           ANSI C12.22, IEEE 1703, and MC12.22 Transport Over IP

Abstract

   This RFC provides a framework for transporting ANSI C12.22/IEEE
   1703/MC12.22 Advanced Metering Infrastructure (AMI) Application Layer
   Messages on an IP network.

   This document is not an official submission on behalf of the ANSI
   C12.19 and C12.22 working groups. It was created by participants in
   those groups, building on knowledge of several proprietary C12.22-
   over-IP implementations. The content of this document is an
   expression of a consensus aggregation of those implementations.

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/rfc6142.

the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.

Table of Contents

1. Introduction

   The ANSI C12.22 standard [1] provides a set of application layer
   messaging services that are applicable for the enterprise and End
   Device components of an Advanced Metering Infrastructure (AMI) for
   the Smart Grid. The messaging services are tailored for, but not
   limited to, the exchange of the Data Table Elements defined and
   co-published in ANSI C12.19 [2], IEEE P1377 [3], and MC12.19 [23].
   These standards were developed jointly by ANSI (ANSI C12.22 and ANSI
   C12.19), IEEE (IEEE 1377 and IEEE 1703), and Measurement Canada
   (MC12.19 and MC12.22).

   ANSI C12.22, which is an application level messaging protocol, may be
   transported over any underlying transport network. This RFC defines
   the requirements governing the transmission of ANSI C12.22 Messages
   via the TCP and UDP transports in IP networks (whereby the OSI
   Session, Presentation, and Application Layers of ANSI C12.22 are
   collapsed into a single Application Layer).

   Specifically, this RFC applies to the operational details of
   Section 5, "C12.22 Node to C12.22 Network Segment Details", of ANSI
   C12.22, and covers the mapping, encoding, and interpreting of ANSI
   C12.19 Device Network Table Elements and Native Addresses for use on
   IP networks.

2. Terminology

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
   document are to be interpreted as described in RFC 2119 [4].

   Throughout this document, we use terms like "ANSI C12.22" or "ANSI
   C12.19", as in "C12.22 Relay" or "ANSI C12.19 Device". These terms
   are interchangeable with the terms "IEEE 1703 Relay" and "IEEE 1377
   Device", respectively. However, the recent versions of the Utility
   End Device communication standards were developed under the auspices
   of ANSI C12 SC17 WG1 and ANSI C12 SC17 WG2. For that reason, the
   terminology used in this document expands on the ANSI C12.22-2008 [1]
   and ANSI C12.19-2008 [2] definitions as revised by IEEE 1703-2010 [5]
   and IEEE 1377-2010 [3].

3. Definitions

   This specification uses a number of terms to refer to the roles
   played by participants (actors) in, and objects of, the ANSI C12.22
   [1], IEEE 1703 [5], and MC12.22 [24] protocol. Any terms prefixed by
   "C12.22" or "C12.19" that are not defined in this document can be
   resolved in [1], [5], [24] or in [2], [3], [23].

ACSE

   Association Control Service Element. In the context of this
   specification and of [1], ACSEs are encoded per ISO/IEC 10035-1
   [6] using the ASN.1 Basic Encoding Rules (BER) [7].

Active-OPEN UDP

   Active-OPEN UDP is a state used by a local C12.22 IP Node to
   expect and receive incoming C12.22 Messages that it solicited from
   a foreign C12.22 IP Node using UDP. The local C12.22 IP Node MAY
   exit the Active-OPEN UDP state when it has received all of the
   expected C12.22 Messages or a C12.22 Message timeout has occurred.
   The local C12.22 IP Node receives all C12.22 Response Messages
   solicited from the foreign C12.22 IP Node that arrive at the local
   port number that matches the source port number used to solicit
   the C12.22 Messages from the foreign C12.22 IP Node.

Active-OPEN TCP

   Active-OPEN TCP is a state used by a local C12.22 IP Node to
   establish a TCP connection with a fully specified foreign C12.22
   IP Node using TCP and the foreign C12.22 IP Node's registered
   Native IP Address. The Active-OPEN TCP state is identical to a
   local "Active-OPEN" as defined in [9].

APDU

   Application Protocol Data Unit. In the context of the ANSI C12.22
   Application, it is an ACSE C12.22 Message.

ACSE APDU

   ACSE Application Protocol Data Unit; same as APDU.

ApTitle

   An ANSI C12.22 Application-process Title. An ApTitle is a name
   for a system-independent application activity that exposes
   application services to the application agent, e.g., a set of
   application service elements that together perform all or part of
   the communication aspects of an application process. An ApTitle
   is encoded as a unique registered (as per [1]) object identifier.

C12.22 IP Node

   A C12.22 Node that is located on a C12.22 IP Network Segment and
   communicates using the Internet Protocol.

C12.22 IP Network Segment

   A collection of all C12.22 IP Nodes that implement the IP-based
   protocols, as defined in this specification, and can communicate
   with each other using IP routers, switches, and bridges and
   without the use of a C12.22 Relay.

C12.22 IP Relay

   A C12.22 IP Node that performs the functions of a C12.22 Relay.
   A C12.22 IP Relay acts as a bridge between a C12.22 IP Network
   Segment and an adjacent, C12.22 Network Segment.

C12.22 Message

   An ACSE APDU that is fully assembled, or a segment of a C12.22
   Request Message, or a segment of a C12.22 Response Message. The
   C12.22 Message described in this specification MUST be encoded
   using [7].

