ARINC SPECIFICATION 8XX
TABLE OF CONTENTS

APPENDICES

1.0 INTRODUCTION

1.1 Purpose

ARINC 485 Part 2 defined a low-speed serial communications interface between Electronic equipment in the passenger seat. Its design focused on obtaining status from in-seat electronic equipment.

Cabin Equipment has evolved from the very simple to quite sophisticated systems. The resulting communications needs have surpassed the ability of ARINC 485 to provide the necessary data capacity and response times.

This document specifies the Cabin Equipment Network Bus utilizing a new, serial communications protocol based on IEEE 802.3bw operating at 100 Mbps and utilizing a single twisted pair wire.

1.2 Applicable Documents

ARINC Specification 485: *Cabin Equipment Interfaces Part 1, Head End Equipment Protocol*

ARINC Specification 628: *Cabin Equipment Interfaces Part 1, Cabin Management and Entertainment System - Peripherals*

ARINC Specification 628: *Cabin Equipment Interfaces Part 2, Cabin Management and Entertainment System – Seat Interfaces*

ARINC Specification 628: *Cabin Equipment Interfaces Part 3, In-Flight Entertainment System (IFES) to Aircraft Systems Interfaces*

ARINC Specification 628: *Cabin Equipment Interfaces Part 4A, Cabin Management and Entertainment System - Cabin Distribution System – Daisy Chain*

ARINC Specification 628: *Cabin Equipment Interfaces Part 4B, Cabin Management and Entertainment System - Cabin Distribution System – Daisy Chain*

ARINC Specification 628: *Cabin Equipment Interfaces Part 9, Cabin Interface Network (CIN)*

IEEE 802-2014*: IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture*

IEEE 802.3-2012*: IEEE Standard for Ethernet*

IEEE 802.3bw-2015: Physical Layer Specifications and Management Parameters for 100 Mb/s Operation over a Single Balanced Twisted Pair Cable (100BASE-T1)

TIA/EIA-485: *Standard for Electrical Characteristics of Generators and Receivers for use in Balanced Digital Multipoint Systems*

TIA/ EIA Telecommunications System Bulletin TSB 89: *Application Guideline for TIA/EIA-485-A*

1.3 Scope

This document .

2.0 BUS ARCHITECTURE / PHYSICAL LAYER

An IEEE 802.3bw network link consists of two network interfaces and the twisted pair interconnect wires between them. Communications between the nodes over the link is full duplex (both nodes can transmit at the same time). Each network interface must have a transformer and PHY as Illustrated in Figure 2.1.

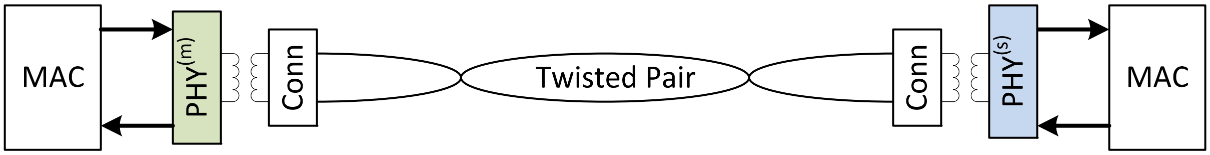

Figure 2.1 – Physical Layer

While the 100BaseT1 standard calls out unshielded twisted pair wire, it is common in the aircraft industry to utilize shielded twisted pair due to the more stringent emissions containment required in a commercial aircraft.

Larger networks are constructed out of multiple network links with nodes providing packet forwarding according to the rules applicable to each network layer.

2.1.1 Master/Slave Relationship

The PHYs support full duplex communications using a technique called Echo Cancellation. In principle, each node subtracts the signal it is transmitting from the signal it is receiving with the result of the subtraction being the signal from the distant node. The IEEE 802.3bw specification calls for one PHY on a link to be set up as MASTER and the PHY on the other side must be set up as SLAVE. The specification indicates that operation is undefined if both sides of a link are the same (MASTER or SLAVE).

COMMENTARY

While initially this requirement to choose whether a node connection is a MASTER or SLAVE appears complex and vulnerable to error, in actual applications, there seems to rarely be any ambiguity in the choice. If you pick one node to be the Bridge to a higher level network and you establish an upstream/downstream relationship between all network nodes with the bridge node the upstream connection, then an upstream node on a link is the MASTER and the downstream node on a link is the SLAVE.

2.2 Generic Network

Multiple nodes can be combined into an extended network by utilizing components called network switches that receive and retransmit messages based on the addressing rules appropriate for the protocol layer in which they operate.

Four types of network nodes can exist:

- Endpoint Node (one port)
- Relay Node (two ports)
- Star Node (more than two ports)
- Bridge Node (connects two independent networks)

These nodes can be combined in a large number of ways to construct a complete private network. In addition this private network can be connected to a larger network.

2.2.1 Two-Node Network

The simplest network consists of two End-Point nodes with a network link between them as illustrated in Figure 2.2. In such a network, one of the End Point nodes will be designated a master and the other must be designated a slave (see Master/Slave Relationship).

