White Paper Contributed to AVnu Alliance ™

Requirements for Automotive AVB System Profiles

3/15/2011

Author
Junichi Takeuchi, Renesas

Contributor
Hideki Goto, Shinichi Iiyama, Takumi Nomura, Toyota
Hajime Kosugi, NEC Engineering
Michael Johas Teener, Yong Kim, Broadcom

Executive Summary

The IEEE 802.1 Audio/Video Bridging (AVB) standards will enable time-synchronized low latency streaming services through 802 networks, ensuring interoperability between devices using the AVB specifications through a system profile called 802.1BA. Automotive applications, such as infotainment and drivers assistance, can deploy those specifications for an in-vehicle high bandwidth, synchronized network, as discussed in AVnu White Paper, AVB for Automotive Use, July 20, 2009. This paper presents automotive system profiles for general streaming applications as well as critical control applications, discussing basic profiles, additional network management, acknowledge and retry, and a low latency method.

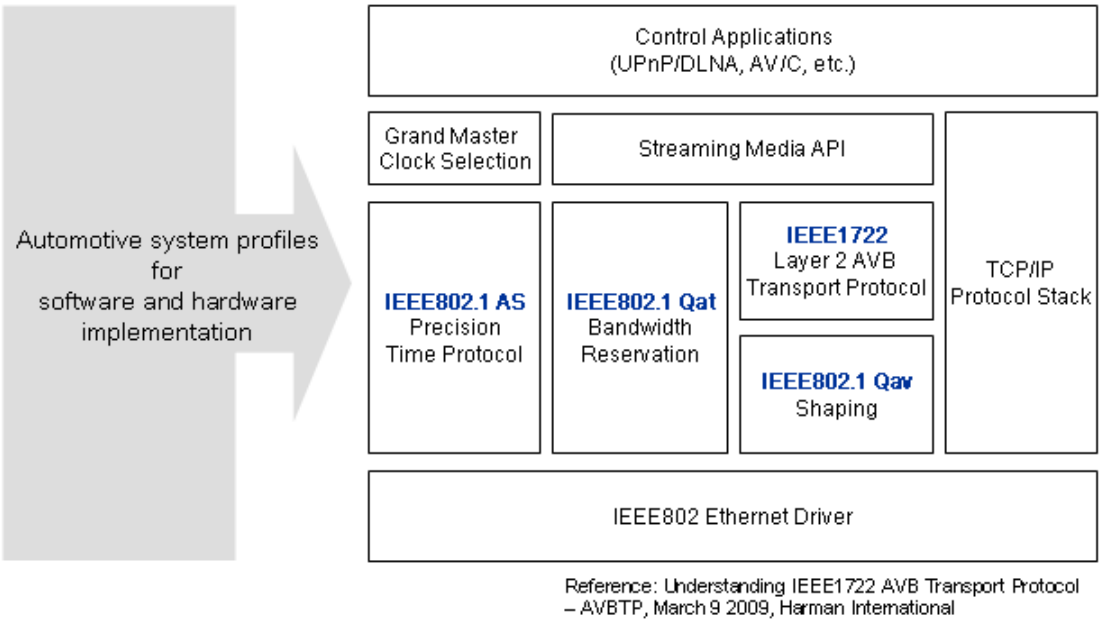


Figure 1. Automotive system profiles and IEEE802.1 AVB

Assumptions

The automotive system profiles in this paper are discussed under the following assumptions and goals.

1. The AVB network supports both automotive multimedia applications and critical control applications.
2. Critical control applications send and receive messages which require fault-tolerant, low-latency communication.
3. There will be no more than 32 endpoints in an automotive network.
4. There will be no more than 7 switch hops in any path taken by reserved streams.
5. The maximum cable length is 24m. The maximum total aggregate end-to-end cable length in a network is 30m.
6. The most time-sensitive applications use Class A streaming, which has a 125µs class measurement interval. Class B, which has a 250µs class measurement interval, also can be used for lower priority streaming. There are best effort frames using the lowest priority.
7. Maximum end-to-end delay for Class A streaming needs to be less than 100us for the cases where it is used for critical control applications (AVB guarantees 2ms for Class A, as default).
8. Maximum network recovery time needs to be less than 100ms, for the cases where it is used for critical control applications. Recovery time is measured from the detection of a failure event to the time that the network is ready to transmit data from applications.

Contents

1. Basics network requirements and profiles

1-1. Standards: 802.1AS, Qat, Qav, BA, and 1722, 1722.1

Automotive Ethernet AVB products comply with the base standards in **Table 1**, although some products might not use all these specifications, selecting some subsets based on the requirements of the target system. On the other hand, some products might add additional specifications discussed in this paper for converged network systems, or critical control systems.

