# INDIAN CC CERTIFICATION SCHEME (IC3S)

# CERTIFICATION REPORT

| | |
|---|---|
| **Report Number:** | **STQC/CC/0708/05/CR** |
| **Product / system:** | **Network Operating System Comware Ver.: 5.2 Release No. 1002 (CC)**<br>**(Running on MSR 20, MSR 30, MSR 50, SR 66 and SR 88 series routers)** |

**Dated: 31st Dec 2010**

**Version: 1.3**

**Government of India**

**Ministry of Communication & Information Technology**

**Department of Information Technology**

**Standardization, Testing and Quality Certification Directorate**

**6. CGO Complex, Lodi Road, New Delhi – 110003**

**India**

**Product developer:** H3C Technologies Co. Ltd.,
Hangzhou, China

**TOE evaluation sponsored by**: Hewlett Packard India, 24, Salapuria Arena, Hosur
Main Road, Adugodi, Bangalore -560030, India

(**Original sponsor**: 3COM India Pvt.Limited, Regus, Level 15, EROS Corporate Tower, Nehru Place, New Delhi -110019. Subsequently, 3COM was taken over by Hewlett Packard; hence the present sponsor is Hewlett Packard).

**Evaluation facility**: Common Criteria Test Laboratory (CCTL),
ERTL (East),
DN Block, Sector V, Salt Lake,
Kolkata-700091,
India.

**Evaluation Personnel:** Tapas Bandyopadhyay
Malabika Ghose
Subhendu Das

**Evaluation report:** **STQC/CC/0708/05/ETR**
Version 1.3, dated 31$^{st\ th}$ Dec, 2010

**Validation Personnel**: Arvind Kumar
Mitali Chatterjee

## CONTENTS

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

### A1 Certification Statement

| **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.** | |
|---|---|
| Sponsor | Hewlett Packard India Limited |
| Developer | H3C Technologies Co. Ltd |
| Product and Version | Network Operating System Comware Ver: 5.2 Release No. 1002 (CC) (Running on MSR 20, MSR 30, MSR 50, SR 66 and SR 88 series routers) |
| Brief description of product | The product which is the Target of Evaluation (TOE) is a Network Operating System (NOS) identified as 'Comware', (NOS) Version 5.2, Release No. 1002 (CC). The same NOS running on MSR 20, MSR 30, MSR 50, SR 66 and SR 88 series routers. The router hardware acts as an environment to the TOE. The routing, forwarding, and control functions in all these routers are separated to achieve network management flexibility and security control. |
| CC Part 2 | Conformant |
| CC Part 3 | Conformant |
| EAL | EAL 2 |
| Evaluation Lab | Common Criteria Test Laboratory, ERTL(E), Kolkata |
| Date Authorized | **31st Dec 2010** |

## 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 service for evaluating the security functions or mechanisms of the IT products. It also provides a 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/DIT);
c) Common Criteria Testing Laboratories (CCTLs).

## A.3 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 Schème (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, R3
- Common Evaluation Methodology (CEM) Version 3.1.

## A.4 Process of Evaluation and Certification

The certification body monitors each individual evaluation to ensure uniform procedures, interpretations of the criteria, and ratings. The product Network Operating System Comware Ver: 5.2 Release No. 1002 (CC) (Running on MSR 20, MSR 30, MSR 50, SR 66 and SR 88 series routers) 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 recognised under the IC3S scheme of STQC IT Certification Body.

The developer is H3C Technologies Co. Ltd., Hangzhou, China and sponsor is Hewlett Packard, India Ltd.

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

This evaluation was completed on 27th December, 2010. 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 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.

With regard to the meaning of the evaluation assurance levels (EAL) please refer to part C of this report.

## A.5 Publication

The following Certification Results consist of Sections B1 to B13 of this report. The product Network Operating System Comware Ver: 5.2 Release No. 1002 (CC) (Running on MSR 20, MSR 30, MSR 50, SR 66 and SR 88 series routers)
will be included in the list of the products certified under I3CS Scheme of STQC IT Certification Body. The list of certified products is published at regular intervals in the Internet at http://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

## B1 Executive Summary

### B 1.1 Introduction

**The Certification Report documents the outcome of Common Criteria security evaluation of Network Operating System Comware Ver: 5.2 Release No. 1002 (CC) (Running on MSR 20, MSR 30, MSR 50, SR 66 and SR 88 series routers). 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 Security Target (Section D), 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 Security Target (ST, Ver 1.07) written by the developer Hewlett-Packard Development Company, L.P and the Evaluation Technical report (STQC/CC/0708/05/ETR, ver1.3) written by CCTL, ERTL(East), 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 product evaluated was:

**Network Operating System Comware Ver: 5.2 Release No. 1002 (CC) (Running on MSR 20, MSR 30, MSR 50, SR 66 and SR 88 series routers)**

Routers are appliances that can be used to connect different types of networks or network segments, and are mainly used to forward packets between networks or network segments.

Users of the product fall into two types: the first type is users using the data communication services, referred to as network users; the second type is users performing system configuration management, referred as system administrators. The network users cannot manage the appliance. They can only use the data communication services in the security environments defined by the system administrator.

A system administrator can log in locally through the local management interface (Console port or AUX port) of the router or remotely through SSH, and then use the CLI to configure security functions.

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 in Para 2, 3, 4, 5 and 6 of this Section respectively.

### B 1.3 Security Claims

The Security Target, Para 4.1 specifies the security objectives of the TOE, the threats that they counter the Security Functional Requirements (SFRs) and the security functions. All SFRs are taken from CC Part 2.

The TOE security policy is detailed in the Security Target, para 3.2.

### 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/07-08/07 dated 28th Feb 2009.

All the five configurations as stated in the ST were supplied by the developer in the form of **.bin** files. These files consisted of Comware V5.2 release no. 1002(CC) and respective firmware of each series of router. The MD5 Hash values of the **.bin** files were used to uniquely identify the different configurations of the TOE for which the evaluation result is valid. The **.bin** files were installed and configured by the evaluators on respective hardware platforms (IT environment) as per the preparatory guidance document of the TOE on the respective models for the purpose of evaluation. One model from each series, as given below, was taken up for evaluation:

1. MSR 20 Series: 2011
2. MSR 30 Series 3010
3. MSR 50 Series: 5040
4. SR 66 Series: SR 6602
5. SR 88 Seeoies: SR 8802

The TOE was evaluated through evaluation of its documentation, site visit; testing and vulnerability assessment using methodology stated in Common Evaluation Methodology [CEM Ver3.1] and CCTL, Kolkata Operating Procedure OP-07.

The evaluation has been carried out under written agreement [dated 23-06-2009] between CCTL, Kolkata and the sponsor

### B 1.5 Independence of Certifier

In the last two years, 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 of the product indicated in the certificate and on the stated conditions as detailed in this certification report. This certificate is not an endorsement of the IT product by the Certification Body or any other organisation that recognises 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 Security Target. The TOE should be used in accordance with the environmental assumptions mentioned in the Security Target.

