterprise environment, typically within the United States, to access various applications, data stores, and computing resources. Some characteristics of a joint operations mission include the following:

- The joint task force commander may be assigned from any one of the armed services.
- Multiple service components from the armed services operate in the mission.
- The operations may have short or long durations.
- The operations may include on-the-move and fixed resources.

In addition, joint operations usually include communications with coalition forces and reachback communications to the continental United States, and the communication services may adapt or change during the mission. As a consequence, joint operations require agile and effective network management.

## TACTICAL COMMUNICATIONS/NETWORK MANAGEMENT CONTEXT

Communications among interconnecting devices implement a protocol stack in accordance with the Open Systems Interconnection basic reference model.[1] Figure 1 illustrates two devices communicating with each other. The physical communication path uses some media (e.g., wire/cable or RF) to interconnect the physical layer component of the protocol stack in each device. Depending on the device type (e.g., computer, router, or modem), one or more upper layers of the protocol stack are implemented. A peer-to-peer communication relationship is established between same layers of the protocol stack. The figure illustrates that each layer of the protocol stack within each device may be managed using a network element layer. The network element layer enables a local or remote manager to configure and monitor the status and performance of each implemented layer.

Within the network management domain, managers are arranged in hierarchical and peer-to-peer relationships. The arrangement of network managers is in accordance with the Telecommunications Management

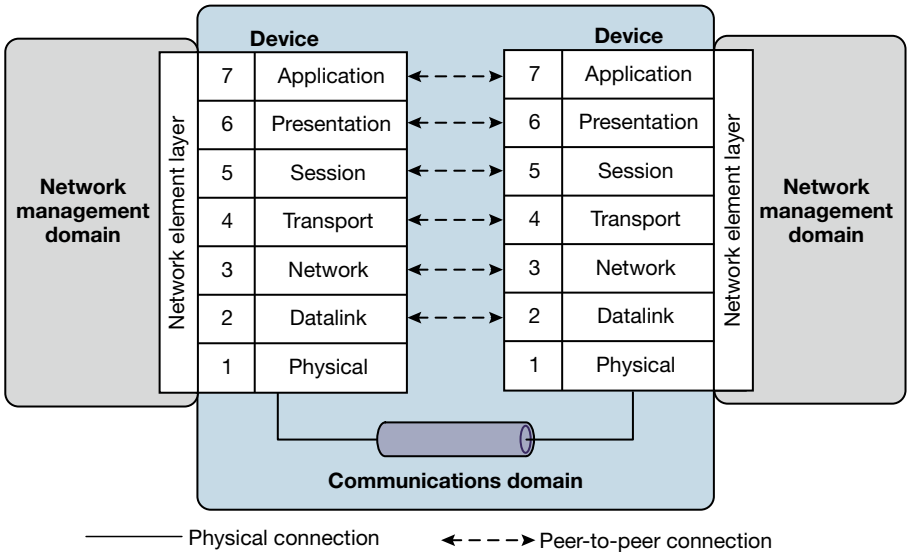


**Figure 1.** Communications devices with network management interfaces.

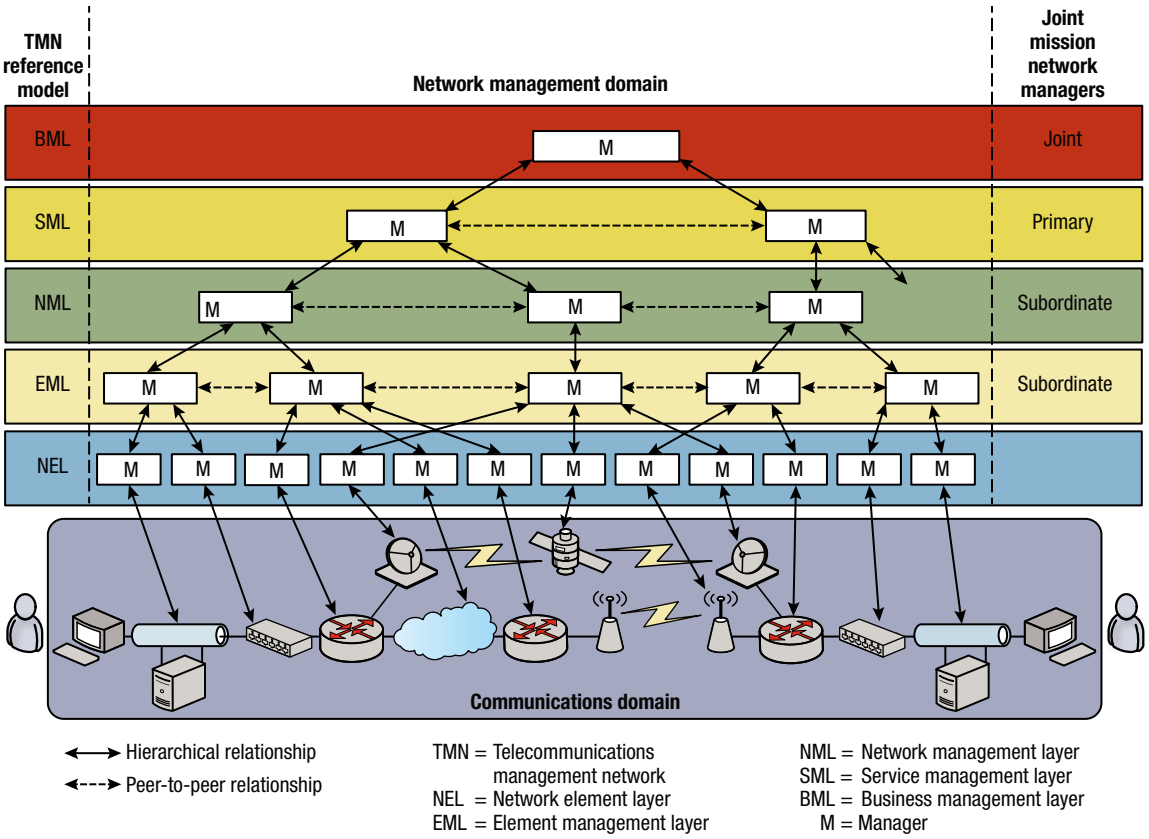


**Figure 2.** Overview of network management domains.

Network (TMN) reference architecture and guiding principles.[2] Figure 2 illustrates the network manager arrangement and identifies the types of network managers (i.e., joint, primary, and subordinate) within a joint tactical mission and the joint tactical mission network manager's relationship to the TMN. The interoperability areas of concern are the hierarchical and peer-to-peer relationships among the joint, primary, and subordinate managers that are implementing the element management layer, network management layer, service management layer, and business management layer of the TMN.

