

ANSI/CEA Standard

Tunneling Device Area Network Protocols over Internet Protocol Channels

ANSI/CEA-852-C

April 2014



CEA
Consumer Electronics Association

Documents
www.CE.org
Document Sharing Hub

NOTICE

Consumer Electronics Association (CEA[®]) Standards, Bulletins and other technical publications are designed to serve the public interest through eliminating misunderstandings between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for his particular need. Existence of such Standards, Bulletins and other technical publications shall not in any respect preclude any member or nonmember of CEA from manufacturing or selling products not conforming to such Standards, Bulletins or other technical publications, nor shall the existence of such Standards, Bulletins and other technical publications preclude their voluntary use by those other than CEA members, whether the standard is to be used either domestically or internationally.

Standards, Bulletins and other technical publications are adopted by CEA in accordance with the American National Standards Institute (ANSI) patent policy. By such action, CEA does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the Standard, Bulletin or other technical publication.

This document does not purport to address all safety problems associated with its use or all applicable regulatory requirements. It is the responsibility of the user of this document to establish appropriate safety and health practices and to determine the applicability of regulatory limitations before its use.

This document is copyrighted by the Consumer Electronics Association (CEA[®]) and may not be reproduced, in whole or part, without written permission. Federal copyright law prohibits unauthorized reproduction of this document by any means. Organizations may obtain permission to reproduce a limited number of copies by entering into a license agreement. Requests to reproduce text, data, charts, figures or other material should be made to CEA.

(Formulated under the cognizance of the CEA **R7 Home Networks Committee.**)

Published by
©CONSUMER ELECTRONICS ASSOCIATION 2014
Technology & Standards Department
www.CE.org

All rights reserved

FOREWORD

This standard was developed under the auspices of the CEA R7 Home Networks Committee.

Unless otherwise indicated, the designator 852 refers to the latest revision of CEA-852, which at the time of this writing was CEA-852-C.

Unless otherwise indicated, the designator 709 and 709.1 refers to the latest revision of CEA-709.1, which at the time of this writing was CEA-709.1-D.

Unless otherwise indicated, the designator 852.1 refers to the latest revision of CEA-852.1, which at the time of this writing was CEA-852.1-A.

[This page intentionally left blank.]

Copyright 2014 by Consumer Technology Association

CONTENTS

1 General	1
1.1 Scope	1
1.2 Revision History.....	1
1.2.1 CEA-852 Revision B	1
1.3 Definitions	2
1.4 Acronyms.....	3
2 Normative References	4
2.1 Reference Acquisition	4
3 Introduction	5
4 Requirements	6
5 CN/IP Device Specification.....	7
5.1 IP Related Device Specifications	7
5.2 CN Related Device Specifications.....	7
5.2.1 Packet Formats.....	7
5.2.2 Addressing Schemes	7
6 IP Channel Specification	8
6.1 IP Transport Mechanisms	10
6.1.1 Informative Considerations	12
7 CN/IP Device Configuration	12
7.1 Configuration Parameters.....	12
7.1.1 Channel Definition Parameters	13
7.1.2 Send List Parameters	13
7.1.3 Device Parameters	14
7.2 Configuration Techniques	14
7.2.1 Manual Configuration	14
7.2.2 BOOTP and DHCP	14
7.2.3 Configuration Servers.....	14
8 CN/IP Messages and Modes of Operation	15
8.1 Common Message Header.....	16
8.2 Packet Segmentation	17
8.2.1 Overview.....	17
8.2.2 Segment Exchange	18
8.2.3 Discussion	19
8.3 Data Packet Exchange.....	20
8.3.1 Out of Order Packets.....	20
8.3.2 Duplicate Packet Detection	21
8.3.3 Stale Packet Detection	21
8.4 Configuration Server Interactions.....	22
8.4.1 General Device Interaction	22
8.4.2 General Protocol Interaction	24
8.4.3 Packet Segmentation	25
8.4.4 Device Registration	26
8.4.5 Channel Membership	27
8.4.6 Send List	28
8.4.7 Channel Routing.....	29

8.5 Miscellaneous Status Messages	31
8.5.1 CN/IP Device Status	31
8.5.2 Device Registration	32
8.5.3 Device Send List.....	33
8.5.4 Channel Membership List.....	33
8.5.5 Channel Routing Information	33
8.6 Vendor Specific Messages	34
8.7 Packet Authentication	34
9 Packet Formats.....	36
9.1 Packet Types	36
9.2 Common CN/IP Header	37
9.3 Segment Packet	39
9.4 CN Data Packets	40
9.5 CN/IP Device Registration Packets	40
9.6 Channel Membership Packet.....	44
9.7 Channel Routing Packet	45
9.8 Request Packet	48
9.9 Acknowledge Packet	50
9.10 Send List Packet	51
9.11 Node Status/Health/Statistics Response Message	51
10 Annex A Specifications for ANSI/CEA-709.1-D (Normative)	54
11 Annex B Specifications for CEA-709 (Informative)	55
12 Annex C Specifications for CEA-600 (Normative)	55
13 Annex D Specifications for CEA-600 (Informative)	55