C12.22 Request Message

   A fully assembled C12.22 APDU that contains an ACSE user-
   information element, which includes one or more EPSEM Service
   Requests.

C12.22 Response Message

   A fully assembled C12.22 APDU that contains an ACSE user-
   information element, which includes one or more EPSEM service
   responses.

Connection

   A logical and physical binding between two or more users of a
   service [1].

EPSEM

   Extended Protocol Specification for Electronic Metering. EPSEM
   defines structures and services used to encode multiple requests
   and responses for use by devices such as gas, water, electricity,
   and related electronic modules or appliances.

Initiating C12.22 IP Node

   A role of a C12.22 IP Node in which it initiates the transmission
   of a C12.22 Request Message.

   Native Address

      The term "Native Address" refers to the transport address that may
      be used to reach a C12.22 Node on its C12.22 Network Segment [1].
      In this specification, the Native Address refers to the Native IP
      Address.

   Passive-OPEN UDP

      Passive-OPEN UDP is a state used by a local C12.22 IP Node to
      expect and receive incoming C12.22 Messages from any foreign
      C12.22 IP Node using UDP. When the Passive-OPEN UDP state is
      active, the local C12.22 IP Node accepts all C12.22 Messages that
      arrive at the local port number that was registered by the local
      C12.22 IP Node.

   Passive-OPEN TCP

      Passive-OPEN TCP is a state used by a local C12.22 IP Node that
      wants to establish a TCP connection with an unspecified foreign
      C12.22 IP Node using TCP. In this case, any foreign C12.22 IP
      Node MAY connect to the local C12.22 IP Node as long as the local
      port matches the port used by the foreign C12.22 IP Node. The
      Passive-OPEN TCP state is identical to "local passive OPEN"
      defined in [9].

   Responding C12.22 IP Node

      A role of a C12.22 IP Node in which it responds to the reception
      of a C12.22 Request Message.

   Target C12.22 IP Node

      The C12.22 IP Node that is the destination for a C12.22 Message.

4. The C12.22 IP Network Segment

   This section defines the characteristics of the C12.22 IP Network
   Segment.

4.1. Composition of a C12.22 IP Network Segment

   A C12.22 Network Segment is a collection of C12.22 Nodes that can
   communicate with each other directly -- without having to forward
   C12.22 Messages through a C12.22 Relay.

   A C12.22 IP Network Segment comprises C12.22 IP Nodes and the network
   infrastructure that enables any one node to reach all other nodes on

the same segment. All C12.22 IP Nodes on the C12.22 IP Network
Segment employ the same IP address encoding scheme (per Figures 1
and 2) and the same network and transport protocols in accordance
with this specification.

There is no restriction on the size of a C12.22 IP Network Segment.
It MAY be as small as a single LAN or subnet, or it MAY include
numerous, heterogeneous LANs and WANs connected by routers, bridges,
and switches. The C12.22 IP Network Segment MAY be completely
private, or include communication across the global Internet.

4.2. Native IP Address

   The term "Native IP Address" denotes a Native Address that MAY be
   used to reach a C12.22 Node on its C12.22 IP Network Segment. The
   Native IP Address includes the binary IP address, and an OPTIONAL
   port number that MAY be followed by an OPTIONAL protocol identifier.
   The Native IP Address SHALL be encoded as described below in
   Section 4.3, "Encoding of Native IP Addresses".

   The IP address of the C12.22 IP Node MUST be configured before the
   C12.22 IP Node attempts to send or receive any C12.22 Message on its
   C12.22 IP Network Segment. If the port number is not explicitly
   configured by the controlling application, it SHALL be set to the
   default port number, 1153 (see Section 4.4, "Standardized Port
   Numbers", below).

   It is beyond the scope of this specification to define the method of
   configuration, the configuration parameters, or any administrative
   controls that the system administrator may wish to implement to
   assign an IP address.

4.3. Encoding of Native IP Addresses

   ANSI C12.22 defines binary fields for encoding a C12.22 Native
   Address for transport within C12.22 Messages and for storage in
   C12.19 Device Tables. In this RFC, the fields SHALL contain an IPv4
   or an IPv6 binary native IP address that is followed by an OPTIONAL
   two-byte TCP or UDP port number. The TCP or UDP port number, when
   present, MAY be followed by an OPTIONAL one-byte transport protocol
   identifier ("Protocol" for IPv4 or "Next Header" for IPv6). The
   transport protocol identifier SHALL be set to 17 (0x11) for UDP
   transport, or to 6 (0x06) for TCP transport, or not set (absent) for
   both UDP and TCP transports. The transport protocol values SHALL be
   consistent with the C12.22 Node's registered attributes (see
   Connectionless (CL) and Connection-Oriented (CO) flags in
   Section 5.1, "C12.22 Connection Types and TCP/UDP Transport Modes",
   below).

ANSI C12.22 allows the Native Address fields to be conveyed in select
ANSI C12.22 EPSEM service elements (e.g., ANSI C12.22 Registration
Service <native-address>, ANSI C12.22 Resolve Service response
<local-address>, and ANSI C12.19 INTERFACE_CTRL_TBL Element
NATIVE_ADDRESS). The length of the C12.22 Native Address is
qualified by an ANSI C12.22 address length field (e.g., ANSI C12.22
Registration Service <address-length>, ANSI C12.22 Resolve Service
response <local-address-length>, and ANSI C12.19 ACT_NETWORK_TBL
Element NATIVE_ADDRESS_LEN).

