

# Volume I, Appendix C - Table of Contents

<b>C. Campus Area Network Design Template.....</b>	<b>C-1</b>
C.1 Purpose.....	C-1
C.2 Drivers.....	C-2
C.3 Elements/Features/Specifications.....	C-3
C.3.1 Topology.....	C-3
C.3.2 Physical Overlay.....	C-6
C.3.3 Switches, Routers, and Hubs .....	C-8
C.3.4 Transmission Overlay.....	C-10
C.3.5 ATM Technology Overlay.....	C-11
C.3.6 IP Overlay.....	C-14
C.3.7 Switching and Routing Overlay.....	C-17
C.3.8 Voice Overlay.....	C-18
C.4 Functional and Performance Specifications .....	C-19
C.4.1 Security.....	C-19
C.4.2 Functionality.....	C-20
C.4.3 Interoperability .....	C-21
C.4.4 Performance.....	C-21
C.4.5 Cost.....	C-23
C.5 Evaluating CAN Products and Services .....	C-23

This page intentionally left blank.

## C.Campus Area Network Design Template

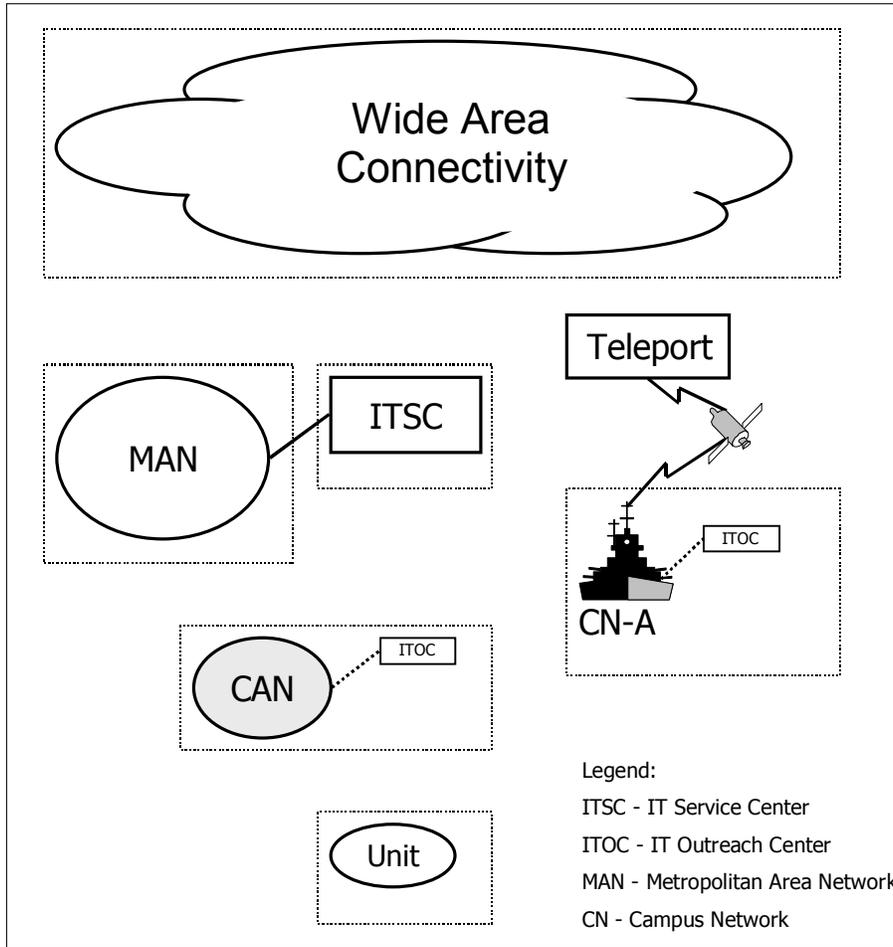


Figure C-1. High Level Components of the TI Architecture

### C.1 Purpose

Figure C-1 depicts the relationship of the campus area network (CAN) to the other components of the ITI architecture. Navy and Marine Corps campuses vary widely in their network connectivity requirements but they must all function together effectively within the DON enterprise network.

The purpose of this CAN template is to establish a set of general guidelines within which a campus network may be built. The template provides a consistent means to address campus network components, identifies appropriate instances for specific ITI solutions, and details a list of implementation considerations. The guidance is presented in a manner that allows considerable variance to address local needs, to support a best value solution, and to align campuses within the context of a DON enterprise infrastructure solution.

*The architecture guidance for shipboard ITI is included in the CAN template. The majority of the campus architecture guidance is common to both terrestrial and shipboard environments. In the absence of shipboard-specific guidance to the contrary, the general campus guidance should be*

*implemented for shipboard networks. When there are shipboard unique architecture requirements, they will be noted in blue italics.*

## C.2 Drivers

The campus contains the tactical and support units that perform the Navy and Marine Corps mission. Performance of the mission is directly affected by the quality of the information provided to the units operating on the campuses. The drivers that determine quality are as follows:

- **Interconnectivity.** A robust IT infrastructure is rooted in the interconnectivity of the networks and systems that comprise the DON enterprise information system. It is a fundamental element of the RMA. Global connectivity through the WANs, MANs, and CANs must be supported by a well-defined and supported ITI architecture.
- **Interoperability.** Implementation of campus area networks must provide for interoperability among units within campuses, among campuses, between regions, and with external organizations. *Shipboard networks must provide for interoperability among units within ships, between ships, and with external organizations.*
- **Seamlessness.** Infrastructure systems at the campuses must be able to identify and communicate with systems across the DON enterprise infrastructure, without the need for special human intervention, on other campuses *or shipboard networks*, in regions, and outside the DON enterprise.
- **Integrated, Supportable Solution.** The campus architecture must support integration at both the campus *or shipboard network* and MAN/region levels. Integration of voice, video, and data is required to reduce infrastructure duplication and support cost. The integration of network services across the MAN must reduce duplication of functions and enable supported organizational units to focus on their primary missions. Regional supportability – especially the ability to remotely manage devices at the ITSC – is an important component.
- **Affordability.** The campus networks and services must be realigned to leverage resources, eliminate redundancy, and consolidate underused or common functions to enable the same or better network services at reduced cost.
- **Availability.** *Unlike many of the functions supported by CAN or MAN networks, shipboard networks support tactical functions that are critical to personnel safety and mission success. Shipboard networks will require higher levels of redundancy and a more robust design philosophy than their shore-based counterparts.*
- **Latency.** *Shipboard networks will have to support real-time applications with latency requirements in the millisecond range.*
- **Mobility.** *Shipboard networks move from homeport to sea to foreign ports and require connectivity into the global ITI under each of these circumstances.*
- **Bandwidth disadvantages.** *Shipboard networks will never have the unlimited “uplink” bandwidth potential that is available to shore-based campus networks.*

