SFO

San Francisco International Airport

SFO ITT Operating Environment: Current and Targeted (OECT)

Version: 3.6

Formerly the Platform Compatibility Matrix

Prepared by:
SFO Information Technology and Telecommunications
Last updated on:
October 7, 2009

Document Information

Authors

Table 1 lists the authors and their contact information.

Table 1 – Document Authors

Names	Title	Email	Phone
Bo Pitsker	Lead, Solutions Architecture	bo.pitsker@flysfo.com	650.821.4316
Erik Joelsson	Manager/Systems Engineering	erik.joelsson@flysfo.com	650.821.4362
Martin Taras	Manager/Application Development	martin.taras@flysfo.com	650.821.3380
Rene Leedeman	Manager/Telecom	rene.leedeman@flysfo.com	650.821.3395
Zihong Gorman	Director/Information Access	zihong.gorman@flysfo.com	650.821.3368

Approvers

The following approvals are required for this document to take effect.

Table 2 – Document Approval

Approver Names	Title/Department
Daniel Gonzales	Director, Technical Services
Rene Leedeman	Director, Communications Services
Frank Lara	Director, Quality Assurance and ITIL
Ray Ricardo	Director, Projects and Planning Services
Zihong Gorman	Director, Information Engineering Services
Jonathan Kaplan	CISO/Director, Information Security Services
John Payne	CIO

Edit History

Table 3 – Document Edit History

Version	Date	Who	Revision
1.4	2006	Oren Eshel	Created the original "ITT Standards"
2.1	2/18/2008	Zee Gorman	Re-created and renamed the document
2.2	6/30/2008	Zee Gorman	Added SNMP Requirement Section authored by Bo Pitsker

Version	Date	Who	Revision
2.3	7/7/2008	Zee Gorman	Updated SNMP Requirements Section and renamed it to Systems Monitoring Requirements.
3.0	7/9/2008	Bo Pitsker	Completed "Networks" section; provided new frameworks for other sections
3.1	8/11/2008	Erik Joelsson	Updated Systems Section
3.1	8/11/2008	Rene Leedeman	Updated Telecom Section
3.2	8/12/2008	Zee Gorman	Updated Applications Section
3.3	8/16/2008	Zee Gorman	Edits for section and table consistency
3.4	9/2/2008	Zee Gorman	Updated "Application" sections and moved some of the contents to appendix
3.5	12/4/2008	Bo Pitsker	Updated System Monitoring, Appendices A and B
3.6	9/6/2009	Bo Pitsker	Changed title; added new intro; added new desktop section; updated Networks section; added to Appendices A and B extensively

Distribution List

This document should be distributed to program managers and project managers of all SFO projects with an ITT systems implementation components, who can distribute to all parties including vendors and consultants engaged in building these components.

Introduction

SFO Information Technology and Telecommunications (ITT)'s operating environment is complex and diverse. It supports both internal Airport staff and numerous revenue generating customers, including airlines, concessionaires, tenants and support services, as well as contractors, visitors, and passengers.

Suppliers, vendors, consultants and others supplying good or services must acquaint themselves with ITT's current and targeted operating environments, so that they can furnish offerings that integrate easily into the Airport's IT infrastructure. It is incumbent upon outside offerors to explain and rationalize why their products and/or services are not consistent with the Airport's current or future operating environments.

This document provides a high-level view into all aspects of the operating environment, and furnished extensive references to internal and external standards and guidelines. However, it is intended to be descriptive and not necessarily normative.

Background

San Francisco International Airport ("SFO") is the principal commercial services airport for the San Francisco Bay Area. The San Francisco Airport Commission operates the Airport as a separate enterprise department of the City and County of San Francisco (the "City"). The Airport Commission manages a talented and committed alliance of Airport staff, airlines, concessionaires, consultants, contractors, and support organizations who operate and maintain the Airport facilities that accommodate air and ground transportation for more than 33 million passengers and over half a million metric tons of cargo each year. The total number of airlines flying out of SFO exceeds 55, with United and American being the largest carriers.

SFO is comprised of 3 domestic terminals and an international terminal. The domestic terminals are a total square footage of 2.6 million, 66 gates, and 25 baggage carousals. The International terminal has 1.8 million square feet, 24 gates, and 25 baggage carousals. SFO's annual revenues are approximately $503M, and the airport is 14th in size domestically, and 30th in size worldwide. Airport commission staff number about 1,300. Total employment at SFO from all sources approaches 30,000.

Information Technology and Telecommunications (ITT)

The Information Technology and Telecommunications organization has as its mission "to provide access to information to enable better business decisions." It is an element of the Administration section of the Airport, and is headed by John M. Payne, Chief Information Officer (CIO). ITT offers a wide range of services to the Airport Commission, airlines and tenants, and passengers. It has 65 employees, and an annual budget of approximately $12 million, excluding capital projects. ITT is divided into a number of service groups:

Table 4 – SFO ITT Service Groups

Group	Services provided
Business Services	IT-related procurements; vendor management; finance; budgets; HR
Information Engineering Services	Application development and support; database and application consulting; data warehousing; business reporting and analytics
Technical Services	Application hosting and support; data storage; desktop and software services; computers and peripherals; service desk and support; remote access; email
Project and Planning Services	Project management; customer relationship management; change management
Communication Services	Voice services; network services, including Ethernet, SONET, Internet access and WAN circuits; cabling and physical connectivity
Information Security Services	Security management; risk management; compliance
Quality Assurance	Product testing and evaluation; ITIL implementation
Technical Design Services	Enterprise architecture; collaborative platform development, IT standards

ITT produces significant revenue for the Airport via its ASIC and STS services, include voice, data and video services.

Desktop Platforms

SFO targets specified minimum configurations as outlined in the following tables. The installed base of Commission users may or may not possess the current platforms, as the desktop refresh cycle at SFO is 4 – 5 years.

Standard Desktop Hardware

The current supplier of choice is Dell Computer.

Table 5 – Standard Desktop Hardware

Component	Description
Processor	E8000 series Intel® Core™2 Duo/Quad 6M/4M, 1333 FSB (2.0 GHz or higher)
Memory (RAM)	2 GB 800 MHz DDR2 SDRAM (Expandable to 4GB)
Mass Storage	80 GB SATA II (7200 rpm), upgradable to additional 80, 120 or 200 GB
Video	256 MB integrated Intel® Graphics Media Accelerator 4500 or better
Network Adapter	10/100/1000 Gbit/s integrated on motherboard
Removable media	CDRW/DVD combo drive
Monitor	19" Dell Ultra Sharp flat panel
Keyboard	Standard USB
Mouse	USB 2-button entry mouse with scroll
Model(s)	Dell Optiplex 745/755/760
Form factor	Desktop (15.7” x 4.5” x 13.9” approx.)

Standard Laptop Hardware

The current supplier of choice is Dell Computer. IBM/Lenovo Thinkpads were previously deployed widely, and many remain in the field.

Table 5 – Standard Laptop Hardware

Component	Description
Processor	E8000 series Intel® Core™2 Duo, 1333 FSB (2.0 GHz or higher)
Memory (RAM)	2 GB 800 MHz DDR2 SDRAM (Expandable to 8GB)
Mass Storage	80 GB SATA II (7200 rpm), upgradable to additional 80, 120 or 160 GB
Video	256 MB integrated Intel® Graphics Media Accelerator 4500 or NVIDIA® Quadro® NVS 160M or better
Network Adapter, wired	10/100/1000 Gbit/s integrated on motherboard
Network Adapter, 802.11	Intel WiFi Link 5300 [802.11a/g/n (3x3)]
Removable media	CDRW/DVD combo drive
Monitor	14.1" UltraSharpTM WXGA+ (1440x900) LED Display
Keyboard	Standard (built-in)
Mouse	USB 2-button entry mouse with scroll
Model(s)	Dell Latitude E6400 (4.3 lbs) Dell Latitude E4200 (2.2 lbs)
Form factor	Laptop (13.1” x 9.37” x 1.5” approx.)

Standard Software

The following software is included in the base image, with patches applied as available.

Table 7 – Standard Client Software

Type	Description
Operating System	Windows XP, SP 3 [will transition to Windows 7 in near future]
Application Suite	Microsoft Office 2007, SP3
Internet Browser	IE 6/7
Email Client	Microsoft Outlook 2007 (with Exchange 2007 server)
PDF Viewer	Adobe Reader 8.1.6
Flash	Adobe Flash Player 10.0.32.18
Anti-Virus	Symantec Endpoint Protection Ver:11.0.4202.75/12 (coming soon)
Remote Access (VPN)	Cisco VPN Client 4.8.02/5.0.05.0290
Java JRE	Sun Java SE JRE 6, 6u16
.NET Framework	Microsoft .NET Framework 3.5 SP1

Optional Software

The following software is available as needed, but is not in the base image, with patches applied as available.

Table 8 – Optional Client Software

Type	Description
Client Database	Microsoft Access 2007, SP1
Project Management	Microsoft Project 2007, SP2
PDF Document Creation	Adobe Acrobat Standard, 8.1.5
Image Processing	Adobe Photoshop CS4 11.0.1
Graphics	Adobe Photoshop CS4 11.0.1 Microsoft Visio 2007, SP2
Mainframe Terminal Emulation	Rumba 2000
Employee Time Accounting	Tess
Database Reporting	EIS/Cognos

Server Hardware Platform

SFO utilizes IBM BladeCenter technology with Intel based blades as a standard hardware platform across all servers to allow efficient use of resources and to facilitate business resumption.

Standard Server Hardware

The IBM BladeCenter solution[1] is used for all Intel-based servers. SFO supports the use of the HS22 or newer model line. *SFO ITT does not support AMD, POWER, PowerXCell or Cell/B.E. based IBM blades.*

Where BladeCenter technology is not sufficient SFO will utilize IBM System x series servers. Please note that the use of non-blade servers at SFO is dependent on many factors, including but not limited to: available rack space, HVAC, Fiber-Channel and network port availability.

All server systems must be compatible with the IBM Systems Director Server platform management suite of centralized management tools, version 6.1.1 or newer current version. The use of this tool ensures a uniform hardware deployment and configuration so that SFO-ITT can honor business resumption requirements and various service level agreements (SLA). All OS deployment and redeployment is handled by the Remote Deployment Manage (RDM) extension to IBM Systems Director Server.

All system backups at SFO are done centrally with IBM Tivoli Storage Manager (TSM) backup suite. IBM servers supplied by third parties must be configured for management by ITT's IBM Director and the support contract transferred to SFO before they can be considered a production system.

Storage Area Network

Where local storage is not sufficient or does not meet retention or other policies, SFO are reliant upon SAN storage. The SAN storage is based on the EMC Clariion product line and Brocade Fiber Channel Switches, providing Fiber Channel storage and remote mirroring capabilities between separate locations on the Airport campus. Failover controllers are implemented at each storage facility. Multiple paths between facilities are available to the operating system for failover, and logical drives are partitioned so that they are visible only to the intended operating system.

Any application where SAN storage is requested must work with this setup.
SFO uses Navisphere on all SAN management servers for SAN management, any new SAN systems must support Navisphere management application v 6.26 or newer.

Non-standard Server Hardware

Non Intel based IBM-Blade Servers, non System x hardware is considered on an individual basis.

[1] Additional information about the IBM Blade Center platform is available at: http://www-03.ibm.com/systems/bladecenter/hardware/servers/x86.html

Server Virtualization

ITT has standardized its virtualization strategy around EMC’s VMWare product line, including ESX VMs, VirtualCenter, and VMotion.

Operating Systems

SFO will support servers running both Microsoft Windows 2003, Standard and Enterprise Server, or newer. SFO will also support SuSE Linux Enterprise Server 10.

Windows Server

SFO will support the Windows Server family of operating system, version 2003 SP2 and later, both 32bit and 64bit.

Before connected to the production network all servers must be configured with Symantec Antivirus software, centrally managed by SFO-ITT, SFO AV management server is Symantec’s SEP 11 or newer current version.

All Windows installation must support and be configured for SFO’s implementation of Microsoft System Center Configuration Manager 2007SP1, or newer current version.

OS support includes Network Load Balancing (NLB) and Windows Cluster setups, Standard applications that come bundled with Windows are usually supported, some of which include Active Directory, IIS web and IIS ftp, and DNS server.

Linux

SFO supports two Linux server distributions: Red Hat Enterprise Linux (RHEL) 5.4 or later, and Novell SuSE Enterprise Server (SLES) 11.0 or later. Applications included with the distributions are generally supported, as is the default package managers for the distributions. Community editions and/or derivative distributions may be considered on a case by case basis, but will be discouraged. Note that SFO does not support Linux desktop distributions at this time.

Other Operating Systems

Any other operating system is considered on an individual basis.

Networks

General

The SFO network is a three-tier network with complex connectivity requirements. The network consists of approximately 300+ network devices, ranging from Cisco Catalyst 6509s to ASA 5500 firewalls. The Airport also operates an OC-48 SONET ring that provides for voice and data transport both on and off campus.

The network architecture is a fully-meshed, geographically distributed network. There are two 6509s serving as core switches, and ten 6509s providing distribution-layer routing. The access layer switches are a mixture of switch models. Internet connectivity is provided via a 30-Mbit/s link to AT&T or via a 9-Mbit/s fractional DS-3 secondary link to Sprint. Other wide area network (WAN) connections include various T-1s to City offices downtown and to satellite locations on and off campus.

A separate network is provided for tenant usage, the Public Internet Access or “PIA” network, but airlines may elect to use the Commission network in lieu of obtaining a dedicated circuit from SFO ITT. PIA Internet connectivity is provided via a 30-Mbit/s link to AT&T. There are numerous instances of private peering, both to a bastion DMZ and to specific subnets. Some subnets are protected via VPNs, some are not. The network has various security elements in place including Cisco and Juniper firewalls, Cisco IPS devices, and Cisco ACS. Websense is used to filter traffic to the SFO (Commission) network, and Packeteer provides bandwidth management from the Internet.

The network is migrating to an MPLS service provider model using MPLS TE fast re-route. EIGRP will be de-commissioned, and IS-IS will replace it. iBGP will be implemented, together with BGP route reflectors, for optimal performance. The Core Distribution Upgrade project will replace the 6509s with Cisco ASR 9000s running a 10 Gbit/s backbone.

Ethernet-based Network Equipment

ITT has standardized on Cisco hardware for the majority of its network needs. The hardware used is intended to provide the Airport with excellent performance, reliability, security and services. Cisco hardware can be categorized as WAN routers, access layer switches, distribution switch routers, and core switch routers. Specialized devices include standalone firewalls, intrusion prevention systems, and integrated services modules. Table 9 summarizes our targeted equipment standards and the equipment being installed as part of the Core Distribution Upgrade project. Note that the entries are not all-inclusive; components such as software, connector interfaces, flash memory, power supplies, etc. are not shown. Also excluded are supporting servers, consoles, etc.

