

Joint Total Asset Visibility System Architecture



VOLUME II

Joint Total Asset Visibility Office

October 6, 1997

Table of Contents

1 INTRODUCTION.....	1
1.1 Background	1
1.2 Purpose	1
1.3 Scope.....	1
2 DEVELOPMENT APPROACH.....	2
2.1 C4ISR Guidelines	2
2.2 JTAV Operational Architecture Inputs.....	2
2.2.1 Process Flows	2
2.2.2 Information Exchange Requirements (IER) Matrix.....	3
2.3 Data Information Requirements Definition	3
2.4 System/Database Identification.....	3
3 SYSTEM ARCHITECTURE SUMMARY	4
3.1 Overview.....	4
3.2 System Architecture Components.....	7
3.2.1 JTAV User Interface.....	8
3.2.2 JTAV Application Servers.....	9
3.2.3 Data Access Servers.....	11
3.2.4 Global Data Access Services.....	12
3.3 Node Definition.....	13
3.3.1 User Nodes	14
3.3.2 Data Provider Nodes	15
3.3.3 Communications Nodes	15
3.4 Node Connectivity.....	15
3.5 Node Configuration.....	19
3.5.1 User Nodes	19
3.5.2 JTAV Nodes	20
3.5.3 USTRANSCOM Node.....	20
3.5.4 DAASC Node.....	21
3.5.5 Component / Service / Agency Nodes (Data Sources).....	22
3.5.6 Communications Nodes	22
4 DESIGN CRITERIA AND ALTERNATIVES.....	23
4.1 Overview.....	23

4.2 Evaluation Criteria	23
4.3 User Interface	24
4.3.1 User Interface Alternatives	24
4.3.2 User Interface Recommendations	25
4.4 Data Access	26
4.4.1 Data Types	26
4.4.2 Data Access Factors.....	26
4.4.3 Data Access Control.....	28
4.4.4 Data Access Recommendations.....	28
4.5 Data Quality.....	28
4.6 Data Topology.....	29
4.7 Data Management Responsibility.....	30
4.8 JTAV Security.....	31
4.8.1 Security Requirements Description.....	32
4.8.2 Security Mechanisms.....	33
4.8.3 Security Alternatives.....	34
4.8.4 Security Recommendations.....	35
5 SYSTEM ARCHITECTURE APPLICATION AND USE.....	36
5.1 Technical Architecture.....	36
5.2 Specific Configurations	36
5.3 Implementation Plan.....	40
Appendix A: Asset Visibility Source Systems And Databases.....	41
Appendix B: JTAV In Theater Interfaces To Data Source Systems	43
Appendix C: Node Identification and Node Connectivity Diagrams Node Identification.....	44
Appendix D: Node Configuration	57
Appendix E: Common Operating Environment (COE) Services.....	66

Figures

Figure 3.1-1 Jtav “As Is” System Architecture	5
Figure 3.1-2 Jtav “To Be” System Architecture	7
Figure 3.2-1 General System Architecture	8
Figure 3.2-2 Application Or Web Server Architecture	10
Figure3.2-3 Dynamic Web Page Generation	11

Figure 3.2-3 Gdas Architecture.....	12
Figure 3.3-1 Total Asset Visibility Nodes.....	14
Figure 3.4-1 Query / Query Results Flow From User Workstation To Legacy System.....	16
Figure 3.4-2 Legacy System To Shared Data Resource Node Connectivity/System Overlay Diagram.....	17
Figure 3.4-3 Shared Data Resource To Gdas Node Connectivity/System Overlay Diagram	18
Figure 3.4-4 Gdas To User Node Connectivity/System Overlay Diagram.....	18
Figure 3.5-1 Total Asset Visibility User Node (General)	19
Figure 3.5-2 Jtav Node System Configuration (General)	20
Figure 3.5-3 Ustranscom Node System Configuration.....	21
Figure 3.5-4 Daasc Node System Configuration.....	21
Figure 3.5-5 Defense Megacenter Node System Configuration (General)	22
Figure 5.2-1 Specific Configuration Translation Process	37
Figure 5.2-2 Current Site Configurations	38
Figure 5.2-3 Architecture Design Alternatives	39
Figure 5.2-4 Selected Architecture Design With Migration Path.....	39

Tables

Table 4.2-1 Alternative Analysis by Weighted Criteria.....	24
Table 4.4-1 Data Access Factors for Total Asset Visibility Data.....	27
Table 4.5-1 Total Asset Visibility Data Location Alternatives.....	29

1.0 Introduction

1.1 Background

The Department of Defense (DoD) logistics and personnel business processes, including those involving joint deployments, require visibility of assets in-storage, in-process, and in-transit in the continental United States and all theaters of operation. Without this visibility, redundant material orders, inaccurate personnel accounting, and a general lack of confidence in the dependability of the logistic and personnel, pipelines will continue to plague DoD. The Deputy Under Secretary of Defense (Logistics) (DUSD(L)) established the Joint Total Asset Visibility (JTAV) Office to develop a clear, comprehensive plan for implementing an integrated JTAV capability throughout DoD. This capability is to provide timely and accurate information on the location, movement, status, and identity of units, personnel, equipment, and supplies. Achieving JTAV is an enormous task that involves all logistics disciplines and DoD components. Several organizations have put substantial effort into JTAV related architectures in recent years, however their work was not synchronized nor integrated. In response to this situation the JTAV Integrated Process Team (JIPT) was established to develop JTAV Operational and System “To Be” Architectures.

1.2 Purpose

The purpose of this document is to define the JTAV System “To Be” Architecture. The document provides a summary of the system architecture concept, discusses design alternatives and issues, and describes the necessary infrastructure and methodology for applying the system architecture to specific installations and configurations. The system architecture was intentionally developed to be generic in nature; allowing maximum flexibility to support the differences in operational parameters and technical capabilities that exist at individual sites.

1.3 Scope

This document assumes the existence and infrastructure of the JTAV “As Is” architecture and provides the information necessary to develop an implementation plan for moving toward a JTAV “To Be” system architecture by the year 2000. The document is considered a living document and anticipates the incorporation of emerging technologies.

2.0 Development Approach

2.1 C4ISR Guidelines

The Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Architecture Framework was developed to provide a common basis for developing architectures that can be universally understood and readily compared to other architectures. It will facilitate the reuse of architectural information and results, and will serve as the foundation for expansion and integration of architectures across organizational and functional boundaries.

The C4ISR provides the following architecture definitions:

- **Operational Architecture:** Descriptions of the tasks, operational elements, and information flows required to accomplish or support a warfighting function.
- **Systems Architecture:** Descriptions, including graphics, of systems and interconnections providing for or supporting warfighting functions.
- **Technical Architecture:** A minimal set of rules governing the arrangement, interaction, and interdependence of all the parts or elements whose purpose is to ensure that a conferment system satisfies a specified set of requirements.

These definitions clarify the distinctions among the types of architectures, emphasizing the precept operational architectures present the functional or logical requirements while the system and technical architectures describe the physical capabilities that actually meet operational needs.

2.2 JTAV Operational Architecture Inputs

Development of the JTAV System Architecture is dependent upon receiving inputs from the JTAV Operational Architecture that describe process flows and defines the activities, users, and information exchange requirements (IER). The JTAV Operational Architecture, Volume I, Mobilization, Deployment, Sustainment, Employment and Redeployment, defines the current architecture products provided for JTAV System Architecture development.

2.2.1 Process Flows

The JTAV Process Flows: define the specific activities and events associated with each phase of a warfighting process; identify which event/activity has an asset visibility requirement; and, specify the specific users associated with a particular activity/event. The JTAV Operational Architecture, Volume I, Mobilization, Deployment, Sustainment, Employment and Redeployment, Appendix B defines the specific activities and sub-tasks, identifies asset visibility requirements and specific users associated with each phase of Joint Warfighting.

2.2.2 Information Exchange Requirements (IER) Matrix

The information exchange requirements (IER) matrix defines the requirements for information to be passed between and among forces, organizations, or administrative structures concerning ongoing activities. The IERs are built from the information provided by the process flows and user identification. IERs identify *who* exchanges *what* information with *whom* as well as *why* the information is necessary and *how* that information will be used. The IER also includes the information attributes such as quality, quantity, and type of information. The JTAV Operational Architecture, Volume I, Mobilization, Deployment, Sustainment, Employment and Redeployment, Appendices C, D, and E provides the IERs for use by the JTAV System Architecture.

2.3 Data Information Requirements Definition

The JTAV Operational Architecture specifies the users and define the activities/events that occurs within a business process, (e.g. Deployment), and identify which of those activities/events have an asset visibility requirement. Based on this input the specific asset visibility data requirement can be identified.

2.4 System/Database Identification

Once the specific asset visibility data requirement has been identified, the systems, databases, and specific data elements containing the data needed to satisfy the requirement can be identified. In addition to identifying the specific databases, information on access frequency, classification, user location, user interface type, database location and infrastructure characteristics (communication bandwidth in particular) will be collected.

A list of the currently identified Asset Visibility Source Systems and Databases is contained in Appendix A. The databases currently being accessed by JTAV In Theater, together with their interfaces, is listed in Appendix B.

3.0 System Architecture Summary

3.1 Overview

The JTAV system architecture is the foundation enabling total asset visibility users to obtain quality data. Characteristics of quality data are accuracy, integrity, accessibility, timeliness, relevance, consistency, and completeness. In the total asset visibility system architecture, quality data is provided through several different data access methods. This architecture makes the data access process transparent to the user. The system architecture components are described in Section 3.1, Section 3.2 describes the three major types of nodes, Section 3.3 details the interaction between the nodes, and Section 3.4 is a description of the physical system configurations at each node.

Figure 3.1-1 depicts the JTAV business environment in the “As Is” System Architecture. The current architecture consists of two views: a theater user’s view and an Inventory Control Point (ICP) user’s view. At the ICP, local business applications are used to access both local and globally distributed shared data. Theater users access asset visibility information from the JTAV database. The theater architecture components include:

- A user workstation executing JTAV client functions (query creation);
- A JTAV server providing query processing functions using client server technology;
- A JTAV database containing theater specific data and GTN, DAAS, and ATAV data;
- A local LAN providing user access to the JTAV server and database; and
- SIPRNET/NIPRNET communication facilities to download data from CONUS.

The significant architectural characteristics for the “As Is” architecture are:

Application software resides on the workstation, allowing only one type of workstation to be used, and allowing only one user to access the application from the workstation (single user/single box);

- The architecture is based on client/server technology using a fat client, demanding heavy client resources, and not taking advantage of current web technology;
- Information is fused at the time the database is loaded, which does not support Ad Hoc query capabilities; and
- Data is tailored to the theater environment and specific user group resulting in only pre-staged data being available to users.

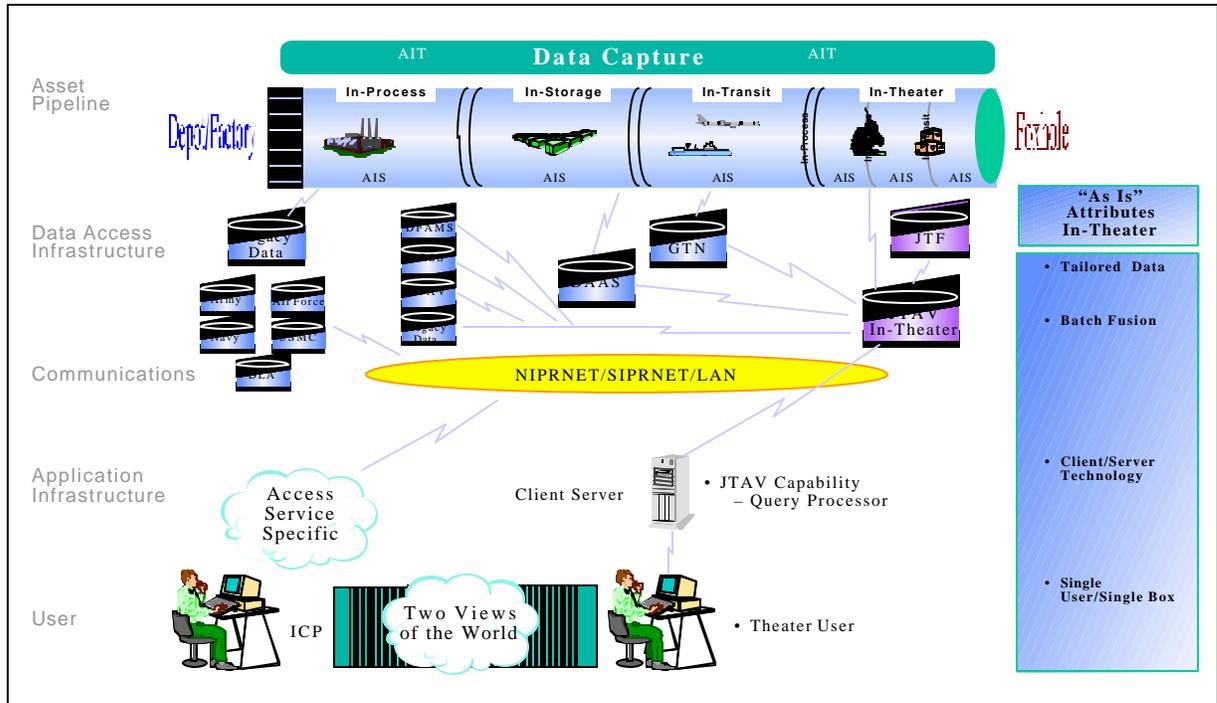


Figure 3.1-1 JTAV “As Is” System Architecture

Achieving the JTAV “To Be” system Architecture, pictured in Figure 3.1-2, requires obtaining inputs from four sources:

- Requirements from the Operational Architecture effort;
- Management direction about issues beyond JTAV’s immediate control;
- GCSS design principles; and
- Existing JTAV System Architecture.

System architecture requirements are provided in the form of a Information Exchange Requirements (IER) matrix produced during the operational architecture phase. The contents of the IER are:

- Supported Operational Tasks - Military activity supported within deployment, sustainment, and redeployment processes and identification of asset visibility requirements;
- Operation Elements Involved - Producing and consuming nodes for asset visibility information supporting that activity;
- Description of Information - Description of asset visibility information required;

- Data Source - Authoritative source for the required asset visibility information (in terms of application database) including data element identification;
- Quality - User requirements for data timeliness, accuracy, and completeness; and
- Quantity - The amount or frequency of data required per time period by the consuming node.

A number of assumptions were made to arrive at the JTAV “To Be” System Architecture. Two major assumptions are that communications capacity and response time are not a constraint and that technology supporting access control will be available.

A third set of architectural constraints come from the GCSS design principles, and a fourth set from the existing JTAV prototype architecture. These include the following:

- Data access is primarily an issue to be resolved by the architecture;
- Data quality is the responsibility of the data provider;
- Fused information is required;
- The architecture must be flexible enough to allow extension to GCSS;
- The architecture must support data access from COTS and user customized applications;
- The architecture must be DII/COE compliant; and
- The architecture must support a migration path from the existing JTAV system architecture.

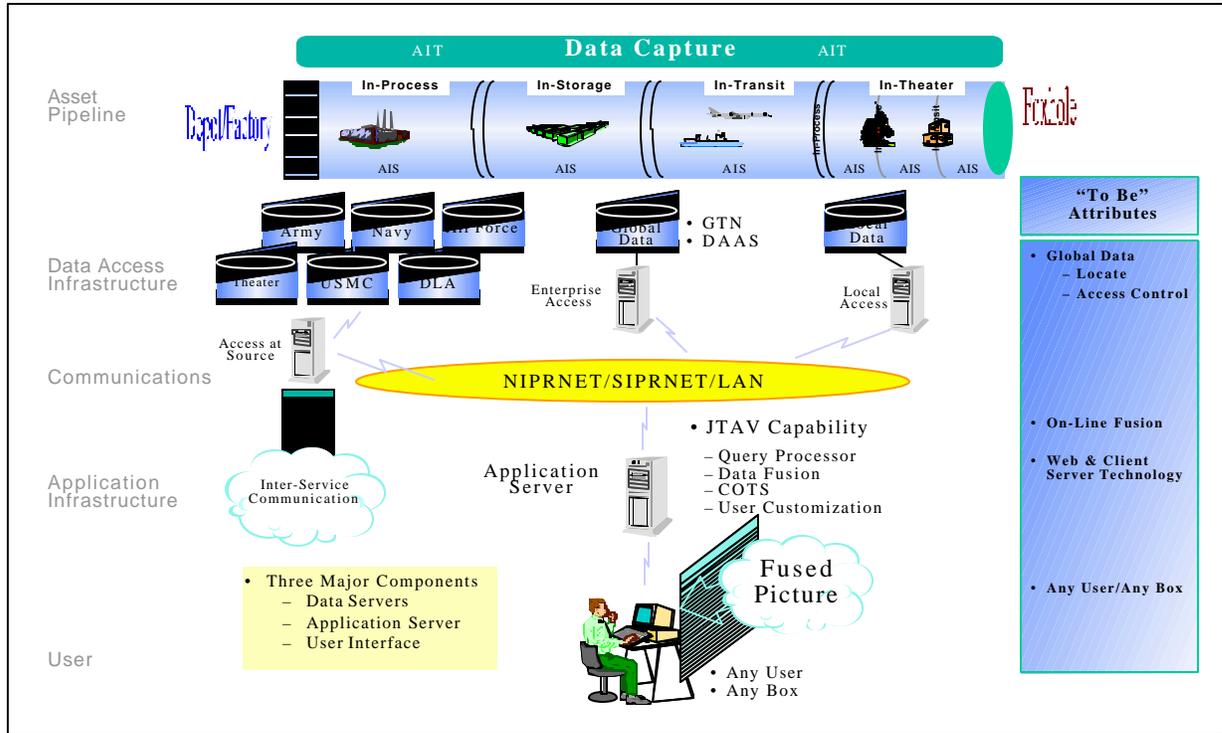


Figure 3.1-2 JTAV “To Be” System Architecture

3.2 System Architecture Components

The components of the system architecture can be grouped into three major categories: client/server interface, data access servers, and Global Data Access Services (GDAS). Figure 3.2-1 depicts the components of the total asset visibility system architecture. The following subsections describe each component that makes up the architecture. The descriptions include a definition of the component, its basic functionality, and how this component will provide and/or receive data.

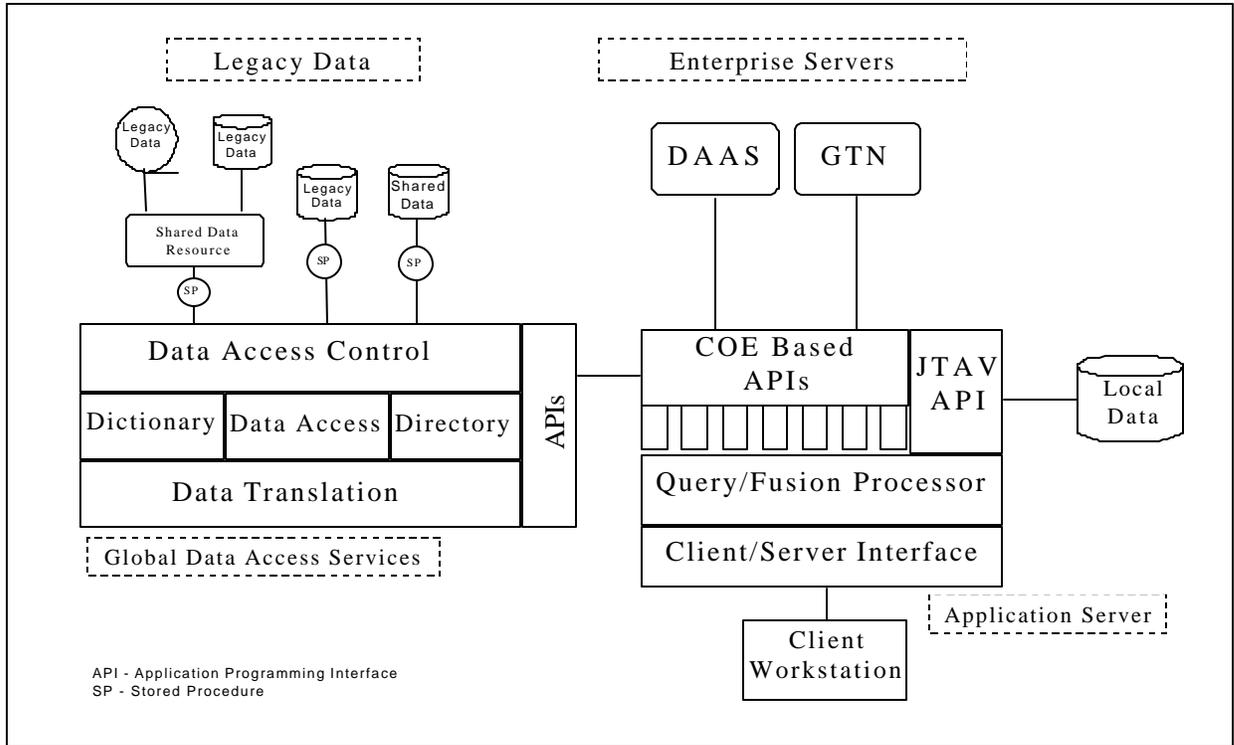


Figure 3.2-1 General System Architecture

3.2.1 JTAV User Interface

The total asset visibility system architecture will use a client/server architecture for the user interface. The client/server architecture for the user node is comprised of a user workstation and a total asset visibility server. The client workstation requests information or services from the server. Clients contain the presentation portion of the application. The server hosts the software necessary to perform application processing, manage databases, and provide services to the client. The following paragraphs describe JTAV clients; JTAV servers are discussed in section 3.1.2.

Two types of user interfaces will be available in the total asset visibility system architecture. User sites can choose between a traditional client/server configuration and a web browser/web server configuration. This choice allows users to select the configuration which best suits their needs at the time of JTAV implementation. Due to the enhanced capability of web technology, it is recommended that all user sites eventually move to the web browser/web server solution. Many user sites are already using web technology to access applications and will be able to use the web solution right away. For those sites still using traditional client/server methods, an incremental implementation of web technology will reduce the impact of training and cost on the site.

a. Application Client Workstation

Users have the option of creating an ad hoc query or using a canned query provided by the application. Once a user has requested a query, the application client software will build a Structured Query Language (SQL) query. The client then sends the query to the application server for processing. Periodically, the client polls the server for the completion status of the query. Once it gets the proper signal, the client reads the results from the application server and displays the results to the user.

b. Web Client

The web client uses a web browser to provide a universal client interface for all applications using World Wide Web (WWW) based protocols and standards, for example HyperText Transfer Protocol (HTTP), and HyperText Markup Language (HTML). HTTP provides the protocol for communication between the client browser and the web server, while HTML provides the standard format for 'pages' or documents transferred from the web server for display within the web browser.

