# APPENDIX A

# DEFINITIONS, ABBREVIATIONS AND ACRONYMS, AND REFERENCES

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS

**SECTION** **PAGE**

# LIST OF FIGURES

**FIGURE** **PAGE**

# SECTION A1
# INTRODUCTION

## A1.1 SCOPE

Appendix A1 contains definitions for the various Unified Capabilities (UC) systems, subsystems, and components, along with acronyms and abbreviations used within the entire Unified Capabilities Requirements 2008, Change 3.

## A1.2 APPENDIX A1 OVERVIEW

This appendix consists of four sections as follows:

- Section A1 describes the scope of this appendix.
- Section A2 contains a glossary describing the terminology used within the UCR 2008, Change 3.
- Section A3 lists the abbreviations and acronyms used within the UCR 2008, Change 3.
- Section A4 contains the references used within the UCR 2008, Change 3.

THIS PAGE INTENTIONALLY LEFT BLANK

# SECTION A2
# GLOSSARY AND TERMINOLOGY DESCRIPTION

## A2.1 OVERVIEW

This glossary defines terms as they apply to the UCR 2008, Change 3. It is understood that other documents or organizations may define the terms differently. These terminology definitions are not requirements and are defined to provide context for a requirement in the UCR 2008, Change 3.

**A B C D E F G H I J K L M N O P Q R S T U V W Numbers**

## Numbers

**4 Common Intermediate Format (4CIF)** A video format defined in ITU-T Recommendation H.263 that is characterized by 704 luminance pixels on each of 576 lines, with half as many chrominance pixels in each direction. Four times the resolution of CIF, respectively. See *chrominance*, *FCIF*, *luminance*.

**16 Common Intermediate Format (16CIF)** A video format defined in ITU-T Recommendation H.263 that is characterized by 1408 luminance pixels on each of 1152 lines, with half as many chrominance pixels in each direction. Sixteen times the resolution of CIF, respectively. See *chrominance*, *FCIF*, *luminance*.

## A

**Add-On Transfer and Conference Calling** A feature set that provides the user with the capabilities to handle more than one call at a time on a given line.

**Admission Control** The process by which flows are allowed to enter a network based on their level of quality of service. See *quality of service*.

**Aggregate Service Class** An aggregation of service classes based on a selected set of quality of service criteria. See *quality of service*, *service class*.

**A-Law** A companding (compressing and expanding) method for encoding and decoding audio waveforms into/from digital data in a pulse code modulated system. A-Law is the primary companding method for E1 transmissions. See *μ-Law*.

**Annotation** Text, graphics, or free hand markings used to highlight or provide explanation to areas of interest on an image or whiteboard.

**Appliance** A hardware platform with its supporting software that performs a single function or multiple functions.

**Application Layer Control Protocol** See *call control*.

**Approved Products List (APL)** A list of products that have received Joint Interoperability Certification and Information Assurance Accreditation from the Defense Information System Network Designated Approval Authorities in accordance with the Department of Defense Instruction 8100.04. The list is published on the Joint Interoperability Test Command home page (https://aplits.disa.mil).

**Approved Products List System Under Test (SUT)** The set of appliances required to meet a Defense Switched Network switch certification (i.e., Multifunction Switch, End Office). Examples of a SUT include Time Division Multiplexing or circuit switch components, Voice over Internet Protocol system components (e.g., Local Session Controller and gateway), local area network components (e.g., routers and Ethernet switches), and End Instruments. See *approved products list*, *appliance*, *Defense Switched Network*, *end instrument*, *end office*, *gateway*, *local session controller*, *multifunction switch*, *router*, *SUT*.

**Assured Forwarding (AF)** Provides delivery of Internet Protocol (IP) packets in four independently forwarded AF classes. Within each AF class, an IP packet can be assigned one of three different levels of drop precedence. In case of congestion, the drop precedence of a packet determines the relative importance of the packet within the AF class. A congested Differentiated Services (DS) node tries to protect packets with a lower drop precedence value from being lost by preferably discarding packets with a higher drop precedence value. A DS node must allocate forwarding resources (i.e., buffer space and bandwidth) to AF classes so that, under reasonable operating conditions and traffic loads, packets of an AF class x do not have a higher probability of timely forwarding than packets of an AF class y if x is less than y. [RFC 2597] See *DS*.

**Assured Service** The ability of a system to optimize session completion rates for all IMMEDIATE/PRIORITY (I/P) users despite degradation because of network disruptions, natural disasters, or surges during crisis or war.

**Assured Services Admission Control (ASAC)** A process by which the quality of service requirements of a higher precedence service will be met at the expense of a lower precedence service if the network conditions do not allow meeting quality of service requirements of all services. See *admission control*, *assured service*, *precedence*, *quality of service*.

**Assured Services Local Area Network (ASLAN)** The Internet Protocol (IP) network infrastructure components used to provide command and control voice services to end users. It applies to switch certifications for Multifunction Switches, End Office Switches, Small End Office Switches, and Private Branch Exchange 1, and to certifications for Local Session Controllers, Multifunction Softswitches, and Softswitches. A local area network that supports IMMEDIATE/PRIORITY (I/P) users is considered an ASLAN. The ASLAN has two configurations depending on whether it supports I/P users or FLASH/FLASH OVERRIDE (F/FO) users. An ASLAN that supports I/P users is classified a Medium Availability ASLAN and the primary requirements that differentiate it from a non-ASLAN are that it requires a 2-hour power backup capability for all ASLAN components in addition to providing 0.99997 reliability. An ASLAN that supports F/FO users is classified a High Availability ASLAN and the primary requirements that differentiate it from a Medium Availability ASLAN are that it requires an 8-hour power backup capability for all ASLAN components in addition to providing 0.99999 reliability. See *assured service*, *end office switch*, *F/FO user*, *I/P user*, *local session controller*, *multifunction softswitch*, *multifunction switch*, *private branch exchange 1*, *reliability*, *small end office switch*, *softswitch*.

**Assured Services Session Initiation Protocol (AS-SIP)** A session signaling protocol consisting of a defined set of Session Initiation Protocol signaling standards and incorporating Department of Defense Assured Service functionality. See *assured service*, *Session Initiation Protocol*.

**Assured Services Session Initiation Protocol (AS-SIP) End Instrument (AEI)** A user appliance that interacts with an associated serving appliance using the AS-SIP to originate, accept, and/or terminate a voice, video, and/or data session(s). See *appliance*, *AS-SIP*, *assured service*.

**Assured Services Session Initiation Protocol (AS-SIP) Signaling Appliance** Any Department of Defense signaling appliance (exclusive of End Instruments) that supports the receipt, processing, or forwarding of AS-SIP messages. These appliances MAY support the receipt and forwarding of encapsulated Integrated Services Digital Network (ISDN) User Part (ISUP) Multipurpose Internet Mail Extension (MIME) objects. See *appliance*, *AS-SIP*, *assured service*, *end instrument*, *message*.

**Asymmetric DSL (ADSL)** ADSL is a technology for transmitting digital information on a metallic twisted pair that allows high-speed data transmission between the network operator end and the customer end. Systems allow approximately 6 Mbps downstream and approximately 640 Kbps upstream data rates, depending on line distance - up to 12,000 feet (about 2.3 miles) from the central office.

**Asymmetric DSL 2 (ADSL2)** ADSL2 extends the capability of basic ADSL in data rates that range up to a minimum of 8 Mbps downstream and 800 Kbps upstream. Support of net data rates above 8 Mbps downstream and support of net data rates above 800 Kbps upstream are

optional. ADSL2 utilizes the same bandwidth as ADSL but achieves higher throughput via data compression techniques.

**Audio** The voice or sound portion of a teleconference.

**Audio Add-On** A feature that allows a participant to join a videoconference via audio (telephone) only.

**Audio Mixing** The process of combining two or more audio signals to produce a single composite audio signal. This allows each participant in a conference to hear all other participants simultaneously.

**Audio Switching** The process of switching the audio portion of the video teleconferencing (VTC) system to be heard by all participants so that the input signal comes from the designated speaker. No other participants can be heard until they are selected as the audio source. See *VTC*.

**Audio Teleconferencing** See *conference call*.

**Automated Receiving Devices (ARD)** A family of automated devices, which are customer premises equipment or network elements that attaches to the receiving end of a telephone call. Typical ARDs will have an automatic call distribution front-end, which could be as simple as a queue that handles incoming calls on a first come first serve basis. More complex ARDs can be full function Automatic Call Distributors that also include predetermined schemes and route calls based on routing criteria and, quite often, database handling instructions. Once in queue, if the call is not answered in a specified amount of time and the caller had not terminated the call, ARD can terminate the call or send the call to another location. Usually the ARD invokes a network carrier-based "take back and transfer" to the alternative location. Automated Receiving Devices do not originate calls to the network. See *network element*.

**Availability** The fraction of the time the system is available to a service user's requests. The time during which the system is unavailable is called downtime; the time during which the system is available is called uptime. In Internet Protocol terms, it is the percentage of time that the packet loss is less than the threshold. [GESP] See *system*.

## B

**Back-to-Back User Agent (B2BUA)** "A back-to-back user agent (B2BUA) is a logical entity that receives a request and processes it as a user agent server (UAS). In order to determine how the request should be answered, it acts as a user agent client (UAC) and generates requests. Unlike a proxy server, it maintains dialog state and must participate in all requests sent on the

dialogs it has established. Since it is a concatenation of a UAC and UAS, no explicit definitions are needed for its behavior." [RFC 3261] See *proxy server*, *UAC*, *UAS*.

**Basic Rate Interface (BRI)** The basic Integrated Services Digital Network (ISDN) service, consisting of two 64 kbps B-channels (bearer channels) that carry data and voice in both directions, and one 16 kbps D-channel (data channel) that carries call-control information. See *ISDN*.

**Bitmap** A two-dimensional array of pixels representing an image.

**Bit-Rate Allocation Signal (BAS)** An 8-bit word within the frame structure of ITU-T Recommendation H.221 that is used to transmit commands, control and indication signals, and capabilities.

**Blocking** The process by which a message is denied entry to a network that is caused by a lack of resources in the network. See *message*.

**Broadband Streaming** For the purposes of this document, Broadband Streaming refers to the transfer of data in a continuous audio and/or video stream over a network using bandwidth from 2 to 15 Mbps.

**Broadband ISDN (B-ISDN)** An Integrated Services Digital Network (ISDN) offering broadband capabilities. A B-ISDN is a proposed service that may (1) include interfaces operating at data rates from 150 to 600 Mbps, (2) use asynchronous transfer mode (ATM) to carry all services over a single, integrated, high-speed packet-switched network, (3) have local area network (LAN) interconnection capability, (4) provide access to a remote, shared disk server, (5) provide voice, video, or data teleconferencing, (6) provide transport for programming services, such as cable television, (7) provide single-user controlled access to remote video sources, (8) handle voice/video telephone calls, and (9) access shop-at-home and other information services. See *ISDN*, *VTC*.

**Broadcasting** The transmission of data or information that may be simultaneously received by stations that usually make no acknowledgement. See *multicasting*, *unicasting*.

## C

**Call** A message that is subject to Call Admission Control or Session Admission Control. A Voice over Internet Protocol (IP) or Video over IP call that is placed or answered by a Proprietary End Instrument or Assured Services Session Initiation Protocol (AS-SIP) End Instrument end user. See *assured service*, *AS-SIP*, *AS-SIP end instrument*, *call admission control*, *proprietary end instrument*.

**Call Admission Control (CAC)** A process in which a call is accepted or denied entry (blocked) to a network based on the network's ability to provide resources to support the quality of service requirements for the call. See *blocking*, *call*, *quality of service*.

**Call Connection Agent (CCA)** The CCA is part of the Session Control and Signaling functions and includes both the Interworking Function (IWF) and the Media Gateway Controller. As a result, the scope of the CCA includes the following areas:

- Control of Assured Services Session Initiation Protocol (AS-SIP) sessions within the network appliance
- Support for public switched telephone network (PSTN) and Voice over IP (VoIP) signaling protocols
- Protocol interworking of signaling protocols (e.g., AS-SIP ⇔ DoD Common Channel Signaling System No. 7 interworking) through the CCA IWF control of Media Gateways that link the network appliance with Time Division Multiplexing network elements
- Support for interactions with other network appliance functions
- Support for assured services voice and video calls
- Support for assured services user features and services

See *appliance*, *AS-SIP*, *assured service*, *Common Channel Signaling System No. 7*, *media gateway*, *media gateway controller*, *network element*, *session*.

**Call Control** Establishes, modifies, and terminates sessions (e.g., multimedia conferences). It can invite participants to existing sessions, such as multicast conferences. (Referred to as Application Layer Control Protocol in RFC 3261.) See *multicasting*, *session*.

**Call Forwarding Variable (CFV)** This feature allows ROUTINE precedence calls attempting to terminate to a line to be redirected to another customer-specified line served by the same office or by another office for Defense Switched Network and/or commercial.

**Call Hold** A feature that provides the capability for the user to hold a call for an extended period, and then return to the call, with or without making another call.

**Call Stateful** A proxy is call stateful if it retains state for a dialog from the initiating INVITE to the terminating BYE request. A call stateful proxy is always transaction stateful, but the converse is not necessarily true. [RFC 3261]

**Call Waiting** A feature whereby a line in the talking state is alerted by a call waiting tone when another call is attempting to complete to that line. The call waiting tone is only audible to the line with the Call Waiting feature activated. Audible ringing is returned to the originating line.

**Calls Internal and External to Communities of Interest (COIs)** The COI is a Local Session Controller (LSC)-based feature as opposed to a network-wide feature, i.e., no COI information is transported between LSCs (or from an LSC). Calls are defined as being internal to the COI if:

1. For an outgoing call request, the dialed destination matches a code in the user's COI screening list.

2. For local calls only, an incoming call request is to a user who is assigned to the same COI group as the calling user.

   All other local calls to/from a COI member, including incoming call requests received via trunk facilities or from another RTS appliance, are treated as external calls to the COI. Call requests received via incoming trunk facilities are also deemed external but these do not undergo any COI screening and so are not subject to the special COI restrictions and privileges.

See *COI group*, *COI member*, *COI screening list*, *LSC*.

**Camera** In television, an electronic device using an optical system and a light-sensitive pickup tube or chip to convert visual signals into electrical impulses.

**Cancel Call Waiting** A feature that allows the customer with Call Waiting service to inhibit the operation of call waiting for one call. See *call waiting*.

**Cascading** The process of providing a video teleconferencing (VTC) conference involving more than one Multipoint Control Unit (MCU), so that information must pass not only between Conferencing Terminal Unit (CTU) and MCU, but also from one MCU to another. The ability of an MCU to participate in a conference involving more than one MCU is optional and is called cascading. See *CTU*, *multipoint control unit (MCU)*, *VTC*.

**Certificate Path** A sequence of certificates that connect the target certificate to one of the relying party's trust points. Construction of the path is known as path development and verification of that path providing a chain of trust and is known as path processing. A target certificate belongs to an end-entity that either sent a signed message to the relying party or to which the relying party desires to send an encrypted message. This is also called a certificate chain. See *message*, *path*.

**Certificate Trust List (CTL)** A predefined list of items that have been signed by a trusted entity. All items in the list are authenticated and approved for use by the signing entity.

**Chair Control** A method of providing the capability for one of the conferencing terminal units (CTUs) involved in a conference to exercise some measure of authority over the conference, particularly in making the decision of which video will be broadcast to the other CTUs. See *CTU*.

**Chair-Control Conferencing Terminal Unit (CTU)** An enhanced CTU possessing the capability to exert a certain measure of authority over the operation of the multipoint conference. The chair-control assignment may be prearranged, assigned by an operator or by protocol during the call. The person controlling need not be the actual chairperson of the meeting. See *CTU*.

**Chat** The capability for two or more users operating on different computers to exchange text messages in real time. Chat is distinguished from instant messaging (IM) by being focused on group chat, or room-based chat. Typically, room persistence is a key feature of multiuser chat; in contrast with typically ad hoc IM capabilities. See *instant messaging*.

**Chrominance** The color component of a pixel. The Cb and Cr components in YCbCr. The A and B components in CIElab. See *luminance*, *pixel*.

**Circuit Emulation Service (CES) over Internet Protocol (IP)** Circuit Emulation Service over IP is trunking of time division multiplexing (TDM) data between IP points. Circuit Emulation Service over IP provides a method to transport T1/E1 or T3/E3 streams over an IP network. The service is similar to CES over asynchronous transfer mode (ATM) that has been in the industry for some time but the transport layer is IP. The circuit may include compression, which may include silence suppression, and echo cancellation. The CES over IP is also known as Circuit Emulation Service over Packet.

**Classified** Any information that has been determined to require protection against unauthorized disclosure to avoid harm to U.S. national security. The classifications TOP SECRET, SECRET, and CONFIDENTIAL are used to designate such information, referred to as "classified information."

**Classifier** An entity that selects packets based on the content of packet headers according to defined rules. [RFC 2475] See *entity*.

**Client Management Entity (CME)** A data link client that uses Client ID 0x00 to send a complete list of locally registered clients and their optional extra capabilities.

**codec** Acronym for Coder/Decoder. In video teleconferencing, an electronic device that converts analog signals, typically video or voice, into digital form and compresses them into a

fraction of their original size to save frequency bandwidth on a transmission path. It also performs the inverse operation; decompressing received signals and converting them back to analog. See *path*, *VTC*.

**Common Channel Signaling System No. 7 (i.e., SS7 or CCS7)** A global standard for telecommunications defined by the International Telecommunications Union (ITU) Telecommunication Standardization Sector (ITU-T). The standard defines the procedures and protocol by which network elements in the public switch telephone network (PSTN) exchange information over a digital signaling network to effect wireless (cellular) and wire line call setup, routing, and control. The ITU definition of SS7 allows for national variants, such as the American National Standards Institute and Telcordia Technologies standards used in North America, and the European Telecommunications Standards Institute standard used in Europe. See *network element*, *wireless*.

**Common Intermediate Format (CIF)** See *FCIF* component in CIElab.

**Community of Interest (COI)** The COI is a switch-based feature as opposed to a network-wide feature, i.e., no COI information is transported between switches. Calls are defined as being internal to the COI if:

1. For an outgoing call request, the dialed destination matches a code in the user's COI screening list.

2. For local calls only, an incoming call request is to a user who is assigned to the same COI group as the calling user.

All other local calls to/from a COI member, including incoming interswitch call requests received via trunk facilities, are treated as external calls to the COI. Call requests received via incoming trunk facilities are deemed external but these do not undergo any COI screening; and hence, are not subject to the special COI restrictions and privileges. See *COI group classmarks*, *COI member*, *COI screening list*.

**Community of Interest (COI) Group** A feature that enables users to form groups, to and from which access is subject to special restrictions and privileges. A COI group consists of a COI screening list, a COI precedence level, and COI group classmarks. See *COI group classmarks*, *COI member*, *COI precedence level*, *COI screening list*.

**Community of Interest (COI) Group Classmarks** Specify the outgoing and incoming call restrictions and/or privileges for calls internal to the COI group. The COI group classmarks are defined as follows:

1. COI Outgoing Classmarks. A COI group user with no outgoing classmarks limits the COI user to making calls, which are internal to the COI only, i.e., to only those destination codes that are specified within the COI screening list. The user is allowed to exercise the normal authorized precedence for these calls.

2. Outgoing Precedence Allowed. The COI user is allowed to exercise up to and including the COI precedence for calls internal to the COI.

3. Outgoing Precedence Mandatory. Only COI precedence calls are permitted for calls internal to the COI.

4. Outgoing Calls Barred within the COI. This restriction means that a COI user cannot make calls to destination codes specified in the COI screening list.

See *COI precedence*, *COI screening list*.

**Community of Interest (COI) Incoming Classmarks** A COI group user with no incoming classmarks limits the COI user to receiving locals from members of those COIs of which the user is a member. All other local calls are restricted. There is no restriction on calls received over trunk facilities because these do not undergo COI screening.

1. Incoming Precedence Mandatory. This COI service only permits calls internal to the COI that are at the COI precedence level, which only applies for local calls that are internal to the COI (i.e., if the local calling user is a member of those COIs of which the user is a member).

2. Incoming Calls Barred within the COI. This restriction means that a COI user cannot receive calls from members of those COIs of which the user is a member. Unless the member classmark incoming access option is applied, calls from other non-COI members or other COI members are restricted also.

3. COI Member Classmarks. In addition to the COI group classmarks that are part of the COI group, specific COI members can have COI classmarks at the subscriber level that specify the type of incoming and outgoing call restrictions and/or privileges for calls external to the COI.

See *Community of Interest*, *COI group classmarks*, *COI member*, *COI precedence level*, *COI screening list*.

**Community of Interest (COI) Member** A user that has a COI group assigned is defined as being a member of that COI group.

**Community of Interest (COI) Outgoing Access** Allows a COI user to make calls external to the COI, i.e., to all other destination codes not specified in the COI screening list (i.e., external to the COI). The user is only allowed to exercise the normal authorized precedence level for these calls. See *COI precedence level*, *COI screening list*.

**Community of Interest (COI) Precedence Level** A COI feature that allows the precedence level to be required or allowed, depending on the COI group classmarks, for calls to and from users of a COI group. See *COI group classmarks*, *COI precedence level*.

**Community of Interest (COI) Screening List** A COI feature that allows a list to be specified for individual destinations or codes representing groups of destinations. Each code in this list can be from 3 to 15 digits. Outgoing calls are screened against this list together with the COI group classmarks to allow or deny the call request. See *COI group classmarks*.

**Compression** See *data compression*.

**Conditional Requirement [Conditional]** A requirement that addresses features and capabilities that are not considered critical for DoD mission support based on DoD policies. However, it is recognized that such features and capabilities do have utility for some users or for specific operations. To ensure interoperability and consistency of these features and capabilities across all platforms, these features and capabilities are specified with set parameters. If these features and capabilities are provided, the appliance shall perform and meet the specifications as identified in the appropriate section of UCR 2008, Change 3.

**Conditional – Deployable** A variation of the "Conditional" case, where the requirement is Required for Fixed appliances, such as Local Session Controllers (LSCs) and Multifunction Softswitches in Fixed DoD networks, but is Conditional for Deployable appliances, such as LSCs in Deployable DoD networks. In other words, "Conditional – Deployable" means "Required for Fixed appliances, but Conditional for Deployable appliances." See *Conditional requirement*, *local session controller*, *multifunction softswitch*.

**Conference Call** A telephone meeting that involves three or more telephone lines connected via an audio conference bridge. This is also known as audio teleconferencing.

**Conference Calling** A feature that allows the user to establish a call involving up to six conferees (including the user).

**Conferencing** Programs and meetings for purposes such as presenting and exchanging information, comparing views, learning, planning, or decision making. Conferences can be held in one location or conducted simultaneously at multiple locations and linked together by telecommunications systems contains images, annotations, or pointers. See *annotation*.

**Conferencing Terminal Unit (CTU)** Video teleconferencing equipment that performs the following functions: coding/decoding of audio and video; multiplexing of video, audio, data, and control signals; system control; and end-to-end signaling. It does not include input/output devices, embedded and non-embedded cryptographic devices, network interface equipment, end-to-network signaling, network connections, or the network itself.

*NOTE: The scope of this profile is broader than the scope of the CTU because the scope of the profile includes cryptographic devices and other items that the CTU does not include.* See *video teleconferencing*.

**Congested Condition** One hundred percent utilization of bandwidth on the link, or links, under test. Link traffic may be any combination of real time services traffic and data, up to and including specified traffic engineering (i.e., 25 percent voice, 25 percent video, and data up to 100 percent). See *link*.

**Content** Data that is transmitted recorded and/or stored as "audio," "video," "images," "high-resolution graphics," and "slides."

**Content Delivery** The act of being able to route requests for video on-demand (VoD) to the clients nearest a VoD server or cache. Also being able to distribute content to remote VoD or cache servers on-demand or on a scheduled basis. See *content*.

**Continuous Presence** Enables each site to see multiple sites simultaneously. The participants' video window is divided into two, four, six, nine, or more sections that display preselected sites.

**Control Plane** Quality of service mechanism to provide the ability to route data correctly and perform actions during session establishment and operation to allow a network to meet quality of service needs in the data plane. This plane defines the configuration, start-up conditions, and instability conditions of the control protocols, which may include routing protocols, multicast protocols, link management, and Multiprotocol Label Switching protocols. See *data plane*, *quality of service*.

**Converged** All types of services, defined by the GIG Enterprise Service Profile Document (GESP), exist simultaneously on the same Internet Protocol (IP) network.

**Converged Local Area Network (CLAN)** A local area network (LAN) is an Internet Protocol (IP) network, composed of routers and LAN switches, that is used to connect nodes that are geographically close, usually within the same building. In a wider view of a LAN, multiple LANs are interconnected in a geographically compact area, usually by attaching the LANs to a higher speed local backbone called a campus area network (CAN). A CAN is larger than a LAN but smaller than a metropolitan area network (MAN) or wide area network (WAN). A CLAN is a LAN that supports multiple types of IP services. In the DoD, the CLAN supports voice, video,

and data services as a minimum. The CLAN is not intended to support IMMEDIATE/ PRIORITY (I/P) users and the requirements associated with a CLAN are those that are typical for commercial voice and video CLANs to include commercial grade power and availability requirements. See *availability*, *converged*, *IMMEDIATE/PRIORITY user*, *router*.

**Converged Network** An Internet Protocol (IP) network used to transmit a combination of voice, video, and/or data services. See *converged*.

**Converged Network Adapter (CNA)** Converged network adapters consolidate the Ethernet data networking capabilities of a 10 Gigabit Ethernet (GbE) network interface card (NIC) with the storage networking capabilities of a Fibre Channel (FC) Host Bus Adapter (HBA) onto a single 10GbE Ethernet adapter. The CNAs provide traditional data networking for network file system (NFS), Common Internet File System (CIFS) and Internet Small Computer System Interface (iSCSI) storage protocols concurrently with Fibre Channel over Ethernet (FCoE) storage networking. The CNAs provide significant data center cost savings while preserving an existing investment in FC storage. The CNAs are also used in Data Center Bridging (DCB) network infrastructures.

**Cryptographic Boundary** An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module. See *cryptographic module*.

**Cryptographic Module** The set of hardware, software, and/or firmware that implements approved security functions, including cryptographic algorithms and key generation, and are contained within the cryptographic boundary. See *cryptographic boundary*.

**Cryptographic Resynchronization** The process by which the conferencing terminal unit has the capability to automatically send a signal for resynchronization to the cryptographic device whenever resynchronization is needed. See *CTU*.

**Customer Edge Router (CE Router)** A router located at the boundary between the Edge Segment and the Access Segment of the wide area network. The CE Router provides traffic conditioning, bandwidth management on a granular service class (i.e., voice, video) basis, and quality of service using per-hop behaviors. A base/post/camp/station may have a single CE Router or multiple CE Routers based on the local architecture. See *granular service class*, *quality of service*, *router*.

## D

**Data Communications Port** A port used to transfer information between functional units by means of data transmission, according to a protocol.

**Data Compression** Increasing the amount of data that can be stored in a given domain, such as space, time, or frequency, or contained in a given message length. [FED-STD-1037C]

**Data Plane** Quality of service mechanism to provide the ability to manage and forward data packets, including one or more of the following: packet marking and re-marking, implementing scheduling and packet drop priorities, metering the traffic and performing congestion control, and policing and shaping the traffic. This plane defines the configuration, start-up conditions, and instability conditions of the data traffic including the traffic, collection of network elements, links between network elements, and interface profile. See *link*, *metering*, *network element*, *packet marking*, *policing*, *quality of service*.

**Data Port** See *data communications port*.

**Data Rate** In digital data communications, the rate at which data (bits in this case) is transmitted, usually expressed in bits per second.

**Default Best Effort (BE)** This is the common, best-effort forwarding behavior available in existing routers. When no other agreements are in place, it is assumed that the packets belong to this aggregate. Such packets may be sent into a network without adhering to any particular rules, and the network will deliver as many of these packets as possible and as soon as possible, subject to other resource policy constraints. This forwarding behavior is not to be used for VoIP.

**Defense Switched Network (DSN)** An interbase, nonsecure or secure DoD telecommunications system that provides dedicated telephone service, voiceband data, and dial-up video teleconference for end-to-end command use and DoD authorized IMMEDIATE/PRIORITY (I/P) and non-I/P users in accordance with national security directives. Nonsecure dial-up voice (telephone) service is the system's principal service. See *IMMEDIATE/PRIORITY user*, *non-IMMEDIATE/PRIORITY user*, *system*, *video teleconferencing*, *voice band data*.

**Denied Originating Service** A system feature that provides the capability to deny call originations selectively to individual lines.

**Deployable Voice Exchange (DVX)** A Tactical switch with military-unique features capabilities to support the assured service requirements of Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6215.01C used for rapid deployment situations and contingencies in the deployable environment. The DVXs can be either DVX Commercial Off-the-Shelf (COTS) (DVX-C), or DVX legacy (DVX-L) Tactical (TRI-TAC) systems. Normally, a DVX is connected to the Defense Switched Network (DSN) using gateway trunks routed through a Standard Tactical Entry Point/Teleport location. It can be connected directly to the DSN (Tandem Switch/ Multifunction Switch/End Office/Small End Office), if it is to be used as a temporary solution for either of the following:

- An initial capability that will be replaced by a more permanent solution for sustainment of strategic operations.

- A solution for augmenting a strategic communications facility to meet rapid growth or restoration requirements.

See *assured service*, *Defense Switched Network*, *DVX-C*, *DVX-L*, *End Office Switch*, *Small End Office*.

**Deployable Voice Exchange Commercial Off-the-Shelf (DVX-C)** A Government-deployable commercial switch that may have been modified for use within deployable environments to provide military-unique features. See *DVX*.

**Deployable Voice Exchange – Legacy (DVX-L)** A Government-deployable legacy voice switching system, such as the Common Baseline Circuit Switch and Unit Level Circuit Switch. See *DVX*.

**Deployable Private Branch Exchange (PBX**) A PBX that is allowed to connect to the Defense Switched Network via a Standard Tactical Entry Point/Teleport. Deployed PBX Type 1s do not support tandem calls and they are not approved to support FLASH and FLASH OVERRIDE users as their only means of communication. FLASH and FLASH OVERRIDE users shall be supported by other means such as a long local. See *Defense Switched Network*, *FLASH/FLASH OVERRIDE user*, *long local*, *PBX1*.

**Differential Treatment** A mechanism that allows differential handling of packets in the Edge and Core nodes. It also includes providing differential treatment at the time of resource reservation and provisioning requests.

**Differentiated Services (DS)** A quality of service delivery model, in which the flows are classified, policed, marked, and shaped at the edges of a DS domain. The nodes in the core of the network handle packets according to the per-hop behavior that is selected based on the contents of the DS field (Differentiated Services Code Point) in the packet header. See *Differentiated Services Code Point*, *DS field*, *flow*, *policing*.

**Differentiated Services Architecture** Contains two main components. One is the fairly well understood behavior in the forwarding path and the other is the more complex and still emerging background policy and allocation component that configures parameters used in the forwarding path. The differentiated services architecture is based on a simple model where traffic entering a network is classified and possibly conditioned at the boundaries of the network, and assigned to different behavior aggregates. Each behavior aggregate is identified by a single Differentiated Services Code Point (DSCP). Within the core of the network, packets are forwarded according

to the per-hop behavior associated with the DSCP. [RFC 2475] See *differentiated services*, *DSCP*, *path*, *PHB*.

**Differentiated Services (DS) Field (DS Field)** The six most significant bits of the Internet Protocol, version 4, Type of Service octet or the Internet Protocol, version 6, traffic class octet. See *DS*, *traffic class*.

**Differentiated Services Code Point (DSCP)** A value that is encoded in the Differentiated Services (DS) field and that each DS node must use to select the per-hop behavior that is to be experienced by each packet it forwards. See *differentiated services*, *DS*, *DS field*, *PHB*.

**Directed Inward Dial (DID)** A feature that allows an incoming call to reach a specific Private Branch Exchange (PBX) station line without attendant assistance. With DID, the switch seizes a DID trunk and outpulses the station line number to the PBX. If the called station's line is idle and not restricted from receiving terminating calls, the PBX alerts the called station and returns audible ringing on the incoming connection. If the called station's line is busy, the PBX returns a busy tone. If the called station is restricted from receiving terminating calls, the PBX routes the incoming call to an announcement, reorder tone, or to the attendant. See *PBX line*.

**Directed Call Pickup** A feature that permits a user to dial a code and station number and pick up a call that has been answered or is ringing at another telephone, provided the rung telephone permits dial pick-up.

**Directly Connected Conferencing Terminal Unit (CTU)** A CTU that is directly connected to the multipoint control unit (MCU) in question, rather than through another MCU. It may or may not be collocated with the MCU. See *CTU*, *MTU*.

**DISN Video Services, Global (DVS-G)** The DVS-G is a service provided by the Defense Information Systems Agency. It is meant to provide a bridging service for Department of Defense video teleconferencing (VTC) users. It uses industry standards for interoperability and multipoint VTC requirements. The DVS-G has three operational areas—the continental United States, Europe, and Pacific. See *VTC*.

**DISN Video Services II (DVS-II)** The DVS-II is a service provided by the Defense Information Systems Agency. It provides an Internet Protocol and Integrated Services Digital Network (ISDN) bridging service. It uses industry standards for interoperability and multipoint video teleconferencing (VTC) services. It will deliver enhanced services that are video centric in nature to facilitate the use of VTC communications for Department of Defense VTC users. The DVS-II has three operational areas—the continental United States, Europe, and Pacific. See *ISDN*, *VTC*.

**Disruptive** A disruptive action is one that prevents a given quantity of end instruments from placing or receiving a session for more than 5 minutes. See *end instrument*, *session*.

**DoD Directives** Broad DoD policy documents containing what is required by legislation, the President, or the Secretary of Defense to initiate, govern, or regulate actions or conduct by the DoD Components within their specific areas of responsibilities.

**DoD Secure Communications Devices (DSCDs)** Hardware devices that, when placed in the secure mode, protects the transmission of classified voice, data, or facsimile over the Defense Switched Network or other connected networks to another compatible DSCD. See *classified*, *Defense Switched Network*, *wireless*.

**Downspeed** For Integrated Services Digital Network (ISDN) conferences, the ability of a coder/decoder (codec) to carry on a conference, uninterrupted, at a lower ISDN rate, should one ISDN line or channel suddenly fail during a call. See *codec*, *ISDN*, *VTC*.

## E

**Edge Boundary Controller (EBC)** An appliance that provides voice and video firewall functions. The EBC is located at the boundary between the Edge Segment and the Access Segment. The EBC is a logical entity and its functionality may be implemented in one or more physical platforms. The EBC is used to exert control over the signaling and media streams and is involved in setting up, conducting, and tearing down sessions. Edge Boundary Controllers are put into the signaling and/or media path between the calling and the external called party. The effect of this behavior is that not only the signaling traffic, but also the media traffic (i.e., voice, video) crosses the EBC. Ultimately, EBCs allow their owners to control the kinds of session that can be placed through the networks on which they reside, and overcome some of the problems that firewalls and Network Address Translation cause for Internet Protocol voice and video sessions. As a minimum, the EBC provides topology hiding, “pinholing,” and filtering. See *appliance*, *entity*, *path*, *session*.

**Edge Label Switch Router (eLSR)** The eLSR provides the edge function of multiprotocol label switching (MPLS). The eLSR is where the label is first applied when traffic is directed toward the core of the MPLS network or last referenced when traffic is directed toward the customer. The eLSR functions as an MPLS provider edge (PE) node in an MPLS network. The eLSR is a functional PE that sends traffic to provider nodes to traverse the MPLS core, and it sends traffic to the customer interface known in MPLS terminology as the customer edge. The eLSR uses Internet Protocol routing toward the customer interface and “label swapping” toward the MPLS core. The term, label edge router, is used interchangeably with eLSR. See *label edge router*.

**EIA-449 (formerly RS-449)** The EIA-449 serial mechanical interface standard was for transmission of balanced and unbalanced signals between a variety of computer, media, and

multimedia peripherals. The EIA-449 allows a maximum data rate of 10 megabits per second and uses a 37- or 9-pin connector. *(NOTE: EIA-449 has been replaced by TIA/EIA-530; however, equipment that implements this interface is still in use.)* See *EIA*, *Telecommunications Industries Association (TIA)*.

**Elastic Service** A service that has high tolerance for packet loss, delay, and jitter (i.e., delay variation) at packet and overall message level. This service can tolerate a wide variation in the throughput. See *jitter*, *message*, *packet loss*, *throughput*.

**Electronic Industries Association (EIA)** A U.S. commercial standards organization. The abbreviation Telecommunications Industries Association (TIA)/EIA (which replaces the obsolete designation "RS") precedes a technical recommendation's numerical designation. An example is TIA/EIA-232-F, indicating its acceptance by both those bodies, replacing RS-232. See *Telecommunications Industries Association (TIA)*.

**Embedded Encryption** Encryption integrated into the conferencing terminal unit (CTU). See *CTU*.

**E-911 Management System** A UC appliance that interfaces with Local Session Controllers (LSCs) to enable reliable user locations to be provided to emergency response dispatch centers when a 911 call is made from a UC end instrument (EI).

**Emergency Service** A feature that provides a 3-digit universal telephone number (911) that gives the caller access to help and support from an emergency service bureau.

**Encapsulated Time Division Multiplexing (TDM)** T1/E1 or Fractional T1/E1 encapsulated within an alternate transport mechanism that provides assured bandwidth for both signaling and bearer channels.

**Encoder** A device that converts plain text to equivalent cipher text by means of a code.

**Encryption** The process of converting plain text into unintelligible form by means of a crypto system.

**End Instrument (EI)** An EI is a user appliance that initiates, accepts, and/or terminates a voice or video session. End instruments may be standalone applications or may be used in conjunction with other applications (e.g., softphone). They may provide a single service (e.g., voice or video) or multiple services (e.g., videophone). In addition, EIs may signal the Local Session Controller (LSC) with standardized protocols or proprietary protocols.