Table 1. Standards for automotive Ethernet AVB

Abbreviation	name	comments
802.1AS	Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks	- Specified by The Audio/Video Bridging Task Group - All approved IEEE Standards
802.1Qat	Stream Reservation Protocol	
802.1Qav	Forwarding and Queuing Enhancements for Time-Sensitive Streams	
802.1BA	Audio Video Bridging (AVB) Systems	- System profiles that are common to any application - In progress
1722	Layer 2 Transport Protocol for Time Sensitive Applications in a Bridged Local Area Network	- Stream packet format - Approved IEEE Standard
1722.1	Device Discovery, Enumeration, Connection Management & Control Protocol for 1722 based devices	- In progress

1-2. Setup and Operational procedures

While one of the advantages of Ethernet is a simple configuration, which enables data transmissions without complicated network settings, there are a few parameters that must be set either by users during initialization procedures (if the network configuration can be altered) or by the manufacturers (if the network configuration is semi-static or fixed).

Another advantage is Plug-and-Play, but the system doesn't necessarily have to use the dynamic configuration default, because automotive network is a provisioned network, and electronic control units (ECU) in an end-point usually have pre-determined functions. The network could operate using default settings, and could optimize some of the settings during system initialization.

Grand Master selection

The best master clock algorithm in 802.1AS determines the grand master and constructs a time-synchronization spanning tree with the grandmaster as root. In this process, time-aware systems send best master selection information to each other by using Announce messages, which contains a priority vector with some attributes specified in 802.1AS. Developers should provide electronic units with appropriate attributes such as system type priority, clock class, clock accuracy, or time source of the system, referring to 802.1AS standard.

For example, central gateway unit is usually the first one to startup among ECUs in the entire in-vehicle network, and also last one to shutdown. It tends to be the first priority and highest quality unit. There is another higher priority unit, yet less than central gateway unit, and it is head unit including GPS, which is a main source of information for drivers. Then, the central gateway should have the highest priority value used for the grand master selection process, and the head unit should have the second highest value.

System management with 1722.1

The protocols in 1722.1 are complementary to other AVB standards and profiles, since 1722.1 specifies an application-level connection procedure for the AVB network system. It includes 1) Service Discovery process, in which a 1722.1 controller identifies other 1722.1-capable nodes, 2) Enumeration process to find capabilities of the nodes, 3) Connection Management to connect and disconnect virtual links between media sources and media sinks, and 4) Control protocol. The first three functions can be bypassed for pre-configured networks where the configuration will not change, such as in a typical automotive application. The control protocol is very simple, yet easily extended to support industry-specific command sets such as those needed for automotive control and sensing applications.

IEEE 1722.1, although requiring only simple layer 2 protocols (not using TCP/IP), is also designed to be optionally carried on TCP/IP networks using familiar HTTP protocols. 1722.1 suggests that all “controller” devices be capable of performing a simple IP proxy function so that pure IP-only devices on the network can still participate in device discovery, enumeration, and control.

1-3. General Security procedure

Ethernet LAN Security Requirements (trusted network)

Ethernet technology is well-known in the industry, and securing the network from hacking and un-authorized access is required. The best security practices from the IT industry are adoptable to in-vehicle network with the same effectiveness. The general concept is to protect the network infrastructure and control access at the edge (i.e. the first switch connection from the end-point). The cost-benefit balance will be maintained by protecting the network access for various use cases.

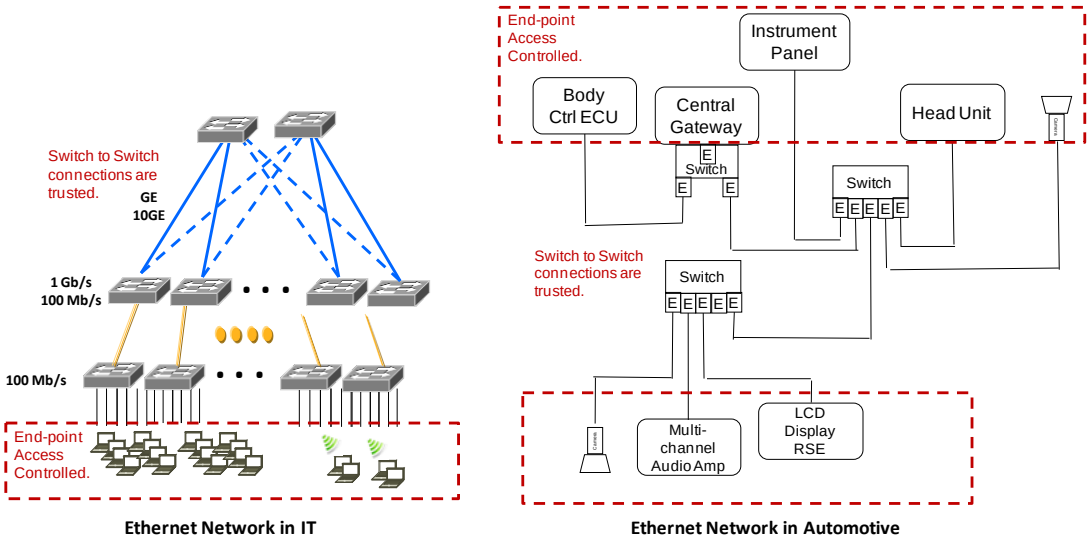


Figure 2. Ethernet network comparison (trusted network)

Many features are available within IEEE 802.1Q Bridge implementations to provide LAN access security methods, and some of these are described in Appendix A.

