The following motion was passed by the SEC on 24 April 2001, with a tally of 9-0-1:

"The SEC considers that ongoing maintenance of the 802 Functional Requirements document is no longer required, given that its useful content has now been documented elsewhere. Therefore, the SEC no longer considers the FRD to be an 802 standing document, and deprecates its use. The FRD is to be archived on the IEEE 802 website for the next five years, along with a record of this motion; after that time, the document is to be deleted."

FUNCTIONAL REQUIREMENTS

IEEE Project 802

Local and Metropolitan Area Networks Standards Committee
This document is intended to supersede the IEEE 802 Functional Requirements Document (FRD), version 5.4, dated Oct. 19, 1981. THIS DOCUMENT HAS NOT BEEN OFFICIALLY REVIEWED OR APPROVED. THIS DOCUMENT IS CIRCULATED FOR REVIEW PURPOSES ONLY! All Rights Reserved by the

Institute of Electrical and Electronics Engineers, Inc. Draft 6.8

Revised: July 10, 1991
(translated into HTML by Vic Hayes, January 1, 1997, update of Jan 13)

TABLE OF CONTENTS

1.0 INTRODUCTION
2.0 APPLICABILITY
3.0 SCOPE
4.0 STANDARDS DEVELOPMENT CRITERIA
5.0 FUNCTIONAL REQUIREMENTS
6.0 ADDITIONAL IVD LAN FUNCTIONAL REQUIREMENTS
7.0 ADDITIONAL MAN FUNCTIONAL REQUIREMENTS
8.0 SECURITY FUNCTIONAL REQUIREMENTS
9.0 CONFORMANCE TESTING
References
FIGURES
Figure 3-1 Local and Metropolitan Area Network Model 5

1.0 INTRODUCTION

1.1 Local Area Networks
1.2 Metropolitan Area Networks

This document defines the functional requirements and guidelines for the IEEE 802 family of Local Area Networks and Metropolitan Area Networks. The functional requirements include the use, environment, functions, and recommended performance of such networks. It also defines the functional requirements for interfaces and protocols. The guidelines are those items which, while not mandatory, give direction to standards developers in development of those standards. The material that is defined as requirements is shown in **bold** text, while the guidance material is shown in *italics*.

1.1 Local Area Networks

A Local Area Network (LAN) is a data communications system which allows a number of independent data devices to communicate with each other. A Local Area Network is distinguished from other types of data networks in that communications are normally confined to a moderately sized geographic area, such as a single building or a campus. This is in contrast to a Wide Area Network (WAN) that may interconnect facilities in different parts of a country or of the world. Interoperation with public switched networks is an optional capability. Local Area Networks are also distinguished by their use of packet mode communications and a common Data Link Layer interface. The physical communications channel of a LAN has a moderate to high data rate and a consistently low error rate.

An Integrated Voice/Data Local Area Network (IVD LAN) allows a number of independent integrated voice/data devices to communicate with one another and with integrated voice/data devices on a MAN or a WAN backbone network. The IVD LAN supports voice, data, facsimile, and other types of digitally encoded information. An IVD LAN differs from traditional (non-IVD) LANs in its physical integration of these information types. The physical communications channel of an IVD LAN has a moderate to high data rate and a consistently low error rate. The IVD LAN provides access to Integrated Services Digital Network (ISDN) WANs, IEEE 802 MANs, and IEEE 802 LANs.

1.2 Metropolitan Area Networks

A Metropolitan Area Network (MAN) is a data communications system which allows a number of independent data devices to communicate with each other. A MAN interoperates with public switched networks. A Metropolitan Area Network is distinguished from other types of data networks in that the communications are normally confined to a limited geographic area, such as a city. This is in contrast to Local Area Networks (building or campus coverage) and Wide Area Networks (unlimited coverage). The physical communications channel of a MAN has a moderate to high data rate and a consistently low error rate. A MAN provides access to Integrated Services Digital Network (ISDN) WANs and IEEE 802 LANs.

