

DAL 67647-116
08 March 2001



NETWORK STANDARD, VERSION 1.4-PR

FOR

DISTRIBUTED MISSION TRAINING OPERATIONS AND INTEGRATION (DMT O&I)

DAL No. 67647-116

08 March 2001

CONTRACT NO: F33657-98-D-2061

Prepared for:

Department of the Air Force
Aeronautical Systems Center
Wright-Patterson AFB
Dayton, Ohio



TABLE OF CONTENTS

Revision / Change Record	ii
Foreword	1
Introduction.....	2
1. Scope	4
2. Conformance	5
2.1. Federate Testing.....	8
2.1.1. Internal Testing Performed by the DMT O&I Contractor	8
2.1.2. Internal Testing Performed by Each Federate System.....	9
2.1.3. Testing Performed between the DOC and each Federate System	9
2.2. Federation Testing	10
3. Normative References.....	11
4. Terms and definitions	12
5. Acronyms	13
6. DMT System Network Interface Requirements	14
6.1. Federate System to DMT System Network Interface	14
6.2. Protocol and Services.....	14
6.3. Bandwidth & Latency	15
6.4. Encryption.....	15
6.5. Internet Protocol (IP) addressing scheme	15
Bibliography.....	16

List of Figures

Figure 1 Typical Base POP Network Architecture.....	2
Figure 2 Typical DMT to MTC Network Architecture	2
Figure 3 Verification of Compliance with the DMT Network Standard Criteria	8
Figure 4 Typical Federate System Site	14

List of Tables

Table 1. Criteria Verification Matrix	6
Table 2. Supported DMT System Protocols	14

Foreword

This standard is one of 13 standards being developed for the DMT System. Each standard in the set addresses one or more aspects of the DMT environment and is categorized under one of three categories. Standards in the first category, Interface Standards, address the network connectivity, software and hardware interfaces, and protocols necessary for Federate Systems to exchange information. Integration Process Standards document common processes and procedures that facilitate coordinated operation of individual simulator systems as a harmonized DMT System. Federate System Performance Standards address consistency, fidelity and performance factors ensuring a fair fight among training participants. As a whole, the set of standards is intended to ensure an interoperable, distributed, simulated battle-training environment.

DMT System standards apply to all Federate Systems participating in DMT Federations or on the DMT System Network. Stakeholders interested in conducting or participating in DMT System Network supported simulation training events must use Federate Systems and processes that comply with effective DMT System standards criteria. Conformance criteria for each standard are individually dated to indicate its effective date. The effective date for initial criteria is the DMT System Initial Operational Capability (IOC) System date.

The 6 standards with initial criteria effective for the DMT System IOC, are those necessary to achieve initial DMT training objectives with the integrated capabilities of the available F-15C and E-3A Federate Systems in a DIS-compliant network. These include Network, DMT Tailored DIS, Event Control, Security, Conformance Testing, and Technical Performance standards.

First Federation standards are driven by HLA requirements and related enhancements to the DMT infrastructure. Standards for the objective system will be refinements of the First Federation standards with an additional emphasis on establishing consistency in scene depiction and entity/environment response across the breadth of users in the training community.

The DMT Standards Development Working Group (SDWG), established under the authority of the DMT System Integration Engineering Team (SIET), charters Tiger Teams to develop standards. Government and industry stakeholders and interested community members are encouraged to actively participate on these Tiger Teams. The DMT Operations and Integration (O&I) Contractor, as leader of the SDWG and chartered Tiger Teams, coordinates standards publication under the authority of the Department of the Air Force Aeronautical Systems Center at Wright-Patterson AFB, Ohio 45433, contract F33657-98-D-2061.

The network standard includes references to the TACLANE encryption device and the Portal. The Security and Portal standards will detail the interfaces for the TACLANE and Portal, respectively. The Technical Performance standard will address latency budgets for the DMT System Network.

