ENT-AN1153

MACsec Interoperability Test

January 2014

Microsemi

a Microchip company

Contents

1 Revision History

The revision history describes the changes that were implemented in the document. The changes are listed by revision, starting with the most current publication.

1.1 Revision 1.0

Revision 1.0 was published in January 2014. This was the first publication of the document.

2 Introduction

Microsemi’s dual port VSC8490 family of 10G/1G Ethernet PHYs with Intellisec™ (MACsec) and VeriTime™ (IEEE 1588v2) offer support for timing-critical applications, including all industry-standard protocol encapsulations. Intellisec enables a realistic and affordable Layer 2 MACsec security solution. Intellisec is a patent-pending technology enabling IEEE 802.1AE MACsec encryption end-to-end over any network, including multi-operator and cloud-based networks, independent of the network's awareness of security protocols. Intellisec is not limited to traditional MACsec linkbased box-to-box applications. Likewise, Intellisec scales easily with the number of interfaces delivering significant cost savings in network deployment. VeriTime is Microsemi's patent-pending distributed timing technology that delivers the industry's most accurate IEEE 1588v2 timing implementation. Integration of MACsec with IEEE 1588v2 time stamping in the PHY is an efficient and low cost method to protect data passing through the network while maintaining highly accurate time of day (ToD).

To ensure that the VSC8490 is field deployable into MACsec relevant applications, Microsemi performed numerous tests on the PHY at various levels of abstraction including ASIC level testing, as a standalone PHY, and system level testing, as a component in typical network equipment. The PHY was tested for protocol compliance against an industry standard tester, in this case the IXIA MACsec tester. To augment the results of these tests, additional tests were performed to confirm interoperability of the PHY with products already available on the market.

This document summarizes various interoperability tests performed on the VSC8490 against the Cisco3560-x platform (catalyst series access switch). The scope is to ensure that Microsemi's IEEE 802.1 AE-2006 implementation interoperates with existing implementations.

Further information about Microsemi's VSC8490 10G/1GbE PHY with Intellisec and VeriTime can be found at https://www.vitesse.com/products/product.php?number=VSC8490

Additional information about Cisco’s Catalyst 3560-X Series Switch platform and the 10G network /service module, C3KX-SM-10G, used for test can be found at http://www.cisco.com/en/US/products /ps10744/index.html

3 The MACsec Interoperability Test

IEEE802.1AE-2006 is the standard governing the operation of MAC security which specifies various features while encrypting and decrypting the L2 Ethernet frames. The purpose of the interoperability test is to ensure that the VSC8490, also known as the device under test (DUT), implements the cipher suites as defined in the standard and can properly communicate with other vendor's implementation. Interoperability testing of MACsec can be done at different levels of abstraction, such as PHY vs. PHY or network equipment vs. network equipment.

This section describes the test model used in the interoperability test and outlines the test procedure along with the description of various hardware and software components used in the test. IEEE802.1X-2010 describes various functions required for establishing a secure MACsec link using port based authentication and MKA protocol for the key exchange mechanism. This section also outlines some of the key steps associated with the MACsec link establishment which is an integral part of the tests performed.

3.1 Scope

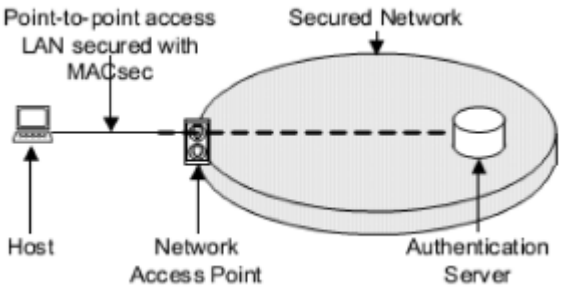
The scope of this test is to ensure that the following MACsec related functions interoperate between the VSC8490 and the defined external equipment.

1. MACsec is functional at the different supported speed modes
2. MACsec is functional with the different supported cipher suites
3. MACsec is functional with the different SECTAG encoding options
4. MACsec is functional at standard and non standard Ethernet frame sizes
5. MACsec is functional without breaking the rest of the L2 control plane (e.g., PAUSE and FLOW control)
6. MACsec is functional for long durations (i.e., without breaking the link during key roll-over conditions)
7. MACsec is functional at the full throughput of the link (i.e., accounting for the frame expansion due to inclusion of the MACsec tag)

3.2 Methodolgy

IEEE802.1X-2010 defines the process of port based authentication and use of MACsec Key Agreement (MKA) protocol for securing point to point links using MACsec. The figure below, from the IEEE802.1X-2010 standard, shows the key elements involved in setting up a MACsec link.

