ARMY RESEARCH LABORATORY

Management of Tactical Ad Hoc Networks With C2 Data Models

by John H. Brand and George W. Hartwig

ARL-TR-2784

July 2002

20020828 037

Army Research Laboratory
Aberdeen Proving Ground, MD 21005-5067

ARL-TR-2784 **July 2002**

Management of Tactical Ad Hoc Networks With C2 Data Models

John H. Brand and George W. Hartwig
Computational and Information Sciences Directorate, ARL

Abstract

The U.S. Army Research Laboratory is investigating the exploitation of preloaded reference data to solve problems in tactical network management. By closely evaluating how communication networks are described in tactical database models such as the Joint Common Database (JCDB), information about the tactical situation can be used to help direct, or at least refine, the process of reconfiguring ad hoc networks. Because the structure of current networks closely follows organizational structures, the concept of Default Operational Organizations (DOO) is being used as a starting point for the evaluation. The DOO concept will be used to address the problem of managing internet protocol addresses in rapidly changing ad hoc organizations to minimize overhead traffic on congested, low-capacity networks. Reducing network loading and improving network response are very important to network centric weapon systems such as the Future Combat System. Based on the data needs for network management, modifications to the IDEF1X database model representing the JCDB are proposed. A working model of an Access database based on a limited, notional test database using these modifications is described.

This study has produced suggested modifications to the existing JCDB-DM that will enhance the ability to rapidly configure networks with reduced network management overhead.

Acknowledgments

The authors wish to extend thanks to Dr. Sam Chamberlain for conceiving the project and for crucial guidance and insight during the course of the study. Thanks are also due to the Army Office of the Deputy Chief of Staff for Programs for initial funding in FY 2000.

INTENTIONALLY LEFT BLANK.

Table of Contents

INTENTIONALLY LEFT BLANK.

List of Figures

INTENTIONALLY LEFT BLANK.

List of Tables

INTENTIONALLY LEFT BLANK.

1. Introduction

The U.S. Army Research Laboratory (ARL) is investigating the use of preloaded reference data for solving problems in tactical network management. A tactical database, such as the Joint Common Database (JCDB), contains information about the tactical situation that can be used to guide the reconfiguration of ad hoc networks. Because the structure of current networks closely follows organizational structure, the concept of Default Operational Organizations (DOO) [1] is used as a starting point for this study. The DOO concept will be used to address the problem of managing internet protocol (IP) addresses in rapidly changing ad hoc organizations while minimizing overhead traffic on congested or low-capacity networks.

This investigation implements the concept of enterprise identifiers (EIDs)* in the management of network data within the JCDB by using unique organizational enterprise identifiers (orgEIDs). The network management data can thus be linked to tactical situational awareness data and operational plans and orders. Proposed modifications to the JCDB Data Model (JCDB-DM), the IDEF1X [2] data model associated with the JCDB, have been developed to accommodate network management data and to relate the data to ad hoc and default organizations. A working model of the proposed database design has been developed using the Microsoft Access database management system. It was populated with notional trial data and exercised with simple network data management tools.

After examination of the JCDB-DM, issues were identified in the following areas:

- datalink (hardware) addresses,
- IP address mapping,
- IP address prefix-network relationship,
- unitary IP address,
- definition of work,
- physical component basis of a network,
- hostnames and domain names,
- e-mail addresses, and
- routing.

In this report, we address each of these points and propose suggested modifications to the data model so that when the database is used to plan and execute maneuver and logistic operations; network management data is naturally produced.

*For more information on what EIDs are and why they should be used, see the article by Lonigro [3]. For a more extensive tutorial on enterprise identifiers, see the series of articles by Johnston [4]–[9].

2. Background

The DOO methodology uses universally unique integers as EIDs to identify the components of the military command structure. These are called orgEIDs. OrgEIDs are numerically unrelated; for example, each platoon's number is random, though unique. Thus, two organizations, such as platoons in the same company, may have very different numbers. Likewise, two companies in the same battalion may share a closely related unit identification code (UIC) but have very different, unrelated orgEID numbers. These orgEID numbers are used as keys in a data model as described by the IDEF1X methodology. By building on this process, all other entities (such as network components) can also be guaranteed unique identifiers. Since the orgEID is universally unique, concatenating a second locally unique number also guarantees a universally unique identifier. This allows data associated with arbitrarily large numbers of things to be tracked and manipulated.

As a starting point for this analysis, both the data model for the JCDB-DM version 4.3 and the Core Architecture Data Model (CADM) version 2.0. [10] were examined. The JCDB-DM was perceived by the authors as having data structures that would need fewer modifications to meet our requirements. It should be noted, however, that both the JCDB-DM and the CADM are living documents and are constantly being refined and updated. It is the expectation of the authors that the modifications proposed for the JCDB-DM could be equally well applied to the CADM. The network-related information in the CADM is described in Appendix A.

When units are attached or placed under control of another unit, traditional hierarchical numbering systems are confused; arbitrary identifications are unaffected. By reference to the EIDs, information may be quickly and easily obtained from a database on such matters as organizational relationships, mission, operational plans, and logistic data.

The problem of networked communication is difficult; each communicating entity on a network has identifiers based on the network, users, an arbitrary hostname, and machine address. Several protocols exist for adding and deleting subscribers and resolving the address problems in a network that work well in an office network environment where communications channels typically equal or exceed 10 Mbps.

An example of such a protocol for assigning IP addresses dynamically is the dynamic host configuration protocol (DHCP) [11]. DHCP requires considerable back-and-forth traffic between a new station and the server controlling the allocation of addresses. In an office environment, this overhead is unimportant. In a tactical environment, two factors are present that are not usually found in the office environment: fast and unpredictable realignments of individuals and subnets and small capacity communication channels already loaded with time-sensitive traffic. The "pipes" found in communication channels at the forward areas may range from less than 1 to 10 Kbps rather than the office environment of 10 Mbps and up [12]. Reducing the overhead load on those channels is highly desirable.

An example of this overhead may make this clearer. A company may have 20–40 radios [13]. The DHCP employs four message types: DISCOVER, OFFER, REQUEST, and ACK. Not counting options, these may total 8000 bits [14]. This means that assuming 40 radios in a company net as much as 320 Kb of traffic just to assign IP addresses. Assuming a throughput of 1 Kbps, and neglecting things like lockout for voice traffic, option fields, and collisions, this amounts to 320 s of traffic just to assign new IP addresses in this company. The addresses are moreover leased for a definite time period, though that can be set arbitrarily large. Partway through the lease period, the renegotiation begins, potentially adding yet more overhead.

Thus, use of protocols such as the DHCP, with its stream of discover and acknowledgment messages, can load a slow net in a fast-moving environment. This is compounded by the overhead added to each message exchange from other protocols, such as X.25 for transmissions over the mobile subscriber equipment (MSE) cellular radio net. Added to that is the fact that much reorganization is done in response to situations that simultaneously demand much activity by subscriber units, and the activity itself generates a great deal of traffic. It is highly desirable that IP addresses and network management data already be available before the network reorganizations and the concomitant traffic increase occur.

In this way, the organizing traffic occurs ahead of time and over channels less loaded with time critical data, possibly on the high-capacity channels typically found in garrison. That is, the relational database can store the unit-network address and other necessary relationships. This data may then be used by network management tools to assign addresses; however, the data must be loaded, kept current, and keyed by time. The work of managing and using the database must be done in such a way as to not load the combat network. And above all, the data must actually be in the database, with defined links ahead of time, and be current. The key to those links is the EID methodology, combined with reference libraries of associated military data.

A key caveat is, however, the need for a mechanism for determining reality or ground truth and modifying the database accordingly. That is, it is desirable for tactical planners to include network planning and for the planned network data to be in the database, ready to invoke on the basis of time or a trigger event such as passing (or not passing) a phase line. It is absolutely crucial for the new network data not to be loaded into servers or individual hosts erroneously or out of sequence with events.

3. Applicability to the Future Combat System (FCS)

The FCS [15] is a program designed to transform the U.S. Army into a reconfigurable, rapidly deployed force that will be "overwhelmingly lethal, strategically deployable, self-sustaining, and highly survivable in combat through the use of integrated command and control capabilities with unsurpassed situational understanding for all levels of commanders." Central to the success of such a program is the ability to rapidly configure and reconfigure units as the immediate situation demands. Perhaps the most difficult of the tasks required by such reconfiguration is the management of communications. To support "network centric concepts for multi-mission combat" built upon a transfer control protocol (TCP)/IP network foundation, the ability to rapidly plan and control addressing and other management functions is paramount.

4. Definitions and Notation

This study requires manipulation of several elusive and nebulous concepts. Some concepts are used widely but defined only by use; other concepts are used with the same word having different meanings in different settings. For this reason, several key definitions are offered in this section. Where differences exist between this study and the JCDB-DM, the differing meanings are discussed separately.

4.1 Notation

The notation used in the database model diagrams and in the text of this report is described.

The notation used in the model diagrams is simple and is illustrated in Figure 1.

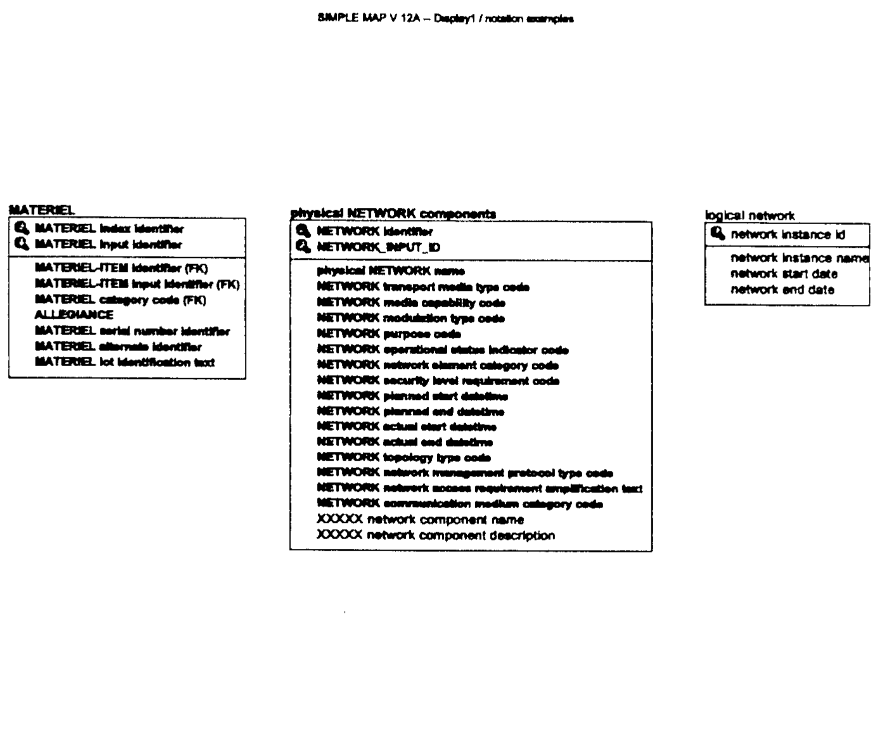


Figure 1. Example of notation.

- Items in sans serif small capital letters are found in the basic JCDB-DM version 4.3 (e.g., the entity labeled MATERIEL).

- Items in sans serif lowercase letters are suggested additions developed during this study (e.g., the entity labeled **logical network**).
- Items of mixed upper and lowercase indicate a JCDB-DM item that includes suggested modifications (e.g., the entity labeled **physical NETWORK components**, which is a modification of the JCDB-DM entity NETWORK).

4.2 Definitions

The words used in the various data models and in reference to the modifications proposed in this report may have different uses and meanings. A few of the most important are addressed in Table 1. For example, the entity labeled NETWORK has a more restricted meaning in the JCDB-DM than is usually used. It relates to several entities in the proposed modifications and, for that matter, may have a different usage in other models.

5. The Joint Common Database

The JCDB-DM is a large data model primarily oriented towards logistics and planning. It is an IDEF1X relational database model. The database is implemented in the field using Oracle. The JCDB-DM may, for the purposes of this analysis, be considered to be organized as three "trees"— a tree for organizational matters, one for planning and documentation issues, and one for materiel issues. That is, the database can be used to determine the relation of a unit to other units, a unit to a plan, the equipment to a unit, and, of course, vice-versa. The use of the orgEID methodology in version 4.3 of the JCDB-DM aids the linkage between the entities in these trees.

These potential network-related modifications are structured to plug into the existing system. They are extensions of the current JCDB-DM into network-related phenomena rather than wholesale changes of the existing data structure.

The present version of the JCDB-DM treats networks as an aggregate of components. These are, in turn, related to items of materiel. This serves well for tracking materiel but does not cover relationships such as those between network components and addresses, which was the emphasis of this study.

Table 1. Key concept definitions.

Concept or Item	Usage in the JCDB-DM	Usage in This Study
Network	The concept "network" is incorporated in the JCDB-DM by use of one entity, NETWORK. The meaning of NETWORK in the current version (4.3) of the JCDB-DM is: "The joining of two or more components for the purpose of exchanging verbal, nonverbal, or electronic communications or transporting personnel, equipment, or other resources." Based on an examination of the attributes, the entity NETWORK is an ensemble of all possible network components, identified by a unique identification number or EIDs, NETWORK identifier. NETWORK is represented as data type index. NETWORK identifier is supplemented by another key entity, NETWORK_INPUT_ID, which presumably is an EID as well but is represented by data type "unknown." The components of an actual "network," e.g., the elements of the "2/52 Armor Battalion Command Network" are identified by a nonkey attribute NETWORK name. NETWORK name is a string data type. There is an apparent dissonance with the association with NETWORK-ASSOCIATION. NETWORK-ASSOCIATION is "The relationship of a NETWORK with another specific NETWORK." This appears to mean that the concept of network is at the aggregate level rather than the component level, as is implied by the key set; however, but the aggregate needed for the association entity can be obtained only by an operation sorting for network name.	A network is an ensemble of communicating elements. These include links and nodes. In this study, only networks running IP over ethernets are analyzed at length, but the basic structure can accommodate other kinds of networks as well, such as ATM, or an X.25 network such as Mobile Subscriber Equipment. The details of "network" vary depending on the purpose of the use of the term. That is, networks can be described logically for address management, in physical terms for engineering management, in terms of the materiel used, and probably many other ways. Thus, there are several network hierarchies in this analysis. These are described.

Table 1. Key concept definitions (continued).

Concept or Item	Usage in the JCDB-DM	Usage in This Study
Logical network	Not used.	A set of communicating elements with a single common IP prefix and netmask, e.g., network IP address 128.63.12.X and mask 255.255.255.0. The entity logical network can be used for address management and is one aspect of connectivity. It can also be associated with a specific unit or instance of an ORGANIZATION. An example is "2/52 Armor Battalion Command Net," which is associated with the 2/52 Armor Battalion.
Physical network	The entity NETWORK in the JCDB-DM has attributes that describe the physical performance or engineering parameters of a physical view of a network. The entity represents a table of network elements or components. The elements of a PHYSICAL NETWORK are also linked to MATERIEL, which provides more logistic and engineering data.	In the proposed modifications, the entity physical NETWORK components represents the actual network components and is a modification of the JCDB-DM entity NETWORK. This entity identifies the actual components and describes how they are connected.

Table 1. Key concept definitions (continued).