A subordinate network manager is a specialized set of network management functions performed in support of a primary network manager. The subordinate network manager focuses on managing one or more of the specific network resources providing the communications service within a subcomponent command. A primary network manager performs a set of network management functions at the highest level of a subcomponent command supporting a joint task force mission. The primary network manager is responsible for the following tasks:

- providing and assuring subcomponent network readiness, security, and performance to support the mission
- overseeing planning, coordination, and network resource and network traffic priority management
- gathering, fusing, and sharing situational awareness
- troubleshooting and resolving network events and security incidents across all networks operating within the subcomponent command purview

Examples of primary network managers are an Army Division G6 and a Brigade S6. Similarly, the joint network manager performs a set of network management functions at the joint task force J6 position in a joint operations area to plan, coordinate, and manage network resources and traffic priorities; maintain situational awareness; and assess availability, performance, and security of all network resources critical to the mission of the joint task force.

Although external information/management systems (not shown in the figure) perform a set of network management functions outside the purview of the joint task force J6 and the joint operations area, they are critical to the mission. The external systems provide important assets (such as frequency allocations and cryptographic key assignments) needed to plan, deploy, and operate tactical resources and may provide other communications resources (such as satellite communications) required as part of an end-to-end communication service.

## COMMUNICATIONS/NETWORK CONTEXT

Information exchanges among the various joint task force network managers address planning, scheduling, provisioning, deployment, monitoring, topology, resource assignment, up/down status, performance, congestion, failures, security incidents, and policy compliance, at a minimum. These information exchanges deal with the overall health and use of the resources providing communication services for the joint tactical users. These resources may be arranged in various types of networks with network-to-network interconnections via direct connections or via gateways. The resources are managed by the various participants in the joint tactical environment (e.g., the joint, primary, and subordinate managers operated by the service components—Army, Navy, Air Force, and Marines).

Figure 3 illustrates the basic components of an operational network—the fundamental building blocks supporting end-to-end communications within the tactical environment. The underlying component is the infrastructure providing the physical and organizational resources needed to transport information from a user to other users in the network. Four frameworks provide the infrastructure: IP network, radio network, space/air layer network, and terrestrial network. In addition to providing basic transport capabilities, each infrastructure framework may provide required encryption, routing, firewalls/guards, virus detection/removal, and intrusion detection capabilities. A subordinate network manager manages each infrastructure framework. Network services, commonly provided by a network provider, are provided in addition to the infrastructure. Sample network services include voice, data, messaging (e.g., e-mail), chat, and virtual private network. An operational network may also provide mission-specific application services to users within the network. Sample application services may include command and

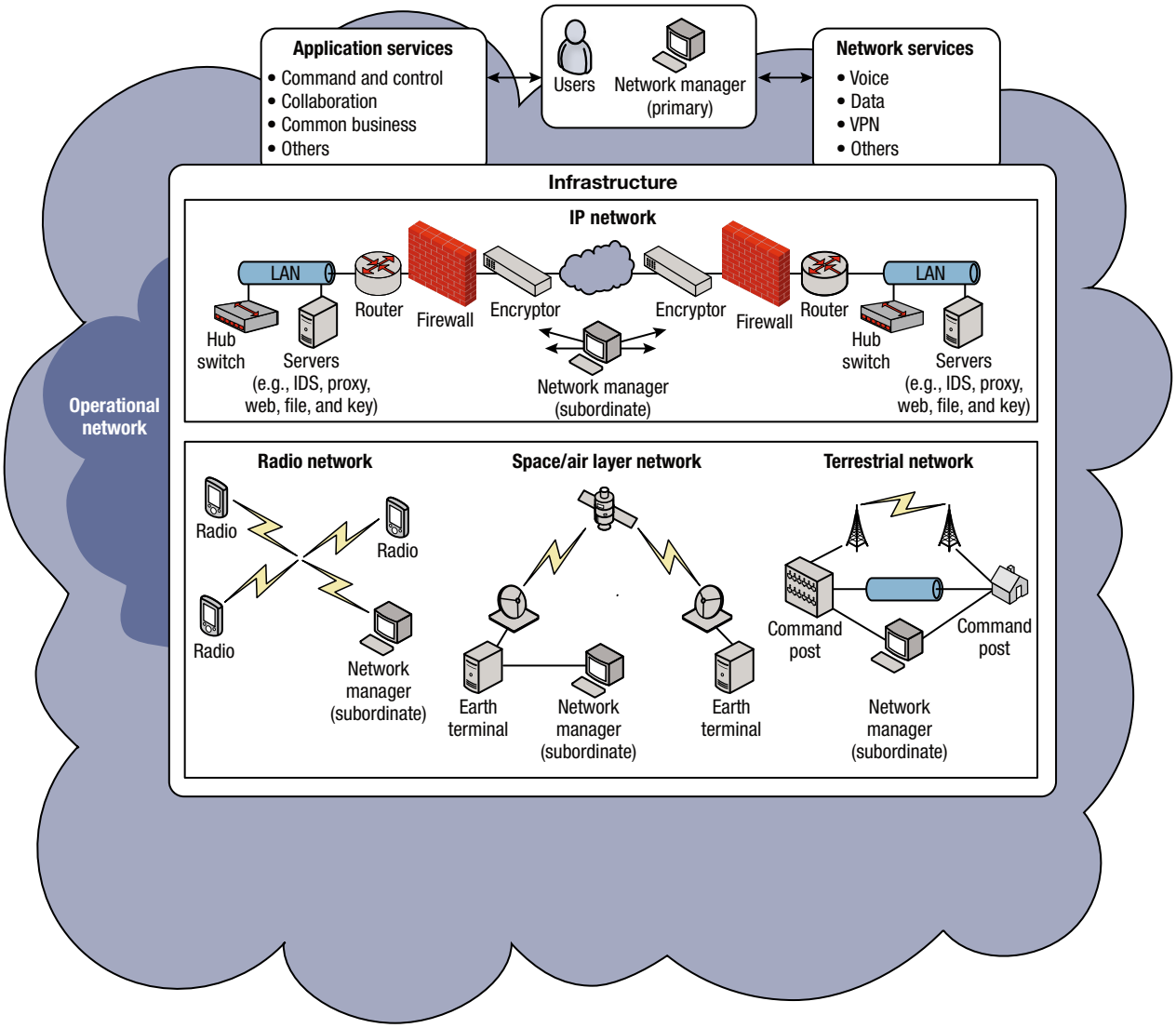


**Figure 3.** Operational networks. LAN, local area network; IDS, Informix Dynamic Server.

control, collaboration, intelligence, business processes, and informational capabilities (e.g., weather information). All services within an operational network are available to all users within the network and may be available to external users depending on the rights and privileges assigned to external users. Typically the network manager for an operational network is a primary network manager.