Table 9 – Standard Network Hardware and Software

Standard Network Hardware and Software			
Vendor	**Model**	**Function**	**Description**
Cisco	ASR 9010	Core/dist	Core-dist layer router
Cisco	A9K Route Switch Processor/fabric controller	Core/dist	System mgmt for ASR 9000s
Cisco	16 port 10-Gigabit Ethernet modules	Core/dist	Core-distribution connections
Cisco	A9K 40-port SFP GE line card	Core/dist	Access-distribution connections
Cisco	IOS XR 3.7.3 IP/MPLS core software with 3DES or newer	Core/dist	Operating system
Cisco	Infrastructure VRF feature license	Access	Enables L3VPN support
Cisco	Catalyst 4510R-E	Access	Chassis-based access layer aggregation switch
Cisco	Catalyst 4507R-E	Access	Chassis-based access layer aggregation switch
Cisco	Catalyst 4500 Supervisor 6-E	Access	System mgmt for 4500s
Cisco	4500 E-Series 6-Port 10GE line card	Access	Access layer connections
Cisco	Cisco Catalyst 4500 Enhanced 48-Port 1000 Base-T (RJ-45)	Access	Access layer connections
Cisco	Cisco Catalyst 4500 48-Port 1000Base-X	Access	Access layer connections
Cisco	Cisco Cat 4500E IOS 12.2.53-SG(ED) Enterprise Services SSH or newer	Access	Operating system
Cisco	Cisco Catalyst 3750-E	Access	Stackable access layer connections
Cisco	IOS 12.2(50)SE IP Services or newer for 3750-E	Access	Operating system
Cisco	2811 ISR	Access	Terminal server (w/NM-32A)
Cisco	IOS 12.4.25(MD) Enterprise Services or newer for 2811	Access	Operating system
Cisco	ASR 1002	Access	Border router
Cisco	ASR1K ESP5	Access	Accelerator module
Cisco	ASR1K 5-port GE SPA	Access	GE line card
Cisco	ASR 1000 firewall feature license	Access	Firewall software
Cisco	ASR 1000 RP1 IOS XE	Access	Operating system

Standard Network Hardware and Software			
Vendor	**Model**	**Function**	**Description**
	2.4.1 Advanced Enterprise or better		
Cisco	ASA 5540 Security Appliance	Security	Internet-facing security services
Cisco	AIP SSM-40 Security Services module	Security	HW for 5540 which provides intrusion prevention
Cisco	ASA 5540 Security Contexts feature license	Security	Adds virtual firewall capabilities to ASR 1000s
Cisco	ASA 5500 Software 8.2(1) or newer	Security	Operating system
Cisco	Aironet 1252 Access Points	Access	802.11a/b/g/n wireless access points
Cisco	5508 Wireless LAN Controller	Network Management	Wireless network management
Cisco	Cisco Unified Wireless Network Software Release 6.0	Network Management	Adds features to APs and controllers
Cisco	3350 Mobility Services Engine (MSE)	Security	Geo-location/tracking HW for wireless devices
Cisco	3350 Mobility Services Engine (MSE) software 6.0.85.0 or later	Security	Operating system/application for MSE
Cisco	Context-Aware Mobility Service Software	Security	Geo-location/tracking SW for wireless devices
Cisco	Cisco Adaptive Wireless IPS	Security	Intrusion prevention for wireless networks
	Wireless Control System (WCS) 6.0.132.0 or later	Network Management	Wireless configuration management
Cisco	Wireless Control System (WCS) Navigator 1.5.128.0 or later	Wireless Management	Enterprise software that manages wireless controllers
Cisco	Cisco Spectrum Expert 3.3.52 or later	Wireless Management	Wireless spectrum analyzer software
Cisco	CiscoWorks LAN Management Solution (LMS) v3.2 or later	Network Management	Distributed router/switch management
Cisco	ASA 5580 Security Appliance	Security	Centralized VPN services platform
Cisco	ASA 5520 Security Appliance	Security	Endpoint firewall/ authentication
Cisco	IPS 4270 Security Appliance	Security	Intrusion detection/ protection Appliance
Cisco	IPS 4270 System SW v6.1(3)E3 or later	Security	Intrusion detection/ protection

Standard Network Hardware and Software			
Vendor	**Model**	**Function**	**Description**
Cisco	Cisco Security Monitoring, Analysis, and Response System (MARS) 210	Security	Event detections/analysis appliance
Cisco	CS-MARS) v6.03 or later	Security	Event detections/analysis software for MARS devices
Cisco	Cisco NAC Appliance 3350	Security	Network access control
Cisco	ACS 1120 Server	Security	Centralized access control system; coordinates with AD
Cisco	ACS 5.0/5.1	Security	Operating system/application for ACS servers
Cisco	CiscoWorks Network Compliance Manager (NCM)) v.1.4 or later	Security	Policy management, enforcement across network
Cisco	Cisco Security Manager (CSM)) v.3.3 or later	Security	Server-based software, manages ACLs, security configurations of Cisco devices
Cisco	Cisco Security Agent (CSA) v6.01 or later	Security	End user security protection application
Juniper	Netscreen 50	Security	Firewall
Packeteer	PacketShaper	Network	Traffic policing
Websense	Cisco appliance	Security	Web filtering and blocking
BlueSocket	Appliance	Security	Wireless security

SONET Network Description and Hardware

The telecommunications infrastructure is a critical component of the Airport's operation that needs to be fully redundant and fault tolerant. By having two physically separate MPOEs and two separate service providers present in each location, the Airport safeguards itself from any possible disasters such as fires, earthquakes, terrorist attacks, and/or plane crashes. SONET is the technology used to provide highly reliable telecommunications and access on and off the SFO campus.

San Francisco International Airport has two main points of entry (MPOE) where telecommunication service providers deliver and terminate their circuits. This is the demarcation point where SFO can accept telecommunication services and control access into the Airport. The two locations, which are NMPOE and SMPOE, provide redundancy by eliminating a facility from being a single point of failure. In addition, SFO utilizes two different service providers, AT&T and Legacy ATT/LNS, which provide an extra level of redundancy and fault tolerance.

Currently, both AT&T and ATT/LNS have an OC-12 ring that terminates into NMPOE. SFO utilizes that bandwidth to provide Telco services to the Airlines, Tenants, Commission, and Concessions over the Airport's OC-48 SONET Ring. These services consist of OC-12, OC-3, DS3, DS1, and DS0, which include POTS and

Coin Phones. AT&T is currently has a second OC-12 into SMPOE, which will provide SFO an even higher level of redundancy by having AT&T presence in two different MPOEs. Should one MPOE ever become inoperable, SFO can continue to provide service through the alternate location. By having the redundancy at the MPOE level, SFO recovery time goes from weeks and/or months, to just a few hours.

The SONET network is comprised of Alcatel Add Drop Multiplexers (ADM) and Digital Loop Carriers (DLC) installed as transport network elements on an intra-campus OC-48 SONET ring. The SONET ring transports AT&T and Legacy ATT/LNS service to multiple SONET nodes in the Airport campus. The SONET ring is set up in a UPSR configuration to provide path redundancy in the event of a fiber cable failure. The OC-48 ring is currently using 75% of the bandwidth capacity to transport TDM service to the San Francisco Airport. The SONET infrastructure is reliable, stable and doesn’t approach the OC48 bandwidth capacity in its current configuration. SFO has submitted a capitol request to increase the capacity of the current SONET ring from OC-48 to OC-192 for future growth and equipment refresh.

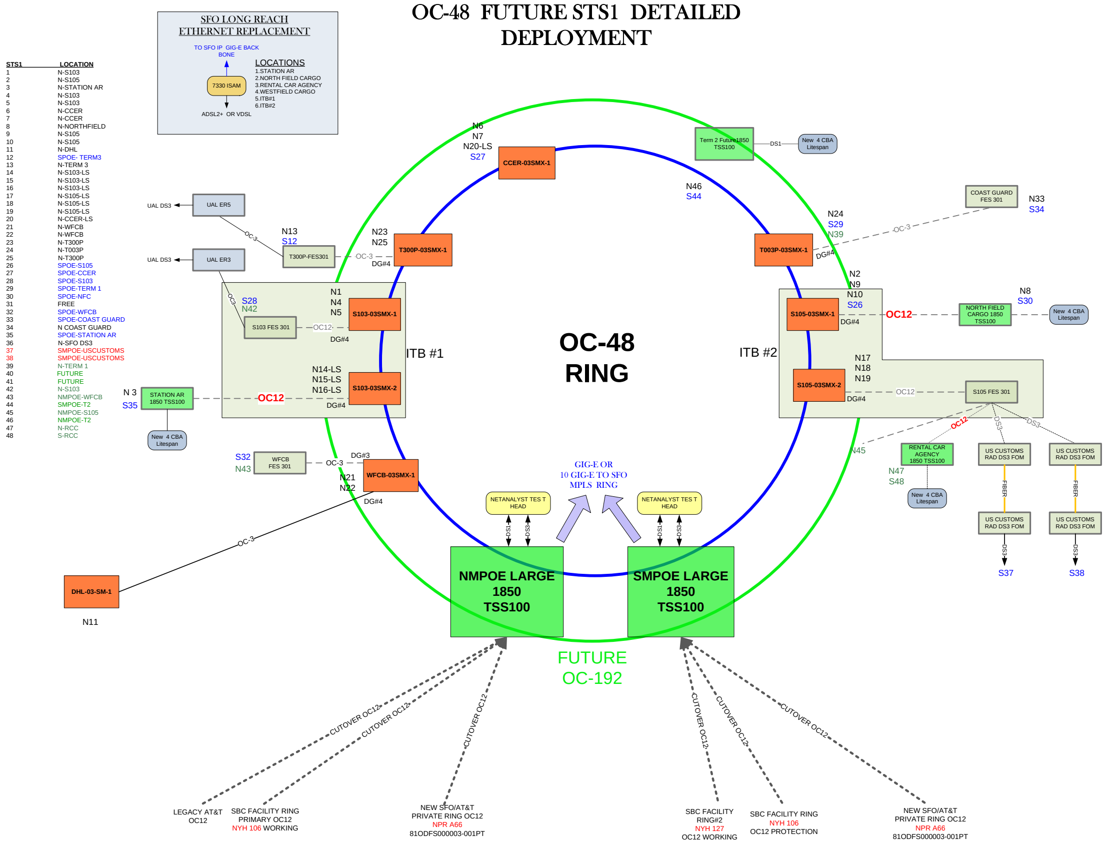
Table 10 lists the major SONET components in use at SFO.

Table 10 – SFO SONET Hardware

Standard SONET Hardware			
Vendor	**Model**	**Function**	**Description**
Alcatel	1850 TSS-100	SONET support	The 1850 TSS-100 is a high capacity device used to interface with multiple LECS at an OC-12 rate and break down the signal to DS1s. The signal is then muxed back to SONET format to be sent out to the SFO SONET OC-48 or OC-192 ring for distribution.
Alcatel	1340 INC	SONET support	Alcatel 1340 INC is the management tool for the the1850 TSS-100. It works in tandem with 1301NMX for alarm monitoring, provisioning and troubleshooting of the 1603 ADMs, all on a single screen.
Telmar	1603 SMX, 1603SM,1603SE	SONET support	The 1603xx SONET muxs are used to build the SFO OC-48 ring. The ADM (add drop mux) is used to distribute the following services: OC12, OC-3, DS-3, DS-1
Alcatel	1301NMX	SONET support	1301NMX is the primary management software for the 1603xx nodes. 1301 is used to

Standard SONET Hardware			
Vendor	**Model**	**Function**	**Description**
			provision new services, perform cross connects, monitor alarms, and communicate with the 1320NM.
Alcatel	LITESPAN 2000	SONET support	The Litespan 2000 is used to distribute DS0 services: analog voice, DDS(56k,64k), ISDN, DSL, COIN phones .
Alcatel	LITESPAN 2012	SONET support	The Litespan 2012 is used to distribute DS0 services: analog voice, DDS(56k,64k), ISDN, DSL, COIN phones . It has the ability to deliver 2,012 DS0s
Alcatel	AMS 5520	SONET support	The Alcatel Management System is used to provision new service, cross connects, and monitor alarms for the LS2000.
Alcatel	7330 ISAM	ADSL 2+, VDSL2	The 7330 delivers data transport, ranging from 2Mbps-45Mbps on legacy copper using the technologies of ADSL2+ and VDSL2. Data rates vary depending on quality and copper distances of up to 5000ft. This is the technology that ATT UVERSE currently uses to provide high speed internet access as well as HDTV to residential customers.
Alcatel	AMS 5526	7330 ISAM network management	AMS 5526 is used as a provisioning tool as well as a network management tool for Alcatel 7330 ISAM.
ADTRAN	OPTI 6100	SONET support	SONET extension Mux used to deliver variable service rates ranging from OC-12 thru DS1 service.
JDSU	Netanalyst	SONET support	Controls Centest 650s which allows mutiple DS1/DS3 testing sessions.
JDSU	Centest 650s	SONET support	DS1/DS3 continuity tester between SFO and LECS

OC-48 FUTURE STS1 DETAILED DEPLOYMENT



STS1	LOCATION
1	N-S103
2	N-S105
3	N-STATION AR
4	N-S103
5	N-S103
6	N-CCER
7	N-CCER
8	N-NORTHFIELD
9	N-S105
10	N-S105
11	N-DHL
12	SPOE- TERM3
13	N-TERM 3
14	N-S103-LS
15	N-S103-LS
16	N-S103-LS
17	N-S105-LS
18	N-S105-LS
19	N-S105-LS
20	N-CCER-LS
21	N-WFCB
22	N-WFCB
23	N-T300P
24	N-T003P
25	N-T300P
26	SPOE-S105
27	SPOE-CCER
28	SPOE-S103
29	SPOE-TERM 1
30	SPOE-NFC
31	FREE
32	SPOE-WFCB
33	SPOE-COAST GUARD
34	N COAST GUARD
35	SPOE-STATION AR
36	N-SFO DS3
37	SMPOE-USCUSTOMS
38	SMPOE-USCUSTOMS
39	N-TERM 1
40	FUTURE
41	FUTURE
42	N-S103
43	NMPOE-WFCB
44	SMPOE-T2
45	NMPOE-S105
46	NMPOE-T2
47	N-RCC
48	S-RCC

Standards and Protocols

A network is more than a collection of hardware and software. It must include protocols and standards for the carrying of numerous functions, including switching, routing, security, network management, failover, etc. SFO supports both vendor-independent standards and, when necessary, proprietary protocols. It should be understood that not all standards and protocols are applicable to every network device. Moreover space limitations prevent a comprehensive enumeration of all protocols and standards in use at SFO.

Many standards overlap in their scope, and may state contradictory requirements. Where such conflicts occur, the more stringent requirement will prevail. Similarly, earlier standards may be revised by later standards. Accordingly, the later standard shall prevail. Finally, where drafts or pre-standards are cited, it is expected that the latest version available shall be used, regardless of the status of the draft or prestandard. When in doubt ITT should be consulted as to which standards requirement is controlling for a given project or procurement.

A note about IPv6: The tables in ***Appendix A*** reflect on IPv4 standards and protocols. However, SFO ITT anticipates that IPv6 conversion will begin within 5 years. Therefore, new procurements will be reviewed in part based on their ability to support IPv6 and derivative protocols, as the typical life cycle for network equipment is greater than 5 years.

Application Platforms and Components

Applications at SFO serve a wide range of needs, including internal SFO operations, airline operations, tenant operations, and passenger services. It is worth noting that the Airport Commission, being a City and County of San Francisco (CCSF) agency, also operates on a variety of applications provided and maintained by the central IT group of CCSF, i.e., Department of Technologies.

The SFO internal support group for applications Information Access is a unit inside ITT. This group provides application development, application administration and maintenance services.

Application Development Platforms

When assessing software solutions, we prefer buy over build in general. In the case where the business need is such that no commercial-off-the-shelf solutions can satisfy the core requirements, Information Access will build the application. Table 11 describes the standard application development platforms.

Table 11 – Application Development Platforms

Type	Platform
Platform #1	
Database	Oracle 10g on Linux 10
Web Server	IIS 6 or higher for Windows
Application Server	ColdFusion 8 on Windows 2003
Target Browser	Internet Explorer 7
Directory Server	Microsoft Active Directory
Version Control	Concurrent Versions System (CVS)
Platform #2	
Database	Oracle 10g
SDK	Remedy AR Server API
Platform #3	
Database	Oracle 10g on Suse Linux 10
Web Server	IIS 6 or higher for Windows
Application Server	IBM Websphere Application Server on Windows
Version Control	Concurrent Versions System (CVS)

Application Hosting Platforms

With very few exceptions, all SFO procured and operated applications are hosted in the ITT supported hosting facility. Please refer to Section One for the different levels of support services. Detailed support agreements should be established with approval from all stakeholders, including business users, ITT, the software provider(s), and the systems integrator(s).

ITT supports the following application infrastructures as illustrated in Table 12. Deviation from the standard stacks in terms of components and version numbers shall be reviewed by ITT prior to approval on a case by case basis.

Table 12 – Application Hosting Platforms

Type	Supported Platforms and Components
J2EE Standard:	
Web Servers	• IBM HTTP Server 6.0 or higher
Application Servers	• IBM Websphere Application Server (WAS) 6.0 or higher
Databases	• Oracle Database 10g or higher
Open-source Standard:	
Web Servers	• Apache HTTP Server
Application Servers	• IBM Websphere Application Server Community Edition (WASCE) • Apache Tomcat
Databases	• MySQL, PostgreSQL
Microsoft Standard:	
Web Servers	• Apache HTTP Server 1.3.41 or higher • IIS 6.0 or higher – to be considered on a case-by-case basis
Application Servers	• .Net Framework 3.5 or higher
Databases	• Oracle Database 10g or higher • SQL Server 2005 or higher
Server-based Standard:	
Programming Language	• Not specified. The requirement is clean start-up with no manual intervention necessary
Databases	• Oracle Database 10g or higher

Enterprise Application Integration Model

Enterprise Application Integration is crucial to all future SFO application implementations. This section explains the current and future SFO EAI standard practices. At a minimum, conformation to the current practice is required. Conformation to an SFO future EAI model is, however, preferable.

ODBC & JDBC

SFO will at a minimum pursue a data-centric integration model by enforcing a standard RDBMS platform, i.e., Oracle Database 10g. ODBC and JDBC are accepted as standard data connectivity protocols.

Open and Documented API

Open and documented API is highly desirable for all future software implementations.

Data Warehousing

SFO's data-centric integration model is also supplemented by Data Warehousing standard practice. A data warehouse serves as the central data storage for data sharing among heterogeneous database platforms as well as business operations. Please see the next section for detailed SFO Data Warehousing requirements.

