GLOSSARY

3GPP (Third-Generation Partnership Project) The Third-Generation Partnership Project unites (six) telecommunications standards bodies, known as "organizational partners," and provides their members with a stable environment to produce the Reports and Specifications that define 3GPP technologies. Wireless technologies are constantly evolving through—what have become known as—generations of commercial cellular/mobile systems. 3GPP was originally the standards partnership evolving global system for mobile (GSM) systems toward the third generation. However, since the completion of the first LTE and the evolved packet core specifications, 3GPP has become the focal point for mobile systems beyond 3G. From 3GPP Release 10 onward, 3GPP is compliant with the latest ITU-R requirements for IMT-advanced "Systems beyond 3G." The standard now allows for operation at peak speeds of 100 Mbps for high-mobility and 1 Gbps for low-mobility communication.

The original scope of 3GPP was to produce Technical Specifications and Technical Reports for a 3G Mobile System based on evolved GSM core networks and the radio access technologies that they support (i.e., Universal Terrestrial Radio Access [UTRA] both frequency division duplex [FDD] and time division duplex [TDD] modes). The scope was subsequently amended to include the maintenance and development of the GSM communication Technical Specifications and

Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications, First Edition. Daniel Minoli.

Technical Reports including evolved radio access technologies (e.g., general packet radio service [GPRS] and enhanced data rates for GSM evolution [EDGE]) (1). The term "3GPP specification" covers all GSM (including GPRS and EDGE), W-CDMA, and LTE (including LTE-advanced) specifications. The following terms are also used to describe networks using the 3G specifications: UTRAN, universal mobile telecommunications system (UMTS) (in Europe), and FOMA (in Japan).

3GPP2 (Third-Generation Partnership Project 2) The Third-Generation Partnership Project 2 is a collaborative third-generation (3G) telecommunications specifications-setting project comprising North American and Asian interests developing global specifications for ANSI/TIA/EIA-41 cellular radiotelecommunication intersystem operations network evolution to 3G and global specifications for the radio transmission technologies (RTTs) supported by ANSI/TIA/EIA-41. 3GPP2 was born out of the International Telecommunication Union's (ITU) International Mobile Telecommunications "IMT-2000" initiative, covering high-speed, broadband, and internet protocol (IP)-based mobile systems featuring network-to-network interconnection, feature/service transparency, global roaming, and seamless services independent of location. IMT-2000 is intended to bring high-quality mobile multimedia telecommunications to a worldwide mass market by achieving the goals of increasing the speed and ease of wireless communications, responding to the problems faced by the increased demand to pass data via telecommunications, and providing "anytime, anywhere" services (2). 3GPP2 provides globally applicable Technical Specifications for a 3G mobile system based on the evolving ANSI-41 core network and the relevant radio access technologies to be transposed by standardization bodies (organizational partners) into appropriate deliverables (e.g., standards).

6LoWPAN: IPv6 Over Low-Power Area Networks (IEEE 802.15.4) 6LoWPAN is now a widely accepted approach to run IP on 802.15.4 based on RFC 4944 (September 2007.) It is supported in TinyOS, Contiki, and in standards such as ISA100, ZigBee Smart Energy (SE) 2.0. RFC 4944 makes 802.15.4 look like an IPv6 link. It provides basic encapsulation and efficient representation of packets $< \sim$100 bytes. It addresses topics such as (3):

- Fragmentation (how to map 1280 byte MTU to packets 128 bytes or less);
- First approach to stateless header compression;
- Datagram tag/datagram offset;
- Mesh forwarding;
- Identify originator/final destination;
- Minimal use of complex MAC (media access control) layer concepts.

6over4 An IPv6 transition technology that provides IPv6 unicast and multicast connectivity through an IPv4 infrastructure with multicast support, using the IPv4 network as a logical multicast link.

6over4 Link-Local Address An IPv6 address of the form FE80::WWXX:YYZZ, where WWXX:YYZZ is the hexadecimal representation of w.x.y.z, a public or private IPv4 address assigned to the 6over4 device interface.

6over4 Unicast Address An IPv6 address of the form 64-bit prefix:0:0:WWXX:YYZZ, where WWXX:YYZZ is the hexadecimal representation of w.x.y.z, a public or private IPv4 address assigned to the 6over4 device interface.

6to4 An IPv6 transition technology that provides unicast connectivity between IPv6 networks and devices through an IPv4 infrastructure. 6to4 uses a public IPv4 address to build a global IPv6 prefix.

6to4 Address A global IPv6 address of the form 2002:WWXX:YYZZ:SLA_ID:interface ID, where WWXX:YYZZ is the hexadecimal representation of w.x.y.z, a public IPv4 address assigned to a 6to4 router's IPv4 interface and SLA_ID is the site-level aggregation identifier (SLA ID). The address space 2002::/16 is assigned to 6to4 addresses.

6to4 Host An IPv6 device that is configured with at least one 6to4 address (a global address with a 2002::/16 prefix). 6to4 devices do not require manual configuration and they create 6to4 addresses by means of standard autoconfiguration mechanisms.

6to4 Relay Router An IPv6/IPv4 router that forwards traffic between 6to4 routers and IPv6 Internet devices.

6to4 Router A router that participates in the 6to4 transition technology, providing unicast connectivity between IPv6 networks and devices through an IPv4 infrastructure.

Actuator An actuator is a mechanized device of various sizes (from ultra-small to very large) that accomplishes a specified physical action, for example controlling a mechanism or system, opening or closing a valve, starting some kind or rotary or linear motion, and initiating physical locomotion. It is the mechanism by which an entity acts upon an environment. The actuator embodies a source of energy, such as an electric current (battery, solar, motion), a hydraulic fluid pressure, or a pneumatic pressure; the device converts that energy into some kind of action or motion upon external command.

Address In this context a network-layer identifier assigned to an interface or set of interfaces that can be used as source or destination field in IP datagrams. An IP layer identifier for an interface or a set of interfaces.

The IPv6 128-bit address is divided along 16-bit boundaries. Each 16-bit block is then converted to a 4-digit hexadecimal number, separated by colons. The resulting representation is called colon-hexadecimal. This is in contrast to the 32-bit IPv4 address represented in dotted-decimal format, divided along 8-bit boundaries, and then converted to its decimal equivalent, separated by periods (4).

The following example shows a 128-bit IPv6 address in binary form:

0010000111011010000000001101001100000000000000000010111100111011
000000101 0101010000000001111111111111110001010001001110001011010

The following example shows this same address divided along 16-bit boundaries:

0010000111011010 0000000011010011 0000000000000000
0010111100111011 0000001010101010 0000000011111111
1111111000101000 1001110001011010

The following example shows each 16-bit block in the address converted to hexadecimal and delimited with colons.

21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

IPv6 representation can be further simplified by removing the leading zeros within each 16-bit block. However, each block must have at least a single digit. The following example shows the address without the leading zeros:

21DA:D3:0:2F3B:2AA:FF:FE28:9C5A

Address Autoconfiguration The automatic configuration process for IPv6 addresses on an interface; specifically, the process for configuring IP addresses for interfaces in the absence of a stateful address configuration server, such as dynamic host configuration protocol version 6 (DHCPv6).

Address Maximum Valid Time Time period during which a unicast address, obtained by means of stateless autoconfiguration mechanism, is valid.

Address Resolution Procedure used by a node for determining the link-layer address of other nodes on a link. In an IPv6 context, the process by which a node resolves a neighboring node's IPv6 address to its link-layer address. In IPv4, the procedure is accomplished via the ARP protocol. In IPv6, the procedure is accomplished via neighbor advertisement and neighbor solicitation ICMPv6 messages.

Advanced Encryption Standard (AES) Cryptographic algorithm; National Institute of Standards and Technology (NIST)-approved standard. It was chosen by NIST because it is considered to be both faster and smaller than its competitors (5).

Advanced Meter Infrastructure (AMI) system An infrastructure that contains meters capable of two-way communications with a centralized grid control system. These are meters that can receive signals, including the cost of electricity and status of the grid, track electricity usage on a short-term basis, and automatically report the meter readings back to the utility (6).

Aggregatable Global Unicast Address Also known as global addresses, these addresses are identified by means of the 3-bit format prefix 001 (2000::/3). IPv6 global addresses are equivalent to IPv4 public addresses and they are routable in the IPv6 Internet.

Air Interface In radio-frequency identification (RFID) environments, the complete communication link between an interrogator and a tag including the physical layer,

collision arbitration algorithm, command and response structure, and data-coding methodolog (7).

Ambient Intelligence Ambient intelligence is a vision where environment becomes smart, friendly, context aware, and responsive to any type of human needs. In such a world, computing and networking technology coexist with people in a ubiquitous, friendly, and pervasive way. Numerous miniature and interconnected smart devices create a new intelligence and interact with each other seamlessly. For health care, this translates into proliferation of remote monitoring and telemedicine (8).

AMI (Advanced Metering Infrastructure) The electric information service infrastructure between the end-user or end device and the electric company. A system for implementing smart grid (SG) and a principal means of realizing demand response. AMI has several methods to connect from end device to applications of utility, and there are many standards communication protocols. To communicate between physical service layers, some combinations and transformations of the protocols are required. AMI environment is very complex because it should be considered the area of home area network (HAN) and demand respond application (9).

AMR Automated meter reader

ANT™/ANT+™ ANT is a low-power proprietary wireless technology introduced in 2004 by the sensor company Dynastream. The system operates in the 2.4 GHz band. ANT devices can operate for years on a coin cell. ANT's goal is to allow sports and fitness sensors to communicate with a display unit. ANT+ extends the ANT protocol and makes the devices interoperable in a managed network. ANT+ recently introduced a new certification process as a prerequisite for using ANT+ branding (10).

Anycast Address A unicast address that is assigned to several interfaces and is used for the delivery of IP datagrams to one of the several interfaces. With an appropriate route, datagrams addressed to an anycast address will be delivered to a single interface—the nearest one.

Asymmetric Encryption Type of encryption in which encryption keys are different from decryption keys, and one key is computationally difficult to determine from the other. Uses an asymmetric algorithm (5).

Attempt Address Unicast address where uniqueness is no longer checked.

Authentication The process of proving the genuineness of an entity (such as a smart card) by means of a cryptographic procedure. Authentication entails using a fixed procedure to determine whether someone is actually the person he or she claims to be (5).

Authentication, Authorization, and Accounting (AAA) Authentication refers to the confirmation that a user who is requesting services is a valid user of the network services requested. Authorization refers to the granting of specific types of service (including "no service") to a user, based on their authentication, what services they are requesting, and the current system state. Accounting refers to the tracking of the consumption of network resources by users. This information may be used for management, planning, billing, or other purposes (11).

Authorization An authorization provides access (or legal power) to some protected service. In a CA system, the authorization gives access to encrypted services (channels, movies, and so on) (5).

Automatic IPv6 Tunnel Automatic creation of tunnels, generally through the use of various IPv6 address formats that contain the IPv4 tunnel endpoints.

Autonomous System (AS) A network domain that belongs to the same administrative authority.

Bandwidth The amount of information that can be sent through a connection. In digital settings, it is measured in bits-per-second. Full-motion full-screen video requires 2.5–12 Mbps depending on compression (e.g., MPEG-2, MPEG-4) and format (SD or HD).

Bluetooth Bluetooth is a personal area network (PAN) technology based on IEEE 802.15.1. It is a specification for short-range wireless connectivity for portable personal devices, initially developed by Ericsson. The Bluetooth special interest group (SIG) made their specifications publicly available in the late 1990s; soon thereafter the IEEE 802.15 group has took the Bluetooth work developed a vendor-independent standard. The sublayers of IEEE 802.15 are: (i) RF layer, (ii) baseband layer, (iii) the link manager, and (iv) the logical link control and adaptation protocol (L2CAP). Bluetooth has evolved through four versions; all versions of the Bluetooth standards maintain downward compatibility. Bluetooth low energy (BLE) is a subset to Bluetooth v4.0, with an entirely new protocol stack for rapid build-up of simple links. BLE is an alternative to the "power management" features that were introduced in Bluetooth v1.0 to v3.0 as part of the standard Bluetooth protocols.

The functionality is as follows:

- RF layer: The air interface is based on antenna power range starting from 0 dBm up to 20 dBm, 2.4 GHz band, and the link range from 0.1 to 10 m.
- Baseband layer: The baseband layer establishes the Bluetooth *piconet*. The piconet is formed when two Bluetooth devices connect. In a piconet, one device acts as the master and the other devices act as slaves.
- Link manager: The link manager establishes the link between Bluetooth devices. Additional functions include security, negotiation of baseband packet sizes, power mode and duty cycle control of the Bluetooth device, and the connection states of a Bluetooth device in a piconet.
- Logical link control and adaptation protocol (L2CAP): This sublayer provides the upper-layer protocols with connectionless and connection-oriented services. The services provided by this layer include protocol multiplexing capability, segmentation and reassembly of packets, and group abstractions.

(Bluetooth is a trademark of the Bluetooth Alliance, a commercial organization that certifies the interoperability of specific devices designed to the respective IEEE standard.)

Broadcasting Satellite Service (BSS) A satellite service that (for ITU Region 2 segments covering the majority of the Americas) operates at 17.3–17.8 GHz for the uplink and 12.2 to 12.7 GHz for the downlink. High-power geostationary satellites are utilized.

Buffering The temporary storing data before playing it back. A buffer is a temporary holding area in memory for data; buffers can be on the input or output side of a data-carrying link.

Certificate A digital certificate consists of three things, as follows: (1) The public-key portion of the certificate holder's public and private key pair. (2) Information that identifies the holder of the certificate (the owner of the corresponding private key). (3) The digital signature of a trusted entity attesting to the validity of the certificate (i.e., that the key and the certificate information truly go together) (5).

Circular Orbit (Satellite) A satellite orbit where the distance between the center of mass of the satellite and of the earth is constant.

Clarke Belt (Satellite) The circular orbit (geostationary orbit [GEO]) at approximately 35,786 km above the equator, where the satellites travel at the same speed as the earth's rotation and thus appear to be stationary to an observer on earth (named after Arthur C. Clarke who was the first to describe the concept of geostationary communication satellites).

Client The originating endpoint of a request; the destination endpoint of a response.

Cloud Computing The latest term to describe a grid/utility computing service. Such service is provided in the network. From the perspective of the user, the service is virtualized. In turn, the service provider will most likely use virtualization technologies (virtualized computing, virtualized storage, etc.) to provide the service to the user.

Codec (COmpressor/DECompressor)—The system (hardware, software, or combination of both) used to compress/decompress an audio and/or video file for storage or transmission. Codecs convert data between uncompressed and compressed formats, thereby reducing the bandwidth a clip consumes.

Collocated Satellites Two or more satellites occupying approximately the same geostationary orbital position such that the angular separation between them is effectively zero when viewed from the ground. To a small receiving antenna, the satellites appear to be exactly collocated; in reality, the satellites are kept several kilometers apart in space to avoid collisions. Different operating frequencies and/or polarizations are used.

Colon Hexadecimal Notation The notation used to represent IPv6 addresses. The 128-bit address is divided into eight blocks of 16 bits. Each block is represented as a hexadecimal number and is separated from the next block by means of a colon (:). Inside each block, left zeros placed are removed. An example of an IPv6 unicast address represented in hexadecimal notation is 3FFE:FFFF:2A1D:48C:2AA:3CFF:FE21:81F9.

Compatibility Addresses IPv6 addresses used when IPv6 traffic is sent through an IPv4 infrastructure. Some examples are IPv4 compatible addresses, 6to4 addresses, and ISATAP addresses.

Compressing Zeros Some IPv6 addresses expressed in colon-hexadecimal contain long sequences of zeros. A contiguous sequence of 16-bit blocks set to 0 in the colon-hexadecimal format can be compressed to :: (known as double-colon). The following shows examples of compressing zeros (4):

The link-local address of FE80:0:0:0:2AA:FF:FE9A:4CA2 can be compressed to FE80::2AA:FF:FE9A:4CA2.

The multicast address of FF02:0:0:0:0:0:0:2 can be compressed to FF02::2.

Zero compression can only be used to compress a single contiguous series of 16-bit blocks expressed in colon-hexadecimal notation.

Confidentiality The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Constrained Application Protocol (CoAP) CoAP is a simple application layer protocol targeted to simple electronics devices (e.g., IoT/M2M things) to allow them to communicate interactively over the Internet. CoAP is designed for low-power sensors and for actuators that need to be controlled or monitored remotely, using IP/Internet networks.