## C.3 Elements/Features/Specifications

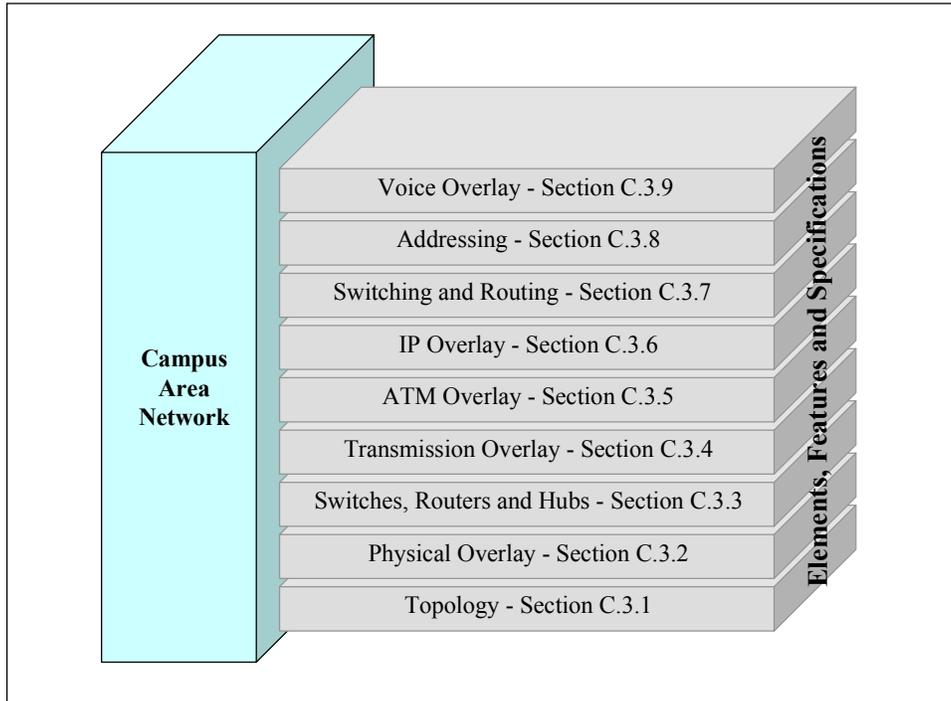


Figure C-1. Layered Description of the Campus Area Network

The complexity of a campus area network is illustrated by the elements depicted in Figure C-1. These layers roughly correspond to the Open System Interconnect (OSI) protocol stack. Each of these is discussed in the nine sub-sections that follow, including a description of important features, recommended implementations, and required specifications.

### C.3.1 Topology

The elements of the CAN are depicted in a notional drawing shown in Figure C-1. To summarize, the campus is connected to other campuses through an ATM Private Network-Network Interface (PNNI) service or Permanent Virtual Path (PVP) mesh, normally OC-3 or higher, as provided by the MAN. The campus premise switch is the demarcation point for the campus network infrastructure.

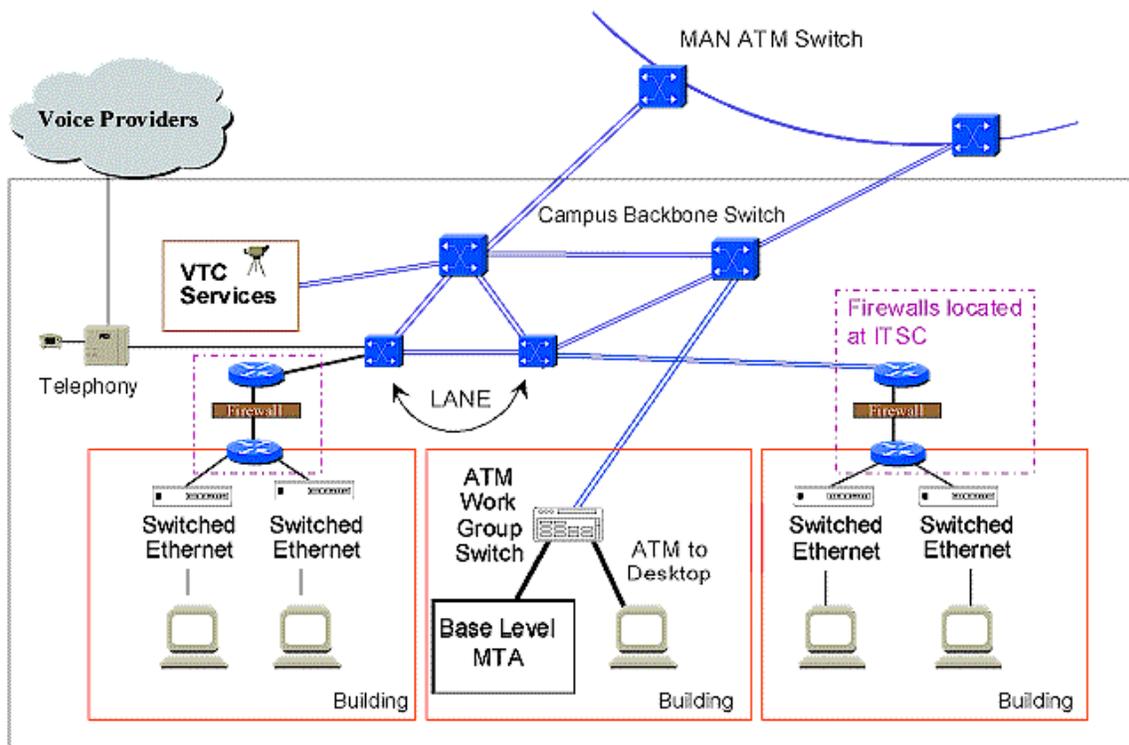


Figure C-1. Notional Campus Area Network

Within the campus, the information architecture supports a multi-media infrastructure through a heterogeneous ATM/IP technology solution. The voice infrastructure will eventually be integrated into the multi-media infrastructure using ATM technology. The CAN provides interconnectivity to a node at each of the buildings on the campus. The topology of the multi-media infrastructure is dependent upon the physical layout of the campus, traffic demand patterns, the degree of required survivability, and other location-specific considerations. Basic guidance is provided to address these expected implementation differences.

The multimedia transport topology at a particular campus is defined in the campus blueprint and should be consistent with the general design and implementation guidance provided in this template.

*The elements of shipboard networks are depicted in Figure C-2. To summarize, the shipboard network is connected to shore-based or other shipboard networks via satellite or through a pier-side cable connection. An ADNS router is the demarcation point for the shipboard network infrastructure.*