Figure 1 • Host Access with MACsec and Point-to-Point LANs



Authentication Server

This server ensures that the participant trying to gain access to the secured network is authenticated prior to being allowed access to use the network resource. These servers are also called authentication, authorization, and accounting (AAA) servers. They typically use the RADIUS protocol as defined in IETF RFC3579.

Network Access Point (Authenticator)

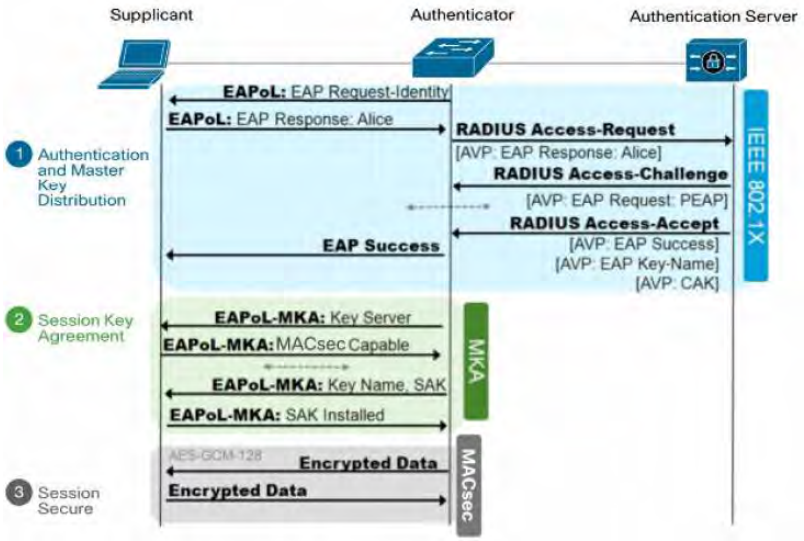
A system, typically incorporating bridging or routing functionality, comprises one or more network access ports that provide controlled access to a network. In the context of MKA protocol this is typically called the Authenticator.

Host (Supplicant)

A system requesting network access through the network access point is often called a host. In the context of MKA protocol this may be referred to as the Supplicant, as this is the one at one end of a point-to-point LAN segment that seeks to be authenticated by an Authenticator attached to the other end of that link.

The figure below shows the process of bringing up a secure link using these components.

Figure 2 • Various Phases in Securing a Link Using MACsec



Phase1: Authentication and Master Key Distribution

This step uses the extensible authentication protocol over LAN (EAPoL) and RADIUS protocols for authentication of the participants, such as the Authentication server and Supplicant.

The Authenticator merely forwards or relays the credential details of the Supplicant and Authentication server to each other for authentication. Once Authentication is done, and based on the network authorization details stored in the Authentication server, the Supplicant may be given access to the network. This will be identified by the “EAP Success” message sent by the Server to the Authenticator in the RADIUS attribute value pairs (AVP). During this process from the details of the EAP session, both Supplicant and authentication server derive the Master Session Key (MSK). However, since the Authenticator is merely acting as a relaying agent, it will not have details of the session and hence no MSK. At the end of the authorization, the RADIUS server, along with the EAP success message, will send the MSK to the Authenticator. At this point, both the Authenticator and Supplicant possess the same MSK which is restricted to the current session. During this stage, the MACsec capabilities of Supplicant and Authenticator do not come into play yet. For authentication purposes, where key derivation for MACsec is required, EAP methods such as EAP-TLS are preferred.

Phase 2: Session Key Agreement

Once the MSK is available with both Authenticator and Supplicant, using the procedure defined in IEEE802.1X-2010 (Ref. Annex H), a Connectivity Association Key (CAK) and Connectivity Association Name (CKN) are derived. Then the MKA acts on each of the entities to start negotiating the parameters relevant for MACsec, such as cipher suite, confidentiality offset, etc. During this negotiation, one of the entities becomes the MKA key server and starts distributing the Secure Association Key (SAK), required for encrypting the MAC service units using MACsec. With the distribution of the SAK using EAPoL-MKA for both transmit and receive secure channels, both ends of the link are ready to encrypt and decrypt data.