The ANSI C12.22 Registration Service permits only one Native Address
to be recorded with each registered ApTitle. For this reason, a
C12.22 IP Node that wishes to register different port numbers for UDP
and TCP MUST register twice using different ApTitles.

The binary Native IP Address fields SHALL be encoded in network byte
order, as shown in Figure 1.

```
                            IP Address (ADDR), Port (P), Transport (T)
                  Address
                  Length                       Octet
                               0                       1
                               0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8
                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       IPv4         4          | ADDR4 |
                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+


                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       IPv4+Port    6          | ADDR4 | P |
                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+


                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       IPv4+Port    7          | ADDR4 | P |T|
       +Transport              +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+


                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       IPv6        16          |            ADDR6            |
                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+


                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       IPv6+Port   18          |            ADDR6            | P |
                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+


                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       IPv6+Port   19          |            ADDR6            | P |T|
       +Transport              +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: Encoding of the Native IP Addresses for ANSI C12.22

When an ANSI C12.22 Native Address is encoded in the ANSI C12.19
Tables' BINARY data Elements, the size of the Native Address Element
is defined by ACT_NETWORK_TBL.NATIVE_ADDRESS_LEN (see Table 121 of
[1], and [2]). This is the actual number of octets that are placed
inside the C12.19 BINARY Element. This value is common to all of the
C12.22 Node's interfaces, including those that are not IP based (thus
not conforming to this specification). For this reason, the
ACT_NETWORK_TBL.NATIVE_ADDRESS_LEN MAY be greater than, and SHALL NOT
be smaller than, the actual length needed to encode a Native IP
Address per Figure 1. When this is the case, the C12.22 Native IP
Address SHALL be padded with zero (0) to fill the Table's BINARY data
Element.

In instances where the Native IP Address length does not exactly
match any of the Address Lengths listed in Figure 1, the actual
Address Length SHALL be determined by stripping all trailing binary
zeros (0x00) and then adjusting the Address Length upwards to the
next largest value shown in Figure 1.

4.4. Standardized Port Numbers

IANA (Internet Assigned Numbers Authority) has assigned port 1153 for
UDP [8] and TCP [9] C12.22 IP Messages.

By default, C12.22 IP Nodes SHALL send all C12.22 Application
association initiation message requests with 1153 set as the
destination port number.

To ensure interoperability among C12.22 IP Nodes, all C12.22 IP
Relays and Master Relays SHALL monitor and accept UDP and TCP
messages destined to port 1153.

Any IP firewalls or Access Control Lists (ACLs) shielding C12.22
Nodes and the IP network MUST be configured to forward UDP and TCP
traffic destined to port 1153 and other ports that are assigned and
registered by the network administrator, in order to maintain the
continuity of the C12.22 IP Network Segment.

4.5. Use of UDP Source Port 0

Although RFC 768 [8] allows for a source port number of zero (0),
C12.22 IP Nodes SHALL NOT send datagrams on UDP with the source port
set to zero. A C12.22 IP Node SHALL ignore and SHALL NOT respond to
any C12.22 Message that it receives from source port 0.

Further details of the C12.22 IP Node's use of UDP, and of TCP, are
given in Section 5, "IP Message Transport", below.

4.6. IP Multicast

   In addition to unicast, the ANSI C12.22 protocol requires the support
   of a multicast message delivery service from the network. In cases
   where C12.22 IP Nodes MUST perform Native IP Address discovery (e.g.,
   the discovery of the Native IP Address of C12.22 IP Relays that
   provide a route out of the C12.22 IP Network Segment, or the
   discovery of the Native IP Address of a C12.22 IP Master Relay on the
   C12.22 IP Network), the C12.22 IP Nodes use IP multicast to send a
   C12.22 Message that contains an EPSEM Resolve Service Request on the
   IP LAN.

   IP multicast is also desirable, for example, when a C12.22 Host needs
   to read a multitude of C12.22 Nodes (e.g., meters) that are
   configured with a common C12.22 multicast group ApTitle. Using IP
   multicast, the C12.22 Host MAY send a C12.22 Message containing an
   EPSEM Read Service Request that reaches all C12.22 Nodes on the
   C12.22 IP Network Segment.

   For these reasons, all C12.22 IP Relays and Master Relays SHALL
   support IP multicast, and it is RECOMMENDED that all C12.22 Nodes
