

# **National Information Assurance Partnership**



## **Common Criteria Evaluation and Validation Scheme**

### **Validation Report**

**For**

**Hewlett-Packard 6125XLG Ethernet Blade Switch**

**Report Number: CCEVS-VR-VID10601-2015**

**Dated: February 24, 2015**

**Version: 1.0**

**National Institute of Standards and Technology  
Information Technology Laboratory  
100 Bureau Drive  
Gaithersburg, MD 20899**

**National Security Agency  
Information Assurance Directorate  
9800 Savage Road STE 6940  
Fort George G. Meade, MD 20755-6940**

## Table of Contents

1	Executive Summary .....	1
2	Identification .....	3
2.1	Threats.....	3
2.2	Organizational Security Policies.....	4
3	Architectural Information .....	5
4	Assumptions.....	7
4.1	Clarification of Scope .....	7
5	Security Policy .....	8
5.1	Security Audit .....	8
5.2	Cryptographic Support.....	8
5.3	User Data Protection .....	8
5.4	Identification and Authentication .....	8
5.5	Security Management .....	8
5.6	Protection of the TSF.....	8
5.7	TOE Access .....	9
5.8	Trusted Path/Channels .....	9
6	Documentation.....	10
7	Independent Testing.....	11
8	Evaluated Configuration .....	12
9	Results of the Evaluation .....	13
10	Validator Comments/Recommendations .....	14
11	Annexes 15	
12	Security Target.....	16
13	Abbreviations and Acronyms .....	17
14	Bibliography .....	19

VALIDATION REPORT  
Hewlett-Packard 6125XLG Ethernet Blade Switch

## List of Tables

Table 1: Evaluation Details.....	2
Table 2: ST and TOE Identification.....	3

VALIDATION REPORT  
Hewlett-Packard 6125XLG Ethernet Blade Switch

## 1 Executive Summary

This report is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should read carefully the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation Hewlett-Packard (HP) Company 6125XLG Ethernet Blade Switch running Comware 7.1.045, Release 2406P01. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of Hewlett-Packard Company 6125XLG Ethernet Blade Switch was performed by Leidos (formerly Science Applications International Corporation (SAIC)) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in February 2015. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 4 and assurance activities specified in Protection Profile for Network Devices, Version 1.1, 8 June 2012 and Security Requirements for Network Devices Errata #2. The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site ([www.niap-ccevs.org](http://www.niap-ccevs.org)).

The Leidos evaluation team determined that Hewlett-Packard Company 6125XLG Ethernet Blade Switch is conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in the ST. The information in this VR is largely derived from the Assurance Activities Report (AAR) and associated test report produced by the Leidos evaluation team.

The TOE is a hardware and software solution that consists of the Hewlett-Packard (HP) Company 6125XLG Ethernet Blade Switch running Comware 7.1.045, Release 2406 P01. The network on which it resides is considered part of the operational environment.

The following modules, extending the physically available ports, are supported by the HP 6125XLG Ethernet Blade Switch and can optionally be used since they do not affect any of the claimed security functions but rather serve to extend available network connectivity:

- HP X120 1G SFP LC SX 850nm Transceiver JD118B
- HP X120 1G SFP LC LX 1310nm Transceiver JD119B
- HP X125 1G SFP LC LH40 1310nm Transceiver JD061A
- HP X120 1G SFP LC LH40 1550nm Transceiver JD062A
- HP X125 1G SFP LC LH70 1550nm Transceiver JD063B
- HP X120 1G SFP LC RJ45 T Transceiver JD089B
- HP BLc 1Gb SFP LC SX 850nm Transceiver
- HP BLc 1Gb SFP LC RJ45 T Transceiver
- HP X130 10G SFP+ LC SR 850nm Transceiver JD092B
- HP X130 10G SFP+ LC LRM 1310nm Transceiver JD093B
- HP X130 10G SFP+ LC LR 1310nm Transceiver JD094B