Figures

Figure 1 Typical CN/IP Application	6
Figure 2 IP Protocol Stack	11
Figure 3 Packet Aggregation.....	17
Figure 4 Packet Authentication Encoding and Decoding	35
Figure 5 Packet Aggregation with Authentication	36

Tables

Table 1 Device Registration with Configuration Server Protocol	27
Table 2 Server to Device Unsolicited Registration Message Protocol	27
Table 3 Device to Server Channel Membership Request Protocol	28
Table 4 Device to Server Send List Request Protocol	29
Table 5 Device to Server Channel Routing Update Protocol	30
Table 6 Device to Server Channel Routing Request Protocol	30
Table 7 Protocol for Requesting a Device's Registration	33
Table 8 Protocol for Requesting a Device's Send List	33
Table 9 Protocol for Requesting a Device's Channel Definition	33
Table 10 Protocol for Requesting a Device's Channel Routing Information	33
Table 11 Message Type Cross Reference.....	37

Table 12 Common Packet Header Format	37
Table 13 Segment Packet Format	39
Table 14 Data Packet Format	40
Table 15 Device Registration Packet Format	41
Table 16 Channel Membership Packet Format	45
Table 17 Channel Routing Packet Formats	46
Table 18 Configuration Request Packet Format	48
Table 19 Request Reason Codes.....	49
Table 20 Request Amount Codes	49
Table 21 Request Action Codes.....	49
Table 22 Acknowledge Packet Formats.....	50
Table 23 Send List Packet Format.....	51
Table 24 Node Status/Health/Statistics Response Message	53

[This page intentionally left blank.]



Tunneling Device Area Network Protocols Over Internet Protocol Channels

1 General

1.1 Scope

The CEA-852 standard specifies a communications method that allows networked data acquisition and control devices to communicate with each other over the internet. The purpose of such devices are widely varying and include functions such as appliance monitoring, meter reading, and HVAC and lighting control to name a few. CEA-852 does not replace existing device communications protocols, but instead allows those protocols to use the internet as a communications medium. CEA-852 currently supports the existing device protocols CEA-600 (CEBus) and CEA-709 (LonTalk®) and was designed to allow the support of others.

Unless otherwise indicated, the designator 852 refers to the latest revision of CEA-852, which at the time of this writing was CEA-852-C.

1.2 Revision History

Since the original CEA-852 standard specification was released in 2001, several vendors have released implementations of the standard and more are in development. Unfortunately, as is the case with almost any new specification, experience in its use and interoperation between different implementations has brought to light several errors, omissions, unforeseen limitations and poorly defined requirements. Moreover, the CEA-852 specification is being adopted by other International standards bodies. As part of an ongoing effort to refine the standard, revisions to the original CEA-852 specification have been developed.

1.2.1 CEA-852 Revision B

Because CEA-852 Revision A was limited to modifications that would maintain a high degree of backwards compatibility with the installed base of 852 devices, it did not address all of the limitations that have been discovered in the original specification. As a result, CEA-852 Revision B has been developed.

The major change between CEA-852-A and CEA-852-B is the addition of a new flag. This flag is called the Protocol Escape Bit. When set, the Protocol Escape Bit indicates that the device or configuration server sending the 852-B packet, supports and is allowed to operate using a different protocol such as the CEA-852.1-A [13.] protocol. An 852 device or configuration server that supports both CEA-852 and another related protocol is called *Bilingual*. This protocol escape bit allows Bilingual configuration servers to correctly form channels with devices that support CEA-852, another protocol, or are Bilingual. (For reference see the Hybrid Channel Bootstrap Algorithm in the CEA-852.1-A [13.] specification).

The description of packet authentication in CEA-852-A is ambiguous especially with regard to segmented packets and aggregated packets. This ambiguity is removed in CEA-852-B. Other typos and minor clarifications were also added in CEA-852-B:

- Defined Bit 6 in the protocol flags field of the common header as the Protocol Escape Bit.
- Clarified the description of packet authentication especially with regard to segmented packets and aggregated packets.
- Fixed typos and minor clarifications.

1.3 Definitions

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 [10.].

A Component Network (CN) is a network of nodes (devices) that are capable of computing, sensing, and actuating. Typically these devices are used for control and telemetry purposes including applications such as HVAC, security, energy management, machine control, etc. These devices are typically not used for data processing or general purpose computing purposes. Some of the characteristics of CNs that set them apart from traditional data networks include:

- Typically lower bandwidth requirements.
- Small packet/message sizes.
- Tighter constraints on message reliability and delivery latencies.

A number of existing standards apply to networks of this type including ANSI/CEA-709.1-D [2.] and CEA-600 CEBus [11.].

Tunneling refers to the encapsulation of one protocol's packet within the payload of another protocol's packets.