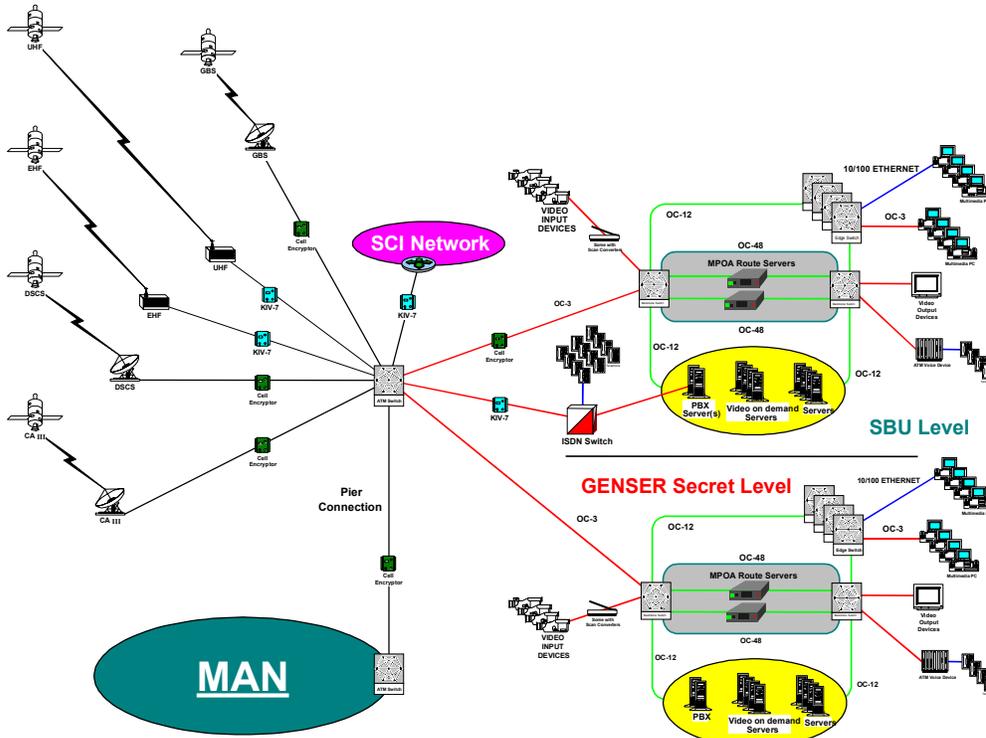


Figure C-2. Notional Shipboard Network

*Shipboard networks provide interconnectivity to sensors, processors, weapons systems, and user workstations throughout the ship. The multimedia transport topology at a particular shipboard network is defined in the shipboard network blueprint and should be consistent with the general design and implementation guidance provided in this template.*

### C.3.1.1 Discussion of Alternatives

Three common methods can be used to connect networks.

- Ring: Fiber Data Distribution Interface (FDDI) is a common example of a ring topology. FDDI is a high performance fiber optic token ring technology in which the “token” is passed from one node to another until it reaches the desired node. Other network technologies such as SONET can be configured as a ring in which each circuit is given a provisioned time slot.
- Star: A star network connects each device to a center location by a point-to-point link. The center device is usually called a hub or concentrator in which the center point may be passive, active, or intelligent. This topology can be extended by connecting one star to another. Networks based on ATM and switched Ethernet are traditionally configured as stars.
- Mesh: In a mesh network, each component is directly connected to several other devices in the network. A full mesh indicates that each device is connected to all others while a partial mesh indicates that not all links are in place.

*There are two logical alternatives to the recommended shipboard network architecture:*

- *Multiple “stovepipe” networks interconnected via routers. This architecture, which currently exists on a number of ships, does not support the desired levels of interoperability.*
- *A single multi-level security (MLS) network instead of the separate Genser Secret and SBU networks. This architecture is preferable but is not practically realizable today with existing security components.*

### **C.3.1.2 Recommended Topology Implementation**

Campus networks are typically built with a backbone that can have its capacity increased without affecting end users (by swapping out hubs and switches). Backbones may consist (initially) of 10Base-T Ethernet, 100Base-T Ethernet (fast Ethernet), 1000Base-T Ethernet (gigabit Ethernet), FDDI rings, or ATM meshes. The border of the network -- the interface a user sees -- is most commonly 10Base-T Ethernet. For those users with higher capacity requirements, the backbone network can be extended to them.

*Shipboard backbones can have their capacity increased by swapping out edge devices and switches. Backbones should consist exclusively of fiber ATM mesh networks. The border of the network may consist of copper 10Base-T, fiber 10Base-FL, copper or fiber Fast Ethernet, or fiber OC-3 ATM. Gigabit Ethernet and 25 Mbps ATM should be avoided for shipboard network users.*

The network topology implementation should support future growth and accommodate future networking technology. Cost of both fiber optic and copper media are very small compared to the labor cost of installation. Therefore, it is almost always economical to put extra fibers in between-building runs (known as ‘dark fiber’) and extra Category 5 copper runs within buildings that can be brought into the network later. Campus backbones (the runs between buildings) should normally have alternate routes (dual rings or mesh topologies) so that the effect of single points of failure can be contained.

*To maintain the flexibility to support future growth and accommodate future networking technology, sufficient fiber optic media must be installed in ships in as adaptable a configuration as possible. To achieve this objective, the physical topology of the fiber optic cable plant between core nodes will, in general, be a partial mesh topology with dual-homed connections to the edge devices.*

Each core node will be connected to at least two other core nodes via separate, physically diverse paths to enhance survivability of the backbone transport system. This topology allows implementation of physical and logical ring, point-to-point, hub, or mesh topologies which can be used in an ATM or combined ATM and SONET transport environment.

### **C.3.2 Physical Overlay**

Cable and cable equipment must meet current and future requirements for data transmission, electrical characteristics, and topology. Fortunately, manufacturers have boosted data transfer rates on copper twisted-pair wire so that it can meet some bandwidth demands to the desktop. *Copper cable should not be used for the backbone of shipboard networks.* The advantages of fiber cable, however, are many and include support of many times higher transmission rates and far greater security because they produce no emissions and are not affected by radiation.

### **C.3.2.1 Discussion of Alternatives**

This discussion of alternatives includes both metal wire and fiber-optic cable. They are addressed in the context of new installation/replacement media and retention of existing media.

#### **C.3.2.1.1 New installation/Replacement**

To maintain flexibility, support future growth, and accommodate future networking technology, sufficient fiber optic media should be installed on the campus in an adaptable, standards-based configuration. The exact number and type of fibers to be installed on the campus backbone should be based on careful analysis of current and future growth. A rich mixture of 62.5-micron multi-mode and 8 micron single mode fiber is recommended.

Although fiber is the preferred medium for outside plant (between buildings), it may be permissible to install new copper in certain situations such as within a building or long runs of low-bandwidth signals (such as remote guard shacks). Category 5 (at least) Unshielded Twisted Pair (UTP) is the recommended copper media. (Category 5 cable is suitable for POTS telephone use as well as LANs. But Category 3 telephone cable is unsuitable for LAN use. In the interests of a single cable plant, Category 5 is recommended for both applications).

*For shipboard low-end workstations that do not need the multimedia capability provided by fiber interfaces, standard Screened Twisted Pair (SCTP) Category 5 is the recommended copper media.*

Coaxial cable should not be installed on the campus for inside or outside plant connectivity unless there are special circumstances that dictate its use. *Coaxial cable should not be installed for shipboard networks.*

#### **C.3.2.1.2 Retention of Existing Media**

Although fiber is the preferred medium, metallic (copper) transmission media should be retained or reused where the evaluation of performance, mission priority, security, and cost dictate. Asymmetric Digital Subscriber Line (ADSL) is a technology that may be effectively and economically used to salvage existing telephone wiring in a campus environment. ADSL can provide point-to-point capability with capacities in the range of T1.

### **C.3.2.2 Recommended Physical Implementation**

The notional CAN in Figure C-1 shows two ATM top level switches for connection to the MAN and, ideally, this concept would be repeated for connection of these top level switches to all building switch/routers.

Fiber links should be used to connect floors of buildings to the locations of the interface points to the ATM switches. *Fiber links should be used for all shipboard backbone networks.*

The exact number and type of fibers to be installed on backbone routes between network nodes, devices, and buildings will be based on engineering analysis of current and future growth requirements. In most cases, the cost of installation far exceeds the media cost, so overbuilding is usually the right answer to the analysis.

The decision to use multi-mode or single-mode fiber to connect core switches should be based on current and near-term bandwidth needs and cost. For example, multi-mode fiber is cost-effective for OC-3 long distances, but single mode fiber is needed for all OC-12 and OC-48 connections. In all cases, single-mode fiber should be run between core switches and between buildings. In FDDI

(100Mbps capacity), multi-mode fiber reaches around 2 km between nodes, and single mode fiber will reach 20-30 km.

