Internet Engineering Task Force (IETF)
Request for Comments: 6272
Category: Informational
ISSN: 2070-1721

F. Baker
D. Meyer
Cisco Systems

June 2011

Internet Protocols for the Smart Grid

Abstract

This note identifies the key infrastructure protocols of the Internet Protocol Suite for use in the Smart Grid. The target audience is those people seeking guidance on how to construct an appropriate Internet Protocol Suite profile for the Smart Grid. In practice, such a profile would consist of selecting what is needed for Smart Grid deployment from the picture presented here.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6272.

Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

This document provides Smart Grid designers with advice on how to best "profile" the Internet Protocol Suite (IPS) for use in Smart Grids. It provides an overview of the IPS and the key infrastructure protocols that are critical in integrating Smart Grid devices into an IP-based infrastructure.

In the words of Wikipedia [SmartGrid]:

> A Smart Grid is a form of electricity network utilizing digital technology. A Smart Grid delivers electricity from suppliers to consumers using two-way digital communications to control appliances at consumers' homes; this saves energy, reduces costs and increases reliability and transparency. It overlays the ordinary electrical Grid with an information and net metering system, that includes smart meters. Smart Grids are being promoted by many governments as a way of addressing energy independence, global warming and emergency resilience issues.
>
> A Smart Grid is made possible by applying sensing, measurement and control devices with two-way communications to electricity production, transmission, distribution and consumption parts of the power Grid that communicate information about Grid condition to system users, operators and automated devices, making it possible to dynamically respond to changes in Grid condition.
>
> A Smart Grid includes an intelligent monitoring system that keeps track of all electricity flowing in the system. It also has the capability of integrating renewable electricity such as solar and wind. When power is least expensive the user can allow the smart Grid to turn on selected home appliances such as washing machines or factory processes that can run at arbitrary hours. At peak times it could turn off selected appliances to reduce demand.
>
> Other names for a Smart Grid (or for similar proposals) include smart electric or power Grid, intelligent Grid (or intelliGrid), futureGrid, and the more modern interGrid and intraGrid.

That description focuses on the implications of Smart Grid technology in the home of a consumer. In fact, data communications technologies of various kinds are used throughout the Grid, to monitor and maintain power generation, transmission, and distribution, as well as the operations and management of the Grid. One can view the Smart Grid as a collection of interconnected computer networks that connects and serves the needs of public and private electrical utilities and their customers.

At the time of this writing, there is no single document that can be described as comprising an internationally agreed standard for the Smart Grid; that is in part the issue being addressed in its development. The nearest approximations are probably the Smart Grid Interoperability Panel's Conceptual Model [Model] and documents comprising [IEC61850].

The Internet Protocol Suite (IPS) provides options for numerous architectural components. For example, the IPS provides several choices for the traditional transport function between two systems: the Transmission Control Protocol (TCP) [RFC0793], the Stream Control Transmission Protocol (SCTP) [RFC4960], and the Datagram Congestion Control Protocol (DCCP) [RFC4340]. Another option is to select an encapsulation such as the User Datagram Protocol (UDP) [RFC0768], which essentially allows an application to implement its own transport service. In practice, a designer will pick a transport protocol that is appropriate to the problem being solved.

The IPS is standardized by the Internet Engineering Task Force (IETF). IETF protocols are documented in the Request for Comments (RFC) series. Several RFCs have been written describing how the IPS should be implemented. These include:

- Requirements for Internet Hosts - Communication Layers [RFC1122],
- Requirements for Internet Hosts - Application and Support [RFC1123],
- Requirements for IP Version 4 Routers [RFC1812], and
- IPv6 Node Requirements [RFC4294].

At the time of this writing, RFC 4294 is in the process of being updated, in [IPv6-NODE-REQ].

This document is intended to provide Smart Grid architects and designers with a compendium of relevant RFCs (and to some extent, Internet Drafts), and is organized as an annotated list of RFCs. To that end, the remainder of this document is organized as follows:

- Section 2 describes the Internet Architecture and its protocol suite.
- Section 3 outlines a set of protocols that may be useful in Smart Grid deployment. It is not exhaustive.
- Finally, Section 4 provides an overview of the business architecture embodied in the design and deployment of the IPS.

2. The Internet Protocol Suite

Before enumerating the list of Internet protocols relevant to Smart Grid, we discuss the layered architecture of the IPS, the functions of the various layers, and their associated protocols.

2.1. Internet Protocol Layers

While Internet architecture uses the definitions and language similar to language used by the ISO Open System Interconnect (ISO-OSI) reference model (Figure 1), it actually predates that model. As a result, there is some skew in terminology. For example, the ISO-OSI model uses "end system" while the Internet architecture uses "host". Similarly, an "intermediate system" in the ISO-OSI model is called an "internet gateway" or "router" in Internet parlance. Notwithstanding these differences, the fundamental concepts are largely the same.

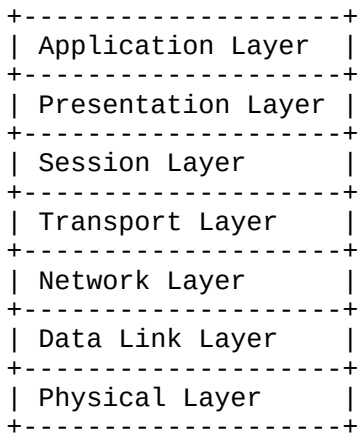

Figure 1: The ISO OSI Reference Model

The structure of the Internet reference model is shown in Figure 2.

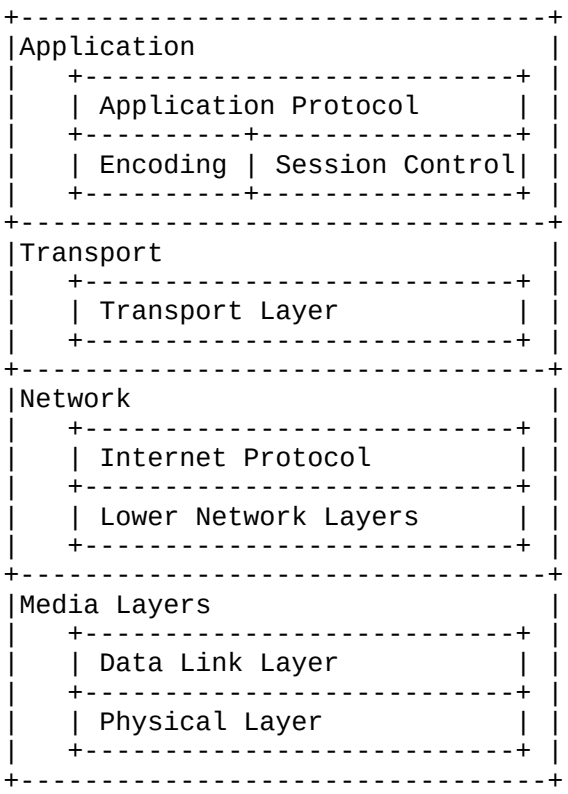

Figure 2: The Internet Reference Model

2.1.1. Application

In the Internet model, the Application, Presentation, and Session layers are compressed into a single entity called "the application". For example, the Simple Network Management Protocol (SNMP) [RFC3411] describes an application that encodes its data in an ASN.1 profile and engages in a session to manage a network element. The point here is that in the Internet, the distinction between these layers exists but is not highlighted. Further, note that in Figure 2, these functions are not necessarily cleanly layered: the fact that an application protocol encodes its data in some way and that it manages sessions in some way doesn't imply a hierarchy between those processes. Rather, the application views encoding, session management, and a variety of other services as a tool set that it uses while doing its work.

2.1.2. Transport

The term "transport" is perhaps among the most confusing concepts in the communication architecture, to a large extent because people with various backgrounds use it to refer to "the layer below that which I am interested in, which gets my data to my peer". For example, optical network engineers refer to optical fiber and associated electronics as "the transport", while web designers refer to the Hypertext Transfer Protocol (HTTP) [RFC2616] (an application layer protocol) as "the transport".

In the Internet protocol stack, the "transport" is the lowest protocol layer that travels end-to-end unmodified, and it is responsible for end-to-end data delivery services. In the Internet, the transport layer is the layer above the network layer. Transport layer protocols have a single minimum requirement: the ability to multiplex several applications on one IP address. UDP [RFC0768], TCP [RFC0793], DCCP [RFC4340], SCTP [RFC4960], and NORM [RFC5740] each accomplish this using a pair of port numbers, one for the sender and one for the receiver. A port number identifies an application instance, which might be a general "listener" that peers or clients may open sessions with, or a specific correspondent with such a "listener". The session identification in an IP datagram is often called the "five-tuple", and consists of the source and destination IP addresses, the source and destination ports, and an identifier for the transport protocol in use.

In addition, the responsibilities of a specific transport layer protocol typically include the delivery of data (either as a stream of messages or a stream of bytes) in a stated sequence with stated expectations regarding delivery rate and loss. For example, TCP will reduce its rate in response to loss, as a congestion control trigger, while DCCP accepts some level of loss if necessary to maintain timeliness.

2.1.3. Network

The main function of the network layer is to identify a remote destination and deliver data to it. In connection-oriented networks such as Multi-protocol Label Switching (MPLS) [RFC3031] or Asynchronous Transfer Mode (ATM), a path is set up once, and data is delivered through it. In connectionless networks such as Ethernet and IP, data is delivered as datagrams. Each datagram contains both the source and destination network layer addresses, and the network is responsible for delivering it. In the Internet Protocol Suite, the Internet Protocol is the network that runs end to end. It may be encapsulated over other LAN and WAN technologies, including both IP networks and networks of other types.

2.1.3.1. Internet Protocol

IPv4 and IPv6, each of which is called the Internet Protocol, are connectionless ("datagram") architectures. They are designed as common elements that interconnect network elements across a network of lower-layer networks. In addition to the basic service of identifying a datagram's source and destination, they offer services to fragment and reassemble datagrams when necessary, assist in diagnosis of network failures, and carry additional information necessary in special cases.

The Internet layer provides a uniform network abstraction network that hides the differences between various network technologies. This is the layer that allows diverse networks such as Ethernet, 802.15.4, etc. to be combined into a uniform IP network. New network technologies can be introduced into the IP Protocol Suite by defining how IP is carried over those technologies, leaving the other layers of the IPS and applications that use those protocol unchanged.

2.1.3.2. Lower-Layer Networks

The network layer can be recursively subdivided as needed. This may be accomplished by tunneling, in which an IP datagram is encapsulated in another IP header for delivery to a decapsulator. IP is frequently carried in Virtual Private Networks (VPNs) across the public Internet using tunneling technologies such as the Tunnel mode of IPsec, IP-in-IP, and Generic Route Encapsulation (GRE) [RFC2784]. In addition, IP is also frequently carried in circuit networks such as MPLS [RFC4364], GMPLS, and ATM. Finally, IP is also carried over wireless networks (IEEE 802.11, 802.15.4, or 802.16) and switched Ethernet (IEEE 802.3) networks.

2.1.4. Media Layers: Physical and Link

At the lowest layer of the IP architecture, data is encoded in messages and transmitted over the physical media. While the IETF specifies algorithms for carrying IPv4 and IPv6 various media types, it rarely actually defines the media -- it happily uses specifications from IEEE, ITU, and other sources.

2.2. Security Issues

While complaining about the security of the Internet is popular, it is important to distinguish between attacks on protocols and attacks on users (e.g., phishing). Attacks on users are largely independent of protocol details, reflecting interface design issues or user education problems, and are out of scope for this document. Security problems with Internet protocols are in scope, of course, and can

often be mitigated using existing security features already specified for the protocol, or by leveraging the security services offered by other IETF protocols. See the Security Assessment of the Transmission Control Protocol (TCP) [TCP-SEC] and the Security Assessment of the Internet Protocol version 4 [IP-SEC] for more information on TCP and IPv4 issues, respectively.

These solutions do, however, need to get deployed as well. The road to widespread deployment can sometimes be painful since often multiple stakeholders need to take actions. Experience has shown that this takes some time, and very often only happens when the incentives are high enough in relation to the costs.

Furthermore, it is important to stress that available standards are important, but the range of security problems is larger than a missing standard; many security problems are the result of implementation bugs and the result of certain deployment choices. While these are outside the realm of standards development, they play an important role in the security of the overall system. Security has to be integrated into the entire process.

The IETF takes security seriously in the design of their protocols and architectures; every IETF specification has to have a Security Considerations section to document the offered security threats and countermeasures. RFC 3552 [RFC3552] provides recommendations on writing such a Security Considerations section. It also describes the classical Internet security threat model and lists common security goals.

In a nutshell, security has to be integrated into every protocol, protocol extension, and consequently, every layer of the protocol stack to be useful. We illustrate this also throughout this document with references to further security discussions. Our experience has shown that dealing with security as an afterthought does not lead to the desired outcome.

The discussion of security threats and available security mechanisms aims to illustrate some of the design aspects that commonly appear.

2.2.1. Physical and Data Link Layer Security

At the physical and data link layers, threats generally center on physical attacks on the network -- the effects of backhoes, deterioration of physical media, and various kinds of environmental noise. Radio-based networks are subject to signal fade due to distance, interference, and environmental factors; it is widely noted that IEEE 802.15.4 networks frequently place a metal ground plate between the meter and the device that manages it. Fiber was at one

time deployed because it was believed to be untappable; we have since learned to tap it by bending the fiber and collecting incidental light, and we have learned about backhoes. As a result, some installations encase fiber optic cable in a pressurized sheath, both to quickly identify the location of a cut and to make it more difficult to tap.

