FAA-HDBK-002
June 27, 1997

U.S Department of Transportation

Federal Aviation Administration

HANDBOOK
Systems Management

AREA DCPS

DISTRIBUTION STATEMENT A Approved for public release; distribution is unlimited

Foreword

This handbook is approved for use by all organizations of the Federal Aviation Administration (FAA). It was created to provide guidance for the uniform implementation of the systems and network management architectures recommended for use within the FAA. It provides the recommendations for ensuring interoperability between commercial off-the-shelf (COTS) system management products provided by vendors. The recommendations contained in this document are based on Open System Interconnection (OSI) management standards issued by the International Organization for Standardization (ISO), as well as requirements based on the internet protocol standard management standards developed by the Internet Engineering Task Force (IETF).

The recommendations contained in this document are applicable to specifying interfaces between FAA systems and network management systems and the systems that they manage.

This handbook is for guidance only; it cannot be cited as a requirement. If it is, the contractor does not have to comply.

CONTENTS

CONTENTS

CONTENTS

CONTENTS

1. SCOPE

1.1 Scope. This document provides the guidance necessary for implementing an open systems management capability within the FAA to support management of the Agency's automation, communication, navigation, surveillance, weather, and environmental systems. The document provides recommendations for implementing open systems management using the OSI management standards and the Internet Protocol Suite (IPS) management standards. Guidance also is provided to facilitate the use of the management standards in the Aeronuatical Telecommunications Network (ATN) environment.
This handbook is for guidance only; it cannot be cited as a requirement. If it is, the contractor does not have to comply.

1.2 Purpose. This document is a guide for selecting a systems management architecture to enable management of FAA systems. It also provides guidance for ensuring interoperability when procuring standards-based COTS systems management products (i.e. management system, agent, proxy agent).

2. APPLICABLE DOCUMENTS

2.1 General. The documents listed below are needed to fully understand the information provided by this handbook. They not necessarily all the documents referenced herein.

2.2 Government documents.
FAA STANDARDS

Document Number	Document Name	Mgmt. Std.
FAA-STD-039b:1996	Open Systems Architecture and Protocols	CMIP
FAA-STD-042a:1994	NAS Open System Interconnection Naming and Addressing	CMIP
FAA-STD-043b:1996	NAS Open System Interconnection Priority	CMIP
FAA-STD-045:1994	Open Systems Interconnection Security Architecture, Protocols, and Mechanisms	CMIP
ENET1370-001.1:1995	FAA Enterprise Network Naming and Addressing Standard	SNMPv1, SNMPv2

2.3 Non-goverment documents.
International Civil Aviation Organization (ICAO)

Document Number	Document Name	Mgmt. Std.
Draft ATN SARPs:1995	Draft Aeronautical Telecommunication Network (ATN) Standards and Recommended Practices (SARPs) and Guidance Material, Version 1.0	CMIP

Internet Engineering Task Force, Request for Comment

Document Number	Document Name	Mgmt. Std.
IETF RFC 791:1981	Darpa Internet Program Protocol Specification - Internet Protocol	SNMPv1 SNMPv2
IETF RFC 792:1981	Internet Control Message Protocol	SNMPv1 SNMPv2
IETF RFC 768:1980	User Datagram Protocol (UDP)	SNMPv1 SNMPv2
IETF RFC 1155:1990	Structure and Identification of Management Information for TCP/IP-Based Internets	SNMPv1
IETF RFC 1157:1990	A Simple Network Management Protocol (SNMP)	SNMPv1
IETF RFC 1212:1991	Concise MIB Definitions	SNMPv1

IETF RFC 1213:1991	Management Information Base for Network Management of TCP/IP-Based Internets: MIB-II	SNMPv1 SNMPv2
IETF RFC 1230:1991	IEEE 802.4 Token Bus MIB	SNMPv1
IETF RFC 1231:1991	IEEE 802.5 Token Ring MIB	SNMPv1
IETF RFC 1271:1991	Remote Network Monitoring MIB	SNMPv1
IETF RFC 1381:1992	SNMP MIB Extension for X.25 LAPB	SNMPv1
IETF RFC 1382:1992	SNMP MIB Extension for the X.25 Packet Layer	SNMPv1
IETF RFC 1442:1993	Structure of Management Information for Version 2 of the Simple Network Management Protocol	SNMPv2
IETF RFC 1443:1993	Textual Conventions for Version 2 of the Simple Network Management Protocol	SNMPv2
IETF RFC 1448:1993	Protocol Operations for Version 2 of the Simple Network Management Protocol	SNMPv2
IETF RFC 1451:1993	Manager-to-Manager MIB	SNMPv2
IETF RFC 1471:1993	The Definitions of Managed Objects for the Link Control Protocol of the Point to Point Protocol	SNMPv1
IETF RFC 1512:1993	FDDI Management Information Base	SNMPv1
IETF RFC 1643:1994	Definitions of Managed Objects for the Ethernet-like Interface Types	SNMPv2
IETF RFC 1650:1994	Definitions of Managed Objects for Ethernet-like Interface Types using SMIv2	SNMPv2
IETF RFC 1661:1994	The Point-to-Point Protocol (PPP)	SNMPv1
IETF RFC 1748:1994	IEEE 802.5 MIB using SMIv2	SNMPv2
IETF RFC 1757:1995	Remote Network Monitoring MIB	SNMPv1

International Organization for Standardization (ISO)

Document Number	Document Name	Mgmt. Std.
ISO 7498-4:1984	Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 4: Management Framework	OSI, SNMPv1, SNMPv2
ISO/IEC 8073:1992	Information Technology – Telecommunications and Information Exchange Between Systems – Open Systems Interconnection – Protocol for Providing the Connection-Mode Transport Service	CMIP
ISO 8326:1987	Information Processing Systems – Open Systems Interconnection – Basic Connection Oriented Session Service Definition	CMIP
ISO 8327:1987	Information Processing Systems – Open Systems Interconnection – Basic Connection Oriented Session Protocol Specification	CMIP
ISO 8327 DAM 2:1988	Information Processing Systems – Open Systems Interconnection – Basic Connection Oriented Session Protocol Specification – Addendum 2: Incorporation of Unlimited User Data	CMIP
ISO 8348:1988	Information Technology – Open Systems Interconnection – Network Service Definition	CMIP
ISO 8473:1988	Information Processing Systems – Protocol for Providing the Connectionless-mode Network Service	CMIP
ISO 8649:1988	Information Processing Systems Open Systems Interconnection – Service Definition for the Association Control Service Element	CMIP
ISO 8650:1988	Information Processing Systems – Open Systems Interconnection – Protocol Specification for Association Control Service Element	CMIP