   support IP multicast. Any IPv4 C12.22 IP Node that supports IP
   multicast SHALL use the Internet Group Management Protocol version 1
   (IGMPv1) [10] as a minimum, to report (i.e., request) membership in
   the C12.22 multicast group to its local router(s). It is RECOMMENDED
   that C12.22 IP Nodes implement IGMPv3 [11].

   Any IPv6 C12.22 IP Node that supports IP multicast SHALL use
   Multicast Listener Discovery version 2 (MLDv2) (RFC 3810 [12]),
   possibly within ICMPv6 (RFC 4443 [13]), to report membership.

   Routers that interconnect C12.22 IP Nodes on the C12.22 IP Network
   Segment MUST support Protocol Independent Multicast - Sparse Mode
   (PIM-SM) (RFC 4601 [14]) along with IGMPv1 (RFC 1112 [10]) as a
   minimum for IPv4, or MLDv2 for IPv6 (RFC 3810 [12]). It is
   RECOMMENDED that they implement IGMPv3 [11]. It is beyond the scope
   of this specification to define the mechanism for selecting an
   initial Rendezvous Point (RP) for the C12.22 multicast group, the use
   of shared versus source trees, or the mechanism for inter-domain
   multicast routing.

   IANA has registered the "All C1222 Nodes" multicast group, and has
   assigned the IPv4 multicast address of 224.0.2.4 and the IPv6
   multicast address of FF0X::204, where X represents the Scope field as
   defined in RFC 4291, "IP Version 6 Addressing Architecture" [15].

For IPv6, all C12.22 IP Relays, C12.22 IP Master Relays, and all
C12.22 IP Nodes configured to support broadcast and multicast (see
Section 5.3, "Using IP Broadcast/Multicast", below) SHALL join the
global-scope multicast address, FF0E::204, as well as all of the
assigned, reduced-scope, multicast addresses:

                    link-local   -- FF02::204;
                    admin-local   -- FF04::204;
                    site-local   -- FF05::204; and
                    organization-local -- FF08::204.

IPv6 C12.22 IP Nodes SHOULD use the minimum scope needed, when
initiating IP multicast messages to reach another C12.22 IP Node on
the C12.22 Network. This practice allows the sender to limit
unnecessary propagation of C12.22 IP Multicast Messages.

To determine the minimum scope required to reach the closest C12.22
IP Relay on the C12.22 Node's IP Network Segment, this specification
RECOMMENDS the following simple steps:

1. Starting with the smallest (local-most) scope (i.e., link-local
    scope or another pre-configured scope), send the C12.22 EPSEM
    Resolve Service Request for the purpose of C12.22 IP Relay
    discovery.

2. Listen for a response from a C12.22 IP Relay; then:

    A. If no response is received, assign the next wider scope
        level, then repeat steps (1) and (2) at the newly assigned
        scope.

    B. If a response is received, then record the scope level as the
        minimum scope to use on the node's C12.22 IP Network Segment.

A C12.22 IPv6 Node that initiates any EPSEM Service Request SHOULD
use the minimum scope necessary to reach its Target C12.22 IP Nodes.
A C12.22 IPv6 Relay SHALL use the global scope for any C12.22 Message
destined for the global Internet.

This specification does not preclude the use of the unassigned scope
values defined in [15]; those scope values MAY be used on a private
basis, or through mutual operating agreements.

For IPv4, all C12.22 IP Relays, C12.22 IP Master Relays, and all
C12.22 IP Nodes configured to support broadcast/multicast SHALL join
the assigned multicast address of 224.0.2.4. This global address
does not provide for the type of scoping discussed above for IPv6,
nor is it compatible with the administratively scoped IP multicast

   specification in RFC 2365 [16]. Therefore, a different technique to
   limit the propagation of C12.22 IP Multicast Messages is needed. One
   available technique to control IPv4 multicast scope is through the
   use of the Time-to-Live (TTL) attribute in the IP packet header.
   This attribute is not managed by the C12.22 protocol.

   In the implementation of this technique, an administrative domain
   MUST include at least one C12.22 IP Relay, and all C12.22 IP Nodes in
   the administrative domain SHOULD be configured with a TTL
   sufficiently large to reach that C12.22 IP Relay.

   A C12.22 IPv4 Node that initiates any C12.22 Request Message SHOULD
   use the minimum TTL needed to reach its Target C12.22 IP Nodes.

4.7. IP Broadcast

   IP broadcast is not generally suitable as a replacement for, or an
   alternative to, multicast in a C12.22 IP Network Segment. IP
   broadcast is not supported in IPv6, and it suffers from limited scope
   in IPv4. This specification, however, does not preclude the use of
   IP network directed or limited/local scope (address 255.255.255.255)
   broadcast within a controlled management domain (as per RFC 2644
   [17]).

4.8. Encoding of Multicast and Broadcast Addresses

   ANSI C12.22 Tables provide BINARY Elements for encoding a broadcast
   or multicast Native IP Address for transport within a C12.22 Message.
   The encoding of these Table Elements is identical to that defined in
   Section 4.3, "Encoding of Native IP Addresses". These fields SHALL
   be used as shown in Figure 2.