Concept or Item	Usage in the JCDB-DM	Usage in This Study
Functional network	Not used in the JCDB-DM.	In this study, the concept is represented by the entity functional network. It is a description of the network in terms of what it does, e.g., "A Co. command net" or "2/52 Armor Battalion logistic net."
Functional network type	Not used in the JCDB-DM.	This is used in this study to describe what the network does in general, for example, "armor company command net."
Organization	As used in the JCDB-DM, ORGANIZATION points to a specific organization or unit. It is defined as "An administrative structure with a mission." The entity is described by attributes such as "ORGANIZATION unit identification code." That code is "The code that uniquely identifies an ORGANIZATION to the company echelon level. This is an important legacy field inversion entry. In many cases, this data provides the same information as that held in the ORG_TYPE_SRC code lookup. [Currently evaluating ORGANIZATION ID, UIC, and ORGANIZATION NAME being linked.]" It is therefore used to describe a specific instance of an organization, such as "A Co., 2/52 Armor Battalion, 52nd Armor Division."	Same
Organization type	Not used in the JCDB-DM.	In this study, it refers to a generic organization that can usually be described by a general organizational template, such as "Armor Company, Armor Battalion."

Table 1. Key concept definitions (continued).

Concept or Item	Usage in the JCDB-DM	Usage in This Study
Node	The concept appears in the JCDB-DM as NETWORK-NODE. A NETWORK-NODE is "A singular physical object or set of objects that can be interconnected to form an information and communication group or system, and that is addressable. [A NETWORK-NODE may consist of a network-device or an aggregation of many network- devices.]" It is described by several attributes, including NETWORK-NODE role code, a string data type.	In this study, the entity NETWORK-NODE is used as a network element that is related to other elements through an interface device. It is a logical concept. NETWORK-NODE is associated with a host-name, and through association with one or more node interfaces, has various addresses including network addresses and names. It may be associated with a physical device in **physical NETWORK components.**
Link	The concept appears as NETWORK-LINK. A NETWORK-LINK is "The physical interconnection (or group) of communication media which interconnects interoperable NETWORK-NODEs." A NETWORK-LINK is described by attributes such as **NETWORK-LINK modulation type code**, which is "The code that denotes the scheme used to encode information on a NETWORK-LINK." It is therefore an engineering abstraction. It is not clear how a NETWORK-LINK can be associated with a given NETWORK-NODE, which lessens the utility in network engineering.	In this study, a link is a derived element, in the physical view of a network. It is defined by interface-to-interface relationships and node-to-node interface relationships, in the logical view of a network. That is, in the physical world, a computer (one kind of node) has (is associated with) a given network interface card which, in turn, has a common network address linking the interface card to other interfaces.

Views of the present JCDB-DM data structures pertaining to network, address, and materiel are shown in Figures 2–4.

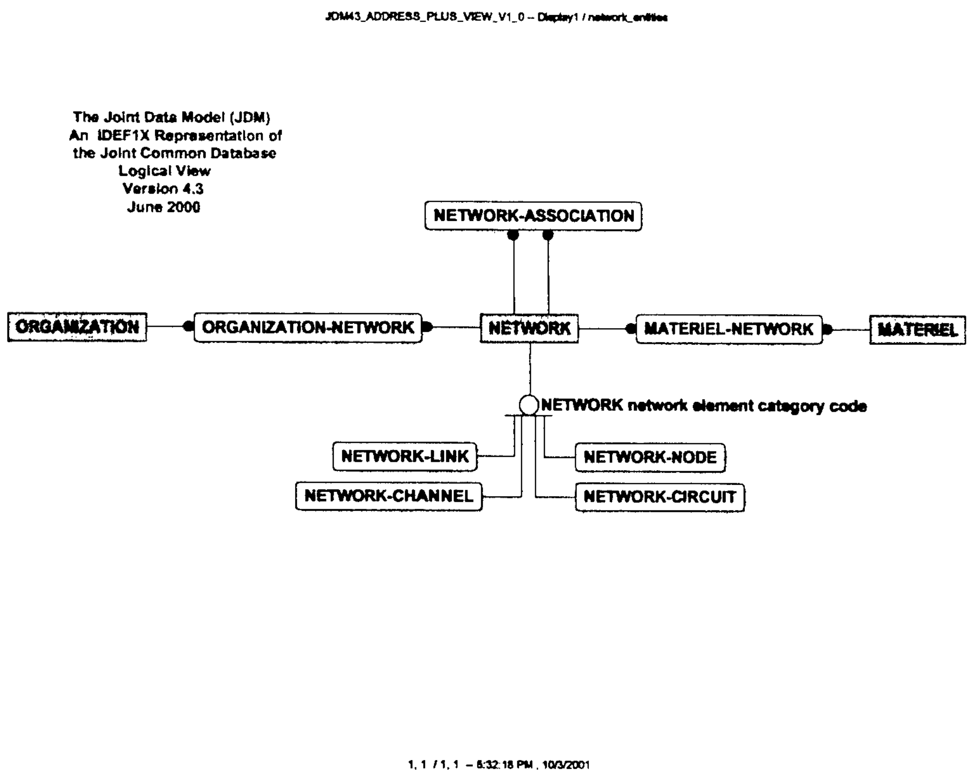


Figure 2. Network view from the JCDB-DM version 4.3.

There are several observations that can be made concerning problems in using the present JCDB-DM structure for network management. The basic problem is a lack of information describing the elements of a network for use in a given task, such as address management. Protocols exist for a host when determining what IP address it presently has, but the datalink address is permanently inserted in a network interface card. There is no provision for such an address, nor for hostnames, in the present data model. To manage the network and allow it to function properly, the network and its manager must have information that links machines to their addresses, names, and IP addresses. For instance, in a reasonably stable network, IP routing tables are built either manually or by listening for packets and deducing from the traffic who can be reached from where. It is desirable to be able to add the data to appropriate tables when a reassigned element signs on to its new network and remove it

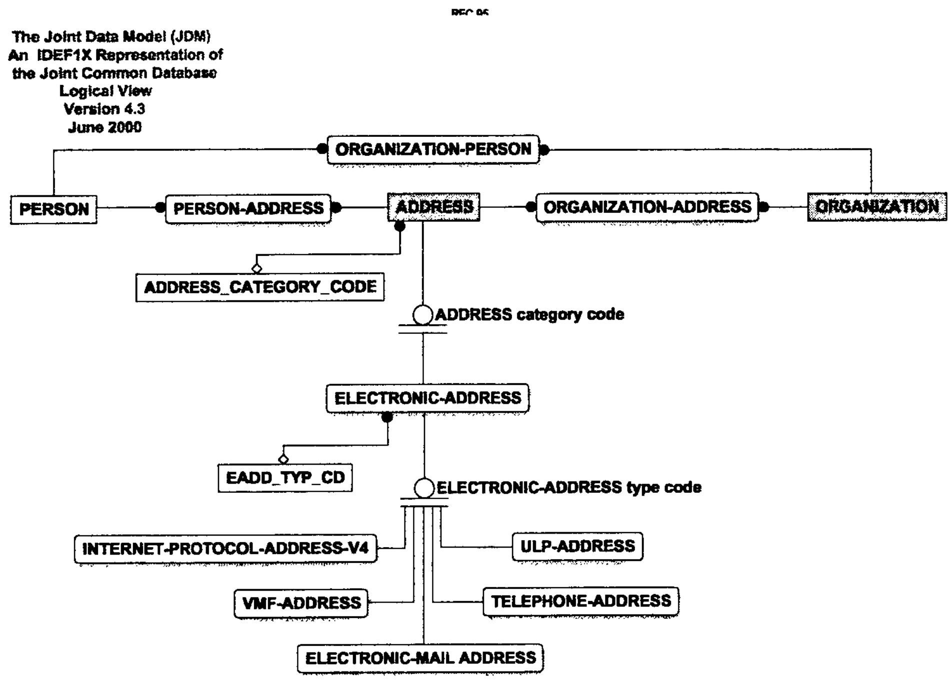


Figure 3. Address view from the JCDB-DM version 4.3.

from other routing tables at the effective time. These table modifications could be generated from the network data and time phased by reference to a signal plan of some kind. There are other issues, such as planning and resource deconfliction, that could be profitably addressed by an extended JCDB-DM. The issues and their resolutions are discussed next.

6. Use of the Network Data Model

The data model framework must be usable in several ways for managing the network. These are as follows:

- Network planning. The network manager must know what the requirements are and have a means of implementing them. Starting with the operational plan (op plan) and using the operations order (op order) or its shorter and more fragmentary cousins, the planner can access network templates (types); from these templates, the materiel types used in the network are determined. The materiel types are associated with a library of performance and logistic parameters (effective radiated power, space, weight,

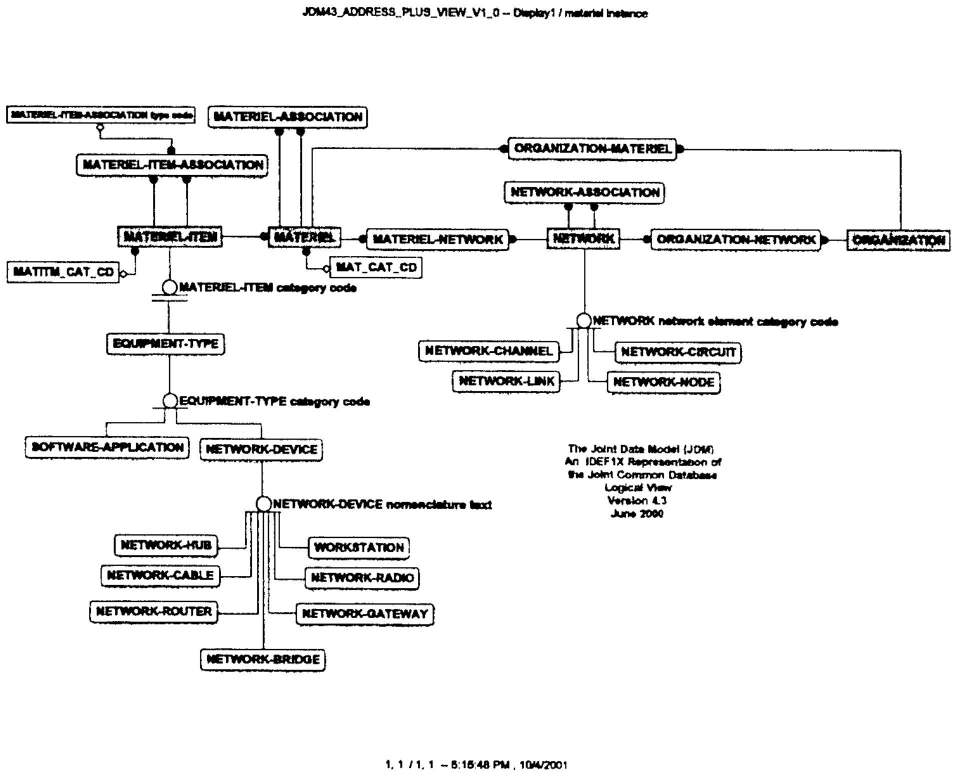


Figure 4. Materiel view from the JCDB-DM version 4.3.

power requirements, etc.) that permit the network engineering and logistic planning. Likewise, the op plan and op order contain the data necessary for tactical planning such as network requirements and movement orders—trafficability maps, enemy order of battle, friendly order of battle, and so forth. The arbitrary numbers, orgEIDs, assigned to the op plan and op order are the linking factors to those data, as are the orgEID numbers assigned to the network templates (types) and so on.

- Network management. The associative entities relating key parameters can be time-phased according to the signal plan. The bindings can be sent to the servers that manage network control factors such as the distribution of IP addresses. This way, an operator at a unit may know what IP addresses to insert into his/her machines upon attachment to another unit, the domain name server (DNS) will have an update already waiting for them, and so forth. Likewise, the S3 (operations officer) of a battalion can have traffic routed directly to him/her upon effective time of attachment to a given headquarters rather than rely on waiting for routing tables to be updated manually or through traffic analysis. The orgEIDs will be the linking factor.

- Other management issues. Generation of the communications-electronic operation instructions (CEOI) can be aided by easy access to network address data. Thus, in the database, use of a given unit's orgEID leads automatically to the serial numbered signal assets and then, in turn, to the assigned frequencies or hopsets, all in one database, keyed to time. The possibility of tracking machine configuration and software version and installed patches is attractive as well. This may help avoid security vulnerabilities due to misconfiguration or use of outdated or unpatched software.

These requirements make it extremely difficult to use a single network data design for all purposes. This is reflected in the current network data design — a network is represented in different ways for different purposes.

The data requirements for use of the model to support these uses are reflected in the proposed modifications (see Figure 5).

7. Network-Related Modifications to the JCDB-DM

The proposed network-related modifications to the JCDB-DM are based on defining a model of networks that can be applied universally, facilitated by templates or network types, and related to the instances of networks. Additionally, relational entities are defined that mirror the bindings or data files used for network management and which may be kept current through other means besides using automatic management protocols on an already overloaded net.

It is proposed that a basic network be depicted in several ways, depending on the use of the representation. These uses and the resulting representations correlate roughly with the Open Systems Interconnection (OSI) Reference Model [16]. That is, for network management or engineering at the physical level or layer, a representation that accommodates data concerning engineering parameters is required. The parameters may be accessed for some kinds of network engineering or set for other network engineering procedures. Through the association with the MATERIEL entity and to MATERIEL-ITEM, basic logistical and engineering capability data may be obtained. This network representation is through the entity physical NETWORK components. In order to not hinder extension of the model to non-IP networks such as X.25, the TCP/IP Reference Model [16] was not used.

The proposed modifications and entity level are shown in Figure 5. The attribute level is displayed in Appendix B.

The instance of a network is described in this study using the entity **logical network**. **Logical network** is defined as an association of network components that share the same IP prefix or network address. **Logical network** is composed of one or more NETWORK-NODEs, * an entity borrowed from the JCDB-DM, each of which is linked to a node interface. That is, an instance of a NETWORK-NODE is a network element that has or is connected in some

*In the JCDB-DM and in these proposed modifications, NETWORK-NODE is an element of a network. In the CADM, NETWORK-NODE is an association entity linking a NODE to a NETWORK.