From the building switch/routers to the server and desktop sites, several alternatives can be used. For maximum reuse of existing cable plant and for least-cost network interface cards (NICs), standard unshielded twisted pair (UTP Category 5) copper cable can be used. *Again, SCTP has been determined to be clearly superior to UTP for both noise immunity and security and should replace UTP where appropriate.*

For very high-end servers such as multimedia servers or high-end workstations (bandwidth requirements in excess of 100 Mbps), fiber to the office or location can be used. The CAN implementation does not mandate exclusive use of fiber, but should evolve to fiber where it can be justified by cost benefit analysis.

Given future bandwidth needs, an initial investment in a robust set of multi-mode and single-mode fiber will be justified.

The EIA standards for Category 5 installations include documentation standards. Since overbuilds are recommended, documenting the dark fiber and unused UTP is important so that it can be located later for use. Therefore, a configuration management scheme that documents the as-built configuration is important.

### **C.3.3 Switches, Routers, and Hubs**

Switches, routers, and hubs are the major components of LANs, and their selection requires careful attention. Generally, campus implementers are wise to obtain specific components from a single vendor for interoperability and support reasons. Also, these components should have management agents embedded in them to support remote electronic monitoring by the Information Technology Service Center (ITSC).

#### **Switches**

FDDI and all variants of Ethernet are standardized on the IEEE Committee 802 model and use a common (802.2) logical link controller. In practice, this means that all these LAN technologies can be bridged together with appropriately-configured switching hubs.

Interoperability of switches is based on standards-based routing, and support for dynamic routing is accomplished through the PNNI protocol. Prior to selecting a vendor, have a thorough interoperability test that has been demonstrated on networks of similar size. The burden can, and should, be placed on the vendor. A suggested contracting option is to specify that a detailed test plan must be demonstrated before final award. Should the test plan be extensive, a preliminary award can be made to the potential vendor, but the final award should be held until the successful passing of the test plan.

The sizing of core and secondary switches should be based on current and near-term cost-effective technologies. For example, OC-12 is now a reasonably-priced interconnection link between core switches. While the current population/use may not fully justify a switch initially, expected growth should be accommodated by the design of the switch chassis.

#### **Routers**

Two classes of routers can be implemented in DON networks. Conventional routers provide network-layer route computation and packet forwarding in a single physical device. Virtual

routers are comprised of route servers that are used to perform route calculations and non-routing edge devices.

The two major classes of routing information protocols currently implemented in contemporary networks are distance vector (Bellman-Ford algorithm) and link state. The Open Shortest Path First (OSPF) link state routing protocol is the most predominant routing protocol on DON networks and is the recommended interior gateway protocol.

Routers with ATM interfaces will be needed for routing between the switched ATM backbone network and existing LANs. These routers should be capable of supporting a minimum of OSPF plus any locally-required routing information protocols (consistent with the ITSG). If virtual LANs (VLANs) are implemented, these routers must also be able to perform routing between multiple VLANs on various network segment types (such as Ethernet, Token Ring, and ATM). Future versions of edge switches may also support multi-protocol routing, which reduces the necessity of a physical router. The ATM router, when used as connection between the ATM CAN and the existing legacy LANs, should be capable of supporting the following features:

- LAN Emulation (LANE)
- Classic IP and Address Resolution Protocol (ARP) over ATM as defined in RFC 1577
- Multi-protocol encapsulation as defined in RFC 1483
- PVC and SVC connections
- ATM Forum UNI signaling (UNI 3.0/3.1, UNI 4.0)
- AAL3/4, AAL5
- Multi-protocol routing over ATM (MPOA) (routing of IPX, DECnet, and Appletalk are local options -- extra-campus routing is IP only).

For campuses that run ATM and are supported by a MAN that uses PNNI, the CAN template assumes that the ATM backbone switches on the campus also perform routing using PNNI.

## **Hubs**

Hubs fan the circuits out to the borders of the LAN. They also perform bridging between separate, disparate LAN technologies. Furthermore, if configured in accordance with DON ITI architecture recommendations, the hub can provide significant network monitoring data for centralized monitoring and management in the ITSC. The following guidance applies to hubs.

### **Protocols Supported**

- Ethernet. The vast majority of end systems (such as desktop computers) have 10Base-T (Ethernet) (IEEE 802.3) interfaces. Hubs should therefore have 10Base-T ports by default.
- Ethernet and Fast Ethernet. Hubs that can handle both 10Base-T and 100Base-T (fast Ethernet) are quite common. These hubs support two functions: attach a mix of 10Base-T and 100Base-T end systems to the hub and provide 10Base-T for the end systems and 100Base-T for the campus backbone. Hubs can also bridge the varieties of 802.3 Ethernet, FDDI, and token ring with the appropriate interfaces.

## **Types of Hubs**

- Shared media hubs are at the lower end of the price range and have the disadvantage that all end users receive all traffic on the LAN whether it is addressed to them or not. *Shared media hubs should not be used on ships.*
- Switching hubs have the identical external interfaces of shared media hubs. But switching hubs provide each end system with a bridging function that eliminates contention on the connection between the hub and end system—the hub sends traffic out one port that is only destined to the end system attached to that port. One means of controlling congestion is replacement of a shared media hub with a switching hub.

## **Network Monitoring**

Hubs that contain an SNMP agent are referred to as intelligent hubs. Once programmed, the SNMP agent interacts with the ITSC network operations center so that the network monitoring software at the ITSC can determine remotely what is and is not working and the levels of congestion at the network hub. (Additional information is contained in Appendix D under Performance Management).

The cost of the SNMP agent is a marginal increase over the cost of an unmanaged hub; hubs should be purchased with SNMP agents installed.

## **C.3.4 Transmission Overlay**

The SONET protocol has replaced much of the world's PDH equipment (Plesiochronous Digital Hierarchy). All future systems should support the SONET protocol, be it circuit emulation via ATM or SONET Add/Drop Multiplexers (ADMs). PDH circuits (DS-0, DS-1 and DS-3) can ride on this equipment.

### **C.3.4.1 Discussion of Alternatives**

DS-1 (formerly T-1) is basically a conditioned telephone line and is the most common digital leased-line service and provides 1.544 Mbits/sec. DS-3 (formerly T-3) is also common and provides 45 Mbps.

SONET defines a fiber-optic transmission that is standard for cell relay. Typical line speeds are OC-3 (155 Mbps) and OC-12 (622 Mbps). When appropriate, SONET provides a number of advantages:

- Higher capacity, scaleable bandwidth from OC-1 (51.84 Mbps) to OC-192 (9.6 Gbps)
- Improved Survivability - protection switching in less than 50 msec
- Bandwidth management allows a customer to obtain more, less, or redirected bandwidth as needed
- Rapid provisioning - ability to provision a service in minutes as opposed to days or weeks as is typical in the existing environment
- Improved operation, maintenance, and provisioning - voice channels for operators and data channels for network management
- Single channel visibility - frame interleaving enables single channel visibility via SONET ADMs. Depending on the equipment used, individual channels down to the DS-1 or DS-0 level may be added or dropped.