ISO/IEC 8802-2:1990	Information Processing Systems – Local Area Networks – Part 2: Logical Link Control, 1st Edition	CMIP, SNMPv1, SNMPv2
ISO/IEC 8802-3:1990	Information Processing Systems – Local Area Networks – Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specification, 2nd Edition	CMIP, SNMPv1, SNMPv2
ISO/IEC 8802-4:1990	Information Processing Systems – Local Area Networks – Part 4: Token-Passing Bus Access Method and Physical Layer Specification, 1st Edition	CMIP, SNMPv1, SNMPv2
ISO/IEC 8802-5:1990	Information Processing Systems – Local Area Networks – Part 5: Token-Passing Ring Access Method and Physical Layer Specification, 1st Edition	CMIP, SNMPv1, SNMPv2
ISO 8822:1988	Information Processing Systems – Connection Oriented Presentation Service Definition	CMIP
ISO 8823:1988	Information Processing Systems – Connection Oriented Presentation Protocol Specification	CMIP
ISO 8824:1987	Information Processing Systems – Open Systems Interconnection – Specifications of Abstract Syntax Notation one (ASN.1)	CMIP, SNMPv1, SNMPv2
ISO 8825:1987	Information Processing Systems – Open Systems Interconnection – Specifications of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)	CMIP, SNMPv1, SNMPv2
ISO/IEC 9072-1:1989	Information Processing Systems – Text Communication – Remote Operations – Part 1: Model, Notation and Service Definition	CMIP
ISO/IEC 9072-2:1989	Information Processing Systems – Text Communication – Remote Operations – Part 2: Protocol Specification	CMIP
ISO 9314-1:1989	Information Processing Systems – Fibre Distributed Data Interface (FDDI) – Part 1: Physical Layer Protocol	CMIP, SNMPv1, SNMPv2
ISO 9314-2:1989	Information Processing Systems – Fibre Distributed Data Interface (FDDI) – Part 2: Token Ring Media Access Control (MAC)	CMIP, SNMPv1, SNMPv2

ISO/IEC 9542:1988	Information Technology - End System to Intermediate System Routing Information Exchange Protocol for Use in Conjunction with the Protocol for Providing the Connectionless-mode Network Service	CMIP
ISO/IEC 9595:1991	Information Technology - Open Systems Interconnection - Common Management Information Service Definition	CMIP
ISO/IEC 9596-1:1991	Information Technology - Open Systems Interconnection - Common Management Information Protocol - Part 1: Specification	CMIP
ISO/IEC 10040:1991	Information Technology Open Systems Interconnection - System Management Overview	CMIP
ISO/IEC 10164-1:1993	Information Technology - Open Systems Interconnection - Systems Management - Part 1: Object Management Function	CMIP
ISO/IEC 10164-2:1993	Information Technology - Open Systems Interconnection - Systems Management - Part 2: State Management Function	CMIP
ISO/IEC 10164-3:1993	Information Technology - Open Systems Interconnection - Systems Management - Part 3: Attributes for Representing Relationships	CMIP
ISO/IEC 10164-4:1993	Information Technology - Open Systems Interconnection - Systems Management - Part 4: Alarm Reporting Function	CMIP
ISO/IEC 10164-5:1993	Information Technology - Open Systems Interconnection - Systems Management - Part 5: Event Reporting Management Function	CMIP
ISO/IEC 10164-6:1993	Information Technology - Open Systems Interconnection - Systems Management - Part 6: Log Control Function	CMIP
ISO/IEC 10164-7:1993	Information Technology - Open Systems Interconnection - Systems Management - Part 7: Security Alarm Reporting Function	CMIP
ISO/IEC 10164-8:1993	Information Technology - Open Systems Interconnection - Systems Management - Part 8: Security Alarm Trail Function	CMIP

ISO/IEC 10164-9:1993	Information Technology - Open Systems Interconnection - Systems Management - Part 9: Objects and Attributes for Access Control	CMIP
ISO/IEC 10164-10:1993	Information Technology - Open Systems Interconnection - Systems Management - Part 10: Accounting Metering Function	CMIP
ISO/IEC 10164-11:1992	Information Technology - Open Systems Interconnection - Systems Management - Part 11: Workload Monitoring Function	CMIP
ISO/IEC 10164-12:1992	Information Technology - Open Systems Interconnection - Systems Management - Part 10: Test Management Function	CMIP
ISO/IEC 10164-13:1992	Information Technology Open Systems Intereonnection - Systems Management - Part 13: Summarization Function	CMIP
		Mgmt. Std.
ISO/IEC 10165-1:1991	Information Technology - Structure of Management Information - Part 1: Management Information Model	CMIP
ISO/IEC 10165-2:1991	Information Technology - Open Systems Interconnection - Structure of Management Information - Part 2: Definition of Management Information	CMIP
ISO/IEC 10165-4:1992	Information Technology - Open Systems Interconnection - Structure of Management Information - Part 4: Guidelines for the Definition of Managed Objects	CMIP
ISO/IEC 10742:1993	Information Technology Telecommunications and Information Exchange Between System - Elements of Management Information Related to OSI Network Layer Standards	CMIP
ISO/IEC 10733:1993	Information Technology - Telecommunications and Information Exchange Between System - Elements of Management Information Related to OSI Data Link Layer Standards	CMIP

ISO/IEC 10737:1993	Information Technology - Telecommunications and Information Exchange Between Systems - Elements of Management Information Related to OSI Transport Layer Standards	CMIP
ISO/IEC 10747:1992	Information Technology - Telecommunications and Information Exchange Between Systems - Protocol for Exchange of Inter-Domain Routing Information Among Intermediate Systems to Support Forwarding of ISO 8473 PDUs	CMIP
ISO/IEC DISP 11183-1:1991	Information Technology - International Standardised Profiles AOMnn OSI Management - Management Communication Protocols - Part 1: specification of ACSE, Presentation of ACSE, Presentation and Session Protocols for the Use by ROSE and CMISE	CMIP
ISO/IEC DISP 11183-2:1991	Information Technology - International Standardised Profiles AOMnn OSI Management - Management Communication Protocols - Part 2: AOM12 - Enhanced Management Communications	CMIP

International Telecommunications Union - Telecommunications

Document Number	Document Name	Mgmt. Std.
ITU-T Recommendation X.215bis (1995)	Open Systems Interconnection - Service Definition for Session Layer Efficiency Enhancements	CMIP
ITU-T Recommendation X.216bis (1995)	Open Systems Interconnection - Service Definition for Presentation Layer Efficiency Enhancements	CMIP
ITU-T Recommendation X.225bis (1995)	Open Systems Interconnection - Protocol Specification for Session Layer Efficiency Enhancements	CMIP
ITU-T Recommendation X.226bis (1995)	Open Systems Interconnection - Protocol Specification for Presentation Layer Efficiency Enhancements	CMIP

3. DEFINITIONS

3.1 Acronyms. The acronyms used in this handbook are defined as follows:

ACF	Access Control Function
ACSE	Association Control Service Element
AMF	Accounting Meter Function
ARF	Alarm Reporting Function
ARR	Attributes for Representing Relationships
ASE	Application Service Element
ATN	Aeronautical Telecommunications Network
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CMISE	Common Management Information Service Element
CMIP	Common Management Information Service Protocol
COTS	Commercial off-the-Shelf
DMI	Definition of Management Information
ERF	Event Reporting Function
ES-IS	End System to Intermediate System
FAA	Federal Aviation Administration
FDDI	Fibre Distributed Data Interface
GDMO	Guidelines for the Definition of Managed Objects
ICMP	Internet Control Message Protocol
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPS	Internet Protocol Suite
ISO	International Organization for Standardization
ITU-T	International Telecommunications Union - Telecommunications
LCF	Log Control Function

MIB	Management Information Base
MO	Managed Object
NAS	National Airspace System
OMF	Object Management Function
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
RFC	Request for Comment
RO	Remote Operations
ROSE	Remote Operation Service Element
SARF	Security Alarm Reporting Function
SARPs	Standards And Recommended Practices
SATF	Security Audit Trail Function
SF	Summarization Function
SMAP	System Management Application Process
SMASE	System Management Application Service Element
SMF	System Management Function
SMFA	System Management Functional Area
SNMP	Simple Network Management Protocol
STMF	State Management Function
TCP	Transmission Control Protocol
TMF	Test Management Function
UDP	User Datagram Protocol
WMF	Workload Monitoring Function

3.2 Agent. Entity capable of performing management operations on managed objects and emitting notifications on their behalf.