The Internet Protocol (IP) is a packet switched protocol that allows networks to be built that consists of a loose confederation of hosts that can communicate over a wide range of physical media and topologies to exchange data. Refer to RFC 791 [7.].

A channel refers to the common communications transport mechanism that a specific collection of CN devices share and communicate over without the use of a router. Channels are used to transport CN packets below the link layer of the CN protocol stack. Typically this refers to some type of physical media such as power line, RF, or twisted pair, but in the case of IP networks this channel is not physical, but a protocol tunnel.

A CN device is considered to be any device that uses the CN protocol to communicate with other CN devices. The CN protocols that are compatible with the 852 standard are provided in the appendices. References to CN devices in this specification assume the device is using a compatible CN protocol.

A CN router is special type of CN device that routes CN protocol packets between two or more channels.

A CN node is special type of CN device that can send or receive CN protocol packets, but does not route them between channels.

A CN/IP device is a CN device that communicates with other CN devices over an IP channel using this, the 852 protocol. In other words, in this specification a CN/IP device is synonymous with an 852 device.

A CN/IP router is a CN router in which at least one of the channels it routes packets over is an 852 tunnel on an IP channel.

A CN/IP node is a CN node in which at least one of the channels it sends and receives packets over is an 852 tunnel on an IP channel.

All CN devices are either CN Routers, CN Nodes or both.

All CN/IP devices are either CN/IP Routers, CN/IP Nodes or both.

A CN group is a collection of CN devices that share a common multi-cast address in the CN protocol.

The Address Resolution Protocol (ARP) is a TCP/IP protocol used to convert an IP address into a physical address such as an Ethernet address. A host wishing to obtain a physical address broadcast an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address.

There is also Reverse ARP (RARP) that can be used by a host to discover its IP address. In this case, the host broadcasts its physical address and a RARP server replies with the host's IP address.

The Internet Control Message Protocol (ICMP) is an extension to the Internet Protocol (IP) defined by RFC 791 [7.]. ICMP supports packet containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

Internet Group Management Protocol (IGMP) is defined in RFC 1112 [1.] as the standard for IP multi-casting in the Internet. It's used to establish host memberships in particular multi-cast groups on a single network. The mechanisms of the protocol allow a host to inform its local router, using Host Membership Reports that it wants to receive messages addressed to a specific multi-cast group. All hosts conforming to level 2 of the IP multi-casting specification require IGMP.

A domain is a group of computers and devices on a network that are administered as a unit with common rules and procedures. Domains are defined by an address referred to as the "domain address". Different network protocols specify the domain address in different ways.

A subnet is a portion of a network that shares a common address component known as the "subnet address". Different network protocols specify the subnet address in different ways.

A node ID is a logical network address that differentiates nodes within the same subnet or domain.

A unique ID is a network address that is globally unique. No two nodes anywhere can share the same unique ID.

Data Skew refers to the situation that exists when a data set that forms the basis for a message changes while the message is in the course of being transmitted to another device.

The term MBZ in protocol fields stands for Must Be Zero. This stands for a reserved field that may be used in following versions of the protocol. Such fields shall be sent as zero and ignored by the receiver in implementations conforming to the current version of the specification.

1.4 Acronyms

ACK	Acknowledge
ARP	Address Resolution Protocol
BOOTP	Bootstrap Protocol
CN	Component Network
CRC	Cyclical Redundancy Check
CTP	Channel Timeout Period
DHCP	Dynamic Host Configuration Protocol
GMT	Greenwich Mean Time
HTTP	HyperText Transfer Protocol
IANA	Internet Assigned Number Authority
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol

IP	Internet Protocol
LAN	Local Area Network
LFS	Last Forwarded Sequence
LPDU	Link layer Protocol Data Unit
MAC	Media Access Control
MBZ	Must Be Zero
MPDU	MACS Protocol Data Unit
NAT	Network Address Translation
NTP	Network Time Protocol
PDU	Protocol Data Unit
PSN	Packet Sequence Number
QOS	Quality of Service
RARP	Reverse ARP
SA/DA	Source Address/Destination Address
SID	Session ID
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTC	Coordinated Universal Time
WAN	Wide Area Network

2 Normative References

- [1.] Deering, S.E., "Host extensions for IP Multicasting", STD 5, RFC 1112, Stanford University, August 1989
- [2.] CEA, ANSI/CEA-709.1-D, Control Network Protocol Specification, April 2014
- [3.] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, Bucknell University, March 1997
- [4.] Croft, W.J., Gilmore, J., "Bootstrap Protocol", RFC 951, September 1985
- [5.] Mills, D., "Network Time Protocol (Version 3) Specification, Implementation and Analysis", RFC 1305, University of Delaware, March 1992
- [6.] Mills, D., "Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI", RFC 2030, University of Delaware, October 1996
- [7.] Postel, J., "Internet Protocol", STD 5, RFC 791, USC Information Sciences Institute, September 1981
- [8.] Postel, J., "User Datagram Protocol", STD 6, RFC 768, USC Information Sciences Institute, August 1980
- [9.] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, USC Information Sciences Institute, September 1981
- [10.] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, Harvard University, March 1997
- [11.] CEA, "CEBus Standard", CEA STANDARD CEA-600 CEBus Set, March 1996
- [12.] Rivest, R. "The MD5 Message-Digest Algorithm", RFC 1321, April 1992
- [13.] CEA, ANSI/CEA-852.1-A, Enhanced Protocol for Tunneling Component Network Protocols Over Internet Protocol Channels, April 2014

