



# Indian CC Certification Scheme (IC3S)

## Certification Report

**Report Number** : STQC/CC/16-17/18/CR  
**Product / system** : TejNOS EN software Version 6.2 and Version 10.0 running on Tejas Networks POTP/PTN Access Systems Model TJ1400 and TJ1600 respectively

**Dated:** 10<sup>th</sup> Feb 2020

**Version:** 1.0

**Government of India**  
**Ministry of Electronics & Information Technology**  
**Standardization, Testing and Quality Certification Directorate**  
**6. CGO Complex, Lodi Road, New Delhi – 110003**  
**India**

<b>Product developer:</b>	Tejas Networks Limited, Plot no 25, J. P. Software Park, Electronic City, Phase I, Hosur Road, Bangalore 560100
<b>TOE evaluation sponsored by:</b>	Tejas Networks Limited, Plot no 25, J. P. Software Park, Electronic City, Phase I, Hosur Road, Bangalore 560100
<b>Evaluation facility:</b>	Common Criteria Test Laboratory, ERTL (East), DN-Block, Sector V, Salt Lake, Kolkata-700091, India.
<b>Evaluation Personnel:</b>	<b>Evaluators:</b> Malabika Ghose, Manikanta Das, Nishchal & Aniruddha Ghosh <b>Test engineers:</b> Nischal, Sumit & Aniruddha Ghosh
<b>Evaluation report:</b>	STQC IT (KOL)/STQC/CC/16-17/18/ETR/0013
<b>Validation Personnel:</b>	Subhendu Das, Scientist G

## Table of Contents

### Contents

PART A: CERTIFICATION STATEMENT AND BACKGROUND OF THE CERTIFICATION BODY .....	4
A1 Certification Statement .....	4
A2. About the Certification Body .....	4
A3 Specifications of the Certification Procedure .....	5
A4 Process of Evaluation and Certification .....	5
A5 Publication .....	5
PART B: CERTIFICATION RESULTS .....	6
B.1 Executive Summary.....	6
B2 Identification of TOE .....	7
B3 Security policy .....	8
B.4 Assumptions .....	8
B.5 Evaluated configuration.....	8
B6 Document Evaluation .....	12
B7 Product Testing .....	13
B 8 Evaluation Results .....	15
B 9 Validator Comments .....	15
B 10 List of Acronyms.....	16
B 11 References .....	16

## PART A: CERTIFICATION STATEMENT AND BACKGROUND OF THE CERTIFICATION BODY

### A1 Certification Statement

<p>The product below has been evaluated under the terms of the Indian Common Criteria Certification Scheme (IC3S) and has met the stated Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.</p>	
Sponsor	Tejas Networks Limited, Plot no 25, J. P. Software Park, Electronic City, Phase I, Hosur Road, Bangalore 560100
Developer	Tejas Networks Limited, Plot no 25, J. P. Software Park, Electronic City, Phase I, Hosur Road, Bangalore 560100
The Target of Evaluation (TOE)	TejNOS EN software Version 6.2 and Version 10.0 running on Tejas Networks POTP/PTN Access Systems Model TJ1400 and TJ1600 respectively
Security Target	Security Target TejNOS software running on Tejas Networks POTP / PTN Access Systems, Version 1.8
Brief description of product	<p>The TOE is a software only product and the TOE components are specified in software package, running on the TJ1400 / TJ1600 system hardware. TJ1400 Ultra-Converged packet access and aggregation platforms. It provides integration of Access, Transport and IP Network technologies in one integrated box, which is one of the key element of building modern-day telecom infrastructure.</p> <p>The TJ1600 balances Packet and TDM transport. Its hybrid architecture allows for three configurations; TDM with Packet Transport, Hybrid TDM &amp; Packet Transport and all DWDM Optical Transport using the same hardware, software.</p> <p>The TOE is the TejNOS EN software, running on POTP/PTN access system TJ1400 &amp; TJ1600 series of products, for management of the system and control of user data flow. Without TJ1400/TJ1600, TOE won't work alone and vice-versa.</p> <p>TejNOS EN software has the two basic components data plane and control &amp; management plane. The data plane is the part of a network that carries user traffic. Control &amp; management plane manages the security function of the TOE and sets the control for the data flow in the data plane.</p> <p>A proprietary web server, which is a part of the TOE, provides interface for both users and administrators of the TOE. The users submit connection requests via an HTTPS encrypted tunnel.</p> <p><b>TOE shall be installed and managed only in private network through NMS/EMS and not in public network.</b></p>
CC Part 2 [CC-II]	Conformant
CC Part 3 [CC-III]	Conformant
EAL	EAL2
Evaluation Lab	Common Criteria Test Laboratory, ERTL(E), Kolkata
Date Authorized	08-01-2019