The EI is the primary user interface to customers for voice or video and is the originating or terminating endpoint for all voice or video sessions. It is the appliance at which the user assigns the precedence to the voice or video session, and the EI is responsible for collecting and

disseminating the user authentication information to the LSC. Finally, the EI is the point at which the network level Class of Service markings are set based on instructions from the LSC. See *appliance*, *LSC*, *precedence*, *session*, *softphone*.

**End Office (EO)** A legacy central office at which user lines and trunks are interconnected, providing long-distance service by interconnecting with Defense Switched Network (DSN) nodal switches. End Office switches provide users with switched call connections and all DSN service features, including Multilevel Precedence and Preemption.

A switch that is integral to the DSN and serves as a primary switch for long-distance services for either an installation or group of installations in a geographic area by interconnecting users to the DSN nodal switches.

**End Terminal (ET)** Optical terminal capable of terminating up to 80 channels in one direction.

**Ethernet** Popular network hardware standard that uses data transfer rates of either 10 megabits per second (Mbps) or 100 Mbps.

**Expedited Forwarding (EF)** The forwarding treatment for a particular Differentiated Services (DS) aggregate where the departure rate of the aggregate's packets from any DS node must equal or exceed a configurable rate. The EF traffic should receive this rate independent of the intensity of any other traffic attempting to transit the node. If the EF per-hop behavior is implemented by a mechanism that allows unlimited preemption of other traffic (e.g., a priority queue), the implementation shall include some means to limit the damage EF traffic could inflict on other traffic (e.g., a token bucket rate limiter). Traffic that exceeds this limit shall be discarded. [RFC 3246]

**Explicit Routing** In explicit routing, the entire list of nodes traversed by the label switched path is specified in advance. The path specified could be optimal or not, but is based on the overall view of the network topology and, potentially, on additional constraints. This is called constraint-based routing. Along the path, resources may be reserved to ensure quality of service. This permits traffic engineering to be deployed in the network to optimize use of bandwidth.

## F

**Fast Ethernet** A high-speed Ethernet network that uses data transfer rates of 100 megabits per second. See *Ethernet*.

**Fiber Maintenance Margin** The additional margin allocated to the fiber network to warrantee the continuous operation to the end of life of the Dense Wave Division Multiplex (DWDM)

system. This Fiber Maintenance Margin does not include any margins for DWDM seller's equipment.

**Fiber Span** The span loss is the attenuation between Dense Wave Division Multiplex (DWDM) equipment at adjacent DWDM locations (i.e., Optical Line Amplifier (OLA), Reconfigurable Optical Add Drop Multiplexer (ROADM), and End Terminal). The span loss consists of the outside plant (OSP) loss, the intraoffice loss, and the fiber maintenance margin. The OSP loss is the loss from the Fiber Service Delivery Point (FSDP) to FSDP. The intraoffice is from FSDP to DWDM equipment as illustrated in Figure A-1. The entrance/exist points of the DWDM equipment are the reference points MPI-S/R according to ITU-T Recommendation G.692. See *end terminal*, *fiber maintenance margin*, *OSP loss*, *ROADM*.

**Fixed Wireless End Instrument (WEI)** Those WEIs that access a single wireless local area network (WLAN) access system (WLAS) for the duration of the session and are not expected to traverse between WLASs so that handoffs are required.

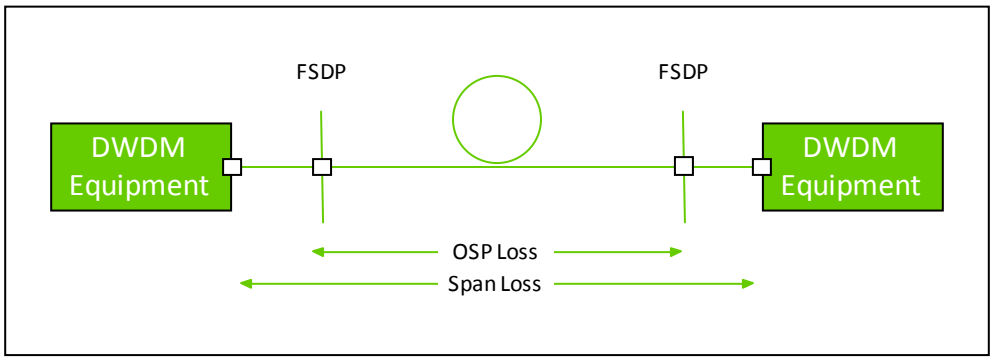


**Figure A-1. Difference between OSP Loss and the Span Loss**

**FLASH and FLASH OVERRIDE Users** A special class of users who have access to the Defense Switched Network for "essential communications for planning, directing, and controlling operations of assigned forces pursuant to assigned missions. This user requires capabilities that provide crises, pre-attack, and theater non-nuclear war telecommunications service for intelligence, alert, and strategic readiness." This user also requires communications among the President, Secretary of Defense, Chairman of the Joint Chiefs of Staff, and other members of the Joint Chiefs of Staff, Service Chiefs, and the Combatant Commanders.

**Flow** A group of packets with similar attributes as defined by a subset of the parameters in the Internet Protocol (IP) header of each packet.

**Forward Equivalence Class (FEC)** Each multiprotocol label-switching router independently selects the next hop for a given FEC. An FEC describes a group of packets of the same type; all

packets assigned to an FEC receive the same routing treatment. An FEC can be based on an IP address route or the service requirements for a packet, such as low latency.

**Frame** 1. When referring to an image, the set of all the picture elements in an image. 2. When referring to ITU-T Recommendation H.221, a frame consists of 80 octets (bytes) of multiplexed signals. This is opposed to the term field referring to interlaced television pictures where 60 fields per seconds considered full motion compared to 30 frames per second for our case of computer displays.

**Frame Alignment** In the profile, frame alignment refers to the ITU-T Recommendation H.221 frame, not the image frame. See *frame*.

**Frame Alignment Signal (FAS)** In the transmission of data frames, a distinctive sequence of bits used to accomplish frame alignment. In ITU-T Recommendation H.221, this signal also contains additional bits for status, control, and error detection. See *frame*, *frame alignment*.

**Freeze-Frame Image** A frame of visual information selected from a video signal and processed through the video codec, usually for transmission to remote sites. See *codec*, *frame*.

**Full Common Intermediate Format (FCIF)** A video format defined in ITU-T Recommendation H.261 that is characterized by 352 luminance pixels on each of 288 lines, with half as many chrominance pixels in each direction. See *chrominance*, *luminance*, *pixel*.

**Future Narrowband Digital Terminal/Secure Communications Interoperability Protocol (FNBDT/SCIP)** A protocol used to conduct a secure session with another FNBDT/SCIP capable device. SCIP and FNBDT are synonymous terms and refer to the protocols currently documented in the SCIP series of documents (e.g., SCIP-215, 216). The current preference is to use SCIP because it more accurately reflects a protocol (layer 7) as opposed to the use of FNBDT, which implies a terminal type.

## G

**Gatekeeper** An H.323 entity that provides management functions, such as address translation and control access for terminals and other endpoints.

**Gateway** An H.323 entity that provides real-time communication between H.323 terminals and terminals on other networks, such as Integrated Services Digital Network or Public Switched Telephone Network. See *Integrated Services Digital Network*,

**Grade of Service (GOS)**
a. The probability of a call being blocked or delayed more than a specified interval, expressed as a decimal fraction, (e.g., P.09 means nine calls out of 100 will be blocked). GOS may be viewed independently from the perspective of incoming versus outgoing calls and is not necessarily equal in each direction. GOS may be applied to the busy hour or to some other specified period or set of traffic conditions.

b. In telephony, the QoS for which a circuit is designed or conditioned to provide; e.g., voice grade or program grade. Criteria for different grades of service may include equalization for amplitude over a specified band of frequencies, or in the case of digital data transported via analog circuits, equalization for phase.

**Granular Service Class** Represents the atomic identification of a service class. A set of granular service classes sharing similar traffic characteristics forms an aggregate service class. See *aggregate service class*, *service class*.

**Guaranteed Service** The use of signaling to reserve network resources end-to-end to meet preset performance objectives.

## H

**H.323 to H.320 Gateway** A videoconferencing endpoint that converts between H.323 IP endpoint protocols and services and H.320 endpoint protocols and services for transport of videoconferencing data between IP and serial or integrated services digital network (ISDN) sessions. See *ISDN*.

**High Assurance Internet Protocol Encryption (HAIPE)** A Type I encryptor device used to encrypt data used on an IP network.

**High Bit Rate DSL (HDSL)** HDSL is a bidirectional and symmetrical transmission system that allows the transport of signals with a bit rate of 1544 Kbps or 2048 Kbps on the copper twisted pairs of an access network at a distance of up to 12,000 feet.

**High-Resolution Graphics** Graphics captured and displayed at a higher resolution than the National Television System Committee standard (EIA-170-A).

**Hub** 1. A distribution point in a network. 2. A device that accepts a signal from one point and redistributes it to one or more points.

## I

**IMMEDIATE/PRIORITY (I/P) Users** IMMEDIATE/PRIORITY users include any person (regardless of the position in the chain of command) who issues or receives guidance or orders that direct, control, or coordinate any military forces regardless of the nature of the military mission (including combat support, administration, and logistics), whether said guidance or order is issued or effected during peacetime or wartime.

**In-band** Term used when network management system connects to the network device using the same Ethernet port communication channel used for user traffic.

**Incoming Access** Allows a community of interest (COI) user to receive local calls from all other non-COI users and from those other COI users who allow outgoing access. See *COI*.

**Incoming Access with Precedence** Allows a community of interest (COI) user to receive only local COI precedence level calls from all other non-COI users and from those other COI users who allow outgoing access. See *COI*, *COI precedence level*.

**Individual Line** A line arranged to serve only one main station, although additional stations may be connected to the line as extensions of the main station.

**Inelastic Service** A voice and video service that typically requires strict bounds on packet loss, delay, and jitter. See *jitter*, *packet loss*, *throughput*.

**Information Assurance Enabled Product** A system whose primary function is not Information Assurance, but does have some Information Assurance functions. See *system*.

**Information Assurance Product** A system that provides Information Assurance functions consistent with the Information Assurance services and categories (i.e. authentication, confidentiality). An Information Assurance product's primary purpose is to provide Information Assurance functions. See *system*.

**Information Technology (IT) Products** Systems that receive, process, store, display, or transmit Department of Defense voice and video services. See *system*.

**Instant Messaging (IM)** The capability for users to exchange one-to-one ad hoc text messages over a network in real time. Instant Messaging is not the same as and must not be confused with signaling or equipment messaging; IM is always user generated and user initiated. See *message*.

**Integrated Services Digital Network (ISDN)** See *FED-STD-1037C, Integrated Services Digital Network*.

*NOTE: Access channels include a basic rate (two 64-kilobits per second (kbps) B-channels plus one 16-kbps D-channel) and a primary rate (twenty-three 64-kbps B-channels and one 64-kbps D-channel). Also known as Narrowband-ISDN or N-ISDN.*

**Integrated Services Digital Network (ISDN) Device** An ISDN specifies a number of reference points that define logical interfaces between functional ISDN devices such as terminals, terminal adapters, network termination devices, and line termination equipment. An ISDN specifies a number of reference points that define the interconnection of these devices.

Integrated Services Digital Network devices are defined as:

TE1 Terminals with built-in ISDN connection capability (also referred to as TE).

TE2 An existing terminal device, designed for existing protocols. It is not capable of directly interoperating with ISDN.

TA An adaptive device designed to permit TE2s to interoperate with ISDN.

See *ISDN reference points*, *ISDN terminal adapter*, *ISDN terminal equipment 1*, *ISDN terminal equipment 2*.

**Integrated Services Digital Network (ISDN) Integrated Access Interface** An ISDN user-network interface in which the interface structure is composed of multiple B-channels and one D-channel.

**Integrated Services Digital Network (ISDN) NT 1** A single (physical) layer device that contains all the necessary interface elements to communicate with the network. It terminates the local loop and provides the user interface to the network while isolating this user from the operation of the network.

**Integrated Services Digital Network (ISDN) R** The reference point representing a standardized non-ISDN interface, such as Electronics Industries Alliance (EIA)-232, EIA-422, V.24, V.35, and others. The combination of a Terminal Adapter and Terminal Equipment Type 2 is equivalent to a Terminal Equipment Type 1.

**Integrated Services Digital Network (ISDN) Reference Points** The reference points applicable for Defense Switched Network customer premises equipment are as follows:

U The reference point for a basic rate interface (BRI) connection between a local loop and a customer premise. The U interface specifies a single pair loop over which a logical 4-wire circuit is derived.

S The reference point between ISDN user terminal equipment (i.e., Terminal Equipment Type 1 (TE1) or Terminal Adapter (TA)) and the network termination equipment. This is a 4-wire interface that supports the BRI 2B+D protocol.

R The reference point representing a standardized non-ISDN interface such as Electronics Industries Alliance (EIA)-232, EIA-422, V.24, V.35, and others. The combination of a TA and Terminal Equipment Type 2 (TE2) is equivalent to a TE1.

**Integrated Services Digital Network (ISDN) S** The reference point between ISDN user terminal equipment (i.e., Terminal Equipment Type 1 or Terminal Adapter) and the network termination equipment (NT1). This is a 4-wire interface that supports the Basic Rate Interface 2B+D protocol.

**Integrated Services Digital Network (ISDN) Terminal Adapter** An adaptive device designed to permit Terminal Equipment Type 2 to interoperate with ISDN.

**Integrated Services Digital Network (ISDN) Terminal Equipment (TE) 1** Terminals with built-in ISDN connection capability (also referred to as TE).

**Integrated Services Digital Network (ISDN) Terminal Equipment (TE) 2** An existing terminal device designed for existing protocols. It is not capable of directly interoperating with ISDN.

**Integrated Services Digital Network (ISDN) U** The reference point for a Basic Rate Interface connection between a local loop and a customer premise. The U interface specifies a single pair loop over which a logical 4-wire circuit is derived.

**Internet Protocol (IP) Centric** Internet Protocol centric architectures are designed around an IP core packet switching system. These solutions have distributed IP devices that function together to provide voice and video over IP services.

**Internet Protocol (IP) Data Subscriber** A user connected to an IP network to receive Department of Defense IP services, such as data and IP video. Defense Switched Network IP telephony is not included. See *Defense Switched Network*.

**Internet Protocol Packet Delay Variation (IPDV)** The one-way IPDV(n) is defined as the difference between the one-way delay of the selected packet and the packet with the lowest IP Packet Transfer Delay (IPTD) in the evaluation interval: IPDV(n) = IPTD(n) – IPTD(0). [ITU-T Recommendation Y.1540, IETF RFC 3393]. In the case of voice and video services, the measurements are typically taken at the end instruments. This is also referred to as jitter.

**Internet Protocol Packet Loss Ratio (IPLR)** A metric measured for packets traversing the network segment between the source reference point and destination reference point. The IPLR metric is reported as the number of lost packets at the destination reference point divided by the number of packets sent at the sender reference point to that destination. [ITU-T

Recommendation Y.1540, IETF RFC 2680]. This is also referred to as packet loss. See *packet loss*.

**Internet Protocol Packet Transfer Delay (IPTD)** The single instance of the one-way IPTD measurement is defined as the time the test packet traverses the network segment(s) between two reference points. The metric is defined as a time starting from the time the first bit of the packet is put on the wire at the source reference point to the time the last bit of the packet is received at the receiver reference point. [ITU-T Recommendation Y.1540, IETF RFC 2679] In the case of voice and video services, the measurement points are the end instruments. This is also referred to as latency. See *end instrument*, *latency*.

**Internet Protocol Signaling Gateway (IPSG) Function** A signaling appliance that relays, translates, or terminates IP messages between various IP signaling protocols such as Assured Service Session Initiation Protocol, H.323, H.248, and IP proprietary signaling protocols. See *appliance*, *Assured Service Session Initiation Protocol*, *assured service*, *message*.

**Internet Protocol (IP) Telephony Subscriber** A Defense Switched Network IMMEDIATE/PRIORITY (I/P) or non-I/P user that receives voice service via an IP telephone instrument (also known as an End Instrument). See *Defense Switched Network*, *end instrument*, *I/P user*, *non-I/P user*.

**Internet Protocol (IP) Transport** The aggregation of various types of IP traffic, such as voice, video, and data that is transmitted over IP link. See *link*.

**Internet Protocol Version 6 (IPv6) Capable** A system or product capable of receiving, processing, and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IP version 4. See *system*.

**Internet Protocol Version 6 (IPv6) Capable Networks** Networks that can receive, process, and forward IPv6 packets from/to devices within the same network and from/to other networks and systems, where those networks and systems may be operating with only Internet Protocol version 4 (IPv4), only IPv6, or both IPv4 and IPv6. See *system*.

**Internet Protocol Version 6 (IPv6) Capable Products** Products (whether developed by commercial vendor or the Government) that can create or receive, process, and send or forward (as appropriate) IPv6 packets in mixed Internet Protocol version 4/IPv6 environments.

**Internet Protocol Version 6 (IPv6) Enabled Network** An IP network that is supporting operational IPv6 traffic through the network end-to-end.

**Internet Protocol (IP) Video Subscriber** A Defense Switched Network non-IMMEDIATE/ PRIORITY user that receives video service via an IP video system. See *Defense Switched Network*, *non-IMMEDIATE/PRIORITY user*, *system*.

**Inverse Multiplexer (IMUX)** A device used to create a single, higher speed network data channel by combining, separating, and synchronizing multiple, independent 56- or 64 kilobits per second network data channels. Also known as an aggregator.

## J

**Jitter** The one-way jitter is defined as the difference between the one-way delay of the selected packet and the packet with the lowest IP Packet Transfer Delay (IPTD) in the evaluation interval: IPDV(n) = IPTD(n) – IPTD(0). [ITU-T Recommendation Y.1540, IETF RFC 3393]. In the case of voice and video services, the measurements are taken at the end instruments. This is also referred to as the IP Packet Delay Variation (IPDV). The difference in arrival time of packets sent over a network at the receiving end compared to the difference in packet spacing at the sending end. See *end instrument*, *IPDV*, *IPTD*.

## K

**kbps** An abbreviation for kilobits per second, a measure of bandwidth. A measurement of digital information transmission speed of data measured in 1,024 bits per second.

**KG-194/194A** (National Security Agency cryptographic device nomenclature) A Federally certified cryptographic device used to provide data encryption at data rates from 9.6 kilobits per second up to 13 megabits per second over synchronous serial links, typically on dedicated circuit networks. See *link*.

**KIV-7/KIV-7HS** (National Security Agency cryptographic device nomenclature) A Federally certified cryptographic device used to provide data encryption at data rates up to 2.048 megabits per second on dial-up and other nondedicated networks. See *link*.

**KIV-19/19A** (National Security Agency cryptographic device nomenclature) A Federally certified cryptographic device used to provide data encryption at data rates from 9.6 kilobits per second up to 13 megabits per second over synchronous serial links on dedicated circuit or dial-up network paths. The KIV-19/19A is interoperable with the KG-194/194A. See *link*.

## L

**Label** A header created by an Edge Label Switch Router and used by Label Switch Routers to forward packets. The header format various based on the network media type. In the Assured Services Local Area Network environment, the header is a "shim" located between the Layer 2 and Layer 3 headers. See *assured services local area network*, *edge label switch router*, *label switch router*.

**Label Distribution Protocol (LDP)** This protocol defines a set of procedures used by multiprotocol label switching (MPLS) routers to exchange label and stream mapping information. It is used to establish label switched paths, mapping routing information directly to Layer 2 switched paths. It is also commonly used to signal at the edge of the MPLS network the critical point where non-MPLS traffic enters. For example, such signaling is required when establishing MPLS virtual private networks. See *label switched path*.

**Label Edge Router (LER)** The LER provides the edge function of multiprotocol label switching (MPLS). The LER is where the label is first applied when traffic is directed toward the core of the MPLS network or last referenced when traffic is directed toward the customer. The LER functions as an MPLS provider edge (PE) node in an MPLS network. The LER is a functional PE that sends traffic to provider nodes to traverse the MPLS core, and it sends traffic to the customer interface known in MPLS terminology as the customer edge. The LER uses IP routing toward the customer interface and "label swapping" toward the MPLS core. The term Edge Label Switch Router is used interchangeably with LER. See *edge label switch router*, *label*, *label swapping*.

**Label Information Base (LIB)** As the network is established and signaled, each multiprotocol label switching router builds a LIB, a table that specifies how to forward a packet. This table associates each label with its corresponding Forward Equivalence Class and the outbound port to forward the packet to. Typically, the LIB is established in addition to the routing table that traditional routers maintain. See *forward equivalence class*, *label*.

**Label Swapping** A forwarding decision process set that allows streamlined forwarding of data by using labels to identify classes of data packets, which are treated indistinguishably when forwarding. See *label*.

**Label Switch Router (LSR) or Label-Switching Router (LSR)** The LSR provides the core function of multiprotocol label switching (MPLS). The LSR is equipped with both Layer 3 routing and Layer 2 switching characteristics. The LSR functions as a provider node in an MPLS network.

**Label Switched Path (LSP)** Multiprotocol label switching networks establish LSPs for data crossing the network. An LSP is defined by a sequence of labels assigned to nodes on the packet's path from source to destination. An LSP directs packets in one of two ways: hop-by-hop routing or explicit routing. The path goes through one or more Label Switch Routers at one level of the hierarchy followed by a packet in a particular Forward Equivalence Class. See *forward equivalence class*, *label*, *label switch router*, *path*.

**Latching** The ability of the reconfigurable optical add drop multiplexer to maintain its current state in the event of power failure. See *reconfigurable optical add drop multiplexer*.

**Latency** The single instance of the one-way latency measurement is defined as the time the test packet traverses the network segment(s) between two reference points. The metric is defined as a time from the time the first bit of the packet is put on the wire at the source reference point to the time the last bit of the packet is received at the receiver reference point. [ITU-T Recommendation Y.1540 and IETF RFC 2679] In the case of voice and video services, the measurement points are the end instruments. This is also referred to as IP packet transfer delay (IPTD). See *end instrument*, *IPTD*.

**Link** The communications facilities between adjacent nodes of a network. For voice over IP systems, a link is an Ethernet connection used for IP transport as opposed to trunks used for time division multiplexing transport. See *Ethernet*.

**Link Pair** To ensure no single point of failure to more than 64 Internet Protocol (IP) telephony subscribers, IP network links shall have a second link (standby or load sharing). The combination of the two links is called a link pair. See *link*.

**Local Area Network (LAN) Access or Edge Layer** The point at which local end users are allowed into the LAN. In addition, these layers may use access lists or filters to optimize further the needs of a particular set of users. This term should not be confused with the wide area network (WAN) Edge or WAN Access Layer.

**Local Area Network (LAN) Core Layer** A high-speed switching backbone that is designed to switch packets as fast as possible within the LAN. This term should not be confused with the wide area network Core Layer.

**Local Area Network (LAN) Distribution or Building Layer** The distribution or building layer of the LAN is the demarcation point between the Access and Core Layers, and it helps to define and differentiate the core. This layer provides boundary definition, and it is where packet manipulation can take place. See *LAN Access Layer*, *LAN Core Layer*.

**Local Area Network (LAN) Network Links** Internal Internet Protocol (IP)/Ethernet links that interconnect LAN components. See *Ethernet*, *link*.

**Local Area Network (LAN) Switch** A LAN switch is an appliance that reduces contention on LANs by reducing the number of nodes on a segment using microsegmentation techniques. On a microsegmented network, a LAN segment may have many nodes or a single node. The LAN switch handles all the connections between nodes on different LAN segments when they need to communicate through an internal matrix switch that processes the packets at the Media Access Control (MAC) layer. When a packet arrives at the switch, its destination MAC address is quickly noted and a connection is set up to the appropriate end segment. Subsequent packets are relayed through the switch without the need to store and forward packets, as is necessary with bridges. Many LAN switches in the DoD Internet Protocol Unified Capabilities architecture include router functions. See *appliance*, *router*.

**Local Session Controller (LSC)** A call stateful Assured Service Session Initiation Protocol (AS-SIP) signaling appliance at a base/post/camp/station that directly serves Internet Protocol (IP) end instruments (EIs). The LSC MAY consist of one or more physical platforms. On the trunk side, the LSC uses AS-SIP signaling. On the line side, the LSC may serve any combination of Session Initiation Protocol EIs, H.323 EIs, and proprietary EIs. The LSC MUST be an intermediary for every inbound and outbound call signaling message received and transmitted by each IP EI served by the given LSC. See *appliance*, *AS-SIP*, *assured service*, *call stateful*, *EI*, *message*, *Session Initiation Protocol*.

**Local Session Controller (LSC) Level Assured Services Admission Control (L-ASAC)** The processes on an LSC that ensure that quality of service requirements of a higher precedence service will be met at the expense of a lower precedence service if the network conditions do not allow meeting quality of service requirements of all services. Typically, the processes are associated with the preemption of lower precedence sessions to an end instrument to ensure that higher precedence sessions can be completed. See *assured service*, *ASAC*, *end instrument*, *LSC*, *quality of service*, *session*.

**Location Server** The location server provides information on call routing and called address translation (where a called address is contained within the called Session Initiation Protocol Secure Uniform Resource Identifier in the form of the called number). The service provided by the server typically is referred to as location services. The Call Connection Agent uses the routing information stored in the location server:

- To route internal calls from one Local Session Controller (LSC) end instrument (EI) to another EI on the same LSC,
- To route outgoing calls from an LSC EI to another LSC, a multifunction softswitch (MFSS), or a time division multiplexing (TDM) network, and
- To route incoming calls from another LSC, an MFSS, or a TDM network to an LSC EI or MFSS.

See *Call Connection Agent*, *EI*, *LSC*, *MFSS*, *Session Initiation Protocol*

**Long Local** A long-local telephone is connected remotely through an assured transmission means, time division multiplexing or Internet Protocol, to a distant site. This interface is handled as a local loop to the host Defense Switched Network switch. See *Defense Switched Network*.

**Luminance** The intensity component of a pixel. The Y component in YCbCr. The L component in CIElab. See *chrominance*, *pixel*.

## M

**Management Plane** A quality of service mechanism to access network elements for network management purposes, such as provisioning and policy setting. This plane is used to define the configuration, startup conditions, and instability conditions of the management protocols and features including Simple Network Management Protocol, Logging/Debug, statistics collection, and management configuration sessions such as telnet, Secure Shell, and serial console. See *network element*, *quality of service*,

**Maximum Segment Size (MSS)** The MSS is the largest amount of data, specified in bytes, that a computer or communications device can handle in a single, unfragmented piece. The MSS is an important consideration in Internet Protocol (IP)-based networks. As data is routed over an IP network, it must pass through multiple gateway routers. Ideally, each TCP segment can pass through every router without being fragmented. If the data segment size is too large for any of the routers through which the data passes, the oversized segments are fragmented. This fragmentation slows down the connection speed seen by the computer user, in some cases dramatically. The likelihood of such fragmentation can be minimized by keeping the MSS as small as reasonably possible. For most computer users, the MSS is set automatically by the operating system. See *router*.

**Maximum Transition Unit (MTU)** A term for the size (in bytes) of the largest datagram that can be passed by a layer of a communications protocol.

**Mbps (Megabits Per Second)** A measure of bandwidth. A measurement of the transmission speed of data measured in 1,048,576 bits per second. A unit of how much digital information is transferred over time.

**Mean Time Between Failures (MTBF)** For a particular interval, the total functional life of a population of an item divided by the total number of failures (requiring corrective maintenance actions) within the population.

**Mean Time To Repair (MTTR)** The total amount of time spent performing all corrective maintenance repairs divided by the total number of those repairs.

**Measurement-Based Admission Control** An approach that bases a call control decision on the monitoring of network capacity. Admits, rejects, or redirects calls based on current network congestion. See *call control*.

**Media Gateway (MG)** An MG within the DoD environment is defined in accordance with the Internet Engineering Task Force Request for Comments 2805, "Media Gateway Control Protocol Architecture and Requirements," and provides the media mapping and/or transcoding functions between time division multiplexing and Internet Protocol (IP) networks. The MG terminates switched circuit network (SCN) facilities (e.g., trunks, loops), packetizes the media stream, if it is not already packetized, and delivers packetized traffic to an IP network. It would perform these functions in the reverse order for media streams flowing from the IP network to the SCN.

**Media Gateway Controller (MGC)** The function in a signaling appliance that controls a media gateway. See *appliance*, *media gateway*.

**Media Server** A platform in an Internet Protocol telephony network that transmits dial tones, busy signals, and announcements.

**Meet-Me Conferencing** A conference that is established when each conferee dials into the conference bridge at a scheduled time as directed by a conference attendant. See *conferencing*.

**Message** A unit of data transfer from an application in one host to an application in another host.

**Message Discrimination and Distribution Function** A function that examines the Destination Point Code of a received signaling message to determine whether it is destined to the receiving signaling point.

**Metering** The process of measuring the temporal properties (e.g., rate) of a traffic stream selected by a classifier. The instantaneous state of this process may be used to affect the operation of a marker, shaper, or dropper, and/or may be used for accounting and measurement purposes. [RFC 2475] See *classifier*.

**Metric** A quality of service delivery parameter such as delay, packet loss, data rates, and availability. See *availability*, *packet loss*, *quality of service*.

**Microflow** A single instance of an application-to- application flow of packets that is identified by source address, source port, destination address, destination port, and protocol identification. [RFC 2475] See *flow*.

**Minimum Requirements** Features and capabilities considered necessary for a particular switch type to support warfighter missions in the DoD. These features and capabilities will require certification before introduction into the Defense Switched Network. See *Defense Switched Network*.

**Mobile Code** Software modules obtained from or provided by remote systems, transferred or downloaded across a network, and then executed on local systems without explicit installation or execution by the recipient.

**Modem over IP (MoIP)** The transport of modem data across an Internet Protocol network, via either modem relay or voiceband data (modem pass-through) techniques. See *voiceband data*.

**Modem Relay** A subset of Modem over IP in which modem termination is used at gateways, thereby allowing only the baseband data to reach the packet network. See *Modem over IP*.

**MPEG (Moving Picture Experts Group)** A standard for a digital video and audio compression.

**MTU** See *Maximum Transition Unit*.

***μ-Law*** The pulse code modulation coding and companding (compressing and expanding) standard used for non-linear compression in the analog-to-digital conversion process that is used primarily in Japan and North America. See *A-Law*.

**Multicasting** The ability of the reconfigurable optical add drop multiplexer to allow one input wavelength to be duplicated on multiple output tributary and line ports. Also, the process of transmitting data/information from one source to many destinations in a single transfer. See *broadcasting*, *reconfigurable optical add drop multiplexer*, *unicasting*.

**Multifunction Softswitch (MFSS)** A network appliance that provides the following functions:

- Provides all multifunction switch (MFS) functions:
  - Tandem Switch
  - End Office
  - Softswitch functions
  - Global directory services
  - Local Session Controller (LSC) functions
  - Media Gateway functions
  - Signaling Gateway functions
  - Network management
  - Fault, configuration, accounting, performance, and security

- Supports Policy Based Network Management:
  - Assured Services Admission Control budget controls
  - Customer Edge Router queue bandwidth allocations
  - End instrument (EI) session origination control (according to designated groups)
  - EI session destination control (according to designated groups)

The MFSS is a logical entity and its functionality MAY be implemented in one or more physical platforms.

The MFSS is an MFS that is enhanced with an Internet Protocol (IP) interface. As with any MFS, the MFSS supports End Office and Tandem Switch capabilities. In addition, the MFSS also includes LSC and Assured Real Time Services (ARTS) Softswitch (SS) functions to support line-side IP EI and trunk-side Assured Service Session Initiation Protocol (AS-SIP) and AS-SIP for Telephones signaling. For Tandem Switch EIs connected to the MFSS, the MFSS is the media endpoint for sessions connected to an IP EI at the terminating location. See *appliance*, *AS-SIP*, *assured services admission control*, *customer edge router*, *EI*, *end office*, *entity*, *LSC*, *MFS*, *media gateway*, *signaling gateway function*, *SS*.

**Multifunction Switch (MFS)** "A switch that combines the tandem function of the SA [Standalone] switch with the EO [End Office] function of connecting the user's lines to the backbone trunks. Logically the SA and EO are separate, but within the same physical configuration." [CJCSI 6215.01C] See *end office*.

**Multilevel Precedence and Preemption (MLPP)** In circuit-switched systems, a priority scheme:

- For assigning one of several precedence levels to specific calls or messages so that the system handles them in a predetermined order and timeframe,

- For gaining controlled access to network resources in which calls and messages can be preempted only by higher priority calls and messages,

- That is recognized only within a predefined domain, and

- In which the precedence level of a call outside the predefined domain is usually not recognized.

See *FLASH/FLASH OVERRIDE user*, *IMMEDIATE/PRIORITY user*, *precedence*.

**Multilevel Precedence and Preemption (MLPP) Call** A call that has a precedence level established and is either being set up or is set up. In Digital Subscriber Signaling System No. 1

(DSS1: ISDN Q.931 signaling), an MLPP call is a call from an MLPP subscriber for which a setup has been sent but no DISCONNECT has been sent or received. See *MLPP*, *precedence*.

**Multilevel Precedence and Preemption (MLPP) Service Domain** A set of MLPP subscribers (MLPP users) and the network and access resources that are in use by that set of MLPP subscribers at any given time. Connections and resources that are in use by MLPP subscribers may be preempted only by higher precedence calls from MLPP subscribers within the same domain. The service domain consists of a 3-octet field ranging from 00 00 00 to FF FF FF in hexadecimal. The Defense Switched Network service domain is zero (0). See *Defense Switched Network*, *MLPP*, *precedence*.

**Multipoint** A telecommunications system that permits three or more locations to intercommunicate in a conference call. See *conference call*.

**Multipoint Control Unit (MCU)** 1. An endpoint that enables intercommunication of three or more video teleconferencing (VTC) endpoints in a conference call. It can be used with two VTC endpoints, for example, while beginning or ending a multipoint conference. The MCU may perform mixing or switching of audio, video, and data. 2. A multiport device, by means of which three or more conferencing terminal units **(**CTUs) may intercommunicate in a conference call. It can also be used with two CTUs, e.g., while beginning or ending a multipoint conference. See *conference call*, *CTU*, *VTC*.

**Multipoint Controller (MC)** The MC is an H.323 entity on the network that provides for the control of three or more terminals participating in a multipoint conference. It may also connect two terminals in a point-to-point conference, which may later develop into a multipoint conference. The MC provides for capability negotiation with all terminals to achieve common levels of communications. It may also control conference resources such as who is multicasting video. The MC does not perform mixing or switching of audio, video, and data. See *entity*, *multicasting*.

**Multipoint Processor (MP)** The MP is an H.323 entity on the network that provides for the centralized processing of audio, video, or data streams in a multipoint conference. The MP provides for the mixing, switching, or other processing of media streams under the control of the Multipoint Controller. The MP may process a single media stream or multiple media streams depending on the type of conference supported. See *multipoint controller*.

## N

**Nailed Up Connections** A **s**pecial use permanently established path through a switch for either a network circuit (trunk) or a special service facility. See *path*.

**Narrowband Streaming** For the purposes of this document, Narrowband Streaming refers to the transfer of data in a continuous audio and/or video stream over a network using bandwidth from 28.8 kilobits per second to 1.5 megabits per second.

**Network** 1. All telecommunications equipment that has any part in processing a call or a supplementary service for the user referred to. It may include local exchanges, transit exchanges, and Network Termination 2 but does not include the integrated services digital network (ISDN) terminal and is not limited to the "public" network or any other particular set of equipment. 2. Refers to the system of cables, microwave links, and switching centers that allow the transmission of data, as opposed to the terminal equipment (such as codecs and input/output devices) connected to the cables. [FED-STD-1037C] See *codec*, *ISDN*.

**Network Domain** A contiguous set of network elements that belongs to the same administrative authority. See *network element*.

**Network Element (NE)** A component of a network through which the Defense Switched Network (DSN) bearer and/or signaling traffic transits. For Internet Protocol (IP) transport, the IP connection may transit a Local Area Network (LAN), Metropolitan Area Network (MAN), Campus Area Network (CAN), or Wide Area Network (WAN) dependent on its deployment. Network elements may include multiplexers, routers, Channel Service Units/Digital Service Units (CSU/DSUs), compression devices, circuit emulation, channel banks, and/or any network device that could have an effect on the performance of the associated network traffic. The network diagram, shown in Figure A-2, Network Element Diagram, shows the typical NE as a standalone device or integrated into the transmission interfaces of switches or other network devices. The use of NEs shall not provide the means to bypass the DSN as the first choice for all switched voice and dial-up video telecommunications between DoD user locations. See *DSN*, *router*.

**Network Interface Equipment** The equipment connected between the network and the conferencing terminal unit (CTU). Such examples of this equipment include (a) the channel service unit (CSU), (b) the data service unit (DSU), and the (c) terminal adapters. See *CTU*.

**Network Signaling Based Admission Control** Determines based on requests indicated through a signaling protocol whether a node or network has sufficient available resources to meet the requested quality of service. [RFC 2205] See *admission control*, *quality of service*.