1-4. Network application: Multimedia example

By selecting some of the AVB standards described in the previous sections, a high-speed automotive network can be implemented. Here, we discuss application-related functions rather than network functions, in order to show how an automotive network can benefit from 802.1 AS and 1722.

Audio and Video Lip-Sync

One of the key advantages of Ethernet AVB is providing all media synchronization in its native form, with a transport protocol that provides presentation time to the application layer such that real-time synchronized rendering, i.e. “lip-sync” can be achieved. Because AVB provides the network time accurate to 1μ sec anywhere in a network, presentation time carried in a transport protocol can be honored by all media renderers in a network. A detailed example of this use of presentation time in AVB network is in Appendix B.

Summary

There are multitude of network-enabled in-vehicle Ethernet use that can be serviced with IEEE 802.1, IEEE 802.3, and IEEE 1722 standards that provide professional quality streaming, precision time synchronization in Ethernet, and related transport protocols. The use cases include vehicular multi-media, driver-assist camera and displays, and consumer owned portable content integration. There are a few further requirements that helps to harden the use of Ethernet AVB to meet the all of the vehicular backbone requirements. These are discussed in the next section.

2. Additional requirements for Critical control and Converged backbone network

2-1. Fail-safe systems and Quick recovery

RSTP with quick recovery

Some control applications need redundant paths for fail-safe capability of the network. With Rapid Spanning Tree protocol (RSTP) in IEEE802.1Q, physical mesh network or ring network will be configured as a logical tree topology. When it detects a fault in a path, the network will be automatically reconfigured so that all nodes can be re-attached to the network by a new logical tree.

There are two performance requirements in RSTP in vehicle use to provide the fastest practical reconfiguration time in case of a link or port failure: Maximum RSTP processing delay and Maximum BPDU transmission delay. The default value of Maximum RSTP processing delay is 1.0 seconds, measured from the occurrence of an external event to the transmission of BPDUs on all ports. The default value of Maximum BPDU transmission delay is 0.2 seconds, measured from internal timer related events to the transmission of all BPDUs on ports. Considering handshake procedures of RSTP, there are several BPDU exchanges in the network to complete a network configuration to a logical tree. The total configuration time depends on the delay values as well as hops in the network, and it could be several seconds.

Automotive systems require a shorter configuration time. Then, it is necessary to implement RSTP referring to a quick version of Maximum RSTP processing delay and Maximum BPDU transmission delay, as in **Table 2** to provision for this goal.

Table 2. Transmission and reception delays (quick version example)

Parameter	Absolute maximum value
Maximum provisioned RSTP processing delay	10.0 ms
Maximum provisioned BPDU transmission delay from a link or port failure detection.	5.0 ms

The values were estimated by using existing Ethernet switch designs with real-time RSTP protocol services. Based on the estimation, it is possible to set RSTP parameters to achieve less than 70ms RSTP recovery time over 7 switch hops when a single link or port

failure occurs. Furthermore, when a designated backup port state is used in a provisioned RSTP network, the failure recovery time is limited to the "Maximum provisioned BPDU transmission delay measured from a link or port failure detection time" of 5 ms in the **Table 2**. Thus, unless the designated root bridge itself fails, the recovery time for any single failure is limited to this 5 ms if every bridge that requires quick recovery uses Alternate backup port (**Figure 3**).

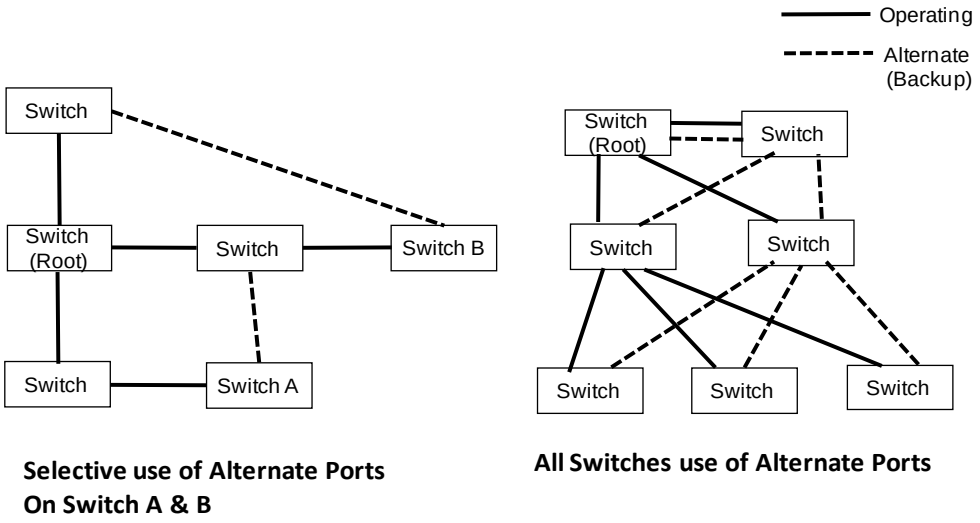


Figure 3. Use of alternate ports

RSTP Root selection

An RSTP root selection process only occurs when RSTP is implemented as discussed in the previous section. Each bridge has a bridge ID, which consists of 16 priority bits and 48bit MAC address. The smallest bridge ID will be the root of the network. The time for configuration is affected by the position of the root in a network. By knowing all the bridge IDs in a network, it is possible to calculate the startup and recovery time quite accurately.