### A2. About the Certification Body

STQC IT Certification Services, the IT Certification Body of Standardization Testing and Quality Certification – was established in 1998 and offers a variety of services in the context of security evaluation and validation. It is the first Certification Body in India for BS 7799/ISO 27001 certification of Information Security Management Systems (ISMS). The Indian CC Certification Scheme (IC3S) is the IT security evaluation &

certification Scheme based on Common Criteria standards, it is established by Govt. of India under Department of Information Technology, STQC Directorate to evaluate & certify the trustworthiness of security features in Information Technology (IT) products and systems. The IC3S is an Indian independent third party evaluation and certification scheme for evaluating the security functions or mechanisms of the IT products. It also provides framework for the International Mutual Recognition of such certificates with the member countries of CCRA (Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security). The principal participants in the scheme are:

- a) Applicant (Sponsor/Developer) of IT security evaluations;
- b) STQC Certification Body (STQC/DeitY/MCIT/Govt. of India);
- c) Common Criteria Testing Laboratories (CCTLs).

### A3 Specifications of the Certification Procedure

The certification body operates under the official administrative procedures according to the criteria and procedures laid down in the following:

- ISO/IEC Guide 65, and the requirements laid down in Annex C of CCRA
- Indian Common Certification Scheme (IC3S)
- STQC/CC/DO2: Standard Operating Procedure (SOP) for Certification Body - Quality Manual – describes the quality management system for the Scheme.
- Common Criteria for Information Technology Security Evaluation (CC) part 1-3, Version 3.1
- Common Evaluation Methodology (CEM) Version 3.1.

### A4 Process of Evaluation and Certification

The certification body monitors each individual evaluation to ensure uniform procedures, interpretations of the criteria, and ratings. The TOE has undergone the certification procedure at **STQC IT Certification Body**. The evaluation of the product was conducted by the evaluation body Common Criteria Test Laboratory (CCTL), ERTL (East), DN Block, Sector V, Salt Lake, Kolkata-700091, India. Hereafter this has been referred as CCTL. The evaluation facility is recognized under the IC3S scheme of STQC IT Certification Body.

**Tejas Networks Limited, Plot no 25, J. P. Software Park, Electronic City, Phase I, Hosur Road, Bangalore 560100** is the developer and sponsor of the TOE evaluation.

The certification process is concluded with the completion of this certification report.

This evaluation was completed on 24<sup>th</sup> JAN 2020 after submission of [ETR] to the certification body. The confirmation of the evaluation assurance level (EAL) only applies on the condition that

- all stated condition regarding configuration and operation, as given in part B of this report, are observed,
- The product is operated – where indicated – in the environment described.

This certification report applies only to the version and release of the product indicated here. The validity of the certificate can be extended to cover new versions and releases of the product, provided the applicant applies for re-certification of the modified product, in accordance with the procedural requirements, and provided the evaluation does not reveal any security deficiencies.

### A5 Publication

The following Certification Results consist of Sections B1 to B11 of this report. The TOE will be included in the list of the products certified under IC3S Scheme of STQC IT Certification Body. The list of certified products is published at regular intervals in the Internet at <https://www.commoncriteria-india.gov.in>. Further copies of this certification report may be ordered from the sponsor of the product. The certification report may also be obtained in electronic form on request to the Certification Body.

## PART B: CERTIFICATION RESULTS

### B.1 Executive Summary

#### B.1.1 Introduction

The Certification Report documents the outcome of Common Criteria security evaluation of the TOE. It presents the evaluation results and the conformance results. This certificate is intended to assist the prospective buyers and users when judging the suitability of the IT security of the product for specified requirements.

Prospective buyers and users are advised to read this report in conjunction with the referred [ST] of the product, which specifies the functional, environmental and assurance requirements.

The evaluation was performed by Common Criteria Test Laboratory (CCTL), ERTL (East), DN Block, Sector V, Salt Lake, Kolkata-700091, India. The information in the test report is derived from the [ST] written by the developer and the Evaluation Technical Report [ETR] written by Common Criteria Test Laboratory [ERTL (E)-CCTL], ERTL (EAST), Block-DN Sector-V, Kolkata. The evaluation team determined the product to be CC Version 3.1, Part 2 and Part 3 conformant and concluded that the Common Criteria requirements for Evaluation Assurance Level (**EAL 2**) have been met.

#### B 1.2 Evaluated product and TOE

The TOE is TejnOS EN software Version 6.2 and Version 10.0 running on Tejas Networks POTP/PTN Access Systems Model TJ1400 and TJ1600 respectively .