While there are protocol behaviors that can detect certain classes of physical faults, such as keep-alive exchanges, physical security is generally not considered to be a protocol problem.

For wireless transmission technologies, eavesdropping on the transmitted frames is also typically a concern. Additionally, those operating networks may want to ensure that access to their infrastructure is restricted to those who are authenticated and authorized (typically called 'network access authentication'). This procedure is often offered by security primitives at the data link layer.

2.2.2. Network, Transport, and Application Layer Security

At the network, transport, and application layers, it is common to demand a few basic security requirements, commonly referred to as CIA (Confidentiality, Integrity, and Availability):

1. Confidentiality: Protect the transmitted data from unauthorized disclosure (i.e., keep eavesdroppers from learning what was transmitted). For example, for trust in e-commerce applications, credit card transactions are exchanged encrypted between the Web browser and a Web server.

2. Integrity: Protect against unauthorized changes to exchanges, including both intentional change or destruction and accidental change or loss, by ensuring that changes to exchanges are detectable. It has two parts: one for the data and one for the peers.

   * Peers need to verify that information that appears to be from a trusted peer is really from that peer. This is typically called 'data origin authentication'.

   * Peers need to validate that the content of the data exchanged is unmodified. The term typically used for this property is 'data integrity'.

3. Availability: Ensure that the resource is accessible by mitigating of denial-of-service attacks.

To this we add authenticity, which requires that the communicating peers prove that they are in fact who they say they are to each other (i.e., mutual authentication). This generally means knowing "who" the peer is, and that they demonstrate the possession of a "secret" as part of the security protocol interaction.

The following three examples aim to illustrate these security requirements.

One common attack against a TCP session is to bombard the session with reset messages. Other attacks against TCP include the "SYN flooding" attack, in which an attacker attempts to exhaust the memory of the target by creating TCP state. In particular, the attacker attempts to exhaust the target's memory by opening a large number of unique TCP connections, each of which is represented by a Transmission Control Block (TCB). The attack is successful if the attacker can cause the target to fill its memory with TCBs.

A number of mechanisms have been developed to deal with these types of denial-of-service attacks. One, "SYN Cookies", delays state establishment on the server side to a later phase in the protocol exchange. Another mechanism, specifically targeting the reset attack cited above, provides authentication services in TCP itself to ensure that fake resets are rejected.

Another approach would be to offer security protection already at a lower layer, such as IPsec (see Section 3.1.2) or TLS (see Section 3.1.3), so that a host can identify legitimate messages and discard the others, thus mitigating any damage that may have been caused by the attack.

Another common attack involves unauthorized access to resources. For example, an unauthorized party might try to attach to a network. To protect against such an attack, an Internet Service Provider (ISP) typically requires network access authentication of new hosts demanding access to the network and to the Internet prior to offering access. This exchange typically requires authentication of that entity and a check in the ISPs back-end database to determine whether corresponding subscriber records exist and are still valid (e.g., active subscription and sufficient credits).

From the discussion above, establishing a secure communication channel is clearly an important concept frequently used to mitigate a range of attacks. Unfortunately, focusing only on channel security may not be enough for a given task. Threat models have evolved and even some of the communication endpoints cannot be considered fully trustworthy, i.e., even trusted peers may act maliciously.

Furthermore, many protocols are more sophisticated in their protocol interaction and involve more than two parties in the protocol exchange. Many of the application layer protocols, such as email, instant messaging, voice over IP, and presence-based applications, fall into this category. With this class of protocols, secure data, such as DNS records, and secure communications with middleware, intermediate servers, and supporting applications need to be considered as well as the security of the direct communication. A detailed treatment of the security threats and requirements of these multi-party protocols is beyond this specification but the interested reader is referred to the above-mentioned examples for an illustration of what technical mechanisms have been investigated and proposed in the past.

2.3. Network Infrastructure

While the following protocols are not critical to the design of a specific system, they are important to running a network, and as such are surveyed here.

2.3.1. Domain Name System (DNS)

The DNS' main function is translating names to numeric IP addresses. While this is not critical to running a network, certain functions are made a lot easier if numeric addresses can be replaced with mnemonic names. This facilitates renumbering of networks and generally improves the manageability and serviceability of the network. DNS has a set of security extensions called DNSSEC, which can be used to provide strong cryptographic authentication to the DNS. DNS and DNSSEC are discussed further in Section 3.4.1.

2.3.2. Network Management

Network management has proven to be a difficult problem. As such, various solutions have been proposed, implemented, and deployed. Each solution has its proponents, all of whom have solid arguments for their viewpoints. The IETF has two major network management solutions for device operation: SNMP, which is ASN.1-encoded and is primarily used for monitoring of system variables, and NETCONF [RFC4741], which is XML-encoded and primarily used for device configuration.

Another aspect of network management is the initial provisioning and configuration of hosts, which is discussed in Section 3.4.2. Note that Smart Grid deployments may require identity authentication and authorization (as well as other provisioning and configuration) that may not be within the scope of either DHCP or Neighbor Discovery. While the IP Protocol Suite has limited support for secure

provisioning and configuration, these problems have been solved using IP protocols in specifications such as DOCSIS 3.0 [SP-MULPIv3.0].

3. Specific Protocols

In this section, having briefly laid out the IP architecture and some of the problems that the architecture tries to address, we introduce specific protocols that might be appropriate to various Smart Grid use cases. Use cases should be analyzed along with privacy, Authentication, Authorization, and Accounting (AAA), transport, and network solution dimensions. The following sections provide guidance for such analysis.

3.1. Security Toolbox

As noted, a key consideration in security solutions is a good threat analysis coupled with appropriate mitigation strategies at each layer. The IETF has over time developed a number of building blocks for security based on the observation that protocols often demand similar security services. The following sub-sections outline a few of those commonly used security building blocks. Reusing them offers several advantages, such as availability of open source code, experience with existing systems, a number of extensions that have been developed, and the confidence that the listed technologies have been reviewed and analyzed by a number of security experts.

It is important to highlight that in addition to the mentioned security tools, every protocol often comes with additional, often unique security considerations that are specific to the domain in which the protocol operates. Many protocols include features specifically designed to mitigate these protocol-specific risks. In other cases, the security considerations will identify security-relevant services that are required from other network layers to achieve appropriate levels of security.

3.1.1. Authentication, Authorization, and Accounting (AAA)

While the term AAA sounds generic and applicable to all sorts of security protocols, it has been, in the IETF, used in relation to network access authentication and is associated with the RADIUS ([RFC2865]) and the Diameter protocol ([RFC3588], [DIME-BASE]) in particular.

The authentication procedure for network access aims to deal with the task of verifying that a peer is authenticated and authorized prior to accessing a particular resource (often connectivity to the Internet). Typically, the authentication architecture for network access consists of the following building blocks: the Extensible

Authentication Protocol (EAP [RFC4017]) as a container to encapsulate EAP methods, an EAP Method (as a specific way to perform cryptographic authentication and key exchange, such as described in RFC 5216 [RFC5216] and RFC 5433 [RFC5433]), a protocol that carries EAP payloads between the end host and a server-side entity (such as a network access server), and a way to carry EAP payloads to back-end server infrastructure (potentially in a cross-domain scenario) to provide authorization and accounting functionality. The latter part is provided by RADIUS and Diameter. To carry EAP payloads between the end host and a network access server, different mechanisms have been standardized, such as the Protocol for Carrying Authentication for Network Access (PANA) [RFC5191] and IEEE 802.1X [IEEE802.1X]. For access to remote networks, such as enterprise networks, the ability to utilize EAP within IKEv2 [RFC5996] has also been developed.

More recently, the same architecture with EAP and RADIUS/Diameter is being reused for application layer protocols. More details about this architectural variant can be found in [ABFAB-ARCH].

3.1.2. Network Layer Security

IP security, as described in [RFC4301], addresses security at the IP layer, provided through the use of a combination of cryptographic and protocol security mechanisms. It offers a set of security services for traffic at the IP layer, in both the IPv4 and IPv6 environment. The set of security services offered includes access control, connectionless integrity, data origin authentication, detection and rejection of replays (a form of partial sequence integrity), confidentiality (via encryption), and limited traffic-flow confidentiality. These services are provided at the IP layer, offering protection in a standard fashion for all protocols that may be carried over IP (including IP itself).

The architecture foresees a split between the rather time-consuming (a) authentication and key exchange protocol step that also establishes a security association (a data structure with keying material and security parameters) and (b) the actual data traffic protection.

For the former step, the Internet Key Exchange protocol version 2 (IKEv2 [RFC5996]) is the most recent edition of the standardized protocol. IKE negotiates each of the cryptographic algorithms that will be used to protect the data independently, somewhat like selecting items a la carte.

For the actual data protection, two types of protocols have historically been used, namely the IP Authentication Header (AH)

[RFC4302] and the Encapsulating Security Payload (ESP) [RFC4303]. The two differ in the security services they offer; the most important distinction is that ESP offers confidentiality protection while AH does not. Since ESP can also provide authentication services, most recent protocol developments making use of IPsec only specify use of ESP and do not use AH.

In addition to these base line protocol mechanisms a number of extensions have been developed for IKEv2 (e.g., an extension to perform EAP-only authentication [RFC5998]) and since the architecture supports flexible treatment of cryptographic algorithms a number of them have been specified (e.g., [RFC4307] for IKEv2, and [RFC4835] for AH and ESP).

3.1.3. Transport Layer Security

Transport Layer Security v1.2 [RFC5246] are security services that protect data above the transport layer. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. TLS is application protocol independent.

TLS is composed of two layers: the TLS Record protocol and the TLS Handshake protocol. The TLS Record protocol provides connection security that has two basic properties: (a) confidentiality protection and (b) integrity protection.

The TLS Handshake protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. The negotiated parameters and the derived keying material is then used by the TLS Record protocol to perform its job.

Unlike IKEv2/IPsec, TLS negotiates these cryptographic parameters in suites, so-called 'cipher suites'. Examples of cipher suites that can be negotiated with TLS include Elliptic Curve Cryptography (ECC) [RFC4492] [RFC5289] [AES-CCM-ECC], Camellia [RFC5932], and the Suite B Profile [RFC5430]. [IEC62351-3] outlines the use of different TLS cipher suites for use in the Smart Grid. The basic cryptographic mechanisms for ECC have been documented in [RFC6090].

TLS must run over a reliable transport channel -- typically TCP. In order to offer the same security services for unreliable datagram traffic, such as UDP, the Datagram Transport Layer Security (DTLS [RFC4347] [DTLS]) was developed.

3.1.4. Application Layer Security

In certain cases, the application layer independent security mechanisms described in the previous sub-sections are not sufficient to deal with all the identified threats. For this purpose, a number of security primitives are additionally available at the application layer where the semantic of the application can be considered.

We will focus our description on a few mechanisms that are commonly used throughout the Internet.

Cryptographic Message Syntax (CMS [RFC5652]) is an encapsulation syntax to sign, digest, authenticate, or encrypt arbitrary message content. It also allows arbitrary attributes, such as signing time, to be signed along with the message content, and it provides for other attributes such as countersignatures to be associated with a signature. The CMS can support a variety of architectures for certificate-based key management, such as the one defined by the PKIX (Public Key Infrastructure using X.509) working group [RFC5280]. The CMS has been leveraged to supply security services in a variety of protocols, including secure email [RFC5751], key management [RFC5958] [RFC6031], and firmware updates [RFC4108].

Related work includes the use of digital signatures on XML-encoded documents, which has been jointly standardized by W3C and the IETF [RFC3275]. Digitally signed XML is a good choice where applications natively support XML-encoded data, such as the Extensible Messaging and Presence Protocol (XMPP).

More recently, the work on delegated authentication and authorization often demanded by Web applications have been developed with the Open Web Authentication (OAuth) protocol [RFC5849] [OAUTHv2]. OAuth is used by third-party applications to gain access to protected resources (such as energy consumption information about a specific household) without having the resource owner share its long-term credentials with that third-party. In OAuth, the third-party application requests access to resources controlled by the resource owner and hosted by the resource server, and is issued a different set of credentials than those of the resource owner. More specifically, the third-party applications obtain an access token during the OAuth protocol exchange. This token denotes a specific scope, duration, and other access attributes. As a result, it securely gains access to the protected resource with the consent of the resource owner.

3.1.5. Secure Shell

The Secure Shell (SSH) protocol [RFC4253] has been widely used by administrators and others for secure remote login, but is also usable for secure tunneling. More recently, protocols have chosen to layer on top of SSH for transport security services; for example, the NETCONF network management protocol (see Section 3.5.2) uses SSH as its main communications security protocol.

3.1.6. Key Management Infrastructures

All of the security protocols discussed above depend on cryptography for security, and hence require some form of key management. Most IETF protocols at least nominally require some scalable form of key management to be defined as mandatory to implement; indeed the lack of such key management features has in the past been a reason to delay approval of protocols. There are two generic key management schemes that are widely used by other Internet protocols, PKIX and Kerberos, each of which is briefly described below.

3.1.6.1. PKIX

Public Key Infrastructure (PKI) refers to the kind of key management that is based on certification authorities (CAs) issuing public key certificates for other key holders. By chaining from a trust anchor (a locally trusted copy of a CA public key) down to the public key of some protocol peer, PKI allows for secure binding between keys and protocol-specific names, such as email addresses, and hence enables security services such as data and peer authentication, data integrity, and confidentiality (encryption).