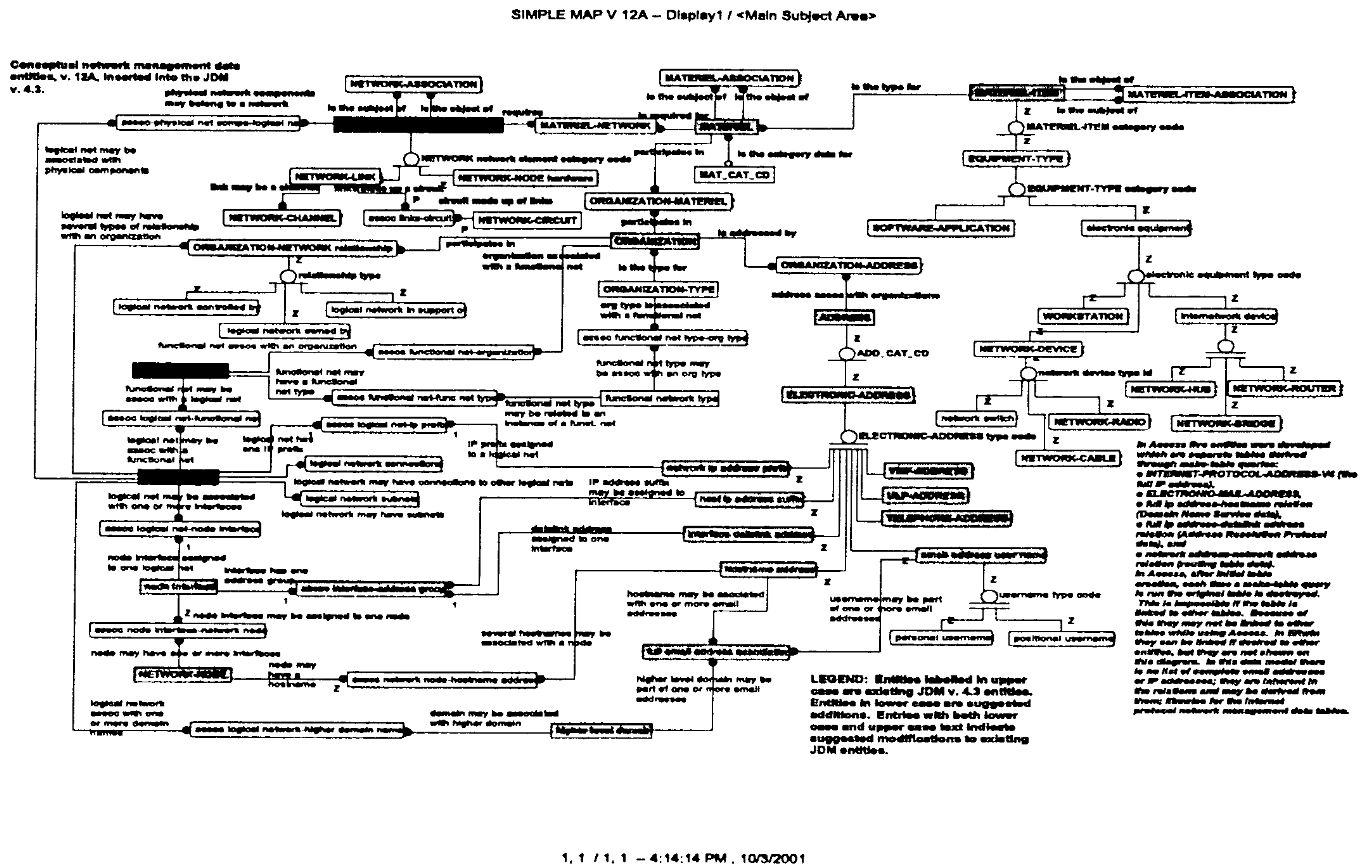


Figure 5. Proposed changes to the JCDB-DM version 4.3.

way to an interface. Physically, the **node interface** is usually a network adapter card installed in the computer serving as the NETWORK-NODE. This interface is identified by a unique hardware or datalink address. For ethernets running IP, this is a network adapter or interface card, usually plugged into a computer of some kind. For other types of networks, the picture may be different.

One interesting feature of this view of a network is the definition of a "host." Host is a term used, for historical reasons, for a general-purpose computer. A NETWORK-NODE may be a general-purpose computer or host. It may also be something else entirely, provided only that it be associated with an interface. The NETWORK-NODE is, however, associated with a **hostname address**. All nodes may not have a hostname but will have (be associated with) an **interface datalink address** and a **host IP address suffix**. The interface is the element that ties the network together in this representation. The interface is associated with a given instance of a network, the **logical network**, which, in turn, is associated with a **network IP address** or prefix. The association could easily be the reverse — an interface might be associated with an IP prefix, and a logical network would then be associated with the same prefix. Either is functionally equivalent.

Interestingly, due to the presence of two different kinds of addresses — the datalink address and the IP address in this representation, the **logical network** is a representation that uses both layers 2 and 3, the link and network layers, though it is defined at level 3.

A notional example of a **logical network** might be a network named "fizzle," with EID 32, a data network to be established effective 23 March 2010 at 0200, in support of the first brigade in the attack. It is to be established by the 422nd Signal Battalion. It is thus associated in two different ways with two ORGANIZATIONs and also, incidentally, with an operation plan and order. The latter are not treated here, but it would be straightforward within the present JCDB-DM. The network can also be related to one or more network types. For instance, **logical network type** entity (which might also be called a network template) might, in this case, be a "Brigade Support Network" composed of a generic MSE node center switch with two subnets and a connection to Division HQ.

The ERwin representation in IDEF1X of a **logical network** and its related entities is shown in terms of its building blocks in Figure 5. For simplicity, only logical entities are shown; logical attributes and the physical representation of the model are not shown. The representation at the attribute level may be found in Appendix B. Relations are defined between the list of building blocks of a network instance and the individual materiel end items. These are represented by MATERIEL, instances of which might be enumerated by control measures such as serial number or bumper number. The network types (templates) are related to the types of materiel used to make the networks listed.

The proposed interfaces with the existing JCDB-DM are shown in gray. The current JCDB-DM does not distinguish between network and network types and also uses the term network rather differently than here. Associative entities link network entities to entities such as different kinds of addresses–hardware or datalink, IP address, hostname, and so forth. The network representation is based on relationships between network interfaces, in this case, network interface cards (NICs). The relationships are defined in terms of ELECTRONIC ADDRESSs. A node is associated with (possesses) one or more NICs; these cards are associated with IP addresses which, in turn, are composed of a host suffix and a network prefix. There is no single entity in this representation that is the complete IP address. The reason is that reassigning to different networks and possibly changing the host IP address are more easily done if the tasks are performed separately. The version of the JCDB-DM used in this study originally listed entities for complete IP addresses and email addresses. This proposed scheme associates them differently. New, explicit associative entities are defined between individual networks and network nodes and their associated IP addresses and net masks.

Electronic mail programs and protocols are not addressed in detail here. There are a number of email systems. The treatment here is generic and, based on associating the components of the email address, may be found in separate tables. Use of an association entity is simple conceptually and allows considerable aliasing. It thus involves email address usernames, both organizational and personal, associated with one or more hosts and one or more **higher level domain names** and their various aliases. These are, in turn, associated with a **logical network** which, in turn, is associated with a network IP address prefix and a host IP address suffix. The domain name might well not be the same as the name field of logical network. An association may be derived between individual nodes in a net and the email addresses associated with them through the hostname. Likewise, associative entities may be defined that relate individual persons to the email addresses and the slots in a given organization. For example, one email address might be person related: jones@hostname.higherleveldomainname. Another might be s3@hostname.higherleveldomainname, related to a specific slot in an ORGANIZATION.

The concept of link here is defined in terms of relationships between interfaces. It is not explicitly used in the **logical network** representation. That is, a node has one or more interfaces which can communicate with other nodes through their interfaces. The requirement is a common IP prefix or network address and connectivity. Connectivity between addresses is assumed here but may, of course, not be in the field. A field may be added to the association tables or to the various address tables or other tables to define a start and an end time or "effectivity."

In this case, "link" is a derived entity. In the working model Access database described and developed in this study, pairs of interfaces sharing a common host may be derived. EIDs identify the pairs of interfaces, one for each interface. Access refuses to allow these keys to be inserted into a table together because that would include two AutoNumber fields in a common table. As a result, the interface names are used as identifiers in the associative table. This works because the names, as used here, are "smart names" which contain information about the interface, e.g., "gateway 1 net 2 to net 6." This locates the interface in net 2, with connection to net 6. Smart names were used for convenience in setting up the model. Using Oracle, an implementation in the field should not have this problem, so the EIDs identifying the interfaces could be used instead of the names. In this way, arbitrary interface names such as "S-3 machine 1" or "Fred" could be used, with the EIDs used in the association table.

Each instance of a **logical network** may be associated with a plan that it supports. As previously mentioned, it is possible to implement this in the following way. The network type or template desired is associated with an operational plan. The specific network instance, including its movement and operation timelines, is associated with the operations order that implements the plan. These plans, in turn, must be associated with the units involved in the plan. The association of the network with units is done through two relationships — ownership and support. That is, a brigade net might be based on a supporting MSE element owned by a signal battalion. The common link is the organizational ID.

8. Issues and Their Resolution

The issues previously listed can now be discussed in the light of the proposed modifications to the JCDB-DM.

- Issue 1. Datalink (hardware) addresses. There are no provisions in the JCDB-DM for datalink or hardware addresses in a separate table. A number of network management data files require datalink or hardware addresses. There is mention of hardware or medium access control (MAC) addresses, but the use of MAC addresses is not clear. It appears in several places, such as the entity or table E_ORG_ADD, as a definition for the attribute or data column for ENEMY-ORGANIZATION input identifier: "The MAC address of the machine creating the record. The unique input identifier that represents a specific ENEMY-ORGANIZATION." The same type of definition is found in three attributes in the entity PERSON-ASSOCIATION: "The MAC address of machine creating the record. The unique input identifier." This is not useful for network management.

  Resolution: Interface **datalink addresses** are added to the data structure and linked by an associative entity to the network interfaces. This allows replacement of network cards and consequent changing of the datalink address or even interchange of the cards on two networks. The interface **datalink address** is then linked to the network prefix of the network it resides on through the network instance and to the IP suffix through an associative table. A query can then generate the full IP address–datalink address pairing that mirrors the ARP table in networked hosts.

- Issue 2. IP address mapping. The INTERNET-PROTOCOL-V4 to NETWORK-NODE relationship is nonunique in the JCDB-DM. IP address is broken out separately as a type of address (INTERNET-PROTOCOL-V4), but ADDRESS is not linked either to NETWORK or to NETWORK-NODE, which is a subtable within NETWORK, except through the entity ORGANIZATION. This creates a nonunique mapping of IP addresses to either NETWORK-NODE or to NETWORK or of the IP prefix to NETWORK.

  Resolution: The IP address is broken into its components — the network address prefix and the host IP address suffix. The two together form the entire IP address. The IP address is determined by two relationships — the relation of an IP address prefix to a logical net and the relation of an interface to the logical network. The interface is also associated with its datalink address and its host IP address suffix. The IP address components then reside in the tables or entities **network IP address prefix** and **host IP address suffix**, which are linked by association with logical network and node interface. This allows easy manipulation; the network prefix for a network can be changed en masse, and IP suffixes deconflict easily when adding new hosts. In particular, the mapping of an IP address to a given interface is unique, though a host may have several interfaces and hence IP addresses. The actual list of full IP addresses represented by the JCDB-DM entity INTERNET-PROTOCOL-V4 must, in the working model, be constructed with a make-table query, as it resides nowhere in its entirety.

- Issue 3. IP address prefix-network relationship. There is no way to link a network to an IP prefix or to a netmask. IP address is not broken down to network prefix and host suffix in this scheme.

  Resolution: The network IP address prefix and host IP suffix are put in separate tables. The network IP prefix information is associated with logical network. The mapping is unique.

- Issue 4. Unitary IP address. IP address is a single element in this database. In practice, it is desirable to manipulate the network prefix and the host suffix independently.

  Resolution: As previously described, the requirements for use of the information relating to a network largely paralleled the OSI reference model. This required descriptions of the network for each required level. Management at the logical or address level, at the functional level, and the physical component level were chosen for this exercise. The physical level in the OSI model refers more to functional electrical or optical data rather than hardware (physical components), but the latter is essential for practical engineering and logistical management of networks. The data required for managing a network at each level is thus parceled out among three entities representing the management tasks under consideration. It should be mentioned that the original scheme tried in this study used first one then two descriptions of a network; but even two descriptions of a network did not address all the cases posed by the authors.

  The scheme chosen also supports classless IP subnetting [16]. That can be done two ways — either by a recursive relationship in the logical network entity or by linking to a table pairing networks and any subnets. The latter is chosen for simplicity and is incorporated in the Access working model.

- Issue 5. Definition of NETWORK. NETWORK is a table that includes all possible network elements. These network elements can be grouped by a nonkey attribute NETWORK NAME. NETWORK has a unique identifier, NETWORK IDENTIFIER, which is a primary key, but it differentiates all the various components of a network from each other and from components in other networks, not one network from other networks. In this database, a network has identity only as an ensemble of discrete elements with the same NETWORK NAME. The network has a topology descriptor, but the arrangement or connectivity of nodes within the network is not determinable from the data presented. That is, the NETWORK elements identified by a specific NETWORK NAME may share a given topology, say ring, but who connects to whom is not determinable. Likewise, NODE function (e.g., gateway, workstation, switch, etc.) may be specified by the attribute NETWORK

ELEMENT CATEGORY CODE, which is defined as "The code that denotes the network element category for a NETWORK," but that is not clear.

Resolution: As previously described, it was necessary to resolve NETWORK into different elements, depending on the management requirements for that network view – physical, logical, or functional. In particular, the concepts of CIRCUIT and CHANNEL are not used. They would probably be useful in manipulating ATM or X.25 networks, but those are not addressed in this study.

- Issue 6. Physical component basis of a network. In the JCDB-DM a NETWORK is composed of NETWORK-NODEs, NETWORK-LINKs, NETWORK-CIRCUITs, and NETWORK-CHANNELs. This appears to convolve elements at different levels of abstraction. NETWORK-NODEs and NETWORK-LINKs may well be coequal parts of a NETWORK, but NETWORK-CHANNELs and NETWORK-CIRCUITs appear more closely related to NETWORK-LINK. That is, a NETWORK-LINK may go over a NETWORK-CHANNEL, and a NETWORK-CIRCUIT is composed of one or more NETWORK-LINKs. Further, some of the characteristic attributes, or data columns, are appropriate for one or the other entity, but the attributes are not common to all. However, NETWORK-CHANNEL and NETWORK-CIRCUIT are entirely appropriate for describing networks such as MSE at the physical level.

  Resolution: In the proposed model, a network, which is really a grab bag of physical components in the JCDB-DM, is renamed PHYSICAL NETWORK COMPONENTS for clarity. Further analysis is needed to define the concepts of LINK and CHANNEL. For instance, is a LINK a logical thing, a geometric thing, a set of frequencies, or a physical thing such as a cable? In NETWORK, it appears to be a physical thing such as a cable, but network planning and engineering require more abstract concepts as well.

- Issue 7. Hostnames and domain names. It is not clear how the network can be managed through the domain name hierarchy within the context of the JCDB-DM. There is no subtype of electronic address corresponding to the hostname of a computer. The hostname and domain names are essential for electronic mail addresses and the domain name service.

  Resolution: Hostnames and domain names are added. The basis of domain naming is added. This is necessary for a later extension of this scheme to electronic mail and is necessary for the management of networks running under TCP/IP. In particular, the domain name service requires it. The domain name of a network need not be the same as the name of the logical network; an associative entity can relate any number of aliases to the same net. There is provision for the attribute NETWORK name, but if that datum is used to name the network, as is usually done for the convenience of humans (e.g., "2nd Battalion Logistic Net"), other names that may be more directly applicable to the DNS are not simultaneously usable (e.g., <synapse.2_42bn.1cd.army.mil>). In addition, use of an associative entity to link networks and domain, as is done here, makes it simple to add any number of convenient aliases to the name structure.

  It should also be noted that the data in the DNS servers and such data structures as the command and control (C2) registry include hostnames and may act as sources of data for this function.

- Issue 8. E-mail addresses. ELECTRONIC-MAIL, or e-mail, addresses are specified and are linked to PERSON by an associative entity through ADDRESS; however, the link of the hostname portion of the address is not apparently linked to a specific node. E-mail addresses of a given slot in an organization, such as S-3, are not determinable with this scheme. For example, <s3@serendipity.1bde.1cd.army.mil> may be listed in its entirety as a separate email address, but for management reasons, it should be linked to the network domain name, the hostname, and a personal screen name or organization position.