```
                                   IP Address (ADDR), Port (P), Transport (T)
                      Address
                       Length                         Octet
                                    0                        1
                                    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8
           IPv4                     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           Broadcast     4          |BADDR4 |
                                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

           IPv4                     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           Broadcast     6          |BADDR4 | P |
           +Port                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

           IPv4                     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           Broadcast     7          |BADDR4 | P |T|
           +Port+Transport          +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

           IPv4                     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           Multicast     4          |MADDR4 |
                                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

           IPv4                     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           Multicast     6          |MADDR4 | P |
           +Port                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

           IPv4                     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           Multicast     7          |MADDR4 | P |T|
           +Port+Transport          +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

           IPv6                     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           Multicast     16         |              MADDR6               |
                                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

           IPv6                     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           Multicast     18         |              MADDR6               | P |
           +Port                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

           IPv6                     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           Multicast     19         |              MADDR6               | P |T|
           +Port+Transport          +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

        Figure 2: Encoding of Broadcast/Multicast Native IP Addresses

   The IPv4 and IPv6 multicast addresses -- MADDR4 and MADDR6,
   respectively -- are those assigned by IANA for use by ANSI C12.22.

When a broadcast/multicast Native IP Address is encoded in the ANSI
C12.19 Tables' BINARY data Elements, the size of the Native Address
Element transmitted is defined by ACT_NETWORK_TBL.NATIVE_ADDRESS_LEN
(see Table 121 of [1], and [2]). This is the actual number of octets
that are placed inside the C12.19 BINARY Element. This value is
common to all of the C12.22 Node's interfaces, including those that
are not IP based (thus not conforming to this specification). For
this reason, the ACT_NETWORK_TBL.NATIVE_ADDRESS_LEN MAY be greater
than, and SHALL NOT be smaller than, the actual length needed to
encode a broadcast/multicast Native IP Address per Figure 2. When
this is the case, the C12.22 Native IP Address SHALL be padded with
zero (0) to fill the Table's BINARY data Element.

The IPv4 network directed broadcast address can be computed by
performing a bitwise OR between the bit complement of the subnet mask
of the target IP subnet and the IP address of any host on that IP
subnet.

5. IP Message Transport

   This section defines a C12.22 Node's usage of the Connection-Oriented
   (CO) and Connectionless (CL) transport layer protocols -- TCP and
   UDP, respectively.

5.1. C12.22 Connection Types and TCP/UDP Transport Modes

   A C12.22 IP Node's use of TCP and UDP is based on its registered
   capabilities as defined in its configuration parameters (flags) and
   as expressed in the Node's accepted registration attributes [1]:

        CL Flag = <connection-type>.CONNECTIONLESS_MODE_SUPPORTED;
        CL Accept Flag = <connection-type>.ACCEPT_CONNECTIONLESS;
        CO Flag = <connection-type>.CONNECTION_MODE_SUPPORTED; and
        CO Accept Flag = <connection-type>.ACCEPT_CONNECTIONS.

   The mapping of the connection-type parameters to the IP-based
   transport variants that a C12.22 Node MAY support is defined in
   Table 1.

CL Flag	CO Flag	CL Accept Flag	CO Accept Flag	IP Transport Mode Supported
0	0	x	x	Invalid
0	1	0	0	TCP, Active-OPEN
0	1	0	1	TCP, Passive- and Active-OPEN
0	1	1	0	Invalid
0	1	1	1	Invalid
1	0	0	0	UDP, Active-OPEN
1	0	0	1	Invalid
1	0	1	0	UDP, Passive- and Active-OPEN
1	0	1	1	Invalid
1	1	0	0	UDP, Active-OPEN; TCP Active-OPEN
1	1	0	1	UDP, Active-OPEN; TCP, Passive- and Active-OPEN
1	1	1	0	UDP, Passive- and Active-OPEN; TCP, Active-OPEN
1	1	1	1	UDP, Passive- and Active-OPEN; TCP, Passive- and Active-OPEN

Table 1: C12.22 Node Parameters to IP Transport Mapping

Every C12.22 IP Node MUST support at least one of the unicast CO or CL operating capabilities (as advertised in Decade 12, "Node Network Control Tables" [1], where available, and as registered using the C12.22 Registration Service [1]).

5.2. IP Message Transport Details

5.2.1. TCP and UDP Port Use

General rules:

1. A C12.22 IP Node that implements [CL Accept=1] SHALL receive incoming UDP C12.22 Messages on its registered Native IP Address (IP address and port number).

2. A C12.22 IP Node that implements [CO Accept=1] SHALL receive incoming TCP connections on its registered Native IP Address (IP address and port number).

3. A C12.22 IP Relay that forwards a UDP C12.22 Message to a C12.22
    IP Node on the C12.22 IP Network Segment SHALL send the C12.22
    Message to the C12.22 IP Node's registered Native IP Address (IP
    address and port number).

4. A C12.22 IP Relay that forwards a TCP C12.22 Message to a C12.22
    IP Node on the C12.22 IP Network Segment MAY use an established
    TCP connection to that C12.22 IP Node, or it SHALL establish a
    new TCP connection to the C12.22 IP Node's registered Native IP
    Address (IP address and port number).

5. A C12.22 IP Node that implements [CL=1] SHOULD set the source
    port number in outbound UDP C12.22 Messages to its registered
    port number. When the target UDP C12.22 IP Node is reachable
    using direct messaging (as defined in [1]), the C12.22 IP Node
    MAY set the source port number to a UDP port number that is
    different than its registered port number.

6. When the registered Native IP Address of a C12.22 IP Node does
    not include the OPTIONAL port number, then port 1153 SHALL be
    assumed and used as the registered port number.

7. All C12.22 IP Nodes SHOULD use port 1153 in their Native IP
    Address when registering.

5.2.2. Active-OPEN UDP Mode (CL=1, CL Accept=0)

   A C12.22 IP Node that supports this mode SHALL NOT monitor for
   unsolicited incoming C12.22 Messages via UDP. As a result, the
   C12.22 IP Node is incapable of receiving unsolicited C12.22 Messages
   using UDP.

   The C12.22 IP Node MAY enter the Active-OPEN UDP state by initiating
   an unsolicited UDP transmission to a Target C12.22 IP Node, which is
   expected to implement the Passive-OPEN UDP mode.

   C12.22 IP Nodes SHOULD use their registered UDP port number, or if
   not yet registered, then they SHOULD use port 1153 as the source port
   number for all UDP C12.22 IP Messages.

5.2.3. Passive-OPEN UDP Mode (CL=1, CL Accept=1)

   A C12.22 IP Node that operates in this mode SHALL be capable of
   receiving solicited and unsolicited C12.22 Messages from other C12.22
   IP Nodes. The C12.22 Node MAY change the port number that it
   monitors by using the <native-address> parameter of the ANSI C12.22
   Registration Service. The C12.22 IP Node MAY initiate unsolicited
   Active-OPEN UDP transmissions to other C12.22 IP Nodes that implement
   the Passive-OPEN UDP mode.