The main Internet standard for PKI is [RFC5280], which is a profile of the X.509 public key certificate format. There are a range of private and commercial CAs operating today providing the ability to manage and securely distribute keys for all protocols that use public key certificates, e.g., TLS and S/MIME. In addition to the profile standard, the PKIX working group has defined a number of management protocols (e.g., [RFC5272] and [RFC4210]) as well as protocols for handling revocation of public key certificates such as the Online Certificate Status Protocol (OCSP) [RFC2560].

PKI is generally perceived to better handle use-cases spanning multiple independent domains when compared to Kerberos.

3.1.6.2. Kerberos

The Kerberos Network Authentication System [RFC4120] is commonly used within organizations to centralize authentication, authorization, and policy in one place. Kerberos natively supports usernames and passwords as the basis of authentication. With Public Key Cryptography for Initial Authentication in Kerberos (PKINIT) [RFC4556], Kerberos supports certificate or public-key-based authentication. This may provide an advantage by concentrating policy about certificate validation and mapping of certificates to user accounts in one place. Through the GSS-API [RFC1964] [RFC2743] [RFC4121], Kerberos can be used to manage authentication for most applications. While Kerberos works best within organizations and enterprises, it does have facilities that permit authentication to be shared between administrative domains.

3.2. Network Layer

The IPS specifies two network layer protocols: IPv4 and IPv6. The following sections describe the IETF's coexistence and transition mechanisms for IPv4 and IPv6.

Note that on 3 February 2011, the IANA's IPv4 free pool (the pool of available, unallocated IPv4 addresses) was exhausted, and the Regional Internet Registrars' (RIRs') free pools are expected to be exhausted during the coming year, if not sooner. The IETF, the IANA, and the RIRs recommend that new deployments use IPv6, and that IPv4 infrastructures be supported via the mechanisms described in Section 3.2.1.

3.2.1. IPv4/IPv6 Coexistence Advice

The IETF has specified a variety of mechanisms designed to facilitate IPv4/IPv6 coexistence. The IETF actually recommends relatively few of them: the current advice to network operators is found in Guidelines for Using IPv6 Transition Mechanisms [RFC6180]. The thoughts in that document are replicated here.

3.2.1.1. Dual Stack Coexistence

The simplest coexistence approach is to

- provide a network that routes both IPv4 and IPv6,
- ensure that servers and their applications similarly support both protocols, and

- require that all new systems and applications purchased or upgraded support both protocols.

The net result is that over time all systems become protocol agnostic, and that eventually maintenance of IPv4 support becomes a business decision. This approach is described in the Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213].

3.2.1.2. Tunneling Mechanism

In those places in the network that support only IPv4, the simplest and most reliable approach to coexistence is to provide virtual connectivity using tunnels or encapsulations. Early in IPv6 deployment, this was often done using static tunnels. A more dynamic approach is documented in IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) [RFC5569].

3.2.1.3. Translation between IPv4 and IPv6 Networks

In those cases where an IPv4-only host would like to communicate with an IPv6-only host (or vice versa), a need for protocol translation may be indicated. At first blush, protocol translation may appear trivial; on deeper inspection, it turns out that protocol translation can be complicated.

The most reliable approach to protocol translation is to provide application layer proxies or gateways, which natively enable application-to-application connections using both protocols and can use whichever is appropriate. For example, a web proxy might use both protocols and as a result enable an IPv4-only system to run HTTP across an IPv6-only network or to a web server that implements only IPv6. Since this approach is a service of a protocol-agnostic server, it is not the subject of standardization by the IETF.

For those applications in which network layer translation is indicated, the IETF has designed a translation mechanism, which is described in the following documents:

- Framework for IPv4/IPv6 Translation [RFC6144]
- IPv6 Addressing of IPv4/IPv6 Translators [RFC6052]
- DNS extensions [RFC6147]
- IP/ICMP Translation Algorithm [RFC6145]
- Translation from IPv6 Clients to IPv4 Servers [RFC6146]

As with IPv4/IPv4 Network Address Translation, translation between IPv4 and IPv6 has limited real world applicability for an application protocol that carries IP addresses in its payload and expects those addresses to be meaningful to both client and server. However, for those protocols that do not, protocol translation can provide a useful network extension.

Network-based translation provides for two types of services: stateless (and therefore scalable and load-sharable) translation between IPv4 and IPv6 addresses that embed an IPv4 address in them, and stateful translation similar to IPv4/IPv4 translation between IPv4 addresses. The stateless mode is straightforward to implement, but due to the embedding, requires IPv4 addresses to be allocated to an otherwise IPv6-only network, and is primarily useful for IPv4-accessible servers implemented in the IPv6 network. The stateful mode allows clients in the IPv6 network to access servers in the IPv4 network, but does not provide such service for IPv4 clients accessing IPv6 peers or servers with general addresses; it has the advantage that it does not require that a unique IPv4 address be embedded in the IPv6 address of hosts using this mechanism.

Finally, note that some site networks are IPv6 only while some transit networks are IPv4 only. In these cases, it may be necessary to tunnel IPv6 over IPv4 or translate between IPv6 and IPv4.

3.2.2. Internet Protocol Version 4

IPv4 [RFC0791] and the Internet Control Message Protocol (ICMP) [RFC0792] comprise the IPv4 network layer. IPv4 provides unreliable delivery of datagrams.

IPv4 also provides for fragmentation and reassembly of long datagrams for transmission through networks with small Maximum Transmission Units (MTU). The MTU is the largest packet size that can be delivered across the network. In addition, the IPS provides ICMP [RFC0792], which is a separate protocol that enables the network to report errors and other issues to hosts that originate problematic datagrams.

IPv4 originally supported an experimental type of service field that identified eight levels of operational precedence styled after the requirements of military telephony, plus three and later four bit flags that OSI IS-IS for IPv4 (IS-IS) [RFC1195] and OSPF Version 2 [RFC2328] interpreted as control traffic; this control traffic is assured of not being dropped when queued or upon receipt, even if other traffic is being dropped. These control bits turned out to be less useful than the designers had hoped. They were replaced by the Differentiated Services Architecture [RFC2474] [RFC2475], which

contains a six-bit code point used to select an algorithm (a "per-hop behavior") to be applied to the datagram. The IETF has also produced a set of Configuration Guidelines for DiffServ Service Classes [RFC4594], which describes a set of service classes that may be useful to a network operator.

3.2.2.1. IPv4 Address Allocation and Assignment

IPv4 addresses are administratively assigned, usually using automated methods, using the Dynamic Host Configuration Protocol (DHCP) [RFC2131]. On most interface types, neighboring systems identify each others' addresses using the Address Resolution Protocol (ARP) [RFC0826].

3.2.2.2. IPv4 Unicast Routing

Routing for the IPv4 Internet is accomplished by routing applications that exchange connectivity information and build semi-static destination routing databases. If a datagram is directed to a given destination address, the address is looked up in the routing database, and the most specific ("longest") prefix found that contains it is used to identify the next-hop router or the end system to which it will be delivered. This is not generally implemented on hosts, although it can be; a host normally sends datagrams to a router on its local network, and the router carries out the intent.

IETF specified routing protocols include RIP Version 2 [RFC2453], OSI IS-IS for IPv4 [RFC1195], OSPF Version 2 [RFC2328], and BGP-4 [RFC4271]. Active research exists in mobile ad hoc routing and other routing paradigms; these result in new protocols and modified forwarding paradigms.

3.2.2.3. IPv4 Multicast Forwarding and Routing

IPv4 was originally specified as a unicast (point to point) protocol, and was extended to support multicast in [RFC1112]. This uses the Internet Group Management Protocol [RFC3376] [RFC4604] to enable applications to join multicast groups, and for most applications uses Source-Specific Multicast [RFC4607] for routing and delivery of multicast messages.

An experiment carried out in IPv4 that is not part of the core Internet architecture but may be of interest in the Smart Grid is the development of so-called "Reliable Multicast". This is "so-called" because it is not "reliable" in the strict sense of the word -- it is perhaps better described as "enhanced reliability". A best effort network by definition can lose traffic, duplicate it, or reorder it, something as true for multicast as for unicast. Research in

"Reliable Multicast" technology intends to improve the probability of delivery of multicast traffic.

In that research, the IETF imposed guidelines [RFC2357] on the research community regarding what was desirable. Important results from that research include a number of papers and several proprietary protocols including some that have been used in support of business operations. RFCs in the area include The Use of Forward Error Correction (FEC) in Reliable Multicast [RFC3453], the Negative-acknowledgment (NACK)-Oriented Reliable Multicast (NORM) Protocol [RFC5740], and the Selectively Reliable Multicast Protocol (SRMP) [RFC4410].

3.2.3. Internet Protocol Version 6

IPv6 [RFC2460], with the Internet Control Message Protocol "v6" [RFC4443], constitutes the next generation protocol for the Internet. IPv6 provides for transmission of datagrams from source to destination hosts, which are identified by fixed-length addresses.

IPv6 also provides for fragmentation and reassembly of long datagrams by the originating host, if necessary, for transmission through "small packet" networks. ICMPv6, which is a separate protocol implemented along with IPv6, enables the network to report errors and other issues to hosts that originate problematic datagrams.

IPv6 adopted the Differentiated Services Architecture [RFC2474] [RFC2475], which contains a six-bit code point used to select an algorithm (a "per-hop behavior") to be applied to the datagram.

The IPv6 over Low-Power Wireless Personal Area Networks RFC [RFC4919] and the Compression Format for IPv6 Datagrams in 6LoWPAN Networks document [6LOWPAN-HC] addresses IPv6 header compression and subnet architecture in at least some sensor networks, and may be appropriate to the Smart Grid Advanced Metering Infrastructure or other sensor domains.

3.2.3.1. IPv6 Address Allocation and Assignment

An IPv6 Address [RFC4291] may be administratively assigned using DHCPv6 [RFC3315] in a manner similar to the way IPv4 addresses are. In addition, IPv6 addresses may also be autoconfigured. Autoconfiguration enables various models of network management that may be advantageous in different use cases. Autoconfiguration procedures are defined in [RFC4862] and [RFC4941]. IPv6 neighbors identify each others' addresses using Neighbor Discovery (ND) [RFC4861]. SEcure Neighbor Discovery (SEND) [RFC3971] may be used to secure these operations.

3.2.3.2. IPv6 Routing

Routing for the IPv6 Internet is accomplished by routing applications that exchange connectivity information and build semi-static destination routing databases. If a datagram is directed to a given destination address, the address is looked up in the routing database, and the most specific ("longest") prefix found that contains it is used to identify the next-hop router or the end system to which it will be delivered. Routing is not generally implemented on hosts (although it can be); generally, a host sends datagrams to a router on its local network, and the router carries out the intent.

IETF-specified routing protocols include RIP for IPv6 [RFC2080], IS-IS for IPv6 [RFC5308], OSPF for IPv6 [RFC5340], and BGP-4 for IPv6 [RFC2545]. Active research exists in mobile ad hoc routing, routing in low-power networks (sensors and Smart Grids), and other routing paradigms; these result in new protocols and modified forwarding paradigms.

3.2.4. Routing for IPv4 and IPv6

3.2.4.1. Routing Information Protocol

The prototypical routing protocol used in the Internet has probably been the Routing Information Protocol [RFC1058]. People that use it today tend to deploy RIPng for IPv6 [RFC2080] and RIP Version 2 [RFC2453]. Briefly, RIP is a distance vector routing protocol that is based on a distributed variant of the widely known Bellman-Ford algorithm. In distance vector routing protocols, each router announces the contents of its route table to neighboring routers, which integrate the results with their route tables and re-announce them to others. It has been characterized as "routing by rumor", and suffers many of the ills we find in human gossip -- propagating stale or incorrect information in certain failure scenarios, and being in cases unresponsive to changes in topology. [RFC1058] provides guidance to algorithm designers to mitigate these issues.

3.2.4.2. Open Shortest Path First

The Open Shortest Path First (OSPF) routing protocol is one of the more widely used protocols in the Internet. OSPF is based on Dijkstra’s well known Shortest Path First (SPF) algorithm. It is implemented as OSPF Version 2 [RFC2328] for IPv4, OSPF for IPv6 [RFC5340] for IPv6, and the Support of Address Families in OSPFv3 [RFC5838] to enable [RFC5340] routing both IPv4 and IPv6.

The advantage of any SPF-based protocol (i.e., OSPF and IS-IS) is primarily that every router in the network constructs its view of the

network from first-hand knowledge rather than the "gossip" that distance vector protocols propagate. As such, the topology is quickly and easily changed by simply announcing the change. The disadvantage of SPF-based protocols is that each router must store a first-person statement of the connectivity of each router in the domain.

3.2.4.3. ISO Intermediate System to Intermediate System

The Intermediate System to Intermediate System (IS-IS) routing protocol is one of the more widely used protocols in the Internet. IS-IS is also based on Dijkstra's SPF algorithm. It was originally specified as ISO DP 10589 for the routing of Connectionless Network Service (CLNS), and extended for routing in TCP/IP and dual environments [RFC1195], and more recently for routing of IPv6 [RFC5308].

As with OSPF, the positives of any SPF-based protocol and specifically IS-IS are primarily that the network is described as a lattice of routers with connectivity to subnets and isolated hosts. It's topology is quickly and easily changed by simply announcing the change, without the issues of "routing by rumor", since every host within the routing domain has a first-person statement of the connectivity of each router in the domain. The negatives are a corollary: each router must store a first-person statement of the connectivity of each router in the domain.

3.2.4.4. Border Gateway Protocol

The Border Gateway Protocol (BGP) [RFC4271] is widely used in the IPv4 Internet to exchange routes between administrative entities -- service providers, their peers, their upstream networks, and their customers -- while applying specific policy. Multiprotocol Extensions [RFC4760] to BGP allow BGP to carry IPv6 Inter-Domain Routing [RFC2545], multicast reachability information, and VPN information, among others.