2.0 APPLICABILITY

This document is applicable to all project groups of IEEE 802. An exception to the requirements stated in this document shall require the prior approval of the IEEE 802 Executive Committee. *When possible, this request for exception should be made at the time of initial Project Authorization Request (PAR) approval.*

3.0 SCOPE

3.1 Model
3.2 Applications and Devices

The goal of LANs (including IVD LANs) and MANs is to facilitate compatibility and interoperability between equipment made by different manufacturers such that communications can take place between the equipment. To accomplish this, these standards provide specifications that establish common interfaces and protocols for Local Area Networks (including IVD LANs) and for Metropolitan Area Networks.

The intent of these standards is to provide an architecture that permits the effective interconnection of moderate cost devices, and is in itself, a moderate cost network. For some networks, low cost alternatives may also be provided.

3.1 Model

Packet mode data communication in LANs (including IVD LANs) and MANs shall be described in terms of, and designed to be in conformance with, layered services and protocols as defined by the ISO Standard entitled "Open Systems Interconnection - Basic Reference Model" (ISO 7498) [1]. In so far as packet mode data communication is concerned, the focus of IEEE Project 802 is on the lower two layers (data link and physical) of the reference model (see Figure 3-1).

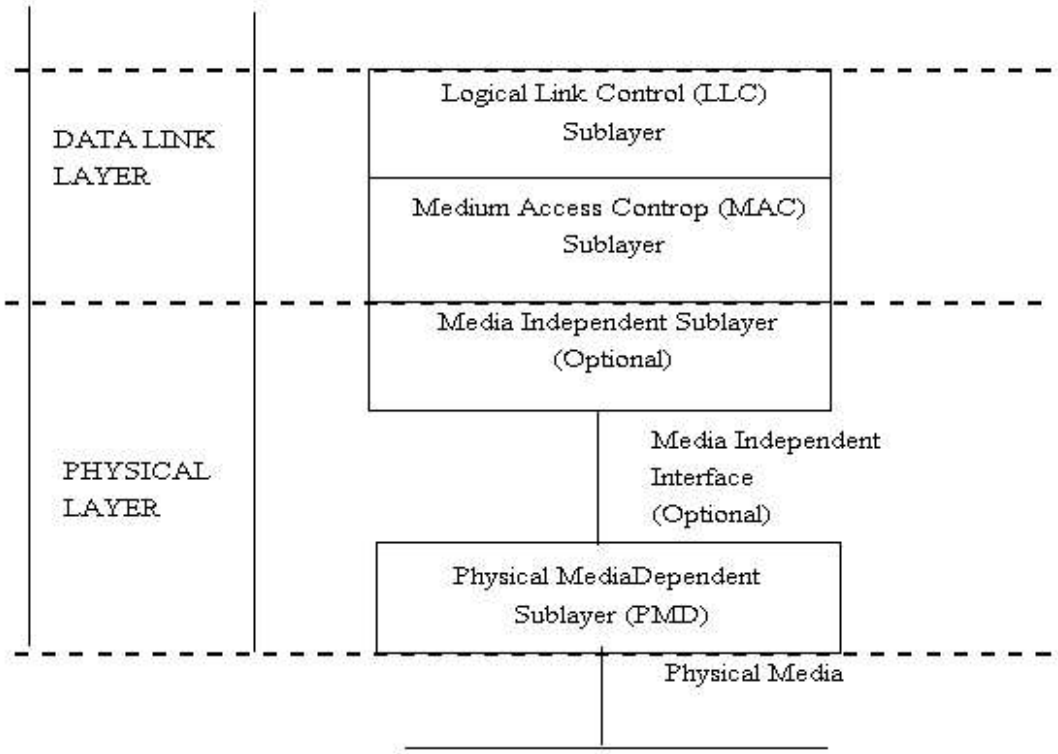


Figure 3-1. Local and Metropolitan Area Network Model

The layers shall be defined in such a way as to be relatively device and application independent. The intent of the Local and Metropolitan Area Network Model is to allow individual protocol and service layers to be replaced as needed without requiring changes in other protocols or service layers used to realize the desired LAN service.