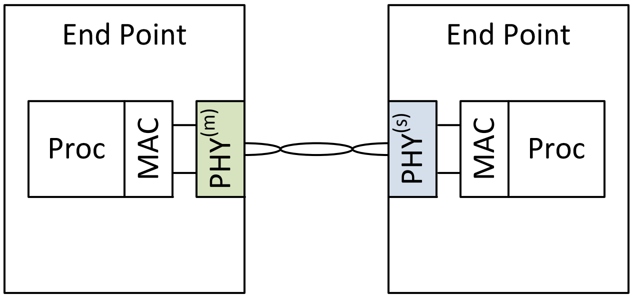

Figure 2-2 Simple One-Link with Two Endpoints

2.2.2 Three-Node Network

The next level of network sophistication is a three-node network where one of the network nodes must perform a relay function between two endpoint nodes as illustrated in Figure 2.3. In this configuration, a Relay node

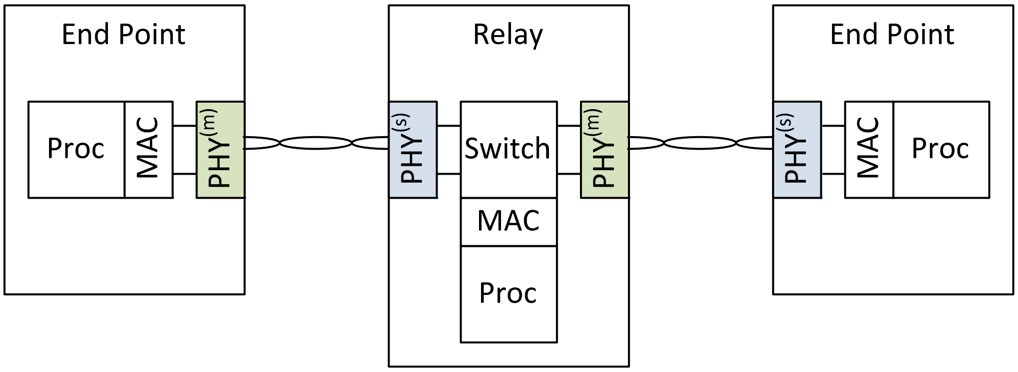

Figure 2.3 Three Node Network: Relay with two End-Points

2.2.3 Four Node Networks

As more nodes are added, the variety of potential interconnect strategies, increases as well. One way in which the network can be expanded is to add additional relay nodes as illustrated in Figure 2.4a. This architecture requires all intermediate connections to be relay nodes.

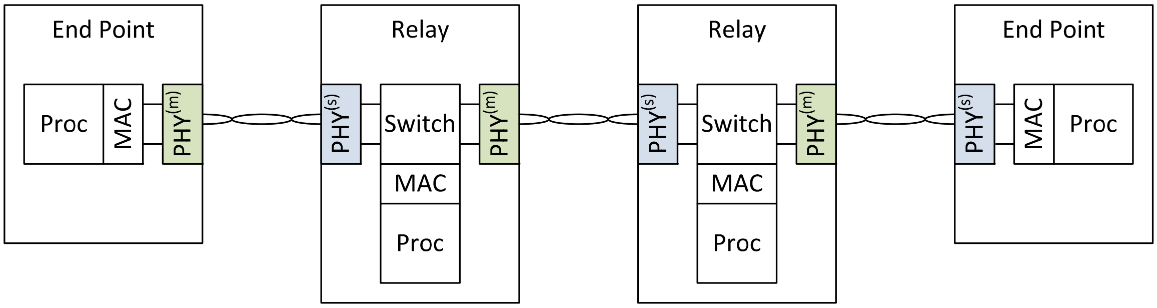

Figure 2.4a Four Node Network: Two Relay and Two End-points

An alternate approach can be used by introducing a Start Node into the architecture. As illustrated in Figure 2.4b. This architecture requires a slightly more sophisticated intermediate connection (the Star Node) but permits all other nodes to be simple end-points.

