Combat Information Transport System (CITS)

Information Transport System (ITS) Architecture
FY10 Version

Abstract

The purpose of this document is to provide an Architectural framework for work that our Integration Contractors can use when supporting the ITS program. This ITS Architecture will provide an enterprise context for the ITS technical baseline which is defined in the Baseline Program Description (BPD). The document describes the set of capabilities that the CITS program management office (PMO) will consider when reviewing individual ITS solutions that are intended to meet base unique requirements. Specific installation/implementation direction is separated into multiple sections dealing with System, Network Hardware and Cable Distribution (both outside and inside) requirements.

4 January 2010

Table of Contents

Reference Documents

Final Operational Requirements Document (ORD) for Combat Information Transport System (CITS), AFCA 003-97-I/II/III, 15 January 1998.

CITS Program Management Directive (PMD) 0026(10).

Unified Capabilities Requirements (UCR) 2008, Dated 22 January 2009

1 INTRODUCTION

1.1 Purpose

The existing basewide information transport system for many Air Force bases cannot support the future information needs of the warfighter. The proliferation of new information systems and an increasing reliance by the Air Force on information technologies require that the base information transport systems be modernized to meet the needs of the 21st Century. At the same time, budget reductions throughout DoD create a demand for greater efficiency in the way we implement our information and information transport systems.

The Combat Information Transport System (CITS) is a multi-billion dollar Air Force acquisition program to provide fixed-base information infrastructure and network management/network defense (NM/ND) capabilities to meet the wartime, crisis, and day-to-day multimedia information transport needs of MAJCOMs, functional areas, and Air Force Bases. CITS is the Air Force component of the National Information Infrastructure (NII) and the Defense Information Infrastructure (DII). CITS was founded in 1997, when the AF saw the need for a centrally managed and funded Program Management Office (PMO) that would provide the reliable, secure, manageable, affordable, and robust network infrastructure necessary to support all AF network communications over the Wide Area Network (WAN). The CITS charter is to provide centralized Command and Control (C2) and Information Assurance (IA) tools, upgrade existing base backbones with high speed data transport capabilities, upgrade and manage base telephone switches and management systems, provide network management of information systems, and to provide the training, sustainment capabilities, and help desk activities necessary to support those core functions. CITS is responsible for the information transport of all network traffic in the AF, both on the Non-Secure Internet Protocol Router Network (NIPRNET) and the Secret Internet Protocol Router Network (SIPRNET). This infrastructure provides the warfighter and wing command center with full access to real-time C2 information during day-to-day operations and contingencies.

The CITS program encompasses optical cable systems, digital voice/data/video/ sensor/imagery systems, allied support, network management and operations systems, information assurance systems for fixed and initial deployed networks and life-cycle management resources. CITS comprises an integrated set of Commercial-off-the-Shelf (COTS) networking components, as well as commercially available NM/ND software applications that are hosted on COTS computer hardware. The use of commercially proven COTS hardware and software allows rapid acquisition of networking functionality with relatively low risk.

1.2 Direction

CITS is being implemented in accordance with the CITS Operational Requirements Document (ORD) and per direction of the CITS Program Management Directive (PMD) 0026(10).

1.3 Scope

CITS comprises the following major component subsystems:

- Information Transport System (ITS)
- Network Management and Network Defense (NM/ND) and
- Voice Switching System (VSS) and Telecommunications Management System (TMS)

Collectively, these subsystems provide the networking infrastructure, management mechanisms, security features, and associated services (e.g., directory services, billing) for voice, data, video, sensor, control, and other forms of wired and wireless electronic communications at fixed AF facilities (bases, GSUs, etc.) throughout the world. They also include standard interfaces for interworking with DoD and commercial long-haul communication facilities and for interoperation with the communications and networking components of other DoD services.

CITS is comprised of the Information Transport System (ITS), the Network Management and Network Defense (NM/ND), and the Telecommunications Management System and Voice Switching System (TMS/VSS). Although interfaces between the ITS and the NM/ND and TMS/VSS are discussed briefly, only the ITS component of CITS is documented in detail in this document.

The ITS comprises a common, base wide backbone transport network (cable plant, other transmission facilities, and switching components), links from the backbone network to specific end buildings, interfaces to external and internal networks, components required to implement the various transport services (data, voice, video, etc.), and interfaces with the NM/ND. Each of these is discussed in more detail in the following sections.

In general, the ITS does not include distribution facilities within buildings (except for cabling among multiple communications closets) or end-device user attachments. However, the CITS program may procure equipment required to interface existing end-building systems with the ITS backbone network. CITS will provide the basic unclassified backbone and backbone-to-end building transport capabilities for both unclassified and classified services.

1.4 CITS Architecture Framework

Combat Information Transport System (CITS) provides war fighters at fixed Air Force facilities (bases, GSUs, etc.) throughout the world the means to exchange critical mission command and control information with both fixed and deployed DoD elements. CITS also enables communications among core mission-support organizations and, in its ultimate implementation, will support all fixed-facility Air Force communications throughout the world. CITS comprises the base-level, Air Force component of the world-wide Global Information Grid, with integrated transport for classified and unclassified

voice, data, video, imagery, control, sensor data, and other information sources. Integrity, availability, security, and other key characteristics of a global network are provided by the Network Management/Network Defense (NM/ND) components of CITS.

Figure 1 (CITS OV-1 High Level Operational Architecture) outlines the high-level operational concept of the CITS Program. The CITS domain comprises all of the fixed-facility components within the grey area of the diagram, i.e., fixed bases (including contingency or "temporary" bases), geographically-separated units (GSUs), etc. [Note: Although the NM/ND portion of CITS may support temporary and GSU locations, the ITS does not.] "Although AFCIOC, AFCERT, I-NOSCs and ESUS (hereafter referred to as the AFNETOPS organizations) are located on Air Force bases, they are considered separate functional entities, because of their functional roles and the manner in which they connect to and interwork with other AF and non-AF entities. Note that the I-NOSCs and ESUs also support many of the application, database, and ancillary servers for user applications and communications.

As illustrated in the Operational Architecture diagram, CITS enables classified and unclassified mission and support users to communicate with similar users at AF facilities throughout the world. The CITS domain also facilitates the flow of management (network monitoring, control, configuration, security, etc.) data between Network Management/Network Defense (NM/ND) components within a CITS facility as well as between that facility and the AFNETOPS organizations. CITS also enables information exchange between fixed AF facilities and other AF units (deployed, mobile, etc.), as well as information exchange with other services and DoD organizations. Finally, CITS provides the mechanisms by which information can be exchanged with the global civilian information and telephony networks.

Note from the Operational Architecture diagram that long-haul, wide area network data transport is actually (and predominantly) provided by the Defense Information Systems Network (DISN), although some use of leased commercial transport also exists. However, CITS provides the mechanisms (gateways, security boundaries, logical circuits, etc.) by which information is exchanged and controlled across the DISN. CITS does not provide wide area data transport, but is a user of long-haul, wide-area data transport services provided by the Defense Information Systems Agency (DISA).

Figure 2 (CITS SV-1 Inter-System Interface Diagram) offers a high level description of how the major components of CITS are related to each other and the systems that interface with them. As noted in the diagram, the ITS portion of CITS does not include the first 400 feet where CITS users and computer systems are typically located. Nor does ITS include the NM/ND components which provides services to the ITS and its users. At some locations, the NM/ND components may actually reside within a designated ITS facility.

While the ITS does not include either network or telephone end appliances, the ITS backbone system is being designed so that it can meet future growth needs as well as all of the high reliability, availability and rapid recovery requirements for both of these

systems. An action has also been initiated under CITS to fully integrate Air National Guard (ANG) organizations into the One Air Force -- One Network Architecture. At most fixed base locations, the ITS portion of CITS will simply incorporate the ANG units as another element of the base network. A complete description of the tasks involved with the full integration of the ANG organization into the Air Force network is beyond the scope of this document.

1.5 ITS Baseline Program Description

The CITS Program Management Office (PMO) at Electronic Systems Center (ESC) Hanscom AFB, MA is currently responsible for the fielding of the ITS portion of CITS. The PMO receives funding and requirements direction from the CITS Lead Command and maintains a document titled ITS Baseline Program Description that defines how requirements are managed to keep contractual expenses within the funding baseline.

2 GENERAL CHARACTERISTICS THAT DEFINE THE BASELINE ITS ARCHITECTURE

Before describing the proposed baseline architecture for the ITS, we outline a number of assumptions and discuss the major technological and topological characteristics that typically define a campus-wide Local Area Network architecture.

First, the CITS program provides full network interconnection to core buildings and those selected non-core buildings with a defined requirement for VoIP service. Furthermore, even if a base does not have a current requirement for VoIP, the ITS backbone should be designed to support the requirement at a future date without requiring a complete system replacement. The ITS portion of CITS is assumed to comprise a predominantly "fixed plant," ground based system with one or more discrete nodes at which communications are switched, routed, or otherwise transferred via one or more connecting transmission links to other nodes and to end-user devices connected to those nodes. This is a typical configuration for most fixed plant networks, whether for telephone, data, or other communications.