   When operating in this mode, the C12.22 IP Nodes SHALL use their
   registered UDP port number as the source port number for all UDP
   C12.22 IP Messages.

   All C12.22 IP Relays SHALL support the Passive-OPEN UDP mode. C12.22
   Authentication Hosts and C12.22 Notification Hosts that implement UDP
   SHALL support the Passive-OPEN UDP mode. For all other C12.22 IP
   Nodes, the Passive-OPEN UDP mode is the RECOMMENDED mode when
   implementing UDP.

5.2.4. Active-OPEN TCP Mode (CO=1, CO Accept=0)

   A C12.22 IP Node that supports this mode SHALL NOT monitor for
   inbound TCP connections. As a result, the node is incapable of
   accepting incoming connections via TCP. The C12.22 IP Node MAY
   initiate TCP connections to Target C12.22 IP Nodes, which are
   expected to implement the Passive-OPEN TCP mode.

   In this mode, C12.22 Messages exchanged by a pair of associated
   C12.22 IP Nodes can only be communicated through any of the TCP
   connections that were initiated by the C12.22 IP Node that implements
   this mode. The loss or closure of a connection SHALL NOT
   automatically result in the termination of the C12.22 associations
   between the peer nodes. In order to continue exchanging C12.22
   Messages without loss of association, the initiating C12.22 IP Node
   MAY re-establish new TCP connections with the peer node, or use
   existing connections to the peer node. The termination of the C12.22
   Application associations is dependent upon C12.22 Application timeout
   attributes and C12.22 link management services (such as Procedure 25,
   "Network Interface Control" [1]).

5.2.5. Passive-OPEN TCP Mode (CO=1, CO Accept=1)

   A C12.22 IP Node that operates in this mode SHALL monitor and accept
   incoming TCP connections. The C12.22 Node MAY change the port number
   that it monitors by using the <native-address> parameter of the ANSI
   C12.22 Registration Service. The C12.22 IP Node MAY initiate Active-
   OPEN TCP connections to other C12.22 IP Nodes that implement the
   Passive-OPEN TCP mode.

   In this mode, C12.22 Messages exchanged by a pair of associated
   C12.22 IP Nodes can arrive through any of the TCP connections that
   were established by either node. The loss or closure of a connection
   SHALL NOT automatically result in the termination of the C12.22
   associations between the peer nodes. In order to continue exchanging
   C12.22 Messages without loss of association, either C12.22 IP Node
   MAY re-establish new TCP connections with the peer node, or use
   existing connections to the peer node. The termination of the C12.22
   Application associations is dependent upon C12.22 Application timeout
   attributes and C12.22 link management services (such as Procedure 25,
   "Network Interface Control" [1]).

   All C12.22 IP Relays SHALL support the Passive-OPEN TCP mode. C12.22
   Authentication Hosts and C12.22 Notification Hosts that implement TCP
   SHALL support Passive-OPEN TCP mode. For all other C12.22 IP Nodes,
   Passive-OPEN TCP mode is the RECOMMENDED mode when implementing TCP.

5.2.6. TCP and C12.22 Message Directionality

   C12.22 IP Nodes MAY use TCP in one of two ways: bi-directional
   traffic flow or uni-directional traffic flow.

   When TCP connections are used, any new or established TCP connection
   between the two C12.22 IP Nodes MAY be used equivalently by the
   C12.22 IP Nodes to send and to receive C12.22 Messages. This is the
   RECOMMENDED and default mode of operation because ANSI C12.22
   requires the transport network to be reliable and connectionless (per
   connectionless-mode ACSE). For this reason, ANSI C12.22 defines
   peer-to-peer application associations and not peer-to-peer
   connections.

   It is known that some C12.22 implementations have been deployed in
   which TCP is used for uni-directional traffic flow. For these types
   of implementations, an established TCP connection SHALL be used by
   the initiator of that connection to send C12.22 Messages and by the

target node (that accepted the connection) to receive C12.22
Messages. If a C12.22 IP Node wishes to send a C12.22 Message to a
peer C12.22 IP Node, it MUST establish and use a new TCP connection,
or use an existing TCP connection that it had previously initiated,
for its outbound uni-directional traffic flow.

For increased interoperability, the initiator of the connection
SHOULD accept incoming C12.22 Messages on that connection in case the
target node attempts to use the connection for bi-directional traffic
flow.

Uni-directional use of TCP is a special mode of operation; it is NOT
RECOMMENDED because multiple one-way channel communication is not
described by ANSI C12.22, and it utilizes one-half of the TCP
connection capability. As a result, it doubles the number of TCP
connections used to communicate C12.22 Messages and thus could become
a burden when a large number of connections are required.

5.3. Using IP Broadcast/Multicast

A C12.22 IP Node's use of broadcast/multicast is based on its
capabilities as defined in its configuration parameters (flags) and
as expressed in the Node's accepted registration attributes [1]
(<connection-type>.BROADCAST_AND_MULTICAST_SUPPORTED). The mapping
of the C12.22 IP Node's Broadcast/Multicast parameter (flag) to IP
broadcast/multicast usage is defined in Table 2.