2.1 Reference Acquisition

CEA Standards:

Global Engineering Documents, World Headquarters, 15 Inverness Way East, Englewood, CO USA 80112-5776; Phone: 800-854-7179; Fax: 303-397-2740; Internet: <http://global.ihs.com>; E-mail: global@ihs.com.

IETF Documents:

Internet Engineering Task Force (IETF) Secretariat, c/o Corporation for National Research Initiatives, 1895 Preston White Drive, Suite 100, Reston, VA 20191-5434, USA; (703) 620-8990 / (703) 620-9071 (FAX); URL: www.ietf.org, IETF RFCs may be downloaded from www.ietf.org/rfc.html, IETF Internet drafts may be downloaded from www.ietf.org/ID.html

3 Introduction

This document provides specifications for the transporting of Component Network (CN) packets over Internet Protocol (IP) networks using a tunneling mechanism wherein the CN packets are encapsulated within the IP packets. It applies to both CN nodes and CN routers.

The purpose of this specification is to insure interoperability between various CN devices that wish to use IP networks to communicate using a particular CN protocol. The specification is intended to be general enough to handle a wide range of CN protocols. In particular this specification will cover the following standard CN protocols:

- ANSI/CEA-709.1-D [2.]
- CEA-600 CEBus [11.]

The main body of this specification is independent of the CN protocol being transported over the IP network. The reader is directed to Annex A and Annex B for the normative and informative, respectively, aspects of this specification that are specific to ANSI/CEA-709.1-D. Likewise Annex C and Annex D are the normative and informative, respectively, aspects of this specification as they apply to CEA-600 CEBus.

Figure 1 shows a possible configuration of such CN devices and networks connected to an IP network.

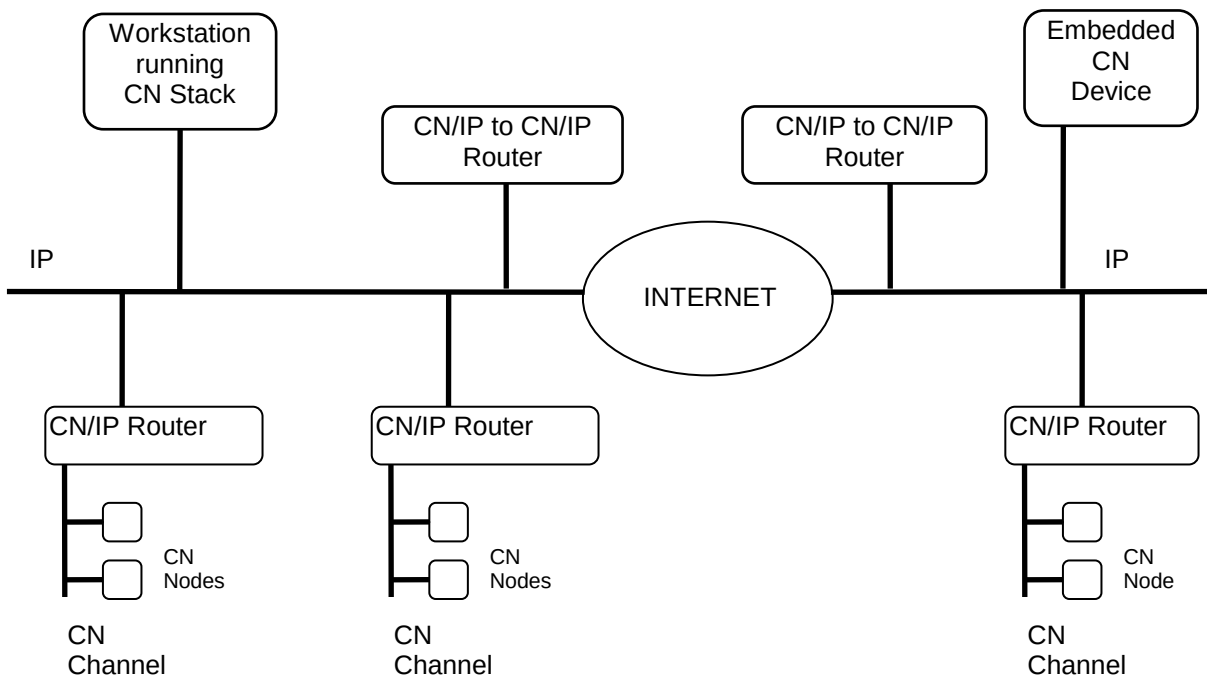


Figure 1 Typical CN/IP Application

Figure 1 depicts two types of CN devices: CN nodes and CN routers. Note that the routers shown can route packets between typical CN channels (such as twisted pair or power line) and an IP channel or it can route CN packets between two IP channels. In this document the IP channel will be defined in such a way to allow it to be used like any other CN channel.

