

# Volume I, Appendix B - Table of Contents

<b>B. Metropolitan Area Network Design Template.....</b>	<b>B-1</b>
B.1 Purpose.....	B-1
B.2 Drivers.....	B-2
B.3 Elements, Features, and Specifications .....	B-3
B.3.1 ATM Overlay.....	B-3
B.3.2 IP Overlay.....	B-7
B.3.3 MAN Specifications .....	B-9
B.4 Service Considerations.....	B-10
B.4.1 ATM MAN Ownership.....	B-10
B.4.2 Selecting a Commercial Service Provider.....	B-11
B.4.3 Balanced Implementation .....	B-12
B.5 Outcome Based Implementations - Metrics.....	B-13
B.5.1 Security.....	B-13
B.5.2 Functionality.....	B-14
B.5.3 Interoperability .....	B-15
B.5.4 Performance.....	B-15
B.5.5 Cost.....	B-16
B.6 Evaluating MAN Products and Services .....	B-16

This page intentionally left blank.

## B. Metropolitan Area Network Design Template

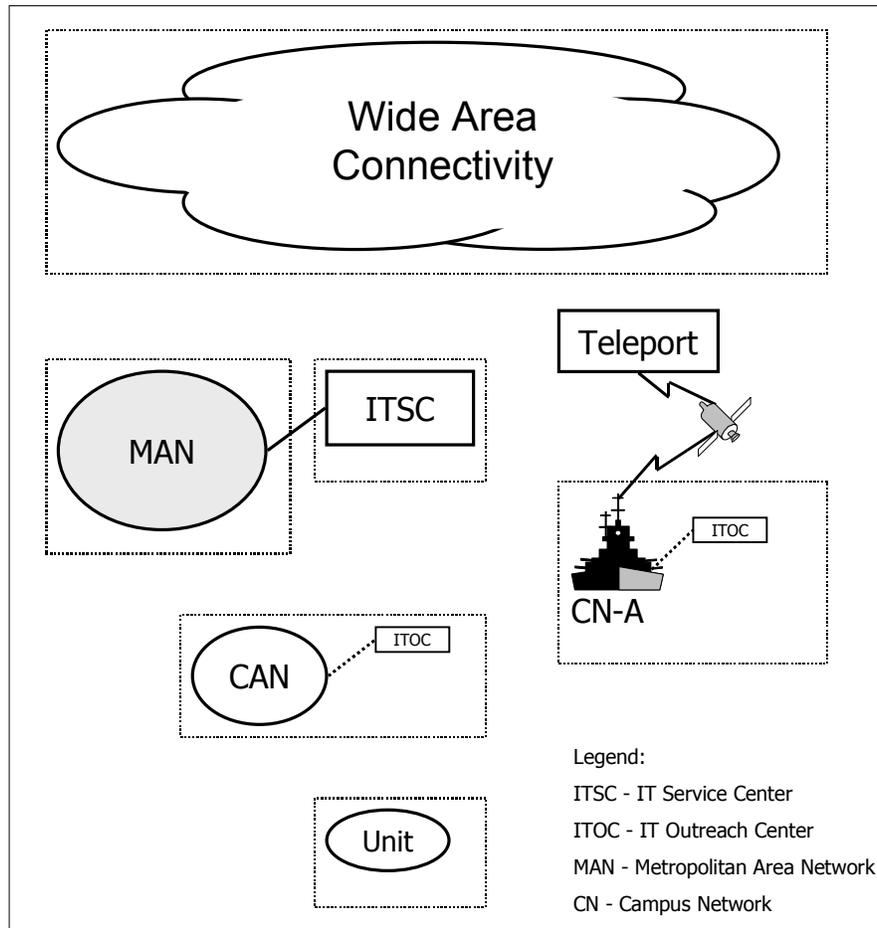


Figure B-1. High Level Components of the TI Architecture

### B.1 Purpose

The foundation for integrated, enterprise IT and systems in the DON is the technology infrastructure. Figure B-1 depicts the relationship of the Metropolitan Area Network (MAN) to the other components of this infrastructure. This MAN template defines the technology infrastructure interfaces between the Base, Post, Camp or Station, their associated Information Technology Service Center (ITSC), and any other entities that may constitute a given region. It also addresses connectivity to the DON enterprise network or WAN.

The MAN template is intended to provide design guidance to infrastructure planners and implementers. This guidance is provided in the form of connectivity graphics and associated relevant descriptive text. The template supports decentralized design and implementation of connectivity solutions that are consistent, complementary, and interoperable with the overall DON technology infrastructure.

The MAN approach enables the consolidation of voice, video, and data onto a single network and offers the advantages of speed, economy, and interoperability for the entire spectrum of networking applications. The MAN's underlying physical infrastructure connectivity is essentially leased by the DON regional managers from local and regional wide area service providers. Riding on this leased network is a DON enterprise infrastructure that relies on ATM. ATM is the technology basis for the Navy and Marine Corps autonomous networks and community of interest networks.