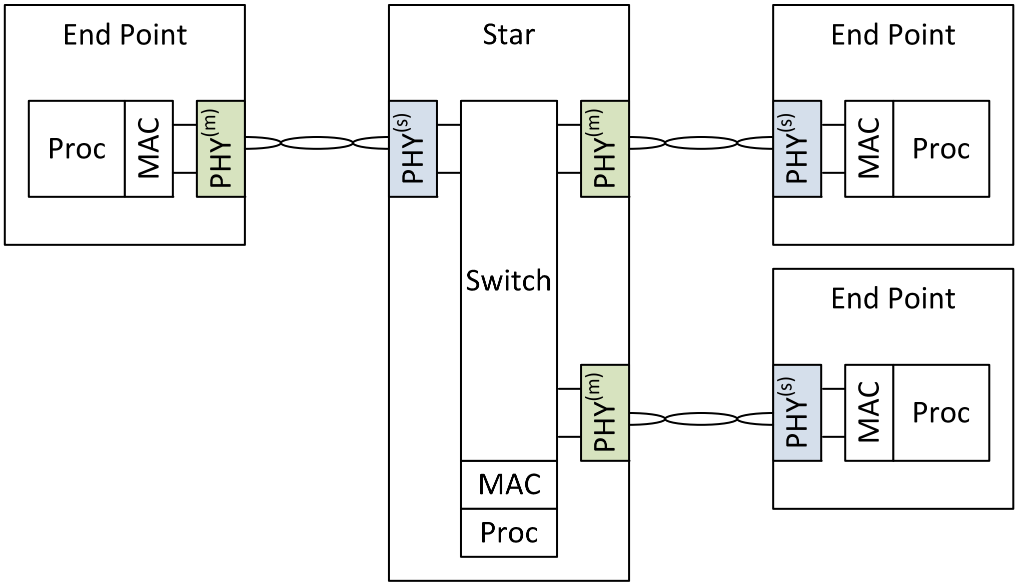

Figure 2.4b Four Node Network: Three End-Points and one Star

2.2.4 Bridge

In an application like a Cabin System, the local private network may in fact be part of a bigger system. In such an application, one of the nodes may need to be a network bridge between the local private network and the larger system network. In addition, it is often desirable to limit the amount of traffic and to restrict the interaction between the large network and the local private network. In figure 2.5, such a configuration is illustrated using a Bridge Node between a larger network (using 4-TP Gigabit Ethernet in the example) and the local network.

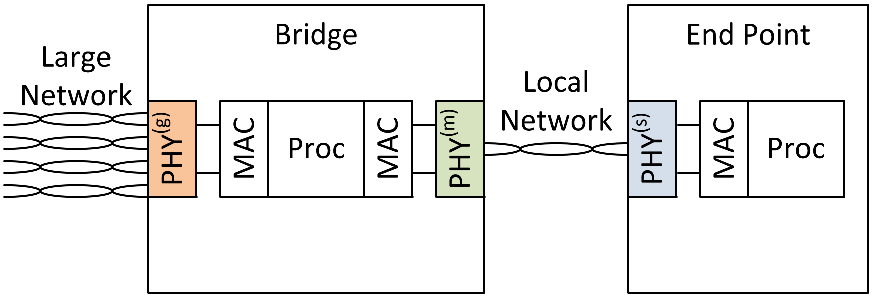

Figure 2.5 Two Node network with Bridge Node to Larger Network

2.3 Application to Passenger Seat

With the types of network nodes defined, we can look at a specific application of this network. The architecture illustrated in Figure 2.6 shows an SVD functioning as a Bridge Node between the more global cabin network (4-TP Gigabit Ethernet) and the local seat network. In this example, the local network consists of the SVD (bridge node), an SPB (star node), an ECU/SAC (relay node), a PCU, (end-point) and an LC (end-point).

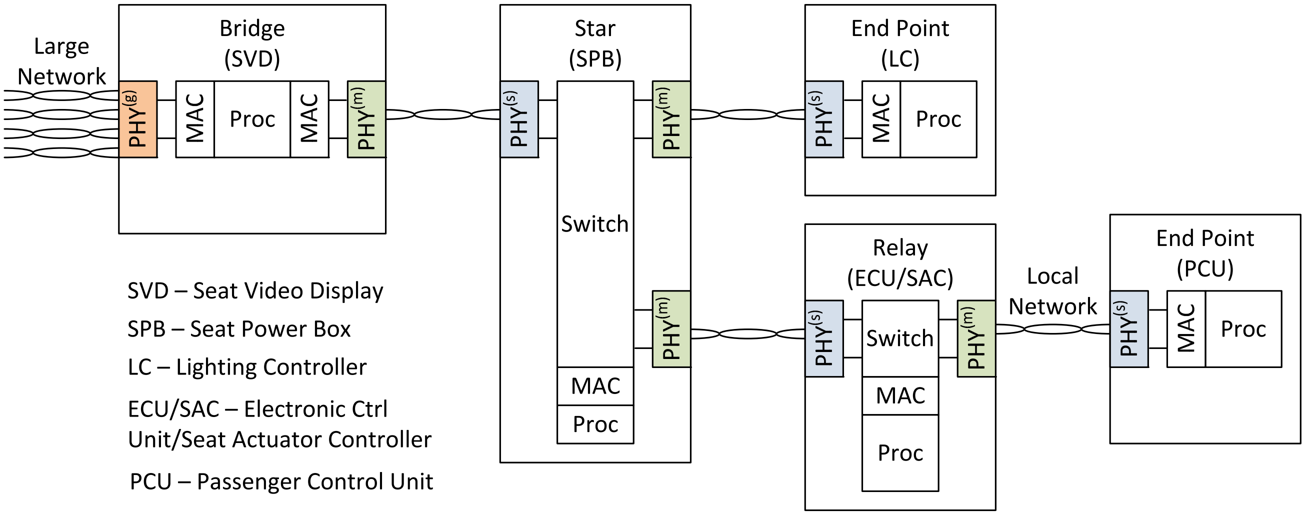

Figure 2.6 Complex Seat Application

3.0 BUS PROTOCOL LAYERS

The IEEE 802 / IETF protocol layers selected for the Cabin Network Bus are identified in this section. The details of the various formats and fields are contained in the specifications referenced.

In most instances, developers of equipment that uses the Cabin Network Bus do not have to deal with the details of the protocols identified herein. The network protocol stack selected by each supplier should provide the assembly and encapsulation described in this section.

The material contained herein is to provide a general overview of the protocols and the way in which they are layered to provide communications. These protocols are capable of supporting a wide range of options and it is highly desirable that the Cabin Network bus be kept as simple as at all practical. To that end, this section is also intended to reduce the number of options that need to be accommodated by each network node.

