ENT-AN1152

Application Note

MACsec Interoperability Test

November 2015

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 1.1

The following is a summary of the changes in revision 1.1 of this document.

- The test speed was updated. For more information, see Test Procedure.
- The Cisco 3560-X switch version was updated. For more information, see Table 1.
- Test results were updated. For more information, see Table 2.

1.2 Revision 1.0

Revision 1.0 was the first publication of this document.

2 Introduction

The quad port VSC8584 Gigabit Ethernet PHY with Intellisec™ and VeriTime™ is ideal for securing cloud network applications including e-commerce, database, collaboration, smart grid, video, and enterprise or government communications. Intellisec enables a realistic and affordable Layer 2 MACsec security solution.

Intellisec is Microsemi’s 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 MACseclink-based box-to-box applications. Likewise, Intellisec scales easily with the number of interfaces delivering significant cost savings in network deployment.

VeriTimeis Microsemi’s patent-pending 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 VSC8584 is field deployable in 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 a typical network equipment. The PHY was tested for protocol compliance against an industry standard tester, in this case the IXIA MACsec tester. Additional tests are also planned to confirm interoperability of the PHY with products already available on the market. This document summarizes various interoperability tests performed on the VSC8584 against the Cisco3560-x (Catalyst series Access Switch). The scope is to verify that Microsemi’s IEEE802.1AE-2006 implementation interoperates with existing implementations.

For more information about Microsemi's VSC8584 Gigabit Ethernet PHY with Intellisec and VeriTime, see http://www.microsemi.com.

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

Log into use GingerLimited modeIntellisec enables a realistic and affordable Layer 2 music security solution×

3 The 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 verify that the VSC8584, also known as the device under test (DUT), implements the cipher suites as defined in the standard and is able to 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.networkequipment. 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-2010describesvariousfunctionsrequiredforestablishing a secure MACsec link using port based authentication and MKA protocol for the key exchange mechanism. This section also outlines some of the key stepsassociatedwiththeMACseclinkestablishment, which is an integralpartofthetestsperformed.

3.1 Scope

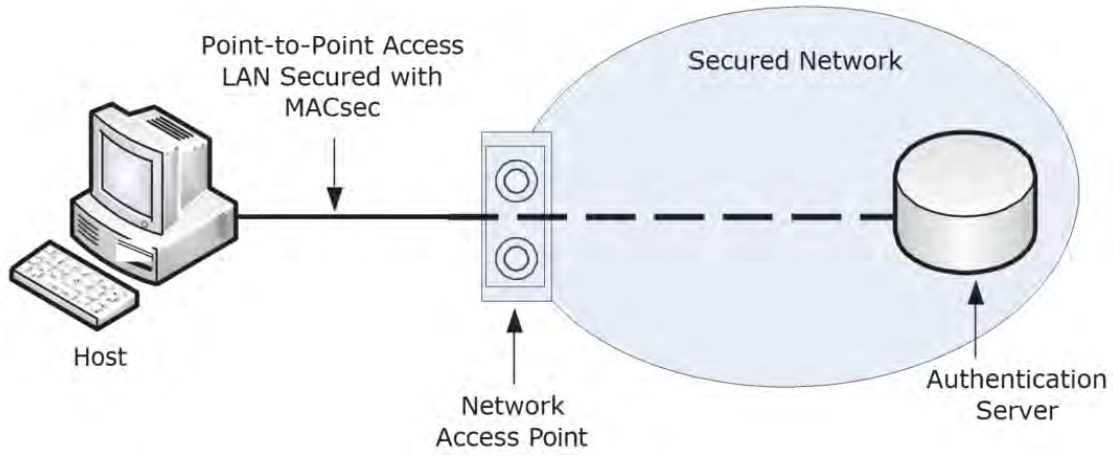
The scope of this test is to verify that the following MACsecrelatedfunctionsinteroperatebetweentheVSC8584 and the defined external equipment.

1. MACsecisfunctionalatthe different supported speed modes
2. MACsecisfunctionalwiththe different supported cipher suites
3. MACsecisfunctionalwiththe different SECTAG encoding options
4. MACsecisfunctionalatstandard and non standard Ethernet frame sizes
5. MACsecisfunctionalwithoutbreakingthe rest of the L2 control plane (for example, PAUSE and FLOW control)
6. MACsecisfunctionalforlong durations without breaking thelinkduringkeyroll-overconditions
7. MACsecisfunctionalatthe full throughput of the link, accounting for the frameexpansionduetoinclusionoftheMACsectag

3.2 Methodology

IEEE802.1X-2010 defines the process of port based authentication and use of MACsec Key Agreement (MKA)protocolforsecuringpointtopointlinksusingMACsec. The following illustration shows the key elements involved in setting up a MACsec link.