Such networks are typically defined by the characteristics of the switching nodes and their interconnecting transmission links, including:

- Number and distribution of nodes,
- Switching technologies used (to include, for example, circuit switching, frame switching and routing, cell switching),
- High reliability, rapid reconfiguration and overall robustness are important characteristics when a data network is being considered as a host platform for C2 applications and integrated voice data systems,
- Transmission technologies (optical fibers, copper wires, point-to-point radio systems, etc.), and
- Connectivity among nodes and end-user systems (e.g., star, meshed, or bus networks, as well as hybrid combinations and hierarchical configurations).

The geographical distribution, number, and interface requirements for end-user devices influence the selection of a specific switching technology (or technologies) and the overall network topology. Such requirements include data rates and traffic characteristics, as well as reliability, maintainability, availability, and security. Selections are also influenced by local constraints, such as the need to interwork with existing or proposed on- and off-base networks and systems and, of course, by fiscal limitations.

2.1 CITS Definitions

Several definitions are useful before proceeding. First, note that ITS installations are not fully funded and, therefore, cannot include every possible building on a base. Only those buildings that are identified as having mission impacts will initially be connected to the

ITS. Such buildings are defined to be *core buildings* and, as discussed in Appendix A, are further divided into three categories; these are intended to help tailor solutions that are in alignment with the mission content of the facility.

Standard facility management techniques have called for Core buildings to be logically grouped into a number of discrete geographical areas or zones. Each zone is served by a single, major switching node that is called an *Information Transfer Node (ITN*). Physically, an ITN comprises one or more switching components plus any transmission and ancillary equipment required for connections to other ITNs and to *End Building Nodes (EBN).* EBNs comprise the switching subsystems that are found in each building and that connect end-user equipment (workstations, terminal, servers, etc.) via a *local subscriber link* to the ITN serving the zone in which the building resides. EBNs also provide local switching among end-user systems. Finally a *transit ITN* is an ITN that is located in a building or other facility where there are concentrations of transmission systems and distribution equipment, but with no local users or attached EBNs.

The CITS ITS Program uses the same ITN and EBN building designations. The ITS Architecture however makes a distinction between the Outside Plant (OSP) cable and the network hardware components of ITS. The OSP portion of the ITS *backbone network* is therefore comprised of all the transmission systems (fiber optic cables, copper cables, patch panels, discrete radio links) that interconnect all of the designated ITN buildings. By definition, each ITN building will usually be connected to two or more other ITN locations (with an average typically greater than two), although, in a few cases (where extreme local geography or cost considerations override) an ITN may be connected to the backbone via a single transmission link. Thus the backbone is typically (and by objective) a *partially meshed* network, although *fully meshed* networks (every ITN connected to every other ITN) may be implemented on bases with only a few ITNs.

The OSP portion of ITS also includes transmission facilities that interconnect EBN building locations to a parent ITN building. Usually this involves a single uplink to the main ITN building in the same geographical area as the EBN. However, the OSP connectivity to EBNs may be adjusted under special circumstances. For instance, a building that has been designated as a Mission-Critical End Building (CEBN) may call for the installation of two, physically diverse uplink cables to different ITN buildings. Buildings with unusually large user populations may also need additional OSP fiber, even if they remain uplinked to a single ITN building.

To assist with the design process, four types of *non-standard EBNs* are defined:
(1) Key, *mission-critical EBNs*; are EBNs that cannot tolerate the extended failures associated with a cable cut, or even the shorter outages that occur from equipment failures. This applies only to those EBNs with critical, time-sensitive missions. *Mission-critical EBNs* are candidates for including dual, physically diverse cable connections in the outside cable plant design. Any discussion of the need for a physically diverse path to any EBN should be based on a documented mission need statement for the building as well as a complete assessment of supporting factors such as availability of alternate facilities, backup power, and perimeter security. In most cases, this complete analysis

will demonstrate that the physically diverse path will not add sufficient capability to warrant the additional expense.

(2) Other, *Important-EBNs*; include those EBNs to which the loss of connectivity may otherwise endanger life or property, and could significantly impact the base's ability to support mission requirements. EBNs with assured service transport requirements will likely fit into this category. Dual homed connections to one or more ITNs may be needed to meet the higher availability and reliability requirements, but a physically diverse cable path is not typically necessary.

(3) *Very large EBNs*; include those for which a single equipment failure might isolate hundreds of users and, perhaps, result in CITS system availability objectives not being met. Again, dual homed connections to one or more ITNs may be needed, but a physically diverse cable path is not typically necessary.

(4) *Medical EBNs*; include any facility that is dedicated to medical support functions and some mixed-use facilities with significant medical support operations.

Note also that dual homing has two different implementations. In its broadest interpretation, dual homing includes installation of separate fiber cables, each of which is routed to a different ITN. Less costly configurations are also possible, depending on what level of service the design is trying to achieve. For example, separate fiber pairs in the same OSP cable sheath can be terminated on different network modules within the same ITN, to achieve improvements in equipment availability. Another option is the use of separate fiber pairs in the same OSP cable sheath, each of which is connected to a different ITN by patching one of those pairs through an inter-ITN trunk to another ITN (again, to lessen the impact of equipment failures on overall system availability).

These concepts and definitions are illustrated and summarized in Figure 3 (ITS Backbone Topology Overview). This diagram provides an example of a typical partially meshed OSP topology. Please note that additional connectivity enhancements can be achieved with the network design.

Finally, the *medical enclave*, comprises dedicated and mixed-use facilities with at least 25 percent medical personnel and/or more than 40 computers or servers for medical support. These facilities are usually the hospital, clinic, and any other buildings (pharmacy, dental clinic, medical laboratories, medial warehouses, etc.) that are covered by the Law of Armed Conflict (LoAC) and subject to those laws and restrictions. The medical enclave meets multiple mission requirements for the medical community. Medical buildings will be physically and/or logically homed to the *main medical enclave* (MME) (usually the hospital) at which the majority of medical servers are located and/or from which communications to the external (off-base) medical community are established. Current law requires that communications among facilities in the medical enclave be segregated from other base communications. The critical nature of the medical enclave requires that its communications be robust and reliable. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) adds a requirement to ensure medical security and privacy when transporting medical information. At the same time, LoAC prohibits medical facilities from supporting command-and-control and other mission traffic. Most or all of these objectives can be satisfied as illustrated in Figure 3.

Connections among medical facilities can be provided via dedicated point-to-point cables, via separate fibers in existing cables, by transport over the ITS backbone via dedicated VLANs or in conjunction with a VPN, and (not illustrated) via dedicated time-division multiplexed channels (e.g., SONET tributaries on the ITS backbone). The MME can be dual-homed via physically separate cables to redundant networking components within a single ITN. LoAC has been interpreted as prohibiting connections from the MME to multiple ITNs, since the MME can, in principle, be used as an alternate path for non-medical traffic.

2.2 Alternative Backbone Transport Media

Because of the cost associated with installing new fiber optic cable, there are some circumstances where alternative transport media should be considered. These locations include, but are not limited to backup and/or secondary cable routes that are added for reliability purposes and excessively long or difficult cable routes. Figure 3, which defines the relationships between ITNs and various EBNs serviced by the ITS architecture, also addresses the possible application of alternative backbone transport media. The technical alternatives that may be considered on a case-by-case basis include:

- Point-to-Point and Point-to-Multi-Point radio systems and
- Line-of-Sight optical systems

Depending on the installation location, trunk encryption devices may be required. A cost benefit trade-off between the options may be required to help select the "Best Value" option.

2.3 Classified Transport

In the past, classified transport in the base environment employed point-to-point link encryption. Point-to-point link encryption is wasteful of fiber bandwidth and the point-to-point link is subject to complete failure if a fiber is broken.

Network layer encryption operates at the IP layer, which has been designated as the convergence layer for net-centric operations. The convergence of encrypted classified data with unclassified data makes more efficient use of fiber bandwidth and provides higher availability than a dedicated point-to-point link. With the High Assurance Internet Protocol Interoperability Specification (HAIPIS), there is a shift from link-layer encryption to network-layer encryption. Convergence of encrypted classified transport (at multiple levels) with unclassified transport on a common black core on a base network is analogous with the planned implementation of the GIG for wide area transport.

The ideal, of course, would be the use of multilevel secure user devices with end-to-end encryption and authenticated, per session encryption keys. Since such devices are not yet available at reasonable cost, the current baseline architecture prescribes encryption with Inline Network Encryption (INE) devices with transport over the base (ITS) network for connections between classified enclaves and the SIPRNET Service Delivery Point (SDP).

2.4 Interfaces to Other Local and External Networks

Finally, the architecture is influenced by local/external networks and communications systems with which ITS must interconnect. These include interfaces to:

- A variety of existing unclassified and classified data networks,
- The Network Management and Network Defense (NM/ND),
- NIPRNET (via NM/ND),
- SIPRNET,
- Voice switching system, and
- Various legacy video, sensor and imagery systems.