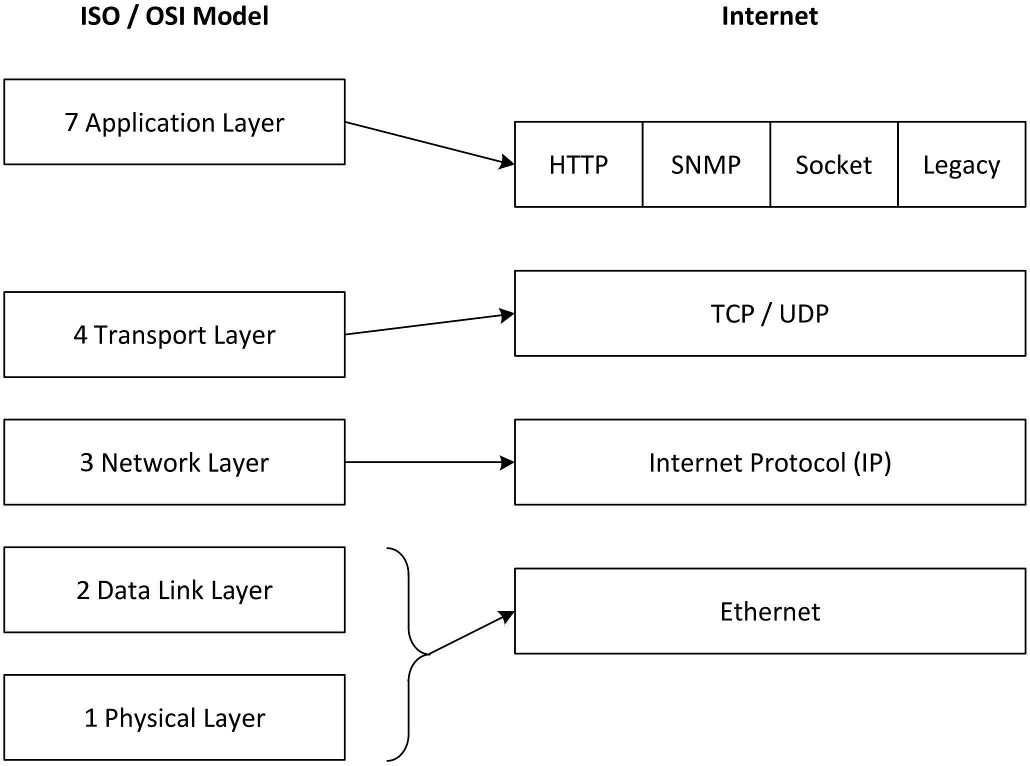

Figure 3.1 – Bus Protocol Layers

The way in which data from the various layers is assembled into a compete Maximum Transmission Unit (MTU) is illustrated in Figure 3.x. Application data (layer 7) is passed as data to the Transport Layer (layer 4), where the header for the selected protocol is added and the assembly is passed to the next layer down in the stack. Each layer adds the header (and tail if appropriate) as the packet is assembled.

3.0 BUS PROTOCOL LAYERS

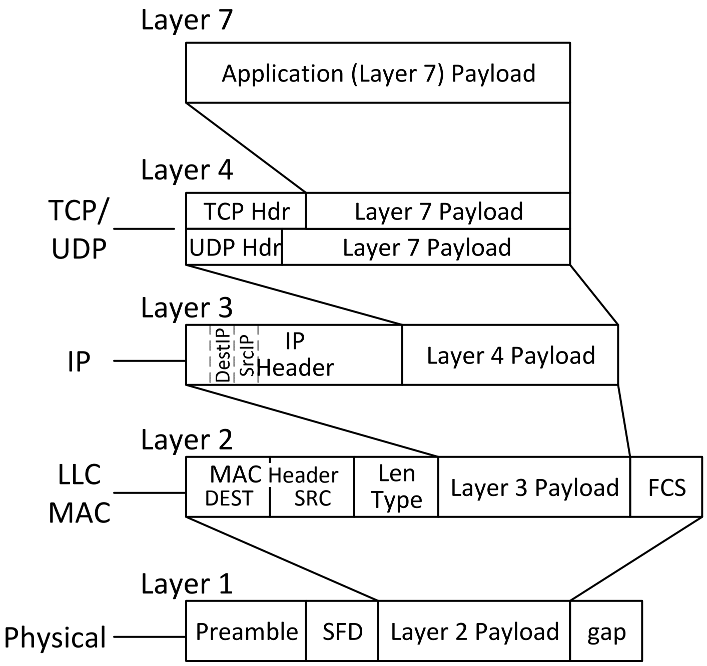

Figure 3.x – Layer by Layer Encapsulation into an MTU

An MTU is not necessarily a complete message. Messages of arbitrary size can be handled as the application layer divides the message into appropriate sized payload packets and passes it into the protocol stack. When packets are received they are reassembled by Layers 1-4 to reflect the original message.

3.1 Physical Layer (OSI Layer 1)

The Physical Layer of the network is covered by section 2, Bus Architecture.

3.2 Data Link Layer (OSI Layer 2)

The Data Link Layer of 802.3-2012 provides node-to-node transfer of data over the physical layer. The Data Link Layer (DLL) described in IEEE 802.3-2012 contains two sublayers:

- Media Access Control (MAC)
- Logical Link Control (LLC)

The Data Link Layer handles link setup, divides data into frames, and handles DLL level integrity verification and acknowledgement.