VALIDATION REPORT  
Hewlett-Packard 6125XLG Ethernet Blade Switch

- HP X130 10G SFP+ LC ER 1550nm Transceiver JG234A
- HP BladeSystem c-Class 10G SFP+ LC SR 850nm Transceiver
- HP BladeSystem c-Class 10G SFP+ LC LR 1310nm Transceiver
- HP X140 40G QSFP+ MPO SR4 850nm Transceiver JG325A

**Table 1: Evaluation Details**

<b>Item</b>	<b>Identifier</b>
<b>Evaluated Product</b>	Hewlett-Packard (HP) Company 6125XLG Ethernet Blade Switch running Comware 7.1.045, Release 2406 P01.
<b>Sponsor &amp; Developer</b>	Hewlett-Packard Development Company, L.P. 11445 Compaq Center Drive West Houston, Texas 77070
<b>CCTL</b>	Leidos (formerly SAIC) Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
<b>Completion Date</b>	February 2015
<b>CC</b>	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
<b>Interpretations</b>	There were no applicable interpretations used for this evaluation.
<b>CEM</b>	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
<b>PP</b>	Protection Profile for Network Devices, Version 1.1, 8 June 2012 Security Requirements for Network Devices Errata #2, 13 January 2013
<b>Evaluation Class</b>	None
<b>Disclaimer</b>	The information contained in this Validation Report is not an endorsement of the Hewlett-Packard (HP) Company 6125XLG Ethernet Blade Switch running Comware 7.1.045, Release 2406 P01 by any agency of the U.S. Government and no warranty of Hewlett-Packard (HP) Company 6125XLG Ethernet Blade Switch running Comware 7.1.045, Release 2406 P01 is either expressed or implied.
<b>Evaluation Personnel</b>	Katie Sykes Tony Apted Pascal Patin Greg Beaver Dragua Zenelaj
<b>Validation Personnel</b>	Paul Bicknell The MITRE Corporation Jean Petty The MITRE Corporation

VALIDATION REPORT  
Hewlett-Packard 6125XLG Ethernet Blade Switch

## 2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

The following table identifies the evaluated Security Target and TOE.

**Table 2: ST and TOE Identification**

Name	Description
ST Title	Hewlett-Packard Company 6125XLG Ethernet Blade Switch Security Target
ST Version	2.0
Publication Date	February 19, 2015
Vendor	Hewlett-Packard Company
ST Author	Leidos (formerly SAIC)
TOE Reference	Hewlett-Packard (HP) Company 6125XLG Ethernet Blade Switch running Comware 7.1.045, Release 2406 P01
TOE Hardware Models	HP 6125XLG Ethernet Blade Switch
TOE Software Version	Comware 7.1.045, Release 2406 P01
Keywords	Switch, Layer 2, Layer 3

### 2.1 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

- An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
- Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
- A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
- Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.

## VALIDATION REPORT

### Hewlett-Packard 6125XLG Ethernet Blade Switch

- User data may be inadvertently sent to a destination not intended by the original sender.

## **2.2 Organizational Security Policies**

The ST identifies the following organizational security policy that the TOE and its operational environment are intended to fulfill:

- The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

### 3 Architectural Information

The HP 6125XLG Ethernet Blade Switch comprising the TOE includes a common software code base, called Comware. Comware is special purpose appliance system software that implements a wide array of networking technology, including: IPv4/IPv6 dual-stacks; a data link layer; layer 2 and 3 routing; Ethernet switching; VLANs; IRF routing; and Quality of Service (QoS). The evaluated version of Comware is 7.1.045, Release 2406 P01. It should be noted that although Comware can run on a variety of underlying architectures, including VxWorks, Linux, pSOS and Windows, the only underlying architecture found in the evaluated configuration is Linux.