2.5 ITS Design Constraints for VoIP

In order to support VoIP systems over CITS, the ITS Layer 3 network transport architecture and protocols may need to be designed to support an even higher level of availability and reliability equal to that being achieved today by circuit-switched networks that carry voice traffic. CITS ITS Architecture Design should follow the guidelines contained in the DISA document titled: Appendix 3, **Generic Switching Center Requirements (GSCR)**. Based on an interpretation of basic telephony requirements from other sources, this document addresses the associated reliability and availability requirements for a Layer 3 transport network that is designed to handle VoIP and/or Assured Service LAN (ASLAN) systems.

As examples of the higher availability/reliability requirements that are mandated:

- Partial outages effecting more than 64 phones are limited to less than 3.0 minutes/year; thereby affecting the number of EBN uplinks required.
- Disruption of stable, active calls due to hardware failures affecting trunk circuits are limited to values which will affect the capacity of ITN Backup Power.

Based on these requirements, an ITS Backbone design that will support C2 Voice Grade user systems over an ASLAN will require a higher degree of network redundancy and UPS power may be included for any LAN equipment or LAN segment supporting more than 64 users. It further requires use of network CoS/QoS protocols and effectively limits bandwidth occupancy (number of IP phones) over ITS Backbone network segments.

The high availability and maintenance of calls (with no more than 2 seconds down-time due to equipment or link failures) is often achieved by use of highly redundant, dual collapsed backbone architecture for connecting ITNs to the SDP/DCO. In addition, any LAN access switches supporting more than 64 users will require dual logical connections to the ITS backbone distribution switches. This may impact the number of fibers needed in the backbone OSP cable design. All network equipment requires UPS power that can provide 2 or 8-hour backup power depending on whether ordinary C2 or Special C2 users are located on that segment.

An example of a dual collapsed backbone hardware configuration is shown in Figure 4. In this figure, each EBN with more than 64 IP phones may require a second logical connection to another ITN to meet the availability requirements. The backbone trunk fiber count may also need to be re-sized to support the dual connections for <u>all</u> buildings that will either now or in the future service more than 64 IP phone users.

(NOTE: This also includes Core 4 buildings that will need to be dual connected to the backbone network if their size warrants.)

The ITS backbone network should be designed to meet basic CITS reliability / availability requirements first. Buildings that require immediate IP phone service may necessitate that the design be augmented to meet the additional requirements in GSCR Appendix 3. Buildings for which IP phone service will not be required any sooner than two years need not meet the additional network requirements such as dual connectivity and UPS. However, the OSP cable system should be capable of supporting the ASLAN architecture in the future.

3 ITS BASELINE ARCHITECTURE

3.1 ITS Topology Considerations

3.1.1 ITS Fiber Optic Cable Plant

Single-mode optical fiber cables comprise the great majority of backbone and local subscriber links in the ITS. Single-mode fiber is the only medium considered to possess the high bandwidth-distance performance characteristics required to satisfy both immediate and future requirements for data transport within and across the base environment. Multimode fibers may be retained in the design when cables are reused and considered as a supplement to single-mode fibers on new ITN-EBN subscriber links (when technically feasible and cost-effective). For new cable installations, the baseline architecture for the ITS calls for:

- 36 single-mode fibers per link between ITNs and
- 12 single-mode fibers per link from an ITN to an EBN.

These fiber counts were selected as a compromise between the objective integration of services and the need for a transitional period during which various legacy systems must be supported, and as a compromise between cost and reliability/availability considerations for spare fibers. Sufficient fibers are provided on the backbone links to support any reasonable parallel configuration of SONET and frame-switched networks.

Where determined to be cost-effective, hybrid cables can accommodate a combination of SONET and frame transport mechanisms on EBN links, as well as other, legacy transport applications.

Note:
Those bases that have either a current or planned requirement for VoIP systems and need an ASLAN capable backbone may need to investigate backbone cable requirements more carefully. While this Architecture Document does not attempt to define a specific solution, it is recognized that the additional availability, reliability, and recovery requirements may necessitate additional design features.

3.1.2 Physical Network Cable Topology

The physical cable topology chosen for the ITS is a partially meshed backbone with (mostly) single subscriber links from the backbone to the EBNs (see Figure 3). The rationale for the meshed backbone is the high availability objective specified in the CITS ORD, and the requirement for redundant transmission links between each ITN and the remainder of the backbone. That is, multiple physically independent links (a minimum of two) provide alternate paths that are capable of accommodating link failures or regions of traffic congestion within the backbone network.

While it might appear that two links would suffice everywhere (i.e., a topological ring network), a meshed cable designed according to established traffic engineering principles more effectively utilizes the capacity of both transmission and switching subsystems, while affording an extra degree of redundancy for enhanced availability.

Where the installation of multiple optical fiber links (even two) is prohibitively expensive, alternatives to optical fiber cables, such as point-to-point radio or optical systems, must be considered. Such links may be economically and technically feasible. If necessary, these alternative links may have lower capacities than the primary link. In exceptional cases, connecting an ITN without physical diversity will be permitted only with explicit MAJCOM and AFNIC coordination and approval.

Redundant subscriber links are desirable from the point of view of survivability and availability. However, it is considered economically infeasible to implement two or more links from every EBN located on a "typical" Air Force base, where the number of EBNs may exceed 100. Thus it is expected that most EBNs will be singly connected to one of the ITNs on the backbone network. Certain mission critical buildings, or buildings with large user populations (that do not already host an ITN), should be considered candidates for dual homing to multiple ITNs. On small bases with only a few ITNs, it may be necessary to dual home one or more of the larger EBNs to meet ORD requirements for availability. Again, these are local design issues.

3.1.3 Logical Network Topologies

Logical network topologies for the frame-switched backbone networks are overlaid on the partially meshed, physical cable topology. The frame-switched network may follow the physical configuration, with appropriate Layer 2 and Layer 3 routing protocols acting to prevent routing loops. However, all traffic on the network must have access to diversely routed paths between ITNs.

Other logical network topologies for the frame-switched network can also be overlaid on the partially meshed physical cable configuration of the backbone network. As illustrated in Figure 4, a popular implementation of Gigabit Ethernet networks uses a dual switch, redundant collapsed-backbone network with a second layer of distribution switches or switch-routers. The distribution switches are dual-homed with an uplink to each of the collapsed-backbone switches. EBNs are connected, in turn, to the distribution switches. The implementation of this logical configuration, when overlaid on the partially meshed physical network, may require use of multiple pairs of fibers in a common cable,.

ITS network designs involving a Gigabit Ethernet only solution, must still provide for alternate routing over physically diverse paths between ITN switches. Because CITS cannot afford a full mesh OSP cable topology, secondary links may need to be implemented with routed connections and or patched fiber paths traversing intermediate ITN buildings.

3.1.4 Gigabit Ethernet ITS Architecture

As part of the CITS program, most bases are choosing to implement a stand-alone Gigabit Ethernet (GigE) as their primary backbone transport service, with no circuit transport switches or multiplexers. These bases typically identify few or no requirements for circuit-mode transport beyond standard telephone service, they see no need for implementing and maintaining a complex SONET infrastructure, and they may, in fact, have already initiated efforts to place some circuit services onto the GigE network. A notional GigE-only ITS is illustrated in Figure 5 [CITS SV-2(e) Gigabit Ethernet-Based ITS Architecture], which shows all frame-mode data traffic carried via a fully routed GigE backbone over a partial mesh topology. As discussed previously, a dual collapsed backbone architecture is also an alternative GigE backbone solution. Telephone services are provided via a centralized circuit switch (with some VoIP services riding the GigE backbone). In addition, a very small number of point-to-point connections are implemented via the use of fiber or copper cable for DS1 connections (such as encrypted data streams or VTC services).

In the past, the CITS Program Office and AFNIC (Formerly AFCA) have maintained that GigE-based circuit transport services do not yet satisfy the requirements defined in the CITS ORD. In particular, it was not clear that networks using frame-based transport could provide either real-time service guarantees or meet the stringent delay characteristics required for many circuit-mode services. This is particularly a concern should the frame network be stressed by severe traffic overloads (e.g., by denial-of-service attacks). Hence, on most bases, a GigE-only backbone is not considered to be a satisfactory approach for the ITS. However, it may be considered on a case-by-case basis, with a request by the Base/MAJCOM and appropriate approval from the program office and/or AFNIC.

In addition, USAF is currently trying to standardize techniques for convergence of services, particularly voice services, over a frame-switched IP network. This action is in response to efforts at a number of AF bases to install Voice-over-IP (VoIP) systems. These systems have, to some extent, relied on vendor-proprietary solutions and may not be interoperable with similar systems from other vendors. Consequently, Air Staff placed a hold on additional VoIP installations[1]. The desired approach is one in which the converged services will be based on interoperable standards and equipment.