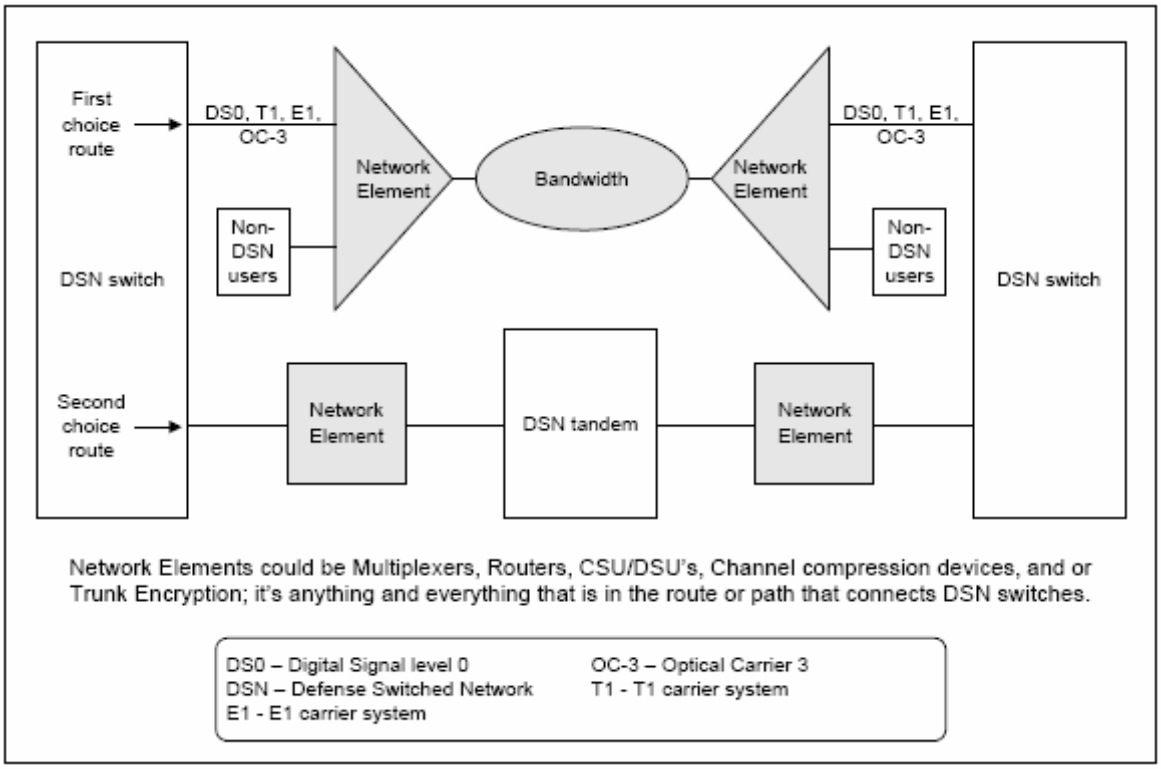


**Figure A-2. Network Element Diagram**

**Network Terminator Type 1 (NT-1)** A device that converts a 2-wire U-interface to a 4-wire S/T interface, allowing multiple conferencing terminal unit connections. See *CTU*.

**New Call** The event that precipitates a trunk seizure or when preemption for reuse of a trunk is used to support multilevel precedence and preemption calls in the Defense Switched Network. See *Defense Switched Network*, *multilevel precedence and preemption*.

**Nomadic Wireless End Instrument (WEI)** Those WEIs that are mobile and may traverse different wireless local area network access systems during a single session. See *session*, *WEI*, *wireless local area network*.

**Non-Assured Service Local Area Network (Non-ASLAN)** The Internet Protocol (IP) network infrastructure components used to provide services (i.e., voice, video, and data) to end users. Non-ASLANs are "commercial grade" and provide support to IMMEDIATE/PRIORITY (I/P) (ROUTINE only calls) (I/P(R)) or non-I/P voice subscribers. See *ASLAN*, *I/P user*, *non-I/P user*.

**Non-Assured Video** Video sessions that are established independent of any call admission control exercised by either a local session controller or H.323 Gatekeeper. See *call admission control*, *H.323 gatekeeper*, *local session controller*.

**Non-Assured Voice** Audio sessions that are established independent of any call admission control exercised by a local session controller. See *call admission control*, *local session controller*.

**Nonblocking Local Area Network (LAN)** A LAN that is provisioned so all Internet Protocol telephone instruments can be off hook simultaneously and successfully engaged in a full duplex voice call. See *blocking*.

**Non-Converged Network** A network that is used solely to provide Defense Switched Network Voice over Internet Protocol (IP) services. A separate IP network will be used to provide IP data services. See *converged*, *Defense Switched Network*.

**Non-IMMEDIATE/PRIORITY (I/P) Users** Those users, DoD, non-DoD, non-U.S. Government and foreign government users that have no missions or communications (equipment) requirements to originate or receive I/P communications under the existing military scenarios. These users are provided access to the Defense Switched Network (DSN) for economic benefit of the DoD. During a crisis or contingency, these users may be denied access to the DSN. It is the primary means of secure communications for non-Tactical I/P users. The DSN must be the user's first choice; however, if the DSN is not immediately available, or if the called party does not have access to DSN service, other long-distance calling methods may be used. See *DSN*, *I/P user*.

**Nonpreemptive Service** A Global Information Grid service that offers a committed information rate between two or more Edge networks, where the bandwidth cannot be preempted for the use of any other party than the one contracting for the service.

**Nonsignaled Flow** A flow that does not require signaling to enter a network. See *flow*.

## O

**Objective Requirement [Objective]** A requirement that does not have to be met in the initial operational capability (IOC), but must be met in the final operational capability (FOC). The timeframe associated with the IOC is fiscal year (FY) 2008 and the timeframe associated with the FOC is FY 2012 unless specifically stated.

**Offered Load Control** A mechanism that allows control of packet transfer loads to keep them within specified bounds (possibly described in service level agreements) so that network domains can deliver the promised quality of service. See *network domain*, *quality of service*, *service level agreement*.

**Operations, Administration, and Maintenance (OA&M)** A set of network management functions, providing network fault indication, performance information, and data and diagnosis functions.

**Optical Line Amplifier (OLA)** Provides optical signal reamplification without converting to electrical signal along the spans between optical terminal equipment.

**Originating Internet Protocol (IP)/Time Division Multiplexing (TDM) Signaling Gateway Function** The function related to receiving an Initial Address Message (IAM) from the Signaling System No. 7 network and generating an Assured Service Session Initiation Protocol INVITE with the encapsulated Integrated Services Digital Network (ISDN) User Part (ISUP) IAM that is sent over the IP network—identical to Outgoing Interworking Unit in International Telecommunications Union – Telecommunication Standardization Sector Recommendation Q.1912.5, "Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control Protocol or ISDN User Part." See *Assured Service Session Initiation Protocol*, *Signaling System No. 7*, *SIP*.

**Originating Gateway** An Assured Service Session Initiation Protocol for Telephones signaling appliance performing the originating Internet Protocol/Time Division Multiplexing Signaling Gateway function. See *appliance*, *Assured Service Session Initiation Protocol*, *Signaling Gateway function*.

**Outgoing Call Trace** A feature that allows the tracing of nuisance calls to a specified directory number suspected of originating from a given local office. The tracing is activated when the specified directory number is entered. A printout of the originating directory number, outgoing trunk number, or terminating number, and the time and date is generated for every call to the specified directory number.

**Out-of-Band** A term used to describe network management systems that connect to the network device using a physically separated network from the network used for user traffic. This requires an additional network infrastructure to support management traffic.

**Outside Plant (OSP) Loss** The OSP loss is measured from the fiber connector in the Fiber Service Delivery Point (FSDP) of a Dense Wave Division Multiplex (DWDM) equipment location to the fiber connector (at the other end of the fiber) in the FSDP of the next DWDM equipment location. The OSP loss is the combined loss of the fiber attenuation itself and the attenuation due to splices and connectors across the span.

**Overflow Process** A process that allows calls of a lower precedence level and narrower calling area to utilize unused calling capacity of a higher precedence level and equal and wider calling area, and equal precedence level and wider calling area call types without blocking calls of a higher precedence level and wider calling area. See *blocking*, *precedence*.

## P

***p*** An integer that can range from 1 to 30 and is limited to the values of 1, 2, 3, 4, 5, 6, 12, 18, 23, 24, and 30 for conferencing terminal unit (CTU) operation over digital-switched networks. It relates to CTUs that operate at nominal bit rates of integer "*p*" multiples of 64,000 bits per second (bps). For unrestricted channels, such as provided by integrated services digital network, each increment of data rate may actually be 64,000 bps, but in restricted channels, each increment may be only 56,000 bps. See *CTU*, *integrated services digital network*.

**Packet Loss** A metric measured for packets traversing the network segment between the source reference point and destination reference point. The Packet Loss metric is reported as the number of lost packets at the destination reference point divided by the number of packets sent at the sender reference point to that destination. [ITU-T Y.1540, IETF RFC 2680]. This is also referred to as Internet Protocol packet loss ratio. See *Internet Protocol packet loss ratio*.

**Packet Marking** Marking in packets following their classification for a given service delivery, which includes Differentiated Services Code Point, Flow Label, or Security Parameter Index bit fields. See *differentiated services code point*.

**Path** Communications link between two network components. A path may include a number of communications links. See link.

**PC (Personal Computer)** A computer specifically designed for use by one person at a time, equipped with its own CPU, memory, operating system, keyboard and display, hard/floppy disks, as well as other peripherals when needed.

**Per-Domain Behavior (PDB)** An externally observable edge-to-edge functional and performance quality of service behavior on a per-domain basis. See quality of service.

**Per-Hop Behavior (PHB)** An externally observable forwarding behavior applied at a Differentiated Services (DS)-compliant node to a DS behavior aggregate based on the Differentiated Services Code Point marking in the packet. [RFC 2475] See *differentiated services code point*, *DS*.

**Pixel (Picture Element)** Converts the input light image to an electronic signal. The smallest discrete picture element that can be transmitted using the video or still image coding algorithms. A pixel is similar to grains in a photograph or dots in a halftone. Each pixel can represent a number of different shades or colors, depending on how many bits are allocated for it.

**Point-to-Point VTC** A two-party video teleconference. See *VTC*.

**Policing** The process of discarding packets (by a dropper) within a traffic stream in accordance with the state of a corresponding meter enforcing a traffic profile. [RFC 2475]

**Port** A point of access where signals may be inserted or extracted into or out of a device, such as a conferencing terminal unit or multipoint control unit. See *conferencing terminal unit*, *multipoint control unit*.

**Precedence** The designation assigned to a message by the originator to indicate its relative level of importance of the message up to the originator's maximum authorization level as defined by DoD requirements documents. See *FLASH/FLASH OVERRIDE user*, *IMMEDIATE/PRIORITY user*.

**Precedence-Based Assured Service (PBAS)** This service implies that, in general, quality of service requirements of a higher precedence class will be met at the expense of a lower precedence class if the network conditions do not allow meeting quality of service requirements of all service classes. See *assured service*, *precedence*, *quality of service*, *service class*.

**Precedence-Based Treatment** The process of allocating network resources to the higher precedence messages more favorably while restricting lower precedence traffic during periods of resource shortage. See *message*, *precedence*.

**Precedence Inversion** The phenomenon that occurs when a higher precedence flow or flow aggregate does not receive its quality of service commitments, while a lower precedence flow or flow aggregate competing for the same communications source does receive its quality of service commitments. See *flow*, *precedence*, *quality of service*.

**Precondition** "A precondition is a set of constraints about the session that are introduced in the offer. The recipient of the offer generates an answer, but does not alert the user or otherwise proceed with session establishment. That only occurs when the preconditions are met. This can be known through a local event (such as a confirmation of a resource reservation), or through a new offer sent by the caller." [RFC 3312]

**Preemptable Circuit** A circuit that is active with or reserved for a multilevel precedence and preemption call: (a) within the same domain as the preempting call and (b) with a lower precedence than the preempting call. A busy or reserved circuit for which a precedence level has not been specified is not a preemptable circuit. See *multilevel precedence and preemption*, *precedence*.

**Preemption Initiating Exchange** An exchange that is congested (i.e., no idle circuits) and has received a preempting call setup.

**Preferred Elastic** A specially created service class category to meet unique DoD application requirements; it has varying degrees of service class categories. Examples include short, interactive transactions and delay-sensitive file transfers. See *service class*.

**Presence/Awareness** A status indicator that conveys ability and willingness of a potential user to communicate. A user's client provides presence information (presence state) via network connection to a presence service, which is stored in what constitutes the user's personal availability record (called a *presentity*) and can be made available for distribution to other users (called *watchers*) to convey the user's availability for communication. Presence information has wide application in many communication services and is one of the innovations driving the popularity of instant messaging (IM) or recent implementations of voice over IP clients.

A user client may publish a presence state to indicate its current communication status. This published state informs others that wish to contact the user of the user's availability and willingness to communicate. The most common use of presence is to display a status indicator icon on IM clients, and a list of corresponding text descriptions of each of the states. Even when technically not the same, the "on-hook" or "off-hook" state of a called telephone is an analogy; the caller receives a distinctive tone indicating unavailability ("line busy") or availability ("ring-back tone" followed by voice mail). See *availability*, *IM*.

**Primary Rate Interface (PRI)** A high-speed ISDN service, consisting of 23 B-channels (30 in Europe) and one D-channel.

**Private Branch Exchange (PBX) Line** A line appearance at the local switching system that permits connection to a customer premise switching system. The connecting facility may be 1- or 2-way, and it may be loop start or ground start. A PBX line is like an individual line except for ringback, power cross test, and permanent signal treatment.

**Private Branch Exchange (PBX) Type 1 (PBX1)** A PBX with multilevel precedence and preemption capabilities. Based on mission requirements, this switch may serve those non-IMMEDIATE/PRIORITY (I/P) users defined as DoD users having a military mission that might receive I/P calls for orders or direction at precedence levels above a ROUTINE precedence, even though they do not have a I/P mission for issuing guidance or orders. FLASH and FLASH OVERRIDE users are unauthorized to be served by a PBX1 and must connect to an End Office Switch or a Small End Office Switch. See *end office*, *FLASH/FLASH OVERRIDE user*, *IMMEDIATE/PRIORITY user*, *non-IMMEDIATE/PRIORITY user*, *multilevel precedence and preemption*, *small end office*.

**Private Branch Exchange (PBX) Type 2 (PBX2)** A PBX with no multilevel precedence and preemption capabilities. This switch can serve only DoD, non-DoD, non-governmental, and foreign government users having no missions or communications requirement to ever originate or receive IMMEDIATE/PRIORITY (I/P) communications under existing military scenarios.

These users are provided access to the Defense Switched Network (DSN) for the economic or policy benefits of the DoD, when it is not in conflict with local Public Telephone and Telegraph ordinances. During a crisis or contingency, they may be denied access to the DSN. The I/P, FLASH, and FLASH OVERRIDE users are unauthorized to be served by a PBX2. See *DSN*, *end office*, *FLASH/FLASH OVERRIDE user*, *IMMEDIATE/PRIORITY user*, *multilevel precedence and preemption*, *small end office*.

**Propagation Delay** Travel time of an electromagnetic signal from one measurement point to another.

**Proprietary End Instrument (PEI)** A user appliance that interacts with the serving appliance (i.e., local session controller, Multifunction Softswitch, or Wide Area Network Softswitch), using a proprietary protocol to originate, accept, and/or terminate a voice, video, or data session(s). See appliance, *local session controller*, *Multifunction Softswitch*, *Wide Area Network Softswitch*.

**Proprietary IP Trunk (PIPT)** A virtual network element that provides a virtual IP trunk connection between a pair of certified switches (e.g., Deployable Voice Exchange (DVX) to DVX, DVX to Private Branch Exchange (PBX) Type 1, DVX to PBX Type 2). The PIPT may use proprietary signaling but must support the equivalent features and functions of a Primary Rate Interface, multilevel precedence and preemption (MLPP) (T1.619a), or non-MLPP (NI 1/2), as appropriate. See *DVX*, *MLPP*, *PBX1*, *PBX2*, *virtual network element*.

**Protection** A preplanned alternate path for the service. See *path*.

**Proxy Server** "An intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. A proxy server primarily plays the role of routing, which means its job is to ensure that a request is sent to another entity "closer" to the targeted user. Proxies are also useful for enforcing policy (for example, making sure a user is allowed to make a call). A proxy interprets, and, if necessary, rewrites specific parts of a request message before forwarding it." [RFC 3261]

***p*x64** In video teleconferencing, pertaining to a family of ITU-T Recommendations, where *p* is a non-zero positive integer indicating the number of 64 kilobits per second channels. These recommendations form the basis for video telecommunications interoperability. *(NOTE: The p × 64 family includes ITU-T Recommendations H.261, H.221, H.242, H.230, and H.320.)* See *video teleconferencing*.

## Q

**Quality of Service (QoS)** The capability to provide resource assurance and service differentiation in a network. Used with the local area network to provide different priority to traffic flows or sessions, or guarantee a certain level of performance to a traffic flow or session in accordance with requests from the application program. Quality of service is used in conjunction with traffic tagging to guarantee that prioritized traffic flows or sessions are given preferential treatment.

Also, the collective effects of service performances that determine the degree of satisfaction of a *user* of the *service*. See *flows*, *sessions*.

**Quality of Service Domain** An administrative network domain that is designed based on a single quality of service architecture and operated under the same set of quality of service policies. See *quality of service*.

**Quality of Service Network** A quality of service aware or enabled network; it consists of one or more interconnected quality of service domains. See *quality of service*, *quality of service domain*.

**Quarter Common Intermediate Format (QCIF)** A video format defined in ITU-T Recommendation H.261 that is characterized by 176 luminance pixels on each of 144 lines, with half as many chrominance pixels in the horizontal and vertical directions. QCIF has one fourth as many pixels as Full Common Intermediate Format (q.v.). See *chrominance*, *Full Common Intermediate Format*, *luminance*, *pixel*,

**Queuing Delay** Waiting time of a packet for its turn to be serviced at the interface of a network device, such as a router.

## R

**Real Time** At the same time, simultaneously. An event where two or more people communicate simultaneously, similar to the way people speak on a telephone at the same time. Any event that occurs in real time indicates that the event is happening, as we would see it, in actual time. Recording video in real time would require at least 30 frames per second. If the user defines or initiates an event and the event occurs instantaneously, the computer is said to be operating in real time. Real-time support is especially important for multimedia applications.

**Real Time Protocol (RTP)** As defined in IETF RFC 1889, a transport protocol for real-time applications. Real Time Protocol is designed to provide end-to-end network transport functions for applications transmitting real-time data, such as audio, video, or simulation data, over

multicast or unicast network services. Real Time Protocol provides services such as payload type identification, sequence numbering, timestamping, and delivery monitoring to real-time applications. Real Time Protocol is used by all the Voice over Internet Protocol and H.323 signaling protocols. See *multicasting*, *unicasting*.

**Real Time Control Protocol (RTCP)** As defined in IETF RFC 1889, the Real Time Transport Control Protocol (RTP control protocol or RTCP) is based on the periodic transmission of control packets to all participants in the session, using the same distribution mechanism as the data packets.

**Real Time Streaming Protocol (RTSP)** An open, standards-based protocol for multimedia streaming. The Real Time Streaming Protocol enables the controlled delivery of real-time data, such as audio and video. Sources of data can include both live data feeds, live audio and video, and stored content. The Real Time Streaming Protocol is designed to work with established protocols, such as Real Time Protocol (RTP) and HyperText Transfer Protocol. The Real Time Streaming Protocol provides an extensible framework to enable controlled, on-demand delivery of real-time data, such as audio and video. The Real Time Streaming Protocol is intended to control multiple data delivery sessions, provide a means for choosing delivery channels such as User Datagram Protocol (UDP), multicast UDP, and Transmission Control Protocol (TCP), and provide a means for choosing delivery mechanisms based on RTP. See *RTP*.

**Reconfigurable Optical Add Drop Multiplexer (ROADM)** Optical terminal equipment capable of terminating up to 80 channels in both directions. It performs wavelength add and drop functions, as well as allowing wavelengths to pass through.

**Reliability** The ability of a system and its parts to perform its mission without failure, degradation, or demand on the support system. See *Mean Time between Failures (MTBF)* and Mean Time Between Maintenance (MTBM).

**Release to Pivot (RTP)** A network routing capability that consists of a collection of call setup procedures that provides flexibility to a Tandem Switch/Multifunction Switch/End Office-type switch to determine conditions for either forwarding a call or releasing it back to a previous switch in the call path. The RTP is a network capability that is invoked in support of service or business needs, and not invoked directly by an end user. After an operator services switch has determined a new destination for the call, the RTP network capability permits an operator services switch to have the connection established from the originating switch. The basic capability allows any switch to indicate to switches farther forward in the call path that it has the ability to pivot the call. Then an application that determines the new destination for the call (in this case, the operator services switch) can release the call with a Redirection Number parameter containing the address of the new destination. The Pivot switch (in this case, the originating switch) will not terminate the call on receipt of the Release message, but will pass the call forward toward the new destination. The result is that the Release switch, which determined the

new destination, saves an incoming and an outgoing trunk relative to the case where the call is forwarded to the new destination. See *End Office*, *Multifunction Switch*.

**Required Requirement [Required]** A requirement is required if it must be met in the initial operational capability (IOC). The IOC is associated with the fiscal year 2008 timeframe. An IOC requirement is often labeled a Threshold requirement to differentiate the requirement from an Objective requirement.

**Reservationless** A conferencing service that allows you to initiate a conference 24 hours a day, 7 days a week, without the need to make a reservation or rely on an operator. A Meet-Me conference that does not require advance reservations. See *Meet-Me conferencing*.

**Resolution** A measurement of the number of pixels in the horizontal and vertical directions. For example, the resolution of Full Common Intermediate Format is 352 X 288 meaning that it contains 352 pixels in each horizontal row and 288 rows of pixels in the vertical direction for a total of 101,376 pixels. See *Full Common Intermediate Format*, *pixel*.

**Resource Reservation Protocol (RSVP)** A protocol developed by the Internet Engineering Task Force for hosts (applications) and routers to communicate service requirements to the network and to enable the routers in the network to set up the reservations. See *router*.

**Response Time** Round-trip delay from a network application source through destination, back to the application source.

**Restoration** The switching of the service to an alternate path after a failure. See *path*.

**Round Trip Time (RTT)** The RTT is the time required to send a signal from point A to point B and back to point A over a particular end-to-end communication path. Networks with both high bandwidth and a high RTT can have a very large amount of unacknowledged data "in flight" at any given time, known as the bandwidth-delay product. Such networks require special protocol design considerations, such as larger packet receive buffers for high input/output streaming protocol sessions. See *path*.

**Route Code** A special purpose Defense Switched Network code that permits the customer to inform the switch of special routing or termination requirements. Presently, the route code is used to determine whether a call will use circuit-switched data or voice-grade trunking. The route code may be used to disable echo suppressers and cancellers, and override satellite link control. See *Defense Switched Network*.

**Router** A router is an appliance that is a packet switch that operates at the network layer of the Open Systems Interconnection Protocol model. Routers within the Internet Protocol (IP) Unified Capabilities architecture interconnect networks over local and wide areas, and provide traffic

control and filtering functions when more than one pathway exists between two endpoints on the network. The primary function of routers is to direct IP packets along the most efficient or desired path in a meshed network that consists of redundant paths to a destination. Many routers in the DoD IP Unified Capabilities architecture include local area network switch functions and the distinction between the two types of appliances continues to blur. See *appliance*, *path*.

## S

**Scalability** The degree to which the H.323 standard and products based on that standard can support IP-based conferences containing both small and large numbers of participants. Typically, for large numbers of participants, most would be in a receive-only mode, listening to one or a small group (panel) of talkers.

**Secure Communications Interoperability Protocol (SCIP) over Internet Protocol (IP)** The transport of SCIP information over an IP network. The SCIP traffic can be transmitted over an IP network in many ways, but currently, the U.S. Government requires SCIP devices to support transmission of SCIP on IP networks via V.150.1 Modem Relay.

**Secure Cryptographic Processes** Secure cryptographic processes constitute the basic requirement for effective data security and effective data protection in the use of information technology. The basic requirements include digital signatures, authentication and access control, and encryption.

**Secure End Instrument (SEI)** An end instrument that is able to operate in the normal real time services (RTS) mode and in a secure (typically type 1 encryption) mode. See *AS-SIP*, *end instrument*, *local session controller*.

**Secure Telephone Equipment (STE)** This term refers to both a DoD Secure Communications Device (DSCD) and a mode of operation. It is a DSCD that uses any one of the multiple supported protocols to conduct a secure session with another compatible protocol device. See *DSCD*, *FNBDT/SCIP*, *STU*.

**Secure Voice over IP (SVoIP)** Provides Type 1 encrypted communications end to end. Security (encryption for confidentiality) is provided at the Application layer using Secure Communication Interoperability Protocol (SCIP) (formerly known as Future Narrow Band Digital Terminal (FNBDT)) devices. The encryption is typically Type 1; however, SCIP/FNBDT devices can use other crypto methods and libraries, such as Advanced Encryption Standard. Secure VoIP provides talker-to-listener security and session-unique security levels. It is capable of transitioning through BLACK Public Switch Telephone Network and provides interoperability with legacy service voice systems (Secure Telephone Unit and Secure Telephone Equipment). See *FNBDT/SCIP*, *STU*, *STE*,.

**Secure Voice over Secure IP (SVoSIP)** The use of SVoIP devices on a Voice over Secure Internet Protocol (VoSIP) network that provides the following features:

- Security (confidentiality) is provided at both the application and network layers
- Using Secure High Assurance Internet Protocol Encryptor (HAIPES) + Future Narrow Band Digital Terminal (FNBDT)
- Confidentiality within HAIPES domain (end-to-end on top of system high)
- Independent negotiations can permit interoperability with FNBDT only
- HAIPES only systems

See *FNBDT/SCIP*, *VoSIP*.

**Selective Call Forwarding** A feature that allows customers to have only calls from selected calling parties forwarded.

**Service Class** A set of traffic that requires specific delay, loss, and jitter characteristics from the network for which a consistent and defined per-hop behavior applies. See *jitter*, *per-hop behavior*.

**Service Definition** A standards document that defines the scope of the standardization effort of commercial standards. Service definitions for video teleconferencing have been written by the ANSI T1A1.5 committee, and by ITU-T Study Group 1.

**Service Level Agreement (SLA)** Binding contractual agreement between two parties, Global Information Grid (GIG) networks service provider and GIG users, listing offered services and service-level specifications about the technical parameters of the service requested. An SLA may include traffic conditioning rules. An SLA is often the results of the mission planning process.

**Service Level Commitment (SLC)** A numerical performance value that specifies a commitment made by the provider to the user, in the service level specifications of the service level agreement. See *service level agreement*.

**Service Level Specification (SLS)** A set of quantitative performance metrics that together define the service offered to a traffic stream by a differentiated services domain related to a specific service level agreement. See *differentiated services*, *metric*, *service level agreement*.

**Service Provisioning Policy** A policy that defines how traffic conditioners are configured on differentiated services (DS) boundary nodes and how traffic streams are mapped to DS behavior aggregates to achieve a range of services. [RFC 2475] See *DS*.

**Session** The underlying Assured Services Session Initiation Protocol (AS-SIP) or Proprietary Voice over Internet Protocol (VoIP) session that is processed by the proprietary end instrument/AS-SIP end instrument and the local session controller. The VoIP signaling and media streams in the appliance that support an individual end user's call. See *appliance*, *AS-SIP*, *AS-SIP end instrument*, *local session controller*, *proprietary end instrument*.

**Session Initiation Protocol (SIP)** The SIP is "…an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences." [RFC 3261]

**Session Initiation Protocol (SIP) User Agents** Intelligent Internet Protocol (IP) telephones with SIP software that create and manage a SIP session. See *SIP*.

**Session Initiation Protocol (SIP) Proxy Server** Equivalent to time division multiplexing call processing software that detects call for service ("off-hook"), analyzes address digits received, and based on data contained in translation tables/local subscriber line tables obtains the called telephone addressing information. Then it forwards the session invitation directly to the called telephone if it is located in the same domain, or to another proxy server if the call telephone resides in another domain. See *proxy server*.

**Session Initiation Protocol (SIP) Redirect Server** Equivalent to time division multiplexing routing tables that allow SIP proxy servers to direct SIP session invitations to external domains. The SIP redirect servers may reside in the same hardware as SIP registrar and Internet service provider proxy servers. See *proxy server*, *SIP*.

**Session Initiation Protocol (SIP) Registrar Server** Equivalent to time division multiplexing subscriber line database tables and classmarks for all telephones served directly off or by the local session controller controlling a domain. In SIP messaging, these servers retrieve and send participant's IP addresses and other pertinent information to the SIP proxy server. See *local session controller*, *proxy server*, *SIP*.

**SETUP Message** The SETUP message is sent by the calling user to the network or by the network to the called user to initiate call establishment. Defense Switched Network (DSN) calls shall use the SETUP message specified in American National Standards Institute T1.607. The Channel Identification, Calling Party Number (when available), and Called Party Number are mandatory information elements (IEs). For a multilevel precedence and preemption (MLPP) call

(invoking MLPP feature) on the DSN user-to-network interface, the SETUP message shall include the Precedence Level IE. It shall contain other IEs, such as the Business Group IE for the Community of Interest feature, when such unique DSN features are required and the call identity IE (as defined in International Telecommunication Union (ITU) Recommendation Q.931) for the MLPP feature. The precedence level and MLPP service domain (both contained in the Precedence Level IE), and the Calling Party Number (contained in the Calling Party Number IE) shall be used to mark the circuit (identified in the Channel Identification IE) to be preempted as "reserved" for reuse by the preempting call when the Look-Ahead for Busy option is exercised on the DSN user-to-network interface. See *community of interest*, *DSN*, *MLPP*, *precedence*.

**Seven Digit Dialing** The ability to dial using the seven digits of the switch code and line number to establish either interswitch or intraswitch calls within the same numbering plan area.

**Shaping** The process of delaying packets within a traffic stream to cause it to conform to some defined traffic profile. [RFC 2475]

**Signaled Flow** A flow that requires signaling to determine whether there are sufficient resources to support its quality of service requirements. If the resources do not exist or they cannot be preempted, the flow is blocked from entering the network. See *blocking*, *flow*, *quality of service*.

**Signaling** The process of exchanging information between two or more parties to initiate or terminate a communication session, and for the management and maintenance of the session.

**Signaling Appliance** See *Assured Services Session Initiation Protocol (AS-SIP) Signaling Appliance*.

**Signaling Gateway (SG) Function** A Signaling Gateway function receives or sends switched circuit network native signaling at the edge of a data network. For example, the SG function MAY relay, translate, or terminate Signaling System No. 7 (SS7) signaling in an SS7-Internet Gateway. The SG function MAY also be co-resident with the Media Gateway (MG) function to process switched circuit network signaling associated with line or trunk terminations controlled by the MG, such as the D-channel of an Integrated Services Digital Network (ISDN) Primary Rate Interface trunk. The use of the SG function within the Assured Real Time Services Generic System Requirements refers only to SS7 signaling. The use of the SG within the Assured Services Session Initiation Protocol Generic System Specification allows the SG to be co-resident with the MG. [RFC 2805] See *Assured Services Session Initiation Protocol*, *MG*, *SS7*.

**Single-Pair High-Speed DSL (SHDSL)** SHDSL is a symmetric DSL designed primarily for duplex operation over mixed gauge two-wire twisted metallic pairs. Optional multi-pair operation is supported for extended reach applications. Optional signal regenerators are supported for both single-pair and multi-pair operation SHDSL transceivers are capable of

supporting selected symmetric user data rates in the range of 192 Kbps to 2312 Kbps. Optional extensions allow user data rates up to 5696 Kbps. Loop distances can be from 2.4 to 4 miles.

**Small End Office (SMEO)** "A switch that serves as the primary switch, functions as an EO [End Office], but at smaller DOD [Department of Defense] installations. A SMEO does not have full DSN [Defense Switched Network] Network Traffic Management capabilities. It offers limited performance reporting and may not support SS7 [Signaling System No. 7] signaling. Therefore, SMEOs will not serve installations that are critical to combatant command missions where NM [network management] control and network visibility for situational awareness is required." [CJCSI 6215.01C] See *DSN*, *EO*, *SS7*.

**Softphone** An end-user software application on an approved operating system that enables a general-purpose computer to function as a telephony end instrument. It will be tested on an approved operating system as part of the system under test. The softphone application is considered an IP end instrument and is associated with the IP telephone switch. See *end instrument*, *system under test*.

**Softswitch** A programmable network appliance that:

- Controls connection services for a media gateway and/or native IP endpoints.
- Selects processes and services that can be applied to a call.
- Provides routing for call control within the network based on signaling and customer database information.
- Transfers control of the call to another network element.
- Interfaces to and supports management functions such as provisioning, fault, and billing.
- Ability to control the access of sessions within and external to its domain. [International Softswitch Consortium]

See *appliance*, *call control*, *media gateway*, *network element*, *session*.

**STEP** An acronym for Standardized Tactical Entry Point.

**Still Image** Non-moving visual information such as graphs, drawings, pictures, or video frames not processed by the video codec portion of the conferencing terminal unit. See *codec*, *conferencing terminal unit*.

**Strong Authentication** The process of authenticating a user based on at least two of three factors: something you know (i.e., username and password), something you have (i.e., token device), and something you are (i.e., fingerprints).

**Sub Quarter Common Intermediate Format (SQCIF)** A video format defined in ITU-T Recommendation H.263 that is characterized by 128 luminance pixels on each of 96 lines, with half as many chrominance pixels in each direction. SQCIF has half as many pixels as Quarter Common Intermediate Format. See *chrominance*, *luminance*, *pixel*, *Quarter Common Intermediate Format*.

**Subscriber** The owner of a public key contained in a Public Key Infrastructure certificate. A subscriber may be an appliance or a person. See *appliance*.

**Survivability** The capability of a system to survive in a specified threat environment and accomplish its designated mission.

**Synchronization** An arrangement for operating digital switching systems at a common (or uniform) clock rate whereby the data signal is accompanied by a phase-related clock. Improperly synchronized clock rates result in the loss of portions of the bit streams and a concomitant loss of information.

**System** An appliance or group of appliances. The systems described in this document include Multifunction Softswitches, Softswitches, local session controllers, Media Gateways, border controllers, end instruments, local area network switches, and routers. See *appliance*, *end instrument*, *local session controller*, *Media Gateway*, *Multifunction Softswitch*, *router*, *softswitch*.

**System Under Test (SUT)** The inclusive components required to test a Unified Capabilities product for Approved Products List certification. Examples of a SUT include time division multiplexing or circuit-switch components, Voice over Internet Protocol system components (e.g., local session controller and gateway), local area network components (e.g., routers and Ethernet switches), and end instruments. See *Approved Products List*, *end instrument*, *local session controller*, *router*.

## T

**Tactical Network Element (T-NE)** A T-NE is any network element used in the Tactical network. A T-NE can be used for long local, encapsulated time division multiplexing, and proprietary Internet Protocol trunks. See *network element*.

**Tandem Call Trace** A feature that identifies the incoming trunk of a tandem call to a specified office directory number. The feature is activated by entering the specified distant office

directory number for a tandem call trace. A printout of the incoming trunk number and terminating directory number, and the time and date is generated for every call to the specified directory number.

**Telebroadcast** Transmitted video or audio data that is viewed (or listened to) in real time, i.e., as the information is received. Streaming media may be user-controlled (as in on-demand, pay-per-view content) or server-controlled (as in webcasting).

**Telecom Switch/Device** Hardware or software designed to send and receive voice, data, or video signals across a network that provides customer voice, data, or video equipment access to the Defense Switched Network or public switch telecommunications network. See *Defense Switched Network*,

**Teleconferencing** A conference among people remote from one another who are linked by one or more telecommunications devices.

**Teleconferencing System** A collection of equipment and integral components (customer premises equipment and facilities) required to process teleconferencing programs and control data, less network interface devices.

**TEMPEST-approved** See *TEMPEST* in FED-STD-1037C. A device endorsed by the National Security Agency as meeting stringent signal radiation requirements. The electromagnetic waves it emits have been reduced through shielding or other techniques to a point where it would be extremely difficult for a hostile force to gather information from the electromagnetic waves and disclose the classified information being transmitted. See *classified*.

**Ten-Digit Dialing** The ability to use ten digits comprising the area code, switch code, and line number to establish interswitch calls where the number plan area of the calling party is different from the number plan area of the called party.

**Terminal Equipment** A device or devices connected to a network or other communications system used to receive or transmit data. It usually includes some type of input/output device.

**Terminal ID** A form of identification that allows a conferencing terminal unit to be assigned an alphanumeric string such as a name or location rather than just an arbitrary terminal number. See *conferencing terminal unit*.

**Terminal Number** A number assigned by an multipoint control unit to a conferencing terminal unit (CTU) for identifying CTUs in a conference. Terminal numbering is necessary for call association, chair control, and video select capabilities. See *chair control*, *CTU*, *multipoint control unit*.

**Terminating Internet Protocol (IP)/Time Division Multiplexing (TDM) Signaling Gateway Function** The function related to receiving an Assured Services Session Initiation Protocol (AS-SIP) INVITE from the IP network and sending an Initial Address Message (IAM) onto the Signaling System No. 7 network. If the AS-SIP INVITE included an encapsulated Integrated Services Digital Network (ISDN) User Part (ISUP) IAM, then it is decapsulated—identical to Incoming Interworking Unit in International Telecommunications Union – Telecommunication Standardization Sector (ITU-T) Recommendation Q.1912.5, Interworking between Session Initiation Protocol and Bearer Independent Call Control Protocol or ISUP. See *AS-SIP*, *Session Initiation Protocol*, *SS7*.

**Terminating Gateway** Assured Services Session Initiation Protocol (AS-SIP) for Telephones signaling appliance performing the terminating Internet Protocol (IP)/Time Division Multiplexing (TDM) Signaling Gateway function in the case of TDM bridging call flows and IP-to-TDM call flows, and either directly serving the destination IP end instruments (EIs) or the AS-SIP signaling appliances representing the destination IP EIs in the case of TDM-to-IP call flows. See *AS-SIP*, *AS-SIP signaling appliance*, *EI*, *flow*, *Signaling Gateway function*.