The TOE should be used in accordance with the supporting guidance documentation.

This Certification report is only valid for the evaluated TOE.

## B 2 Identification of TOE and Evaluated Configuration

The TOE is identified as:

| **Network Operating System (NOS)** | **Running on Series (IT hardware environment)** |
|---|---|
| **Comware V5.2** | **MSR 20**<br>MSR 20-11 |
| | **MSR 30**<br>MSR 30-10 |
| | **MSR 50**<br>MSR 50-40 |
| | **SR 66**<br>SR6602 |
| | **SR 88**<br>SR8802 |

*Table 1: TOE Identification*

## B 3 Security policy / Security functions

TOE is intended to protect the IP packets against incorrect routing caused by unauthorized changes in the network configuration. TOE provides the following security functions:

### Audit

The TOE can generate various logs, such as TOE operation logs and event logs. The contents of the logs are compliant with RFC 3164. The audited events of the TOE include: administrative events, SSH access control events, and RADIUS authentication events.

### Identification and authentication

With the unified authentication mechanism provided by NOS - Comware V5.2, the TOE can identify and authenticate users. Comware V5.2 provides RADIUS and LOCAL authentication methods.

### Traffic filtering and routing

The TOE provides the access control list (ACL) function to check packets arriving at each interface and depending on the check results makes permit or deny decisions. An ACL allows the TOE to make access control based on packet information such as source and destination IP address, upper layer protocol fields, and other information.

The TOE forwards traffic to its destination based on the routing table. The routing table includes both entries generated with routing protocols and entries created manually.

### Access control / Security management

Access control is to control access to the services provided by the TOE. Access control uses the identification and authentication function to authenticate users, uses the authorization mechanism to authorize access privileges, and uses the audit function to log user accesses.

The TOE provides the command line interface (CLI) for user account management (used for authentication and authorization), system time setting, and system shutdown and re-start. By providing the access control function for the system management services, the TOE ensures that the functions are accessible only to users authorized with the appropriate management privileges, thus realizing secure management.

### TSF protection

The TOE uses the access control mechanism to protect various system-provisioned services, including TSF. Additionally, Comware V5.2 is not an open generic operating system. Only Comware itself can access the hardware resources such as memory and the operating system services. No third-party IT entities can use such resources.

## B 4 Assumptions

### B 4.1 Personnel Assumptions

| Assumption code | Description |
|---|---|
| A.NOEVIL | The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance. |
| A.TRAIN_AUDIT | Administrators will be trained to periodically review audit logs to identify sources of concern. |

| Assumption code | Description |
|---|---|
| A.TRAIN_GUIDAN | Administrators will be trained in the appropriate use of the TOE to ensure security. |

*Table 2: Personnel Assumptions*

### B 4.2 Physical Environmental Assumptions

| Assumption code | Description |
|---|---|
| A.LOCATE | The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. |

*Table 3: Environmental Assumptions*

### B 4.3 Operational assumptions

| Assumption code | Description |
|---|---|
| A.CONFIDENTIALITY | The hard copy documents that describe the configuration of the TOE, I&A information and Audit storage will be kept confidential and access will be limited to Authorized administrators. |
| A.GENPUR | There are no general-purpose computing capabilities (for example, the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE. |
| A.INTEROPERABILITY | The TOE will be able to function with the software and hardware of other vendors' routers/switches, and the Log Server, and iMC Server on the network. The Log Server, iMC Server and NTP Server should be connected in the internal trusted network. |
| A.LOWEXPT | The threat of malicious attacks aimed at exploiting the TOE is considered low. |
| A.SECSHELL | Administrators shall use SSH or SSL when remotely logging in to the TOE or external servers to access security-related information. |
| A.RADIUSMD5 | When RADIUS is used for remote authentication, make sure that RADIUS has been implemented properly, and 128-bit MD5 protection is performed for the password. |
| A.TIME | The NTP server in the network is available. |

*Table 4: Operational Assumptions*

## B 5 Architectural Information

### B 5.1 Architecture descriptions

The architecture of the Network Operating System - Comware V5.2 can be described in terms of three functional planes, '**Service Core (SC**)plane, '**System Service** Plane **(SSP**) and '**System** Manage Plane **(SMP**)' .

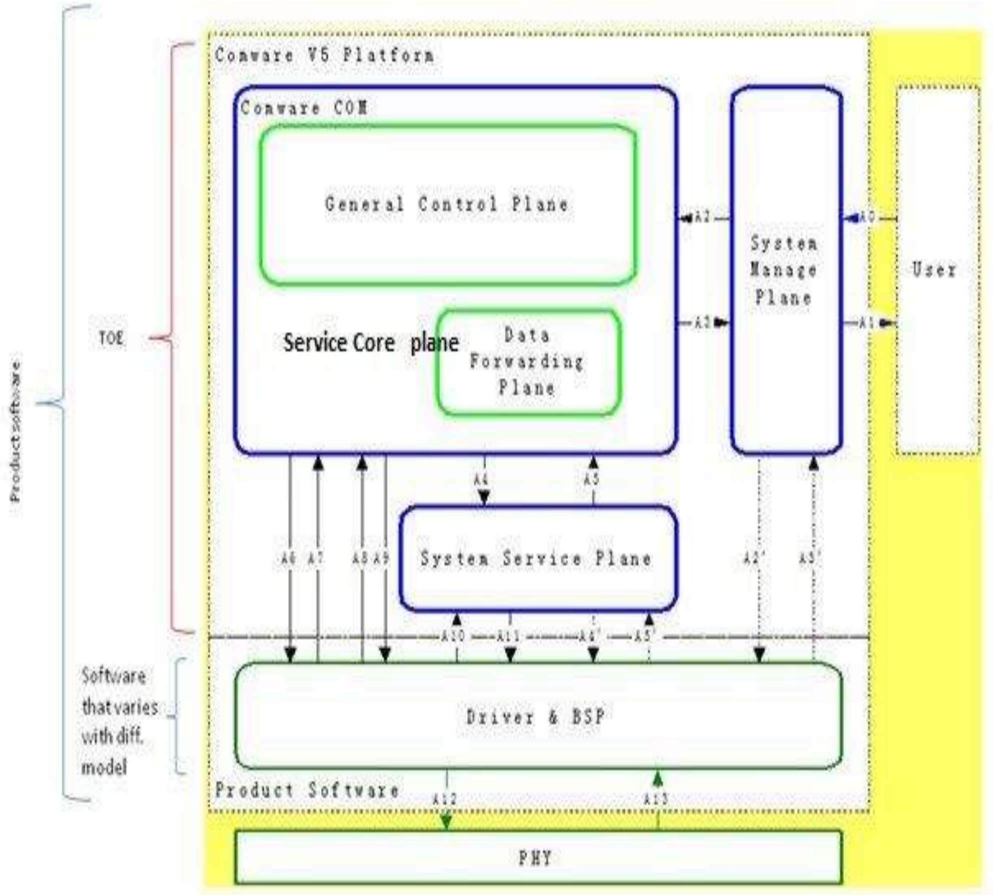

Fig1: TOE architecture diagram

General Control Plane and Data forwarding Plane are jointly known as 'Service **Core (SC**)' Plane. Seven subsystems belong to this plane. They are Protocol stack (PSTK), Forwarding (FDW), Routing (RS), Security (SEC), MPLS, Voice and VPN.