### **C.3.4.2 Recommended Transmission Implementation**

The preferred choice for transmission systems is an ATM switch fabric with optional SONET ADMs. The use of an ATM-only switch fabric has cost benefits and allows for dynamic circuit creation and interconnection to the WAN. The added expense of SONET is warranted for certain applications such as real-time data acquisition *and circuit-switched voice*.

When deploying ATM in the core backbone, equipment from a single vendor is desired because of the state of the protocol implementation (ATM protocols are still evolving and not all features are fully implemented by all vendors).

At campuses where SONET is implemented, SONET equipment from a single vendor should be installed to facilitate interoperability; simplify maintenance and circuit restoration actions; and allow operation, administration, and network management functions to be performed from a single integrated hardware/software platform.

### **C.3.5 ATM Technology Overlay**

ATM is a communications networking technology that supports many types of traffic, including voice, data, real-time video, and imaging. ATM is a cell relay technology, implying that the data packets have a fixed size. Same-size cells provide a way of predicting and guaranteeing bandwidth for applications that need it. The ATM fast VLSI cell switching fabric also provides a means to replace the time-consuming CPU-bound packet forwarding of traditional routers with switches that reduce traffic delays. Unlike Ethernet, FDDI, and token ring that used a shared media, ATM provides an any-to-any connection and allows any pair of communicating nodes to transmit simultaneously.

#### **C.3.5.1 Discussion of Alternatives**

The alternatives for the campus are ATM cell switching and IP packet routing coupled with switching hubs; however, no matter what technology is selected for the campus backbone, IP to the host must be supported. Both ATM switching and IP routing have distinct advantages and should be carefully evaluated in relation to the specific campus requirements. Because IP has such a tremendous legacy implementation, any acceptable ATM solution must fully support (and enhance) the IP environment. This section is focused on ATM and necessarily includes IP; additional IP discussion is provided in Section C.3.6. Other supporting architecture information for both IP and ATM is provided in Chapter 2 of this document. The ATM alternatives are addressed in the following context.

- ATM networking solution
- Support for IP (LANE, MPOA)
- Specific ATM Routing Performance
- Security of ATM

### **C.3.5.2 ATM Networking Solution**

There are two potential topologies for implementing ATM: (1) ATM switches in a partial mesh, and (2) ATM with a SONET ring using ADM. Both topologies may also implement VLANs.

An ATM switch is located at the primary node that is the campus ingress/egress for all multimedia transport. Secondary nodes and building nodes, typically implemented as IP routers, may be implemented as ATM switches for campuses hosting organizations requiring ATM access to the DON enterprise network.

Alternative topologies are appropriate in order to accommodate campus geographical features and existing outside cable plant infrastructure. To enhance survivability of the backbone transport system, each secondary node should be connected to at least two other secondary nodes via separate and physically diverse paths.

To support integrated services networks at most DON locations, the recommended implementation is a switched ATM backbone network configured in a mesh topology initially supporting OC-3 (155 Mbps) and later supporting OC-12 (622 Mbps) transmission rates. The core ATM mesh network is designed by connecting each backbone ATM switch to at least two or more other backbone ATM switches.

Connection of legacy LAN technologies (such as Ethernet and Token Ring) to the ATM backbone will be made using LAN switches referred to as ATM edge switches. Redundancy in the switched network base backbone is provided through multiple connections from the ATM edge switches and ATM workgroup switches to ATM base backbone switches. These connections should be capable of supporting 155 Mbps transmission rates. ATM switches should be capable of automatic (transparent-to-end systems) re-establishment of virtual circuits in the event of switch or link failure. This reconfiguration is automatic in routers and available in ATM switches – but the planner must ensure that the capability is received.

#### **C.3.5.2.1 ATM Addressing on the Campus**

In instances in which the campus has implemented an ATM network infrastructure, an addressing solution described in Chapter 4 (Section 4.4) is appropriate.

The MAN or region ITSC will obtain an ATM address block to support the participating campuses. Within a MAN/region hierarchy, each campus will be reflected (and announced to the MAN) by a single prefix and mask. Each campus will be allocated sufficient address space.

The ATM address form is based on Network Service Access Point (NSAP) addressing, which means that the end station address includes the host routing information. This includes support of the PNNI routing in which the MAN implements a PNNI routing hierarchy.

*For the fleet autonomous ATM net, the DISA Globally Unique Identifier (GUI) or home port geographic address space as offered for deployed forces does not meet DON requirements and will not be used. The Naval solution, under which each ship will have a single prefix and mask, will be developed and presented in a subsequent version of this architecture.*

#### **C.3.5.2.2 ATM Routing on the Campus**

When a MAN has implemented a PNNI routing hierarchy, the campus should participate as is appropriate.

Transporting IP packets by encapsulation into ATM cells provides significant potential for improved routing performance via LANE and MPOA, as discussed in the following section.

### **C.3.5.2.3 Support for IP (LANE, MPOA)**

The campus ATM solution must support interoperability between devices on ATM LANs and the traditional LANs (Ethernet, Token Ring, and FDDI). It must also support configurations connecting traditional LANs over an ATM backbone.

In the near term, LANE provides a solution for interoperability of LANs independently of any higher networking layer (such as IP, IPX, or DECnet) that uses the services of the LAN.

In the longer term, MPOA is the preferred solution and allows end devices which are attached to separate ATM networks to communicate directly with each other instead of through intervening routers, even when end devices are located on two different subnets (known as cut-through routing). MPOA substantially enhances performance by reducing routing delays. MPOA is defined by an ATM Forum protocol but is not yet fully implemented by vendors and must be implemented in a Switched Virtual Circuit (SVC) environment.

#### **C.3.5.2.3.1 LAN Emulation (LANE)**

ATM and IP attached LANs and accompanying end stations must both communicate over the ATM backbone. LANE provides the technology to enable this mixed environment to communicate. This is made possible by having the ATM network "emulate" the characteristics of broadcast LANs and was fully described in Chapter 2.

At the campus, it is possible to implement the LANE functions in an ATM switch, but this should be avoided for performance reasons. While it is possible to provide support for legacy networks (e.g., Ethernet) via LANE services in the core switches, most LANE should be implemented in the edge or intermediate switches.

(For clarity, core switches are dedicated switching systems without additional processing requirements. Edge switches are located at the logical "end" of an ATM network and are typically an ATM switch that supports legacy networks via LANE services or ATM end system workstation/hosts. Intermediate switches lie between the backbone and an edge switch.)

For smaller campus networks, an intermediate switch may not be necessary; the edge switch can connect directly to the core. The decision on when to deploy LANE devices depends on the particular ATM implementation and on how the individual ATM devices handle the LANE processes.

For campus networks which include many autonomous networks, the LAN Emulation Server/Broadcast and Unknown Server (LES/BUS) services should be implemented on the edge switch close to the organizations that connect to the various emulated LANs (e-LANs).

Every e-LAN functions independently using its own LES/BUS and interconnecting multiple emulated LANs which require a router. Instead of routing between multiple physical interfaces like a typical router, the router simply routes the Layer 3 protocols onto multiple Emulated LANs connected through the same interface. The router can be a card that is inserted into an ATM switch or it can be a stand-alone router.

#### **C.3.5.2.3.2 Multiprotocol over ATM (MPOA)**

MPOA splits the traditional role of the router into two roles by off-loading packet forwarding from the router to the hosts and edge devices. The ability to separate packet forwarding from other router functions allows a more flexible implementation of the two components. Enabling packet forwarding in a separate device from the router is known as cut-through routing, which uses the Next Hop Resolution Protocol (NHRP). NHRP defines the methods for routers to communicate among each other to determine unknown IP-to-ATM address mappings regardless of IP subnets of the end devices.