Continuous Wave In RFID environments, typically a sinusoid at a given frequency, but more generally any interrogator waveform suitable for powering a passive tag without amplitude and/or phase modulation of sufficient magnitude to be interpreted by a tag as transmitted data (7).

Correspondent Node Refers to a node that is communicating with a node that is using mobile IP.

Cover-coding In RFID environments, a method by which an interrogator obscures information that it is transmitting to a tag. To cover-code data or a password, an interrogator first requests a random number from the tag. The interrogator then performs a bit-wise EXOR of the data or password with this random number and transmits the cover-coded (also called ciphertext) string to the tag. The tag uncovers the data or password by performing a bit-wise EXOR of the received cover-coded string with the original random number (7).

DASH7 A long range low-power wireless networking technology, with the following features:

- Range: dynamically adjustable from 10 m to 10 km;
- Power: <1 milliwatt power draw;
- Data rate: dynamically adjustable from 28 Kbps to 200 Kbps;
- Frequency: 433.92 MHz (available worldwide);
- Signal propagation: penetrates walls, concrete, water;
- Real-time locating precision: within 4 m;
- Latency: configurable, but worst case is less than 2 s;
- P2P messaging;
- IPv6 support;
- Security:128-bit AES, public key; and
- Standard: ISO/IEC 18000-7; advanced by the DASH7 Alliance.

DASH7 Alliance The DASH7 Alliance was formed to advance the use of DASH7 wireless data technology by developing extensions to the ISO 18000-7 standard, ensuring interoperability among devices, and educating the market about DASH7 technology. Formed in 2009, the Alliance had more than 20 members at press time. Manufacturers, systems integrators, developers, regulators, academia, and end-users all work together to promote the use of DASH7 technology in a wide array of industries and applications.

Data Encryption Standard (DES) A 64-bit block cipher, symmetric algorithm also known as data encryption algorithm (DEA) by ANSI and DEA-1 by ISO. Widely used for over two decades, adopted in 1976 as FIPS 46 (5).

Data Origin Authentication The corroboration that the source of data received is as claimed.

Datagram Another name for an IP-level packet.

Decoding The decompression of an encoded file for playback or use.

Decoding Time Stamp (DTS) Time stamps are inserted close to the material to which they refer (normally in the PES packet header). They indicate the exact moment where a video frame or an audio frame has to be decoded or presented to the user respectively. These rely on reference time stamps for operation (12).

Default Route The route with a ::/0 prefix. The default route is the route used to obtain the next destination address when there are no other matching routes.

Default Routers List A list of routers that can be used as a default router. The list is populated based on router advertisement messages received that have a non-null router lifetime.

Delay-Tolerant Network (DTN) An architecture being developed by the Delay-Tolerant Networking Research Group (DTNRG), which is a research group chartered as part of the Internet Research Task Force (IRTF). Members of DTNRG are concerned with how to address the architectural and protocol design principles arising from the need to provide interoperable communications with and among extreme and performance-challenged environments where continuous end-to-end connectivity cannot be assumed. Stated another way, one is concerned with interconnecting highly heterogeneous networks together even if end-to-end connectivity may never be available. Examples of such environments include spacecraft, military/tactical, some forms of disaster response, underwater, and some forms of ad-hoc sensor/actuator networks. It may also include Internet connectivity in places where performance may suffer such as developing parts of the world (13). This work is also related to DARPA's disruption tolerant networking program.

Delay-tolerant networks make use of store-and-forward techniques within the network in order to compensate for intermittent link connectivity. In the DTN, the fundamental concept is an architecture based on Internet-independent middleware where protocols at all layers are used that best suit the operation within each environment, with a new overlay network protocol (bundle protocol) inserted between the applications and the locally optimized communications stacks. Many applications can benefit from the reliable delivery of messages in

a disconnected network. The Internet, in contrast, is a connected network where IPs, most notably transmission control protocol/IP (TCP/IP), are dependent upon (low) latencies of approximately milliseconds. This low latency, coupled with low bit error rates (BERs), allows TCP to reliably transmit and receive acknowledgements for messages traversing the terrestrial Internet. One of the best examples of high latency, high BER links, with intermittent connectivity is that of space communications. One-way trip times, at the speed of light, from the Earth to the moon incur a delay of 1.7 s, while one-way trip times to Mars incur a minimum delay of 8 min. Military applications in the DTN arena are substantial, allowing the retrieval of critical information in mobile battlefield scenarios using only intermittently connected network communications (14).

Denial of Service (DoS) The prevention of authorized access to resources or the delaying of time-critical operations.

Device Lower Layer (DLL) Component of the lower layer in an M2M device.

Digital Signature Data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery for example, by the recipient.

Digital Subscriber Line (DSL) A 1990s technology that exploits unused frequencies on copper telephone lines to transmit traffic typically at multi-megabit speeds. DSL can allow voice and high-speed data to be sent simultaneously over the same line. Because the service is "always available," end-users do not need to dial in or wait for call setup. Asymmetrical variations include ADSL, G.lite ADSL (or simply G.lite), VDSL (ITU-T G.993.1), and VDSL2 (ITU-T G.993.2). The standard forms of ADSL (ITU G.992.3, G.992.5, and ANSI T1.413—Issue 2) are all built upon the same technical foundation, discrete multitone (DMT). The suite of ADSL standards facilitates interoperability between all standard forms of ADSL (15).

Digital Subscriber Line Access Multiplexer (DSLAM) Telephone carrier equipment typically residing at the Central Office that terminates multiple DSL lines (usually 96, 192, or 384) and multiplexes the combined output to an ATM, MPLS, or IP uplink. The uplink is typically an OC-3 (155 Mbps) or an OC-12 (622 Mbps).

Distance Vector Routing Protocol A routing protocol in which a router periodically informs its neighbors of topology changes. This is in contrast to link state routing protocols, which require a router to inform all the nodes in a network of topology changes (16).

DNP3 DNP3 is a protocol for transmission of point-to-point data using serial communications. It has been used primarily by utilities, but can also be used in other areas. The DNP3 is specifically developed for interdevice communication involving SCADA RTUs. It is based on the three-layer model contained in the IEC 60870-5 standards.

Domain Name System (DNS) A hierarchical storage system and its associated protocol to store and retrieve information about names and IP addresses.

Double Colon Notation used in compressing continuous series of 0 blocks in IPv6 addresses. For example, the FF02:0:0:0:0:0:0:2 multicast address is expressed as FF02::2.

Dual Stack Architecture A node architecture in which two complete protocols stack implementations exist, one for IPv4 and one for IPv6, each with its own implementation of the transport layer (TCP and UDP).

Dynamic Host Configuration Protocol (DHCP) A configuration protocol that provides IP addresses and other configuration parameters when connected to an IP network.

Dynamic Host Registration A mechanism that informs the network that a host (receiver) is a member of a particular group (otherwise, the network would have to flood rather than multicast the transmissions for each group.) For IP networks, the Internet Group Multicast Protocol (IGMP) serves this purpose.

EDGE (Enhanced Data Rates for Global Evolution) An enhancement of the GSM™ radio access technology to provide faster bit rates for data applications, both circuit and packet switched. As an enhancement of the existing GSM physical layer, EDGE is realized via modifications of the existing layer 1 specifications rather than by separate, stand-alone specifications. Other than providing improved data rates, EDGE is transparent to the service offering at the upper layers, but is an enabler for high-speed circuit switched data (HSCSD) and enhanced GPRS (EGPRS). GPRS can offer a data rate of 115 Kbps, whereas EDGE can increase this to 384 Kbps. This is comparable with the rate for early implementations of wideband code division multiple access (W-CDMA), leading some parties to consider EDGE as a 3G technology rather than 2G (a capability of 384 Kbps allows EDGE systems to meet the ITU's IMT-2000 requirements). EDGE is generally viewed as a bridge between the two generations: a sort of 2.5G (17).

eHealth A term for healthcare practice supported by electronic processes and communication.

Electronic Product Code (EPC) A unique identifier for a physical object, unit load, location, or other identifiable entity playing a role in business operations. EPCs are assigned the following rules designed to ensure uniqueness despite decentralized administration of code space and to accommodate legacy coding schemes in common use. EPCs have multiple representations, including binary forms suitable for use on RFID tags and text forms suitable for data exchange among enterprise information systems.

Encapsulating Security Payload An IPv6 extension header that provides data source authentication, data integrity, and confidentiality.

Encapsulator A network device that receives PDUs (also known as SNDUs) (Ethernet frames or IP datagrams) and formats these for output as a transport stream of TS packets (18).

Encoder A device that converts an audio or video signal to a specific streaming format, for example, MPEG-4 (or MPEG-2). The conversion typically includes compression and generation on an IP packet.

Encoding Converting a file into a compressed format.

Encryption The process of making a message unintelligible for all who do not have the proper key.

Entitlement Access criteria authorizations.

EPCglobal Architecture Framework A collection of interrelated standards ("EPCglobal Standards"), together with services operated by EPCglobal, its delegates, and others ("EPC Network Services"), all in service of a common goal of enhancing business flows and computer applications through the use of EPCs.

ESN Electronic serial number.

Ethernet Over an MPLS (EoMPLS) Transport of native Ethernet over an MPLS pseudowire.

ETSI Machine-to-Machine (M2M) Machine-to-machine (M2M) communications is the communication between two or more entities that do not necessarily need any direct human intervention. M2M services intend to automate decision and communication processes. Defined in ETSI TS 102 689 V1.1.1 (2010-08) and ETSI TS 102 690 V1.1.1 (2011-10) (and elsewhere). Basic applications include, but are not limited to, smart meters, eHealth, track and trace, monitoring, transaction, control, home automation, city automation, connected consumers, and automotive (19, 20).

EUI-64 Address 64-bit link-layer address that is used as the basis to generate interface identifiers in IPv6.

eUICC A certified tamper-resistant hardware component, performing the role of a traditional UICC (universal integrated circuit card), which may be soldered into mobile devices, to run the secure network access application (s) and enable the secure changing of subscription identity and other subscription data.

European Telecommunications Standards Institute (ETSI) An independent, nonprofit European-focused organization whose mission is to produce telecommunications standards.

Extended Access Barring (EAB) 3GPP-defined capability that extends legacy access control barring (ACB), which can bar all User Equipment (UEs) in a cell.

Extended Unique Identifier (EUI) Link-layer address defined by the Institute of Electrical and Electronic Engineers (IEEE).

Extension Headers Headers placed between the IPv6 header and higher-level protocols headers to provide additional functionalities to IPv6.

Fibre Channel (FC) The dominant storage networking protocol used in the enterprise data center and for (multimedia) content storage. A high-speed storage/networking interface that offers a high performance, large transfer capacity, long cabling distance, system configuration flexibility and scalability, and simplified cabling. The current operating speed is 8 Gbps; the expectation is that a 16 Gbps rate will be achievable by mid-decade (by comparison, 10 Gbps Ethernet is expected to move up to a 40 Gbps or even 100 Gbps rates over the same period).

File Formats Container file formats for various platforms. The more common formats include:

avi (audio video interleave)—A multimedia container file format developed by Microsoft to allow synchronous audio-with-video playback.

.flv—Flash video file format; used to deliver video over the Internet.

.mov—A video publishing file format developed by Apple for use with their QuickTime video players.

.wmv (windows media video)—An audio and video file encoded for use with Windows media player.

Fixed Satellite Service (FSS) A satellite service that (for ITU Region 2 segments covering the majority of the Americas) operates at 14.0–14.5 GHz for the uplink and 11.7–12.2 GHz the downlink. Geostationary satellites are utilized. The service is utilized by television stations/broadcast networks/cable TV systems to distribute signals to affiliates across a wide geographic region, as well as for other traditional telecommunications (voice and data communications) applications. Typical video applications include content distribution from a content-generation center (e.g., studios) to local cable headends. FSS satellites have also been used for direct-to-home (DTH) applications, although Direct Broadcast Satellite (DBS) services at the ku-BSS frequencies (such as those used by DirecTV and Dish Network) are specifically intended for those applications. The term "fixed" is used to imply that the sending station is fixed and the receiving stations are generally (but not always) fixed. This is in contrast to the mobile satellite services (MSSs), which refer to communications satellites intended for use with mobile and portable wireless devices/telephones. MSS-supporting services can be delivered using GEO, medium earth orbit (MEO), or low earth orbit (LEO) satellites.

Flow A series of IP datagrams exchanged between a source and a destination.

Format Prefix Variable number of high-order bits of an IPv6 address that defines an IPv6 address type.

Forward Direction The dominant direction of data transfer over a network path. Data transfer in the forward direction is called "forward transfer." Packets traveling in the forward direction follow the forward path through the IP network (18).

Forward Error Correction (FEC) FEC is a family of well-known simplex error correction techniques that add "coding" bits to the information bits at the transmit end (encoder) that enables the decoder to determine which bits are in error and correct them (up to a limit); for example, R 4/5 FEC means 1 coding bit is added for every 4 information bits (thereby transmitting 5 bits); the more coding bits, the "stronger" the code (requires less transmit power or link quality to get the same performance), but more coding bits mean more bandwidth required. Because satellite transmission can attenuate the signal by up to 200 db, FEC is critical. High coding: R 1/2; low coding: R 7/8. Typical satellite FEC is either convolutional/viterbi with Reed–Solomon or Turbo coding. Typical Turbo codes provide about a 2 dB advantage over conventional codes. 'Viterbi' soft-decision decoding has been the norm (<4.4dB gain). "Turbo coding" has been advanced recently (<6.3dB gain). "Low Density Parity Check" (LDPC) is the newest algorithm (<7.8dB gain).

Fragment A portion of a message sent by a host in an IPv6 datagram. Fragments contain a fragmentation header to allow reassembly at the destination.

Fragmentation Process in which the source device divides a message into some number of smaller messages, termed fragments.

Fragmentation Header An IPv6 extension header that contains information that allows the receiving node to reassemble fragments into the original message.

Frame Rate The rate at which video frames are displayed. The frame rate for movies on film is 24 frames per second (24 fps). Standard NTSC video has a frame rate of 30 fps (actually 60 fields per second). The frame rate of a progressive-scan video format is twice that of an interlaced-scan format. For example, interlaced formats like 480i and 1080i deliver 30 complete frames per second; progressive formats like 480p, 720p and 1080p provide 60 (21).

Full-Rate Asymmetrical DSL (ADSL) Access technology that offers differing upload and download speeds and can be configured to deliver up to six megabits of data per second (6000 Kbps) from the network to the customer that is up to 120 times faster than dialup service and 100 times faster than integrated services digital network (ISDN). ADSL enables voice and high-speed data to be sent simultaneously over the existing telephone line. This type of DSL is the most predominant in commercial use for business and residential customers around the world. Good for general Internet access and for applications where downstream speed is most important, such as video-on-demand. ITU-T Recommendation G.992.1 and ANSI Standard T1.413-1998 specify full-rate ADSL. ITU Recommendation G.992.3 specifies ADSL2 that provides advanced diagnostics, power-saving functions, PSD shaping, and slightly better performance than G.992.1. ITU Recommendation G.992.5 specifies ADSL2Plus that provides the benefits of ADSL2Plus twice the bandwidth so that bit rates as high as 20 Mbps downstream can be achieved on relatively short lines (15).

Fully Qualified Domain Name (FQDN) FQDN gives the full location of a resource within the whole DNS name space. When interpreting the FQDN, one starts at the root and then follows the sequence of domain labels from right to left, going top to bottom within the name space tree. An FQDN includes the top-level domain. For example, www.cnn.com is an FQDN. www is the host, cnn is the second-level domain, and com is the top-level domain. This is in contrast to a partially qualified domain name (PQDN), which does not give the full path to the domain. One can only use a PQDN within the context of a particular parent domain.

Future Network (FN) The ITU-T FN is a network that will be able to provide revolutionary services, capabilities, and facilities that are hard to support using existing network technologies. Also, it is expected that the FN will overcome the limitations of the current networks. The FN includes core technologies that are necessary for constructing future networking infrastructure and application service infrastructure. In 2009, ITU-TSG13 established "Focus Group on Future Networks (FG-FN)" to share the discussion on FNs and ensure global common understanding about FNs with collaboration and harmonization with relevant entities and activities. The FG successfully completed its work in 2010. The FG, by

collaborating with worldwide FN communities (e.g., research institutes, forums, academia), aims to

- collect and identify visions of FNs, based on new technologies,
- assess the interactions between FNs and new services,
- familiarize ITU-T and standardization communities with emerging attributes of FNs, and
- encourage collaboration between ITU-T and FN communities.