'**System Service** Plane **(SSP**)' consists of OS subsystems. '**System** Manage Plane **(SMP**)' consists of three subsystems configuration Management subsystem (CFM), Information Center (IC) & Interface Management Subsystem (IFM)

So in total, Comware V5.2 is composed of 11 subsystems. Out of 11 subsystems, 8 subsystems are related to TOE Security functions and out of 8 subsystems 4 (PSTK, FWD, RS and IFM) are security-supporting subsystems, and rest 4 (OS, SEC, IC, and CFM ) are security-enforcing subsystems . The subsystems OS, SEC and CFM are directly responsible for some TSF and as well work as supporting subsystems to other TSFs also. Table -2 below indicates the subsystems and their TSF related responsibilities. Other three subsystems of the product, MPLS, Voice & VPN are non TSF subsystems.

The TOE does not provide third-party computing or storage services. A single security domain exists for the TOE. No domain separation exists. All interactions available to the users are severely constrained by the TSF. It is always under the control of the Comware software and all Comware software runs in an address space. The TOE maintains a suit of data structures to identify and isolate user data traffic.

### B 5.2 TOE Sub-systems

| | TSFs | | | | | |
|---|---|---|---|---|---|---|
| Sub system | Audit | Identification & Authentication | Traffic Filtering and Routing | Security Management | Access Control | Protection of the TSF |
| OS | X(supp) | X(supp) | X(supp) | X | X | X |
| SEC | X(supp) | X | X(supp) | X | X | X |
| IC | X | | | | | |
| CFM | X(supp) | X(supp) | | X | X(supp) | |
| IFM | X(supp) | | | | X(supp) | |
| FWD | | | X(supp) | | X(supp) | |
| PSTK | | | X(supp) | | | |
| RS | | | X(supp) | | | |

*Table 5: TOE Sub-systems*

**Note:** X: Security enforcing subsystem X: (supp): Security supporting subsystem

### B 5.3 Hardware and firmware dependencies

The TOE must be configured in the network environment described in Fig 2 and the soft/hard devices forming the network environment.

The following hardware/software/firmware of non-TOE should be acquired additionally:

H3C iMC software
Windows 2000 server or Linux server, where H3C iMC can run
NTP server, which may be required when a router has no hardware clock
A log server as needed
SSH client software

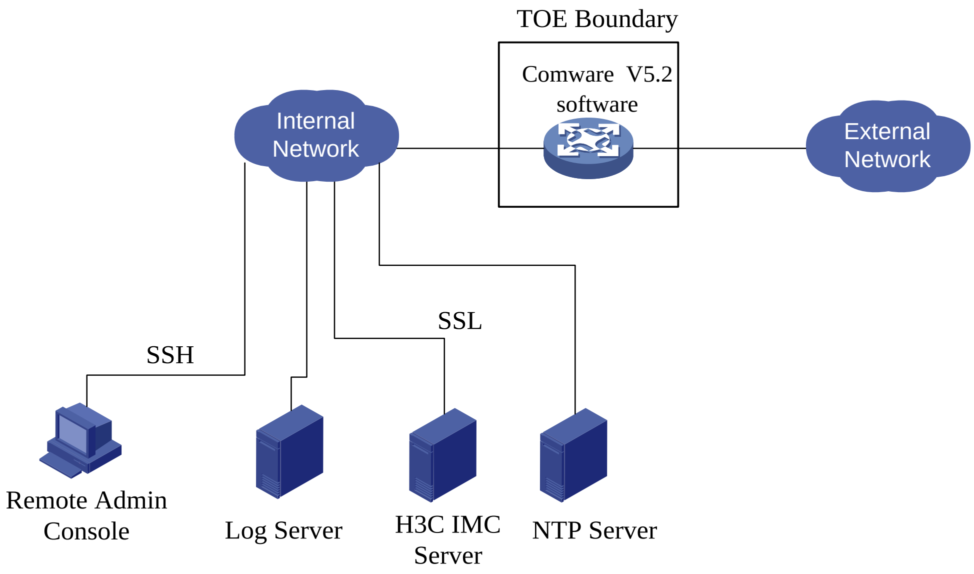

Fig 2

### B 5.4 Product interfaces

Two product interfaces are available:

a) Console port or AUX port of the router for local management
b) Ethernet network interface for IP packet trafficking and remote access of the TOE through SSHv2.

## B 6 Evaluated configuration

The Five configurations of the TOE are stated in the ST. All the five configurations were supplied by the developer in the form of **.bin** files as listed in Table 2 below. The **.bin** files consist of Comware V5.2 release no. 1002(CC) and respective firmware of each series of router. The MD5 Hash values of the **.bin** files are used to uniquely identify the different configurations of the TOE for which this evaluation result is valid. The **.bin** files were installed and configured on respective hardware platforms (IT environment) as per the preparatory guidance document of the TOE on the respective models for the purpose of evaluation.

| **Model no** | **Hardware SN** | **File name (NOS and Firmware)** | **File size** | **MD5 Hash value for the executable** |
|---|---|---|---|---|
| MSR 2011 | 210235A31VB096000020 | MSR201X-CMW520-R1002.bin | 20746 KB | 9af5186d63d2da7e01d98c4e3abe0b7b |
| MSR 3010 | 210235A39HB092000001 | MSR301X-CMW520-R1002.bin | 20499 KB | 1ebc955772682d29cd1aaae8cbbc3f35 |
| MSR 5040 | 210235A20NX099000001 | MSR50-CMW520-R1002-EPUSI.bin | 27578 KB | f62b1bf1d9caacf175cacffb159fe680 |
| SR 6602 | 210235A27DX091000001 | SR6602-CMW520-R1002.bin | 18513 KB | 7c32fbc9f2fcdc711aaccb0d01291325 |
| SR 8802 | 210235A31BX093000002 | SR8800-CMW520-R1002-SI.bin | 27622 KB | 081fdb4a6b13785539bd0ba3ae62fb5b |

*Table 6: Evaluated Configurations of TOE*

## B 7 Documentation

The documents supplied by the developer evaluation evidences to the evaluators at the evaluation facility is attached as **Appendix 2**

.