  Resolution: E-mail addresses are addressed in this study only in a general way, but the data structure previously described appears compatible with any email scheme known to the authors. In this scheme, the full e-mail address would be a derived entity, just as the full IP address is. In particular, the basis for domain naming is present, and the link of the parts of the email address with either a function in an ORGANIZATION or to a PERSON is conceptually simple. Each component of the email address may be manipulated or associated independently from the others, and any number of convenient aliases may also be incorporated.

- Issue 9. Routing. Routing is done by reference to pairs of linked IP addresses — where must a packet be sent to reach its destination from this address? Concatenation of pairs of IP addresses available on a single node allows determination of possible paths. This scheme does not make allowance for network addresses nor interfaces and their addresses.

  Resolution: Routing depends on associating IP prefixes with gateways. This is easy, given the association of IP prefixes with interfaces, which are then associated with a common gateway node. The association of IP address pairs based on pairs of interface addresses present on the same node is straightforward, however, fairly clumsy using Access. It is demonstrated in the working model.

9. The Working Model

A working model of the database design developed in ERwin is constructed using Access. Network management tools are developed in Access as well. Due to the limitations of Access, these tools are useful only as proof of principle and to gain confidence that the data model is actually practical. There are many possible ways to construct a data model of this kind. Some work well, others look plausible; but in practice, they are too unwieldy to be useful. Many data models are actually devised and eliminated upon attempted use. The limitations of Access are not expected to apply to an Oracle database used in the field, with management tools written in structured query language (SQL).

The database design constructed in ERwin is inserted into Access using the forward engineer function of ERwin. Forward engineering of version 12 is accomplished in successful completion of over a thousand actions. However, the peculiarities of Access lead to the addition of a host of unwanted relationships, leading to the necessity of deleting the derived relationships and redoing them. The entities (tables) established are also edited to restore normalization, lost because of another peculiarity of either ERwin's forward engineering tool or Access. The tables are then populated with sample data for a fictional set of tactical networks.

The networks used are parts of two notional battalions. The test case involves assigning a platoon of mechanized infantry to an armored company. The limitations of Access require a mix of queries and several forms to be able to accomplish this, but using Oracle, an SQL programmer will have no such limits. To exercise the network management tools, several more networks and nodes are created and linked, including subnetting of an IP address. Once the nets are initially populated, this is surprisingly easy, except for the usual idiosyncratic "features" of large programs such as Access.

Each network is initially composed of three workstations and a router. Each item has one or more network interfaces, each with its unique datalink address. A summary of the initial network parameters is given in Appendix C. The actions taken to manipulate the networks are discussed next.

Goals for the working model include developing management constructs (tools) that would demonstrate the ability to insert or extract network management data from the data base describing the networks and modifying associations among the objects managed. That is, one should know what the network looks like in a logical sense and be able to perform network tasks such as assigning a platoon to another company. The data extracted or manipulated should satisfy the requirements for network management such as the following:

- mirroring the address resolution protocol (ARP) cache,
- generating routing table data,
- generating DNS data,
- making and modifying IP assignments both individually and by unit,
- adding hosts and assigning or modifying hostnames and IP addresses,
- changing or adding new network interfaces and assigning them to networks, and
- adding new networks and assigning or changing IP addresses, network names, and netmasks.

10. Network Management Tools

A set of network management tools is developed to perform the network management requirements within the working model; these are listed. This set includes several queries to find information and display it, where it can then be sorted and otherwise manipulated, as well as forms to actually alter the information on the tables. Due to a peculiarity of Access, queries with more than two tables do not permit manipulation of the tabular data within the query, leading to the requirement to use forms. In a form, another subform linking the data fields to another table can then be inserted. Another form can then be inserted in that subform. Thus, one may relate information in a chain of several tables, e.g., [datalink address–association table–interface] or [node–association table–interface] or [datalink address– association table–interface address–association table–node–association table–owning organization]. One may also devise a query to display the information (see the node parameters query in Appendix D). It should be possible to devise a single large form, perhaps with pop-up subforms encompassing every use; however, it is conceptually simpler to develop several forms to be used in turn to manipulate the data in the underlying tables. This is the reason the working model uses several forms, each to manage one network relationship, rather than a single, master form. Again, a management and display tool for Oracle, coded in SQL, should not be limited in this fashion.

Several of the network management entities are shown in Appendix D. Both design and data views are shown. For the make-table query, the query design and the table results are shown. The management tools are as follows:

- node parameters summary query,
- interface pairs (network connection) make-table query,
- node management form,
- routing table pairs form,
- hostname management form,
- network IP address management form, and
- link management form.

Using these tools, the basic data sets were manipulated to the following steps:

- Step 1. Populate six test nets with network data.
- Step 2. Generate exterior interfaces and link with parent nets.
- Step 3. Generate new parent nets with one gateway, add interfaces to the gateways of the subordinate nets, and link the gateways of the subordinate nets with the parent nets.
- Step 4. Reassign 3rd Platoon, A Company, 7/41 Mechanized Infantry Battalion, to A Company 2/52 Armor Battalion.

To exercise the tools, other nets representing brigade and division are formed, and two of them, in turn, are subnetted.

These steps are described in more detail in the following paragraphs.

The structure of the initial version of the working model and the individual network data is shown in Appendix C. The working model starts with isolated networks, each composed of three workstations and a gateway. Each element of these networks has an IP suffix and datalink (hardware) address and hostname. Each network has an IP prefix, a netmask, and a network name and is for a specific unit (e.g., A Company, 2/52 Armor Battalion); so an ORGANIZATION association is implicit. The network name is functional in nature (e.g., "A Company 2/52 Armor command net"). This could, in turn, be associated with a network type; however, that is trivial and is not done in this study.

Once the data tables are populated from the data in Appendix C, new datalink cards are added to the gateways to provide an exterior interface, and the new interfaces are linked to another network. For instance, an interface is added to the gateway for 3rd Platoon, A Company 2/52 Armor, and this interface is linked to the IP prefix for the "A Company 2/52 Armor Battalion command net." Once the network is established, two new battalion command networks are created, and each is populated with one gateway. Interface cards are added to the company level nets' gateways and linked to the parent battalion command nets. The 3rd Platoon, 7/41 Infantry then had its exterior interface for its gateway reassigned to the IP address of the A Company 2/52 Armor command net.

A number of other functions are exercised as well: other higher networks are created and linked, two networks are subnetted, hostnames and network cards are swapped and created, network IP prefixes are swapped and created, functional nets are created and realigned with logical nets, and email addresses are created and modified. Another useful exercise involves generating data that mirrors the address resolution protocol cache resident in each machine. This involves generating a query that links the hostname and full IP address pairs present in the test data sets. Data tables, including part of the data for the DNS files and routing table pairs, are also created, and their changes resulting from other network management functions are noted.

11. Populating and Maintaining the Database

The first step in using a database is populating it with data. In the field, this is a major operation. In the case of network parameters, this would be a formidable job if done manually. The benchmark to use is the size of a division; depending on the type (armor, etc.), this can be on the order of 17,000 soldiers. The modern division will almost certainly be smaller; but each soldier has one or more email addresses, a unit billet, a unit association with an owning and possibly a controlling unit, perhaps half of a radio and vehicle, and so forth. These numbers start adding up quickly.

It is proposed that the initial data population be accomplished by allowing the normal protocols such as DHCP to operate — a node has an IP address assigned to it, router tables are generated based on traffic, etc. In this way, the necessary data sets are generated based on the initial connectivity of the division. After that, new IP addresses would be assigned based on the effective time of unit assignment, driven ultimately by the operation plan and order. The DNS and routing tables could be generated ahead of time based on the required network address structure. That way, the unit has IP addresses assigned to it and waiting when it plugs into its new net. Thus, when a new unit is formed, the nodes negotiate IP addresses, and host name tables and such are generated in the normal way. The division is initialized, so to speak. These tables could then be sent to a common server and consolidated into the instance of the JCDB for that unit. After that, updates to satellite tables such as the C2 registry would be passed down from the central database, driven by operations plans and orders. It would be essential to also have provision for feedback from the working data tables in order to enable error correction. The normal protocols must remain operative to correct errors resulting from bad information flow, delay of a unit en route to a new assignment, and so forth. Updates to a DHCP server, for instance, would occur periodically from above, using presumably higher capacity links, rather than as a result of traffic from multiple sources from below, along presumably lower capacity links. If the server finds a discrepancy, it would correct it and report it to the next higher database.

The Integrated System Control (ISYSCON) should be a useful source and perhaps user of the data in this database, although currently, the ISYSCON functionality does not extend to the IP address space directly. The logistic data and tactical planning data used by ISYSCON should be analyzed in any further efforts.

12. Further Work

This scheme can be extended to address materiel very simply. Addressing the problems at the physical layer description of a network poses very thorny problems. The taxonomy of physical network elements can be strictly related to things that have a line item number, or be more abstract. In particular, application of graph theory to network design requires consideration of edges and vertices in a network. This, in turn, requires resolution of the definition of an element and a link. Whatever schemes are proposed should be tested in a working model. The working model is used in this study to winnow out plausible schemes that prove unwieldy. The same approach should be used to test future database designs.

The present JCDB-DM does not address key items such as virtual private networks or other kinds of networks such as asynchronous transfer mode (ATM) and networks operating under X.25. It is possible that this scheme, which is restricted to TCP/IP over ethernets, can be extended to accommodate the other networks; but it is more likely that somewhat different schemes will be necessary. It is clear that such proposals will need to be tested with sample data. It has also become apparent that these tests should be done with Oracle and SQL rather than an office package such as Access.

13. Summary

The JCDB-DM and related database systems have been analyzed for functionality in network management. A proposal for extension of the JCDB-DM to network management of ethernets using IP is devised. This design is embodied in Access and is tested using sample data input. Several network management tools are developed and exercised. These tools are constrained by the basic limitations of the Access package, which is an office management program. The tools are used to show addition of nodes, reassigning of nodes, reassigning networks to other networks, and adding new nodes and networks. It is proposed that further work be done to extend this scheme to the probable email package to be used by the field forces. It is also proposed that the scheme be extended to a detailed treatment of the physical layer. An analysis of different types of networks, at a minimum ATM and X.25, is highly desirable as these are already present in the field forces, and the JCDB-DM should accommodate them as well as ethernets. A working data model should be constructed in Oracle to verify the practicality of any proposed data base designs.

INTENTIONALLY LEFT BLANK.

14. References

1. Chamberlain, S. "Default Operational Representations of Military Organizations." ARL-TR-2172, U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, February 2000.
2. Bruce, T. A. "Designing Quality Databases with IDEF1X Information Models." New York, NY:Dorset House Publishing Co., 1992.
3. Lonigro, M. "The Case for the Surrogate Key." Intelligent Enterprise's database online, <http://www.dbpd.com/vault/9805xtra.htm>, Miller Freeman, Inc., May 1998.
4. Johnston, T. "De-Embedding Foreign Keys: Part 1." *DM Direct*, <http://dmreview.com/master.cfm?NavID=198&EdID=2308>, June 2000.
5. Johnston, T. "De-Embedding Foreign Keys: Part 2." *DM Direct*, <http://dmreview.com/master.cfm?NavID=198&EdID=2322>, June 2000.
6. Johnston, T. "De-Embedding Foreign Keys: Part 3." *DM Direct*, <http://dmreview.com/master.cfm?NavID=198&EdID=2331>, June 2000.
7. Johnston, T. "De-Embedding Foreign Keys: Part 4." *DM Direct*, <http://dmreview.com/master.cfm?NavID=198&EdID=2341>, June 2000.
8. Johnston, T. "Primary Key Reengineering Projects: The Problem." *DM Review*, <http://dmreview.com/master.cfm?NavID=198&EdID=1866>, February 2000.
9. Johnston, T. "Primary Key Reengineering Projects: The Solution." *DM Review*, <http://dmreview.com/master.cfm?NavID=198&EdID=2004>, March 2000.
10. C4ISR Architectures Working Group. "Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Core Architecture Data Model (CADM) Version 2.0 Final Report." <http://www.c3i.osd.mil/org/cio/i3/AWG_Digital_Library/index.htm>, 14 April 1998.
11. Droms, R. "Dynamic Host Configuration Protocol." RFC 2131, <http://www.dhcp.org/rfc2131.html>, March 1997.
12. Kaste, V. A. T., A. E. M. Brodeen, and B. D. Broome. "An Experiment to Examine Protocol Performance Over Combat Net Radios." BRL-MR-3978, U.S. Army Ballistic Research Laboratory, Aberdeen Proving Ground, MD, June 1992.
13. Sutherland, J. *Battle Book.* Alexandria, VA: Byrd Enterprises, 1999.
14. Comer, D. E. *Internetworking with TCP/IP.* Upper Saddle River, NJ: Prentice Hall, 4th ed., 2000.
15. Van Fosson, LTC M. "FCS Overview." DARPA PM for Future Combat Systems, <http://www.darpa.mil/tto/programs/fcs.html>.
16. Tanenbaum, A. S. *Computer Networks.* Upper Saddle River, NJ: Prentice Hall, 3rd ed., 1996.

INTENTIONALLY LEFT BLANK.

List of Abbreviations

ARL	U.S. Army Research Laboratory
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
CADM	Core Architecture Data Model
CEOI	Communications-Electronic Operation Instructions
C2	Command and Control
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DOO	Default Operational Organizations
DARPA	Defense Advanced Research Projects Agency
EIDs	Enterprise Identifiers
FCS	Future Combat System
IP	Internet Protocol
ISYSCON	Integrated System Control
JCDB	Joint Common Database
JCDB-DM	JCDB Data Model
Kbps	Kilobits Per Second
MAC	Medium Access Control
Mbps	Megabits Per Second
MSE	Mobile Subscriber Equipment
NICs	Network Interface Cards
orgEID	Organizational Enterprise Identifier
orgID	Organizational Identifier
OSI	Open Systems Interconnection
SQL	Structured Query Language
TCP	Transfer Control Protocol
UIC	Unit Identification Code

INTENTIONALLY LEFT BLANK.

Appendix A:

Network Treatment in the C4ISR Core Architecture Data Model (CADM 2.0)

INTENTIONALLY LEFT BLANK.

This discussion is based on the network related entities in the C4ISR Core Architecture Data Model (CADM 2.0). The version examined was a draft dated 22 February 2001. It was prepared by the Institute for Defense Analysis for the Office of the Assistant Secretary of Command, Control, Communications, and Intelligence (OASD(C3I))-Information Integration and Interoperability and the Office of the Deputy Chief of Staff for Command, Control, Communication, Computers, and Intelligence (ODCSC4I). The model is extremely complicated, as it incorporates input from several other models. It is well documented internally.

The view shown in Figures A-1 and A-2 includes only the NETWORK entity and related entities. These include the elements of network addressing. The differences with the JCDB-DM are interesting. The first is the nature of the NETWORK entity itself. The JCDB-DM NETWORK entity is a collection of network components. The NETWORK-NODE entity in the JCDB-DM is an element of a network; NETWORK-NODE in the CADM is an associative entity linking a node to a network.

The treatment of internet protocol (IP) addresses in the Core Architecture Data Model (CADM) is useful and versatile and represents what might be called the "address book" view of IP addressing. The approach chosen for this report is rather different but is consistent with the CADM approach, as a query could easily form the IP address book linked to a network, which is embodied in the CADM. Likewise, the node-to-node association and network-to-network associations in CADM are easily generated. The latter is an intermediate step to the table in the working model that represents elements of router tables.