**Three-Way Calling** A feature that allows a station in the talking state to add a third party to the call without operator assistance.

**Throughput** The number of octets is transmitted successfully (Internet Protocol) during the measurement interval (typically seconds). Assumes the packets sent do not exceed the capacity of the link. [GESP]

**TIA (Telecommunications Industry Association)** (http://www.tiaonline.org) A U.S. commercial standards organization aligned with the Electronic Industries Association (EIA). The acronym TIA/EIA precedes a numerical designation, such as TIA/EIA-232-F, that replaces the now obsolete RS (Recommended Standard) designation, for example, RS-232. See *EIA*.

**TIA/EIA-232-F (formerly RS-232)** A serial interface standard for transmission of unbalanced signals between a variety of computer, media, and multimedia peripherals. TIA/EIA-232-F transmits at a maximum of 19.2 kilobits per second for up to a distance of about 50 feet and uses a type D-subminiature 25-pin (DB-25) connector, though other connectors have been used.

**TIA/EIA-422 (formerly RS-422)** A serial electrical interface standard for transmission of balanced and unbalanced signals between a variety of higher end computer, media, and multimedia peripherals. TIA/EIA-422 allows a maximum data rate of 10 megabits per second at a distance of 40 feet.

**TIA/EIA-423 (formerly RS-423)** A serial electrical interface standard for transmission of unbalanced signals between a variety of higher end computer, media, and multimedia

peripherals. TIA/EIA-423 allows a maximum data rate of 100 kilobits per second at a distance of 30 feet.

**TIA/EIA-530** A replacement for EIA-449 that uses a DB-25 connector instead of a 37-pin connector, while keeping the critical EIA-449 signals intact. TIA/EIA-530 is to be used in conjunction with TIA/EIA-422-B. See *EIA-449*.

**Tracing of Terminating Calls** A feature that identifies the calling number on intraoffice calls or the incoming trunk on incoming calls for calls terminating to a specified directory number. When this feature is activated, a printout of the originating directory number or incoming trunk number, terminating directory number, and the time and date is generated for every call to the specified line.

**Trace Call in Progress** A feature that identifies the originating directory number or incoming trunk for a call in progress. The feature is activated by authorized personnel entering a request that includes the specific terminating directory number or trunk involved in the call.

**Traffic Classification** A mechanism that allows the networks to distinguish among different categories of traffic, connection requests, and provisioning requests. The classification may be performed at the Edge and Core nodes during packet transport, as well as through indications in the control and management planes for setting up connections and provisioning. Classification can be based on fields in the packets and/or indications in control and management messages.

**Traffic Conditioner** An entity that performs traffic conditioning functions and may contain meters, markers, droppers, and shapers. Typically, traffic conditioners are deployed in differentiated services boundary nodes only. A traffic conditioner may re-mark a traffic stream or may discard or shape packets to alter the temporal characteristics of the stream and bring it into compliance with a traffic profile. [RFC 2475] See *DS*.

**Traffic Conditioning** Control functions performed to enforce traffic classification rules and may include traffic metering, marking, shaping, and policing. Traffic conditioning, when used, will be tied to the parameters chosen for the offered load control. See *metering*, *policing*, *shaping*.

**Traffic Conditioning Agreement (TCA)** An agreement specifying classifier rules and any corresponding traffic profiles and metering, marking, discarding, and/or shaping rules that are to apply to the traffic streams selected by the classifier. A TCA encompasses all traffic conditioning rules explicitly specified within a service level agreement along with all the rules implicit from the relevant service requirements and/or from a differentiated services domain's service provisioning policy. [RFC 2475] See *classifier*, *differentiated services*, *metering*, *shaping*, *service level agreement*.

**Traffic Engineering** An operator or automaton with the express purpose of minimizing congestion in a network. It encompasses the application of technology and scientific principles to the measurement, modeling, characterization, and control of Internet traffic, and the application of such knowledge and techniques to achieve specific performance objectives. [RFC 2702]

**Transcoding** Provides the ability of converting a media stream from one format to another. Transcoding is often used to convert video/audio formats (i.e., H.261 to H.263, G.711 to G.722) to allow conference participants to communicate with each other even though their video endpoints are equipped with different encoding/decoding capabilities.

**Trunks** Time division multiplexing links used by a circuit switch system to connect to or interconnect Defense Switched Network switches. See *Defense Switched Network*, *link*, *system*.

**Trust Point** Public keys (or certificates containing them) that the relying party designates as reliable and trustworthy. The relying party should obtain the public keys (or certificates) through a reliable out-of-band method. Trust points are usually Root Certificates. Under certain circumstances, a relying party may decide to trust an intermediate Certificate Authority (CA) or even an end entity. Trust is transitive. If the relying party trusts a CA, it also trusts other CAs to which the CA delegates its CA responsibilities. This is also known as a trust anchor.

**Turnkey** Pertaining to a procurement process that (1) includes contractual actions at least through the system, subsystem, or equipment installation phase, and (2) may include follow-on contractual actions, such as testing, training, logistical, and operational support. (188)

NOTE: Precise definition of the types of allowable contractual features are contained in the Federal Acquisition Regulations (FAR).

**Type 1** A classified or controlled cryptographic equipment, assembly, component, or item endorsed by the National Security Agency for securing telecommunications and automated information systems for the protection of classified or sensitive U.S. Government information exempted by the Warner Amendment for use by the U.S. Government and its contractors, and subject to restrictions in accordance with the International Traffic in Arms Regulation. See *Warner Amendment*.

**Type 2** An unclassified cryptographic equipment, assembly, component, or item endorsed by the National Security Agency for use in telecommunications and automated information systems for the protection of unclassified but sensitive information. Type 2 equipment is exempted by the Warner Amendment. Type 2 is available to U.S. Government departments, agencies, sponsored elements of state and local government, sponsored U.S. Government contractors, and sponsored private sector entities. It is subject to restrictions in accordance with the International Traffic in Arms Regulation. See *Warner Amendment*.

**Type 3** An unclassified cryptographic equipment, assembly, component, or item that implements an unclassified algorithm registered with the National Institute of Standards and Technology as a Federal Information Processing Standard for use in protecting unclassified sensitive, or commercial, information. This definition does not include Warner-Amendment-exempt equipment. See *Warner Amendment*, Warner-exempt.

## U

**Unclassified** Information or material that does not require protection in the interests of national security and that is not classified for such purposes by appropriate classifying authority in accordance with the provisions of Executive Order 12356, "National Security information," of April 2, 1982.

**Unclassified Sensitive** A designation for information that is not classified, but needs to be protected from unauthorized disclosure. Examples of types of information that fall under this category are For Official Use Only (FOUO), proprietary, contractor sensitive, limited distribution, and personal in nature.

**Unicasting** The process of transmitting data/information from one source to many destinations using multiple point-to-point transmissions. See *broadcasting*, *multicasting*.

**Unified Capabilities (UC)** The seamless integration of voice, video, and data services delivered ubiquitously across a secure and highly available network independent of technology infrastructure to provide increased mission effectiveness to the warfighter and business communities. Unified capabilities integrate standards-based communication and collaboration services including, but not limited to, the following:

- Messaging
- Voice, video, and web conferencing
- Unified communication and collaboration applications or clients

These standards-based UC services are integrated with available enterprise applications, both business and warfighting. See *conferencing*.

**User Agent Client (UAC)** "A user agent client is a logical entity that creates a new request, and then uses the client transaction state machinery to send it. The role of UAC lasts only for the duration of that transaction. In other words, if a piece of software initiates a request, it acts as a UAC for the duration of that transaction. If it receives a request later, it assumes the role of a user agent server for the processing of that transaction." [RFC 3261] See *entity*, *user agent server*.

**User Agent Server (UAS)** "A user agent server is a logical entity that generates a response to a SIP request. The response accepts, rejects, or redirects the request. This role lasts only for the duration of that transaction. In other words, if a piece of software responds to a request, it acts as a UAS for the duration of that transaction. If it generates a request later, it assumes the role of a user agent client for the processing of that transaction." [RFC 3261] See *entity*, *user agent client*.

## V

**Very High Speed DSL (VDSL)** VDSL is a DSL technology that permits the transmission of asymmetric and symmetric aggregate data rates up to tens of Mbps on twisted pairs. The maximum downstream rate is about 52 Mbps over lines up to 1,000 feet (300 meters) in length. The maximum upstream rate is 16 Mbps for lines up to 1,000 feet in length.

**Very High Speed DSL 2 (VDSL2)** VDSL2 is an access technology that exploits the existing infrastructure of copper wires that were originally deployed for POTS services. It can be deployed from central offices, from fiber-fed cabinets located near the customer premises, or within buildings. VDSL2 is an enhancement to VDSL that supports asymmetric and symmetric transmission at a bidirectional net data rate up to 200 Mbps on twisted pair wiring. Loop distances can be up to 8,200 feet.

**Video** That portion of a signal that is related to moving images.

**Video codec** See *codec*.

**Videoconferencing** See *video teleconferencing*.

**Video Mixing** The process of combining two or more video signals to produce a single composite frame (video image). This allows each participant in a conference to view more than one of the other participants in the conference simultaneously. For example, the composite video image may be a two-by-two array in which the video from four participants appears in four blocks within the array (i.e., Hollywood Squares (See *continuous presence*)). This is contrasted with the method of mixing signals in the analog domain using a video quad splitter. This is also contrasted with windowing that uses multiple frames to display images from different sources, such as data, motion video, or graphics. See *frame*.

**Video Server** A server that distributes video images on demand.

**Video Switching** The process of switching the video signal that a participant sees to one of the other participants. The participant that is seen can be determined by the chairperson, the participants, or as a function of the audio signal. See *Voice Activated Switching*.

**Video Teleconferencing (VTC)** Two-way electronic form of communications that permits two or more people in different locations to engage in face-to-face audio and visual communication. Meetings, seminars, and conferences are conducted as if all the participants are in the same room. Video teleconferencing provides the capability to exchange and distribute combinations of voice, video, imagery, messages, files, and streams.

**Video Teleconferencing Unit (VTU)** Video teleconferencing endpoint equipment that performs the following functions: coding/decoding of audio and video; multiplexing of video, audio, data, and control signals; system control; and end-to-end signaling. It may include input/output functions, embedded cryptographic functions, network interface functions, end-to-network signaling, and connections to networks. See *video teleconferencing*.

**Video Telephony** Relating to videophones and video teleconferencing.
**Virtual Network Element (VT-NE**) A VT-NE is any network element integrated into a certified Defense Switched Network switch. A VT-NE can be used for long local, encapsulated time division multiplexing, and proprietary Internet Protocol trunks. See *Defense Switched Network*, *long local*.

**Voice Activated Switching** The function of a multipoint control unit that determines which video signal is seen by the participants in a conference based on the audio signal. Typically, the loudest speaker will be seen by all the participants. See *multipoint control unit*.

**Voice over IP (VoIP) System** A set of components required to provide Defense Switched Network (DSN) Internet Protocol (IP) voice services from end instrument to DSN trunk, or IP phone to IP phone. The VoIP system includes, but is not limited to, the IP telephony instrument, the local area network, the local session controller, and the IP gateway. See *DSN*, *end instrument*, *local session controller*.

**Voice over Secure Internet Protocol (VoSIP)** The instantiation of Internet Protocol (IP) Telephony on a classified local area network or wide area network infrastructure that provides the routing of voice conversations using the Secure Internet Protocol Router Network (SIPRNet) as the transport medium. The use of the SIPRNet allows users in secure environments to communicate at the Secret level without the need for specialized phones or the use of key material. Bidirectional interoperability with the Defense Red Switch Network is provided through the Defense Information Systems Agency-managed IP-to-Time Division Multiplexing interfaces.

**Voiceband Data (VBD) (Modem Pass-Through)** A subset of Modem over Internet Protocol in which modem signals are transmitted over the voice channel of a packet network. See *Modem over Internet Protocol*.

## W

**Warner Amendment** Title 10, United States Code, Section 2315, "Law inapplicable to the procurement of automatic data processing equipment and services for certain defense purposes." Enacted as Public Law 97-86, 1 December 1981. The Warner Amendment amends Section 111 of the Federal Property and Administrative Services Act of automatic data processing equipment (currently defined to include telecommunications services and equipment) if the function, operation, or use of the equipment or services:

- Involves intelligence activities.
- Involves cryptologic activities related to national security.
- Involves the command and control of military forces.
- Involves equipment that is an integral part of a weapon or weapons system.
- Subject to (6) is critical to the direct fulfillment of military or intelligence missions.
- Subpart (5) does not include procurement of automatic data processing equipment or services to be used for routine administrative and business applications, including payroll, finance, logistics, and personnel management applications.

**Warner-exempt** A telecommunications requirement that meets the stipulations as stated in the Warner Amendment. See *Warner Amendment*.

**Web-Scheduled Conferences** These conferences have a guaranteed time slot on a conference bridge for the number of participants, date, and time that you select. You reserve this time slot in advance by using an online scheduling interface.

**Wide Area Network (WAN) Level Assured Services Admission Control (W-ASAC)** The processes on a Multifunction Softswitch or Assured Real Time Services Softswitch that ensure that quality of service requirements of a higher precedence service will be met at the expense of a lower precedence service if the WAN conditions do not allow meeting quality of service requirements of all services. The processes are associated typically with the preemption of lower

precedence sessions within the WAN to ensure that higher precedence sessions can be completed. In addition, the W-ASAC ensures that its subtended local session controllers remain within their traffic-engineered real time service allocations. See *ASAC*, *local session controller*, *Multifunction Softswitch*, *precedence*, *quality of service*.

**Wide Area Network Softswitch (WAN SS)** A stand-alone Approved Products List product that acts as an Assured Services Session Initiation Protocol Back-to-Back User Agent within the Unified Capabilities (UC) architecture. It provides the equivalent functionality of a commercial SS and has similar functionality to the SS component of a Multifunction Softswitch (MFSS). The functionality of the Local Session Controller (LSC) is a conditional requirement and the support of a Signaling Gateway is not required. The inclusion of the product in the UC architecture allows the functionality of an MFSS to be achieved by interconnecting two separate appliances (Multifunction Switch and WAN SS), possibly provided by different vendors. The creation of a WAN SS provides Government flexibility in the rollout of UC Voice and Video over Internet Protocol (IP) capabilities and eases the migration of time-division multiplexing technology-based services to IP technology-based services. See *Approved Products List*, *Assured Services Session Initiation Protocol*, *Back-to-Back User Agent*, *LSC*, *Multifunction Switch*, *MFSS*, *SS*.

**Wideband Audio** In audio transmission, an audio signal of a wider bandwidth than 3 kilohertz (KHz) (nominal), or a carrier channel or system supporting that signal. *(NOTE: G.722 specifies a bandwidth of 7 KHz.)*

**Wireless** Can refer to either 802.x devices or cellular telephones (see Section 5.3.1.6.2, Operational Changes, for more details).

**Wireless Device** An 802.x device or cellular phone.

**Wireless Access Bridge (WAB)** A device that connects two local area network segments together via wireless transmission.

**Wireless End Instrument (WEI)** A Defense Switched Network IMMEDIATE/PRIORITY (I/P) or non-I/P user device that receives voice service via an IP telephone instrument using wireless technologies, such as 802.11 or 802.16. Also known as a wireless telephony subscriber. See *Defense Switched Network*, *IMMEDIATE/PRIORITY user*, *non-IMMEDIATE/PRIORITY user*.

**Wireless Local Area Network (LAN) (WLAN)** Generic term used to describe the use of wireless technologies in the LAN. The WLAN includes all the wireless terminology (i.e., wireless access bridge, wireless end instrument, and wireless LAN access system). See *wireless access bridge*, *wireless end instrument*, and *wireless LAN access system*.

**Wireless Local Area Network (LAN) Access System (WLAS)** An implementation of wireless technologies considered to be the replacement of the physical layer of the wired Access Layer of a LAN. See *LAN Access Layer*.

# SECTION A3
# ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| 1xRTT | One Times Radio Transmission Technology |
| 10 GbE | 10 Gigabit Ethernet |
| 16CIF | 16 Common Intermediate Format |
| 16FCIF | 16 Full Common Intermediate Format |
| 2W | Two-Wire |
| 2G | Second Generation Wireless Telephone Technology |
| 2.5G | 2.5 Generation Wireless Telephone Technology |
| 24/7 | 24-Hours, 7 Days A Week |
| 3G | Third Generation |
| 3GPP | Third Generation Partnership Project |
| 3GSM | Third Global System for Mobile |
| 4CIF | 4 Common Intermediate Format |
| 4G | Fourth Generation |
| | |
| A/V | Audio/Visual |
| AAA | Authentication, Authorization, and Accounting |
| AAdmin | Audit Administrator |
| AAF | Army Air Field |
| AAG | Access Aggregation Function |
| AAL5 | ATM Adaptation Layer 5 |
| ac | Alternating Current |
| ACC | Automatic Congestion Control |
| ACD | Attendant/Call Director |
| ACD | Automatic Call Distribution |
| ACD | Automatic Call Distributor |
| ACL | Access Control List |
| ACM | Address Complete Message |
| ACTA | Administrative Council for Terminal Attachments |
| ADIMSS | Advanced DSN Integrated Management Support System |
| ADM | Add-Drop Multiplexer |
| ADN | Area Distribution Node |
| ADSL | Asymmetric DSL |
| AEI | AS-SIP End Instrument |
| AES | Advanced Encryption Standard |
| AES-256 | Advanced Encryption Standard 256 |
| AES-CCMP | Advanced Encryption Standard – Counter with Cipher Block Chaining – Message Authentication Code Protocol |
| AF | Assured Forwarding |

| | |
|---|---|
| AF3 | Class 3 Assured Forwarding |
| AF4 | Class 4 Assured Forwarding |
| AFB | Air Force Base |
| AG | Access Gateway |
| AG | Access Gateway |
| AGF | Access Grooming Function |
| AGF | Aggregate Grooming Function (Sec. 5.3.5) |
| AGW | Access Gateway |
| AH | Authentication Header |
| AHWG | Ad Hoc Working Group |
| AIA | Authority Information Access |
| AIS | Alarm Indication Signal |
| AIS | Automated Information System |
| AIS-CI | Alarm Indication Signal – Customer Installation |
| a.k.a. | also known as |
| ALI | Automatic Line Identification |
| A-link | Access Link |
| AMA | Automatic Message Accounting |
| AMI | Alternate Mark Inversion |
| AMR | Adaptive Multi-Rate |
| AMSL | Above Mean Sea Level |
| ANAT | Alternative Network Address Type |
| AND | Area Distribution Node |
| ANI | Automatic Number Identification |
| ANM | Answer Message |
| ANS | Answer Message |
| ANSI | American National Standards Institute |
| Ao | Operational Availability |
| AO&M | Administration, Operation, and Maintenance |
| OAM&P | Operations, Administration, Maintenance, and Provisioning |
| AOR | Address of Record |
| AOR | Area of Responsibility |
| API | Application Programming Interface |
| APL | Approved Products List |
| APRI | Address Presentation Restricted Indicator |
| APS | Automatic Protection Switching |
| AR | Aggregated Router |
| AR | Aggregation Router |
| ARD | Automated Receiving Device |
| ARDIMSS | Advanced DRSN Integrated Management Support System |
| ARP | Address Resolution Protocol |
| ARTS | Assured Real Time Services |

| | |
|---|---|
| AS | Application-Specific Maximum |
| AS | Assured Services |
| AS | Autonomous System |
| AS-NE | Assured Services-Network Element |
| ASA | Automatic Security Authentication |
| ASAC | Assured Services Admission Control |
| ASCII | American Standard Code for Information Interchange |
| ASD(NII) | Assistant Secretary of Defense for Networks & Information Integration |
| ASF | Assured Services Features |
| ASLAN | Assured Service Local Area Network |
| ASN.1 | Abstract Syntax Notation One |
| AS-SIP | Assured Services Session Initiation Protocol |
| AS-SIP-T | Assured Services Session Initiation Protocol for Telephones |
| ATA | Analog Terminal Adapter |
| ATB | All Trunk Busy |
| ATC | Authority to Connect |
| ATIS | Alliance for Telecommunications Industry Solution |
| ATM | Asynchronous Transfer Mode |
| ATO | Authority to Operate |
| ATP | Acceptance Test Procedure/Plan |
| ATQA | Attendant Queue Announcement |
| AU-3 | Administrative Unit-3 |
| AU-4 | Administrative Unit-4 |
| AU-4-Xc | Administrative Unit-4-Xc |
| AUC | Authentication Center |
| Auth | Authorization |
| AVCC | Available Link Call Capacity |
| A/V | Audio Video |
| AVP | Audio/Video Profile |
| AVPF | Audio-Visual Profile with Feedback |
| AVSC | Available Link Session Capacity |
| AVT | Audio and Video Transport |
| | |
| B/P/C/S | Base/Post/Camp/Station |
| B2BUA | Back-to-Back User Agent |
| B3ZS | Bipolar 3 Zero Substitution |
| B8ZS | Bipolar with Eight-Zero Substitution |
| BA | Billing Agent |
| BAF | Bellcore AMA Format |
| BASE | Baseband |
| BB | Backbone |

| | |
|---|---|
| BC | Bearer Capability |
| BC | Border Controller |
| BCE | Bridged Call Exclusion |
| BCI | Backwards Call Indicator |
| BCP | Best Current Practice |
| BCP | Bridge Control Protocol |
| BE | Block Error |
| BE | Best Effort |
| BEHAVE | Behavior Engineering for Hindrance Avoidance |
| BER | Basic Encoding Rules |
| BER | Bit Error Rate |
| BERT | Bit Error Rate Tester |
| BFCP | Binary Floor Control Protocol |
| BG | Business Group |
| BGMP | Border Gateway Multicast Protocol |
| BGP | Border Gateway Protocol |
| BGP-4 | Border Gateway Protocol 4 |
| BICC | Bearer-Independent Call Control |
| BITS | Building Integrated Timing Supply |
| BLSR | Bidirectional Line Switched Ring |
| BLV | Busy Line Verification |
| BNEA | Busy Not Equipped Announcement |
| BNF | Backus-Naur Form |
| BoD | Bandwidth on Demand |
| BOOTP | Bootstrap Protocol |
| BPV | Bipolar Violation |
| BPA | Blocked Precedence Announcement |
| BPON | Broadband Passive Optical Network |
| BPP | BitsPerPictureMaxKb |
| bps | Bits per Second |
| BRAC | Base Realignment and Closure |
| BRDB | Backup Routing Database |
| BRI | Basic Rate Interface |
| BSA | Base Station Antenna |
| BSC | Base Station Controller |
| BSR | Bootstrap Router |
| BSS | Base Station Subsystem |
| BT | BASE-T |
| BTS | Base Transceiver Station |
| BW | Bandwidth |
| | |
| C | Conditional |

| | |
|---|---|
| C&A | Certification and Accreditation |
| C-PE | Classified Customer Edge Router |
| C/P/S | Camp, Post, or Station |
| C/RD | Confidential/Restricted Distribution |
| C2 | Command and Control |
| C4 | Command, Control, Communications, and Computers |
| CA | Call Appearance |
| CA | Certificate/Certification Authority |
| CA 1 | Call Appearance 1 |
| CA 2 | Call Appearance 2 |
| CAA | Certification Approval Authority |
| CAC | Call Admission Control |
| CAC | Common Access Card |
| CAdmin | Cryptographic Administrator |
| CAG | Channel Access Grooming |
| CAL | Confidential Access Level |
| CALEA | Communications Assistance to Law Enforcement Act |
| CAN | Campus Area Network |
| CANF | Cancel From |
| CANT | Cancel To |
| CAP | Common Alerting Protocol |
| CAS | Channel-Associated Signaling |
| CAT | Category |
| CAT5 | Category 5 |
| CB-WFQ | Class-Based Weighted Fair Queuing |
| CC | Common Criteria |
| CC | Country Code |
| CC/S/A | Combatant Commander/Service/Agency |
| CCA | Call Connection Agent |
| CCA | Call Control Agent |
| CCAT | Continuous Concatenation |
| CCB | Configuration Control Board |
| CCITT | International Telegraph and Telephone Consultative Committee (now ITU-T) |
| CCM | Codex Control Message |
| CCM | Configuration Control and Management |
| CCMP | Counter with Cipher Block Chaining-Message Authentication Code Protocol |
| CCS | Common Channel Signaling |
| CCS7 | Common Channel Signaling System No. 7 |
| CDMA | Code Division Multiple Access |
| CDMA2000 | Code Division Multiple Access 2000 |

| | |
|---|---|
| CDMI | Cloud Data Management Interface |
| CDP | CRL Distribution Point |
| CdPN | Called Party Number |
| CDR | Call Detail Recording |
| CDR | Call Detail Record |
| CE | Customer Edge |
| CE | Connection Endpoint |
| CE Router | Customer Edge Router |
| CEE | Converged Enhanced Ethernet |
| CE-R | Customer Edge Router |
| CER | Customer Edge Router |
| CERT | Computer Emergency Response Team |
| CES | Circuit Emulation Service |
| CF | Call Forwarding |
| CFB | Call Forwarding Busy |
| CFBL | Call Forwarding Busy Line |
| CFDA | Call Forwarding – Don't Answer |
| CFI | Canonical Format Indicator |
| CFR | Code of Federal Regulations |
| CFV | Call Forwarding Variable |
| CGA | Carrier Group Alarm |
| CGB | Circuit Group Blocking Message |
| CgPA | Calling Party Address |
| CgPN | Calling Party Number |
| ChN | Charge Number |
| CI | Customer Installation |
| CIC | Circuit Identification Code |
| CID | Craft Input Device |
| CIDR | Classless Inter-Domain Routing |
| CIF | Common Intermediate Format |
| CIFS | Common Internet File System |
| CIFSv1.0 | Common Internet File System Version 1.0 |
| CIFSv2.0 | Common Internet File System Version 2.0 |
| CIO | Chief Information Officer |
| CIR | Committed Information Rate |
| CJCS | Chairman of the Joint Chiefs of Staff |
| CJCSI | Chairman of the Joint Chiefs of Staff Instruction |
| CJCSM | Chairman of the Joint Chiefs of Staff Manual |
| Ckt | Circuit |
| CLAN | Converged Local Area Network |
| CLI | Calling Line Identification |
| CLI | Command Line Interface |

| | |
|---|---|
| CLID | Calling Line Identifier |
| CM | Call Menu |
| CM | Configuration Management |
| CM | Countermeasure |
| CM | Cryptographic Modernization |
| CMD | Circuit Mode Data |
| CMI | Cryptographic Modernization Initiative |
| CN | Congestion Notification |
| CNA | Converged Network Adapter |
| CND | Calling Number Delivery |
| CNDSP | Computer Network Defense Service Provider |
| CNSS | Committee on National Security Systems |
| CNT | Count |
| CO | Central Office |
| COCOM | Combatant Commander |
| codec | Coder/Decoder |
| COI | Community of Interest |
| COIN | Community of Interest Network |
| COMSEC | Communications Security |
| CON | Connect |
| CONOPS | Concept of Operations |
| CONUS | Continental United States |
| COOP | Continuity of Operations Planning |
| COPS | Common Open Policy Service |
| COR | Carrier Operated Relay |
| CORBA | Common Object Request Broker Architecture |
| COS | Carrier Operated Switch |
| CoS | Class of Service |
| COS | Class of Service |
| COT | Continuity Testing |
| COT | Customer Originated Trace |
| COTS | Commercial Off-the-Shelf |
| CPC | Calling Party Category |
| CPCF | Custom Picture Clock Frequency |
| C-PE | Classified Provider Edge |
| CPE | Customer Premises Equipment |
| CPG | Call Progress Message |
| CPN | Calling Party Number |
| CPS | Calls Per Second |
| CPSG | Call Park Subscriber Group |
| CPT | Cryptographic Products Testing |
| CPU | Central Processing Unit |

| | |
|---|---|
| CQ | Custom Queuing |
| CR | Conditionally Required |
| CR | Customer Router |
| CRC | Cyclic Redundancy Check |
| CRD | Capabilities Requirements Document |
| CRL | Certificate Revocation List |
| CS | Circuit-Switched |
| CS | Class Selector |
| CSeq | Command Sequence |
| CSPF | Constrained Shortest Path First |
| CS-PSTN | Circuit-Switched Public Switched Telephone Network |
| C-SS | Classified Softswitch |
| CSU | Channel Service Unit |
| CTCP | Compound TCP |
| CTI | Computer Telephony Integration |
| CTL | Certificate Trust List |
| CTU | Conferencing Terminal Unit |
| CUC | Classified Unified Capabilities |
| CUG | Closed User Group |
| CUI | Controlled Unclassified Information |
| CV | Code Violation |
| CVSD | Continuously Variable Slope Delta |
| CVVoIP | Classified Voice and Video over IP |
| CW | Call Waiting |
| CY | Calendar Year |
| CYBERCOM | U.S. Cyber Command |
| | |
| DA | Destination Address |
| DAA | Designated Accrediting/Approval Authority |
| DAC | Discretionary Access Control |
| DAD | Duplicate Address Detection |
| DAM | Diagnostic Acceptability Measure |
| DAMA | Demand Assigned Multiple Access |
| DASAC | Dynamic Assured Services Admission Control |
| DATMS | DISN Asynchronous Transfer Mode Services |
| dB | Decibel |
| DB | Database |
| DBA | Database Administrator |
| DBMS | Database Management System |
| dc | Direct Current |
| DCA | Defense Communications Agency |
| DCB | Data Center Bridging |

| | |
|---|---|
| DCBX | Data Center Bridging Exchange Protocol |
| DCC | Data Communications Channel |
| DCCC | DISN Customer Call Center |
| DCE | Data Circuit-Terminating Equipment |
| DCE | Data Communication Equipment |
| DCID | Director of Central Intelligence Directive |
| DCN | Data Communications Network |
| DCO | Defense Connect Online |
| DCP | Designated Called Party |
| DCS | Defense Collaboration Service |
| DCS-1800 | Digital Cellular System 1800 MHz |
| DCVX | Deployed Cellular Voice Exchange |
| D-D | Deployable-to-Deployable |
| DEMUX | Demultiplexer |
| DF | Default |
| DFSU | Dual Frequency Signaling Unit |
| DHCP | Dynamic Host Configuration Protocol |
| DIA | Defense Intelligence Agency |
| DIACAP | Defense Information Assurance Certification and Accreditation Process |
| DIAM | Defense Intelligence Agency Manual |
| DiffServ | Differentiated Services |
| DISA | Defense Information Systems Agency |
| DISN | Defense Information System Network |
| DISR | DoD Information Technology Standards Registry |
| DIT | Directory Information Tree |
| DITO | DISA Ipv6 Transition Office |
| DLAN | Deployable LAN |
| DLC | Digital Loop Carrier |
| DLoS | Direct Line of Sight |
| DLSC | Deployed Local Session Controller |
| DMS | Defense Message System |
| DMSC | Deployed Mobile Switching Center |
| DMVPN | Dynamic Multipoint Virtual Private Network |
| DEMUX | Demultiplexer |
| DMZ | Demilitarized Zone |
| DN | Directory Number |
| DNA | Defense Nuclear Agency |
| D-NE | Deployed Network Element |
| DNIS | Dialed Number Identification Service |
| DNS | Domain Naming System |
| DoD | Department of Defense |

| | |
|---|---|
| DODAF | Department of Defense Architecture Framework |
| DoDD | DoD Directive |
| DoDI | DoD Instruction |
| DOIM | Director of Information Management |
| DoS | Denial of Service |
| DOTS | "DISN Overarching Technical Strategy" |
| DP | Dial Pulse |
| DPC | Destination Point Code |
| DQ | Database Query |
| DR | Disaster Recovery |
| DRSN | Defense Red Switch Network |
| DRT | Diagnostic Rhyme Test |
| DS | Differentiated Services |
| DS | Digital Signal |
| DS Field | Differentiated Services Field |
| DS0 | Digital Signal Level 0 |
| DS1 | Digital Signal Level 1 |
| DS3 | Digital Signal Level 3 |
| DS12 | Digital Signal Level 12 |
| DSAWG | DISN Security Accreditation Working Group |
| DSC | Data Storage Controller |
| DSCD | DoD Secure Communications Device |
| DSCP | Differentiated Services Code Point |
| DSCS | Defense Satellite Communications System |
| DSL | Digital Subscriber Line |
| DSLAM | DSL Access Multiplexer |
| DSMCU | Dual-Signaling Multipoint Control Unit |
| DSN | Defense Switched Network |
| DSP | Digital Signal Processing |
| DSS | DISN Subscription Service |
| DSS1 | Digital Subscriber Signaling System No. 1 |
| DSSS | Dual-Signaling Softswitch |
| DSU | Digital Service Unit |
| DTE | Data Terminating Equipment |
| DTEP | "DISN Technology Evolution Plan" |
| DTLS | Datagram Transport Layer Security |
| DTM | Delegated Trust Model |
| DTMF | Dual-Tone Multifrequency |
| DTR | Desktop Review |
| DTR | Deployable Tactical Radio |
| DTU | Digital Test Unit |
| DVS | DISN Video Services |

| | |
|---|---|
| DVS-G | DISN Video Services – Global |
| DVS II | DISN Video Services II |
| DVX | Deployable Voice Exchange |
| DVX-C | Deployable Voice Exchange – COTS |
| DVX-L | Deployable Voice Exchange – Legacy |
| DWDM | Dense Wave Division Multiplex |
| | |
| E&M | Ear and Mouth |
| E2E | End-to-End |
| E911 | Enhanced Emergency Service |
| EA | Enterprise Architecture |
| EAL4 | Evaluated Assurance Level 4 |
| EAP | Extensible Authentication Protocol |
| EAP-TLS | Extensible Authentication Protocol- Transport Layer Security |
| EA-TJTN | Executive Agent for Theater Joint Tactical Networks |
| EBC | Edge Boundary Controller |
| EBER | Excessive Bit Error Rate |
| eBGP | External Border Control Protocol |
| EC | Echo Canceller |
| EC | European Community |
| ECAR-1 | Enclave and Computing Environment Audit Record Content-1 |
| ECAR-2 | Enclave and Computing Environment Audit Record Content-2 |
| ECAR-3 | Enclave and Computing Environment Audit Record Content-3 |
| ECN | Explicit Congestion Notification |
| ECTP-1 | Enclave and Computing Environment Audit Trail Protection-1 |
| ECU | End Cryptographic Unit |
| EDC | Electronic Dispersion Compensation |
| EF | Expedited Forwarding |
| EF&I | Engineer, Furnish, and Install |
| EI | End Instrument |
| EIA | Electronics Industries Alliance |
| EICC | End Instrument Call Capacity |
| EIR | Equipment Identity Register |
| EISC | End Instrument Session Capacity |
| EFM | Ethernet in the First Mile |
| EFMCu | Ethernet in the First Mile over Copper |
| EKTS | Electronic Key Telephone System |
| ELIN | Emergency Location Identfication Number |
| E-LSP | EXP-Inferred LSP |
| EMC | Electromagnetic Compatibility |
| EMI | Electromagnetic Interference |
| eMLPP | Enhanced Multilevel Precedence and Preemption |

| | |
|---|---|
| EMPT | Electromagnetic Pulse Testing |
| EMS | Element Management System |
| EMSS | Enhanced Mobile Satellite Systems |
| ENUM | Electronic Numbering |
| EO | End Office |
| EOL | End of Life |
| EPON | Ethernet Passive Optical Network |
| ertPS | Extended Real-Time Polling Service |
| ERL | Emergency Response Location |
| ES | Errored Seconds |
| ESCON | Enterprise Systems Connection |
| ESD | Electrostatic Discharge |
| ESF | Extended Superframe |
| eLSR | Edge Label Switch Router |
| ESONET | Enhanced Synchronous Optical Network |
| ESP | Encapsulating Security Payload |
| ESP | Essential Service Protection |
| ET | End Terminal |
| ETN | Enterprise Telecommunications Network |
| ETS | Electronic Tandem Switching |
| ETS | Enhanced Transmission Selection |
| ETSI | European Telecommunications Standards Institute |
| EUB | End User Building |
| EVDO | Evolution-Data Optimized |
| EV-DO | Evolution-Data Optimized |
| EWSE | Enterprise-Wide Systems Engineering |
| EXP | Experimental |
| | |
| F | Factor |
| F | FLASH |
| FAS | Facility Associated Signaling |
| fax | Facsimile |
| FBI | Federal Bureau of Investigation |
| FC | Fibre Channel |
| FCAPS | Fault, Configuration, Accounting, Performance, and Security |
| FCC | Federal Communications Commission |
| FCI | Forward Call Indicators |
| FCIP | Full Common Intermediate Format |
| FCoE | Fibre Channel over Ethernet |
| FCP | Fibre Channel Protocol |
| F-D | Fixed-to-Deployable |
| FDCC | Federal Desktop Core Configuration |

| | |
|---|---|
| FDL | Facility Data Link |
| FDM | Frequency-Division Multiplexing |
| FE | Fast Ethernet |
| FEAC | Far-End Alarm and Control |
| FEBE | Far-End Block Error |
| FEC | Forward Equivalence Class |
| FEC | Forward Error Correction |
| FECC | Far-End Camera Control |
| FED-STD | Federal Standard |
| FEOOF | Far-End Out of Frame |
| F-F | Fixed-to-Fixed |
| FFR | Fast Failure Recovery |
| FIB | Forwarding Information Base |
| FICON | Fiber Connectivity |
| FIFO | First-In First-Out |
| FIPS | Federal Information Processing Standard |
| FIR | Full Intra Request |
| FISMA | Federal Information Security Management Act |
| FNBDT | Future Narrowband Digital Terminal |
| F-NE | Fixed Network Element |
| FNPA | Foreign Numbering Plan Area |
| FO | FLASH OVERRIDE |
| FOC | Final Operational Capability |
| FoIP | Facsimile over Internet Protocol |
| FOO | FLASH OVERRIDE OVERRIDE |
| FOUO | For Official Use Only |
| FQDN | Fully Qualified Domain Name |
| FRR | Fast Reroute |
| FSAL | Fixed Security Access Level |
| FSD | Feature Service Description |
| FSD | Feature Specific Document |
| FSDP | Fibre Service Delivery Point |
| FSO | Field Security Office |
| ft | Foot |
| FT | Fast Track |
| F-T | Fixed-to-Tactical |
| FTP | File Transfer Protocol |
| FTPS | File Transfer Protocol Secure |
| FTR | Federal Telecommunications Recommendation |
| FTS | Federal Technology Service |
| FTS 2001 | Federal Telecommunications System 2001 |
| FW | Firewall |