External Data Sharing

Currently SFO supports FTP of structured data as one means of data sharing over the internet. Data format can be fixed-length, delimited or XML.

Service Oriented Architecture (SOA)

SFO's long-term EAI strategy is to adapt a Service Oriented Architecture based on Web Services.

Data Warehousing Requirements

All business systems contain vital operational statistics for SFO and its partners. It is SFO ITT's policy that the data that support these statistics be extracted and stored in SFO's Data Warehouse to support management decision-making. It is the software vendor's responsibility to provide metadata documentation as well as data access mechanism to SFO as part of the systems implementation project.

The following documents shall be accepted as "metadata documents":

- Physical Entity Relationship Diagram + Data Dictionary
- Table and Field Descriptions in tabular format
- Business Views and Fields Descriptions in tabular format

Table 13 describes the infrastructure of SFO Data Warehouse.

Table 13 – SFO Data Warehouse Components

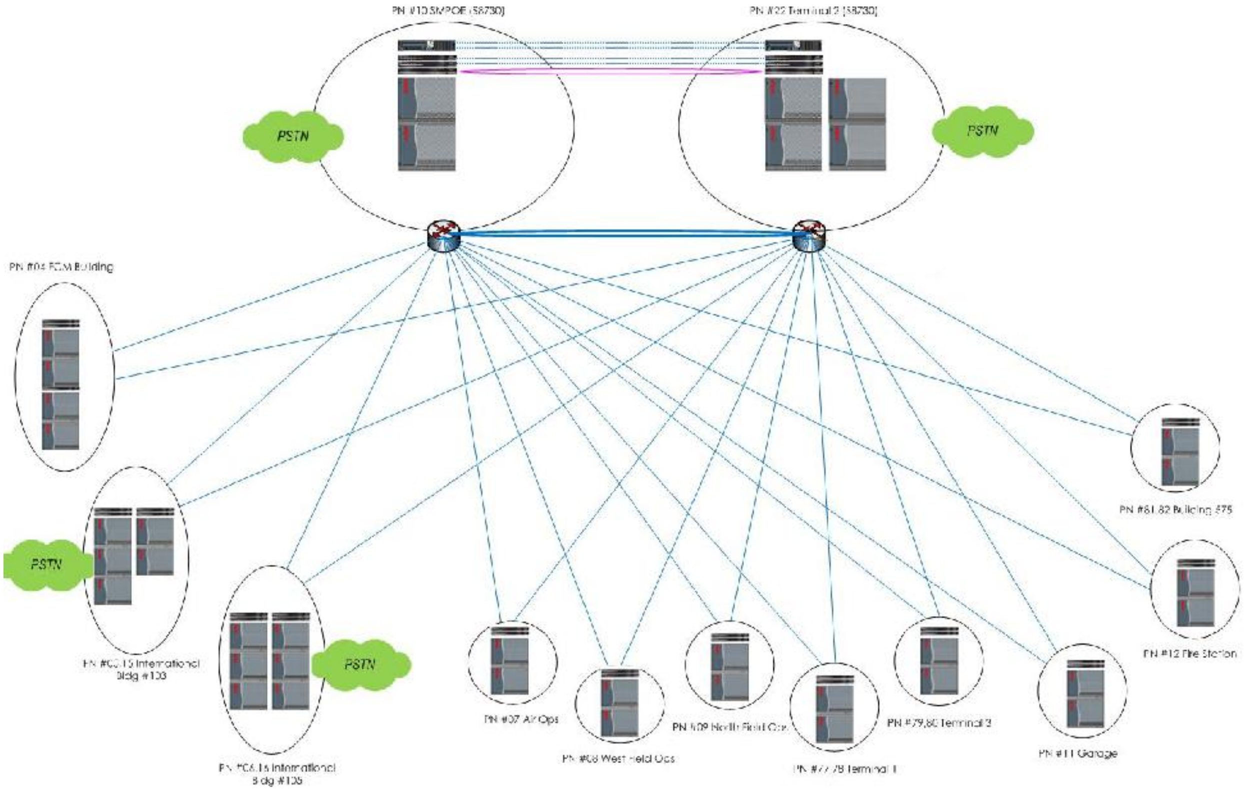
Type	Supported Platforms and Components
Database	• Oracle 9i
Reporting Software	• IBM Cognos Series 7.3 • IBM Cognos Business Intelligence 8.3
ETL	• (TBD)

Type	Supported Platforms and Components
Directory Integration and Authentication	- Microsoft Active Directory

Telecom

The SFO telecommunications network is comprised of an Avaya S8730 with Communications Manager running on CM load 5.x. The network is fully redundant, with CM media servers installed in separate and bio-metrically secured facilities. The network includes Avaya G650 nodes installed in strategic locations across the airport campus. These nodes are networked together to the CM media servers (main processors) via dual 1G Ethernet links connected to redundant Juniper EX4200 switches across a diverse fiber backbone. Inbound and outbound voice traffic is transported via 16 ISDN PRI DS1. The phone sets that are used are mixture of 2500 (analog) and 8400 and 6400 series digital sets. There is also a small deployment of H.323 IP soft phones. Also included in the overall telecommunications network are: Avaya Modular Messaging Voicemail Release 5.x, Avaya Meeting Exchange 5.1 Conference Bridge, and Sierra Gold Call Detail Recording system. The network supports approximately 4000 end users. The SFO Telecommunications staff operates and manages this network. Avaya is the system maintenance provider.

Figure 1 – SFO Telecommunication Infrastructure.



Systems Support and Maintenance

ITT Service Desk

The ITT Service Desk is responsible for fielding problem reports and requests for service and for providing Level 1 support. Events are documented as trouble tickets in an Incident Tracking System (ITS) database that is based on BMC/Remedy IT Service Management. Events that cannot be resolved immediately are routed to the appropriate ITT support group or 3rd party partner for follow-up and resolution. Vendors providing 1st-level support for SFO applications or systems are expected to create and manage tickets in Remedy directly, following agreed-upon processes and procedures.

ITT Network Operations Center

The Network Operations Center (NOC) is responsible for monitoring Airport systems as well as monitoring, maintaining, and provisioning the Cisco and SONET networks within the Airport Campus, providing Level 2 support as needed. NOC personnel are additionally charged with the installation and maintenance of the network management tools required in order to accomplish their prime tasks. Management tools include HP OpenView, CiscoWorks, SolarWinds, and Alcatel's NM1353GEM, 1301NMX and AMS. SiteScope is utilized for system monitoring, and BMC/Remedy's ITSM is used for trouble ticketing. Tickets for NOC support should be opened with the Service Desk, which will then escalate the ticket to the NOC.

Hours of Operation

Airport hours of operation are 24 hours per day, 365 days per year. ITT currently staffs NOC and Helpdesk positions during ITT Business Hours which are 07:00 – 19:00 Pacific Time, Monday through Friday, not including holidays. Outside these hours, Network and Helpdesk Support is currently subcontracted to Alcatel's Customer Network Operations Center (CNOC), with ITT maintaining on-call staff that is contacted and called out as needed and on a case-by-case basis. CNOC currently utilizes a dedicated T-1 circuit with backup VPN connections to the Airport networks in order to provide remote network monitoring services, and also a dedicated, branded, toll-free telephone line for receiving calls which are automatically transferred from the ITT Helpdesk phone switch during off-hours.

The City and County of San Francisco Airport Commission currently observers the following 11 holidays, which may be subject to change:

- New Years Day
- Martin L. King, Jr. Day
- President's Day
- Memorial Day
- Independence Day
- Labor Day
- Columbus Day

- Veteran's Day
- Thanksgiving Day
- Day after Thanksgiving
- Christmas Day

Should the holiday fall on a weekend, the holiday is observed on either the preceding Friday or following Monday.

Routine system maintenance is performed on server operating systems and hardware with the appropriate service level in place. Please contact SFO ITT for the standard list for your desired operating system, hardware combination.

Maintenance Windows

Scheduled maintenance is performed during a maintenance window of 1 AM – 4 AM, Pacific Standard Time (PST), or 2 AM – 5 AM, Pacific Daylight Time (PDT). The available days are Tuesday – Thursday. No changes may be made on holidays or during the period from the week of Thanksgiving through New Years Day. Advance notice must be given to customers/end users at least 48 hours in advance.

ITT Support may or may not be available to 3rd-party vendors or contractors during maintenance periods. Physical access to SFO facilities should be arranged through SFO business units, the Airport Duty Managers (ADMs) or otherwise as directed. Appropriate security badges will be required to access such facilities.

Shared Support Responsibilities

Where 3rd party support is required for a system, a Memorandum of Understanding (MOU) should be issued and signed for each system to clearly identify the division of responsibilities between SFO ITT and the 3rd party prior to any SLA is assumed.

Change Management Process

ITT has a formal change management process. Someone requesting a change is required to initiate the change request through a Remedy ticket. The change request will be directed to the service, system or process owner, who will evaluate it and manage the change control process. The request will be screened based on its urgency, impact and risk, and the change will be planned, reviewed and approved accordingly. Vendors, contractors, consultants and the like are expected to comply with ITT's change management policies.

Security and IT Best Practices

Site Security

As an airport, SFO has numerous security obligations and responsibilities. Access to the airport campus is a privilege, not a right. Compliance with Federal state and local security requirements is a necessity.

Security Zones: The airport can be roughly divided into 3 security zones: pre-security, post-security, and aircraft operation area (AOA). Each of these has different security requirements for access, badging, screening and materials handling.

Badges: Badges are required for access to most areas. Some badges require a security background check, to include fingerprinting, and site-specific training, before the badge can be issued. See www.flysfo.com/web/page/sao/info/badges for more information and forms.

Security Access Office (SAO): SAO is responsible for badging, keys, vehicle ramp passes, etc. They can be reached at: 650-821-5233, or www.flysfo.com/web/page/sao/info/sec .

Information Security

SFO's servers, networks and applications are subject to numerous security and QA standards and requirements. Some are derived from Federal agencies or standards (FAA, TSA, HIPAA, etc.), while other are industry requirements (PCI, ISO 27002, COBIT). While these and other standards and best practices are in varying stages of implementation, vendors, business partners, contractors and individual contributors are expected to comply with, and sustain, ITT's security, best practices and quality assurance initiatives.

ITT has begun a program to implement information security policies based on the Federal Information Security Management Act (FISMA) and ISO 17799-2005. The following table lists the initial documents current in development or approved.

Table 14 – ITT Information Security Policies

Doc ID	Title
SP-01	Creation of an Information Security Plan
SP-02	Roles and Responsibilities - CISO
SP-03	Roles and Responsibilities – Directors and Managers within ITT
SP-04	Positions of Special Trust
SP-05	Management of Authentication Identifiers
SP-06	Management of Passwords
SP-07	Management of Restricted Rights and Privileges
AT-01	Security Awareness and Training Policy and Procedures
CP-01	Contingency Planning Policy and Procedures

PM-01	Security Program Plan

For some of the recommended standards, especially NIST, that are current and/or future guidelines for SFO ITT policies, please refer to ***Appendix B***.

Best Practices

SFO ITT is a young organization evolved from the Airport Master Program. In order to meet the challenges of changing economy and business strategies of the Airport, ITT is currently actively engaged in a process to establish its practice standards. ITT has committed to industry “best practices,” as exemplified by ITIL version 3, Microsoft’s MOF, and so forth.

Quality Assurance

Quality Assurance is an important aspect of the ITT organization. Depending on the nature of the implementation, Test Plans and Test Case documentation may be required of the vendors.

For some of the recommended best practices that are current and/or future guidelines for SFO ITT policies, please refer to ***Appendix B***.

System Monitoring Requirements

Introduction

While there is no comprehensive, universal mechanism to collect fault and performance management data from a variety of hardware and software elements, two standards stand out as having very broad support: the Simple Network Management Protocol (SNMP), and the syslog protocol. The former was developed originally to manage network devices, and the latter to report operating system errors. Both now support numerous hardware and software platforms and applications.

As part of its criteria for procurement and/or support of hardware, software, and systems, SFO will evaluate the extent of a vendor’s support for one or both of these protocols. Vendors are strongly encouraged add or extend their support of these protocols, and to include that support as part of any RFPs.

This is an informal document that is intended to serve as the basis for detailed technical discussions of application logging, SNMP and syslog implementations and requirements. It is subject to change at any time.

The Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) has evolved from a protocol to manage router and switches to a ubiquitous means for managing and reporting on elements at all levels of the OSI protocol stack. All major operating systems support SNMP, as do major applications such as Oracle, Websphere, MS-Exchange, etc. Hardware vendors also support SNMP, including UPS manufacturers, blade server vendors, and storage product manufacturers, to mention just a few. Accordingly, support for SNMP is a critical part of our evaluation of vendors, and product. Further, we strongly encourage developers of custom applications to embed SNMP functionality into the application. There are commercial firms that sell SNMP development kits, and there are open source SNMP agents available as well. Finally, there are firms that perform SNMP conformance and interoperability testing, either as a service or as a software test suite.

This section is intended to collect the information necessary to evaluate vendor SNMP implementations. It is not exhaustive; in particular, it does not attempt to address the adequacy or completeness of a vendor’s own SNMP Management Information Base (MIB) modules. It does attempt to determine whether a vendor supports all of the Public MIBs appropriate for the device or application question.

SNMP Questions for Vendors

1. What public (i.e RFC-based) MIBs do you support? See Table 4 for examples.
2. Do you have private (enterprise) MIBs?
   2.1. If yes, can it be loaded into any SNMP manager?

   2.2. Does it contain any encrypted fields?
   2.3. Which other MIBs does it depend on?
3. Which version(s) of SNMP do you support?
4. Can your agent send traps?
   4.1. If yes, does it support multiple trap receivers?
   4.2. What kinds of conditions/events can generate a trap?
5. Can you agent be set to ignore management commands, e.g SETs?
6. Has your SNMP implementation been tested or certified by an independent SNMP testing organization?
7. Please provide a list of enterprise OID(s) supported by your application

Selected SNMP and Public MIB References

Appendix B contains references for the latest version of SNMP, together with selected MIBs, for various IETF RFCs. Preference has been given for SNMP V3, and references to V1 and the numerous V2 variants have been omitted. The text of the cited RFCs can be found at www.rfc-editor.org. It is understood that not all MIBs are applicable to all types of network elements. However, vendors are expected to conform to all applicable public MIBs, and to use private MIBs only for those functions not defined in a public MIB. This list is not necessarily complete, and the omission of a particular RFC should not be construed as meaning that there is not a compliance requirement. Vendors are encouraged to discuss the scope of their implementation with ITT as early as possible, and to furnish technical documentation and a copy of their MIB(s) for review. ***Appendix C*** is a SNMP MIB questionnaire designed to make it easy to indicate which MIBs are supported by a given device or application.

General Log File Objectives

All applications should log critical data for later use. Historically, applications and operating systems used log files for gathering run time data[1]. The kinds of data written to log files typically consist of the following:

- Contextual metadata – command line parameters, environmental variables, property file values, system variables, connection information, etc.
- Trace/debug data. Not usually used in production application, except when a startup switch/parameter is specified. There are usually multiple levels of debug output. This should go to a separate file, especially as it can be voluminous.
- Exception/error logging. Error, exceptions, and unexpected conditions. The quantity and verboseness of error messages should be parameter driven. Errors are the most common log data that is monitored.
- Statistics. This consists of information that measures the overall performance of the application and thr system it runs on.

[1] This paragraph is a re-statement of an informal paper by Lance Diduck; it can be found at: www.lancediduck.com/papers/logging/Monitoring and Logging.htm

- Transaction log data. This records discrete units of work performed by the application, together with relevant metadata, such as date and time, transaction size, checksums, etc.
- Security logs. This includes access control events, user account management, application configuration changes, unauthorized attempts access sensitive data, etc. This should be written to a separate file, preferably encrypted and cryptographically signed.

Systems and application logging provides invaluable data that can be used for monitoring, debugging, auditing, and forensics. It is arguable if an application can be considered "production ready" if it doesn't provide at least some logging. Additionally, consideration should be given to logging at least some data to standard mechanisms such as syslog servers.

Syslogs

Syslog was originally developed as a system logging utility in early BSD and BSD-derived Unix systems, hence the name. It was available to both the OS and to application that called the system's syslog API. The data, in a simple text format, was written to a single file, regardless of origin. Much, much later, the format was documented in RFC 3164, The BSD syslog Protocol.

Subsequently, a syslog protocol for writing to syslog files across TCP/IP networks was developed. The original implementations used UDP port 514. However, RFC 3195 defines several means to use TCP instead. Currently, work is underway by IETF to address numerous issues not considered in the original syslog standards, such as time synchronization, security, Unicode and internationalization, and format extensions.