Introduction

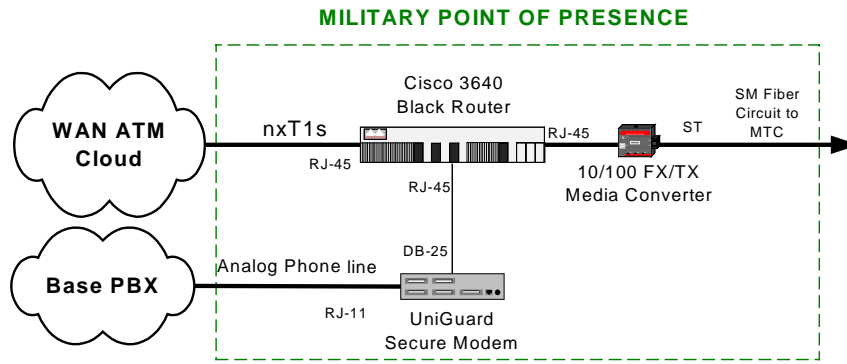


Figure 1 Typical Base POP Network Architecture

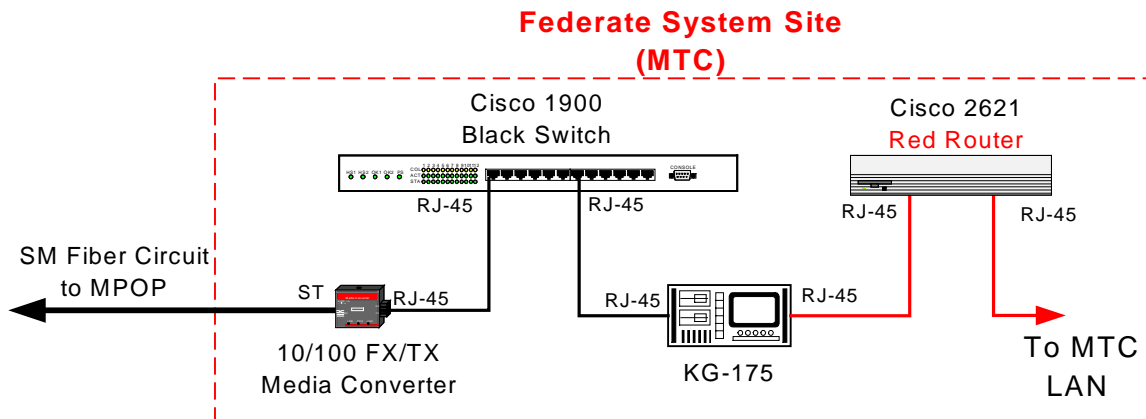


Figure 2 Typical DMT to MTC Network Architecture

The above figures show the typical base network architecture. On the Federate System side of the Military Point of Presence (MPOP), the Federate System LAN using TCP/IP will transport simulation data to the Red router which will then forward the data to the KG-175 encryption device. The O&I contractor will configure a "Red" router to properly interface with red (Ciphertext) side of the TACLANE for the Federate Systems. The KG-175 TACLANE will decrypt and encrypt the data to and from the Federate System LAN. The Cisco 1900 black switch will serve as a buffer between the full-duplex interface of the Cisco 3640 black router and the half-duplex interface of the TACLANE in IP mode. The 10/100 FX/TX media converter transitions twisted pair Ethernet communications to singlemode fiber Ethernet communications and vice versa.

At the MPOP, the black router uses Inverse Multiplexing over ATM (IMA) to provide the capability to transmit and receive data across multiple DS1 circuits to the ATM WAN. Within the ATM WAN, Switched Virtual Circuits (SVC) provide rapid reliable connectivity with a high Quality of Service (QoS) supporting these connections that require a steady and predictable throughput with minimal delay and low cell loss. In addition, within the ATM WAN, Permanent Virtual Circuits (PVC) provide the means for continuous monitoring and control of the DMT System Network. The UniGuard modem allows secure remote configuration of the black router.

IEEE 802.3, RFC's 792, 793 and 1042, ATT Publication 62411, and ATM Forum Specifications af-uni-0010.002 define the standards necessary to achieve the DMT Network System architecture. In identifying this network architecture, TRW conducted tests on a variety of network configurations to produce the highest quality of network services. A lab environment was established at the TRW office in Orlando, Florida to simulate Federate Systems communicating over a Wide Area Network. Within this simulated environment, using unicast and broadcast, TRW successfully transmitted voice, video, and simulation data at bi-directional rates up to 5.52 Mbps across 4 DS1 circuits. This limitation was due to the tested hardware configuration (i.e., There were only 4 DS1 ports available on the test router IMA WAN interface card). TRW then expanded the test across the wide area network by using the TRW location in Carson, California. Each TRW location simulated a Federate System Site. Once again, using unicast and broadcast, TRW successfully transmitted voice, video, and simulation data at bi-directional rates up to 2.76 Mbps across 2 DS1 circuits. Within the lab environment, TRW was able to test IMA and transparent bridging router configurations. A transparent bridging scheme is a technique often used in Ethernet and IEEE 802.3 in which bridges pass frames along one hop at a time based on tables associating end nodes with bridge ports. Since the presence of bridges is transparent to the network end node, the term "Transparent bridging" is used.