| | |
|---|---|
| FX | Foreign Exchange |
| FY | Fiscal Year |
| | |
| G3 | Group 3 |
| G3 Fax | Group 3 Facsimile |
| GAP | Generic Address Parameters |
| GBNP | Global Block Numbering Plan |
| Gbps | Gigabits per Second |
| GCCS-J | Global Command and Control Systems-Joint |
| GCIRD | Generic Cryptographic Interoperability Requirements Document |
| GDS | Global Directory Service |
| GE | Gigabit Ethernet |
| GEI | Generic End Instrument |
| GEM | GIG Enterprise Management |
| GESP | GIG Enterprise Service Profile |
| GETS | Government Emergency Telecommunications Service |
| GFP | Generic Framing Procedure |
| GHz | Gigahertz |
| GIG | Global Information Grid |
| GIG 2.0 | Global Information Grid 2.0 |
| GIG-BE | Global Information Grid – Bandwidth Expansion |
| GK | Gatekeeper |
| GLS | Global Location Server |
| GMPLS | Generalized Multiprotocol Label Switching |
| GMT | Greenwich Mean Time |
| GNOSC | Global Network Operations and Security Center |
| GNS | Global Name Space |
| GNSC | Global Network Support Center |
| GOS | Grade of Service |
| GOTS | Government Off-the-Shelf |
| GPON | Gigabit Passive Optical Network |
| GPRS | General Pocket Radio System |
| GPS | Global Positioning System |
| GR | Generic Requirement |
| GR | Graceful Restart |
| GRE | Generic Routing Encapsulation |
| GRS | Circuit Group Reset Message |
| GSA | General Services Administration |
| GSM | Global System for Mobile |
| GSR | Generic System Requirement |
| GSTP | Generic Switching Test Plan |
| GUI | Graphical User Interface |

| | |
|---|---|
| GW | Gateway |
| | |
| HAIPE | High Assurance Internet Protocol Encryptor |
| HBA | Host Bus Adapter |
| HBSS | Host-Based Security System |
| HDLC | High-Level Data Link Control |
| HDSL | High Bit Rate DSL |
| HEMP | High-Altitude Electromagnetic Pulse |
| HEX | Hexadecimal |
| HF | High Frequency |
| HLC | High Layer Compatibility |
| HLR | Home Location Register |
| hr | Hour |
| HR | Hybrid Routing |
| HRD | Hypothetical Reference Decoder |
| HSPD | Homeland Security Presidential Directive |
| HTTP | HyperText Transfer Protocol |
| HTTPS | HyperText Transfer Protocol, Secure |
| Hz | Hertz |
| | |
| I | IMMEDIATE |
| I3MP | Installation Information Infrastructure Modernization Program |
| I&A | Identification and Authentication |
| I/P | IMMEDIATE/PRIORITY |
| IA | Information Assurance |
| IAC | Industry Advisory Council |
| IAD | Integrated Access Device |
| IAM | Initial Address Message |
| IANA | Internet Assigned Numbers Authority |
| IAO | Information Assurance Officer |
| IAS | Integrated Access Switch/System |
| IASRD | Information Assurance Security Requirements Document |
| IAT | Information Assurance Tools |
| IATC | Interim Authority to Connect |
| IATO | Interim Authority to Operate |
| IATP | Information Assurance Test Plan |
| IATT | Information Assurance Test Team |
| IATT | Interim Authority to Test |
| IAVA | Information Assurance Vulnerability Alert |
| IAVM | Information Assurance Vulnerability Management |
| IAW | In Accordance With |
| iBGP | Internal Border Control Protocol |

| | |
|---|---|
| IC | Interexchange Carrier |
| ICA | Isolated Code Announcement |
| ICCS | Intra-Cluster Communication Signaling |
| ICD | Initial Capabilities Document |
| ICE | Interactive Connectivity Establishment |
| ICMP | Internet Control Message Protocol |
| ICMPv6 | Internet Control Message Protocol for IPv6 |
| ID | Identification |
| IDLC | Integrated Digital Loop Carrier |
| IDNX | Integrated Digital Network Exchange |
| IDP | Integrated Data Protection |
| IDR | Instantaneous Decoder Refresh |
| IDR | Inter-Domain Routing |
| IDS | Intrusion Detection System |
| IDT | Integrated Digital Terminal |
| Ie | Equipment Impairment Factor |
| IE | Information Element |
| IE | Information Enterprise |
| IEC | International Electrotechnical Commission |
| IEEE | Institute of Electrical and Electronics Engineers, Inc. |
| IETF | Internet Engineering Task Force |
| IGMP | Internet Group Management Protocol |
| IGMPv3 | Internet Group Management Protocol, Version 3 |
| II | Information Integrity |
| I-IWU | Incoming Interworking Unit |
| IKE | Internet Key Exchange |
| IKEv1 | Internet Key Exchange Version 1 |
| IKEv2 | Internet Key Exchange Version 2 |
| ILMI | Integrated Local Management Interface |
| IM | Instant Messaging |
| IMAP | Internet Message Access Protocol |
| IMUX | Inverse Multiplexer |
| INE | In-Line Network Encryptor |
| INFOSEC | Information Security |
| INMS | Integrated Network Management System |
| Intserv | Integrated Services |
| I/O | Input/Output |
| IO | Interoperability |
| IOC | Initial Operational Capability |
| IP | Internet Protocol |
| IPDV | IP Packet Delay Variation |
| IPLR | IP Packet Loss Ratio |

| | |
|---|---|
| ipm | Impulses Per Minute |
| IPS | Intrusion Protection System |
| IPSec | Internet Protocol Security |
| IPSEC | Internet Protocol Security |
| IPSG | Internet Protocol Signaling Gateway |
| IPT | Integrated Product Team |
| IPTD | IP Packet Transfer Delay |
| IPv4 | Internet Protocol Version 4 |
| IPv6 | Internet Protocol Version 6 |
| IR | Intermediate Reach |
| IS | Information Security |
| IS | Information System |
| IS | Information Systems |
| IS | Intermediate System |
| IS | Interoperability Specification |
| ISAKMP | Internet Security Association and Key Management Protocol |
| iSCSI | Internet Small Computer System Interface |
| ISDN | Integrated Services Digital Network |
| IS-IS | Intermediate System to Intermediate System |
| iSNS | Internet Storage Name Service |
| ISO | International Standardization Organization |
| ISP | Information Support Plan |
| ISP | Internet Service Provider |
| ISS | Integrated Security Solution |
| ISSU | In-Service Software Upgrades |
| IST | Interswitch Trunk |
| ISUP | ISDN User Part |
| IT | Information Technology |
| ITU | International Telecommunications Union |
| ITU-T | International Telecommunications Union – Telecommunication Standardization Sector |
| IUA | ISDN User Adaptation |
| IVR | Interactive Voice Response |
| IWF | Interworking Function |
| IWU | Interworking Unit |
| I-x | Intraoffice (Interface) |
| | |
| J2EE | Java 2 Platform, Enterprise Edition |
| JC2 | Joint Command and Control |
| JCIDS | Joint Capabilities Integration and Development System |
| JEDS | Joint Enterprise Directory Services |
| JIC | Joint Interoperability Certification |

| | |
|---|---|
| JID | Jabber Identifier (XML IM Technology) |
| JIDS | Joint Intrusion Detection System |
| JIP | Jurisdiction Information Parameter |
| JITC | Joint Interoperability Test Command |
| JM | Joint Menu |
| JNO | Joint Net-Centric Operations |
| JNN | Joint Network Node |
| JROC | Joint Requirements Oversight Council |
| JROCM | Joint Requirements Oversight Council Memorandum |
| JS | Joint Staff |
| JSCMWG | Joint Services Cryptographic Modernization Working Group |
| JTF | Joint Task Force |
| JTF-GNO | Joint Task Force – Global Network Operations |
| JTRS | Joint Tactical Radio System |
| JTTP | Joint Tactics, Techniques, and Procedures |
| JWICS | Joint Worldwide Intelligence Communications System |
| | |
| kb/s | Kilobits per Second |
| kbit/s | Kilobits per Second |
| kbps | Kilobits per Second |
| Kbps | Kilobytes per Second |
| KEYMAT | Keying Material |
| kHz | Kilohertz |
| Km | Kilometer |
| KMI | Key Management Infrastructure |
| | |
| L2 | OSI Layer 2 |
| L3 | OSI Layer 3 |
| L2VPN | Layer 2 Virtual Private Network |
| L3VPN | Layer 3 Virtual Private Network |
| LAN | Local Area Network |
| L-ASAC | LSC Level Assured Services Admission Control |
| LATA | Local Access and Transport Area |
| LBO | Line Buildout |
| LCAS | Link Capacity Adjustment Scheme |
| LCD | Liquid Crystal Display |
| LDAP | Lightweight Directory Access Protocol |
| LDAPv3 | Lightweight Directory Access Protocol, Version 3 |
| LDIF | LDAP Interchange Format |
| LDP | Label Distribution Protocol |
| LE | Link Encryptor |
| LEF | Link Encryptor Family |

| | |
|---|---|
| LER | Label Edge Router |
| LFB | Look-Ahead for Busy |
| LLC | Logical Link Control (Sublayer) |
| LLDP | Link Layer Discovery Protocol |
| LLS | Local Location Server |
| LLS | Local Location Service |
| L-LSP | Label-Only-Inferred LSP |
| LMR | Land Mobile Radios |
| LNP | Local Number Portability |
| LNP | Local Network Protection |
| L-n.x | Long-Haul (Interface) |
| LOC | Letter of Compliance |
| LOC2 | Loss of Command and Control |
| LOF | Loss of Frame |
| LOP | Loss of Pointer |
| LR | Long Reach |
| LRDB | Local Routing Database |
| LRN | Local Routing Number |
| LS | LAN Switch |
| LSC | Local Session Controller |
| LSP | Label-Switched Path |
| LSR | Label Switch Router |
| LSR | Label-Switching Router |
| LSSGR | LATA Switching Systems Generic Requirements |
| LSSU | Link Status Signaling Unit |
| LUN | Logical Unit |
| | |
| m | Meter |
| M&S | Modeling and Simulation |
| M/SM | Mesh/Semi-Mesh |
| M13 | Multiplexer |
| M2PA | MTP2 User Peer-to-Peer Adaptation |
| M2UA | MTP2 User Adaptation |
| M3UA | MTP3 User Adaptation |
| MA ICD | Mission Area Initial Capabilities Document |
| MA | Mission Area |
| MAC | Media Access Control |
| MAC | Message Authentication Code |
| MAN | Metropolitan Area Network |
| Mbps | Megabits per Second |
| MBSS | Multifunction Mobile Device Backend Support System |
| MC | Multipoint Controller |

| | |
|---|---|
| MCEB | Military Communications-Electronics Board |
| MCEP | Multicarrier Entry Point |
| MCN | Main Communication Node |
| MCS | Mobile Cellular Systems |
| MCU | Multipoint Conferencing Unit |
| MCU | Multipoint Control Unit |
| MDR | Maximum Deployment Range |
| MDT | Mean Downtime |
| MEGACO | Media Gateway Control |
| MELPe | Enhanced Mixed Excitation Linear Production |
| MER | Minimum Essential Requirements |
| MF | Multifrequency |
| MF(R1) | Multifrequency (R1) |
| MFS | Multifunction Switch |
| MFSS | Multifunction Softswitch |
| MG | Media Gateway |
| MGC | Media Gateway Controller |
| MGCP | Media Gateway Control Protocol |
| MHP | Mobile Host Protocol |
| MHz | Megahertz |
| mi | Mile |
| MIB | Management Information Base |
| MIB II | Management Information Base II |
| MIDCOM | Middlebox Communication |
| MILDEP | Military Department |
| MILSATCOM | Military Satellite Communication |
| MIME | Multipurpose Internet Mail Extension |
| MIV | Multipoint Indication Visualization |
| MKI | Master Key Identifier |
| MLD | Multicast Listener Discovery |
| MLDv2 | Multicast Listener Discovery Version 2 |
| MLPP | Multilevel Precedence and Preemption |
| MLPPP | Multilink Point-to-Point Protocol |
| MLS | Multilevel Security |
| MLSC | Master Local Session Controller |
| MMF | Multi-Mode Fiber |
| MNWS | Mass Notification Warning System |
| MoIP | Modem over Internet Protocol |
| MOP | Maintenance Operations Protocol |
| MOR | Maximum Operational Range |
| MOS | Mean Opinion Score |
| MP | Multilink Protocol |

| | |
|---|---|
| MP3 | MPEG 1 and 2 Layer III Audio |
| MPBGP | Multi-Protocol Border Gateway Protocol |
| MPEG | Motion Picture Experts Group |
| MPI | Minimum Picture Interval |
| MPLS | Multiprotocol Label Switching |
| MPLS-TE | Multiprotocol Label Switching – Traffic Engineered |
| MPT | Maximum Possible Throughput |
| MRDB | Master Routing Database |
| MRP | Modem Relay Preferred |
| ms | Microsecond |
| MS | Multiplex Section |
| MSDP | Multicast Source Discovery Protocol |
| msec | Milliseconds |
| MSO | Mobile Switching Office |
| MSPP | Multi-Service Provisioning Platforms |
| MSS | Maximum Segment Size |
| MSU | Message Signal Unit |
| MTBF | Mean Time between Failures |
| MTBM | Mean Time between Maintenance |
| MTIE | Maximum Time Interval Error |
| MTOSI | Multi-Technology Operations System(s) Interface |
| MTP | Message Transfer Part |
| MTP1 | Message Transfer Part 1 |
| MTP2 | Message Transfer Part 2 |
| MTP3 | Message Transfer Part 3 |
| MTR | Maximum Transmission Range |
| MTTR | Mean Time to Repair |
| MTU | Maximum Transmission Unit |
| MU | Message Unit |
| MUF | Military Unique Features |
| MUX | Multiplexer |
| MVI | Multivendor Interoperable |
| MWR | Morale, Welfare, and Recreation |
| | |
| N/A | Not Applicable |
| NA/SS | Network Appliances and Simple Servers |
| NAC | Network Access Controller |
| NALU | Network Abstraction Layer Unit |
| NAPT | Network Address Port Translation |
| NAS | Network Access Server |
| NAS | Network Attached Storage |
| NAT | Network Address Translation |

| | |
|---|---|
| NATO | North American Treaty Organization |
| NBT | NetBIOS over TCP/IP |
| NCES | Net-Centric Enterprise Services |
| NCI | Network Component Infrastructure |
| NCM | Network Cluster Member |
| NCP | Network Cutover Plan |
| NCTAMS | Naval Computer and Telecommunications Area Master Station |
| NE | Near End |
| NE | Network Element |
| NEBS | Network Equipment-Building System |
| NEBS-3 | Network Equipment Building System 3 |
| NEMO | Network Mobility |
| NENA | National Emergency Number Association |
| NetOps | Network Operations |
| NETOPS | Network Operations |
| NEXT | Near End Crosstalk |
| NFAS | Non-Facility Associated Signaling |
| NFS | Network File System |
| NFSv3 | Network File System Version 3 |
| NFSv4 | Network File System Version 4 |
| NFSv4.1 | Network File System Version 4.1 |
| NI | Network Identifier |
| NI-1/2 | National ISDN 1/2 |
| NI-1 | National ISDN 1 |
| NI-2 | National ISDN 2 |
| NI-3 | National ISDN 3 |
| NIAP | National Information Assurance Partnership |
| NIC | Network Interface Card |
| NIPR | Unclassified but Sensitive Internet Protocol |
| NIPRNet | Unclassified but Sensitive Internet Protocol Router Network |
| NIPRNET | Unclassified but Sensitive Internet Protocol Router Network |
| NIS | Network Information Service |
| NISP | Network Infrastructure Products |
| NIST | National Institute of Standards and Technology |
| NLAS | No Loss of Active Sessions |
| NM | Network Management |
| NMCC | National Military Command Center |
| NMS | Network Management System |
| NOA | Nature of Address |
| NOC | Network Operations Center |
| NOSC | Network Operations and Security Center |
| NP | Network Provided |

| | |
|---|---|
| NP | Not Permitted |
| NP | Number Portability |
| NPA | Numbering Plan Area |
| npdi | Number Portability Database Dip Indicator |
| NR-KPP | Net-Ready Key Performance Parameter |
| NRT | Near Real Time |
| nrtPS | Non-Real-Time Polling Service |
| ns | Nanosecond |
| NSA | National Security Agency |
| NSI | National Security Information |
| NSS | National Security Systems |
| NSS | National Security Space (Sec. 5.3.5) |
| NSTISS | National Security Telecommunications and Information Systems Security |
| NSTISSAM | National Security Telecommunications and Information Systems Security Advisory Memorandum |
| NSTISSI | National Security Telecommunications and Information Systems Security Instruction |
| NSTISSP | National Security Telecommunications and Information Systems Security Policy |
| NT1 | Network Termination 1 |
| NT2 | Network Termination 2 |
| NTM | Network Traffic Management |
| NTMOS | Network Traffic Management Operating System |
| NTP | Network Time Protocol |
| NTSWG | National Telecommunications Security Working Group |
| | |
| O&M | Operations and Maintenance |
| OA | Optical Amplifier |
| OADM | Optical Add Drop Multiplexer |
| OAN | Operational Area Network |
| OA&M | Operations, Administration, and Maintenance |
| OC-1 | Optical Carrier Level 1 |
| OC-3 | Optical Carrier Level 3 |
| OC-3c | Optical Carrier Level 3c |
| OC-12 | Optical Carrier Level 12 |
| OC-12c | Optical Carrier Level 12c |
| OC-48 | Optical Carrier Level 48 |
| OC-48c | Optical Carrier Level 48c |
| OC-192 | Optical Carrier Level 192 |
| OC-192c | Optical Carrier Level 192c |
| OC-768 | Optical Carrier Level 768 |

| | |
|---|---|
| OCONUS | Outside the Continental United States |
| OCN | Original Called Number |
| OCSP | Online Certificate Status Protocol |
| ODBC | Open Database Connectivity |
| ODXC | Optical Digital Cross-Connect |
| O/E | Optical/Electrical |
| OEO | Optical-to-Electrical-to-Optical |
| OIF | Optical Internetworking Forum |
| O-IWU | Outgoing Interworking Unit |
| OL | Open Loop |
| OLA | Optical Line Amplifier |
| OLT | Optical Line Termination |
| ONT | Optical Network Terminal |
| ONU | Optical Network Units |
| OOB | Out-of-Band |
| OOBM | Out-of-Band-Management |
| OOF | Out of Frame |
| OP | Optical Protection |
| OPC | Originating Point Code |
| OPSEC | Operations Security |
| ORL | Optical Return Loss |
| OS | Operations System |
| OSA | Optical Spectrum Analyzer |
| OSC | On-Line Status Check |
| OSC | Optical Supervisory Channel |
| OSD | Office of the Secretary of Defense |
| OSI | Open Systems Interconnect |
| OSI | Open Systems Interconnection |
| OSNR | Optical Signal to Noise Ratio |
| OSP | Outside Plant |
| OSPF | Open Shortest Path First |
| OSS | Operational Support System |
| OTAR | Over-The-Air-Rekey |
| OTGR | Operations Technology Generic Requirements |
| OTN | Optical Transport Network |
| OTS | Optical Transport System |
| | |
| p | Probability of Blocking |
| P | Permitted |
| P | PRIORITY |
| P | Provider |
| P2P | Point-to-Point |

| | |
|---|---|
| P2N | Point-to-Multipoint |
| PAC | Pacific |
| PALA | Precedence Access Limitation Announcement |
| PAM | Pass Along Message |
| PAS | Priority Access Service |
| PAT | Precedence Access Threshold |
| PAT | Port Address Translation |
| PB | Petabyte |
| PBAS | Precedence-Based Assured Service |
| PBNM | Policy-Based Network Management |
| PBX | Private Branch Exchange |
| PBX1 | Private Branch Exchange 1 |
| PBX2 | Private Branch Exchange 2 |
| PC | Personal Computer |
| PC | Point Code |
| PCD | Precedence Call Diversion |
| PCM | Pulse Code Modulation |
| PCMA | Paired Carrier Multiple Access |
| PCMU | Pulse Code Modulation mu-law |
| PCS | Personal Communications Services |
| PDA | Personal Digital Assistant |
| PDB | Per-Domain Behavior |
| PDH | Plesiochronous Digital Hierarchy |
| PDS | Protected Distribution System |
| PDU | Protocol Data Unit |
| PE | Provider Edge |
| PE Router | Provider Edge Router |
| PEAP | Protected Extensible Authentication Protocol |
| PED | Personal Equipment Device |
| PED | Portable Electronic Device |
| PEI | Proprietary End Instrument |
| PE-R | Provider Edge Router |
| PESQ | Perceptual Evaluation of Speech Quality |
| PFC | Priority-based Flow Control |
| PHB | Per-Hop Behavior |
| PHY | Physical Layer |
| PII | Personally Identifiable Information |
| PIM | Protocol Independent Multicast |
| PIM-SM | Protocol Independent Multicast-Sparse Mode |
| PIN | Personal Identification Number |
| PIPT | Proprietary Internet Protocol Trunk |
| PIV | Personal Identity Verification |

| | |
|---|---|
| PKCS#7 | Public- Key Cryptographic Standard No. 7 |
| PKE | Public Key Enabled |
| PKI | Public Key Infrastructure |
| PL/CA | Precedence Level/Calling Area |
| PLCP | Physical Layer Convergence Protocol |
| PLL | Phase Locked Loop |
| PM | Performance Management |
| PM | Performance Monitoring |
| PMD | Polarization Mode Dispersion |
| PMO | Program Management Office |
| PMT | Performance Measurement Tool |
| PND | Private Networking Domain |
| PO | Program Office |
| POM | Program Objective Memorandum |
| PON | Passive Optical Network |
| POS | Packet over SONET |
| POTS | Plain Old Telephone Service |
| ppm | Parts Per Million |
| PPP | Point-to-Point Protocol |
| pps | Pulses per Second |
| PPS | Packets per Second |
| PQ | Priority Queuing |
| PRA | Primary Rate Access |
| PRI | Primary Rate Interface |
| ps | Poincaré Sphere |
| $ps/Km^{1/2}$ | PMD Coefficient |
| PSAP | Public Safety Answering Point |
| PSDS | Public Switched Digital Service |
| PSIP | Program and System Information Protocol |
| PSQM | Perceptual Speech Quality Measure |
| PSTN | Public Switch Telephone Network |
| PTT | Public Telephone and Telegraph |
| PTT | Push-To-Talk |
| PV | Proprietary VoIP |
| PVN | Private Virtual Network |
| | |
| Q | Quality Factor |
| Q&A | Question and Answer |
| QCIF | Quarter Common Intermediate Format |
| QoR | Query on Release |
| QoS | Quality of Service |

| | |
|---|---|
| R | Required |
| R | Router |
| R | ROUTINE |
| RAC | Resource Availability Confirmation |
| RADIUS | Remote Authentication Dial In User Service |
| RAE | Required Ancillary Equipment |
| RAI | Remote Alarm Indication |
| RAI | Resource Availability Indicator |
| RAI-CI | Remote Alarm Indication – Customer Installation |
| RAID | Redundant Array of Independent Disks |
| RAID-5 | Redundant Array of Independent Disks – 5 |
| RAID-6 | Redundant Array of Independent Disks – 6 |
| RAN | Radio Access Network |
| RAS | Remote Access Service(s) |
| RBAC | Role-Based Access Control |
| RBF | Radio Bridge Function |
| RDI | Remote Defect Indication |
| REI | Radio End Instrument |
| REL | Release Message |
| RES | Resume Message |
| REST | Representational State Transfer |
| RFC | Request for Comment |
| RFI | Remote Failure Indication |
| RG | Radio Gateway |
| RIB | Routing Information Base |
| RJ | Registered Jack |
| RLC | Release Complete Message |
| RLR | Receive Loudness Rating |
| RM | Remote Management |
| RMAS | Remote Memory Administration System |
| RMON | Remote Monitoring |
| RMON2 | Remote Monitoring 2 |
| RMS | Root Mean Square |
| RMUX | Real-Time Multiplexer |
| ROADM | Reconfigurable Optical Add Drop Multiplexer |
| RoE | Rules of Engagement |
| RP | Rendezvous Point |
| RPF | Reverse Path Forwarding |
| RPH | Resource-Priority Header |
| RPOA | Recognized Private Operating Agency (CCITT) |
| RPR | Resilient Packet Ring |
| RR | Reroute |

| | |
|---|---|
| RSA | Rivest, Shamir, & Adleman |
| RSC | Reset Circuit Message |
| RSF | RTS Stateful Firewall |
| RSU | Remote Switching Unit |
| RSVP | Resource Reservation Protocol |
| RSVP-TE | Resource Reservation Protocol-Traffic Engineering |
| RTCP | Real Time Control Protocol |
| RTCP | Real Time Control Protocol Extended Report |
| RTP | Real Time Protocol |
| RTP | Release to Pivot |
| rtPS | Real Time Polling Service |
| RTS | Real Time Services |
| RTS | Routing and Translation Server |
| RTT | Round-Trip Time |
| Rx | Receive |
| | |
| S&U | Secure and Unsecure |
| SA | Security Association |
| SA | Situational Awareness |
| SA | Source Address |
| SAC | Session Admission Control |
| SAD | Security Association Database |
| SAFI | Sub-Address Family Identifier |
| SAL | Security Access Level |
| SAN | Storage Area Network |
| SAN | Storage Array Network |
| S-AR | Secret Aggregation Router |
| SAR | Segmentation and Reassembly |
| SAS | Serial Attached Small Computer Systems Interface |
| SAS | Standalone Switch |
| SASL | Simple Authentication and Security Layer |
| SATA | Serial Advanced Technology Attachment |
| SATCOM | Satellite Communications |
| SBC | Session Border Controller |
| SBSS | Smartphone Backend Support System |
| SBU | Sensitive, But Unclassified |
| SC/A | Signal Converter/Allotter |
| SCCP | Signaling Connection Control Part |
| SCCP | Signaling Connection Control Protocol |
| SCCS | Switching Control Center System |
| S-CE | Secret Customer Edge Router |
| SCF | Selective Call Forwarding |

| | |
|---|---|
| SCIF | Secure Compartmental Facility |
| SCIP | Secure Communications Interoperability Protocol |
| SCN | Switched Circuit Network |
| SCP | Service Control Point |
| SCP | Signaling Control Point |
| SCPC | Single Channel Per Carrier |
| SCS | Session Control and Signaling |
| SCTP | Stream Control Transmission Protocol |
| SD | Signal Degrade |
| SD | Security Devices |
| SDH | Synchronous Digital Hierarchy |
| SDN | Service Delivery Node |
| SDP | Session Description Protocol |
| SDTI | SONET Digital Trunk Interface |
| SEF | Severely Errored Frame |
| SEF | Severely Errored Framing |
| SEFS | Severely Errored Framing Seconds |
| SEI | Secure End Instrument |
| SEP | Signaling End Point |
| SF | Superframe |
| SFD | Start Frame Delimiter |
| SFTP | SSH File Transfer Protocol |
| SG | Signaling Gateway |
| SG | Steering Group |
| SHA | Secure Hash Algorithm |
| SHDSL | Single Pair High-Speed DSL |
| SI | Service Indicator |
| SIGTRAN | Signaling Transport |
| SILC | Selective Incoming Load Control |
| SIMPLE | SIP for Instant Messaging and Presence Leveraging Extensions |
| SIO | Status Indication Out-of Alignment |
| SIP | Session Initiation Protocol |
| SIPO | Signal Units Indicating Processor Outage |
| SIPR | Secure Internet Protocol Router |
| SIPRNet | Secure Internet Protocol Router Network |
| SIPRNET | Secure Internet Protocol Router Network |
| SIPS | Session Initiation Protocol Secure |
| SIP-T | Session Initiation Protocol for Telephones |
| SIP-T(AS) | SIP-T (Assured Service) |
| SIPv2 | Session Initiation Protocol, Version 2 |
| SIT | Special Information Tone |
| SLA | Service Level Agreement |

| | |
|---|---|
| SLAAC | Stateless Address Auto-Configuration |
| SLC | Signal Link Code |
| SLR | Send Loudness Rating |
| SLS | Signaling Link Selection |
| SLSC | Subtended LSC |
| SLTE | Signaling Link Terminal Equipment |
| SMC | SONET Minimum Clock |
| SMCU | Signaling Multipoint Control Unit |
| SME | Subject Matter Expert |
| SME PED | Secure Mobile Environment Portable Electronic Device |
| SMEO | Small End Office |
| SMF | Single Mode Fiber |
| SMI | Security Management Infrastructure |
| SMIv2 | Structure of Management Information Version 2 |
| SMS | Short Message Service |
| SMTP | Simple Message Transfer Protocol |
| SNAP | System/Network Approval Process |
| SNCP | Subnetwork Connection Protection |
| S-NE | Strategic Network Element |
| SNIA | Storage Networking Industry Association |
| SNMP | Simple Network Management Protocol |
| SNMPv1 | Simple Network Management Protocol, Version 1 |
| SNMPv2 | Simple Network Management Protocol, Version 2 |
| SNMPv3 | Simple Network Management Protocol Version 3 |
| SNR | Signal to Noise Ratio |
| S-n.x | Short-Haul (Interface) |
| SOAP | Simple Object Access Protocol |
| SONET | Synchronous Optical Network |
| SP | Signaling Point |
| SPC | Signaling Point Code |
| SPCS | Stored Program Control System |
| SPD | Security Policy Database |
| S-PE | Secret Provider Edge |
| SPF | Shortest Path First |
| SPFI | Substandard Performance Fault Isolation |
| SPI | Security Parameter Index |
| SPIT | SPAM over Internet Telephony |
| SpoA | Service Point of Attachment |
| SQF | System Quality Factors |
| SQL | Structured Query Language |
| SR | Selective Router |
| SR | Short Reach |

| | |
|---|---|
| SRTCP | Secure Real-Time Control Protocol |
| SRTP | Secure Real-Time Protocol |
| SS | Softswitch |
| SS7 | Signaling System No. 7 |
| SSA | Subsystem-Allowed |
| SSAA | System Security Authorization Agreement |
| SSH | Secure Shell |
| SSHv2 | Secure Shell Version 2 |
| SSL | Secure Socket Layer |
| SSL3.1 | Secure Socket Layer Version 3.1 |
| SSM | Single System Manager |
| SSM | Source-Specific Multicast |
| SSM | Synchronization Status Message |
| SSO | Stateful Switch Over |
| SSP | Service Switching Point |
| SSP | Subsystem-Prohibited |
| SST | Subsystem Status Test |
| ST | Signaling Terminal |
| STE | Secure Terminal Equipment |
| STEP | Standardized Tactical Entry Point |
| STIG | Security Technical Implementation Guide |
| STM | Synchronous Transport Module |
| STM-1 | Synchronous Transport Module 1 |
| STM-1c | Synchronous Transport Module 1c |
| STM-4 | Synchronous Transport Module 4 |
| STM-4c | Synchronous Transport Module 4c |
| STM-16 | Synchronous Transport Module 16 |
| STM-16c | Synchronous Transport Module 16c |
| STM-64 | Synchronous Transport Module 64 |
| STM-256 | Synchronous Transport Module 256 |
| STM-O | Synchronous Transport Module O |
| STP | Signaling Transfer Point |
| STRATCOM | United States Strategic Command |
| STS | Synchronous Transport Signal |
| STS-1 | Synchronous Transport Signal-1 |
| SU | Signal Unit |
| SUA | SCCP User Adaptation |
| SUS | Suspend Message |
| SUT | System Under Test |
| SVGA | Super Video Graphics Array |
| SVoIP | Secure Voice over Internet Protocol |
| SVoSIP | Secure Voice over Secure Internet Protocol |

| | |
|---|---|
| Sw | Switch |
| SW64 | Switched 64 kbps |
| SWA | Southwest Asia |
| SYN | Synonym (Filename Extension) |
| Syslog | System Log |
| SysLog | System Log |
| | |
| T | Ethernet Half-Duplex |
| T&E | Test and Evaluation |
| T&S | Timing and Synchronization |
| TA | Terminal Adapter |
| TACACS+ | Terminal Access Controller Access Control System |
| TBD | To Be Determined |
| TCA | Threshold Crossing Alert |
| TCAP | Transaction Capability Application Part |
| TCC | Telephony Country Code |
| TCCC | Theater C4I Coordination Center (EUCOM) |
| TCI | Tag Control Information |
| TCLw | Weighted Terminal Coupling Loss |
| TCP | Transmission Control Protocol |
| TCP | Transport Control Protocol |
| TDEA | Triple Data Encryption Algorithm |
| TDM | Time Division Multiplexing |
| TDMA | Time Division Multiple Access |
| TE | Terminal Equipment |
| TE | Traffic Engineering |
| TE1 | Terminal Equipment Type 1 |
| TE2 | Terminal Equipment Type 2 |
| TFTP | Trivial File Transfer Protocol |
| TG | Trunk Gateway |
| TG | Trunk Group |
| TIA | Telecommunications Industry Association |
| TIAS | Transport Independent Application-Specific |
| TIF | Terminal Indicate Floor-Request |
| TIPHON | Telecommunications and Internet Protocol Harmonization over Networks |
| TISP | Tailored Information Support Plan |
| TJTN | Theater Joint Tactical Networks |
| TJTNCCB | Theater Joint Tactical Networks Configuration Control Board |
| TL1 | Transaction Language 1 |
| TLP | Transmission Level Point |
| TLS | Transport Layer Security |

| | |
|---|---|
| TLS1.0 | Transport Layer Security Version 1.0 |
| TLSC | Transmission Link Session Capacity |
| TLV | Type-Length-Value |
| TMR/USI | Transmission Medium Requirement/User Service Information |
| TN | Tactical-Edge Network |
| TNC | Theater Network Operations Center |
| T-NE | Tactical Network Element |
| TOC | Tactical Operations Center |
| TOD | Time of Day |
| TOE | TCP/IP Offload Engine |
| TOS | Type of Service |
| TP | Test Plan |
| TPID | Tag Protocol Identification |
| TpoA | Transport Point of Attachment |
| Tri-Tac | Tri-Service Tactical Communications |
| TRN | Tactical Radio Network |
| TS | Tandem Switch |
| TS/SCI | Top Secret/Sensitive Compartmented Information |
| TSA | Time Slot Assignment |
| TSAT | Transformational Communications Satellite System |
| TSF | Transport Switching Function |
| TSF | Trusted Security Filter |
| TSG | Telephone Security Standard |
| TSGR | Transport Systems Generic Requirements |
| TSI | Time Slot Interchange |
| TSRD | Telecommunications Security Requirements Document |
| TSSI | Telecom Switched Services Interoperability |
| TTA | Telecommunication Technology Association |
| TTC | Telecommunication Technology Committee |
| TTL | Time to Live |
| TURN | Traversal Using Relay NAT |
| TWC | Three-Way Calling |
| TX | Ethernet Full-Duplex |
| | |
| U | Unclassified |
| U.S.C. | United States Code |
| UA | User Agent |
| UAC | User Agent Client |
| U-AR | Unclassified Aggregation Router |
| UAS | Unavailable Seconds |
| UAS | User Agent Server |
| UC | Unified Capabilities |

| | |
|---|---|
| UCCO | Unified Capabilities Connection Office |
| UCCS | UC Conference System |
| U-CE | Unclassified Customer Edge Router |
| UCR | Unified Capabilities Requirements |
| UCR 2007 | Unified Capabilities Requirements 2007 |
| UCR 2008 | Unified Capabilities Requirements 2008 |
| UCR 2008, Change 3 | Unified Capabilities Requirements 2008, Change 3 |
| UCTP | Unified Capabilities Test Plan |
| UDDI | Universal Discovery Description Interface |
| UDP | User Datagram Protocol |
| UDT | Unitdata |
| UDTS | Unitdata Service |
| UFC | Unified Facilities Criteria |
| UFS | User Features and Services |
| UGS | Unsolicited Grant Service |
| UHF | Ultra High Frequency |
| UI | Unit Interval |
| UIpp | Unit Interval Peak-to-Peak |
| UIrms | Unit Interval Root Mean Square |
| ULA | Unique Local IPv6 Unicast Addresses |
| UNI | User Network Interface |
| UPA | Unauthorized Precedence Level Announcement |
| U-PE | Unclassified Provider Edge |
| UPPS | User Provided Passed Screening |
| UPS | Uninterruptible Power Supply |
| UPSR | Unidirectional Path Switched Ring |
| UPU | User Part Unavailability |
| URI | Uniform Resource Identifier |
| USF | User Service and Feature |
| USI | User Service Information |
| USM | User-Based Security Model |
| USSTRATCOM | U.S. Strategic Command |
| UTP | Unshielded Twisted Pair |
| | |
| V | Volt |
| VAD | Voice Activity Detection |
| VBD | Voiceband Data |
| VC | Virtual Circuit |
| VCA | Vacant Code Announcement |
| VCAT | Virtual Concatenation |
| VCB | Video Command Broadcast |
| VCFC | Video Channel Flow Control |

| | |
|---|---|
| VCFUR | Video Channel Fast Update Request |
| VCL | Video Coding Layer |
| VCS | Video Command Select |
| VDC | Volt Direct Current |
| VD-NE | Virtual Deployed Network Element |
| vDSC | Virtualized Data Storage Controller |
| VDSL | Very High Speed DSL |
| VF | Voice Frequency |
| VG1 | Voice Grade 1 |
| VG2 | Voice Grade 2 |
| VG3 | Voice Grade 3 |
| VG4 | Voice Grade 4 |
| VG5 | Voice Grade 5 |
| VG6 | Voice Grade 6 |
| VGA | Video Graphics Array |
| VHF | Very High Frequency |
| VID | VLAN Identification |
| VIN | Video Indicate Number |
| VLAN | Virtual Local Area Network |
| VLR | Visitor Location Register |
| VMPS | VLAN Management Policy Server |
| VNAR | Voice Net Access Radio |
| VoIP | Voice over Internet Protocol |
| VoSIP | Voice over Secure Internet Protocol |
| VNAR | Voice Net Access Radio |
| VPIM | Voice Profile for Internet Mail |
| VPLS | Virtual Private LAN Service |
| VPN | Virtual Private Network |
| VP-P | Volts Peak-to-Peak |
| VRRP | Virtual Router Redundancy Protocol |
| VSAL | Variable Security Access Level |
| VSAT | Very Small Aperture Terminal |
| VSR | Very Short Reach |
| VSU | Video Session Unit |
| VT | Virtual Tributary |
| VTC | Video Teleconferencing |
| VTCoIP | Video Teleconferencing over IP |
| VT-NE | Virtual Tactical Network Element |
| VTU | Video Teleconferencing Unit |
| VVoIP | Voice and Video over Internet Protocol |
| | |
| WAB | Wireless Access Bridge |

| | |
|---|---|
| WAN | Wide Area Network |
| W-ASAC | WAN Level ASAC |
| WATS | Wide Area Telecommunications Service |
| WAV | Waveform Audio |
| WD | Weather Day |
| WDCS | Wideband Digital Cross-Connect System |
| WebDAV | Web-Based Distributed Authoring and Versioning |
| WEI | Wireless End Instrument |
| WFQ | Weighted Fair Queuing |
| WG | Working Group |
| WIDS | Wireless Intrusion Detection System |
| WINS | Windows Internet Name Service |
| WIN-T | Warfighter Information Network – Terrestrial |
| WLAN | Wireless Local Area Network |
| WLAS | Wireless LAN Access System |
| WPA | Wi-Fi Protected Access |
| WPS | Wireless Priority Service |
| WSDL | Web Service Description Language |
| WTR | Wait to Restore |
| WWNDP | World Wide Numbering and Dialing Plan |
| | |
| XEP | XMPP Extension Protocol |
| XGA | Extended Graphics Array |
| XML | Extensible Markup Language |
| XMPP | Extensible Messaging and Presence Protocol |
| XUDT | Extended Unitdata |
| XUDTS | Extended Unitdata Service |

# SECTION A4
# REFERENCES

## A4.1 AMERICAN NATIONAL STANDARDS INSTITUTE DOCUMENTATION

American National Standard Institute (ANSI), "Operations, Administration, Maintenance, and Provisioning Security Requirements for Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane," T1M1.5/2003-007R4, Draft Proposed April 1, 2003.