3.2.2 JTAV Application Servers

User requirements will determine the type of client/server configuration. In some cases the server will be a traditional application server and in others a web server will be used. Regardless of the client/server configuration a user node decides to implement, total asset visibility clients will be "thin" clients. This means that the bulk of the application processing will be done on the server rather than the client. This architecture has many advantages. The primary advantage is that it offers central control over the applications. In addition, thin client architectures place hardware requirements on the server rather than the clients.

a. Traditional Application Server

Once the application server receives a query from the client workstation, it begins to process the query. The application server performs any necessary translation of the query and then executes the query. When the query has finished executing, the application server prepares the results to be returned to the user. This includes any translation required to present the query results in the proper format. The server then stages the results for access by the client workstation.

b. Web Technology Application Server

The Web server interacts with the client browser through the HTTP protocol to supply pages or 'screens' to the client workstation. As the client selects from pick lists on his browser interface to navigate from one screen of the application to another, the web server returns the appropriate page and component objects (such as graphics) for display on the client browser. The web server can be considered a librarian for the total asset visibility system, which selects appropriate documents from the web server's repository for delivery to the client, based on its indicated choice.

In the web server, HTML documents will be dynamically generated from data stored in relational databases and other data repositories. These technologies rely on a standardized methodology such as the Common Gateway Interface (CGI) or on a documented Application Program Interface (API) to activate scripts or applications which communicate with the supporting database. The web server is made up of the four modules shown in Figure 3.2-2 and described below.

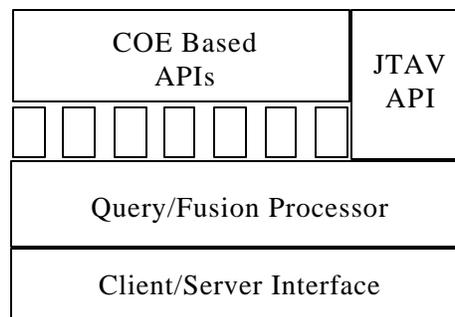


Figure 3.2-2 Application or Web Server Architecture

- **Web Client/Server Interface** - This is a COTS product and acts as a front end to the other modules of the web server. The server interface is the module that communicates with the client web browser. This allows users to use a standard COTS access method to reach data hosted on disparate systems. The communication mechanism between the server interface and the client is through an intranet or LAN.
- **Query / Fusion Processor** - To originate the query, the user will do one of two things. Either he will submit a canned query, or he will create an ad hoc query. The ad hoc query is built through the use of web pages that resemble forms to be filled out. Each blank line of the form will either require the user to type input or will have a drop down pick list that the user selects from. These pick lists are drawn from their respective databases. The user's selections determine which route the query will take. GDAS pick lists are based on a metadata dictionary, giving a common view of data. GTN pick lists are dynamically created as the user makes initial choices. JTAV pick lists are based on a combination of fixed

menus and dynamically created lists. These lists are built by incrementally narrowing the user's area of interest.

The query processor responds to requests from the web browser for dynamic web pages by activating the script/program associated with that page. The associated program formulates the query, develops the page templates, and activates, through the web server API, the associated application on the query processor.

After the result set is delivered back to the requesting program by the data access server, it is merged with the static page template as shown in Figure 3.2-3. The merged document is sent back by the query processor to the web server, which then transfers it for viewing to the web client. It is this mechanism which allows the web pages to display current, up-to-date information from the data providers' data repositories.

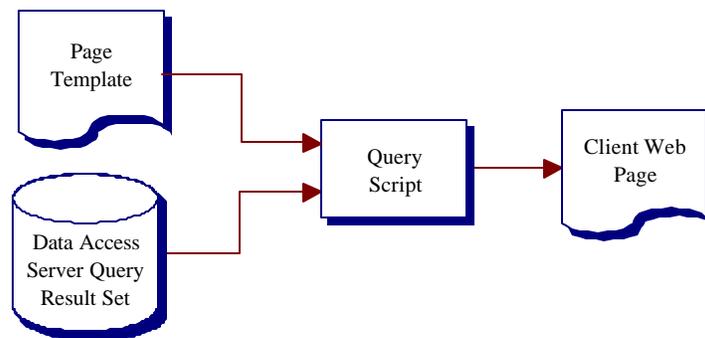


Figure 3.2-3 Dynamic Web Page Generation

- **COE Based, JTA V APIs** - These APIs allow the web server to communicate with their respective data access servers. They are implemented in accordance with the requirements of the source system. COE based APIs are standardized APIs used to access segments of the DII COE.

3.2.3 Data Access Servers

Data access servers are the primary mechanisms that provide information to total asset visibility users. There are three main points of data collection in the total asset visibility system architecture: shared data resource servers, local servers, and enterprise servers. Each of these systems obtains data from authoritative sources and aggregates the data in the manner that is useful to the total asset visibility user.

- **Shared Data Resource Servers** - Shared data resource servers will be located in CONUS. These servers are a collection point for directly downloaded legacy data. This data is stored in a centralized database and managed as corporate data. There are several reasons these data servers are necessary: there may be no direct access to operational data, increased reliability, better performance, enhanced security, and the avoidance of impact to

operational data. Users interact with these servers through the use of global data access services (GDAS).

- Local Servers** - These servers are a collection point for directly downloaded asset visibility data. Theater users interact with these servers via the client/server interface using a JTAV API. CONUS users must access JTAV data through the use of GDAS. JTF units will maintain their own local servers from downloads of the in-theater local data. This will allow the JTF to have a portable copy of the data. In-theater local servers currently receive downloads from the following systems: ATAV, DFAMS, DBSS, SBSS, RF/ITV, FITS-Navy, AMS, JTRACS, USAF-Unit Equipment, and CAS.
- Enterprise Servers** - There are currently two systems which supply enterprise services: The Global Transportation Network (GTN) System and the Defense Automatic Addressing System (DAAS)/ Logistics Information Processing System (LIPS). GTN is a centralized system that gathers transportation data from many disparate systems, aggregates the information, then downloads the information to its users. The GTN system will have a separate enterprise database containing replicated GTN data that is of interest to total asset visibility users. GTN's interface with asset visibility users will be via COE based APIs. The DAAS/LIPS system is comprised of many databases containing information pertaining to requisitions. DAAS will also provide data to asset visibility users through COE based APIs.

3.2.4 Global Data Access Services

Global Data Access Services (GDAS) are mechanisms which provide data, direct queries to the proper location, and translate data to the desired format. Interaction with other systems is done through the use of a standard application program interface (API), or stored procedures (SP). GDAS segments are shown in Figure 3.2-3. GDAS functionality is described following the figure.

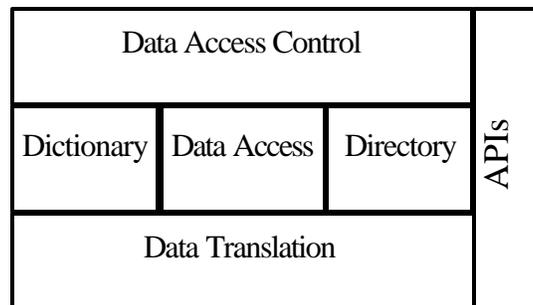


Figure 3.2-3 GDAS Architecture

- **Data Translation Service** - provides the processes necessary to access data from databases using unique protocols and formats. This service uses the conceptual to logical metadata mappings from the data dictionary to identify the logical tables necessary to respond to the user query. For simple queries, table joins can be built dynamically and are limited to only the required columns. More complex queries use a predefined conceptual view that appears as logical tables in the data dictionary.
- **Data Access Control Service** - implements DoD security policy on access to two different processing environments. The first is an environment where data is at most sensitive but unclassified while the second is a classified environment operated in a system high mode. User access is based on community of interest. The Data Access Control Service is integrated with the data access service and supports ad hoc queries for data across the global shared data environment.
- **Data Directory Service** - provides information on the location of data modules within the shared data environment. This information is used by the Data Access Service to route requests for data to the appropriate data stores.
- **Data Dictionary Service** - provides metadata describing the common view of data within the shared data environment and mapping information required to translate legacy data into the common view. The Data Dictionary Service is used by the Data Access Service to translate queries of data in data stores and to translate data retrieved from legacy data stores into the common shared data view.
- **Data Access Service** - interprets the user request to retrieve data, execute the requested function, and provide status information to the user. In those cases where a retrieval request requires data from multiple databases these mechanisms provide for data translation and aggregation as required. The Data Access Service retrieves legacy data via stored procedures (SPs).

3.3 Node Definition

The total asset visibility system consists of data user nodes, data provider nodes, and communication nodes. The data provider nodes are further divided into Global Data Access nodes, JTAV nodes, Enterprise nodes, and Service/Component/Agency nodes. Figure 3.3-1 graphically depicts the classes of nodes in the total asset visibility architecture. The types of nodes are described in the following sections. The system configuration of each node type is described in section 3.4.

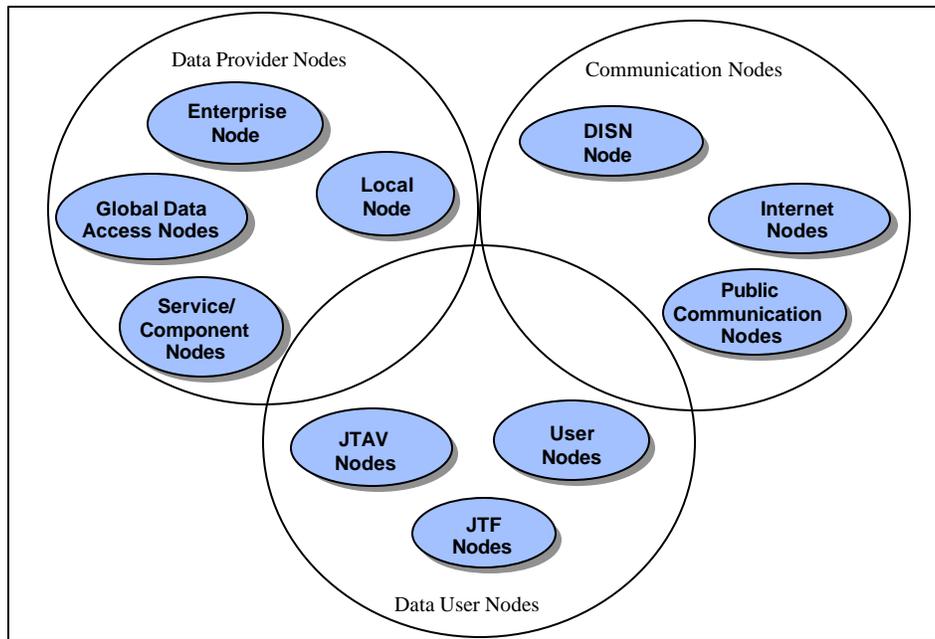


Figure 3.3-1 Total Asset Visibility Nodes

3.3.1 User Nodes

User nodes will be configured in a client/server architecture. In most cases users, both in theater and in CONUS, will interact with the other nodes of the system through the use of a web browser. This web browser links through an intranet to a web server. The users send ad hoc or canned queries to the web server. The web server then returns the results in an HTML format to the user. Some exceptions to the use of web browsers in the client may exist. In these cases, an appropriate client/server architecture will be constructed for these sites.

The following list represents the JTAV user group:

- Joint Chiefs of Staff (JCS)
- Atlantic Command (ACOM)
- European Command (EUCOM)
- Central Command (CENTCOM)
- Pacific Command (PACOM)
- Southern Command (SOUTHCOM)
- Special Operations (SOCOM)
- Space Command (SPACECOM)
- Strategic Command (STRATCOM)
- Transportation Command (TRANSCOM)
- Joint Task Force (JTF)
- Service Headquarters

- Component Inventory Control Point (ICP)
- Component Command
- Service Repair Depot
- Distribution Warehouses (DLA)
- Weapon System Management
- Service Retail Inventory Management

3.3.2 Data Provider Nodes

Data provider nodes are responsible for providing the highest quality data possible to the total asset visibility user. These nodes will be located throughout the world. The major data provider nodes are listed below:

- GDAS Nodes
- JTAV Nodes
- Enterprise Nodes
- Component / Service /Agency Nodes

3.3.3 Communications Nodes

High level communication will be provided throughout the total asset visibility network via DISN. Depending on the level of security, long haul communications will be provided by NIPRNET or SIPRNET. In theater, communications are established using available infrastructure. Theater users may use land lines, satellite communications, cellular phones, etc., or a combination of methods.

3.4 Node Connectivity

This section describes the interconnection of the total asset visibility nodes identified in section 3.2. This interconnection is described in terms of query information flows (IF) and node connectivity (NC) diagrams with system overlays. Figure 3.4-1 shows an example of a query information flow. The node connectivity diagrams with system overlays describe connections between two nodes. In most cases, the nodes used in the diagrams are generic nodes, e.g. “Legacy System Node.” However, some specific nodes are described, e.g. “DAASC Node.” These diagrams show the node activities, what data is passed from one node to the next, which systems are used to process the data, and the communications mechanism between the nodes. Figures 3.4-2 through 3.4-4 are the node connectivity diagrams that correspond to the information flow shown in figure 3.4-1. Appendix C contains all of the information flow and node connectivity diagrams for the total asset visibility architecture.

Figure 3.4-1 shows the query information flow from an in-theater user workstation to a legacy system and back to the user workstation. The user submits a query through the application server or its web browser located on the user workstation. The application or web server then processes the query and routes it to the proper data access provider. In this example the query is passed to the GDAS. GDAS then locates the data the user is interested in, translates the

query into the format the shared data resource server uses, and sends the query to the shared data resource server. The shared data resource server then requests the information from the legacy system. Information is downloaded to the shared data resource server from the legacy system. This server then passes the information to GDAS through a set of stored procedures. Next, GDAS translates the data to the desired user format, and passes the information to the application or web server using a standard API. The results of the query are then returned to the user. If the user is a web client, the web server creates the web page that it will send to the user and passes it along to the web browser on the user's workstation.

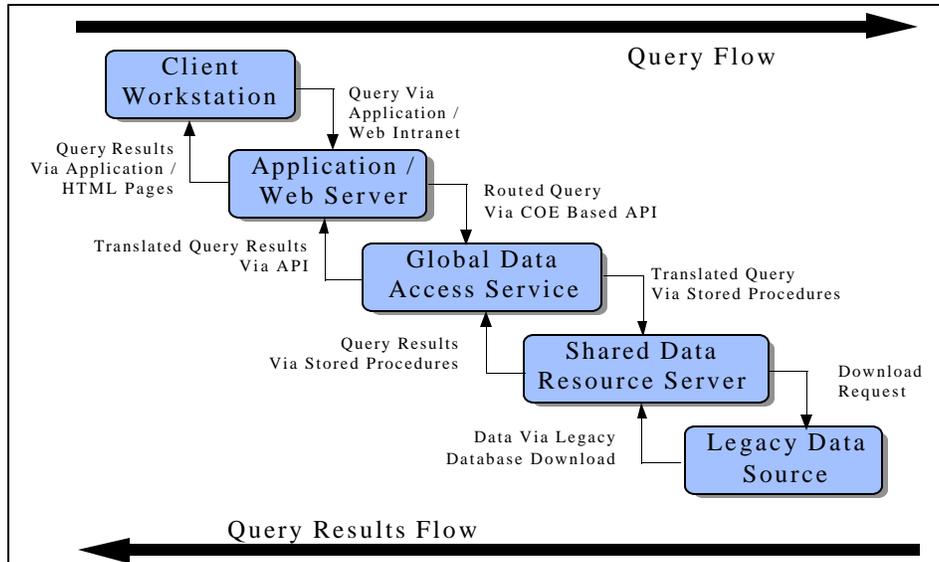


Figure 3.4-1 Query / Query Results Flow from User Workstation to Legacy System

Figure 3.4-2 shows the interconnectivity of the Legacy system node and the shared data resource node. The shared data resource node must collect data that has been requested by the user from the legacy node. Once the shared data resource node submits its request for data, the legacy node will provide the information. Data which may be exchanged between the two nodes is requisition data, in transit data, personnel data, medical supply data, etc. Because the information being exchanged is sensitive but unclassified (SBU), the two nodes communicate through NIPRNET.

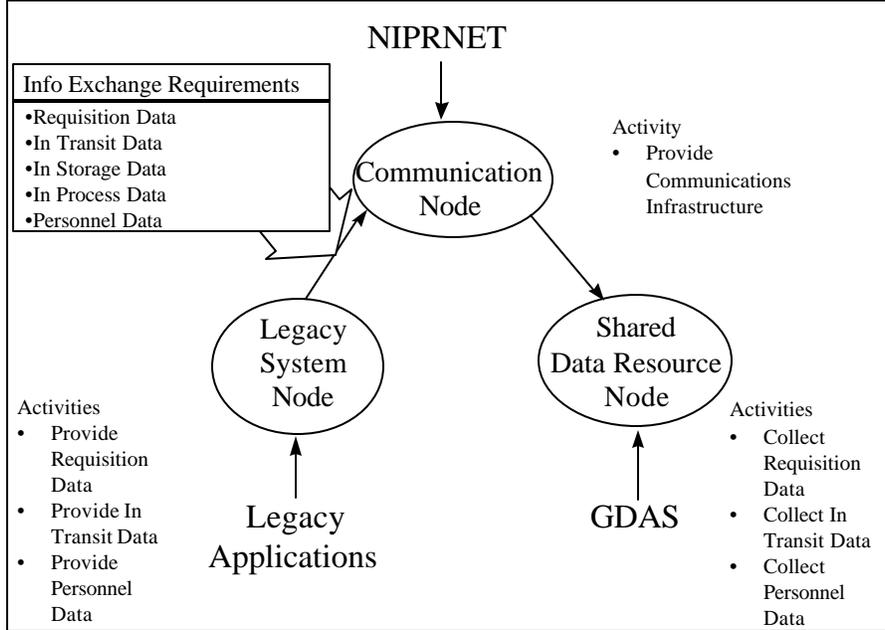


Figure 3.4-2 Legacy System to Shared Data Resource Node Connectivity/System Overlay Diagram

The shared data resource node's role in the node to node connection shown in Figure 3.4-3 is to provide the asset visibility data it has collected to the GDAS node. To transfer the data, a specific set of stored procedures will be used. These stored procedures perform all the processing necessary to transition the data to the GDAS node. GDAS nodes and shared data resource nodes will communicate over the NIPRNET, and in some cases through a LAN.

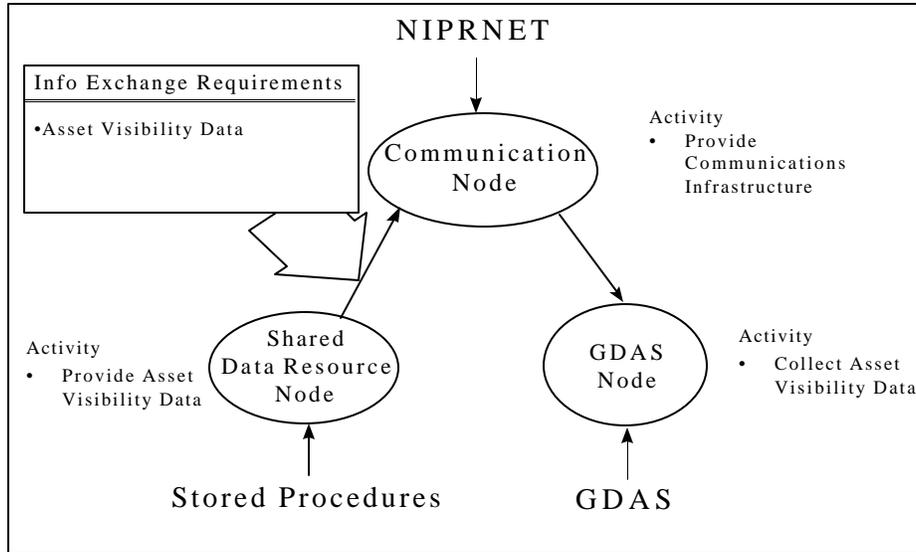


Figure 3.4-3 Shared Data Resource to GDAS Node Connectivity/System Overlay Diagram

Figure 3.4-4 shows the final interconnection in this information flow: the connection between the GDAS node and the User node. The GDAS node provides asset visibility data, requisition data, in-transit data, personnel data, medical data, etc. to the User node. GDAS links to the User node's application or web server via a COE based API. The server then sends the information it has collected to the user workstation's client interface or web browser. The GDAS node and the User node will communicate using NIPRNET. In cases where the GDAS node is co-located with the user node, the two nodes may be part of a LAN.

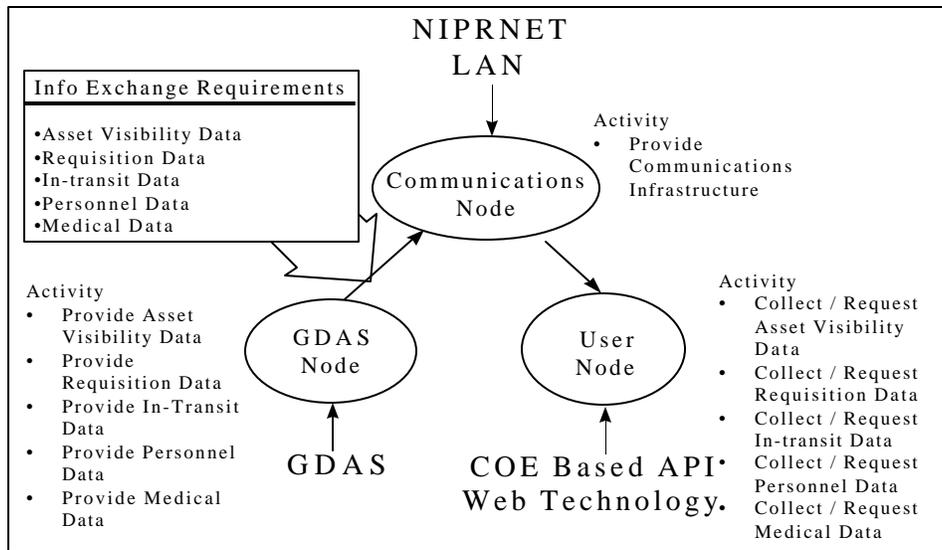


Figure 3.4-4 GDAS to User Node Connectivity/System Overlay Diagram

3.5 Node Configuration

This section will describe the system configurations at each node. With the exception of the DAASC node and the USTRANSCOM node, the system configurations are generalizations of the equipment, software, applications, network configurations, and communications that will be present at each unique site. Uncompressed diagrams and a more detailed description of the system configurations are contained in Appendix F.

3.5.1 User Nodes

User nodes are unique to each site. Figure 3.5-1 shows a generalized total asset visibility user node. In general all user workstations will be DII COE compliant workstations. Critical to the user node are the web browser on the workstation and the web server. In cases where web technology is not in use, a customized total asset visibility client/server interface will be used. Some user nodes may also host a JTAV server and/or a GDAS server. The user nodes can support both local and remote workstations. User nodes may be secret environments, unclassified environments, or a combination of both. Appendix F shows the system configurations of two more specific user nodes.