The packet/frame format for the Data Link Layer is illustrated in Figure 3.1

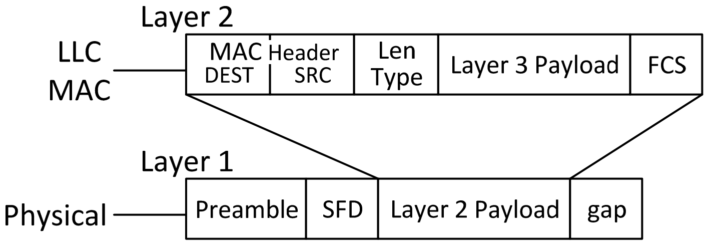

Figure 3.1 – Physical and Data Link Layer Framing

3.2.1 Media Access Control (MAC)

The Media Access Control (MAC) sublayer is identified in IEEE 802-2014 and further details are specified in IEEE 802.3-2012. Essentially, the MAC sublayer is responsible for the following:

- Data Encapsulation (transmit and receive)
  - Framing (frame boundary delimitation, frame synchronization
  - Addressing (handling of source and destination address)
  - Error Detection (detection of physical medium transmission errors)
- Media Access Management
  - Medium Allocation (collision avoidance)
  - Contention Resolution (collision handling)

Since the Cabin Bus is full duplex, Media Access Management is not required.

3.2.1.1 Packet Framing

The header associated with the MAC layer is illustrated in Figure 3.x. Each packet to be transmitted to the network has the MAC header added as well as a Frame Check Sequence (FCS) added to the end of the packet. The MAC header contains the physical source and destination MAC addresses which is used to properly route the packet though the physical network. The FCS is used to verify the integrity of each packet. If the Frame Check fails on the receipt of a packet, the packet should be discarded.

The introduction of Virtual Private Network (VPN) routing in IEEE 802.1Q complicated the MAC layer and the routing associated with it. Virtual network Tags are used to restrict the routing of packets through a network. One use of VPN tags is to prevent network conflicts when there is a loop in the network architecture (such as with redundancy). Since the physical routing of packets is affected by VPNs, the MAC header is different depending on whether VPN routing is used or not. Figure 3.x illustrates the MAC header both with and without IEEE 802.1Q.

The Cabin Network Bus will not support IEEE 802.1Q.

Media Access Control (MAC) Frame without 802.11Q Tag

		0								1								2								3							
	Octet	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
MAC w/o Q	0	Dest MAC Address (MSBs)																															
	4	Dest MAC Address (LSBs)																Source MAC Address (MSBs)															
	8	Source MAC Address (LSBs)																															
	10	Ether Type / Len (LSBs)																No Data															

Media Access Control (MAC) Frame with 802.11Q Tag (Not Used by Cabin Network Bus)

		0								1								2								3							
	Octet	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
MAC wQ	0	Dest MAC Address (MSBs)																															
	4	Dest MAC Address (LSBs)																Source MAC Address (MSBs)															
	8	Source MAC Address (LSBs)																															
	12	0x8100 (802.1Q taged Frame)																802.1Q Tag LSBs (optional)															
	14	Ether Type / Len (LSBs)																No Data															

Figure 3.x - MAC Layer Header Format

This header is added to the front of the payload from Layer 3, a Frame Check Sequence is added, and the resulting data stream is passed onto the physical layer to be sent across the network. Figure 3.x illustrates the way in which the headers and check values are assembled into a complete packet.

		0								1								2								3							
	Octet	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
E’net	0	Preamble																															
	4	Preamble (cont)																								Start Frame Delimiter							
MAC	0	Dest MAC Address (MSBs)																															
	4	Dest MAC Address (LSBs)																Source MAC Address (MSBs)															
	8	Source MAC Address (LSBs)																															
	10	Ether Type / Len (LSBs)																No Data															
	0-n	Layer 3 Payload																															
E’net	n+4	Frame Check Sequence																															
	n+8 - n+20	InterPacket Gap (12 octets)																															

3.x – Complete MAC Layer Packet

3.2.1.2 Media Access Control (MAC) Address

The Layer 2 address or Media Access Control or MAC address is sometimes called the Ethernet hardware address or physical address as every Ethernet interface node ever made is to have a unique value. An Ethernet MAC address consists of 48 bits and is commonly expressed by 6 hexadecimal octets. For example, “3A:25:B2:00:1F:DC” is how a MAC address would be presented.

To avoid any the potential for duplicate MAC addresses, the industry has appointed the IEEE-Standards Association as an administration agency for assigning blocks of addresses to equipment manufacturers. It is left to the equipment manufacturers to assign MAC addresses within their block and to ensure there are no duplicates.

Manufacturers of equipment to be placed on any Ethernet network must obtain a block of addresses from the IEEE. Information on the procedure for obtaining MAC address blocks is available from the following IEEE website:

http://standards.ieee.org/develop/regauth/grpmac/

Once a manufacturer has its block of MAC addresses, it is the obligation of the manufacturer to avoid any duplications. Should a duplicate MAC address appear in any network, the performance of the entire network may be seriously degraded.

3.2.1.3 Media Access Control (MAC) Channel Access

The Media Access Control (MAC) Channel access method for 100BaseT1 is full-duplex (no contention on the media).