The evaluated sub-set and configuration of the product is described in this report as the Target of Evaluation (TOE). The Evaluated Configuration, its security functions, assumed environment, architectural information and evaluated configuration are given below (Refer B2 to B5).

#### B 1.3 Security Claims

The [ST] specifies the security objectives of the TOE and the threats that they counter (Refer 3.3 and 4.1 of ST). All the Security Functional Requirements (SFRs) (listed in 6.1 of ST) are taken from CC Part 2.

#### B 1.4 Conduct of Evaluation

The evaluation was initiated by the IC3S Certification Scheme of STQC IT Certification Body vide communication no. STQC/CC/16-17/18.

The TOE as described in the [ST] is TejnOS EN software Version 6.2 and Version 10.0 running on Tejas Networks POTP/PTN Access Systems Model TJ1400 and TJ1600 respectively. The TOE was evaluated through evaluation of its documentation; testing and vulnerability assessment using methodology stated in Common Evaluation Methodology [CEM] and Common Criteria Test Laboratory, ERTL (E), Kolkata, Operating Procedure OP-07.

The evaluation has been carried out under written agreement between Common Criteria Test Laboratory, ERTL (E), Kolkata and the sponsor.

#### B 1.5 Independence of Certifier

The certifier did not render any consulting or other services for the company ordering the certification and there was no relationship between them, which might have an influence on this assessment.

#### B 1.6 Disclaimers

The certification results only apply to the version and release of the product as indicated in the certificate. The certificate is valid for stated conditions as detailed in this report. This certificate is not an endorsement of the IT product by the Certification Body or any other organization that recognizes or gives effect to this certificate. It is also not an endorsement of the target of evaluation (TOE) by any agency of the Government of India and no warranty of the TOE is either expressed or implied.

**B 1.7 Recommendations and conclusions**

- The conclusions of the Certification Body are summarized in the Certification Statement at Section A1.
- The specific scope of certification should be clearly understood by reading this report along with the [ST].
- The TOE should be used in accordance with the environmental assumptions mentioned in the [ST].
- The TOE should be used in accordance with the supporting guidance documentation.
- This Certification report is only valid for the evaluated configurations of the TOE.

**B2 Identification of TOE**

The TOE is the TejNOS EN software Version 6.2 and Version 10.0 running on Tejas Networks POTP/PTN Access Systems Model TJ1400 and TJ1600 respectively. Tejas Network POTP/PTN Access system model TJ1400 and TJ1600 are completely self-contained, housing the software and hardware necessary to perform all functions. The TOE, TejNOS Software has two basic components Data plane and control & management plane. The data plane is the part of a network that carries user traffic. Control and management plane manages the security function of the TOE and sets the control for the data flow in the data plane.

**TOE components along with users’ manuals are listed below:**

S/N	Part Number	Description
1.	142-SW0000130-S	TejNOS EN software Version 6.2 running on Tejas Networks POTP/PTN Access System Model TJ1400, Version 6.2
2.	142-SKU000059-P	TJ1400 POTP / PTN System
3.	170-SW0000034-S	TejNOS EN software Version 10.0 running on Tejas Networks POTP/PTN Access System Model TJ1600, Version 10.0
4.	170-PCA000052-E	TJ1600 POTP / PTN System
5.	142-DOC000110-E	TJ1400 Preparative guidance document, Version 1.8
6.	142-DOC000111-E	TJ1400 Operation guidance document, Version 1.8
7.	170-DOC000097-E	TJ1600 Preparative guidance document, Version 1.8
8.	170-DOC000098-E	TJ1600 Operation guidance document, Version 1.6

The md5 hashes of the TOE instances are as follows:

Running on TJ1400: **“def803822cc77655e98c853b868cdabc”**

Running on TJ1600: **“aefa6860d3b0321d9f6add91e2b3b2c3”**

Physical Environments and boundaries of the TOE

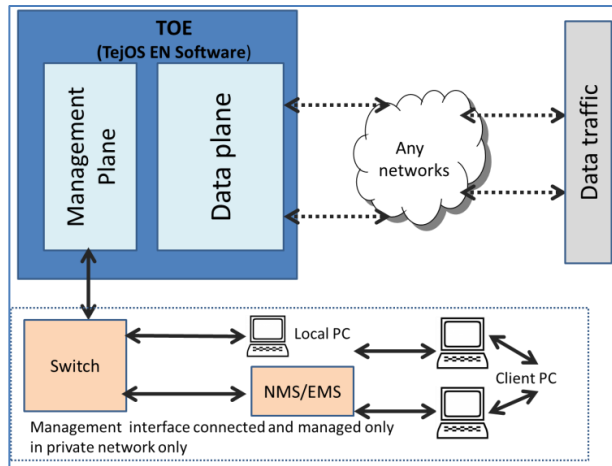


Figure 1: TOE boundary

### B3 Security policy

The TOE is not intended to meet any specific organizational security policy (ies).