3.3 Attribute. A property of a managed object.

3.4 Managed object. Resources that may be managed through the use of management protocols.

3.5 Managed system. System whose resources are managed by a management system.

3.6 Management system. System that manages the resources of other systems.

3.7 Manager. Entity capable of issuing management operations and receiving notifications.

3.8 Proxy agent. Entity capable of providing interface conversion with a nonstandard agent to perform management operations on managed objects and emit notifications on behalf of managed objects.

4. GENERAL RECOMMENDATIONS

4.1 General. COTS systems management platforms implementing the following management architectures should be in accordance with the applicable industry or international standards as specified in this document. Detailed recommendations are provided in Section 5 as follows:

OSI systems management	Section 5.1
IPS systems management - SNMPv1	Section 5.2
IPS systems management - SNMPv2	Section 5.3

4.1.1 System management application support. Management systems provide manager-to-agent, manager-to-manager, and agent application processes. The FAA management system should, at a minimum, provide a "manager" application process. It also should enable communication between management systems and support an "agent" application process.

The management system should manage the managed system by communicating with the agent application process, which may be embedded or external to the managed system, see Figure 1.

A proxy agent should be provided for managed systems whose agent management interfaces are incompatible with the management system.

The management system should provide both systems and network management capabilities. The management system application support should be provided in the following functional areas, in accordance with ISO 7498-4:

Configuration management
Fault management
Performance management
Security management
Accounting management.

At a minimum, system management applications should be provided as follows:

4.1.1.1 Configuration management. Configuration management applications should be provided to:

Associate names with managed objects and sets of managed objects
Activate and close down managed objects
Collect data on the managed object state on a routine basis
Obtain notification of managed objects state changes.

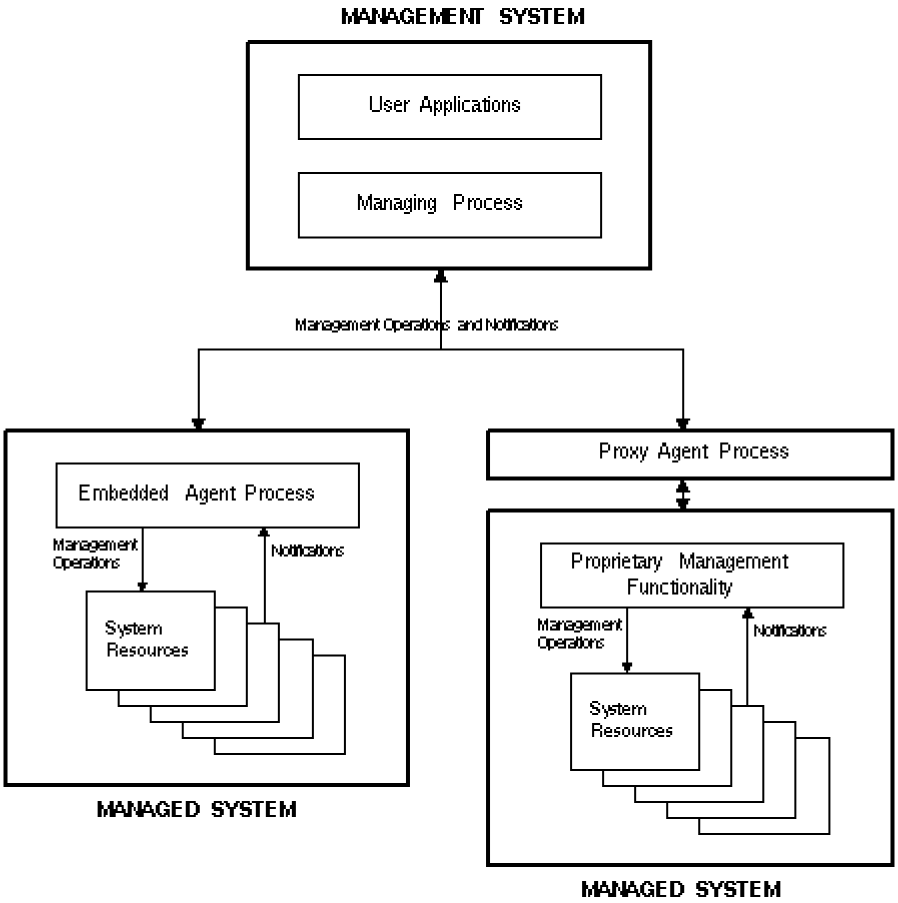


Figure 1. Management/agent interface

4.1.1.2 Fault management. Fault management applications should be provided to:
Maintain and examine error logs
Accept and act upon error detection notifications
Trace faults
Coordinate diagnostic tests
Correct faults.

4.1.1.3 Performance management. Performance management applications should be provided to:
Maintain and examine performance logs
Obtain performance parameters
Determine quality of service
Measure quality of service with pre-determined performance objectives.

4.1.1.4 Security management. Security management applications should be provided to:
Maintain and examine security logs
Control and maintain authorization network and system security
Support authentication control management
Support access control management.

4.1.1.5 Accounting management. Accounting management applications should be provided to:
Maintain and examine accounting logs
Obtain accounting information of managed resources
Obtain accounting information on personnel or resource-related activities related to managed-resources
Inform users of costs incurred or resources consumed
Enable costs to be combined where multiple managed resources are used to achieve a given service objective.

4.1.2 Systems management communications architecture. The management system may support one or more system management protocol architectures. The OSI Common Management Information Protocol (CMIP), Simple Network Management Protocol Version 1 (SNMPv1), or SNMPv2-based systems management architecture should be used when required.
The FAA intends to minimize the number of interfaces through standardization. Therefore, this document does not provide for management protocols in the variety of possible protocol stack configurations. Other configurations will be provided on an as-needed basis and documented in the associated interface requirements document.

4.1.3 Managed objects. The management system should provide a management information base (MIB) that contains standard managed object (MO) definitions. The MIB should provide support for FAA or vendor-defined MO definitions. Abstract Syntax Notation One (ASN.1), defined in ISO 8824:1987 and ISO 8825:1987 should be used to represent MO data types.