3.2 Applications and Devices

LANs (including IVD LANs) and MANs are intended to be used for commercial, educational, governmental, and industrial applications. The use of these Networks in other environments, while not specifically precluded, is not within the scope of Project 802.

LANs (including IVD LANs) and MANs are intended to support many diverse applications. To this end, these networks, in conjunction with other higher layer protocols, should support applications, processes, and services such as:

a) File Transfer and Access Protocols
b) Graphical Applications

c) Word Processing
d) Electronic Messaging
e) Industrial Automation
f) Remote Data Base Access
g) Digitized Voice Applications

LANs (including IVD LANs) and MANs are intended to support the connection of various data devices, such as:

a) Hosts and Servers
b) Personal Computers and Workstations
c) Mini and Mainframe Computers
d) Mass Storage Devices
e) Printers and Plotters
f) Monitoring and Control Equipment
g) Bridges and Routers to Other Networks

All LANs (including IVD LANs) and MANs shall be capable of supporting digital voice applications when these services are similar to normal digital data traffic (e.g., voice messages, low traffic volume intercom facilities, public address facilities, and limited teleconferencing facilities). In addition, all IVD LAN and MAN networks shall be capable of providing full support of digital voice services (e.g., real-time interactive voice).

NOTE: The lists in this section show typical applications and devices and, as such, are not intended to be exhaustive, nor do they constitute a set of required items.

4.0 STANDARDS DEVELOPMENT CRITERIA

4.1 Broad Market Potential
4.2 Compatibility
4.3 Distinct Identity
4.4 Technical Feasibility
4.5 Economic Feasibility

All projects authorized within the IEEE 802 family of LANs (including IVD LANs) and MANs shall meet the following five criteria.

4.1 Broad Market Potential

A standards project authorized by IEEE 802 shall have a broad market potential. Specifically, it shall have the potential for:

a) Broad sets of applicability.
b) Multiple vendors and numerous users.
c) Balanced costs (LAN versus attached stations).

4.2 Compatibility

IEEE 802 defines a family of standards. **All standards shall be in conformance with IEEE 802.1 Architecture, Management and Interworking.**

All LLC and MAC standards shall be compatible with ISO 10039[20], MAC Service Definition1, at the LLC/MAC boundary. Within the LLC Working Group there shall be one LLC standard, including one or more LLC protocols with a common LLC/MAC interface. Within a MAC Working Group there shall be one MAC standard and one or more Physical Layer standards with a common MAC/Physical layer interface.

Each standard in the IEEE 802 family of standards shall include a definition of managed objects which are compatible with OSI systems management standards.

1. Note: This requirement is subject to final resolution of corrections and revision to current ISO 10039, currently inconsistent with ISO 8802 series standards.

4.3 Distinct Identity

Each IEEE 802 standard shall have a distinct identity. To achieve this, each authorized project shall be:

a) Substantially different from other IEEE 802 standards.
b) One unique solution per problem (not two solutions to a problem).
c) Easy for the document reader to select the relevant specification.

4.4 Technical Feasibility

For a project to be authorized, it shall be able to show its technical feasibility. At a minimum, the proposed project shall show:

a) Demonstrated system feasibility.
b) Proven technology, reasonable testing.
c) Confidence in reliability.

4.5 Economic Feasibility

For a project to be authorized, it shall be able to show economic feasibility (so far as can reasonably be estimated), for its intended applications. At a minimum, the proposed project shall show:

a) Known cost factors, reliable data.
b) Reasonable cost for performance.
c) Consideration of installation costs.

5.0 FUNCTIONAL REQUIREMENTS

5.1 GENERAL FUNCTIONAL REQUIREMENTS
5.2 PHYSICAL LAYER CHARACTERISTICS
5.3 MEDIA ACCESS CONTROL CHARACTERISTICS
5.4 LOGICAL LINK CONTROL CHARACTERISTICS
5.5 INTERWORKING
5.6 ERRORS, FAILURES AND MAINTENANCE

The following functional requirements shall be met, where applicable, by all IEEE 802 standards. These functional requirements are divided into six sections:

a) General Functional Requirements
b) Physical Layer Characteristics
c) Media Access Control Characteristics
d) Logical Link Control Characteristics
e) Interworking
f) Errors, Failures and Maintenance

5.1 GENERAL FUNCTIONAL REQUIREMENTS

5.1.1 Use of Standards
5.1.2 Regulatory Issues
5.1.3 Safety

5.1.4 Use of Proprietary Materials
5.1.5 Components
5.1.6 Use of LSI

The general functional requirements apply to all areas of the standard.