## **B.2 Drivers**

The DON mission requirements require a world-class information infrastructure. Each MAN is an integral part of the DON enterprise network and supports the collective requirements of the Navy and Marine Corps customers operating within an individual fleet concentration area. The set of drivers that must be addressed is:

- ***Information superiority*** - This architecture must support improved security, functionality, performance, configuration management, and cost avoidance and provide cheaper, better, and faster service.
- ***Decentralized implementation*** - The DON campus and base networks are implemented in a decentralized fashion and must be based upon a clear and well-defined technical architecture that provides a basis for interoperability in the region, between campuses, and with external organizations.
- ***Customer-based*** - The connectivity and services required by all DON customers operating in a metropolitan area (or region) must be provided for by a fully functional MAN.
- ***Consolidation*** - Underused or common information technology infrastructure (ITI) functions must be consolidated and streamlined whenever appropriate to provide better services at significantly less cost.

## B.3 Elements, Features, and Specifications

This section describes the technology elements of the MAN template, their operational features, and their design specifications. The specific sections are depicted in Figure B-1.

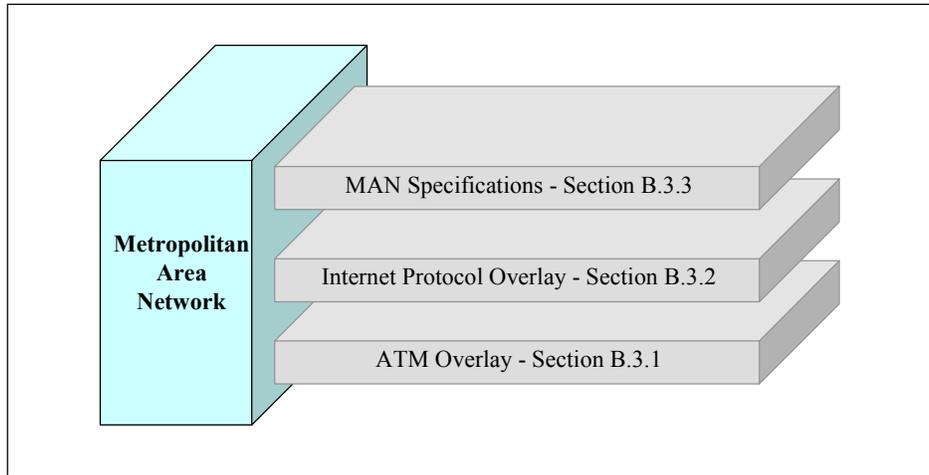


Figure B-1. Layered Description of Metropolitan Area Network

The guidance provided here is intended for technical planners and implementers to produce MANs that are based on the best technology solutions available, that offer satisfactory levels of network performance and reliability, and that can operate successfully in the context of a global enterprise network. This section will require frequent updating to ensure that changes in technology, services offered, and Naval requirements are adequately reflected.

### B.3.1 ATM Overlay

The notional MAN template in Figure B-1 shows typical DON campuses or bases that are connected to the MAN backbone using ATM switches. The features of the ATM overlay are described in subsequent subsections titled Physical Layer, Switching and Routing, and Security.

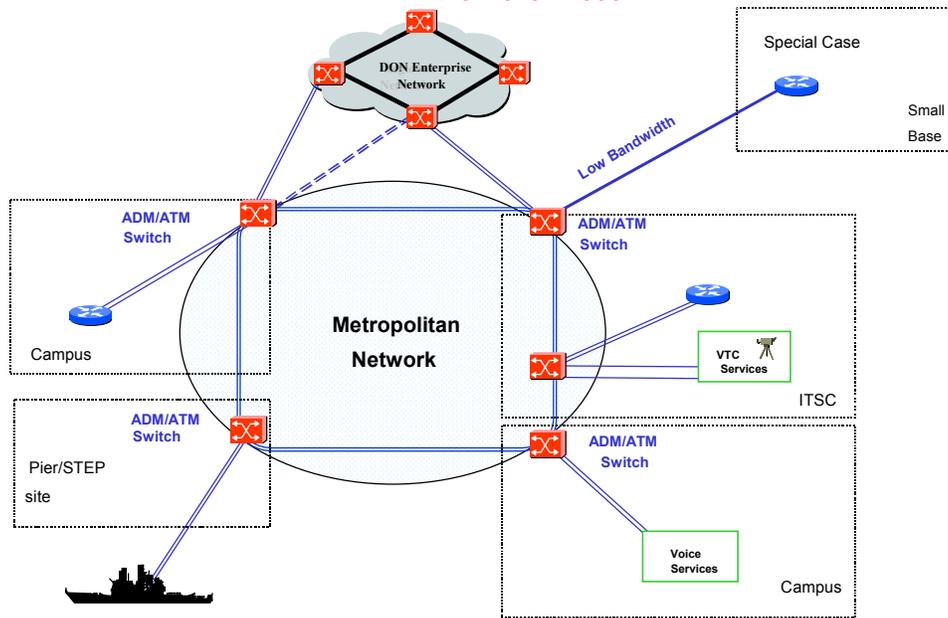


Figure B-1. Metropolitan Area Network Template (ATM Overlay)