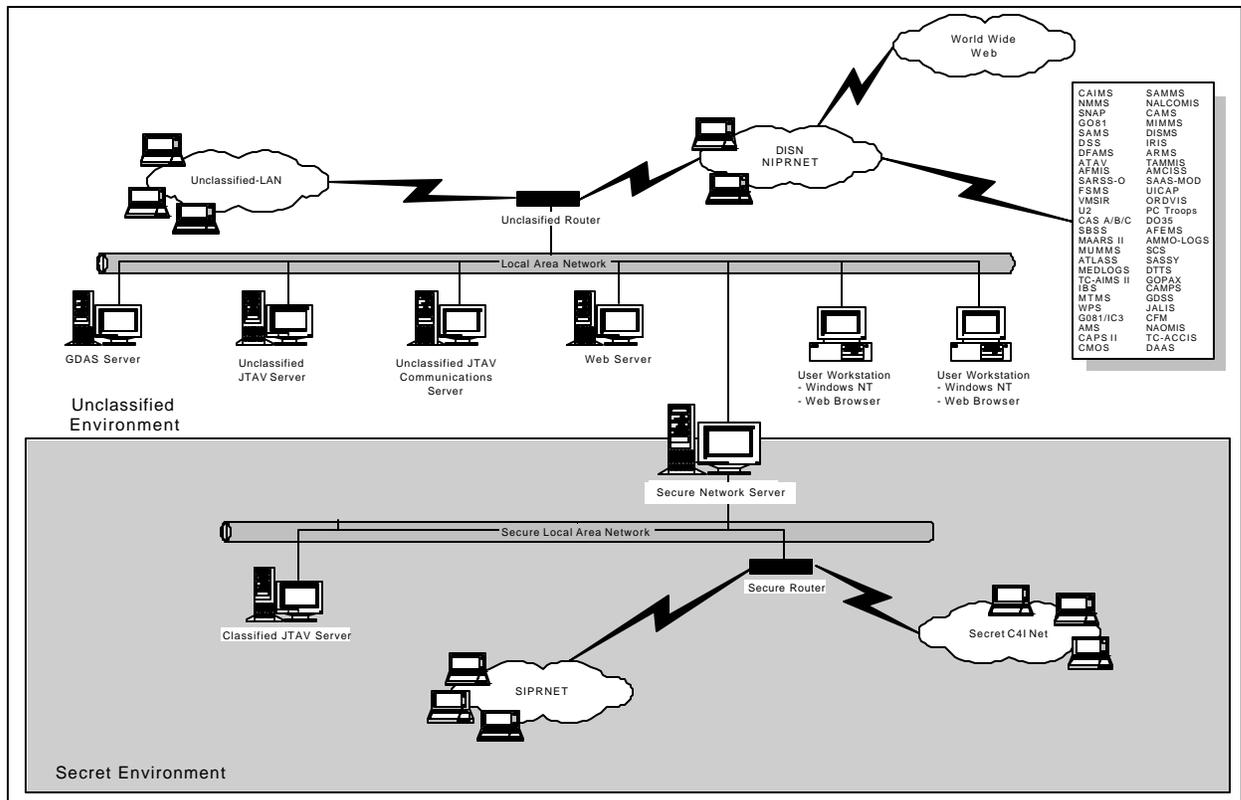


Figure 3.5-1 Total Asset Visibility User Node (General)

3.5.2 JTAV Nodes

Figure 3.5-2 depicts the general system configuration of a JTAV node. The key elements of the node are the JTAV data and communications servers, the GDAS server, the web server, and the secure network server.

It is important to note that this node is a combination of secure and non-secure environments. While logistics data is sensitive but unclassified information, users of the data may work only in classified environments. Therefore there is a one way secure guard server between the secure and non-secure environments. This server allows JTAV data to flow from the unclassified environment into the secret environment, thus allowing remote users to access JTAV data over SIPRNET.

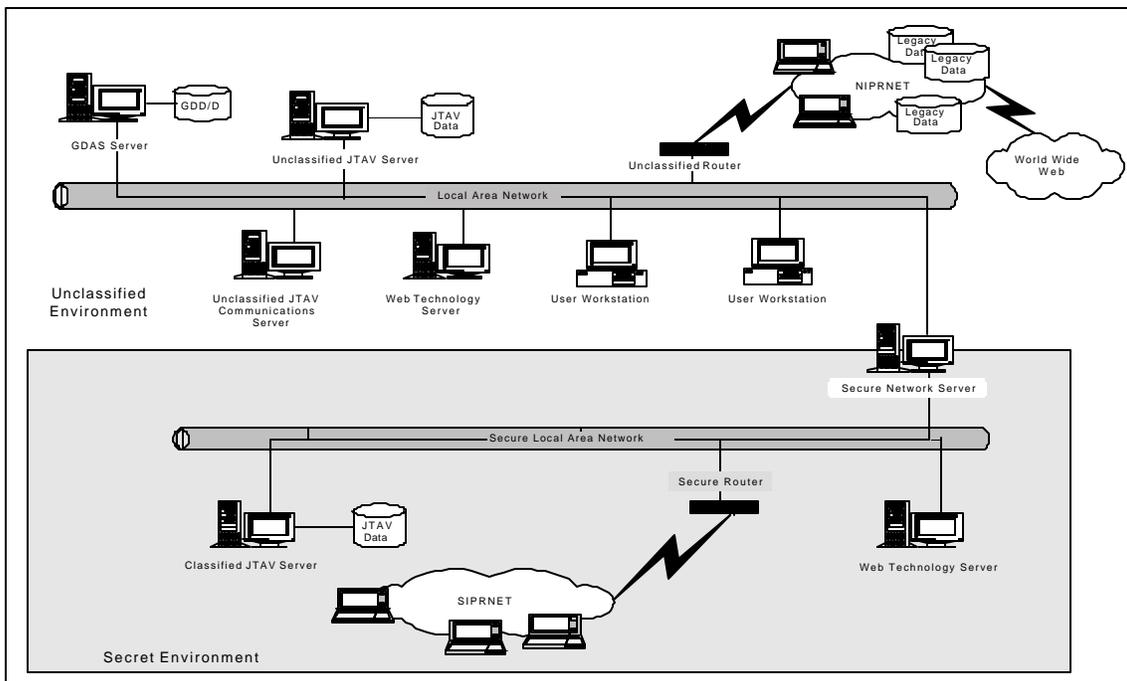


Figure 3.5-2 JTAV Node System Configuration (General)

3.5.3 USTRANSCOM Node

The USTRANSCOM node hosts a technically complex system configuration. Constraints such as security and access to many disparate legacy systems create the need for a sophisticated architecture. Figure 3.5-3 depicts a simplified version of the USTRANSCOM node. This node is comprised of secure and non-secure servers as shown in the figure.

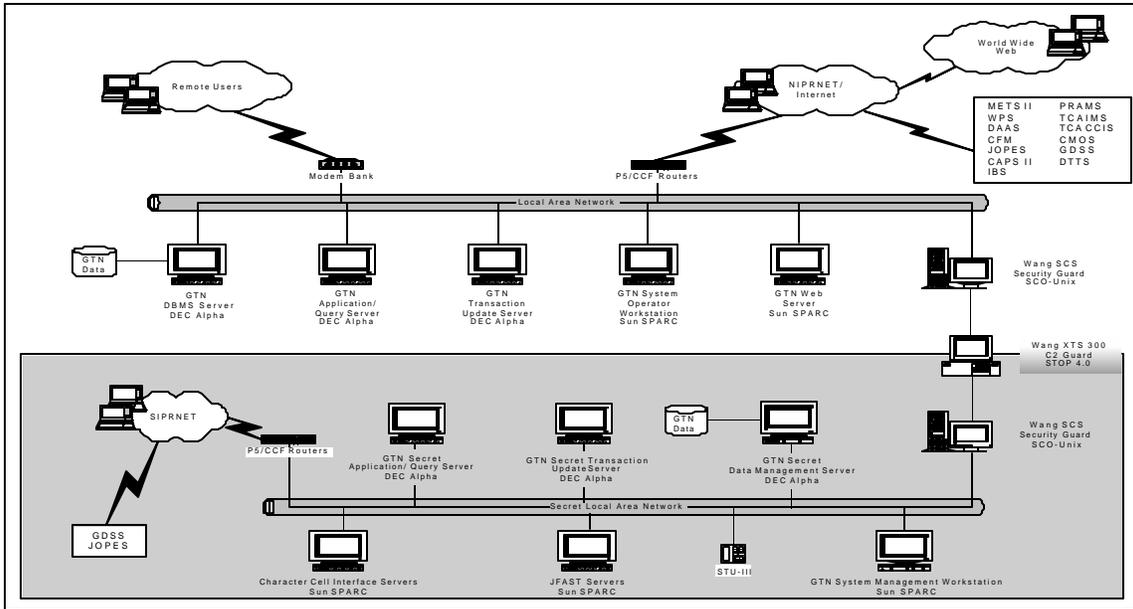


Figure 3.5-3 USTRANSCOM Node System Configuration

3.5.4 DAASC Node

The DAASC node provides many data and communication related services. The focus in the total asset visibility architecture is on the data that this node provides. Therefore, a simplified version of the DAASC system architecture is presented in Figure 3.5-4. DAASC is a rich source of aggregate requisition data. The Logistics Online Transaction System (LOTS) database is the primary storage location for logistics requisition data. The DAASC node is duplicated at a second physical location for redundancy purposes.

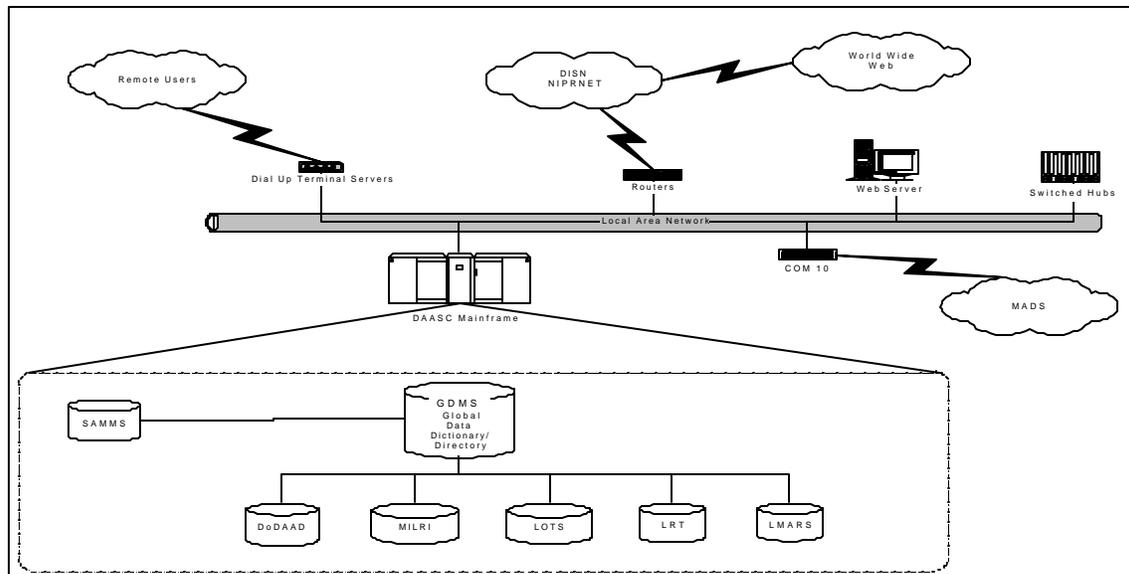


Figure 3.5-4 DAASC Node System Configuration

3.5.5 Component / Service / Agency Nodes (Data Sources)

Each component, service, and agency has a unique system configuration. For that reason it is not possible to describe or diagram them all. A generalized diagram of a Defense Megacenter is shown in Figure 3.5-5 to demonstrate the general configuration needs of a total asset visibility data source.

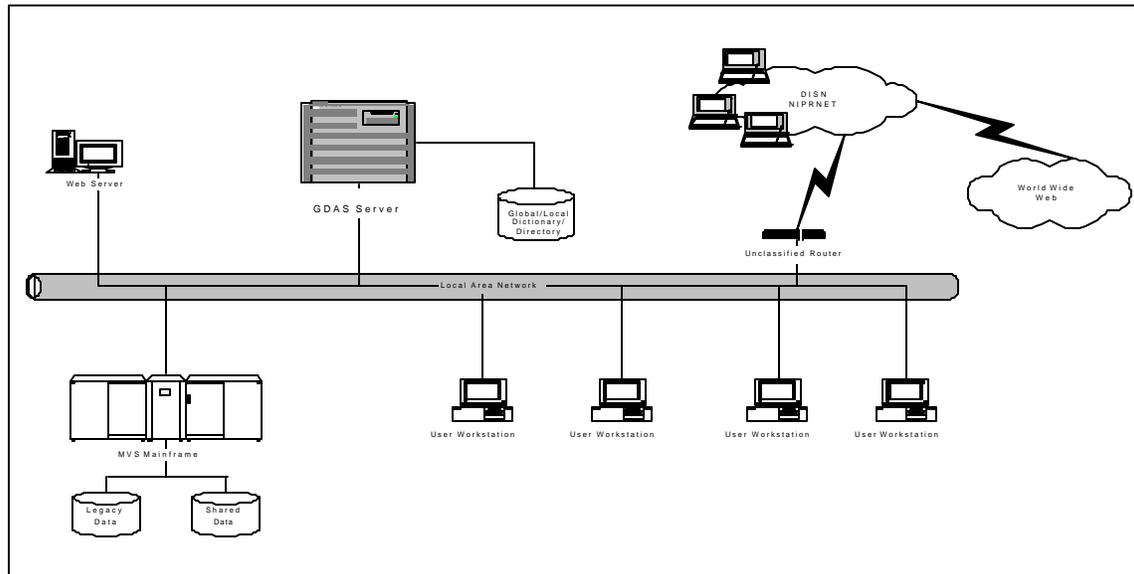


Figure 3.5-5 Defense Megacenter Node System Configuration (General)

3.5.6 Communications Nodes

All communications between the total asset visibility nodes will be accomplished using existing communications infrastructure. Wide area communications will be achieved through the use of DISN's NIPRNET and SIPRNET and commercial WANs. Local area, metropolitan area, and campus area communications will be provided by the local infrastructure using COTS LANs, MANs, or CANs where appropriate. As necessary, commercial communication methods such as land lines, satellites, and cellular services will be used.

4.0 Design Criteria and Alternatives

4.1 Overview

The Joint Total Asset Visibility network is made up of many data provider and user sites. Each of these sites has characteristics that make them unique. Designing one total asset visibility systems architecture solution for all of these unique sites is impossible. Therefore, this document is intended as guidance to the site system architecture implementers. This section is intended to provide system architecture alternatives, criteria for analyzing the alternatives, and general recommendations. Site implementers of this architecture must make the decisions as to the optimal choices for their site.

4.2 Evaluation Criteria

In the following sections, elements of the system architecture design are discussed. Several possible alternatives exist for implementing the user interface, data access mechanisms, access control, data locations, and data security. The alternatives should be carefully analyzed and evaluated using the following criteria:

- Meets Operational Requirements
- Data Quality and Timeliness
- Responsiveness
- Life Cycle Cost
- Ease of Use
- Reliability, Maintainability, and Availability
- Flexibility
- Ease of Transition

Finally, any design decisions made must be scrupulously assessed with regard to their effect on the warfighter. These criteria are general enough to be useful across the network of total asset visibility nodes and across the system architecture design elements. Criteria can be ranked or weighted by implementers to reflect the system architecture requirements at their site.

An example of criteria weighting is given in Table 4.2-1. Criteria are assigned a weight between 1 and 5, 5 being the highest or best. Then each alternative is given a score for the criteria between 1 and 5, 5 being the highest. It is important that the criteria be worded such that a score of 5 is the highest score that it can receive. For instance, unless the word “low” is added to the “Life Cycle Cost” criteria, a score of 5 would indicate a negative impact but still give the alternative a high score. The criterion weight is multiplied by the alternative score, giving the weighted score. After the alternative has been given a weighted score for each criterion, the alternative’s scores are added up. The alternative with the highest weighted score is the best solution. In this example, the alternatives have the same raw score. However, when the scores are weighted, alternative B is the best solution. This demonstrates how criteria weighting can be used to tailor the evaluation criteria to reflect local user and system requirements.

Table 4.2-1 Alternative Analysis by Weighted Criteria

Criteria	Criteria Weight	Alternative A Score	Alternative A Weighted Score	Alternative B Score	Alternative B Weighted Score
Meets Operational Requirements	5	3	15	4	20
Data Quality and Timeliness	4	4	16	3	12
Responsiveness	3	5	15	4	12
Life Cycle Cost (Low)	4	4	16	5	20
Ease of Use	2	4	8	3	6
Reliability, Maintainability, and Availability	4	4	16	4	16
Flexibility	3	3	9	4	12
Ease of Transition	3	4	12	4	12
Total Score		31	107	31	110

4.3 User Interface

One of the requirements of the JTAV system architecture is to provide the total asset visibility user with a unified user interface. In various DoD programs this is referred to as “any user, any box, anywhere,” “fused picture,” “one picture, one net,” etc. What these terms actually mean is that there will be one standard user interface for any total asset visibility user. Behind this single view is the global data access network of logistics. This new architecture allows users to access data that they have not previously been able to access but are authorized to use. Access to this data is obtained through one user login.

4.3.1 User Interface Alternatives

There are several alternatives for the user interface. All alternatives must comply with DoD standards such as the Technical Architecture Framework for Information Management (TAFIM), the Defense Information Infrastructure Common Operating Environment (DII COE), and the Joint Technical Architecture (JTA). It is also critical for the user interface to be compatible with commercial industry standards. The DoD will continue to migrate toward open systems design and increase its use of commercial off the shelf (COTS) products. The JTAV system architecture supports the continual change of technology.

Evaluation criteria for the alternatives are listed below:

- Fused picture – how well the alternative provides one standard interface to all users;

- Compliance with standards – how well alternative complies with all published DoD standards;
- Commercial Compatibility – how compatible the alternative is with commercial products and standards; how much it resembles commercial products;
- User familiarity – how familiar the average user would be with this type of presentation;
- Performance – the speed of the alternative’s response time; and
- Resource requirements – constraints placed on the alternative by resource requirements

Three alternatives are under consideration in DOD today:

- Client/Server Client Interface – built to comply with DoD standards, also designed to take advantage of user familiarity with commercial de facto standards. This alternative is built with a specific application or application environment in mind.
- Web Client Interface – a COTS product, complies with all DoD standards. This client alternative provides a flexible user interface that can be used to support access to many applications and environments.
- Graphic/ Map-based Client Interface – this client interface uses maps to present query results. Instead of a text based presentation, the user will see the assets they have inquired about overlaid on their geographical location. This interface provides an intuitive user presentation.

4.3.2 User Interface Recommendations

The web-based client interface should be implemented wherever economically and technically feasible. This client interface will provide the most flexibility for the total asset visibility user. Users who require highly complex and large query processing may elect to maintain traditional client/server interfaces. However, these users will require high-end workstations. The development of a map-based client interface is a future option for total asset visibility users.

4.4 Data Access

Data access is the primary purpose of the JTAV capability. Total asset visibility users must have access to the highest quality joint data. In order to meet this requirement, the JTAV data access architecture supports a combination of data access methods tailored to fit the specific user/application requirements.

4.4.1 Data Types

Total asset visibility users will need to access data of three types:

- Legacy Data - data which is relatively inaccessible by today's interoperability standards. This data is generally not standardized, and translation and data manipulation must occur to make it usable across the total asset visibility network.
- Shared Data - data that has been identified as corporate data. This data is standardized, created by only one authoritative source, of high quality, and is separated from applications to make it widely available to other applications and users.
- Local Data - data which is directly applicable to the user's business area. The user has expert knowledge of this data. This data may or may not be standardized. Regardless, no translation or manipulation must occur for the user to access it.

4.4.2 Data Access Factors

Nine factors affect total asset visibility data access. Analysis and prioritization of these factors will provide input into the to-be data topology design. The factors are defined as follows:

- Data Usage - how the total asset visibility users will use the data. For instance their local data will be used in their day to day operations and they can create, read, update, or delete the data. On the other hand, legacy data will be used for informational purposes only.
- Data Location - where the data is stored in relation to the total asset visibility user.
- Data Volume - how much of this type of data exists. Shared data is evolving as more and more data sharing partnerships are established and more corporate data is identified.
- Access Frequency - how often the total asset visibility user will access this type of data.
- User Subject Knowledge - how much a user knows about the data, its existence, location, and meaning.
- Data Standardization - whether or not this type of data is typically standardized in nature.
- Access Mechanism - how the total asset visibility user will access the data. Global Data Access Services (GDAS) will be used to access some of the total asset visibility data, other data will be accessed using native application methods.
- Replication of Data - whether or not the data will have to be replicated. A replicate is a fully controlled table copy with a system-level relationship to the authoritative source and a system-level update control mechanism.
- Response Time - how quickly the results of a query, or operation are returned to the total asset visibility user.

Table 4.4-1 relates the data access factors listed above to the data types listed in section 4.4.1.

Table 4.4-1 Data Access Factors for Total Asset Visibility Data

Data Access Factors	Data Type		
	Legacy Data	Shared Data	Local Data
Data Usage	Ad-hoc Queries	Query	Production/ Operational
Data Location	Globally Distributed	Globally Distributed	User Business Area
Data Volume	High	Evolving	Low
Access Frequency	Low	Low-High	High
User Subject Knowledge	Low	Low - High	High
Is Data Standardized?	No	Yes	Both Standard and Non-Standard Data
Access Mechanism	GDMS	Native / GDMS	Native
Replication of Data	Possibly	Yes	Possibly
Response Time	Slow	Varies	Fast

4.4.3 Data Access Control

The JTAV environment encompasses two levels of security environments. In general, logistics data is considered sensitive but unclassified (SBU). JTAV will be operating in user environments that are classified and operating at system high level. In these environments, JTAV information must be transferred from an unclassified environment to a secret environment. JTAV will accomplish this through the use of one way security software. Information can come in to the classified area, but no information can leave it.

Access must be controlled at two physical levels. Local data access requires user identification and authentication (I&A). Local I&A, typically the responsibility of the base or base commander, can be accomplished by using locally defined and managed mechanisms or by using mechanisms provided by GDAS. If local mechanisms are used, the global data manager

must be modified to accommodate them. The GDAS mechanisms use Role Based Access Control (RBAC).

Global access control is necessary to protect remote data sources from unauthorized access. A different approach to access control is required in a distributed environment, because of the increased volume of database access. SBU environments will use GDAS Organizational Based Access Control (OBAC). Using this method, access to a database is determined based on the user's organizational affiliation. Classified / System High environments will retain access control based on user identification.