End-point failure discovery

When RSTP detects an error in its active spanning tree, it changes the logical tree by using other paths in the physical network. However, a trouble at end-point cannot be detected by RSTP.

In order to learn the status of connection between end-point and switch, Link Layer Discovery Protocol specified in 802.1AB, Station and Media Access Control Connectivity Discovery, can be used. It defines frame format for multicast initiated by end-point, and by using the frame, end-point can send its system information to the adjacent node. It is possible to set an appropriate cycle time for the frame transmission according to the system requirements. Yet, alternatively, the 1722.1 "heartbeat" protocol can be used to check on endpoint operation as a byproduct of using 1722.1 for control.

2-2. Acknowledge and Retry

It is each node's responsibility to avoid a buffer overflow for Class A streaming by managing the reservation. On the other hand, lower class data can be dropped due to interference and queuing. In order to avoid data loss of lower classes, developers can use TCP/IP just above the AVB protocol layer. However, since TCP/IP is still costly for some low cost units, defining a simple confirmation procedure is suggested.

The procedure doesn't require a sophisticated function like the sequence handling in TCP/IP, or definition of several acknowledge types in IEEE1394. The target node returns acknowledge frame to the sender node, by notifying the frame has been received (**Figure 4**). If there is no acknowledge returned, or bridging node returns an acknowledge frame indicating an error, the sender retries the frame that was send before receiving an acknowledge frame.

This Acknowledge and Retry procedure is designed for a single Ethernet packet, not streaming, since it assumes to be used for automotive control frames such as CAN. If a system needs more sophisticated version of acknowledge process, such as streaming management, it should use TCP/IP, or other confirmation methods.

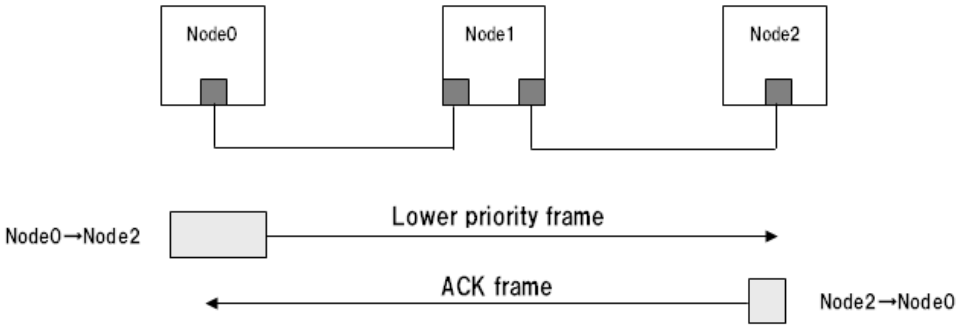


Figure 4. Acknowledge process

2-3. AVB automotive Frame definition

Automotive systems can use 1722 AVTP frame format for streaming applications, including the 61883 subtype within AVTP. While, as discussed in this chapter, 802.1 AVB can also be used for critical control applications, which leads us to define additional frame formats. Currently, it is necessary to define frames for Acknowledge and Retry, and frames for encapsulating packets from other automotive network such as CAN.

Acknowledge and Retry, and CAN

A new frame format for fault-tolerant network management such as Acknowledge and Retry for vehicular control should be defined within a header following a new 1722 subtype. In addition, to allow for vehicular Ethernet backbone usage, with a message transport to Ethernet from other existing networks such as CAN, it is necessary to request an assignment of a new Ethertype from IEEE and related transport standard to be developed.

2-4. Smaller Frame size for low latency

One of the unique requirements from in-vehicle network systems is a “small maximum delay” from a sender to target. For example, CAN takes a bus architecture, and the physical transmission delay from node to node is far smaller than 1ms. Since the default 802.1 AVB’s maximum delay is 2ms, it cannot be used for CAN data bridging.

As a solution, the most of a switch delay is caused by “storing time” of receiving frame and “waiting time” against the preceding frame, and it is possible to reduce the storing and waiting time by restricting the maximum frame length. **Table 3** shows the result of the calculation of the total end-to-end delay value, depending on the frame length varying 128 bytes, 256 bytes, and 1500 bytes. In this calculation, Ethernet Link rate and talker-to-listener hops are also taken into account as variables. If the frame length is 256 bytes, then total maximum delay is under 500us for 100Mbps link, and under 100us for 1Gbps link.