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



Source: IEEE802.1X-2010 Figure 7-6-Network access control with MACsec and a point-to-point LAN

3.2.1 Authentication Server

An authentication server ensures that the participant trying to gain access to the secured network is authenticated before 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.

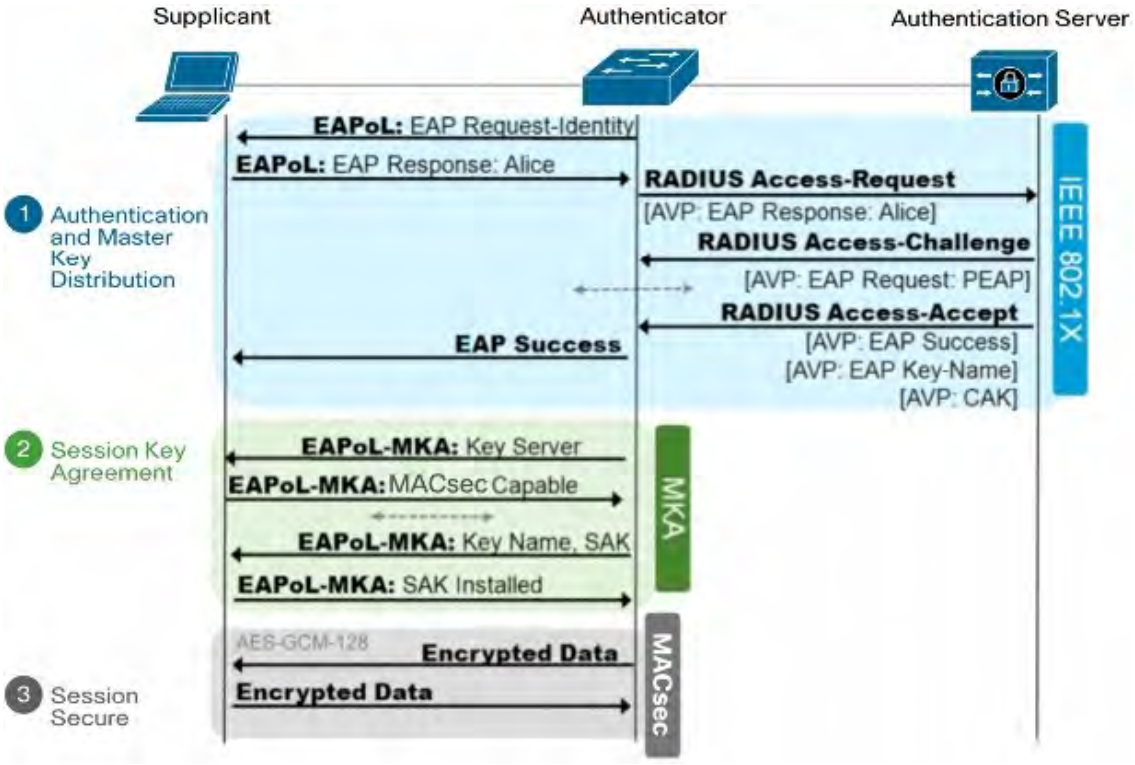
3.2.2 Network Access Point (Authenticator)

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 because it seeks to be authenticated by an Authenticator attached to the other end of a point-to-point LAN segment. 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



Source: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/deploy_guide_c17-663760.html

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 completed, 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 both Supplicant and Authentication server derive the Master Session Key (MSK) from the details of the EAP session. 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 keyderivationforMACsecisrequired, 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, a Connectivity Association Key (CAK) and Connectivity Association Name (CKN) are derived using the procedure defined in IEEE802.1X-2010 (Ref. Annex H). 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 serviceunitsusingMACsec. 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.

