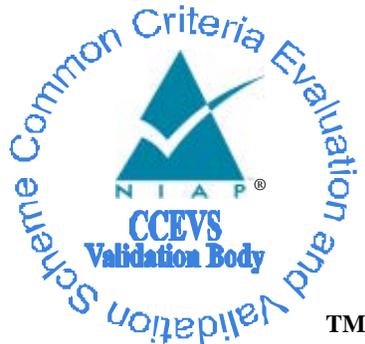


# **National Information Assurance Partnership**



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

**for**

### **Hewlett-Packard Company 6125 Ethernet Blade Switch Series**

**Report Number: CCEVS-VR-VID10549-2014**

**Dated: June 30, 2014**

**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 .....	4
2.1	Threats.....	4
2.2	Organizational Security Policies.....	5
3	Architectural Information .....	6
4	Assumptions	8
4.1	Clarification of Scope .....	8
5	Security Policy .....	9
5.1	Security Audit .....	9
5.2	Cryptographic Support.....	9
5.3	User Data Protection .....	9
5.4	Identification and Authentication .....	9
5.5	Security Management .....	9
5.6	Protection of the TSF.....	9
5.7	TOE Access .....	10
5.8	Trusted Path/Channels .....	10
6	Documentation .....	11
7	Independent Testing.....	13
8	Evaluated Configuration .....	14
9	Results of the Evaluation .....	15
10	Validator Comments/Recommendations .....	16
11	Annexes 17	
12	Security Target.....	18
13	Abbreviations and Acronyms .....	19
14	Bibliography .....	20

VALIDATION REPORT  
HP 6125 Ethernet Blade Switch Series

## List of Tables

Table 1: Switches in the Evaluated Configuration .....	1
Table 2: Evaluation Details.....	2
Table 3: ST and TOE Identification.....	4

VALIDATION REPORT  
HP 6125 Ethernet Blade Switch Series

## 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 of Hewlett-Packard Company 6125 Ethernet Blade Switch Series with Comware version 5.2 Series (hereinafter referenced as HP 6125). 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 HP 6125 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 June 2014. 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 HP 6125 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 Company 6125 Ethernet Blade Switch Series with Comware version 5.20.99, Release 2108. The network on which it resides is considered part of the operational environment.

**Table 1: Switches in the Evaluated Configuration**

Hardware	Picture	Size	Interfaces
HP 6125G Blade Switch		10.5 x 7.5 x 1.1 in	sixteen 1GB downlink (server) ports up to eight 1GB uplink ports up to two 10 GB IRF stacking ports one 10GB cross-link port

VALIDATION REPORT  
HP 6125 Ethernet Blade Switch Series

Hardware	Picture	Size	Interfaces
HP 6125G/XG Blade Switch		10.5 x 7.5 x 1.1 in	sixteen 1GB downlink server ports a combination of 1GB and 10GB uplink ports one 10GB crosslink port.

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PPs had been completed successfully and that the product satisfies all of the security functional and assurance requirements stated in the ST. Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

**Table 2: Evaluation Details**

Item	Identifier
<b>Evaluated Product</b>	Hewlett-Packard Company 6125 Ethernet Blade Switch Series with Comware version 5.20.99, Release 2108
<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>	June 2014
<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

VALIDATION REPORT  
HP 6125 Ethernet Blade Switch Series

<b>Item</b>	<b>Identifier</b>
<b>Disclaimer</b>	The information contained in this Validation Report is not an endorsement of the HP 6125 Ethernet Blade Switch Series by any agency of the U.S. Government and no warranty of HP 6125 Ethernet Blade Switch Series is either expressed or implied.
<b>Evaluation Personnel</b>	Katie Sykes Chris Keenan Pascal Patin
<b>Validation Personnel</b>	Paul Bicknell CISM, CISSP Brad O'Neill

VALIDATION REPORT  
HP 6125 Ethernet Blade Switch Series

## 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 3: ST and TOE Identification**

<b>Name</b>	<b>Description</b>
ST Title	Hewlett-Packard Company 6125 Ethernet Blade Switch Series Security Target
ST Version	2.3
Publication Date	June 26, 2014
Vendor	Hewlett-Packard Company
ST Author	Leidos (formerly SAIC)
TOE Reference	Hewlett-Packard Company 6125 Ethernet Blade Switch Series with Comware version 5.20.99, Release 2108
TOE Hardware Models	HP 6125G Blade Switch HP 6125G/XG Blade Switch
TOE Software Version	Comware version 5.20.99, Release 2108
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.