Operational networks support end-to-end communications for users within the network. They are interconnected to form larger networks supporting many users. Figure 4 illustrates the use of interconnected operational networks in the joint tactical environment. Within a particular service domain (e.g., Army, Air Force, Navy, or Marines), one or more operational networks may interconnect via an internal gateway. The service domain provides a primary network manager to operate and maintain the interconnected networks. Service domains may also interconnect via an internal gateway (e.g., internal because the networks are part of the joint domain). A joint network manager manages the joint domain, which is the aggregation of all interconnected service domain networks. The joint domain may also communicate with external domains that would interconnect using an external gateway. External domains may be allied/coalition networks and could reach back to continental United States networks. Depending on the rights and privileges assigned to users in the gateways and operational networks, end-to-end communication service is provided to users.

## INTEROPERABILITY APPROACHES FOR NMSs FOR THE JOINT TACTICAL ENVIRONMENT

NMSs in the joint tactical environment are generally specific to the underlying communication resources they are managing. Each system implements the network management functions and underlying information in accordance with the resource needs. Although these systems manage the resources efficiently and effectively

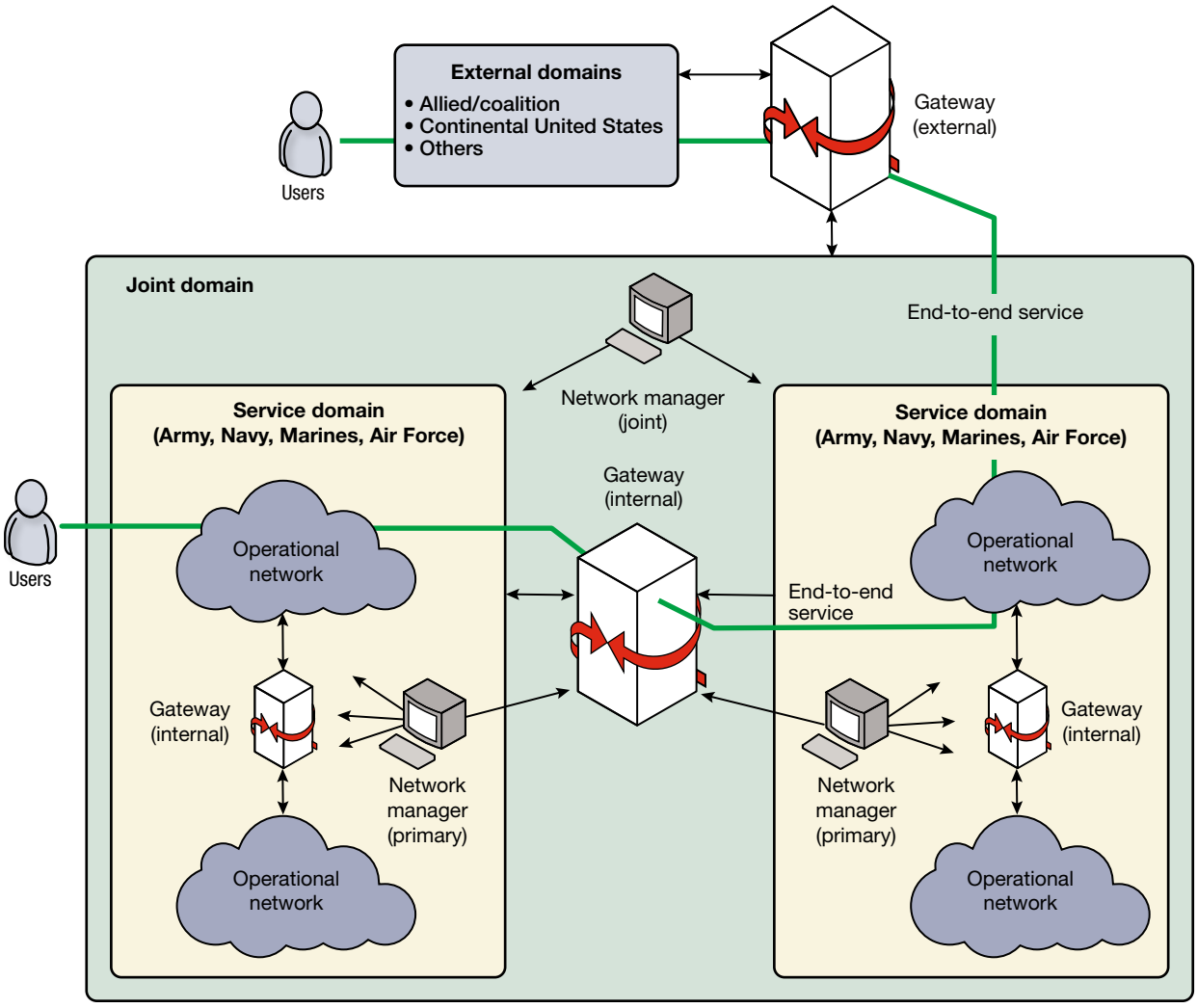


**Figure 4.** End-to-end communication service.

and provide network managers with information they are accustomed to receiving, they have not been designed to share information with other management systems. This is especially evident when the multiple management systems are designed for different communication resources (e.g., a communication satellite system versus a terrestrial radio network). The concern with sharing information among disparate NMSs is that each NMS's underlying information has semantics and structure unique to the resources the system is managing. The system's processes and data are generally implemented to satisfy a particular network manager and its needs (e.g., the Army may perform network management differently from the other armed services). In addition, if several systems use a similar network management function, there is no guarantee that the function in one system can interoperate with a similar function in another. For example, trouble ticketing functions are common functions of NMSs. Although several NMSs might use the same trouble ticket system, each NMS can configure the trouble ticket system to perform specific business processes and speak its information language. Thus, one system might define a trouble ticket as an *incident report*, a *trouble ticket*, or a *trouble event*, whereas another system may use one of these terms or something else entirely. Similarly, the content of a trouble ticket may be configured and formatted differently within the various systems (e.g., representation of a date and time may be different). The end result is that sharing information among various NMSs is difficult.