G.lite ADSL (or Simply G.lite A standard that was specifically developed to meet the plug-and-play requirements of the consumer market segment. G.lite is a medium bandwidth version of ADSL that allows Internet access at up to 30 times the speed of the fastest 56K analog modems—up to 1.5 Mbps downstream and up to 500 Kbps upstream. G.lite is an International Telecommunications Union (ITU) standard, globally standardized interoperable ADSL system per ITU G.992.2. G.lite has seen comparatively little use, but it did introduce the valuable concept of splitterless installation (15).

Gateway Lower Layer (GLL) Component of the lower layer in an M2M gateway.

General Packet Radio Service (GPRS) Packet-switched functionality for GSM, which is essentially circuit switched. GPRS is the essential enabler for always-on data connection for applications such as web browsing and push-to-talk over cellular. GPRS was introduced into the GSM specifications in Release 97, and usability was further approved in Releases 98 and 99. It offers faster data rates than plain GSM by aggregating several GSM time slots into a single bearer, potentially up to eight, giving a theoretical data rate of 171 Kbps. Most operators do not offer such high rates, because obviously if a slot is being used for a GPRS bearer, it is not available for other traffic. Also, not all mobiles are able to aggregate all combinations of slots. The "GPRS class number" indicates the maximum speed capability of a terminal, which might be typically 14 Kbps in the uplink direction and 40 kbit/s in the downlink, comparable with the rates offered by current wireline dial-up modems. Mobile terminals are further classified according to whether or not they can handle simultaneous GSM and GPRS connections: class A = both simultaneously, class B = GPRS connection interrupted during a GSM call, automatically resumed at end of call, class C = manual GSM/GPRS mode switching. Further data rate increases have been achieved with the introduction of EDGE (17).

Geostationary Orbit/Satellite The orbit of a geosynchronous satellite whose orbit lies in the plane of the earth's equator. A satellite orbiting the earth at such speed that it permanently appears to remain stationary with respect to the earth's surface.

Geosynchronous Object An object orbiting the earth at the earth's rotational speed and with the same direction of rotation. The object appears at the same position in the sky at a particular time each day, but will not appear stationary if it is not orbiting in the equatorial plane.

GLOB Addressing RFC 2770 recommended that the 233.0.0.0/8 address range be reserved for statically defined addresses by organizations that already have an AS number reserved. The AS number of the domain is embedded into the second and third octets of the 233.0.0.0/8 range. GLOP is a mechanism that allocates multicast addresses to ASs. (GLOP is neither an acronym nor an abbreviation.)

Global Address See aggregatable global unicast address.

GPRS (General Packet Radio Service) A mobile packet data service available to users of GSM. It provides data rates of up to 40–170 Kbps, depending upon device capabilities, network configurations, and system load.

Group-Based Machine-Type Communications (MTC) Feature A group-based MTC feature is an MTC feature that applies to an MTC group. This is a 3GPP concept (22).

Group Identifier Last 112 bits (for predefined multicast addresses) or last 32 bits (for new multicast addresses) of an IPv6 multicast address used to identify a multicast group (RFC2373).

GSM (Global System for Mobile Communications) GSM is a global cellular network standard, but used mostly outside the U.S.

GSM EDGE Radio Access Network (GERAN) GERAN is a radio access network architecture, based on GSM/EDGE radio access technologies. GERAN is the term given to the second-generation digital cellular GSM radio access technology, including its evolutions in the form of EDGE and, for most purposes, the GPRS. The GERAN is harmonized with the UMTS terrestrial radio access network (UTRAN) through a common connectivity to the UMTS core network making it possible to build a combined network for GSM/GPRS and UMTS. GERAN is also the name of the 3GPP™ Technical Specification Group responsible for its development. The Technical Specifications which together comprise a 3GPP system with a GERAN are listed in 3GPP TS 41.101.

HDSL (High Data Rate DSL) A DSL variety created in the late 1980s delivers symmetric service at speeds up to 2.3 Mbps in both directions. Available at 1.5 or 2.3 Mbps, this symmetric fixed rate application does not provide standard telephone service over the same line and is already standardized through ETSI and ITU. Seen as an economical replacement for T1 or E1, it uses one, two, or three twisted copper pairs (15).

HDSL2 (Second-Generation HDSL) A variant of DSL that delivers 1.5 Mbps service each way, supporting voice, data, and video using either ATM (asynchronous transfer mode), private-line service, or frame relay over a single copper pair. This ATIS standard (T1.418) for this symmetric service gives a fixed 1.5 Mbps rate both up and downstream. HDSL2 does not provide standard voice telephone service on the same wire pair. HSDL2 differs from HDSL in that HDSL2 uses one pair of wires to convey 1.5 Mbps, whereas ANSI HDSL uses two wire pairs (15).

HDSL4 A HDSL that is virtually the same as HDSL2 except it achieves about 30% greater distance than HDSL or HDSL2 by using two pairs of wire (thus, four conductors), whereas HDSL2 uses one pair of wires (15).

Hierarchical Storage Management (HSM) A storage system in which new, frequently used data is stored on the fastest, most accessible (and generally more expensive) media (e.g., RAID) and older, less frequently used data is stored on slower (less expensive) media (e.g., tape) (23).

Higher-Level Checksum A checksum based on the IPv6 pseudo-header, used in ICMPv6, TCP, and UDP.

Higher-Level Protocol Protocol that uses IPv6 as transport and is carried as a payload in IPv6, such as ICMPv6, TCP, and UDP.

Home Area Network (HAN) A local area network (LAN) applicable to a residential home. Can be wired or wireless.

Home Network (HN) A communication system designed for the residential environment, in which two or more devices exchange information.

Hop-By-Hop Option Header An IPv6 extension header that contains options that must be processed by all intermediate routers as well as final router.

Host Any node that is not a router.

Host-To-Host Tunnel An IPv6 over IPv4 tunnel where endpoints are hosts.

Host-To-Router Tunnel An IPv6 over IPv4 tunnel in which the tunnel begins at a host and ends at an IPv6/IPv4 router.

HTTP Streaming The default higher-layer protocol for streaming audio and video over the Internet. It involves the simultaneous download and viewing/listening of the file through HTTP (24).

Hypertext Transfer Protocol (HTTP) An application-level, stateless, object-oriented protocol for distributed, collaborative, hypermedia information systems.

ICC Terminal/integrated circuit card

ICMPv6 See Internet control message protocol for IPv6.

IEEE 802.11v 802.11v, wireless network management, is an extension of existing 802.11 Wi-Fi devices first proposed in 2004 to add some networking capabilities to Wi-Fi systems and to address power management issues. 802.11v automatically cutting power to the Wi-Fi chip when it is not being used. Specifically, it provides further extension to base 802.11 power saving, which allows for longer power-off times for 802.11 radios; it enables "wake on WLAN." The access point responds to address resolution protocol (ARP) requests to enable stations to power down for longer periods (25). As of press time, balloting on P802.11v D15.0 had closed; however, an additional recirculation ballot had taken place to address assigned number issues discovered subsequently in industry interoperability testing.

IEEE 802.15.4 IEEE standard for local and metropolitan area networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs). IEEE 802.15.4-conformant devices support a wide range of industrial and commercial applications. The amended MAC sublayer facilitates industrial applications such as process control and factory automation in addition to the MAC behaviors that support the Chinese wireless personal area network (CWPAN) standard.

IEEE 802.15.4j (TG4j) Medical Body Area Networks The purpose of Task Group 4j (TG4j) is to create an amendment to 802.15.4, that defines a physical layer for IEEE 802.15.4 in the 2360 to 2400 MHz band and complies with Federal Communications Commission (FCC) MBAN rules. The amendment may also define modifications to the MAC needed to support this new physical layer. This amendment allows 802.15.4- and MAC-defined changes to be used in the MBAN band (26).

IEEE 802.1ad IEEE 802.1ad (provider bridges) is an amendment to IEEE standard IEEE 802.1Q-1998, intended to develop an architecture and bridge protocols to provide separate instances of the MAC services to multiple independent users of a bridged LAN in a manner that does not require cooperation among the users and requires a minimum of cooperation between the users and the provider of the MAC service. This is a standard version of the Q-in-Q protocol used by Cisco for carrier Ethernet service (11).

IEEE 802.1ah Provider backbone bridges (PBBs) is being formalized by IEEE 802.1ah standards. It allows for layering the Ethernet network into customer and provider domains with complete isolation among their MAC addresses. It defines a B-DA and B-SA to indicate the backbone source and destination address. It also defines B-VID (backbone Virtual LAN (VLAN) ID) and I-SID (service instance VLAN ID).

IEEE 802.1q IEEE 802.1Q was a project in the IEEE 802 standards process to develop a mechanism to allow multiple bridged networks to transparently share the same physical network link without leakage of information between networks (i.e., trunking). IEEE 802.1Q is also the name of the standard issued by this process, and in common usage the name of the encapsulation protocol used to implement this mechanism over Ethernet networks. IEEE 802.1Q also defines the meaning of a virtual LAN or VLAN with respect to the specific conceptual model underpinning bridging at the MAC layer and to the IEEE 802.1D-spanning tree protocol. This protocol allows for individual VLANs to communicate with one another with the use of a layer 3 (network) router (11).

IETF-Constrained RESTful Environments (CoRE) Working Group IETF Working Group that is working on standardization for constrained networks, such as, but not limited to, low-power and lossy networks (LLNs). LLN is class of networks in which both the routers and their interconnects are constrained. LLN routers typically operate with constraints on processing power, memory, and energy (battery power).

IMEI International mobile equipment identity.

IMEISV International mobile equipment identity and software version.

Inclination (Satellite) The angle between the plane of the orbit of a satellite and the earth's equatorial plane. An orbit of a perfectly geostationary satellite has an inclination of 0.

Inclined Orbit An orbit that approximates the GEO but whose plane is tilted slightly with respect to the equatorial plane. The satellite appears to move about its nominal position in a daily "figure-of-eight" motion when viewed from the ground.

Spacecrafts (satellites) are often allowed to drift into an inclined orbit near the end of their nominal lifetime in order to conserve on-board fuel, which would otherwise be used to correct this natural drift caused by the gravitational pull of the sun and moon. North–South maneuvers are not conducted, allowing the orbit to become highly inclined.

Incoming Interface (iif) In protocol-independent multicast-sparse mode (PIM-SM), the iif of a multicast route entry indicates the interface from which multicast data packets are accepted for forwarding. The iif is initialized when the entry is created (27).

Industrial, Scientific, and Medical (ISM) Radio Bands The ISM radio bands are radio bands allocated internationally for the said purpose. The ISM bands are defined by the ITU-R in 5.138, 5.150, and 5.280 of the radio regulations. In the United States, uses of the ISM bands are governed by Part 15 and Part 18 of the FCC rules. There are a number of ISM bands, but the most well known is the one covering the 2400–2500 MHz region (some other bands include allocations a 6.7 MHz, 13.5 MHz, 26.9 MHz, 40.6 MHz, 433 MHz, 902 MHz, and 5725 MHz.)

Infrared Data Association (IrDA®) IrDA is an SIG consisting of about 40 members at press time. The SIG is pursuing a 1 Gbps connectivity link; however, this link only operates over a distance of less than 10 cm. One of the challenges with infrared (IR) signaling is its requirement for line-of-sight (LOS) requirement. Additionally, IrDA is also not very power efficient (power per bit) when compared with radio technologies.

Integrated Services Digital Network DSL (ISDL) A form of DSL that supports symmetric data rates of up to 144 Kbps using existing phone lines. It is unique in that it has the ability to deliver services through a DLC (digital loop carrier: a remote device often placed in newer neighborhoods to simplify the distribution of cable and wiring from the phone company). While DLCs provide a means of simplifying the delivery of traditional voice services to newer neighborhoods, they also provide a unique challenge in delivering DSL into those same neighborhoods. IDSL addresses this market along with ADSL and G.lite as they are implemented directly into those DLCs. IDSL differs from its relative ISDN in that it is an "always-available" service, but capable of using the same terminal adapter, or modem, used for ISDN (15).

Integrity The property that data has not been altered or destroyed in an unauthorized manner.

Interface A node's attachment to a link. A representation of a physical or logical link of a node to a link. An example of a physical interface is a network interface. An example of a logical interface is a tunnel interface.

Interface Identifier Last 64 bits of a unicast or anycast IPv6 address.

Intermediary (in the CoAP Environment) A CoAP endpoint that acts both as a server and as a client toward (possibly via further intermediaries) an origin server. There are two common forms of intermediary: proxy and reverse proxy. In some cases, a single endpoint might act as an origin server, proxy, or reverse proxy, switching behavior based on the nature of each request (28).

Internet-Based TV (IBTV) Video distribution approaches such as Web television, Internet television, and/or user-generated video (UGV).

Internet Control Message Protocol for IPv6 (ICMPv6) Protocol for internet control messages for IPv6. A protocol that provides error messages for the routing and delivery of IPv6 datagrams and information messages for diagnostics, neighbor discovery (ND), multicast receiver discovery, and IPv6 mobility.

Interrogator In RFID environments, a device that modulate/transmit and receive/demodulate a sufficient set of the electrical signals defined in the signaling layer to communicate with conformant tags while conforming to all local radio regulations. A typical interrogator is a passive-backscatter, interrogator-talks-first (ITF), RFID system operating in the 860 MHz–960 MHz frequency range. An interrogator transmits information to a tag by modulating an RF signal in the 860 MHz–960 MHz frequency range. The tag receives both information and operating energy from this RF signal. Tags are passive, meaning that they receive all of their operating energy from the interrogator's RF waveform. An interrogator receives information from a tag by transmitting a continuous-wave (CW) RF signal to the tag; the tag responds by modulating the reflection coefficient of its antenna, thereby backscattering an information signal to the interrogator (7).

Interworking Mechanisms for IPv6 and IPv4 Well-known interworking mechanisms include (29):

- Dual stack: A technique for providing complete support for both protocols—IPv4 and IPv6—in hosts and routers.
- Configured tunneling of IPv6 over IPv4: Manually configured point-to-point tunnels for encapsulating IPv6 packets within IPv4 headers to carry them over an IPv4 routing infrastructures.
- Automatic tunneling of IPv6 over IPv4: Mechanisms for automatically tunneling IPv6 packets over IPv4 networks.
- Translation: Refers to the direct conversion of protocols.

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) An IPv6 transition technology that provides IPv6 unicast connectivity between devices placed in an IPv4 intranetwork. ISATAP obtains an interface identifier from the IPv4 address (public or private) assigned to the device. This identifier is used for the establishment of automatic tunnels through the IPv4 infrastructure (16).

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Address An IPv6 address of the form 64-bit prefix:0:5EFE:w.x.y.z, where w.x.y.z is a public or private IPv4 address allocated to an ISATAP device.

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Device A device to which an ISATAP address is assigned to.

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Name The name "ISATAP" is resolved by computers with Windows XP or Windows Server 2003 operating system to automatically discover the ISATAP router address for initial configuration.

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Router An IPv6/IPv4 router that answers ISATAP node requests and routes traffic to and from ISATAP nodes.

IP Multimedia Subsystem (IMS) IMS is a 3GPP/3GPP2 initiative to define an all IP-based wireless network as an evolution from historically distinct voice, data, signaling, and control network elements.

IP Over Ethernet (IPoE) IP over Ethernet is used in DSL and PON access networks in place of PPPoE.

IP Storage Using IP and gigabit Ethernet to build storage area networks (SANs). Traditional SANs were developed using the FC transport, because it provided gigabit speeds compared to 10 and 100 Mbps Ethernet used to build messaging networks at that time. FC equipment has been costly, and interoperability between different vendors' switches was not completely standardized. Since gigabit Ethernet and IP have become commonplace, IP storage enables familiar network protocols to be used, and IP allows SANs to be extended throughout the world. Variants include:

- Internet FCP (iFCP)
- Metro fiber channel protocol (mFCP)
- Internet small computer system interface (iSCSI)
- Fiber channel over Internet protocol (FCIP)

IP6.arpa The DNS domain created for the IPv6 reverse resolution (RFC 3596). The reverse resolution has the purpose of "reverse mapping" of IPv6 addresses to DNS names.

IPoDWDM Optical Network Carriage of IP packets directly over the optical layer provided by a dense-wavelength division multiplexing optical system.

