ENT-AN1147

Application Note

MACSec Interoperability Test

Released

Dec 2018

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 2.0

In revision 2.0 of this document, formatting was updated.

1.2 Revision 1.0

Revision 1.0 was the first publication of this document.

2 Introduction

The VSC8258 device is part of Microsemi's SynchroPHY™ product family. It is a four channel 1G/10G serial-to-serial Ethernet PHY featuring Microsemi's VeriTime™ IEEE 1588v2 precision network timing technology and Intellisec™ 128/256-bit MACsec encryption. It also supports dual-sided 10GBASE-KR functionality including auto-negotiation and training in a small form factor, low-power FCBGA ideal for a wide array of board-level signal integrity designs, and system-level IEEE standard compliant (intelligent) Ethernet connectivity.

VeriTime™ is Microsemi's patent-pending timing technology that delivers the industry's most accurate IEEE 1588v2 timing implementation. It is the only IEEE 1588v2 solution to be validated by major OEMs in real-world tests and adopted as the preferred low-cost upgrade for meeting emerging requirements in 4G/LTE-Advanced (LTE-A). With its integration of VeriTime, VSC8258 delivers the quickest, lowest cost method of implementing the network timing accuracy that is critical in maintaining existing service levels as provider architectures migrate from TDM to packet-based technologies. The VSC8258 device supports both 1-step and 2-step PTP frames for ordinary clock, boundary clock, and transparent clock modes of operation, along with complete Y.1731 OAM performance monitoring capabilities.

Intellisec™ is Microsemi's patent-pending flow-based extension of the IEEE 802.1AE-based, end-to-end MACsec solution for confidential communications over any MEF CE 2.0 Ethernet or MPLS service provider connections. It is the world's first FIPS 197-certified CGM-AES 256-bit strong MACsec, with legacy support for today's CGM-AES 128-bit field deployments. The VSC8258 device supports full line rate encryption at both 1 GbE and 10 GbE speeds over multiple media types.

To ensure that the VSC8258 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 VSC8258 device 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 VSC8258 10G/1GbE PHY with Intellisec and VeriTime can be found at https://www.vitesse.com/products/product/VSC8258.

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

3 MACsec Interoperability Test

IEEE802.1AE-2006 is the standard governing the operation of MAC security that specifies various features while encrypting and decrypting the L2 Ethernet frames. The purpose of the interoperability test is to ensure that the VSC8258, also known as the device under test (DUT), implements the cipher suites as defined in the standard and can properly communicate with other vendor implementations. 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

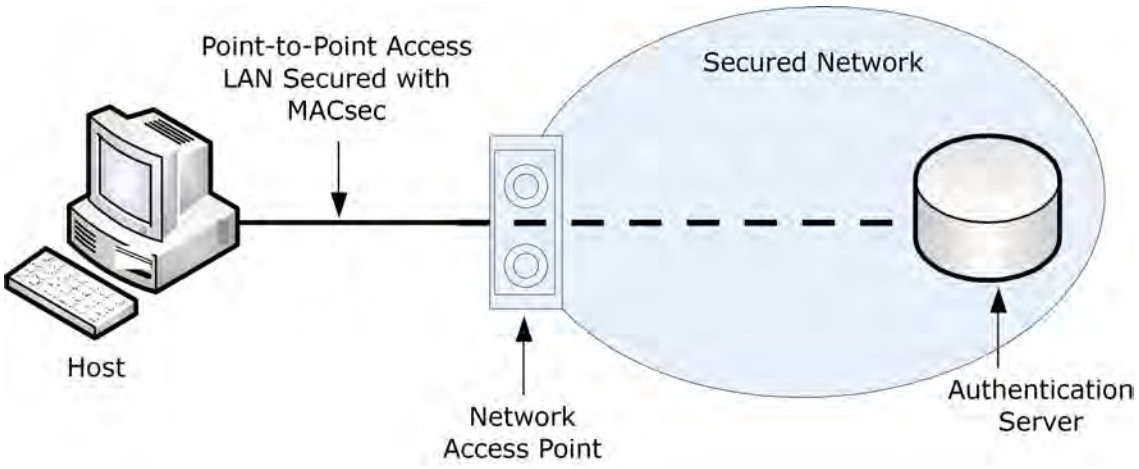
The scope of this test is to ensure that the following MACsec related functions interoperate between the VSC8258 and the defined external equipment.

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 (for example, PAUSE and FLOW control)
6. MACsec is functional for long durations without breaking the link during key roll-over conditions
7. MACsec is functional at the full throughput of the link, accounting for the frame expansion due to inclusion of the MACsec tag

3.2 Methodology

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 following illustration from the IEEE802.1X-2010 standard (IEEE802.1X-2010 Figure 7-6-Network access control with MACsec and a point-to-point LAN), shows the key elements involved in setting up a MACsec link.