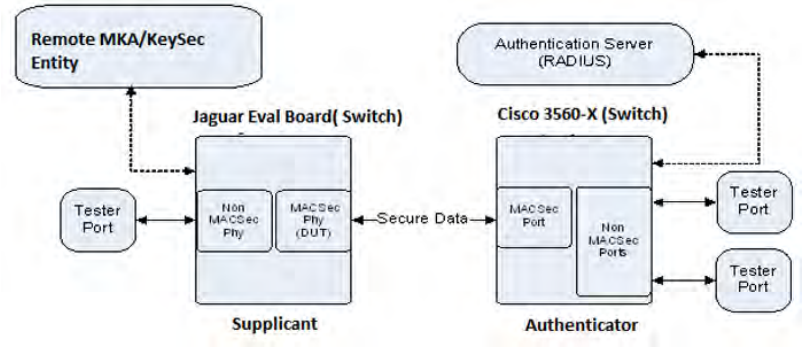
Phase 3: Session Secure

After the distribution of the SAK by the Key Server, the SecY entities in both Authenticator and Supplicant are ready to encrypt and decrypt the data frames, thus the link is secured.

3.3 Methodolgy

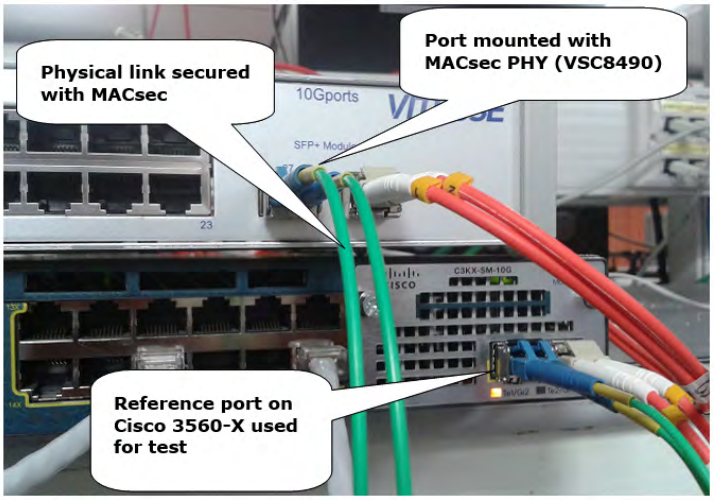
The following illustration shows the block diagram of the setup used to implement the methodology outlined above. The setup enables interoperability testing along with various traffic checks performed after the link is secured with MACsec.

Figure 3 • VSC8490 and Cisco 3560-X Interoperability Test Block Diagram



The following illustration shows the physical bench setup used for the VSC8490 and Cisco 3560-X interoperability tests.

Figure 4 • VSC8490 and Cisco 3560-X Interoperability Bench Setup



The role and description of each of the items from the figures above are enumerated and described in the following table.

Table 1 • Role and Description of the Equipment Used in the Test

S No.	Name	Role in the Test	Description
1	DUT	SecY- Actual MACsec encryption and decryption device (SecY) under test	DUT is the dual port 10G/1GbE PHY capable of MACsec (VSC8490). A SecY will be realized using MACsec API.
2	Jaguar Evaluation Board	Supplicant with SecY- Together with the DUT and Remote MKA/Keysec entity, this forms the Supplicant	This eval board is a reference design for Switch engine ASIC (VSC7434). This board is built as a managed 24 port 1G and 4 port 10G L2 switch by Vitesse on which dual port 10/1GbE PHY (VSC8490) is mounted for use with the 10G ports.
3	Remote MKA/Keysec entity	Supplicant KaY- Together with the DUT and Jaguar Eval Board, this forms the Supplicant's key agreement entity (KaY)	MKA application (developed by Microsemi) running on an external CPU (LINUX Operating System) used for the Key Management and EAP between the Jaguar reference system and Cisco 3560-X switch.
4	Authentication Server (RADIUS)	Authentication Server	A Radius Server running on a Linux Machine is used as the Authentication server. FreeRadius is the open source RADIUS server software used in the test.[1]
5	Cisco 3560-X	Authenticator with MACsec capability	An enterprise switch platform in Cisco Catalyst series, with 24 1G port and 2 no of 10G ports available in market, capable of MACsec encryption (HW+SW ready). This switch is run with Cisco IOS 15.2 version, with universal Image.
6	C3KX-SM-10G	Network plugin module for Cisco 3560-X switch	This pluggable network module provide MACsec on 10G/1G ports.
7	EAP –TLS	EAPoL for Authentication	EAP-TLS is used for Authentication, by using a locally generated CA and server and Client certificate hierarchy.
8	Tester Port	Source and Sink of the traffic in the secure network.	These are Raw Ethernet Frame generators used as Traffic source and sinks. 1. SmartBits with 10G and 1G ports 2. JDSU Test Point
9	Non MACsec PHY	PHY mounted on non-secured ports of the switch.	These are normal ports on the Switch with-out MACsec capability.
10	Interface Connections	Connections between various components	Dashed lines indicate the L3/IP connectivity between the components. Solid lines indicate the L1/Physical connections using optical fiber. 10G/1G ports are used in fiber mode.