Table 4 shows the details of the calculation of the total delay. Reasonable PHY, MAC delays were selected, and there are three unique parameters in switches: storing time, queue/schedule, and interference by one lower priority frame. Storing time is measured from “the time the frame arrived in a switch from MAC” to “the time the entire frame is stored in its switch buffer”, which can be calculated by using a frame length. Queue/schedule is the time for the process of selecting the next frame based on the priority of frames in the switch buffer. Lastly, there is a possibility that a lower-priority frame is departing from the switch right before the queuing is done for a higher-priority frame, and then the higher priority frame needs to wait until the entire lower-priority frame is sent out, which also can be calculated from the length of a frame.

As a conclusion of this study, if the usage of the network includes control signals that require less-than-ms maximum delay, all the nodes should take a restricted smaller maximum frame size such as 258 bytes, as a system requirement. One drawback is that a smaller frame size deteriorates network efficiency because gaps between frames will increase, reducing the available bandwidth for data transmission. As a result, network designers need to make a trade-off carefully, in terms of required total bandwidth in each path, and maximum delay of control signals.

Table 3. Results of delay calculation

(a) Payload length = 128 Bytes

Variables						
Payload length (Bytes)	128	128	128	128	128	128
Link rate (Mbps)	100	100	100	1000	1000	1000
hops	3	5	7	3	5	7
Calculation results						
Total delay (μs)	**114.5**	**172.2**	**229.9**	**16.6**	**25.3**	**34.0**
Max streams (max delay = 100us)	-	-	-	61	55	49

(b) Payload length = 256 Bytes

Variables						
Payload length (Bytes)	256	256	256	256	256	256
Link rate (Mbps)	100	100	100	1000	1000	1000
Hops	3	5	7	3	5	7
Calculation results						
Total delay (μs)	**196.4**	**295.1**	**393.7**	**24.8**	**37.6**	**50.4**
Max streams (max delay = 100us)	-	-	-	32	26	21

(c) Payload length = 1500 Bytes

Variables						
Payload length (Bytes)	1500	1500	1500	1500	1500	1500
Link rate (Mbps)	100	100	100	1000	1000	1000
hops	3	5	7	3	5	7
Calculation results						
Total delay (μs)	**992.6**	**1489.3**	**1986.0**	**104.4**	**157.0**	**209.6**
Max streams (max delay = 100us)	-	-	-	-	-	-

Table 4. Delay calculation example (128 Bytes, 100 Mbps, 7 hops)

Measuring points		Delays (μs)	
End-point node delay (Talker)	Transmitting time		13.6
	MAX TX		0.12
	PHY TX		0.08
Switch node delay	PHY RX	0.2	
	MAX RX	0.24	
	Storing time	13.6	
	Queue/schedule	1	
	MAC TX	0.12	
	PHY TX	0.08	
	Interference by one lower priority frame	13.6	
	Total switch delay	28.84	
Total switch delay with 7 hops			201.88
End-point node delay (Listener)	PHY RX		0.2
	MAC RX		0.24
	Receiving time		13.6
Total cable delay			0.15
Total delay			229.9

2-5. Requirements for ultra-low latency

The smaller frame size option in this paper revealed that it is possible to guarantee the max delay of less than 1ms under certain conditions, which is sufficient for most of the current automotive applications such as multimedia and simple camera network. On the other hand, critical control applications such as driving control require even smaller latency as shown in **Table 5**.

Table 5. Additional requirements for critical control system

Conditions		Requirements
Minimum hops	Cable Link	Maximum Latency
3	100Mbps/1Gbps	100μs

In order to achieve the maximum latency requirement, a new method other than the small frame method needs to be developed.

Conclusion

This paper discussed automotive system profiles using 802.1 AS, Qat, Qav, BA, 1722, and 1722.1, targeting at multimedia applications as well as critical control applications. The profiles include network management, acknowledge and retry, automotive frame format, and a low latency method. A simple multimedia network wouldn't need all of the profiles for implementation, while critical control applications, or a converged network, would need most of them. Regarding requirements for low latency, we have shown the fact that a small frame restriction can reduce the maximum delay, but for critical control applications, still another method needs to be developed.

The next step would be to examine each profile at Technical working group in AVnu, in order to create a specification for interoperability testing, and work with IEEE 802.1 AVB Task Force to help standardize the low latency requirements for critical control applications.