Federate System LANs incorporate 100Mbps Fast Switched Ethernet using 100BaseT routers, hubs, switches, and Network Interface Cards (NICs) with Category 5 UTP cabling. The DMT System Network supports this well-established network standard. To this end, no new standards were established for the DMT Network System. However, while a particular standard, specification, or protocol is well establish, it may not be widely deployed in the commercial environment. IMA is one such protocol. This technology is currently not available for DMT but will be by June 2001. Until this time, transparent bridging will fulfil DMT System Network bandwidth and latency requirements.

1. Scope

The Network Standard describes the method for interfacing to the DMT System Network. The DMT System Network encompasses the ATM WAN and the collection of network devices up to the RJ45 10Base-T port on the Federate System side of the DMT Portal. As required, this standard references the appropriate standards to define additional interface requirements for DMT System Network.

2. Conformance

Table 1 contains the criteria for the DMT Network Standard. In addition, this table identifies the verification method(s) used to ensure that DMT is in conformance with the criteria and allocates the criteria to test phases and to responsible parties. The DMT Conformance Test Standard defines test phases and verification methods. The comment column includes any additional information required to support the verification activities and the Initial Effectivity column the date (either directly or by reference to a DMT milestone) that the criteria is effective.

Table 1. Criteria Verification Matrix

Criteria ID	Criteria	Verification Method(s)	Federate Testing		Federation Testing			Responsible Party(s)			Comments	Initial Effectivity
			HLA Conformance Testing	Application Testing	Integration Testing	Functional Testing	Scenario Testing	DMT O&I Contractor	Federate Sponsor	Federation Sponsor		
NTW-001	Each Federate System will demonstrate the ability to ping the DMT interface point from the Federate System LAN. The packet size for the pings must range in size from 300 bytes to 1500 bytes in 200 byte increments.	T		X				X	X		The interface point for all IOC Federate Systems to the DMT System Network is the KG-175 encryption device. Detailed discussion of this device is not part of this standard. However, each MTC will provide the TACLANE device while TRW will provide configuration and setup instructions. When the DMT Portal application deploys, it becomes the Federate System entry point to the DMT System Network.	IOC
NTW-002	Each Federate System will follow the IP addressing scheme for interfacing to the DMT System Network as defined in the section entitled "Internet Protocol (IP) addressing scheme" of the Network Standard.	D		X	X			X	X		Each Federate System will have the responsibility of its assigned subnet configuration management. Federate System owners are asked to provide the O&I contractor with the addressing plan for their system for coordination purposes. For IOC, Boeing may use a subnet mask of 255.255.0.0.	IOC
NTW-003	The DMT System Network defines ports 3000, 6993, and 11111 for UDP Broadcast and Unicast operations. The Federate Systems will demonstrate usage of at least one of the defined ports.	D		X	X			X	X		These ports were used during DNS development to test UDP Broadcast and Unicast operations. The Federate Systems will provide the O&I contractor with a complete list of other required ports as needed. For IOC, the Federate Systems have selected port 6993.	IOC
NTW-004	The DMT System Network supports TCP, UDP, IP, FTP, and TFTP. Each Federate System will demonstrate FTP capability.	D		X	X			X	X		Federate Systems may demonstrate these services using other Federate Systems and the DOC.	IOC

Table 1. Criteria Verification Matrix

Criteria ID	Criteria	Verification Method(s)	Federate Testing		Federation Testing			Responsible Party(s)			Comments	Initial Effectivity
			HLA Conformance Testing	Application Testing	Integration Testing	Functional Testing	Scenario Testing	DMT O&I Contractor	Federate Sponsor	Federation Sponsor		
NTW-005	Reserved											
NTW-006	Each Federate System will demonstrate the ability to ping other Federate System sites from the Federate System LAN. The packet size for the pings must range in size from 300 bytes to 1500 bytes in 200 byte increments. Each site must demonstrate the ability to ping.	D			X			X	X		This criterion will test connectivity between Federate Systems.	IOC

Verification Methods: N/A - Not Applicable, C – Compliance, I - Inspection, A – Analysis, D – Demonstration, T - Test

Figure 2 depicts the process used to ensure that DMT is compliant with the criteria contained in the DMT Network Standard.