### B.3.1.1 Physical Layer

The MAN switches are connected using an underlying transport alternative that can be a point-to-point mesh using dark fiber, a point-to-point or ring configuration using Synchronous Optical Network (SONET) technology, or an ATM regional network. For any of these three methods, the conditions under which the service provider supports the underlying DON ATM MAN is important to establish. In any support arrangement, the DON must maintain positive control over the MAN ATM infrastructure to ensure that the transport technology is protocol-independent and to ensure support of a variety of ATM configurations that operate on top of the physical layer.

It is important that the physical layer support high network availability. This requirement necessitates dual threading (redundancy in components and circuits) to thereby eliminate single points of failure.

### B.3.1.2 Switching and Routing

Voice, video, imagery, and data are encapsulated in ATM cells and transported over the MAN backbone. The underlying MAN transport is transparent to the users of the campus and base networks as long as the service exhibits satisfactory availability, bandwidth, and latency. A number of configurations can be supported between the MAN and the campus environments including switch-to-switch links and switch-to-router links. The most desirable configuration is the switch-to-switch link (with ATM switching available at each campus endpoint); the switch-to-switch link provides the most flexibility and robustness in satisfying networking requirements.

ATM switch connections to the carrier backbone should be dual-homed for appropriate redundancy as shown in Figure B-1. ATM switch connections may also be the preferred solution for campus sites that use the MAN backbone to interconnect voice switches (e.g., 5ESS) to the DON infrastructure. Aggregation of campus video teleconferencing infrastructures (using multiple Basic Rate Interface (BRI) Integrated Services Digital Network (ISDN) channels) into

the MAN ATM switching fabric is also desirable to the extent that the ATM backbone can be leveraged to provide cost savings over FTS-2000.

### B.3.1.3 Security

The placement of security mechanisms in the ATM overlay as shown in Figure B-1 is highly dependent on the type of MAN construction. Two basic cases for security solutions are presented in this section: MANs using commercial ATM services (not under positive DON control) and MANs using point-to-point fiber or SONET links (or mesh) under DON-controlled ATM services.

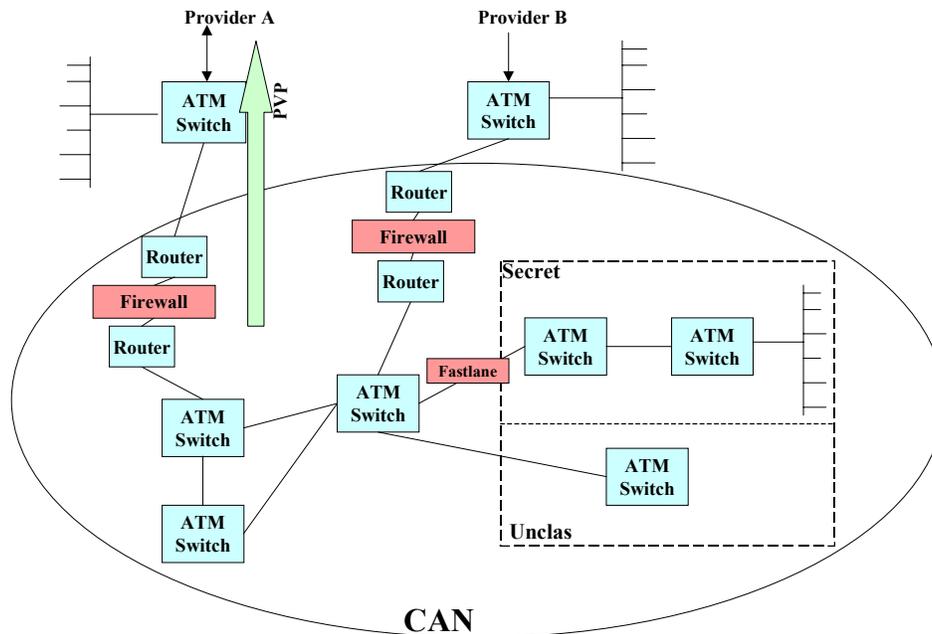


Figure B-1. MAN ATM Not Under DON Control (Security Case 1)

In the case illustrated in Figure B-1, the commercial ATM service provider and other customers receiving services from the commercial ATM cloud must be assumed to be threats to the confidentiality, integrity, and robustness/reliability of the DON ATM overlay. To mitigate these threats, the following security mechanisms are required:

- Fastlane ATM encryption devices must be employed to encrypt the SBU information passed between campuses. Secret information is already encrypted before it enters the CAN (at higher layers in the ISO model using object level security, such as secure e-mail) via Virtual Private Networks or under NES/EIP enclaving.
- The vendor's ATM cloud must be analyzed in detail in order to determine its susceptibility to single points of failure. If the commercial cloud is not found to have sufficient redundancy, a second provider must be used to provide redundancy. This points out the need to have visibility into the vendor's management domain. One way to obtain this visibility is to export on a continuing basis the relevant Simple Network Management Protocol (SNMP) data from the vendor to the ITSC.