4.4.4 Data Access Recommendations

In the total asset visibility system, data will be accessed using a combination of methods. Because data sources and data user sites are somewhat unique, solutions to data access must be tailored to each situation. Data architecture designers must carefully analyze user requirements, data types, data access factors, and data access control to determine the best method for each case.

4.5 Data Quality

Data quality is defined in DoD 8320.1-M as “The correctness, timeliness, accuracy, completeness, relevance, and accessibility that makes data appropriate for use.” The goal of data quality is to “ensure that DoD operations and decision making are supported with data meeting needs of availability, accuracy, timeliness, integrity, and need-to-know requirements.

The JTAV data environment will foster data quality by using the data's authoritative source and by using shared data whenever possible. Shared data is created once by the authoritative source and accessed as needed by multiple users. Data sharing promotes quality by reducing the inconsistencies that may arise from multiple creation and translation.

4.6 Data Topology

The JTAV data topology describes the placement of data at locations within the enterprise. The purpose of the data topology is to improve access to data with higher quality, with greater efficiency, and at reduced costs. To achieve total asset visibility users' business and functional requirements, a to-be data topology for the JTAV data environment must be designed. Through the analysis of the as-is topology, a clear picture of the optimum to-be topology will emerge. Data in the as-is topology will be analyzed for consistency, timeliness, security, reliability, survivability, and communications. Armed with this information, decisions of where to place total asset visibility data can be made.

There are several possible data locations in the total asset visibility architecture. Data may be located at the originating source. This is referred to as “in-place” data. Shared data resources offer additional storage for corporate data. Another data location is the JTAV in CONUS data server. Finally, data may be located at JTAV sites in theater. There are trade-offs associated

with each data location alternative. Keeping data in-place offers high reliability, but may provide unacceptable responsiveness. Shared data resources are tailored to provide data that is of interest to the total asset visibility user population. Data in theater is usually the most easily user-accessed data. However, it may also be the oldest data. The pros and cons of each alternative listed below must be carefully analyzed. The data location alternative that most closely matches the user data requirements should be implemented. It is important to note that the optimal data location may be different for different types of data. Thus a melding of all four alternatives will characterize the JTAV data architecture. Table 4.5-1 displays some data location alternatives.

Table 4.5-1 Total Asset Visibility Data Location Alternatives

Data Location Alternatives	Pros	Cons
In-Place: Data contained in the originating source database	Data is current, highly accurate, JTAV users can access only when they need data	Response time may be poor, data may need translation
Shared Data Resource: Data located in designated corporate databases	Data is in sharable format, easily accessible, JTAV users pull data as needed	Data is not as current as at source, must manage replication
JTAV: CONUS: Data contained in a JTAV database in the continental U.S.	Data is directly pertinent to JTAV user requirements, data is easily accessible to JTAV users	Currency of data degraded, data must be pushed, amount of data to be stored increases
JTAV: In-Theater: Data contained in a JTAV database located at a user site	Fast response time for users, data accessible at all times	Data currency suffers, must manage replication and synchronization, must store large amount of data

4.7 Data Management Responsibility

The purpose of data management is to ensure that authorized total asset visibility users have access to data that meets defined standards of quality and security. Data management in the JTAV data environment is concerned specifically with corporate data and must deal with requirements for sharing, positioning, and managing data in a distributed environment. A unique aspect of data management in the JTAV environment is that none of the data that the JTAV capability uses is originated by JTAV. This aspect creates some unusual data management issues. JTAV data managers must work closely with the data managers from all of the systems that JTAV receives data from. Business agreements must be established between the data provider and JTAV. These business agreements institute policy and procedures between the data sharing partners.

In the legacy environment, common information is exchanged through interfaces with data being translated as necessary for use by different applications. Or common information is represented by the creation of redundant data elements, each used in stovepipe fashion by different applications. In order to make data available to total asset visibility users, corporate data must be placed in a shared data resource and reflected in the corporate, or global, data repository so that users can access it.

A database may contain local data, corporate data, or both. Local data is that data which is only used by local applications and users. Corporate data is data that is shared globally among authorized systems and users. The global data management servers host the global data repository used to access corporate data from distributed databases, but each database may be associated with a local repository that contains the metadata used by the local database management system (DBMS) to manage the local data. Corporate data can remain in a local database if the local database can act as one of the total asset visibility shared data resources. This is the case of in-place data access. Otherwise, the data will be moved to a designated corporate shared data resource.

Corporate shared data resources will require effective data management to neutralize potential problems. Two of the more serious problems that are controlled by data management are: uncoordinated changes to JTAV or source database structure, and data which is out of synch, caused by mismatched update cycles, etc. Neglecting effective management of the JTAV data could result in users getting incomplete, incorrect, or out of date data.

Regardless of the location of the data, it will still be managed locally with established data management procedures. However, it must also be managed at a global level to maintain it as a part of the total asset visibility system. Effective global data management ensures:

- Changes to data attributes or the database structure of JTAV or source databases are coordinated with all affected parties;
- Global data creation, retrieval, update, and deletion privileges are clearly established and enforced;
- Data changes are synchronized throughout all database sites; and
- Database maintenance responsibilities are clearly established, to include supporting software such as database engines and global database communication.

Failure to provide effective global data management will result in JTAV and source database mismatches, the promulgation of invalid data, and database out-of-synchronization conditions. At a minimum JTAV data management procedures will have to encompass the following subjects:

- Providing Data Access
- Controlling Data Access
- Ensuring Data Security
- Ensuring Data Quality
- Managing Distributed Data
- Managing Fragmented Data
- Managing Replicated Data
- Coordinating Heterogeneous Data Sources
- Managing Global Data Dictionary and Directory
- Managing Global Repository, Models, and Metadata
- Constructing Data Mappings
- Maintaining Local Models, and Databases
- Coordinating Data Synchronization

4.8 JTAV Security

The JTAV environment must comply with security standards that the DoD has instituted. These policies can be found in DoD 5200.28-STD, “DoD Trusted Computer System Evaluation Criteria Standard” and NCSC-TG-021, “Trusted Database Management System Interpretation.” At a minimum, JTAV must support security for sensitive but unclassified (SBU) data. The JTAV capability will address these security issues by enforcing data security and access control.

As with data management, the responsibility for defining security requirements, including classification levels, belongs to the local data administrator. However, JTAV, as a user of that data also has data security responsibilities. JTAV must, at a minimum, ensure that the data it receives and distributes to users retains:

- Confidentiality - data must not be disclosed to unauthorized users; and
- Integrity - data must not be accidentally or maliciously altered or destroyed.

To achieve this goal, the JTAV data architecture must provide the environment to prevent the following security breaches:

- Unauthorized Access - inadvertent or intentional access of restricted data;
- Human Error - inadvertent changes or disclosure by authorized users;
- Internal Malice - malicious changes or disclosure by authorized users;
- External Malice - malicious changes or disclosure by unauthorized users;
- Virus - unauthorized introduction of destructive software; and
- Physical Loss - destruction of equipment or facilities by natural or hostile action.

The JTAV environment must also support the security plan for the logistics community at large. In order to support these global initiatives, the JTAV environment must be capable of integration with the various security approaches being developed by other DoD initiatives.

4.8.1 Security Requirements Description

JTAV information protection will include the proper levels and types of access control and assurance of availability, despite expected threats, required to assure secure in-theater visibility of assets for the warfighter. Range and levels of assurance vary widely across the JTAV sources, data, and users. Therefore, no single security solution is expected to meet all the security needs. The following factors will be considered in deriving the appropriate security solution:

- Logistics data is sensitive but unclassified (SBU);
- Both system high and SBU operational environments;
- Replication from SBU to system high environments required; and
- JTAV sources have different levels and types of access control.

Six security administration services are required to satisfy DoD security standards:

- Accountability – enables activities to be traced to individuals who may then be held responsible for their actions. Similar to identification and authentication (I&A).
- Access Control – mediates, monitors, and controls access to information or to resources of an information system, ensuring access by only authorized users.
- Confidentiality – protects data from unauthorized disclosure during communications.
- Integrity – ensures that data is transmitted from the source to the destination without undetected alteration.
- Non-repudiation - protects against the denial by one of the entities involved in information exchange of having participated in the exchange.
- Availability – ensures reliable and correct operation of information and system resources.

4.8.2 Security Mechanisms

There are many security methods available for providing accountability, access control, confidentiality, integrity, non-repudiation, and availability. However, there is currently no solution that satisfies all of these requirements. Therefore, a combination of methods will be used to implement security in the total asset visibility environments. The following list describes some of the security alternatives:

- User ID and password with access control lists – satisfies user I&A, non-repudiation, and access control requirements. This alternative includes support for role and organizational based access control tied to a managed user login with a unique password. Data location is

transparent to the user and access is based upon the user's pre-defined login profile and associated data access privileges.

- IP address/domain name address filtering – satisfies I&A, access control, and non-repudiation requirements. This security mechanism restricts client access to a specified network or server based upon an accepted list of IP addresses or domain names. This method is primarily implemented via hardware through a smart router smart hub which filters access requests to a local area network (LAN).
- DCE-based security – used in a distributed computing environment (DCE), provides I&A, confidentiality, access control, integrity, and availability. The Open Group provides guidance for DCE based security. These security specifications detail areas such as I&A, file access, and encryption. Some security methods DCE supports include use of public keys to authenticate login and Kerberos authentication.
- Transmission encryption – satisfies confidentiality, and integrity requirements. This mechanism involves the use of a cipher to encrypt a data packet prior to transmission across a network and decrypting the packet upon receipt at the other end of the transmission.
- Virtual private network - provides confidentiality, access control, and availability. A mechanism implemented by creating an insulated network environment to and from which access is strictly controlled. This entails securing dedicated connection lines which are not connected to commercial network lines and controlling access to these lines at both the server and client levels.
- Firewalls/guards – satisfies access control, confidentiality, and integrity requirements. These mechanisms are implemented by creating a hardware, software, or hardware/software combination buffer between a LAN and Wide Area Network (WAN) lines or between a server and its LAN. This method of security is commonly used between a private corporate LAN and the commercial Internet. Firewalls/guards can also be implemented for low-to-high security environments.
- Token-based (hardware or software) Public Key Infrastructure (PKI) with client certificates – satisfies I&A, access control, confidentiality, and non-repudiation requirements. This security mechanism uses a two-key encryption system. For this method, a public key is used to encrypt a message to the owner of a private key. Decryption of the message is only accomplished by possessing both keys. Keys can be generated by hardware or software.

4.8.3 Security Alternatives

These mechanisms can be combined into several alternatives. Note that it is assumed that these alternatives will be in addition to local site security configurations such as firewalls and domain filtering. The selected alternatives may affect the existing site security configurations.

Alternative 1: Use User ID and passwords with access control list. This alternative is not secure. When used on the SBU networks that are attached to the Internet, this alternative creates significant risk through password sniffing to the application.

Alternative 2: Use User ID and passwords with access control list. Provide transmission encryption through point-to-point encryption or through a mechanism like Secure Sockets Layer (SSL). This alternative is a reasonable very near-term alternative (weeks to implement) for web-based implementations. Products for non-web-based FTP clients are available, although not as widely used. A stronger I&A mechanism is preferable for DoD SBU systems.

Alternative 3: Use a web-based PKI for I&A, access control, and confidentiality. Access can be individual-based, or with the combination of other local security products, organization or role-based. This alternative meets most of the security requirements and can be implemented through GCSS-WEB in the near-term (months to implement). However, it will not address the non-web-based clients in the near term.

Alternative 4: Use a hardware or software-based general PKI for I&A, access control, and confidentiality. Access can be individual-based, organization-based, or role-based. This alternative meets most of the security requirements. It will take over 1-2 years to implement.

Alternative 5: Use SIPRNET, a virtual private network, for classified information. Use back-end low-to-high guards for replicating SBU data to the Secret database. This option does not provide the privacy or community of interest protection required by JTAV.

Alternative 6: Use SIPRNET with user IDs, passwords, and transmission encryption (e.g., SSL). Use back-end low-to-high guards for replicating SBU data to the Secret database. This option provides the necessary privacy and community of interest protection required by JTAV. However, it does not meet the single login requirement of GCSS.

Alternative 7: Use SIPRNET with a PKI (see options 3 and 4 above). Use back-end low-to-high guards for replicating SBU data to the Secret database. This option provides the necessary privacy and community of interest protection required by JTAV.

4.8.4 Security Recommendations

The best near term (next 2-3 months) solution is to implement alternative 2 for sensitive but unclassified environments. Alternative 6 is the optimal solution for secret environments. The GCSS-Web certificate authority can be used as the root authority for Web server certificates. For current JTAV users that use traditional client access instead of web access, evaluate impact of moving to web-based access and move them to the web client unless the impact is negative.

For the short term (next 6-9 months), alternative 3 is the best solution for the SBU web-based client, alternative 7 is optimal for the secret web-based clients. This will support the GCSS goal of single log-in. Traditional client/server clients will continue to use alternative 2's security mechanisms.

In the long term (2-4 years), a single, integrated DoD PKI supporting web and non-web applications, HTTP guards, and middleware guards will be the optimal solution

5.0 System Architecture Application and Use

5.1 Technical Architecture

In the context of the C4ISR Framework, the technical architecture provides the minimal set of rules that govern the arrangement, interaction, and interdependence of the parts or elements whose purpose is to ensure that a conformant system satisfies a specified set of requirements. The technical architecture identifies the services, interfaces, standards and their relationships. It provides the guidelines for implementation of systems upon which engineering specifications are based, common building blocks are built, and product lines are developed.

In accordance with DoD Directive 4630.5, and the 22 August 1996 Memorandum jointly signed by the USD (A&T) and ASD (C3I), the JTAV capabilities will be implemented using the Joint Technical Architecture (JTA). Though initially developed for the C4ISR community, the JTA is evolving to provide the technical capabilities required for all joint operations. Capabilities required in the JTAV system architecture that are not currently provided for in the JTA, will be submitted to the JTA Working Group as combat support technical capability requirements.

5.2 Specific Configurations

The system architecture specified in this document was intentionally developed to be generic in nature. This allows maximum flexibility required to support the differences in operational parameters and technical capabilities that may exist at individual sites. It does not specify the exact physical configurations required to support specific sites that will require the JTAV capabilities.

Figure 5.2-1 shows the process to apply the generic system architecture to a specific site configuration. It requires the following steps:

- **Identify Operational Parameters** - The operational parameters required to support users at the site must be identified. This must, at a minimum, include the data required at the site (media (e.g., text, graphics), amount, and frequency) and minimum acceptable user response time.
- **Identify Current Site Configuration** - The “as-is” site configuration must be documented. This must, at a minimum, include the existing hardware, software, and communications capabilities.
- **Develop Specific Configuration Alternatives** - Using the system architecture design alternatives and criteria outlined in Sections 3 and 4, the current site configuration, and the JTA, develop possible site configurations. The specific configurations should include the “to-be” configuration and resulting migration alternatives based on the availability of proven products.

- **Evaluate Alternatives Against Operational Parameters** - The specific configuration alternatives needs to be evaluated against the operational parameters to see if they meet the user requirements. The evaluation must also include the availability of proven products.
- **Select Specific Configuration** - The alternative that best meets the users' requirements should be selected. If multiple alternatives meet the users operational parameters, then programmatic factors like cost and schedule risk should be used as criteria to select the specific configuration.

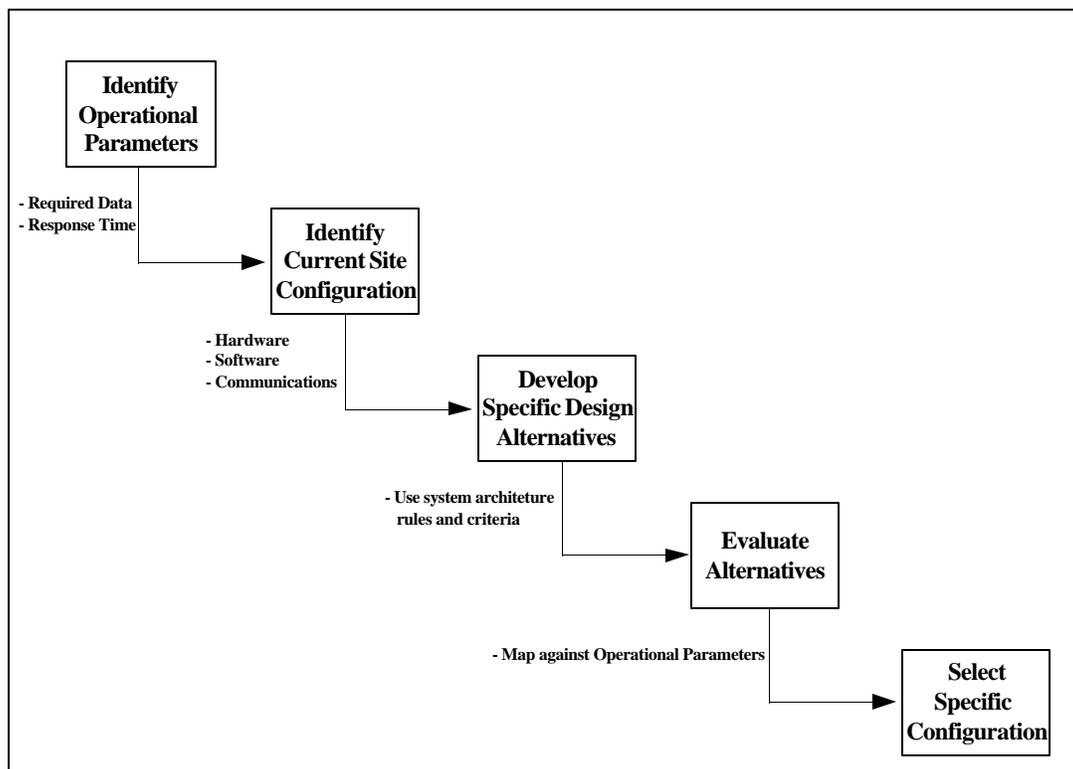


Figure 5.2-1 Specific Configuration Translation Process

The following example shows a simple application of the process:

- A CINC User Site requires access to asset visibility information on the status of a class of critical munitions supply items. The data is available from a Service database that resides at a CONUS depot. The data is in text format, is 20MB and must be updated every 2 hours. The acceptable user response time to a query on the status of the asset is 5 minutes.
- The current site configurations are shown in Figure 5.2-2.

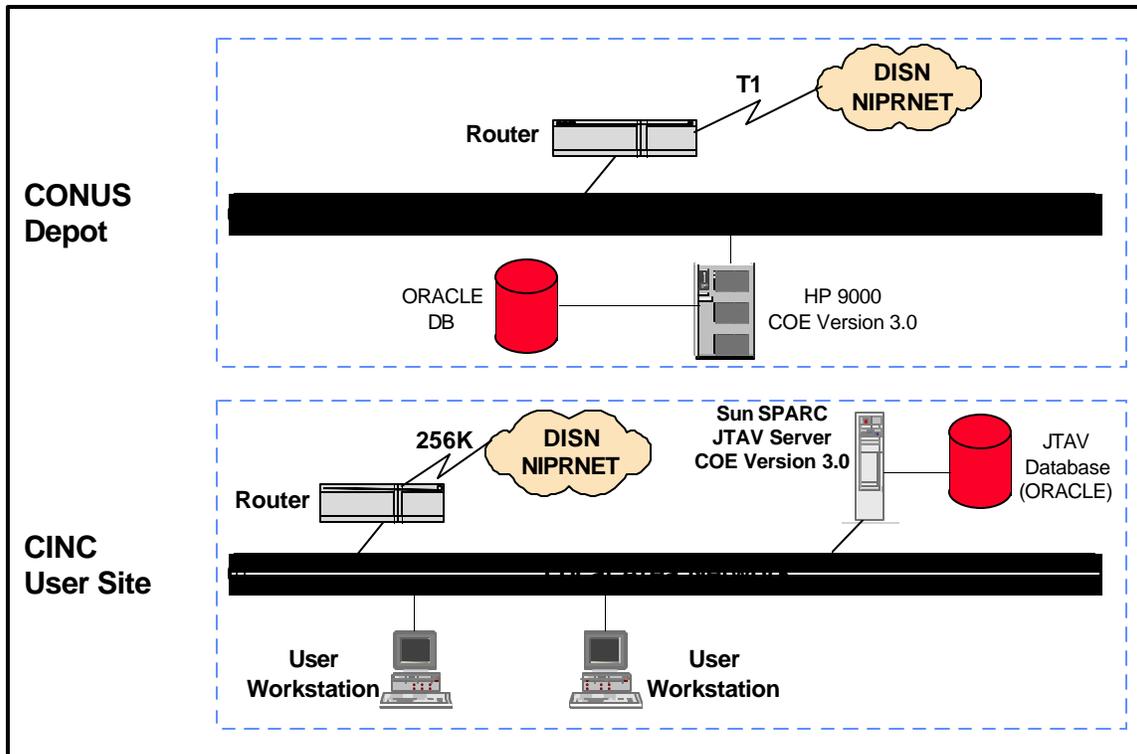


Figure 5.2-2 Current Site Configurations

- The specific design alternatives are shown in Figure 5.2-3. Using the JTAV system architecture, the best “to-be” solution would include the use of global data access capabilities to directly query the CONUS database, with the data being fused in a JTAV Server and presented to the user through a Web Based Client.
- An evaluation of the alternatives shows that the communications capabilities are not available to support the “to-be” solution and meet the user response time. Therefore, a near-term migration solution is chosen that replicates the data to the CINC site, and puts in place the rest of the “to-be” components. This is shown in Figure 5.2-4.