### B.4 Assumptions

There are following assumptions exist in the TOE environment.

A.Type	Description
A.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance.
A.PHYSEC	The processing resources of the TOE will be located within controlled access* facilities, which will prevent unauthorized physical access.
A.PUBLIC	The TOE does not host public data.
A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

\* ST Assumes that TOE shall be installed and managed only in private network through NMS/EMS and not in public network

### B.5 Evaluated configuration

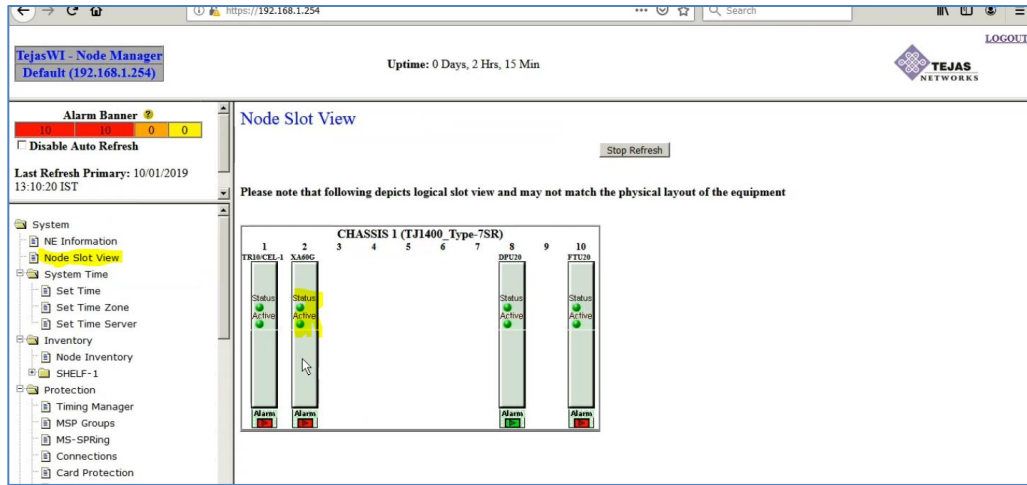
TejNOS EN software Version 6.2 and Version 10.0 running on Tejas Networks POTP/PTN Access Systems Model TJ1400 and TJ1600 respectively.

**TOE configuration:**

#### Hardware Environment

##### TJ1400 Hardware

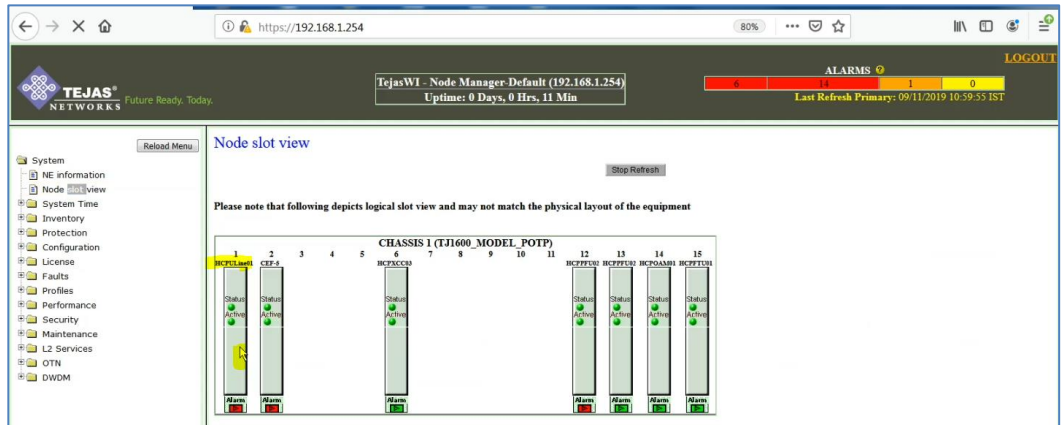




**Figure 2: TJ1400 Chassis**

#	CARD NO /PART NO	Description
1	TJ1400 Type 7SR	Chassis
2	XA60G	Cross connect Card (TOE V 6.2 installed on this HW)
3	TR10/CEL-1	Cross connect Card
4	DPU20	Cross connect Card
5	FTU20	Cross connect Card