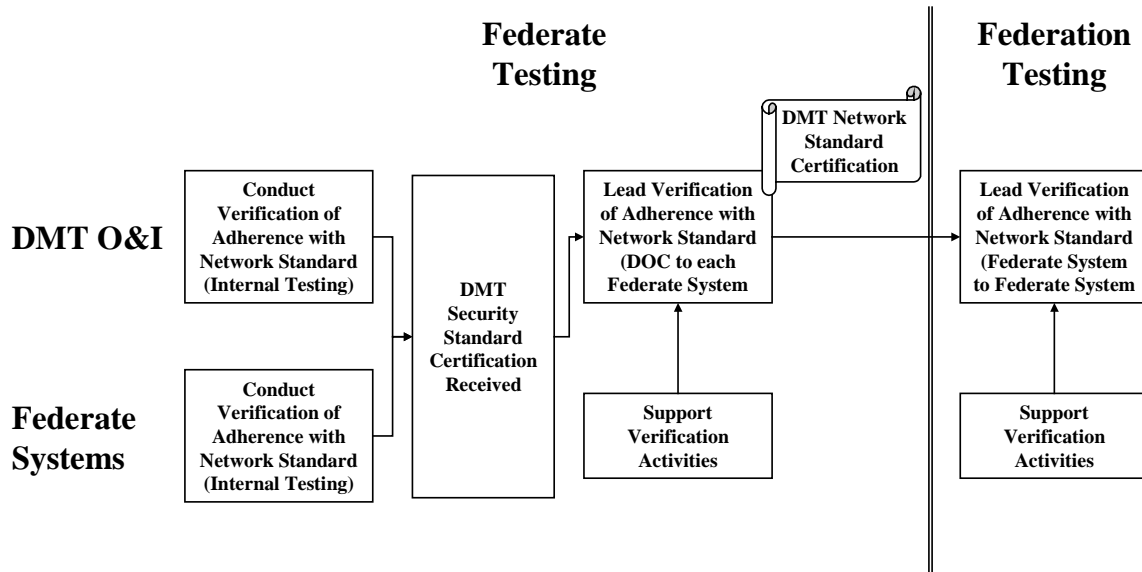


Figure 3 Verification of Compliance with the DMT Network Standard Criteria

2.1. Federate Testing

2.1.1. Internal Testing Performed by the DMT O&I Contractor

During Federate Testing the DMT O&I Contractor will verify the capability of the DMT network to support the following functions:

- a. The ability of the DMT O&I Contractor to ping various points on the DMT System Network from the DMT NOC.
- b. UDP Broadcast and Unicast operations (NTW-003).
- c. FTP and TFTP capabilities (NTW-004).

These capabilities will be verified at the following points:

- a. Between the NOC and the Router located in the MPOP of each Federate System site.
- b. Between the NOC and the Media Converter in the MTC at each Federate System site.
- c. Between the NOC and the TACLANE in the MTC at each Federate System site (if possible using Unclassified Keys).
- d. Between the Media Converters at each Federate System site.

These activities occur before the Federate Systems are connected to the DMT Network and are performed in accordance with the DMT O&I Contractor's internal policies and processes.

2.1.2. Internal Testing Performed by Each Federate System

During Federate Testing each Federate System will verify the capability of their system to support the following functions:

- a. FTP capability (NTW-004).
- b. Ability to perform UDP broadcast. (NTW-003).

In addition, each Federate System will verify:

- a. Implementation of the IP addressing scheme for its assigned subnet (NTW-002).
- b. Implementation of the port addressing scheme as agreed to by the Federate Systems in the Federation under test (NTW-002).

These activities occur before the Federate Systems are connected to the DMT Network and are performed in accordance with the internal policies and processes of each Federate System.

2.1.3. Testing Performed between the DOC and each Federate System

The entry criteria for this phase of testing are as follows:

- a. The DMT O&I Contractor and the Federate System have successfully completed their internal testing activities as outlined above.
- b. The DMT O&I Contractor has received the Certification and Accreditation Letter from the DAA for the DOC.
- c. The Federate System has received the Certification and Accreditation Letter from the DAA for their site and a copy is on file with the DMT O&I Contractor.
- d. The Memorandum of Agreement authorizing connectivity among the sites has been signed by each of the Federate Systems and by the DMT O&I Contractor and a copy is on file with the DMT O&I Contractor.