Entities representing email and network interface addresses could be added to the CADM scheme easily. Hostnames are implicit already. These would form the basis for the information files used in network management.

The CADM treatment of NETWORK has a great deal of functionality with respect to network utility, association with organizations, etc. The description of a network as a logical net, functional net, and so forth could be accommodated easily if desired. Use of network IP prefixes and host IP suffixes seems to be an easier way of managing addresses at the network level than an address book approach using the whole IP address. But the address book of full IP addresses is generated as a matter of course in the working model reported here.

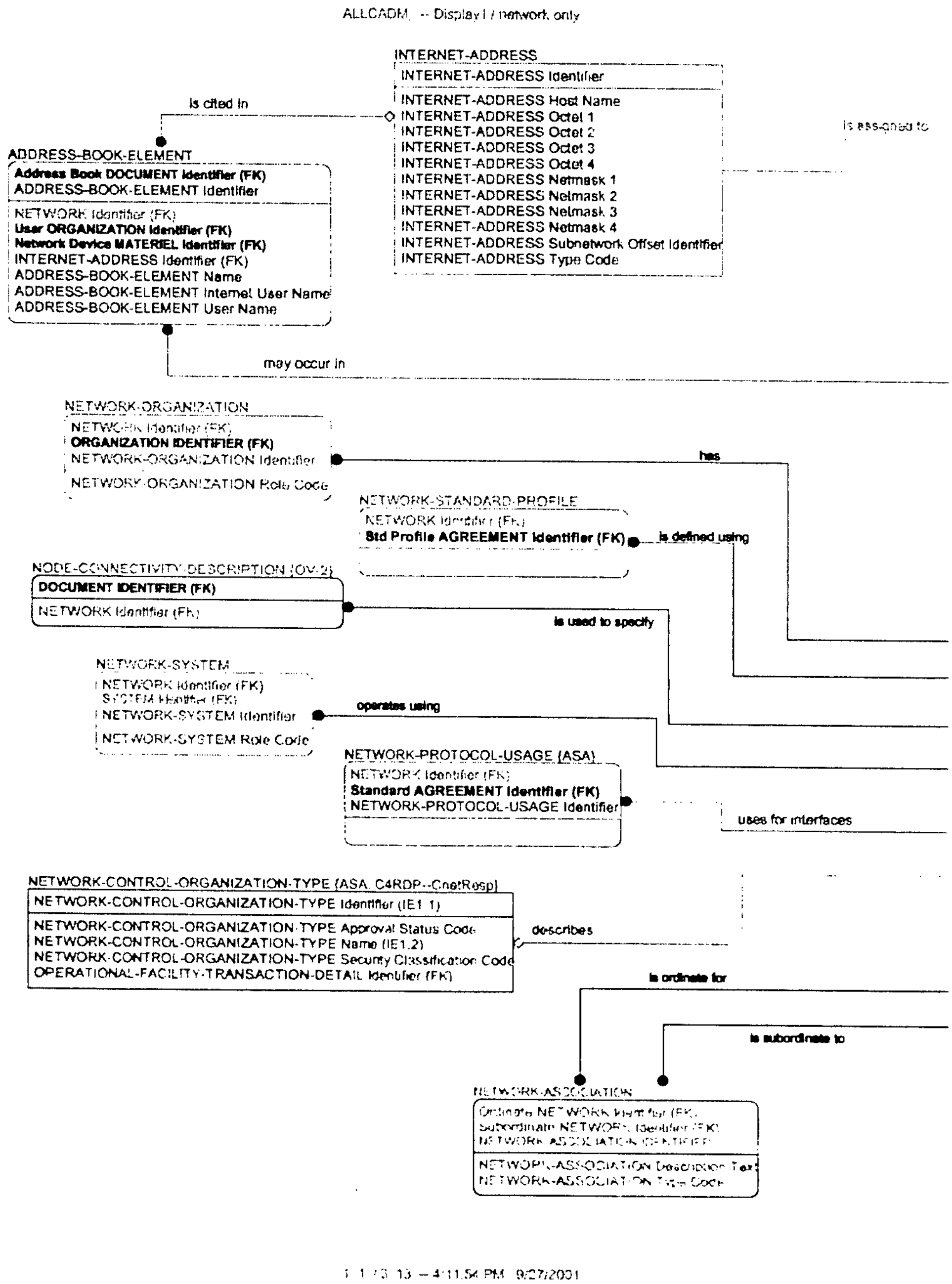


Figure A-1. ALLCADM network view, panel 1 of 2.

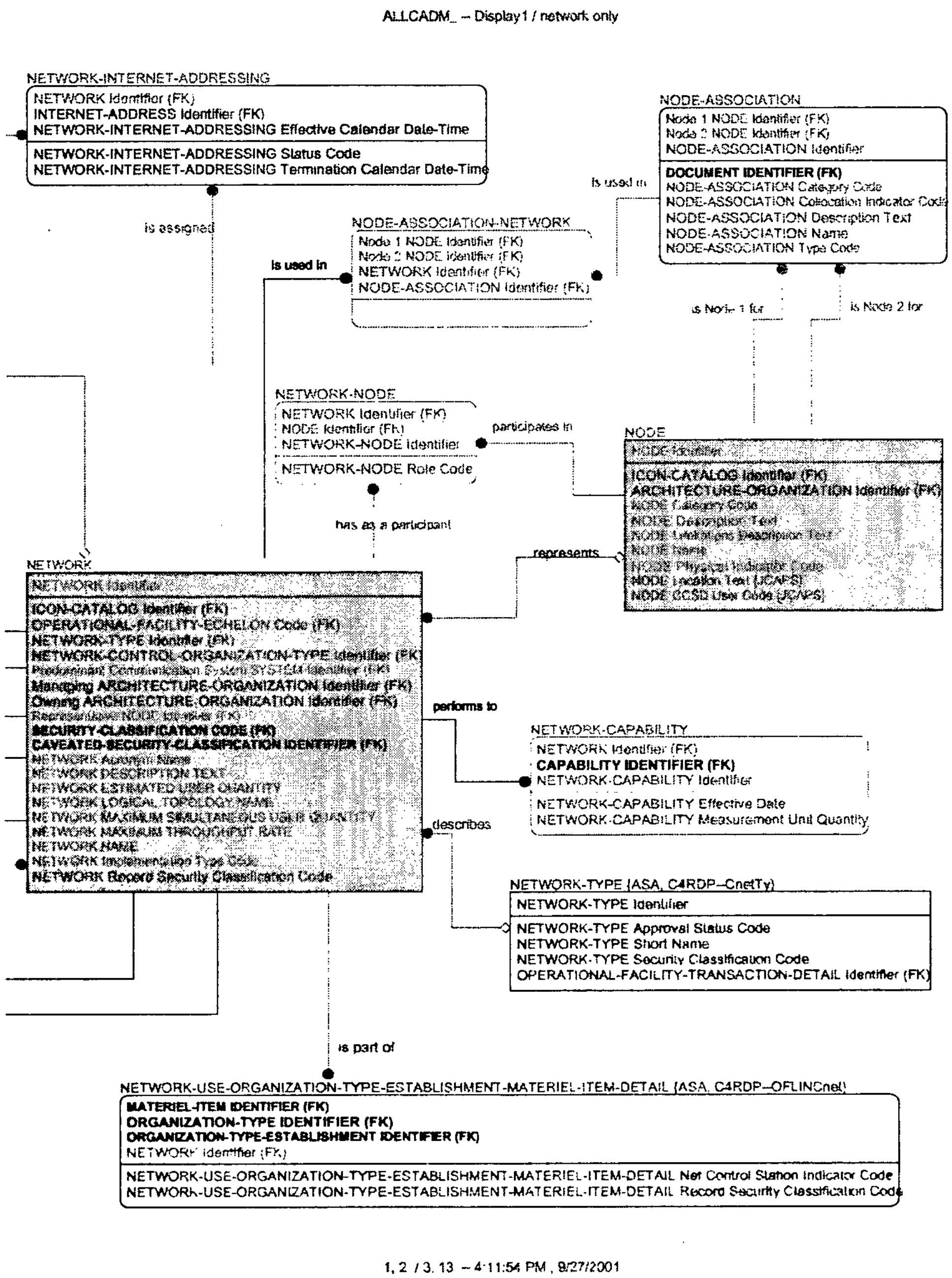


Figure A-2. ALLCADM network view, panel 2 of 2.

INTENTIONALLY LEFT BLANK.

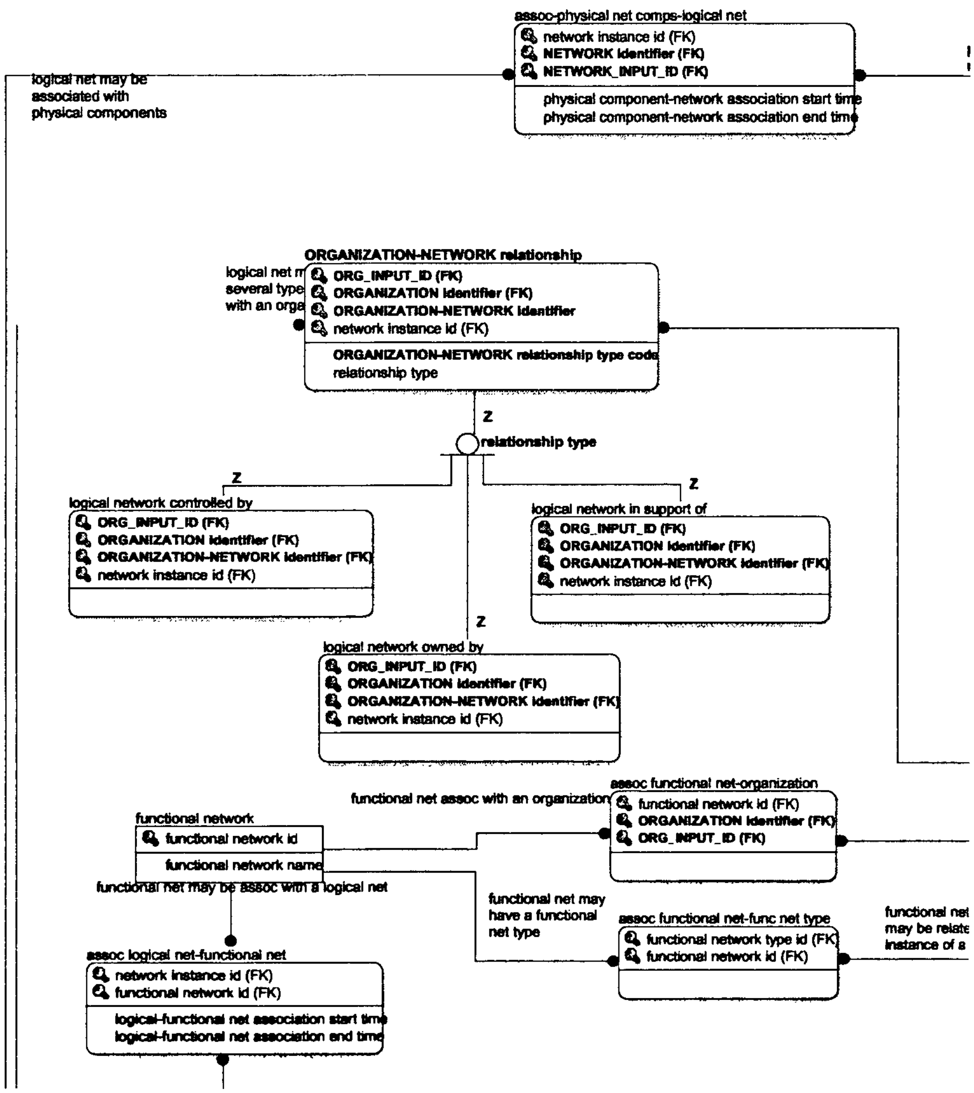
Appendix B:

The Network-Related Modification, SIMPLE MAP Version 12A–Attribute Level View, in ERwin 3.5.2

INTENTIONALLY LEFT BLANK.

SIMPLE MAP V 12A -- Display1 / <Main Subject Area>

Conceptual network management data entities, v. 12A, inserted into the JDM v. 4.3.



1, 1 / 2, 4 -- 5:15:36 PM, 10/2/2001

Figure B-1. SIMPLE MAP version 12A, Conceptual network data management modifications inserted into the JCDB-DM Version 4.3, panel 1, row 1 of 2 rows.

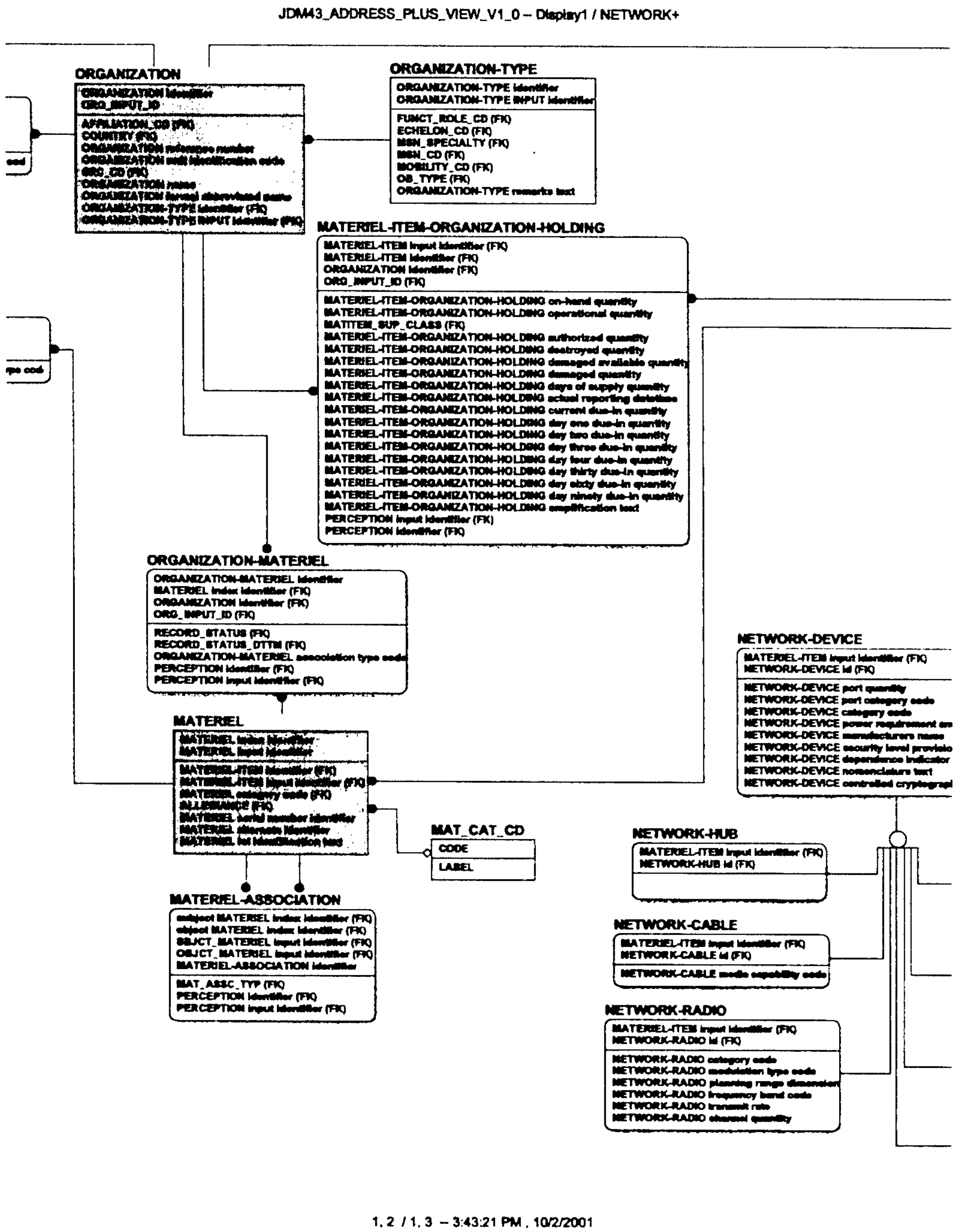


Figure B-2. SIMPLE MAP Version 12A, conceptual network data management modifications inserted into the JCDB-DM Version 4.3, panel 2, row 1 of 2 rows.