Traditional approaches for providing interoperability have been tried with varying degrees of success. One basic approach is relatively straightforward but is costly to implement, operate, and maintain. This approach provides interoperability as a specific interchange between two cooperating NMSs. While it is not difficult to implement the electronic interface, difficulty arises when the semantics are different. In this case, one of the NMSs needs to provide a translator in the form of a wrapper between its semantics and the semantics required by the other system, or one NMS must modify its internal system to use the appropriate semantics. This approach requires significant development and implementation effort before the system can be deployed in the field. This approach works fairly well when there are few systems in the environment. It is affordable to provide the information exchanges on a pair-by-pair interface. However, the maintenance of the interchange can become expensive and time consuming depending on the number of paired interfaces. Connecting each NMS with each other system ultimately becomes an M × N interface problem. The paired interface does not scale well when more than a handful of systems exist and information needs to flow among all the systems. In addition, the information exchange can consume considerable communications bandwidth when the systems need to share information in a fully connected mesh network. Communications bandwidth is a precious commodity in the tactical environment. A joint tactical force is typically implemented for a specific mission and the NMSs of the joint tactical force most likely are not the same systems for each mission. With the paired interface approach, it is necessary to ensure that there is a translator or that system modifications are made for each possible combination of NMSs.

Another approach has also been tried, again with mixed results. This approach is a variant of the pairwise translator approach described above. In this approach, instead of implementing the translator as a paired interface, a universal translator is available across the enterprise and each NMS has an independent interface with it. This approach is similar to the paired interface concept except all translators are in a central location. The key advantages of this approach are that the individual management systems are not impacted (i.e., multiple modifications to individual programs are not needed) and operation and maintenance of the universal translator is simpler and, to some degree, less expensive. However, the disadvantages outweigh the advantages and include the following:

- The universal translator becomes a single point of failure (i.e., all interoperability ceases when the translator is unavailable).
- The translator does not scale well (i.e., many translators are needed to handle each interconnection of systems).
- The translator is fairly rigid and is not easily adaptable to change (i.e., interoperability remains a paired implementation depending on specific and unique semantic transformations from one system to another).

Another implementation following this approach uses a common data model with transformation adapters for each interface with a NMS. The data model is independent of each NMS's data. Each interconnection with a NMS contains a transformation function that essentially performs mapping and mediation. Mapping references the individual system's data elements to the data model elements and can be straightforward or complex depending on the data semantics in each system. Mediation can be performed for the interface whereby simple modifications to the system's data can be performed so that the data can be mapped to the model (e.g., units of measurement can be changed to match the units specified in the model).

## ONTOLOGY OVERVIEW

One approach to resolving interoperability is an ontology. Ontologies have been used in the commercial

environment but are new to the DoD. Ontologies are used widely for Internet web search engines (e.g., semantic search), providing a rich and robust way to discover information on the Internet. In addition, there are several instantiations of ontologies that provide interoperability among various business enterprises.[3] The ontology approach is an enhanced implementation of the data model approach. The Johns Hopkins University Applied Physics Laboratory (APL) is applying the ontology approach to the development of a network management model to identify and define the information exchanged among the NMSs.

Ontology is a shared conceptualization of a domain of interest.[4] Ontologies have many uses and purposes including

- sharing common understanding of the structure of information among people or software agents;
- formalizing a shared viewpoint of information (e.g., agreement on how to model dates and times);
- providing a global means to retrieve information that isolates the retrieval from the underlying system's handling of information;
- reusing domain knowledge;
- defining domain assumptions;
- separating domain knowledge from operational knowledge (e.g., enhancing separate development and maintenance of component ontologies); and
- supporting reasoning on (and expansion of) the information.[5]

Ontologies enhance interoperability between systems that have been developed independently and that may use different languages and information representation. Some uses of ontology include

- neutral authoring (e.g., creating an information artifact and distributing it to multiple targeted systems, resulting in knowledge reuse, maintainability, and long-term retention);
- creating specifications (e.g., using ontologies to define information and interfaces, resulting in knowledge reuse, good documentation, reliability, and maintenance);
- providing common access to information (e.g., providing shared understanding of the terms, definitions, and structure of information, supporting interoperability and knowledge reuse); and
- providing enhanced search capabilities.

Basic elements of ontologies are classes, object properties, data properties, assertions (axioms), and rules.[6, 7] Classes identify and define specific resources (e.g., a person, location, equipment, or network service) and are often arranged in hierarchies (e.g., a class contains subclasses), with lower-level classes inheriting the properties and attributes of higher-level classes. Object properties define the relationships among the individual members (i.e., instances) of classes (e.g., a person named Joe is responsible for the equipment earth terminal). Similar to classes, object properties may be defined in an object property hierarchy with inheritance. Object properties are defined as various types and further refine how a class member is related to another class member. Object property types are symmetric (e.g., if John isFriendOf Jane, then Jane isFriendOf John), functional (e.g., Joe hasBirthDate 20110123), transitive (e.g., If Ohio isPartOf US and US isPartOf North America, then Ohio isPartOf North America), and inverse (e.g., If Maryland hasCapital Baltimore, then Baltimore isCapitalOf Maryland). Data properties identify and define attributes associated with class members (e.g., a class member named Joe has a LastName "Smith"). Data properties may be defined in a hierarchical fashion with inheritance. Reasoning, or inferencing, is supported via Horn (IF-THEN) rules that may be applied to class members and properties to allow inferring new information from the details defined in the ontology. An example of reasoning is if X isType AcademicDepartment and X hasFacultyMember Y and Y isMemberOfGraduateField Z, then X hasAssociateGraduateField Z.

APL has developed tactical network management ontologies with conceptual implementations as illustrated in Fig. 5. The ontology models are modularly designed with various information areas developed with individual namespaces (i.e., each information area is specified using a single namespace). These individual ontologies reuse industry-available ontologies (such as those in the Internet Engineering Task Force Management Information Bases and Distributed Management Task Force, Inc.'s Common Information Model) when practical. Some of the namespaces are Actor (e.g., defining people and resource agents), Resource (e.g., defining hardware, software, firmware, spectrum, and cryptographic material), Network (e.g., defining the composition of various networks), Service (e.g., defining the communication, application, and network services), and Location (e.g., defining places with addresses and coordinates). These namespaces can include various properties such as dates and times, statuses, and life cycle phases (e.g., planned/scheduled, approved, being implemented, and in operations). An integrating model is also created whereby all the individual namespaces are imported and equivalences and more complex cross-module properties are defined.