3.2.2 Logical Link Control (LLC)

The Logical Link Control sublayer is primarily responsible for multiplexing different protocols and is not used (null) for the Cabin Equipment Network Bus.

3.3 Network Layer (OSI Layer 3)

It is undesirable for the potentially large volume of unrelated traffic to appear on a Cabin Equipment Network Bus. It is desirable for each Cabin Equipment Network Bus to be isolated from large cabin networks and each other with communications between Cabin Equipment Network bus and more extensive busses or between Cabin Equipment Network Busses to be limited and managed by Bridge/Router nodes.

The Network Layer for the Cabin Equipment Network Bus is Internet Protocol Version 4 (IPv4). Furthermore, each Cabin Equipment Network bus is an isolated private network consistent with RFC 1918.

COMMENTARY

> Note that an IFE Cabin Network is also an isolated private network in accordance with RFC 1918 as well but using a different address range. The Cabin IP Address Scheme is specified in ARINC 628 Part 9 attachment 4

The format of an IPv4 frame is to encapsulate the layer 4 payload with an IP header and pass it on as Layer 3 payload to the Layer 2. The IP header contains a source IP address (the address of the node originating the message) destination IP address (the address of the node to which the message is intended or an address indicating how the message is to be distributed). The basic format of an IP frame is illustrated in Figure 3.x. The basic format of an IPv4 Header is illustrated in Figure 3.x with the definition of the various fields contained in RFC 791.

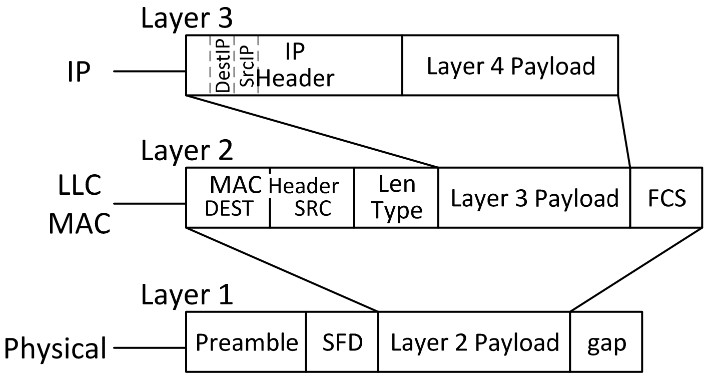

Figure 3.x – IPv4 Framing

		0								1								2								3							
	Octet	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
IPv4	0	Ver=4				IHL=4				Service Type								Total Length															
	4	Identification																Flags			Fragment Offset												
	8	TTL								Protocol								Header Checksum															
	12	Source IP Address																															
	16	Destination IP Address																															

(note: IP Header Length, IHL is assumed to be 4 for this application)

Figure 3.x IPv4 Header Format

3.3.1 Internet Protocol Addressing

IPv4 addresses consist of 32-bit addresses and are most often expressed in “dot decimal” notation which consists of 4 octets in decimal format with period/dot separator. For example:

Hexidecimal address: 0xC0A8ED05 = 192.168.237.5 in IPv4 address format

3.3.1.1 Cabin Equipment Network Bus Address Range

In accordance with RFC1918, nodes on the Cabin Equipment Network Bus are assigned addresses in the address space: 192.168.237.x or 192.168.237.0/24. The netmask applied for components on this bus is 255.255.255.0 (appropriate for the /24 address space).

3.3.1.2 Cabin Equipment Network Bus Address Assignments

A Cabin Equipment Network Bus is a relatively small, fixed network with a very static configuration. Most of the nodes on the Cabin Equipment Network Bus are simple devices which should not be encumbered with unnecessary or inappropriate network complexity. Any change to the network would require wiring changes and the appropriate level of certification oversight. The nodes on the network should be known and fixed when assembled and installed on the aircraft and the network should identify and flag any changes as potential security breaches.

Simplicity, fixed configuration, and consistency with the principles established by the predecessor to this network in ARINC 628 Part 2 have resulted in the declaration this network uses fixed IP addressing. This means that the Cabin Equipment Network Bus will not provide any dynamic IP address assignment services such as Dynamic Host Configuration Protocol (DHCP) RFC 2131.

In principle, each type of network node is assigned a small range in the Bus address space. Normally, the lowest number address is the default. If a network has more than one LRU of the same type (which would cause a conflict if both use the default address) a simple differentiation method (such as a pin-programmed discrete) will be used to indicate a specific unit is to use a non-default address.

Table 3.1 IP Address Assignments for Seat Network Application

LRU	IP Address	Note/Comment
SVD (default)	192.168.237.241	Bridge/Router between cabin network and seat network (0xF1)
SVD#2	192.168.237.242	(.241 - .254 reserved for SVDs)
SPB (default)	192.168.237.33	(0x21)
SPB#2	192.168.237.34	(.33 – .41 reserved for SPB)
SAC (default)	192.168.237.1	(0x01)
SAC#2	192.168.237.2	(.1 - .7 reserved for ECU/SAC
LCM (default)	192.168.237.49	(0x31)
LCM#2	192.168.237.50	(.49-.57 reserved for LCM)
PCU (default)	192.168.237.17	(0x11)
PCU#2	192.168.237.18	(.17 - .25 reserved for PCUs)
IDM (default)	192.168.237.65	(0x41)
IDM#2	192.168.237.66	(.65 - .73 reserved for IDMs)

SVD – Seat Video Display

SPB – Seat Power Box

SAC – Seat Actuator Controller, Electronic Control Unit (ECU)

LCM – Lighting Control Module

IDM – Information Display Module

3.3.1.3   Other IPv4 Addresses

Several Additional IPv4 Addresses are relevant to nodes on the Cabin Equipment Network Bus.