SFO's expectation for vendors is that syslog will be supported in addition to SNMP. While there is a modest overlap between the protocols, they serve different purposes. SNMP is valuable for status, alerting and control, while syslog is useful for transaction tracking, error messages and routine event recording. Some applications have their own log file formats. Syslog is not a replacement for proprietary log formats. Instead it is a means to centralize collection of log data to facilitate troubleshoot and reporting across systems. Accordingly, vendors should support syslog in addition to any other logging they may perform.

Syslog Questions For Vendors

1. Do you support syslog functionality in your application or device?
   1.1. If yes, are you strictly compliant with RFC 3164; ie. do you include all fields, and do they conform to RFC 3164?
   1.2. If you support a variation of RFC 3164, describe the differences in the format.

- 1.3. Do you embed additional structured formatting in the Content sub-field portion of the syslog message?
- 1.4. In addition to syslog device functionality, do you support syslog relay or collector functionality?

2. Do you implement some or all of RFC 3195? If yes, which portions are supported?
3. Are you aware of the current IETF syslog draft standards, and if so, are you planning on implementing them?

Appendix A – Standards for OSI Layers 1-4

Table 15 lists major standards and protocols for layer 1 media and connectors, and layer 2 physical media-dependent (PMD) interfaces. Where newer standards overlap older standards, the newer standards shall be controlling.

Table 15 – OSI Layer 1 Physical and Layer 2 PMD Standards

OSI Layer 1 Physical and Layer 2 PMD Standards	
Organization	**Description**
ANSI/EIA/TIA	TIA/EIA-568-B (2001) Commercial Building Telecommunications Cabling Standard [see also TIA-568-C.0 *et seq*]
ANSI/EIA/TIA	TIA/EIA-568-B.1 General Requirements
ANSI/EIA/TIA	TIA/EIA-568-B.2 Balanced Twisted Pair Cabling Components [Cat 5e]
ANSI/EIA/TIA	TIA/EIA-568-B.2-1 Category 6 Transmission Performance
ANSI/EIA/TIA	TIA/EIA-568-B.2-10-2008 Addendum 10, Augmented Cat 6 Transmission Performance
ANSI/EIA/TIA	TIA/EIA-568-B.2.7 Addendum 7 Reliability Requirements for Connecting Hardware Used in Balanced Twisted-Pair Cabling
ANSI/EIA/TIA	TIA-568-C.0-2009 Generic Telecommunications Cabling for Customer Premises
ANSI/EIA/TIA	TIA-568-C.1-2009 Commercial Building Telecommunications Cabling Standard
ANSI/EIA/TIA	TIA-568-C.2-2009 Balanced Twisted-Pair Telecommunications Cabling and Components Standard
ANSI/EIA/TIA	TIA-568-C.3-2008 Optical Fiber Cabling Components Standard
ANSI/EIA/TIA	TIA-568-C.4 (draft) 75Ω Broadband Coaxial Structured Cabling and Components Standard
ISO/IEC	ISO 11801 2nd Ed., Information technology - Generic Cabling for Customer Premises, Amendment 1, Class E_A 2008 [Defines E_A and F_A channels]
ISO/IEC	ISO 11801 2nd Ed., Information technology - Generic Cabling for Customer Premises, Amendment 2, Class E_A draft [Defines ISO/IEC Cat 6A and 7A cabling and components; similar to EIA/TIA Cat 6 specs]
IEC	60793-2-10, Type A1b (OM-1 fiber) Optical Fibres - Part 2-10: Product Specifications - Sectional Specification for Category A1 Multimode Fibres
ANSI/EIA/TIA	ANSI/EIA/TIA-492AAAA-B-2008 Detail Specification for 62.5-um Core Diameter/l25-um Cladding Diameter Class Ia Graded-Index Multimode Optical Fibers [OM-1]
ANSI/EIA/TIA	ANSI/EIA/TIA-492AAAB-A-2008 Detail Specification for 50-um Core Diameter/l25-um Cladding Diameter Class Ia Graded-Index Multimode Optical Fibers [OM-2]
ANSI/EIA/TIA	ANSI/EIA/TIA-492AAAC-B-2008 Detail Specification for 850-nm Laser-Optimized, 50µm Core Diameter/ 125-µm Cladding Diameter Class Ia Graded-Index Multimode Optical Fibers [OM-3]
ANSI/EIA/TIA	ANSI/EIA/TIA-492AAAD-B-2009 Detail Specification for 850-nm Laser-Optimized, 50µm Core Diameter/ 125-µm Cladding Diameter Class Ia Graded-Index Multimode Optical Fibers [OM-4]

OSI Layer 1 Physical and Layer 2 PMD Standards	
Organization	**Description**
ITU-T	G.652.D Characteristics of a Single-Mode Optical Fibre and Cable, Low Water Peak
ITU-T	G.657, Category A Characteristics of Bend-Insensitive, Single Mode Optical Fibre and Cable for the Access Network
ISO/IEC	IEC 60793-2-50 B1.3:2008 Sectional Specification for Class B Single-Mode Fibres
ANSI/EIA/TIA	TIA/EIA-568-B.3 Optical Fiber Cabling Components
ANSI/EIA/TIA	TIA TSB-162 (2006) Telecommunications Cabling Guidelines for Wireless Access Points
SFF Committee	Gigabit Interface Converter (GBIC) Specification SFF-INF-8053i
SFF Committee	SFP (Small Form Factor Pluggable) Transceiver SFF-INF-8074i
SFF Committee	SFP+ (Enhanced Small Form Factor Pluggable Module “SFP+” SFF-8431
Telcordia	GR-320-CORE, Fundamental Generic Requirements for Metallic Digital Signal Cross-Connect Systems DSX-1, -1C, -2, -3 , Issue 1, Aug 2003 [same as Bellcore TR-NPL-000320, Issue 1, April 1988]
Telcordia	GR-139-CORE, Generic Requirements for Central Office Coaxial Cable, Issue 1, Oct 1996
ANSI	T1.417-2003(R2007) Spectrum Management
ATIS	PP-0600007 Dynamic Spectrum Management (DSM) Levels 0-3
ANSI/ATIS	T1.427.2 (2005) Ethernet-based multi-pair bonding [basis for G.998.2]
ITU	G.992.5 (2009) Asymmetric Digital Subscriber Line (ADSL) transceivers - Extended bandwidth ADSL2 (ADSL2+)
ITU	G.993.2 Very High-speed Digital Subscriber Line Service 2 w/Amendment 1 [VDSL 2
ITU	G.997.1 (2005) Physical layer management for DSL transceivers
ITU	G.998.2 (2005) Ethernet-based multi-pair bonding [adapted from T1.427.2]
ITU	G.998.3 (2005) Multi-pair bonding using time division inverse multiplexing
IEEE	802.3-2008 Ethernet Base Standards
IEEE	802.3az Energy Efficient Ethernet (draft 2.0)
IEEE	802.3u-1995 Fast Ethernet; 100BASE-TX, 100BASE-T4, 100BASE-FX
IEEE	802.3z-1998 1000BASE-X 1 Gbit/s over Fiber Optic Cabling
IEEE	802.3ab-1999 1000BASE-T 1 Gbit/s over Unshielded Twisted Pair Cabling
IEEE	802.3ae-2003 10GBASE-X 10 Gbit/s over Fiber Optic Cabling
IEEE	802.3an-2006 10GBASE-T 10 Gbit/s over Unshielded Twisted Pair Cabling
IEEE	802.3ah-2004 Ethernet in the First Mile (EFM) or 1 Gb EPON
IEEE	802.3av-2009 10Gb/s Passive Optical Networks (EPON)
IEEE	802.3aj Two-port MAC Relay (draft 3.3) [Supports 802.3ah and 802.1ad]
IEEE	802.11-2007 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications [WiFi; consolidates numerous amendments]

Table 16 lists major standards and protocols for layer 2 devices, interfaces and media.

Table 56 – OSI Layer 2 Switching and VLAN Standards

OSI Layer 2 Switching and VLAN Standards	
Organization	**Description**
IEEE	802.3ba 40-Gbit/s and 100 Gbit/s Ethernet (draft 2.2)
IEEE	802.1AB-2005 Link Layer Discovery Protocol (LLDP)
IEEE	802.1AB-REV Link Layer Discovery Protocol (draft 6) (LLDP)
IEEE	802.1ag-2007 Ethernet Connectivity Fault Management (CFM)
IEEE	802.1D-2004 MAC Bridges [Includes RSTP from 802.1w, 802.1p]
IEEE	802.1w Rapid Spanning-Tree Protocol (RSTP) [Included in 802.1D]
IEEE	802.1s Multiple STP (MSTP) [now part of 802.1q]
IEEE	802.1Q-2005 Virtual Bridged LANs (VLAN Tagging)
IEEE	802.1ad-2005 Provider Bridges (Q-in-Q or Stacked VLANs)
IEEE	802.1ah-2008 Provider Backbone Bridges (PBB) (Mac-in-Mac, or MinM)
IEEE	802.1Qay-2009 Provider Backbone Bridge Traffic Engineering (PBB-TE)
IEEE	802.1X-2004 Port Based Network Access Control
IEEE	802.1X-REV Port Based Network Access Control (draft 2.1)
IEEE	802.1AR Secure Device Identity (draft 2.1)
IEEE	802.1AE-2006 Media Access Control (MAC) Security
IEEE	802.1AS Timing and Synchronization (draft 6.1)
IEEE	1588-2008 Precision Clock Synchronization
IEEE	802.1p LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization [Included in 802.1D]
IEEE	802.3-2008 Ethernet Base Standards
IEEE	802.3ac-1998 Ethernet Frame Size Extension [to allow for VLAN tagging]
IEEE	802.3af-2005 Power over Ethernet
IEEE	802.3at-2009 POE Plus [aka Enhanced POE]
IEEE	802.1AS Timing and Synchronization (draft 5.0)
IEEE	802.1Qat Stream Reservation Protocol (draft 3.2)
IEEE	802.1Qau Congestion Notification (draft 2.2)
IEEE	802.1Qav Forwarding and Queuing Enhancements for Time-Sensitive Streams (draft 6.0)
IEEE	802.1Qaw-2009 Management of Data Driven and Data Dependent Connectivity Faults
IEEE	802.1Qaz Enhanced Transmission Selection (draft 0.3)
IEEE	802.1Qbb Priority-based Flow Control (draft 1.0)
IEEE	IEEE 802.11-2007 Wireless LAN PHY and MAC Standard [Incorporates 801.11a, b, d, e, g, h, i, j]
IEEE	IEEE 802.11a-1999(R2003) High-speed Physical Layer in the 5 GHz Band
IEEE	IEEE 802.11b-1999(R2003) Higher-Speed Physical Layer Extension in the 2.4 GHz Band
IEEE	IEEE 802.11g-2003 Further Higher Data Rate Extension in the 2.4 GHz Band
IEEE	IEEE 802.11e-2005 Medium Access Control (MAC) Quality of Service Enhancements
IEEE	IEEE 802.11i-2004 Medium Access Control (MAC) Security Enhancements
IEEE	IEEE 802.11k-2008 Radio Resource Measurement of Wireless LANs

OSI Layer 2 Switching and VLAN Standards	
Organization	**Description**
IEEE	IEEE 802.11r-2008 Fast Basic Service Set (BSS) Transition
IEEE	IEEE 802.11y-2008 3650-3700 MHz Operation in USA (Contention Based Protocol)
IEEE	IEEE 802.11n-2009 Enhancements for Higher Throughput
IEEE	IEEE 802.11s-(draft 3.0) Mesh Networking
IEEE	IEEE 802.11w-(draft 9.0) Protected Management Frames
IEEE	IEEE 802.11u-(draft 8.0) Interworking with External Networks
IEEE	IEEE 802.11v-(draft 5.0) Wireless Network Management
IEEE	802.1ak-2007 MRP, Multiple Registration Protocol [amends 802.1q-2005]
IEEE	802.1ak-2007 MMRP, Multiple MAC Registration Protocol [Uses MRP]
IEEE	802.1ak-2007 MVRP - Multiple VLAN Registration Protocol [Uses MRP]
IEEE	802.1ap-2009 Management Information Base (MIB) definitions for VLAN Bridges
IEEE	802.1aq Shortest Path Bridging (draft 2.0)
IEEE	IEEE 802.1AX-2008 Link Aggregation Control Protocol (LACP); formerly “802.3ad-2000”
IETF	SMLT - Split Multi-link Trunking [draft standard; IEEE 802.3ad extension]
IETF	RFC 3768 Virtual Router Redundancy Protocol (VRRP)
Cisco	PVST+ - Per-VLAN Spanning-Tree Plus Protocol
Cisco	PVRST - Per-VLAN Rapid Spanning-Tree Protocol
Cisco	Spanning Tree PortFast and PortFast guard
Cisco	Spanning Tree root guard
Cisco	VTP - VLAN Trunking Protocol, version 3
Cisco	Multicast VLAN Registration (MVR)
Cisco	DTP - Dynamic Trunking Protocol
Cisco	ISL - Inter-Switch Link [deprecated]
Cisco	DISL - Dynamic Inter-Switch Link Protocol
Cisco	EtherChannel [link bonding/trunking for up to 8 Ethernet links]
Cisco	

Table 17 lists major standards and protocols for layer 3/4 devices and applications. Only TCP/IP-related protocols are supported. The references have been grouped by subject matter, and shaded accordingly.

Table 67 – OSI Layer 3/4 Routing, Transport, Control and Related Standards

OSI Layer 3/4 Routing, Transport, Control and Related Standards	
Organization	**Description**
	IP
IETF	RFC 791 Internet Protocol
IETF	RFC 894 A Standard for the Transmission of IP Datagrams over Ethernet Networks
IETF	RFC 919 Broadcasting Internet Datagrams
IETF	RFC 922 Broadcasting Internet datagrams in the presence of subnets

OSI Layer 3/4 Routing, Transport, Control and Related Standards	
Organization	**Description**
IETF	RFC 950 Internet Standard Subnetting Procedure
IETF	RFC 1042 Standard for the transmission of IP datagrams over IEEE 802 networks
IETF	RFC 1112 Host extensions for IP multicasting
IETF	RFC 1918 Address Allocation for Private Internets
IETF	RFC 2113 IP Router Alert Option
IETF	RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
IETF	RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
IETF	RFC 2711 IPv6 Router Alert Option
IETF	RFC 3021 Using 31-Bit Prefixes on IPv4 Point-to-Point Links
IETF	RFC 3168 The Addition of Explicit Congestion Notification (ECN) to IP
IETF	RFC 3484 Default Address Selection for Internet Protocol version 6 (IPv6)
IETF	RFC 3587 IPv6 Global Unicast Address Format
IETF	RFC 4291 IP Version 6 Addressing Architecture
IETF	RFC 4293 Management Information Base for the Internet Protocol (IP) [MIB]
IETF	RFC 4632 Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan
IETF	RFC 4861 Neighbor Discovery for IP version 6 (IPv6)
IETF	RFC 4862 IPv6 Stateless Address Autoconfiguration
IETF	RFC 5389 Session Traversal Utilities for NAT (STUN)
	Differentiated Service (DiffServ)
IETF	RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
IETF	RFC 2475 An Architecture for Differentiated Service
IETF	RFC 2597 Assured Forwarding PHB Group
IETF	RFC 2697 A Single Rate Three Color Marker
IETF	RFC 2698 A Two Rate Three Color Marker
IETF	RFC 2998 A Framework for Integrated Services Operation over Diffserv Networks
IETF	RFC 3086 Definition of Differentiated Services Per Domain Behaviors and Rules for their Specification
IETF	RFC 3246 An Expedited Forwarding PHB (Per-Hop Behavior)
IETF	RFC 3260 New Terminology and Clarifications for Diffserv
IETF	RFC 3287 Remote Monitoring MIB Extensions for Differentiated Services [MIB]
IETF	RFC 3289 Management Information Base for the Differentiated Services Architecture [MIB]
IETF	RFC 3290 An Informal Management Model for Diffserv Routers
IETF	RFC 3662 A Lower Effort Per-Domain Behavior (PDB) for Differentiated Services
IETF	RFC 3670 Information Model for Describing Network Device QoS Datapath Mechanisms
IETF	RFC 3747 The Differentiated Services Configuration MIB
IETF	RFC 5127 Aggregation of DiffServ Service Classes