Failure of one Federate System to complete the security certification process will not inhibit other Federate Systems from execution of this activity.

Following successful completion of the entrance criteria, the Federate System is connected to the DMT Network and the following criteria are verified:

- a. The ability of the Federate System to ping the DMT interface point from various points on the Federate System LAN (NTW-001, NTW-002).
- b. The ability of the Federate System to perform UDP Broadcast and Unicast operations in accordance to the port addressing scheme agreed to by the Federate Systems in the Federation under test (NTW-003).
- c. FTP capability (NTW-004).

The DMT O&I Contractor will lead this activity, will provide the necessary verification procedures, and will document the results. The Federate Systems will support this activity by providing the appropriate manpower to support test execution. The verification procedures will be provided in the Federation Test Plan.

The evidence required by the DMT O&I Contractor to support Federate System Certification for adherence to the DMT Network Standard Criteria is the documented results from this phase of testing as provided by the DMT O&I Contractor.

2.2. Federation Testing

Following successful completion of Federate Testing and the Certification of the Federate Systems as compliance with the DMT Network Standard, the following criteria are verified:

- a. The ability of the each Federate System to ping other Federate Systems in the Federation under test (NTW-006).
- b. The ability of the Federate System to perform UDP Broadcast and Unicast, operations in accordance to the port addressing scheme agreed to by the Federate Systems in the Federation under test (NTW-003).
- c. FTP capability (NTW-004).

The DMT O&I Contractor will supervise this activity and will provide the necessary verification procedures. One of the Federate Systems will be designated to lead this activity and document the results. The Federate Systems will support this activity by providing the appropriate manpower to support test execution. The verification procedures will be provided in the Federation Test Plan.

3. Normative References

The following normative documents contain provisions that, through reference in this text, constitute provisions of this Network Standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this Network Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the referred normative document applies.

1. IEEE 802.3, Standard for Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access, Method and Physical Layer Specifications
2. IEEE 802.3u, Local and Metropolitan Area Networks-Supplement - Media Access Control (MAC) Parameters, Physical Layer, Medium Attachment Units and Repeater for 100Mb/s Operation, Type 100 BASE-T (Clauses 21-30)
3. RFC 793 - Transmission Control Protocol
4. RFC1042 - A Standard for the Transmission of IP Datagrams over IEEE 802 Networks
5. RFC 792 - Internet Control Message Protocol
6. ATM Forum Specifications af-uni-0010.002, ATM User Network Interface specification
7. ATT Publication 62411, T1 digital transmission, packet switched, by ACCUNET T1.5 network service

4. Terms and definitions

The DMT Common Definitions document will define terms and definitions applicable to this Network Standard. This document is posted on the DMT web site at:
http://www.trwdmt.com/dmt/sdwg/common_definitions.doc.

5. Acronyms

This section contains some acronyms used in this document. The DMT web site at contains the DMT Common Definitions document http://www.trwdmt.com/dmt/sdwg/common_definitions.doc. This document defines additional acronyms.

ATM	Asynchronous Transfer Mode
DIS	Distributed Interactive Simulation
DMT	Distributed Mission Training
DNS	Domain Name Service
DS1	Data Service Level 1
FTP	File Transfer Protocol
HLA	High Level Architecture
HTTP	Hypertext Transfer Protocol
IAB	Internet Activities Board
IEEE	Institute of Electrical and Electronics Engineers
IMA	Inverse Multiplexing over ATM
IOC	Initial Operational Capability
IP	Internet Protocol
ITU	International Telecommunication Union
MIB	Management Information Base
MPOP	Military Point of Presence
MTU	Maximum Transmission Unit
NIC	Network Interface Card
PVC	Permanent Virtual Circuits
QoS	Quality of Service
RFC	Request for Comment
SDWG	Standards Development Working Group
SIET	System Integration Engineering Team
SMTP	Simple Mail Transfer Protocol
SNMP	Signalling Network Management Protocol
SVC	Switched Virtual Circuits
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
UTP	Unshielded Twisted Pair

6. DMT System Network Interface Requirements

The following subsections will define the DMT System Network interface and supported protocols and services. Each Federate System provider will be responsible for proper configuration of its Federate System to bring that system onto the DMT System Network.