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

- A Permanent Virtual Path (PVP) solution, with appropriate committed information rates, will be used to ensure that the commercial provider can satisfy the minimum bandwidth requirements of the MAN. However, if DISN ATM services are subscribed, it may be possible to use a Switched Virtual Circuit (SVC) solution with Memorandums of Agreement (MOA) guaranteeing a minimum bandwidth.
- Bandwidth allocation management within the DON-controlled portion of the ATM overlay must be provided. This portion of the overlay may actually exist in the CAN when commercial ATM services are used to construct the MAN. This management must provide administrators with the capability to identify the priority of data transport requests and to allocate network bandwidth to the highest priority when contention occurs. Additionally, the ATM overlay must feature mechanisms to “order and add” additional required bandwidth from the commercial ATM cloud.
- The ATM overlay must provide mechanisms that ensure that the DON-controlled components of the overlay (these may be considered part of the CAN) can only be managed by authorized administrators, are resistant to penetration attempts, and are resistant to ATM signaling based denial of service (DoS) attacks. The use of KG-75 Fastlanes significantly reduces the potential for unauthorized administration and successful penetration originating from outside the DON-controlled portion of the overlay. In order to reduce the potential for successful penetrations originating from within the DON-controlled portion of the overlay, remotely-managed network components must feature a non-spoofable authentication mechanism.

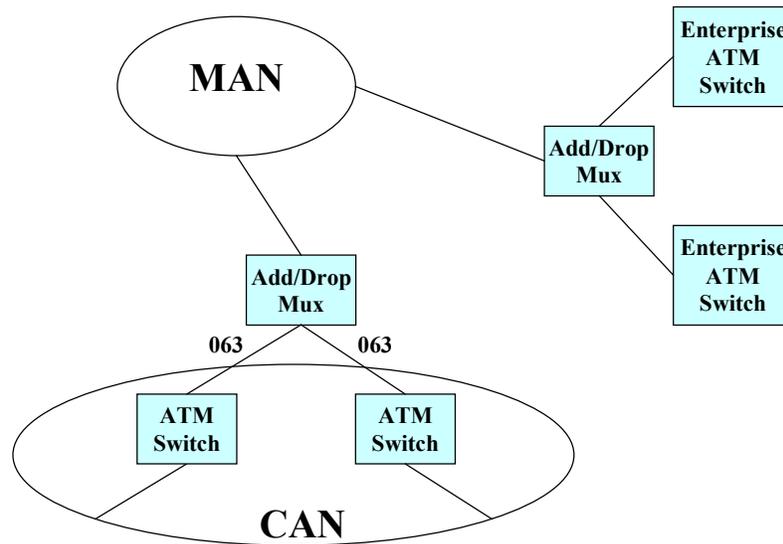


Figure B-2. SONET MAN Under DON Control (Security Case 2)

Figure B-2 shows the condition of implementing a SONET MAN service in which the MAN is under DON control. The potential threats to the confidentiality, integrity, and survivability of the DON ATM overlay are significantly reduced. However, certain security mechanisms are required and are outlined in the following.

- Fastlane ATM encryption devices are only required for secret information (installed between secret buildings and SBU CANs) because the entire ATM MAN is operated at the SBU system high level.
- The ATM MAN must be constructed in a redundant fashion such that the failure of a single network component or interconnection will not lead to the disconnection of a CAN from the MAN or failure of the MAN.
- Bandwidth allocation management must be provided within the ATM overlay. This management must provide authorized administrators with the capability to identify the priority of data transport requests and allocate network bandwidth to the highest priority when contention occurs. Additionally, the ATM overlay should be designed with the ability to “order and add” additional bandwidth as required (such as by adding additional links to the ATM mesh).
- The ATM overlay must provide mechanisms to ensure that DON-controlled components of the overlay (these may be considered part of the CAN) can only be managed by authorized administrators, are resistant to penetration attempts, and are resistant to ATM signaling-based DoS attacks. In order to reduce the potential of successful penetrations originating from inside the DON-controlled portion of the overlay, remotely managed network components must feature a non-spoofable authentication mechanism.