In the above diagram the IP network can be considered to be one or more IP channels. This specification covers only how CN packets are transported over IP channels. It does not cover how CN packets are routed between standard CN channels and IP channels. This specification is not intended to cover the lower layers (physical, MAC and link) layers of either standard CN or IP channels.

4 Requirements

The following is a set of general requirements for the transporting of CN packets over IP channels:

- Be as efficient as possible to allow quasi Realtime operation.
- Be independent of the application level interface used to receive the packets. For example the tunneling protocol should not rely on the existence of a socket interface or how that interface may be used.
- Insure that CN packet ordering is preserved.
- Insure that CN packets that are “stale” (outside the maximum timeout characteristics of the IP channel) are not forwarded.
- Detect packets that get duplicated in the IP network.
- Support IP routing devices that prioritize IP packets.
- Optional security measures to prevent malicious users from tampering with devices.
- Scalable.
- Allow status information to be extracted from CN/IP devices.

- Support the exchange of configuration information between CN/IP devices and configuration servers.

5 CN/IP Device Specification

5.1 IP Related Device Specifications

A CN/IP device MUST behave like any standard IP host capable of exchanging IP packets with any other IP host either on the same IP subnet or anywhere else in the Internet cloud. A CN/IP device MUST have a single uni-cast IP address and MAY be capable belonging to as many as 32 multi-cast groups. It is OPTIONAL that a CN/IP device support multi-casting. This document does not address the routing of IP packets between subnets or through the Internet. The CN/IP devices MUST be compatible with whatever standard mechanisms (IP routers, switches, etc.) are required to perform the IP routing functions.

5.2 CN Related Device Specifications

5.2.1 Packet Formats

The general format of CN packets which are tunneled over the IP channel are those packets that are received from or sent to the Link layer (layer 2) of the CN protocol stack. Refer to Annex A (ANSI/CEA-709.1-D Normative) and Annex C (CEA-600 Normative) for a precise specification of the packet formats corresponding to specific CN protocols. Link layer packets are called LPDU's in the OSI protocol stack formalism.

5.2.2 Addressing Schemes

Different CN protocols generally use different addressing schemes to exchange packets. Although it is generally not necessary to understand the contents of a CN packet or its addresses in order to tunnel CN packets over IP, some aspects of the CN addressing scheme are reflected in the process of configuration. This is especially true when it comes to setting up the IP channels that are used for tunneling. Since CN protocols use different addressing schemes the terminology used in the main body of this specification for describing addresses are meant to be general and rich enough to describe the superset of addressing schemes used in all CN protocols. The following CN addressing terms are used in this specification.

- Unique ID. This refers to an ID that is globally unique to all devices within a specific protocol. Unique ID's are generally fixed in nature in that they never change through the life of a device.
- Domain. This is the highest level of a three level hierarchical addressing scheme. Domain ID's should be unique within a particular network. This means that in a particular network where Domain is used if two devices have the same Domain ID they belong to the same Domain. Domain ID's are generally logical in nature and can be changed and configured.
- Subnet. This is the middle level of a three level hierarchical addressing scheme. Subnet ID's should be unique within a particular domain. This means that in a particular network where subnet ID's are used if two devices have the same Domain ID and the same Subnet ID then they belong to the same Subnet. Some CNs does not use Domains in which case the Subnet may be the highest level of address for a device. Subnet ID's are generally logical in nature and can be changed and configured.
- Node. This is the lowest level of any hierarchical addressing scheme. Node ID's should be unique within a particular Subnet. No two devices within the same subnet should have the same Node ID. Node ID's are generally logical in nature and can be changed and configured.
- Group. Groups are an orthogonal addressing scheme to the hierarchical Domain/Subnet/Node triplet just described. Groups are used to allow multi-casting of messages. Some CNs may not support group addresses and even those that do will have

different rules for how they relate to the other addressing schemes. These considerations are not relevant to this specification.

The definitions above are fairly general and are provided as a guideline for how to map specific CN protocols to these terms. In general how the various addressing schemes work within a CN protocol is not relevant to this specification. It is only necessary to know what the various addressing terms refer to.

Of special note is how these addresses are used for routing within a particular CN protocol. Some CN protocols support more routing functions than others. This is relevant because one of the optional configuration packets that can be exchanged include routing information. For those CN protocols that do not support routing this message may simply not be supported or the addresses specified within the message appropriately limited.