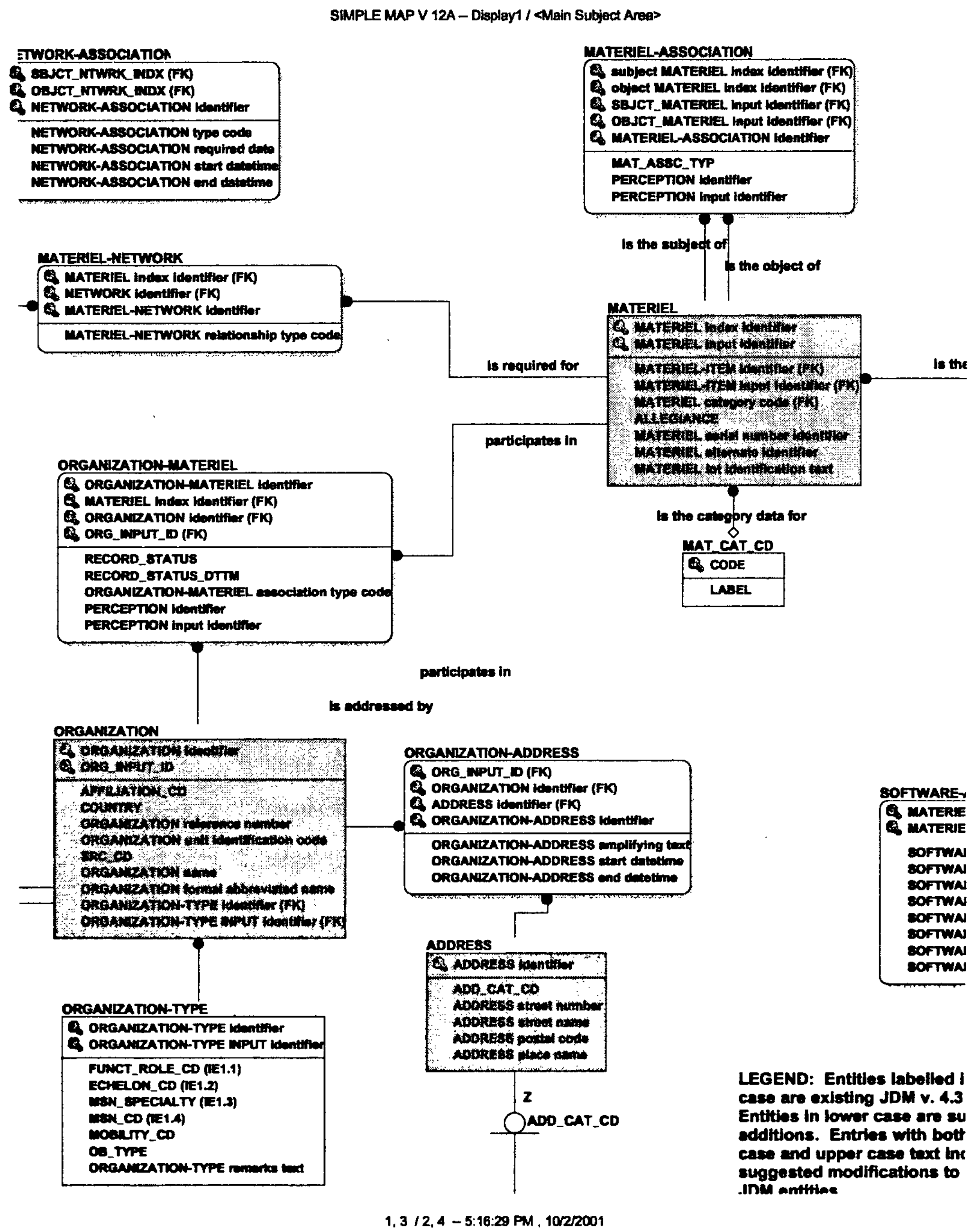


Figure B-3. SIMPLE MAP Version 12A, conceptual network data management modifications inserted into the JCDB-DM Version 4.3, panel 3, row 1 of 2 rows.

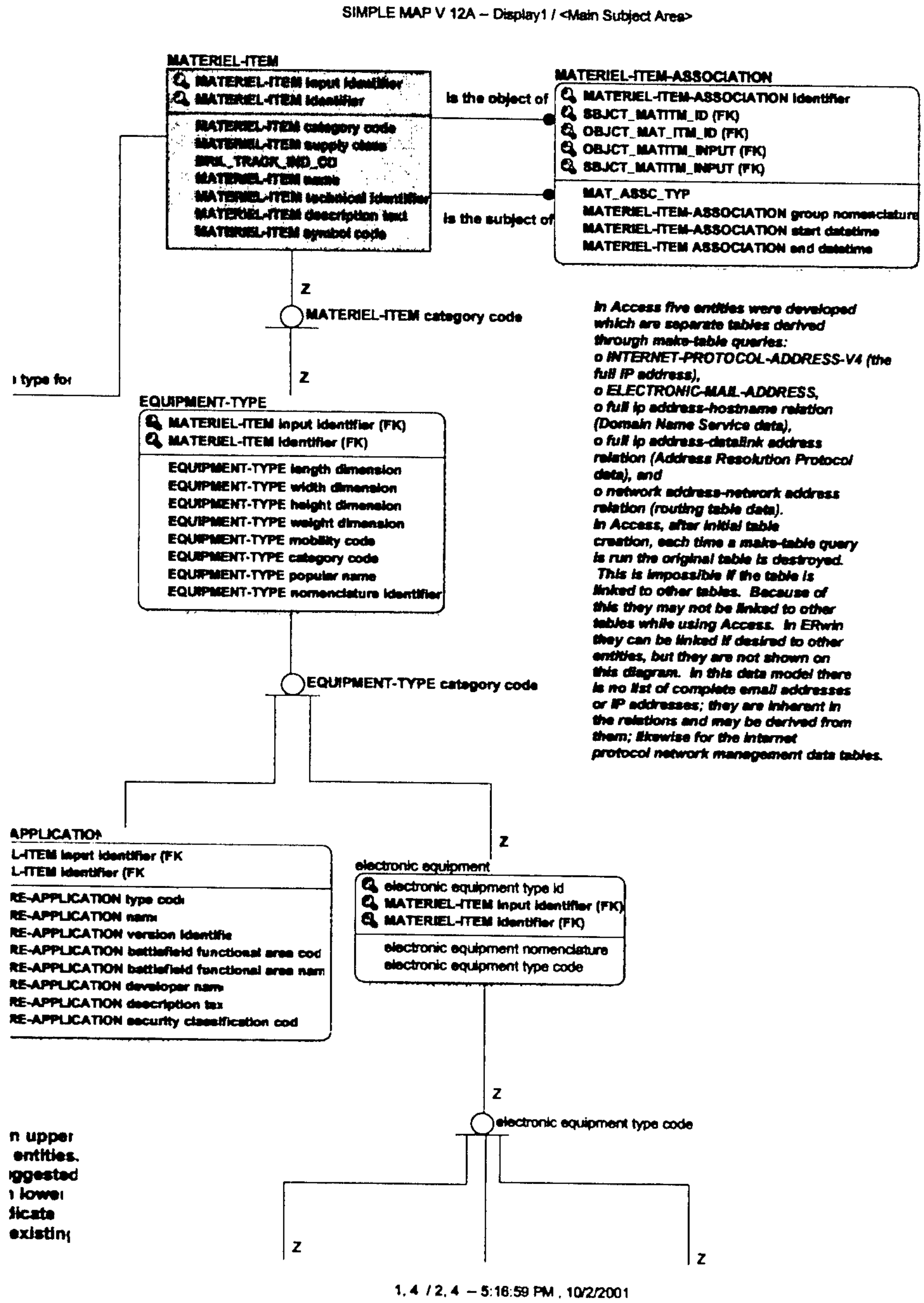


Figure B-4. SIMPLE MAP Version 12A, conceptual network data management modifications inserted into the JCDB-DM Version 4.3, panel 4, row 1 of 2 rows.

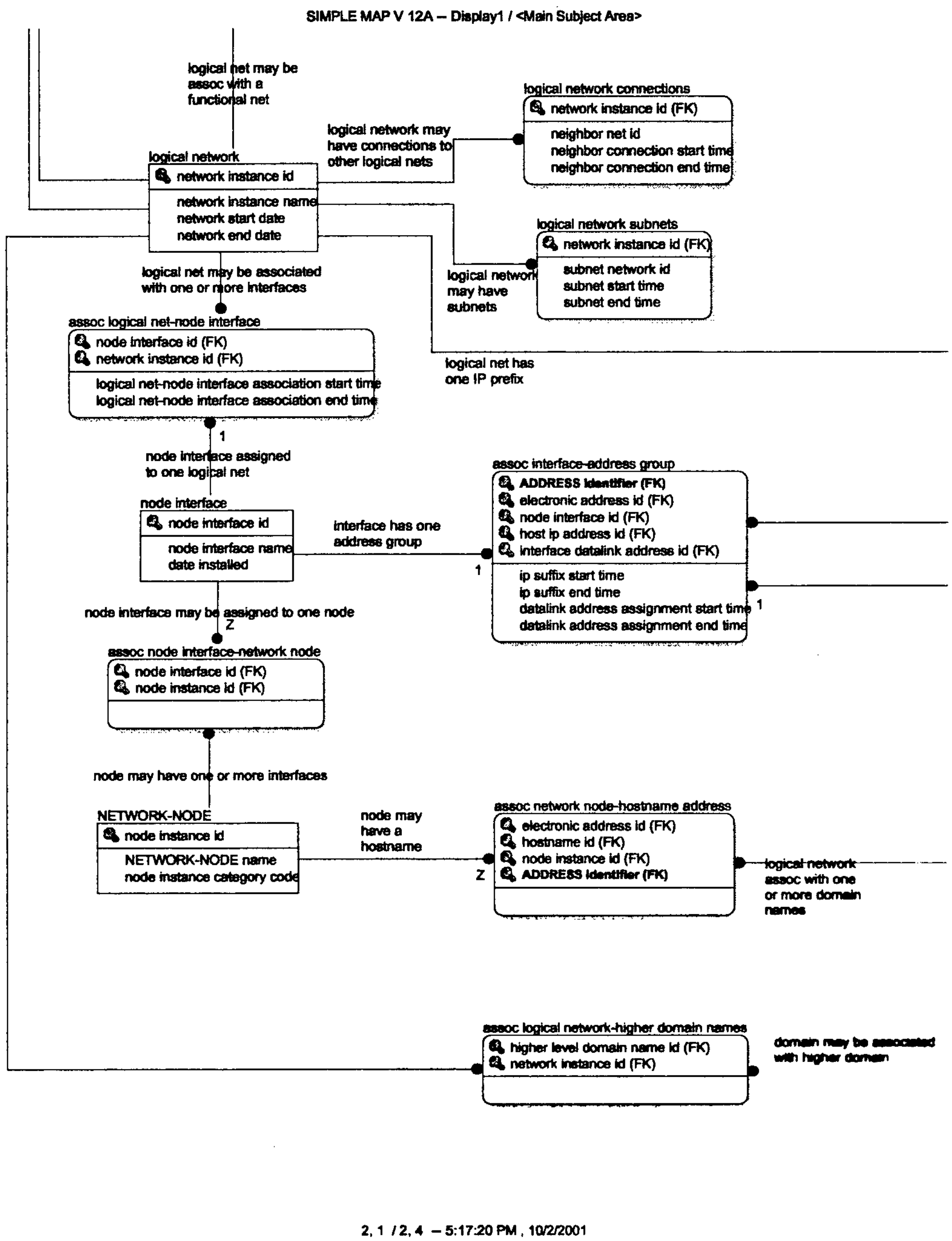
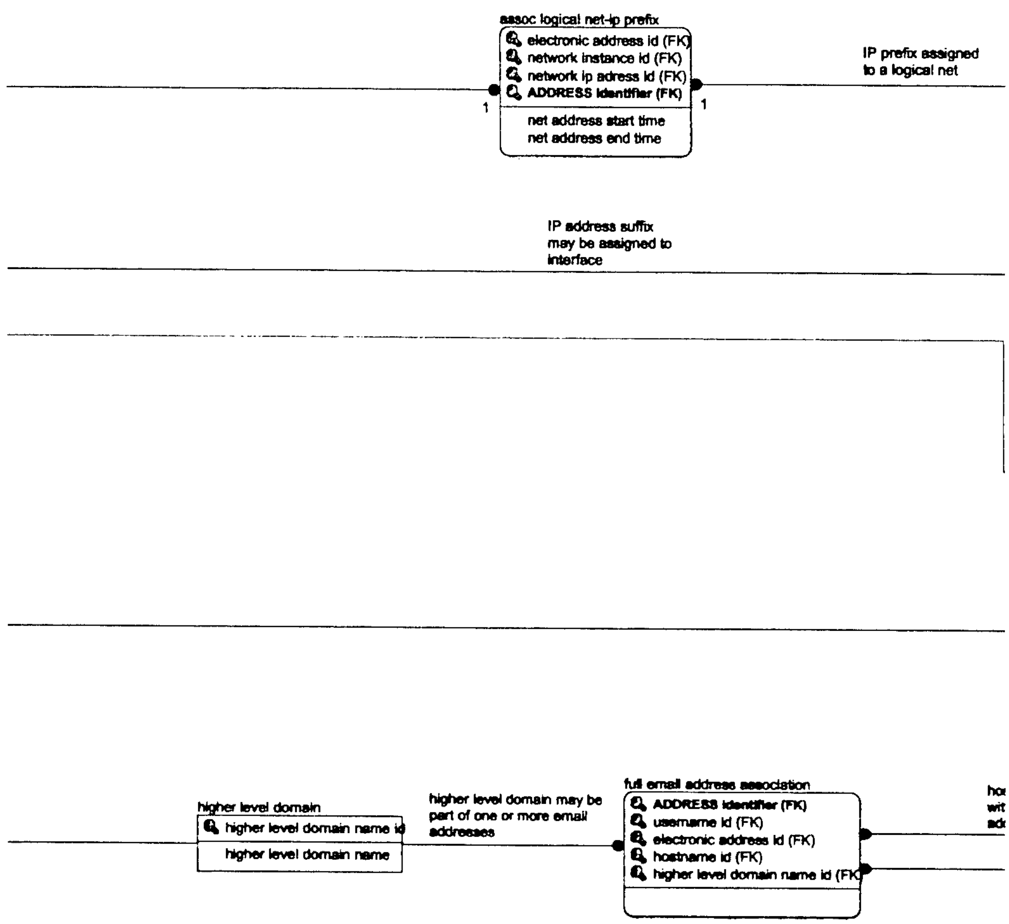


Figure B-5. SIMPLE MAP Version 12A, conceptual network data management modifications inserted into the JCDB-DM Version 4.3, panel 1, row 2 of 2 rows.