Users and applications that need to store and/or retrieve information interact via the SPARQL (Simple Protocol and RDF Query Language) Protocol and RDF

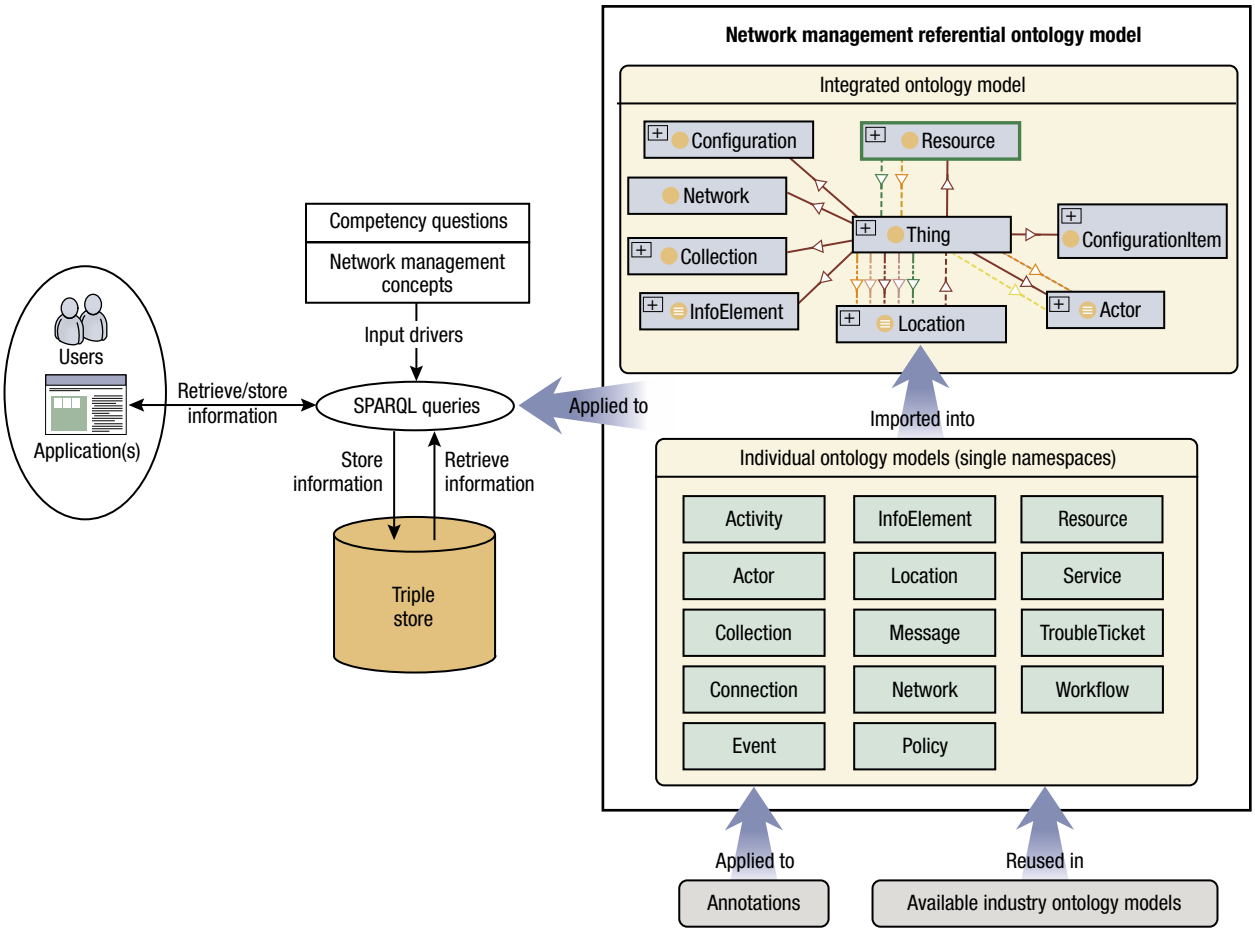


**Figure 5.** Conceptual ontology implementation for tactical network management.

(Resource Description Framework) Query Language.[8,9] SPARQL queries and updates exchange information with any database (such as a triple store or even a relational database) implementing a SPARQL endpoint. The ontology model or models define the specific details of the SPARQL queries, either generically requesting all the instances of a particular class (e.g., requesting all individuals of equipment type router) or requesting information related to a specific individual as defined by its object and data properties.

The basic data constructs of a triple store database and SPARQL are the subjects, predicates, and objects of triples. A triple can be thought of as a simple English sentence consisting of a noun (the subject), a verb (the predicate), and another noun or attribute (the object). The subject is always an individual of some class (type), and the object is either another individual or a data value. When the object is another individual, then the predicate is an object property (e.g., Actor Joe isServiceDeskRepresentativeFor TroubleTicket X). When the object is a data value, then the predicate is a data property (e.g., Service hasPlannedStartDate 20140215). Each part of the triple is assigned a specific identifier or uniform resource identification (URI). The triple approach, along with URIs, allows easy storing of information. Data are represented in graphs that fully express the complete interrelationships of the triples.

Implementing an ontology model is different than using a relational data model. The latter requires information to fit into the tabular and columnar structure of the underlying relational data store. Triples simply link individuals (as URIs) to other individuals or to data values. SPARQL queries simply follow a graph according to the predicates defined in the ontology models. For example, a user might want to know the start dates and service representatives for all active trouble tickets. To find this information, the following SPARQL query could be written (where the namespaces of the predicate URIs are shortened to use prefixes only):

```
SELECT ?ticket ?rep ?startDate WHERE {
        ?ticket rdf type troubleTicket:TroubleTicket.
        ?ticket network:hasStatus 'Active'.
        ?rep troubleTicket:hasServiceDeskRepresen
        tativeFor ?ticket.
        ?ticket troubleTicket hasPlannedStartDate
        ?startDate.}
```

SPARQL queries can be constructed as needed and are locally planned (optimized) by the triple stores. Standard queries are typically represented as competency questions, which are also used in the development of the ontology model(s). Competency questions represent the kinds of things that a user or application wants to know about or needs in order to store the information (e.g., what are the resources supporting mission X and communication service Y?). Competency questions include the network management concepts that must be represented within the management domain (e.g., an end-to-end communication service for a user may use underlying, or component, communication services like an infrastructure trunk).

Figure 6 illustrates the implementation of a traditional entity-relationship-type data storage and use versus the ontology approach. Characteristics of the traditional approach include

- *a priori* established associations among data elements or resources;
- resources that are uniquely identified within a context but not necessarily across an enterprise;
- rules and/or reasoning that are left for an application to define and implement; and
- rules and/or reasoning that accomplish the same thing across applications but are structured inconsistently.

Similarly, characteristics of ontology include

- multiple and rich associations among data elements or resources;
- resources that are uniquely identified;
- associations that can be dynamically established with resources in different or distributed ontologies;
- efficient rules and/or reasoning across the enterprise;
- simple management of the rules and/or reasoning; and
- consistent rules and/or reasoning across the applications.