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



3.2.1 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.

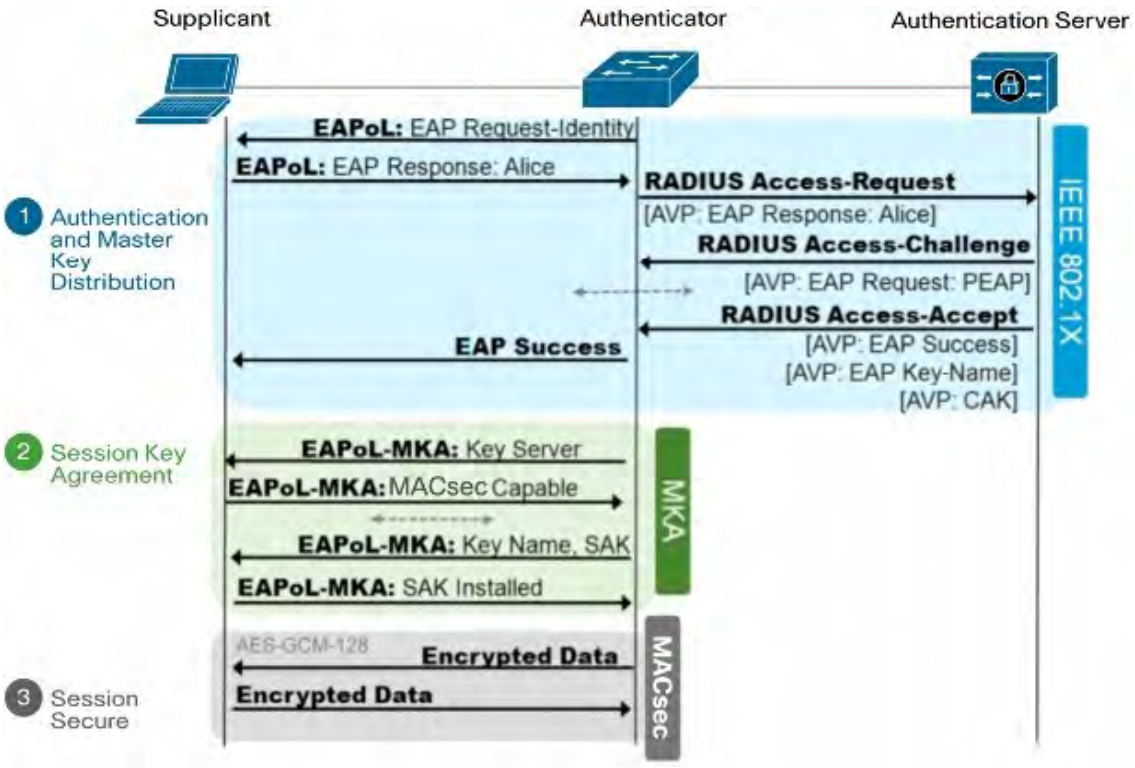
3.2.2 Network Access Point (Authenticator)

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.

3.2.3 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 following illustration from Cisco shows the process of bringing up a secure link using these components.

Figure 2 • Phases in Securing a Link Using MACsec



3.2.4 Phase 1: 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, because 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. For authentication purposes, where key derivation for MACsec is required, EAP methods such as EAP-TLS are preferred.

3.2.5 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 and confidentiality offset. 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.