SIMPLE MAP V 12A – Display1 / <Main Subject Area>



2, 2 / 2, 4 – 5:17:39 PM , 10/2/2001

Figure B-6. SIMPLE MAP Version 12A, conceptual network data management modifications inserted into the JCDB-DM Version 4.3, panel 2, row 2 of 2 rows.

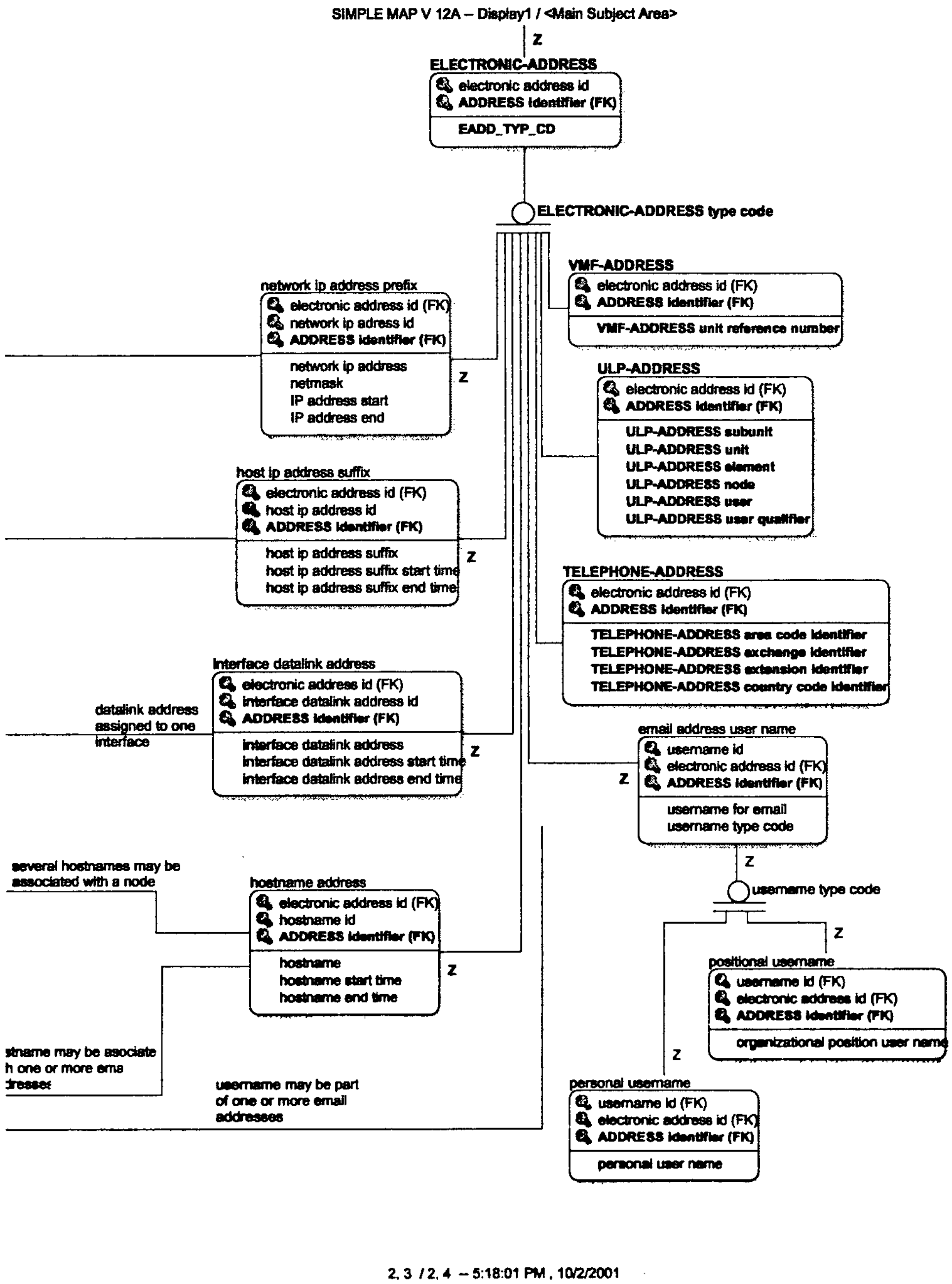


Figure B-7. SIMPLE MAP Version 12A, conceptual network data management modifications inserted into the JCDB-DM Version 4.3, panel 7, row 2 of 2 rows.

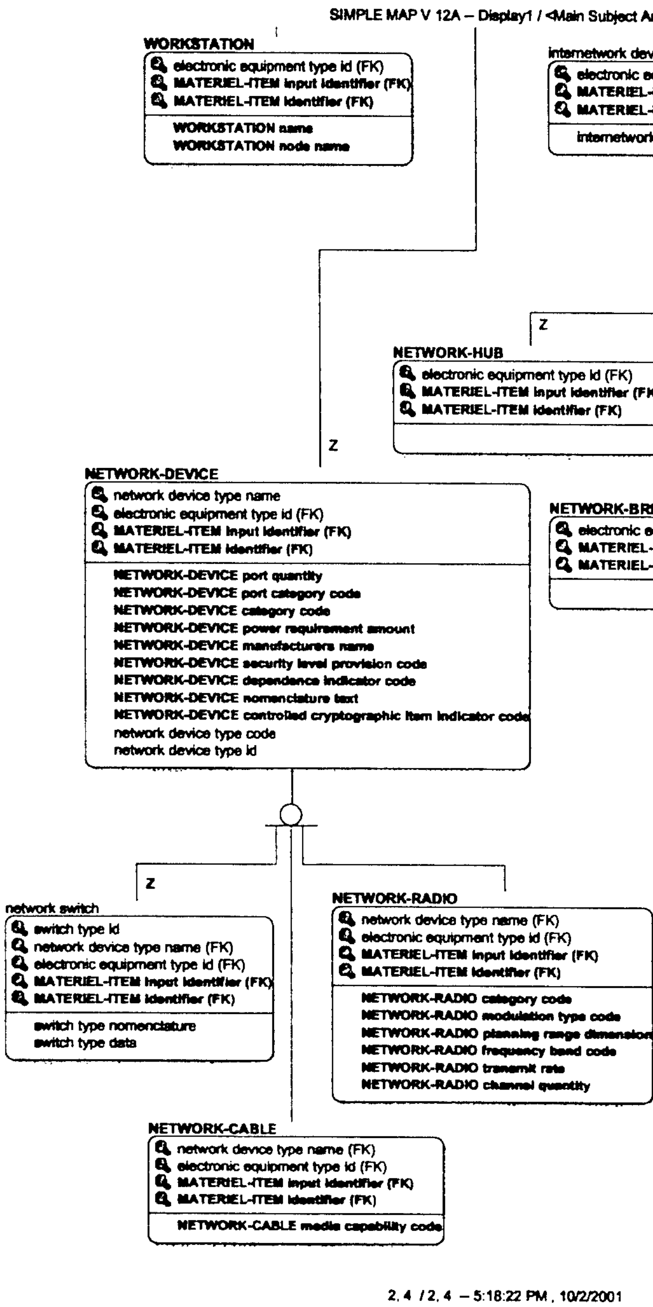


Figure B-8. SIMPLE MAP Version 12A, conceptual network data management modifications inserted into the JCDB-DM Version 4.3, panel 8, row 2 of 2 rows.

Appendix C:

Initial Test Networks for Working Model

INTENTIONALLY LEFT BLANK.

Table C-1. Initial test data for the working model.

A Co. 2/52 AR Network id: 1 Net IP Prefix: 192.168.12	B Co. 2/52 AR Network id: 2 Net IP Prefix: 192.168.11	A Co. 7/41 Mech Network id: 6 Net IP Prefix: 192.168.2
Desc: ws1 net Hostname: surrogate Hw Addr: 225.225 IP Suffix: 115	Desc: ws1 net2 Hostname: serenade Hw Addr: 175.175 IP Suffix: 12	Desc: ws1 net6 Hostname: suspense Hw Addr: 179.179 IP Suffix: 73
Desc: ws2 net Hostname: sundance Hw Addr: 333.333 IP Suffix: 104	Desc: ws2 net2 Hostname: serenity Hw Addr: 176.176 IP Suffix: 63	Desc: ws2 net6 Hostname: surround Hw Addr: 180.180 IP Suffix: 65
Desc: ws3 net1 Hostname: silent Hw Addr: 334.334 IP Suffix: 15	Desc: ws3 net2 Hostname: sneezy Hw Addr: 177.177 IP Suffix: 121	Desc: ws3 net3 Hostname: salient Hw Addr: 181.181 IP Suffix: 167
Desc: gw1 net1 Hostname: somber Hw Addr: 174.174 IP Suffix: 1	Desc: gw1 net2 Hostname: snowy Hw Addr: 178.178 IP Suffix: 1	Desc: gw1 net3 Hostname: sunrise Hw Addr: 182.182 IP Suffix: 1
1PLT A Co. 2/52 AR Network id: 3 Net IP Prefix: 192.168.17	2PLT A Co. 2/52 AR Network id: 4 Net IP Prefix: 192.168.3	3PLT A Co. 7/41 MX Network id: 5 Net IP Prefix: 192.168.8
Desc: ws1 net3 Hostname: sunlight Hw Addr: 3.3 IP Suffix: 8	Desc: ws1 net4 Hostname: sensational Hw Addr: 41.41 IP Suffix: 6	Desc: ws1 net5 Hostname: saint Hw Addr: 56.56 IP Suffix: 44
Desc: ws2 net3 Hostname: sunset Hw Addr: 12.12 IP Suffix: 57	Desc: ws2 net4 Hostname: synapse Hw Addr: 103.103 IP Suffix: 17	Desc: ws2 net5 Hostname: satan Hw Addr: 11.11 IP Suffix: 128
Desc: ws3 net3 Hostname: siamese Hw Addr: 13.13 IP Suffix: 52	Desc: ws3 net4 Hostname: synonym Hw Addr: 107.107 IP Suffix: 51	Desc: ws3 net5 Hostname: samantha Hw Addr: 38.38 IP Suffix: 111
Desc: gw1 net3 Hostname: sargon Hw Addr: 21.21 IP Suffix: 1	Desc: gw1 net4 Hostname: snowy Hw Addr: 15.15 IP Suffix: 1	Desc: gw1 net5 Hostname: sunrise Hw Addr: 117.117 IP Suffix: 1

INTENTIONALLY LEFT BLANK.

Appendix D:

Management Tools for the Network Management Working Subscale Database (Working Model), Version 12A

INTENTIONALLY LEFT BLANK.

Prefatory remark. Use of these forms to manipulate data within Access requires some care due to a peculiarity in the use of autonumbering. The data must be manipulated from the inner subform outward. If the entry is a manipulation of an existing data file on the underlying table, the transaction proceeds normally. If a new data table entry is created, the procedure is less simple. On entry of the first character in the data field of the inner subform, Access generates an error message automatically. This occurs when a new entry is typed in the field requiring an automatically generated primary key number. For a new data line, lack of an existing key entry generates an error message. The act of beginning to type a new entry also generates a new data line and triggers generation of a corresponding key number in the underlying data table. The user then accepts the error message, and the blank data line may be manipulated as desired. The new key value must then be manually added to the next higher subform, generating a change in the data table associating the entry with the next level. This procedure can be avoided if a number of blank entries with corresponding key values are maintained. A production tool would not be hampered by such procedural circumlocutions.

The nested subforms also have data entry windows at each level. This allows data to be manipulated and also allows errors to be found more easily. A production tool could avoid these or put them in a pop-up format to not clutter the display.

The domain name association tool is a form that allows association of a domain name with a network and with a specific hostname (see Figure D-1). No attempt was made to provide hostname-network deconfliction, as this is a not a production tool. Use of this tool allows assignment of a higher level domain name (higher being relative to a specific network). In the screen shot provided, network id 7, "fumble," is the command net for the 2/52 Armor Battalion and is associated with the higher level domain id number 3, 12ad_3bde. An individual's email address associated with the host "sargon" would then have the format user@sargon.12ad_3bde. The rest of the full hostname, ending in ".army.mil" could be added if no other intervening domain names were wanted. The additional subforms allow a user to scroll through the list of hostnames associated with a given network; this is a convenience, not a requirement. The full domain name for a host is defined through the association with the logical net; manipulation of the hostname assignment through this form would be possible but would change the network assignment. The result could have been obtained by use of a query as well as nested subforms.

It should be noted that the names are "smart names;" that is, the network has a name "fumble" that is arbitrary, but part of the name is descriptive. That is only for the convenience of the humans and is not required.

The email address management tool allows assignment of a user name to a specific host. The host is associated with the higher level domain name through its association with a given logical network (see Figure D-2). This also allows both personal and organizational usernames to be assigned to a given host. Association of a specific person with any number of organizational or personal usernames is a straightforward addition. Association of a person directly with a host could, in this scheme, be independent of the association of a person with an organization.

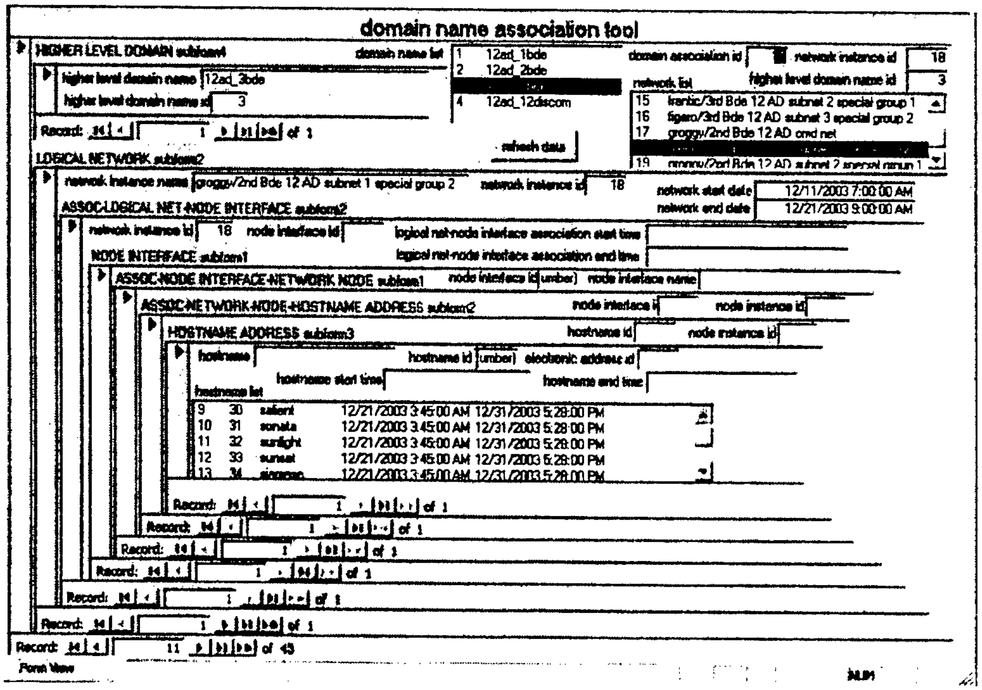


Figure D-1. Domain name association tool.

The logical network management form (Figure D-3) allows association of a given network IP address with a logical network. That is, IP address 192.168.252 is associated with the network "fumble/ 2/52 Armor Bn. Command Net." The unit designation and purpose included in the network name is for convenience in setting up the database. The logical network "fumble" is also associated with a given functional network, 2/52 Armor Bn. Command Net.