6.1. Federate System to DMT System Network Interface

The MTC Contractor will be responsible for the networks within its facility and must provide an interface point for connection to the DMT System Network. The interface to the DMT System Network will be an 8-position modular jack (RJ45) at the DMT defined gateway. For IOC the gateway will be the Red Router. In figure 3, a crossover UTP Cat5 cable is used between the TACLANE and the red router. The DMT System Network interface is set for 100 BaseT Full-Duplex Ethernet operation. Users of the DMT System Network should disable "auto negotiation" at the interface port.

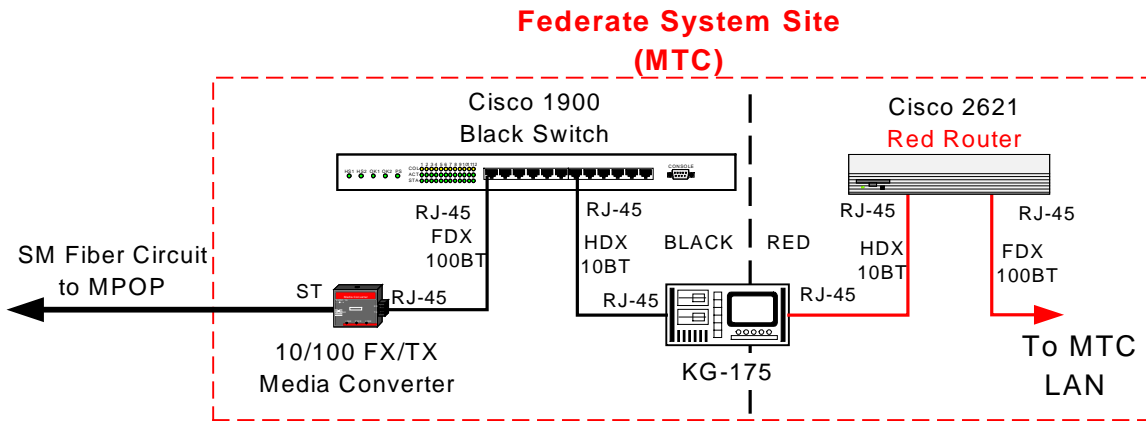


Figure 4 Typical Federate System Site

6.2. Protocol and Services

Users of the DMT System Network interface will communicate via Ethernet as described in the IEEE 802.3 standard. The DMT System Network supports both UDP and TCP operation. The Layer 3 network protocol will be Internet Protocol (IP) as governed by the Internet Activities Board (IAB). The network will support the suite of protocols that are required as a part of the IP standards. The table below shows the supported DMT System Network protocols and services at the interface point.

Table 2. Supported DMT System Protocols

Protocol or Service	Yes	No
TCP	X	
UDP	X	
FTP	X	
IP	X	
TFTP	X	
Telnet *		X
HTTP		X
SNMP		X
SMTP		X
DNS		X

* Telnet service may be available once the security issues are resolved (Post IOC).

6.3. Bandwidth & Latency

The DMT System Network will provide the bandwidth required for the training scenarios to be run within the DMT program. Objective system bandwidth requirements will depend on results of First Federation testing.

6.4. Encryption

Each MTC will encrypt all data that leaves its facility. This encryption will be accomplished with NSA approved encryption gear and with key material defined in the DMT Security Standard. The KG-175 TACLANE provides a 10Bbase-T Half-Duplex interface both on the black (Plaintext) and red (Ciphertext) side of the encryptor through a RJ-45 connector. The MTC contractor will be responsible for TACLANE configuration per the DMT TACLANE Configuration Procedure. The procedures are further discussed in the DMT Security Standard.

6.5. Internet Protocol (IP) addressing scheme

For more information on the Internet Protocol addressing scheme, see Version 1.4.

Bibliography

- [1] Oppenheimer, Priscilla. Top-Down Network Design, Indianapolis, IN: Macmillan Technical Publishing; 1999.
- [2] Comer, Douglas E. Internetworking with TCP/IP Principles, Protocols, and Architectures 4th Ed., Upper Saddle River, New Jersey: Prentice Hall; 1995.
- [3] Joint Technical Architecture (JTA) 3.0; 15 NOV 1999.