5.1.1 Use of Standards

Where possible and appropriate, LANs (including IVD LANs) and MANs should be defined to comply with existing and, in cognizance of, emerging standards [1] through [7].

5.1.2 Regulatory Issues

Where necessary and appropriate, the LANs (including IVD LANs) and MANs should conform to the mandatory requirements of relevant national and international regulating and licensing agencies. Specifically, LANs (including IVD LANs) and MANs should be designed such that they can operate in installations that comply with standards and codes such as those for commercial building wiring, flammability and emissions.

5.1.3 Safety

LANs (including IVD LANs) and MANs shall be specified in a manner that allows implementations that are consistent with electrical, mechanical, and material safety requirements of the intended user's environment [16], [17], [18].

5.1.4 Use of Proprietary Materials

Any material specified in a LAN (including IVD LAN) or MAN standard must be non-proprietary or must be available on a reasonable and non-discriminatory basis. Due diligence shall be exercised to determine that all material specified in the standard is available on this basis.

5.1.5 Components

Where possible and appropriate, the LAN (including IVD LAN) or MAN should be defined so as to use standard and commercially available, multiple sourced, components.

5.1.6 Use of LSI

Where possible and appropriate, the LAN (including IVD LAN) and MAN standards should permit the use of high volume Large Scale Integration (LSI) circuitry.

5.2 PHYSICAL LAYER CHARACTERISTICS

5.2.1 Data Device Interface
5.2.2 Data Transparency
5.2.3 Data Interchange
5.2.4 Connected Devices
5.2.5 Transmission Rates
5.2.6 Distance
5.2.7 Addition and Removal of Devices
5.2.8 Sharing Network Resources
5.2.9 Lightning and Galvanic Protection

The following physical characteristics describe functional requirements that are unique to the Physical Layer.

5.2.1 Data Device Interface

The data device interface in LANs (including IVD LANs) and MANs should be kept as simple and economical as possible.

5.2.2 Data Transparency

LANs (including IVD LANs) and MANs shall provide for data transparency: that is, the data paths through the network shall be insensitive to unique combinations of the character or bit patterns used by higher layer~~s of the~~ protocols.

5.2.3 Data Interchange

The architecture of the LANs (including IVD LANs) and MANs shall not preclude direct data interchange between any two data devices using the network. It shall be possible to transmit data units between any two data devices on the same LAN without requiring intermediate systems Network Layer routing.

5.2.4 Connected Devices

LANs (including IVD LANs) and MANs shall be capable of supporting at least two hundred (200) connected devices.

5.2.5 Transmission Rates

The transmission rate over LANs (including IVD LANs) and MANs shall be at least one million bits per second.

5.2.6 Distance

LANs (including IVD LANs) shall be capable of supporting segments at least 100 meters in length. LANs (including IVD LANs), composed of segments connected by physical layer interworking devices, shall be capable of operating over a physical medium that is at least 2 Km in length. MANs shall be capable of operating over an area up to 50 Km in diameter.

5.2.7 Addition and Removal of Devices

LANs (including IVD LANs) and MANs shall be designed such that user data devices and medium access units can be easily added or removed. The connection of data devices to, or the disconnection of data devices from, the LAN (including IVD LAN) or MAN shall not introduce a transient fault lasting more than one second.

5.2.8 Sharing Network Resources

When the various nodes of a LAN (including IVD LAN) or MAN have the need to share resources such as media bandwidth, media access, and multiplexed user ports, the network shall provide a mechanism to arbitrate and manage the use of these shared network resources in a manner construed to be "fair" to all network nodes. ~~(~~Fair means that all devices with messages of equal priority shall have equal probability of access to the network.~~)~~

5.2.9 Lightning and Galvanic Protection

LANs (including IVD LANs) and MANs shall provide protection from lightning and galvanic effects for itself, connected data devices, and users.