The node interface management tool (see Figure D-4) allows manipulation of the relationship between a node and the interface card address. That is, a new interface card may be added to a node and its address associated with the node using this form. A new card may be generated or an address modified using the INTERFACE DATALINK ADDRESS subform and the interface associated with a new node by using the ASSOC INTERFACE ADDRESS GROUP subform. This form also allows association of a given interface address with a host IP address suffix and assignment of the interface to a logical network through the network IP address subform.

This form (Figure D-5) allows management of the parameters associated with a node. The node is associated with a given interface, which can also be done from the interface down

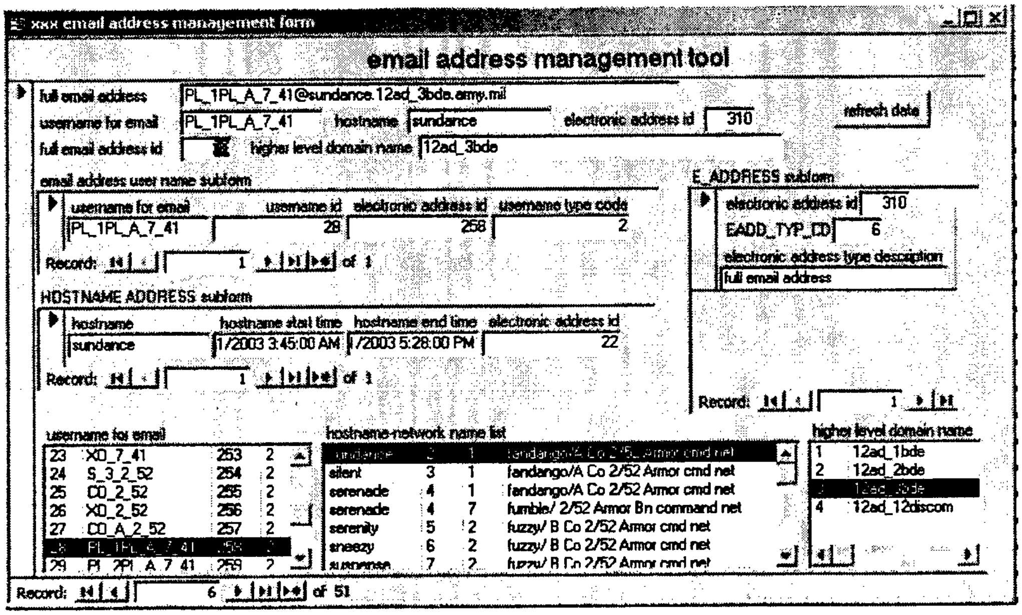


Figure D-2. Email address management tool.

in a preceding form. The interface is the element of the data structure that is associated with the host IP address suffix and the interface address. Those must be manipulated separately.

Subnetting can be managed with the form in Figure D-6. It manipulates the table associating subnets with a primary or master network. It is desirable for the subnetting relationship to be described by a recursion relationship with the network list, but for simplicity, a separate table is used. This form can be used to generate subnets as well as linking existing nets. Actions to insert the new subnets into the master list of networks could be programmed into the form if desired but, for simplicity, were not.

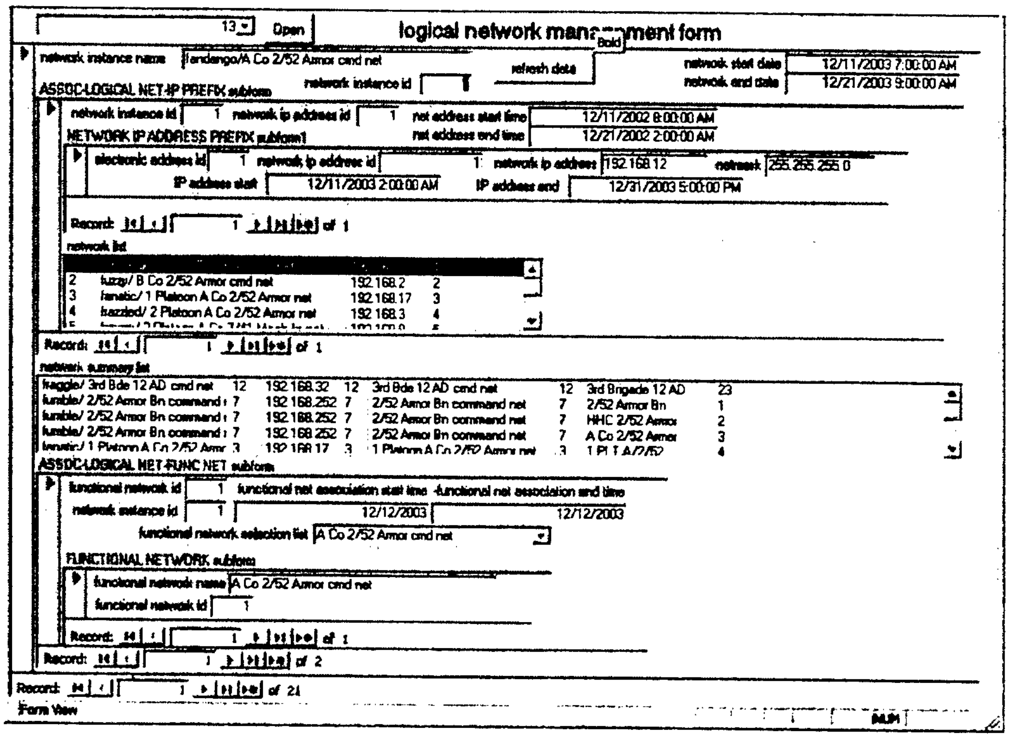


Figure D-3. Logical network management form.

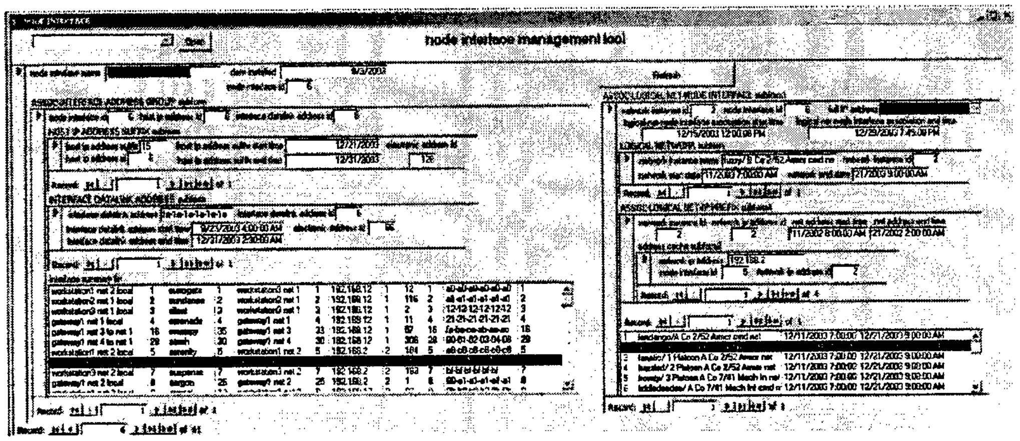


Figure D-4. Node interface management tool.

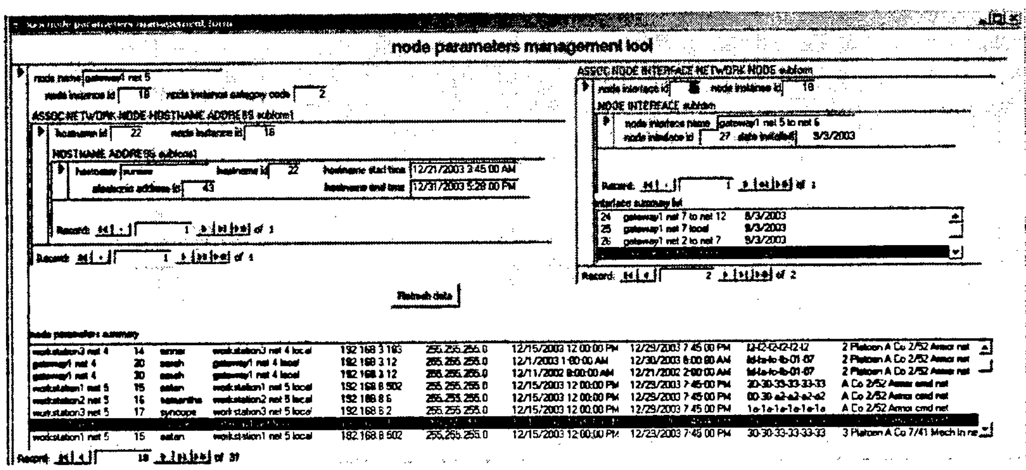


Figure D-5. Node parameter management tool.

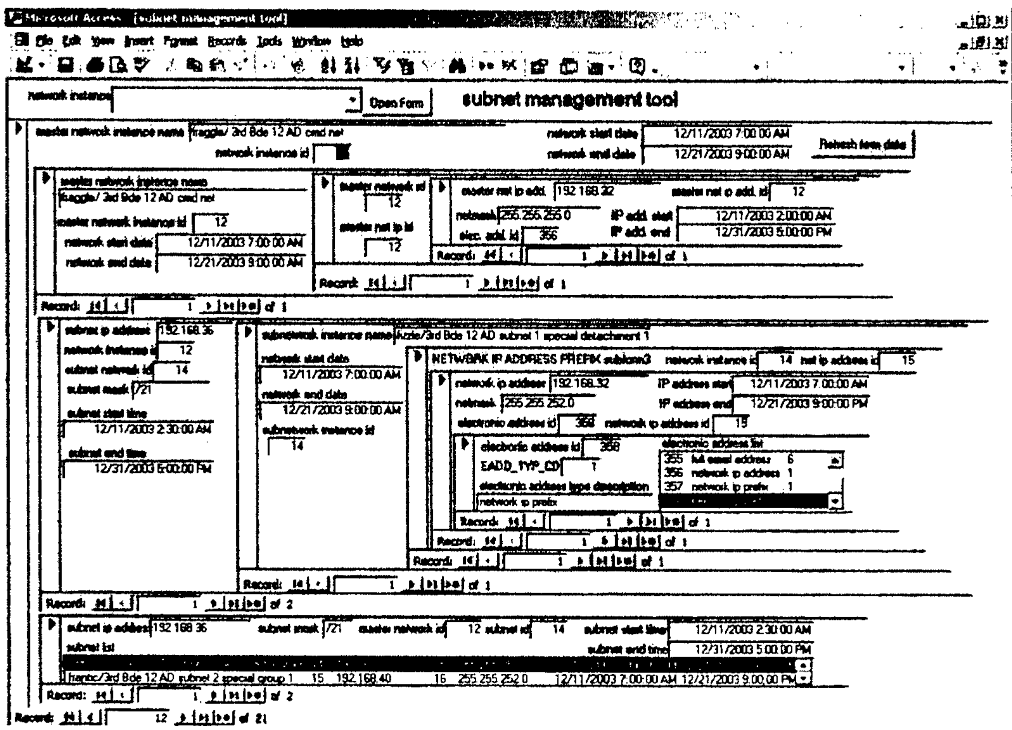


Figure D-6. Subnet management tool.

NO. OF COPIES	ORGANIZATION
2	DEFENSE TECHNICAL INFORMATION CENTER DTIC OCA 8725 JOHN J KINGMAN RD STE 0944 FT BELVOIR VA 22060-6218
1	HQDA DAMO FDT 400 ARMY PENTAGON WASHINGTON DC 20310-0460
1	OSD OUSD(A&T)/ODDR&E(R) DR R J TREW 3800 DEFENSE PENTAGON WASHINGTON DC 20301-3800
1	COMMANDING GENERAL US ARMY MATERIEL CMD AMCRDA TF 5001 EISENHOWER AVE ALEXANDRIA VA 22333-0001
1	INST FOR ADVNCD TCHNLGY THE UNIV OF TEXAS AT AUSTIN 3925 W BRAKER LN STE 400 AUSTIN TX 78759-5316
1	US MILITARY ACADEMY MATH SCI CTR EXCELLENCE MADN MATH THAYER HALL WEST POINT NY 10996-1786
1	DIRECTOR US ARMY RESEARCH LAB AMSRL D DR D SMITH 2800 POWDER MILL RD ADELPHI MD 20783-1197
1	DIRECTOR US ARMY RESEARCH LAB AMSRL CI AI R 2800 POWDER MILL RD ADELPHI MD 20783-1197
3	DIRECTOR US ARMY RESEARCH LAB AMSRL CI LL 2800 POWDER MILL RD ADELPHI MD 20783-1197

NO. OF COPIES	ORGANIZATION
3	DIRECTOR US ARMY RESEARCH LAB AMSRL CI IS T 2800 POWDER MILL RD ADELPHI MD 20783-1197
	ABERDEEN PROVING GROUND
2	DIR USARL AMSRL CI LP (BLDG 305)

NO. OF COPIES	ORGANIZATION
1	PEO C3T SFAE C3T PM GCC2 R CARNAVEL BLDG 2525 FT MONMOUTH NJ 07703
1	INSTITUTE FOR DEFENSE ANALYSIS R WALKER 4850 MARK CENTER DR ALEXANDRIA VA 22311-1882
1	DCD MATERIAL REQUIREMENTS DIVISION M HAYTHORN 506 CHAMBERLAIN AVE BLDG 29808 3RD FLOOR FT GORDON GA 30905
	ABERDEEN PROVING GROUND
24	DIR USARL AMSRL CI CT B BODT J BRAND (5 CPS) A BRODEEN F BRUNDICK S CHAMBERLAIN (5 CPS) J DUMER T HANRATTY G HARTWIG (5 CPS) R HELFMAN H INGHAM P JONES M LOPEZ

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	July 2002	Final, October 2000–October 2001

4. TITLE AND SUBTITLE
Management of Tactical Ad Hoc Networks With C2 Data Models

5. FUNDING NUMBERS
622120.H16

6. AUTHOR(S)
John H. Brand and George W. Hartwig

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Research Laboratory
ATTN: AMSRL-CI-CT
Aberdeen Proving Ground, MD 21005-5067

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-TR-2784

9. SPONSORING/MONITORING AGENCY NAMES(S) AND ADDRESS(ES)

10.SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT*(Maximum 200 words)*

The U.S. Army Research Laboratory is investigating the exploitation of preloaded reference data to solve problems in tactical network management. By closely evaluating how communication networks are described in tactical database models such as the Joint Common Database (JCDB), information about the tactical situation can be used to help direct, or at least refine, the process of reconfiguring ad hoc networks. Because the structure of current networks closely follows organizational structures, the concept of Default Operational Organizations (DOO) is being used as a starting point for the evaluation. The DOO concept will be used to address the problem of managing internet protocol addresses in rapidly changing ad hoc organizations to minimize overhead traffic on congested, low-capacity networks. Reducing network loading and improving network response are very important to network centric weapon systems such as the Future Combat System. Based on the data needs for network management, modifications to the IDEF1X database model representing the JCDB are proposed. A working model of an Access database based on a limited, notional test database using these modifications is described.

This study has produced suggested modifications to the existing JCDB-DM that will enhance the ability to rapidly configure networks with reduced network management overhead.

14. SUBJECT TERMS
network modeling, joint data model, organizational identifier

15. NUMBER OF PAGES
58

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18 298-102

INTENTIONALLY LEFT BLANK.