### **B.3.2 IP Overlay**

The MAN IP overlay describes the connectivity infrastructure which transports IP traffic onto the MAN and then through Navy and Marine Corps organizational sites. This MAN architecture spans the physical, network, and application layers and leverages ATM to support a robust implementation of IP. In combination, the IP and ATM technologies support the creation of a high performance, flexible, and proven infrastructure. The features of the IP overlay are described in these subsections:

- Integration with ATM
- Routing Determination
- Performance Provisioning
- Security

#### **B.3.2.1 Integration with ATM**

The MAN template in Figure B-1 builds on Figure B-1 and depicts the close relationship between the IP layer and the ATM layer. The IP networking design is irrevocably tied to the ATM implementation. The specific methods for transporting IP over ATM, such as using request for comments (RFC) 1483 encapsulation techniques, RFC 1577 address mapping, and the internetworking capabilities of LAN Emulation (LANE) and Multiple Protocol Over ATM (MPOA), are discussed in Chapter 2. The ATM technology attributes also provide the capability to transfer IP packets with a “Quality of Service”-like guarantee of network performance.

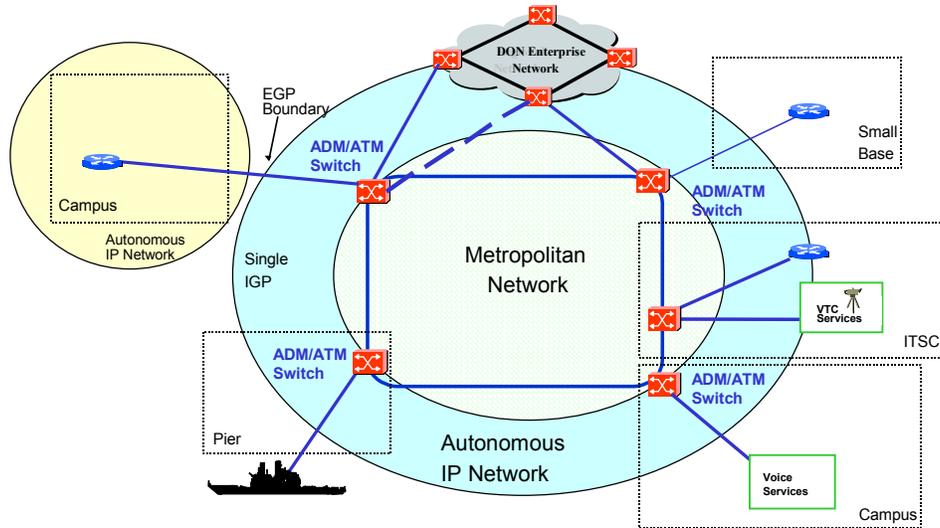


Figure B-1. Metropolitan Area Network Template (IP Overlay)

### B.3.2.2 Routing Determination

The general design for internal and external routing is described here as a basis for MAN implementation decision-making. For internal routing, Open Shortest Path First (OSPF) is the preferred Interior Gateway Protocol (IGP) to connect the campus/base to the backbone MAN. There are other satisfactory solutions by which bases can exchange information with the MAN, but only the preferred solution is addressed here.

*The MAN will be OSPF Backbone Area “0”, the ITSC is a separate backbone area, and the campus/base can be a separate area.*

In the case of the campus/base, the alternative to OSPF is to use an external router solution based on Border Gateway Protocol (BGP) 4 – if supported by a favorable evaluation in performance tradeoffs. The MAN/regional ITSC will provide the OSPF “border router” and will also provide access to other autonomous systems.

The DON autonomous systems as described in Chapter 2 will connect to the MAN using BGP 4 as the preferred Exterior Gateway Protocol (EGP).

### B.3.2.3 Performance Provisioning

The MAN template depicts a model using IP and ATM technology that provides for flexible, high-bandwidth, IP-based “autonomous networks” on top of ATM-based “virtual circuits.” This design supports the flexibility to provide bandwidth as it is needed without being constrained by congested IP paths. These services should extend to all campuses within a MAN. In support of the fleet sites, the autonomous network service extends to the piers, to the Naval Computer and Telecommunications Area Master Stations (NCTAMS), and to the Standard Tactical Entry Point (STEP) sites.

#### **B.3.2.4 Security**

The DON IP overlay will use the DON ATM overlay to provide required confidentiality, integrity, reliability, and robustness. Confidentiality and integrity for SBU information are provided by ATM on a bulk basis. It is further concluded that for confidentiality, authenticity, and non-repudiation of classified information, additional network and higher layer tools must be provided. The following guidance outlines the additional security mechanisms required to secure the DON IP overlay at the MAN level.

- Connections to external networks (NIPRnet at SBU and SIPRnet at Secret) will only be provided via regional/MAN firewalls. These firewalls will enforce a uniform access control policy for outside NIPRnet and SIPRnet entities attempting access to the DON IP overlay. These firewalls will most likely be installed at regional ITSCs or firewall facilities (FWFs). A centrally-monitored intrusion detection system (IDS) should be installed in concert with the network firewall at all interconnections to external IP networks. Additional information on network firewalls and IDSs are provided in Appendix E.
- Exchange of routing table information updates between DON IP overlay routers will use cryptographic authentication mechanisms as specified in the DON CIO ITSG section 3.4.1.4.
- The IP overlay must provide mechanisms to ensure that network components of the CAN are only managed by authorized administrators. At a minimum, network components that are remotely managed must feature a non-spoofable authentication mechanism. It is expected that this management will be accomplished in-band across the IP overlay from a regional management center (such as an ITSC).
- Contractor network connections to the MAN are described in Chapter 3.7.6. These connections must be consistent with this architecture and should be negotiated through the ITSC.