T1.101-1987 *Synchronization Interface Standards for Digital Networks*, 1987.

T1.102-1993 *Digital Hierarchy – Electrical Interfaces*, December 1993.

T1.102-1999 *Digital Hierarchy – Electrical Interfaces*, 1999.

T1.105-2001 *Synchronous Optical Network (SONET) – Basic Description including Multiplex Structure, Rates, and Formats*, May 2001.

T1.105.1-2000 *Synchronous Optical Network (SONET) – Automatic Protection*, Revised 2005.

T1.105.03-1994 *Synchronous Optical Network (SONET) – Jitter Network Interfaces*, Revised 2008.

T1.105.03-2003 *Synchronous Optical Network (SONET) – Jitter Network Interfaces*, Revised 2008.

T1.105.06-2002 *Synchronous Optical Network (SONET) – Physical Layer Specifications*, Revised 2007.

T1.107-2002 *Digital Hierarchy – Formats Specifications*, Revised 2006.

T1.111 *Signaling System Number 7 (SS7) – Message Transfer Part (MTP)*, 2001.

T1.112 *Signaling System Number 7 (SS7) – Signaling Connection Control Part (SCCP)*, 2001.

T1.113 *Signaling System No. 7 (SS7) – Integrated Services Digital Network (ISDN) User Part*, 1995.

T1.113-2000 *Signaling System No. 7 (SS7) – Integrated Services Digital Network (ISDN) User Part* (Revision of T1.113-1995; includes two Supplements: T1.113a-2000 and T1.113b-2001).

T1.113.3 *Signaling System No. 7 (SS7) – Signaling Link*.

T1.114-2000 *Signaling System Number 7 (SS7) – Transaction Capabilities and Application Part (TCAP)*, 2000.

T1.231-1993 *Digital Hierarchy - Layer 1 In-Service Digital Transmission Performance Monitoring*, 1993.

T1.231.01-2003 *Digital Subscriber Line (DSL) – Layer 1 In-Service Digital Transmission Performance Monitoring*, Revised 2007.

T1.403-1999 *Network to Customer Installation Interfaces – DS1 Electrical Interface*, Revised 2007.

T1.404-2002 *Network and Customer Installation Interfaces – DS3 Metallic Interface Specification* (Revision and Consolidation of T1.404-1994 and T1.404a-1996), Revised 2006.

T1.523-2000 *Telecom Glossary 2000.*

T1.601-1999 *ISDN Basic Access Interface for Use on Metallic Loops for Application at the Network Side of NT, Layer 1 Specification*.

T1.602 *Data Link Layer Signalling Specification for Application at the User-Network Interface*, February 2000.

T1.605-1991 (1999) *ISDN Basic Access Interface for S and T Reference Points and Layer 1 Specification*.

T1.607-1998 *ISDN Layer 3 Signaling Specifications for Circuit Switched Bearer Service for Digital Subscriber Signaling System No. 1 (DSS1).*

T1.613-1992 *ISDN Call Waiting Supplementary Service*.

T1.615-1992 (R1999) *Digital Subscriber Signalling System No. 1 (DSS1)-Layer 3 Overview.*

T1.616-1992 *ISDN Call Hold Supplementary Service*.

| | |
|---|---|
| T1.619-1992 (R2005) | *Integrated Services Digital Network (ISDN) – Multi-Level Precedence and Preemption (MLPP) Service Capability*, February 1992, Reaffirmed 2005. |
| T1.619a-1994 (R1999) | *Integrated Services Digital Network (ISDN) – Multi-Level Precedence and Preemption (MLPP) Service Capability (MLPP Service Domain and Cause Changes)*, July 1994, Reaffirmed 1999. |
| T1.621-1992 | *ISDN User-to-User Signaling Supplementary Service*. |
| T1.632-1993 | *ISDN Normal Call Transfer Supplementary Service*. |
| T1.642-1993 | *ISDN Call Deflection Supplementary Service*. |
| T1.643-1995 | *ISDN Explicit Call Transfer Supplementary Service*. |
| T1.646-1995 | *Broadband ISDN – Physical Layer Specification for User-Network Interfaces including DS1/ATM*, Supersedes ANSI T1.624-1993), 1995. |
| T1.647-1995 | *ISDN Conference Calling Supplementary Service*. |
| T1.679-2004 | *Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control or ISDN User Part*, June 2004. |
| T1.801.01 | *Digital Transport of Video Teleconferencing/Video Telephony Signals Video Test Scenes for Subjective and Objective Performance Assessment," November 1995.* |
| T1.801.02 | *Digital Transport of Video Teleconferencing/ Video Telephony Signals Performance Terms, Definitions and Examples*, May 1996. |
| T1.801.03 | *Digital Transport of One-Way Signals - Parameters for Objective Performance Assessment*, February 1996. |
| T1.801.04 | *Multimedia Communications Delay, Synchronization, and Frame Rate Measurement*, 1997. |
| ANSI/TIA-1057 | *Link Layer Discovery Protocol for Media Endpoint Device*s, April 2006 |
| T1X1.3/94-001R5 | *Jitter Measurement Methodology*. |

T11 FC-BB-5 *Fibre Channel – Fibre Channel Backbone – 5 (FC-BB-5)*, Revision 2.00, 4 June 2009.

X3.230 See ANSI INCITS 230-1994.

X3.296 *Information Technology – Single-Byte Command Code Sets Connection (SBCON) Architecture*, Replaces ANSI X3.296-1997.

X3.297 *Fibre Channel Physical and Signalling Interface – 2 (FC-PH-2)*, 1997.

X3.303 *Fibre Channel Physical and Signalling interface - 3 (FC-PH-3)*, 1997.

INCITS 230-1994 *Information Technology - Fibre Channel - Physical and Signaling Interface (FC-PH) - Amendment 2* (supplement to ANSI X3.230-1994) (formerly ANSI X3.230-1994/AM 2-1999).

INCITS 374-2003 *Information Technology – Fibre Channel – Single-Byte Command Code Sets Mapping Protocol – 3 (FC-SB-3)*, 2003.

ANSI/TIA-810-B *Telecommunications – Telephone Terminal Equipment – Transmission Requirements for Narrowband Voice over IP and Voice over PCM Digital Wireline Telephones*, SP-3-4352-RV2 (to become ANSI/TIA-810-B).

## A4.2 AMERICAN SOCIETY OF MECHANICAL ENGINEERS

ASME Y14.24 "Types and Applications of Engineering Drawings," 01 January 1999, Reaffirmed 2009.

ASME Y14.34M "Associated Lists," 2008.

ASME Y14.35M "Revision of Engineering Drawings and Associated Documents." 1997, Reaffirmed 2008.

ASME Y14.100 "Engineering Drawing Practices," 2004, Reaffirmed 2009.

## A4.3 ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS & INFORMATION INTEGRATION/DOD CHIEF INFORMATION OFFICE

ASD(NII)/DoD CIO Memorandum, "Department of Defense Unified Capabilities Requirements," current edition.

ASD(NII)/DoD CIO, "Global Information Grid (GIG) Architectural Vision."

ASD(NII)/DoD CIO, "DoD Unified Capabilities 2008 (UCR 2008)," January 2009.

ASD(NII)/DoD CIO, "DoD Unified Capabilities 2008 (UCR 2008) Change 1," January 2010.

ASD(NII)/DoD CIO, "DoD Unified Capabilities 2008 (UCR 2008) Change 2," December 2010.

## A4.4 BRITISH STANDARDS INSTITUTE DOCUMENTATION

BS EN 60950-1:2006 "Information technology equipment. Safety. General requirements," August 6, 2006.

## A4.5 CHAIRMAN OF THE JOINT CHIEFS OF STAFF DOCUMENTATION

CJCS Standing Execute Order for Computer Network Attack and Computer Network Defense, 20 January 2004.

CJCSI 3170.01G "Joint Capabilities Integration and Development System," 1 March 2009, http://www.dtic.mil/cjcs_directives/cdata/unlimit/3170_01.pdf.

CJCSI 6211.02C "Defense Information Systems Network (DISN): Policy and Responsibilities," 9 July 2008, http://www.dtic.mil/cjcs_directives/cdata/unlimit/6211_02.pdf.

CJCSI 6212.01E "Interoperability and Supportability of Information Technology and National Security Systems," 15 December 2008, http://www.dtic.mil/cjcs_directives/cdata/unlimit/6212_01.pdf.

CJCSI 6212.01E "Interoperability and Supportability of Information Technology and National Security Systems," 15 December 2008, http://www.dtic.mil/cjcs_directives/cdata/unlimit/6212_01.pdf.

CJCSI 6215.01C "Policy for Department of Defense (DoD) Voice Networks with Real Time Services (RTS)," 9 November 2007, http://www.dtic.mil/cjcs_directives/cdata/unlimit/6215_01.pdf.

CJCSI 6215.02A "Policy, Responsibilities, Processes, and Administration for the Department of Defense Global Information Grid Networks," 31 July 2004.

CJCSI 6510.01E "Information Assurance (IA) and Computer Network Defense (CND)," 15 June 2004.

CJCSI 6510.01E "Information Assurance (IA) and Computer Network Defense (CND)," 15 August 2007, http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf.

CJCSM 3150.07A "Joint Reporting Structure Status Communications," 19 April 19 2001, http://www.dtic.mil/doctrine/jel/cjcsd/cjcsm/m315007a.pdf.

CJCSM 3500.04C "Universal Joint Task List (UJTL)," Version 4.0, 1 July 2002, http://www.dtic.mil/doctrine/jel/cjcsd/cjcsm/m350004c.pdf.

CJCSM 6231.01C "Manual for Employing Joint Communications Systems: Joint Tactical Systems Management," 20 June 2003.

CJCSM 6231.02 "Manual for Employing Joint Tactical Communications Systems, Joint Voice Communications Systems," 01 August 1998.

CJCSM 6510.01 "Defense in Depth: Information Assurance (IA) and Computer Network Defense (CND)," 25 March 2003, Change 1, 10 August 2004, and Change 2, 26 January 2006.

Joint Chiefs of Staff, "Joint Vision 2020," May 1996.

Joint Publication 0-2, "Unified Action Armed Forces (UNAAF)," 24 February 1995.

## A4.6 DEFENSE INFORMATION SYSTEMS AGENCY DOCUMENTATION

Defense Information Systems Agency, DISA Circular 300-115-7, "Communications Security: Defense Red Switch Network (DRSN) Security Guidance," 19 February 2002.

Defense Information Systems Agency, DISA Circular 310-55-1.
Defense Information Systems Agency, DISA Circular 310-255-1, "DSN User Services Guide," 21 April 1998.

Defense Information Systems Agency, DISA Circular 370-V130-1, 5 November 1965.

Defense Information Systems Agency, DISA Instruction 630-230-19, "Automated Data Processing Information Systems Security Program," 9 July 1996.

Defense Information Systems Agency "Global Information Grid (GIG) Convergence Master Plan (GCMP)," Version 5.25b, 29 March 2006.

Defense Information Systems Agency, "Defense Information Systems Agency (DISA) Campaign Plan."

Defense Information Systems Agency, "DISN Overarching Technical Strategy (DOTS)."

Defense Information Systems Agency, "DISN Technology Evolution Plan (DTEP)."

DISA Field Security Operations, DoD, "Application Security and Development Security Technical Implementation Guide."

DISA Field Security Operations, DoD, "Database Security Technical Implementation Guide," Version 8, Release 1, 19 September 2007.

DISA Field Security Operations, "Enclave Security Technical Implementation Guide."

DISA Field Security Operations, DoD, "Instant Messaging Security Technical Implementation Guide," Version 1, Release 2, 15 February 2008.

DISA Field Security Operations, "Network Infrastructure Security Technical Implementation Guide."

DISA Field Security Operations, "DoD Personal Computer Communications Client (Voice/Video/Collaboration Security Technical Implementation Guide," Version 1, Release 1, 15 June 2008.

NOTE: "The VVoIP STIG supersedes, merges, and replaces the following:

- Voice over Internet Protocol (VoIP) STIG and Checklist
- Personal Computer Communications Client (PCCC) STIG and Checklist."

DISA Field Security Operations, "DoD Secure Telecommunications and Defense Red Switch Network Security Technical Implementation Guide," Version 1, Release 1, 28 March 2006.

DISA Field Security Operations, "DoD Telecommunications and Defense Switched Network Security Technical Implementation Guide," Version 2, Release 3, 30 April 2006.

DISA Field Security Operations, "Instant Messaging Checklist," Version 1, Release 1.3, 15February 2008.

DISA Field Security Operations, "Network Infrastructure Security Technical Implementation Guide," Version 6, Release 4, 16 December 2005.

DISA Field Security Operations, "Personal Computer Communications Client (Voice/Video/Collaboration) Checklist," Version 1, Release 1.1, August 15, 2008.

NOTE: "The VVoIP STIG supersedes, merges, and replaces the following:

- Voice over Internet Protocol (VoIP) STIG and Checklist
- Personal Computer Communications Client (PCCC) STIG and Checklist."

DISA Field Security Operations, "Voice over Internet Protocol (VoIP) Security Technical Implementation Guide," Version 2, Release 1, 29 August 2005.

NOTE: "The VVoIP STIG supersedes, merges, and replaces the following:

- Voice over Internet Protocol (VoIP) STIG and Checklist
- Personal Computer Communications Client (PCCC) STIG and Checklist."

DISA Field Security Operations, "Voice and Video over Internet Protocol (VVoIP) Security Technical Implementation Guide," Version 3, Release 1, 23 December 2009.

DISA Field Security Operations, "Voice and Video over Internet Protocol (VVoIP) Security Technical Implementation Guide Checklist."

NOTE: "The VVoIP STIG supersedes, merges, and replaces the following:

- Voice over Internet Protocol (VoIP) STIG and Checklist
- Personal Computer Communications Client (PCCC) STIG and Checklist."

DISA Field Security Operations, "Wireless Security Technical Implementation Guide," Version 6, Release 2, 23 April 2010.

"Initial Capabilities Document for Global Information Grid 2.0 (GIG 2.0)," May 29, 2009.

Global Information Grid Enterprise Services, DISA Web page.

## A4.7 DEPARTMENT OF DEFENSE DOCUMENTATION

Center for DISN Services, "DISN Service Level Agreement for the Defense Information Systems Agency and its customers."
Common Criteria Evaluation and Validation Scheme, 6 August 2004.

Department of Defense 5200.2, "DOD Information Security Program Regulation," 9 April 1997.

Department of Defense 5200.40, "DOD Information Technology Security Certification and Accreditation (CandA) Process (DITSCAP)," 30 December 1997.

Department of Defense 8510.1-M, "DOD Information Technology Security Certification and Accreditation Process (DITSCAP)," 31 July 2000,

Department of Defense 8910.1-M, "DoD Procedures for Management of Information Requirements," 30 June 1998.

Department of Defense, "Application Security Checklist."

Department of Defense, "Application Development Security Technical Implementation Guide."

Department of Defense Assured Service Session Initiation Protocol (AS-SIP) Generic System Requirement (GSR), Defense Information Systems Agency, Version 1.2.1, 12 May 2006.

"Department of Defense (DoD) Class 3 Public Key Infrastructure (PKI) Public Key-Enabled Application Requirements," Version 1.0, 13 July 2000.

Department of Defense Collaboration Interoperability Standards, J.P. Stenbit, Memorandum of 1 November 2002.

Department of Defense, "GIG Architecture Master Plan," Final Draft, 29 November 2002.

Department of Defense, "GIG Architecture Project Management Plan," 14 August 2002.
"Department of Defense Joint Technical Architecture (JTA)," Version 6, Volumes I and II, 3 October 2003.

Department of Defense Real Time Services (RTS) Information Assurance (IA) Generic System Requirement (GSR), Defense Information Systems Agency, Revision 1.4, 8 September 2006.

Department of Defense Real-Time Services (RTS) Generic System Requirements (GSR) and Generic System Specifications (GSS) Appendices Overview, Revision 0.2, 16 August 2006.
Department of Defense Voice Networks Generic Switching Center Requirements (GSCR), 8 September 2003, ERATA Change 1, 1 March 2005.

Department of Defense Wide Area Network (WAN) Generic System Requirement (GSR), Defense Information Systems Agency, Revision 1.3, 18 May 2006.

Deputy Assistant Secretary of Defense (Deputy CIO), "DSN Generic Switching Center Specification (GSCR)," signed by the Deputy Assistant Secretary of Defense (Deputy CIO), September 8, 2003.

Deputy Secretary of Defense, "Smart Card Adoption and Implementation," 10 November 1999.

Director of Central Intelligence Directive (DCID) 6/3, "Protecting Sensitive Compartmented Information within Information Systems," 5 June 1999.

"DoD Architecture Framework Version 1.0," February 8, 2004.

DoD CIO, "Department of Defense Global Information Grid Architectural Vision: Vision for a Net-Centric, Service-Oriented DoD Enterprise," Version 1, June 2007.

DoD CIO Guidance IA6-8510 IA.

"DoD Class 3 Public Key Infrastructure Public Key-Enabled Application Requirements," July 13, 2000.

DoD Information Technology Standards Registry (DISR) IPv6 Standards Technical Working Group (TWG), "DoD IPv6 Standard Profiles for IPv6 Capable Products," Version 1.0, 1 June 2006.

"DoD PKI Functional Interface Specification," June 2007.

DoD PKI PMO, "DoD PKE Application Requirements Specification," latest version.

"DoD Policy for Enterprise-wide Deployment of IPv6," 9 June 2003.

"DoD RTS Information Assurance Countermeasures," Version 0.7, DoD RTS Information Assurance Working Group, 29 March 2006.

DoD CIO Memorandum, "Internet Protocol Version 6 (IPv6) Interim Transition Guidance," 29 September 2003.

DoD CIO Memorandum, "Internet Protocol Version 6 (IPv6)," 9 June 2003.

DoD CIO Memorandum "DoD IPv6 Definitions," 26 June 2008.

"DoD Internet Protocol Version 6 (IPv6) Interim Transition Guidance," 29 September 2003.

DoD Policy for Enterprise-wide Deployment of IPv6," 9 June 2003.

DoD Real Time Services Working Group, "DoD RTS IA Countermeasures," 29 March 2006.

DoD RTS Information Assurance Working Group, "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment," Version 3.4, 22 May 2009.

DoD Unified Facilities Criteria (UFC), "Design and O&M: Mass Notification Systems", Change 1, January 2010.

"DoD Voice Networks Generic Switching Center Requirements (GSCR)," 8 September 2003, Errata Change 1, 1 March 2005.

DSN Systems Design, Implementation, and Transition Branch, "Defense Switched Network (DSN) IPv6 Transition Plan," Version 1.1, 28 June 2006.

Interim Department of Defense (DoD) Certification and Accreditation (C&A) Process Guidance, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," July 6, 2006.

Office of DoD CIO, "DoD Internet Protocol Version 6 (IPv6) Transition Plan," Version 1.0, November 2003.

"The Global Information Grid (GIG) Enterprise Service Profile."

United States Strategic Command (STRATCOM), "Joint Concept of Operations for Global Information Grid Network Operations (NetOps)," 20 April 2004.

## A4.8 DOD DIRECTIVES

DoDD C-3222.5 (SECRET) "Electromagnetic Compatibility (EMC) Management Program for SIGINT Sites (U)," 22 April 1987.

DoDD 4630.05 "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2005, Certified Current as of 23 April 2007, http://www.dtic.mil/whs/directives/corres/pdf/463005p.pdf.

DoDD 5000.01 "The Defense Acquisition System," 12 May 2003, Certified current as of 20 November 2007.

DoDD 5144.1 "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005.

DoDD 5200.28 "Security Requirements for Automated Information Systems (AISs)," 21 March 1988.

DoDD 8000.01 "Management of the Department of Defense Information Enterprise," 10 February 2009, http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf.

DoDD 8100.1 "Global Information Grid (GIG) Overarching Policy," 19 September 2002, Certified Current as of 21 November 2003.

DoDD 8115.01 "Information Technology Portfolio Management," 10 October 2005.

DoDD 8260.1 "Data Collection, Development, and Management," 6 December 2002.

DoDD 8320.02 "Data Sharing in a Net-Centric Department of Defense," 2 December 2004, Certified Current as of 23 April 2007, http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf.

DoDD 8500.01E "Information Assurance (IA)," October 24, 2002, Certified Current as of April 23, 2007, http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf.

DoDD 8500.2 "Information Assurance Implementation," 6 February 2003.

DoDD 8520.1 "Protection of Sensitive Compartmented Information (SCI)," December 20, 2001.

DoDD O-8530.1 (FOUO) "Computer Network Defense (CND)," 8 January 2001.

DoDD O-8530.2 (FOUO) "Computer Networking Defense (CND)," 1 April 2004.

DoDD 8570.01 "Information Assurance Training, Certification, and Workforce Management, 15 August 2004, Certified Current as of 23 April 2007, http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf.

## A4.9 DOD INSTRUCTIONS

DoDI 4630.8 "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 30 June 2004.

DoDI 5000.02 "Operation of the Defense Acquisition System," 8 December 2008.

DoDI 5200.40 "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," 30 December 1997. Issuance cancelled by: DoDI 8510.01.

DoDI 8100.04 "DoD Unified Capabilities," December 2010.

DoDI 8260.01 "Support for Strategic Analysis," 11 January 2007.

DoDI 8410.02 "NetOps for the Global Information Grid (GIG)," 19 December 2008.

DoDI 8500.2 "Information Assurance (IA) Implementation," 6 February 2003.

DoDI 8510.01 "DoD Information Assurance (IA) Certification and Accreditation Process (DIACAP)," 28 November 2007.

DoDI 8551.1 "Ports, Protocols, and Services Management (PPSM)," 13 August 2004, http://www.dtic.mil/whs/directives/corres/pdf/855101p.pdf.

DoDI 8552.01 "Use of Mobile Code Technologies in DoD Information Systems," 23 October 2006.

## A4.10 ELECTRONICS INDUSTRIES ALLIANCE

EIA/TIA-232-E "Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange," (superseded by TIA-232-F), January 1991.

EIA/TIA-530-A "High Speed 25-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment, Including Alternative 26-Position Connector," ANSI/TIA/EIA-530-A-92) (R98) (R2003), June 1992.

EIA-170-A "Electrical Performance Standards Monochrome Television Studio Facility, with Revision IET NTS 1 Color Television Studio Picture Line Amplifier Output Drawing," November 1977.

EIA-310-C "19-inch rack mounting equipment specification."

EIA-366-A "Interface Between Data Terminal Equipment and Automatic Calling Equipment for Data Communication," March 1979.

EIA-422-B "Electrical Characteristics of Balanced Voltage Digital Interface Circuits," 1994.

EIA-449-1 "General Purpose 37-Position and 9-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange," January 2000.

EIA-530 "Interconnection of DTE and DCE Employing Serial Binary Data Interchange with Control Information Exchanged on Separate Control Circuits."

## A4.11 ETSI DOCUMENTATION

EN 50022 "Specification for low voltage switchgear and controlgear for industrial gear," 1977.

EN 50082
ETS-FN-50022 "Electromagnetic compatibility. Generic immunity standard. Residential, commercial and light industry," January 1998.

ETS 300 019 "Equipment Engineering (EE); Environmental conditions and environmental tests for telecommunications equipment," 1994.

EN 300 386 "Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunication network equipment; ElectroMagnetic Compatibility (EMC) requirements," Version 1.5.1, May 2010.

TS 102 165-1 "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN) – Methods and protocols; Part 1: Method

and Proforma for Threat, Risk, Vulnerability Analysis," Version 4.2.1, December 2006.

TS 102 165-2 "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols;; Part 2: Protocol Framework Definition; Security Counter Measures," Version 4.2.1, February 2007.

TS 183 029 Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services: Explicit Communication Transfer (ECT); Protocol specification, Version 2.6.0, June 2008.

## A4.12 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATIONS

FIPS PUB 140-2 U.S. Department of Commerce/National Institute of Standards and Technology, "Security Requirements for Cryptographic Modules," 25 May 2001.

FIPS PUB 186-2 U.S. Department of Commerce/National Institute of Standards and Technology, "Digital Signature Standard (DSS)," 27 January 2000.

FIPS PUB 197 Federal Information Processing Standards Publication 197, "Advanced Encryption Standard (AES)," 26 November 2001.

## A4.13 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC. DOCUMENTATION

455-1985 IEEE Standard for Standard Test Procedure for Measuring Longitudinal Balance of Telephone Equipment Operating in the Voice Band, 1 January 2001.

802.1p IEEE Standard for Traffic Class Expediting and Dynamic Multicast Filtering (published in 802.1D-1998).

802.1AB-2009 IEEE Standard for Station and Media Access Control Connectivity Discovery, 11 September 2009.

802.1AX-2008 IEEE Standard for IEEE Standard for Local and Metropolitan Area Networks – Link Aggregation, 2008.

802.1D™-2004 IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges, June 2004.

802.1Q™-1998 IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks, 1 January 1998.

802.1Q™-2003 IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks, 2003.

802.1Qau IEEE Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks – Amendment: 10: Congestion Notification, 15 September 2006.

802.1Qaz IEEE Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks – Amendment: Enhanced Transmission Selection, 27 March 2008.

802.1Qbb IEEE Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks – Amendment: Priority-based Flow Control, 27 March 2008.

802.1s IEEE Standard for Local and Metropolitan Area Networks: Multiple Spanning Trees, 2003. (Merged into 802.1Q-2003).

802.1w IEEE Standard for Local and Metropolitan Area Networks: Rapid Reconfiguration of Spanning Tree, 2003. (Merged into 802.1D-2004).

802.1X™-2001 IEEE Standard for Local and Metropolitan Area Networks: Port Based Network Access Control, 2001.

802.1X™-2004 IEEE Standard for Local and Metropolitan Area Networks: Port Based Network Access Control, 2004.

802.3™-1993 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications, 1993.

802.3™-2008 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, 26 December 2008.

802.3i IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: 10BASE-T 10 Mbit/s (1.25 MB/s) over twisted pair, 1990.

802.3u-1995 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: 100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet at 100 Mbit/s (12.5 MB/s) w/autonegotiation, 1995.

802.3x-1997 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: Full Duplex and flow control, 1997.

802.3z-1998 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: 1000BASE-X Gbit/s Ethernet over Fiber-Optic at 1 Gbit/s (125 MB/s), 1998.

802.3ab-1999 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: 1000BASE-T Gbit/s Ethernet over twisted pair at 1 Gbit/s (125 MB/s), 1999.

802.3ad-2000 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: Link aggregation for parallel links, 2000.

802.3ae-2003 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: 10 Gbit/s (1,250 MB/s) Ether over fiber; 10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-SW, 10GBASE-LW, 10GBASE-EW, 2003.

802.3ah-2004 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: Media Access Control Parameters, Physical layers, and Management Parameters for Subscriber Access Networks, 2004.

802.11™-2007 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, June 2007.

802.11a Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHz Band, June 2003.

802.11b Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band, June 2003.

802.11e Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Wireless LAN for Quality of Service, June 2003.

802.11e-2005 Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications:

Amendment 8, Medium Access Control (MAC) Quality of Service Enhancements, 9 February 2006.

802.11h Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 5, 29 December 2003.

802.11i Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6, Medium Access Control (MAC), 14 February 2005.

802.11g Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band, June 2003.

802.16™-2004 IEEE Standard for Local and metropolitan area networks—Part 16: Air Interface for Fixed Broadband Wireless Access Systems, 1 October 2004.

802.16d™ Standard for Amendment to IEEE Standard for Local and metropolitan area networks—Part 16: Air Interface for Fixed Broadband Wireless Access Systems – Detailed System Profiles for 2-11 GHz, 11 December 2002.

802.16e™ IEEE Standard for Local and metropolitan area networks— Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands *and* Corrigendum 1, 28 February 2006.

802.17-2004 IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 17: Resilient Packet Ring (RPR) Access Method and Physical Layer Specifications, 24 September 2004.

## A4.14 INTERNATIONAL TELECOMMUNICATION UNION DOCUMENTATION

E.164 ITU-T Recommendation E.164, "The International Public Telecommunication Numbering Plan," Geneva, Switzerland, 2005.

G.107 ITU-T Recommendation G.107, "The E-model: a computational model for use in transmission planning," Geneva, Switzerland, April 2009.

G.165 ITU-T Recommendation G.165, "Echo cancellers," Geneva, Switzerland, November 1988.

G.168 ITU-T Recommendation G.168, "Digital network echo cancellers," Geneva, Switzerland, January 2007.

G.651 ITU-T Recommendation G.651, "Characteristics of a 50/125 µm multimode graded index optical fibre cable," February 1998.

G.651.1 ITU-T Recommendation G.651.1, "Characteristics of a 50/125 µm multimode graded index optical fibre cable for the optical access network," Geneva, Switzerland, July 2007.

G.652 ITU-T Recommendation G.652, "Characteristics of a single-mode optical fibre and cable," Geneva, Switzerland, June 2005.

G.655 ITU-T Recommendation G.655, "Characteristics of a non-zero dispersion-shifted single-mode optical fibre and cable," Geneva, Switzerland, March 2006.

G.691 ITU-T Recommendation G.691, "Optical interfaces for single channel STM-64 and other SDH systems with optical amplifiers," Geneva, Switzerland, March 2006.

G.693 ITU-T Recommendation G.693, "Optical interfaces for intra-office systems," Geneva, Switzerland, May 2006.

G.694.1 ITU-T Recommendation G.694.1, "Spectral grids for WDM applications: DWDM frequency grid," Geneva, Switzerland, 2002.

G.703 ITU-T Recommendation G.703, "Physical/Electrical Characteristics of Hierarchical Digital Interfaces at 1544, 2048, 8448, and 44736 kbit/s Hierarchical Levels," 2001.

G.704 ITU-T Recommendation G.704, "Series G: Transmission Systems and Media, Digital Systems and Networks—Digital transmission systems – Terminal equipments –

General Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels," October 1998.

G.707/ Y.1322 ITU-T Recommendation G.707/Y.1322, "Network node interface for the synchronous digital hierarchy (SDH)," Geneva, Switzerland, January 2007.

G.709/ Y.1331 ITU-T Recommendation G.709/Y.1331, "Network node interface for the optical transport network (OTN)," Geneva, Switzerland, March 2003.

G.711 ITU-T Recommendation G.711, "General Aspects of Digital Transmission Systems, Terminal Equipments, Pulse code modulation (PCM) of voice frequencies," Geneva, Switzerland, November 1988.

Appendix I, "A high quality low complexity algorithm for packet loss concealment with G.711," Geneva, Switzerland, September 1999.

Appendix II, "A comfort noise payload definition for ITU-T G.711 use in packet-based multimedia communication systems," Geneva, Switzerland, February 2000.

G.722 ITU-T Recommendation G.722, "7 kHz audio-coding within 64 kbit/s," Geneva, Switzerland, November 1988.

G.723.1 ITU-T Recommendation G.723.1, "Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s," Geneva, Switzerland, May 2006.

G.726 ITU-T Recommendation G.726, "32 kbps Adaptive Differential Pulse Code Modulation (ADPCM)," Geneva, Switzerland, December 1990.

G.728 ITU-T Recommendation G.728, "Coding of speech at 16 kbit/s using low-delay code excited linear prediction," Geneva, Switzerland, September 1992.

G.729 ITU-T Recommendation G.729, "Coding of speech at 8 kbit/s conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)," Geneva, Switzerland, March 1996, plus Erratum 1, April 2006, and Annexes A through J, and Appendices I, II, and III.

G.729.1 ITU Recommendation G.729.1 (2006) Amendment 1, "New Annex A on G.729.1 usage in H.245, plus corrections to the main body and updated test vectors," Geneva, Switzerland, January 2007.

*This corrigendum was never published, its content having been included in the published ITU-T Recommendation G.729.1 (2006)*

G.729.1 ITU Recommendation G.729.1 (2006), "G.729 based Embedded Variable bit-rate codor: An 8-32 kbit/s scalable wideband coder bit stream interoperable with G.729," Geneva, Switzerland, May 2006.

*This edition includes the modifications introduced by G.729.1 (2006) Amd. 1 approved on 13 January 2007, and G.729.1 (2006) Amd. 2 approved on 13 February 2007.*

G.732 ITU-T Recommendation G.732, "Characteristics of primary PCM multiplex equipment operating at 2048 kbit/s," Geneva, Switzerland, November 1988.

G.783 ITU-T Recommendation G.783, "Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks," Geneva, Switzerland, March 2006.

G.811 ITU-T Recommendation G.811, "Timing characteristics of primary reference clocks," 1997.

G.825 ITU-T Recommendation G.825, "The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)," Geneva, Switzerland, March 2003.

G.826 ITU-T Recommendation G.826, "End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections," Geneva, Switzerland, December 2002.

G.829 ITU-T Recommendation G.829, "Error performance events for SDH multiplex and regenerator sections," Geneva, Switzerland, December 2002.

G.831 ITU-T Recommendation G.831, "Management capabilities of transport networks based on the synchronous digital hierarchy (SDH)," Geneva, Switzerland, March 2000.

G.841 ITU-T Recommendation G.841, "Types and characteristics of SDH network protection architectures," Geneva, Switzerland, October 1998.

G.842 ITU-T Recommendation G.842, "Interworking of SDH network protection architectures," Geneva, Switzerland, April 1997.

G.872 ITU-T Recommendation G.872, "Architecture of optical transport networks," Geneva, Switzerland, November 2001.

G.957 ITU-T Recommendation G.957, "Optical interfaces for equipments and systems relating to the synchronous digital hierarchy," Geneva, Switzerland, March 2006.

G.958 ITU-T Recommendation G.958, "Digital line systems based on the synchronous digital hierarchy for use on optical fibre cables." [Withdrawn]

G.991.1 ITU-T Recommendation G.991.1, "High bit rate digital subscriber line (HDSL) transceivers," 1998.

G.991.2 ITU-T Recommendation G.991.2, "Single-pair high-speed digital subscriber line (SHDSL) transceivers," 1998.

G.992.1 ITU-T Recommendation G.992.1, "Asymmetric digital subscriber line (ADSL) transceivers," 1999.

G.992.2 ITU-T Recommendation G.992.2, "Splitterless asymmetric digital subscriber line (ADSL) transceivers," 1999.

G.992.3 ITU-T Recommendation G.992.2, "Asymmetric digital subscriber line transceivers 2 (ADSL2)," 2009.

G.992.4 ITU-T Recommendation G.992.4, "Splitterless asymmetric digital subscriber line transceivers 2 (splitterless ADSL2)," 2002.

G.992.5 ITU-T Recommendation G.992.5, "Asymmetric digital subscriber line (ADSL) transceivers – Extended bandwidth ADSL2 (ADSL2plus)," 2009.