5. DETAILED RECOMMENDATIONS

5.1 OSI systems management. OSI Management should be provided in accordance with ISO 7498-4, Basic Reference Model - Part 4: Management Framework, ISO/IEC 10040:1991 System Management Overview, and the ATN Standards and Recommended Practices (SARPs). This section provides recommendations necessary for providing OSI system management functions (SMF), protocols, and managed objects.

5.1.1 Systems management applications support. System management capability should be provided in five system management functional areas (SMFA): configuration management, fault management, performance management, security management, and accounting management. System management application processes (SMAP) should use ISO defined SMFs to enable the desired management capability when applicable.

5.1.1.1 System management functions. System management application service elements (SMASE) are application service elements that provide system management functions or services to the SMAP. Many SMASEs are currently in various stages of development. Therefore, the management system should provide the capability to support additional SMASEs when they become commercially available.
At a minimum, the management system should provide SMASEs implementing the following SMFs:

Object Management Function: ISO/IEC 10164-1
State Management Function: ISO/IEC 10164-2
Attributes for Representing Relationships: ISO/IEC 10164-3
Alarm Reporting Function: ISO/IEC 10164-4
Event Reporting Function: ISO/IEC 10164-5
Log Control Function: ISO/IEC 10164-6.

The management system should have the capability to add additional SMFs, which include the following, when applicable and available:

Security Alarm Reporting Function: ISO/IEC 10164-7
Security Audit Trail Function: ISO/IEC 10164-8
Objects and Attributes for Access Control: ISO/IEC 10164-9
Accounting Metering Function: ISO/IEC 10164-10
Workload Monitoring Function: ISO/IEC 10164-11
Test Management Function: ISO/IEC 10164-12
Summarization Function: ISO/IEC 10164-13.

5.1.1.1.1 Object management functions. The object management functions (OMF) enables the manager SMAP to request the creation, deletion, examination, and modification of objects managed by the agent SMAP. The OMF also enables the manager SMAP to be notified of managed object creation, deletion, and modifications from the agent SMAP. The OMF should be implemented in accordance with ISO/IEC 10164-1.

5.1.1.1.1.1 Manager SMASE. The manager SMASE should implement the following specific object management notification services on behalf of the manager SMAP, in accordance with ISO/IEC 10164-1:

Reporting creation and deletion of managed objects
Reporting name changes of managed objects
Reporting changes to attribute values of managed objects.

The manager SMASE should implement the following object management pass-through services on behalf of the manager SMAP, in accordance with ISO/IEC 10164-1:

Creation and deletion of managed objects
Performing actions upon managed objects
Attribute changing
Attribute reading
Event reporting.

5.1.1.1.1.2 Agent SMASE. The agent SMASE should implement the following specific object management notification services on behalf of the agent SMAP, in accordance with ISO/IEC 10164-1:

Reporting creation and deletion of managed objects
Reporting name changes of managed objects
Reporting changes to attribute values of managed objects.

The agent SMASE should implement the following object management pass-through services on behalf of the agent SMAP, in accordance with ISO/IEC 10164-1:

Creating and deleting managed objects
Performing actions upon managed objects
Attribute changing
Attribute reading
Event reporting.

5.1.1.1.2 State management function. The state management function (STMF) SMASE enables the manager SMAP to examine and be notified of the changes in state, to monitor overall operability and usage of resources in a consistent manner, and to control the general availability of specific resources managed by the agent SMAP. The STMF should be implemented in accordance with ISO/IEC 10164-2.

5.1.1.1.2.1 Manager SMASE. The manager SMASE should implement the state change reporting service on behalf of the manager SMAP, in accordance with ISO/IEC 10164-2.
The manager SMASE should implement the following pass-through services on behalf of the manager SMAP, in accordance with ISO/IEC 10164-1:

Attribute changing
Attribute reading.

5.1.1.1.2.2 Agent SMASE. The agent SMASE should implement the state change reporting service in accordance with ISO/IEC 10164-2.
The agent SMASE should implement the following pass-through services on behalf of the agent SMAP, in accordance with ISO/IEC 10164-1:

Attribute changing
Attribute reading.

5.1.1.1.3 Attributes for representing relationships. The attributes for representing relationships (ARR) SMF enables the manager SMAP to examine the relationship among various parts of the system to determine the interdependency of operations. The ARR SMFs also enables the manager SMAP to change relationships and be notified by agent SMAP of such changes when they occur due to other causes. The ARR SMF should be implemented in accordance with ISO/IEC 10164-3.

5.1.1.1.3.1 Manager SMASE. The manager SMASE should implement the relationship change reporting service on behalf of the manager SMAP, in accordance with ISO/IEC 10164-3.
The manger SMASE should implement the following pass-through services on behalf of the manager SMAP, in accordance with ISO/IEC 10164-3:

Attribute changing
Attribute reading.

5.1.1.1.3.2 Agent SMASE. The agent SMASE should implement the relationship change reporting service on behalf of the agent SMAP, in accordance with ISO/IEC 10164-3.
The agent SMASE should implement the following pass-through services on behalf of the agent SMAP, in accordance with ISO/IEC 10164-3:

Attribute changing
Attribute reading.

5.1.1.1.4 Alarm reporting function. The alarm reporting function (ARF) enables the manager SMAP to receive reports of alarms, errors, and related information in a standard fashion from the agent SMAP. The ARF should be implemented in accordance with ISO/IEC 10164-4.

5.1.1.1.4.1 Manager SMASE. The manager SMASE should implement the alarm reporting service on behalf of the manager SMAP, in accordance with ISO/IEC 10164-4.

5.1.1.1.4.2 Agent SMASE. The agent SMASE should implement the alarm reporting service on behalf of the agent SMAP, in accordance with ISO/IEC 10164-4.

5.1.1.1.5 Event reporting function. The event reporting functions (ERF) enables the manager SMAP to control the type, transmission, and destination of event reports received from the agent SMAP.
The ERF should be implemented in accordance with ISO/IEC 10164-5.

5.1.1.1.5.1 Manager SMASE. The manager SMASE should implement the following event report management services on behalf of the manager SMAP, in accordance with ISO/IEC 10164-5:

Initiation of event forwarding
Termination of event forwarding
Suspension of event forwarding
Resumption of event forwarding
Modification of event forwarding
Retrieval forwarding.

5.1.1.1.5.2 Agent SMASE. The agent SMASE should implement the following event report management services on behalf of the agent SMAP, in accordance with ISO/IEC 10164-5:

Initiation of event forwarding
Termination of event forwarding
Suspension of event forwarding
Resumption of event forwarding
Modification of event forwarding
Retrieval forwarding.

5.1.1.1.6 Log control function. The log control function (LCF) enables the manager SMAP to preserve information events that have occurred or operations that may have been performed on various objects managed by the agent SMAP. Sufficient resources to accommodate logs of these records should be provided for storage of this information.
The LCF should be implemented in accordance with ISO/IEC 10164-6.