**TJ1600 Hardware**

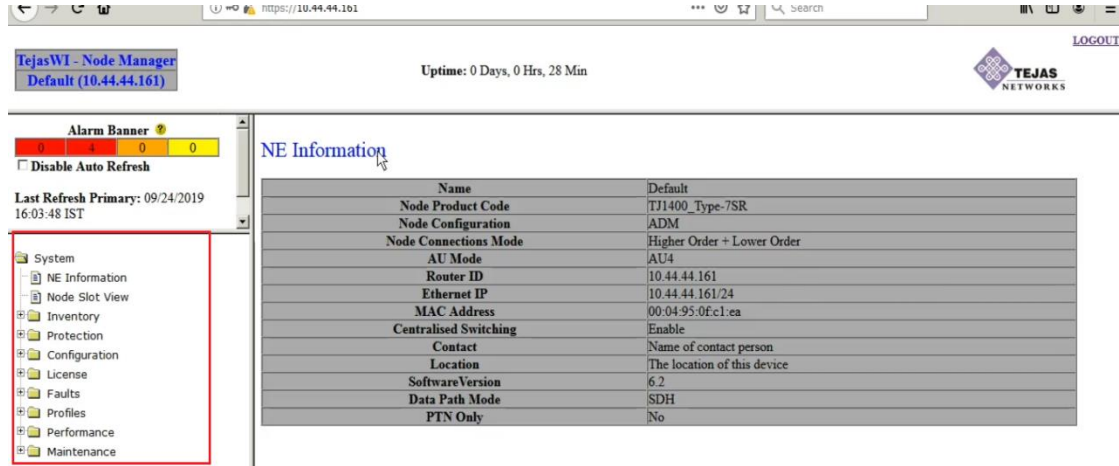


**Figure 3: TJ1600 Chassis**

#	CARD NO /PART NO	Description
1	TJ1600 Model POTP	Chassis
2	HCPXCC03	Cross connect Card(TOE 10.0 installed on this HW)
3	HCPULise01	Cross connect Card
4	CEF-5	Cross connect Card
5	HCPPFU02 (2)	Cross connect Card
6	HCPPOAM01	Cross connect Card
7	HCPFTU01	Cross connect Card

## TOE Software configuration

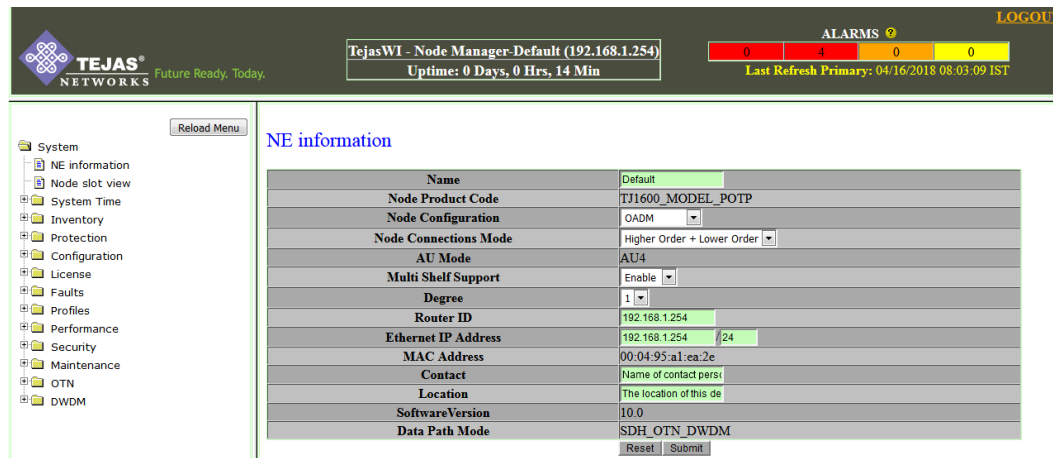
### TJ1400 Software



The screenshot shows the 'NE Information' page in the TejasWI Node Manager. The interface includes a navigation menu on the left with categories like System, NE Information, Node Slot View, Inventory, Protection, Configuration, License, Faults, Profiles, Performance, and Maintenance. The main content area displays a table of system parameters.

Name	Default
Node Product Code	TJ1400_Type-7SR
Node Configuration	ADM
Node Connections Mode	Higher Order + Lower Order
AU Mode	AU4
Router ID	10.44.44.161
Ethernet IP	10.44.44.161/24
MAC Address	00:04:95:0E:c1:ea
Centralised Switching	Enable
Contact	Name of contact person
Location	The location of this device
SoftwareVersion	6.2
Data Path Mode	SDH
PTN Only	No

Figure 4: TOE Identification: Software Version 6.2 running on TJ1400



The screenshot shows the 'NE information' page in the TejasWI Node Manager for a TJ1600 device. The interface includes a navigation menu on the left with categories like System, NE information, Node slot view, System Time, Inventory, Protection, Configuration, License, Faults, Profiles, Performance, Security, Maintenance, OTN, and DWDM. The main content area displays a table of system parameters.