Note:

1. FreeRadius is an open source RADIUS server implementation. The Microsemi team worked with FreeRadius developers to include the capability of delivering the EAP-Session ID to the Authenticator. The FreeRadius repository used for this test is found at http://git.freeradius.org/freeradius-server.

3.4 Test Procedure

Following steps are used to perform the interoperability tests.

1. Connections are made as per the setup described above.
2. The DUT (VSC8490), along with the Jaguar evaluation board was configured to act as a supplicant by the use of the remote MKA/Keysec entity.
3. MACsec/MKA was enabled on the Cisco switch with the required parameters such as confidentiality offset, replay window, etc.
4. The RADIUS server was configured to support EAP-TLS by sharing relevant certificates among the Supplicant and Authentication server. Refer to the usage guidelines provided in the FreeRadius documentation for addition information.
5. The MAC address tables in each of the participants (Jaguar evaluation board and Cisco 3560-X) were loaded with randomly chosen MAC addresses at the ports connected to the testers.
6. Both the DUT ports and Cisco 3560-X ports were configured for the speed at which the test was performed, (i.e., 10 G or 1 G)
7. The Supplicant was invoked to start Authentication requests.
8. Ensure that the key derivation was done and the required secure channels were installed on both partners of the link. This was verified by polling the status of the MKA (KaY) status in the MKA /Keysec entity for the DUT and by using the CLI for the Cisco -3560X.
9. Once the transmit and receive secure channels were installed and ready for use, different traffic streams were sent with the following patterns.
    a. Left tester port (connected to the Jaguar evaluation board)
    - 2 streams of frames destined to each tester port on the right side of the Cisco switch
    - Frames of random and fixed sizes ranging from 64 to 1518 and non standard sizes were used as well
    - Frames with fixed and pseudo random payload (PRBS) were used
    - The raw frame rate of each stream was chosen such that the total resultant line rate after MACsec encryption did not exceed the maximum throughput for the speed of the test
    b. Right tester ports (connected to Jaguar evaluation board)
    - A single stream of frames destined to the tester port on the left side of the Jaguar evaluation platform
    - Frames of random and fixed sizes ranging from 64 to 1518 and non standard sizes were used as well
    - Frames with fixed and pseudo random payload (PRBS) were used
    - The raw frame rate of each stream was chosen such that the total resultant line rate after MACsec encryption did not exceed the maximum throughput for the speed of the test
10. Traffic was sent from each of the tester port to the ports on the other side of the MACsec link
11. The traffic duration was long enough to ensure at least 1 key change event was included (some test conditions and duration were chosen to include multiple AN changes)
12. Traffic from each tester port was accounted for and verified at its destination to ensure no frame loss, nor error
13. MACsec encryption/decryption functionality was verified by matching the number of frames through the ports between the Jaguar board and Cisco-3560X switch by matching the SC/SA statistics
14. The above procedure was repeated for numerous features supported by MACsec on both the link partners (i.e., DUT and Cisco -3560X)
15. The tests were performed using the Smart Bits (SMB) for testing L3/IP payloads and the JDSU Test Point (for pseudo random payloads)

It should be noted that the use of PRBS payloads in the testing was not only to ensure frame integrity after encryption and decryption but also to ensure payload integrity.

4 MACsec Interoperability Results

Through the use of the procedure outlined in the previous section the MACsec functionality was verified between two vendors. This section details the modes and test results.