5.1.1.1.6.1 Manager SMASE. The manager SMASE should provide the following services on behalf of the manager SMAP, in accordance with ISO/IEC 10164-6:

Creation of a log
Deletion of a log
Modification of log attributes
Suspension and termination of log activity
Deletion and retrieval of log records
Initiation and resumption of log activity.

5.1.1.1.6.2 Agent SMASE. The agent SMASE should provide the following services on behalf of the agent SMAP, in accordance with ISO/IEC 10164-6:

Creation of a log
Deletion of a log
Modification of log attributes
Suspension and termination of log activity

Deletion and retrieval of log records
Initiation and resumption of log activity.

5.1.1.1.7 Security alarm reporting function. The security alarm reporting function (SARF) enables the manager SMAP to:

Receive notifications of security-related events and any malfunction of security services and mechanisms
Receive notification from the agent SMAP of attacks and breaches of system security
Receive notification from the agent SMAP of the perceived severity of any failed operation attack, or breach of security.

The SARF should be implemented in accordance with ISO/IEC 10164-7.

5.1.1.1.7.1 Manager SMASE. The manager SMASE should implement the security alarm notification service on behalf of the manager SMAP, in accordance with ISO/IEC 10164-7.

5.1.1.1.7.2 Agent SMASE. The agent SMASE should implement the security alarm notification service on behalf of the agent SMAP, in accordance with ISO/IEC 10164-7.

5.1.1.1.8 Security audit trail function. The security audit trail function (SATF) enables the manager SMAP to record a security audit trail log of security-related events that occur in the management domain. The SATF should be provided in accordance with ISO/IEC 10164-8.

5.1.1.1.9 Objects and attributes for access control. Objects and attributes for access control enable the manager SMAP to:

Prevent unauthorized establishment of management associations
Protect management information from unauthorized creation, deletion, modification, or disclosure by means of management operations
Prevent an unauthorized initiator from using management operations
Prevent management information from being transmitted to unauthorized recipients by means of confirmed and non-confirmed event reports.

Multiple levels of access control should be provided (e.g., read only access as opposed to read/write). Objects and attributes, provided in accordance with ISO/IEC 10164-9, should be used to develop the access control function.

5.1.1.1.9.1 Manager SMASE. The manager SMASE should implement an access control function (ACF) for establishing management associations. The managed object classes for access control defined in ISO/IEC 10164-9 and ISO/IEC 10165-2 should be supported.

5.1.1.1.9.2 Agent SMASE. The agent SMASE should implement an ACF for establishing management associations. The managed object classes for access control, as defined in ISO/IEC 10164-9 and ISO/IEC 10165-2, should be supported.

5.1.1.1.10 Accounting meter function. The accounting meter functions (AMF) defines accounting meters and logs. It also provides services for retrieving, reporting, and recording resource usage data and for selecting which usage data are to be collected and under what conditions they are to be reported. The AMF should be provided in accordance with ISO/IEC 10164-10.

5.1.1.1.11 Workload monitoring function (WMF). The WMF enables the manager SMAP to monitor the attributes of managed objects to determine system performance. It should define managed objects that can report events based on the values of counters and gauges that reflect system performance. The WMF should be provided in accordance with ISO/IEC 10164-11.

5.1.1.1.11.1 Manager SMASE. The manager SMASE should provide the following WMF services on behalf of the manager SMAP, in accordance with ISO/IEC 10164-11:

Initiation of workload monitoring
Termination of workload monitoring
Suspension of workload monitoring
Resumption of workload monitoring
Modification of workload monitoring.

5.1.1.1.11.2 Agent SMASE. The agent SMASE should provide the following WMF services on behalf of the agent SMAP, in accordance with ISO/IEC 10164-11:

Initiation of workload monitoring
Termination of workload monitoring
Suspension of workload monitoring
Resumption of workload monitoring
Modification of workload monitoring.

5.1.1.1.12 Test management function (TMF). The TMF provides managed object classes to enable the manager SMAP to control confidence and diagnostic test procedures, which may be conducted either interactively or asynchronously, with the results to be reported later.
The TMF should be provided in accordance with ISO/IEC 10164-12.

5.1.1.1.12.1 Manager SMASE. The manager SMASE should provide the following pass-through services on behalf of the manager SMAP, in accordance with ISO/IEC 10164-12:

Retrieve test-object attributes
Modify test-object attributes
Delete test-objects.

5.1.1.1.12.2 Agent SMASE. The agent SMASE should provide the following pass-through services on behalf of the agent SMAP, in accordance with ISO/IEC 10164-12:

Retrieve test-object attributes
Modify test-object attributes
Delete test-objects.

The agent SMASE should provide the following specific services on behalf of the agent SMAP:

Test request asynchronous service
Test request synchronous service
Test suspend/resume service
Test termination service
Schedule-conflict service.

5.1.1.1.13 Summarization function. The summarization function (SF) provides model and managed object classes used to summarize and apply statistical analysis to management information. The SF should be provided in accordance with ISO/IEC 10164-13.

5.1.1.1.13.1 Manager SMASE. The manager SMASE should provide the following pass-through services on behalf of the manager SMAP, in accordance with ISO/IEC 10164-1:

Create summarization object
Delete summarization object
Modify summarization object.

The manager SMASE should implement the following specific services on behalf of the manager SMAP, in accordance with ISO/IEC 10164-13:

Scan report service to report the values of scanned attributes
Statistical report service to report scanned attributes statistics
Buffered scan report service to report scanned attributes over a specified period

Dynamic scan report service to request the observance of specified attributes and return the results.

5.1.1.1.13.2 Agent SMASE. The agent SMASE should implement the following pass-through services on behalf of the agent SMAP, in accordance with ISO/IEC 10164-1:

Create summarization object
Delete summarization object
Modify summarization object.

The agent SMASE should implement the following specific services on behalf of the agent SMAP, in accordance with ISO/IEC 10164-13:

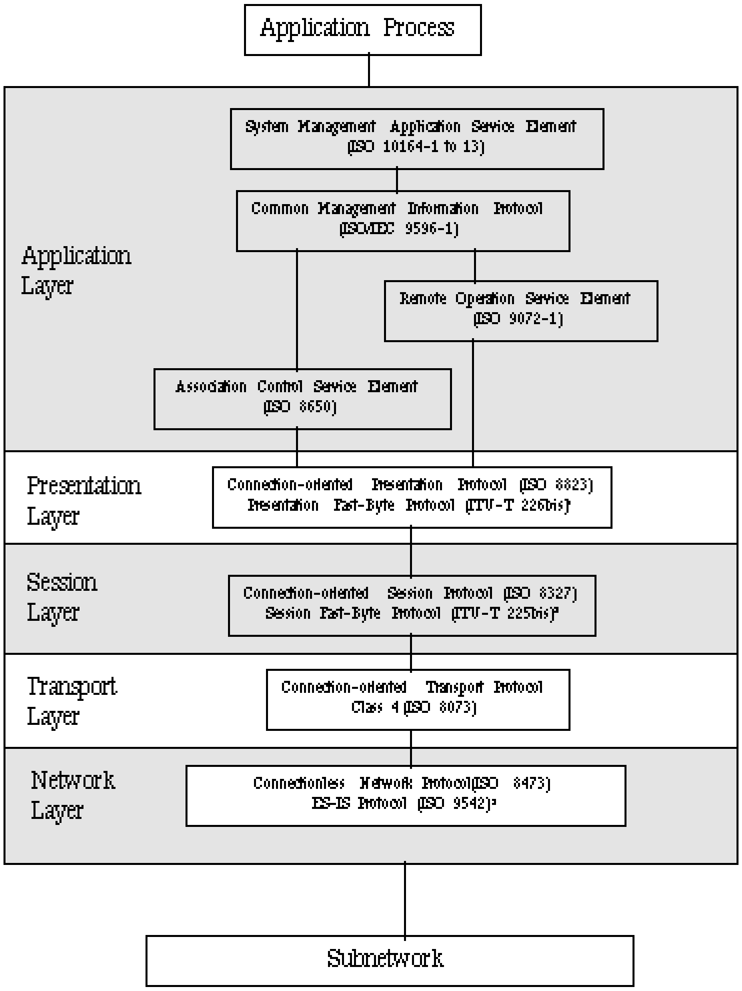
Scan report service to report the values of scanned attributes
Statistical report service to report scanned attributes statistics
Buffered scan report service to report scanned attributes over a specified period
Dynamic scan report service to request the observance of specified attributes and return the results.

5.1.2 Systems management communications architecture. The OSI and ATN systems management protocol architecture should be as specified in Figure 2.

OSI naming and addressing should be provided in accordance with FAA-STD-042a. OSI message priority should be provided in accordance with FAA-STD-043b. OSI security should be provided, when applicable, in accordance with FAA-STD-045.

5.1.2.1 Applications layer services. Application layer services should be provided by the following application service elements (ASE):

SMASE
Common Management Information Service Element (CMISE)


Application Process
System Management Application Service Element (ISO 10164-1 to 13)
Common Management Information Protocol (ISO/IEC 9596-1)
Application Layer
Remote Operation Service Element (ISO 9072-1)
Association Control Service Element (ISO 8650)
Presentation Layer
Connection-oriented Presentation Protocol (ISO 8823)
Presentation Fast-Byte Protocol (ITU-T 226bis)[1]
Session Layer
Connection-oriented Session Protocol (ISO 8327)
Session Fast-Byte Protocol (ITU-T 225bis)[2]
Transport Layer
Connection-oriented Transport Protocol Class 4 (ISO 8073)
Network Layer
Connectionless Network Protocol(ISO 8473)
ES-IS Protocol (ISO 9542)[3]
Subnetwork

[1] ATN presentation layer efficiency enhancement

[2] ATN session layer efficiency enhancement

[3] Required when connecting via a router subnetworks

Figure 2. OSI/ATN systems management architecture

Remote operations service element (ROSE)
Association control service element (ACSE).

5.1.2.1.1 Systems management applications service element. SMASE should be used to enable the transfer of information received from the SMAP. The following services should be provided to the SMAP, in accordance with ISO/IEC 10164-(1-13):

PT-GET
PT-SET
PT-ACTION
PT-CREATE
PT-DELETE
PT-CANCEL-GET
PT-EVENT-REPORT.

SMASE services should be mapped to CMISE services in accordance with ISO/IEC 10164 (1 13).

5.1.2.1.2 Common management information service element. CMISE should be used to enable the transfer of management information received from the SMASE. The CMISE services should be mapped to the ROSE remote operations (RO)-Invoke service, as defined in ISO 9072 1. The following CMISE services should be provided to the SMASE in accordance with ISO/IEC 9595:

M-GET
M-EVENT-REPORT
M-SET
M-ACTION
M-CREATE
M-CANCEL-GET
M-DELETE.

5.1.2.1.2.1 CMISE functional units. The following CMISE functional units should be provided as specified in DISP 11183-2: International Standardized Profiles AOMnn OSI Management - Management Communications Protocols - Part 2: AOM12 - Enhance Management Communications:

Kernel - include all of the CMIS services defined in Paragraph 5.1.2.1.2 with the exception of the M-CANCEL-GET service.

CANCEL-GET - enables use of the M-CANCEL-GET service.

Filter - enable use of the filter parameter in the services provided by the Kernel functional unit.

Multiple object selection - enable use of the scope and synchronization parameters in the services provided by the Kernel functional unit. The scope parameter allows one or more managed objects to be selected based on a sub-tree within the managed object containment hierarchy. The synchronization parameter indicates how the CMISE service user requires the requested operation to be synchronized across the selected object instances. If the Multiple Object Selection functional unit is selected for use on a given association, then the Multiple Reply functional unit must also be selected.

Multiple reply - enable use of the "linked identification" parameter in the services provided by the Kernel functional unit, and allow more than one response to be generated for a given management operation if the invoking CMISE user selects multiple managed objects or requests an M-ACTION operation for a single managed object in which the action is defined to produce multiple responses.

5.1.2.1.3 Remote operations service element. ROSE should be provided to enable the transfer of management information received from CMISE. The following ROSE service should be provided, in accordance with ISO 9072-1.

RO-Invoke
RO-Result
RO-Error
RO-Reject-U
RO-Reject-P.

The ROSE services should be mapped to the P-Data services defined in ISO 8822.

5.1.2.1.4 Association control service element. The ACSE should be used to establish SMAP associations. The ACSE services should be implemented as defined in ISO 8649. The ACSE services should be mapped to the P-Connect, P-Release, P-U-Abort, and the P-P-Abort service of the presentation service.

5.1.2.2 ACSE services

5.1.2.2.1 A-Associate. The A-Associate should be provided to enable the establishment of an association between the manager and agent SMASEs.

5.1.2.2.2 A-Release. The A-Release should be provided to enable the termination of the manager-agent association without losing information in transit.

5.1.2.2.3 A-Abort. The A-Abort service should be provided to indicate abnormal termination of manager-agent association with possible loss of information.

5.1.2.2.4 A-P-Abort. The A-P-Abort service should be provided to indicate abnormal termination of manager-agent association as a result of action by the underlying presentation service and the possible loss of information.

5.1.2.3 Applications layer protocols. The SMASE should use the CMIP protocol defined in ISO 9596-1 and the ROSE protocol defined in 9072-2 to transfer management information. The ACSE protocol defined in ISO 8650 should be used to transfer SMAP connection establishment information. The use of protocol elements to provide the CMISE and ROSE services should be as specified in DISP 11183-2: International Standardized Profiles AOMnn OSI Management - Management Communications Protocols - Part 2: AOM12 - Enhanced Management Communications. The use of ACSE protocols should be as specified in DISP 11183-1:
AOMnn - Management Communications Protocols - Part 1: Specification of ACSE, Presentation, and Session Protocols for the Use by ROSE and CMISE.

5.1.2.4 Presentation layer services and protocols. A minimum set of presentation layer services and protocols should be as defined in ISO 8822 and ISO 8823. The use of the presentation layer protocol should be as specified in DISP 11183-1.
ATN systems should implement the presentation fast-byte protocol as defined in International Telecommunications Union - Telecommunications (ITU-T) X.216bis and ITU-T X.226bis.