- Broadcast Address: 255.255.255.255 is used for any message that originates from one node and is to go to all nodes on the network.
- Loopback Address: 127.0.0.0 is used by nodes to send messages to themselves.
- Multicast Address as specified in RFC 5771 may be applicable to the Cabin Equipment Network Bus. These include the address range 224.x.x.x and 232.x.x.x.

3.3.2 Address Mapping

At layer 2, packets are routed using the MAC address. A message sent from one node places its MAC address in the Source MAC Address field of the header and a destination MAC address is used to specify the destination node. Layer 2 routing provides for the message to get to the appropriate destination.

We have established fixed IP addresses for the nodes on private Cabin Network Bus but we have said equipment manufacturers must obtain a block of MAC addresses from the IEEE and assign complete and unique MAC addresses to their equipment. In the Cabin Network Bus, there is a one to one correlation between the physical address (MAC address) of a node and the IP address. (Note: in other network applications, a physical MAC address might correspond to multiple device IP addresses). A network protocol called Address Recognition Protocol (ARP) as defined in RFC 826 should be implemented in each node to permit it to discover the physical to IP address translation for each of the nodes on the network.

At layer 3, packets are routed using the Internet Protocol or IP address. The Cabin Network Bus utilizes IPv4 so the 32-bit addresses established above are used. At even higher levels of the protocol stack, names (usually referred to as Host Names) may be assigned to network devices. Utilizing names provides for one more layer of abstraction from the using program to the physical hardware, nodes, and connections. Names can be assigned in a number of different ways and may not be assigned at all.

While individual network nodes may internally utilize a Host Name to IP address translation service, the Cabin Network bus will not provide a centralized translation service such as Domain Name System (DNS).

3.4 Transport Layer (OSI Layer 4)

When a transport layer packet is passed to the network layer, an number is passed identifying the transport protocol. This number is placed in the “Protocol” field of the IP packet identified above. The protocol numbers were originally assigned in RFC 790 but due to the dynamic nature of protocol development a working list is maintained by the Internet Numbers Assigned Authority. The protocols anticipated for use on the Cabin Equipment Network Bus have been established for a long time and their protocol number should not change.

While there are a variety of Transport Layer protocols available, at a minimum nodes on the Cabin Equipment Network Bus should support the following transport layer protocols:

- User Datagram Protocol (UDP) number 0x11 from RFC 768
- Transport Control Protocol (TCP) number 0x06 from RFC 793
- Internet Control Message Protocol (ICMP) number 0x01 from RFC 792

Since it is anticipated that most message traffic will be point to with message integrity verification desired, TCP is the most likely protocol to be used on a wide basis.

Other Transport Layer protocols that might be relevant in the future but which are not currently identified as applicable on this bus are as follows:

- Internet Group Management Protocol (IGMP) number 0x02 from RFC 1112

3.4.1 User Datagram Protocol (UDP)

User Datagram Protocol (UDP) is often used where error checking and correction are either not necessary or is performed at higher levels in the protocol stack. Time-Sensitive applications favor UDP as dropping packets is often favorable to the complexities of retransmission delay, out-of-order arrival, etc. Multicast and broadcast traffic utilizes UDP as the destination IP address does not represent a single network node.

The basic characteristics of User Datagram Protocol (UDP) are contained in RFC 768. The format of the UDP header is illustrated in Figure 3.x.

	0								1								2								3							
Octet	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	Source Port																Destination Port															
4	Length																Checksum															

Figure 3.x - UDP Header Format

		0	1	2	3
	Octet	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31
E'net	0	Preamble			
	4	Preamble (cont)			Start Frame Delimiter
MAC	0	Dest MAC Address (MSBs)			
	4	Dest MAC Address (LSBs)		Source MAC Address (MSBs)	
	8	Source MAC Address (LSBs)			
	10	Ether Type / Len (LSBs)		No Data	
IPv4	0	Ver=4 IHL=4	Service Type	Total Length	
	4	Identification		Flags Fragment Offset	
	8	TTL	Protocol	Header Checksum	
	12	Source IP Address			
	16	Destination IP Address			
UDP	0	Source Port		Destination Port	
	4	Length		Checksum	
App	0 - n	Application Data			
E'net	n+4	Frame Check Sequence			
	n+8 - n+20	InterPacket Gap (12 octets)			

3.x – Complete UDP Packet

3.4.2 Transport Control Protocol (TCP)

The basic characteristics of Transport Control Protocol (TCP) are contained in RFC 793. A number of adaptions and features have occurred to TCP and are documented in other RFCs. The basic format of the TCP header from RFC 793 are illustrated in Figure 3.x.