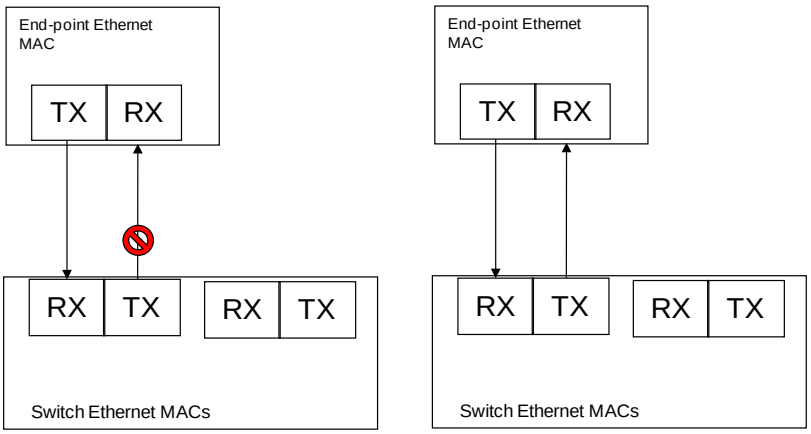
Appendix A. General Security procedure methods and examples

[1] MAC-address Static Entry Table and MAC source address learning enable/disable

Consumer-targeted Ethernet switches (IEEE 802.1 Bridges) and non-secure LAN access is configured with the plug-&-play friendly defaults. When a new device is introduced to the network, switches learn the MAC address and forward frames, thereby allowing network connection to any other nodes. Switches also has ability to lock-down the MAC addresses in a static entries of all known allowed addresses only, and disallow new devices until it is explicitly configured (add new MAC address to the table) to allow network access. This feature could work alone through vehicular management action, or with the Port Access protocol (IEEE 802.1X) to seamlessly integrate end-point access to the network.

[2] Port Access (IEEE 802.1X) Extensible Access Protocol (EAP)

IEEE 802.1X EAP has two components, 1) one explicit port state that allows for transmission of Extensible Access Protocol frame but does not allow receipt of any frames, and 2) a standard secure protocol to allow the upper layer (of authentication method of choice) to authenticate the credentials of an end-point. The new revision of the 802.1X-2010 allows for the stronger authentication method that is managed short-lived session keys, and use of the hardware protected secure device keys (802.1AR). Once authenticated, the port state transitions form EAP state to operating state, thereby allowing network access from the node. Most, if not all, modern Ethernet switch silicon implement this optional port state in support of this feature.



1. Initial State – Link is up, and End-point could send Ethernet packets, i.e. authentication request, but switch does not send any network packets to the End-point.

2. Final State – Link is up, and the Ethernet Switch port is configured to operate normally after authentication.

Figure 5. Access control

[3] Default VLAN as DMZ use

An alternative (or an additional method) to Port Access EAP is to provide default VLAN of in-vehicle switch to be non-operational VLAN value, where any new device connects to the network through the default VLAN awaiting to be configured (assigned) to the proper VLAN. This mode of operation is common called De-Militarized Zone (DMZ) VLAN network. The vehicle management and authenticator connects to this DMZ VLAN network to listen for new devices, authenticate through any preferred means, and then allow for connection by a VLAN assignment and optionally configuring the Static MAC address entry. In addition, amount of network load that is offered onto DMZ VLAN could be limited through the bandwidth limiter built-into most Ethernet switches, so that bandwidth based denial of service could be mitigated.

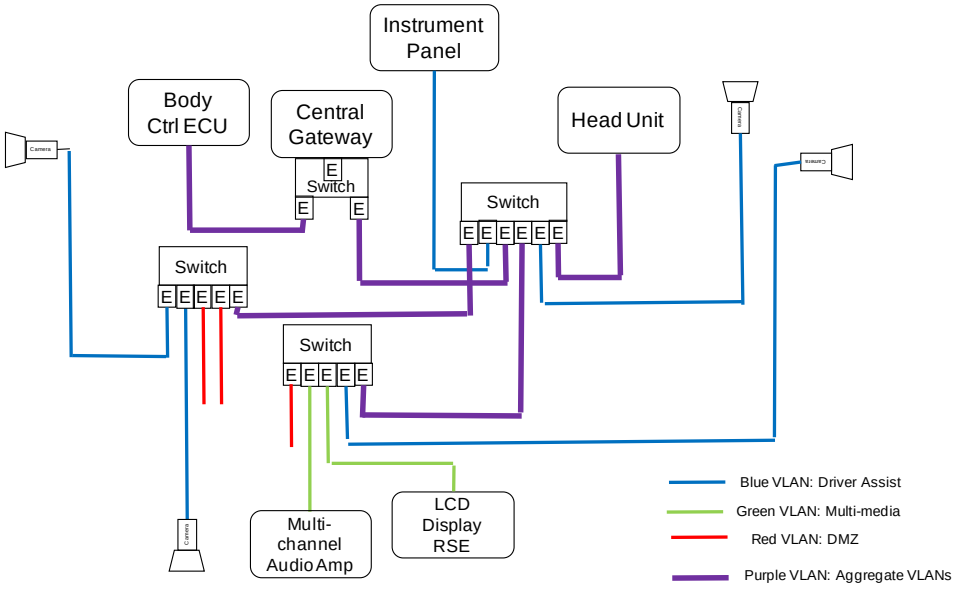


Figure 6. DMZ VLAN network

[4] MAC Security (IEEE 802.1AE with 802.1X)

MAC or Link Security, also known as MACSec, or LinkSec, defined in IEEE 802.1AE and is in use by the most secure LAN application provides frame by frame AES encryption as well as frame by frame authentication, provided by the use of the AES 128 GCM (Galois/Counter mode), protecting data as well as man-in-the-middle replay attacks. MACSec implementations in the Ethernet PHY as well as in the Ethernet Switch are available to be

adopted into most secure in-vehicle application. The AES encryption is a block-cipher and therefore some additional link delay need to be provisioned. The key management for MACSec is reflected in the IEEE 802.1X-2010 revision as published.