G.993.1 ITU-T Recommendation G.993.1, "Very high speed digital subscriber line transceivers (VDSL)," 2004.

G.993.2 ITU-T Recommendation G.993.2, "Very high speed digital subscriber line transceivers 2 (VDSL2)," 2006.

G.998.1 ITU-T Recommendation G.993.2, "ATM-based multi-pair bonding," 2005.

G.998.2 ITU-T Recommendation G.993.2, "Ethernet-based multi-pair bonding," 2005.

G.998.3 ITU-T Recommendation G.993.2, "Multi-pair bonding using time-division inverse multiplexing," 2005.

G.1070 ITU-T Recommendation G.1070, "Opinion model for video-telephony applications," Geneva, Switzerland, April 2007.

G.7041/ Y.1303 ITU-T Recommendation G.7041/Y.1303, "Generic framing procedure (GFP)," Geneva, Switzerland, Geneva, Switzerland, October 2008.

G.7042/ Y.1305 ITU-T Recommendation G.7042/Y.1305, "Link capacity adjustment scheme (LCAS) for virtual concatenated signals," Geneva, Switzerland, March 2006.

G.7043 Y.1343 ITU-T Recommendation G.7043/Y.1343, "Virtual concatenation of plesiochronous digital hierarchy (PDH) signals," Geneva, Switzerland, July 2004.

G.8251 ITU-T Recommendation G.8251(G.otnjit), "The control of jitter and wander within the optical transport network (OTN)," Geneva, Switzerland, November 2001.

H.224 ITU-T Recommendation H.224, "A real time control protocol for simplex applications using the H.221 LSD/HSD/MLP channels," Geneva, Switzerland, January 2005.

H.200 ITU-T Recommendation H.200, "Framework for recommendations for audiovisual services," March 1993.

H.221 ITU-T Recommendation H.221, "Frame structure for a 64 to 1,920 kbit/s channel in audiovisual teleservices," March 2004.

H.222 ITU-T Recommendation H.222, "Coding of moving pictures and associated audio: systems," July 1995.

H.224 ITU-T Recommendation H.224, "Real time control protocol for simplex applications using the H.221LSD/HSD/MLP channels," February 2000.

H.225.0 ITU-T Recommendation H.225.0, "Call signalling protocols and media stream packetization for packet-based multimedia communication systems," July 2003.

H.230 ITU-T Recommendation H.230, "Frame-synchronous control and indication signals for audiovisual systems," March 2004.

H.231 ITU-T Recommendation H.231, "Multipoint control units for audiovisual systems using digital channels up to 2 Mbit/s," July 1997.

H.234 ITU-T Recommendation H.234, "Encryption key management and authentication system for audiovisual services," November 1994.

H.235 ITU-T Recommendation H.235, "Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals," August 2003.

H.239 ITU-T Recommendation H.239, "Role management and additional media channels for H.300-series terminals," July 2003.

H.241 ITU-T Recommendation H.241, "Extended video procedures and control signals for H.300-series terminals," July 2003.

H.242 ITU-T Recommendation H.242, "System for establishing communication between audiovisual terminals using digital channels up to 2 Mbit/S," March 2004.

H.243 ITU-T Recommendation H.243, "Procedures for establishing communications between three or more audiovisual terminals using digital channels up to 2 Mbit/s," February 2000.

H.244 ITU Recommendation H.244, "Synchronized aggregation of multiple 64 or 56 kbit/s channels," Geneva, Switzerland, July 1995.

H.245 ITU-T Recommendation H.245, "control protocol for multimedia communication," July 2003.

H.246 ITU-T Recommendation H.246, "Interworking of H-series multimedia terminals with H-series multimedia terminals and voice/voiceband terminals on GSTN and ISDN," February 1998.

H.248.1 ITU-T Recommendation H.248.1, "Gateway control protocol: Version 3," Geneva Switzerland, September 2005.

H.248.24 ITU-T Recommendation H.248.24, "Gateway control protocol: Multi-frequency tone generation and detection packages," Geneva, Switzerland, July 2003.

H.248.25 ITU-T Recommendation H.248.24, "Gateway control protocol: Basic CAS packages," Geneva, Switzerland, January 2007.

H.248.28 ITU-T Recommendation H.248.28, "Gateway control protocol: International CAS packages," Geneva, Switzerland, January 2007.

H.261 ITU-T Recommendation H.261, "Video codec for audiovisual services at p x 64 kbit/s," Recommendation H.261, Geneva, Switzerland, March 1993.

H.263 ITU-T Recommendation H.263, "Video coding for low bit rate communication," Geneva, Switzerland, January 2005. (H.263a, H.323+, H.263 (1999)).

H.264 ITU-T Recommendation H.264, "Advanced video coding for generic audiovisual services," Geneva, Switzerland, March 2005. (Also, known as H.264/AVC)

H.281 ITU-T Recommendation H.281, "A far end camera control protocol for videoconferences using H.224," Geneva, Switzerland, November 1994.

H.282 ITU-T Recommendation H.282, "Remote device control protocol for multimedia applications," May 1999.

H.283 ITU-T Recommendation H.283, "Remote device control logical channel transport," May 1999.

H.320 ITU-T Recommendation H.320, "Narrow-band visual telephone systems and terminal equipment," Geneva, Switzerland, March 2004.

H.323 ITU-T Recommendation H.323, "Packet-based multimedia communications systems," Geneva, Switzerland, June 2006.

H.341 ITU-T Recommendation H.341, "Multimedia management information base," May 1999.

H.350 ITU-T Recommendation H.350, "Directory services architecture for multimedia conferencing," August 2003.

H.350.1 ITU-T Recommendation H.350.1, "Directory services architecture for H.323," August 2003.

H.350.3 ITU-T Recommendation H.350.3, "Directory services architecture for H.320," August 2003.

H.350.4 ITU-T Recommendation H.350.4, "Directory services architecture for SIP," August 2003.

I.361 ITU-T Recommendation I.361, "B-ISDN ATM layer specification," 1999.

H.350.4 ITU-T Recommendation H.350.4, "Directory services architecture for SIP," August 2003.

H.363.5 ITU-T Recommendation H.363.5, "B-ISDN ATM Adaptation Layer specification : Type 5 AAL," 1999.

M.2101 ITU-T Recommendation M.2101, "Performance limits for bringing-into-service and maintenance of international multi-operator SDH paths and multiplex sections," Geneva, Switzerland, June 2003.

M.3100 ITU-T Recommendation M.3100, "Generic network information model," Geneva, Switzerland, April 2005.

P.563 ITU-T Recommendation P.563, "Single Ended Method for Objective Speech Quality Assessment in Narrow-Band Telephony Applications," Geneva, Switzerland, April 2004.

P.800 ITU-T Recommendation P.800, "Methods for subjective determination of transmission quality," Geneva, Switzerland, 1996. (Formerly ITU-T Recommendation P. 80)

P.800.1 ITU-T Recommendation P.800.1, "Methods for Subjective Determination of Transmission Quality - Series P: Telephone Transmission Quality; Methods for Objective and Subjective Assessment of Quality," Geneva, Switzerland, August 1996.

P.862 ITU-T Recommendation P.862, "Perceptual evaluation of speech quality (PESQ): An objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codecs," Geneva, Switzerland, February 2001.

Q.735.3 ITU-T Recommendation Q.735.3, "Stage 3 description for community of interest supplementary services using Signalling System No. 7: Multi-level precedence and preemption," Geneva, Switzerland, March 1993.

Q.850 ITU-T Recommendation Q.850, "Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN User Part," Geneva, Switzerland, May 1998.

Q.921 ITU-T Recommendation Q.921, "ISDN user-network interface – Data link layer specification," Geneva, Switzerland, September 1997.

NOTE: This Recommendation is published with the double number Q.921 and I.441.

Q.922 ITU-T Recommendation Q.922, "ISDN data link layer specification for frame mode bearer services," February 1992.

Q.931 ITU-T Recommendation Q.931, "ISDN user-network interface layer 3 specification for basic call control," Geneva, Switzerland, May 1998.

NOTE: This Recommendation is also included but not published in I series under alias number I.451.

Q.955.3 ITU-T Recommendation Q.955.3, "Stage 3 description for community of interest supplementary services using DSS 1 – Multi-level precedence and preemption (MLPP)," Geneva, Switzerland, March 1993.

Q.1912.5 ITU-T Recommendation Q.1912.5, "Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control Protocol or ISDN User Part," Geneva, Switzerland, March 2004.

T.4 ITU-T Recommendation T.4, "Standardization of Group 3 facsimile terminals for document transmission," Geneva, Switzerland, July 2003.

T.38 ITU-T Recommendation T.38, "Procedures for real-time Group 3 facsimile communication over IP networks," Geneva, Switzerland, April 2007.

T.140 ITU-T Recommendation T.140, "Protocol for multimedia application text conversion," February 1998.

V.14 ITU-T Recommendation V.14, "Transmission of start-stop characters over synchronous bearer channels," Geneva, Switzerland, March 1993.

V.24 ITU-T Recommendation V.24, "List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE)," Geneva, Switzerland, February 2000.

V.32 ITU-T Recommendation V.32, "A family of 2-wire, duplex modems operating at data signalling rates of up to 9600 bit/s for use on the general switched telephone network and on leased telephone-type circuits," Geneva, Switzerland, March 1993.

V.34 ITU-T Recommendation V.34, "A modem operating at data signalling rates of up to 33 600 bit/s for use on the general switched telephone network and on leased point-to-point 2-wire telephone-type circuits," Geneva, Switzerland, February 1998.

V.35 ITU-T Recommendation V.35, "Data transmission at 48 kilobits per second using 60-108 kHz group band circuits," Geneva, Switzerland, October 1984.

V.42bis ITU-T Recommendation V.42bis, "Data compression procedures for DCEs using error correction procedures," January 1990.

V.54 ITU-T Recommendation V.54, "Loop test devices for modems," Geneva, Switzerland, November 1988.

V.90 ITU-T Recommendation V.90, "A digital modem and analogue modem pair for use on the Public Switched Telephone Network (PSTN) at data signalling rates of up to 56 000 bit/s downstream and up to 33 600 bit/s upstream," Geneva, Switzerland, September 1998.

V.92 ITU-T Recommendation V.92, "Enhancements to Recommendation V.90," November 2000.

V.120 ITU-T Recommendation V.120, "Support by an ISDN of data terminal equipment with V-series type interfaces with provision for statistical multiplexing," October 1996.

V.150.1 ITU-T Recommendation V.150.1, "Modem-over-IP networks: Procedures for the end-to-end connection of V-series DCEs," Geneva, Switzerland, January 2003.

ITU-T Recommendation V.150.1, Amendment 1, Geneva, Switzerland, January 2005.

X.21 ITU-T Recommendation X.21, "Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for synchronous operation on public data networks," September 1992.

X.731 ITU-T Recommendation X.731, "Information technology – Open Systems Interconnection – Systems management: State management function," Geneva, Switzerland, January 1992.

X.805 ITU-T Recommendation X.805, "Security architecture for systems providing end-to-end communications," Geneva, Switzerland, October 2003.

Y.1540 ITU-T Recommendation Y.1540, "Internet protocol data communication service - IP packet transfer and availability performance parameters," November 2007.

Y.1541 ITU-T Recommendation Y.1541, "Network performance objectives for IP-based services," Geneva, Switzerland, February 2006.

## A4.15 INTERNET ENGINEERING TASK FORCE REQUESTS FOR COMMENT

RFC 125 J. McConnell, "Proposal for Network Standard Format for a Graphic Data Stream," April 1971.

RFC 233 A. Bhushan and B. Metcalfe, "Standardization of Host Call Letters," September 1971.

RFC 768 Postel, J., "User Datagram Protocol," August 1980.

RFC 791 Information Services Institute, "Internet Protocol," September 1981.

RFC 793 Information Services Institute, "Transmission Control Protocol," September 1981.

RFC 1046 Prue, W. and J. Postel, "A Queuing Algorithm to Provide Type-of-Service for IP Links," February 1988.

RFC 1142 Oran, D., Ed., "OSI IS-IS Intra-domain Routing Protocol," February 1990.

RFC 1157 Case, J., M. Fedor, M. Schoffstall, and J. Davin, "A Simple Network Management Protocol (SNMP)," May 1990.

RFC 1195 R. Callon, "A Use of OSI IS-IS for Routing in TCP/IP and Dual Environments," December 1990.

RFC 1213 McCloghrie, K. and M. Rose, Eds., "Management Information Base for Network Management of TCP/IP-based internets: MIB-II," March 1991.

RFC 1215 Rose, M., Ed., "A Convention for Defining Traps for use with SNMP," March 1991.

RFC 1256 Deering, S., Ed., "ICMP Router Discovery Messages," September 1991.

RFC 1215 Rose, M., Ed., "A Convention for Defining Traps for use with SNMP," March 1991.

RFC 1305 Mills, D., "Network Time Protocol (Version 3) Specification, Implementation and Analysis," March 1992.

RFC 1332 McGregor, G., "The PPP Internet Protocol Control Protocol," May 1992.

RFC 1471 Kastenholz, F., "The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol," June 1993.

RFC 1472 Kastenholz, F., "The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol," June 1993.

RFC 1473 Kastenholz, F., "The Definitions of Managed Objects for IP Network Control Protocol of the Point-to-Point Protocol," June 1993.

RFC 1519 Fuller, V., Li, T., Yu, J., and K. Varadhan, "Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy," September 1993.

RFC 1570 Simpson, W., Ed., "PPP LCP Extensions," January 1994.

RFC 1629 Colella, R., R. Callon, E. Gardner, and Y. Rekhter, "Guidelines for OSI NSAP Allocation in the Internet," May 1994.

RFC 1657 Willis, S., Burruss, J., and J. Chu, "Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2," July 1994.

RFC 1662 Simpson, W., Ed., "PPP in HDLC-like Framing," July 1994.

RFC 1772 Rekhter, Y., P. Gross, "Application of the Border Gateway Protocol in the Internet," March 1995.

RFC 1812 Baker, F., Ed., "Requirements for IP Version 4 Routers," June 1995.

RFC 1883 Deering, S., R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," December 1995.

RFC 1918 Rekhter, Y., B. Moskowitz, D. Karrenberg, G. J. De Groot, and E. Lear, "Address Allocation for Private Internets," February 1996.

RFC 1981 McCann, J., S. Deering, and J. Mogul, "Path MTU Discovery for IP Version 6," August 1996.

RFC 1989 Simpson, W., "PPP Link Quality Monitoring," August 1996.

RFC 1990 K. Sklower, B. Loyd, et al, "The PPP Multilink Protocol (MP)," August 1996.

RFC 1994 Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)," August 1996.

RFC 1997 Chandra, R., P. Traina, and T. Li, "BGP Communities Attribute," August 1996.

RFC 2006 Dong, D., Hamlen, M., and C. Perkins, "The Definitions of Managed Objects for IP Mobility Support using SMIv2," October 1996.

RFC 2032 Turletti, T. and C. Huitema, "RTP Payload Format for H.261 Video Streams," October 1996.

RFC 2119 Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.

RFC 2126 Pouffary, Y. and A. Young, "ISO Transport Service on top of TCP (ITOT)," March 1997.

RFC 2131 Droms, R., "Dynamic Host Configuration Protocol," March 1997.

RFC 2132 Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions," March 1997.

RFC 2190 Zhu, C., "Payload Format for H.263 Video Streams," September 1997.

RFC 2198 Perkins, C, I. Kouvelas, O. Hodson, V. Hardman, M. Handley, J.C. Bolot, A. Vega-Garcia, and S. Fosse-Parisis, "RTP Payload for Redundant Audio Data," September 1997.

RFC 2205 Braden, R., Ed., L. Zhang, S. Berson, S. Herzog, and S. Jamin, "ReSerVation Protocol (RSVP)–Version 1 Functional Specification," September 1997.

RFC 2206 Baker, F., J. Krawczyk, and A. Sastry, "RSVP Management Information Base using SMIv2," September 1997.

RFC 2207 Berger, L. and T. O'Malley, "RSVP Extensions for IPSEC Data Flows," September 1997.

RFC 2210 Wroclawski, J., "The Use of RSVP with IETF Integrated Services," September 1997.

RFC 2211 Wroclawski, J., "Specification of the Controlled-Load Network Element Service," September 1997.

RFC 2212 Shenker, S., C. Partridge, and R. Guerin, "Specification of Guaranteed Quality of Service," September 1997.

RFC 2215 Shenker, S. and J. Wroclawski, "General Characterization Parameters for Integrated Service Network Elements," September 1997.

RFC 2251 Lightweight Directory Access Protocol (V3)

RFC 2252 Lightweight Directory Access Protocol (V3): Attribute Syntax Definitions

RFC 2253 Lightweight Directory Access Protocol (V3): UTF-8 String Representation of Distinguished Names

RFC 2254 The String Representation of LDAP Search Filters

RFC 2255 The LDAP URL Format

RFC 2256 A Summary of the X.500(96) User Schema for use with LDAPv3

RFC 2327 Handley, M. and V. Jacobson, "SDP: Session Description Protocol," April 1998.

RFC 2328 Moy, J., "OSPF Version 2," April 1998.

RFC 2332 Luciani, J., Katz, D., Piscitello, D., Cole, B., and N. Doraswamy, "NBMA Next Hop Resolution Protocol (NHRP)," April 1998.

RFC 2362 Estrin, D., D. Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P. Sharma, and L. Wei, "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification," June 1998.

RFC 2365 Meyer, D., "Administratively Scoped IP Multicast," July 1998.

RFC 2385 Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option," August 1998.

RFC 2401 Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol," November 1998.

RFC 2404 Madson, C. and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH," November 1998.

RFC 2407 Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP," November 1998.

RFC 2408 Maughan, D., M. Schertler, M. Schneider and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)," November 1998.

RFC 2409 Harkins, J. and D. Carrel, "The Internet Key Exchange (IKE)," November 1998.

RFC 2427 Brown, C. and A. Malis, "Multiprotocol Interconnect over Frame Relay," September 1998.

RFC 2429 Bormann, C., L. Cline, G. Deisher, T. Gardos, C. Maciocco, D. Newell, J. Ott, G. Sullivan, S. Wenger and C. Zhu, "RTP Payload Format for the 1998 Version of ITU-T Rec. H.263 Video (H.263+)," October 1998.

RFC 2439 Villamizar, C., R. Chandra, and R. Govindan, "BGP Route Flap Damping," November 1998.

RFC 2460 Deering S. and R. Hinden, "Internet Protocol Version 6 (IPv6) Specification," December 1998.

RFC 2461 Narten, T., E. Nordmark, and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)," December 1998.

RFC 2462 Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration," December 1998.

RFC 2464 Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks," December 1998.

RFC 2472 Haskin, D. and E. Allen, "IP Version 6 over PPP," December 1998.

RFC 2473 Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification," December 1998.

RFC 2474 Nichols, K., S. Blake, F. Baker, and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers," December 1998.

RFC 2475 Blake, S., D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "An Architecture for Differentiated Services," December 1998.

RFC 2507 Degermark, M., Nordgren, B., and S. Pink, "IP Header Compression," February 1999.

RFC 2508 Casner, S. and V. Jacobson, "Compressing IP/UDP/RTP Headers for Low-Speed Serial Links," February 1999.

RFC 2543 Handley, M., H. Schulzrinne, E. Schooler, J. Rosenberg, "SIP: Session Initiation Protocol," March 1999.

RFC 2544 Bradner, S. and J. McQuaid, "Benchmarking Methodology for Network Interconnect Devices," March 1999.

RFC 2545 Marques, P. and F. Dupont, "Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing," March 1999.

RFC 2547 Rosen, E. and Y. Rekhter, "BGP/MPLS VPNs," March 1999.

RFC 2560 Myers, M., Ankney, R., Malpani, A., Galperin, S. and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP," June 1999.

RFC 2578 McCloghrie, K., D. Perkins, and J. Schoenwaelder, "Structure of Management Information Version 2 (SMIv2)," April 1999.

RFC 2579 McCloghrie, K., D. Perkins, and J. Schoenwaelder, "Textual Conventions for SMIv2," April 1999.

RFC 2580 McCloghrie, K., D. Perkins, and J. Schoenwaelder, "Conformance Statements for SMIv2," April 1999.

RFC 2581 Allman, M., Paxson, V. and W. Stevens, "TCP Congestion Control," April 1999.

RFC 2597 Heinanen, J., F. Baker, W. Weiss, and J. Wroclawski, "Assured Forwarding PHB Group," June 1999.

RFC 2598 Jacobson, V., Nichols, K. and K. Poduri, "An Expedited Forwarding PHB," June 1999.

RFC 2605 Mansfield, G. and S. Kille, "Directory Server Monitoring MIB," June 1999.

RFC 2615 Malis, A. and W. Simpson, "PPP over SONET/SDH," June 1999.

RFC 2660 Rescorla, E., and A. Schiffman, "The Secure HyperText Transfer Protocol," August 1999.

RFC 2684 Grossman, D, and J. Heinanem, "Multiprotocol Encapsulation over ATM Adaptation Layer 5," September 1999.

RFC 2685 Fox, B., B. Gleeson, "Virtual Private Networks Identifier," September 1999.

RFC 2702 Awduche, D., J. Malcolm, J. Agogbua, M. O'Dell, and J. McManus, "Requirements for Traffic Engineering Over MPLS," September 1999.

RFC 2710 Deering S., W. Feener, and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6," October 1999.

RFC 2711 Partridge, C. and A. Jackson, "IPv6 Router Alert Option," October 1999.

RFC 2719 L. Ong, I. Rytina, M. Garcia, H. Schwarzbauer, L. Coene, H. Lin, I. Juhasz, M. Holdredge, C. Sharp, "Architectural Framework for Signaling Transport," October 1999.

RFC 2737 McCloghrie, K. and A. Bierman, "Entity MIB (Version 2)," December 1999.

RFC 2740 Coltun, R., D. Ferguson, and J. Moy, "OSPF for IPv6," December 1999.

RFC 2747 Baker, F., Lindell, B., Talwar, M., "RSVP Cryptographic Authentication," January 2000.

RFC 2766 Tsirtsis, G. and P. Srisuresh., "Network Address Translation – Protocol Translation (NAT-PT)," February 2000.

RFC 2778 Day, M., Rosenberg, J., "A Model for Presence and Instant Messaging," February 2000.

RFC 2782 Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for Specifying the Location of Services (DNS SRV)," February 2000.

RFC 2784 Farinacci, D., T. Li, S. Hanks, D. Meyer, and P. Traina, "Generic Routing Encapsulation (GRE)," March 2000.

RFC 2787 Jewell, B., "Definitions of Managed Objects for the Virtual Router Redundancy Protocol," March 2000.

RFC 2788 Freed, N., and S. Kille, "Network Services Monitoring MIB," March 2000.

RFC 2796 Bates, T., Chandra, R., and E. Chen, "BGP Route Reflection – An Alternative to Full Mesh IBGP" April 2000.

RFC 2805 Greene, N., M. Ramalho, and B. Rosen, "Media Gateway Control Protocol Architecture and Requirements," RFC 2805, April 2000.

RFC 2818 Rescorla, E., "HTTP over TLS, May 2000.

RFC 2819 Waldbusser, S., "Remote Network Monitoring Management Information Base," May 2000.

RFC 2829 Authentication Methods for LDAP

RFC 2830 Lightweight Directory Access Protocol (V3) Extension for Transport Layer Security (TLS)

RFC 2833 Schulzrinne, H. and S. Petrack, "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals," May 2000.

RFC 2858 Bates, T., Y. Rekhter, R. Chandra, and D. Katz, "Multiprotocol Extensions for BGP-4," June 2000.

RFC 2863 McCloghrie, K. and F. Kastenholz, "The Interface Group MIB," June 2000.

RFC 2865 Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)," June 2000.

RFC 2866 Rigney, C., "RADIUS Accounting," June 2000.

RFC 2917 Muthukrishnan, K. and A. Malis, "A Core MPLS IP VPN Architecture," September 2000.

RFC 2918 Chen, E., "Route Refresh Capability for BGP-4," September 2000.

RFC 2961 Berge, L., Gan, D., Swallow, G., Pan, P., Tommasi, F., Molendini, S., "RSVP Refresh Overhead Reduction Extensions," April 2001.

RFC 2973 Balay, R., Katz, D., Parker, J., "IS-IS Mesh Groups," October 2000.

RFC 3031 Rosen, E., A. Viswanathan, and R. Callon, "Multiprotocol Label Switching Architecture," January 2001.

RFC 3032 Rosen, E., D. Tappan, G. Fedorkow, Y. Rekter, D. Farinacci, T. Li, and A. Conta, "MPLS Label Stack Encoding," January 2001.

RFC 3036 Andersson, L., P. Doolan, N. Feldman, A. Fredette, and B. Thomas, "LDP Specification," January 2001.

RFC 3037 Thomas, B. and E. Gray, "LDP Applicability," January 2001.

RFC 3041 Narten, T. and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6," January 2001.

RFC 3053 Durand, A., P. Fasano, I. Guardini, and D. Lento, "IPv6 Tunnel Broker," January 2001.

RFC 3060 Moore, B., Ellesson, E., Strassner, J., and A. Westerinen, "Policy Core Information Model – Version 1 Specification," February 2001.

RFC 3086 Nichols, K. and B. Carpenter, "Definition of Differentiated Services Per Domain Behaviors and Rules for their Specification," April 2001.

RFC 3097 Braden, R. and L. Zhang, "RSVP Cryptographic Authentication – Updated Message Type Value," April 2001.

RFC 3107 Rekhter, Y. and E. Rosen, "Carrying Label Information in BGP-4," May 2001.

RFC 3140 Black, D., S. Brim, B. Carpenter, and F. Le Faucheur, "Per Hop Behavior Identification Codes," June 2001.

RFC 3162 Aboba, B., G. Zorn, and D. Mitton, "RADIUS and IPv6," August 2001.

RFC 3164 Lonvick, C., "The BSD syslog Protocol" August 2001.

RFC 3168 Ramakrishnan, K., Floyd, S., and D. Black, "RADIUS and IPv6," September 2001.

RFC 3173 Shacham, A., Monsour, B., Pereira, R., and M. Thomas, "IP Payload Compression Protocol (IPComp)," September 2001.

RFC 3181 Herzog, S., "Signaled Preemption Priority Policy Element," October 2001.

RFC 3195 New, D. and M. Rose, "Reliable Delivery for syslog," November 2001.

RFC 3204 Zimmerer, E., J. Peterson, A. Vemuri, L. Ong, F. Audet, M., Watson, and M. Zonoun, "MIME media types for ISUP and QSIG Objects," December 2001.

RFC 3209 Awduche, D., L. Berger, D. Gan, T. Li, V. Srinivasan, and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels," December 2001.

RFC 3210 Awduche, D., A. Hannan, and X. Xiao, "Applicability Statement for Extensions to RSVP for LSP-Tunnels," December 2001.

RFC 3246 Davie, B., A. Charny, J.C.R. Bennett, K. Benson, J.Y. Le Boudec, W. Courtney, S. Davari, V. Firoiu, and D. Stiliadis, "An Expedited Forwarding PHB (Per-Hop Behavior)," March 2002.

RFC 3260 Grossman, D., "New Terminology and Clarification for Diffserv," April 2002.

RFC 3261 Rosenberg, J., H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and R. Schooler, "SIP: Session Initiation Protocol," June 2002.

RFC 3262 Rosenberg, J. and H. Schulzrinne, "Reliability of Provisional Responses in Session Initiation Protocol (SIP)," June 2002.

RFC 3264 Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with the Session Description Protocol (SDP)," June 2002.

RFC 3265 Roach, A. B., "Session Initiation Protocol (SIP)-Specific Event Notification," June 2002.

RFC 3266 Olson, S., G. Camarillo, and A. B. Roach, "Support for IPv6 in Session Description Protocol," June 2002.

RFC 3267 Sjoberg, J., M. Westerlund, A. Lakaniemi, and Q. Xie, "Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs," June 2002.

RFC 3270 Le Faucheur, F., L. Wu, B. Davie, S. Davari, P. Vaananen, R. Krishnan, P. Cheval, and J. Heinanen, "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services," May 2002.

RFC 3273 Waldbusser, S., "Remote Network Monitoring Management Information Base for High Capacity Networks," July 2002.

RFC 3310 Niemi, A., J. Arkko, and V. Torvinen, "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)," September 2002.

RFC 3311 Rosenberg, J., "The Session Initiation Protocol (SIP) UPDATE Method," September 2002.

RFC 3312 Camarillo, G., W. Marshall, and J. Rosenberg, "Integration of Resource Management and Session Initiation Protocol (SIP)," October 2002.

RFC 3315 Droms, E., J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," July 2003.

RFC 3323 Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)," November 2002.

RFC 3325 Jennings, C., J. Peterson, and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks," November 2002.

RFC 3326 Schulzrinne, H., D. Oran, and G. Camarillo, "The Reason Header Field for the Session Initiation Protocol (SIP)," December 2002.

RFC 3329 Arkko, J., V. Torvinen, G. Camarillo, A. Niemi, and T. Haukka, "Security Mechanism Agreement for the Session Initiation Protocol (SIP)," January 2003.

RFC 3331 Morneault, K., R. Dantu, G. Sidebottom, B. Bidulock, and J. Heitz, "Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) – User Adaptation Layer," September 2002.

RFC 3344 Perkins, C., "IP Mobility Support for IPv4," August 2002.

RFC 3345 McPherson, D., Gill, V, Walton, D., and A. Retana, "Border Gateway Protocol (MGP) Persistent Route Oscillation Condition," August 2002.

RFC 3359 Przygienda, T., "Reserved Type, Length and Value (TLV) codepoints in Intermediate System to Intermediate System" August 2002.

RFC 3366 Fairhurst, G., and L. Wood, "Advice to link designers on link Automatic Repeat reQuest (ARQ)," August 2002.

RFC 3376 Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3," October 2002.

RFC 3392 Chandra, R. and J. Scudder, "Capabilities Advertisement with BGP-4", November 2002.

RFC 3393 Demichelis, C. and P. Chimento, "IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)", November 2002.

RFC 3398 Camarillo, G., A. B. Roach, J. Peterson, and L. Ong, "Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping," December 2002.

RFC 3410 Case, J., R. Mundy, D. Partain, and B. Stewart, "Introduction and Applicability Statements for Internet Standard Management Framework," December 2002.

RFC 3411 Harrington, D., R. Presuhn, and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks," December 2002.

RFC 3412 Case, J., D. Harrington, R. Presuhn, and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)," December 2002.

RFC 3413 Levi, D., P. Meyer, and B. Stewart, "Simple Network Management Protocol (SNMP) Applications," December 2002.

RFC 3414 Blumenthal, U., and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)," December 2002.

RFC 3415 Wijnen, B., R. Presuhn, and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)," December 2002.

RFC 3416 Presuhn, R., Ed., J. Case, K. McCloghrie, M. Rose, and S. Waldbusser, "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)," December 2002.

RFC 3417 Presuhn, R., Ed., J. Case, K. McCloghrie, M. Rose, and S. Waldbusser, "Transport Mappings for the Simple Network Management Protocol (SNMP)," December 2002.

RFC 3418 Presuhn, R., Ed., J. Case, K. McCloghrie, M. Rose, and S. Waldbusser, "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)," December 2002.

RFC 3443 Agarwal, P. and B. Akyol, "Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks," January 2003.

RFC 3446 Kim, D., Meyer, D., Kilmer, H., and D. Farinacci, "Anycast Rendevous Point (RP) Mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)," January 2003.

RFC 3455 Garcia-Martin, M., E. Henrikson, and D. Mills, "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)," January 2003.

RFC 3471 Berger, L., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description," January 2003.

RFC 3473 Berger, L., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions," January 2003.

RFC 3478 Leelanivas, M., Y. Rekhter, and R. Aggarwal, "Graceful Restart Mechanism for Label Distribution Protocol," February 2003.

RFC 3479 Farrel, A., Ed., "Fault Tolerance for the Label Distribution Protocol (LDP)," February 2003.

RFC 3484 Draves, R., "Default Address Selection for Internet Protocol Version 6 (IPv6)," February 2003.

RFC 3486 Camarillo, G., "Compressing the Session Initiation Protocol (SIP)," February 2003.

RFC 3515 Sparks, R., "The Session Initiation Protocol (SIP) Refer Method," April 2003.

RFC 3539 Aboda, B. and J. Wood, "Authentication, Authorization and Accounting (AAA) Transport Profile," June 2003.

RFC 3544 Koren, T., Casner, S., and C. Bormann, "IP Header Compression over PPP," July 2003.

RFC 3550 Schulzrinne, H., S. Casner, R. Frederick, and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications," July 2003.

RFC 3564 Le Faucheur, F. and W. Lai, "Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering," July 2003.

RFC 3569 Bhattacharyya, S., "An Overview of Source-Specific Multicast (SSM)," July 2003.

RFC 3579 Aboda, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support for Extensible Authentication Protocol (EAP)," September 2003.

RFC 3581 Rosenberg, J. and H. Schulzrinne, "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing," August 2003.

RFC 3584 Frye, R., D. Levi, S. Routhier, and B. Wijnen, "Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework," August 2003.

RFC 3585 Jason, J., Rafalow, L., and E. Vyncke, "IPsec Configuration Policy Information Model," August 2003.

RFC 3586 Blaze, M., Keromytis, A., Richardson, M., and L. Sanchez, "IP Security Policy (IPSP) Requirements," August 2003.

RFC 3588 Calhoun, P., Loughney, J. Guttman, E., Zorn, G. and J. Arkko, "Diameter Base Protocol," September 2003.

RFC 3595 Wijnen, B., "Textual Conventions for IPv6 Flow Label," September 2003.

RFC 3596 Thomson, S., C. Huitema, V. Ksinant, and M. Souissi, "DNS Extensions to Support IPv6," October 2003.

RFC 3603 Marshall, W. and F. Andreasen, "Private Session Initiation Protocol (SIP) Proxy-to-Proxy Extensions for Supporting the PacketCable Distributed Call Signaling Architecture," October 2003.

RFC 3608 Willis, D., and B. Hoeneisen, "Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration," October 2003.

RFC 3611 Friedman, T., Caceres, R., and A. Clark, "RTP Control Protocol Extended Reports (RTCP XR)," November 2003.

RFC 3618 Fenner, B. and D. Meyer, "Multicast Source Discovery Protocol (MSDP)," October 2003.

RFC 3618 Fenner, B. and D. Meyer, "Multicast Source Discovery Protocol (MSDP)," October 2003.

RFC 3623 Moy, J., Pillay-Esnault, F., and A. Lindem, "Graceful OSPF Restart," November 2003.

RFC 3644 Snir, Y., Ramberg, Y. Strassner, J. Cohen, R., and B. Moore, "Policy quality of Service (Qos) Information Model," November 2003.

RFC 3647 Chokhani, S., W. Ford, R. Sabett, C. Merrill, and S. Wu, "Internet X.509 Public Key Infrastructure Certification Policy and Certification Practices Framework," November 2003.

RFC 3662 Bless, R., K. Nichols, and K. Wehrle, "A Lower Effort Per-Domain Behavior (PDB) for Differentiated Services," December 2003.

RFC 3670 Moore, B., D. Durham, J. Strassner, A. Westerinen, and W. Weiss, "Information Model for Describing Network Device QoS Datapath Mechanism," January 2004.

RFC 3711 Baugher, M., D. McGrew, M. Naslund, E. Carrara, and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)," March 2004.

RFC 3725 Rosenberg, J., Peterson, J., Schulzrinne, H., and G. Camarillo, "Best Current Practices for Third Party Call Control (3pcc) in the Session initiation Protocol (SIP)," March 2004.

RFC 3748 Aboba, B., Blunk, L, Vollbrecht, J. Carlson, J. and H. Levkowetz, Ed., "Extensible Authentication Protocol IEAP)," June 2004.

RFC 3764 Person, J., "enumservice registration for Session initiation Protocol (SIP) Addresses-of-Record)," April 2004.

RFC 3810 Vida, R., Ed. and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6," June 2004.

RFC 3826 Blumenthal, U., F. Maino, and K. McCloghrie, "The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model," June 2004.

RFC 3840 Rosenberg, J., H. Schulzrinne, and P. Kyzivat, "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)," August 2004.

RFC 3842 Mahy, R., "A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)," August 2004.

RFC 3853 Peterson, J., "S/MIME Advanced Encryption Standard (AES) Requirements for the Session Initiation Protocol (SIP)," July 2004.

RFC 3868 Loughney, J., Ed., G. Sidebottom, L. Coene, G. Verwimp, J. Keller, and B. Bidulock, "Signalling Connection Control Part User Adaptation Layer (SUA)," October 2004.

RFC 3879 Huitema, C. and B. Carpenter, "Deprecating Site Local Addresses," September 2004.

RFC 3890 Westerlund, M., "A Transport Independent Bandwidth Modifier for the Session Description Protocol (SDP)," September 2004.

RFC 3891 Mahy, R., B. Biggs, and R. Dean, "The Session Initiation Protocol (SIP) "Replaces" Header," September 2004.

RFC 3892 Sparks, R., "The Session Initiation Protocol (SIP) Referred-By Mechanism," September 2004.

RFC 3893 Peterson, J., "Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format," September 2004.

RFC 3913 Thaler, D., "Border Gateway Multicast Protocol (BGMP)," September 2004.

RFC 3920 Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core," draft-ietf-xmpp-3920bis-17, October 6, 2010.

RFC 3921 Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence," draft-ietf-xmpp-3921bis-15, October 06, 2010.

RFC 3936 Kompella, K. and J. Lang, "Procedures for Modifying the Resource reSerVation Protocol (RSVP)," October 2004.

RFC 3948 Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and M. Stenberg, "UDP Encapsulation of IPsec ESP Packets," January 2005.

RFC 3966 Schulzrinne, H., "The tel URI for Telephone Numbers," December 2004.