For each CN protocol supported in this specification a table is given in the appropriate appendix that specifies how the appropriate addresses used in that protocol map to the terms given above.

6 IP Channel Specification

IP channels are not like typical CN channels that currently exist. Typical CN channels are physical busses by nature. This implies that all devices on the channel will by default receive all packets transmitted on that channel. In addition when a new device is added to the channel it is not necessary that other devices on the channel become aware of it before they can exchange packets. To transmit a packet on a channel it is only necessary that a device be capable of physically transmitting the packet on the channel, nothing more. If a device is simply physically connected to a channel it is capable of exchanging packets with other devices on the channel.

By contrast an IP channel is not physical, but logical in nature. There are a number of different physical media that can support IP communications and any of them should be capable of supporting a CN channel. Because we are dealing with a logical channel it is necessary to “construct” the channel by informing each device on the channel of the existence of the other devices on that channel. In other words before a device can transmit a packet to some other device on an IP channel it must be made aware of how to specifically send a packet to that device, i.e. it’s IP address.

Another significant difference between physical and logical channels is that in the case of typical physical channels it is possible to calculate fixed upper bounds on the length of time it will take a packet to traverse from one device to another once the packet is transmitted on the channel. This is not always possible for IP networks. The deviation of packet delivery times between CN devices on an IP channel are much higher than those experienced with typical CN channels.

As depicted in Figure 1 the IP channel is used as an intermediary transport mechanism for the CN packets by a variety of CN/IP devices. When a CN packet is transported on an IP channel, an IP message encapsulating the CN packets is sent to other CN/IP devices on that IP channel. On reception of one of the IP messages by a CN/IP device the CN packets are extracted and processed. A single IP message may contain more than one CN packet. Therefore the IP messages must be formatted in such a way to allow the extraction of the individual CN packets. This is referred to a packet “aggregation”. CN/IP devices MUST support the reception of bunched packets. Likewise the aggregation MUST be done in such a fashion that each CN packet contained within a bunched IP message is complete, i.e. CN packets should not cross IP message boundaries as a result of aggregation. It is also a requirement that intermediate IP devices be capable of unbundling bunched CN packets and aggregating them in a different manner before forwarding them.

The IP channel is specified by the list of unique pairs. Each pair consists of a uni-cast IP host address and a uni-cast port, with exactly one pair for each CN/IP device. Multiple devices may share the same host address but must have different ports. Conversely, multiple devices may all

use the same port but must have different host addresses. Unfortunately, in the original specification the channel routing request packet did not include a field for the uni-cast port only the host address. Consequently, 852 channels with devices and/or servers that implement the original specification have the limitation that no two devices with the same host address may be on the same 852 channel even if they have different ports. This limitation has been removed in revision A of the specification. The updated channel routing request packet includes a uni-cast port field. There is no maximum to the number of CN/IP devices on a single IP channel.

If every CN/IP device on an IP channel contained a list of uni-cast IP addresses for every other CN/IP device on that IP channel, this is all that would be required to enable the tunneling of CN packets. In the most brute force approach, for each CN packet to be forwarded on the IP channel a separate uni-cast IP message could be sent to each CN/IP device in the channel. This does not scale very well, so the following techniques will be used to reduce the IP traffic:

- IP Multi-cast groups.
- Selective forwarding.

IP multi-cast groups allow a single IP message to be sent to more than one CN/IP device. Therefore a complete definition of CN/IP channel should contain not only the uni-cast IP addresses of all the CN/IP devices on the channel but also the IP multi-cast groups to which they belong. Each CN/IP device can belong to up to 32 multi-cast addresses.

Selective forwarding refers to examining the contents of the CN packet before forwarding it to determine if it should be sent to a particular CN/IP device. In order to do this additional CN specific information must be known about each potential destination. If the CN/IP device is a router then the information necessary to perform selective forwarding is the routing tables of the CN/IP router. If the device is simply a node then the domain, subnet, node ID, unique ID, and CN groups that the node belongs to should be known. Therefore all of this information is also part of a complete IP channel definition. In short, a complete IP channel definition contains all known information that may be relevant to the forwarding of packets to the other CN/IP devices in the IP channel. It is the universe of all relevant knowledge about the IP channel.

It is important that whatever forwarding scheme is used by CN/IP device the following conditions are always true:

1. CN protocol packets are always received by all CN/IP devices on the IP channel that need to receive them regardless of whether they are routers or nodes. If there is any ambiguity or uncertainty concerning which CN/IP devices should receive a CN packet then that packet may or may not be discarded depending upon specific implementation considerations of the device. The device may either forward the packet to all devices on the channel or it may simply discard it and not forward it to any.
2. A specific CN packet should never be transmitted twice to the same CN/IP device unless it is because of some retry mechanism above the link layer of the CN protocol stack. Due to the nature of IP networks it may happen that a CN/IP device may receive duplicate IP messages, but this should never be the result of the message being transmitted more than once from another CN/IP device.