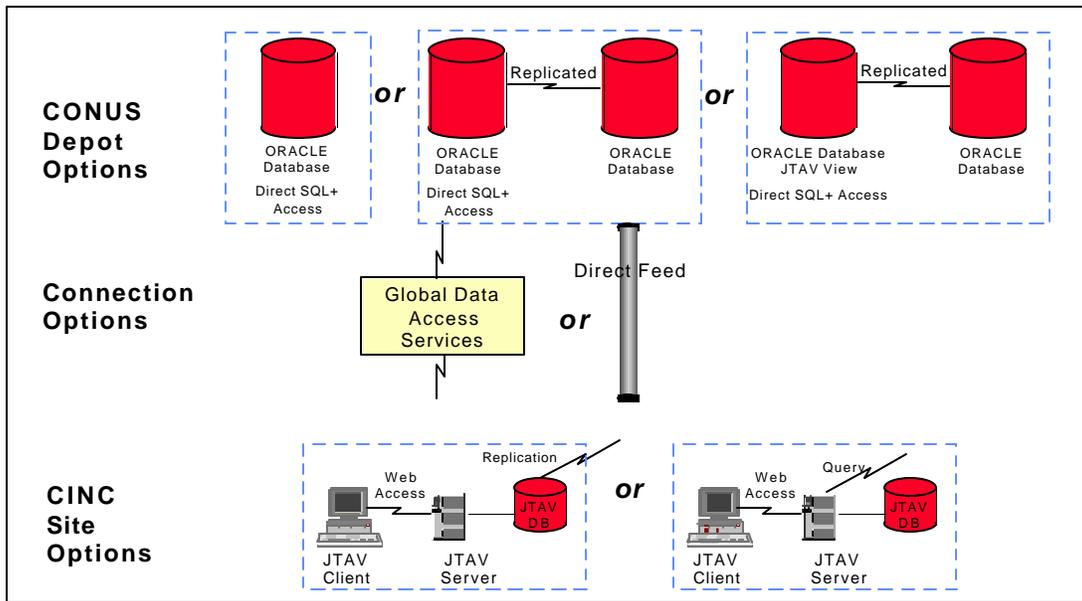


Figure 5.2-3 Architecture Design Alternatives

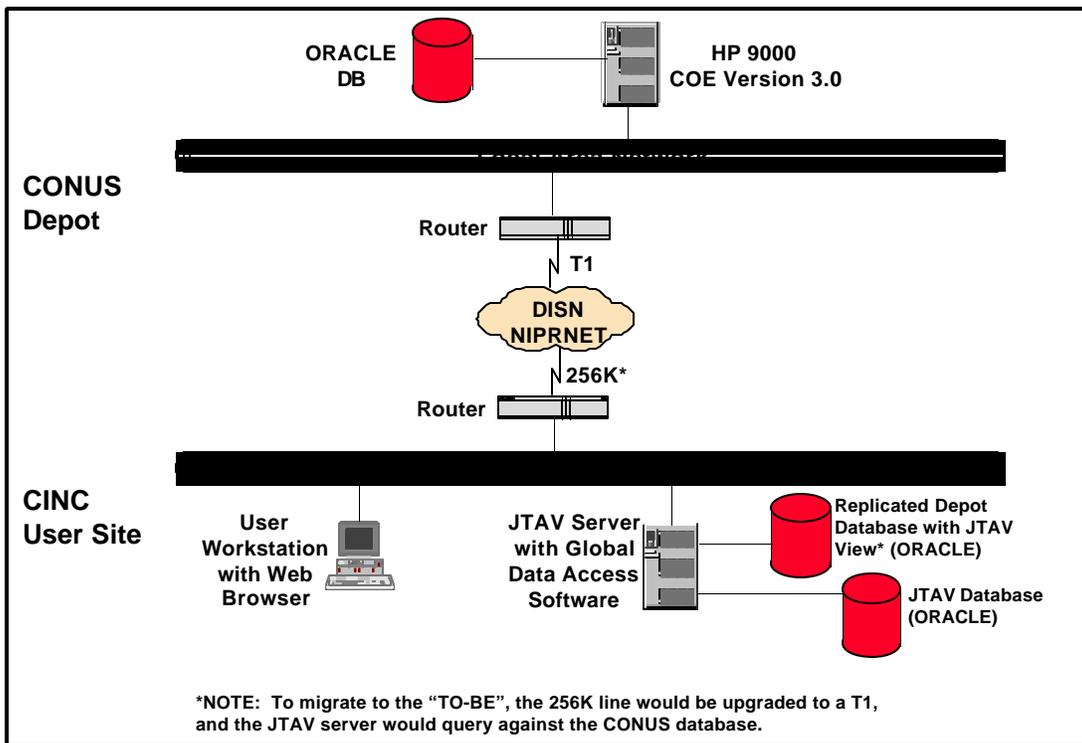


Figure 5.2-4 Selected Architecture Design with Migration Path

- The specific configuration highlighted above is chosen and an implementation plan developed that includes details on the migration to the “to-be” configuration.

5.3 Implementation Plan

The JTAV System Architecture is an evolutionary product that will be implemented in a phased approach based on operational requirements, deployment schedules and the availability of DII and GCSS compliant capabilities. The following lists the first level work breakdown structure for continued refinement and implementation of the architecture:

- Use the system architecture to develop the specific configuration for the GTN-JTAV interface;
- Develop and field GTN-JTAV interface solution;
- Develop detailed implementation plan covering all JTAV capabilities and data feeds;
- Perform cost/benefit analysis and determine fielding schedule;
- Develop and field incremental capabilities;
- Revise architecture based on lessons learned and new operational requirements; and

Develop technical infrastructure requirements

APPENDIX A

Asset Visibility Source Systems And Databases

Acronym	System Name
ADAM-III	Aerial Port Documentation and Planning System
ADMF	Active Duty Master File
AFEMS	Air Force Equipment Management System
AFMIS	Army Food Management Information System
AMMOLOGS	Ammunition Logistics System
AMS	Automated Manifest System
APADE	Automated Procurement and Data Entry System
ATAC	Advanced Traceability and Control System
ATAV	Army Total Asset Visibility
ATLASS	Asset Tracking Logistics and Supply System
AWRDS	Army War Reserve Deployment System
BASS	Base Automated Service Store
BCAS	Base Contracting Automated System
CAEMS	Computer-Aided Embarkation Management System
CAIMS	Conventional Ammunition Inventory Management System
CALM	Computer-Aided Air Load Manifesting System
CALM	Computer-Aided Air-Loading Manifesting System
CAPS-II	Consolidated Aerial Port System
CBS-X	Continuing Balance System - Expanded
CCSS	Commodity Command Standard System
CFM	CONUS Freight Management System
CMOS	Cargo Movement Operations System
COMPES	Contingency Operation/Mobility Planning and Execution System
CRAMSI	Consolidated Residual Asset Management Screening Information
DAMMS-R	Department of the Army Movements Management System - Redesigned
DFAMS	Defense Fuel Automated Management System
DISMS	Defense Integrated Subsistence Management System
DO35	DO35
DS4	Direct Support Standard Supply System
DSS	Depot Standard System
DTTS	Defense Transportation Tracking System
DTTS-E	Defense Transportation Tracking System - Europe
FOSAMS	Fleet Optical Scanning Automated Management System
FSM	Food Service Management
GDSS	Global Decision Support System
GTN	Global Transportation Network
IRIS	Interrogation Requirements Information System
LIF	Logistics Intelligence File
LIPS	Logistics Information Processing System
MAARS-II	Marine Corps Automated Ammunition Requisitioning System II

Acronym	System Name
MAGTF	Marine Air Ground Task Force/Logistics Automated Information System
MANPER-B	Manpower and Personnel Module
MDSS-II	MAGTF Deployment Support System II
Micro-SNAP	Micro-Shipboard Non-Tactical Automation Program
MUMMS	Marine Corps Unified Materiel Management System
MVIS	Materiel Visibility System
NADEPVIS	Navy Aviation Depot Visibility System
NATDS	Navy Automated Transportation Data System
OHMS	Ordnance Handling Management System
ORDVIS	Ordnance Visibility System
OSC	Objective Supply Capability
PASS	Personnel Asset Status System
PC-Troop	Personal Computer Troop
PRAMS	Passenger Reservation and Manifesting System
RCAPS-C	Remote Consolidated Aerial Port System - Cargo
RCAPS-P	Remote Consolidated Aerial Port System - Passenger
SAAS	Standard Army Ammunition System
SAILS	Standard Army Intermediate Logistics System
SAMMS	Standard Automated Materiel Management System
SARSS	Standard Army Retail Supply System
SASSY	Supported Activity Supply System
SBSS	Standard Base Supply System
SCS	Stock Control System
SDS	Standard Depot System
SDS	Source Data System
SNAP-Supply	Shipboard Non-Tactical Automation Program - Supply
STACCS	Standard Theater Army Command and Control System
TCACCIS	Transportation Coordinator Automated Command and Control Information System
TCACCIS	Transportation Coordinator's Automated Information and Movement System
TERMS	Terminal Management On-Line System
TRAC2ES	TRANSCOM Regulating and Command and Control Evacuation System
U2	U2
UADPS-Level-II	Uniform Automated Data Processing System -Level II
UADPS-SP	Uniform Automated Data Processing System - Stock Points
UD/MIPS	Unit Diary/Marine Integration Personnel System
UICP	Uniform Inventory Control Point
ULLS	Unit-Level Logistics System
VMSIR	Virtual Master Stock Item Record
WPS	Worldwide Port System

APPENDIX B - PROCESS MAPS

Joint Deployment and Sustainment Process Map

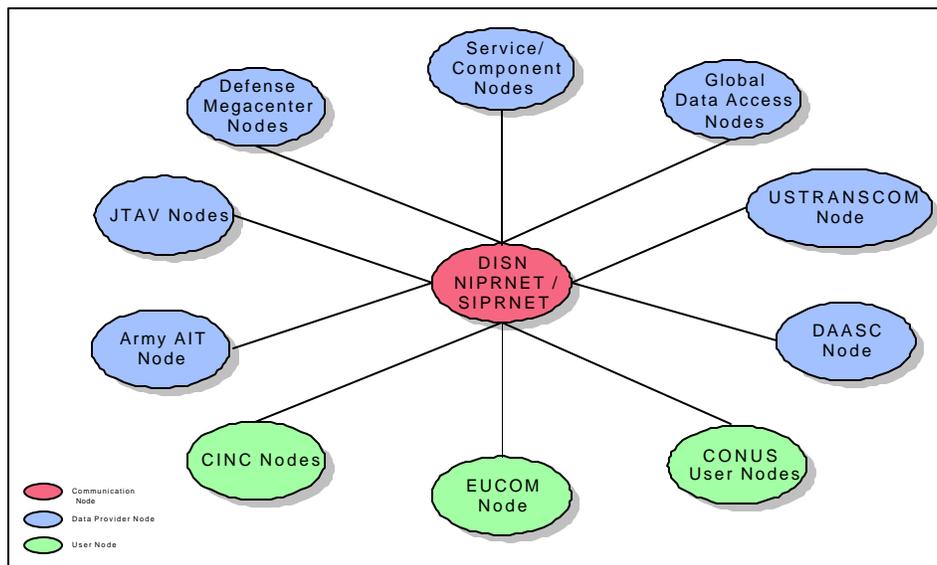
Joint Redeployment Process Map

NOTE : The process maps are not attached. They may be viewed in hard copy at the JTAV Program Office.

APPENDIX C

Node Identification and Node Connectivity Diagrams Node Identification

The following diagram illustrates an overview of the JTAV system architecture nodes. There are three general types of nodes: user nodes, data provider nodes, and communication nodes. User nodes are represented by the CINC Nodes, the EUCOM Node, and the CONUS User Nodes. The JTAV, Defense Megacenter, Service/Component, Global Data Access Service (GDAS), USTRANSCOM, DAASC, and Army AIT nodes typify the data provider nodes. The user nodes and data provider nodes communicate using the third type of node, the communications node, designated by the DISN Node.



Overall Node Connectivity Diagram

The relationship between nodes is illustrated using two types of diagrams: information flows (IF) and node connectivity (NC) diagrams. The information flows describe the data access process beginning from the information return point, i.e., after the query has been processed, the proper data source accessed, and the requested information compiled. The end point of the information flows are the requesting users. The node connectivity diagrams, beginning on page C-12, show the interconnection of two particular nodes. Information flow diagrams may have several node connectivity diagrams that correspond to them. The corresponding node connectivity diagrams will be listed under each information flow diagram.

Information Flow Diagrams

Figure IF-1 shows the information flow from a legacy system to a JTAV user. The data is downloaded from the legacy system to a shared data resource server. The data is then processed using stored procedures and passed to the Global Data Access Services (GDAS) node. The GDAS then performs any necessary data translation. Finally, GDAS sends the data to the requesting JTAV server using a COE based API. The server then transfers the data to the JTAV user.

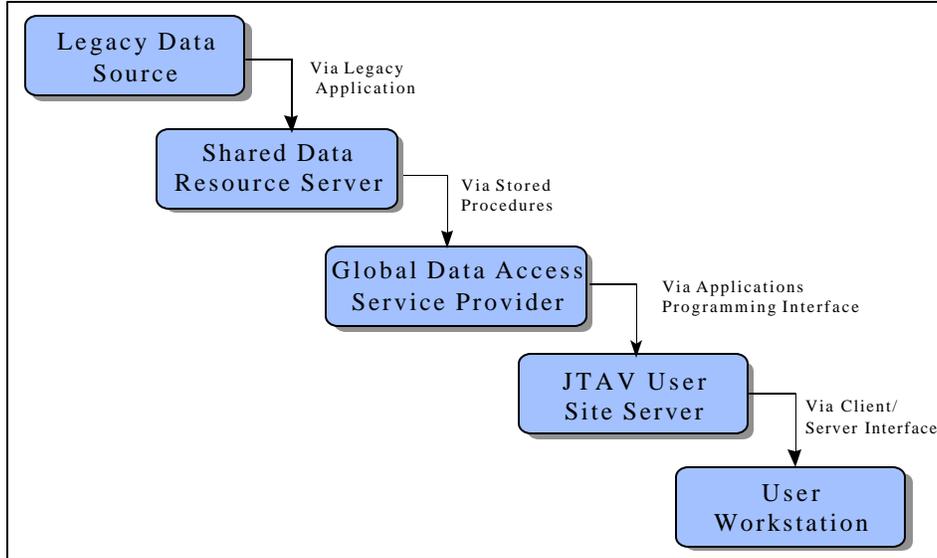


Figure IF-1 Legacy Data to JTAV User

The following node connectivity diagrams correspond to the Figure IF-1 information flow:

- NC-1 Legacy System to Shared Data Resource
- NC-3 Shared Data Resource to GDAS or NC-4 Defense Megacenter to GDAS
- NC-5 GDAS to JTAV User Site
- NC-12 JTAV to User

The information flow from a legacy system to a Joint Task Force (JTF) user is shown in Figure IF-2. This information flow is very similar to that in Figure IF-1. The main difference is that instead of the JTAV server passing the data to the JTF user, the JTAV server periodically downloads its data to the JTF JTAV server. The JTF user then queries this database for total asset visibility data.

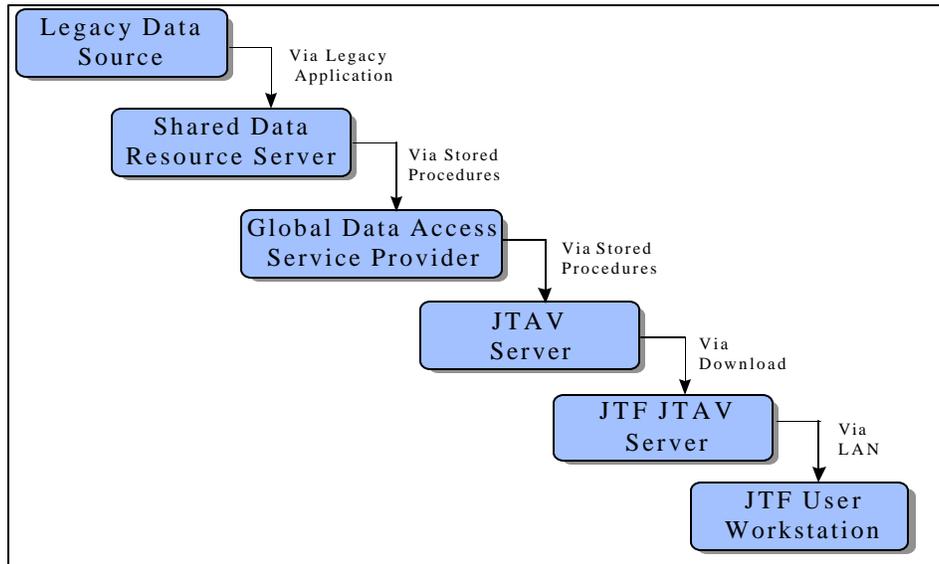


Figure IF-2 Legacy Data to JTF User via JTAV

The following node connectivity diagrams correspond to the Figure IF-2 information flow:

- NC-1 Legacy System to Shared Data Resource
- NC-3 Shared Data Resource to GDAS or NC-4 Defense Megacenter to GDAS

- NC-6 GDAS to JTAV Server
- NC-13 JTAV Server to JTF User

Figure IF-3 illustrates the flow from a legacy system to a JTAV user via the GDAS. Legacy systems send requested data to GDAS by using customized stored procedures. The GDAS passes the information to the JTAV server. The server then passes the data to the user workstation.

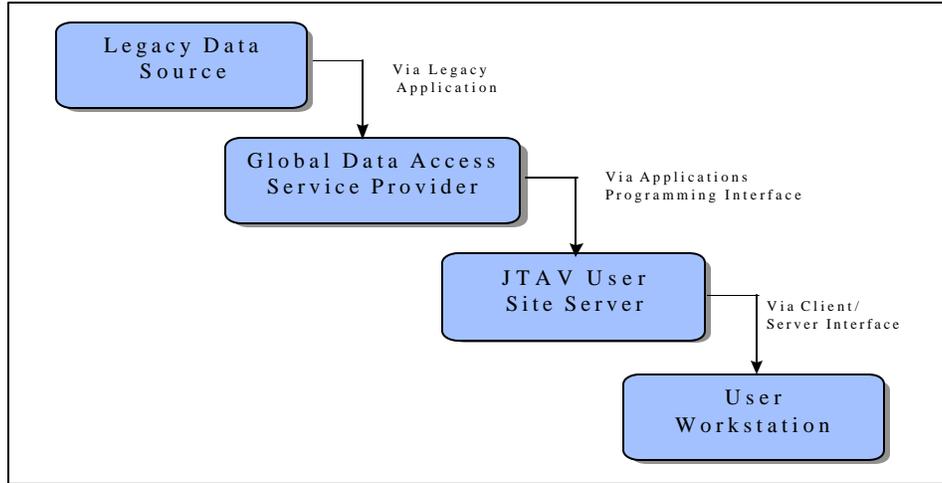


Figure IF-3 Legacy Data to JTAV User

The following node connectivity diagrams correspond to the Figure IF-3 information flow:

- NC-2 Legacy System to GDAS
- NC-5 GDAS to JTAV User Site

As shown in Figure IF-4, requested data is transferred from the legacy system to the GDAS. GDAS passes the data to the JTAV theater server using stored procedures. The JTAV server then downloads the data to the JTF JTAV server. The JTF JTAV database can then be queried by JTF users.

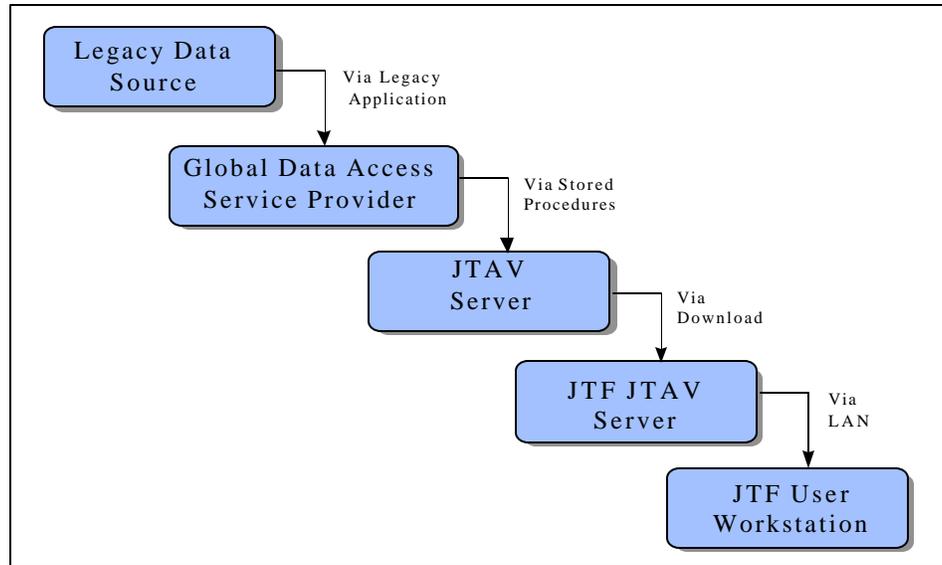


Figure IF-4 Legacy Data to JTF User via JTAV

The following node connectivity diagrams correspond to the Figure IF-4 information flow:

- NC-2 Legacy System to GDAS
- NC-6 GDAS to JTAV
- NC-13 JTAV to JTF User

Represented in Figure IF-5 is the information flow from GTN to JTAV users. GTN interfaces with the JTAV server using a GTN specific API. The server then passes the data to the JTAV user workstation.

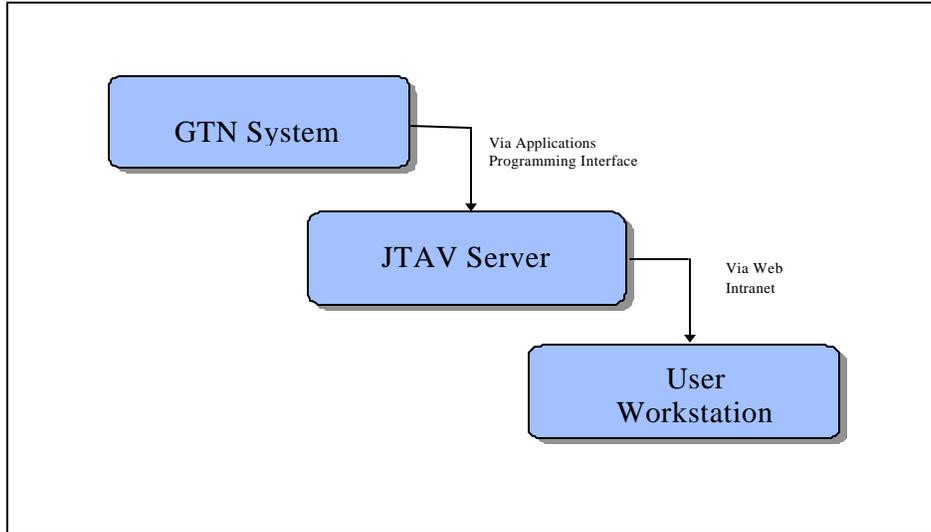


Figure IF-5 GTN Data to User

The following node connectivity diagrams correspond to the Figure IF-5 information flow:

- NC-7 GTN to User

Figure IF-6 portrays the information flow from the GTN system to JTF users. GTN downloads asset visibility data to a special JTAV database. JTAV accesses the special database and downloads information the JTAV theater database. The JTAV server then downloads the data to the JTF JTAV server. JTF users access the data directly from the JTF JTAV server.