## B 8 Product Testing

### B 8.1 IT Product Testing by Developer

The developers test effort is summarized as below.

| # | Aspects | Validator's comments |
|---|---|---|
| 1 | On overall developer **testing strategy & approach** employed | The developer has carried out tests, conforming to the TOE security environment (as described in the ST document) and covering all the security functionalities. Testing was done manually. |
| 2 | **On TOE test configurations**: The particular configurations of the TOE that were tested, including whether any privileged code were required to set up the test or clean up afterwards. | The TOE was tested in the defined test configuration consistent with the ST document. |
| 3 | **On depth of testing** in respect of all functionalities of all TSFs: | The developer has carried out testing taking into account all the six TOE security functions ( Audit , Traffic Filtering and Routing, Identification & Authentication, Security Management , Access Control and TSF protection) as described in the ST document and covering all the TSFIs defined in the FSP document. |
| 4 | **On test results:** A description of the overall developer testing results | The results obtained by the developer are consistent, reproducible and matching with the expected results. The tests were repeated at CCTL, Kolkata and it is found that the test results are tallying. |

*Table 7: Developers Test Efforts*

The validator analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was found to be complete.

### B 8.2 IT Product Independent Testing by Evaluation Team

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

| # | Aspects | Validator's comments |
|---|---|---|
| 1 | On overall evaluator **testing strategy & approach** | The evaluators repeated all the developers' tests relating to the security functionalities of the TOE; |

| # | Aspects | Validator's comments |
|---|---|---|
| | | in addition to that they developed test cases that augment the developer tests and conducted the same independently at CCTL, Kolkata. |
| 2 | **On TOE test configurations**: The particular configurations of the TOE that were tested, including whether any privileged code were required to set up the test or clean up afterwards. | The evaluators have examined the TOE, Comware V5.2, Release 1002(CC) and it is found to be configurable as per the description given in the developer's test documentation and results are reproducible. The test configuration is consistent with the description as given in the security target document.<br>The TOE, Comware V5.2, release 1002( CC) have been installed properly as per the preparative procedure AGD_PRE document in the following five router hardware models:<br>MSR 2011, MSR 3010, MSR 5040, SR 6602, SR 8802 |
| 3 | **On depth of testing** in respect of all functionalities of all TSFs | The evaluators have repeated the developer's tests at CCTL, Kolkata to verify the reproducibility of test results and to ensure the coverage of all TSFIs, as mentioned in the FSP document.<br>While making the test strategy for carrying out independent tests, consideration was given to cover all security functional requirements (as defined in the security target), interfaces visible to the users, design and security architecture document of the TOE. Test scenarios were designed to examine the implementation of security features, the management aspects of TSF by different set of users with different privileges and related audit functions. |
| 4 | **On test results:** A description of the overall evaluator testing results | The evaluator conducted tests on the TOE executable delivered by the developer and found some deficiency during testing. The deficiencies were addressed by the developer through new release of the software which was put into next cycle of the test. In this way the TOE went through total 7 iterations during the period of evaluation. The final version of the TOE was found to be in compliance with the ST. |

*Table 8: Evaluators Test Effort*

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

### B 8.3 Vulnerability Analysis and Penetration testing

In search of potential vulnerabilities, the evaluator has conducted public domain search, focussing on the type of the TOE. Following 'urls' have been searched:

- http://nvd.nist.gov/
- http://cwe.mitre.org/

The listed vulnerabilities in the public domain for this type of TOE were analyzed and a filtered list was prepared with those which are candidate for testing The TOE documents like, Security Target (ST), TOE architecture & Design (TDS), TOE Preparatory guidance document etc. were analysed to find out potential security vulnerability. The attack potential for each of the vulnerabilities was calculated using guidance given in CEMv3.1 and considering various factors like the time to identify & exploit the vulnerability, expertise required, knowledge of the TOE, windows of opportunity and equipment requirement. Penetration Test effort

| # | Aspects | Validator's comments |
|---|---|---|
| 1 | On overall evaluator **testing strategy & approach** | The vulnerabilities with basic attack potential and all the filtered vulnerabilities as obtained from the public domain information were selected by Evaluators for Penetration testing. The TOE has two types of users, Authenticated and Unauthenticated. The Authenticated user, accesses the TOE through console, Aux port or through SSH to use CLI to configure the TSFs. The Unauthenticated users access the TOE through network interface (in the form of IP packets), if allowed by ACL rules.These CLI (remote and console) and Ethernet network interfaces were in focus during penetration testing.<br>No other interface was available in the TOE. |
| 2 | **On TOE test configurations**: The particular configurations of the TOE that were tested, including whether any privileged code were required to set up the test or clean up afterwards. | The TOE, Comware V5.2, release 1002(CC) have been installed properly as per the preparative procedure AGD_PRE document in the following five router hardware models:<br>MSR 2011,MSR 3010,MSR 5040, SR 6602,SR 8802 |

| # | Aspects | Validator's comments |
|---|---|---|
| 3 | **On depth of penetration testing** | The penetration testing was conducted by Evaluator considering the listed vulnerabilities with basic attack potential focusing on the issues like bypassing, tampering, direct attack of TSFs, monitoring of secrets and misuse of the privileges. |
| 4 | **On test results:** A description of the overall evaluator penetration testing results | Penetration testing was carried out by Evaluator for each of the identified potential vulnerabilities which are candidate for testing. The evaluator was not able to exploit the identified vulnerabilities. |

*Table 9: Penetration Test Efforts by Evaluators*

Residual vulnerabilities: Considering the attack potential as 'Basic', no identified vulnerabilities could be exploited by the evaluators. Hence the TOE does not contain any exploitable vulnerability for 'Basic Attack Potential'. However, these vulnerabilities may be exploited with higher attack potential. The identified vulnerabilities with more that 'Basic Attack Potential' was not considered for Penetration Testing. Hence, these vulnerabilities may be considered as residual vulnerabilities.

## B 9 Evaluation Results

The evaluation results have been presented by the evaluator in Evaluation Technical Report (ETR) No. STQC IT (KOL)/STQC/CC/0708/05/ETR Version No. 1.3.

The TOE was evaluated through evaluation of its documentation, site visit; testing and vulnerability assessment using methodology stated in Common Evaluation Methodology [CEM Ver3.1] and laboratory operative procedure OP-07.

Documentation evaluation results: The documents for TOE and its development life cycle provided by the developer were analyzed by the Evaluator in view of the requirements of the respective work units of CEM and the same was recorded in work sheets in the ETR. The deficiencies and clarifications, if any, were communicated to the developer by the Evaluator through observation reports [Ors]. The responses of the developer were scrutinized by the evaluator and recorded in the respective work sheets. Further ORs were raised and cycle was carried out for several iterations till all the deficiencies were addressed and requirements for each work units met. The final version of the respective evaluation evidences were found to comply with the requirements of CCv3.1 for EAL 2. The Evaluation Test Report Section 4.0 cover the detailed results of evaluation.

Site visit: The evaluators visited the distribution hub of the developer at Singapore to assess the implementation of the documented delivery process. The products, containing the TOE, are developed and manufactured at H3C 3Com, Hangzhu, China and being distributed through their distribution hub at Singapore. The evaluators performed the sub-activity, 'Site Visit' at the distribution hub at Singapore on 20th March 2010 with an objective to determine whether the developer uses all documented procedure for secure delivery of the product. The evaluators, in their report, have opined for convergence of the practice and the documented procedure. In practice, the procedure followed at the distribution hub was found to be satisfying the requirements of CCv3.1. The developer has subsequently corrected their documented delivery procedure document according to the practice. The site visit report is stated in 3.2.2 and 4.1.3 of Evaluation Rest report. The modified document for 'delivery of the TOE' was found by the Evaluator to be consistent with the practice and satisfies the requirements of the standards [CCv3.1].