5.3 MEDIA ACCESS CONTROL CHARACTERISTICS

5.3.1 Multicast and Broadcast
5.3.2 Addressing
5.3.3 Address Administration
5.3.4 Octet Alignment
5.3.5 Bit Ordering

The Media Access Control characteristics describe the functional requirements that are unique to the Media Access Control Sublayer.

5.3.1 Multicast and Broadcast

The address mechanisms of LANs (including IVD LANs) and MANs shall include the capability to simultaneously address a given message to more than one receiving data device, and shall include the capability to simultaneously address a given message to all data devices connected to the LAN (including IVD LAN) or MAN.

5.3.2 Addressing

All MAC standards shall support 48 bit MSAP addresses. A MAC standard may also, but need not, support 16 bit MSAP addresses as mandatory or optional. MANs and IVD LANs may also support additional address formats to provide compatibility with other standards providing that they can be interworked with the 48 bit address format. (Note from translator: 16 bit MSAP addresses have been removed)

5.3.3 Address Administration

For certain classes of service, LANs (including IVD LANs) and MANs shall permit end users to administer part of their address space.

5.3.4 Octet Alignment

The Link Service Data Units (LSDUs) shall be composed of an integral number of octets (the data unit shall be exactly 8*n bits in length, where n is an integer).

5.3.5 Bit Ordering

A consistent bit order (least significant bit first) shall be used .

5.4 LOGICAL LINK CONTROL CHARACTERISTICS

5.4.1 Service Provided
5.4.2 Entity Access
5.4.3 Reserved LSAP Assignment

The Logical Link Control characteristics describe the functional requirements that are unique to the Logical Link Control Sublayer.

5.4.1 Service Provided

LANs (including IVD LANs) and MANs shall provide a service to deliver, with a high probability, data link layer data units to one or more addressed destinations using peer-to-peer communications.

5.4.2 Entity Access

The Logical Link Control Sublayer shall provide Link Service Access Points (LSAPs) to Layer 3 protocols to allow access to:

a) Multiple, alternate Network Layer protocol entities.
b) Management entity.

5.4.3 Reserved LSAP Assignment

The LSAP address space shall be divided into two parts. One part shall be user assignable, the other part shall be reserved for assignment by the standards committee. The rules for assigning the reserved LSAPs shall be as follows:

a) The Network Layer protocol shall be well defined so that devices built to it by different manufacturers can communicate unambiguously.
b) The Network Layer protocol shall have a potentially large usage.
c) The Network Layer protocol shall be publicly available and changed only after public review and notification.
d) The Network Layer protocol shall be a standard or a draft standard by a recognized standards body.
e) The Network Layer protocol shall not already have an assigned LSAP.

5.5 INTERWORKING

5.5.1 Bridging
5.5.2 Interworking with Common Carrier Facilities

Interworking functional requirements include bridging and connection to other networks.

5.5.1 Bridging

A transparent MAC sublayer bridge shall be capable of interconnecting all IEEE 802 LANs (including IVD LANs) and MANs using the same address length.

5.5.2 Interworking with Common Carrier Facilities

LANs (including IVD LANs) and MANs shall be capable of interworking with common carrier facilities.

5.6 ERRORS, FAILURES AND MAINTENANCE

5.6.1 MAC Frame Error Rate
5.6.2 MAC Undetected Error Rate
5.6.3 Hamming Distance
5.6.4 Burst Error Detection
5.6.5 Protection Against Device Failure
5.6.6 Maintenance
5.6.7 Duplicate Address Detection

This section includes the functional requirements concerning errors, failures and maintenance.

5.6.1 MAC Frame Error Rate

The probability that a MAC Protocol Data Unit (MPDU), excluding any preamble, transmitted by one MAC entity is not reported correctly at the PHY service interface of a peer MAC entity, due to operation of the conveying Physical Layer entity, and not due to the normal operation of the MAC protocol, shall be less than 8 * 10-8 per octet of MPDU length (This error rate applies to operation within a single LAN).