5.1.2.5 Session layer services and protocols. A minimum set of session layer services and protocols corresponding to the Kernel and Duplex functional units defined in ISO 8326 and ISO 8327 should be implemented. The session layer protocol should provide for the use of unlimited data, as specified by ISO 8327: Addendum 2. The use of the session layer protocol should be as specified in ISO/IEC 11183 Part-2. ATN systems should implement the presentation fast-byte protocol as defined in ITU-T X.215bis and ITU-T X.225bis.

5.1.2.6 Transport layer services and protocols. The transport layer services and protocols should be provided in accordance with ISO 8072 and ISO 8073, Class 4.

5.1.2.7 Network layer services and protocols. Connectionless network services and protocols should be provided in accordance with ISO 8348 and ISO 8473.
The End System to Intermediate System (ES-IS) protocol should be provided in accordance with ISO 9542, when internetworking via routers is required.

5.1.2.8 Subnetworks

5.1.2.8.1 Local area network. Local area network protocol should be provided in accordance with FAA-STD-036.

5.1.2.8.2 Wide area network (packet switching network). Wide area network protocols should be provided in accordance with FAA-STD-039.

5.1.2.8.3 Point-to-point connections. Point-to-point connections should be provided in accordance with FAA-STD-039.

5.1.3 Managed objects. An MIB should be modeled in accordance with ISO/IEC 10165, which defines the structure of management information in the following three documents:

ISO/IEC 10165-1: Management Information Model
ISO/IEC 10165-2: Definition of Management Information (DMI)
ISO/IEC 10165-4: Guidelines for the Definition of Managed Objects (GDMO).

Standard managed objects should be used to the greatest extent possible. MOs should be selected from the MO definitions in the following standards documents:

ISO 10165-2: Definition of Management Information
ISO 10733: Elements of Management Information Related to OSI Network Layer Standards
ISO 10737: Elements of Management Information Related to OSI Transport Layer Standards
ISO 10742: Elements of Management Information Related to OSI Data Link Layer Standards.

FAA specific managed objects should be defined in accordance with ISO/IEC 10165-4.

5.2 IPS systems management - SNMPv1. The SNMPv1 should be provided in accordance with RFC 1157 and the following requirements:

5.2.1 Systems management application support. Systems management capability should be provided in five SMFAs: configuration management, fault management, performance management, security management and accounting management. Standards-based COTS application interfaces should be provided to the greatest extent possible.

5.2.2 Systems management communications architecture. The IPS system management protocol architecture should be as specified in Figure 3. Naming and addressing requirements should be in accordance with ENET1370-001.1: FAA Enterprise Network Naming and Addressing Standards. IPS security requirements are provided in FAA-STD-045: Open Systems Interconnection Security Architecture, Protocols, and Mechanisms.

5.2.2.1 Application layer protocols

5.2.2.1.1 SNMPv1. SNMPv1 may be used to enable the transfer management between the managed system and the management system. SNMPv1 should be in accordance with the Simple Network Management Protocol Request for Comment (RFC) 1157. The following SNMPv1 operations should be supported:

5.2.2.1.1.1 GetRequest. The GetRequest protocol data unit (PDU) should be provided, in accordance with RFC 1157, to enable the manager SMAP to retrieve a scalar object value from the agent SMAP.

5.2.2.1.1.2 GetNextRequest. The GetNextRequest PDU should be provided, in accordance with RFC 1157, to enable the manager SMAP to retrieve a list of scalar object values from the agent SMAP. For each value, the agent SMAP returns the object that is next in lexicographical order.

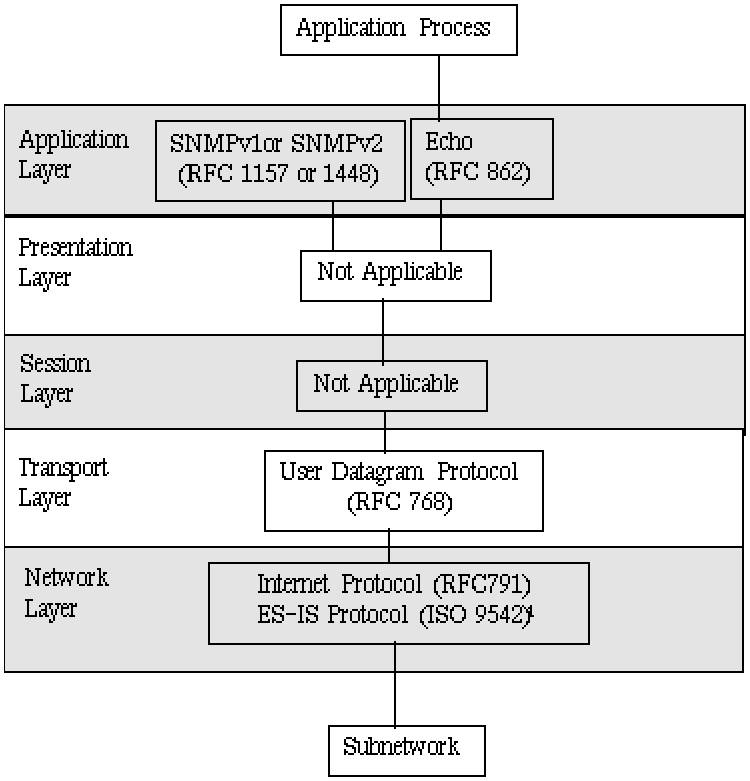


Figure 3. IPS systems management architecture

[1] Required when connecting via a router subnetworks

5.2.2.1.1.3 SetRequest. The SetRequest PDU should be provided, in accordance with RFC 1157, to enable the manager SMAP to request the agent SMAP to change the value of an object.

5.2.2.1.1.4 GetResponse. The GetResponse PDU should be provided, in accordance with RFC 1157, to enable the agent SMAP to respond to a GetRequest, GetNextRequest, or SetRequest from the manager SMAP.

5.2.2.1.1.5 Trap. The Trap PDU should be provided, in accordance with RFC 1157, to enable the agent SMAP to send an unsolicited scalar-object value notifying the manager SMAP of a significant event (i.e., alarm). The "enterprise specific" capability should be provided to enable the notification of FAA-specific events not provided by the simple network management protocol (SNMP) generic trap capability.

5.2.2.1.2 Echo. The Echo protocol should be provided, in accordance with RFC 862 , to enable datagrams received to be echoed in an answering datagram.

5.2.2.2 Transport layer. The user datagram protocol (UDP) should be used in accordance with RFC 768 to transport SNMP PDUs.

5.2.2.3 Network layer. The internet protocol (IP) should be used in accordance with RFC 791. The Internet Control Message Protocol (ICMP) should be used in accordance with RFC 792.
The ES-IS protocol should be provided in accordance with ISO 9542 when internetworking via routers is required.