Convergence of services on the (IP) frame-switched network is currently thought to be the future of communications. The technology is maturing rapidly. Consequently, any frame-based network architecture must include a number of features required for future implementation of IP-converged services. Specifically, CITS networks must support some level of end-to-end "Quality-of-Service" (QoS) for IP traffic[2]. This means that all frame switches used in a specific CITS network implementation must support IP and/or

[1] MEMORANDUM FOR ALL MAJCOMS: Air Force Policy on Voice over Internet Protocol, Lt. Gen. John L. Woodward, USAF/SCM, 22 June 2001

[2] "Quality of Service," or QoS as used in this text refers to the capability of a network to differentiate between traffic or service types and to preferentially treat one or more classes of traffic differently.

Ethernet Quality-of-Service mechanisms, and interwork properly. It also means that all transport components must work together in a seamless manner that allows end-to-end IP traffic to be prioritized according to service or administrative requirements and transported or rejected/dropped according to assigned priorities and traffic levels.

Note that the general QoS requirements in the CITS ORD encompass frame-mode services. Integration of mission-critical classified services over the backbone network requires support for precedence and priority handling of such services. Similarly, future implementations of VoIP, streaming-mode video over IP, and other non-classified, non-critical services will work well only if the infrastructure provides suitable QoS mechanisms. Therefore, all frame-mode switches, routers, switch-routers, etc., used on the CITS backbone and within the EBNs must support some level (TBD) of QoS and interwork appropriately with other QoS devices/mechanisms across the ITS.

The QoS requirements typically extend from user-to-user across an individual base's ITS for those devices or applications that are capable of requesting QoS support from the network. However, most users or applications do not yet request QoS services from the network, but many still require (static) priority handling by the network. For those, the QoS requirement can be considered to extend across the ITS from network ingress to network egress. NMS switch administration, end user port configurations for precedence marking/remarking, frame acceptance/dropping, queuing strategies, etc. are some typical examples of managed QoS requirements. Managed QoS configurations can be based on port IDs, MAC addresses, IP addresses, IP or TCP ports, and a number of other networking parameters.

Where a base has either a current or planned requirement for VoIP systems, it may be necessary to reassess the backbone cable plant design to insure that there are adequate fiber counts to meet the requirements for availability, redundancy and recovery; as well as the spares.

3.2 EBN Configurations

3.2.1 CITS Installation of EBN Equipment

With the widespread deployment of GigE network solutions, it is generally recognized that the term EBN Equipment applies to all edge devices where users are connected to the ITS network. As such, EBN Equipment is routinely found in both EBN and ITN buildings. Furthermore, the concept of keeping user attachment off the backbone hardware has resulted in a concept where EBN hardware is located anywhere horizontal user cables terminate within a building. Switch hardware used to attach users to the network is generally referred to as being part of the network access layer.

Relative to equipment and network configurations in EBNs, the CITS program will provide suitable Access Layer hardware (switches) and interface them to the backbone network at the most appropriate location. The long-term objective is to provide users in

all buildings with full access to a rich variety of services that have been converged onto a common transport mechanism (IP over GigE) across the ITS backbone.

3.2.2 EBNs with Multiple Equipment Locations

Larger buildings frequently have more than one location at which networking and/or transport equipment is located. For non-critical EBNs, CITS has, in the past, connected a single downlink from the serving ITN to one of these equipment/wire closets, and then connected from that location to other closets in the building. Mission-critical buildings (CEBNs) may be dual-homed to more than one ITN, as noted earlier.

This approach leaves large buildings subject to a single-point-of failure; should equipment in the entry closet fail or become congested, the entire building can lose connectivity to the backbone network.

For larger buildings with multiple equipment locations, the ITS architecture will allow the use of multiple downlinks (typically two) from the serving ITN. Each downlink will be routed through the optical patch panel at the building's entry point; however, separate connections will be made from the entry point to one or more additional equipment locations within the building. This configuration will enhance the overall reliability of larger EBNs, with little additional cost.

3.3 Interfaces to the CITS Network Management / Network defense (NM/ND) Systems

The CITS NM/ND architecture continues to evolve independently of the ITS architecture. Information Assurance and Network Operations systems may be distributed among main operating bases, ESUs, I-NOSCs and other AFNETOPS organizations and MAJCOM locations. Specifically, the IA Firewalls may be located at either the local base and/or at the MAJCOM location. Regardless of the location or operating agency, In either case, IA systems provide the interface point for all network traffic leaving the local ITS.

Enterprise-wide Network Operations systems are being deployed at CITS locations. Systems such as Network Management Systems, Trouble Ticket Systems, SYSLOG, Authentication and Domain Name Service systems are all part of the NM/ND architecture. Historically the ITS Architecture has not included any of these systems, but rather has relied on direct integration with the Network Management systems provided by NM/ND. Where possible, ITS requirements for configuration management, diagnostics and troubleshooting were expected to be satisfied through integration with the existing NM/ND product.

Beginning with FY04 projects, ITS Integration Contractors were permitted to install Element Managers and other Network Management Systems that were required to configure and control the ITS system on a separate host platform. This approach is being reconsidered, because the NM/ND portion of CITS still has the lead responsibility for

addressing enterprise architectural changes necessary to meet evolving changes such as firewall consolidation, NOSC-centric remote management, enhanced troubleshooting, and improved performance monitoring. Configuration Control of all NM/ND systems at the base and MAJCOM is maintained by the CITS Configuration Control Board (CCB).

3.4 Classified Data Transport

The ITS system is intended (per the CITS ORD) to provide integrated transport for all networking and communications services on an Air Force base. This includes transport of encrypted classified and unclassified information in support of mission and support systems. Providing transport for critical, mission systems on the ITS implies that the ITS is, itself, a mission-critical system.

Optimal system design involves integration of the inter-building transport network with the internal distribution network within a building (a.k.a. *the first 400 feet*). For classified data transport, this level of integration is difficult to achieve within the scope of the CITS program for the following reasons:

(1) CITS is currently tasked with and funded to provide only the transport network down to the work-group switch (e.g. communications closet). Except in extraordinary circumstances, the intra-building distribution network(first 400 feet) and end user devices within the end buildings are not provided by the CITS program;

(2) Costs are prohibitive and suitable technologies not yet available for providing high-throughput Type 1 encryption devices at every end instrument;

(3) The CITS program does not control either the system architectures nor the (sub)network implementations for most classified systems (e.g., GCCS).

Nonetheless, this level of integration is a long-term and necessary objective of the CITS program. It provides a basis for defining an objective architecture for transporting and protecting classified data across a local CITS network, for interworking with the DISN and other components of the world-wide Global Grid network, and for transporting information securely across the combined global network.

Consistent with the overall Global Grid architecture, the objective security architecture for the ITS employs the High Assurance IP Encryption (HAIPE) family of equipment otherwise known as Inline Network Encryptors (INE). These network layer encryption devices are being developed for the NSA, and include the TACLANE/E100. Until additional HAIPE devices become available TACLANE/E100 will be the primary devices for protection of IP traffic between classified enclaves on the typical base. The characteristics of the TACLANE/E100 are summarized in the following section and subsequently discussed in the context of the recommended architecture for classified services in CITS.

Although the basic architecture for classified data transport in the ITS relies on the use of Inline Network Encryptors, concepts for classified data transport within CITS must also include transitional mechanisms that:

- Facilitate interworking with existing classified systems,

- Replace specific components of those systems where technically and economically feasible, or
- Provide bandwidth or suitable transmission facilities for existing systems.

For most classified systems, CITS ITS shall provide a reasonable degree of service assurance to the classified users, particularly for the systems that support mission critical applications.

The following sections describe the capabilities of the INE family of encryptors, outline the objective architecture for classified data transport in the CITS program, identify techniques for accommodating existing classified systems, and discuss approaches to transitioning such systems to the objective architecture.

3.4.1 Inline Network Encryptors (INE)

As noted above, the CITS architecture for classified data transport focuses on the use of IP encryption devices developed for the GIG. HAIPIS is the High Assurance Internet Protocol Interoperability Specification. It is a document that defines basic interoperability for HAIPE devices in these modes:

- HAIPE Device to HAIPE Device
- HAIPE Device to KMI & EKMS
- HAIPE Device to Security Management
- HAIPE Device to Network Infrastructure

HAIPIS specifies retaining the original TACLANE (KG-175) hardware architecture.

The TACLANE "Classic" model operates at 10Mbps, while the TACLANE E-100 supports 100Mbps Fast Ethernet. A version that supports Gigabit Ethernet is expected in the future.

3.4.2 Objective Architecture for Classified Data Transport

A simplified example of the ITS classified architecture is illustrated in Figure 5 and discussed below. Note that the figure is based on a GE Ethernet only architecture in which only IP level encryption techniques are used.

(1) Classified enclaves with Ethernet and Fast Ethernet connections to the ITS backbone are connected to their respective edge devices in the ITN using TACLANE encryptors. When the GE version of TACLANE becomes available, it will enable implementation of protected GE links to EBNs and classified servers.