C12.22 Broadcast and Multicast Supported Flag	IP Broadcast/Multicast Supported
0	The C12.22 IP Node does not accept IP broadcast, and it does not accept IP multicast messages.
1	The C12.22 IP Node accepts both IP broadcast (IPv4 only) and IP multicast messages (IPv4 and IPv6).

Table 2: C12.22 to IP Broadcast/Multicast Mapping

If a C12.22 IP Node is configured to accept IP broadcast and
multicast messages, it SHALL join the "All C1222 Nodes" multicast
group (see Section 4.6, "IP Multicast", above), and SHALL use the
default port 1153. In addition, it SHALL accept IP network directed
or limited (local scope) broadcast messages sent to port 1153. Note
that successful communication using network directed broadcast
requires configuration of network routers, which by default SHALL NOT
forward directed broadcasts as per RFC 2644 [17].

5.4. Transport Protocol Decisions

5.4.1. Unicast Versus Multicast Versus Broadcast

   An initiating C12.22 IP Node MAY send any C12.22 Message using UDP or
   TCP. However, in accordance with Section 5.3.2.4.12, "Resolve
   Service", of ANSI C12.22, it is RECOMMENDED that the C12.22 Resolve
   Request Message be transported using UDP/IP multicast when the Native
   IP Address of the Target C12.22 Node is not known. The use of UDP/IP
   multicast is preferred over the use of IP network directed or limited
   broadcast; therefore, when UDP/IP multicast is supported, its use is
   RECOMMENDED over network broadcast.

5.4.2. Sending Large C12.22 APDUs Using UDP

   When sending via UDP a large C12.22 Message that exceeds the path
   MTU, the sender SHALL segment the ACSE APDU in accordance with the
   ANSI C12.22 Datagram Segmentation and Reassembly algorithm, such that
   the size of the resulting IP datagram does not exceed the path MTU
   and thus avoids UDP packet fragmentation. The fundamental issue with
   fragmentation exists for both IPv4 and IPv6. Section 3.2 of RFC 5405
   [18] provides additional guidelines for determining the appropriate
   UDP message size. When the path MTU is not known, the sender SHALL
   follow the guidelines stipulated in Section 3.2 of RFC 5405 [18]: for
   IPv4, use the smaller of 576 bytes and the first-hop MTU [19], and
   for IPv6, use 1280 bytes [20]. Sending large APDUs via UDP may lead
   to network congestion. For more information on avoiding network
   congestion see Section 5.6, "Congestion Control".

5.4.3. Choice of Protocol for C12.22 Response APDUs

   When a Target C12.22 IP Node receives a C12.22 Request Message from
   an initiating C12.22 IP Node, it SHALL send a C12.22 Response Message
   using the same transport protocol (i.e., TCP to TCP, UDP to UDP).

   In the case of UDP, the target SHALL send the C12.22 Response Message
   to the source IP address and port number.

5.5. Quality of Service

   The ANSI C12.22 standard provides a configuration parameter in the
   APDU's <calling-AE-qualifier>.URGENT attribute to mark a message as
   urgent. There are numerous IP-based technologies that enable
   enhanced levels of message delivery and quality of service. This
   specification does not define the technology to be used to send
   urgent messages over IP.

5.6. Congestion Control

   Designers of unicast applications that implement the upper layers of
   C12.22 messaging over UDP SHOULD follow the congestion control
   guidelines in Section 3.1 of RFC 5405 [18].

   For the transmission of C12.22 Messages that are greater than what
   the TCP initial window would be over a given Internet path, TCP
   SHOULD be used rather than UDP as the transport protocol. TCP's
   initial window depends on the maximum segment size (MSS), which in
   turn depends on the path MTU, and is computed according to formula
   (1) in RFC 3390 [21]. For unknown path MTUs, the smallest allowable
   MSS MUST be used, and the C12.22 Application SHOULD assume the
   maximum C12.22 Message size to be 2048 bytes. By using TCP, the
   C12.22 Application benefits from the built-in TCP congestion control
   mechanism.

   When UDP is the preferred transport mechanism, or when UDP multicast
   or broadcast are the preferred modes of communication, then the
   C12.22 Application SHOULD use C12.22 acknowledged Messages that are
   smaller than TCP's initial window over the return path, as computed
   by formula (1) in [21] and described above. The size of the C12.22
   Message MAY be managed through the use of ANSI C12.22 EPSEM Partial
   Table Read/Write Service Requests and Responses.

6. Security Considerations

   The ANSI C12.22 Application Layer Security is defined in
   Section 5.3.4.13, "C12.22 Security Mechanism", of the ANSI C12.22
   standard. The security mechanisms include provisions for message
   privacy and authentication, playback rejection, and message
   acceptance windows, as well as ANSI C12.19 [2] role-based data access
   and secured register mechanisms. The ANSI C12.22 Application Layer
   default security mechanism provides three options to choose from when
   sending C12.22 Messages:

   1. Sending cleartext messages over the C12.22 Network [1], [5],
       which MAY result in altered C12.22 Messages and exposure to
       password sniffing attacks, as described in RFC 3552 [22].

   2. Sending of authenticated plaintext messages over the C12.22
       Network [1], [5], which MAY result in password sniffing attacks
       as described in RFC 3552 [22].

   3. Sending of authenticated ciphertext over the C12.22 Network,
       providing for message and peer node authentication and privacy.