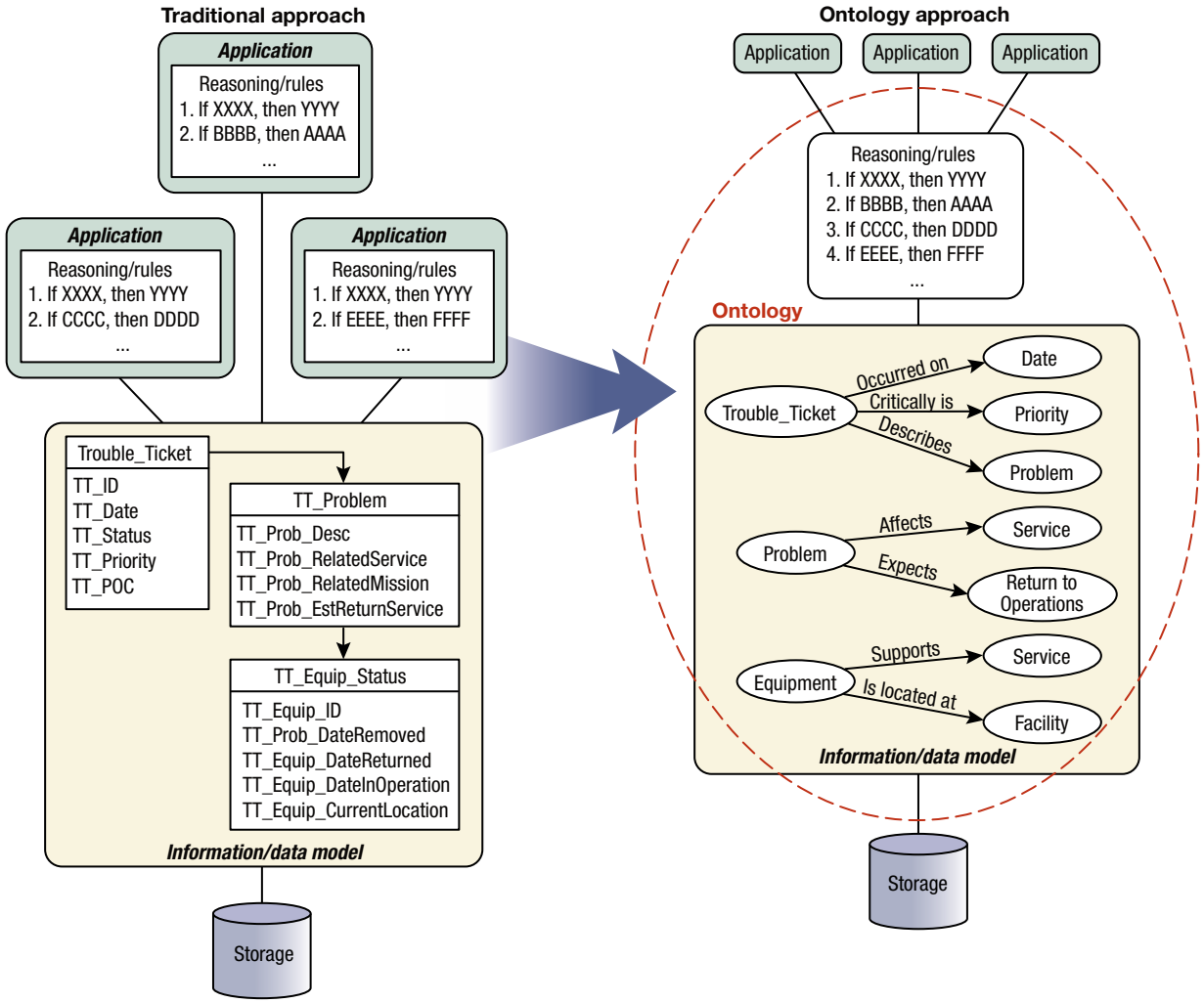


**Figure 6.** Traditional versus ontology approaches.

## NETWORK INFORMATION EXCHANGE CONCEPT USING ONTOLOGY APPROACH

A network management ontology model identifies and defines information elements expected to be exchanged among all network managers in the joint tactical environment as well as those expected to be exchanged with network managers external to the environment. The model represents the common understanding and reasoning structure for the information exchange. The intent is to allow each network manager to internally implement its network management functions by using its own method for doing business. However, when internal network management information is exchanged with other network managers, then the information exchanged conforms to the ontology model at the network manager's interface point. If the network manager does not adopt the ontology model for its internal use, then the network manager must transform or mediate its information into the structure and contents conforming to the model.

Figure 7 illustrates the implementation of the ontology approach to support interoperability among systems. The implementation uses a distributed concept whereby each system contains elements of the model. Each system contains its native NMS as well as ontology elements