5 VSC8490 and Cisco3560-X Results

The following table summarizes the interoperability test results between the VSC8490 PHY mounted in the Microsemi Jaguar evaluation platform and the Cisco 3560-X switch.

An L2 switch along with a LINUX PC was used to delay a particular stream of encrypted frames so they reach the destination after a certain delay, thereby ensuring they fall outside the replay window. Using this setup, a delay of a few frame lengths was achieved. Testing was also done for shorter windows.

Stream of traffic used for this test contained frame size of 64-128 bytes.

Cisco 3560X platform is not able to decrypt when AN=2 or 3 on it's network module, C3KX-SM-10G ports, however the key change events and decryption by DUT is ok for this AN, and link will be functional in both directions when the AN changes back to 0 after 3.

Table 2 • Test Results Summary

Parameter	Supported Range or modes	Tested Range or modes	Direction of Traffic Test	Test Result	Comments
Speed mode	10 G	10 G	Egress/Ingress	PASS	10 G Optical PHY mode
	1 G	1 G	Egress/Ingress	PASS	1 G Optical PHY mode
Cipher Mode	AES-GCM-128 AES-GCM-256	AES-GCM-128	Egress/Ingress	PASS	Cisco3560X supports 128 bit encryption only
SecTAG	ES=0,1	ES=1,SC=0	Egress only	PASS	
	SC=0,1	ES=0,SC=1	Egress only	PASS	
		ES=0,SC=1	Ingress only	PASS	
	E=0,1 C=0,1	E=1 C=1	Egress/Ingress	PASS	Default value on Cisco switch
Confidentiality Offset	0-64 bytes	0	Egress/Ingress	PASS	
		30	Egress/Ingress	PASS	
		50	Egress/Ingress	PASS	
Replay Protection	Replay protection=0,1 Replay Window = 0 - 2^{32}–1	Strict Ordering, window=0	Ingress only	PASS	
		0 < window < 20	Ingress only	PASS	Limitation on the setup(1)
Frame Size	64-Jumbo	64-9198	Egress/Ingress	PASS	Cisco supports max frame size of 9198 bytes
Flow control		Pause Generation bypassing MACsec	Egress only	PASS	
SA rollover	AN=0..3	AN=0,1	Egress/Ingress	PASS	Tested at 10G for 24 hrs and 1G for 72 hrs[2,3]
Random combination of above parameters			Egress/Ingress	PASSED so far	

Notes:

1. The direction of traffic was in reference to the DUT. Traffic from the host interface to the line interface is called Egress with the opposite path called Ingress.
2. All features listed as supported above were not tested in the interoperability tests due to the limitations on features supported by Cisco3560-X HW and SW (IOS).
3. Wherever needed, if the tester only supported a line rate of 10 G then the line rate was changed to 1 G by additional mechanisms to assist the test.
4. Above results were performed with Cisco IOS15.2(1) release.

6 MACsec Interoperability Future Work

Additional interoperability tests are planned for the VSC8490 and Cisco-3560X when new MACsec features are enabled.

Although there are other products in the market which support MACsec, they are only hardware ready, not software ready yet. Attempts will be made to verify interoperability when they become available. The following table lists network equipment with MACsec hardware which is currently available today.

Table 3 • Test Results Summary

Vendor Name	Product	Network Equipment Type	MACsec Readiness
Cisco	Catalyst 6500,4500	Switch	HW and SW ready
Aruba Networks	S3500	Mobility Access Switch	HW ready, SW due for release
Aruba Networks	AP130	Wireless Access Point	
Brocade	ICX-6450	LAN Switch	HW ready, SW due for release
Juniper	EX-3300	Access Switch	HW ready, SW due for release
AVAYA	VSP-9000	Network processor based virtual service platform	HW ready, SW due in next releases
AVAYA	ERS-4800 series	Switch	HW ready, SW due in next releases

7 References

1. IEEE802.1AE-2006, IEEE standard defining the MACsec protocol
2. IEEE802.1X-2010, IEEE standard for Port-based Network Access Control (PNAC), defining the MKA protocol used by MACsec
3. RFC5216- This document defines EAP-TLS, which includes support for certificatebased mutual authentication and key derivation
4. IXIA MACsec tester http://www.ixiacom.com/products/interfaces/display?skey=in_10g_macsec

Microsemi Headquarters
One Enterprise, Aliso Viejo,
CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996
Email: sales.support@microsemi.com
www.microsemi.com

VPPD-03542