IPSO Alliance The IPSO Alliance is an advocate for IP networked devices for use in energy, consumer, healthcare, and industrial applications. The objective of the Alliance is not to define technologies or standards, but to document the use of IP-based technologies defined at the standard organizations such as IETF with focus on support by the Alliance of various use cases.

IPv4 Node A node that implements IPv4; it can send and receive IPv4 packets. It can be an IPv4-only node or a dual IPv4/IPv6 node.

IPv4-Compatible IPv6 Address A 0:0:0:0:0:0:w.x.y.z or ::w.x.y.z address, where w.x.y.z is the decimal representation of a public IPv4 address. For example, ::131:107:89:42 is an IPv4-compatible address. IPv6 transition mechanisms no longer use IPv4-compatible address scheme.

IPv4-Mapped IPv6 Address A 0:0:0:0:0:FFFF:w.x.y.z (or ::FFFF:w.x.y.z) address, where w.x.y.z is the IPv4 address of an IPv4-only node. Mapped IPv4 addresses are used to represent an IPv4-only host.

IPv6 in IPv4 See IPv6 over IPv4 tunnel.

IPv6 Node Node that implements IPv6; it can send and receive IPv6 packets. An IPv6 node can be an IPv6-only node or a dual IPv6/IPv4 node.

IPv6 Over IPv4 Tunnel Encapsulating IPv6 packets into an IPv4 datagram and transporting the datagram over an IPv4 infrastructure. In the IPv4 header, the protocol field value is 41.

IPv6 Prefixes The initial bits of an IP address. The number of bits is represented via the prefix-length notation. Prefixes for IPv6 routes and subnet identifiers are expressed in the same way as classless interdomain routing (CIDR) notation for IPv4. For example, 21DA:D3::/48 is a route prefix and 21DA:D3:0:2F3B::/64 is a subnet prefix. IPv4 implementations commonly use a dotted decimal representation of the network prefix known as the subnet mask. A subnet mask is not used in IPv6. Only the prefix-length notation is used (4).

IPv6 Routing Protocol for LLNs (RPL) A mechanism proposed by the IETF to support multipoint-to-point traffic from devices inside LLNs toward a central control point, as well as point-to-multipoint traffic from the central control point to the devices inside the LLN (30).

IPv6 Routing Table Set of routes used to determine the next node address and interface when forwarding IPv6 traffic.

IPv6/IPv4 Node A node that has both IPv4 and IPv6 implementations.

ISA100.11a ISA SP100 standard for wireless industrial networks developed by the International Society of Automation (ISA) to address all aspects of wireless technologies in a plant. The ISA100 Committee addresses wireless manufacturing and control systems in the areas of the: (i) environment in which the wireless technology is deployed; (ii) technology and life cycle for wireless equipment and systems; and (iii) application of wireless technology. The wireless environment includes the definition of wireless, radio frequencies (starting point), vibration, temperature, humidity, EMC, interoperability, coexistence with existing systems, and physical equipment location. ISA100.11a Working Group Charter addresses (31):

- Low-energy consumption devices, with the ability to scale to address large installations
- Wireless infrastructure, interfaces to legacy infrastructure and applications, security, and network management requirements in a functionally scalable manner
- Robustness in the presence of interference found in harsh industrial environments and with legacy systems
- Coexistence with other wireless devices anticipated in the industrial work space
- Interoperability of ISA100 devices

Key A digital code used to encrypt, sign, decrypt, and verify messages and files. A sequence of symbols that controls the operations of encipherment and decipherment.

Key Management Generation, distribution, storage, replacement, and destruction of keys.

Key Pair A public key and its complementary private key. In public-key systems, each user has at least one key pair.

KNX and KNX-RF KNX (administered by the KNX Association) is an OSI-based network communications protocol for intelligent buildings defined in standards CEN EN 50090 and ISO/IEC 14543. KNX is the follow-on standard built on the European Home Systems Protocol (EHS), BatiBUS, and the European Installation Bus (EIB or Instabus). Effectively, KNX uses the communication stack of EIB but augmented with the physical layers and configuration modes BatiBUS and EHS; thus, KNX includes the following PHYs:

- Twisted pair wiring (inherited from the BatiBUS and EIB Instabus standards). This approach uses differential signaling with a signaling speed of 9.6 Kbps. MAC is controlled with the CSMA/CA method;
- Powerline networking (inherited from EIB and EHS);
- Radio (KNX-RF);
- IR; and
- Ethernet (also known as EIBnet/IP or KNXnet/IP).

Layer 2 Layer 2 of the protocol stack. This typically refers to the set of Ethernet protocols that operate below the IP layer of the protocol stack.

Layer 2 Tunneling Protocol (L2TP) Layer 2 tunneling protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs).

Layer 3 Layer 3 of the open systems interconnection (OSI) protocol stack. This refers to the IP used for routing in the Internet.

Lifetime in Preferred State Time during which a unicast address, obtained by means of stateless autoconfiguration mechanism, stays in the preferred state. This time is specified by the preferred lifetime field in Routers Advertisement message prefix information option.

Limited Scope Addresses (also known as Administratively Scoped Addresses) The range of addresses from 239.0.0.0 through 239.255.255.255. RFC2365 defines these addresses to be limited to a local group or organization (RFC2365). Routers are required to be configured with packet filters to prevent multicast traffic in this address range from flowing outside of an AS.

Link A communication facility or medium over which nodes can communicate at the link layer, i.e., the layer immediately below IPv6. Examples include Ethernet environments (simple or bridged); PPP links; X.25 Packet Switching, Frame Relay, Cell Relay/ATM; or IPv4.

Link-Local Addresses IP multicast addresses that have been reserved for specific functions. Addresses in the 224.0.0.0 through 224.0.0.255 are reserved to be used by network protocols on a local network segment. Network protocols make use

of these addresses for automatic router discovery and to communicate routing information (e.g., OSPF uses 224.0.0.5 and 224.0.0.6 to exchange link state information). IP packets with these addresses are not forwarded by a router; they remain local on a particular LAN segment (they have a time-to-live [TTL] parameter set to 1; even if the TTL is different from 1, they still are not forwarded by the router).

Link State Routing Protocol A routing protocol in which a router informs all the nodes in a network of topology changes. Information exchanged consists of prefixes of networks connected to the router and their associated cost. This is in contrast to distance vector routing protocols that exchange routing table information but only with neighboring nodes.

Link-Layer Identifier A link-layer identifier for an interface. Examples include IEEE 802 addresses for Ethernet or token ring network interfaces and E.164 addresses for ISDN links.

Link-Local Address An IPv6 address having a link-only scope, indicated by the prefix (FE80::/10), which can be used to reach neighboring nodes attached to the same link. Every interface has a link-local address.

Local Address An IPv6 unicast address that is not reachable on IPv6 Internet. Local addresses include "link-local" and "site-local" addresses.

Local Interface Internal interface that allows a node to send packets to itself.

Long-Term Evolution (LTE) (aka 4G) LTE is a project named an "all IP" standard for mobile traffic that will increase the broadband capabilities beyond current 3G mobile technologies. LTE is the 3GPP initiative to evolve the UMTS technology toward a fourth generation (4G.) LTE can be viewed as an architecture framework and a set of ancillary mechanisms that aims at providing seamless IP connectivity between User Equipment (UE) and the packet (IPv4, IPv6) data network without any disruption to the end-users' applications during mobility. In contrast to the circuit-switched model of previous-generation cellular systems, LTE has been designed to support *only* packet-switched services.

Loopback Address The IPv6 address—0:0:0:0:0:0:0:1 or ::1—assigned to the local interface.

Low-Power and Lossy Networks (LLNs) A class of network in which both the routers and their interconnects are constrained. LLN routers typically operate with constraints on processing power, memory, and energy (battery power). Their interconnects are characterized by high loss rates, low data rates, and instability (30).

Lower Layer (LL) Allows DSCL, GSCL, and NSCL components to exchange data on behalf of applications and perform other appropriate communication.

M2M (Machine-to-Machine) Term used to refer to M2M communication, i.e., automated data exchange between machines. ("Machine" may also refer to virtual machines such as software applications.) M2M is an enabler of the Internet of things (IoT).

M2M Area Network Layer Provides the communication between DA/GA components and DSCL/GSCL components.

M2M Service Provider's Domain Domain that includes the network application domain and any standardized systems under the control of the M2M service provider which interact with the M2M service capabilities.

M2M System Comprises network application domain, M2M devices domain, and any interfaces or networks required to connect those entities.

MAC Address A link-layer address for LAN technologies such as Ethernet and token ring. It is also referred to as a physical address, hardware address, or network adapter address.

MAC Header The link-layer header of the IEEE 802.3 standard or Ethernet v2. It consists of a 6B destination address, 6B source address, and 2B type field (see also NPA, LLC) (32).

Machine (Host) A node that cannot send datagrams not created by itself. A machine (host) is both the source and destination of IPv6 traffic and will discard traffic that is not specifically addressed to it.

Machine-to-Machine (M2M) Communication Communication between remotely deployed (generally low-end) devices with specific responsibilities and requiring little or no human intervention, which are all connected to an application server via the mobile network data communications.

Machine-Type Communications (MTC) M2M system communication as described by the 3GPP.

Machine-Type Communications (MTC) Device An MTC device is a UE equipped for MTC, which communicates through a *public land mobile network* (PLMN) with MTC server(s) and/or other MTC device(s).

NOTE: An MTC device might also communicate locally (wirelessly, possibly through a PAN, or hardwired) with other entities which provide the MTC device "raw data" for processing and communication to the MTC server(s) and/or other MTC device(s). This is a 3GPP concept (22).

Machine-Type Communications (MTC) Feature MTC features are network functions to optimize the network for use byM2M applications. This is a 3GPP concept (22).

Machine-Type Communications (MTC) Group An MTC group is a group of MTC devices that share one or more group-based MTC features and that belong to the same MTC subscriber. This is a 3GPP concept (22).

Machine-Type Communications (MTC) Server An MTC server is an entity, which communicates to the PLMN itself, and to MTC devices through the PLMN. The MTC server also has an interface that can be accessed by the MTC user. The MTC server performs services for the MTC user. This is a 3GPP concept (22).

Machine-Type Communications (MTC) User An MTC user uses the service provided by the MTC server. This is a 3GPP concept (22).

Maximum Transmission Unit (MTU) Maximum transmission unit (MTU) refers to the size (in bytes) of the largest packet that a given layer of a communications

protocol can pass onward. MTUs are defined at the link layer (frame maximum size) and at the network or Internet layer (maximum IPv6 packet size).

Maximum-Level Aggregation Identifier (aka top-level aggregation identifier—TLA ID). Thirteen-bit field inside the global unicast address reserved for large organizations or ISP by the IANA; hence, it identifies the address range that they have delegated. The TLA scheme has been obsolete by RFC 3587.

M-BUS The M-Bus ("Meter-Bus") is a European standard for remote reading of gas and electric meters; it is also usable for all other types of consumption meters. It is specified as follows:

- EN 13757-2 (physical and link layer)
- EN 13757-3 (application layer)
- Note: the frame layer uses IEC 870 and the network (packet layer) is optional.

A radio variant of M-Bus (wireless M-Bus) is also specified in EN 13757-4.

Media Access Control (MAC) Media access and control of the Ethernet IEEE 802 standard and protocols (18). Its functionalities include the creation of frames and the management of medium sharing and access.

Medical Body Area Network System (MBANS) Low-power radio system used for the transmission of non-voice data to and from medical devices for the purposes of monitoring, diagnosing, and treating patients as prescribed by duly authorized healthcare professionals (33).

MEO satellite A satellite with an earth orbit within the range from a few hundred miles to a few thousand miles above the earth's surface; this orbit is called medium earth orbit, hence MEO. MEO satellites orbit higher than LEO satellites, but lower than geostationary (GEO) satellites.

MEID Mobile equipment identifier.

mHealth A term for eHealth services using mobile phones or cellular networks.

Mobility The ability for the end-user or other mobile entities to communicate and access services irrespective of changes of the location or technical environment.

Motion Picture Expert Group (MPEG) A family of standards used for coding audio-visual information (e.g., movies, video, music) in a digitally compressed format. There are three major MPEG standards: MPEG-1, MPEG-2, and the newer MPEG-4. Both MPG-2 and MPEG-4 are important for IPTV, but the recent trend is in favor of MPEG-4.

MPEG-2 (Motion Picture Experts Group-2) A set of multiplexing/encoding standards specified by the Motion Picture Experts Group (MPEG) and standardized by the International Organization for Standardization (ISO/IEC 113818-1) and ITU-T (H.220).

MPLS VPN A layer 3 virtual IP network specified by RFC2547bis. It used a combination of border gateway protocol (BGP) routing and MPLS forwarding to create

a virtual IP network on top of a service provider's physical IP network. MPLS VPN services are replacing frame relay and ATM services (11).

Multicast A methodology and supporting mechanisms, technologies, and standards for distribution of information (including video content) over the Internet. Multicast allows a server to inject a single copy of a given content into the Internet and many receivers (computers, smart phones, Internet-ready TV sets, and so on), but not the entire universe of receivers as would be the case in broadcast, to receive and play the same stream simultaneously.

Multicast Address An address that identifies several interfaces and is used to deliver data from one source to several destinations. That is, an identifier for a set of interfaces typically belonging to different nodes. By means of the multicast routing topology, packets to a multicast address will be delivered to all interfaces identified by that address.

An identifier for a group of nodes. An IP multicast address or group address, as defined in "Host Extensions for IP Multicasting," STD 5, RFC 1112, August 1989, and in "IP Version 6 Addressing Architecture," RFC2373, July 1998. The Internet Assigned Numbers Authority (IANA) controls the assignment of IP multicast addresses. IANA has allocated what has been known as the Class D address space to be utilized for IP multicast. IP multicast group addresses are in the range 224.0.0.0 through 239.255.255.255.

Multicast Address Dynamic Client Allocation Protocol (MADCAP) A protocol defined in RFC2730 that allows hosts to request multicast addresses from multicast address allocation servers. This protocol is part of the IETF Multicast Address Allocation Architecture (34).

Multicast Address Set Claim Protocol (MASC) Protocol defined in RFC2909 that can be used for interdomain multicast address set allocation. MASC is used by a node (typically a router) to claim and allocate one or more address prefixes to that node's domain. While a domain does not necessarily need to allocate an address set for hosts in that domain to be able to allocate group addresses, allocating an address set to the domain does ensure that interdomain group-specific distribution trees will be locally rooted, and that traffic will be sent outside the domain only when and where external receivers exist (35).

Multicast Environment Environment where one system communicates to a select group of other systems.

Multicast Group Set of interfaces listening to a specific multicast address.

Multicast IPv4 Tunnel See 6over4.

Multicast Listener Discovery Protocol (MLDv2) MLDv2 is an MLD protocol that is used by an IPv6 router to discover the presence of multicast listeners on directly attached links, and to discover which multicast addresses are of interest to those neighboring nodes. MLDv2 is designed to be interoperable with MLDv1. MLDv2 adds the ability for a node to report interest in listening to packets with a particular multicast address only from specific source addresses or from all sources except for specific source addresses (36).

The Internet Group Management Protocol (IGMP) (RFC1112, IGMPv2, IGMPv3) allows an IPv4 host to communicate IP multicast group membership information to its neighboring routers; IGMPv3 provides the ability for a host to selectively request or filter traffic from individual sources within a multicast group. MLD defined in RFC2710 (MLDv2) offers similar functionality for IPv6 hosts. MLDv2 provides the analogous "source filtering" functionality of IGMPv3 for IPv6 (37).

Multicast OSPF (MOSPF) Protocol defined in RFC 1584 that provides enhancements to OSPF Version 2 to support IP multicast routing. With MOSPF, an IP multicast packet is routed based both on the packet's source and on its multicast destination (commonly referred to as source/destination routing). As it is routed, the multicast packet follows a shortest path to each multicast destination. During packet forwarding, any commonality of paths is exploited; when multiple hosts belong to a single multicast group, a multicast packet will be replicated only when the paths to the separate hosts diverge.

OSPF, a link-state routing protocol, provides a database describing the AS's topology. A new OSPF link state advertisement has been added describing the location of multicast destinations. A multicast packet's path is then calculated by building a pruned shortest-path tree (SPT) rooted at the packet's IP source. These trees are built on demand, and the results of the calculation are cached for use by subsequent packets (38).