VALIDATION REPORT  
HP 6125 Ethernet Blade Switch Series

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

## **2.2 Organizational Security Policies**

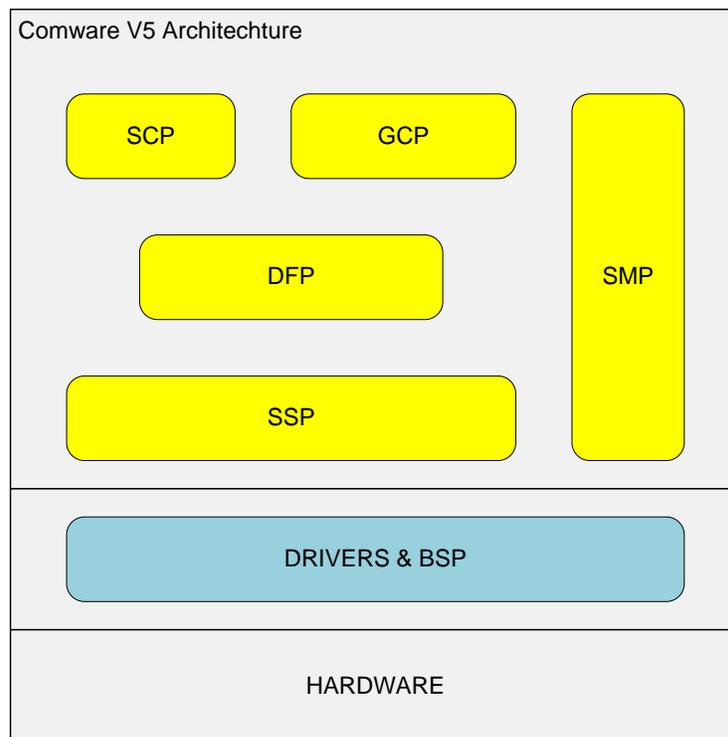
The ST identifies the following organizational security policy that the TOE and its operational environment are intended to fulfill:

- 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.

VALIDATION REPORT  
HP 6125 Ethernet Blade Switch Series

### 3 Architectural Information

The HP 6125 Ethernet Blade Switch Series devices share a common software code base, called Comware. Comware is special purpose appliance system software that implements an array of networking technology, including: IPv4/IPv6 dual-stacks; a data link layer; layer 2 and 3 routing; Ethernet switching; VLANs; Intelligent Resilient Framework (IRF); routing; and Quality of Service (QoS). The evaluated version of Comware is 5.20.99, Release 2108. It should be noted that although Comware runs on a variety of underlying architectures including VxWorks, Linux, pSOS and Windows, the only underlying architecture found in the evaluated configuration is Linux kernel 2.6.26.



**Figure 1: Comware v5.2 Architecture**

- **General Control Plane (GCP)** – The GCP fully supports the IPv4 and IPv6 protocol stacks and provides support to a variety of IPv4/IPv6 applications including routing protocols, voice, WAN link features, and QoS features.
- **Service Control Plane (SCP)** – The SCP supports value-added services such as connection control, user policy management AAA, RADIUS, and TACACS+.
- **Data Forwarding Plane (DFP)** – The DFP underpins all network data processing. The forwarding engine is the core of the DFP.
- **System Management Plane (SMP)** – The SMP provides user interfaces for device management. This includes implementation of a Command Line Interface (CLI) accessible remotely via SSHv2.
- **System Service Plane (SSP)** – The SSP provides a foundation layer that implements primitives on which the other planes rely, for example, memory management, task management, timer management, message queue management, semaphore management, time

VALIDATION REPORT  
HP 6125 Ethernet Blade Switch Series

management, inter-process communication, remote procedure call, module loading management and component management.