Considerations that apply with BGP deal with the flexibility and complexity of the policies that must be defined. Flexibility is a good thing; in a network that is not run by professionals, the complexity is burdensome.

3.2.4.5. Dynamic MANET On-Demand (DYMO) Routing

The Mobile Ad Hoc working group of the IETF developed, among other protocols, Ad hoc On-Demand Distance Vector (AODV) Routing [RFC3561]. This protocol captured the minds of some in the embedded devices industry, but experienced issues in wireless networks such as

802.15.4 and 802.11's Ad Hoc mode. As a result, it is in the process of being updated in the Dynamic MANET On-demand (DYMO) Routing protocol [DYMO].

AODV and DYMO are essentially reactive routing protocols designed for mobile ad hoc networks, and usable in other forms of ad hoc networks. They provide connectivity between a device within a distributed subnet and a few devices (including perhaps a gateway or router to another subnet) without tracking connectivity to other devices. In essence, routing is calculated and discovered upon need, and a host or router need only maintain the routes that currently work and are needed.

3.2.4.6. Optimized Link State Routing Protocol

The Optimized Link State Routing Protocol (OLSR) [RFC3626] is a proactive routing protocol designed for mobile ad hoc networks, and can be used in other forms of ad hoc networks. It provides arbitrary connectivity between systems within a distributed subnet. As with protocols designed for wired networks, routing is calculated whenever changes are detected, and maintained in each router's tables. The set of nodes that operate as routers within the subnet, however, are fairly fluid, and dependent on this instantaneous topology of the subnet.

3.2.4.7. Routing for Low-Power and Lossy Networks

The IPv6 Routing Protocol for Low power and Lossy Networks (RPL) [RPL] is a reactive routing protocol designed for use in resource constrained networks. Requirements for resource constrained networks are defined in [RFC5548], [RFC5673], [RFC5826], and [RFC5867].

Briefly, a constrained network is comprised of nodes that:

- Are built with limited processing power and memory, and sometimes energy when operating on batteries.
- Are interconnected through a low-data-rate network interface and are potentially vulnerable to communication instability and low packet delivery rates.
- Potentially have a mix of roles such as being able to act as a host (i.e., generating traffic) and/or a router (i.e., both forwarding and generating RPL traffic).

3.2.5. IPv6 Multicast Forwarding and Routing

IPv6 specifies both unicast and multicast datagram exchange. This uses the Multicast Listener Discovery Protocol (MLDv2) [RFC2710] [RFC3590] [RFC3810] [RFC4604] to enable applications to join multicast groups, and for most applications uses Source-Specific Multicast [RFC4607] for routing and delivery of multicast messages.

The mechanisms experimentally developed for reliable multicast in IPv4, discussed in Section 3.2.2.3, can be used in IPv6 as well.

3.2.5.1. Protocol-Independent Multicast Routing

A multicast routing protocol has two basic functions: building the multicast distribution tree and forwarding multicast traffic. Multicast routing protocols generally contain a control plane for building distribution trees, and a forwarding plane that uses the distribution tree when forwarding multicast traffic.

The multicast model works as follows: hosts express their interest in receiving multicast traffic from a source by sending a Join message to their first-hop router. That router in turn sends a Join message upstream towards the root of the tree, grafting the router (leaf node) onto the distribution tree for the group. Data is delivered down the tree toward the leaf nodes, which forward it onto the local network for delivery.

The initial multicast model deployed in the Internet was known as Any-Source Multicast (ASM). In the ASM model, any host could send to the group and inter-domain multicast was difficult. Protocols such as Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised) [RFC3973] and Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised) [RFC4601] were designed for the ASM model.

Many modern multicast deployments use Source-Specific Multicast (PIM-SSM) [RFC3569][RFC4608]. In the SSM model, a host expresses interest in a "channel", which is comprised of a source (S) and a group (G). Distribution trees are rooted to the sending host (called an "(S,G) tree"). Since only the source S can send on to the group, SSM has inherent anti-jamming capability. In addition, inter-domain multicast is simplified since finding the (S,G) channel they are interested in receiving is the responsibility of the receivers (rather than the networks). This implies that SSM requires some form of directory service so that receivers can find the (S,G) channels.

3.2.6. Adaptation to Lower-Layer Networks and Link Layer Protocols

In general, the layered architecture of the Internet enables the IPS to run over any appropriate layer two architecture. The ability to change the link or physical layer without having to rethink the network layer, transports, or applications has been a great benefit in the Internet.

Examples of link layer adaptation technology include:

Ethernet/IEEE 802.3: IPv4 has run on each link layer environment that uses the Ethernet header (which is to say 10 and 100 MBPS wired Ethernet, 1 and 10 GBPS wired Ethernet, and the various versions of IEEE 802.11) using [RFC0894]. IPv6 does the same using [RFC2464].

PPP: The IETF has defined a serial line protocol, the Point-to-Point Protocol (PPP) [RFC1661], that uses High-Level Data Link Control (bit-synchronous or byte synchronous) framing. The IPv4 adaptation specification is [RFC1332], and the IPv6 adaptation specification is [RFC5072]. Current use of this protocol is in traditional serial lines, authentication exchanges in DSL networks using PPP Over Ethernet (PPPoE) [RFC2516], and the Digital Signaling Hierarchy (generally referred to as Packet-on-SONET/SDH) using PPP over SONET/SDH [RFC2615].

IEEE 802.15.4: The adaptation specification for IPv6 transmission over IEEE 802.15.4 Networks is [RFC4944].

Numerous other adaptation specifications exist, including ATM, Frame Relay, X.25, other standardized and proprietary LAN technologies, and others.

3.3. Transport Layer

This section outlines the functionality of UDP, TCP, SCTP, and DCCP. UDP and TCP are best known and most widely used in the Internet today, while SCTP and DCCP are newer protocols that were built for specific purposes. Other transport protocols can be built when required.

3.3.1. User Datagram Protocol (UDP)

The User Datagram Protocol [RFC0768] and the Lightweight User Datagram Protocol [RFC3828] are properly not "transport" protocols in the sense of "a set of rules governing the exchange or transmission of data electronically between devices". They are labels that

provide for multiplexing of applications directly on the IP layer, with transport functionality embedded in the application.

Many exchange designs have been built using UDP, and many of them have not worked out. As a result, the use of UDP really should be treated as designing a new transport. Advice on the use of UDP in new applications can be found in Unicast UDP Usage Guidelines for Application Designers [RFC5405].

Datagram Transport Layer Security [RFC5238] can be used to prevent eavesdropping, tampering, or message forgery for applications that run over UDP. Alternatively, UDP can run over IPsec.

3.3.2. Transmission Control Protocol (TCP)

TCP [RFC0793] is the predominant transport protocol used in the Internet. It is "reliable", as the term is used in protocol design: it delivers data to its peer and provides acknowledgement to the sender, or it dies trying. It has extensions for Congestion Control [RFC5681] and Explicit Congestion Notification [RFC3168].

The user interface for TCP is a byte stream interface -- an application using TCP might "write" to it several times only to have the data compacted into a common segment and delivered as such to its peer. For message-stream interfaces, ACSE/ROSE uses the ISO Transport Service on TCP [RFC1006][RFC2126] in the application.

Transport Layer Security [RFC5246] can be used to prevent eavesdropping, tampering, or message forgery. Alternatively, TCP can run over IPsec. Additionally, [RFC4987] discusses mechanisms similar to SCTP's and DCCP's "cookie" approach that may be used to secure TCP sessions against flooding attacks.

Finally, note that TCP has been the subject of ongoing research and development since it was written. The Roadmap for TCP Specification Documents [RFC4614] captures this history, and is intended to be a guide to current and future developers in the area.

3.3.3. Stream Control Transmission Protocol (SCTP)

SCTP [RFC4960] is a more recent reliable transport protocol that can be imagined as a TCP-like context containing multiple separate and independent message streams (unlike TCP's byte streams). The design of SCTP includes appropriate congestion avoidance behavior and resistance to flooding and masquerade attacks. As it uses a message stream interface, it may also be more appropriate for the ISO Transport Service than using RFC 1006/2126 to turn TCP's octet streams into a message interface.

SCTP offers several delivery options. The basic service is sequential non-duplicated delivery of messages within a stream, for each stream in use. Since streams are independent, one stream may pause due to head-of-line blocking while another stream in the same session continues to deliver data. In addition, SCTP provides a mechanism for bypassing the sequenced delivery service. User messages sent using this mechanism are delivered to the SCTP user as soon as they are received.

SCTP implements a simple "cookie" mechanism intended to limit the effectiveness of flooding attacks by mutual authentication. This demonstrates that the application is connected to the same peer, but does not identify the peer. Mechanisms also exist for Dynamic Address Reconfiguration [RFC5061], enabling peers to change addresses during the session and yet retain connectivity. Transport Layer Security [RFC3436] can be used to prevent eavesdropping, tampering, or message forgery. Alternatively, SCTP can run over IPsec.

3.3.4. Datagram Congestion Control Protocol (DCCP)

DCCP [RFC4340] is an "unreliable" transport protocol (e.g., one that does not guarantee message delivery) that provides bidirectional unicast connections of congestion-controlled unreliable datagrams. DCCP is suitable for applications that transfer fairly large amounts of data and that can benefit from control over the tradeoff between timeliness and reliability.

DCCP implements a simple "cookie" mechanism intended to limit the effectiveness of flooding attacks by mutual authentication. This demonstrates that the application is connected to the same peer, but does not identify the peer. Datagram Transport Layer Security [RFC5238] can be used to prevent eavesdropping, tampering, or message forgery. Alternatively, DCCP can run over IPsec.

3.4. Infrastructure

3.4.1. Domain Name System

In order to facilitate network management and operations, the Internet community has defined the Domain Name System (DNS) [RFC1034] [RFC1035]. Names are hierarchical: a name like example.com is found registered with a .com registrar, and within the associated network other names like baldur.cincinatti.example.com can be defined, with obvious hierarchy. Security extensions, which allow a registry to sign the records it contains and in so doing demonstrate their authenticity, are defined by the DNS Security Extensions [RFC4033] [RFC4034] [RFC4035].

Devices can also optionally update their own DNS record. For example, a sensor that is using Stateless Address Autoconfiguration [RFC4862] to create an address might want to associate it with a name using DNS Dynamic Update [RFC2136] or DNS Secure Dynamic Update [RFC3007].

3.4.2. Dynamic Host Configuration

As discussed in Section 3.2.2, IPv4 address assignment is generally performed using DHCP [RFC2131]. By contrast, Section 3.2.3 points out that IPv6 address assignment can be accomplished using either autoconfiguration [RFC4862] [RFC4941] or DHCPv6 [RFC3315]. The best argument for the use of autoconfiguration is a large number of systems that require little more than a random number as an address; the argument for DHCP is administrative control.

There are other parameters that may need to be allocated to hosts requiring administrative configuration; examples include the addresses of DNS servers, keys for Secure DNS, and Network Time servers.

3.4.3. Network Time

The Network Time Protocol was originally designed by Dave Mills of the University of Delaware and CSNET, implementing a temporal metric in the Fuzzball Routing Protocol and generally coordinating time experiments. The current versions of the time protocol are the Network Time Protocol [RFC5905].

3.5. Network Management

The IETF has developed two protocols for network management: SNMP and NETCONF. SNMP is discussed in Section 3.5.1, and NETCONF is discussed in Section 3.5.2.

3.5.1. Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol, originally specified in the late 1980’s and having passed through several revisions, is specified in several documents:

- An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks [RFC3411]
- Message Processing and Dispatching [RFC3412]
- SNMP Applications [RFC3413]

- User-based Security Model (USM) for SNMP version 3 [RFC3414]
- View-based Access Control Model (VACM) [RFC3415]
- Version 2 of the SNMP Protocol Operations [RFC3416]
- Transport Mappings [RFC3417]
- Management Information Base (MIB) [RFC3418]

It provides capabilities for polled and event-driven activities, and for both monitoring and configuration of systems in the field. Historically, it has been used primarily for monitoring nodes in a network. Messages and their constituent data are encoded using a profile of ASN.1.

3.5.2. Network Configuration (NETCONF) Protocol

The NETCONF Configuration Protocol is specified in one basic document, with supporting documents for carrying it over the IPS. These documents include:

- NETCONF Configuration Protocol [RFC4741]
- Using the NETCONF Configuration Protocol over Secure SHell (SSH) [RFC4742]
- Using NETCONF over the Simple Object Access Protocol (SOAP) [RFC4743]
- Using the NETCONF Protocol over the Blocks Extensible Exchange Protocol (BEEP) [RFC4744]
- NETCONF Event Notifications [RFC5277]
- NETCONF over Transport Layer Security (TLS) [RFC5539]
- Partial Lock Remote Procedure Call (RPC) for NETCONF [RFC5717]

NETCONF was developed in response to operator requests for a common configuration protocol based on ASCII text, unlike ASN.1. In essence, it carries XML-encoded remote procedure call (RPC) data. In response to Smart Grid requirements, there is consideration of a variant of the protocol that could be used for polled and event-driven management activities, and for both monitoring and configuration of systems in the field.

3.6. Service and Resource Discovery

Service and resource discovery are among the most important protocols for constrained resource self-organizing networks. These include various sensor networks as well as the Home Area Networks (HANs), Building Area Networks (BANs), and Field Area Networks (FANs) envisioned by Smart Grid architects.