In addition selective forwarding can be performed on multi-cast groups if the groups were formed based upon some criteria. For example multi-cast group 'A' may contain all CN/IP devices belonging to domain ID 'W'. If a CN packet is destined for domain 'W' then it would be sufficient to forward it only to multi-cast group 'A'. In order to perform the selective forwarding on multi-cast addresses it is necessary to know if these groups were formed based upon some criteria.

In recognition of the fact that the complete IP channel definition can be unwieldy to use and maintain it is not a requirement that CN/IP device use it to forward packets. An alternative data structure called the "Send List" can be maintained within each CN/IP device. The Send List may

contain both uni-cast and multi-cast addresses and is subject to the same conditions given above. It can be created and loaded into the CN/IP device with third party configuration tools that are better suited to creating multi-cast groups based upon some criteria. The Send List represents the minimum amount of information required to allow proper forwarding of CN packets and is structured to simplify the forwarding process such that the CN/IP device need only forward packets to every address (uni-cast or multi-cast) in the Send List. In order to allow CN/IP device to blindly forward packets to each address in the list the following conditions must be true:

1. CN protocol packets MUST be received by all CN/IP devices that need to receive them regardless of whether they are routers or nodes (same as above).
2. A specific CN packet is never transmitted twice to the same CN/IP device (same as above).
3. If device A is a destination in device B's Send List then device B should be a destination in device A's Send List. This is necessary to support the Acknowledged service of the CN protocol.

It should be possible to perform simple forms of selective forwarding using the Send List by associating characteristics with the multi-cast entries in the list.

In general it is important to note that the IP channel definition represents complete global information about the IP channel while the Send List is derived and may result from an intelligent grouping of devices based upon some characteristic. The Send List's main purpose is to allow fairly efficient operation of CN/IP devices without requiring them to do extensive processing of the complete channel definition list. It is also important to note that the Send List is a configured property of CN/IP device meaning that it is controlled and input to a device through some explicit configuration process. Although the Send List is a configured property it does not preclude CN/IP device from doing self-configuration and calculating its own Send List.

In order to have tight controls over the behavior of CN/IP devices and how they forward packets it SHOULD be possible to configure CN/IP device to use an explicit Send List and ignore any IP channel configuration information it may have.

6.1 IP Transport Mechanisms

IP is a Network level protocol as shown in Figure 2. It is designed to operate over a wide range of Physical media and Link layer protocols. As such this document does not specify anything about the Link or Physical layers of the IP stack.