#### **B.3.3 MAN Specifications**

Technical specifications are required to ensure that network services and capabilities are consistent for MANs across the Navy and Marine Corps. In this way, performance is assured and large organizational customers and operators functioning in MANs across the DON see consistency in the following areas:

- ***Interconnectivity to other joint services*** – Seamless connectivity among Army, Navy, Air Force, Marine Corps, and Coast Guard must be ensured.
- ***Virtual private networks (VPN)s*** – Selected commands require VPNs and will require that the ITSC support and manage these VPNs.
- ***Voice, video, imagery, and data over ATM*** – Network-centric warfare requires the full spectrum of telecommunications.
  - ◆ For data, the MAN should support end-to-end SVCs.
  - ◆ For voice, regional planners and designers should ensure that NI-1-compliant ISDN telephone service is available to support the Secure Terminal Equipment (STE) secure telephony.

- **Routing and addressing** must be managed and supported for all organizations within the MAN, including participating joint services.
  - ♦ MANs must interface into one or more ATM routing domains, become part of a DON-wide ATM Network Service Access Point (NSAP) addressing plan, and participate in a consistent, hierarchical routing architecture.
  - ♦ Unrestricted IP traffic between campuses (that is, the associated IP networks) is supported on the backbone using the routing scheme described in this document.
  - ♦ In order to minimize the size of internal routing tables, MANs should obtain a Classless Inter Domain Routing (CIDR) block sufficiently large enough to provide IP service to all organizations within the MAN. The required size is based upon the number of campuses and the population of each campus.
- **Name resolution** must be managed and supported for interconnectivity throughout the DON enterprise.
- **Integrated encryption** – Selected commands will require encryption services for voice, video, and data.
- **Circuit management for voice, video, and data** – Selected (if not all) commands will require management (to include provisioning and billing) of their circuits.
- **Remote management of CANs through the MAN** – Closed networks will require the ability to pass management traffic through the MAN to other central management centers outside the MAN (such as TIMPO at San Antonio, Texas).
- **“.com” traffic allowed to the campus** – Commercial traffic must have the ability to access closed networks within the MAN while maintaining overall information security.

## **B.4 Service Considerations**

Decisions relating to the service provider affect more than best value. In many cases, particularly with ATM technology, the source of the services may determine what is possible to implement. Examples include support of SVC or Private Node-Node Interface (PNNI) hierarchical-based routing that many commercial service providers do not support. Also, ownership of some components may be the sole answer to implementing some desired network capabilities. This section provides a discussion of buying versus leasing, a checklist of services, and a balanced MAN implementation that addresses the needs of all customers.

### **B.4.1 ATM MAN Ownership**

The intended ownership (public versus private) of the components of the MAN is a major factor in the consideration of planning and implementation issues. Ownership carries with it control, including many factors that affect the ultimate level of network services and security. Relevant considerations include Naval requirements, commercial services available, and business case analysis. The ownership answer is by no means the same for every MAN and must be determined based on careful analysis.

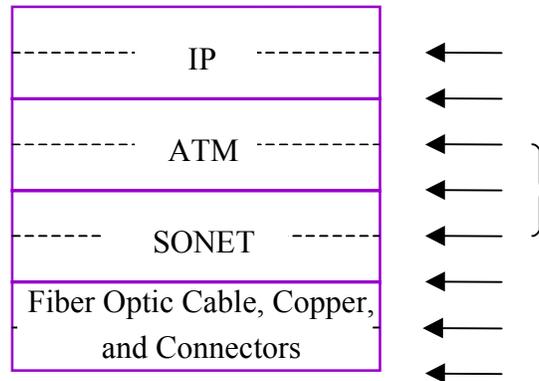


Figure B-1. Network Layers Relevant to MAN Planning

The layers shown in Figure B-1 depict the network components and services that are roughly related to the layers of the Open System Interconnect model. The components and services are discussed in the following bullets:

- IP services will be DON-owned in all envisioned circumstances.
- Naval ownership of ATM services provides many advantages, including performance, security, and reliability. Where justified by mission requirements, existing service offerings, and business case analysis, DON ownership should be an option.
- SONET (including both the cable runs between SONET multiplexing devices and the standards for transporting signals on a fiber optic cable, for multiplexing data, and for frame generation) is usually obtained as a commercial service. In selected instances, the DON may want to own the SONET layer. Examples might include a Naval mission requirement under which bandwidth at the SONET layer is established. Implementation can be made practical by placing a Naval SONET layer on top of the commercial provider's SONET service. In certain cases, direct ATM interconnectivity can occur with an intervening SONET ADM layer (the physical layer will still be SONET but there will be no SONET ADMs).
- Ownership of the MAN physical connectivity (including the fiber optic cable, copper, and connectors) is not supported by Naval requirements or by business case analysis. Physical connectivity will be obtained as a service from commercial service providers, except in special cases such as remote/overseas sites like Guam, Bahrain, and Sigonella.