3.6.1. Service Discovery

Service discovery protocols are designed for the automatic configuration and detection of devices, and the services offered by the discovered devices. In many cases service discovery is performed by so-called "constrained resource" devices (i.e., those with limited processing power, memory, and power resources).

In general, service discovery is concerned with the resolution and distribution of host names via multicast DNS [MULTICAST-DNS] and the automatic location of network services via DHCP (Section 3.4.2), the DNS Service Discovery (DNS-SD) [DNS-SD] (part of Apple's Bonjour technology), and the Service Location Protocol (SLP) [RFC2608].

3.6.2. Resource Discovery

Resource Discovery is concerned with the discovery of resources offered by end-points and is extremely important in machine-to-machine closed-loop applications (i.e., those with no humans in the loop). The goals of resource discovery protocols include:

- Simplicity of creation and maintenance of resources
- Commonly understood semantics
- Conformance to existing and emerging standards
- International scope and applicability
- Extensibility
- Interoperability among collections and indexing systems

The Constrained Application Protocol (CoAP) [COAP] is being developed in IETF with these goals in mind. In particular, CoAP is designed for use in constrained resource networks and for machine-to-machine applications such as smart energy and building automation. It provides a RESTful transfer protocol [RESTFUL], a built-in resource discovery protocol, and includes web concepts such as URIs and content-types. CoAP provides both unicast and multicast resource

discovery and includes the ability to filter on attributes of resource descriptions. Finally, CoAP resource discovery can also be used to discover HTTP resources.

For simplicity, CoAP makes the assumption that all CoAP servers listen on the default CoAP port or otherwise have been configured or discovered using some general service discovery mechanism such as DNS Service Discovery (DNS-SD) [DNS-SD].

Resource discovery in CoAP is accomplished through the use of well-known resources that describe the links offered by a CoAP server. CoAP defines a well-known URI for discovery: "/.well-known/r" [RFC5785]. For example, the query [GET /.well-known/r] returns a list of links (representing resources) available from the queried CoAP server. A query such as [GET /.well-known/r?n=Voltage] returns the resources with the name Voltage.

3.7. Other Applications

There are many applications that rely on the IP infrastructure, but are not properly thought of as part of the IP infrastructure itself. These applications may be useful in the context of the Smart Grid. The choices made when constructing a profile of the Internet Profile Suite may impact how such applications could be used. Some of them, not by any means an exhaustive list, are discussed here.

3.7.1. Session Initiation Protocol

The Session Initiation Protocol [RFC3261] [RFC3265] [RFC3853] [RFC4320] [RFC4916] [RFC5393] [RFC5621] is an application layer control (signaling) protocol for creating, modifying, and terminating multimedia sessions on the Internet, and is meant to be more scalable than H.323. Multimedia sessions can be voice, video, instant messaging, shared data, and/or subscriptions of events. SIP can run on top of TCP, UDP, SCTP, or TLS over TCP. SIP is independent of the transport layer, and independent of the underlying IPv4/v6 version. In fact, the transport protocol used can change as the SIP message traverses SIP entities from source to destination.

SIP itself does not choose whether a session is voice or video, nor does it identify the actual endpoints' IP addresses. The Session Description Protocol (SDP) [RFC4566] is intended for those purposes. Within the SDP, which is transported by SIP, codecs are offered and accepted (or not), and the port number and IP address at which each endpoint wants to receive their Real-time Transport Protocol (RTP) [RFC3550] packets are determined. The introduction of Network Address Translation (NAT) technology into the profile, whether IPv4/

IPv4, IPv4/IPv6 as described in Section 3.2.1.3, or IPv6/IPv6, increases the complexity of SIP/SDP deployment. This is further discussed in [RFC2993] and [RFC5626].

3.7.2. Extensible Messaging and Presence Protocol

The Extensible Messaging and Presence Protocol (XMPP) [RFC6120] is a protocol for streaming Extensible Markup Language (XML) elements in order to exchange structured information in close to real time between any two network endpoints. Since XMPP provides a generalized, extensible framework for exchanging XML data, it has been proposed as an application structure for interchange between embedded devices and sensors. It is currently used for Instant Messaging and Presence [RFC6121] and a wide variety of real-time communication modes. These include multi-user chat, publish-subscribe, alerts and notifications, service discovery, multimedia session management, device configuration, and remote procedure calls. XMPP supports channel encryption using TLS [RFC5246] and strong authentication (including PKIX certificate authentication) using SASL [RFC4422]. It also makes use of Unicode-compliant addresses and UTF-8 [RFC3629] data exchange for internationalization.

XMPP allows for End-to-End Signing and Object Encryption [RFC3923], access to objects named using Uniform Resource Names (URN) [RFC4854], use of Internationalized Resource Identifiers (IRIs) and Uniform Resource Identifiers (URIs) [RFC5122], and the presentation of Notifications [RFC5437].

3.7.3. Calendaring

Internet calendaring, as implemented in Apple iCal, Microsoft Outlook and Entourage, and Google Calendar, is specified in Internet Calendaring and Scheduling Core Object Specification (iCalendar) [RFC5545] and is in the process of being updated to an XML schema in iCalendar XML Representation [xCAL]. Several protocols exist to carry calendar events, including the iCalendar Transport-Independent Interoperability Protocol (iTIP) [RFC5546], the iCalendar Message-Based Interoperability Protocol (iMIP) [RFC6047], and open source work on the Atom Publishing Protocol [RFC5023].

4. A Simplified View of the Business Architecture

The Internet is a network of networks in which networks are interconnected in specific ways and are independently operated. It is important to note that the underlying Internet architecture puts no restrictions on the ways that networks are interconnected; interconnection is a business decision. As such, the Internet

interconnection architecture can be thought of as a "business structure" for the Internet.

Central to the Internet business structure are the networks that provide connectivity to other networks, called "transit networks". These networks sell bulk bandwidth and routing services to each other and to other networks as customers. Around the periphery of the transit network are companies, schools, and other networks that provide services directly to individuals. These might generally be divided into "enterprise networks" and "access networks"; enterprise networks provide "free" connectivity to their own employees or members, and also provide them a set of services including electronic mail, web services, and so on. Access networks sell broadband connectivity (DSL, Cable Modem, 802.11 wireless, or 3GPP wireless) or "dial" services (including PSTN dial-up and ISDN) to subscribers. The subscribers are typically either residential or small office/home office (SOHO) customers. Residential customers are generally entirely dependent on their access provider for all services, while a SOHO buys some services from the access provider and may provide others for itself. Networks that sell transit services to nobody else -- SOHO, residential, and enterprise networks -- are generally refereed to as "edge networks"; transit networks are considered to be part of the "core" of the Internet, and access networks are between the two. This general structure is depicted in Figure 3.

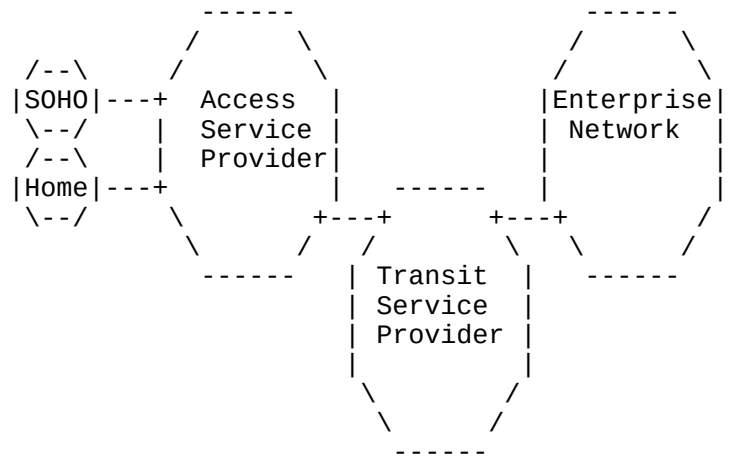

Figure 3: Conceptual Model of Internet Businesses

A specific example is shown in a traceroute from a home to a nearby school. Internet connectivity in Figure 4 passes through

- the home network,
- Cox Communications, an access network using Cable Modem technology,
- TransitRail, a commodity peering service for research and education (R&E) networks,
- Corporation for Education Network Initiatives in California (CENIC), a transit provider for educational networks, and
- the University of California at Santa Barbara, which in this context might be viewed as an access network for its students and faculty or as an enterprise network.

```
<stealth-10-32-244-218:> fred% traceroute www.ucsb.edu
traceroute to web.ucsb.edu (128.111.24.41),
        64 hops max, 40 byte packets
 1  fred-vpn (10.32.244.217)  1.560 ms  1.108 ms  1.133 ms
 2  wsip-98-173-193-1.sb.sd.cox.net (98.173.193.1)  12.540 ms  ...
 3  68.6.13.101 ...
 4  68.6.13.129 ...
 5  langbbr01-as0.r2.la.cox.net ...
 6  calren46-cust.lsanca01.transitrail.net ...
 7  dc-lax-core1--lax-peer1-ge.cenic.net ...
 8  dc-lax-agg1--lax-core1-ge.cenic.net ...
 9  dc-ucsb--dc-lax-dc2.cenic.net ...
10  r2--r1--1.commserv.ucsb.edu ...
11  574-c--r2--2.commserv.ucsb.edu ...
12  * * *
```

Figure 4: Traceroute from Residential Customer to Educational Institution

Another specific example could be shown in a traceroute from the home through a Virtual Private Network (VPN tunnel) from the home, crossing Cox Cable (an access network) and Pacific Bell (a transit network), and terminating in Cisco Systems (an enterprise network); a traceroute of the path doesn't show that as it is invisible within the VPN and the contents of the VPN are invisible, due to encryption, to the networks on the path. Instead, the traceroute in Figure 5 is entirely within Cisco's internal network.

```
<stealth-10-32-244-218:~> fred% traceroute irp-view13
traceroute to irp-view13.cisco.com (171.70.120.60),
       64 hops max, 40 byte packets
 1  fred-vpn (10.32.244.217)  2.560 ms  1.100 ms  1.198 ms
         <tunneled path through Cox and Pacific Bell>
 2  ****
 3  sjc24-00a-gw2-ge2-2 (10.34.251.137)  26.298 ms...
 4  sjc23-a5-gw2-g2-1 (10.34.250.78)  25.214 ms  ...
 5  sjc20-a5-gw1 (10.32.136.21)  23.205 ms  ...
 6  sjc12-abb4-gw1-t2-7 (10.32.0.189)  46.028 ms  ...
 7  sjc5-sbb4-gw1-ten8-2 (171.*.*.*)  26.700 ms  ...
 8  sjc12-dc5-gw2-ten3-1 ...
 9  sjc5-dc4-gw1-ten8-1 ...
10  irp-view13 ...
```

Figure 5: Traceroute across VPN

Note that in both cases, the home network uses private address space [RFC1918] while other networks generally use public address space, and that three middleware technologies are in use here. These are the uses of a firewall, a Network Address Translator (NAT), and a Virtual Private Network (VPN).

Firewalls are generally sold as and considered by many to be a security technology. This is based on the fact that a firewall imposes a border between two administrative domains. Typically, a firewall will be deployed between a residential, SOHO, or enterprise network and its access or transit provider. In its essence, a firewall is a data diode, imposing a policy on what sessions may pass between a protected domain and the rest of the Internet. Simple policies generally permit sessions to be originated from the protected network but not from the outside; more complex policies may permit additional sessions from the outside, such as electronic mail to a mail server or a web session to a web server, and may prevent certain applications from global access even though they are originated from the inside.

Note that the effectiveness of firewalls remains controversial. While network managers often insist on deploying firewalls as they impose a boundary, others point out that their value as a security solution is debatable. This is because most attacks come from behind the firewall. In addition, firewalls do not protect against application layer attacks such as viruses carried in email. Thus, as a security solution, firewalls are justified as a layer in defense in depth. That is, while an end system must in the end be responsible for its own security, a firewall can inhibit or prevent certain kinds of attacks, for example the consumption of CPU time on a critical server.

Key documents describing firewall technology and the issues it poses include:

- IP Multicast and Firewalls [RFC2588]
- Benchmarking Terminology for Firewall Performance [RFC2647]
- Behavior of and Requirements for Internet Firewalls [RFC2979]
- Benchmarking Methodology for Firewall Performance [RFC3511]
- Mobile IPv6 and Firewalls: Problem Statement [RFC4487]
- NAT and Firewall Traversal Issues of Host Identity Protocol Communication [RFC5207]

Network Address Translation is a technology that was developed in response to ISP behaviors in the mid-1990's; when [RFC1918] was published, many ISPs started handing out single or small numbers of addresses, and edge networks were forced to translate. In time, this became considered a good thing, or at least not a bad thing; it amplified the public address space, and it was sold as if it were a firewall. It of course is not; while traditional dynamic NATs only translate between internal and external session address/port tuples during the detected duration of the session, that session state may exist in the network much longer than it exists on the end system, and as a result constitutes an attack vector. The design, value, and limitations of network address translation are described in:

- IP Network Address Translator Terminology and Considerations [RFC2663]
- Traditional IP Network Address Translator [RFC3022]
- Protocol Complications with the IP Network Address Translator [RFC3027]
- Network Address Translator Friendly Application Design Guidelines [RFC3235]
- IAB Considerations for Network Address Translation [RFC3424]
- IPsec-Network Address Translation Compatibility Requirements [RFC3715]
- Network Address Translation Behavioral Requirements for Unicast UDP [RFC4787]

- State of Peer-to-Peer Communication across Network Address Translators [RFC5128]

- IP Multicast Requirements for a Network Address Translator and a Network Address Port Translator [RFC5135]

Virtual Private Networks come in many forms; what they have in common is that they are generally tunneled over the Internet backbone, so that as in Figure 5, connectivity appears to be entirely within the edge network although it is in fact across a service provider's network. Examples include IPsec tunnel-mode encrypted tunnels, IP-in-IP or GRE tunnels, and MPLS LSPs [RFC3031][RFC3032].