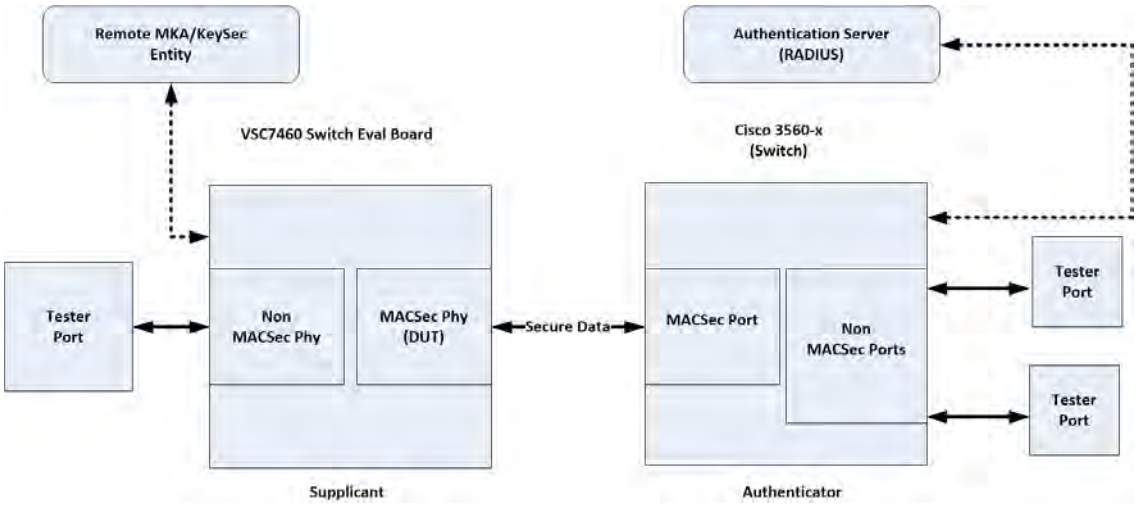
3.2.6 Phase 3: Session Secure

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

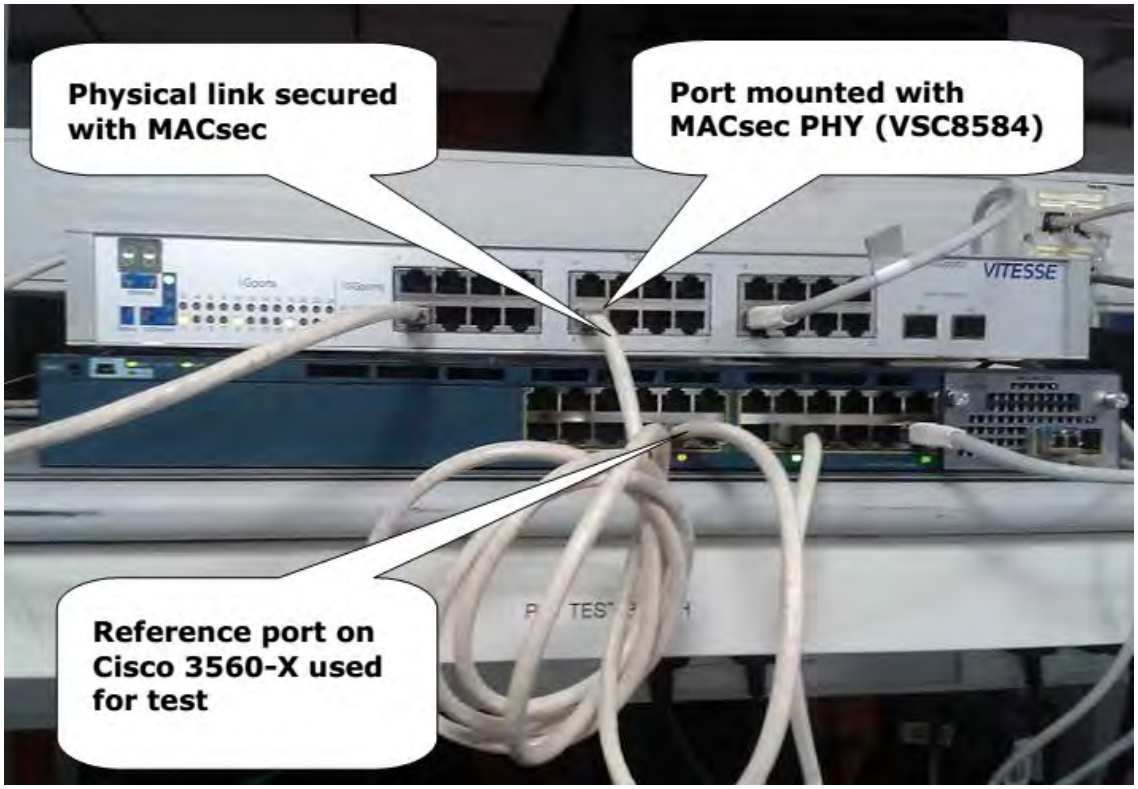
The following block diagram shows the setup used to implement the methodology. The setup enables interoperability testing along with various traffic checks performed after the link is secured with MACsec.

Figure 3 • VSC8584 and Cisco 3560-X Interoperability Test Block Diagram



The following image shows the physical bench setup used for the VSC8584 and Cisco 3560-X interoperability tests.