The results of Testing (Assessment of Developers Testes, Independent Functional Testing by Developer, Vulnerability Assessment and Penetration Testing are given in Section B 8.

**TOE maturity through evaluation**: The developer submitted the TOE executable for evaluation of the assurance requirements in respect of AGD_PRE.1, ATE_IND.2 and AVA_VAN.2. The deficiencies were brought out by the evaluator and addressed by the developer through new release of the software which was put into next cycle of inspection. In this way the TOE went through total 7 iterations during the period of evaluation. The detail of TOE progress is given in **Appendix VII of ETR**

## B 10 Validator Comments

The Validator has reviewed the Evaluation Technical Report No. STQC IT (KOL)/STQC/CC/0708/05/ETR, Version No. 1.3 and is in agreement with the conclusion of this evaluation.

The Security Target identified as H3C Routers EAL2 Security Target, Version: 1.07 has satisfied all the requirements of Security target evaluation [ASE] as defined in evaluation criteria referred in Section 3.1 for evaluation level EAL 2.

The results of evaluation of product and process documentation, testing and vulnerability assessment confirm that the TOE satisfies all the security functional requirements and assurance requirements as defined in its Security Target document.

Hence, the TOE is recommended for EAL 2 Certification.

However the following should be noted:

- There are no Protection Profile compliance claims

## B 11 List of Acronyms

| | |
|---|---|
| ADM | Administrator Guidance |
| CC | Common Criteria for Information Technology Security Evaluation (referenced to as [CC]) |
| CEM | Common Methodology for Information Technology Security Evaluation (referenced to as [CEM]) |
| CM | Configuration Management |
| EAL | Evaluation Assurance Level |
| FSP | Functional Specification |
| HLD | High-level Design |
| IF | Interface |
| IGS | Installation, Generation and Start-up |
| OSP | Organisational Security Policy |
| PP | Protection Profile |
| SAR | Security Assurance Requirement |
| SF | Security Function |
| SFP | Security Function Policy |
| SFR | Security Functional Requirement |
| SIF | Sub-interface |
| SOF | Strength of Function |
| SS | Sub-system |
| SSL | Secure Sockets Layer |
| ST | Security Target |
| TOE | Target Of Evaluation |
| TSC | TSF Scope of Control |
| TSF | TOE Security Functions |
| TSFI | TOE Security Function Interfaces |
| TSP | TOE Security Policy |
| USR | User Guidance |
| VLA | Vulnerability Analysis |

## B 12 References

1. Common Criteria for Information Technology Security Evaluation: Part 1: Version 3.1
2. Common Criteria for Information Technology Security Evaluation: Part 2: Version 3.1
3. Common Criteria for Information Technology Security Evaluation: Part 3: Version 3.1
4. Common Methodology for Information Methodology: Version 3.1

# B 13 Appendices

## B 13.1 Appendix 1 – List of Tables

## B 13.2 Appendix 2 – List of documents provided by developer as evaluation evidences to the evaluators at the evaluation facility

| Assurance classes and components | | | Evaluation evidences |
|---|---|---|---|
| Security target document evaluation | | ASE | |
| 1 | ST introduction | ASE_INT.1 | H3C Routers EAL2 Security Target Version 1.07 |
| 2 | Conformance claim | ASE_CCL.1 | H3C Routers EAL2 Security Target Version 1.07 |
| 3 | Security problem definition | ASE_SPD.1 | H3C Routers EAL2 Security Target Version 1.07 |
| 4 | Security objectives | ASE_OBJ.2 | H3C Routers EAL2 Security Target Version 1.07 |
| 5 | Extended component definition | ASE_ECD.1 | H3C Routers EAL2 Security Target Version 1.07 |
| 6 | IT Security requirements | ASE_REQ.2 | H3C Routers EAL2 Security Target Version 1.07 |
| 7 | TOE Summary Specification | ASE_TSS.1 | H3C Routers EAL2 Security Target Version 1.07 |
| TOE Development evaluation | | ADV | |
| 1 | Security Architecture | ADV_ARC.1 | Comware 5.2 Design version 1.07 |
| 2 | Functional Specification | ADV_FSP.2 | Functional Specification for Comware V5.2 version 1.02 |
| 3 | Basic design | ADV_TDS.1 | Comware 5.2 Design version 1.07 |
| TOE Guidance document evaluation | | AGD | |
| 1 | Operational user guidance | AGD_OPE.1 | 1. Operation User Guidance for CC EAL2 Evaluated Comware V5.2 Routers version 1.20<br>2. CLI command list for different level of users |
| 2 | Preparative procedure | AGD_PRE.1 | 1. Preparative Procedures for CC EAL2 Evaluated Comware V5.2 Routers version 1.11<br>2. Executables and hardware [table 1-1] |
| TOE Life cycle support evaluation | | ALC | |
| 1 | Use of a CM system | ALC_CMC.2 | Configuration Management Procedure version 1.11 |
| 2 | Parts of the TOE CM coverage | ALC_CMS.2 | Configuration Management Procedure version 1.11 |
| 3 | Delivery procedures | ALC_DEL.1 | Product Delivery Procedure version 1.11 |

| Testing of the TOE | | ATE | |
|---|---|---|---|
| 1 | Evidence of coverage | ATE_COV.1 | 1. ATE_H3C Router EAL2 Test Plan and Test Case V1.02(20091210)_en.doc<br>2. CLI command list for different level of users |
| 2 | Functional Testing | ATE_FUN.1 | 1. ATE_H3C Router EAL2 Test Plan and Test Case V1.02(20091210)_en.doc<br>2. ATE_H3C Router EAL2 test report V1.01(20091210)_en.doc<br>3. CC Authentication Cryptography Commands.doc<br>4. CLI command list for different level of users<br>5. ATE_H3C Router EAL2 Test Documentation_MSR2011.doc<br>6. ATE_H3C Router EAL2 Test Documentation_MSR3010.doc<br>7. ATE_H3C Router EAL2 Test Documentation_MSR5040.doc<br>8. ATE_H3C Router EAL2 Test Documentation_SR6602.doc<br>9. ATE_H3C Router EAL2 Test Documentation_SR8802.doc |
| 3 | Independent Testing - Sample | ATE_IND.2 | TOE Executables and hardware [table 1-1] |
| Vulnerability assessment of the TOE | | AVA | |
| 1 | Vulnerability Analysis | AVA_VAN.2 | TOE Executables and hardware [table 1-1] |

## B 13.3 Appendix 3 – Variation in MSR Series and SR Series routers

Variations in MSR series routers and representative unit of the series tested at CCTL