Multicast Payload Forwarding Communication mechanism to forward payload. Almost invariably, this is IP based at the network layer. Typical IP multicast applications make use of user datagram protocol (UDP) at the transport layer; however, TCP can also be used in same applications.

Multicast Routing A mechanism to build distribution trees that define a unique forwarding path between the subnet of the content source and each subnet containing members of the multicast group, specifically, receivers.

Multicast Routing Information Base (MRIB) This is the multicast topology table, which is typically derived from the unicast routing table, or from routing protocols such as MBGP that carry multicast-specific topology information. PIM-DM uses the MRIB to make decisions regarding RPF interfaces (39).

Multicast Scope A range of multicast addresses configured so that traffic sent to these addresses is limited to some subset of the internetwork. Defined in "Administratively Scoped IP Multicast," BCP 23, RFC2365, July 1998.

Multicast Source Discovery Protocol (MSDP) A protocol that allows multiple PIM-SM domains to share information about active sources. The protocol announces active sources to MSDP peers. It is a BGP-like protocol that allows a rendezvous point (RP) to forward source and multicast group information to other RPs (e.g., to support redundant RPs or multidomain applications where each ISP can each have its own RP(s)) (40).

Multichannel audio Audio signal with more than two channels.

Multiprotocol Border Gateway Protocol (MP-BGP) (also referred to by the acronym form MBGP) A protocol that defines multiprotocol extensions to the BGP, the unicast interdomain protocol that supports multicast-specific routing information. MP-BGP augments BGP to enable multicast routing policy and connect multicast topologies within and between BGP ASs. It carries multiple instances of routes for unicast routing as well as multicast routing. Protocol that carries routing information about several protocols, including IP multicast (and also IPv6 and MPLS VPN information, among others). In IP multicast, MP-BGP carries a separate copy of unicast routes. MP-BGP helps establish which links the PIM join messages use, which in turn allows us to control which links the multicast traffic traverses (40).

Name Resolution Procedure to obtain an IP address from a name.

Named Data Networking (NDN) A proposed architecture that moves the communication paradigm from today's focus on "where," i.e., addresses, servers, and hosts, to "what," i.e., the content that users and applications care about. By naming data instead of their location (IP address), NDN transforms data into first-class entities. While the current Internet secures the communication channel or path between two communication points and sometimes the data with encryption, NDN secures the content and provides essential context for security. This approach allows the decoupling of trust in data from trust in hosts and servers, enabling trustworthiness as well as several radically scalable communication mechanisms, for example, automatic caching to optimize bandwidth and the potential to move content along multiple paths to the destination (41). This architecture may be applicable to the IoT.

Near-Field Communication (NFC) A group of standards for devices such as PDAs, smartphones, and tablets that support the establishment of wireless communication when such devices are in immediate proximity of a few inches. These standards encompass communications protocols and data exchange formats; they are based on existing RFID standards including ISO/IEC 14443 and FeliCa (a contactless RFID smart card system developed by Sony, for example utilized in electronic money cards in use in Japan). NFC standards include ISO/IEC 18092, as well as other standards defined by the NFC Forum. NFC standards allow two-way communication between endpoints (earlier generation systems were one-way systems only). Unpowered NFC-based tags can also be read by NFC devices; hence this technology can substitute for earlier one-way systems. Applications of NFC include contactless transactions.

Neighbor Discovery (ND) A set of messages and ICMPv6 processes that fixes the relations between neighbor nodes. ND replaces ARP, ICMP routes discovery, and ICMP redirection messages used in IPv4. It also provides inaccessible neighbor detection.

Neighbor Discovery Options Options in an ND message that show link-layer addresses, information about prefixes, MTU, and routes and configuration information for IPv6 mobility.

Neighbors Nodes connected to the same link.

Neighbors Cache A cache supported by each IPv6 node that stores the IP address of its neighbors on the link, its corresponding link-layer address, and an indication of its accessibility state. Neighbors cache is equivalent to the ARP cache in IPv4.

Network Address Translation-Protocol Translation (NAT-PT) Process performed by a network device on the boundary of an IPv4 and IPv6 network. NAT-PT uses a pool of IPv4 addresses for dynamic assignment to the IPv6 nodes. NAT-PT also allows the multiplexing of multiple sessions on a single IPv4 address via the "port" field.

Network Addresses Translator (NAT) A device that translates IP addresses and port numbers when forwarding packets between a network with private addresses and the Internet.

Network Point of Attachment (NPA) A 6-byte destination address (resembling an IEEE MAC address) within the MPEG-2 transmission network that is used to identify individual receivers or groups of receivers (32).

Network-Attached Storage (NAS) A disk array storage system that is attached directly to a network rather than to the network server (i.e., host attached). It functions as a server in a client/server relationship; has a processor, an operating system, or micro-kernel; and processes file I/O protocols such as SMB and NFS (23).

Next-Generation Network (NGN) According to ITU-T Recommendation Y.2001 (12/2004) "General overview of NGN," an NGN is a packet-based network able to provide Telecommunication Services to users and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent of the underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and services of their choice. It supports generalized mobility, which will allow consistent and ubiquitous provision of services to users.

The NGN is characterized by the following fundamental aspects:

- Packet-based transfer
- Separation of control functions among bearer capabilities, call/session, and application/service
- Decoupling of service provision from transport and provision of open interfaces
- Support for a wide range of services, applications, and mechanisms based on service building blocks (including real-time/streaming/non-real-time services and multimedia)
- Broadband capabilities with end-to-end QoS and transparency
- Interworking with legacy networks via open interfaces
- Generalized mobility
- Unfettered access by users to different service providers
- A variety of identification schemes which can be resolved to IP addresses for the purposes of routing in IP networks
- Unified service characteristics for the same service as perceived by the user

- Converged services between fixed and mobile networks
- Independence of service-related functions from underlying transport technologies
- Support of multiple last mile technologies
- Compliant with all regulatory requirements, for example concerning emergency communications and security/privacy.

Next-Level Aggregation Identifier (NLA ID) 24-bit field inside the global unicast aggregatable address that allows the creation of several hierarchical levels of addressing to organize addresses and routing to other ISPs, as well as to identify organization sites. The NLA scheme has been obsolete by RFC 3587.

NIKE+® A proprietary wireless technology developed by Nike and Apple to allow users to monitor their activity levels while exercising. Its power consumption is relatively high, returning only 40 days of battery life from a coin cell. It is a proprietary radio that only works between Nike and Apple devices. Nike+ devices are shipped as a single unit: processor, radio, and sensor (10).

NIT (Network Information Table) MPEG signaling table that contains details of the bearer network used to transmit the MPEG multiplex, including the carrier frequency (PID=10) (12).

Node A device that implements IP.

Node Types Node types in an IPv6 environment include the following (29):

- IPv4-only node: A host or router that implements only IPv4. An IPv4-only node does not understand IPv6. The installed base of IPv4 hosts and routers existing before the transition to IPv6 begins are IPv4-only nodes.
- IPv6/IPv4 node: A host or router that implements both IPv4 and IPv6.
- IPv6-only node: A host or router that implements IPv6 and does not implement IPv4.
- IPv6 node: Any host or router that implements IPv6. IPv6/IPv4 and IPv6-only nodes are both IPv6 nodes.
- IPv4 node: Any host or router that implements IPv4. IPv6/IPv4 and IPv4-only nodes are both IPv4 nodes.

Non-Broadcast Multiple Access (NBMA) A link-layer technology that supports links with more than two nodes, but without allowing the sending of a packet to all nodes on the link (broadcast). Example technologies include X.25 packet-switching service, frame relay service, and cell relay service/ ATM.

Non-Broadcast Networks A network supporting the attachment of more than two stations, but not supporting the delivery of a single physical datagram to multiple destinations (i.e., not supporting data-link multicast). OSPF describes these networks as non-broadcast, multiaccess networks. An example of a non-broadcast network is an X.25 public data network (38).

Non-Multicast router In the context of MOSPF, a router running OSPF Version 2, but not the multicast extensions. These routers do not forward multicast datagrams, but can interoperate with MOSPF routers in the forwarding of unicast packets. Routers running the MOSPF protocol are referred to as either multicast-capable routers or MOSPF routers (38).

Object An object is a model of an entity. An object is characterized by its behavior, and an object is distinct from any other object. An object interacts with its environment including other objects at its interaction points. An object is informally said to perform functions and offer services (an object that performs a function available to other entities and/or objects is said to offer a service). For modeling purposes, these functions and services are specified in terms of the behavior of the object and of its interfaces. An object can perform more than one function and a function can be performed by the cooperation of several objects (42, 43).

Object Storage An emerging storage approach similar to file-based storage except it makes greater use of metadata. It trades the efficiency and performance of block-based storage for easier management and more automation. Object metadata will let content providers and enterprises manage the storage more effectively and apply policies based on the data content, regulatory requirements, ownership of the data, or based on other principles. The metadata can also be used to dynamically store data at the most appropriate service levels (44).

Operating Environment In RFID environments, a region within which an interrogator's RF transmissions are attenuated by less than 90 dB. In free space, the operating environment is a sphere whose radius is approximately 1000 m, with the interrogator located at the center. In a building or other enclosure, the size and shape of the operating environment depends on factors such as the material properties and shape of the building and may be less than 1000 m in certain directions and greater than 1000 m in other direction (7).

Operating Procedure In RFID environments, collectively, the set of functions and commands used by an interrogator to identify and modify tags (also known as the tag-identification layer (7).

Orbit (Satellite) The path described by the center of mass of a satellite in space, subjected to natural forces, principally gravitational attraction, but occasional low-energy corrective forces exerted by a propulsive device in order to achieve and maintain the desired path.

Orbital Plane (Satellite) The plane containing the center of mass of the earth and the velocity vector (direction of motion) of a satellite.

Outgoing Interface (oif) List In PIM-SM, each multicast route entry has an oif list containing the outgoing interfaces to which multicast packets should be forwarded (27).

Packet Protocol data unit (PDU) at network layer. In IPv6, a packet that consists of an IPv6 header and an IPv6 payload.

Parameter Discovery Part of the ND process that allows nodes to learn configuration parameters, including link MTU, and the default hop limit for outgoing packets.

Passive Tag (or Passive Label) In RFID environments, a tag (or label) whose transceiver is powered by the RF field.

Path Determination Procedure to select the route from the routing table for use in forwarding the datagram.

Path MTU Maximum IPv6 packet size that can be sent without using fragmentation between a source and a destination over an IPv6 network route. The route MTU equates with the smallest link MTU for all links in such route.

Path MTU Discovery Process relating to the use of ICMPv6 "Too Big" message to discover the path MTU.

Path Vector A routing protocols approach that involves the exchange of hop information sequences showing the path to follow in a route. For example, BGP-4 exchanges sequences of numbers of ASs.

Peaking Power Plants (also known as peaker plants or peakers) power plants that typically operate only when there is a high peak demand for electric power.

Peer-Entity Authentication The corroboration that a peer entity in an association is the one claimed.

Peer-to-Peer (P2P) Network A distributed system in which all nodes have identical responsibilities and all communication is symmetric. P2P applications rely by design on the interaction between end nodes. The nodes have significant or total independence of central servers. Every participating node acts as both a server and a client. The idea behind P2P is to (1) bring communication to the edges of the network to avoid overloading central servers and (2) harness the great number of underutilized computers and Internet connections in people's homes and offices. This is accomplished by turning every user into a rebroadcaster. The content stream is divided into small parts, and each part is distributed to one user's computer. The participating computers request missing parts from each other and exchange parts to rebuild the whole content. Users can view the content, for example a movie, as if it were sent directly from the content provider (45).

Personal Mobility Mobility for those scenarios where the end-user changes the terminal device used for network access at different locations. The ability of a user to access telecommunication services at any terminal on the basis of a personal identifier and the capability of the network to provide those services delineated in the user's service profile (46).

Phishing Act of acquiring sensitive or personal information such as usernames, date of birth, passwords or credit card details, by masquerading as a trustworthy entity.

Physical Layer In RFID environments, the data coding and modulation waveforms used in interrogator-to-tag and tag-to-interrogator signaling.

PLC (Powerline Communications) PLC (also called powerline communication as a singular term; also called powerline telecommunications [or PLT]) refers to any technology that enables data transfer through powerlines by using advanced modulation technology. Data communication can take place at narrowband or broadband speeds. The technology has been around since the 1950s, but initially only supported narrowband applications for relay management, for example for

public lighting. Broadband over PLC only began at the end of the 1990s. PLC is thus a term used to identify technologies, equipments, applications, and services aiming at providing users with communication means over existing "powerlines" (cables transmitting electricity). The term broadband over powerline (BPL) is used to underline the technology capability to address broadband services. As for the term Access PLC, it is used to identify those PLC solutions aiming at providing consumers with broadband services through the external electricity grid, while in-home PLC is used to identify PLC solutions aiming at applications within the home (47).

Point-To-Point Protocol (PPP) Point-to-point network encapsulation method that provides frame delimiters, protocol identification, and integrity services at the bit level.

Point-to-Point Protocol over Ethernet (PPPoE) PPPoE is a network protocol for encapsulating PPP frames in Ethernet frames. It is used mainly with ADSL services. It offers standard PPP features such as authentication, encryption, and compression.

Prefix The initial bits of an IP address. The number of bits is represented via the prefix-length notation.

Prefix length The number of bits in a prefix.

Prefix List A collection of prefixes typically used when creating match conditions, for example, for firewall filters.

Prefix-Length Notation Notation used to represent network prefix length. It uses the "address/prefix length" form, where prefix length indicates the number of bits in the prefix.

Presentation Time Stamp (PTS) Time stamps are inserted close to the material to which they refer (normally in the PES packet header). They indicate the exact moment where a video frame or an audio frame has to be decoded or presented to the user respectively (12).

Privacy The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Private Key Decryption key is often called private key in public-key systems. A private key is also used for signing a message.

Private Security Sector Services and solutions such as but not limited to manned guarding, alarm system integration and monitoring, and cash and valuables handling.

Product Metadata Metadata related to a media file, including product id, category, protecting services, access modes, usage rights, pricing info, scheduling info, maturity rating, addressing, and so on (5).

Protocol Data Unit (PDU) A unit of information associated with a particular protocol. During transmission, the PDU of the N-layer in a protocol suite becomes the payload of the PDU of the N-1 layer.

Proxy (in the CoAP Environment) A "proxy" is an endpoint selected by a client, usually via local configuration rules, to perform requests on behalf of the client, doing any necessary translations. Some translations are minimal, such as for proxy requests for "coap" URIs, whereas other requests might require translation to and from entirely different application-layer protocols (28).

Pseudo-Header Provisional header that is built to calculate the needed checksum for higher layer protocols. IPv6 uses a new pseudo-header format to calculate UDP, TCP, and ICMPv6 checksums.

Pseudo-Periodic Event that is repeated at intervals of various lengths. For example, the routes advertisement sent by an IPv6 router is made at intervals that are calculated between a minimum and a maximum (16).

Pseudowire (PW) Emulation of a native service over a packet-switched network (PSN). The native service may be ATM, frame relay, Ethernet, low-rate TDM, or SONET/SDH, while the PSN may be MPLS, IP (either IPv4 or IPv6), or L2TPv3. The first PW specifications were the Martini draft for ATM PWs, and the TDMoIP draft for transport of E1/T1 over IP. In 2001, the IETF set up the PWE3 Working Group, which was chartered to develop an architecture for service provider edge-to-edge PWs, and service-specific documents detailing the encapsulation techniques. Other standardization forums, including the ITU and the MFA Forum, are also active in producing standards and implementation agreements for PWs (11).

Public Key Encryption key is often called public key in public-key systems. A public key can also be used for verification of signatures (5).

Public-Key Algorithm An algorithm where the key used for encryption is different from the key used for decryption. Furthermore, the private (decryption) key cannot be calculated from the public (encryption) key (5).

Public-Key Infrastructure (PKI) System that provides public-key encryption and digital signature services.

Public-Key Cryptography Standards (PKCS) Set of standards for public-key cryptography from RSA Security Inc. See www.rsasecurity.com (5).

Q-in-Q An enhancement of IEEE 802.1q that allows service providers to create carrier Ethernet VLANs that will preserve the IEEE 802.1q headers used in the internal enterprise VLAN.

Quadrature Amplitude Modulation (QAM) Modulation technique that has been used in Cable TV broadcasting (as well as in other applications).