Figure 4 • VSC8584 and Cisco 3560-X Interoperability Bench Setup



The following table shows the roles and descriptions 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	SecYActualMACsecencryption and decryption device (SecY) under test.	DUTisthequad port PHY capable of MACsec (VSC8584).ASecYwillbe realized using MACsec API.
VSC7460 evaluation board	Supplicant with SecYTogether with the DUT and Remote MKA /Keysec entity, this forms the Supplicant	This board is a reference design for Switch engine ASIC (VSC7460). This board is built as a managed 24-port 1G and 4-port 10G L2 switch by Microsemi on which the quad port PHY (VSC8584) is mounted for use with the 1G or 10G ports.
Remote MKA /Keysec entity	Supplicant KaYTogether with the DUT and VSC7460 evaluation 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 VSC7460 evaluation board and Cisco 3560-X switch.
Authentication server (RADIUS)	Authentication server.	A Radius server running on a Linux machine is used as the Authentication server. FreeRadiusistheopen source RADIUS server software used in the test.[1]
Cisco 3560-X	Authenticator with MACsec capability.	An enterprise switch in Cisco Catalyst series, with 24 1G ports and two10G ports, capable of MACsec encryption (HW+SW ready). This switch is run with Cisco IOS 15.0(2)SE8 -C3560E-IPBASEK9-M.
EAP -TLS	EAPoL for authentication.	EAP-TLS is used for Authentication, by using a locally generated CA and server and Client certificate hierarchy.

Name	Role in the Test	Description
Tester port	Source and Sink of the traffic in the secure network.	These are Raw Ethernet Frame generators used as Traffic source and sinks. –SmartBitswith10G 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 RJ-45 connectors and CAT-5 Cables.

1. FreeRadiusisan 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 (VSC8584), along with the VSC7460 evaluation board 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 (10/100/1000 Base T or 1000 Base X).
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)statusintheMKA/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.
   Left tester port (connected to the reference platform)
   a. Two streams of frames destined to each tester port on the right side of the Cisco switch.
   b. Frames of random and fixed sizes ranging from 64 to 1518 and non-standard sizes were used as well.
   c. Frames with fixed and pseudo random payload (PRBS) were used.
   d. 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.

   Right tester ports (connected to the reference platform)
   a. A single stream of frames destined to the tester port on the left side of the reference switch platform.
   b. Frames of random and fixed sizes ranging from 64 to 1518 and non standard sizes were used as well.
   c. Frames with fixed and pseudo random payload (PRBS) were used.
   d. 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.
   e. Traffic was sent from each of thetesterporttothe ports on the other side of the MACsec link.
10. 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).
11. Traffic from each tester port was accounted for and verified at its destination to ensure no frame loss or errors.

12. MACsecencryption/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.
13. The procedure was repeated for numerous features supported by MACsec on both the link partners, DUT and Cisco -3560X.
14. 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.

Log into use GingerLimited modeFreeRadiusisthe×

4 MACsec Interoperability Results

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

4.1 VSC8584 and Cisco3560-X Results

The following table summarizes the interoperability test results between the VSC8584 PHY mounted on the Microsemi VSC7460 evaluation board 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	10 Base T	10 Base T	Egress /Ingress	Pass	100 Base FX not supported on Cisco 3560X
	100 Base T	100 Base T			
	1000 Base T	1000 Base T			
	1000 Base X	1000 Base X			
	100 Base FX				
Cipher mode	GCM-AES-XPN-128	GCM-AES-128	Egress /Ingress	Pass	Cisco 3560X supports AES-GCM-128 bit encryption only
	GCM-AES-XPN-256				
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	E = 1, C = 1	Egress /Ingress	Pass	Default value on Cisco switch
	C= 0, 1				
Confidentiality offset	0 to 64 bytes	0	Egress /Ingress	Pass	
		30	Egress /Ingress	Pass	
		50	Egress /Ingress	Pass	
Replay protection	Replay protection = 0, 1 Replay Window = 0 to 232–1	Strict Ordering, window = 0	Ingress only	Pass	
		0<window< 20	Ingress only	Pass	Limitation on the setup[1]
Frame size	64 to Jumbo	64 to 9,198	Egress /Ingress	Pass	Cisco supports maximum frame size of 9,198 bytes
Flow control		Pause Generation bypassing MACsec encryption	Egress only	Pass	
SA rollover	AN = 0 to 3	AN = 0 to 3	Egress /Ingress	Pass	Tested at 1000 M for 24 hrs [2]

Parameter	Supported Range or Modes	Tested Range or Modes	Direction of Traffic Test	Test Result	Comments
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.

Notes:

- 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.

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-03402