5. Security Considerations

Security is addressed in some detail in Section 2.2 and Section 3.1.

6. Acknowledgements

Review comments were made by Adrian Farrel, Andrew Yourtchenko, Ashok Narayanan, Bernie Volz, Chris Lonvick, Dan Romascanu, Dave McGrew, Dave Oran, David Harrington, David Su, Don Sturek, Francis Cleveland, Hemant Singh, James Polk, Jari Arkko, John Meylor, Joseph Salowey, Julien Abeille, Kerry Lynn, Lars Eggert, Magnus Westerlund, Murtaza Chiba, Paul Duffy, Paul Hoffman, Peter Saint-Andre, Ralph Droms, Robert Sparks, Russ White, Sean Turner, Sheila Frankel, Stephen Farrell, Tim Polk, Toerless Eckert, Tom Herbst, Vint Cerf, and Yoshihiro Ohba. Several of the individuals suggested text, which was very useful, as the authors don't claim to know half as much as their reviewers collectively do.

7. References

7.1. Normative References

[RFC1122] Braden, R., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, October 1989.

[RFC1123] Braden, R., "Requirements for Internet Hosts - Application and Support", STD 3, RFC 1123, October 1989.

[RFC1812] Baker, F., "Requirements for IP Version 4 Routers", RFC 1812, June 1995.

[RFC4294] Loughney, J., "IPv6 Node Requirements", RFC 4294, April 2006.

7.2. Informative References

[6LOWPAN-HC] Hui, J. and P. Thubert, "Compression Format for IPv6 Datagrams in Low Power and Lossy Networks (6LoWPAN)", Work in Progress, February 2011.

[ABFAB-ARCH] Howlett, J., Hartman, S., Tschofenig, H., and E. Lear, "Application Bridging for Federated Access Beyond Web (ABFAB) Architecture", Work in Progress, March 2011.

[AES-CCM-ECC] McGrew, D., Bailey, D., Campagna, M., and R. Dugal, "AES-CCM ECC Cipher Suites for TLS", Work in Progress, January 2011.

[COAP] Shelby, Z., Hartke, K., Bormann, C., and B. Frank, "Constrained Application Protocol (CoAP)", Work in Progress, March 2011.

[DIME-BASE] Fajardo, V., Ed., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol", Work in Progress, January 2011.

[DNS-SD] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", Work in Progress, February 2011.

[DTLS] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security version 1.2", Work in Progress, March 2011.

[DYMO] Chakeres, I. and C. Perkins, "Dynamic MANET On-demand (DYMO) Routing", Work in Progress, July 2010.

[IEC61850] Wikipedia, "Wikipedia Article: IEC 61850", June 2011, <http://en.wikipedia.org/w/index.php?title=IEC_61850&oldid=433437827>.

[IEC62351-3] International Electrotechnical Commission Technical Committee 57, "POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE. DATA AND COMMUNICATIONS SECURITY -- Part 3: Communication network and system security Profiles including TCP/IP", May 2007.

[IEEE802.1X] Institute of Electrical and Electronics Engineers, "IEEE Standard for Local and Metropolitan Area Networks - Port based Network Access Control", IEEE Standard 802.1X-2010, February 2010.

[IP-SEC] Gont, F., "Security Assessment of the Internet Protocol Version 4", Work in Progress, April 2011.

[IPv6-NODE-REQ] Jankiewicz, E., Loughney, J., and T. Narten, "IPv6 Node Requirements", Work in Progress, May 2011.

[MULTICAST-DNS] Cheshire, S. and M. Krochmal, "Multicast DNS", Work in Progress, February 2011.

[Model] SGIP, "Smart Grid Architecture Committee: Conceptual Model White Paper http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/SGIPConceptualModelDevelopmentSGAC/Smart_Grid_Conceptual_Model_20100420.doc".

[OAUTHv2] Hammer-Lahav, E., Recordon, D., and D. Hardt, "The OAuth 2.0 Authorization Protocol", Work in Progress, May 2011.

[RESTFUL] Fielding, "Architectural Styles and the Design of Network-based Software Architectures", 2000.

[RFC0768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[RFC0792] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, September 1981.

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, September 1981.

[RFC0826] Plummer, D., "Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware", STD 37, RFC 826, November 1982.

[RFC0894] Hornig, C., "Standard for the transmission of IP datagrams over Ethernet networks", STD 41, RFC 894, April 1984.

[RFC1006] Rose, M. and D. Cass, "ISO transport services on top of the TCP: Version 3", STD 35, RFC 1006, May 1987.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC1058] Hedrick, C., "Routing Information Protocol", RFC 1058, June 1988.

[RFC1112] Deering, S., "Host extensions for IP multicasting", STD 5, RFC 1112, August 1989.

[RFC1195] Callon, R., "Use of OSI IS-IS for routing in TCP/IP and dual environments", RFC 1195, December 1990.

[RFC1332] McGregor, G., "The PPP Internet Protocol Control Protocol (IPCP)", RFC 1332, May 1992.

[RFC1661] Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC1964] Linn, J., "The Kerberos Version 5 GSS-API Mechanism", RFC 1964, June 1996.

[RFC2080] Malkin, G. and R. Minnear, "RIPng for IPv6", RFC 2080, January 1997.

[RFC2126] Pouffary, Y. and A. Young, "ISO Transport Service on top of TCP (ITOT)", RFC 2126, March 1997.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC2136] Vixie, P., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.

[RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.

[RFC2357] Mankin, A., Romanov, A., Bradner, S., and V. Paxson, "IETF Criteria for Evaluating Reliable Multicast Transport and Application Protocols", RFC 2357, June 1998.

[RFC2453] Malkin, G., "RIP Version 2", STD 56, RFC 2453, November 1998.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, December 1998.

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, December 1998.

[RFC2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, December 1998.

[RFC2516] Mamakos, L., Lidl, K., Evarts, J., Carrel, D., Simone, D., and R. Wheeler, "A Method for Transmitting PPP Over Ethernet (PPPoE)", RFC 2516, February 1999.

[RFC2545] Marques, P. and F. Dupont, "Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing", RFC 2545, March 1999.

[RFC2560] Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 2560, June 1999.

[RFC2588] Finlayson, R., "IP Multicast and Firewalls", RFC 2588, May 1999.

[RFC2608] Guttman, E., Perkins, C., Veizades, J., and M. Day, "Service Location Protocol, Version 2", RFC 2608, June 1999.

[RFC2615] Malis, A. and W. Simpson, "PPP over SONET/SDH", RFC 2615, June 1999.

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[RFC2647] Newman, D., "Benchmarking Terminology for Firewall Performance", RFC 2647, August 1999.

[RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.

[RFC2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.

[RFC2743] Linn, J., "Generic Security Service Application Program Interface Version 2, Update 1", RFC 2743, January 2000.

[RFC2784] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 2784, March 2000.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC2979] Freed, N., "Behavior of and Requirements for Internet Firewalls", RFC 2979, October 2000.

[RFC2993] Hain, T., "Architectural Implications of NAT", RFC 2993, November 2000.

[RFC3007] Wellington, B., "Secure Domain Name System (DNS) Dynamic Update", RFC 3007, November 2000.

[RFC3022] Srisuresh, P. and K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, January 2001.

[RFC3027] Holdrege, M. and P. Srisuresh, "Protocol Complications with the IP Network Address Translator", RFC 3027, January 2001.

[RFC3031] Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, January 2001.

[RFC3032] Rosen, E., Tappan, D., Fedorkow, G., Rekhter, Y., Farinacci, D., Li, T., and A. Conta, "MPLS Label Stack Encoding", RFC 3032, January 2001.

[RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, September 2001.

[RFC3235] Senie, D., "Network Address Translator (NAT)-Friendly Application Design Guidelines", RFC 3235, January 2002.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC3265] Roach, A., "Session Initiation Protocol (SIP)-Specific Event Notification", RFC 3265, June 2002.

[RFC3275] Eastlake, D., Reagle, J., and D. Solo, "(Extensible Markup Language) XML-Signature Syntax and Processing", RFC 3275, March 2002.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.

[RFC3411] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, December 2002.

[RFC3412] Case, J., Harrington, D., Presuhn, R., and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3412, December 2002.

[RFC3413] Levi, D., Meyer, P., and B. Stewart, "Simple Network Management Protocol (SNMP) Applications", STD 62, RFC 3413, December 2002.

[RFC3414] Blumenthal, U. and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", STD 62, RFC 3414, December 2002.

[RFC3415] Wijnen, B., Presuhn, R., and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3415, December 2002.

[RFC3416] Presuhn, R., "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3416, December 2002.

[RFC3417] Presuhn, R., "Transport Mappings for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3417, December 2002.

[RFC3418] Presuhn, R., "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3418, December 2002.

[RFC3424] Daigle, L. and IAB, "IAB Considerations for UNilateral Self-Address Fixing (UNSAF) Across Network Address Translation", RFC 3424, November 2002.

[RFC3436] Jungmaier, A., Rescorla, E., and M. Tuexen, "Transport Layer Security over Stream Control Transmission Protocol", RFC 3436, December 2002.

[RFC3453] Luby, M., Vicisano, L., Gemmell, J., Rizzo, L., Handley, M., and J. Crowcroft, "The Use of Forward Error Correction (FEC) in Reliable Multicast", RFC 3453, December 2002.

[RFC3511] Hickman, B., Newman, D., Tadjudin, S., and T. Martin, "Benchmarking Methodology for Firewall Performance", RFC 3511, April 2003.

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, July 2003.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.

[RFC3561] Perkins, C., Belding-Royer, E., and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561, July 2003.

[RFC3569] Bhattacharyya, S., "An Overview of Source-Specific Multicast (SSM)", RFC 3569, July 2003.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC3590] Haberman, B., "Source Address Selection for the Multicast Listener Discovery (MLD) Protocol", RFC 3590, September 2003.

[RFC3626] Clausen, T. and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", RFC 3626, October 2003.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.

[RFC3715] Aboba, B. and W. Dixon, "IPsec-Network Address Translation (NAT) Compatibility Requirements", RFC 3715, March 2004.

[RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

[RFC3828] Larzon, L-A., Degermark, M., Pink, S., Jonsson, L-E., and G. Fairhurst, "The Lightweight User Datagram Protocol (UDP-Lite)", RFC 3828, July 2004.

[RFC3853] Peterson, J., "S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)", RFC 3853, July 2004.

[RFC3923] Saint-Andre, P., "End-to-End Signing and Object Encryption for the Extensible Messaging and Presence Protocol (XMPP)", RFC 3923, October 2004.

[RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[RFC3973] Adams, A., Nicholas, J., and W. Siadak, "Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)", RFC 3973, January 2005.

[RFC4017] Stanley, D., Walker, J., and B. Aboba, "Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs", RFC 4017, March 2005.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[RFC4108] Housley, R., "Using Cryptographic Message Syntax (CMS) to Protect Firmware Packages", RFC 4108, August 2005.

[RFC4120] Neuman, C., Yu, T., Hartman, S., and K. Raeburn, "The Kerberos Network Authentication Service (V5)", RFC 4120, July 2005.

[RFC4121] Zhu, L., Jaganathan, K., and S. Hartman, "The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2", RFC 4121, July 2005.

[RFC4210] Adams, C., Farrell, S., Kause, T., and T. Mononen, "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)", RFC 4210, September 2005.

[RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, October 2005.

[RFC4253] Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Transport Layer Protocol", RFC 4253, January 2006.

[RFC4271] Rekhter, Y., Li, T., and S. Hares, "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC4307] Schiller, J., "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)", RFC 4307, December 2005.

[RFC4320] Sparks, R., "Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction", RFC 4320, January 2006.

[RFC4340] Kohler, E., Handley, M., and S. Floyd, "Datagram Congestion Control Protocol (DCCP)", RFC 4340, March 2006.

[RFC4347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", RFC 4347, April 2006.

[RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, February 2006.

[RFC4410] Pullen, M., Zhao, F., and D. Cohen, "Selectively Reliable Multicast Protocol (SRMP)", RFC 4410, February 2006.

[RFC4422] Melnikov, A. and K. Zeilenga, "Simple Authentication and Security Layer (SASL)", RFC 4422, June 2006.

[RFC4443] Conta, A., Deering, S., and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.

[RFC4487] Le, F., Faccin, S., Patil, B., and H. Tschofenig, "Mobile IPv6 and Firewalls: Problem Statement", RFC 4487, May 2006.

[RFC4492] Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., and B. Moeller, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)", RFC 4492, May 2006.

[RFC4556] Zhu, L. and B. Tung, "Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)", RFC 4556, June 2006.

[RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, July 2006.

[RFC4594] Babiarz, J., Chan, K., and F. Baker, "Configuration Guidelines for DiffServ Service Classes", RFC 4594, August 2006.

[RFC4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, August 2006.

[RFC4604] Holbrook, H., Cain, B., and B. Haberman, "Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast", RFC 4604, August 2006.

[RFC4607] Holbrook, H. and B. Cain, "Source-Specific Multicast for IP", RFC 4607, August 2006.

[RFC4608] Meyer, D., Rockell, R., and G. Shepherd, "Source-Specific Protocol Independent Multicast in 232/8", BCP 120, RFC 4608, August 2006.