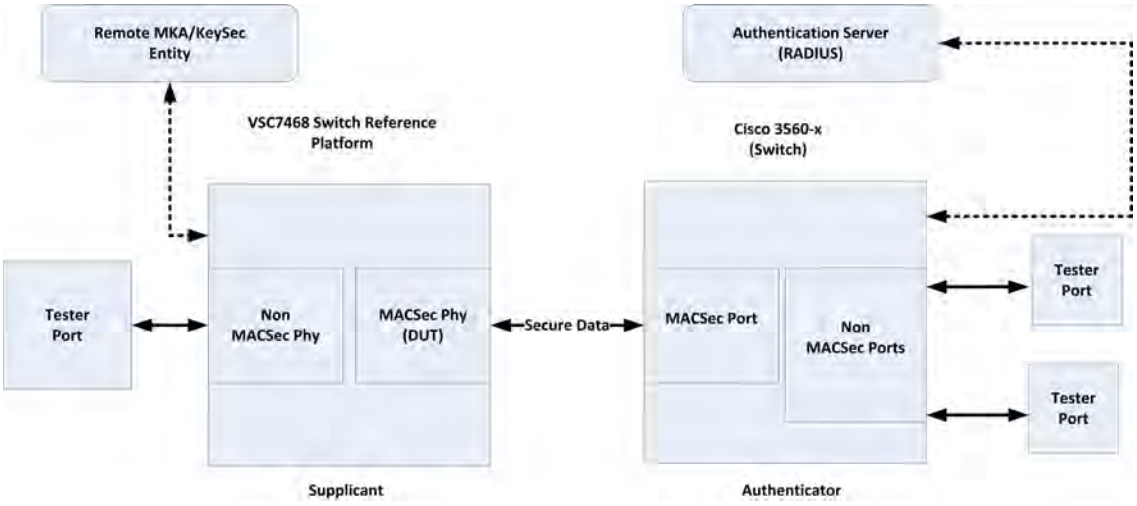
3.2.6 Phase 3: Session Secure

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 Test Setup

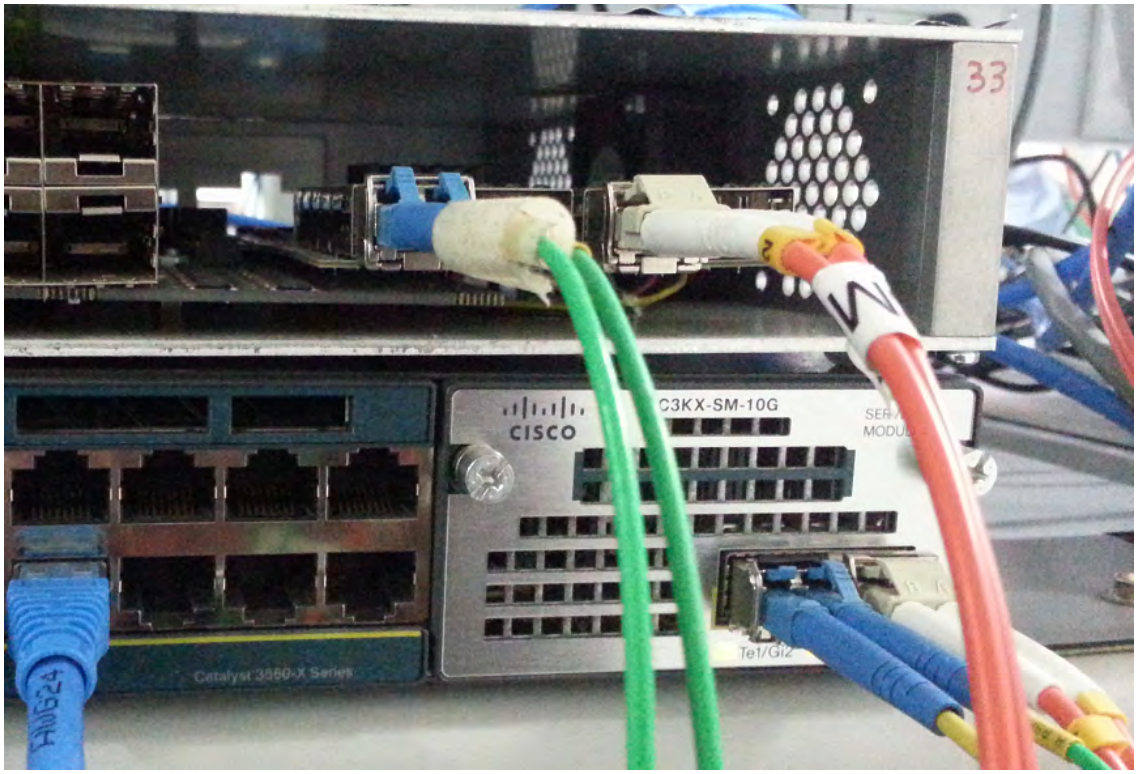
The following figure shows the block diagram of the setup used to implement the methodology. The setup enables interoperability testing along with various traffic checks performed after the link is secured with MACsec.

Figure 3 • VSC8258 and Cisco 3560-X Interoperability Test Block Diagram



The following image shows the physical bench setup used for the VSC8258 and Cisco 3560-X interoperability tests.

Figure 4 • VSC8258 and Cisco 3560-X Interoperability Bench Setup



The following table shows the role and description of each of the items used in the test.

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

Name	Role in the Test	Description
DUT	SecY Actual MACsec encryption and decryption device (SecY) under test.	DUT is the quad port 10G/1GbE PHY capable of MACsec (VSC8258). A SecY will be realized using MACsec API.
VSC7468 switch reference platform	Supplicant with SecY- Together with the DUT and remote MKA /Keysec entity, this forms the Supplicant.	VSC7468 is a managed L2 Ethernet switch. DUT is mounted on one of its front ports, which can be configured as either 10G or 1G port.
Remote MKA /Keysec entity	Supplicant KaY- Together with the DUT and VSC7468 reference platform, this forms the Supplicant's key agreement entity (KaY).	MKA application running on an external CPU (Linux) used for the Key management and EAP between the VSC7468 reference platform and Cisco 3560-X switch.
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]
Cisco 3560-X	Authenticator with MACsec capability.	A Cisco Catalyst series enterprise switch platform with 24 1G ports and two10G ports, capable of MACsec encryption (HW+SW ready). This switch is run with Cisco IOS 1515.0(2) SE2 version.