(2) Standalone, classified servers or workstations may also use TACLANE encryptors:

- TACLANE encryptors (Ethernet, Fast Ethernet, or, in the future, GE) are used where servers, workstations, or other standalone computers attach to the ITS backbone via Ethernet connections.

3.4.3 Service Assurance to Classified Mission-Critical Systems

Mission-critical, classified systems require additional mechanisms to ensure that communications are available when needed. Such systems frequently use dedicated cables or optical fiber pairs to interconnect secure enclaves on base and to connect those

enclaves to long-haul networks or transmission nodes. Communications security is usually provided by using serial mode KGs on the copper or fiber lines. The use of dedicated transmission facilities isolates the mission systems from the effects of traffic overloads on the unclassified networks, from external attacks against the unclassified networks, from disruptive maintenance actions, from power failures, and from a number of other events that could cause loss of communications. If mission-critical systems are to be integrated on the ITS backbone, then the backbone design must offer at least the same level of service and system availability as a dedicated system.

The ITS backbone allows for the functional duplication of dedicated mission-critical networks through the use of IP Quality-of-Service (QoS) features. Previous sections outlined techniques for overlaying classified networks on the ITS backbone using Inline Network Encryptors. Classified, mission-critical enclaves can also be interconnected over the ITS by defining virtual private networks and by assigning appropriate QoS contracts to those virtual networks. IP encryption can be used over these virtual networks. Note that mission-critical, virtual networks established in this manner should not be affected by traffic overloads or failures on non-critical networks that ride on the same ITS infrastructure. Note also that the alternate routing capabilities of the IP backbones allow for automatic rerouting when a link or node fails in the network; thus an added feature is automatic (and rapid) restoral of many failures.

The transport of mission-critical data over the ITS backbone requires a number of additional technical, configuration, and management actions. ITNs must be connected to reliable power systems, with adequate backup capabilities, that at least equal the capabilities of the power systems used by the mission-critical systems themselves. Hardware and software configurations for the components of the ITS must be controlled rigorously. Management and control subsystems must be adequately secured to ensure that only authorized network management personnel can access them. Policies must be re-examined and/or modified accordingly to allow for integrated modes of transport.

3.5 Integration of Voice Services

As discussed in previous sections, voice services in the baseline architecture will generally continue to be supported by the existing telephone End Office switches, PABXs, RSUs, etc., and will operate primarily over the existing twisted pair copper cable plant. New components of the telephony system may be connected to the existing system over the CITS installed fiber optic cable plant using primarily SONET (multiple DS-1 trunk interfaces).

Voice-over-IP (VoIP) is becoming increasingly important as the commercial solution for convergence of voice services onto the frame-transport network. Since essentially all buildings on an Air Force base will be equipped with Ethernet switches that are connected to the backbone network, it is desirable to be able to add VoIP services to a building that requires expansion of voice services. To allow a VoIP solution to be connected to DSN, however, all CITS Ethernet switches, routers, and other network components must be able to meet the developing C2 Voice Grade LAN requirements for VoIP telephony. These requirements are primarily concerned with achieving the same

availability and information assurance as the currently deployed circuit switched telephony system provides. In addition, the VoIP solution that rides over the C2 Voice Grade LAN must be JITC certified as meeting interoperability requirements with legacy equipment and providing all Military Unique Features (MUF) such as Multiple Level Precedence and Preemption (MLPP).

A VoIP solution, which is not certified, can only be connected to the public telephony network and every C2 or mission essential element on base must also have an additional connection to the JITC certified circuit switched network for telephone service.

As noted earlier, additional work is required to define specific requirements of the LAN to carry VoIP services. At this time, it is known that the IP network will be required to provide CoS/QoS features, which will insure that voice traffic takes precedence over all other types of network traffic.

3.6 Network STIG Compliance

All ITS deployed hardware shall be required to be capable of meeting current DISA STIG requirements for Network Data Security. Maintaining STIG compliance is ultimately an operational configuration challenge, so the ITS PMO will work closely with base and MAJCOM personnel on each ITS project to understand how systems need to be initially configured.

3.7 IPv6 Capability

The Secretary of the Air Force has recently directed that as of October 2003, all networking equipment ordered for installation anywhere within the Air Force must be capable of supporting IPv6 network protocols. The technical details on how this directive will be implemented by CITS are provided in the ITS BPD, which is updated annually.

Appendix A

FACILITY IDENTIFICATION AND PRIORITIZATION PROCESS

First, all existing and planned facilities are examined for current and projected requirements to access the CITS. Other parameters, determined during the ensuing implementation process, will determine the viability and feasibility of the facility meeting CITS requirements. At this point, every facility having an information transport requirement is equal in status. The next step is facility prioritization. This is critical to ensure that buildings are given adequate service during the development of the ITS. This includes taking into account the best interest of the base population as a whole. Guidance used in this decision-making process centers around the core war-fighting mission of the base. Core facilities are those identified by the base-level planner and Wing Commander (or authorized designee) as an integral part of the Wing war-fighting mission. This process attempts to further resolve the core facilities into distinct mission priority categories, based on the core role of each facility relative to the base mission. This includes Command and Control (C2) and C4I parameters, resulting in a realistic, phased, implementation approach that aligns with the core mission of the given base. Final discretion on prioritization lies with the Wing Commander or other designated base personnel, and the following guidance is for initial C4I planning purposes only. A definition of what discriminates core from non-core roles, in general terms, is as follows:

Core Facilities (defined as Mission and Direct Mission Support)
Core facilities include the primary functional users in the main industrial area of the base. Examples of primary mission-critical functions include: Wing HQ, Wing Operations Center/Command Post, air traffic control and other operational areas, logistics, supply warehouse(s), civil engineering, personnel, base education, contracting, legal office, accounting and finance, medical/dental clinics, security police, transportation, major communications facilities (BCC, DCO, etc.), and users of downward-directed programs affecting the base (C2IPS, WCCS, DMS-AF, CE-LAN, CTAPS, CAMS, CAS-B, CMOS, etc.). Core facilities also include buildings with existing departmental and/or functional LANs, as well as major tenant organizations (e.g., active duty or AFRES flying units, MAJCOM/Joint Command Headquarters facilities, etc.).

Non-Core Facilities (defined as Indirect Mission Support)
Non-Core facilities include potential user facilities in the industrial area of the base that do not currently have departmental LANs or data connectivity requirements but may house future mission-critical functions. All other indirect mission support user buildings, not fitting the Core description above, are considered non-core (e.g., remote buildings outside the industrial area, base gymnasiums, post offices, BX, commissary, chapels, dorms, dining halls, golf course, MWR support facilities, hobby shops, theater, library, family center, O-Club, NCO-Club, day care centers, schools, military clothing, Class Six, bowling

center, florist, family housing, credit union, kennel, gun range, swimming pool, visiting quarters, shoppette, etc.). To re-iterate, base-level C4I planners should develop an initial proposed ITS target facility list. This encompasses every facility having a defined or projected information transport requirement. After generation of this list, prioritize the targeted facilities using the process shown in Figure A1-1. Tables A1- 1 through A1-4 provide an in-depth method of quantifying target facilities.

Mission Category I Facility Identification

This category constitutes the highest priority Core facilities, covering the major decision-makers directly involved in the core war-fighting mission. This includes the Wing or Air Logistics Center (ALC) Headquarters and Staff, Wing Operations Center, Group or ALC Directorate Headquarters, Wing/Squadron Operations, Wing/Squadron Intelligence, and Air Traffic Control. This category also includes Major tenant organization[1] headquarters and intelligence facilities. This category also includes the major communications service locations to include the Base Dial Central Office (DCO)/Remote Switching Terminals (RSTs), Base Network Control Center (BNCC), WAN Service Delivery Point (SDP), and Data Processing Centers. Also included are all facilities housing any C2 System host or server and all facilities housing at least 10 Command and Control (C2) Systems users. Completion of the following table will quantify the target Mission Priority I facilities:

Table A1-1. Mission Category I Facility Selection

MISSION FUNCTIONALITY	TARGET FUNCTIONS	TARGET FACILITIES
Wing/ALC Headquarters/Staff	CC, CV	
Wing Operations Centers	Wing Ops Center (WOC) Squadron Operations Command Post(s)	
Group Headquarters	OG/CC, LG/CC, SG/CC, MG/CC, CEG/CC	
ALC Directorate Headquarters	LA, LC, LH, LI, LK, LM, LP, QL, TI	
Wing Operations Group Squadron HQs[2]	FS, BS, MS, OSS, RS, ARS, AACS, ACS Other OG Squadrons	
Wing Intelligence Facilities	Wing Intel, Squadron Intel	
Air Traffic Control Facilities	Control Tower, RAPCON, Base Weather	
Major Tenant[1] Headquarters/Intelligence Facilities	Tenant Command, Wing, Group HQs Tenant Intel	
Primary Communications/ Data Processing Facilities	DCO/RSTs, WAN SDP, BNCC, DMC, DPC ITNs[3]	
Major Command and Control (C2) Server Locations (DB Server, Apps Server)	GCCS, WCCS, C2IPS, TBMCS Hosts/Servers	
Major Command and Control (C2) Locations (> = 10 C2 Users)	GCCS, WCCS, C2IPS, TBMCS Users	

1 Major tenants are defined as all units that do not fall under the host Wing or ALC organizational hierarchy but are critical to the warfighting mission of the base, Air Force, or DoD (i.e., Unified Commands, other Air Force units, or other DoD organizations).