When option 1 is used, then it is RECOMMENDED that the network or
transport layer provide authentication and confidentiality service.
When option 2 is used, then it is RECOMMENDED that the network or
transport layer provide confidentiality services. When option 3 is
used, then no additional network or transport layer security services
are necessary.

Additional transport or network layer security protocols are not
required by ANSI C12.22, but they MAY be provided transparently by
C12.22 IP Network Segment integrators (e.g., in C12.22 IP Relays) in
order to improve on the security provisions cited above. However,
any added transport security (e.g., Transport Layer Security (TLS),
RFC 5246 [27]) or IP security (e.g., IPsec, RFC 4302 [25], RFC 4303
[26], RFC 5996 [28]) features SHALL act only to enhance (i.e., not be
a substitute for, or an alteration of) the interoperable ANSI C12.22
and ANSI C12.19 security provisions, and SHALL NOT corrupt and SHALL
NOT alter the C12.22 Message as presented by the C12.22 Application
Layer.

The ANSI C12.22 [1] and ANSI C12.19 [2] standards provide for the
transmission of keys and their storage in C12.19 End Devices (e.g.,
meters and head-end systems). The key management protocol (when and
how keys are exchanged) is not described in the ANSI C12.22 [1] and
ANSI C12.19 [2] standards, except to state that keys MAY not be
readable from a C12.19 End Device (in response to a Read Service
Request). It is RECOMMENDED that all C12.22 Nodes encrypt user
information element key fields and passwords. It is also RECOMMENDED
that all C12.22 Nodes mask user information element key fields and
password fields of EPSEM Read Service Responses (e.g., by replacing
all key and password bytes with zeros (0x00) or spaces (0x20)).

Legacy deployments exist that are not connected to the Internet, so
there are some implementations that do not include security. It is
likely that multi-homed C12.22 Nodes with interfaces to the Internet
will exist in future deployments, so security mechanisms MUST be used
by those C12.22 Nodes to ensure C12.22 Message authentication and
confidentiality.

7. IANA Considerations

   UDP and TCP port 1153, which is used for C12.22 communication over
   IP, is registered with IANA.

   Section 4.6, "IP Multicast", defines the use of multicast. The
   following multicast addresses have been registered by IANA for use by
   the ANSI C12.22 standard:

      IPv4 -- "All C1222 Nodes" address 224.0.2.4

      IPv6 -- "All C1222 Nodes" address FF0X::204

8. Acknowledgments

   The authors wish to recognize Alexander Shulgin for providing
   valuable comments and for conducting feasibility testing in support
   of this work.

   The following people have improved this document through thoughtful
   comments and suggestions: Fred Baker, Ralph Droms, Vijay Gurbani,
   Michael Stuber, Spencer Dawkins, Alfred Hoenes, Russ Housley, Paul
   Hoffman, Lars Eggert, and Sean Turner.

9. References

9.1. Normative References

   [1]   ANSI, "Protocol Specification for Interfacing to Data
          Communication Networks", ANSI C12.22-2008, January 2009.

   [2]   ANSI, "Utility Industry End Device Data Tables", ANSI C12.19-
          2008, February 2009.

   [3]   IEEE, "Draft Standard for Utility Industry Metering
          Communication Protocol Application Layer (End Device Data
          Tables)", IEEE P1377-2010, October 2010.

   [4]   Bradner, S., "Key words for use in RFCs to Indicate Requirement
          Levels", BCP 14, RFC 2119, March 1997.

   [5]   IEEE, "Standard for Local Area Network/Wide Area Network (LAN/
          WAN) Node Communication Protocol to Complement the Utility
          Industry End Device Data Tables", IEEE P1703-2010,
          October 2010.

[6]   ISO/IEC, "Information Technology-Open Systems Interconnection-
      Connectionless Protocol for the Association Control Service
      Element: Protocol Specification", ISO/IEC 10035-1, 1995.

[7]   ISO/IEC, "Information Technology-ASN.1 Encoding Rules:
      Specification of Basic Encoding Rules (BER), Canonical Encoding
      Rules (CER) and Distinguished Encoding Rules (DER)", ISO/
      IEC 8825-1, 2002.

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

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

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

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

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

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

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

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

[16] Meyer, D., "Administratively Scoped IP Multicast", BCP 23,
      RFC 2365, July 1998.

[17] Senie, D., "Changing the Default for Directed Broadcasts in
      Routers", BCP 34, RFC 2644, August 1999.

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

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

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

   [21] Allman, M., Floyd, S., and C. Partridge, "Increasing TCP's
         Initial Window", RFC 3390, October 2002.

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

9.2. Informative References

   [23] Measurement Canada, "Specification for Utility Industry
         Metering Communication Protocol Application Layer (End Device
         Data Tables)", Draft MC12.19, 2011.

   [24] Measurement Canada, "Specification for Local Area Network/Wide
         Area Network (LAN/WAN) Node Communication Protocol to
         Complement the Utility Industry End Device Data Tables",
         Draft MC12.22, 2011.

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

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

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

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

Authors' Addresses

    Avygdor Moise
    Future DOS R&D Inc.
    #303 - 6707 Elbow Drive SW
    Calgary, Alberta T2V 0E5
    Canada

    EMail: avy@fdos.ca
    URI: http://www.fdos.ca

    Jonathan Brodkin
    Future DOS R&D Inc.
    #303 - 6707 Elbow Drive SW
    Calgary, Alberta T2V 0E5
    Canada

    EMail: jonathan.brodkin@fdos.ca
    URI: http://www.fdos.ca