Comware V7.1 implements full modularization and multi-process applications, and provides the following benefits:

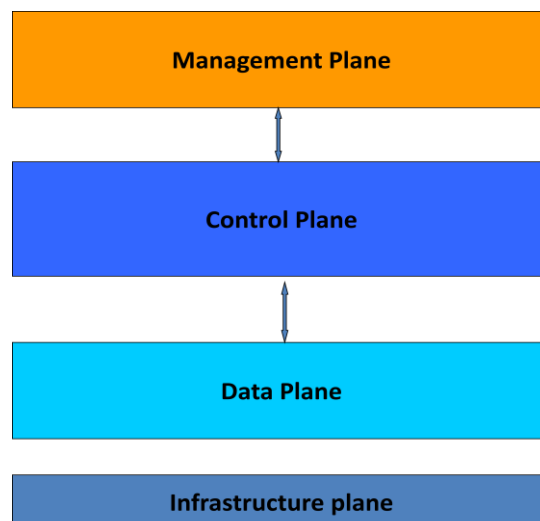
- Full modularization—Brings improvements in system availability, virtualization, multi-core multi-CPU applications, distributed computing, and dynamic loading and upgrading.
- Openness—Comware V7.1 is a generic, open system based on Linux.
- Improved operations—Comware V7.1 improves some detailed operations. For example, it uses preemptive scheduling to improve real-time performance.

Comware V7.1 optimizes the following functions:

- Virtualization—Supports N:1 virtualization.
- In Service Support Updates (ISSU)—Supports ISSU for line cards.
- Auxiliary CPU and OAA—Improves scalability for devices.

In addition, Comware V7.1 supports new technologies for data centers, including TRILL and EVB.

Comware V7.1 comprises four planes: management; control; data; and infrastructure.



**Figure 1: Comware V7.1 Architecture**

- **Infrastructure**—the infrastructure plane provides basic Linux services and Comware support functions. Basic Linux services comprise basic Linux functions, C language library functions,



## VALIDATION REPORT

### Hewlett-Packard 6125XLG Ethernet Blade Switch

data structure operations, and standard algorithms. Comware support functions provide software and service infrastructure for Comware processes, including all basic functions.

- **Data**—the data plane provides data forwarding for local packets and received IPv4 and IPv6 packets at different layers.
- **Control**—the control plane comprises all routing, signaling, and control protocols, such as MPLS, OSPF, and security control protocols. It generates forwarding tables for the data plane.
- **Management**—the management plane provides a management interface for operators to configure, monitor, and manage Comware V7.1. The management interface comprises a Command Line Interface (CLI) accessed using SSH.

The Comware V7.1 software is further decomposed into subsystems designed to implement applicable functions. For example, there are subsystems dedicated to the security management interface. There are also subsystems dedicated to the IPv4 and IPv6 network stacks as well as the applicable network protocols and forwarding, routing, etc.

From a security perspective, the TOE implements NIST-validated cryptographic algorithms that support the IPsec and SSH protocols as well as digital signature services that support the secure update capabilities of the TOE. Otherwise, the TOE implements various network switching protocols and functions.

## 4 Assumptions

The ST identifies the following assumptions about the use of the product:

- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

### 4.1 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific device models and software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
5. The following specific product capabilities are excluded from use in the evaluated configuration:
  - a. Non-FIPS 140-2 mode of operation—this mode of operation allows cryptographic operations that are not FIPS-approved
  - b. TLS is not included in the evaluated configuration.
6. The TOE can be configured to rely on and utilize a number of other components in its operational environment:
  - a. Syslog server—to receive audit records when the TOE is configured to deliver them to an external log server.
  - b. RADIUS and TACACS servers—the TOE can be configured to use external authentication servers.
  - c. Management Workstation—the TOE supports remote access to the CLI over SSHv2. As such, an administrator requires an SSHv2 client to access the CLI remotely.

## 5 Security Policy

The TOE enforces the following security policies as described in the ST.