Name	Role in the Test	Description
C3KX-SM-10G	Network plugin module for Cisco 3560-X switch.	Pluggable network module for MACsec on 10G/1G ports.
EAP -TLS	EAPoL for authentication.	EAP-TLS is used for Authentication, by using a locally generated CA and server and Client certificate hierarchy.
Tester port	Source and Sink of the traffic in the secure network.	Raw Ethernet frame generators used as traffic source and sinks. SmartBits with 10G and 1G ports JDSU Test point
Non MACsec PHY	PHY mounted on non-secured ports of the switch.	Normal ports on the switch without MACsec capability.
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.

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

The following steps were used to perform the interoperability tests.

1. Connections were made as previously described.
2. The DUT (VSC8258), along with the switch reference platform was configured to act as a supplicant using the remote MKA/Keysec entity.
3. MACsec/MKA was enabled on the Cisco switch with the required parameters such as confidentiality offset and replay window.
4. The RADIUS server was configured to support EAP-TLS by sharing relevant certificates among the supplicant and authentication server. For more information, see the usage guidelines provided in the FreeRadius documentation.
5. The MAC address tables in each of the participants (reference platform on which DUT is mounted 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 (1G or 10G).
7. The Supplicant was invoked to start Authentication requests.
8. Verified Key derivation was completed and the required secure channels were installed on both partners of the link. This was done 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 transit 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 reference platform)
        i. Streams of frames destined to each tester port on the right side of the Cisco switch.
        ii. Frames of random and fixed sizes ranging from 64 to 1518 and non standard sizes were used as well.
        iii. Frames with fixed and pseudo random payload (PRBS) were used.
        iv. 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 VSC7468 reference platform)
        i. A single stream of frames destined to the tester port on the left side of the reference switch platform.
        ii. Frames of random and fixed sizes ranging from 64 to 1518 and non standard sizes were used as well.
        iii. Frames with fixed and pseudo random payload (PRBS) were used.
        iv. 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 or errors.
13. MACsec encryption/decryption functionality was verified by matching the number of frames through the ports between the VSC7468 reference board and Cisco-3560X switch by matching the SC /SA statistics.
14. The procedure was repeated for numerous features supported by MACsec on both the link partners, 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).

Using PRBS payloads in the testing ensured frame integrity after encryption and decryption; it also ensured payload integrity.

4 MACsec Interoperability Results

This section details the modes and test results of the procedure outlined in the previous section, which was used to verify the MACsec functionality between two vendors.

4.1 VSC8258 and Cisco3560-X Results

The following table summarizes the interoperability test results between the VSC8258 PHY mounted in the Microsemi VSC7468 reference platform and the Cisco 3560-X switch.

Table 2 • Test Results Summary

Parameter	Supported Range or Modes	Tested Range or Modes	Direction of Traffic Test	Test Result	Comments
Speed mode	10G	10G	Egress /Ingress	Pass	10G Optical PHY mode
	1G	1G	Egress /Ingress	Pass	1G Optical PHY mode
Cipher mode	GCM-AES-128 GCM-AES-256 GCM-AES- XPN-128 GCM-AES- XPN-256	GCM-AES-128	Egress /Ingress	Pass	Cisco3560X supports GCM-AES-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

Parameter	Supported Range or Modes	Tested Range or Modes	Direction of Traffic Test	Test Result	Comments
Flow control		Pause Generation bypassing MACsec encryption	Egress only	Pass	
SA rollover	AN = 0.3	AN = 0, 1	Egress /Ingress	Pass	Tested at 10G for 48 hrs and 1G for 48 hrs [2, 3]
Random parameter combination			Egress /Ingress	Pass	

1. 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.
2. Stream of traffic used for this test contained frame size of 64?128 bytes.
3. Cisco 3560X platform is not able to decrypt when AN = 2 or 3 on its network module, C3KX-SM-10G ports. However, the key change events and decryption by DUT is possible for this AN, and the link will be completely functional in both directions when the AN changes back to 0 after 3.

- The direction of traffic was in reference to the DUT. Traffic from the host interface to the line interface (reference switch platform to Cisco Switch) is called Egress and the opposite path called Ingress.
- All features listed as supported were not tested in the interoperability tests due to the limitations on features supported by Cisco3560-X HW and SW (IOS).
- Wherever needed, if the tester only supported a line rate of 10G then the line rate was changed to 1G by additional mechanisms to assist the test.
- Results are from the tests performed with Cisco IOS15.0(2)SE2 - C3560E-IPBASEK9-M release.

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-03992