RFC 3968 Camarillo, G., "The Internet Assigned Number Authority (IANA) Header Field Parameter Registry for the Session Initiation Protocol (SIP)," December 2004.

RFC 3984 Wenger, S., M. M. Hannuksela, T., Stockhammer, M. Westerlund, and D. Singer, "RTP Payload Format for H.264 Video," February 2005.

RFC 3986 Berners-Lee, T., R. Fielding, and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax," January 2005.

RFC 4003 Berger, L., "GMPLS Signaling Procedure for Egress Control," February 2005.

RFC 4007 Deering, S., B. Haberman, T. Jinmei, E. Nordmark, and B. Zill, "IPv6 Scoped Address Architecture," March 2005.

RFC 4022 Raghunarayan, R., "Management Information Base for the Transmission Control Protocol (TCP)," March 2005.

RFC 4028 Donovan, B., and J. Rosenberg, "Session Timers in the Session Initiation Protocol (SIP)," April 2005.

RFC 4040 Kreuter, R., "RTP Payload Format for a 64 kbit/s Transparent Call," April 2005.

RFC 4040 Kreuter, R., "RTP Payload Format for a 64 kbit/s Transparent Call," April 2005.

RFC 4044 McGloghrie, K., "Fibre Channel Management MIB," May 2005.

RFC 4087 Thaler, D., "IP Tunnel MIB," June 2005.

RFC 4090 Pan, P., Ed., G. Swallow, Ed., and A. Atlas, Ed., "Fast Reroute Extensions to RSVP-TE for LSP Tunnels," May 2005.

RFC 4091 Camarillo, G. and J. Rosenburg, "The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework," June 2005.

RFC 4092 Camarillo, G. and J. Rosenburg, "Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)," June 2005.

RFC 4108 Housley, R., "Using Cryptographic Message Syntax (CMS) to Protect Firmware Packages," August 2005.

RFC 4109 Hoffman, P., "Algorithms for Internet Key Exchange Version 1 (IKEv1)," May 2005.

RFC 4113 Fenner, B. and J. Flick, "Management Information Base for the User Datagram Protocol (UDP)," June 2005.

RFC 4120 Neuman, C., T. Yu, S. Hartman, and K. Raeburn, "The Kerberos Network Authentication Service (V5)," July 2005.

RFC 4122 Leach, P., Mealling, M. and R. Salz, "A Universally Unique Identifier (UUID) URN Namespace," July 2005.

RFC 4123 Schulzrinne, H., "Session Initiation Protocol (SIP)-H.323 Internetworking Requriements," July 2005.

RFC 4124 Faucheur, F., "Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering," June 2005.

RFC 4165 George, T., B. Bidulock, R. Dantu, H. Schwarzbauer, and K. Morneault, "Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) – User Peer-to-Peer Adaptation Layer (M2PA)," September 2005.

RFC 4171 Tseng, J., K. Gibbons, F. Travostino, C. Du Laney, and J. Souza, "Internet Storage Name Service (iSNS)," September 2005.

RFC 4176 El Mghazli, Y., Ed., T. Nadeau, M. Boucadair, K. Chan, AND A. Gonguet, "Framework for Layer 3 Virtual Private Networks (L3VPN) Operations and Management," October 2005.

RFC 4182 Rosen, E., "Removing a Restriction on the use of MPLS Explicit NULL," September 2005.

RFC 4191 Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes," November 2005.

RFC 4193 Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses," October 2005.

RFC 4201 Kompella, K., Y. Rekhter, and L. Berger, "Link Bundling in MPLS Traffic Engineering (TE)," October 2005.

RFC 4204 Lang, J., "Link Management Protocol (LMP)," October 2005.

RFC 4206 Kompella, K. and Y. Rekhter, "Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)," October 2005.

RFC 4213 Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers," October 2005.

RFC 4233 Morneault, K., S. Rengasami, M. Kalla, and G. Sidebottom, "Integrated Services Digital Network (ISDN) Q.921-User Adaptation Layer," January 2006.

RFC 4244 Barnes, M., Ed., "An Extension to the Session Initiation Protocol (SIP) for Request History Information, November 2005.

RFC 4251 Ylonen, T., and C. Lonvick, Ed., "The Secure Shell (SSH) Protocol Architecture," January 2006.

RFC 4252 Ylonen, T., and C. Lonvick, Ed., "The Secure Shell (SSH) Authentication Protocol," January 2006.

RFC 4253 Ylonen, T., and C. Lonvick, Ed., "The Secure Shell (SSH) Transport Layer Protocol," January 2006.

RFC 4254 Ylonen, T., and C. Lonvick, Ed., "The Secure Shell (SSH) Connection Protocol," January 2006.

RFC 4271 Rekhter, Y., T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)," January 2006.

RFC 4282 Aboba, B., M. Beadles, J. Arkk and P. Eronen, "The Network Access Identifier," December 2005.

RFC 4291 Hinden, R. and S. Deering, “IP Version 6 Addressing Architecture,” February 2006.

RFC 4292 Haberman, B., “IP Forwarding Table MIB,” April 2006.

RFC 4293 Routhier, S., “Management Information Base for the Internet Protocol (IP),” April 2006.

RFC 4294 Loughney, E., “IPv6 Node Requirements,” April 2006.

RFC 4301 Kent, S. and K. Seo, “Security Architecture for the Internet Protocol,” December 2005.

RFC 4302 Kent, S., “IP Authentication Header,” December 2005.

RFC 4303 Kent, S., “IP Encapsulating Security Payload (ESP),” December 2005.

RFC 4305 Eastlake, D., “Cryptographic Algorithm Implementation Requirements for the Encapsulating Security Payload (ESP) and Authentication Header (AH),” December 2005.

RFC 4306 Kaufman, E., “Internet Key Exchange (IKEv2) Protocol,” December 2005.

RFC 4307 Schiller, J., "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2),” December 2005.

RFC 4308 Hoffman, P., “Cryptographic Suites for IPSec,” December 2005.

RFC 4309 Housley, R., “Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP),” December 2005.

RFC 4320 Sparks, R., “Action Addressing Identified Issues with the Session Initiation

RFC 4328 Papadimitriou, D., Ed., “Generalized Multi-Protocol Label Switching (GMPLS) Signaling Extensions for G.709 Optical Transport Networks Control,” January 2006.

RFC 4338 DeSanti, C., Carlson, C., and R. Nixon., “Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel,” January 2006.

RFC 4344 Bellare, M., Kohno, T., and C. Namprempre., "The Secure Shell (SSH) Transport Layer Encryption Modes," January 2006.

RFC 4360 Sangli, S., Tappan, D., and Y. Rekhter, "BGP/Extended Communities Attribute," February 2006.

RFC 4362 Jonsson, L-E, Pelletier, G., and K. Sandlund, "RObust Header Compression (ROHC): A Link-Layer Assisted Profile for IP/UDP/RTP," February 2006. (Replaces RFC 2547)

RFC 4364 Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)," February 2006. (Replaces RFC 2547)

RFC 4379 Kompella, K. and G. Swallow, "Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures," February 2006.

RFC 4382 Nadeau, T., Ed., and H. van der Linde, Ed., "MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base," February 2006.

RFC 4411 Polk, J., "Extending the Session Initiation Protocol (SIP) Reason Header for Preemption Events," February 2006.

RFC 4412 Schulzrinne, H. and J. Polk, "Communications Resource Priority for the Session Initiation Protocol (SIP)," February 2006.

RFC 4420 Farrel, A., Ed., D. Papadimitriou, J.P. Vasseur, and A. Ayyangar, "Encoding of Attributes for Multiprotocol Label Switching (MPLS) Label Switched Path (LSP) Establishment Using Resource ReserVation Protocol-Traffic Engineering (RSVP-TE)," February 2006.

RFC 4422 Melnikov, E., Zeilenga, E., "Simple Authentication and Security layer (SASL)," June 2006.

RFC 4443 Conta, A., S. Deering, and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification," March 2006.

RFC 4447 Martini, L., Ed., E. Rosen, N. El-Aawar, T. Smith, and G. Heron, "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)," April 2006.

RFC 4448 Martini, L., Ed., E. Rosen, N. El-Aawar, and G. Heron, "Encapsulation Methods for Transport of Ethernet over MPLS Networks," April 2006.

RFC 4456 Bates, T., Chen, E., "BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)," April 2006.

RFC 4502 Waldbusser, S., "Remote Network Monitoring Management Information Base Version 2," May 2006.

RFC 4510 Zeilenga, E., "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map," June 2006.

RFC 4511 Sermersheim, J., "Lightweight Directory Access Protocol (LDAP): The Protocol," June 2006.

RFC 4552 Gupta, M. and N. Melam, "Authentication/Confidentiality for OSPFV3," June 2006.

RFC 4566 Handley, M., V. Jacobson, and C. Perkins, "SDP: Session Description Protocol," July 2006.

RFC 4568 Andreasen, F., M. Baugher, and D. Wing, "Session Description Protocol (SDP) Security Descriptions for Media Streams," July 2006.

RFC 4573 Even, R., and A. Lochbaum, "MIME Type Registration for RTP Payload Format for H.224," July 2006.

RFC 4574 Levin, O., and G. Camarillo, "Session Description Protocol (SDP) Label Attribute," August 2006.

RFC 4575 Rosenberg, J., Schulzrinne, H., and O. Levin, "A Session Initiation Protocol (SIP) Event Package for Conference State," August 2006.

RFC 4577 Rosen, E., Psenak, P., and P. Pillay-Esnault, "OSPF as the Provided/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)," June 2006.

RFC 4579 Johnston, A. and O. Levin, "Session Initiation Protocol (SIP) Call Control – Conferencing for User Agents," August 2006.

RFC 4582 Camarillo, G., J. Ott, and K. Drage, "The Binary Floor Control Protocol (BFCP)," November 2006.

RFC 4583 Camarillo, G., "Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams," November 2006.

RFC 4585 Ott, J., S. Wenger, N. Sato, C. Burmeister, and J. Rey, "Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF), July 2006.

RFC 4601 Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast – Sparse Mode (PIM-SM): Protocol Specification (Revised)," August 2006.

RFC 4604 Holbrook, H., Haberman, B. and B. Cain, "Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery protocol Version 2 (MLDv2) for Source-Specific Multicast," August 2006.

RFC 4607 Holbrook, H. and B. Cain, "Source-Specific Multicast for IP," August 2006.

RFC 4616 Zeilenga, K., "The PLAIN Simple Authentication and Security Layer (SASL) Mechanism," August 2006.

RFC 4659 De Clercq, J., D. Ooms, M. Carugi, and F. Le Faucheur, "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN," September 2006.

RFC 4666 Morneault, K., Ed., and J. Pastor-Balbas, Ed., "Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) – User Adaptation Layer (M3UA)," September 2006.

RFC 4684 Marques, P., R. Bonica, L. Fang, L. Martini, R. Raszuk, K. Patel, and J. Guichard, "Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)," November 2006.

RFC 4724 Sangli, S., Chen, E., Fernando, R., Scudder, J., Rekhter, Y., "Graceful Restart Mechanism for BGP," January 2007.

RFC 4730 Burger, E. and M. Dolly, "A Session Initiation Protocol (SIP) Event Package for Key Press Stimulus (KPML)," November 2006.

RFC 4733 Schulzrinne, H. and T. Taylor, "RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals," December 2006.

RFC 4750 Joyal, D., Galecki, P., and S. Giacalone, "OSPF Version 2 Management Information Base," December 2006.

RFC 4760 Bates, T., R. Chandra, D. Katz and Y. Rekhter, "Multiprotocol Extensions for BGP-4," January 2007.

RFC 4761 Kompella, K., Ed. and Y. Rekhter, Ed., "Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling," January 2007. (Updated by RFC 5462).

RFC 4762 Lasserre, M., Ed. and V. Kompella, Ed., "Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling," January 2007.

RFC 4783 Berger, L., Ed., "GMPLS – Communication of Alarm Information," December 2006.

RFC 4796 Hautakorpi, J. and G. Camarillo, "The Session Description Protocol (SDP) Content Attribute," February 2007.

RFC 4807 Baer, M., R. Charlet, W. Hardaker and R. Story, "IPSec Security Policy Dtabase Configuration MIB," March 2007.RFC 4835Manral, V., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)," April 2007.

RFC 4835 Manral, V., "Cryptographic Algorithm Implementation Requirements for Encapsulating Secruity Payload (ESP) and Authentication Header (AH)," April 2007.

RFC 4861 Narten, T., E. Nordmark, W. Simpson, and H. Soliman, "Neighbor Discovery for IP Version 6 (IPv6)," September 2007.

RFC 4862 Thomson, S., T. Narten, and T. Jinmei, "IPv6 Stateless Address Autoconfiguration," September 2007.

RFC 4864 Van de Velde, G., Hain, T., Droms, R., Carpenter, B., and E. Klein, "Local Network Protection for IPv6," May 2007.

RFC 4867 Sjoberg, J., Westerlund, M., Lakaniemi, A., and Q. Xie, "RTP Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs," April 2007.

RFC 4869 Law, L. and J. Solinas, "Suite B Cryptographic Suites for IPsec," May 2007.

RFC 4872 Lang, J.P., Ed., Y. Rekhter, Ed., and D. Papadimitriou, Ed., "RSVP-TE Extensions in Support of End-to-End Generalized Multi-Protocol Label Switching (GMPLS) Recovery," May 2007.

RFC 4873 Berger, L., I. Bryskin, D. Papadimitriou, and A. Farrel, "GMPLS Segment Recovery," May 2007.

RFC 4874 Lee, C.Y., A. Farrel, and S. De Cnodder, "Exclude Routes – Extension to Resource ReserVation Protocol-Traffic Engineering (RSVP-TE)," April 2007.

RFC 4904 Gurbani, V. and C. Jennings, "Representing Trunk Groups in tel/sip Uniform Resource Identifiers (URIs)," June 2007.

RFC 4918 Dusseault, L., Ed., "HTTP Extensions for Web Distributed Authoring and Versioning (WebDAV)," June 2007.

RFC 4940 Kompella, K. and B. Fenner, "IANA Considerations for OSPF," June 2007.

RFC 4941 Narten, T., R. Draves, and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6," September 2007.

RFC 4960 Stewart, E., "Stream Control Transmission Protocol," September 2007.

RFC 4966 Aoun, C. and E. Devies, "Reasons to Move the Network Address Translator – Protocol Translator (NAT-PT) to Historic Status," July 2007.

RFC 4974 Papadimitriou, D. and A. Farrel, "Generalized MPLS (GMPLS) RSVP-TE Signaling Extensions in Support of Calls," August 2007.

RFC 5036 Andersson, L, Minei, I., and R. Thomas, "LDP Specification," October 2007.

RFC 5059 Bhaskar, N., Gall, A., Lingard, J., and S. Venaas, "Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)," January 2008.

RFC 5063 Satyanarayana, A., Ed. and R. Rahman, Ed., "Extensions to GMPLS Resource Reservation Protocol (RSVP) Graceful Restart," October 2007.

RFC 5065 Traina, P., McPherson, D. and J. Scudder, "Antonomous System Confederations for BGP," August 2007.

RFC 5072 Varada, S., "IP Version 6 over PPP," September 2007.

RFC 5095 Abley, J., P. Savola, and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6," December 2007.

RFC 5104 Wenger, S., U. Chandra, M. Westerlund, and B. Burman, "Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF)," February 2008.

RFC 5129 Davie, B., B. Briscoe, and J. Tay, "Explicit Congestion Marking in MPLS," January 2008.

RFC 5151 Farrel, A., Ed., A. Ayyangar, and J.P. Vasseur, "Inter-Domain MPLS and GMPLS Traffic Engineering – Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions," February 2008.

RFC 5184 Teraoka, F., Gogo, K., Mitsuya, K., Shibui, R., and K. Mitani, "Unified Layer 2 (L2) Abstractions for layer 3 (L3)-Driven Fast Handover," May 2008.

RFC 5246 Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," August 2008.

RFC 5301 McPherson, D. and N. Shen, "Dynamic Hostname Exchange Mechanism for IS-IS," October 2008.

RFC 5303 Katz, D., Saluja, R. and D. Eastlake, "Three-Way Handshake for IS-IS Point-to-Point Adjacencies," October 2008.

RFC 5304 Li, T. and R. Atkinson, "IS-IS Cryptographic Authentication," October 2008.

RFC 5305 Li, T., Redback Networks, Inc., H. Smit, "IS-IS Extensions for Traffic Engineering," October 2008.

RFC 5306 Shand, M., and L. Ginsberg, "Restart Signaling for IS-IS," October 2008.

RFC 5307 Kompella, K. and Y. Rekhter, "IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)," October 2008.

RFC 5308 Hopps, C., "Routing IPv6 with IS-IS," October 2008.

RFC 5309 Shen, N. and A. Zinin, "Point-to-Point Operation over LAN in Link State Routing Protocols," October 2008.

RFC 5310 Bhatia, M., Manral, V., Li, T., Atkinson, R., White, R. and M. Fanto., "IS-IS Generic Cryptographic Authentication," February 2009.

RFC 5331 Aggarwal, R., Y. Rekhter, and E. Rosen, "MPLS Upstream Label Assignment and Context-Specific Label Space," August 2008.

RFC 5332 Eckert, T., E. Rosen, Ed., R. Aggarwal, and Y. Rekhter, "MPLS Multicast Encapsulations," August 2008.

RFC 5340 Coltun, R., Ferguson, D., Moy, J. and E. Lindem, "OSPF for IPv6," July 2008.

RFC 5359 Johnston, A., Sparks, R., Cunningham, C., Donovan, S. and K. Summers, "Session Initiation Protocol Service Examples," October 2008.

RFC 5415 Calhoun, P., Montemurro, M., and D. Stanley, "Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Specification" March 2009.

RFC 5416 Calhoun, P., Montemurro, M., and D. Stanley, "Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Finding for IEEE 802.11" March 2009.

RFC 5420 Farrel, A., Ed., D. Papadimitriou, J.P. Vasseur, and A. Ayyangarps, "Encoding of Attributes for MPLS LSP Establishment Using Resource Reservation Protocol Traffic Engineering (RSVP-TE)," February 2009.

RFC 5462 Andersson L. and R. Asati, "Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field," February 2009.

RFC 5492 Scudder, J. and R. Chandra, "Capabilities Advertisement with BGP-4," February 2009.

RFC 5501 Kamite, y., Ed., Y. Wada, Y. Serbest, T. Morin, and L. Fang, "Requirements for Multicast Support in Virtual Private LAN Services," March 2009.

RFC 5626 Jennings, C., Mahy, R., and F. Audet, "Managing client-Initiated Connections in the Session initiation Protocol (SIP)," October 2009.

RFC 5746 Rescorla, E., Ray, M., Dispensa, S., and N. Oskov, "Transport Layer Security (TLS) Renegotiation Indication Extension," February 2010.

RFC 5798 Nadas, S., "Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6," March 2010.

RFC 5806 Levy, S. and M. Mohali, "Diversion Indication in SIP," March 2010.

RFC 5853 Hautakorpi, E., Camarillo, G., Penfield, R., Hawrylyshen, A., and M. Bhatia, "Requirements from Session Initiation Protocol (SIP) Session Border Control (SBC) Deployments," April 2010.

RFC 5922 Gurbani, V., Lawrence, S., and A. Jeffrey, "Domain Certificates in the Session Initiation Protocol (SIP)," June 2010.

RFC 5925 Touch, J., Mankin, A., and R. Bonica, "The TCP Authentication Option," June 2010.

RFC 5954 Gurbani, V., Carpenter, B., and B. Tate, "Essential Correction for IPv6 ABNF and URI Comparison for RFC 3261," August 2010.

RFC 6120 Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", March 2011

RFC 6121 Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence", March 2011

RFC 6122 Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Address Format", March 2011

RFC draft Harrison, J., J. Berger, M. Bartlett, Data Connection Ltd (DCL), draft-ietf-isis-ipv6-te, "IPv6 Traffic Engineering in IS-IS," September 2009, expires March 2010.

draft-saarenmaa-ssh-x509-00, http://tools.ietf.org/html/draft-saarenmaa-ssh-x509-00.

## A4.16 JOINT REQUIREMENTS OVERSIGHT COUNCIL DOCUMENTATION

JROCM 048-96 Memorandum for the Under Secretary of Defense for Acquisition and Technology, Subject: Validation of Defense Information Systems Network (DISN) Capstone Requirements Document (CRD), 15 April 1996.

JROCM 134-01 "Global Information Grid (GIG) Capabilities Requirement Document (CRD)," 30 August 2001.

JROCM 202-02 "Global Information Grid (GIG), Mission Area Initial Capabilities Document (MA ICD)," 22 November 2002.

## A4.17 NATIONAL SECURITY AGENCY DOCUMENTATION

National Security Agency, "Commercial COMSEC Endorsement Program Procedures," 31 August 1987.

National Security Agency, "Common Criteria for Protection Profile for Switches and Routers (CCPPSR)," Version 3.1, Revision 3, July 2009; unless superseded by later version that then takes precedence per http://www.niap-ccevs.org/pp/.

National Security Agency, "DoD Class 3 Public Key Infrastructure Interface Specification," Version 1.2, 10 August 2000.

National Security Agency, "INFOSEC System Security Products and Services Catalog," October 1990.

## A4.18 NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY DOCUMENTATION

National Security Telecommunications and Information System Security (NSTISS), NACSIM 5100A, "Compromising Emanations Laboratory Test Requirements, Electromagnetics."

National Security Telecommunications and Information System Security (NSTISS), "TEMPEST/1-92, Electromagnetics."

National Security Telecommunications and Information Systems Security Authority Manual (NSTISSAM), "TEMPEST/2-95, RED/Black Installation Guidance," 12 December 1995.

National Security Telecommunications and Information Systems Security Authority Manual (NSTISSAM), "Compromising Emanations Laboratory Test Requirements."

National Security Telecommunications and Information Systems Security Committee (NSTISSC), "National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, Subject: National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products," January 2000 and revised June 2003.

National Security Telecommunications and Information Systems Security Instruction, NSTISSI No. 4009, "National Information Systems Security (INFOSEC) Glossary," 5 June 1992.

National Security Telecommunications and Information Systems Security Instruction, NSTISSI No. 7000, "TEMPEST Countermeasures for Facilities," 7 October 1988.

National Security Telecommunications and Information Systems Security Policy, NSTISSP 300 "National Policy on the Control of Compromising Emanations," 3 October 1988.

## A4.19 U. S. SECURE COMMUNICATION INTEROPERABILITY PROTOCOL

SCIP-215 U.S. Secure Communication Interoperability Protocol (SCIP) over IP Implementation Standard and Minimum Essential Requirements (MER) Publication, Revision 2.1, 10 December 2009.

SCIP-216 Minimum Essential Requirements (MER) for V.150.1 Gateways Publication, Revision 2.1, 10 December 2009.

## A4.20 TELCORDIA TECHNOLOGIES DOCUMENTATION

Feature Service Description (FSD) 30-33-0000, *Release to Pivot Network Capability*.

FR-E911-1 Requirements to Support E9-1-1 Service, Issue 5, January 2007.

FR-796 Reliability and Quality Generic Requirements (RQGR), Issue 1, October 1995; Issue 2; Issue 3, March 2006; Issue 5, April 2008.

GR-63-CORE *NEBS™ Requirements: Physical Protection*, Issue 1, October 1995, Issue 2, April 2002, Issue 3, March 2006.

GR-217-CORE *LSSGR: CLASS$^{SM}$ Feature: Selective Call Forwarding (FSD-01-02-1410)*, Issue 1, June 2000; Issue 2, April 2002.

GR-246-CORE *Specification of Signalling System Number 7*, 2005/12/30.

GR-253-CORE *Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria*, December 2005.

GR-282-CORE *Software Reliability and Quality Acceptance Criteria (SRQAC)*, Issue 3, December 1996.

GR-303-CORE *Integrated Digital Loop Carrier System Generic Requirements, Objectives, and Interface*, Issue 4, December 2000.

GR-317-CORE *Switching System Generic Requirements for Call Control Using the Integrated Services Digital Network User Part (ISDNUP)*, November 2007.

GR-383-CORE *COMMON LANGUAGE® Equipment Codes (CLEI™ Codes) – Generic Requirements for Product Labels*, Issue 3, February 2006.

GR-394-CORE *Switching System Generic Requirements for Interexchange Carrier Interconnection (ICI) Using the Integrated Services Digital Network User Part (ISDNUP)*, November 2007.

GR-436-CORE *Digital Network Synchronization Plan*, Issue 1 with Revision 1, June 1996.

GR-472-CORE *Network Element Configuration Management*, Revision 2, February 1999.

GR-474-CORE OTGR Section 4: *Network Maintenance: Alarm and Control for Network Elements*, December 1997.

GR-477-CORE *Network Traffic Management*, February 2000.

GR-478-CORE *Measurements and Data Generation*, Issue 4, February 2000.

GR-496-CORE *SONET Add-Drop Multiplexer (SONET ADM) Generic Criteria*, Issue 2, August 2007.

GR-499-CORE *Transport Systems Generic Requirements (TSGR): Common Requirements*, Issue 3, September 2004.

GR-505-CORE *Call Processing*, December 1997.

GR-506-CORE *LSSGR: Signaling for Analog Interfaces*, December 2006.

GR-507-CORE *LSSGR: Transition Section 7*, January 2000.

GR-512-CORE *LSSGR: Reliability*, Section 12, January 1998.

GR-513-CORE *Module of the LSSGR, FR-64*, Issue 1, September 1995.

GR-518-CORE *LSSGR: Synchronization Section 18,* Issue 1, May 1994.

GR-529-CORE *LSSGR: Public Safety*, Issue 1, FSDs 15-01-0000, 15-03-0000, and 15-07-0000, June 2000.

GR-533-CORE *LSSGR: Database Services – Service Switching Points, Toll-Free Service*, (FSD 31-01-000), June 2001.

GR-571-CORE *LSSGR: Call Waiting, FSD 01-02-1201*, June 2000.

GR-572-CORE *LSSGR: Cancel Call Waiting, FSD 01-02-1204*, June 2000.

GR-580-CORE *LSSGR: Call Forwarding Variable, FSD 01-02-1401*, June 2000.

GR-586-CORE *LSSGR: Call Forwarding Subfeatures, FSD 01-02-1450*, April 2002.

GR-590-CORE *LSSGR: Call Pickup Features,* Issue 1, June 2000.

GR-606-CORE *LSSGR: Common Channel Signaling, Section 6.5*, Component of FR-64, December 2004.

GR-740-CORE *Stored Program Control System/Operations System (SPCS/OS) - Network Data Collection Operations System (NDC OS) Interface*, March 200).

GR-782-CORE *SONET Digital Switch Trunk Interface Criteria, A Module of TSGR*, FR-440, Issue 1, June 2000 (Formerly TR-TSY-000782, Issue 2, September 1989).

GR-815-CORE *Generic Requirements for Network Element/Network System (NE/NS) Security: A Module of LSSGR*, Component of FR-64, Issue 2, March 2002.

GR-820-CORE *OTGR Section 5.1: Generic Digital Transmission Surveillance*, Issue 2, December 1997.

GR-874-CORE *An Introduction to the Reliability and Quality Generic Requirements (RQGR),* Issue 3, April 1997.

GR-957-CORE *Optical Interfaces for Equipment and Systems Relating to the Synchronous Digital Hierarchy),* 2006.

GR-1089-CORE *Electromagnetic Compatibility and Electrical Safety - Generic Criteria for Network Telecommunications Equipment*, Issue 05, August 2009.

GR-1100-CORE *Billing Automatic Message Accounting Format (BAF) Generic Requirements*, December 2007.

GR-1230-CORE *SONET Bi-Directional Line-Switched Ring Equipment Generic Criteria*, Issue 4, December 1998.

GR-1244-CORE *Clocks for the Synchronized Network: Common Generic Criteria*, Issue 1, May 2005.

GR-1400-CORE *SONET Unidirectional Path Switched Ring (UPSR) Equipment Generic Criteria*, Issue 3, July 2006.

GR-2911-CORE *Software Inventory for Network Element Software Management*, Issue 1, June 1995.

GR-2932-CORE *Database Functionalities*, May 1997.

GR-2996-CORE *Generic Criteria for SONET Digital Cross-Connect Systems*, Issue 1, January 1999.

GR-3051-CORE *Voice Over Packet: NGN Call Connection Agent Generic Requirements*, Issue 2, January 2001.

GR-3054-CORE *Voice Over Packet: NGN Trunk Gateway Generic Requirements*, Issue 1, March 2000.

GR-3055-CORE *Voice Over Packet: NGN Access Gateway Generic Requirements*, Issue 1, March 2000.

GR-3058-CORE *Voice over Packet (VoP): Next Generation Networks (NGN) Accounting Management Generic Requirements*, December 2005.

SR-2275 *Telcordia Notes on the Networks*, Issue 4, October 2000.

SR-3476 *National ISDN 1995 and 1996*, Issue 1, June 1995.

SR-3580 *NEBS Criteria Levels*, Issue 3, June 2007.

SR-4994 *2000 Version of National ISDN Primary Rate Interface (PRI) Customer Premises Equipment Generic Guidelines*, Issue 1, December 1999.

SR-NWT-002120 *National ISDN-2*, Issue 1, May 1992 with revision 1, June 1993.

SR-NWT-002343 *ISDN Primary Rate Interface Generic Guidelines for Customer Premises Equipment*, Issue 1, June 1993.

SR-NWT-002419 *Software Architecture Review Checklists*, Issue 01, December 1992.

TR-917 *SONET Regenerator (SONET RGTR) Equipment Generic Criteria*, December 1990.

TR-NWT-000057 *Functional Criteria for Digital Loop Carrier Systems*, Issue 2, January 1993.

TR-NWT-000179 *Software Quality Program Generic Requirements*, June 1993.

TR-NWT-000284 *Reliability and Quality Switching Systems Generic Requirements (RQSSGR)*, Issue 2, October 1990.

TR-NWT-000295 *Isolated Ground Planes: Definition and Application to Telephone Central Offices*, Issue 2, July 1992.

TR-NWT-000418 *Generic Reliability Assurance for Fiber Optic Transport Systems*, Issue 2, December 1992.

TR-NWT-001244 *Clocks for the Synchronized Network: Common Generic Criteria*, Issue 1, June 1993.

TR-NWT-001268 *ISDN Primary Rate Interface Call Control Switching and Signaling Generic Requirements for Class II Equipment*, Issue 1, December 1991.

Telcordia and Computer Sciences Corporation, *Call Connection Agent (CCA) Chapter, Assured Real Time Service (ARTS) Generic System Requirement (GRS)*, Draft October 2006.

Telcordia and Computer Sciences Corporation, *Media Gateway Chapter, Assured Real Time Service (ARTS) Generic System Requirement (GRS)*, Draft October 2006.

Telcordia and Computer Sciences Corporation, *Signaling Gateway Chapter, Assured Real Time Service (ARTS) Generic System Requirement (GRS)*, Draft October 2006.

## A4.21 TELECOMMUNICATIONS INDUSTRY ASSOCIATION

EIA/TIA-530-A, "High Speed 25-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment, Including Alternative 26-Position Connector," ANSI/TIA/EIA-530-A-92) (R98) (R2003), June 1992.

TIA/EIA-232-F, "Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange," October 1997.

TIA-422-B, "Electrical Characteristics of Balanced Voltage Digital Interface Circuits," (ANSI/TIA/EIA-422-B-1994) (R2000) (R2005), April 13, 2004.

TIA-810-B, November 3, 2006.

TIA/EIA-470-B, "Telecommunications - Telephone Terminal Equipment - Performance and Compatibility Requirements for Telephone Sets with Loop Signaling," 1997.

TIA TSB-116, "Telecommunications – IP Telephony Equipment – Voice Quality Recommendations for IP Telephony," March 2001.

TIA TSB-116-A, "Telecommunications System Bulletin – Telecommunications – IP Telephony Equipment – Voice Quality Recommendations for IP Telephony," March 2006.

## A4.22 UNITED STATES CODE

Title 10 Section 2224, "Defense Information Assurance Program," http://cio-nii.defense.gov/pocketref.html

Title 40 Section 11331.

Title 44 "Federal Information Security Management Act (FISMA) of 2002."

## A4.23 OTHER DOCUMENTATION

3G TS 24.067 V3.0.0 (1999-05), 3rd Generation Partnership Project; Technical Specification Group Core Network; enhanced MLPP (eMLPP) – Stage 3.

Alberts, Garstka, and Stein, "Network Centric Warfare," 2nd Edition Revised, February 2000.

American National Standards Institute (ANSI)/Electronic Industries Association (EIA) Standard, ANSI/EIA-310-D-92, *Cabinets, Racks, Panels and Associated Equipment*, September 1992.

AT&T TR62411.

ATIS-PP-1000012.2006, Signaling Systems No. 7 (SS7) – SS7 – Network and NNI Interconnection Security Requirements and Guidelines, November 2006.

Bellcore TR-TSY-000170.

Bellcore TR-TSY-000181.

Booze-Allen & Hamilton, Inc., DF v2.1, "Common Criteria for Information Technology Security Evaluation: Protection Profile for Switched and Routers," February 2001.

Defense Intelligence Agency, Defense Intelligence Agency Manual (DIAM) 50-3, "Physical Security Standards for Construction of Sensitive Compartmented Information Facilities." Director of Central Intelligence Directive 6/3, DCID 6/3, Series, "Protecting Sensitive Compartmented Information within Information Systems," 1999.

FED-STD-1037, "Telecommunications: Glossary of Telecommunication Terms," 7 August 1996, http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm.

Federal Telecommunications Recommendation 1080B-2002, *"Video Teleconferencing Services,"* August 15, 2002.

"Generic Cryptographic Interoperability Requirements Document (GCIRD)," Version 1.3, January 7, 2008.

"Global Information Grid 2.0 (GIG 2.0) Initial Capabilities Document (ICD)," 6 January 2003.

Global Information Grid NetOps Guidance and Policy Memorandum No. 10-8460, "Network Operations," 24 August 2000.

Horizontal Fusion Standards and Specifications, 3 November 2004.

House Report 107-436, "Bob Stump National Defense Authorization Act for Fiscal Year 2003": Report of the Committee on Armed Services, House of Representatives on H.R. 4546, 3 May 2002.

International Electrotechnical Commission (IEC), 60950-1, "Information technology equipment – Safety – Part 1: General requirements," Second Edition, 2005-12.

International Standardization Organization, ISO 13871, “Digital Channel Aggregation,” June 2001.

Joint Interoperability Test Center, “Internet Protocol Version 6 Generic Test Plan,” Version 2, June 2006.

Joint Staff, Command, Control, Communications, and Computer Systems Directorate (J-6), “Joint Net-Centric Operations Campaign Plan,” October 2006.

Joint Staff, “Global Information Grid 2.0 (GIG 2.0) Concept of Operations (CONOPS).”

Joint Staff, “Global Information Grid 2.0 (GIG 2.0) Initial Capability Document (ICD).”

Joint Staff, “Global Information Grid 2.0 (GIG 2.0) Implementation Plan.”

National Communications System, NCS Directive 3-10, “Telecommunications Operations, Government Emergency Telecommunications Service (GETS),” 2000.

National Fire Protection Association (NFPA) 72, “National Fire Alarm and Signaling Code”, 2010

National Institute of Standards and Technology (NIST) Special Publication 800-88, “Guidelines for Media Sanitization, Computer Security, Richard Kissel, Matthew Scholl, Steven Skolochenko, and Xing Li, September 2006.

“Net-Centric Operations and Warfare (NCOW) Reference Model (RM),” Draft, Version 0.9 (v0.9).

Newton, Harry, *Newton’s Telecom Dictionary – The Dictionary of Telecommunications, Networking and The Internet*, 25th Ed., June 2009.

North American Treaty Organization (NATO), Standard NATO Agreement (STANAG 4214), “International Rating and Directory for Tactical Communications Systems,” Edition 3, Version T, 07 January 2005.

OASIS Standard Common Alerting Protocol (CAP), v1.1, October, 2005.

Office of Management and Budget (OMB) Circular A-130, Appendix III.

OPNAVINST 3000.12A, “Operational Availability Handbook, March 2003.

"Policy Guidance for use of Mobile Code Technologies in Department of Defense (DOD) Information Systems," 7 November 2000, http://www.defenselink.mil/nii/org/cio/doc/mobile-code11-7-00.html.

Public Law 107-314, Section 353, "Bob Stump National Defense Authorization Act for Fiscal Year 2003," 2 December 2002.

Real-Time Services Information Assurance Working Group, "Analysis of IA Requirements and Threats for the DoD RTS Environment," Version 2.2, July 2005.

Real-Time Services Working Group, "Real Time Services (RTS) Information Assurance (IA) Generic System Requirements (GSR)," Version 1.3, 6 July 2006.

Reference Guide for Nodal Manager, "ESOP and Global Edition," Version 4.0, January 1998.

RS-232, Recommended Standard 232 for Serial Binary Data Signals Connecting Between a DTE and a DCE.

"Terms of Reference for the Implementation of UCP 02," Ch-2 Revision 1, 10 December 2003.

TM 11-5805-681-12 series, "Operator's and Organizational Maintenance Manual for Central Office, Telephone, Automatic AN/TTC-39(V)2."

Underwriters Laboratories, Inc., UL-1950, Standard for Safety, Information Technology Equipment Including Electrical Business Equipment," First Edition, 1999.

"Unified Command Plan 2002," Changes 1 and 2, 10 January 2003.

"Wireless Priority Service (WPS) Industry Requirements for the Full Operating Capability (FOC) for CDMA-Based Systems – Home Location Register (HLR)," Issue 1, 04 June 2004.

"Wireless Priority Service (WPS) Industry Requirements for the Full Operating Capability (FOC) for GSM-Based Systems," Issue 2, January 2004.

THIS PAGE INTENTIONALLY LEFT BLANK