Quaternary Phase Shift Keying (QPSK) Modulation technique for satellite broadcasting.

Radio Frequency for Consumer Electronics (RF4CE) RF4CE is based on ZigBee and was standardized in 2009 by four consumer electronics companies: Sony, Philips, Panasonic, and Samsung. Two silicon vendors support RF4CE: Texas Instruments and Freescale Semiconductor, Inc. RF4CE's intended use is as a device remote control system, for example for television set-top boxes. The intention is

that it overcomes the common problems associated with IR: interoperability, LOS, and limited enhanced features (10).

Rate Adaptive DSL (RADSL) A non-standard version of ADSL. Note that standard ADSL also permits the ADSL modem to adapt speeds of data transfer (15).

Real-Time Streaming Protocol (RTSP) An IETF protocol that is used for continuous (streaming) of audio and video sessions. It provides the control for playing, stopping, and media position control (e.g., fast forward) via bidirectional communication sessions. An application-level protocol for control of the delivery of data with real-time properties. It embodies an extensible framework to enable controlled, on-demand delivery of real-time audio and video data; it uses TCP or/or the user data protocol (UDP), depending on function.

Real-Time Transport Control Protocol (RTCP) (also known as RTP control protocol) An IETF protocol used for signaling, for example, identify and coordinate the reporting of streaming flow information (e.g., lost packets). Control protocol that works in conjunction with RTP to control performance and for diagnostic purposes. RTCP control packets are periodically transmitted by each participant in an RTP session to all other participants.

Real-Time Transport Protocol (RTP) An IETF protocol (a set of commands and processes) that is used to add timing and sequence information to each packet to allow the reassembly of packets to reproduce real-time audio and video information. A UDP-based packet format and set of conventions that provides end-to-end network connectivity functions suitable for applications transmitting real-time data, such as audio, video, and etcetera, over multicast or unicast network services.

RTP provides end-to-end delivery services for data with real-time characteristics, such as interactive audio and video. Those services include payload type identification, sequence numbering, time stamping, and delivery monitoring. Applications typically run RTP on top of UDP to make use of its multiplexing and checksum services; both protocols contribute parts of the transport protocol functionality. However, RTP may be used with other suitable underlying network or transport protocols. RTP supports data transfer to multiple destinations using multicast distribution if provided by the underlying network (48).

Reassembly Procedure to rebuild the original message that had been subject to fragmentation.

Receiver Equipment that processes the signal from a TS multiplex and performs filtering and forwarding of encapsulated PDUs to the network-layer service (or bridging module when operating at the link layer) (32).

Recipient The destination endpoint of a message.

Redirect Procedure included in the ND mechanisms to inform a host about the IPv6 address of another neighbor that is more appropriate as a next hop destination.

Redundant Array of Inexpensive Disks (RAIDs) Also known as "redundant array of independent disks." It is a storage approach (system) that provides high reliability through redundancy. It combines multiple disk drive components into a logical

unit, allowing the data to be distributed across the drives in one of a number of ways called "RAID levels."

Reference Time Stamp Time stamp providing the indication of the current time. Reference time stamps are to be found in the PES syntax (ESCR), in the program syntax (SCR), and in the transport packet adaption program clock reference (PCR) field (12).

Representational State Transfer (REST) REST is an architectural style of large-scale networked software that takes advantage of the technologies and protocols of the World Wide Web; it describes how distributed data objects, or resources, can be defined and addressed, stressing the easy exchange of information and scalability (49).

Repudiation Denial by one of the entities involved in a communication of having participated in all or part of the communication.

Request Headers Request headers are used in client requests to communicate information about the client.

Reverse Path Forwarding (RPF) In PIM-SM, RPF is used to select the appropriate incoming interface (iif) for a multicast route entry. RPF is a multicast forwarding mode in which a data packet is accepted for forwarding only if it is received on an interface used to reach the source in unicast (39). The RPF neighbor for an address X is the next-hop router used to forward packets toward X. The RPF interface is the interface to that RPF neighbor. In the common case, this is the next hop used by the unicast routing protocol for sending unicast packets toward X. For example, in cases where unicast and multicast routes are not congruent, it can be different (27).

Reverse Proxy (in the CoAP Environment) A "reverse proxy" is an endpoint that acts as a layer above some other server(s) and satisfies requests on behalf of these, doing any necessary translations. Unlike a proxy, a reverse proxy receives requests as if it was the origin server for the target resource; the requesting client will not be aware that it is communicating with a reverse proxy (28).

Router Node that can forward datagrams not specifically addressed to it. In an IPv6 network, a router is also used to send advertisements related to its presence and node configuration information.

Router Advertisement ND message sent by a router in a pseudo-periodic way or as a router solicitation message response. The advertisement includes, at a minimum, a prefix that can be used by the host to calculate its own unicast IPv6 address following the stateless address configuration procedures.

Router Discovery ND process that allows a node to discover routers connected to a particular link.

Router-Port Group Management Protocol (RGMP) A protocol that constrains IP multicast on switches that have only routers attached.

Routing Loop Undesirable situation in a network where traffic is relayed over a closed loop and never reaches its destination. The TTL field is used to detect such traffic and delete it.

Routing Over Low-Power and Lossy Networks (ROLL) IETF Working Group that has defined application-specific routing requirements for an LLN routing protocol; it has also specified the IPv6 routing protocol for low-power and lossy networks (RPL) (30).

RP-Set In PIM-SM, the RP-Set is a set of RP addresses constructed by the BSR based on candidate-RP advertisements received. The RP-Set information is distributed to all PIM routers in the BSR's PIM domain (27).

Satellite Footprint The geographic area of the earth on which a satellite's direct transmissions can be received by a ground-based station or home dish.

Satellite Systems Satellite communication plays a key role in commercial, TV/media, government, and military communications because of its intrinsic multicast/broadcast capabilities, mobility aspects, global reach, reliability, and ability to quickly support connectivity in open-space and/or hostile environments. Satellite communications is a LOS one-way or two-way radio frequency (RF) transmission system that is comprised of a transmitting station (uplink), a satellite system that acts as a signal regeneration node, and one or more receiving stations (downlink). Satellites can reside in a number of orbits. A geosynchronous (GEO) satellite circles the earth at the earth's rotational speed and with the same direction of rotation, therefore appearing at the same position in the sky at a particular time each day. When the satellite is in the equatorial plane, it appears to be permanently stationary when observed at the earth's surface, so that an antenna pointed to it will not require tracking or (major) positional adjustments at periodic intervals of time (this satellite arrangement is also known as "geostationary"). The GEO is at 35,786 km (22,236 mi) of altitude from the earth's surface. Other orbits include the following: LEOs, MEOs (aka intermediate circular orbits [ICOs]), polar orbits, and highly elliptical orbits (HEOs). LEOs are either elliptical or (more commonly) circular orbits that are at a height of 2000 km or less above the surface of the earth. The advantage of LEOs is that they significantly reduce the propagation delay of the signal. The orbit period at these altitudes varies between 90 min and 2 h, and the maximum time during which a satellite in LEO orbit is above the local horizon for an observer on the earth is up to 20 min. With LEOs, there are long periods during which a given satellite is out of view of a particular ground station; this may be acceptable for some applications, for example, for earth monitoring. Coverage can be extended by deploying more than one satellite and using multiple orbital planes. A complete global coverage system using LEOs requires a large number of satellites (>12+) in multiple orbital planes and in various orbits (50).

Scope For IPv6 addresses, the scope is the portion of the network to which the traffic will be propagated.

Scope ID The scope ID is an identifier for a specific area or scope.

Scope Zone One multicast scope may have several instances, which are known as scope zones or zones, for short. For instance, an organization may have multiple sites. Each site might have its own site-local scope zone, each of which would be an instance of the site-local scope. However, a given interface on a given host would only ever be in at most one instance of a given scope. Messages sent by

a host in a site-local scope zones to an address in the site-local scope would be limited to the site-local scope zone containing the host (34).

Scrambling Term used as a word for weaker encryption or controlled distortion of an analog signal. The distortion can be removed by possessing and using the descrambling equipment and proper keys (5).

Scrambling Algorithm An algorithm used in a scrambling (encryption) or descrambling (decryption) process.

Second-Generation VDSL (VDSL2) An ITU Recommendation G.993.2 specifies eight profiles that address a range of applications including up to 100 Mbps symmetric transmission on loops about 100 m long (using a bandwidth of 30 MHz), symmetric bit rates in the 10–30 Mbps range on intermediate-length loops (using a bandwidth of 12 MHz), and asymmetric operation with downstream rates in the range of 10–40 Mbps on loops of lengths ranging from 3 km to 1 km (using a bandwidth of 8.5 MHz). VDSL2 includes most of the advanced feature from ADSL2. The rate/reach performance of VDSL2 is better than VDSL (15).

Security Label The marking bound to a resource (e.g., a data unit) that names or designates the security attributes of that resource.

Security Policy The set of criteria for the provision of security services.

Sender The originating endpoint of a message.

Sensor Network A sensor network is an infrastructure comprised of sensing (measuring), computing, and communication elements that gives the administrator the ability to instrument, observe, and react to events and phenomena in a specified environment. The administrator typically is some civil, government, commercial, or industrial entity. Typically, the connectivity is by wireless means, hence the term wireless sensor network (WSN). The environment can be the physical world, a biological system, or an information technology (IT) framework. Network(ed) sensors systems are seen by observers as an important technology that will experience major deployment in the next few years for a plethora of applications, not the least being homeland security. Typical applications include, but are not limited to, data collection, monitoring, surveillance, and medical telemetry. There are four basic components in a sensor network: (i) an assembly of distributed or localized sensors; (ii) an interconnecting network (usually but not always wireless based); (iii) a central point of information clustering; and (iv) a set of computing resources at the central point (or beyond) to handle data correlation, event-trending, querying, and data mining. In this context, the sensing and computation nodes are considered part of the sensor network; in fact, some of the computing may be done in the network itself. Because of the potentially large quantity of data collected, algorithmic methods for data management play an important role in sensor networks. The computation and communication infrastructure associated with sensor networks is often specific to this environment and rooted in the device- and application-based nature of these networks. For example, unlike most other settings, in-network processing is desirable in sensor networks; furthermore, node power (and/or battery life) is a key design consideration.

Sensors Active devices that measure some variable of the natural or man-made environment (e.g., a building, an assembly line). The technology for sensing and control includes electric and magnetic field sensors; radio-wave frequency sensors; optical-, electro-optic-, and IR-sensors; radars; lasers; location/navigation sensors; seismic and pressure-wave sensors; environmental parameter sensors (e.g., wind, humidity, heat); and biochemical homeland security-oriented sensors. Sensors can be described as "smart" inexpensive devices equipped with multiple on-board sensing elements: they are low-cost, low-power, untethered multifunctional nodes that are logically homed to a central sink node. Sensors are typically internetworked via a series of multihop short-distance low-power wireless links (particularly within a defined "sensor field"); they typically utilize the Internet or some other network for long-haul delivery of information to a point (or points) of final data aggregation and analysis. In general, within the "sensor field," WSNs employ contention-oriented random access channel sharing/transmission techniques that are now incorporated in the IEEE 802 family of standards; indeed, these techniques were developed in the late 1960s and 1970s expressly for wireless (not cabled) environments, and for large sets of dispersed nodes with limited channel-management intelligence. Sensors span several orders of magnitude in physical size; they (or, at least some of their components) range from nanoscopic scale devices to mesoscopic scale devices at one end and from microscopic scale devices to macroscopic scale devices at the other end. Nanoscopic (also known as nanoscale) refers to objects or devices in the order of 1–100 nm in diameter; mesoscopic scale refers to objects between 100 and 10,000 nm in diameter; the microscopic scale ranges from 10 to 1000 μm; and the macroscopic scale is at the millimeter-to-meter range. At the low end of the scale, one finds, among others, biological sensors, small passive microsensors (such as "smart dust"—The *Smart Dust* mote is an autonomous sensing, computing, and communication system that uses the optical visible spectrum for transmission; they are tiny and inexpensive sensors developed by UC Berkeley engineers), and "lab-on-a-chip" assemblies. At the other end of the scale, one finds platforms such as, but not limited to, identity tags; toll collection devices; controllable weather data collection sensors; bioterrorism sensors; radars; and undersea submarine traffic sensors based on sonars. Some refer to the latest generation of sensors, especially the miniaturized ones that are directly embedded in some physical infrastructure, as "microsensors." A sensor network supports any kind of generic sensor; more narrowly, networked microsensors are a subset of the general family of sensor networks. Microsensors with on-board processing and wireless interfaces can be utilized to study and monitor a variety of phenomena and environments at close proximity.

Server The destination endpoint of a request; the originating endpoint of a response.

Service Protection Ensuring that an end-user can only acquire a service, and, by extension, the content contained therein, which they are entitled to receive.

Session Description Protocol (SDP) A media description specification used for describing multimedia sessions for the purposes of session announcement, session invitation, and session initiation.

Session Key A key (normally symmetric) used to encrypt each set of data on a transaction basis. A different session key is used for each communication session. The session key is normally transferred to the receiver using a key exchange mechanism or by encrypting the key under the receiver's public key (5).

Shared Tree A tree that uses a single common root placed at some chosen point in the network. This shared root is called a RP (also called core or center). All sources in the multicast group use the common shared tree. The notation (∗, G) is used to represents the tree. In this case "∗" is a wildcard to mean all sources.

Shortest-Path Tree (SPT) In PIM-SM, it is the SPT that is based on the merged shortest paths from all receivers to the multicast source. This is one of the features that distinguishes PIM-SM from core-based trees (CBT). When appropriate, the use of the SPT provides an optimal distribution network that helps to keep the multicast traffic closer to the minimum required to deliver the information to all members. (51). In PIM-SM, the SPT is the multicast distribution tree created by the merger of all of the shortest paths that connect receivers to the source (as determined by unicast routing) (27).

Singulation Identifying an individual tag in a multiple-tag environment.

Site-Level Aggregation Identifier (SLA ID) 16-bit field in the global unicast address that identifies subnetworks. The SLA ID field is used by an individual organization to create its own local addressing hierarchy and to identify subnets.

Site-Local Address Address identified by the 1111 1110 11 (FEC0::/10) prefix. The scope of these addresses is a local site (of an organization). Site-local addresses are not accessible from other sites and routers should not direct site-local traffic out of a site.

Slotted Random Anticollision In RFID environments, an anticollision algorithm where tags load a random (or pseudo-random) number into a slot counter, decrement this slot counter based on interrogator commands, and reply to the interrogator when their slot counter reaches zero (7).

Smart Energy The term "smart energy" refers to actions and technologies that are used to improve the efficiency of energy consumption.

Smart Grid (SG) An electricity network that can intelligently integrate the actions of all users connected to it—consumers, generators, and those that do both—in order to efficiently deliver sustainable, economic, and secure electricity supplies (as defined by the European Technology Platform for Electricity Networks for the Future).

Smart Ubiquitous Networks (SUNs) ITU-T SUNs are IP-based packet networks that can provide transport and delivery to a wide range of existing and emerging services to people and things. The services provided by the networks can cover aspects such as control, processing, and storage. The networks are smart in the sense that they are knowledgeable, context aware, adaptable, autonomous, and programmable and can instigate services effectively and securely. The networks are ubiquitous in the sense that they allow access anytime, anywhere, through

varied access technologies, access devices including end-user devices and human–machine interfaces. Due to emerging trends in Information and Communications Technology (ICT) concerning the extension of communication objects (including not only humans but also machines and objects) and ways of communication, the ITU-T Study Group 13 has proposed a name—SUNs—as a new vision that incorporates current activities and emerging trends. In 2011, it was decided that activities for SUN in the following areas would commence: content awareness, context awareness, programmability, smart resources management, and autonomic network management (52).

Solicited-Node Address IPv6 multicast address used by nodes during the address resolution process. The solicited-node address facilitates efficient querying of network nodes during address resolution. IPv6 uses the neighbor solicitation message to perform address resolution. In IPv4, the ARP request frame is sent to the MAC-level broadcast, disturbing all nodes on the network segment regardless of whether a node is running IPv4. For IPv6, instead of disturbing all IPv6 nodes on the local link by using the local-link scope all-node address, the solicited-node multicast address is used as the neighbor solicitation message destination. The solicited-node multicast address consists of the prefix FF02::1:FF00:0/104 and the last 24-bits of the IPv6 unicast address that is being resolved (16).