#### **B.4.2 Selecting a Commercial Service Provider**

The selection of a service provider is as important as determining the specific network services to be obtained. In many areas, a single service provider is not able to meet the Naval requirement for services. Many service providers are either inexperienced or unwilling to support the desired protocols or provide the service level needed for the DON MAN. The following ATM areas of support are provided as a guide for evaluating service providers:

- **Service categories** - Tuning the ATM to the particular MAN for voice, video, and data may require a variety of service offerings beyond Variable Bit Rate and Constant Bit Rate. The service offering should support the desired service quality and fit the specific applications of the MAN.

- **Quality of service** - Working with service categories, QoS parameters are a determinant of network performance and must support the desired service quality.
- **Size of connections** - Bandwidth estimates should be slightly higher than the expected use and should be matched to the service category.
- **Support of ATM protocols** - SVCs can be an attractive option in many MANs and should be implemented when appropriate. ATM protocols that support voice and multimedia are similarly important.
- **Network optimization** - Maximizing the throughput of Transmission Control Protocol/Internet Protocol (TCP/IP) networks to match the characteristics of the MAN can be performed by knowledgeable service providers.
- **Network monitoring** - Detecting and isolating faults as they occur should be performed to the level of granularity that permits tasking the appropriate repair technician.
- **Support of LANE and MPOA** - These ATM protocols are complementary and are important to support IP and other legacy protocols. They also introduce issues regarding placement of servers, caching of addresses, and the set-up of VPNs.
- **Traffic management** - The service provider operating capabilities and policies affect performance, particularly when the MAN is supporting service interworking.
- **Over-subscription** - Service providers vary in their tolerance for the bursty nature of certain data applications.
- **Automatic rerouting** - Responses to failed scenarios are not equal among all service providers and must be clearly delineated and understood.
- **Service level agreements** - Specific written agreements should cover relevant aspects of service availability. Recommended areas include allowed downtime per year, mean time to repair, and mean time between failures; service performance such as cell loss; and service installation such as intervals for new ports and PVPs. Effective agreements include a sufficient penalty and means to identify missed service levels.

#### **B.4.3 Balanced Implementation**

Determining the balance of enterprise, regional, and organizational functions is a critical success factor in the network connectivity and services implementation. Two overarching ideas (Singularity of Purpose and Autonomous Networks) must be supported.

- **Singularity of Purpose** - Decentralized (i.e. regional and campus) infrastructure performance improvement and consolidation cannot occur without a common DON enterprise network. This assumes that planners incorporate the requirements of all “area” users in the MAN implementation.

*The MAN must provide connectivity services to all user groups defined by any Navy and Marine Corps organization at or above the autonomous network layer. Users may be in multiple communities of interest, but at any one time user computers are probably only connected to a single autonomous network.*

- **Autonomous Networks** - A number of organization networks are built on top of the enterprise connectivity and bandwidth infrastructure. Autonomous networks, to varying degrees, may be independent of each other from the standpoint of media, technology, security, management, and other characteristics. They are more than virtual networks and may include some physical components that are unique to the particular autonomous network. Autonomous network examples include the fleet intranet and other networks which support the Marine Corps (MCEN), NIPRnet, SIPRnet, BUMED, and SYSCOMS. The fact remains that when possible, these organizations must be part of the DON enterprise network to make information superiority and RMA possible.

*To the extent possible, owners of autonomous networks will work with the MAN/regional managers to use the physical components of the MANs to enhance interconnectivity and to reduce duplication and cost.*

## **B.5 Outcome Based Implementations - Metrics**

The MAN template places emphasis on design guidance and establishing service levels or outcomes. Clearly, evaluation of alternatives and definition of desired service levels are an integral part of planning and implementation. They are also necessary to evaluate and determine alternative solutions. A basis for optimizing any decision approach should be to view decision-making in the context of the enterprise, region, MAN, and campus and not just in terms of the immediate entity. Functions that should be aggregated under the next level should not be continued at the present level when no performance/cost rationale exists.

A critical success factor in the life cycle of any MAN planning and implementation is the development of the RFP. A government-developed and -prepared RFP should provide measures that furnish a satisfactory representation of Naval requirements.

The suggested guidance for selection of a commercial service provider is a beginning point. These and other relevant requirements factors should be stated in terms of empirical measures that set expectations and provide accountability for performance.

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

### **B.5.1 Security**

A number of security requirements are allocated to the MAN. Cryptographic equipment is required for the protection of classified (and possibly SBU) information. Redundancy should be used. Mechanisms to control access to critical networking components such as switches, multiplexers, and routers should also be used.