[5] IP Routers/Gateway

In cases where consumer-owned portables and smart phones need to communicate to the in-vehicle systems, such as head units and rear-seat entertainment, the IP routers provides additional application-specific access and filtering.

In-Vehicle LAN Security Considerations and Use Cases

There are many layers of security that could be used to secure in-vehicle networks. And the protection should match the value of the network application that it is trying to protect. The consideration should be further given on the level of access that a potential attacker has: WLAN or IP connection without physical access, physical access to an Ethernet connector, physical access to the Ethernet switch, and physical access to the vehicle management ECU. Another consideration is OEM's requirements to give an access, e.g. dealer-installed and authorized option, after-market authorized, and after-market unauthorized.

[1] Non-mission critical use cases

Driver assist and infotainment applications may only need the use of the features that are built-into every Ethernet switch that complies to IEEE 802.1Q standard, i.e. use of the static MAC address, either DMZ VLAN or Port Access PAE, or both, and optional use of the IP routers to connect to the consumer owned portables.

[2] Mission critical use cases

Mission critical use such as vehicle management, could be physically protected, i.e. no easily available connection into the wiring harness, or protect via MACSec in addition to the aforementioned methods.

Appendix B. Audio and Video Lip-Sync example

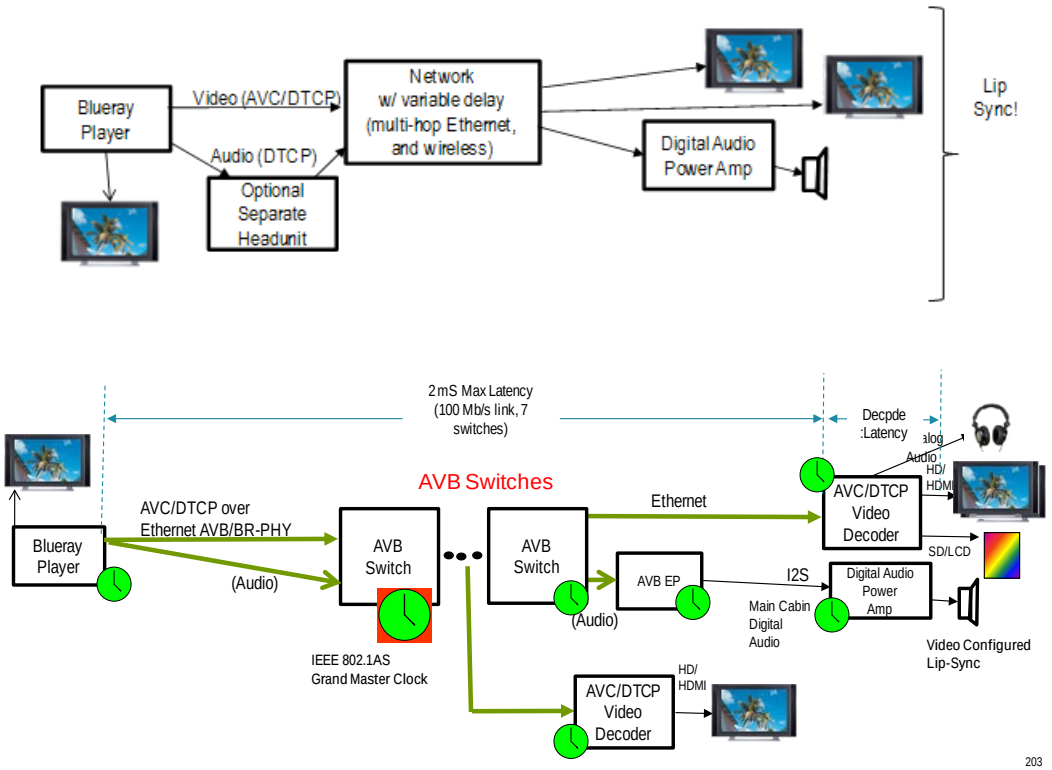


Figure 7. Simplified Data path diagrams

In this example, the Blu-ray video source extracts disc content and it re-encrypts the H.264 compressed content in order to transmit over Ethernet network. AACS licensed use is honored by using DTCP content protection over the network. One Blu-ray source is used to feed multiple HD LCD screens in the car connected by the HDMI cable. A H.264/AVC decoder is connected to each LCD screen, which is connected to the network via the Ethernet port. The screens are all client terminals that are controlled by the content from Blu-ray source. A separate audio data path to the digital audio amplifier is synchronized, through the use of 802.1AS time-sync and honoring the use of presentation time for both video and audio. The video delay is controlled through the video buffer length configuration to match the data path delay in the network and various codec latencies.