Edge devices and hosts discover the ATM address associated with an IP destination by sending NHRP queries to their router servers. The router servers communicate among themselves to learn addresses, and the edge devices can then establish a cut-through route to the destination.

Of LANE and MPOA, MPOA is the preferred solution, but only when planners and implementers are confident that adequate service provider support exists.

#### **C.3.5.2.4 Security of ATM**

The following mechanisms are required to secure the DON ATM overlay at the CAN level.

- Fastlane ATM encryption devices are required for connections between secret enclaves. These devices are installed between secret buildings and SBU CANs. (An entire ATM CAN is operated at the SBU system high level.) Enclaves operating at various classification levels can likewise make use of the DON ATM overlay by using key management to keep the classification levels separate. CoIs requiring complete information isolation between themselves and the rest of the DON ATM overlay can likewise be supported using Fastlanes.
- The ATM CAN must be constructed in a redundant fashion such that the failure of a single network component or interconnection will not lead to the catastrophic failure of the CAN. Redundancy of individual building connections to the CAN should be analyzed on a case-by-case basis by using the net subscriber value (NSV) process. See the DON ITSG Section 10.4.3.2.1 for NSV details.
- Bandwidth allocation management must be provided within the ATM overlay. This includes providing authorized administrators with the capability to identify the priority of data transport requests and allocating network bandwidth to the highest priority requests when contention occurs. In addition, the ATM overlay should be designed with the ability to “order and add” additional bandwidth as required by adding additional links to the ATM mesh.
- The ATM overlay must provide mechanisms to ensure that DON-controlled components of the overlay can only be managed by authorized administrators, that they are resistant to penetration attempts, and that they are resistant to ATM signaling-based denial of service (DoS) attacks. To reduce the potential for successful penetrations originating from inside the DON-controlled portions of the overlay, network components that are remotely managed must feature non-spoofable authentication mechanisms. It is expected that this management will be accomplished in-band across the IP overlay from a regional management center (e.g., an ITSC).

### **C.3.6 IP Overlay**

The campus network template assumes that every campus will support end-to-end IP connectivity to every desktop. Within a given campus, a number of autonomous networks are assumed to exist, and this architecture must support routing from one to another. The campus will have full access to the global Internet; the architecture template will support traffic to the external world. (This will normally occur through the MAN.) The campus network poses security challenges,

which are addressed by the interleaving security mechanisms at every segment of the template and providing the gateway to the Internet solely at the ITSCs, from which access can be appropriately managed.

### **C.3.6.1 IP Addressing for Campuses**

DON IP address management includes the efficient allocation and use of scarce IP addresses for afloat, ashore, tactical, and non-tactical networking environments.

Each campus will have a single adequately-sized address space allocated from a Classless Inter-Domain Routing (CIDR) block that is administered by the ITSC. The size of the block should be large enough to support the long-term needs of the campus by providing the ability to add hosts as requirements change. This allocation size will be carefully managed to provide maximum use of available address space. Campuses within the DON enterprise should be supported by the ITSCs for IP network planning, internal routing architecture, and implementing CIDR subnetworking.

Each CAN will be subnetted under a single net address/network mask, and the campuses in a particular MAN will aggregate to a single MAN address/network mask. This IP network address management will apply to all IP devices and IP addressing services. IP addresses are officially tracked and assigned only to the level of a Class C address.

The use of subnet masking to subdivide IP address space is supported, but is typically a matter for local shipboard and shore-based network administrators. However, due to the inherent complexities of various IP subnet masking techniques, coordination with the MAN IP service provider is encouraged to ensure the most efficient use of assigned IP address space.

When appropriate, CANs may employ address hiding techniques using the private address space (RFC 1918) for internal connectivity. In such cases, a Network Address Translator (NAT) provides access to the DON enterprise IP network, the Internet, and other external networks. It is useful when a campus uses IP addresses that do not need to be advertised to the DON enterprise network or the Internet.

Dynamic Host Configuration Protocol (DHCP) is used on CANs for IP address management to further ensure the efficient use of assigned address space and to reduce the amount of network administrator time. The latter is accomplished by managing a single DHCP server in lieu of tending to individual end users' workstations. DHCP is limited to standard workstations and other devices whose IP address can be changed without DNS reconfiguration. While DHCP is not specifically intended to support mobile users, its use in this architecture simplifies laptop network attachment at remote locations because each campus establishes a DHCP server. Laptops that are configured as DHCP clients are simply connected to the network and the IP configuration information is automatically obtained. DHCP supports several features used within CANs of the DON enterprise network:

- Automatic assignment of IP addresses and configuration data such as net masks and Domain Name System (DNS) servers
- Automatic reclamation of unused IP addresses resulting in economy of IP addresses
- Centralized administration and management of the IP address space without custom desktop IP configuration

CANs (for the both sea and shore commands) can obtain registered IP addresses from the Naval Computer and Telecommunications Station (NCTS) in Pensacola, Florida, at (COMM) 850-452-3501, (DSN) 922-3501. Addresses can also be obtained on-line at the Navy IP Network Number

Registration page at <http://www.netreg.navy.mil/>. This should be done through the cognizant ITSC.

### **C.3.6.2 DNS Service for IP**

Domain name service is a critical support service for IP that matches end system names (host names, Web URLs) with IP addresses. This subject is addressed in depth in Chapter 4. A CAN has three options for DNS service:

1. Rely on the DNS server at the ITSC. This requires that new campus IP address assignments must be communicated to the ITSC's DNS administrator. All DNS requests result in overhead traffic between end systems and the ITSC.
2. Implement a DNS server locally. The local DNS server is the authoritative server for all campus-based end systems and points to the ITSC DNS server as its upstream reference. The disadvantage of this arrangement is that the campus must administer a server, which nullifies the economy of ITSC centralization.
3. Implement a caching DNS server locally. The ITSC server is the authoritative server as in option 1, but the caching function cuts down on overhead traffic outside the campus network. When properly installed, this server is physically resident on the campus network but is managed by the ITSC.

### **C.3.6.3 IP Routing Services for Campuses**

Architecture guidance for routing in the CAN environment depends on two inter-related variables:

- Interior Gateway Protocols (IGP) versus Exterior Gateway Protocols (EGP)
  - IGP** - Routing inside a campus network assumes all users are self-contained, not separated, and contiguous. The preferred IGP is Open Shortest Path First (OSPF) for overall routing.
  - EGP** - The network solution for EGP depends on whether the campus is integrated with the MAN or is independent.
- Campuses that have network services integrated with a regional MAN and ITSC versus those that operate independently as a single Routing Domain
  - Integrated** - Campus networks that receive service from a regional ITSC as part of a MAN will typically be part of that autonomous system, and consequently, OSPF is still the preferred implementation.
  - Independent** - For EGP from campuses in a single routing domain in which, for administrative or technical reasons, the campus is to remain independent of the regional MAN, Border Gateway Protocol v4, (BGP 4) is the preferred solution.

The integrated OSPF implementation will require a detailed implementation plan by the network administrators at the MAN or regional ITSC. Each CAN will be assigned one or more OSPF areas. Connections from the CAN to the MAN IP service provider(s) must be supported by a route redistribution scheme. Within the MAN itself, the ITSC should provide the route redistribution between the separate autonomous networks.