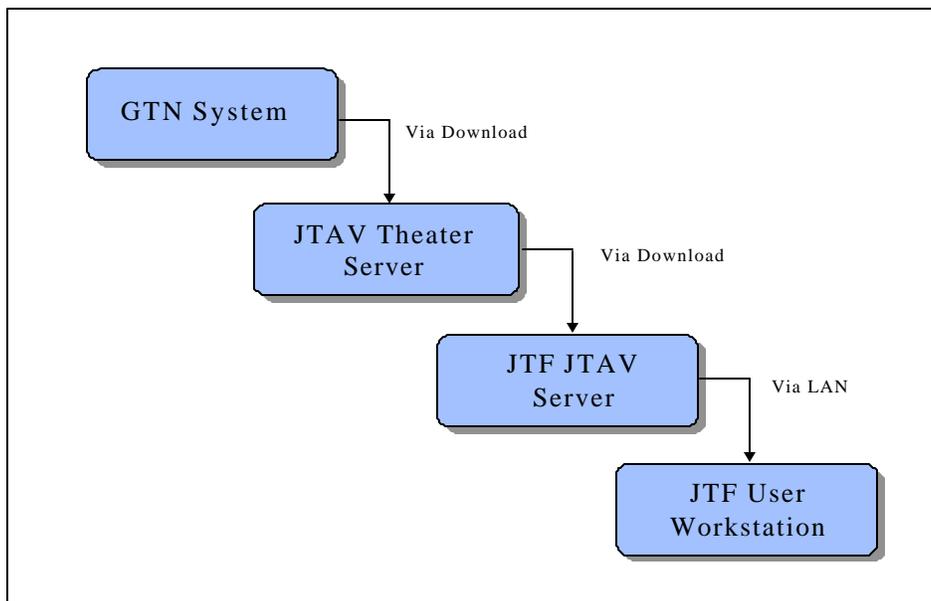


Figure IF-6 GTN Data to JTF User

The following node connectivity diagrams correspond to the Figure IF-6 information flow:

- NC-8 GTN to JTAV
- NC-13 JTAV to JTF User

Figure IF-7 depicts the information flow from the DAAS/LIPS system to JTAV users. DAAS/LIPS uses stored procedures to send data to the GDAS. While in the GDAS process, the data is translated from the form that GDAS receives it from DAAS/LIPS to the form required by the user. GDAS then transfers the data to the JTAV server that, in turn, sends it to the requesting user workstation.

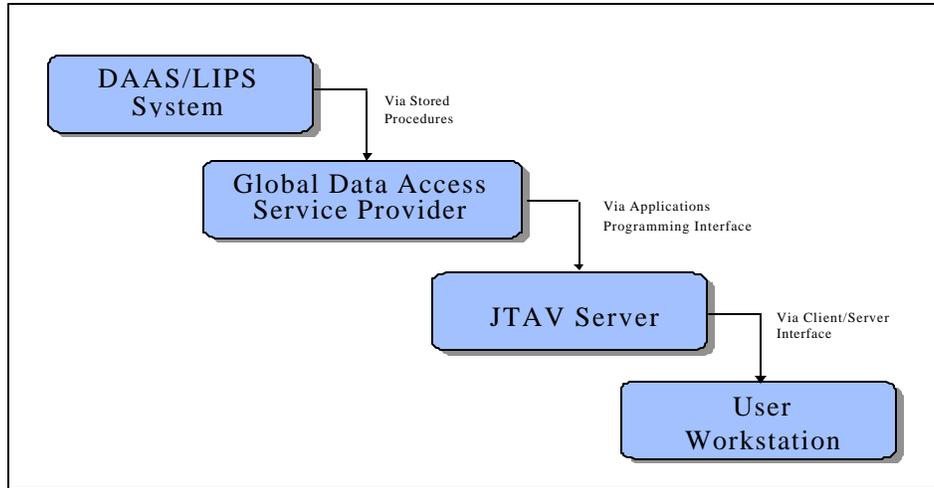


Figure IF-7 DAAS/LIPS Data to User

The following node connectivity diagrams correspond to the Figure IF-7 information flow:

- NC-9 DAAS/LIPS to GDAS
- NC-6 GDAS to JTAV
- NC-12 JTAV to User

DAAS/LIPS sends requisition data to JTF users via JTAV. Periodically, DAAS/LIPS will download its data to the JTAV theater server. The data is then downloaded to the JTF JTAV server where JTF users access the data. Figure IF-8 illustrates the information flow from DAAS/LIPS to JTF users.

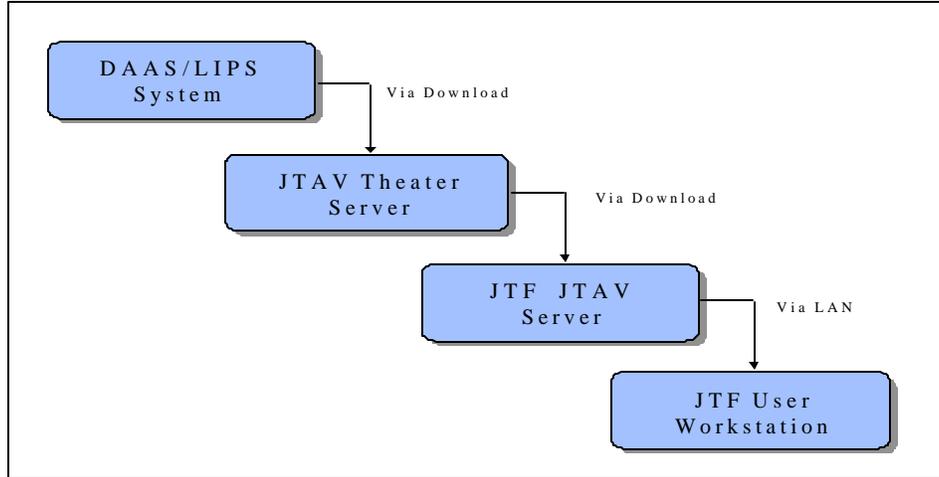


Figure IF-8 DAAS/LIPS Data to JTF User

The following node connectivity diagrams correspond to the Figure IF-8 information flow:

- NC-10 DAASC to JTA V
- NC-13 JTA V to JTF User

Figure IF-9 shows how a JTF user gets data from a component or service data source. The data is downloaded to the JTA V theater server by the data source. Periodically, the JTA V server downloads its data to the JTF JTA V server. The JTF user then access the data over a LAN from the JTF server.

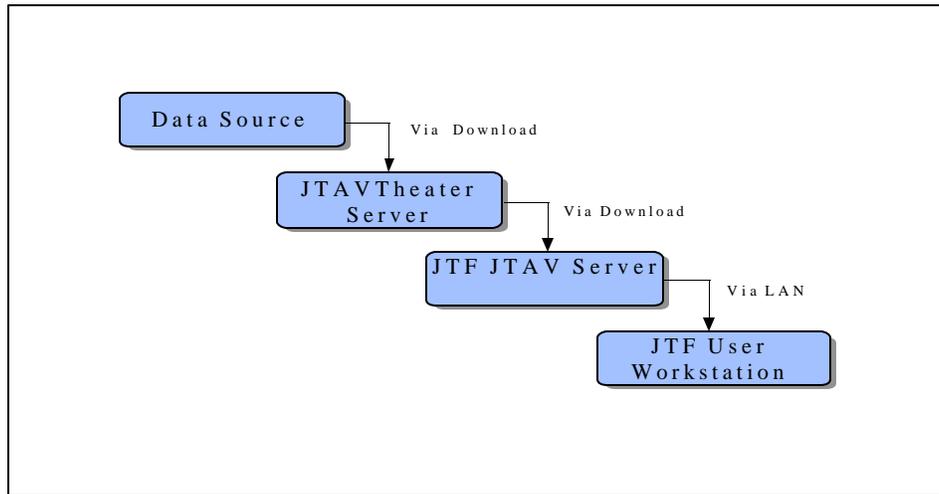


Figure IF-9 Data Source to JTF User

The following node connectivity diagrams correspond to the Figure IF-9 information flow:

- NC-11 Data Source to JTA V
- NC-13 JTA V to JTF User

Node Connectivity Diagrams

The node connectivity diagrams that follow all have the same layout. The node on the lower left hand side of the diagram (node A) is sending data to the node on the lower right hand side of the diagram (node B). The center node is the communications link between the two nodes. Next to each node is a list of activities that the node is required to perform for total asset visibility. In the upper left hand corner is a box containing the “information exchange requirements” which is the data that node A is passing to node B. It can be assumed that node A is passing information to node B because node B has previously requested the data. Any type of query, download, or database replication can be considered as a request.

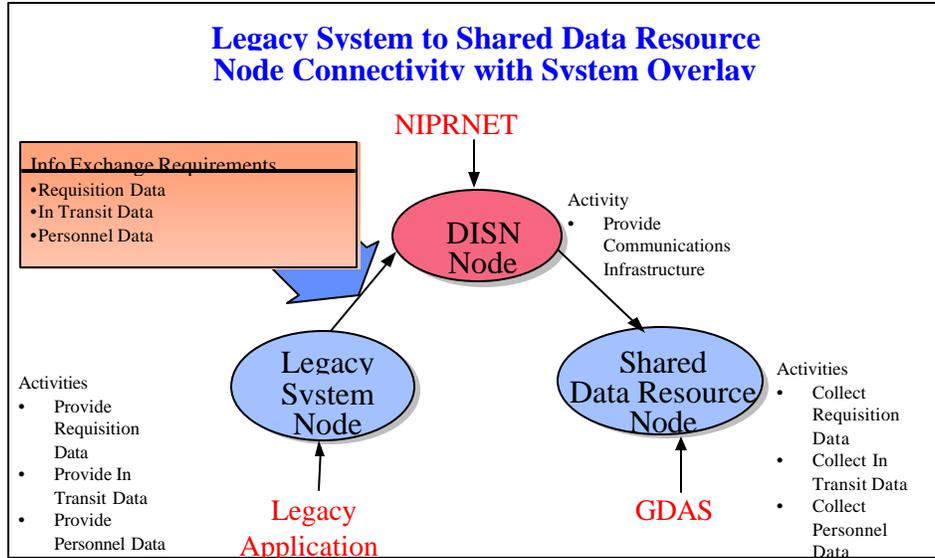


Figure NC-1 Legacy System to Shared Data Resource

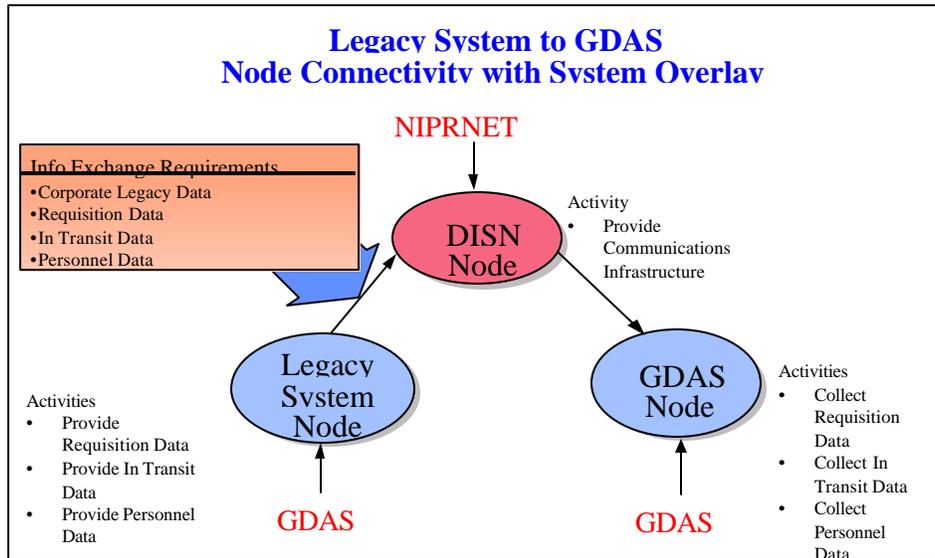


Figure NC-2 Legacy System to GDAS

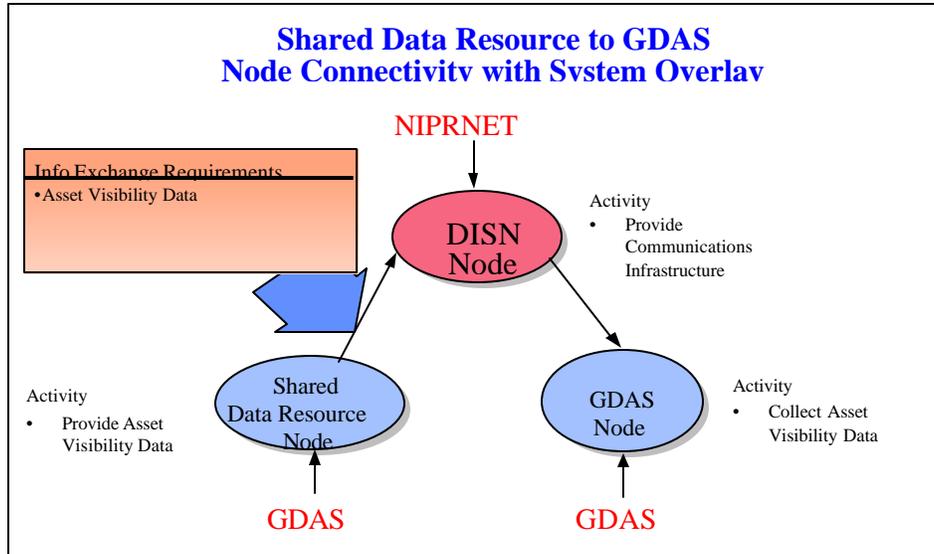


Figure NC-3 Shared Data Resource to GDAS

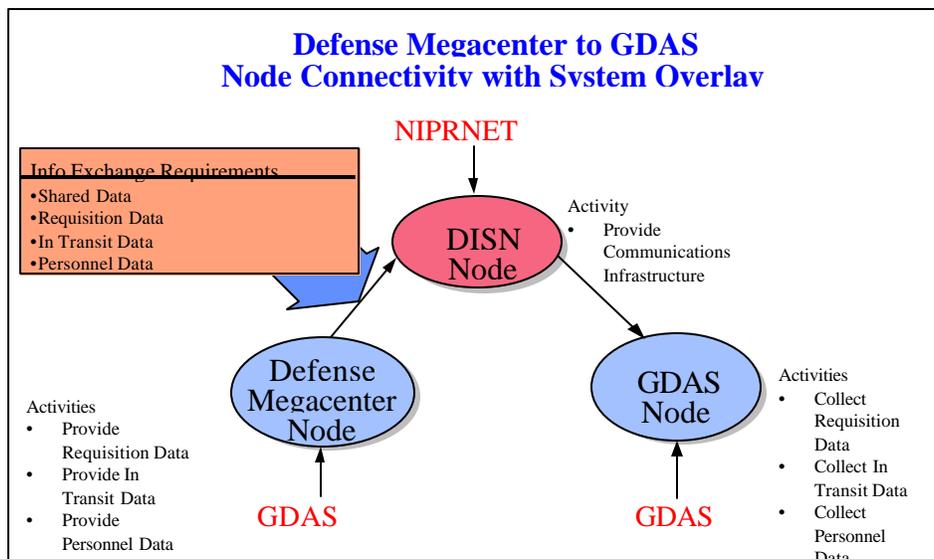


Figure NC-4 Defense Megacenter to GDAS

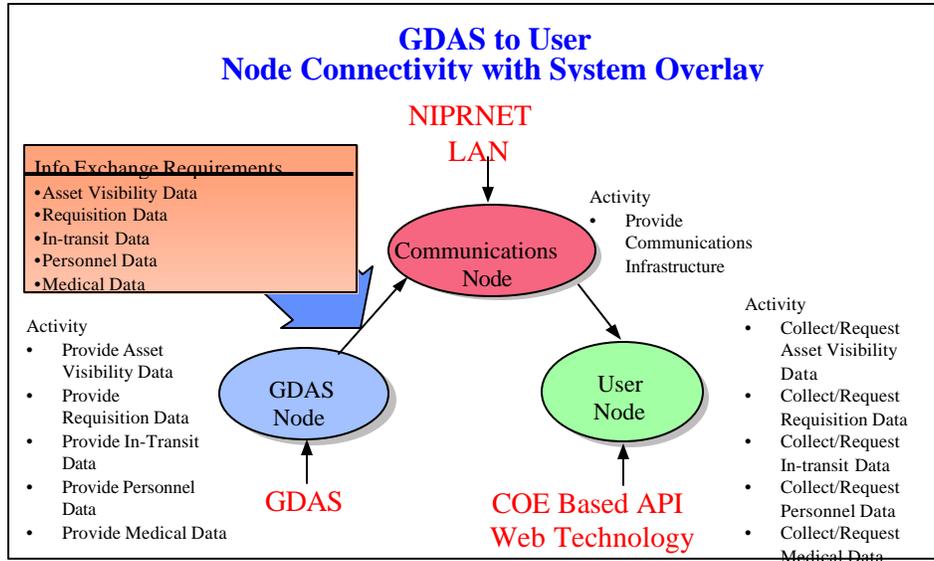


Figure NC-5 GDAS to User

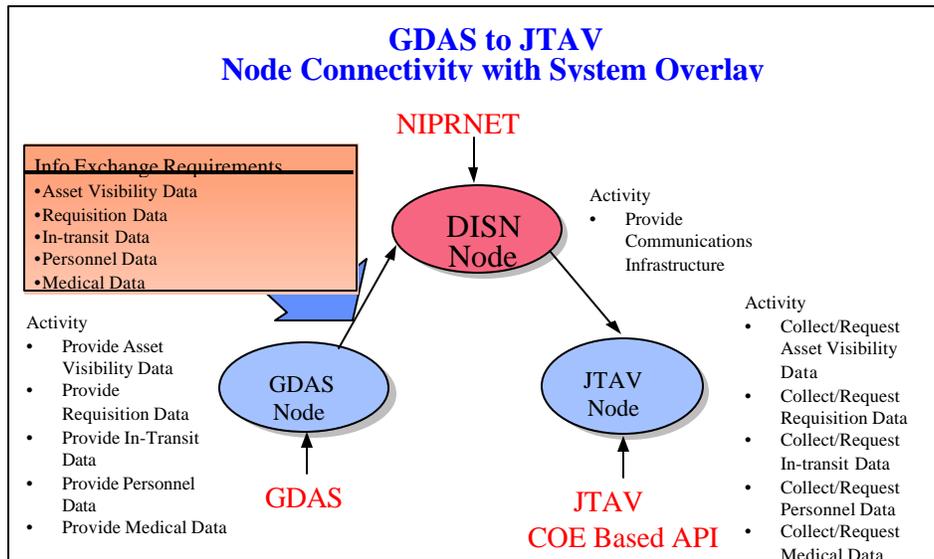
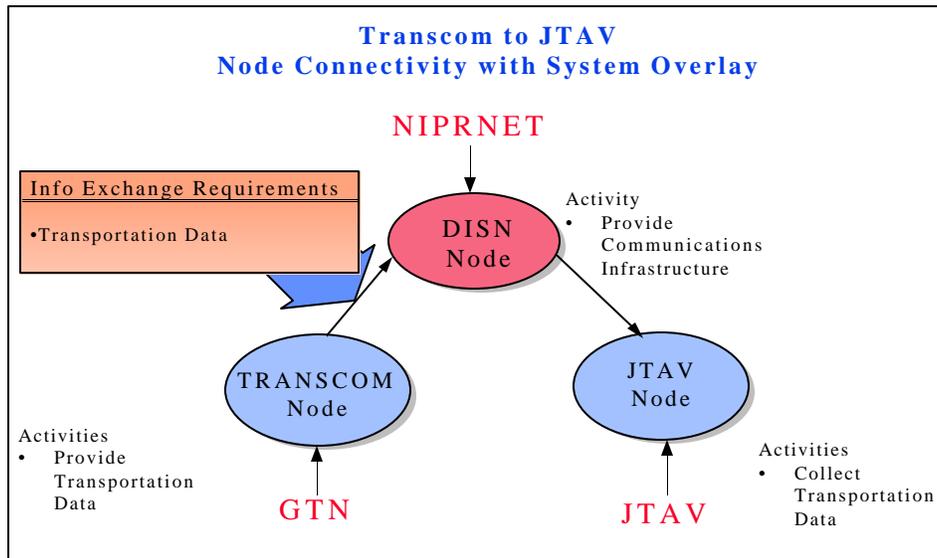
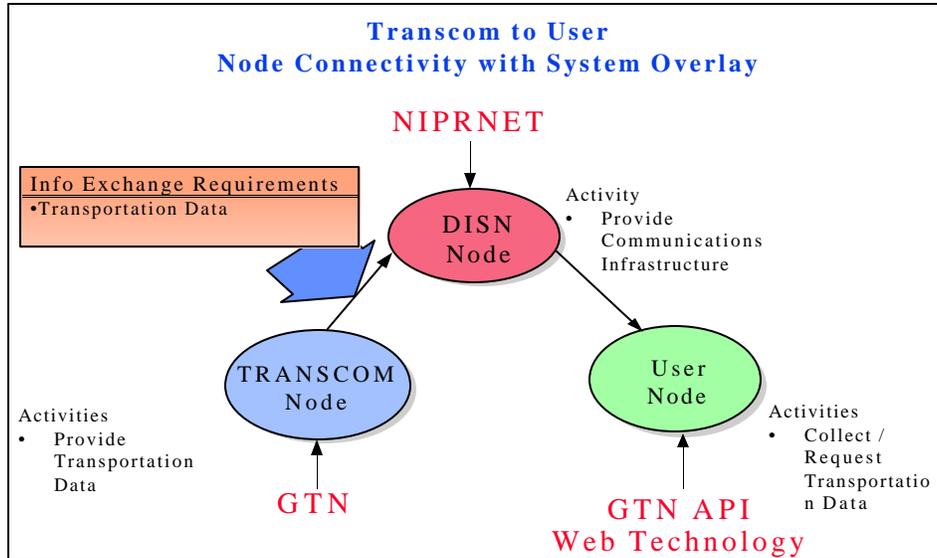