Name	Default
Node Product Code	TJ1600_MODEL_POTP
Node Configuration	OADM
Node Connections Mode	Higher Order + Lower Order
AU Mode	AU4
Multi Shelf Support	Enable
Degree	1
Router ID	192.168.1.254
Ethernet IP Address	192.168.1.254 /24
MAC Address	00:04:95:a1:ea:2e
Contact	Name of contact pers
Location	The location of this de
SoftwareVersion	10.0
Data Path Mode	SDH_OTN_DWDM

Figure 5: TOE Identification: Software Version 10.0 running on TJ1600

```
cctl@kali:~$ ssh tejas@10.44.44.161
This system is provided only for authorized use. The system is monitored for
all lawful purposes, including to ensure that its use is authorized, for
management of the system, to facilitate protection against unauthorized
access, and to verify security procedures, survivability and operational
security. Unauthorized use may subject you to criminal prosecution. Evidence
of any such unauthorized use collected during monitoring may be used for
administrative, criminal or other adverse action.

----- (c) 2000 - 2019 Tejas Networks. All Rights Reserved -----
| NOTICE: Unauthorized access to this system is forbidden and may be
| prosecuted by law. Tejas Networks TJ1400 OPTICALTejas Networks
| TJ1400_Type-7SR-OPTICAL
-----

Password:
Default> cd /etc/bin/tejas
Default> ls
lost+found
xa60g-ppc-REL_6_2_0_a75_1_55.squash.img
Default> md5sum xa60g-ppc-REL_6_2_0_a75_1_55.squash.img
def803822cc77655e98c853b868cdabc xa60g-ppc-REL_6_2_0_a75_1_55.squash.img
Default>
```

Figure 6: The MD5 hash of the TOE on TJ1400

```

cctl@kali:~$ ssh tejas@192.168.1.254
The authenticity of host '192.168.1.254 (192.168.1.254)' can't be established.
RSA key fingerprint is SHA256:CQtbPwiqZ9wwMfppf5GRLT9FVkcxLDeHR+qpi3ghGKXg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.254' (RSA) to the list of known hosts.
This system is provided only for authorized use. The system is monitored for
all lawful purposes, including to ensure that its use is authorized, for
management of the system, to facilitate protection against unauthorized
access, and to verify security procedures, survivability and operational
security. Unauthorized use may subject you to criminal prosecution. Evidence
of any such unauthorized use collected during monitoring may be used for
administrative, criminal or other adverse action.

----- (c) 2000 - 2012 Tejas Networks. All Rights Reserved -----
| NOTICE: Unauthorized access to this system is forbidden and may be   |
| prosecuted by law. Tejas Networks TJ1600_MODEL_POTP_OPTICAL         |
-----

Password:
Default> cd /etc/bi/tejas
-bash: cd: /etc/bi/tejas: No such file or directory
Default> cd /etc/bin/tejas
Default> ls
lost+found
xcc360g-ppc-REL_10_0_2_a49_25.squash.img
Default> md5sum xcc360g-ppc-REL_10_0_2_a49_25.squash.img
aefa6860d3b0321d9f6add91e2b3b2c3 xcc360g-ppc-REL_10_0_2_a49_25.squash.img
Default>

```

**Figure 7: The MD5 hash of the TOE on TJ1600**

The md5 hash of the TOE as given below

Running on TJ1400: **“def803822cc77655e98c853b868cdabc”**

Running on TJ1600: **“aefa6860d3b0321d9f6add91e2b3b2c3”**

The TOE is necessary to be configured as per preparative procedure document to arrive at secure configuration.

## B6 Document Evaluation

### B.6.1 Documentation

The list of documents, those were presented, as evaluation evidences to the evaluators at the evaluation facility, are given below:

1. **Security Target:** Security Target TejNOS software running on Tejas Networks POTP / PTN Access Systems, Version 1.8 , P/N: 999-DOC000056-E
2. **TOE Architecture:** Design and Architecture Of TejNOS software running on Tejas Networks POTP / PTN Access Systems [Version: 1.9], P/N: 999-DOC000058-E
3. **TOE Functional Specification:** Functional Specifications (ADV\_FSP.2) Security Target TejNOS software running on Tejas Networks POTP / PTN Access Systems [Version: 8.0]P/N: 999-DOC000057-E
4. **TOE Design description:** Design and Architecture Of TejNOS software running on Tejas Networks POTP / PTN Access Systems [Version: 1.9], P/N: 999-DOC000058-E
5. **Preparative Guidance:** TJ1400 Preparatory Procedure, Version 1.8 & TJ1600 Preparatory Procedure, version 1.8
6. **Operational Guidance:** TJ1400 Operation Manual, Version 1.8 & TJ1600 Operation Manual, Version 1.6
7. **Configuration Management Capability :** Life-cycle Support process Tejas Networks POTP / PTN Access Systems, Version 1.6
8. **Configuration Management Scope:** Life-cycle Support process Tejas Networks POTP / PTN Access Systems, Version 1.6
9. **TOE delivery:** Life-cycle Support process Tejas Networks POTP / PTN Access Systems, Version 1.6
10. **Test cases, logs and coverage:** Family Functional tests and Coverage (ATE\_FUN & ATE\_COV) TejNOS software running on Tejas Networks POTP / PTN Access Systems, Version: 1.6