**Note:** Much of the description of the security policy has been derived from the ST and the Final ETR.

### 5.1 Security Audit

The TOE is able to generate audit records of security relevant events. The TOE can be configured to store the audit records locally so they can be accessed by an administrator or alternately to send the audit records to a designated log server.

### 5.2 Cryptographic Support

The TOE includes NIST-validated cryptographic mechanisms that provide key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols, including IPsec and SSHv2. Note that to be in the evaluated configuration, the TOE must be configured in FIPS mode, which ensures the TOE's configuration is consistent with the FIPS 140-2 standard.

### 5.3 User Data Protection

The TOE performs network switching and routing functions, passing network traffic among its various physical and logical (e.g., VLAN) network connections. While implementing applicable network protocols associated with network traffic forwarding, the TOE is designed to ensure that it does not inadvertently reuse data found in network traffic.

### 5.4 Identification and Authentication

The TOE requires users (i.e., administrators) to be successfully identified and authenticated before they can access any security management functions available in the TOE. The TOE offers both a locally connected console and a network accessible interface (SSHv2) for interactive administrator sessions.

The TOE supports the local (i.e., on device) definition of administrators with usernames and passwords. Additionally, the TOE can be configured to use the services of trusted RADIUS and TACACS servers in the operational environment to support, for example, centralized user administration.

### 5.5 Security Management

The TOE provides a CLI to access its security management functions. Security management commands are limited to administrators and are available only after they have provided acceptable user identification and authentication data to the TOE.

### 5.6 Protection of the TSF

The TOE implements a number of features designed to protect itself to ensure the reliability and integrity of its security features.

It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability).

The TOE uses cryptographic means to protect communication with remote administrators. When the TOE is configured to use the services of a Syslog server or authentication servers in the operational

## VALIDATION REPORT

### Hewlett-Packard 6125XLG Ethernet Blade Switch

environment, the communication between the TOE and the operational environment component is protected using encryption.

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

#### **5.7 TOE Access**

The TOE can be configured to display an informative banner that will appear prior to authentication when accessing the TOE via the console or SSH interfaces. The TOE subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session will be terminated.

#### **5.8 Trusted Path/Channels**

The TOE protects interactive communication with administrators using SSHv2 for CLI access. Using SSHv2, both integrity and disclosure protection is ensured.

The TOE protects communication with external IT entities, including audit and authentication servers, using IPsec connections, which prevent unintended disclosure or modification of data.

VALIDATION REPORT  
Hewlett-Packard 6125XLG Ethernet Blade Switch

## 6 Documentation

There are numerous documents that provide information and guidance for the deployment of the TOE. In particular, the following Common Criteria specific guides reference the security-related guidance material for all devices in the evaluated configuration:

- Preparative Procedures for CC NDPP Evaluated Hewlett-Packard 6125XLG Network Switch based on Comware V7, v1.02, dated 02/19/2015
- Command Reference for CC Supplement, Revision # v1.04, dated 02/19/2015
- Configuration Guide for CC Supplement, Revision # v1.5 dated 02/19/2015
- Comware V7.1 Platform System Log Messages, Revision # v0.25, dated 4/21/2014.

These CC specific guidance documents are distributed by the HP Federal sales and support team as part of the sales delivery process.

The following documents for the HP 6125XLG Switch can be found under the *General Reference* section of the HP 6125XLG Ethernet Blade Switch documentation page on the HP Web site. The link is provided below.