OSI Layer 3/4 Routing, Transport, Control and Related Standards	
Organization	**Description**
IETF	RFC 5455 Diffserv-Aware Class-Type Object for the Path Computation Element Communication Protocol
	ICMP
IETF	RFC 792 Internet Control Message Protocol
IETF	RFC 1191 Path MTU discovery
IETF	RFC 1256 ICMP Router Discovery Messages
IETF	RFC 1981 Path MTU Discovery for IP version 6
IETF	RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
IETF	RFC 4884 Extended ICMP to Support Multi-Part Messages
IETF	RFC 4950 ICMP Extensions for Multiprotocol Label Switching
IETF	RFC 5508 NAT Behavioral Requirements for ICMP
	TCP
IETF	RFC 793 Transmission Control Protocol
IETF	RFC 1323 TCP Extensions for High Performance
IETF	RFC 2018 TCP Selective Acknowledgment Options
IETF	RFC 2385 Protection of BGP Sessions via the TCP MD5 Signature Option
IETF	RFC 2581 TCP Congestion Control
IETF	RFC 2873 TCP Processing of the IPv4 Precedence Field
IETF	RFC 2883 An Extension to the Selective Acknowledgement (SACK) Option for TCP
IETF	RFC 2988 Computing TCP's Retransmission Timer
IETF	RFC 3042 Enhancing TCP's Loss Recovery Using Limited Transmit
IETF	RFC 3168 The Addition of Explicit Congestion Notification (ECN) to IP
IETF	RFC 3390 Increasing TCP's Initial Window
IETF	RFC 3517 A Conservative Selective Acknowledgment (SACK)-based Loss Recovery Algorithm for TCP
IETF	RFC 3562 Key Management Considerations for the TCP MD5 Signature Option
IETF	RFC 3782 The NewReno Modification to TCP's Fast Recovery Algorithm
IETF	RFC 4015 The Eifel Response Algorithm for TCP
IETF	RFC 4022 Management Information Base for the Transmission Control Protocol (TCP) [MIB]
IETF	RFC 4278 Standards Maturity Variance Regarding the TCP MD5 Signature Option (RFC 2385) and the BGP-4 Specification
IETF	RFC 4898 TCP Extended Statistics MIB
IETF	RFC 5382 NAT Behavioral Requirements for TCP
	UDP
IETF	RFC 768 User Datagram Protocol
IETF	RFC 4113 Management Information Base for the User Datagram Protocol (UDP) [MIB]
IETF	RFC 4787 Network Address Translation (NAT) Behavioral Requirements for Unicast UDP

OSI Layer 3/4 Routing, Transport, Control and Related Standards	
Organization	**Description**
IETF	RFC 5389 Session Traversal Utilities for NAT (STUN)
IETF	RFC 5405 Unicast UDP Usage Guidelines for Application Designers
	ARP/RARP
IETF	RFC 826 Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware [ARP]
IETF	RFC 903 A Reverse Address Resolution Protocol [RARP]
IETF	RFC 2390 Inverse Address Resolution Protocol
IETF	RFC 4338 Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel
	RFC 5227 IPv4 Address Conflict Detection
	RIP - Routing Information Protocol
IETF	RFC 1058 Routing Information Protocol
IETF	RFC 1724 RIP Version 2 MIB Extension
IETF	RFC 2453 Routing Information Protocol, Version 2 (RIPv2)
IETF	RFC 4822 RIPv2 Cryptographic Authentication
	OSPF
IETF	RFC 1793 Extending OSPF to Support Demand Circuits
IETF	RFC 2328 OSPF Version 2
IETF	RFC 3101 The OSPF Not-So-Stubby Area (NSSA) Option
IETF	RFC 3137 OSPF Stub Router Advertisement
IETF	RFC 3509 Alternative Implementations of OSPF Area Border Routers
IETF	RFC 3623 Graceful OSPF Restart
IETF	RFC 3630 Traffic Engineering (TE) Extensions to OSPF Version 2
IETF	RFC 3883 Detecting Inactive Neighbors over OSPF Demand Circuits (DC)
IETF	RFC 3906 Calculating Interior Gateway Protocol (IGP) Routes Over Traffic Engineering Tunnels
IETF	RFC 4124 Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering
IETF	RFC 4136 OSPF Refresh and Flooding Reduction in Stable Topologies
IETF	RFC 4203 OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)
IETF	RFC 4206 Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)
IETF	RFC 4552 Authentication/Confidentiality for OSPFv3
IETF	RFC 4576 Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)
IETF	RFC 4577 OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)
IETF	RFC 4750 OSPF Version 2 Management Information Base [MIB]
IETF	RFC 4811 OSPF Out-of-Band Link State Database (LSDB) Resynchronization
IETF	RFC 4812 OSPF Restart Signaling

OSI Layer 3/4 Routing, Transport, Control and Related Standards	
Organization	**Description**
IETF	RFC 4813 OSPF Link-Local Signaling
IETF	RFC 4915 Multi-Topology (MT) Routing in OSPF
IETF	RFC 4970 Extensions to OSPF for Advertising Optional Router Capabilities
IETF	RFC 5082 The Generalized TTL Security Mechanism (GTSM)
IETF	RFC 5088 OSPF Protocol Extensions for Path Computation Element (PCE) Discovery
IETF	RFC 5185 OSPF Multi-Area Adjacency
IETF	RFC 5187 OSPFv3 Graceful Restart
IETF	RFC 5250 The OSPF Opaque LSA Option
IETF	RFC 5286 Basic Specification for IP Fast Reroute: Loop-Free Alternates
IETF	RFC 5309 Point-to-Point Operation over LAN in Link State Routing Protocols
IETF	RFC 5329 Traffic Engineering Extensions to OSPF Version 3
IETF	RFC 5340 OSPF for IPv6
IETF	RFC 5443 LDP IGP Synchronization
IETF	RFC 5523 OSPF-Based Layer 1 VPN Auto-Discovery
IETF	RFC 5643 Management Information Base for OSPFv3 [MIB]
	IS-IS
ISO/IEC	ISO 10589:1992 - Intermediate System to Intermediate System Intra-Domain Routing Exchange Protocol for use in Conjunction with the Protocol for Providing the Connectionless-mode Network Service (ISO 8473) [IS-IS]
IETF	RFC 1142 OSI IS-IS Intra-domain Routing Protocol
IETF	RFC 1195 Use of OSI IS-IS for routing in TCP/IP and dual environments
IETF	RFC 2763 Dynamic Hostname Exchange Mechanism for IS-IS
IETF	RFC 2973 IS-IS Mesh Groups
IETF	RFC 3277 Intermediate System to Intermediate System (IS-IS) Transient Blackhole Avoidance
IETF	RFC 3359 Reserved Type, Length and Value (TLV) Codepoints in Intermediate System to Intermediate System
IETF	RFC 3719 Recommendations for Interoperable Networks using Intermediate System to Intermediate System (IS-IS)
IETF	RFC 3786 Extending the Number of Intermediate System to Intermediate System (IS-IS) Link State PDU (LSP) Fragments Beyond the 256 Limit
IETF	RFC 3787 Recommendations for Interoperable IP Networks using Intermediate System to Intermediate System (IS-IS)
IETF	RFC 4444 Management Information Base (MIB) for Intermediate System to Intermediate System (IS-IS) [MIB]
IETF	RFC 4971 Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information
IETF	RFC 5029 Definition of an IS-IS Link Attribute Sub-TLV
IETF	RFC 5120 M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)
IETF	RFC 5130 A Policy Control Mechanism in IS-IS Using Administrative

OSI Layer 3/4 Routing, Transport, Control and Related Standards	
Organization	**Description**
	Tags
IETF	RFC 5301 Dynamic Hostname Exchange Mechanism for IS-IS
IETF	RFC 5302 Domain-Wide Prefix Distribution with Two-Level IS-IS
IETF	RFC 5303 Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies
IETF	RFC 5304 Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication
IETF	RFC 5305 Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)
IETF	RFC 5306 Restart Signaling for Intermediate System to Intermediate System (IS-IS)
IETF	RFC 5307 IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)
IETF	RFC 5308 Routing IPv6 with IS-IS
IETF	RFC 5309 Point-to-Point Operation over LAN in Link State Routing Protocols
IETF	RFC 5310 IS-IS Generic Cryptographic Authentication
IETF	RFC 5311 Simplified Extension of Link State PDU (LSP) Space for IS-IS
	EIGRP
Cisco	EIGRP - Enhanced Interior Gateway Routing Protocol
	BGP
IETF	RFC 1772 Application of the Border Gateway Protocol in the Internet
IETF	RFC 1996 BGP Route Reflection - An alternative to full mesh IBGP
IETF	RFC 1997 BGP Communities Attribute
IETF	RFC 2385 Protection of BGP Sessions via the TCP MD5 Signature Option
IETF	RFC 2439 BGP Route Flap Damping
IETF	RFC 2545 Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
IETF	RFC 2796 BGP Route Reflection - An alternative to full mesh IBGP
IETF	RFC 2918 Route Refresh Capability for BGP-4
IETF	RFC 3107 Carrying Label Information in BGP-4
IETF	RFC 3392 Capabilities Advertisement with BGP-4
IETF	RFC 4271 A Border Gateway Protocol 4 (BGP-4)
IETF	RFC 4272 BGP Security Vulnerabilities Analysis
IETF	RFC 4273 Definitions of Managed Objects for BGP-4 [MIB]
IETF	RFC 4360 BGP Extended Communities Attribute
IETF	RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs)
IETF	RFC 4456 BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)
IETF	RFC 4486 Subcodes for BGP Cease Notification Message
IETF	RFC 4724 Graceful Restart Mechanism for BGP
IETF	RFC 4760 Multiprotocol Extensions for BGP-4
IETF	RFC 4761 Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling

OSI Layer 3/4 Routing, Transport, Control and Related Standards	
Organization	**Description**
IETF	RFC 4781 Graceful Restart Mechanism for BGP with MPLS
IETF	RFC 4893 BGP Support for Four-octet AS Number Space
IETF	RFC 5004 Avoid BGP Best Path Transitions from One External to Another
IETF	RFC 5065 Autonomous System Confederations for BGP
IETF	RFC 5195 BGP-Based Auto-Discovery for Layer-1 VPNs
IETF	RFC 5492 Capabilities Advertisement with BGP-4
	DHCP
IETF	RFC 2131 Dynamic Host Configuration Protocol
IETF	RFC 2132 DHCP Options and BOOTP Vendor Extensions
IETF	RFC 2563 DHCP Option to Disable Stateless Auto-Configuration in IPv4 Clients
IETF	RFC 2937 The Name Service Search Option for DHCP
IETF	RFC 3004 The User Class Option for DHCP
IETF	RFC 3011 The IPv4 Subnet Selection Option for DHCP
IETF	RFC 3046 DHCP Relay Agent Information Option
IETF	RFC 3118 Authentication for DHCP Messages
IETF	RFC 3203 DHCP reconfigure extension
IETF	RFC 3396 Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)
IETF	RFC 3442 The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4
IETF	RFC 3456 Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode
IETF	RFC 3527 Link Selection sub-option for the Relay Agent Information Option for DHCPv4
IETF	RFC 3925 Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)
IETF	RFC 3942 Reclassifying Dynamic Host Configuration Protocol version 4 (DHCPv4) Options
IETF	RFC 4014 Remote Authentication Dial-In User Service (RADIUS) Attributes Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option
IETF	RFC 4030 The Authentication Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option
IETF	RFC 4243 Vendor-Specific Information Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option
IETF	RFC 4280 Dynamic Host Configuration Protocol (DHCP) Options for Broadcast and Multicast Control Servers
IETF	RFC 4332 Cisco's Mobile IPv4 Host Configuration Extensions
IETF	RFC 4361 Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)
IETF	RFC 4388 Dynamic Host Configuration Protocol (DHCP) Leasequery
IETF	RFC 4833 Timezone Options for DHCP
IETF	RFC 5010 The Dynamic Host Configuration Protocol Version 4 (DHCPv4) Relay Agent Flags Suboption

OSI Layer 3/4 Routing, Transport, Control and Related Standards	
Organization	**Description**
IETF	RFC 5107 DHCP Server Identifier Override Suboption
	MPLS and Related Standards
IETF	RFC 2702 Requirements for Traffic Engineering Over MPLS
IETF	RFC 3031 Multiprotocol Label Switching Architecture
IETF	RFC 3032 MPLS Label Stack Encoding
IETF	RFC 3270 Multi-Protocol Label Switching (MPLS) Support of Differentiated Services
IETF	RFC 3272 Overview and Principles of Internet Traffic Engineering
IETF	RFC 3443 Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks
IETF	RFC 3468 The Multiprotocol Label Switching (MPLS) Working Group decision on MPLS signaling protocols
IETF	RFC 3469 Framework for Multi-Protocol Label Switching (MPLS)-based Recovery
IETF	RFC 3471 Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description
IETF	RFC 3478 Graceful Restart Mechanism for Label Distribution Protocol
IETF	RFC 3564 Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering
IETF	RFC 3785 Use of Interior Gateway Protocol (IGP) Metric as a second MPLS Traffic Engineering (TE) Metric
IETF	RFC 3812 Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB) [MIB]
IETF	RFC 3813 Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB) [MIB]
IETF	RFC 3970 A Traffic Engineering (TE) MIB [MIB]
IETF	RFC 3814 Multiprotocol Label Switching (MPLS) Forwarding Equivalence Class To Next Hop Label Forwarding Entry (FEC-To-NHLFE) Management Information Base (MIB) [MIB]
IETF	RFC 4023 Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)
IETF	RFC 4090 Fast Reroute Extensions to RSVP-TE for LSP Tunnels
IETF	RFC 4124 Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering
IETF	RFC 4125 Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering
IETF	RFC 4126 Max Allocation with Reservation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering & Performance Comparisons
IETF	RFC 4127 Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering
IETF	RFC 4182 Removing a Restriction on the use of MPLS Explicit NULL
IETF	RFC 4201 Link Bundling in MPLS Traffic Engineering (TE)
IETF	RFC 4203 OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)
IETF	RFC 4220 Traffic Engineering Link Management Information Base [MIB]
IETF	RFC 4221 Multiprotocol Label Switching (MPLS) Management Overview

OSI Layer 3/4 Routing, Transport, Control and Related Standards

Organization	Description
IETF	RFC 4328 Generalized Multi-Protocol Label Switching (GMPLS) Signaling Extensions for G.709 Optical Transport Networks Control
IETF	RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs)
IETF	RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures
IETF	RFC 4382 MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base [MIB]
IETF	RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks
IETF	RFC 4576 Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)
IETF	RFC 4577 OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)
IETF	RFC 4618 Encapsulation Methods for Transport of PPP/High-Level Data Link Control (HDLC) over MPLS Networks [Martini]
IETF	RFC 4619 Encapsulation Methods for Transport of Frame Relay over MPLS Networks
IETF	RFC 4631 Link Management Protocol (LMP) Management Information Base (MIB)
IETF	RFC 4684 Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)
IETF	RFC 4761 Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling
IETF	RFC 4762 Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling [H-VPLS]
IETF	RFC 4972 Routing Extensions for Discovery of Multiprotocol (MPLS) Label Switch Router (LSR) Traffic Engineering (TE) Mesh Membership
IETF	RFC 4801 Definitions of Textual Conventions for Generalized Multiprotocol Label Switching (GMPLS) Management
IETF	RFC 4802 Generalized Multiprotocol Label Switching (GMPLS) Traffic Engineering Management Information Base [MIB]
IETF	RFC 4803 Generalized Multiprotocol Label Switching (GMPLS) Label Switching Router (LSR) Management Information Base [MIB]
IETF	RFC 5036 LDP Specification [Label Distribution Protocol]
IETF	RFC 5129 Explicit Congestion Marking in MPLS
IETF	RFC 5283 LDP Extension for Inter-Area LSPs
IETF	RFC 5332 MPLS Multicast Encapsulations
IETF	RFC 5462 Multiprotocol Label Switching (MPLS) Label Stack Entry: EXP Field Renamed to Traffic Class Field
IETF	RFC 5586 MPLS Generic Associated Channel
	RSVP
IETF	RFC 2205 Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification
IETF	RFC 2206 RSVP Management Information Base using SMIv2 [MIB]
IETF	RFC 2750 RSVP Extensions for Policy Control