Autonomous networks are considered in this architecture to be stand-alone IP networks and for routing purposes, have their own routing domain. These domains are managed separately and have their own IGP (OSPF). For EGP, autonomous networks will interconnect using BGP 4.

Exchange of routing information between IGP and EGP should only be for IGP within the routing domain of the individual EGPs. EGPs should connect with EGPs in other regions and exchange information about end systems only – they should not exchange OSPF information. Networks announced via BGP 4 should be explicitly configured to ensure high network stability.

#### **C.3.6.4 IP Security Overlay**

The DON IP overlay shall use the DON ATM overlay to provide the required confidentiality, integrity, and reliability/robustness. A network intruder can potentially impose an instantaneous and effective denial of service by maliciously reconfiguring routers. The following security mechanisms are included to enable management (and remote management) of routers and to provide protection from spoofing attacks leading to denial of service:

- Exchange of routing table update information between DON IP overlay routers shall use cryptographic authentication mechanisms as specified in the DON ITSG Section 3.4.1.4.
- The IP overlay must provide mechanisms to ensure that CAN network components can only be managed by authorized administrators. At a minimum, network components that are remotely managed must feature non-spoofable authentication mechanisms. It is likely that this management will be accomplished in-band across the IP overlay from a regional ITSC.
- Optional network security mechanisms should be available at the CAN level of the IP overlay to allow for increased security for high value assets or to support command specific security requirements. These optional mechanisms should include:
  - Network Intrusion Filters (NIFs) to provide optional boundary level protections between an organization or CoI and the rest of the DON IP overlay.
  - Network Access Controllers (NACs) to provide a basic level of access control over network connections based on an organization's local security policy.
  - Virtual Private Network (VPN) encryption to allow CoIs to enforce a strict need-to-know separation between their intra-CoI information and the rest of the DON IP overlay. This is normally accomplished by using a COTS VPN encryption mechanism. See the DON ITSG Section 3.4.1.2 for guidance on selection of COTS VPN mechanisms.
- Bringing contractor network connections through the CAN is discouraged. These connections should comply with the guidance in Chapter 3.7.6 and should be negotiated through the ITSC.

#### **C.3.7 Switching and Routing Overlay**

Optimized routing across the ATM network will be done using PNNI. Physical routers equipped with ATM interfaces will be necessary for routing between the switched ATM network and existing non-ATM networks. Servers or workstations running native ATM between the desktop and ATM backbone will have multiple connections to the ATM backbone through an ATM workgroup switch.

The CAN connection to the MAN is a switch. To support network security, a firewall router with an ATM interface to the CAN backbone is required at the MAN access point.

The campus infrastructure should be populated with a variety of multi-function hubs that have integrated switch/router functions to enable ATM switching, LANE or MPOA for legacy networking environments, and Switched Ethernet for VLAN support. Interoperability among VLAN vendors is currently the exception rather than the rule, so care must be taken to ensure vendor commitments to embrace available standards.

A combined routing and switching approach will allow work-groups to receive faster network performance with routing invoked only when logical network segmentation is necessary.

### **C.3.8 Voice Overlay**

The integration of voice and data over a single network infrastructure is an important goal of the DON ITI architecture. There are multiple integration levels that should be considered.

For example, a single cable plant can be more flexible to configure and use, can be easier to maintain, and provides a reduced life cycle cost. Category 5 UTP cabling should be used to support both voice and LAN because Category 5 cable is interchangeable (Category 3 telephone cable is not). But this cabling decision alone does not achieve integration – there are many other decisions that must be correctly made to connect computers and hubs to the CAN and telephones and PBXs to the cable.

The frame-based LAN technologies most used in campus LANs today – Ethernet, Token Ring, and FDDI – support voice by digitizing it and placing the bits in IP datagrams. Over a heavily loaded network, the quality of service is less interactive than the network user is accustomed to on circuit switched voice circuits. Alternatively, ATM provides the real-time response and bandwidth-on-demand necessary for telephone quality voice transmission but does not fully support the enhanced voice services and circuit interfaces that are required for full voice functionality. Both approaches are technically feasible, supported in the commercial marketplace, and interoperable via voice-IP gateways.

A remote switching module (RSM) should be co-located with the core (or primary) campus switch. The RSM serves as a central office for the CAN. It typically provides only basic physical voice connectivity. Enhanced services such as voice mail and conference calls are provided by a central voice switch located in the MAN or regional ITSC. The RSM extends the services and reach of the MAN's centralized Private Branch Exchange (PBX) switch to each CAN.

The RSM does not connect directly to the public switched network or other voice networks, but connects to the MAN or region central voice switch, which in turn connects to these networks. ATM provides the transport from the RSM to the region's central voice switch via the CAN primary switch and the MAN/region ITSC ATM switch. This supports maximum flexibility, use of existing infrastructure, centralization of egress points to minimize circuit costs, centralized trouble reporting operations, and easy expansion.

At the campus, the RSM will use load sharing for routing through dual load-sharing ATM devices. In the event of a failure at the switch, the RSM should have stand-alone capabilities until the failure is resolved. Therefore, sufficient redundancy should be built into the CAN architecture to provide the required level of service.

The campus RSMs will be programmed to perform Least Cost Routing functions regardless of the digits dialed by the user to accomplish the most efficient transport egress for the call.

- If a call is destined for a local destination, the switch will use first choice, high usage DoD trunks to the Local Exchange Carrier (LEC) central office for completion.
- If the call is destined for another campus tied to the MAN, the call will be routed to the hub switch for termination to the proper trunk group for the called location, thereby eliminating all LEC toll charges.
- If the call is destined for termination to a facility outside the MAN, a route to the hub switch and an FTS trunk group will be chosen to minimize the cost of this long distance call. Similar routes will be programmed to handle DISN oriented calls from the RSM.

Each CAN voice instrument is directly linked by Unshielded Twisted Pair (UTP) to an RSM port. The cable plant for the premise distribution of voice circuits parallels that of the data circuits. This architecture does not attempt to implement ATM voice or data to the desktop or LAN/enclave wiring closet. However, this capability is supportable within this architecture and it is anticipated that eventually voice and data will coexist on the same campus ATM cable plan.

In the long term, voice and telephony over ATM (VTOA) will provide support for legacy voice services to an ATM terminal. It is analogous to LANE and MPOA in the data environment. As performed on ATM SVCs, VTOA provides improved bandwidth effectiveness (and potential cost savings) because the voice calls are switched directly. At the same time, voice quality is provided through voice adaptation techniques and QoS support.

The voice architecture should take maximum advantage of commercial off-the-shelf technology and existing DoD-sponsored development programs.

## **C.4 Functional and Performance Specifications**

Traditionally, campus networks have been described in terms of design guidance, not in terms of service levels or outcomes. In other words, the government has specified the precise implementation architecture. It is clear that service levels are an integral part of planning and implementation and are necessary to evaluate and determine alternative solutions.

The CAN template will be measured and evaluated under five categories: security, functionality, interoperability, performance, and cost. A level of service and in some cases, the specific technologies required, should be described for each. The following prescribed specifications are provided as a guide; actual requirements may warrant adjustment of these values, but should be based on solid documentation.