### B.6.2 Analysis of document

The documents related to the following areas were analyzed using [CEM]. The summary of analysis is as below:

**Development process:** The evaluators analyzed the functional specification of the TOE and found that the TOE security function interfaces are described clearly and unambiguously. The evaluators also analyzed design and architectural descriptions of the TOE and determined that the only subsystem of the TOE (i.e. router subsystem) is clearly described in the design description. The evaluators determined that architectural description of the TOE includes secure initialization of the TOE and means of protection of the TOE from tampering and bypassing.

**Guidance Documents:** The evaluators analysed guidance documents like preparative procedure and operational user guidance and determined that preparative procedure describes clear and unambiguous steps to bring the TOE to its secure state. The operational user guidance information were also clear and unambiguous.

**Life-cycle support documents:** The Life cycle support process document, containing information on Configuration Management and Delivery Procedure were evaluated.

**Configuration management:** The evaluators analyzed configuration management documentation and determined that the TOE and its associated documents are clearly identified as configurable items. The evaluators also analyzed access control measures defined in the documentation and found satisfactory.

**Delivery procedure:** The delivery procedure document was audited with the objective to ascertain whether it covers secure delivery of the TOE to the end-users. The secure delivery procedure has been described in the document and the same has been audited by the evaluators during their virtual site visit. The end-users can check integrity of the evaluated TOE using hash value of that, if felt necessary.

The final version of the respective evaluation evidences were found to be complied with the requirements of CCv3.1 for **EAL 2**.

## **B7 Product Testing**

Testing at **EAL 2** consists of the following three steps:

- i. Testing by the developer,
- ii. Independent Testing by Evaluation Team
- iii. Penetration testing by Evaluation Team.

### **B 7.1 IT Product Testing by Developer**

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the [ETR].

The evaluators analysed the developer's test coverage and found them to be **complete** and **satisfactory**. The correspondence between the tests identified in the developer's test documentation and the functional specification and TOE design was **complete**.

### **B 7.2 IT Product Independent Testing by Evaluation Team**

The evaluators' independent functional testing effort is summarized as below.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and reproducibility of results.

The evaluators have examined the TOE and it is found to be configurable as per the description given in the

developer's preparative guidance document. It is also observed that the test configuration is consistent with the description as given in the security target document. Highlights of Independent testing are given below:

The TOE has been installed properly as per the preparative procedure document.

The evaluators have repeated the developer's test at CCTL, Kolkata to confirm the reproducibility of the test results.

While making the test strategy for independent testing, consideration is given to cover the security requirements, as well as the security specification as defined in the security target, interfaces available to the users to cover each of security functional requirements, TOE design and security architecture information. Independent testing is designed to verify the correct implementation of security functionalities available to different levels of users and to check whether audit is being generated for auditable events.

The tests were designed to cover following TSFs and associated TSFIs of the TOE:

**a. Security Audit**

To ensure that the TOE generates audit records for security events. The administrator is the only role who can access the audit trail and view the same

**b. Cryptographic Operations**

To ensure that the TOE supports secure communications between users and the TOE and between the TOE components. This encrypted traffic prevents modification and disclosure of user information.

**c. User Data Protection and Protection of the TSF**

To ensure that the TOE provides an information flow security policy. The security policy limits traffic to specified ports.

**d. Identification and Authentication**

TOE provides an information flow security policy. The security policy limits the flow of the traffic (direction) to specified ports.

**e. Security Management**

To ensure that all users are required to be Identified and authenticated before any management actions are performed.

**f. TOE Access**

To ensure that the TOE provides time initiated termination of any interactive session that is open for a more than specified duration.

**g. Time Stamps**

To ensure that the TOE provides a timestamp for its own use. The timestamp is generated from the clock provided in the hardware.