2 Operations Group Acronyms - FS (Fighter Squadron), BS (Bomber Squadron), MS (Missile Squadron), OSS (Operations Support Squadron), RS (Rescue Squadron), ARS (Air Refueling Squadron), AACS (Airborne Air Control Squadron), ACS (Air Control Squadron)

3 The list of ITNs will be determined in Step 3 of this total process. All selected ITNs will then be added to this Mission Category 1 listing, if not already identified by other mission functionality.

Mission Category II Facility Identification

This category constitutes the next higher priority Core facilities, including all non-Operations Squadron Headquarters. Another focus is on major C4I system user facilities, that are not already covered under Mission Category I quantification. Systems involved include those covered under the C4I for the Warrior (C4IFTW)

concept. Specifically, this involves Command and Control (GCCS, WCCS, C2IPS, TBM Core Systems, etc.), processing (GCSS, BLSM, IMDS, etc.), and messaging (DMS) systems. This category also targets any facility housing more than 5 C2 Systems users or more than 10 C4I Systems users. This includes processing or messaging (DMS) users, existing PC LANs of a Core mission function, or other Automated Information System (AIS) users) not already covered under Category I. Also targeted are facilities housing GCSS servers, major DMS components (CAW, MTA, etc.) or AIS hosts not part of the GCSS such as CHCS, CAMS, CMOS, BCAS and others.

Table A1-2. Mission Category II Facility Selection

MISSION FUNCTIONALITY	TARGET FUNCTIONS	TARGET FACILITIES
Logistics Group Squadron HQs[4]	MSS, LSS, SUPS, TRANS, CONS Other LG Squadrons	
Support Group Squadron HQs[5]	CS, MSS, SPS, Other SG Squadrons	
Medical Group Squadron HQs[6]	DS, MOS, MSS Other MG Squadrons	
Civil Engineering Group Squadron HQs[7]	CES	
ALC Division Headquarters	LA, LC, LH, LI, LK, LM, LP, QL, TI	
Major Tenant Squadron HQs[6]	Tenant Squadron HQs	
Command and Control (C2) Locations (> = 5 C2 Users)	GCCS, WCCS, C2IPS, TBMCS Users	
C4I Systems Host/Server Locations	GCSS Servers DMS Components AIS Hosts	
C4I Systems User Locations (> = 10 C4I Systems Users)	Processing (GCSS, IMDS) Messaging (DMS) PC LANs, AIS Users	

4 **Logistics Group Acronyms** - MSS (Maintenance Support Squadron), LSS (Logistics Support Squadron), SUPS (Supply Squadron), TRANS (Transportation Squadron), CONS (Contracting Squadron)
5 **Support Group Acronyms** - CS (Communications Squadron), MSS (Mission Support Squadron), SPS (Security Police Squadron)
6 **Medical Group Acronyms** - MOS (Medical Operations Squadron), MSS (Medical Support Squadron), DS (Dental Squadron)
7 **Civil Engineering Group Acronyms** - CES (Civil Engineering Squadron)
8 Major tenants are defined as all units which do not fall under the host Wing or ALC organizational hierarchy but are critical to the warfighting mission of the base, Air Force, or DoD (i.e., Unified Commands, other Air Force units, or other DoD organizations).

Mission Category III Facility Identification
This category constitutes the remainder of the Core direct mission support function facilities not already covered under Mission Categories I or II. The grouping includes the remaining low device count C2 Systems (< 5 users) or C4I Systems (<10 users) user facilities. This Category also covers contingency/deployment support facilities[9] that have a likelihood of requiring connectivity to the base network during wartime or exercise contingencies.

Table A1-3. Mission Category III Facility Selection

MISSION FUNCTIONALITY	TARGET FUNCTIONS	TARGET FACILITIES
Wing/ALC Mission Support	BC, CR, DP, EM, FM, HO, IG, JA, MO, PA, PK, QS, SE	
Command and Control (C2) Locations (< 5 C2 Users)	GCCS, WCCS, C2IPS, TBMCS	
C4I Systems User Locations (< 10 C4I Systems Users)	Processing (GCSS, IMDS) Messaging (DMS) PC LANs, AIS Users	
Contingency Support Facilities[1]	Wartime/Crisis Information Transport	

9 Contingency Support facilities are those facilities which support crisis and wartime deployment information transport requirements

Non-Core Facility Identification
This category constitutes "Non-Core" mission facilities that also require access to the overall ITS. Included in this category are locations and functions such as DoDDS schools, the Base Theater, Chapels, Exchange, Commissary, MWR facilities, Gymnasiums, Post Offices, Library, Child Care Centers, Officer's/NCO/Airmen's Clubs, restaurants, and other indirect mission support locations.

Table A1-4. Non-Core Facility Selection

MISSION FUNCTIONALITY	TARGET FUNCTIONS	TARGET FACILITIES
Schools	DoDDS Schools Network Facilities	
Misc. Stations		
MWR Facilities	Clubs, Gymnasiums, Craft Center, Restaurants	
Community Support	Chapels, Rec Center, BX, Commissary, Library	
Youth Activities	Care Centers, Youth Center	
Other Base Support	Shoppettes, Malls, Class Six	