### **C.4.1 Security**

A number of security mechanisms are allocated to the CAN. The first layer of defense is to use object level security and the PKI infrastructure as the key exchange method. This places the security focus on the data rather than on the networks through which the data flows and the computers it is stored in. Secure e-mail is one instance of object level security. Cryptographic equipment is required for the protection of classified information.

Information protection must be provided by information security. This architecture details the mechanisms that must be supported.

- Hardened

Level of service: Must provide sufficient level of protection for denial of service and intrusion detection.

Technology: The Campus Network will use a layered information protection system as follows:

1. End users use object level security (such as secure e-mail) as the first line of defense. This provides confidentiality, authenticity, and non-repudiation features to the level of the supporting PKI trust model.

2. Virtual Private Networks provide secure enclaves at varying levels of granularity and these, along with object level security, should be used when available. Because some applications such as FTP are not supported by object level security implementations, this helps to mask some traffic analysis parameters and to provide greater application-level flexibility.
3. Firewalls are located in the DON intranet at the external network interfaces of the ITSC/MAN. Campus networks shall not install bypass routing (such as a router interface to an external network) around the DON firewalls except when they are configured and managed by the ITSC. A campus network may find it necessary to firewall itself from the rest of the Naval intranet by placing a firewall at the CAN/MAN interface.
4. Link level encryption may also be added to links in the CAN when higher levels of protection are required.

- Survivability (specifically relating to security) (see also Performance)

Level of service: Intrusion detection, denial of service, vulnerability to service attacks

Technology: These network control functions are performed at the ITSC NOC, not at the campus level.

## **C.4.2 Functionality**

The capabilities required of the CAN infrastructure that are necessary to effectively and efficiently support the operational mission and requirements must be clearly defined.

- CAN connectivity

Level of service: Each CAN is provided access to two geographically-separated MAN switches.

Technology: N/A

- ATM

Level of service: If applicable, use as required to support mission requirements (voice, video, and data) of the CAN. ATM provides robustness and potential for growth.

Technology: End-to-end SVC

- Switch functionality

Level of service: Must support constant bit rate QoS.

Technology: Non-blocking and provide separate queuing for different QoS classes. Switches use PNNI. Requires NSAP to IP mapping for support of IP.

- IP

Level of service: Ubiquitous end-to-end IP connectivity is supported across the enterprise. It requires full access to the global Internet. Campus routers are connected to the MAN via a full Virtual Circuit mesh.

Technology: N/A

- Router functionality

Level of service: The CAN routing architecture is integrated with the MAN and with the fleet's single routing domain. IP router functionality includes minimum hops between end points and scalability.

Technology: Routers communicate with each other inside the CAN using OSPF and outside the CAN using BGP 4.

- Availability

Level of service: Accessible to all campuses, MANs, and external customers.

Technology: N/A

### **C.4.3 Interoperability**

The components of the network infrastructure must interconnect and efficiently and effectively communicate signaling and other information transfer data.

- Manageability

Level of service: The selection of critical networking components such as switches, multiplexers, and router components of the network must be controlled so that they are remotely manageable by the ITSC to support availability, performance, and cost. This is essential to control cost.

Technology: Components are required to have network management agents to enable remote network management.

- Service Delivery Points

Level of service: Must support the full suite of ITSG-cited ATM protocols and addressing schemas.

Technology: N/A

### **C.4.4 Performance**

The CAN service must be of sufficient quality to meet information transfer requirements to support the Naval mission.

- Bandwidth

Level of service: The bandwidth should be appropriate to the customer's information requirements and be readily scaleable. This is interrelated to availability and survivability.

Technology: Bandwidth is dependent upon technology selected and is discussed elsewhere in this template.

- Delay

Level of service: the cell switching delay on a CAN switch will not be more than 20 us under a load of 80 percent of the interface rate (for example, OC-3c) of both input and output port. The maximum delay variation/switch shall be less than 2 us under the same load condition as above.

Technology: N/A

- Latency

Level of service: the average latency in completing a call setup for a two level peer group must be less than 100 ms/hop.

Technology: N/A

- Network availability. The prescribed level of service should apply to the campus backbone and to critical servers (both network support and user services) that are attached to the campus backbone.

Level of service: It is neither practical nor necessary to provide high availability (higher than 0.99) for each client on the network, because clients tend to be interchangeable (i.e., they view e-mail from multiple desktops). Similarly, it is neither necessary nor practical to provide high availability at the border of the network.

Technology: Topology provides for no switch or physical circuit being a single point of failure.

- Survivability (specifically relating to performance) (See also Security)

Level of service: Vulnerability to forces of nature, acts of humans (e.g., backhoe, loss of power)

Technology: No switch or physical circuit is a single point of failure

- Quality of Service

Level of service: As noted in the MAN template, automatic virtual circuit crossover should be provided by the service provider to provide continuity of service in the event of a switch failure. Ability to support a number of service classes based on the traffic type, each with an associated QoS parameter.

Technology: N/A

- Mean Time to Repair

Level of service: Premium service: less than 2 hours. A CAN planner/manager should evaluate the tradeoff between repair response and redundant equipment. For example, a second router in a location separate from the first router and on a separate Uninterrupted Power Supply may provide adequate redundancy (and additional capacity) to eliminate the need for a 2-hour maintenance response. The maintenance posture can shift to “next working day.” When making this decision, consider the cost of the second router and associated equipment and whether or not it is greater than the on-call maintenance requirement that it may eliminate.

Technology: N/A

### **C.4.5 Cost**

Implementation cost is an important category for judging value and must be done in the context of the level of service. The principal metric for cost control revolves around people costs. The DON will minimize IT support costs at the campus level (especially the 24-hour watch-standing costs and on-call maintenance costs) by centralizing those functions at the ITSCs and eliminating the requirements for on-call maintenance through redundancy and planning for high availability. This centralization initiative assumes that the ITSC will perform effectively and will not increase the IT infrastructure support burden on end users.

## **C.5 Evaluating CAN Products and Services**

The selection of CAN products and services should be made by an organizational team comprised of representative operational and functional experts.

The determination will be made based on a balanced scorecard approach using as a basis the characteristics defined in the Functional and Performance Specifications in Section C.4. Addressing the proposals of each competing product or service should be in accordance with the criteria in Figure C-1.

**Department of the Navy Chief Information Officer  
Information Technology Infrastructure Architecture, Version 99-1.0  
16 March 1999**

Network Characteristic	Raw Score	Weighting (.xx)	Adjusted Score
Network Security	X	.30	X
Functionality	X	.25	X
Interoperability	X	.20	X
Performance	X	.25	X
Total	—	1.0	X
Total Merit / Cost	—	—	X/\$YY

Figure C-1. Product/Service Evaluation

- Four of the five characteristics will be scored based on a numerical rating system (1-10). The supporting subsets of each characteristic will be evaluated and aggregated to determine the value of the characteristic.
- Also, each characteristic will have a weight factor based on its judged importance to the overall region/MAN/CAN mission. The total of these individual weight factors will be 1.0.
- The numerical value for each characteristic is multiplied by its weight factor, and the total of the five adjusted scores equals the relative merit for the source provider.
- Cost will be viewed as a separate variable. The relative merit will be expressed in a ratio of total merit to cost (e.g, X / \$ YY).
- The team should complete an analysis of the alternative providers and present a recommendation to the regional commander/cognizant decision-making body. Included in the presentation will be a recommendation for the administration and funding of the product or service.