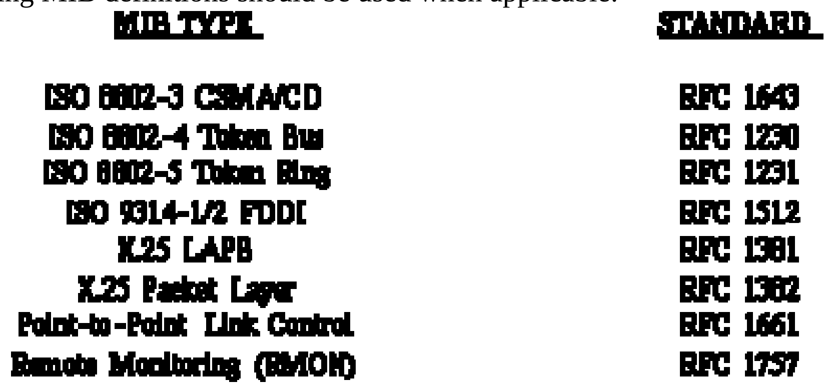
5.2.2.4 Subnetworks.

5.2.2.4.1 Local area network. Local area network protocols should be provided in accordance with FAA-HDBK-004.

5.2.2.4.2 Wide area network (packet switching network). Wide area network protocols should be provided in accordance with FAA-HDBK-004.

5.2.2.4.3 Point-to-point connections. Point-to-point connections should be provided in accordance with FAA-HDBK-004.

5.2.3 Managed objects. The SNMPv1 MIB should be modeled in accordance with RFC 1155 and RFC 1212, which define the structure of management information. Standard managed objects should be used to the extent possible. Standard managed object definitions should be selected from RFC 1213, MIB II. The MIB should enable the inclusion of managed objects not defined in MIB II. FAA-specific objects required should be included under the "enterprise" branch of the Internet object identifier tree. FAA-defined objects should be defined in accordance with RFC 1155.
The following MIB definitions should be used when applicable:



MIB TYPE	STANDARD
ISO 8802-3 CSMA/CD	RFC 1643
ISO 8802-4 Token Bus	RFC 1230
ISO 8802-5 Token Ring	RFC 1231
ISO 9314-1/2 FDDI	RFC 1512
X.25 LAPB	RFC 1381
X.25 Packet Layer	RFC 1382
Point-to-Point Link Control	RFC 1661
Remote Monitoring (RMON)	RFC 1757

5.3 IPS systems management - SNMPv2. The SNMPv2 should be provided in accordance with RFC 1441: Introduction to Version 2 of the internet-standard Network Management Framework and the following requirements.

5.3.1 Systems management application support. Systems management capability should be provided in five SMFAs: configuration management, fault management, performance management, security management, and accounting management. Standards-based COTS application interfaces should be provided to the greatest extent possible.

5.3.2 Systems management communications architecture. The IPS system management protocol architecture should be as specified in Figure 3. Naming and addressing requirements should be in accordance with ENET1370-001.1: FAA Enterprise Network Naming and Addressing Standards. IPS security requirements are provided in FAA-STD-045: Open Systems Interconnection Security Architecture, Protocols, and Mechanisms.

5.3.2.1 Applications layer protocols.

5.3.2.1.1 SNMPv2. SNMPv2 should be used to enable transfer management between the managed systems and the management system. SNMPv2 should be in accordance with RFC 1441: Introduction to SNMPv2 and RFC 1448: Protocol Operations for SNMPv2. The following SNMPv2 operations should be supported:

5.3.2.1.1.1 GetRequest. The GetRequest PDU should be provided, in accordance with RFC 1448, to enable the manager SMAP to retrieve a scalar object value from the agent SMAP.

5.3.2.1.1.2 GetNextRequest. The GetNextRequest PDU should be provided, in accordance with RFC 1448, to enable the manager SMAP to retrieve a list of scalar object values from the agent SMAP. For each value, the agent SMAP returns the object that is next in lexicographical order.

5.3.2.1.1.3 GetBulkRequest. The GetBulkRequest PDU should be provided, in accordance with RFC 1448, to enable the manager SMAP to retrieve a potentially large amount of data from the agent SMAP.

5.3.2.1.1.4 SetRequest. The SetRequest PDU should be provided, in accordance with RFC 1448, to enable the manager SMAP to request the agent SMAP to change the value of an object.

5.3.2.1.1.5 GetResponse. The GetResponse PDU should be provided, in accordance with RFC 1448, to enable the agent SMAP to respond to a GetRequest, GetNextRequest, GetBulkRequest, SetRequest, or InformRequest from the manager SMAP.

5.3.2.1.1.6 Trap. The Trap PDU should be provided, in accordance with RFC 1448, to enable the agent SMAP to send an unsolicited scalar-object value notifying the manager SMAP of a significant event (i.e., alarm). The "enterprise specific" capability should be provided to enable the notification of FAA specific events not provided by the SNMP generic trap capability.

5.3.2.1.1.7 InformRequest. The InformRequest PDU should be provided in accordance with RFC 1448, to enable a manager SMAP acting in a manager role to notify another manager SMAP acting in a manager role of information from a SMAP agent local to the sending SMAP manager.

5.3.2.1.2 Echo. The Echo protocol should be provided, in accordance with RFC 862, to enable datagrams received to be echoed in an answering datagram.

5.3.2.2 Transport layer. The UDP should be used in accordance with RFC 768 to transport SNMP PDUs.

5.3.2.3 Network layer. The IP should be used in accordance with RFC 791. The ICMP should be used in accordance with RFC 792.
The ES-IS protocol should be provided in accordance with ISO 9542 when internetworking via routers is required.

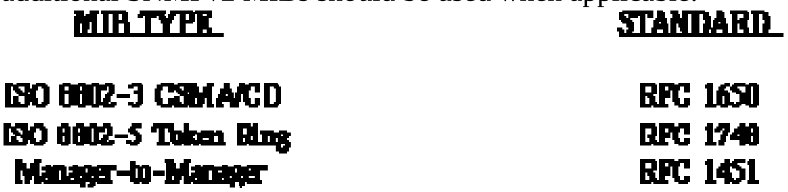
5.3.2.4 Subnetwork layers.

5.3.2.4.1 Local area network. Local area network protocol should be provided in accordance with FAA-HDBK-004.

5.3.2.4.2 Wide area network (packet switching network). Wide area network protocols should be provided in accordance with FAA-HDBK-004.

5.3.2.4.3 Point-to-point connections. Point-to-point connections should be provided in accordance with FAA-HDBK-004.

5.3.2.5 Managed objects. The SNMPv2 MIB should be modeled in accordance with RFC 1442, which defines the structure of management information. Standard managed objects should be used to the extent possible. Standard managed object definitions should be selected from RFC 1450. The MIB should enable the inclusion of managed objects not defined in the SNMPv2 MIB. FAA-specific objects required should be included under the "enterprise" branch of the Internet object-identifier tree. FAA-specified objects should be defined in accordance with RFC 1442 and RFC 1443.
The following additional SNMPv2 MIBs should be used when applicable:



MIB TYPE	STANDARD
ISO 8802-3 CSMA/CD	RFC 1650
ISO 8802-5 Token Ring	RFC 1748
Manager-to-Manager	RFC 1451