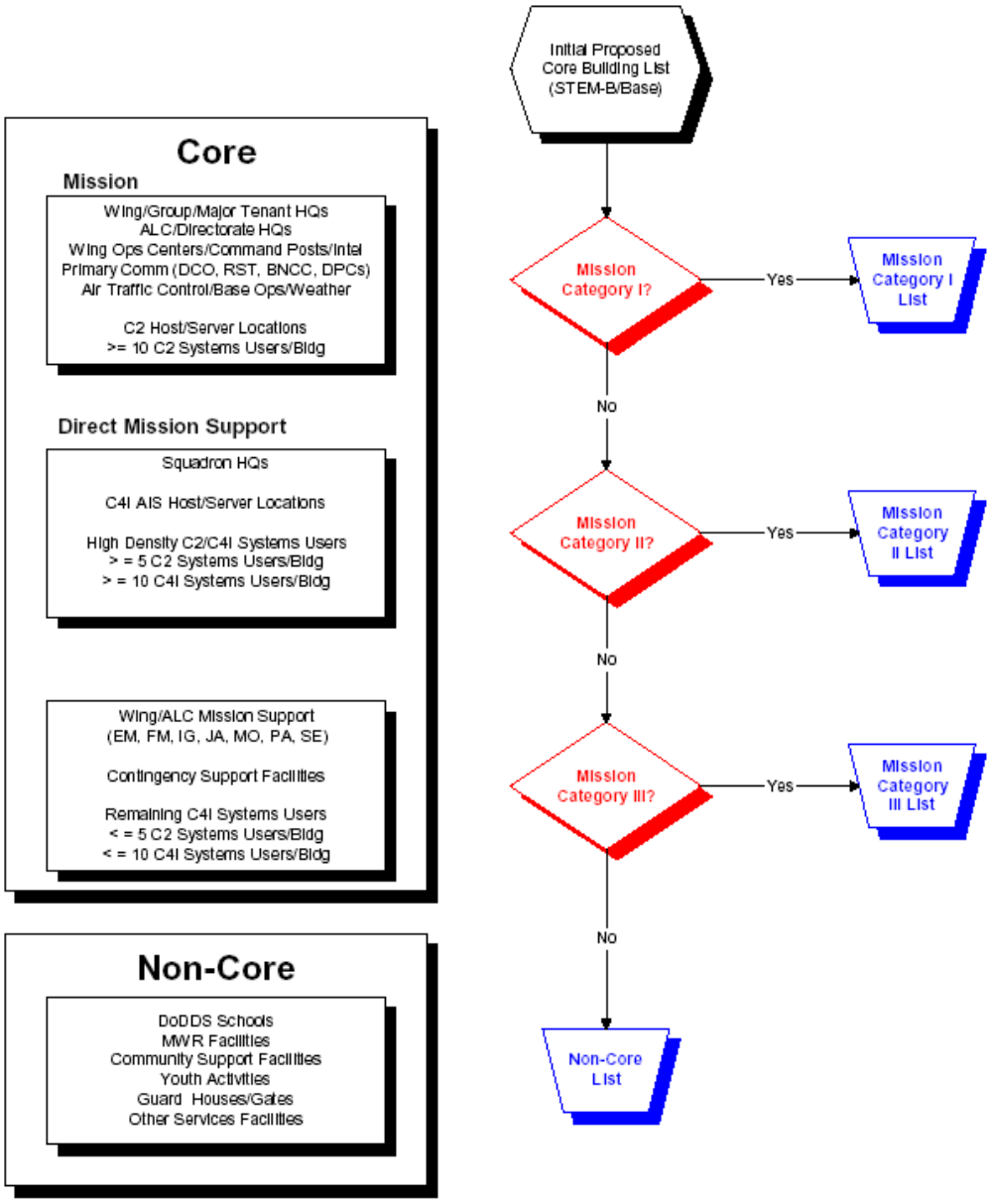

Figure A1-1. Facility Prioritization Process

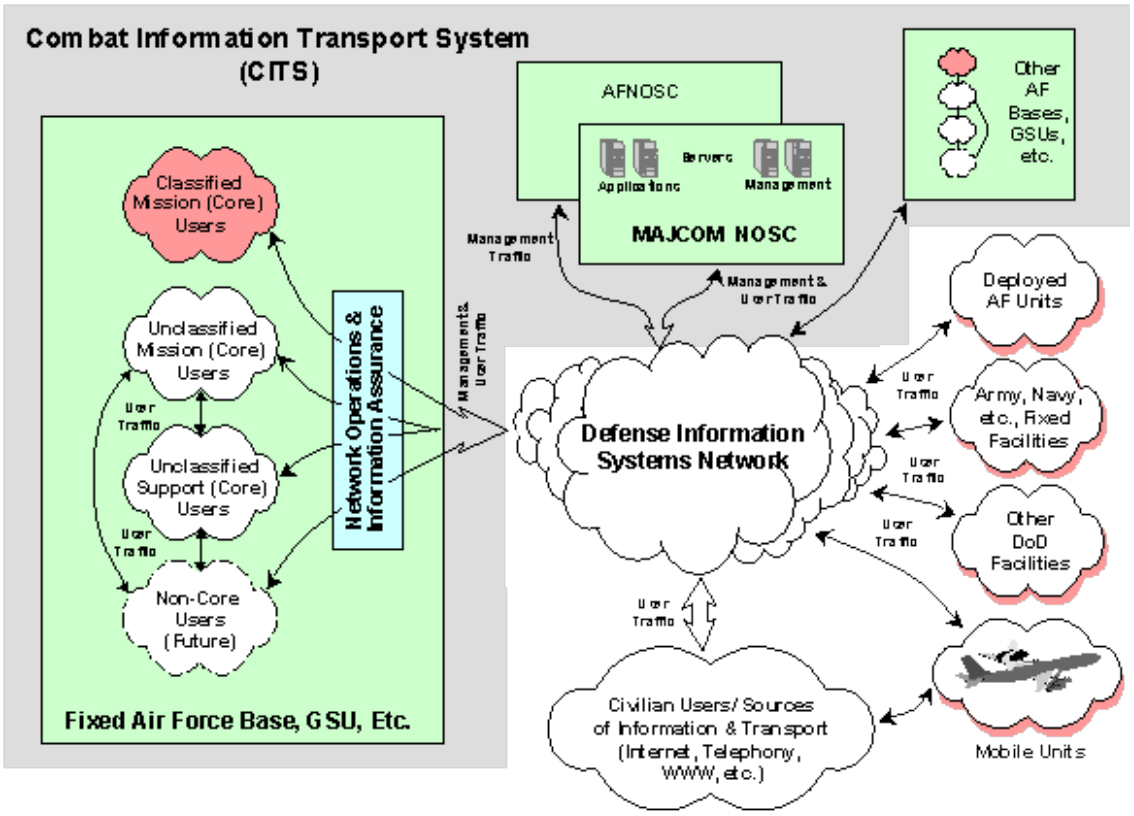

Figure 1: CITS OV-1 High Level Operational Architecture

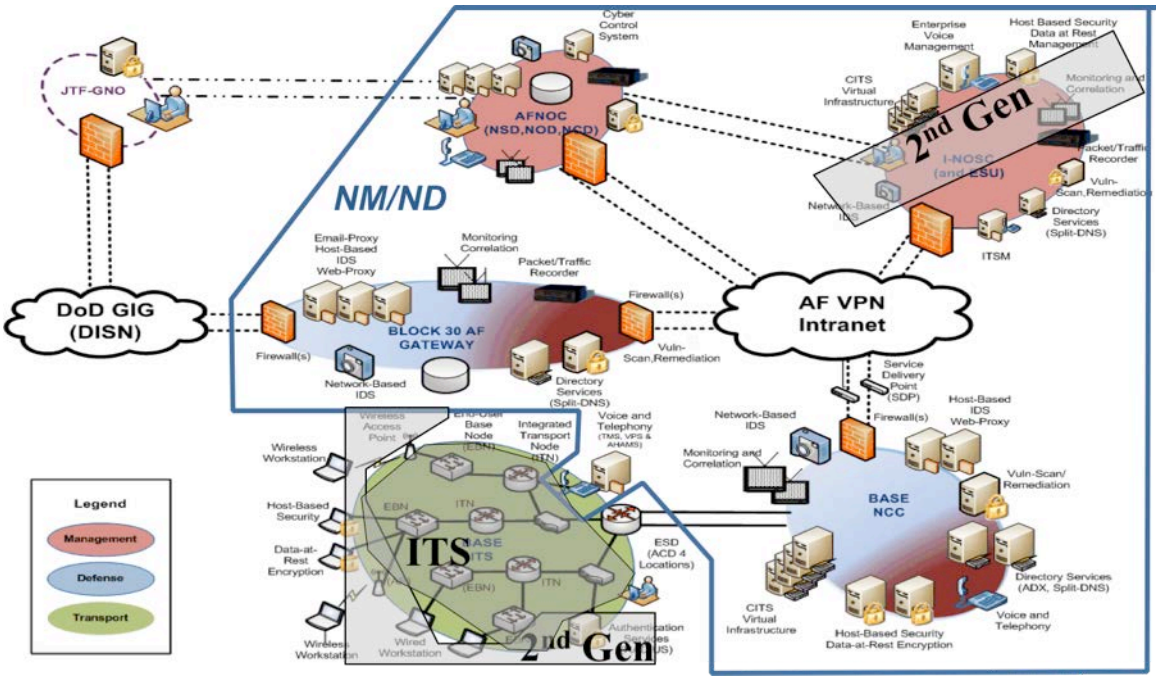

Figure 2: CITS SV-1 Inter-system Interface Diagram

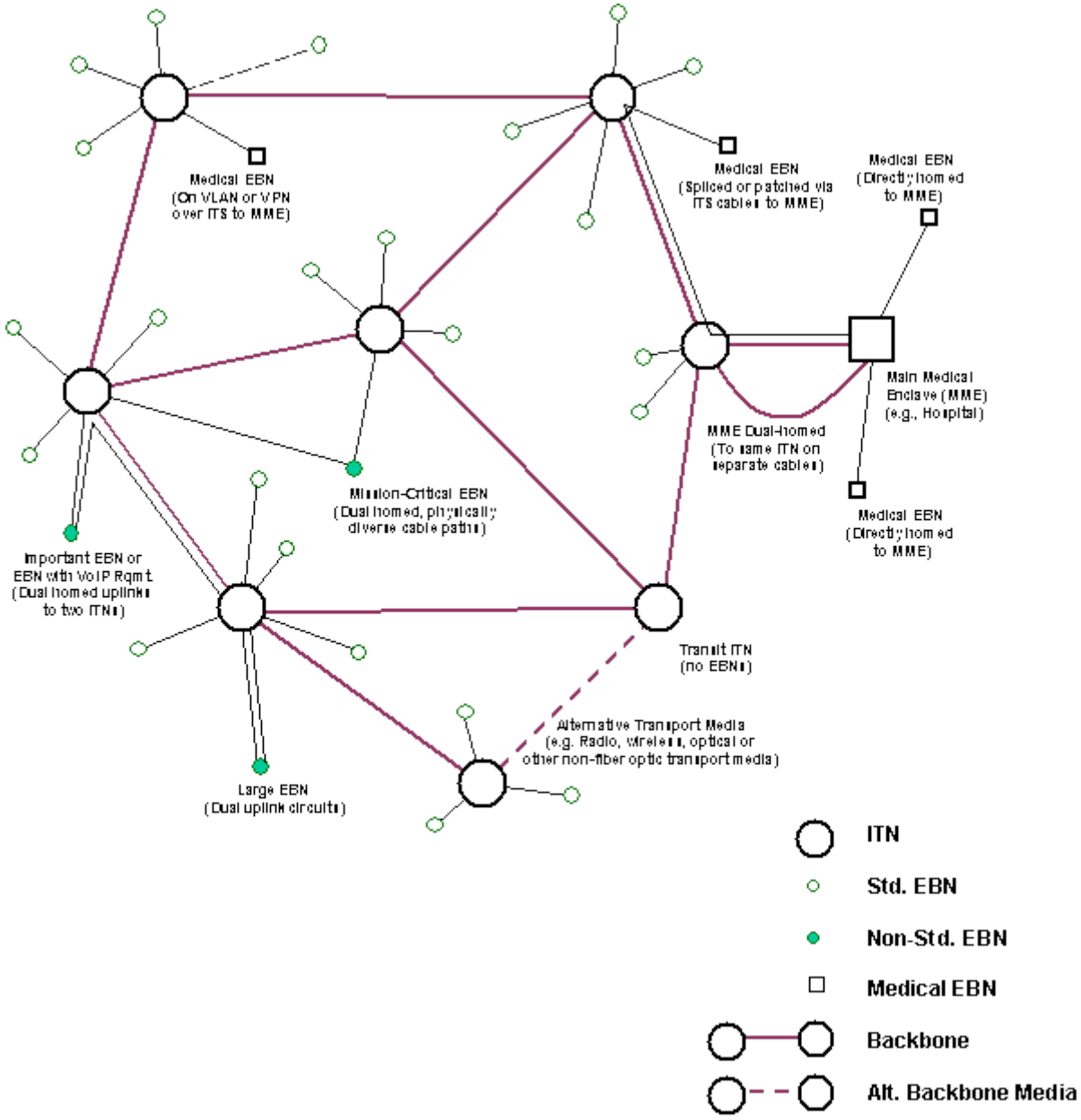