**h. Trusted Path**

To ensure that the connection to and from the TOE are protected using the protocols mentioned within the Cryptographic Support section (of the ST). Trusted paths are used to secure all user sessions through HTTPS. All connections for the TOE are protected using the HTTPS cryptographic mechanism

### **B 7.3 Vulnerability Analysis and Penetration testing**

The evaluators have considered the threats identified in ST and conducted vulnerability search from the information available in the public domain and in the evaluation evidences .The Vulnerability Analysis has

been performed through following three stages:

1. Identification of potential vulnerabilities:
2. Assessment of the identified vulnerabilities: To determine whether those vulnerabilities could allow an attacker with the relevant attack potential to violate the SFRs. The attack potentials for security vulnerabilities, identified, were calculated using method given in Annex B of CEM [v3.1].
3. Penetration testing: To determine whether the identified potential vulnerabilities are exploitable in the operational environment of the TOE. The vulnerabilities with '**Basic**' attack potential were considered for penetration testing.

The attacks with higher than '**Basic**' attack potential are treated as residual vulnerabilities

Evaluation team has searched from the site <http://web.nvd.nist.gov/> , for publicly known security vulnerabilities using the keyword 'router'.

A scanning has been conducted on the TOE with following plugin set of the tool 'nessus' (Plugin Set for Nessus: 202001022130) to find out presence of hypothesized potential vulnerabilities, identified in the public domain, pertaining to this type of product. Port map scanning has been carried out with 'NMap' tool. Based on the results of Port Scanning, web application security Assessment tool '**Acunetix**' used to find out web application security vulnerabilities, if any.

The relevant attack potentials, corresponding to the identified vulnerabilities have been estimated using guidance given in CEMv3.1, considering various factors like the 'time to identify & exploit', 'expertise required', 'knowledge of the TOE', 'windows of opportunity' and 'equipment required'.

The evaluator conducted Penetration Testing (with spent Attack Potential of 8; within Basic) and could not able to exploit the hypothesized Security vulnerabilities of the TOE, those evolved through analysis of evaluation objects.

Hence, it is concluded that the TOE does not contain any exploitable vulnerability for '**Basic Attack Potential**'.

## **B 8 Evaluation Results**

The evaluation results have been documented in the [ETR].

The TOE was evaluated through evaluation of its documentation, testing and vulnerability assessment using methodology stated in [CEM] and laboratory operative procedure [OP-07].

### **Documentation evaluation results:**

The documents for TOE and its development life cycle were analyzed by the evaluator in view of the requirements of the respective work units of the [CEM]. The final versions of the documents were found to comply with the requirements of CCv3.1 for EAL2.

### **Testing:**

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the TOE '**TejNOS EN software Version 6.2 and Version 10.0 running on Tejas Networks POTP/PTN Access Systems Model TJ1400 and TJ1600 respectively**', behaves as specified in its [ST], functional specification and TOE design.

### **Vulnerability assessment and penetration testing:**

The penetration testing with '**Basic**' attack potential could not exploit the potential vulnerabilities identified through vulnerability assessment.

## **B 9 Validator Comments**

The Validators have reviewed the Evaluation Technical Report [ETR] along with all relevant evaluation evidences, documents, records, etc. and are in agreement with the conclusion made in it i.e.

- **The [ST] has satisfied all the requirements of the assurance class ASE.**
- **The results of evaluation of product and process documentation, testing and vulnerability assessment confirm that TejnOS EN software Version 6.2 and Version 10.0 running on Tejas Networks POTP/PTN Access Systems Model TJ1400 and TJ1600 respectively, satisfies all the security functional requirements and assurance requirements as defined in the [ST]. Hence, the TOE is recommended for EAL2 Certification.**

However, it should be noted that there are no **Protection Profile** compliance claims.

## **B 10 List of Acronyms**

- ACL: Access Control List
- CC: Common Criteria
- CCTL: Common Criteria Test Laboratory
- CEM: Common Evaluation Methodology
- DVS: Development security
- EAL: Evaluation Assurance Level
- ETR: Evaluation Technical Report
- FSP: Functional Specification
- IC3S: Indian Common Criteria Certification Scheme
- IT: Information Technology
- PP: Protection Profile
- ST: Security Target
- TOE: Target of Evaluation
- TDS: TOE Design Specification
- TSF: TOE Security Function
- TSFI: TOE Security Function Interface

## **B 11 References**

1. [CC-I]: Common Criteria for Information Technology Security Evaluation: Part 1: Version 3.1
2. [CC-II]: Common Criteria for Information Technology Security Evaluation: Part 2: Version 3.1
3. [CC-III]: Common Criteria for Information Technology Security Evaluation: Part 3: Version 3.1
4. [CEM]: Common Methodology for Information Methodology: Version 3.1
5. [ST] : Security Target TejnOS software running on Tejas Networks POTP / PTN Access Systems, Version 1.8
6. [ETR]: Evaluation Technical Report No. Report No: STQC/CC/16-17/18 /ETR/0013
7. [OP-07]: CCTL operating procedure