	0	1	2	3
Octet	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31
0	Source Port		Destination Port	
4	Sequence Number			
8	Acknowledgment Number			
12	Offset Rsvd	Flags	Window	
16	Checksum		Urgent Pointer	
20	Options			Padding

Figure 3.x - TCP Header Format

		0								1								2								3							
	Octet	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
E'net	0	Preamble																															
	4	Preamble (cont)																								Start Frame Delimiter							
MAC	0	Dest MAC Address (MSBs)																															
	4	Dest MAC Address (LSBs)																Source MAC Address (MSBs)															
	8	Source MAC Address (LSBs)																															
	10	Ether Type / Len (LSBs)																No Data															
IPv4	0	Ver=4				IHL=4				Service Type								Total Length															
	4	Identification																Flags			Fragment Offset												
	8	TTL								Protocol								Header Checksum															
	12	Source IP Address																															
	16	Destination IP Address																															
TCP	0	Source Port																Destination Port															
	4	Sequence Number																															
	8	Acknowledgment Number																															
	12	Offset				Rsvd						Flags						Window															
	16	Checksum																Urgent Pointer															
	20	Options																								Padding							
App	0 - n	Application Data																															
E'net	n+4	Frame Check Sequence																															
	n+8 - n+20	InterPacket Gap (12 octets)																															

Figure 3.x - Complete TCP Packet

3.4.3 Internet Control Message Protocol (ICMP)

The basic characteristics of Internet Control Message Protocol (ICMP) are contained in RFC 792. The basic format of the ICMP header from RFC 792 is illustrated in Figure 3.x.

3.0 BUS PROTOCOL LAYERS

<table>
<tr><td></td><td></td><td colspan="8">0</td><td colspan="8">1</td><td colspan="8">2</td><td colspan="8">3</td></tr>
<tr><td></td><td>Octet</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td rowspan="3">ICMP</td><td>0</td><td colspan="8">Type</td><td colspan="8">Code</td><td colspan="16">Header Checksum</td></tr>
<tr><td>4</td><td colspan="32">Rest of Header</td></tr>
<tr><td>8 - n</td><td colspan="32">Data (optional)</td></tr>
</table>

Figure 3.x – ICMP Header Format

<table>
<tr><td></td><td></td><td colspan="8">0</td><td colspan="8">1</td><td colspan="8">2</td><td colspan="8">3</td></tr>
<tr><td></td><td>Octet</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td rowspan="2">E’net</td><td>0</td><td colspan="32">Preamble</td></tr>
<tr><td>4</td><td colspan="24">Preamble (cont)</td><td colspan="8">Start Frame Delimiter</td></tr>
<tr><td rowspan="4">MAC w/o Q</td><td>0</td><td colspan="32">Dest MAC Address (MSBs)</td></tr>
<tr><td>4</td><td colspan="16">Dest MAC Address (LSBs)</td><td colspan="16">Source MAC Address (MSBs)</td></tr>
<tr><td>8</td><td colspan="32">Source MAC Address (LSBs)</td></tr>
<tr><td>10</td><td colspan="16">Ether Type / Len (LSBs)</td><td colspan="16">No Data</td></tr>
<tr><td rowspan="5">IPv4</td><td>0</td><td colspan="4">Ver=4</td><td colspan="4">IHL=4</td><td colspan="8">Service Type</td><td colspan="16">Total Length</td></tr>
<tr><td>4</td><td colspan="16">Identification</td><td colspan="3">Flags</td><td colspan="13">Fragment Offset</td></tr>
<tr><td>8</td><td colspan="8">TTL</td><td colspan="8">Protocol</td><td colspan="16">Header Checksum</td></tr>
<tr><td>12</td><td colspan="32">Source IP Address</td></tr>
<tr><td>16</td><td colspan="32">Destination IP Address</td></tr>
<tr><td rowspan="3">ICMP</td><td>0</td><td colspan="8">Type</td><td colspan="8">Code</td><td colspan="16">Header Checksum</td></tr>
<tr><td>4</td><td colspan="32">Rest of Header</td></tr>
<tr><td>8 - n</td><td colspan="32">Data (optional)</td></tr>
<tr><td rowspan="2">E’net</td><td>n</td><td colspan="32">Frame Check Sequence</td></tr>
<tr><td>n+1
-
n+3</td><td colspan="32">InterPacket Gap (12 octets)</td></tr>
</table>

Figure 3.x – Complete ICMP Packet

4.0 APPLICATION LAYER

APPENDIX A ACRONYMS

ACK	Acknowledgement
CDS	Cabin Distribution System
CFR	LRU Configuration Request
DSRQ	Download Status Request
DRQ	Download Request
DC	Download Complete
DS	Download Start
ECU	Electronic Control Unit
EIA	Electronic Industry Association
ELC	Error Log Clear
ELR	Error Log Request
ICD	Interface Control Document
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFES	In-Flight Entertainment System
ISPSU	In-Seat Power Supply Unit
LRU	Line Replaceable Unit
NAK	Negative-Acknowledgement
NVM	Non Volatile Memory
OPS	Operational Software
PAC	Power Actuator Control
PAR	Power Actuator Response
PCS	Power Control State
PCU	Passenger Control Unit
PDU	Protocol Data Unit
PUS	Power Up Status
SAC	Seat Actuator Controller
SACS	Seat Actuator Controller System
SAE	Society of Automotive Engineers
SEB	Seat Electronics Box
SFC	Seat Functions
SFR	Seat Functions Response
SPB	Seat Power box
SVU	Seat Video Unit
TIA	Telecommunications Industry Association

APPENDIX B TBD

APPENDIX C LRU DOWNLOAD

C-1