Underlying the main Comware components are the hardware-specific Board Support Package (BSP) and device drivers to provide necessary abstractions of the hardware components for the higher-level software components.

The Comware software components are composed of 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 stack, as well as the applicable network protocols and forwarding, routing, etc.

From a security perspective, the TOE includes NIST-validated cryptographic mechanisms that support IPSec, SSH and also digital signatures used to protect the available remote management and to enable secure update capabilities of the TOE. Otherwise, the TOE implements a wide range of network switching protocols and functions.

The various TOE devices include the same security functions. The salient differences between the devices are the available ports and port adapters (supporting different pluggable modules), primarily representing differences in numbers, types, and speeds of available network connections.

## 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
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 utilize external authentication servers.
  - c. Management Workstation – The TOE supports remote CLI access and as such a remote administrator would need a terminal emulator supporting SSHv2 to utilize the administrative interface.

## 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 configured external audit server.

### 5.2 Cryptographic Support

The TOE includes NIST-validated cryptographic mechanisms that provide key management, random bit generation, symmetric encryption/decryption, digital signature services, secure hashing and keyed-hash message authentication capabilities in support of higher level cryptographic protocols, including IPsec and SSHv2. Note that in order to be in the evaluated configuration, the TOE must be configured in FIPS mode, to ensure that the TOE 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 doesn't 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 (CLI via 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 utilize 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 the 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 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).

VALIDATION REPORT  
HP 6125 Ethernet Blade Switch Series

When deployed as an IRF group, all devices that are part of the IRF group are co-located and directly connected to form one instance of the TOE. IRF communication is not considered communication between distributed TOE components; rather, it is communication among co-located components that logically form an instance of the TOE. Since the IRF communication channels are not protected using mechanisms such as encryption, they need to be as protected as the TOE devices themselves.

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 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 administrator-configured advisory banners. A login banner can be configured to display warning information along with login prompts. The banners will be displayed 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 network peers, such as an audit server, using IPsec connections to prevent unintended disclosure or modification of logs.

## 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:

- *Hewlett-Packard Company 6125 Ethernet Blade Switch Series Security Target, Version 2.3, 26 June 2014*
- *Preparative Procedures for CC NDPP Evaluated Hewlett-Packard 6125G and 6125G/XG Network Switches based on Comware V5, Version 1.04, 25 June 2014*
- *Configuration Guide for CC Supplement, Revision 1.03, 25 June 2014*
- *Comware V5 Platform System Log Messages, Revision 1.21, 4 June 2014*
- *Command Reference for CC Supplement, Revision 1.03, 24 June 2014*

The links in Appendix A for the HP 6125 Ethernet Blade Switch Series can be used to find the full set of documentation for the evaluated switch series. The following documents were specifically examined during the evaluation:

- *ACL and QoS Command Reference*
- *ACL and QoS Configuration Guide*
- *Fundamentals Command Reference*
- *Fundamentals Configuration Guide*
- *High Availability Command Reference*
- *High Availability Configuration Guide*
- *Installation Guide*
- *IP Multicast Command Reference*
- *IP Multicast Configuration Guide*
- *IRF Command Reference*
- *IRF Configuration Guide*
- *Layer-2 LAN Switching Command Reference*
- *Layer-2 LAN Switching Configuration Guide*
- *Layer-3 IP Routing Command Reference*
- *Layer-3 IP Routing Configuration Guide*
- *Layer-3 IP Services Command Reference*
- *Layer-3 IP Services Configuration Guide*
- *Network Management and Monitoring Command Reference*
- *Network Management and Monitoring Configuration Guide*
- *Security Command Reference*

VALIDATION REPORT  
HP 6125 Ethernet Blade Switch Series

- *Security Configuration Guide*

On-line documentation for the TOE devices can be found via the following URLs:

- HP 6125G Blade Switch specifications  
[http://h17007.www1.hp.com/us/en/networking/products/switches/HP\\_6125G\\_Blade\\_Switch/index.aspx#.UZ\\_Bbpx8qCg](http://h17007.www1.hp.com/us/en/networking/products/switches/HP_6125G_Blade_Switch/index.aspx#.UZ_Bbpx8qCg)
- HP 6125G/XG Blade Switch specifications  
[http://h17007.www1.hp.com/us/en/networking/products/switches/HP\\_6125GXG\\_Blade\\_Switch/index.aspx#.UZ\\_CCJx8qCg](http://h17007.www1.hp.com/us/en/networking/products/switches/HP_6125GXG_Blade_Switch/index.aspx#.UZ_CCJx8qCg)

**Supporting TOE Guidance Documentation**

- Hewlett-Packard Company 6125 Ethernet Blade Switch Series Security Target, Version 2.3, 26 June 2014

## 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 6125 Ethernet Blade Switch Series, Version 2.0, June 25, 2014

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 NDPPv1.1 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 and via Webex.

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.

VALIDATION REPORT  
HP 6125 Ethernet Blade Switch Series

## **8 Evaluated Configuration**

The evaluated version of the TOE is HP 6125G/XG running Comware version 5.20.99, Release 2108, as installed and configured according to the Preparative Procedures for CC NDPP Evaluated Hewlett-Packard 6125G & 6125G/XG Network Switches based on Comware V5 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 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

VALIDATION REPORT  
HP 6125 Ethernet Blade Switch Series

## **10 Validator Comments/Recommendations**

The validators note that while the TOE will support use of NTP (Network Time Protocol) that it was not submitted for evaluation. Rather, the TOE, in the evaluated configuration, relies upon an internal hardware clock. This is to be considered a shortcoming only in environments where the use of NTP is mandatory.

## **11 Annexes**

Not applicable.

## **12 Security Target**

Hewlett-Packard Company 6125 Ethernet Blade Switch Series Security Target, Version 2.3, 26 June 2014

## 13 Abbreviations and Acronyms

<b>AAA</b>	Authentication, Authorization and Accounting
<b>AAR</b>	Assurance Activities Report
<b>CAVP</b>	Cryptographic Algorithm Validation Program
<b>CC</b>	Common Criteria
<b>CCEVS</b>	Common Criteria Evaluation and Validation Scheme
<b>CCTL</b>	CC Testing Laboratory
<b>CEM</b>	Common Methodology for IT Security Evaluation
<b>CLI</b>	Command Line Interface
<b>EP</b>	Extended Package
<b>ESP</b>	Encapsulating Security Payload
<b>ETR</b>	Evaluation Technical Report
<b>FIPS</b>	Federal Information Processing Standard
<b>IKE</b>	Internet Key Exchange
<b>IPsec</b>	Internet Protocol security
<b>IT</b>	Information Technology
<b>LAN</b>	Local Area Network
<b>NDPP</b>	Network Device Protection Profile
<b>NIAP</b>	National Information Assurance Partnership
<b>NIST</b>	National Institute of Standards and Technology
<b>NSA</b>	National Security Agency
<b>NTP</b>	Network Time Protocol
<b>NVLAP</b>	National Voluntary Laboratory Assessment Program
<b>OS</b>	Operating System
<b>PCL</b>	Product Compliant List
<b>PP</b>	Protection Profile
<b>RADIUS</b>	Remote Authentication Dial In User Service
<b>RFC</b>	Request For Comment
<b>SA</b>	Security Association
<b>SAR</b>	Security Assurance Requirement
<b>SFP</b>	Small Form-factor Pluggable
<b>SFR</b>	Security Functional Requirement
<b>SNMP</b>	Simple Network Management Protocol
<b>SSHv2</b>	Secure Shell version 2
<b>ST</b>	Security Target
<b>TACACS+</b>	Terminal Access Controller Access-Control System Plus
<b>TOE</b>	Target of Evaluation
<b>TSF</b>	TOE Security Functions
<b>TSS</b>	TOE Summary Specification
<b>VPN</b>	Virtual Private Network
<b>VR</b>	Validation Report
<b>WAN</b>	Wide 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 6125 Ethernet Blade Switch Series Security Target, Version 2.3, 26 June 2014
- [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 6125 Ethernet Blade Switch Series, parts 1 and 2 (and associated AAR and test report), version 2.0, June 2014