[RFC4614] Duke, M., Braden, R., Eddy, W., and E. Blanton, "A Roadmap for Transmission Control Protocol (TCP) Specification Documents", RFC 4614, September 2006.

[RFC4741] Enns, R., "NETCONF Configuration Protocol", RFC 4741, December 2006.

[RFC4742] Wasserman, M. and T. Goddard, "Using the NETCONF Configuration Protocol over Secure SHell (SSH)", RFC 4742, December 2006.

[RFC4743] Goddard, T., "Using NETCONF over the Simple Object Access Protocol (SOAP)", RFC 4743, December 2006.

[RFC4744] Lear, E. and K. Crozier, "Using the NETCONF Protocol over the Blocks Extensible Exchange Protocol (BEEP)", RFC 4744, December 2006.

[RFC4760] Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC 4760, January 2007.

[RFC4787] Audet, F. and C. Jennings, "Network Address Translation (NAT) Behavioral Requirements for Unicast UDP", BCP 127, RFC 4787, January 2007.

[RFC4835] Manral, V., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4835, April 2007.

[RFC4854] Saint-Andre, P., "A Uniform Resource Name (URN) Namespace for Extensions to the Extensible Messaging and Presence Protocol (XMPP)", RFC 4854, April 2007.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[RFC4916] Elwell, J., "Connected Identity in the Session Initiation Protocol (SIP)", RFC 4916, June 2007.

[RFC4919] Kushalnagar, N., Montenegro, G., and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", RFC 4919, August 2007.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, September 2007.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, September 2007.

[RFC4960] Stewart, R., "Stream Control Transmission Protocol", RFC 4960, September 2007.

[RFC4987] Eddy, W., "TCP SYN Flooding Attacks and Common Mitigations", RFC 4987, August 2007.

[RFC5023] Gregorio, J. and B. de hOra, "The Atom Publishing Protocol", RFC 5023, October 2007.

[RFC5061] Stewart, R., Xie, Q., Tuexen, M., Maruyama, S., and M. Kozuka, "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration", RFC 5061, September 2007.

[RFC5072] Varada, S., Ed., Haskins, D., and E. Allen, "IP Version 6 over PPP", RFC 5072, September 2007.

[RFC5122] Saint-Andre, P., "Internationalized Resource Identifiers (IRIs) and Uniform Resource Identifiers (URIs) for the Extensible Messaging and Presence Protocol (XMPP)", RFC 5122, February 2008.

[RFC5128] Srisuresh, P., Ford, B., and D. Kegel, "State of Peer-to-Peer (P2P) Communication across Network Address Translators (NATs)", RFC 5128, March 2008.

[RFC5135] Wing, D. and T. Eckert, "IP Multicast Requirements for a Network Address Translator (NAT) and a Network Address Port Translator (NAPT)", BCP 135, RFC 5135, February 2008.

[RFC5191] Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H., and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", RFC 5191, May 2008.

[RFC5207] Stiemerling, M., Quittek, J., and L. Eggert, "NAT and Firewall Traversal Issues of Host Identity Protocol (HIP) Communication", RFC 5207, April 2008.

[RFC5216] Simon, D., Aboba, B., and R. Hurst, "The EAP-TLS Authentication Protocol", RFC 5216, March 2008.

[RFC5238] Phelan, T., "Datagram Transport Layer Security (DTLS) over the Datagram Congestion Control Protocol (DCCP)", RFC 5238, May 2008.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5272] Schaad, J. and M. Myers, "Certificate Management over CMS (CMC)", RFC 5272, June 2008.

[RFC5277] Chisholm, S. and H. Trevino, "NETCONF Event Notifications", RFC 5277, July 2008.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[RFC5289] Rescorla, E., "TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)", RFC 5289, August 2008.

[RFC5308] Hopps, C., "Routing IPv6 with IS-IS", RFC 5308, October 2008.

[RFC5340] Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF for IPv6", RFC 5340, July 2008.

[RFC5393] Sparks, R., Lawrence, S., Hawrylyshen, A., and B. Campen, "Addressing an Amplification Vulnerability in Session Initiation Protocol (SIP) Forking Proxies", RFC 5393, December 2008.

[RFC5405] Eggert, L. and G. Fairhurst, "Unicast UDP Usage Guidelines for Application Designers", BCP 145, RFC 5405, November 2008.

[RFC5430] Salter, M., Rescorla, E., and R. Housley, "Suite B Profile for Transport Layer Security (TLS)", RFC 5430, March 2009.

[RFC5433] Clancy, T. and H. Tschofenig, "Extensible Authentication Protocol - Generalized Pre-Shared Key (EAP-GPSK) Method", RFC 5433, February 2009.

[RFC5437] Saint-Andre, P. and A. Melnikov, "Sieve Notification Mechanism: Extensible Messaging and Presence Protocol (XMPP)", RFC 5437, January 2009.

[RFC5539] Badra, M., "NETCONF over Transport Layer Security (TLS)", RFC 5539, May 2009.

[RFC5545] Desruisseaux, B., "Internet Calendaring and Scheduling Core Object Specification (iCalendar)", RFC 5545, September 2009.

[RFC5546] Daboo, C., "iCalendar Transport-Independent Interoperability Protocol (iTIP)", RFC 5546, December 2009.

[RFC5548] Dohler, M., Watteyne, T., Winter, T., and D. Barthel, "Routing Requirements for Urban Low-Power and Lossy Networks", RFC 5548, May 2009.

[RFC5569] Despres, R., "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)", RFC 5569, January 2010.

[RFC5621] Camarillo, G., "Message Body Handling in the Session Initiation Protocol (SIP)", RFC 5621, September 2009.

[RFC5626] Jennings, C., Mahy, R., and F. Audet, "Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)", RFC 5626, October 2009.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, September 2009.

[RFC5673] Pister, K., Thubert, P., Dwars, S., and T. Phinney, "Industrial Routing Requirements in Low-Power and Lossy Networks", RFC 5673, October 2009.

[RFC5681] Allman, M., Paxson, V., and E. Blanton, "TCP Congestion Control", RFC 5681, September 2009.

[RFC5717] Lengyel, B. and M. Bjorklund, "Partial Lock Remote Procedure Call (RPC) for NETCONF", RFC 5717, December 2009.

[RFC5740] Adamson, B., Bormann, C., Handley, M., and J. Macker, "NACK-Oriented Reliable Multicast (NORM) Transport Protocol", RFC 5740, November 2009.

[RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, January 2010.

[RFC5785] Nottingham, M. and E. Hammer-Lahav, "Defining Well-Known Uniform Resource Identifiers (URIs)", RFC 5785, April 2010.

[RFC5826] Brandt, A., Buron, J., and G. Porcu, "Home Automation Routing Requirements in Low-Power and Lossy Networks", RFC 5826, April 2010.

[RFC5838] Lindem, A., Mirtorabi, S., Roy, A., Barnes, M., and R. Aggarwal, "Support of Address Families in OSPFv3", RFC 5838, April 2010.

[RFC5849] Hammer-Lahav, E., "The OAuth 1.0 Protocol", RFC 5849, April 2010.

[RFC5867] Martocci, J., De Mil, P., Riou, N., and W. Vermeylen, "Building Automation Routing Requirements in Low-Power and Lossy Networks", RFC 5867, June 2010.

[RFC5905] Mills, D., Martin, J., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, June 2010.

[RFC5932] Kato, A., Kanda, M., and S. Kanno, "Camellia Cipher Suites for TLS", RFC 5932, June 2010.

[RFC5958] Turner, S., "Asymmetric Key Packages", RFC 5958, August 2010.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

[RFC5998] Eronen, P., Tschofenig, H., and Y. Sheffer, "An Extension for EAP-Only Authentication in IKEv2", RFC 5998, September 2010.

[RFC6031] Turner, S. and R. Housley, "Cryptographic Message Syntax (CMS) Symmetric Key Package Content Type", RFC 6031, December 2010.

[RFC6047] Melnikov, A., "iCalendar Message-Based Interoperability Protocol (iMIP)", RFC 6047, December 2010.

[RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052, October 2010.

[RFC6090] McGrew, D., Igoe, K., and M. Salter, "Fundamental Elliptic Curve Cryptography Algorithms", RFC 6090, February 2011.

[RFC6120] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, March 2011.

[RFC6121] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence", RFC 6121, March 2011.

[RFC6144] Baker, F., Li, X., Bao, C., and K. Yin, "Framework for IPv4/IPv6 Translation", RFC RFC6144, April 2011.

[RFC6145] Li, X., Bao, C., and F. Baker, "IP/ICMP Translation Algorithm", RFC 6145, April 2011.

[RFC6146] Bagnulo, M., Matthews, P., and I. Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, April 2011.

[RFC6147] Bagnulo, M., Sullivan, A., Matthews, P., and I. Beijnum, "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", RFC 6147, April 2011.

[RFC6180] Arkko, J. and F. Baker, "Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment", RFC 6180, May 2011.

[RPL] Winter, T., Thubert, P., Brandt, A., Clausen, T., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., and J. Vasseur, "RPL: IPv6 Routing Protocol for Low power and Lossy Networks", Work in Progress, March 2011.

[SP-MULPIv3.0] CableLabs, "DOCSIS 3.0 MAC and Upper Layer Protocols Interface Specification, CM-SP-MULPIv3.0-I10-090529", May 2009.

[SmartGrid] Wikipedia, "Wikipedia Article: Smart Grid", February 2011, <http://en.wikipedia.org/w/index.php?title=Smart_grid&oldid=415838933>.

[TCP-SEC] Gont, F., "Security Assessment of the Transmission Control Protocol (TCP)", Work in Progress, January 2011.

[r1822] Bolt Beranek and Newman Inc., "Interface Message Processor -- Specifications for the interconnection of a host and a IMP, Report No. 1822", January 1976.

[xCAL] Daboo, C., Douglass, M., and S. Lees, "xCal: The XML format for iCalendar", Work in Progress, April 2011.

Appendix A. Example: Advanced Metering Infrastructure

This appendix provides a worked example of the use of the Internet Protocol Suite in a network such as the Smart Grid's Advanced Metering Infrastructure (AMI). There are several possible models.

Figure 6 shows the structure of the AMI as it reaches out towards a set of residences. In this structure, we have the home itself and its Home Area Network (HAN), the Neighborhood Area Network (NAN) that the utility uses to access the meter at the home, and the utility access network that connects a set of NANs to the utility itself. For the purposes of this discussion, assume that the NAN contains a distributed application in a set collectors, which is of course only one way the application could be implemented.

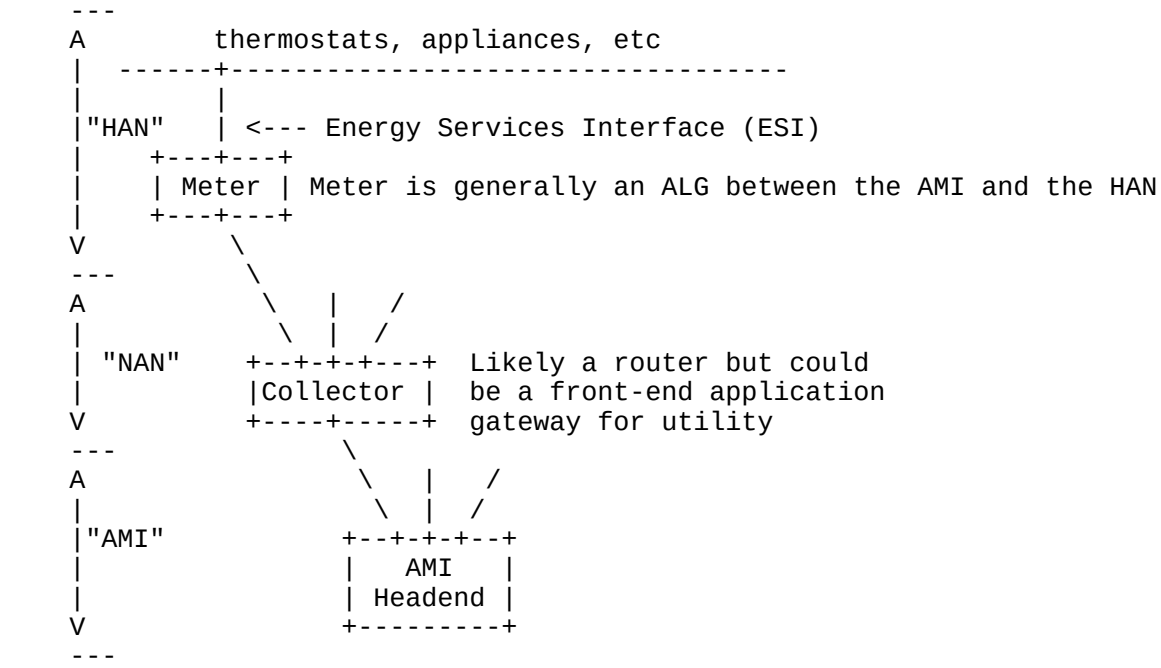

Figure 6: The HAN, NAN, and Utility in the Advanced Metering Infrastructure

There are several questions that have to be answered in describing this picture, which given possible answers yield different possible models. They include at least:

- How does Demand Response work? Either:

    * The utility presents pricing signals to the home,

    * The utility presents pricing signals to individual devices (e.g., a Pluggable Electric Vehicle),

    * The utility adjusts settings on individual appliances within the home.

  o How does the utility access meters at the home?

    * The AMI Headend manages the interfaces with the meters, collecting metering data and passing it on to the appropriate applications over the Enterprise Bus, or

    * Distributed application support ("collectors") might access and summarize the information; this device might be managed by the utility or by a service between the utility and its customers.