OSI Layer 3/4 Routing, Transport, Control and Related Standards	
Organization	**Description**
IETF	RFC 2961 RSVP Refresh Overhead Reduction Extensions
IETF	RFC 3209 RSVP-TE: Extensions to RSVP for LSP Tunnels
IETF	RFC 3473 Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions
IETF	RFC 3936 Procedures for Modifying the Resource reSerVation Protocol (RSVP)
IETF	RFC 4090 Fast Reroute Extensions to RSVP-TE for LSP Tunnels
IETF	RFC 4495 A Resource Reservation Protocol (RSVP) Extension for the Reduction of Bandwidth of a Reservation Flow
IETF	RFC 4783 GMPLS - Communication of Alarm Information
IETF	RFC 4872 RSVP-TE Extensions in Support of End-to-End Generalized Multi-Protocol Label Switching (GMPLS) Recovery
IETF	RFC 4873 GMPLS Segment Recovery
IETF	RFC 4874 Exclude Routes - Extension to Resource ReserVation Protocol-Traffic Engineering (RSVP-TE)
IETF	RFC 4974 Generalized MPLS (GMPLS) RSVP-TE Signaling Extensions in Support of Calls
IETF	RFC 5063 Extensions to GMPLS Resource Reservation Protocol (RSVP) Graceful Restart
IETF	RFC 5151 Inter-Domain MPLS and GMPLS Traffic Engineering -- Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions
IETF	RFC 5420 Encoding of Attributes for MPLS LSP Establishment Using Resource Reservation Protocol Traffic Engineering (RSVP-TE)
	BFD
IETF	draft-ietf-bfd-base-09.txt Bidirectional Forwarding Detection [BFD]
IETF	draft-ietf-bfd-generic-05.txt Generic Application of BFD
IETF	draft-ietf-bfd-v4v6-1hop-09.txt BFD for IPv4 and IPv6 (Single Hop)
IETF	draft-ietf-bfd-mpls-07.txt BFD For MPLS LSPs
IETF	draft-ietf-bfd-multihop-07.txt BFD for Multihop Paths
IETF	draft-katz-ward-bfd-multipoint-02.txt BFD for Multipoint Networks
IETF	draft-ietf-bfd-mib-07 BFD Management Information Base
	Pseudowire and Circuit Emulation
IETF	RFC 3985 Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture
IETF	RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks [Martini]
IETF	RFC 4553 Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
IETF	RFC 4623 Pseudowire Emulation Edge-to-Edge (PWE3) Fragmentation and Reassembly
IETF	RFC 4720 Pseudowire Emulation Edge-to-Edge (PWE3) Frame Check Sequence Retention
IETF	RFC 4863 Wildcard Pseudowire Type
IETF	RFC 5003 Attachment Individual Identifier (AII) Types for Aggregation

OSI Layer 3/4 Routing, Transport, Control and Related Standards	
Organization	**Description**
IETF	RFC 5085 Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires
IETF	RFC 5086 Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)
IETF	RFC 5087 Time Division Multiplexing over IP (TDMoIP)
	RFC 5254 Requirements for Multi-Segment Pseudowire Emulation Edge-to-Edge (PWE3)
	RFC 5287 Control Protocol Extensions for the Setup of Time-Division Multiplexing (TDM) Pseudowires in MPLS Networks
	RFC 5542 Definitions of Textual Conventions for Pseudowire (PW) Management
	RFC 5601 Pseudowire (PW) Management Information Base (MIB)
	RFC 5602 Pseudowire (PW) over MPLS PSN Management Information Base (MIB)
	RFC 5603 Ethernet Pseudowire (PW) Management Information Base (MIB)
	RFC 5604 Managed Objects for Time Division Multiplexing (TDM) over Packet Switched Networks (PSNs)
	NTP
IETF	Network Time Protocol (Version 3) Specification, Implementation and Analysis
IETF/ntp.org	draft-ietf-ntp-ntpv4-proto-11.txt. V4 (4.24). See support.ntp.org/bin/view/Main/WebHome for source code
IETF	draft-ietf-ntp-ntpv4-mib-05
IETF	draft-ietf-ntp-autokey-06
IETF	draft-ietf-ntp-dhcpv6-ntp-opt-04
ntp.org	V4 (4.24p7). See support.ntp.org/bin/view/Main/WebHome for source code
	NETCONF
IETF	RFC 4741 NETCONF Configuration Protocol
IETF	RFC 4742 Using the NETCONF Configuration Protocol over Secure SHell (SSH)
IETF	RFC 4743 Using NETCONF over the Simple Object Access Protocol (SOAP)
IETF	RFC 5277 NETCONF Event Notifications
IETF	RFC 5539 NETCONF over Transport Layer Security (TLS)
	IGMP and Multicasting
IETF	RFC 2365 Administratively Scoped IP Multicast
IETF	RFC 2934 Protocol Independent Multicast MIB for IPv4
IETF	RFC 3446 Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)
IETF	RFC 3376 Internet Group Management Protocol (IGMPv3)
IETF	RFC 3569 An Overview of Source-Specific Multicast (SSM)

OSI Layer 3/4 Routing, Transport, Control and Related Standards	
Organization	**Description**
IETF	RFC 3618 Multicast Source Discovery Protocol (MSDP)
IETF	RFC 3973 Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)
IETF	RFC 4286 Multicast Router Discovery
IETF	RFC 4541 Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
IETF	RFC 4601 Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)
IETF	RFC 4604 Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast
IETF	RFC 4605 Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding (IGMP/MLD Proxying)
IETF	RFC 4609 Protocol Independent Multicast - Sparse Mode (PIM-SM) Multicast Routing Security Issues and Enhancements
IETF	RFC 4610 Anycast-RP Using Protocol Independent Multicast (PIM)
IETF	RFC 4611 Multicast Source Discovery Protocol (MSDP) Deployment Scenarios
IETF	RFC 5015 Bidirectional Protocol Independent Multicast (BIDIR-PIM)
IETF	RFC 5059 Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)
IETF	RFC 5060 Protocol Independent Multicast MIB
IETF	RFC 5132 IP Multicast MIB
IETF	RFC 5240 Protocol Independent Multicast (PIM) Bootstrap Router MIB
IETF	RFC 5501 Requirements for Multicast Support in Virtual Private LAN Services [VPLS]
IETF	RFC 5519 Multicast Group Membership Discovery MIB
	Telnet
IETF	RFC 854 Telnet Protocol Specification
IETF	RFC 855 Telnet Option Specifications
IETF	RFC 856 Telnet Binary Transmission
IETF	RFC 857 Telnet Echo Option
IETF	RFC 858 Telnet Suppress Go Ahead Option
IETF	RFC 859 Telnet Status Option
IETF	RFC 1073 Telnet window size option
IETF	RFC 1079 Telnet terminal speed option
IETF	RFC 1091 Telnet terminal-type option
	FTP
IETF	RFC 959 File Transfer Protocol (FTP)
IETF	RFC 2228 FTP Security Extensions
IETF	RFC 2428 FTP Extensions for IPv6 and NATs
IETF	RFC 2640 Internationalization of the File Transfer Protocol (FTP)
IETF	RFC 3659 Extensions to FTP

OSI Layer 3/4 Routing, Transport, Control and Related Standards	
Organization	**Description**
	TFTP
IETF	RFC 1350 The TFTP Protocol (Revision 2)
IETF	RFC 1785 TFTP Option Negotiation Analysis
IETF	RFC 2347 TFTP Option Extension
IETF	RFC 2348 TFTP Blocksize Option
IETF	RFC 2349 TFTP Timeout Interval and Transfer Size Options
IETF	RFC 3617 Uniform Resource Identifier (URI) Scheme and Applicability Statement for the Trivial File Transfer Protocol (TFTP)
	PPP
IETF	RFC 1332 The PPP Internet Protocol Control Protocol (IPCP)
IETF	RFC 1471 The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol [MIB]
IETF	RFC 1472 The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol [MIB]
IETF	RFC 1473 The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol [MIB]
IETF	RFC 1661 The Point-to-Point Protocol (PPP)
IETF	RFC 1662 PPP in HDLC-like Framing
IETF	RFC 2153 PPP Vendor Extensions
IETF	RFC 2615 PPP over SONET/SDH
IETF	RFC 3241 Robust Header Compression (ROHC) over PPP
IETF	RFC 4815 RObust Header Compression (ROHC): Corrections and Clarifications to RFC 3095
IETF	RFC 5072 IP Version 6 over PPP
IETF	RFC 5172 Negotiation for IPv6 Datagram Compression Using IPv6 Control Protocol
	SIP (Session Initiation Protocol)
IETF	RFC 3261 SIP: Session Initiation Protocol
IETF	RFC 3262 Reliability of Provisional Responses in Session Initiation Protocol (SIP)
IETF	RFC 3263 Session Initiation Protocol (SIP): Locating SIP Servers
IETF	RFC 3264 An Offer/Answer Model with Session Description Protocol (SDP)
IETF	RFC 3265 Session Initiation Protocol (SIP)-Specific Event Notification
IETF	RFC 3515 The Session Initiation Protocol (SIP) Refer Method
IETF	RFC 4780 Management Information Base for the Session Initiation Protocol (SIP) [MIB]
IETF	RFC 5367 Subscriptions to Request-Contained Resource Lists in the Session Initiation Protocol (SIP)
	RTP
IETF	RFC 2250 RTP Payload Format for MPEG1/MPEG2 Video
IETF	RFC 2959 Real-Time Transport Protocol Management Information Base

OSI Layer 3/4 Routing, Transport, Control and Related Standards	
Organization	**Description**
	[RTP MIB]
IETF	RFC 3016 RTP Payload Format for MPEG-4 Audio/Visual Streams
IETF	RFC 3550 RTP: A Transport Protocol for Real-Time Applications
IETF	RFC 3551 RTP Profile for Audio and Video Conferences with Minimal Control
IETF	RFC 3611 RTP Control Protocol Extended Reports (RTCP XR)
IETF	RFC 3640 RTP Payload Format for Transport of MPEG-4 Elementary Streams
IETF	RFC 3711 The Secure Real-time Transport Protocol (SRTP)
IETF	RFC 4585 Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)
IETF	RFC 4629 RTP Payload Format for ITU-T Rec. H.263 Video
IETF	RFC 5391 RTP Payload Format for ITU-T Recommendation G.711.1
IETF	RFC 5506 Support for Reduced-Size Real-Time Transport Control Protocol (RTCP): Opportunities and Consequences
	SDP - Session Description Protocol
IETF	RFC 3264 An Offer/Answer Model with Session Description Protocol (SDP)
IETF	RFC 3388 Grouping of Media Lines in the Session Description Protocol (SDP)
IETF	RFC 3407 Session Description Protocol (SDP) Simple Capability Declaration
IETF	RFC 3524 Mapping of Media Streams to Resource Reservation Flows
IETF	RFC 3556 Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth
IETF	RFC 3605 Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)
IETF	RFC 3890 A Transport Independent Bandwidth Modifier for the Session Description Protocol (SDP)
IETF	RFC 4091 The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework
IETF	RFC 4092 Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)
IETF	RFC 4145 TCP-Based Media Transport in the Session Description Protocol (SDP)
IETF	RFC 4298 RTP Payload Format for BroadVoice Speech Codecs
IETF	RFC 4566 SDP: Session Description Protocol
IETF	RFC 4567 Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)
IETF	RFC 4568 Session Description Protocol (SDP) Security Descriptions for Media Streams
IETF	RFC 4570 Session Description Protocol (SDP) Source Filters
IETF	RFC 4572 Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)
IETF	RFC 4574 The Session Description Protocol (SDP) Label Attribute

OSI Layer 3/4 Routing, Transport, Control and Related Standards	
Organization	**Description**
IETF	RFC 5027 Security Preconditions for Session Description Protocol (SDP) Media Streams
IETF	RFC 5432 Quality of Service (QoS) Mechanism Selection in the Session Description Protocol (SDP)
IETF	RFC 5547 A Session Description Protocol (SDP) Offer/Answer Mechanism to Enable File Transfer
	Security – General and Miscellaneous
IETF	RFC 1321 The MD5 Message-Digest Algorithm
IETF	RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)
IETF	RFC 2385 Protection of BGP Sessions via the TCP MD5 Signature Option
	RADIUS
IETF	RFC 2548 Microsoft Vendor-specific RADIUS Attributes
IETF	RFC 2607 Proxy Chaining and Policy Implementation in Roaming
IETF	RFC 2809 Implementation of L2TP Compulsory Tunneling via RADIUS
IETF	RFC 2865 Remote Authentication Dial In User Service (RADIUS)
IETF	RFC 2866 RADIUS Accounting
IETF	RFC 2867 RADIUS Accounting Modifications for Tunnel Protocol Support
IETF	RFC 2868 RADIUS Attributes for Tunnel Protocol Support
IETF	RFC 2869 RADIUS Extensions
IETF	RFC 2882 Network Access Servers Requirements: Extended RADIUS Practices
IETF	RFC 3162 RADIUS and IPv6
IETF	RFC 3579 RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)
IETF	RFC 3580 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines
IETF	RFC 4372 Chargeable User Identity
IETF	RFC 4672 RADIUS Dynamic Authorization Client MIB
IETF	RFC 4673 RADIUS Dynamic Authorization Server MIB
IETF	RFC 4679 DSL Forum Vendor-Specific RADIUS Attributes
IETF	RFC 4849 RADIUS Filter Rule Attribute
IETF	RFC 5080 Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes
IETF	RFC 5090 RADIUS Extension for Digest Authentication
IETF	RFC 5176 Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)
IETF	RFC 5607 Remote Authentication Dial-In User Service (RADIUS) Authorization for Network Access Server (NAS) Management
	EAP - Extensible Authentication Protocol
IETF	RFC 3748 Extensible Authentication Protocol (EAP) [EAP-MD5]
IETF	RFC 4017 Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs
IETF	RFC 4334 Certificate Extensions and Attributes Supporting Authentication

OSI Layer 3/4 Routing, Transport, Control and Related Standards	
Organization	**Description**
	in Point-to-Point Protocol (PPP) and Wireless Local Area Networks (WLAN)
IETF	RFC 4746 Extensible Authentication Protocol (EAP) Password Authenticated Exchange
IETF	RFC 4764 The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method
IETF	RFC 4793 The EAP Protected One-Time Password Protocol (EAP-POTP)
IETF	RFC 5216 The EAP-TLS Authentication Protocol
IETF	RFC 5247 Extensible Authentication Protocol (EAP) Key Management Framework
IETF	RFC 5281 Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)
IETF	draft-funk-eap-ttls-v1-01 Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv1)
IETF	draft-kamath-pppext-peapv0-00 Protected Extensible Authentication Protocol (PEAPv0/EAP-MSCHAPv2)
IETF	draft-josefsson-pppext-eap-tls-eap-10 Protected Extensible Authentication Protocol (PEAPv1/EAP-GTC)
	Kerberos
IETF	RFC 1964 The Kerberos Version 5 GSS-API Mechanism
IETF	RFC 2712 Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)
IETF	RFC 2942 Telnet Authentication: Kerberos Version 5
IETF	RFC 3961 Encryption and Checksum Specifications for Kerberos 5
IETF	RFC 3962 Advanced Encryption Standard (AES) Encryption for Kerberos 5
IETF	RFC 4120 The Kerberos Network Authentication Service (V5)
IETF	RFC 4121 The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2
IETF	RFC 4402 A Pseudo-Random Function (PRF) for the Kerberos V Generic Security Service Application Program Interface (GSS-API) Mechanism
IETF	RFC 4537 Kerberos Cryptosystem Negotiation Extension
IETF	RFC 4556 Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)
IETF	RFC 4557 Online Certificate Status Protocol (OCSP) Support for Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)
IETF	RFC 4559 SPNEGO-based Kerberos and NTLM HTTP Authentication in Microsoft Windows
IETF	RFC 4752 The Kerberos V5 (GSSAPI) Simple Authentication and Security Layer (SASL) Mechanism
IETF	RFC 4757 The RC4-HMAC Kerberos Encryption Types Used by Microsoft Windows
IETF	RFC 5021 Extended Kerberos Version 5 Key Distribution Center (KDC) Exchanges over TCP
IETF	RFC 5179 Generic Security Service Application Program Interface (GSS-API) Domain-Based Service Names Mapping for the Kerberos V GSS

OSI Layer 3/4 Routing, Transport, Control and Related Standards	
Organization	**Description**
	Mechanism
IETF	RFC 5349 Elliptic Curve Cryptography (ECC) Support for Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)
IETF	RFC 5403 RPCSEC_GSS Version 2
	IPsec
IETF	RFC 1828 IP Authentication using Keyed MD5
IETF	RFC 2085 HMAC-MD5 IP Authentication with Replay Prevention
IETF	RFC 2403 The Use of HMAC-MD5-96 within ESP and AH
IETF	RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH
IETF	RFC 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV
IETF	RFC 2410 The NULL Encryption Algorithm and Its Use With IPsec
IETF	RFC 2451 The ESP CBC-Mode Cipher Algorithms
IETF	RFC 2631 Diffie-Hellman Key Agreement Method
IETF	RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPsec
IETF	RFC 4301 Security Architecture for the Internet Protocol
IETF	RFC 4302 IP Authentication Header
IETF	RFC 4303 IP Encapsulating Security Payload (ESP)
IETF	RFC 4304 Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)
IETF	RFC 4306 Internet Key Exchange (IKEv2) Protocol
IETF	RFC 4835 Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
IETF	RFC 5282 Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol
	TLS - Transport Layer Security
IETF	RFC 2595 Using TLS with IMAP, POP3 and ACAP
IETF	RFC 2712 Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)
IETF	RFC 2817 Upgrading to TLS Within HTTP/1.1
IETF	RFC 2818 HTTP Over TLS
IETF	RFC 3207 SMTP Service Extension for Secure SMTP over Transport Layer Security
IETF	RFC 3436 Transport Layer Security over Stream Control Transmission Protocol
IETF	RFC 3749 Transport Layer Security Protocol Compression Methods
IETF	RFC 4217 Securing FTP with TLS
IETF	RFC 4279 Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)
IETF	RFC 4492 Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)
IETF	RFC 4616 The PLAIN Simple Authentication and Security Layer (SASL) Mechanism
IETF	RFC 4785 Pre-Shared Key (PSK) Ciphersuites with NULL Encryption for Transport Layer Security (TLS)