Table 6 shows generic implementation latency numbers in the network and how much buffering is needed.

Table 6. Lip-Sync latency and buffering

Worst Case Latency	Video Delay (mS)	Video (sum) mS	V Variability	Audio Delay (mS)	Audio (sum) mS	A Variability
DVD Player	0	0		0		
AACS decrypt		0				
H.264/AVC decode	33	33		33	33	
DTCP encrypt	2	35	0.5	1	34	
Queueing to Ethernet	0.5	35.5	1			
Streaming to I2S (extra audio only)				0.01	34.01	0.01
Audio E/P (I2S => Ethernet)						
I2S receive to Packet				0.01	34.02	0.02
Queuing to Ethernet AVB				0.5	34.52	0.145
Ethernet AVB Switch Delay (7 hops)						
Ingress to Egress latency	1.75	37.25	2.875	1.75	36.27	2.145
* Note: Variability 1~7 switch hops						
Audio E/P (Ethernet => I2S)						
Ethernet => I2S Buffer				0.2	36.47	2.345
Presentation Time Buffer (just for completeness)					36.47	2.345
Audio Buf => I2S				0.01	36.48	2.355
Audio Amp						
I2S => DSP Buffer				0.01	36.49	2.365
DSP Buffer to CL D Amp				0.01	36.5	2.365
Video Decoder						
Ethernet => Buffer	0.2	37.45	3.075			
DTCP decrypt	2	39.45	3.075			
Presentation Time Buffer (just for completeness)		39.45	3.075			
H.264/AVC decode	33	72.45	3.575			
HDCP encode	5	77.45	3.575			
Frame Buf => HDMI	1.2	78.65	3.775			
Transcode SD	0	72.45	3.575			
Frame Buf => Compnent out	0.5	72.95	3.775			

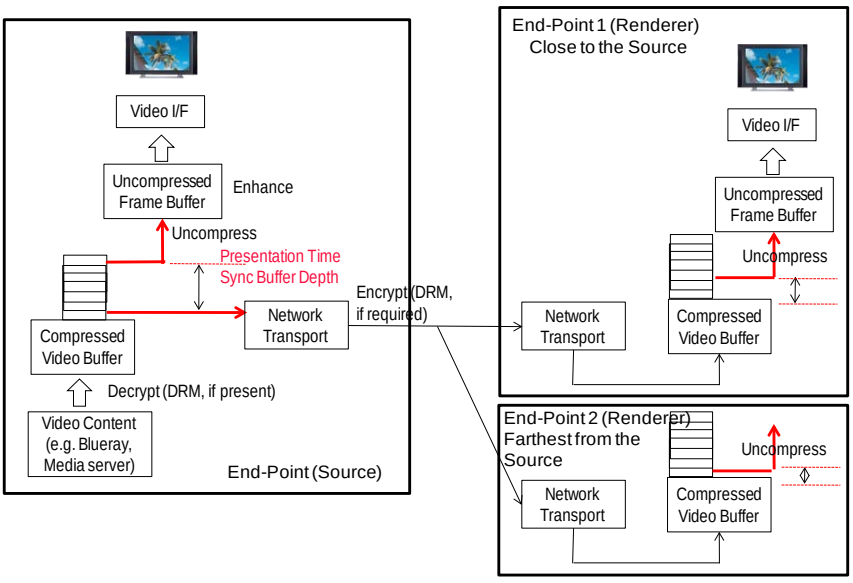


Figure 8. Lip-Sync buffering diagram

Based on generic (and to be firmed up by real implementation numbers) latency analysis, the worst case video decode path is ~78.65 ms, or 74.875~82.425 ms with the latency variability. The audio path includes a number of Ethernet AVB switch hops (1~7 switches) variability is 36.5 ms, or 34.135 ~ 38.865 ms. Thus the maximum provisioned audio buffer must handle 48.29 ms (82.425 – 34.135) audio to video latency differences. For 44.1 KHz, 16 bit stereo, this translates 3.2 KB per audio stream that needs to be synchronized with the compressed video decode. For video, the compressed video buffer requirement is 3.775 ms (5.2 KB @ 11 Mb/s) to meet max/min video delay for the networked video, and the video source (i.e. Blu-ray player) itself requires additional 39.45 ms (54.2 KB @ 11 Mb/s) compressed video buffer.

- Each networked Audio and Video end-point honors presentation time from IEEE 1722 transport protocol, which is mapped to IEEE 802.1AS network clock and locally buffers to meet this presentation time, thereby allowing lip-sync time difference of less than 1μ sec.

- The audio path in all cases needs the deepest time buffer due to its smaller processing delay relative to video, and the (compressed) video buffer only needs to buffer enough to accommodate differential latency among other video display within a network. The amount of buffers required is manageably small (in this example, 5.2 KB for audio, and 54.2 KB for (compressed) video for each device.