Source Tree A tree that has its root at the multicast source and has branches forming a spanning tree over the network to the receivers. The tree uses the shortest path through the network and hence a separate SPT exists for each individual source sending to each group. The notation of (S,G) is used to describe an SPT where S is the IP address of the source and G is the multicast group address.

Source-Specific Multicast (SSM) A form of multicast in which a receiver is required to specify both the network-layer address of the source and the multicast destination address in order to receive the multicast transmission. The 232/8 IPv4 address range is currently allocated for SSM by IANA. In IPv6, the FF3x::/32 range (where "x" is a valid IPv6 multicast scope value) is reserved for SSM semantics, although today SSM allocations are restricted to FF3x::/96 (37).

Sparse-Mode (SM) protocols SM is one mode of operation of a multicast protocol. PIM-SM uses explicit join/prune messages and RPs in place of dense-mode PIM's and DVMRP's broadcast and prune mechanism (27). Multicast routing protocols are designed on the assumption that only few routers in the network will need to distribute multicast traffic for each multicast group. SM protocols start out with an empty distribution tree and add drop-off branches only upon explicit requests from receivers to join the distribution. SM protocols are generally used in WAN environments, where bandwidth considerations are important.

SSM-Aware Host A host that knows the SSM address range and is capable of applying SSM semantics to it (37).

Stateless IP/ICMP Translation (SIIT) An IPv6 transition technique that allows IPv4-only hosts to talk to IPv6-only hosts.

Static Routing Utilization of routes configured manually into a router's routing table.

Static Tunneling Tunneling technique where addresses are manually configured for the tunnel source and destination endpoints.

Storage Infrastructure (typically in the form of appliances) that is used for the permanent or semipermanent online retention of structured (e.g., databases) and unstructured (e.g., business/e-mail files) corporate information. Typically includes (i) a controller that manages incoming and outgoing communications as well as the data steering onto the physical storage medium (e.g., RAIDs, semiconductor memory) and (ii) the physical storage medium itself. The communications mechanism could be a network interface (such as gigabit Ethernet), a channel interface (such as SCSI), or an SAN interface (i.e., FC).

Storage Appliance A storage platform designed to perform a specific task, such as NAS, routers, and virtualization.

Storage Virtualization Software (sub)systems (typically middleware) that abstract the physical and logical storage assets from the host systems.

Stream A flow of a single type of data.

Stream Cipher Algorithms that simply produce a keystream to be XORed with the plaintext. The same keystream is reproduced at the receiver side for decryption (5).

Streaming An approach where a large media file (audio, video, and so on) is partitioned into smaller pieces so it can be viewed or heard immediately; this forgoes having to wait for the whole file to be downloaded first. The process of playing a file while it is still downloading. Streaming technology, also known as streaming media, lets a user view and hear digitized content—video, sound and animation—as it is being downloaded. Using a World Wide Web browser plug-in, streamed sounds and images can arrive within seconds of a user's click (53).

Streaming Media Internet video and/or audio clips that can play directly over the Internet, without needing to be downloaded first onto a computer. Used to view and hear broadcasts, and to interactively play and seek in stored clips (24).

Streaming Protocols Commands, processes, and procedures that can be used to select, set up, start the playing, pausing, recording, and tear down of streaming sessions.

STUB Multicast Routing A mechanism that allows IGMP messages to be forwarded through a non-PIM-enabled router toward a PIM-enabled router.

Stub Network A network having only a single OSPF router attached. A network belonging to an OSPF system is either a transit or a stub network, but never both (38).

Subnet-Router Anycast Address Anycast address that is allocated to router interfaces. Packets sent to the subnet-router anycast address will be delivered to one router on the subnet.

Subnetwork One or more links that use the same 64-bit prefix in IPv6.

Subnetwork Data Unit (SNDU) SNDU is an IPv4 or IPv6 datagram (or other subnetwork packet, e.g., an arp message or bridged Ethernet frame) (18). An encapsulated PDU sent as an MPEG-2 payload unit.

Subscriber A household or business that legally receives and pays for cable or Pay TV services for its own use (not for retransmission).

Suite B security Suite B security is a National Security Agency (NSA) directive that requires that key establishment and authentication algorithms be based on elliptic curve cryptography, and that the encryption algorithm be AES. The United States government has posted the Fact Sheet on NSA Suite B Cryptography that states in part as follows: "To complement the existing policy for the use of the Advanced Encryption Standard (AES) to protect national security systems and information as specified in The National Policy on the use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information (CNSSP-15), the NSA announced Suite B Cryptography at the 2005 RSA Conference. In addition to the AES, Suite B includes cryptographic algorithms for hashing, digital signatures, and key exchange. Suite B only specifies the cryptographic algorithms to be used . . . " The Fact Sheet on Suite B Cryptography requires that key establishment and authentication algorithms be based on elliptic curve cryptography, and that the encryption algorithm be AES. Suite B defines two security levels, of 128 and 192 bits. In particular, Suite B includes (54):

- Encryption: AES—FIPS 197 (with key sizes of 128 and 256 bits)
- Digital signature: Elliptic curve digital signature algorithm (ECDSA)—FIPS 186-2 (using the curves with 256- and 384-bit prime moduli)
- Key exchange: Elliptic curve Diffie–Hellman (ECDH)—NIST Special Publication 800-56A (using the curves with 256- and 384-bit prime moduli)

The 128-bit security level corresponds to an elliptic curve size of 256 bits and AES-128; it also makes use of SHA-256. The 192-bit security level corresponds to an elliptic curve size of 384 bits and AES-256; it also makes use of SHA-384. To accommodate backward compatibility, a Suite B compliant client or server can be configured to accept a cipher suite that is not part of Suite B. Note: Some refer to the two security levels based on the AES key size that is employed instead of the overall security provided by the combination of Suite B algorithms. At the 128-bit security level, an AES key size of 128 bits is utilized; however, at the 192-bit security level, an AES key size of 256 bits is used.

SUNs Smart ubiquitous networks.

Supervisory Control and Data Acquisition (SCADA) A legacy, but widely deployed system used to monitor and control a plant or equipment in industries such as but not limited to energy, oil and gas refining, water and waste control, transportation, and telecommunications. A SCADA system encompasses the transfer of data between a SCADA central host computer and a number of remote terminal units (RTUs) and/or programmable logic controllers (PLCs), and the central host and the operator terminals.

Symmetric DSL (SDSL) A vendor-proprietary version of symmetric DSL that may include bit rates to and from the customer ranging of 128 Kbps to 2.32 Mbps. SDSL is an umbrella term for a number of supplier-specific implementations over a single copper pair providing variable rates of symmetric service. SDSL uses 2B1Q HDSL run on a single pair with an Ethernet interface to the customer. The industry is expected to quickly move toward the higher-performing and standardized G.shdsl technology developed by the ITU with support from T1E1.4 (USA) and ETSI (European Telecommunications Standards Institute) (15).

Symmetric Encryption Type of encryption in which encryption and decryption keys are the same key or can easily be derived from each other. In most cryptographic systems, the decryption key and the encryption keys are identical (5).

Symmetric Flavors DSL Symmetrical variations of DSL that include SDSL, SHDSL, HDSL, HDSL2, and IDSL. The equal speeds make symmetrical DSLs useful for LAN access, video-conferencing, and for locations hosting their own Web sites (15).

Symmetric High-Speed Digital Subscriber Line (SHDSL) A state-of-the-art, industry standard based on ITU Recommendation G.991.2, also known as G.shdsl (2001). SHDSL achieves 20% better loop-reach than older versions of symmetric DSL, it causes much less crosstalk into other transmission systems in the same cable, and multivendor interoperability is facilitated by the standardization of this technology. SHDSL systems may operate at many bit rates, from 192 Kbps to 5.7 Mbps, thereby maximizing the bit rate for each customer. G.shdsl specifies operation via one pair of wires, or for operation on longer loops, two pairs of wire may be used. For example, with two pairs of wire, 1.2 Mbps can be sent over 20,000 feet of 26 AWG wire. SHDSL is best suited to data-only applications that need high upstream bit rates. SHDSL is being deployed primarily for business customers (15).

Tag Air Interface As defined in ISO 19762-3, a conductor-free medium, usually air, between a transponder and a reader/interrogator through which data communication is achieved by means of a modulated inductive or propagated electromagnetic field.

Tag-Identification Layer In RFID environments, collectively, the set of functions and commands used by an interrogator to identify and modify tags (also known as the *operating procedur*) (7).

Telco Traditional telephone company.

Teredo IPv6 transition technology for use when IPv6/IPv4 hosts are located behind an IPv4 network address translator.

Teredo Client Software on an IPv6/IPv4 host allowing it to participate in the Teredo transition technology.

Teredo Relay An IPv6 router that can receive traffic from the IPv6 Internet and forward to a Teredo client.

Teredo Server A node that assists in the provision of IPv6 connectivity to Teredo clients.

Threat A potential violation of security.

Tiered Storage A process for the assignment of different categories of data to different types of storage media. The purpose is to reduce total storage cost and optimize accessibility. In practice, the assignment of data to particular media tends to be an evolutionary and complex activity. Storage categories may be based on a variety of design/architectural factors, including levels of protection required for the application or organization, performance requirements, and frequency of use. Software exists for automatically managing the process based on a company-defined policy. Tiered storage generally introduces more vendors into the environment and interoperability is important.

As an example of tiered storage is as follows: Tier 1 data (e.g., mission-critical files) could be effectively stored on high-quality directly attached storage (DAS) (but relatively expensive) media such as double-parity RAIDs. Tier 2 data (e.g., quarterly financial records) could be stored on media affiliated with an SAN; this media tends to be less expensive than DAS drives, but there may be network latencies associated with the access. Tier 3 data (e.g., e-mail backup files) could be stored on recordable compact discs (CD-Rs) or tapes. (Clearly, there could be more than three tiers, but the management of the multiple tiers becomes fairly complex.)

Another example (in the medical field) is as follows: Real-time medical imaging information may be temporarily stored on DAS disks as a Tier 1, say for a couple of weeks. Recent medical images and patient data may be kept on FC drives (tier 2) for about a year. After that, less frequently accessed images and patient records are stored on AT attachment (ATA) drives (tier-3) for 18 months or more. Tier 4 consists of a tape library for archiving.

Transit Network A network having two or more OSPF routers attached. These networks can forward data traffic that is neither locally originated nor locally destined. In OSPF, with the exception of point-to-point networks and virtual links, the neighborhood of each transit network is described by a network links advertisement (38).

Translation Translation refers to the direct conversion of protocols, for example, between IPv4 and IPv6.

Transport Relay Translator (TRT) TRT partitions the IP layer into two terminated IP legs, one IPv4 and one IPv6. Translation then occurs at the higher layers (16).

Tree Information Base (TIB) This is the collection of state maintained by a PIM router and created by receiving PIM messages and IGMP information from local hosts. The table essentially stores the state of all multicast distribution trees at that router (39).

Tunnel In IPv6 transition context, an IPv6 over IPv4 tunnel.

Tunneling Techniques Tunneling techniques include the following (29):

- IPv6-over-IPv4 tunneling: The technique of encapsulating IPv6 packets within IPv4 so that they can be carried across IPv4 routing infrastructures.
- Configured tunneling: IPv6-over-IPv4 tunneling where the IPv4 tunnel endpoint address is determined by configuration information on the encapsulating

node. The tunnels can be either unidirectional or bidirectional. Bidirectional configured tunnels behave as virtual point-to-point links.

- Automatic tunneling: Tunneling where the IPv4 tunnel endpoint address is automatically determined, generally being embedded in the IPv6 address. Examples include IPv6-compatible addresses and IPv6 6to4 addresses.

UICC (Universal Integrated Circuit Card) UICC, the smart card used in mobile terminals in GSM and UMTS networks. A UICC typically contain several applications, and the same smart card provides access to both GSM and UMTS networks. The UICC also provides storage (e.g., for a directory). In a GSM network, the UICC contains a subscriber identification module (SIM) application; in a UMTS network it is the USIM (universal subscriber identity module) application. It is a new-generation SIM included in cell phones or laptops using high-speed 3G cellular networks. The UICC smart card typically has of a CPU, ROM, RAM, EEPROM, and I/O circuits.

UMTS Terrestrial Radio Access Network (UTRAN) A collective term for the NodeBs (base stations) and radio network controllers (RNC) that comprise the UTRAN. NodeB is the equivalent to the base transceiver station (BTS) concept used in GSM. The UTRAN allows connectivity between the UE and the core network.

Unicast Address An address that identifies an IPv6 interface and allows network-layer point-to-point communication. It identifies a single interface within the scope of the unicast address type. An identifier for a single interface. A packet sent to a unicast address is delivered to the interface identified by that address. The following list shows the types of IPv6 unicast addresses:

- Aggregatable global unicast addresses
- Link-local addresses
- Site-local addresses
- Special addresses, including unspecified and loopback addresses
- Compatibility addresses, including 6to4 addresses

Unicast Environment Environment where one system communicates directly to another system.

Unidirectional Link (UDL) A one-way transmission IP over DVB link, for example, a broadcast satellite link.

Universal Mobile Telecommunications System (UMTS) UMTS is a 3G mobile cellular technology for networks supporting voice and data (IP) based on the GSM standard developed by the 3GPP.

Unspecified Address 0:0:0:0:0:0:0:0 or ::—used to show the absence of any address, equivalent to the IPv4 address 0.0.0.0.

Upstream Interface Interface toward the source of the datagram. Also known as the RPF interface (39).

Upstream Interface (or Router) In CBT, an "upstream" interface (or router) is one that is on the path toward the group's core router with respect to this interface (or router) [BAL199701].

USIM Universal subscriber identity module.

Very High Bit Rate DSL (VDSL) A standard for up to 26 Mbps, over distances up to 50 m on short loops such as from fiber to the curb. In most cases, VDSL lines will be served from neighborhood cabinets that link to a Central Office via optical fiber. VDSL has been introduced in some market to deliver video services over existing phone lines. VDSL can also be configured in symmetric mode (15).

Very Small Aperture Terminal (VSAT) A complete end-user terminal (typically with a small 4–5 ft antenna) that is designed to interact with other terminals in a satellite-delivered data IP-based network, commonly in a "star" configuration through a hub. Contention and/or traffic engineering are typical of these services. Hub or network operator to control the system and present billing based on a data throughput, or other form of usage basis. VSATs are utilized in a variety of remote applications and are designed as low-cost units (say $1500–$3000 depending on application and data rate).

Video Compression The process through which a video file is reduced in size for storing and streaming either on traditional TV systems, IPTV, or IBTV. Performing a digital compression process on a video signal. Compression techniques are used to enable efficient transmission of video signals.

Video Format The file type of a video file. Some of the most well-known formats for digital video include .avi (Microsoft), .mov (Quicktime), .wmv (Windows), and .flv (Flash).

Virtual Infrastructure An infrastructure where there is a dynamic mapping of physical resources to functional service requests, such that the entity requiring service is oblivious to the specific nature of the actual hardware supporting the underlying service.

Virtual Private LAN service (VPLS) VPLS is a way to provide Ethernet-based multipoint-to-multipoint communication over IP/MPLS networks. VPLS allows geographically dispersed sites to share an Ethernet broadcast domain by connecting sites through pseudowires. The technologies that can be used as pseudo-wire can be Ethernet over MPLS, L2TPv3, or even GRE. There are two IETF standards describing VPLS establishment. VPLS requires a full mesh of LSPs which has the n2 scaling problem. H-VPLS helps solve this problem by dividing the virtual LAN into separate hierarchies (11).

Virtualization The abstraction of server, storage, and network resources in order to make them available dynamically for sharing by IT services, both internal to and external to an organization. In combination with other server, storage, and networking capabilities, virtualization offers customers the opportunity to build more efficient IT infrastructures. Virtualization is seen by some as a step on the road to utility computing. An approach that allows several operating systems to run simultaneously on one (large) computer (e.g., IBM's z/VM operating system

lets multiple instances of Linux coexist on the same mainframe computer). It is the practice of making resources from diverse devices accessible to a user as if they were a single, larger, homogenous, appear-to-be-locally available resource. Virtualization depends on being able to dynamically shift resources across platforms to match computing demands with available resources: the computing environment can become dynamic, enabling autonomic shifting applications between servers to match demand.

Web Cache A Web cache fills requests from the Web server, stores the requested information locally, and sends the information to the client. The next time the Web cache gets a request for the same information, it simply returns the locally cached data instead of searching over the Internet, thus reducing Internet traffic and response time (23).