Figure NC-6 GDAS to JTAV



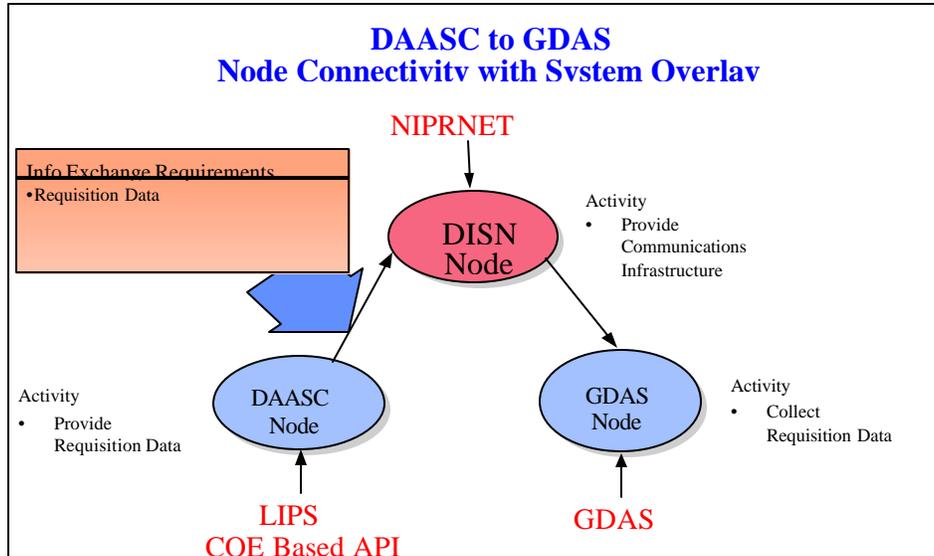


Figure NC-9 DAASC to GDAS

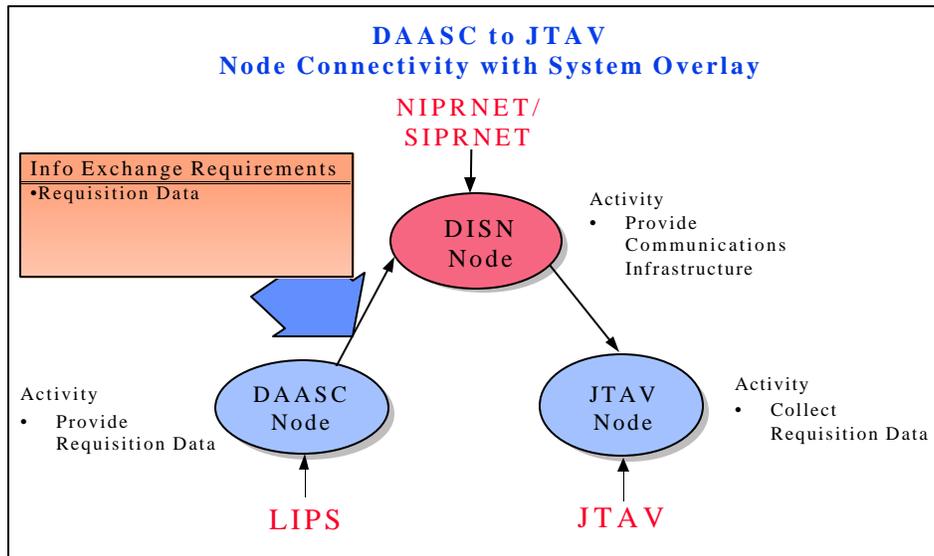


Figure NC-10 DAASC to JTAV

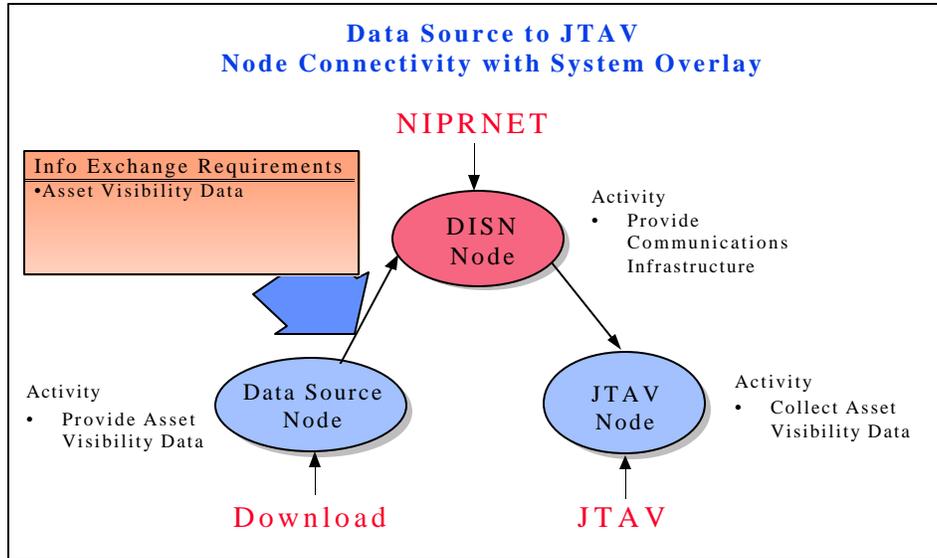


Figure NC-11 Data Source to JTAV

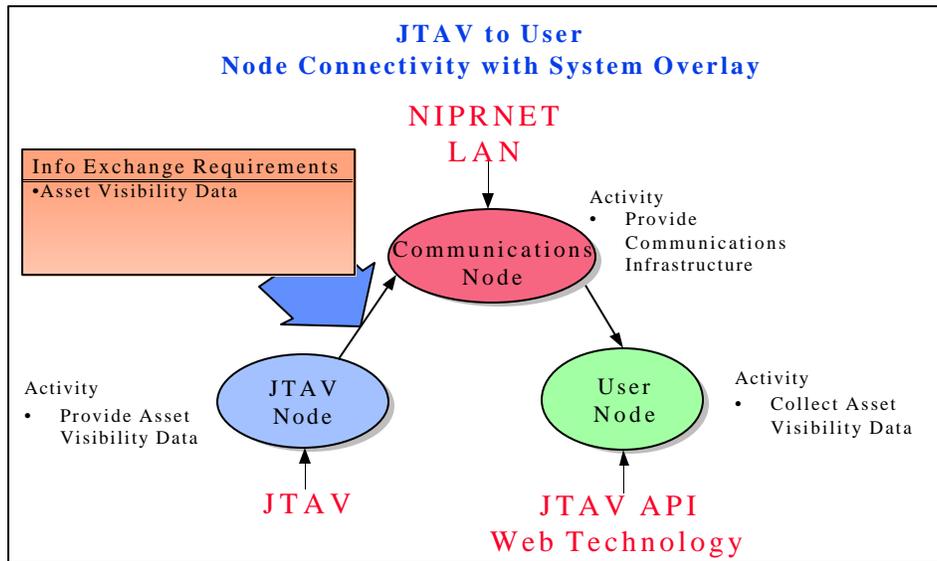


Figure NC-12 JTAV to User

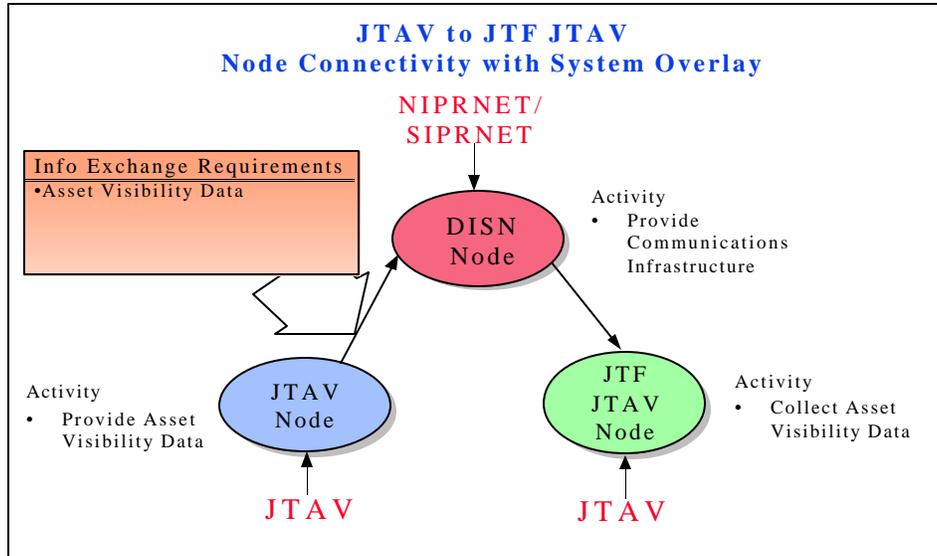


Figure NC-13 JTAV to JTF User

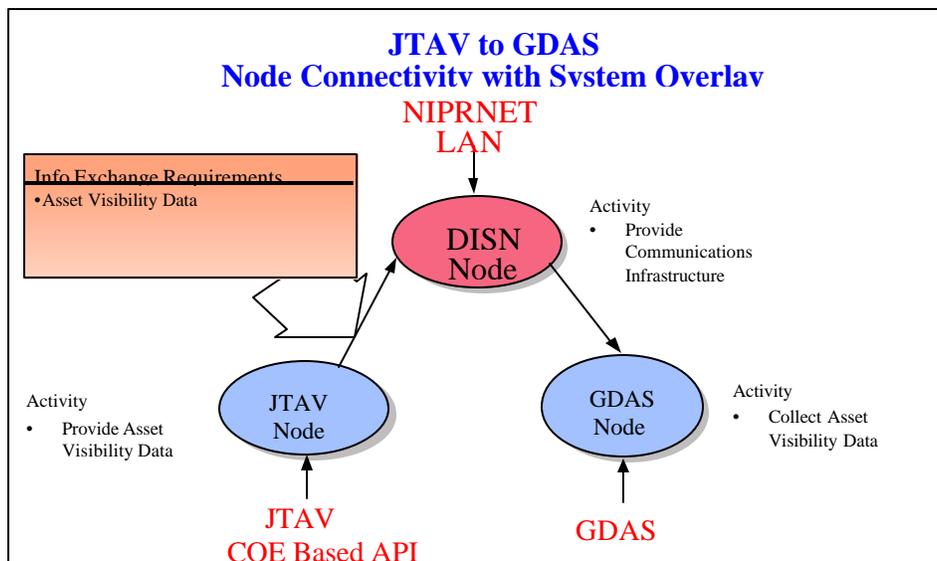
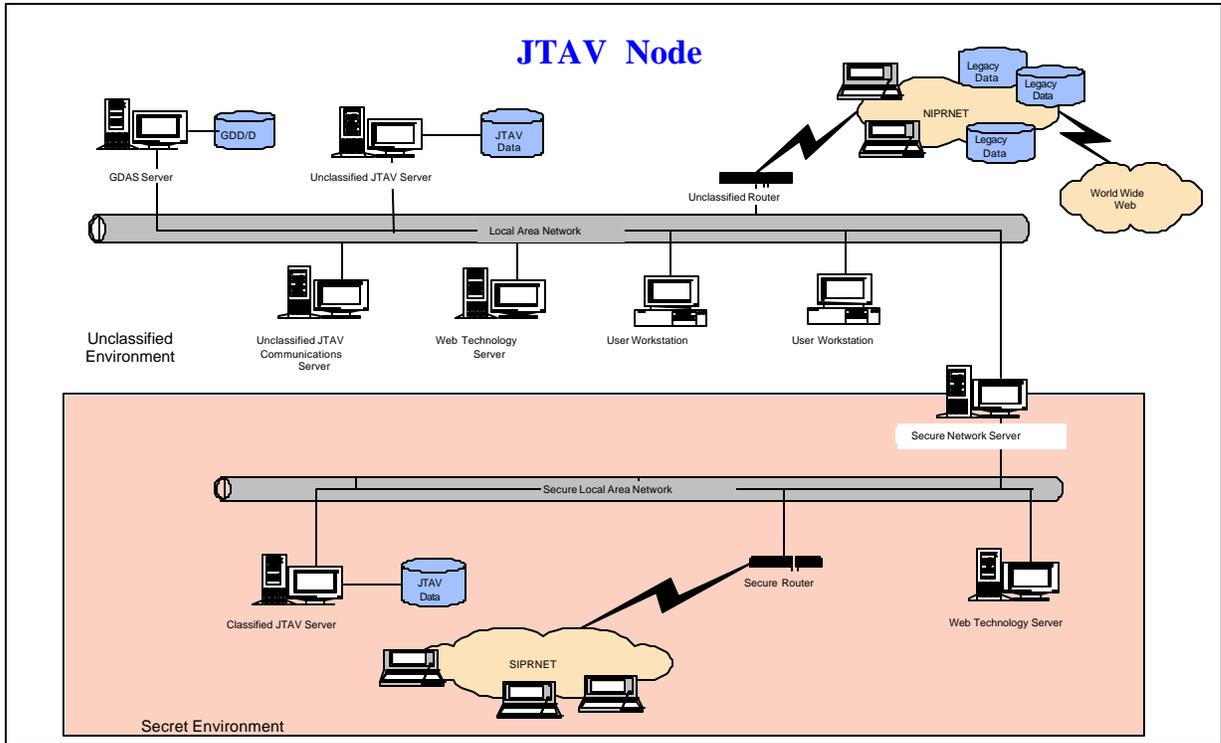


Figure NC-14 JTAV to GDAS

APPENDIX D

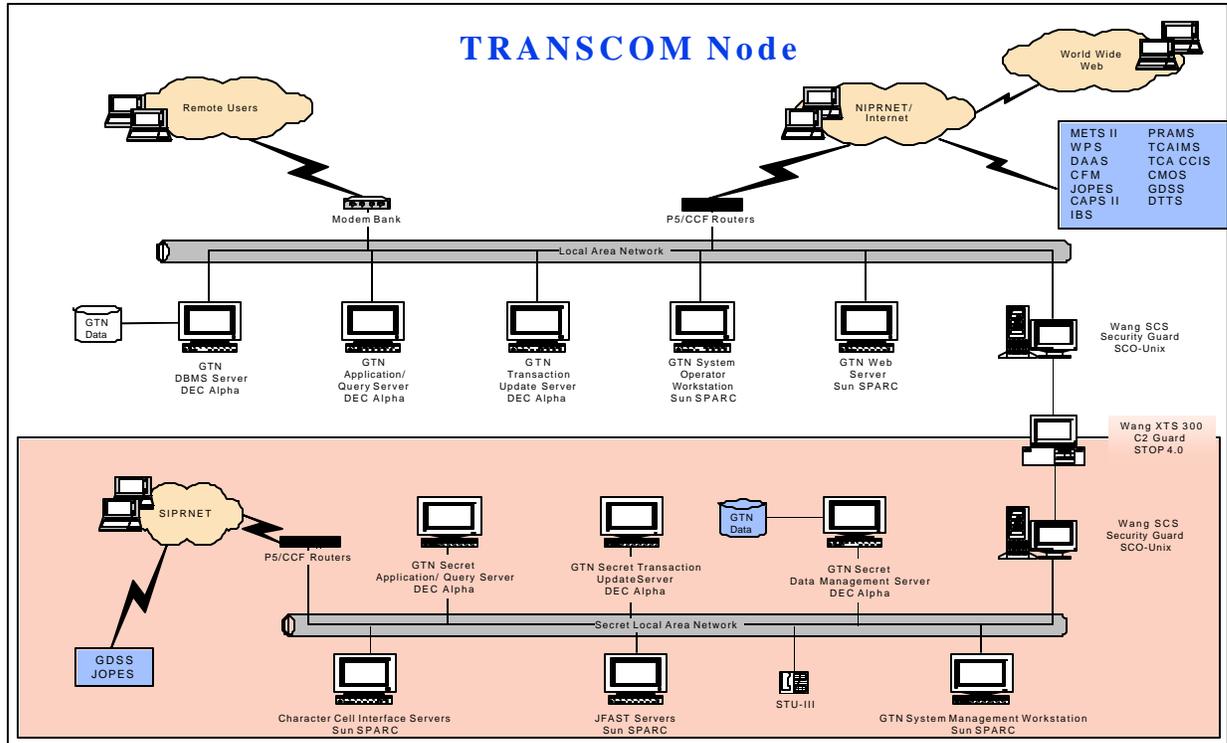
Node Configuration

This appendix contains system configuration diagrams for the total asset visibility nodes. Most of the node diagrams are a generalization of the technology and applications required at the type of node the diagram is representing. The exceptions to this are the GTN, DAASC, EUCOM, and AIT nodes. The hardware and software shown in these node configuration diagrams are the minimum required components to provide the infrastructure for the total asset visibility system to function. It is assumed that nodes will have various other hardware and software which may or may not interact with the total asset visibility infrastructure.



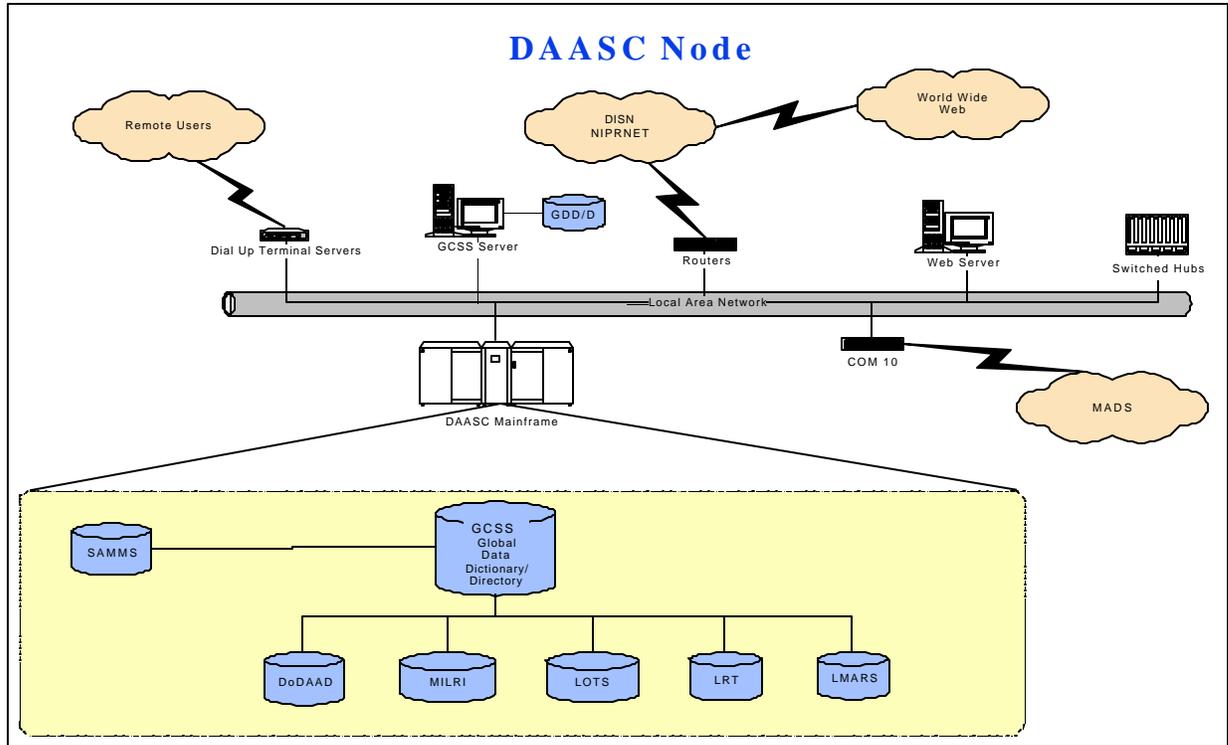
Required Components for the JTAV Node:

Hardware	Network / Communications	Applications	Data
Unclassified JTAV Server	Unclassified JTAV	JTAV	JTAV Data
Classified JTAV Server	Communications Server	ISEE Guard,	Global Dictionary
GDAS Data Server	Unclassified Router	Nighthawk	Global Directory
Web Server	Classified Router	Cyberguard	
User Workstations	Secure Network Server	Web	
	DISN (SIPRNET, NIPRNET)	Applications	
	LAN		
	Secure LAN		
	WWW		



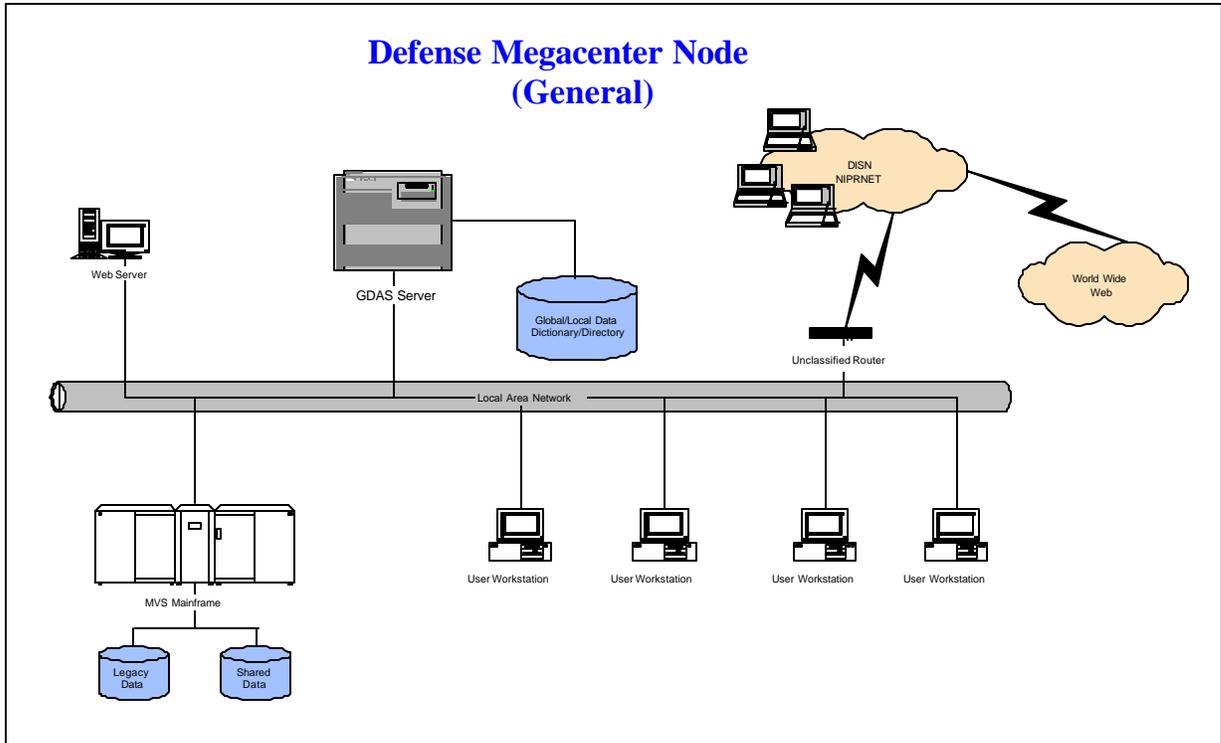
Required Components for the USTRANSCOM Node:

Hardware	Network / Communications	Applications	Data
GTN DBMS Server (Secure, non-Secure)	Unclassified Router Classified Router	GTN Web	GTN Data
GTN Application/Query Server (Secure, non-Secure)	DISN LAN	Applications	
GTN Transaction Update Server (Secure, non-Secure)	Secret LAN WAN	Wang SCS Security Guard	
GTN System Operator Workstation	WWW	Wang XTS 300 C2 Guard	
GTN System Management Workstation	Modem Bank	JFAST	
GTN Web Server	Secure Telephone Unit (STU)		
JFAST Server			
Security Servers			
Character Cell Interface Server			
User Workstations			