- R240x-HP 6125XLG Blade Switch ACL and QoS Command Reference
- R240x-HP 6125XLG Blade Switch Layer 3 - IP Services Command Reference
- R240x-HP 6125XLG Blade Switch Fundamentals Command Reference
- R240x-HP 6125XLG Blade Switch Security Command Reference
- R240x-HP 6125XLG Blade Switch Network Management and Monitoring Command Reference

[http://h20566.www2.hp.com/portal/site/hpsc/public/psi/manualsResults/?cc=us&jumpid=hpr\\_r1002\\_usen\\_link3&lang=en&sp4ts.oid=5404487](http://h20566.www2.hp.com/portal/site/hpsc/public/psi/manualsResults/?cc=us&jumpid=hpr_r1002_usen_link3&lang=en&sp4ts.oid=5404487)

The following documents for the HP 6125XLG Switch can be found under the *Setup and Install* section of the HP 6125XLG Ethernet Blade Switch documentation page on the HP Web site. The link is provided below.

- R2306-HP 6125XLG Blade Switch ACL and QoS Configuration Guide
- R2306-HP 6125XLG Blade Switch Layer 3 - IP Services Configuration Guide
- R2306-HP 6125XLG Blade Switch Fundamentals Configuration Guide
- R240x-HP 6125XLG Blade Switch Security Configuration Guide
- R240x-HP 6125XLG Blade Switch Network Management and Monitoring Configuration Guide

[http://h20566.www2.hp.com/portal/site/hpsc/public/psi/manualsResults/?cc=us&jumpid=hpr\\_r1002\\_usen\\_link3&lang=en&sp4ts.oid=5404487](http://h20566.www2.hp.com/portal/site/hpsc/public/psi/manualsResults/?cc=us&jumpid=hpr_r1002_usen_link3&lang=en&sp4ts.oid=5404487)

### Supporting TOE Guidance Documentation

Hewlett-Packard Company 6125XLG Ethernet Blade Switch Security Target, Version 2.0, 19 February 2015

## 7 Independent Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following:

- Evaluation Team Test Report for Hewlett-Packard Company 6125XLG Ethernet Blade Switch, Version 3.0, February 20, 2015.

The purpose of this activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to Protection Profile for Network Devices, Version 1.1, 8 June 2012 and Security Requirements for Network Devices Errata #2.

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in NDPP v1.1 and Security Requirements for Network Devices Errata #2. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at the developer facility in Boston, MA on the dates September 29 – October 3, 2014.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for NDPPv1.1 and Security Requirements for Network Devices Errata #2 are fulfilled.

## **8 Evaluated Configuration**

The evaluated version of the TOE is Hewlett-Packard 6125XLG Ethernet Blade Switch running Comware 7.1.045, Release 2406 P01, as installed and configured according to the Preparative Procedures for CC NDPP Evaluated Hewlett-Packard 6125XLG Network Switches based on Comware V7, as well as the supporting guidance documentation identified in Section 6.

## 9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in Protection Profile for Network Devices, Version 1.1, 8 June 2012 and Security Requirements for Network Devices Errata #2, in conjunction with version 3.1, revision 4 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

**Table 4: TOE Security Assurance Requirements**

<b>Assurance Component ID</b>	<b>Assurance Component Name</b>
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing - conformance
AVA_VAN.1	Vulnerability survey



## 10 Validator Comments/Recommendations

The validation team suggests that the consumer pay particular attention to the installation guidance to ensure the devices are placed into the evaluated configuration. In order to remain CC compliant, the device(s) must be configured in FIPS mode.

As was noted in the Clarification of Scope section of this report, the devices provide more functionality than was covered by the evaluation. Only the functionality claimed in the SFR's in the Security Target was evaluated. All other functionality provided by the devices needs to be assessed separately and no further conclusions should be drawn as to their effectiveness, nor can any claims be made relative to their security based upon this evaluation.

The validators note that Technical Decision TD0012 was applied to this evaluation. The Technical Decision is available on the NIAP web site, but its impact on this evaluation is described below:

- TD0012: Algorithms not identified in FCS\_SSH\_EXT.1.4 must not be allowed in the evaluated configuration of the TOE; The TOE does not support any algorithms not identified in FCS\_SSH\_EXT.1.4. In FIPS mode, all other cipher suites are disabled.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities prescribed in the NDPPv1.1 with Errata #2, and the Technical Decision listed above. Also, that the evaluation team correctly verified that the product meets the claims of the associated Security Target.