### MSR 20 Series

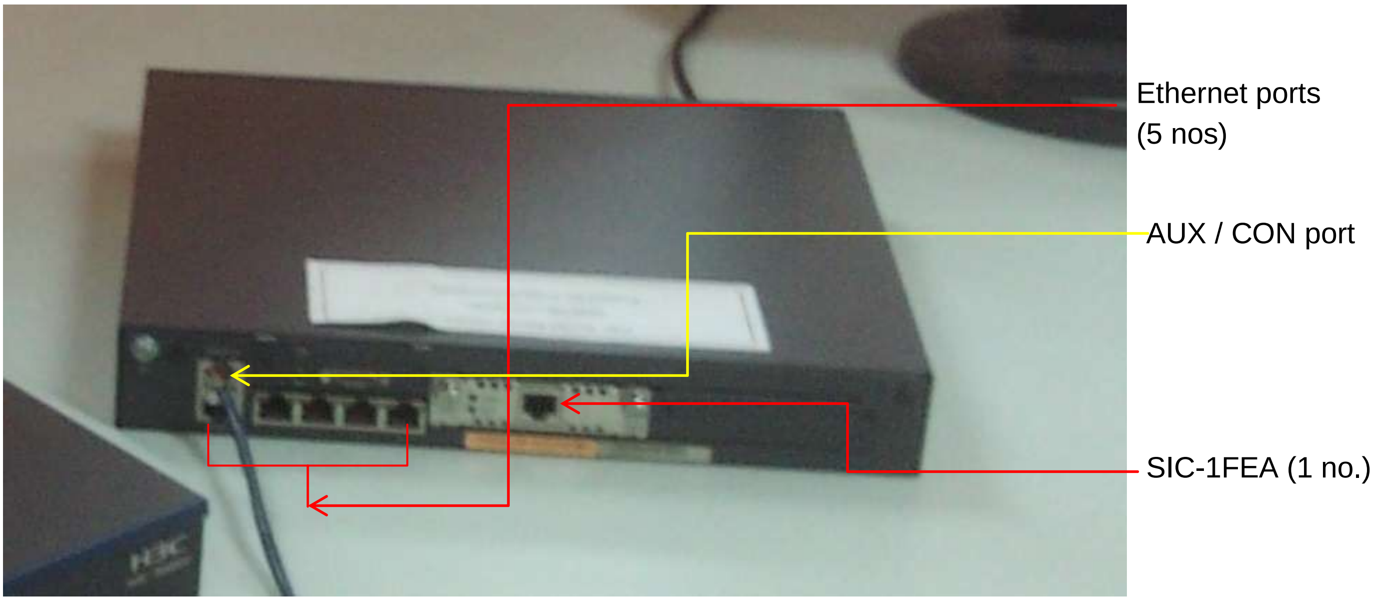

**Figure 1: MSR2011, tested at CCTL, Kolkata**

Across the series, models (MSR2010, MSR2011, MSR2012, MSR2013, MSR2015, MSR2020, MSR2021, and MSR2040) vary in following parameters:

- Processor speed
- Memory size
- Hard disk size
- Removable disk size
- Number of Physical and logical interfaces
- Power consumption
- IPv4 – throughput
- IPSec –ANDE encryption performance
- IPSec – SNDE encryption performance
- IPSec – CPU encryption performance
- SSL VPN – Max number of clients
- SSL VPN – number of SSL connection
- FW – throughput

## MSR 30 Series

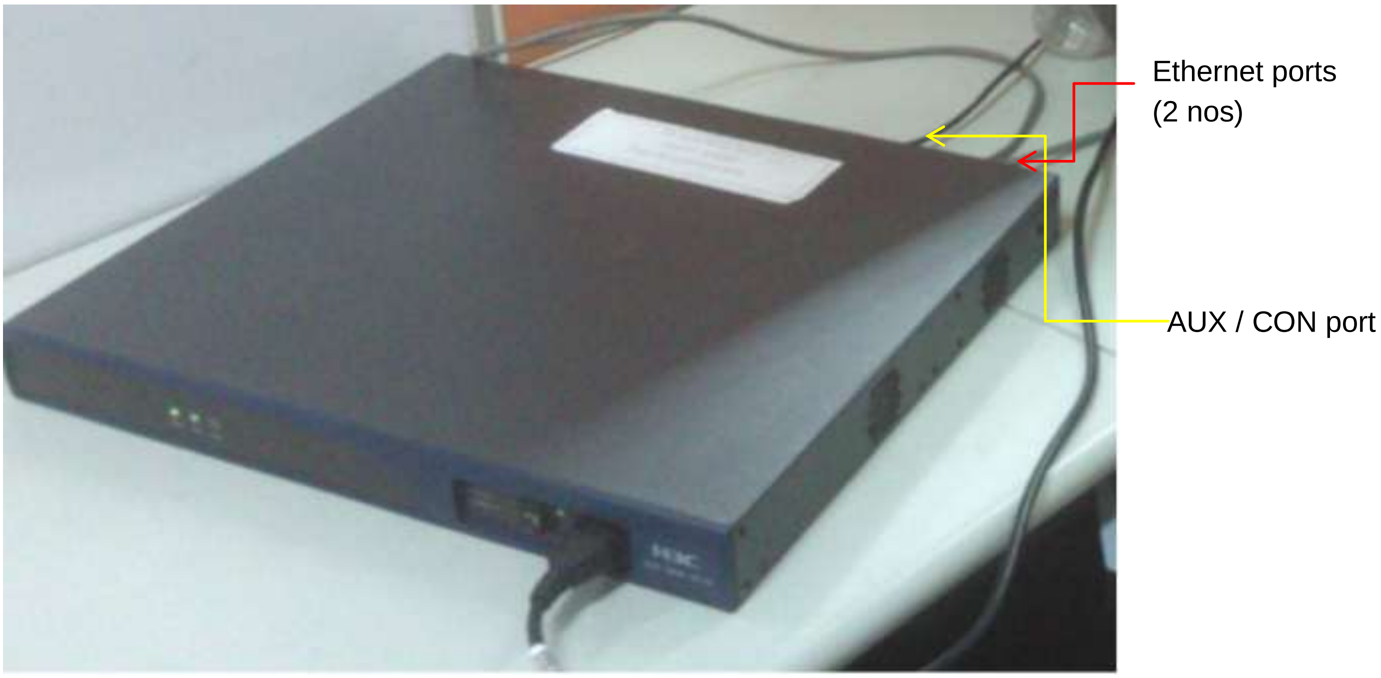

**Figure 2: MSR3010, tested at CCTL, Kolkata**

Across the series, models (MSR3010, MSR3011, MSR3011E, MSR3011F, MSR3016, MSR3020, MSR3040, and MSR3060) vary in following parameters:

- Processor speed
- Memory size
- Hard disk size
- Removable disk size
- Number of USB ports
- Number of Physical and logical interfaces
- Power consumption
- IPv4 – throughput
- IPSec – ANDE encryption performance
- IPSec – SNDE encryption tunnel number
- IPSec – CPU encryption performance
- FW – throughput