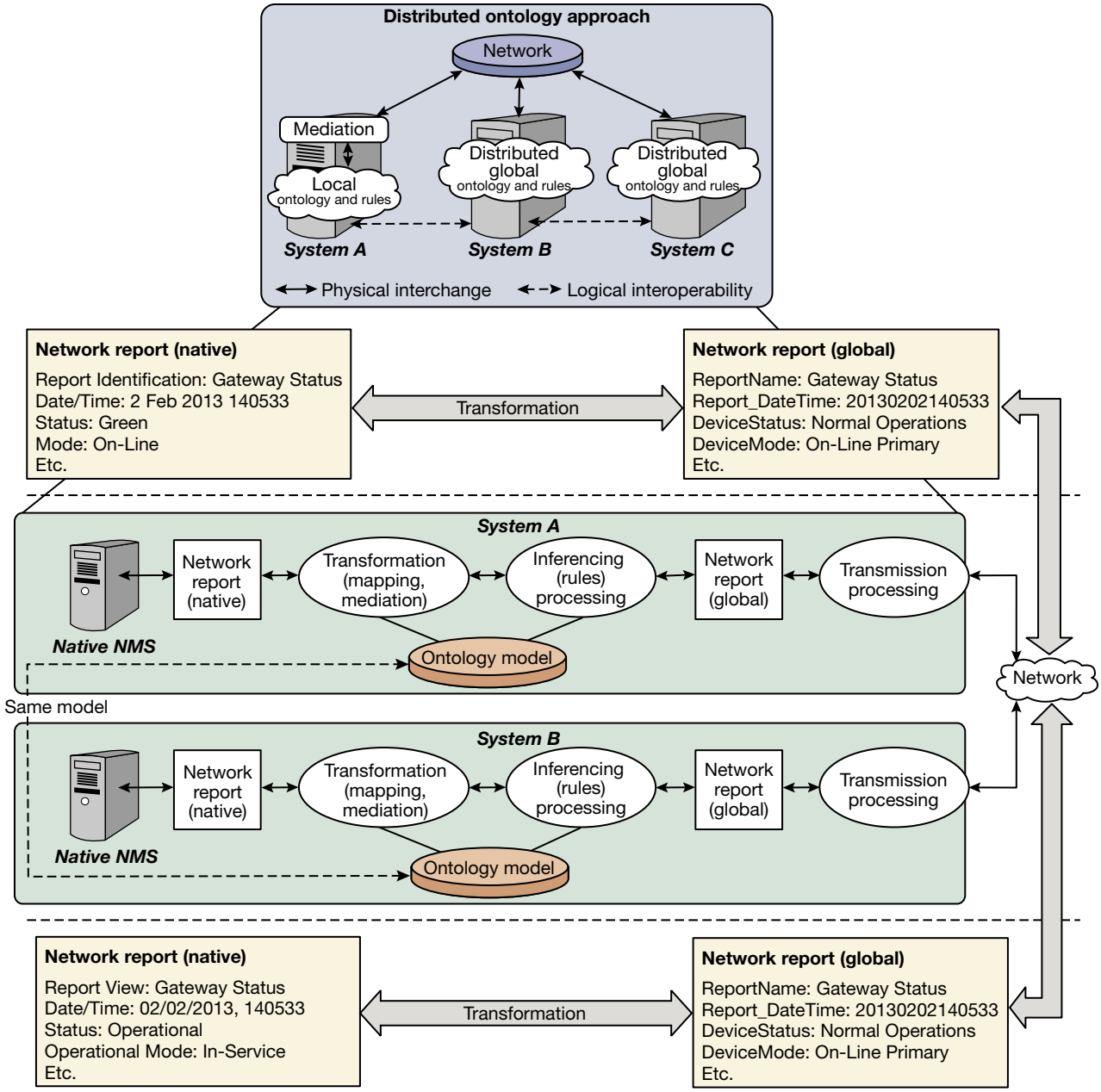


**Figure 7.** Example network report information exchange using ontology.

supporting transformation (or mapping/mediation) to the common ontology model, inference processing (or rule processing), and transmission (SPARQL) processing. The figure illustrates how a native NMS provides its network report, which is then transformed into the common global network report for transmission. At the receiving system, the global network report is transformed into the network report needed by the receiving system's native NMS. The figure shows portions of a network report to demonstrate how information is exchanged between systems using different formats and syntax. For example, one NMS may use the status Green to indicate equipment status, whereas the receiving NMS may use Operational. The ontology approach allows these NMSs to share information because both Green and Operational are mapped to the ontology's Normal Operations.

Although a global information model is expected to manage the exchanged information, the intent is not to make each NMS-to-NMS interoperability area enforce the model in its entirety. Therefore, it is anticipated that each interoperability area may be tailored in the sense that each area may select all or portions of the model to use at the NMS interface point.

Figure 8 illustrates the concept that network management information can be tailored to individual interoperability areas while conforming to the common global network management ontology model. The ontology model is a logical description and definition of the network management information, and portions are allocated to the various interoperability areas via a subscription service. A NMS providing information for exchange with one or more other NMSs registers the information categories and information items that will be present at the NMS's interface point. Another NMS wishing to receive information from the providing NMS queries for the provider's registration and selects (within the subscription service) those categories and items it would like to receive. The providing NMS then has the capability to construct the information exchange in accordance with the receiving NMS's desires. The exchange can occur in two ways: (*i*) the providing NMS may send individual messages to each receiving NMS, or (*ii*) the providing NMS may send a group message containing all needed information and the receiving NMS performs a filter on the message in accordance with the selection made. In the first case, the providing NMS manages the receiving NMS selections, whereas in the second case the receiving NMS manages its selections. The choice between the two cases can affect network performance (e.g., number of messages sent, throughput consumed, and message processing).

It is important to note that although the subscription service allows exchanged information to be tailored for each interoperability area, the ontology model still must

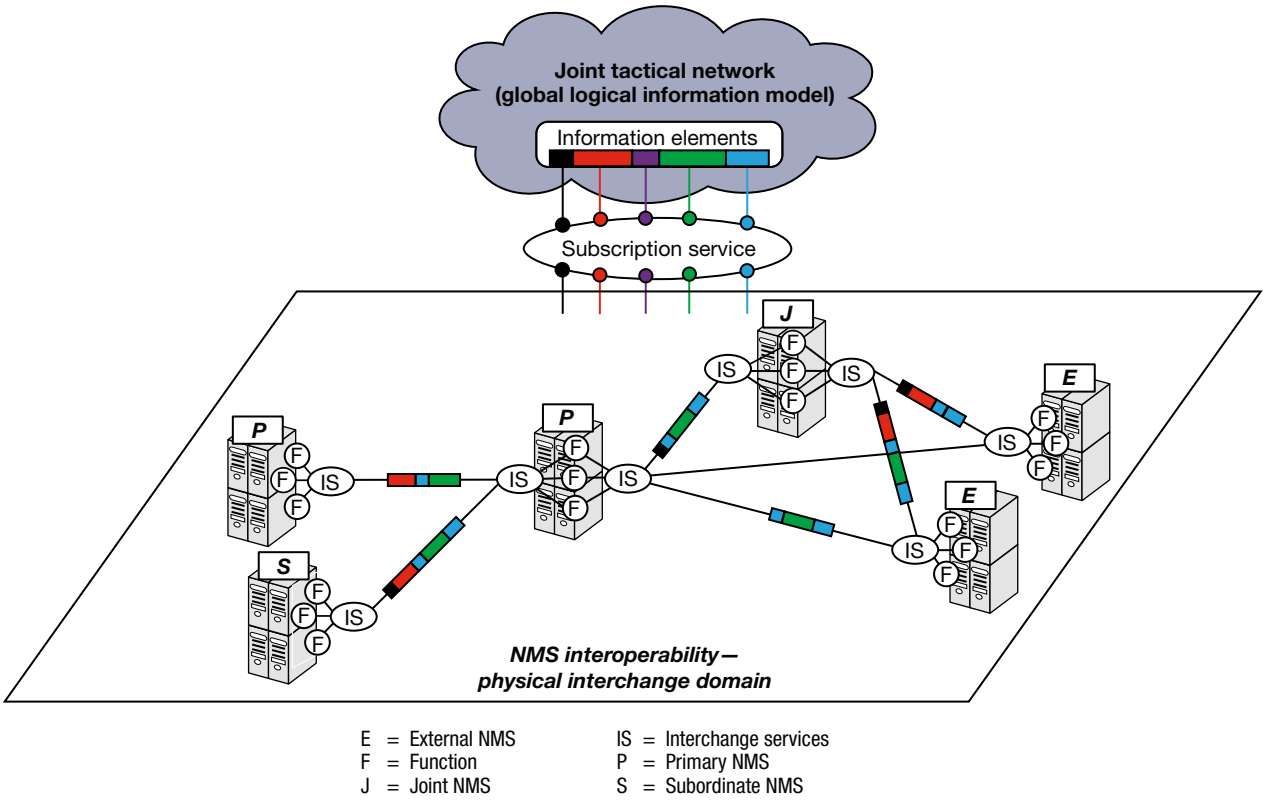


**Figure 8.** NMS information exchange.

identify all information that is available for exchange. This enables a better overall management of the definition and permits NMSs to provide or subscribe to standard (e.g., mapped/mediated) information.