## **11 Annexes**

Not applicable.

## **12 Security Target**

Hewlett-Packard Company 6125XLG Ethernet Blade Switch Security Target, Version 2.0, February 19, 2015.

## 13 Abbreviations and Acronyms

<b>AAA</b>	Authentication, Authorization and Accounting
<b>ACL</b>	Access Control List
<b>AES</b>	Advanced Encryption Standard
<b>AUT</b>	Authentication
<b>CBC</b>	Cipher-Block Chaining
<b>CC</b>	Common Criteria for Information Technology Security Evaluation
<b>CEM</b>	Common Evaluation Methodology for Information Technology Security
<b>CM</b>	Configuration Management
<b>CLI</b>	Command Line Interface
<b>DH</b>	Diffie-Hellman
<b>ECB</b>	Electronic Codebook
<b>EVB</b>	Edge Virtual Bridging
<b>EVI</b>	Ethernet Virtualization Interconnection
<b>FDP</b>	User Data Protection CC Class
<b>FIA</b>	Identification and Authentication CC Class
<b>FIPS</b>	Federal Information Processing Standard
<b>FMT</b>	Security Management CC Class
<b>FSP</b>	Functional Specification
<b>GR</b>	Graceful Restart
<b>HMAC</b>	Hashed Message Authentication Code
<b>IP</b>	Internet Protocol
<b>IPC</b>	Inter-process communication
<b>IPSEC</b>	Internet Protocol Security
<b>IRF</b>	Intelligent Resilient Framework
<b>ISSU</b>	In Service Software Upgrades
<b>IT</b>	Information Technology
<b>LACP</b>	Link Aggregation Control Protocol
<b>MDC</b>	Multitenant device context
<b>MOF</b>	Management of Functions
<b>MPLS</b>	Multiprotocol Label Switching
<b>MTD</b>	Management of TSF Data
<b>NDPP</b>	Protection Profile for Network Devices
<b>OAA</b>	Open Application Architecture
<b>OSP</b>	Organization Security Policy
<b>OSPF</b>	Open Shortest Path First
<b>PP</b>	Protection Profile
<b>QoS</b>	Quality of Service
<b>RADIUS</b>	Remote Authentication Dial In User Service
<b>RPC</b>	Remote procedure call

## VALIDATION REPORT

### Hewlett-Packard 6125XLG Ethernet Blade Switch

<b>RSA</b>	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
<b>SA</b>	Security Association
<b>SAR</b>	Security Assurance Requirement
<b>SFP</b>	Security Function Policy
<b>SFR</b>	Security Functional Requirement
<b>SHA</b>	Secure Hash Algorithm
<b>SM</b>	Security Management
<b>SMR</b>	Security Management Roles
<b>SOF</b>	Strength of Function
<b>SSH</b>	Secure Shell
<b>ST</b>	Security Target
<b>TACACS</b>	Terminal Access Controller Access Control System
<b>TOE</b>	Target of Evaluation
<b>TRILL</b>	Transparent Interconnection of Lots of Links
<b>TSC</b>	TSF Scope of Control
<b>TSF</b>	TOE Security Functions
<b>TSP</b>	TOE Security Policy
<b>UAU</b>	User Authentication
<b>UDP</b>	User Data Protection
<b>VLAN</b>	Virtual Local Area Network

## 14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

- [1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 4, September 2012.
- [2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 4, September 2012.
- [3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.
- [4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012.
- [5] Hewlett-Packard Company 6125XLG Ethernet Blade Switch Security Target, v2.0, February 19, 2015
- [6] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.
- [7] Evaluation Technical Report For Hewlett-Packard Company 6125XLG Ethernet Blade Switch, parts 1 and 2 (and associated AAR and test report), version 2.0, February 20, 2015