## MSR 50 Series

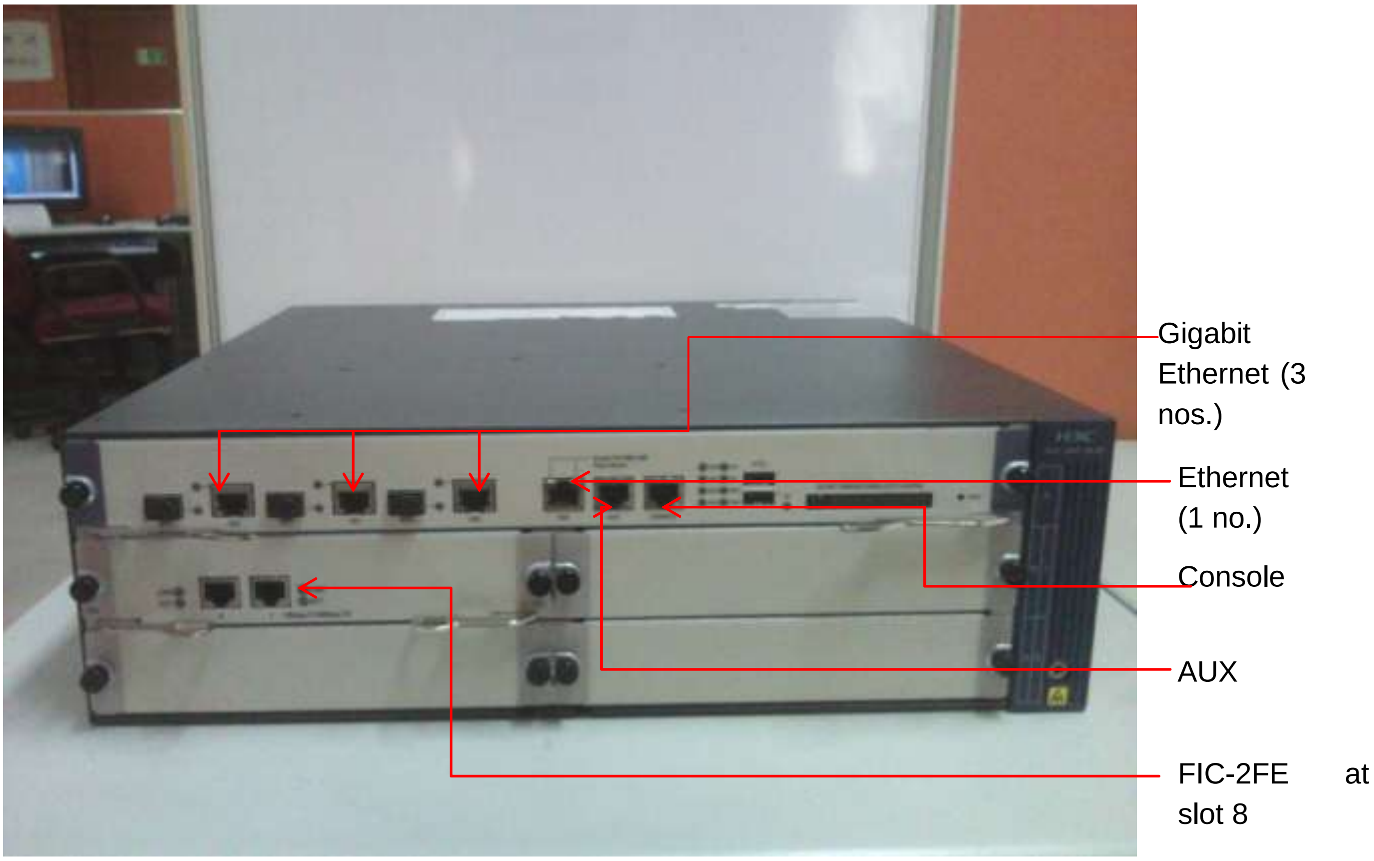

**Figure 3: MSR5040, tested at CCTL,Kolkata**

Across the series, models (MSR 5040, MSR 5060, MSR5040 MPU-G2 and MSR 5060 MPU-G2) vary in following parameters:

- Processor speed
- Memory size
- Hard disk size
- Number of physical and logical interfaces
- WAN protocol – max number of PPPoE connections
- IPv4 – throughput
- Routing protocol – BGP – maximum number of route entrance
- Routing protocol – OSPF – maximum number of route entrance
- Routing protocol – IS_IS – maximum number of route entrance
- MPLS – maximum number of LDP labels
- MPLS – maximum number of dynamic LSP
- NAT – number of concurrent connections
- FW - throughput

Annexure - IX

## Details of variations in hardware configuration and software performance of the MSR series router

### Details of Hrdware variations (MSR series)

| Sl. No | Specification | MSR 20 Series | MSR 30 Series | MSR 50 Series |
|---|---|---|---|---|
| 1 | Processor | RISC,333-400 MHZ | RISC; 400-533 MHz | RISC; 833 -1.7 GHz |
| 2 | Memory (default/max.) | 256MB to 1 GB | DDR; 256 MB-1GB | DDR; 512 M-2G |
| 3 | CF (default/max.) | Up to 1 GB | Max 1 GB | 256 M-1 G |
| 4 | FLASH (default/max.) | 16 Mb | 32 Mb only for MSR 30-11 | 64 M for MPU-G2 models |
| 5 | USB | 1 | Nil for MSR 3011, one for MSR 30-16 and two for others | 2 |
| 6 | AUX | 1 | 1 | 1 |
| 7 | Configuration port | 1 | 1 | 1 |
| 8 | Fixed Ethernet port (L3) | 1 or 2 FE | 2 FE/GE or GE(combo) | 2- 3 GE (combo) |
| 9 | Fixed switching port (L2) | 0-8 slot | 0 | 0 |
| 10 | Other fixed port | 0-1 (DISC or ADSL) | 1(serial) for MSR 30-11 and nil for all models | 1 FE Management interface for MPU-G2 models |
| 11 | SIC slot | Min. 1 and Max.4 | 2 slots for MSR 3011 and 4 slots for others | 4 for MPUF and 0 for MPU-G2 |
| 12 | MIM slot | Nil | 1-6 slots | 0 |
| 13 | FIC slot | Nil | 0 | 4-6 solt |
| 14 | ESM slot | Max 2 | 1 slots for MSR 3011 and 2 slots for others | 2 |
| 15 | VPM slot | Max 2 | 0-3 slot | 4 for MPUF and 0 for MPU-G2 |
| 16 | VCPM slot | 1(max.) for model at the higher end of the series | Nil for MSR 3011 and 1 slot for others | 1 |
| 17 | MiniPCI(WLAN) | Not supported by the models at the higher end of the series | 0 | 0 |

Annexure - IX

| Sl. No | Specification | MSR 20 Series | MSR 30 Series | MSR 50 Series |
|---|---|---|---|---|
| 18 | Real-time clock | Supported in models MSR 20-20 onwards | Support | Support |