5.6.2 MAC Undetected Error Rate

The probability that a MAC Service Data Unit (MSDU) reported at the MAC service boundary contains an undetected error, due to operation of the conveying MAC and Physical Layer entities, shall be less than 5*10-14 per octet of MSDU length.

5.6.3 Hamming Distance

A minimum of four bit cells in error shall be necessary for an undetected error to occur (Hamming distance 4).

5.6.4 Burst Error Detection

~~**The 32 bit CCITT CRC 32 shall be used as a frame check sequence for burst error detection**~~ **In LANs (including IVD LANs) and MANs that do not by other means provide an error detection capability that will insure the MAC Undetected Error Rate probability stated in 5.6.2, the 32 bit CCITT CRC 32 shall be used as a frame check sequence for burst error detection [14].**

5.6.5 Protection Against Device Failure

Each data device connected to a LAN (including IVD LAN) or MAN should be designed such that a single failure in the data device should not cause more than a transient failure of the network as a whole (except as related only to the failed data device). The loss of power to any data device should not cause more than a transient failure of the network as a whole. **LANs (including IVD LANs) and MANs shall be capable of recovering from the effects of such transient failures.** *For the purpose of this document, "transient" is defined as an event that has a duration on the order of one second.*

5.6.6 Maintenance

LANs (including IVD LANs) and MANs should include features that facilitate Network maintenance, diagnostics, and service.

5.6.7 Duplicate Address Detection

The LLC sublayer shall provide one or more mechanisms to detect that two data devices on the same link simultaneously possess the same individual MSAP address. With at least one of these mechanisms, it shall be possible to perform the detection process before both data devices are capable of establishing connections or participating in bi-directional information exchange with other stations.

6.0 ADDITIONAL IVD LAN FUNCTIONAL REQUIREMENTS

In addition to the overall LAN (including IVD LAN) and MAN functional requirements covered in Section 5 of this document, IVD LANs have the following additional functional requirements:

a) Support integrated voice and data services (other forms of digital information transport are not precluded).
b) Support voice traffic within the quality constraints of the RS 464 specification. [19]
c) Provide interconnection between IVD LAN workstations and a wide range of backbones including other IEEE 802 LANs, other backbone networks and PBXs.
d) Allow for the evolution to emerging or existing higher speed LAN backbones.
e) Support, at a minimum, telephone twisted pair (TTP) for wiring.
f) Support both synchronous and asynchronous data.
g) The Physical layer and the MAC sublayer shall not be dependent on the characteristics of the backbone.
h) MAC frame exchange between any two IVD LAN workstations connected to the same access unit shall be independent of any backbone network connected to the access unit.

7.0 ADDITIONAL MAN FUNCTIONAL REQUIREMENTS

7.1 Configuration
7.2 Network Compatibility
7.3 Media
7.4 Interconnection of LANs
7.5 Additional Services
7.6 Network Management

In addition to the overall LAN (including IVD LAN) and MAN functional requirements covered in Section 5 of this document, MANs have the following additional functional requirements:

7.1 Configuration

MANs should be capable of supporting both large and small configurations. They should also be expandable and reconfigurable with a minimum of service disruption.

7.2 Network Compatibility

MANs should be compatible with existing and evolving public network environments. To do this they should be:
a) Capable of using transmission rates and physical wiring schemes that are compatible with public networks.
b) Capable of carrying low and moderate speed telecommunications services.
c) Capable of interworking with public telecommunications networks by allowing reliable support of relevant signalling and addressing information.

7.3 Media

MANs should be capable of using any appropriate media. They should also allow for physical layout flexibility.

7.4 Interconnection of LANs

MANs shall be capable of interconnecting multiple IEEE 802 LANs.

7.5 Additional Services

In addition to supporting LLC and providing isochronous service, MANs shall be capable of supporting a connection oriented data service suitable for compressed video.