In implementation, these models are idealized; reality may include some aspects of each model in specified cases.

The examples include:

1. Appendix A.2 presumes that the HAN, the NAN, and the utility's network are separate administrative domains and speak application to application across those domains.

2. Appendix A.3 repeats the first example, but presuming that the utility directly accesses appliances within the HAN from the collector.

3. Appendix A.4 repeats the first example, but presuming that the collector directly forwards traffic as a router in addition to distributed application chores. Note that this case implies numerous privacy and security concerns and as such is considered a less likely deployment model.

A.1. How to Structure a Network

A key consideration in the Internet has been the development of new link layer technologies over time. The ARPANET originally used a BBN proprietary link layer called BBN 1822 [r1822]. In the late 1970's, the ARPANET switched to X.25 as an interface to the 1822 network. With the deployment of the IEEE 802 series technologies in the early 1980's, IP was deployed on Ethernet (IEEE 802.3), Token Ring (IEEE 802.5) and WiFi (IEEE 802.11), as well as Arcnet, serial lines of various kinds, Frame Relay, and ATM. A key issue in this evolution was that the applications developed to run on the Internet use APIs

related to the IPS, and as a result require little or no change to continue operating in a new link layer architecture or a mixture of them.

The Smart Grid is likely to see a similar evolution over time. Consider the Home Area Network (HAN) as a readily understandable small network. At this juncture, technologies proposed for residential networks include IEEE P1901, various versions of IEEE 802.15.4, and IEEE 802.11. It is reasonable to expect other technologies to be developed in the future. As the Zigbee Alliance has learned (and as a resulted incorporated the IPS in Smart Energy Profile 2.0), there is significant value in providing a virtual address that is mapped to interfaces or nodes attached to each of those technologies.

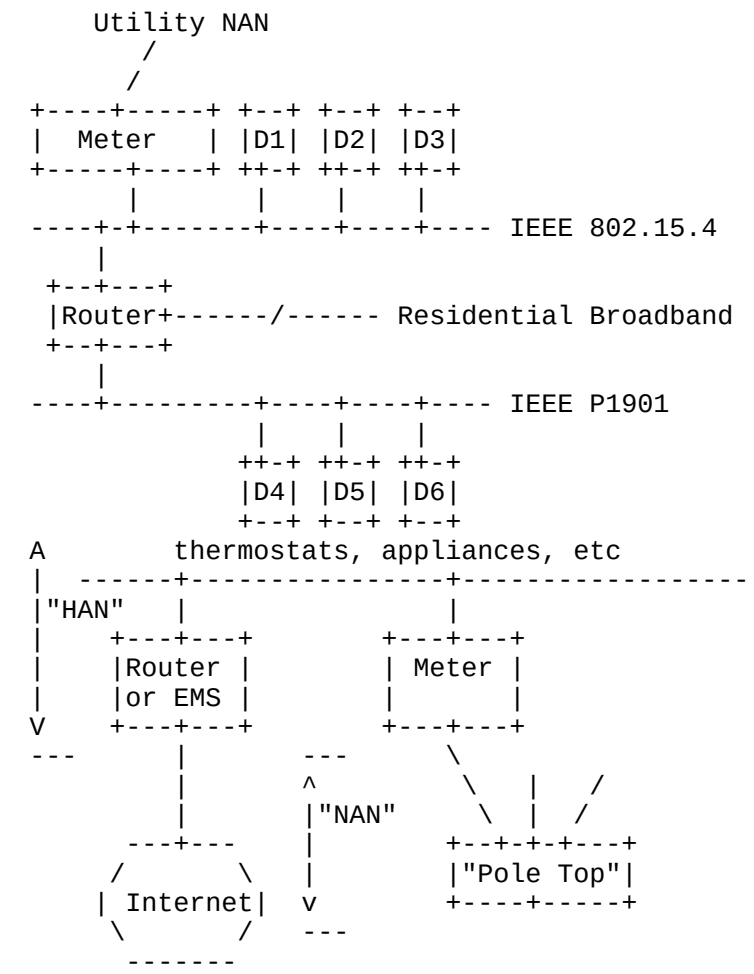

Figure 7: Two Views of a Home Area Network

There are two possible communication models within the HAN, both of which are likely to be useful. Devices may communicate directly with each other, or they may be managed by some central controller. An example of direct communications might be a light switch that directly commands a lamp to turn on or off. An example of indirect communications might be a control application in a Customer or Building that accepts telemetry from a thermostat, applies some form of policy, and controls the heating and air conditioning systems. In addition, there are high-end appliances in the market today that use residential broadband to communicate with their manufacturers, and obviously the meter needs to communicate with the utility.

Figure 7 shows two simple networks, one of which uses IEEE 802.15.4 and IEEE 1901 domains, and one of which uses an arbitrary LAN within the home, which could be IEEE 802.3/Ethernet, IEEE 802.15.4, IEEE 1901, IEEE 802.11, or anything else that made sense in context. Both show the connectivity between them as a router separate from the energy management system (EMS). This is for clarity; the two could of course be incorporated into a single system, and one could imagine appliances that want to communicate with their manufacturers supporting both a HAN interface and a WiFi interface rather than depending on the router. These are all manufacturer design decisions.

A.1.1. HAN Routing

The HAN can be seen as communicating with two kinds of non-HAN networks. One is the home LAN, which may in turn be attached to the Internet, and will generally either derive its prefix from the upstream ISP or use a self-generated Unique Local Addressing (ULA). Another is the utility's NAN, which through an ESI provides utility connectivity to the HAN; in this case the HAN will be addressed by a self-generated ULA (note, however, that in some cases ESI may also provide a prefix via DHCP [RFC3315]). In addition, the HAN will have link-local addresses that can be used between neighboring nodes. In general, an HAN will be comprised of both 802.15.4, 802.11, and possibly other networks.

The ESI is a node on the user's residential network, and will not typically provide stateful packet forwarding or firewall services between the HAN and the utility network(s). In general, the ESI is a node on the home network; in some cases, the meter may act as the ESI. However, the ESI must be capable of understanding that most home networks are not 802.15.4 enabled (rather, they are typically 802.11 networks), and that it must be capable of setting up ad hoc networks between various sensors in the home (e.g., between the meter and say, a thermostat) in the event there aren't other networks available.

A.1.2. HAN Security

In any network, we have a variety of threats and a variety of possible mitigations. These include, at minimum:

Link Layer: Why is your machine able to talk in my network? The WiFi SSIDs often use some form of authenticated access control, which may be a simple encrypted password mechanism or may use a combination of encryption and IEEE 802.1X+EAP-TLS Authentication/

Authorization to ensure that only authorized communicants can use it. If a LAN has a router attached, the router may also implement a firewall to filter remote accesses.

Network Layer: Given that your machine is authorized access to my network, why is your machine talking with my machine? IPsec is a way of ensuring that computers that can use a network are allowed to talk with each other, may also enforce confidentiality, and may provide VPN services to make a device or network appear to be part of a remote network.

Application: Given that your machine is authorized access to my network and my machine, why is your application talking with my application? The fact that your machine and mine are allowed to talk for some applications doesn't mean they are allowed to for all applications. (D)TLS, https, and other such mechanisms enable an application to impose application-to-application controls similar to the network layer controls provided by IPsec.

Remote Application: How do I know that the data I received is the data you sent? Especially in applications like electronic mail, where data passes through a number of intermediaries that one may or may not really want munging it (how many times have you seen a URL broken by a mail server?), we have tools (DKIM, S/MIME, and W3C XML Signatures to name a few) to provide non-repudiability and integrity verification. This may also have legal ramifications: if a record of a meter reading is to be used in billing, and the bill is disputed in court, one could imagine the court wanting proof that the record in fact came from that meter at that time and contained that data.

Application-specific security: In addition, applications often provide security services of their own. The fact that I can access a file system, for example, doesn't mean that I am authorized to access everything in it; the file system may well prevent my access to some of its contents. Routing protocols like BGP are obsessed with the question "what statements that my peer made am I willing to believe", and monitoring protocols like SNMP may not be willing to answer every question they are asked, depending on access configuration.

Devices in the HAN want controlled access to the LAN in question for obvious reasons. In addition, there should be some form of mutual authentication between devices -- the lamp controller will want to know that the light switch telling it to change state is the right light switch, for example. The EMS may well want strong authentication of accesses -- the parents may not want the children

changing the settings, and while the utility and the customer are routinely granted access, other parties (especially parties with criminal intent) need to be excluded.

A.2. Model 1: AMI with Separated Domains

With the background given in Appendix A.1, we can now discuss the use of IP (IPv4 or IPv6) in the AMI.

In this first model, consider the three domains in Figure 6 to literally be separate administrative domains, potentially operated by different entities. For example, the NAN could be a WiMAX network operated by a traditional telecom operator, the utility's network (including the collector) is its own, and the residential network is operated by the resident. In this model, while communications between the collector and the Meter are normal, the utility has no other access to appliances in the home, and the collector doesn't directly forward messages from the NAN upstream.

In this case, as shown in Figure 7, it would make the most sense to design the collector, the Meter, and the EMS as hosts on the NAN -- design them as systems whose applications can originate and terminate exchanges or sessions in the NAN, but not forward traffic from or to other devices.

In such a configuration, Demand Response has to be performed by having the EMS accept messages such as price signals from the "pole top", apply some form of policy, and then orchestrate actions within the home. Another possibility is to have the EMS communicate with the ESI located in the meter. If the thermostat has high demand and low demand (day/night or morning/day/evening/night) settings, Demand Response might result in it moving to a lower demand setting, and the EMS might also turn off specified circuits in the home to diminish lighting.

In this scenario, Quality of Service (QoS) issues reportedly arise when high precedence messages must be sent through the collector to the home; if the collector is occupied polling the meters or doing some other task, the application may not yield control of the processor to the application that services the message. Clearly, this is either an application or an Operating System problem; applications need to be designed in a manner that doesn't block high precedence messages. The collector also needs to use appropriate NAN services, if they exist, to provide the NAN QoS it needs. For example, if WiMax is in use, it might use a routine-level service for normal exchanges but a higher precedence service for these messages.

A.3. Model 2: AMI with Neighborhood Access to the Home

In this second model, let's imagine that the utility directly accesses appliances within the HAN. Rather than expect an EMS to respond to price signals in Demand Response, it directly commands devices like air conditioners to change state, or throws relays on circuits to or within the home.

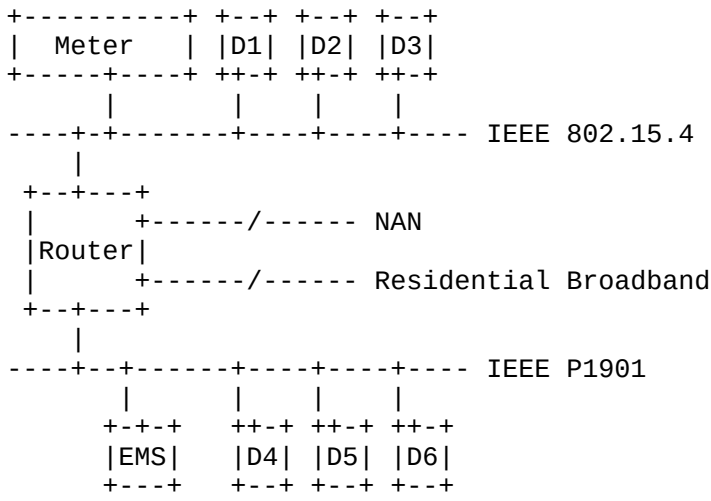

Figure 8: Home Area Network

In this case, as shown in Figure 8, the Meter and EMS act as hosts on the HAN, and there is a router between the HAN and the NAN.

As one might imagine, there are serious security considerations in this model. Traffic between the NAN and the residential broadband network should be filtered, and the issues raised in Appendix A.1.2 take on a new level of meaning. One of the biggest threats may be a legal or at least a public relations issue; if the utility intentionally disables a circuit in a manner or at a time that threatens life (the resident's kidney dialysis machine is on it, or a respirator, for example), the matter might make the papers. Unauthorized access could be part of juvenile pranks or other things as well. So one really wants the appliances to only obey commands under strict authentication/authorization controls.

In addition to the QoS issues raised in Appendix A.2, there is the possibility of queuing issues in the router. In such a case, the IP datagrams should probably use the Low-Latency Data Service Class

described in [RFC4594], and let other traffic use the Standard Service Class or other service classes.

A.4. Model 3: Collector Is an IP Router

In this third model, the relationship between the NAN and the HAN is either as in Appendix A.2 or Appendix A.3; what is different is that the collector may be an IP router. In addition to whatever autonomous activities it is doing, it forwards traffic as an IP router in some cases.

Analogous to Appendix A.3, there are serious security considerations in this model. Traffic being forwarded should be filtered, and the issues raised in Appendix A.1.2 take on a new level of meaning -- but this time at the utility mainframe. Unauthorized access is likely similar to other financially-motivated attacks that happen in the Internet, but presumably would be coming from devices in the HAN that have been co-opted in some way. One really wants the appliances to only obey commands under strict authentication/authorization controls.

In addition to the QoS issues raised in Appendix A.2, there is the possibility of queuing issues in the collector. In such a case, the IP datagrams should probably use the Low-Latency Data Service Class described in [RFC4594], and let other traffic use the Standard Service Class or other service classes.

Authors' Addresses

Fred Baker
Cisco Systems
Santa Barbara, California 93117
USA

EMail: fred@cisco.com

David Meyer
Cisco Systems
Eugene, Oregon 97403
USA

EMail: dmm@cisco.com