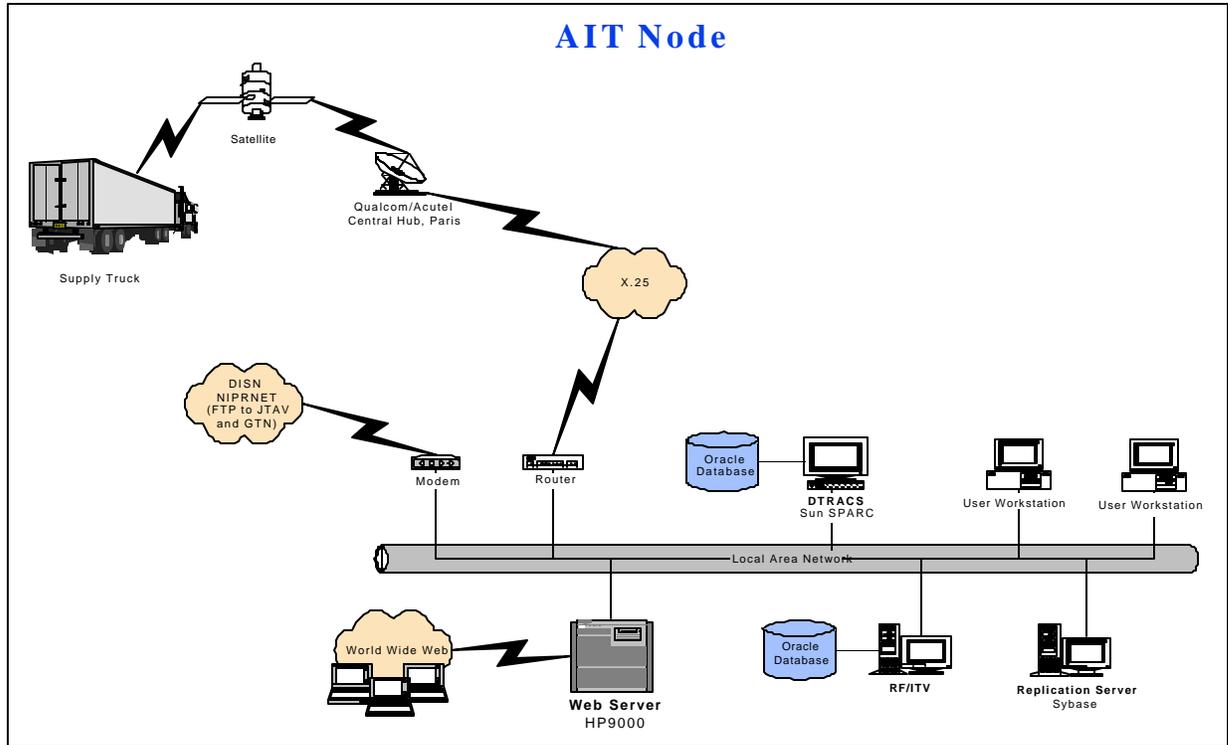
Required Components for the DAASC Node:

Hardware	Network / Communications	Applications	Data
DAAS Mainframe	Switched Hub	LIPS	Global Dictionary
GDMS Data Server	Router	GDMS	Global Directory
Web Server	DISN	SAMMS	DoDAAD Data
	LAN	Web Applications	MILRI Data
	WAN		LOTS Data
	WWW		LRT Data
	Dial Up Terminal Servers		LMARS Data
	COM10		



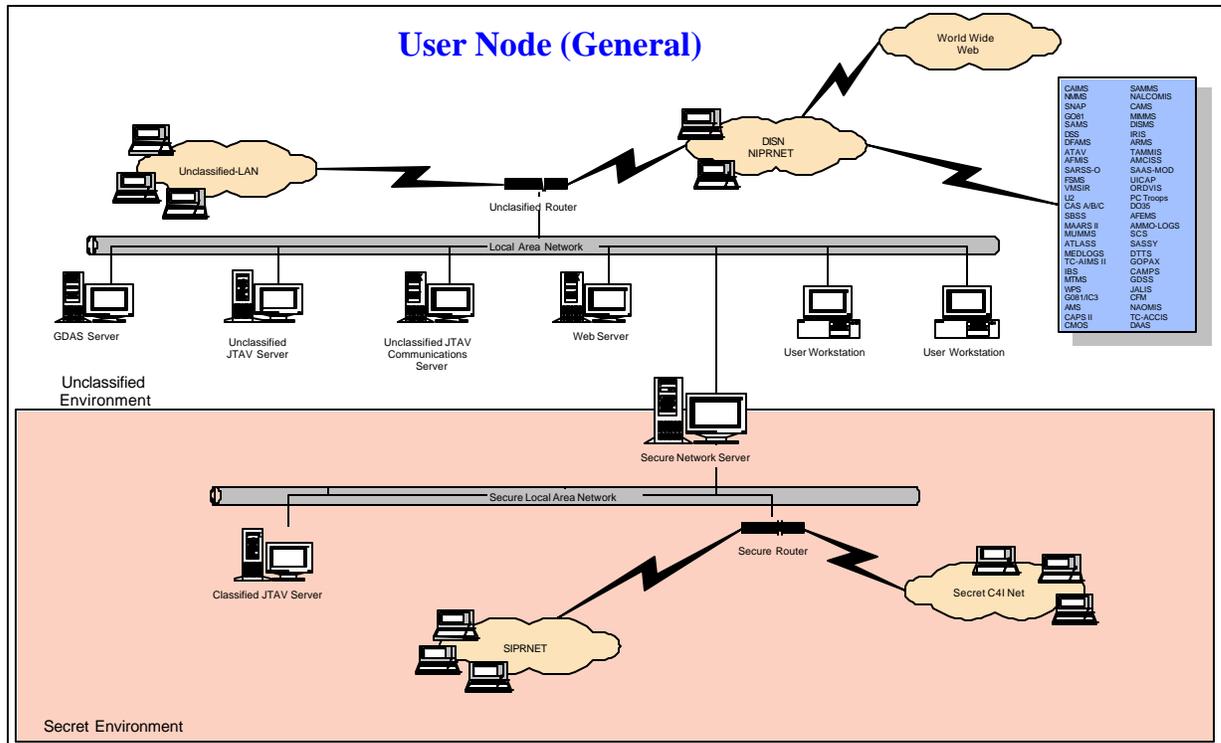
Required Components for the Defense Megacenter Node:

Hardware	Network / Communications	Applications	Data
MVS Mainframe GDAS Server Web Server User Workstations	Router DISN LAN WAN WWW	Mainframe Applications Web Applications	Global Dictionary Global Directory Local Dictionary Local Directory Legacy Data Shared Data



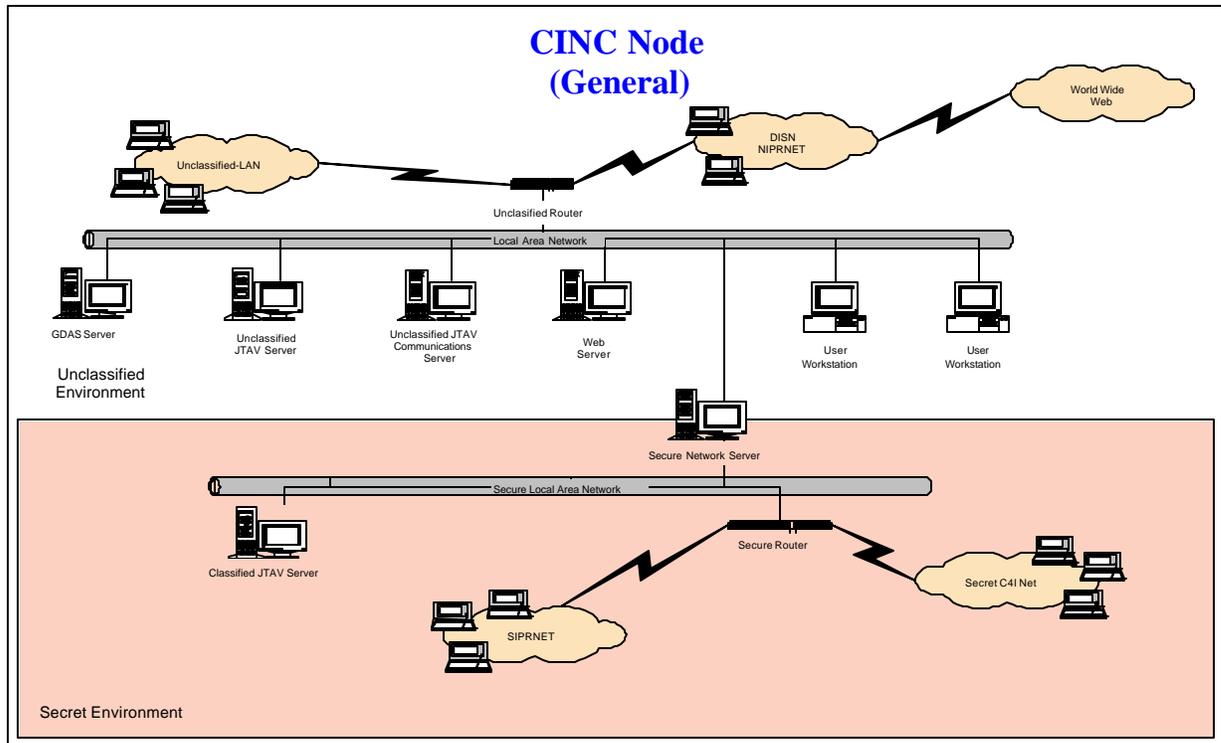
Required Components for the AIT Node:

Hardware	Network / Communications	Applications	Data
Radio Frequency Hardware DTRACS Server RF/ITV Server Replication Server Web Server User Workstations	Modem Router DISN LAN WAN WWW X.25 Satellite	DTRACS RF/ITV Web Applications	Tracking Data Radio Frequency Data Replicated Data



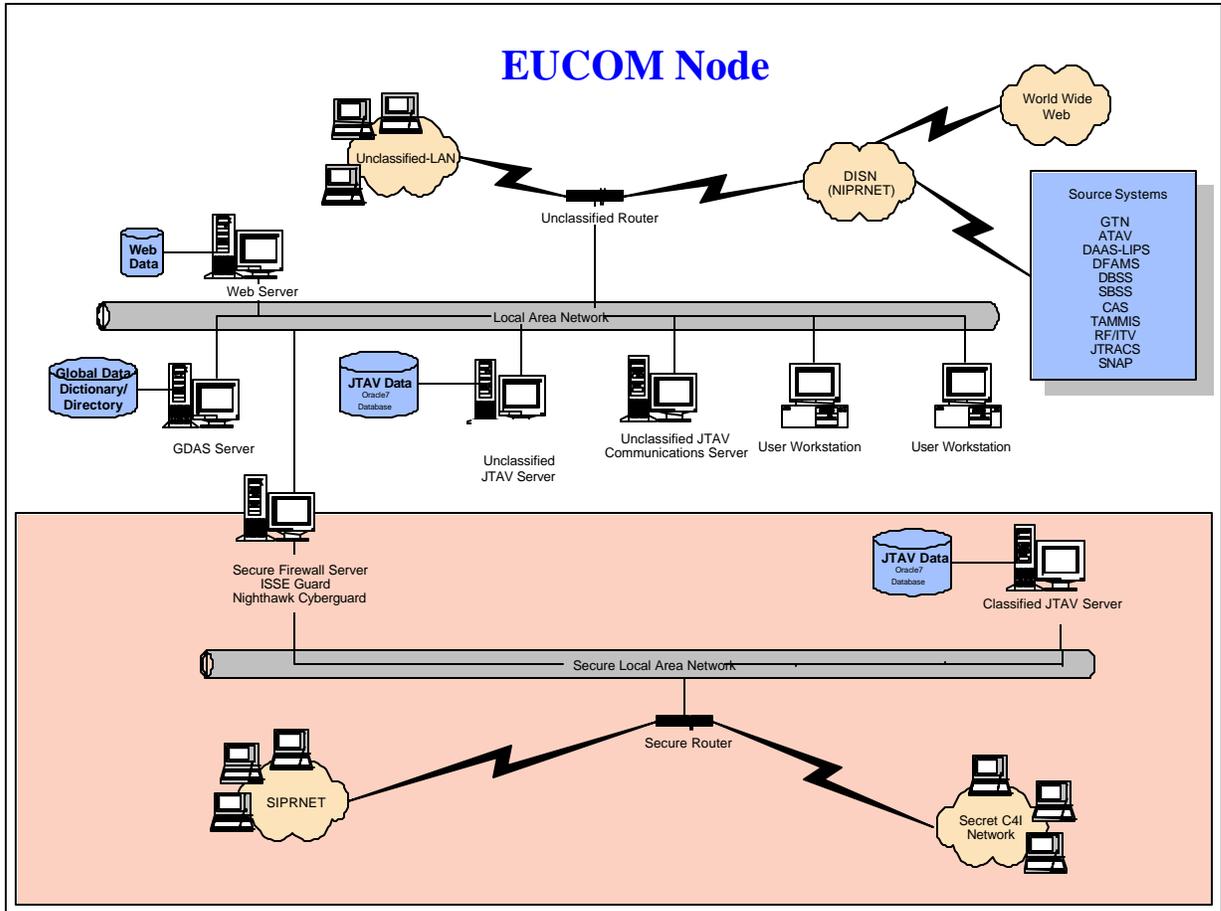
Required Components for the generic User Node:

Hardware	Network / Communications	Applications	Data
Unclassified JTAV Server	Unclassified JTAV	JTAV	JTAV Data
Classified JTAV Server	Communications Server	ISEE Guard,	Global Dictionary
GDAS Data Server	Unclassified Router	Nighthawk	Global Directory
Web Server	Classified Router	Cyberguard	
User Workstations	Secure Network Server	Web	
	DISN (SIPRNET, NIPRNET)	Applications	
	LAN		
	Secure LAN		
	WWW		



Required Components for the generic CINC Node:

Hardware	Network / Communications	Applications	Data
Unclassified JTAV Server	Unclassified JTAV	JTAV	JTAV Data
Classified JTAV Server	Communications Server	ISEE Guard, Nighthawk	Global Dictionary
GDAS Data Server	Unclassified Router	Cyberguard	Global Directory
Web Server	Classified Router	Web	
User Workstations	Secure Network Server	Applications	
	DISN (SIPRNET, NIPRNET)		
	LAN		
	Secure LAN		
	WWW		



Required Components for the EUCOM Node:

Hardware	Network / Communications	Applications	Data
Unclassified JTAV Server	Unclassified JTAV	JTAV	JTAV Data
Classified JTAV Server	Communications Server	GDAS	Global Dictionary
GDAS Data Server	Unclassified Router	ISEE Guard,	Global Directory
Web Server	Classified Router	Nighthawk	
User Workstations	Secure Network Server	Cyberguard	
	DISN (SIPRNET, NIPRNET)	Web	
	LAN	Applications	
	Secure LAN		
	WWW		

APPENDIX E

Common Operating Environment (COE) Services

Shared Data Environment (SHADE)

JTAV will be SHADE compliant where technically appropriate and feasible. The SHADE architecture provides key components to support Global Data Access for JTAV and other users. SHADE'S Global Data Access components include: DOD Data Dictionary; a Registration and Subscription database which identifies DOD's databases, locations, and network IDs; a set of mediation, transformation, and migration tools; and the guidance to create and use these services. These SHADE components should be used as centrally maintained globally accessible services, and they should only be replicated when needed for security or performance issues.

Directory services is the key service which makes Global Data Access work, and a key component of the SHADE Directory services is its Registration and Subscription database which maintains a registry for all of DOD's data. This database will act as the highest entry level for finding data within DOD. Directory services will be built upon the DII COE directory services components that will link and synchronize directories and directory services across the DOD enterprise.

SHADE is currently building a repository for storing all DOD COE/SHADE compliant data segments. The repository will include the metadata needed to search for and find segments as well as the metadata needed to use the segment. Also provided by SHADE is access control services which provide information on user/role/group based data access rights. Finally, SHADE provides and sponsors into the COE data access tools that provide data from the identified data sources according to the rights attributed to the user.

Near Term SHADE Components

The Data Dictionary is already available in the form of the DISA DOD Data Dictionary System, which describes the DOD standard data elements. Additionally, the DDDS is supported with a Defense Data Model (DDM), which provides a high level logical model of the DOD Data Standards. Several data access tools are already being segmented and proposed for COE compliance. They include: Global Data Management Services (GDMS), BrioQuery, OmniReplicator, and VirtualDB. Data Access tools currently in prototype include: Maria, a DARPA sponsored active-agent object-oriented, Web-based tool; the DARPA data server, an object-based Shared Data Server; and Data Access prototype, a SHADE sponsored DDDS dictionary-based access tool.

SHADE data architecture classifies segments into three groups: 1) the DBMS engine (an application); 2) the database (a preliminary lay down of the data structure), and 3) the data, (provides fill for the database). SHADE compliant databases will consist of at least one instance of these segments, but may be made of multiple database and data segments to fully build a database.

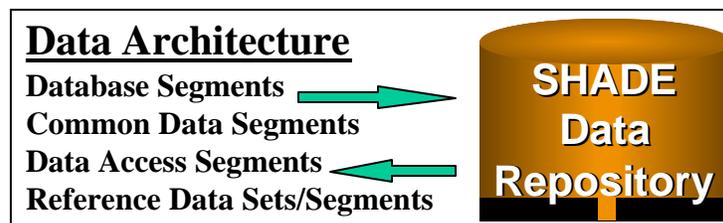


Figure 1 SHADE Data Architecture

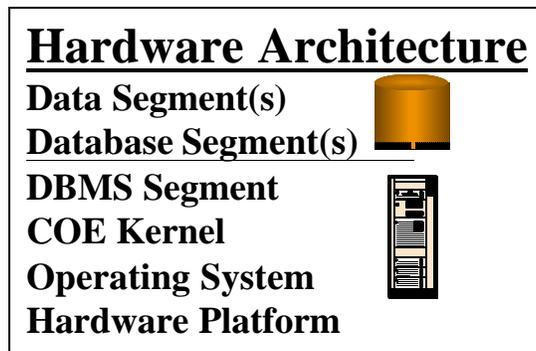


Figure 2 SHADE Hardware Architecture

Future SHADE Components

Components currently under design and development include the directory services database, access control database and services, and additional access tools are constantly being identified and proposed.

Additionally, the SHADE architecture recommends building a series of Shared Data Servers (SDS), and Joint Shared Servers (JSS) which look very much like the JTAV theater deployed and CONUS servers. JTAV, therefore, coincides with the latest COE/SHADE thinking for sharing data across functions and communities of interests.

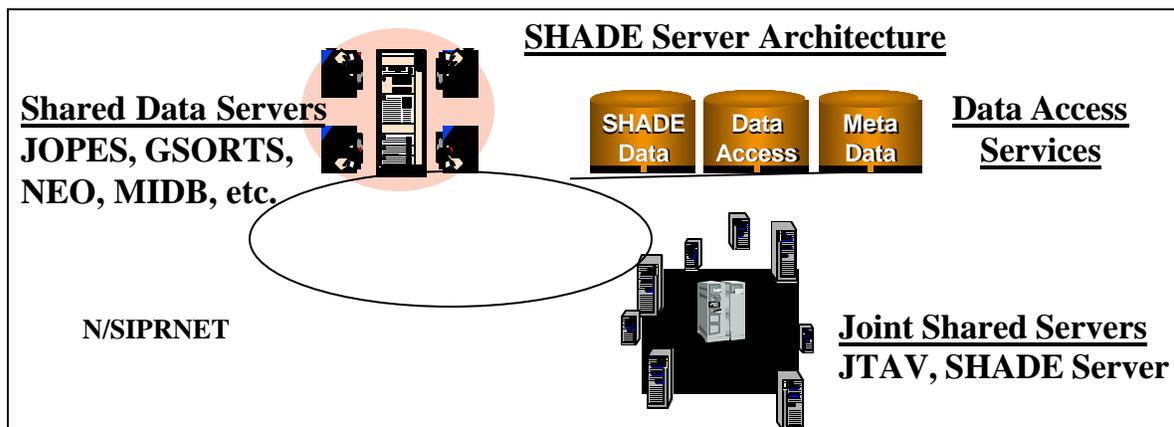


Figure 3 Future SHADE Components

SHADE Data Access

SHADE will identify a range of COE-compliant data access mechanisms that can interpret requests to retrieve/update/create/delete data, execute the requested function, and provide status information (and data in most cases) to the user.

In those cases where a retrieval request requires data from multiple databases and presentation of that data in a form other than that stored, SHADE sanctioned mediation software will provide location, translation and aggregation services as required. The primary function of these mediators will be to consolidate views of data across functional areas. This process will include accessing metadata contained in the JTAV data dictionary and the DOD Data Dictionary System (DDDS) in order to obtain the locations, business rules and mapping/matching criteria required to access data.

The Data Directory Service (DDS), the JTAV instance of SHADE's Metadata Server, will provide the information on the location of required data. This includes information on the site, database and data elements corresponding to the elements specified in the user request. This information will then be used by the Data Access Service (DAS), the JTAV instance of SHADE's Data Access Server, to route requests to retrieve, update, create or delete data to the appropriate data stores. More than one DDS can be configured but each provides comprehensive directory information. The API used to request data directory services will be standard.

DAS is provided by a series of COE/SHADE standard Application Program Interfaces (API) supporting data retrieval, update, creation and deletion functions, data translation functions, and data aggregation functions. This API will be compliant with those data access functions defined in the SQL standard, FIPS 127-2.

The DAS retrieves/updates legacy data via stored procedures and/or other data access processes as required. Stored procedures are typically developed by the functional organization responsible for managing and providing legacy data as a shared data resource. The DAS provides a COE/SHADE standard API to pass data retrieval, update, creation, deletion, and translation requests to these stored procedures and to accept the stored procedures' response to the data access request. The DAS may also provide data aggregation services from multiple stored procedures to satisfy an applications retrieval request that is processed across multiple databases.

The tools required to facilitate DAS will include SHADE Metadata Server functionality such as data directory service tools, and data management tools as well as SHADE Data Access Server functionality such as data replication service tools, repository service tools and application development tools.

Data directory service tools will provide the capability to manage the information on site, database and data elements corresponding to the elements specified in user requests. SHADE Data management tools will be used to govern repository data including the common view of data, mappings from legacy data to the common view, data models, schema, and access control profiles. COE-compliant Data replication products will provide the capability to replicate shared data resources including both horizontal and vertical fragmentation. Functions supported include monitoring data access frequency, automated replication when requested, and updating the data directory to reflect changes to database location and fragmentation. Repository service tools will provide the capability to support storage and management of the data dictionary, data directory, data mappings from legacy to common view of data and data models in the SHADE. The repository is used to provide directory, data dictionary and metadata information to developers, designers and enterprise engineers. Application Development tools will also provide links required to access data within legacy systems.

SHADE Data Access Control

COE/SHADE currently provides some of mechanisms required to control data access consistent with DOD policy. Future versions of the COE/SHADE will provide greater capability. The JTAV Data Access Control Service (DACS) implements DOD security policy in to two different processing environments. The first is an environment where data is at most sensitive but unclassified while the second is a classified environment operated in a system high mode. The DACS is part of the DAS and supports ad hoc queries for data across the JTAV shared data environment (i.e., JTAV subset of the SHADE). This requirement makes conventional data access authorization by individual very difficult. Users may not be aware of the specific databases from which they may want to retrieve data and the number of users that potentially want data from a particular database increases dramatically. The JTAV data access control procedure strives to reduce the administrative burden on the database administrator while still maintaining overall unique identification of data requesters.