Figure 3: ITS Backbone Topology Overview

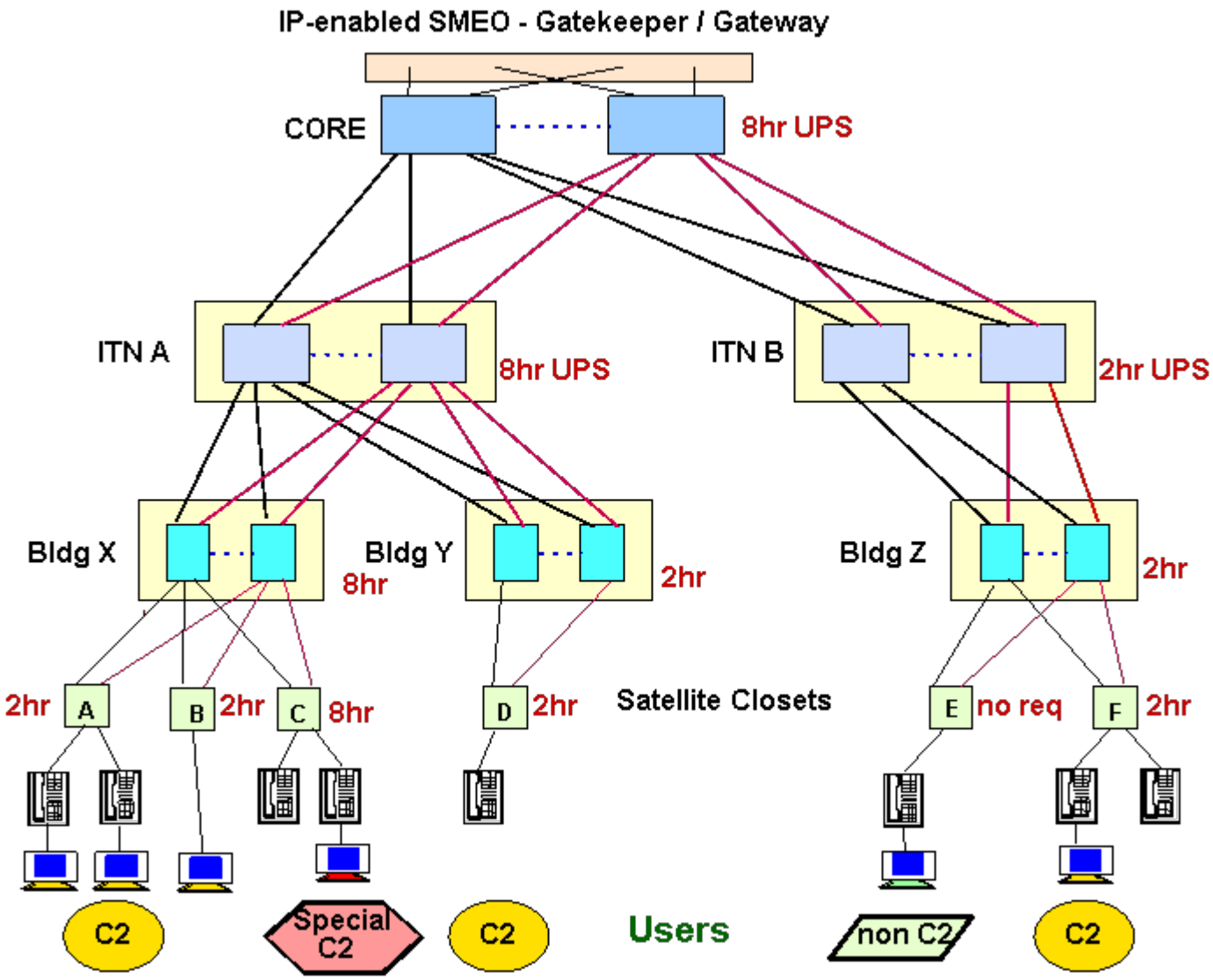

Figure 4: Example Logical Configuration for Dual-Collapsed Backbone Gigabit Ethernet Network (Incl. Dual Homed EBNs with VoIP / High Avail Rqmts)

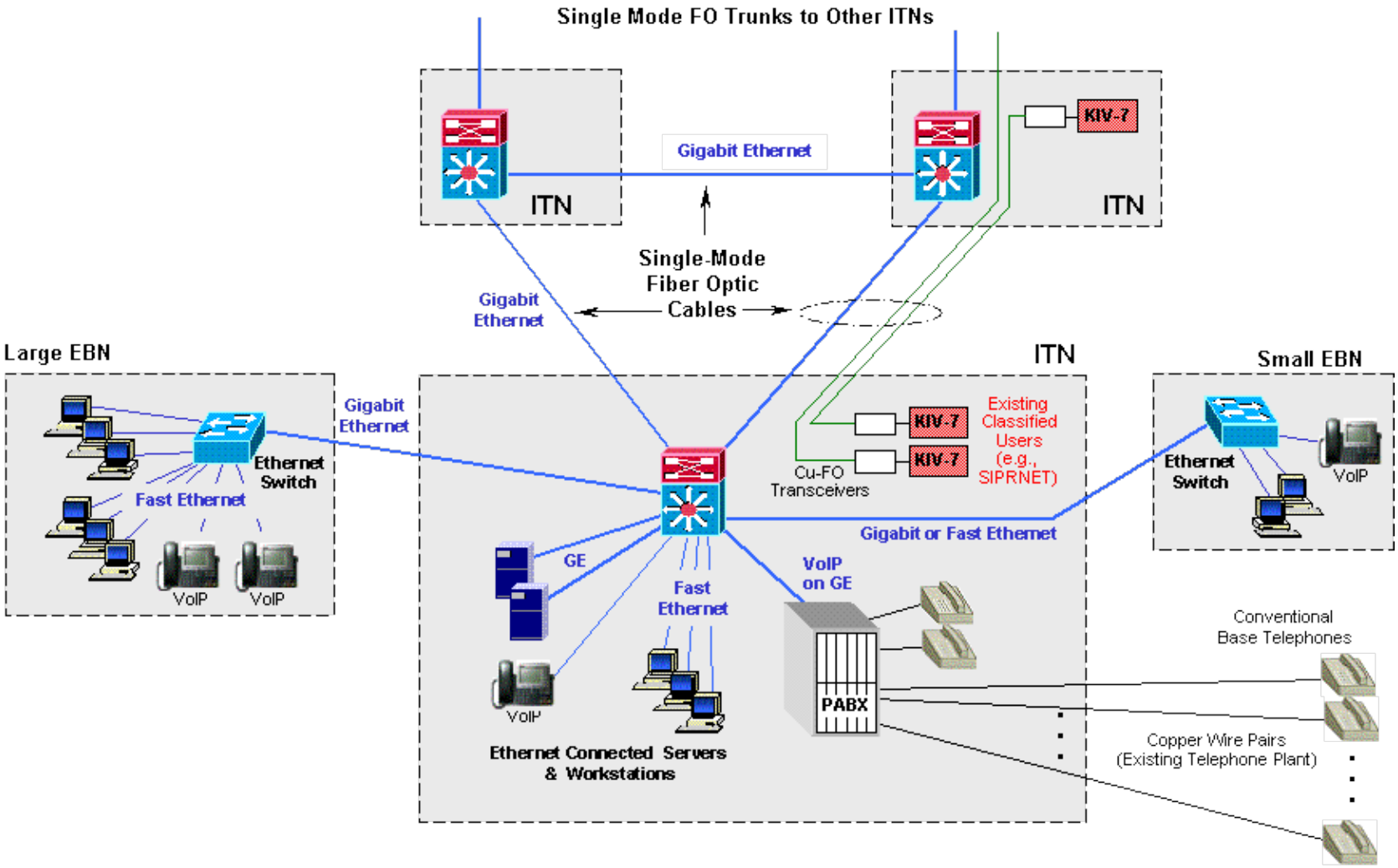

Figure 5. CITS SV-2(e) Gigabit Ethernet-Based ITS Architecture