7.6 Network Management

MANs should allow for monitoring, network management and access control (remote enable and disable of users). They should also provide for protection against access that attempts to interrupt the network.

7.7 Privacy

MANs shall be configurable such that data transmitted by one customer can be prevented from passing through the premises of other customers.

8.0 SECURITY FUNCTIONAL REQUIREMENTS

LANs (including IVD LANs) and MANs are vulnerable to a variety of security threats. **To assure interoperability while providing security services, IEEE Project 802 shall provide options for:**

a) Secure data exchange for all IEEE 802 networks.
b) Cryptographic key management and distribution.
c) Security management to manage objects securely.

In addition, guidelines shall be provided for:

a) Use of particular cryptographic algorithms as examples of how to implement protocols.
b) Philosophy of key distribution to address manual distribution aspects not included in the protocol.

NOTE: Cryptographic algorithms are not a subject for IEEE 802 standardization.

9.0 CONFORMANCE TESTING

The objective of conformance testing is to provide an indication that tested devices conform to the standard. **Abstract test suites shall be developed as part of the standards development process (ideally, as early as possible in that process, but the completion of the Abstract Test Suite shall not gate the release of the basic standard). Conformance testing shall not be required by the standards body.**

Conformance Test Suites shall meet the following functional requirements:

a) Conformance testing shall not raise market barriers or unduly raise the cost of tested products.
b) The standard shall contain all abstract conformance tests required to validate an implementation of that standard.

c) Tests may be classified by importance and difficulty. The selection of tests run against an implementation shall be the result of agreements between vendors and buyers of these implementations.
d) ISO 9646-2 or its successors shall be utilized wherever applicable (when it reaches full IS status) [9].

References

[1]) ISO 7498-1; 15 Oct. 1987, Information Processing Systems--Open Systems Interconnection--Basic Reference Model
[2] ISO 7498-2; March 1987, Information Processing Systems--Open Systems Interconnection--Part 2: Security Architecture
[3] ISO 7498-3; 1984, Information Processing Systems--Open Systems Interconnection--Part 3: Naming and Addressing
[4] ISO IS 7498-4; 1984, Information Processing Systems--Open Systems Interconnection--Part 4: Management Framework
[5] ISO 7498-1/AD Information Processing Systems--Open Systems Interconnection--Addendum 1: Connectionless Data Transmission
[6] ISO 7498-1/PDAD2 Information Processing Systems--Open Systems Interconnection--Addendum 2: Multi-peer Data Transmission
[7] ISO 7498-1/Cor. 1 Information Processing Systems--Open Systems Interconnection--Technical Corrigendum 1
[8] ISO 9646-1 OSI Conformance Testing Methodology and Framework, Part 1: General Concepts.
[9] ISO 9646-2 OSI Conformance Testing Methodology and Framework, Part 2: Abstract Test Suite Specification
[10] ISO 9646-3 OSI Conformance Testing Methodology and Framework, Part 3: Tree and Tabular Combined Notation
[11] ISO 9646-4 OSI Conformance Testing Methodology and Framework, Part 4: Test Realization
[12] ISO 9646-5 OSI Conformance Testing Methodology and Framework, Part 5: Requirements on Test Laboratories and Their Clients for the Conformance Assessment Process
[13] ISO 9646-6 OSI Conformance Testing Methodology and Framework, Part 6: Test Laboratory Operations
[14] Hammond, J.L., Brown, J.E., and Liu, S.S. Development of a Transmission Error Model and Error Control Model. Technical Report RADC-TR-75-138. Rome Air Development Center (1975).
[15] CISPR Publication 22 (1985), Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment.
[16] IEC Publication 380, Safety of electrically energized office machines.
[17] IEC Publication 435, Safety of data processing equipment.
[18] IEC Publication 950, Safety of Information Technology Equipment, Including Electrical Business Equipment.
[19] EIA/TIA-464-A-1989, Private Branch Exchange (PBX) Switching Equipment for Voiceband Application, Feb. 1989
[20] ISO 10039, Information Processing Systems--Local Area Networks--MAC Service Definition