OSI Layer 3/4 Routing, Transport, Control and Related Standards	
Organization	**Description**
IETF	RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2
IETF	RFC 5281 Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)
IETF	RFC 5288 AES Galois Counter Mode (GCM) Cipher Suites for TLS
IETF	RFC 5289 TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)
IETF	RFC 5425 Transport Layer Security (TLS) Transport Mapping for Syslog
IETF	RFC 5487 Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode
IETF	RFC 5734 Extensible Provisioning Protocol (EPP) Transport over TCP
	SNMP – Simple Network Management Protocol
IETF	RFC 1155 Structure and identification of management information for TCP/IP-based internets [V1]
IETF	RFC 1156 Management Information Base for network management of TCP/IP-based internets [V1]
IETF	RFC 1157 Simple Network Management Protocol (SNMP) [V1]
IETF	RFC 1212 Concise MIB definitions
IETF	RFC 1213 Management Information Base for Network Management of TCP/IP-based internets: MIB-II
IETF	RFC 1215 Convention for defining traps for use with the SNMP
IETF	RFC 1445 Administrative Model for version 2 of the Simple Network Management Protocol (SNMPv2) [V2]
IETF	RFC 1441 Introduction to version 2 of the Internet-standard Network Management Framework [V2]
IETF	RFC 1697 Relational Database Management System (RDBMS) Management Information Base (MIB) using SMIv2 [MIB]
IETF	RFC 1901 Introduction to Community-based SNMPv2 [V2c]
IETF	RFC 1909 An Administrative Infrastructure for SNMPv2 [V2u/V2*]
IETF	RFC 2108 Definitions of Managed Objects for IEEE 802.3 Repeater Devices using SMIv2 [MIB]
IETF	RFC 2248 Network Services Monitoring MIB
IETF	RFC 2287 Definitions of System-Level Managed Objects for Applications [MIB]
IETF	RFC 2564 Application Management MIB
IETF	RFC 2578 Structure of Management Information Version 2 (SMIv2) [V2]
IETF	RFC 2579 Textual Conventions for SMIv2 [V2]
IETF	RFC 2582 Conformance Statements for SMIv2 [V2]
IETF	RFC 2594 Definitions of Managed Objects for WWW Services [MIB]
IETF	RFC 2613 Remote Network Monitoring MIB Extensions for Switched Networks Version 1.0 [MIB]
IETF	RFC 2789 Mail Monitoring MIB
IETF	RFC 2790 Host Resources MIB
IETF	RFC 2819 Remote Network Monitoring Management Information Base [RMON MIB]
IETF	RFC 2863 The Interfaces Group MIB

OSI Layer 3/4 Routing, Transport, Control and Related Standards	
Organization	Description
IETF	RFC 2864 The Inverted Stack Table Extension to the Interfaces Group MIB
IETF	RFC 2895 Remote Network Monitoring MIB Protocol Identifier Reference
IETF	RFC 2896 Remote Network Monitoring MIB Protocol Identifier Macros
IETF	RFC 2922 Physical Topology MIB
IETF	RFC 2981 Event MIB
IETF	RFC 3014 Notification Log MIB
IETF	RFC 3144 Remote Monitoring MIB Extensions for Interface Parameters Monitoring
IETF	RFC 3410 Introduction and Applicability Statements for Internet Standard Management Framework [V3]
IETF	RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks [V3]
IETF	RFC 3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) [V3]
IETF	RFC 3413 Simple Network Management Protocol (SNMP) Applications [V3]
IETF	RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) [V3]
IETF	RFC 3415 View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) [V3]
IETF	RFC 3416 Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) [V2]
IETF	RFC 3417 Transport Mappings for the Simple Network Management Protocol (SNMP) [V2]
IETF	RFC 3418 Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) [V2] [MIB]
IETF	RFC 3419 Textual Conventions for Transport Addresses [V2]
IETF	RFC 3434 Remote Monitoring MIB Extensions for High Capacity Alarms [MIB]
IETF	RFC 3440 Definitions of Extension Managed Objects for Asymmetric Digital Subscriber Lines [MIB]
IETF	RFC 3498 Definitions of Managed Objects for Synchronous Optical Network (SONET) Linear Automatic Protection Switching (APS) Architectures [MIB]
IETF	RFC 3577 Introduction to the Remote Monitoring (RMON) Family of MIB Modules
IETF	RFC 3591 Definitions of Managed Objects for the Optical Interface Type [MIB]
IETF	RFC 3635 Definitions of Managed Objects for the Ethernet-like Interface Types [MIB]
IETF	RFC 3584 Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
IETF	RFC 3592 Definitions of Managed Objects for the Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) Interface Type [MIB]
IETF	RFC 3621 Power Ethernet MIB
IETF	RFC 3635 Definitions of Managed Objects for the Ethernet-like Interface

OSI Layer 3/4 Routing, Transport, Control and Related Standards	
Organization	**Description**
	Types [MIB]
IETF	RFC 3728 Definitions of Managed Objects for Very High Speed Digital Subscriber Lines (VDSL) [MIB]
IETF	RFC 3805 Printer MIB v2
IETF	RFC 3826 The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
IETF	RFC 3877 Alarm Management Information Base (MIB) [MIB]
IETF	RFC 3878 Alarm Reporting Control Management Information Base (MIB) [MIB]
IETF	RFC 3896 Definitions of Managed Objects for the DS3/E3 Interface Type [MIB]
IETF	RFC 4008 Definitions of Managed Objects for Network Address Translators (NAT) [MIB]
IETF	RFC 4069 Definitions of Managed Object Extensions for Very High Speed Digital Subscriber Lines (VDSL) Using Single Carrier Modulation (SCM) Line Coding [MIB]
IETF	RFC 4070 Definitions of Managed Object Extensions for Very High Speed Digital Subscriber Lines (VDSL) Using Multiple Carrier Modulation (MCM) Line Coding [MIB]
IETF	RFC 4087 IP Tunnel MIB [MIB]
IETF	RFC 4133 Entity MIB (Version 3) [MIB]
IETF	RFC 4188 Definitions of Managed Objects for Bridges [MIB]
IETF	RFC 4268 Entity State MIB [MIB]
IETF	RFC 4292 IP Forwarding Table MIB [routing MIB]
IETF	RFC 4318 Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol [MIB]
IETF	RFC 4319 Definitions of Managed Objects for High Bit-Rate DSL - 2nd generation (HDSL2) and Single-Pair High-Speed Digital Subscriber Line (SHDSL) Lines [MIB]
IETF	RFC 4363 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions [MIB]
IETF	RFC 4502 Remote Network Monitoring Management Information Base Version 2 [RMON 2 MIB]
IETF	RFC 4706 Definitions of Managed Objects for Asymmetric Digital Subscriber Line 2 (ADSL2) [MIB]
IETF	RFC 4789 Simple Network Management Protocol (SNMP) over IEEE 802 Networks
IETF	RFC 4805 Definitions of Managed Objects for the DS1, J1, E1, DS2, and E2 Interface Types [MIB]
IETF	RFC 4836 Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs) [MIB]
IETF	RFC 4878 Definitions and Managed Objects for Operations, Administration, and Maintenance (OAM) Functions on Ethernet-Like Interfaces [MIB]
IETF	RFC 5017 MIB Textual Conventions for Uniform Resource Identifiers (URIs)
IETF	RFC 5343 Simple Network Management Protocol (SNMP) Context

OSI Layer 3/4 Routing, Transport, Control and Related Standards	
Organization	**Description**
	EngineID Discovery
IETF	RFC 5590 Transport Subsystem for the Simple Network Management Protocol (SNMP)
IETF	RFC 5590 Transport Subsystem for the Simple Network Management Protocol (SNMP)
IETF	RFC 5650 Definitions of Managed Objects for Very High Speed Digital Subscriber Line 2 (VDSL2)
	DNS - Domain Name System
IETF	RFC 1034 Domain names - concepts and facilities
IETF	RFC 1035 Domain names - implementation and specification
IETF	RFC 1794 DNS Support for Load Balancing
IETF	RFC 1982 Serial Number Arithmetic
IETF	RFC 1995 Incremental Zone Transfer in DNS
IETF	RFC 1996 A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)
IETF	RFC 2136 Dynamic Updates in the Domain Name System (DNS UPDATE)
IETF	RFC 2181 Clarifications to the DNS Specification
IETF	RFC 2247 Using Domains in LDAP/X.500 Distinguished Names
IETF	RFC 2308 Negative Caching of DNS Queries (DNS NCACHE)
IETF	RFC 2539 Storage of Diffie-Hellman Keys in the Domain Name System (DNS)
IETF	RFC 2671 Extension Mechanisms for DNS (EDNS0)
IETF	RFC 2672 Non-Terminal DNS Name Redirection
IETF	RFC 2782 A DNS RR for specifying the location of services (DNS SRV)
IETF	RFC 2845 Secret Key Transaction Authentication for DNS (TSIG)
IETF	RFC 2930 Secret Key Establishment for DNS (TKEY RR)
IETF	RFC 3007 Secure Domain Name System (DNS) Dynamic Update
IETF	RFC 3110 RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)
IETF	RFC 3596 DNS Extensions to Support IP Version 6
IETF	RFC 3597 Handling of Unknown DNS Resource Record (RR) Types
IETF	RFC 3645 Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)
IETF	RFC 4025 A Method for Storing IPsec Keying Material in DNS
IETF	RFC 4033 DNS Security Introduction and Requirements
IETF	RFC 4034 Resource Records for the DNS Security Extension
IETF	RFC 4035 Protocol Modifications for the DNS Security Extensions
IETF	RFC 4255 Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints
IETF	RFC 4310 Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)
IETF	RFC 4343 Domain Name System (DNS) Case Insensitivity Clarification
IETF	RFC 4367 What's in a Name: False Assumptions about DNS Names
IETF	RFC 4398 Storing Certificates in the Domain Name System (DNS)
IETF	RFC 4470 Minimally Covering NSEC Records and DNSSEC On-line

OSI Layer 3/4 Routing, Transport, Control and Related Standards	
Organization	**Description**
	Signing
IETF	RFC 4501 Domain Name System Uniform Resource Identifiers
IETF	RFC 4509 Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)
IETF	RFC 4592 The Role of Wildcards in the Domain Name System
IETF	RFC 4635 HMAC SHA (Hashed Message Authentication Code, Secure Hash Algorithm) TSIG Algorithm Identifiers
IETF	RFC 4641 DNSSEC Operational Practices
IETF	RFC 5155 DNS Security (DNSSEC) Hashed Authenticated Denial of Existence
IETF	RFC 5395 Domain Name System (DNS) IANA Considerations
IETF	RFC 5452 Measures for Making DNS More Resilient against Forged Answers
IETF	RFC 5730 Extensible Provisioning Protocol (EPP)
IETF	RFC 5731 Extensible Provisioning Protocol (EPP) Domain Name Mapping
	Syslog
IETF	RFC 3164 The BSD Syslog Protocol
IETF	RFC 3195 Reliable Delivery for syslog
IETF	RFC 5424 The Syslog Protocol
IETF	RFC 5425 Transport Layer Security (TLS) Transport Mapping for Syslog
IETF	RFC 5426 Transmission of Syslog Messages over UDP
IETF	RFC 5427 Textual Conventions for Syslog Management [MIB]
	General and Miscellaneous
IETF	RFC 1242 Benchmarking Terminology for Network Interconnection Devices [NIDs]
IETF	RFC 1738 Uniform Resource Locators (URL)
IETF	RFC 1812 Requirements for IP Version 4 Routers
IETF	RFC 2119 Key words for use in RFCs to Indicate Requirement Levels
IETF	RFC 2368 The mailto URL scheme
IETF	RFC 2544 Benchmarking Methodology for Network Interconnect Devices
IETF	RFC 2644 Changing the Default for Directed Broadcasts in Routers
IETF	RFC 3095 RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed
IETF	RFC 3339 Date and Time on the Internet: Timestamps
IETF	RFC 3986 Uniform Resource Identifier (URI): Generic Syntax
IETF	RFC 5072 IP Version 6 over PPP
IETF	RFC 5198 Unicode Format for Network Interchange
IETF	RFC 5234 Augmented BNF for Syntax Specifications: ABNF
IETF	RFC 5342 IANA Considerations and IETF Protocol Usage for IEEE 802 Parameters
	Metrics
IETF	RFC 2678 IPPM Metrics for Measuring Connectivity
IETF	RFC 2679 A One-way Delay Metric for IPPM

OSI Layer 3/4 Routing, Transport, Control and Related Standards	
Organization	**Description**
IETF	RFC 2680 A One-way Packet Loss Metric for IPPM
IETF	RFC 2681 A Round-trip Delay Metric for IPPM
IETF	RFC 2720 Traffic Flow Measurement: Meter MIB
IETF	RFC 2758 Definitions of Managed Objects for Service Level Agreements Performance Monitoring
IETF	RFC 3357 One-way Loss Pattern Sample Metrics
IETF	RFC 3393 IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)
IETF	RFC 3432 Network performance measurement with periodic streams (IPPM)
IETF	RFC 3593 Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals
IETF	RFC 3729 Application Performance Measurement MIB
IETF	RFC 4148 IP Performance Metrics (IPPM) Metrics Registry
IETF	RFC 4150 Transport Performance Metrics MIB
IETF	RFC 4711 Real-time Application Quality-of-Service Monitoring (RAQMON) MIB
IETF	RFC 4712 Transport Mappings for Real-time Application Quality-of-Service Monitoring (RAQMON) Protocol Data Unit (PDU)
	IP Telephony and Multimedia
ITU-T	H.323 (2006-06) Packet-Based Multimedia Communications Systems
ITU-T	H.225.0 (2006-05) Call signalling protocols and media stream packetization for packet-based multimedia communication systems
ITU-T	H.245 (2008-06) Control protocol for multimedia communication
ITU-T	H.264 (2009-03) Advanced video coding for generic audiovisual services
ITU-T	G.711 (1988-11) Pulse code modulation (PCM) of voice frequencies [codec]
ITU-T	G.711.1 (2008-03) Wideband embedded extension for G.711 pulse code modulation [codec]

Appendix B – Standards, Regulations and Best Practices

ITT's current goal is to become PCI and ISO 17799 compliant. Accordingly, *it is a requirement of future applications and/or systems deployments that they meet the requirements of FIPS 200 and NIST SP 800-53*. The target is to reach compliance with the "medium assurance" level as defined in SP 800-53, using the controls spelled out in that document. There are other legal and regulatory requirements, including some specific to the airport, such as TSA regulations. Table 78 references various security standards and best practices that may be applied to specific situations, projects or procurements.