- Information confidentiality and integrity
  - ♦ Level of service: must provide sufficient level of protection for information confidentiality and integrity. When a DON-controlled MAN is employed, adequate physical and personnel security must be established to protect information at the SBU

level. When a non-DON-controlled MAN is employed, National Security Agency (NSA)-approved encryption devices shall be used to encrypt data before entering the MAN so that it will be unclassified. However, the service provider must ensure that adequate physical and personnel security is established to protect traffic statistics of DON information traversing the MAN.

- ◆ Technology: KG-75 Fastlane, physical security, and personnel security
- Survivability: specifically relating to security; see also performance
  - ◆ Level of service: must provide protection against denial of service threats (including hostile IW, human error, etc.) commensurate with the criticality of information that will traverse the MAN.
  - ◆ Technology: token-based access control for network components, intrusion detection systems, network management systems, contingency planning

## **B.5.2 Functionality**

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

- ATM
  - ◆ Level of service: support voice, video, imagery, and data
  - ◆ Technology: end-to-end switched virtual circuit (SVC) and permanent virtual path (PVP)
- MAN connectivity
  - ◆ Level of service: each MAN is provided access to two geographically-separated WAN switches
  - ◆ Technology: N/A
- Switch functionality
  - ◆ Level of service: must support constant bit rate (CBR) QoS
  - ◆ Technology: non-blocking and provide separate queuing for different QoS classes. WAN switches will support at least 2048 switched and/or permanent virtual circuits (PVCs) per interface.
- Availability
  - ◆ Level of service: accessible to all MANs and outlying bases. It is assumed that the MANs will be carrying data for mission critical applications, therefore, an availability of 99.99 percent is an acceptable minimum. (The level of four nines forces redundancy; a single-threaded system (single points of failure) that fails cannot be repaired fast enough to meet this level.)
  - ◆ Technology: N/A

### **B.5.3 Interoperability**

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

- Service delivery points
  - ♦ Level of service: must support the full suite of Information Technology Standards Guidance (ITSG)-cited ATM protocols and addressing schemas
  - ♦ Technology: N/A

### **B.5.4 Performance**

The MAN service must be sufficiently qualified to meet the following information transfer requirements to support the Naval mission.

- Bandwidth
  - ♦ Level of service: minimum of OC-3
  - ♦ Technology: redundant dual-homed
- Delay
  - ♦ Level of service: maximum end-to-end delay for a CBR service connection should be less than 200 us/switch for processing and queuing plus the necessary propagation delay. The maximum end-to-end cell delay variation should be less than 1 ms.
  - ♦ Technology: N/A
- Latency
  - ♦ Level of service: if switched point-to-point SVC or SVP is supported, the average latency in completing a call setup should be less than 100 ms/hop.
  - ♦ Technology: N/A
- Network availability
  - ♦ Three principles of high availability are established: (1) eliminating single points of failure, (2) reliable crossover, and (3) prompt notification of failures as they occur. All three must be accounted for in performance metrics.
  - ♦ Network monitoring is an issue that requires visibility. A problem in monitoring network availability is determining the failure point when something breaks. The normal situation is for the commercial vendor and base telecommunications to each deny responsibility. Through the ITSC, the capability should exist to immediately sort out the failure point and to call the correct repairman. One means is SNMP visibility of the vendor's network by having access in the ITSC to the real-time availability data that the vendor system monitors are indicating. Having this access should be part of the regional/MAN service provider specification.
  - ♦ Level of service: 99.99 percent
  - ♦ Technology: no switch or physical circuit is a single point of failure

- Survivability (specifically relating to performance; see also Security)
  - ♦ Level of service: vulnerability to forces of nature, acts of humans including enemy action (e.g., backhoe, loss of power, terrorist strike)
  - ♦ Technology: no switch or physical circuit is a single point of failure.
- Quality of Service
  - ♦ Level of service: 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
  - ♦ It is important to note that this decision is highly impacted by the type of system being supported. If the system has double redundancy (is dual-threaded) or triple redundancy, the requirement for premium service may not be justifiable. The trade-off is between adding more redundancy with next day service or a single-threaded system with immediate on-call maintenance.
  - ♦ Technology: N/A

### **B.5.5 Cost**

Implementation cost is a significant category for judging value and must be driven by the context of the level of service.

## **B.6 Evaluating MAN Products and Services**

The selection of MAN products and services should be made by an organizational team comprised of representative operational and IT technical experts.

The determination will be made based on a balanced scorecard approach using as a basis the characteristics defined in Section B.5. Addressing the proposals of each competing product or service should be in accordance with the criteria in Figure B-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	.20	X
Interoperability	X	.20	X
Performance	X	.30	X
Total	—	1.0	X
Total Merit / Cost	—	—	X/\$YY

Figure B-1. Product / Service Evaluation

1. 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.
2. 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. Recommended weight factors are provided.
3. 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.
4. Cost will be viewed as a separate variable. The relative merit will be expressed in a total merit to cost ratio (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.