Web of Things Technology that aims for direct Web connectivity of things in the IoT context by pushing Web capabilities (e.g., web server) down to devices.

Web Services (WSs) WSs provide standard infrastructure for data exchange between two different distributed applications.

Widget A stand-alone application that can be embedded into a (third party) website by a(ny) user on a page where they have rights of authorship (e.g., a profile on a social media site). A widget is a standardized on-screen representation of a control that may be manipulated by the user. Scroll bars, buttons, and textboxes are all examples of widgets. For example, a "search widget" could be added on a personal website by copying and pasting the embed code into the home page (or some similar action on a Facebook profile). Widgets allow users to turn personal content into dynamic web apps. Traditional web widgets provided functions such as advertising banners and link counters.

Wi-Fi Wi-Fi is a brand originally licensed by the Wi-Fi Alliance to describe the underlying technology of wireless local area networks (WLANs) based on the IEEE 802.11 family of standards, including 802.11a, 802.11b, 802.11g, 802.11n, and 802.11v (55). It was developed to be used for business mobile computing devices, such as laptops, in LANs, but is now increasingly used for additional services, including Internet and voice over IP (VoIP) phone access, gaming, and basic connectivity of consumer electronics such as televisions and DVD players, or digital cameras (11). (Wi-Fi is a trademark of the Wi-Fi Alliance, a commercial organization that certifies the interoperability of specific devices designed to the respective IEEE standard.)

Wildcard (WC) Multicast Route Entry In PIM-SM, wildcard multicast route entries are those entries that may be used to forward packets for any source sending to the specified group. Wildcard bots in the join list of a join/prune message represent either a (∗,G) or (∗,∗,RP) join; in the prune list they represent a (∗,G) prune (27).

Wireless M-BUS The Wireless M-BUS standard (EN 13757-4:2005) specifies communications between water, gas, heat, and electric meters and is becoming widely accepted in Europe for smart metering or AMI applications. Wireless M-BUS

is targeted to operate in the 868 MHz band (from 868 MHz to 870 MHz); this band enjoys good trade-offs between RF range and antenna size. Typically, chip manufacturers, for example Texas Instruments, have both single-chip (SoC) and two-chip solutions for wireless M-BUS.

Wireless Sensor Network (WSN) A sensor network is an infrastructure comprised of sensing (measuring), computing, and communication elements that gives the administrator the ability to instrument, observe, and react to events and phenomena in a specified environment. Typically, the connectivity is by wireless means, hence the term WSN (56).

WirelessHART (aka IEC 62591) WirelessHART is a wireless sensor networking technology based on the highway addressable remote transducer protocol (HART). In 2010, WirelessHart was approved by the International Electrotechnical Commission (IEC) as IEC 62591 as a wireless international standard. IEC 62591 entails operation in the 2.4 GHz ISM band using IEEE 802.15.4 standard radios and makes use of a time-synchronized, self-organizing, and self-healing mesh architecture. WirelessHART/IEC 62591 was defined for the requirements of process field device networks. It is a global IEC-approved standard that specifies an interoperable self-organizing mesh technology in which field devices form wireless networks that dynamically mitigate obstacles in the process environment. This architecture creates a cost-effective automation alternative that does not require wiring and other supporting infrastructure (57).

Worldwide Interoperability for Microwave Access (WiMAX) WiMAX is a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL WiMAX is defined by the WiMAX Forum, formed in June 2001, to promote conformance and interoperability of the IEEE 802.16 standard.

Worldwide Interoperability for Microwave Access (WiMAX) Forum The WiMAX Forum was formed in June 2001 to promote conformance and interoperability of the IEEE 802.16 standard. The WiMAX Forum describes WiMAX as "a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL."

ZigBee IP (ZIP) The goal of this protocol stack is to extend the use of IP networking into resource-constrained devices over a wide range of low-power link technologies. The effort related to ZIP development has resulted in significant progress to the goal of bringing IPv6 network protocols over 802.15.4 wireless mesh networks to reality. ZIP is a protocol stack based on IETF- and IEEE-defined standards such as 6LoWPAN and IEEE 802.15.4 to be used for the SE 2.0 profile.

ZigBee RF4CE Specification The specialty-use driven ZigBee RF4CE is designed for simple, two-way device-to-device control applications that do not require the full-featured mesh networking capabilities offered by ZigBee 2007. ZigBee RF4CE offers lower memory size requirements, thereby enabling lower cost implementations. The simple device-to-device topology provides easy development and testing, resulting in faster time to market. ZigBee RF4CE provides a multivendor interoperable solution for consumer electronics featuring a simple, robust, and

low-cost communication network for two-way wireless connectivity. Through the ZigBee-certified program, the Alliance independently tests platforms implementing this specification and has a list of ZigBee-compliant platforms offering support for ZigBee RF4CE (58).

ZigBee Smart Energy A leading standard for interoperable products that monitor, control, inform, and automate the delivery and use of energy and water. It helps create greener homes by giving consumers the information and automation needed to easily reduce their consumption and save money. ZigBee SE version 1.1, the newest version for product development, adds several important features including dynamic pricing enhancements, tunneling of other protocols, prepayment features, over-the-air updates, and guaranteed backward compatibility with certified ZigBee SE products version 1.0. (58).

ZigBee Specification The core ZigBee specification defines ZigBee's smart, cost-effective, and energy-efficient mesh network based on IEEE 802.15.4. It is a self-configuring, self-healing system of redundant, low-cost, very low-power nodes that enable ZigBee's unique flexibility, mobility, and ease of use. ZigBee is available as two feature sets, ZigBee PRO and ZigBee. Both feature sets define how the ZigBee mesh networks operate. ZigBee PRO, the most widely used specification, is optimized for low-power consumption and to support large networks with thousands of devices (58). (ZigBee is a trademark of the ZigBee Alliance, a commercial organization that certifies the interoperability of specific devices designed to the respective IEEE standard.)

Zone Name A human readable name for a scope zone. An ISO 10646 character string with an RFC 1766 language tag. One zone may have several zone names, each in a different language. For instance, a zone for use within IBM's locations in Switzerland might have the names "IBM Suisse," "IBM Switzerland," "IBM Schweiz," and "IBM Svizzera" with language tags "fr," "en," "de," and "it" (34).

Z-Wave Z-Wave is a wireless ecosystem that aims at supporting connectivity of home electronics, and the user, via remote control. It uses low-power radio waves that easily travel through walls, floors, and cabinets. Z-Wave control can be added to almost any electronic device in the home, even devices that one would not ordinarily think of as "intelligent," such as appliances, window shades, thermostats, smoke alarms, security sensors, and home lighting. Z-Wave operates around 900 MHz (the band used by some cordless telephones but avoids interference with Wi-Fi devices). Z-Wave was developed by Zen-Sys, a Danish startup around 2005; the company was later acquired by Sigma Designs. The Z-Wave Alliance was established in 2005; it is comprised of about 200 industry leaders dedicated to the development and extension of Z-Wave as the key enabling technology for "smart" home and business applications.

REFERENCES

1. 3rd Generation Partnership Project (3GPP) Organization, www.3gpp.org.
2. Third Generation Partnership Project 2 Organization, http://www.3gpp2.org.

3. Bormann C. Getting Started with IPv6 in Low-Power Wireless "Personal Area" Networks (6LoWPAN), Universität Bremen TZI, IETF 6lowpan WG and CoRE WG Co-Chair, IAB Tutorial on Interconnecting Smart Objects with the Internet, Prague, Saturday, 2011-03-26, http://www.iab.org/about/workshops/smartobjects/tutorial.html.
4. Microsoft Corporation, MSDN Library, Internet Protocol, 2004, http://MSDn.microsoft.com.
5. Conax AS. Glossary of Terms, Fred Olsensgate 6, NO-0152 Oslo, Norway.
6. Drake J, Najewicz D, Watts W. Energy Efficiency Comparisons of Wireless Communication Technology Options for Smart Grid Enabled Devices. White Paper, General Electric Company, GE Appliances & Lighting, December 9, 2010.
7. EPCglobal Inc™, EPC™ Radio-Frequency Identity Protocols, Class-1 Generation-2 UHF RFID, Protocol for Communications at 860 MHz–960 MHz, Version 1.0.9, January 2005.
8. Practel, Inc., Role of Wireless ICT in Health Care and Wellness—Standards, Technologies and Markets, May, 2012, Published by Global Information, Inc. (GII), 195 Farmington Avenue, Suite 208 Farmington, CT 06032 USA.
9. Jung N-J, Yang I-K, Park S-W, Lee S-Y. A design of AMI protocols for two way communication in K-AMI. Control, Automation and Systems (ICCAS), Conference Proceedings 2011, 11th International Conference on, Date of Conference: 26–29 Oct. 2011, S/W Center, KEPCO Res. Inst., Daejeon, South Korea, Page(s): 1011–1016.
10. Smith P. Comparing Low-Power Wireless Technologies. Tech Zone, Digikey Online Magazine, Digi-Key Corporation, 701 Brooks Avenue, South Thief River Falls, MN 56701 USA.
11. Cisco. IP NGN Carrier Ethernet Design: Powering the Connected Life in the Zettabyte Era. Cisco Whitepaper, 2007, Cisco Systems, Inc., 170 West Tasman Dr., San Jose, CA 95134, USA.
12. Fairhurst G. MPEG-2 Digital Video, Background to Digital Video, University of Aberdeen, King's College, Dept. of Engineering, Aberdeen, AB24 3FX, UK, January 2001, http://www.erg.abdn.ac.uk/research/future-net/digital-video/mpeg2-trans.html.
13. Delay Tolerant Networking Research Group, http://www.dtnrg.org.
14. Gifford K. Disruption Tolerant Networking for Space Operations (DTN). University of Colorado, Boulder, CO, United States, NASA Research, March 2012, http://www.nasa.gov/mission_pages/station/research/experiments/DTN.html.
15. DSL Forum, DSL Forum, 48377 Fremont Blvd, Suite 117, Fremont, CA 94538, http://www.dslforum.org.
16. IPv6 Portal, http://www.ipv6tf.org/meet/faqs.php.
17. ETSI Documentation, ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex—FRANCE.
18. Clausen Horst D, Collini-Nocker Bernhard, et al. Simple Encapsulation for Transmission of IP Datagrams over MPEG-2/DVB Networks, Internet Engineering Task Force, draft-unisal-ipdvb-enc-00.txt, May 2003.
19. Machine-to-Machine Communications (M2M); M2M Service Requirements. ETSI TS 102 689 V1.1.1 (2010-08). ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex—FRANCE.
20. Machine-to-Machine Communications (M2M); Functional Architecture Technical Specification, ETSI TS 102 690 V1.1.1 (2011-10), ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex—FRANCE.

21. Kindig S. TV and HDTV Glossary. December 02, 2009, Crutchfield, 1 Crutchfield Park, Charlottesville, VA 22911.
22. 3GPP TS 22.368 V10.1.0 (2010-06), Technical Specification, June 2010, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements for Machine-Type Communications (MTC); Stage 1 (Release 10).
23. SunStar, Storage Glossary of Terms, 900 West Hyde Park Blvd. Inglewood, CA 90302.
24. ReelSEO.com, Online Video Dictionary—Glossary of Online Video Terms, The Online Video Marketer's Guide, 2010.
25. Gast M. Introduction to 802.11v, Trapeze Networks, Interop Presentation, 2008.
26. Krasinski R, Nikolich P, Heile RF. IEEE 802.15.4j Medical Body Area Networks Task Group PAR, IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs), January18, 2011.
27. Estrin D, Farinacci D, et al. Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification. RFC2362, June 1998.
28. Shelby Z, Hartke K, Bormann C, Frank B. Constrained Application Protocol (CoAP). CoRE Working Group, March 12, 2012, Internet-Draft, draft-ietf-core-coap-09.
29. Gilligan R, Nordmark E. Transition Mechanisms for IPv6 Hosts and Routers, RFC2893, August 2000.
30. Winter T, editor. ROLL/RPL: IPv6 Routing Protocol for Low power and Lossy Networks, March 2011, draft-ietf-roll-rpl-19.
31. ISA, 67 Alexander Drive, P.O. Box 12277, Research Triangle Park, NC 27709, info@isa.org.
32. Fairhurst G, Montpetit M-J. Address Resolution for IP Datagrams over MPEG-2 Networks, Internet Draft draft-ietf-ipdvb-ar-00.txt, IETF ipdvb, June 2005.
33. ETSI TR 101 557 V1.1.1 (2012-02), Electromagnetic Compatibility and Radio Spectrum Matters (ERM); System Reference Document (SRdoc); Medical Body Area Network Systems (MBANSs) in the 1785 MHz to 2500 MHz range.
34. Hanna S, Patel B, Shah M. Multicast Address Dynamic Client Allocation Protocol (MADCAP). RFC2730, December 1999.
35. Radoslavov P, Estrin D, et al. The Multicast Address-Set Claim (MASC) Protocol. RFC2909, September 2000.
36. Vida R, Costa L, editors. Multicast Listener Discovery Version 2 (MLDv2) for IPv6, RFC 3810, June 2004.
37. Holbrook H, Cain B, Haberman B. Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast. RFC4604, August 2006.
38. Moy J. Multicast Extensions to OSPF. RFC 1584, March 1994.
39. Adams A, Nicholas J, Siadak W. Protocol Independent Multicast—Dense Mode (PIM-DM): Protocol Specification (Revised). RFC 3973, January 2005.
40. Welcher PJ. The Protocols of IP Multicast, NetCraftsmen White Paper, Chesapeake NetCraftsmen, LLC., 1290 Bay Dale Drive—Suite #312, Arnold, MD 21012.
41. NSF Future Internet Architecture Project, http://www.nets-fia.net.
42. Lee GM, Choi JK, et al. Naming Architecture for Object to Object Communications. HIP Working Group, Internet Draft, March 8, 2010, draft-lee-object-naming-02.txt.

43. ITU-T Y.2002. Overview of Ubiquitous Networking and of its Support in NGN. November 2009.
44. Radding A. SAN of the Future. Essential Guide To Storage Networking, Storage Media Group/SearchStorage.com Whitepaper, March 2010.
45. Sjöberg D. Content Delivery Networks: Ensuring Quality of Experience in Streaming Media Applications. TeliaSonera International Carrier, CDN White Paper, August 14, 2008.
46. Johnson M. ITU-T IPTV Focus Group Proceedings, ITU-T, 2008.
47. PLCforum, http://www.plcforum.org/frame_plc.html.
48. Schulzrinne H, Casner S, et al. RTP: A Transport Protocol for Real-Time Applications, IETF Request for Comments, July 2003.
49. Kay R. Quick Study: Representational State Transfer (REST). ComputerWorld, August 6, 2007.
50. Minoli D. *Satellite Systems Engineering in an IPv6 Environment*. Boca Raton, FL: Francis and Taylor; 2009.
51. Rodbell M. Protocol Independent Multicast—Sparse Mode, CMP COMMs Design, an EE Times Community, 3 June 2007, http://www.comMSDesign.com/main/9811/9811standards.htm.
52. Service Architecture Lab (a leading French research group with a focus on 'Future Services'), http://servicearchitecture.wp.it-sudparis.eu/.
53. California Software Labs, Basic Streaming Technology and RTSP Protocol—A Technical Report, 2002, California Software Labs, 6800 Koll Center Parkway, Suite 100 Pleasanton CA 94566, USA.
54. Salter M, Rescorla E, Housley R. Suite B Profile for Transport Layer Security (TLS). RFC 5430, March 2009.
55. Minoli D. *Hotspot Networks: Wi-Fi for Public Access Locations*. New York, NY: McGraw-Hill; 2002.
56. Minoli D. *Wireless Sensor Networks* (co authored with K. Sohraby and T. Znati). Hoboken, NJ: Wiley; 2007.
57. Emerson Process Management, *IEC 62591 WirelessHART, System Engineering Guide, Revision 2.3*, Emerson Process Management, 2011.
58. ZigBee Alliance, http://www.zigbee.org/.
59. Cisco Systems, Internet Protocol (IP) Multicast Technology Overview, 2007, Cisco Systems, Inc., 170 West Tasman Dr., San Jose, CA 95134, USA.
60. Open IPTV Forum (OIPF), Services and Functions for Release 2 [V1.0]-[2008-10-20], 2008, Open IPTV Forum, 650 Route des Lucioles - Sophia Antipolis, Valbonne, France.