## CURRENT AND NEXT STEPS

APL is continuing to expand the network management ontology model to ensure representation of all network management information expected to be exchanged in the joint tactical environment. APL is also generating Global Information Grid Technical Profiles (GTPs) that are approved and managed by the Defense Information Systems Agency. GTPs are high-level guidance documents defining standards and interoperability compliance requirements to support net-centric information technology exchanges within the DoD. GTPs are anticipated to be implemented via appropriate program requirements for acquiring or modifying information technology systems. For the joint tactical environment, seven GTPs have been identified for NMS interoperability: network requirements, resource allocation, provisioning and configuration, synchronization and verification, network situational awareness, security policy, and trouble tickets. These GTPs cover the full life cycle of the mission: planning and engineering, deployment and provisioning, operations and management, and disestablishment. APL has submitted the network requirements, resource allocation, situational awareness, and trouble ticket GTPs to the Defense Information Systems Agency for approval, and the trouble ticket and situational awareness GTPs have been approved. The remaining GTPs will be submitted by the middle of FY2015. Each GTP is based on and supported by the ontology approach.

In parallel with developing GTPs, APL is also developing a reference implementation (RI) using the ontology approach. The RI is intended to serve as a validation tool to assess interoperability compliance of NMSs before they are deployed to the field. One component under development is a reference system, which uses the ontology to store internal information and to exchange information. It contains an internal NMS and provides web services to perform the information exchange. A second component under development is an intelligent wrapper that includes the ontology and transformation and mediation processing as well as web services to provide information exchange. This intelligent wrapper is an add-on to existing NMSs. A third component under development is a translation wrapper with web services. This translation wrapper is intended to support NMSs that have adopted ontology for internal use; it adapts the native system's ontology to the ontology needed for information exchange. An initial RI has been created for the trouble ticket GTP. APL staff tested the RI within a laboratory environment and provided demonstrations to the joint tactical community during the Joint Users Interoperability Communications Exercise (JUICE) in the summer of 2014. The exercise provided a realistic tactical environment in which existing and soon-to-be-deployed new systems were evaluated to assess the effectiveness of their interoperability for communication services as well as for network management. The exercise also provided an exceptional opportunity for APL attendees to assess the ontology approach and to fine-tune the RI. APL staff are currently upgrading the RI to include the lessons learned during the exercise and the network situational awareness GTP.

## CONCLUDING REMARKS

Sharing network management information in the commercial industry is a daunting effort and has been achieved to some degree and with mixed results. In today's joint tactical environment, network information is primarily shared manually (e.g., manager-to-manager phone calls, text messages, and hard copies of forms). Several approaches to enhancing interoperability by using electronic interfaces and interactions have been attempted with some success. Each approach has advantages and disadvantages, but, overall, network management interoperability is still a challenge within the agile and dynamic joint tactical environment. The use of ontology to provide a common understanding of information, independently of the underlying NMS's information semantics and structures, shows much promise in enabling NMSs to interoperate. APL is developing a network management information exchange model based on the ontology approach. In addition, APL is generating GTPs to provide guidance on the implementation of network management services to achieve interoperability by using ontology. And, finally, APL is implementing a RI based on ontology to serve as a validation tool for NMS's conformance and compliance with the GTPs.

**ACKNOWLEDGMENTS:** I thank the following APL staff members for their overall support and assistance in the preparation of this paper: Sitaram Kowtha, Xi Jiang, Jack O'Donnel, and Frank Weiskopf. I also thank Andrea Westerinen of Nine Points Solutions, LLC for overall assistance and support of ontology technology.

### REFERENCES

[1]International Standard ISO/IEC 7498-1, *Information Technology—Open Systems Interconnection—Basic Reference Model: The Basic Model*, ISO/IEC, Geneva (15 Nov 1994).

[2]ITU-T M.3010, *Series M: TMN and Network Maintenance: International Transmission Systems, Telephone Circuits, Telegraphy, Facsimile and Leased Circuits—Telecommunications Management Network, Principles for a Telecommunications Management Network*, International Telecommunication Union, Geneva (Feb 2000).

[3]ISO 15926-1:2004, *Industrial Automation Systems and Integration—Integration of Life-Cycle Data for Process Plants Including Oil and Gas Production Facilities—Part 1: Overview and Fundamental Principles*, International Organization for Standardization, Geneva (1 Jul 2004).
[4]Gruber, T., "Ontology," *Encyclopedia of Database Systems*, L. Liu and M. Tamer Özsu (eds.), Springer-Verlag (2009).
[5]López de Vergara, J. E., Villagrá, V. A., and Berrocal, J., "Semantic Management: Advantages of Using an Ontology-Based Management Information Meta-Model," in *Proc. HP Openview University Association Ninth Plenary Workshop* (HP-OVUA 2002), distributed videoconference (11–13 Jun 2002).
[6]Antoniou, G., and van Harmelen, F., *A Semantic Web Primer*, 2nd Ed., MIT Press, Cambridge (2008).
[7]Allemang, D., and Hendler, J., *Semantic Web for the Working Ontologist—Effective Modeling in RDFS and OWL*, 2nd Ed., Elsevier, Waltham (2011).
[8]Harris, S., and Seaborne, A. (eds.), *SPARQL 1.1 Query Language: W3C Recommendation* (21 Mar 2013), http://www.w3.org/TR/sparql11-query/.
[9]Brickley, D., and Guha, R. V. (eds.), *RDF Schema 1.1: W3C Recommendation* (25 Feb 2014), http://www.w3.org/TR/rdf-schema/.

## THE AUTHOR

**John R. Schneider** is a Senior Professional Staff member within the Communication and Networking Systems Group of the Asymmetric Operations Sector. Since joining APL in 1996, he has performed as a project manager, group chief engineer, and lead systems engineer. He is experienced with network management and information systems; satellite command, control, and data processing; and satellite communications management. His skills include systems engineering within a full project life cycle, information/data modeling, information and data management, telecommunications, network technology, and project management. His e-mail address is john.schneider@jhuapl.edu.