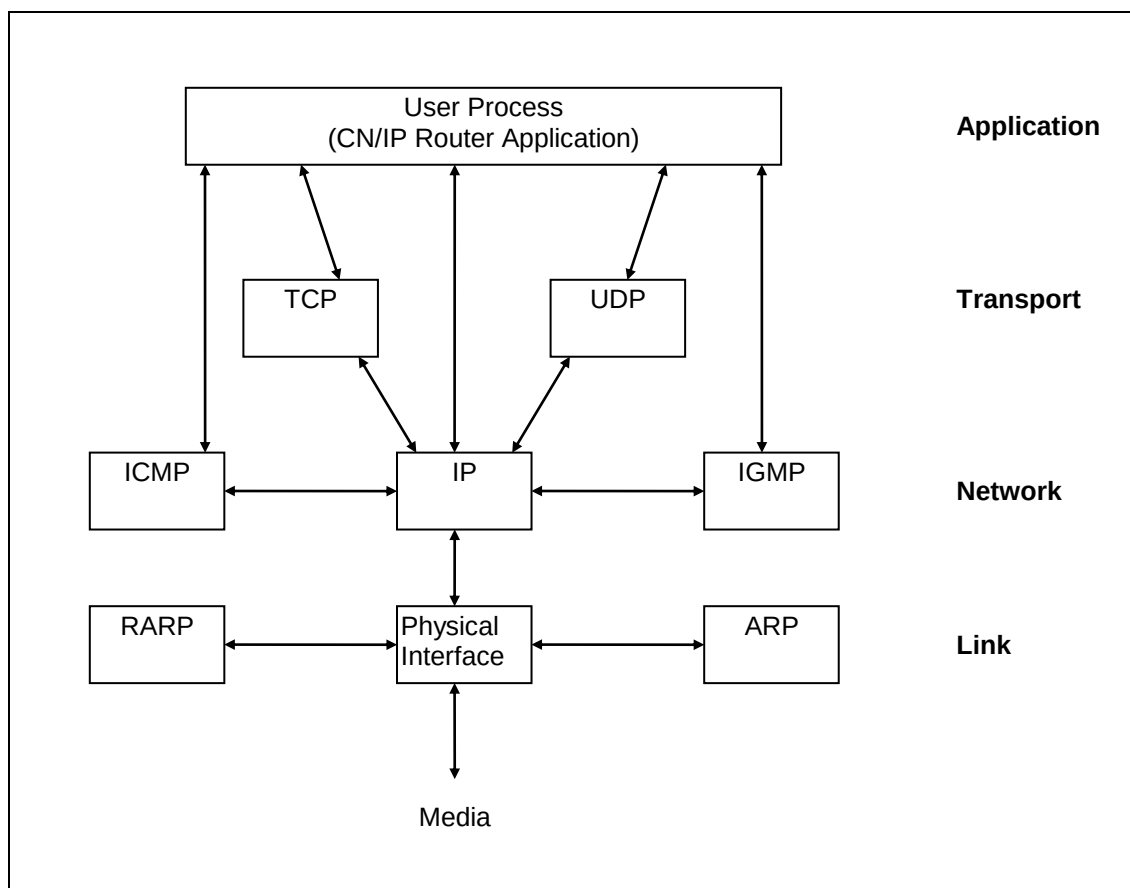


Figure 2 IP Protocol Stack

As depicted in Figure 2 the three most common mechanisms used to transport IP packets are the following:

- Raw IP
- TCP
- UDP

TCP (refer to RFC 793 [9.]) and UDP (refer to RFC 768 [8.]) are transport protocols built on top of IP (refer to RFC 791 [7.]). Given the increased efficiencies of UDP regarding the transport of CN data messages and its support of multi-cast addressing, it will be used to communicate between CN/IP devices. All CN/IP devices **MUST** support UDP. TCP has some advantages for use in the configuration process and **MAY** be supported for certain types of messages in addition to UDP. TCP support in CN/IP devices is **OPTIONAL**.

To address the sequencing issue there will be a sequence number added to the header of packets to help in sequencing them. All UDP datagrams **MUST** be transmitted with valid checksums.

In order to send a packet via TCP/UDP it is necessary to define a port number in addition to the IP address. In general port numbers are configurable and will be used for different purposes as defined below.

Refer to Annex B (Informative) and Annex D (Informative) for recommendations on port number to use for ANSI/CEA-709.1-D and CEA-600 respectively.

Using UDP, datagrams can be sent using either uni-cast or multi-cast addressing. Uni-cast is point-to-point meaning that a datagram is sent from one IP host to a single other IP host. It is much more efficient to use multi-cast addressing when sending the same datagram to multiple IP hosts. Therefore it is RECOMMENDED that CN/IP devices support both uni-cast and multi-cast IP addressing. Recall that an IP channel is defined by a list of IP addresses. A channel definition or Send List can contain any combination of uni-cast and multi-cast addresses. It is not required that CN/IP device support multi-cast in order to inter-operate with CN/IP device that does.

In order for CN/IP router to use multi-cast addressing across IP routers it will be necessary for the CN/IP device to inform the IP router of its intention to join the multi-cast group. There are well-established methods for doing this and it is beyond the scope of this document to specify how it is done. The reader should consult RFC 1112 [1.].

6.1.1 Informative Considerations

Some IP networks contain NAT routers. These routers cannot handle protocols which embed IP addresses in their payloads unless they are specifically designed to do so. The same will be true of the tunneling protocol specified in this document. In general this protocol will not work across NAT routers. The protocol can still be used in a network that uses NAT routers, as long there exists a router that is capable of handling this protocol. That could either be the NAT router itself or another CN/IP to CN/IP router that sits in the same area of the network as the NAT router. A CN/IP router can work through a NAT router if the CN/IP router is given the static IP WAN address of the NAT router as an additional item of configuration data. The NAT router must also support port mapping. The CN/IP port must be mapped so that packets addressed to that port are forwarded by the NAT router to the CN/IP router. The CN/IP router must substitute the static IP WAN address of the NAT router in its own IP uni-cast address field in its Registration Packet, channel routing packet, and channel membership list packet. As a result, other devices in the 852 channel will act as if the CN/IP router is located at its NAT router's WAN address.

7 CN/IP Device Configuration

The CN/IP device has a dual personality. From a CN point of view, it is a CN node on a CN channel and has all such characteristics. These parameters can be configured and managed using the standard CN network management procedures and messages.

From the IP point of view, the CN/IP device is an IP host on an IP network and thus has to be configured like any other host on an IP network.

In addition, there is configuration information that defines the logical IP channel associated with that CN/IP device.

This section describes only those elements relevant to configuring the IP host and IP channel parameters.

In general all IP host and channel parameters will be configurable using a number of techniques and protocols. As a minimum all CN/IP devices MUST support manual configuration of the forwarding mechanism for that device in order to guarantee a minimum level of interoperability between devices that may be configured in different ways. By forwarding we mean the act of tunneling as described above to the other devices on the IP channel.

7.1 Configuration Parameters

This section identifies the parameters that a CN/IP uses (or may use) to operate. This section is not intended to define the data structures used to store the information or define the messages that are used to exchange them. Its only purpose is to have a consolidated section in which all the parameters of a CN/IP device are identified and defined. Subsections discuss mechanisms for communicating this information between devices.