Table 78 – SFO Current/Planned Security and Business Continuity Standards, Recommended Practices, and Guidelines

Security Standards, Recommended Practices

Organization	Description
TSA	49 CFR 1520.5b Sensitive Security Information
PCI	PCI DSS - Payment Card Industry Data Security Standard, v1.2
ISO/IEC	ISO/IEC 15408 - Common Criteria for Information Technology Security Evaluation
ISO/IEC	ISO/IEC 27002 - Information technology - Security techniques - Code of practice for information security management
BSI	BS 25999-2006/7 - Business Continuity Management
NFPA	NFPA 1600 2007 Edition - Standard on Disaster/Emergency Management and Business Continuity Programs
NIST	FIPS PUB 140-2 - Security Requirements for Cryptographic Modules (2001)
NIST	FIPS PUB 140-3 - Security Requirements for Cryptographic Modules (draft)
NIST	FIPS PUB 180-3 - Secure Hash Standard (SHS) (2008)
NIST	FIPS PUB 198-1 - The Keyed-Hash Message Authentication Code (HMAC) (2008)
NIST	FIPS PUB 199 - Standards for Security Categorization of Federal Information and Information Systems (2004)
NIST	FIPS PUB 200 - Minimum Security Requirements for Federal Information and Information Systems (2006)
NIST	SP 800-18 Rev 1 - Guide for Developing Security Plans for Federal Information Systems (2006)
NIST	SP 800-39 - Managing Risk from Information Systems: An Organizational Perspective (2nd Public Draft)
NIST	SP 800-40 Ver 2- Creating a Patch and Vulnerability Management Program (2005)
NIST	SP 800-41 Rev 1 - Guidelines on Firewalls and Firewall Policy (2009)
NIST	SP 800-44 Ver 2 - Guidelines on Securing Public Web Servers (2007)
NIST	SP 800-45 Ver 2 - Guidelines on Electronic Mail Security (2007)
NIST	SP 800-46 Rev 1 - Guide To Enterprise Telework and Remote Access Security (2009)
NIST	SP 800-48 Rev 1 - Wireless Network Security for IEEE 802.11a/b/g and Bluetooth (2008)
NIST	SP 800-53 Rev 3 - Recommended Security Controls for Federal Information Systems and Organizations (2009)
NIST	SP 800-53 A - Guide for Assessing the Security Controls in Federal Information Systems (2008)
NIST	SP 800-54 - Border Gateway Protocol Security (2007)
NIST	SP 800-57 Rev 2 - Recommendation for Key Management (2007)
NIST	SP 800-61 Rev 1 - Computer Security Incident Handling Guide (2008)
NIST	SP 800-63 Rev 1 - Electronic Authentication Guideline (Draft)
NIST	SP 800-64 Rev2 - Security Considerations in the System Development Lifecycle (2008)
NIST	SP 800-66 Rev 1 - An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (2008)
NIST	SP 800-68 Rev 1 - Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist (2008)

	Security Standards, Recommended Practices
Organization	**Description**
NIST	SP 800-77 - Guide to IPsec VPNs (2005)
NIST	SP 800-81 Rev 1 - Secure Domain Name System (DNS) Deployment Guide (draft)
NIST	SP 800-82 - Guide to Industrial Control Systems (ICS) Security Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) (2nd Public Draft)
NIST	SP 800-83 - Guide to Malware Incident Prevention and Handling (2005)
NIST	SP 800-88 - Guidelines for Media Sanitization (2006)
NIST	SP 800-92 - Guide to Computer Security Log Management (2006)
NIST	SP 800-94 - Guide to Intrusion Detection and Prevention Systems (IDPS) (2007)
NIST	SP 800-95 - Guide to Secure Web Services (2007)
NIST	SP 800-97 - Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i (2007)
NIST	SP 800-98 - Guidelines for Securing Radio Frequency Identification (RFID) Systems (2007)
NIST	SP 800-100 - Information Security Handbook: A Guide for Managers (2006)
NIST	SP 800-110 - Information System Security Reference Data Model (Draft)
NIST	SP 800-113 - Guide to SSL VPNs (2008)
NIST	SP 800-114 - User’s Guide to Securing External Devices for Telework and Remote Access (2007)
NIST	SP 800-120 - Recommendation for EAP Methods Used in Wireless Network Access Authentication (2009)
NIST	SP 800-122 - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (Draft)
OWASP	Open Web Application Security Project Development Guide
OWASP	Open Web Application Security Project Code Review Guide
OWASP	Open Web Application Security Project CLASP (Comprehensive, Lightweight Application Security Process)
SANS/MITRE	CWE/SANS Top 25 Most Dangerous Programming Errors
BICSI	Electronic Safety and Security Design Reference Manual (ESSDRM), 2nd Edition (2009)

Table 19 describes information technology best practices SFO ITT intends to follow.

Table 19 – SFO Current/Planned IT Best Practices

	Best Practices
Organization	**Description**
OGC	ITILv3 - Information Technology Infrastructure Library v3
ISO/IEC	ISO 12207:2008 - Systems and software engineering-Software life cycle processes
ISO/IEC	ISO 20000-2 ITSM Code of Practice for Service Management
IEEE	Std 610.12-1990 - IEEE Standard Glossary of Software Engineering

Best Practices	
Organization	**Description**
	Terminology
IEEE	Std 828-2005 - IEEE Standard for Software Configuration Management Plans
IEEE	Std 830-1998 - IEEE Recommended Practice for Software Requirements Specifications
IEEE	Std 982.1-1988 – IEEE Standard Dictionary of Measures to Produce Reliable Software -Description
IEEE	Std 1012-2004 – IEEE Standard for Software Verification and Validation
IEEE	Std 1045-1992 - IEEE Standard for Software Productivity Metrics
IEEE	Std 1062-1998 - IEEE Recommended Practice for Software Acquisition
IEEE	Std 1219-1998 - IEEE Standard for Software Maintenance
IEEE	Std 1233-1998 - IEEE Guide for Developing System Requirements Specifications
IEEE	Std 1362-1998 - Guide for Information Technology—System Definition—Concept of Operations (ConOps) Document -Description
IEEE	Std 1465-1998 (R2004) - IEEE Standard Adoption of ISO/IEC 12119:1994(E), Information Technology-Software packages-Quality requirements and testing
IEEE/EIA	Std 1471-2000 - Recommended Practice for Architecture Description of Software-Intensive Systems [paralleled by ISO 42010:2007]
IEEE/EIA	12207-2008 - Standard for Information Technology-Software Life Cycle Processes [parallels ISO 12207]
IEEE	15288 - Systems Engineering: System Life Cycle Processes [same as ISO 15288
IIBA	Guide to the Business Analysis Body of Knowledge, v2.0 (2009)

Table 20 describes SFO ITT's targeted quality assurance standards.

Table 20 – SFO Current/Planned Quality Assurance Standards

Quality Assurance Standards and Practices	
Organization	**Description**
ISO	ISO 9001:2008 - Quality management systems – Requirements
ISO	ISO 90003:2004 - Guidelines for the application of ISO 9001:2000 to computer software
IEEE	Std 730-2002 - Standard for Software Quality Assurance Plans
IEEE	Std 829-2008 - Standard for Software and System Test Documentation
IEEE	Std 1061-1998 - Software Quality Metrics Methodology

Table 21 – Facility, Electrical, and Environmental Standards

Facility, Electrical, Environmental and Safety Standards and Practices	
Organization	**Description**
	Electrical Surges and Surge Protection
ANSI/IEEE	C62.11-2005 Standard for Metal-Oxide Surge Arresters for AC Power Circuits (>1 kV)

Facility, Electrical, Environmental and Safety Standards and Practices	
Organization	**Description**
ANSI/IEEE	C62.11a-2008 Standard for Metal-Oxide Surge Arresters for AC Power Circuits (>1 kV) Amendment 1
ANSI/IEEE	C62.41.1-2002 Guide on the Surge Environment in Low-Voltage AC Power Circuits
ANSI/IEEE	C62.41.2-2002 Recommended Practice on Characterization of Surges in Low-Voltage AC Power Circuits
ANSI/IEEE	C62.45-2002 Recommended Practice on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits
UL	UL 1283 Electromagnetic Interference Filters, Fifth Edition
UL	UL 1449 3rd Edition 2007 - Standard for Surge Protective Devices
IEC	IEC 61000-4-5 Ed. 2.0 Electromagnetic compatibility (EMC) - Part 4-5: Testing and measurement techniques - Surge immunity test
	RF Emission Control
FCC	CFR Title 47, Part 15, Subpart J – Radio Frequency Devices
IEC	CISPR 11, 5th Ed (2009). Industrial, scientific and medical equipment - Radio-frequency disturbance characteristics - Limits and methods of measurement
IEC	CISPR 22, 6th Ed (2008). Information technology equipment – Radio disturbance characteristics – Limits and methods of measurement
ANSI/IEEE	C63.17-2006. Methods of Measurement of the Electromagnetic and Operational Compatibility of Unlicensed Personal Communication Services Devices
ANSI/IEEE	C63.4-2008 American National Standard for Methods of Measurement of Radio-Noise Emissions from Low-voltage Electrical and Electronic Equipment in the Range of 9 kHz to 40 GHz.
	Power, Grounding, Bonding and Equipment Protection
ANSI/NFPA	NFPA 70-2008 National Electrical Code (2008 NEC)
IEEE	IEEE Std 1100 - 2005 IEEE Recommended Practice for Powering and Grounding Electronic Equipment
IEEE	IEEE 1159 – 1995/R2001 Recommended Practice for Monitoring Electric Power Quality
ANSI	ANSI/J-STD-607-A-2002 Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications
ANSI	ANSI/J-STD-607-B (draft 6+) Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications
BICSI	ANSI/NECA/BICSI-607-2009 Telecommunications Bonding and Grounding Planning and Installation Methods for Commercial Buildings
NEMA	NEMA 250-2008 Enclosures for Electrical Equipment (1000 Volts Maximum)
ANSI/NEMA	NEMA WD 6-2002(R2008) Wiring Devices-Dimensional Specifications [Electrical plugs and receptacles)
IEC	IEC 60320 Appliance couplers for household and similar general purposes [IEC-320 plugs and receptacles]
	Facility Design Standards
Telcordia	Network Equipment-Building System (NEBS) Requirements: Physical Protection, GR-63 CORE, Issue 3, March 2006 [Seismic Zone 4, etc.]
ANSI/TIA	ANSI/TIA/EIA-942-2005 Telecommunications Infrastructure Standards for

Facility, Electrical, Environmental and Safety Standards and Practices	
Organization	**Description**
	Data Centers
ANSI/TIA	ANSI/TIA/EIA-942-1-2008 Data Center Coaxial Cabling Specifications and Applications Distances
BICSI	ANSI/NECA/BICSI 586-2006: Standard for Installing Commercial Building Telecommunications Cabling
BICSI	ANSI/BICSI-002-2009 Data Center Design Standard and Recommended Practices
ANSI/TIA	ANSI/TIA-1005 Telecommunications Infrastructure Standards for Industrial Premises
BICSI	Information Transport Systems Installation Methods Manual (ITSIMM), 5th Edition
BICSI	Telecommunications Distribution Methods Manual (TDMM), 11th Edition
ANSI/ASHRAE	ANSI/ASHRAE Standard 52.2-2007 Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size
ASHRAE	Thermal Guidelines for Data Processing Environments, Second Edition (2009)
ASHRAE	Design Considerations for Datacom Equipment Centers, Second Edition (2009)
ASHRAE	Structural and Vibration Guidelines for Datacom Equipment Centers (2008)
ASHRAE	Particulate and Gaseous Contamination in Datacom Environments (2009)
ANSI/ISA	S71.04-1985 Environmental Conditions for Process Measurement and Control Systems: Airborne Contaminants

Appendix C – SNMP MIB Support Questionnaire

Table22 – Public MIBs Defined by IETF

Y/N?	RFC	Title	Comments
	1697	Relational Database Management System (RDBMS) Management Information Base (MIB) using SMIv2	
	1724	RIP Version 2 MIB Extension	
	2564	Application Management MIB	
	2578	Structure of Management Information Version 2 (SMIv2)	Note: SMIv2 replaces SMIv1
	2579	Textual Conventions for SMIv2	
	2580	Conformance Statements for SMIv2	
	2594	Definitions of Managed Objects for WWW Services (MIB)	
	2605	Directory Server Monitoring MIB	
	2613	Remote Network Monitoring MIB Extensions for Switched Networks	Extends RMON to switches (SMON)
	2741	Agent Extensibility (AgentX) Protocol	
	2788	Network Services Monitoring MIB	Application-level monitoring
	2789	Mail Monitoring MIB	Monitors MTAs only
	2790	Host Resources MIB	
	2819	Remote Network Monitoring MIB	
	2863	The Interfaces Group MIB	Network device interface mgmt
	2864	The Inverted Stack Table Extension to the Interfaces Group MIB	Network device interface mgmt
	2895	Remote Network Monitoring MIB Protocol Identifier Reference	
	2896	Remote Network Monitoring MIB Protocol Identifier Macros	
	2981	Event MIB	Extension of RMON with triggers
	2982	Distributed Management Expression MIB	
	3014	Notification Log MIB	Log tables local to the SNMP agent
	3144	Remote Monitoring MIB Extensions for Interface Parameters Monitoring (IFTOPN)	
	3273	Remote Network Monitoring Management Information Base for	

Y/N?	RFC	Title	Comments
		High Capacity Networks	
	3395	Remote Network Monitoring MIB Protocol Identifier Reference Extensions	
	3411	An Architecture for Describing SNMP	The fundamental SNMP document
	3412	Message Processing and Dispatching for SNMP	
	3414	User-based Security Model (USM)	
	3415	View-based Access Control Model (VACM)	
	3416	Version 2 of the Protocol Operations for SNMP	
	3417	Transport Mappings for SNMP	
	3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)	
	3434	Remote Monitoring MIB Extensions for High Capacity Alarms	
	3498	Definitions of Managed Objects for Synchronous Optical Network (SONET) Linear Automatic Protection Switching (APS) Architectures	SONET failover MIB
	3577	Introduction to the Remote Monitoring (RMON) Family of MIB Modules	Informational
	3584	Coexistence between Version 1, Version 2, and Version 3 SNMP	
	3592	Definitions of Managed Objects for the Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) Interface Type	
	3593	Textual Conventions for MIB Modules Using Performance History	Modeled on the telecom industry's measurement strategy
	3621	Power Ethernet MIB	
	3635	Definitions of Managed Objects for the Ethernet-like Interface Types	
	3728	Definitions of Managed Objects for Very High Speed Digital Subscriber Lines (VDSL)	
	3729	Application Performance Measurement MIB	
	3805	Printer MIB v2	
	3896	Definitions of Managed Objects for	WAN MIB

Y/N?	RFC	Title	Comments
		the DS3/E3 Interface Type	
	4022	Management Information Base for the Transmission Control Protocol (TCP)	Compatible w/SMIv2
	4069	Definitions of Managed Object Extensions for Very High Speed Digital Subscriber Lines (VDSL) Using Single Carrier Modulation (SCM) Line Coding	Compatible w/SMIv2
	4070	Definitions of Managed Object Extensions for Very High Speed Digital Subscriber Lines (VDSL) Using Multiple Carrier Modulation (MCM) Line Coding	Compatible w/SMIv2
	4087	IP Tunnel MIB	Compatible w/SMIv2
	4113	Management Information Base for the User Datagram Protocol (UDP)	Compatible w/SMIv2
	4133	Entity MIB v3	Compatible w/SMIv2
	4150	Transport Performance Metrics MIB	
	4188	Definitions of Managed Objects for Bridges (Bridge MIB)	Compatible w/SMIv2
	4292	IP Forwarding Table MIB	Provides subset of routing table info
	4293	Management Information Base for the Internet Protocol (IP)	Compatible w/SMIv2
	4502	Remote Network Monitoring MIB V2	Compatible w/SMIv2
	4560	Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations (Remops MIB)	Compatible w/SMIv2
	4668	RADIUS Authentication Client MIB for IPv6	Includes IPv4 RADIUS clients
	4669	RADIUS Authentication Server MIB for IPv6	Includes IPv4 RADIUS servers
	4706	Definitions of Managed Objects for Asymmetric Digital Subscriber Line 2 (ADSL2)	Compatible w/SMIv2
	4710	Real-time Application Quality-of-Service Monitoring (RAQMON) Framework	Compatible w/SMIv2
	4711	Real-time Application Quality-of-Service Monitoring (RAQMON) MIB	Compatible w/SMIv2
	4712	Transport Mappings for Real-time Application Quality-of-Service Monitoring (RAQMON) Protocol Data Unit (PDU)	Compatible w/SMIv2

Y/N?	RFC	Title	Comments
	4789	SNMP over IEEE 802 Networks	
	4805	Definitions of Managed Objects for the DS1, J1, E1, DS2, and E2 Interface Types	WAN MIB

Table 23 - Private/Non-RFC MIBs

Y/N?	Source	Title	Comments
	IETF draft-ietf-adslmib-vdsl2-05	Definitions of Managed Objects for Very High Speed Digital Subscriber Line 2 (VDSL2)	
	Sun	JVM Management MIB	Manages JVM properties
	Microsoft	DHCP MIB	MIB that contains object types for monitoring the network traffic between remote hosts and DHCP servers
	Microsoft	HOSTMIB	Contains object types for monitoring and managing host resources
	Microsoft	LMMIB2	
	Oracle	Oracle Private Database MIB	Extends RFC 1697 for Oracle-specific objects
	Oracle	Oracle Listener MIB	
	Oracle	Oracle Enterprise Manager MIB	
	VMware		
	Cisco	BGP4-MIB	Implements RFC1657
	Cisco	CISCO-BRIDGE-EXT-MIB	
	Cisco	CISCO-CASA-MIB	
	Cisco	CISCO-CONFIG-COPY-MIB	
	Cisco	CISCO-CONFIG-MAN-MIB	
	Cisco	CISCO-DHCP-SNOOPING-MIB	
	Cisco	CISCO-ENHANCED-IMAGE-MIB	
	Cisco	CISCO-ENHANCED-MEMPOOL-MIB	New MIB module for monitoring the memory pools of all physical entities on a managed system
	Cisco	CISCO-ENTITY-ASSET-MIB	
	Cisco	CISCO-ENTITY-DIAG-MIB	
	Cisco	CISCO-ENTITY-DISPLAY-MIB	