**Details of performance variations (MSR series)**

| Sl. No. | Specification | MSR 20 Series | MSR 30 Series | MSR 50 Series |
|---|---|---|---|---|
| 1 | Network Size | 100 | 200 | 500 -1000 |
| 2 | Physical and Logical Interface | | | |
| | Max. Number of L3 FE port | Max. 4 slots | 7-26 ports | 18-26 ports |
| | Max. Number of L3 GE port | max.2 slots | 3-16 ports | 11-15 ports |
| | Max. Number of L2 switching Interface | 8-18 Interfaces | 28-130 Interfaces | 64 -96 ports |
| | Max. Number E1/CE1 port | 1-4 ports | 9-52 ports | 32-48 ports |
| | Max. Number of Synchronous serial ports | 1-4 ports | 10-52 ports | 32-48 ports |
| | Max. Number of Asynchronous serial ports | 8-32 port | 32-112 ports | 64-160 ports |
| | Max. Number of CPOS/POS port | nil | 1-2 Ports | 2-3 port |
| | Max. Number of Voice VE1 port | 0-2 port | 2- 5 ports | 8 port |
| | Max. Number of Voice FXS port | 2-8 ports | 8-32 Ports | 24-32 port |
| | Max. Concurrent voice calls | 2-60 calls | 60-150 calls | 240 calls |
| 3 | LAN Protocol | | | |
| 3.1 | Switch Ethernet | | | |
| | MAC Address table | 2K | 16K | 16 K |
| | Number of VLANs | 256 | 512 | 1024 |
| | Number of VLAN ID | 4094 | 4094 | 4096 |
| 3.2 | WAN Protocol | | | |
| | Max. PPPoE Connection | 512 | 1024 | 2048-4096 |
| 3.3 | Network Layer Protocol | | | |
| 3.3.1 | ARP | | | |

Annexure - IX

| Sl. No. | Specification | MSR 20 Series | MSR 30 Series | MSR 50 Series |
|---|---|---|---|---|
| | Static ARP | 2K | 2K | 2K |
| | Dynamic ARP | 2K | 4K | 4K |
| 3.3.2 | DHCP Server | | | |
| | Address Pool Size | 512 | 512 | 512 |
| 3.3.3 | IPv4 | | | |
| | Throughput (pps) | 64 bytes-180 Kpps | 220-360 Kpps | 800Kpps -2 Mpps |
| 3.3.4 | IPv6 | | | |
| | Throughput (pps) | | | |
| 3.4 | Routing Protocol | | | |
| 3.4.1 | Static Routing | | | |
| | Routing table | 2K | 5K | 10K |
| | Max. ECMP (load-balance) | 8 | 8 | 8 |
| 3.4.2 | RIP | | | |
| | Max. Number of Route Entrance | 1K | 2K | 5K |
| 3.4.3 | OSPF | | | |
| | Max. Number of Route Entrance | 5000 | 10000 | 50000 |
| 3.4.4 | BGP | | | |
| | Max. Number of Route Entrance | 10000 | 30000 | 100000 |
| 3.4.5 | IS_IS | | | |
| | Max. Number of Route Entrance | 5000 | 10000 | 50000 |
| 3.5 | MPLS | | | |
| 3.5.1 | LDP | | | |
| | Max. Number of LDP Labels | 2K | 2K | 8K |
| | Max. Number of Dynamic LSP | 2K | 2K | 8K |
| | Max. Number of Static LSP | 1008 | 1008 | 1008 |
| | Max. Number of MPLS supported interface | 100 | 100 | 100 |
| | Max. Number of Local Peer | 100 | 100 | 100 |

Annexure - IX

| Sl. No. | Specification | MSR 20 Series | MSR 30 Series | MSR 50 Series |
|---|---|---|---|---|
| | Max. Number of Remote Peer | 100 | 100 | 100 |
| | Max. Number of Session | 200 | 200 | 200 |
| 3.5.2 | L3VPN | | | |
| | Max. Number of LSP | 2K | 2K | 4K |
| | Max. Number of VRF | 128 | 128 | 256 |
| | Max. Number of VPN target | 20 | 20 | 20 |
| | Max. Number of interface bounded by a single VRF | 128 | 128 | 256 |
| | Max. Number of VRF bounded interface of the system | 256 | 256 | 512 |
| | Max. Number of route Entrance for a single VRF | 1024 | 1024 | 2048 |
| 3.6 | Multicast | | | |
| | Static Multicast Route | 128 | 256 | 256 |
| | Max. Number of PIM peer | 64 | 128 | 200 |
| | Max. Number of Multicast Host | 256 | 512 | 900 |
| 3.7 | Security Function | | | |
| 3.7.1 | NAT | | | |
| | Number of Address Pool | 8 | 16 | 32 |
| | Size of a single address pool | 255 | 255 | 255 |
| | Concurrent connections | 30000 | 50000 | 25000-50000 |
| | Session established Rate (session/second) | 256 | 512 | 1024 |
| | Total number of Nat Servers in a system | 128 | 256 | 512 |
| 3.7.2 | ACL | | | |
| | Number of Basic ACL | 1000 | 1000 | 1000 |
| | Number of Advanced ACL | 1000 | 1000 | 1000 |
| | Total Number of ACL | 3000 | 3000 | 5000 |

| Sl. No. | Specification | MSR 20 Series | MSR 30 Series | MSR 50 Series |
|---|---|---|---|---|
| | ACL forwarding performance | Impaction on forwarding performance < 10% | Impaction on forwarding performance < 10% | Impaction on forwarding performance < 10% |
| 3.7.3 | IPSec | | | |
| | ANDE encryption performance | 100 Mbps | 250Mbps | 600Mbps |
| | Max Tunnel（ANDE） | 2000 | 2000 | 3000 |
| | SNDE encryption performance | 100Mbps | 100-150 Mbps | 300Mbps |
| | Max Tunnel（SNDE） | 1500 | 1500-2000 | 3000 |
| | CPU encryption performance | 30 Mbps | 30-60 Mbps | 150Mbps |
| | Max Tunnel（CPU） | 500-1000 | 1000 | 1500 |
| 3.7.4 | SSL VPN | | | |
| | Max. Number of Client | 5-50 nos | 100 | 200 |
| | SSL connection | 50- 500 nos | 1000 | 2000 |
| 3.7.5 | L2TP | | | |
| | Max. Number of L2tp Tunnel | 256 | 512 | 1024 |
| | Session established Rate (session/second) | 3 | 6 | 8 |
| 3.7.6 | GRE | | | |
| | Max. Number of Tunnels | 256 | 512 | 1024 |
| 3.7.7 | FW | | | |
| | Throughput (Mbps) | 150-200 Mbps | 200-600Mbps | 3Gbps |
| | Max. Number of Concurrent Connections | 1000 | 30000 | 50000 |
| 3.7.8 | Portal Authentication | | | |
| | Number of concurrent connections | 20 | 20 | 20 |
| | Max. Number of Client | 200 | 500 | 1000 |
| 3.8 | QoS | | | |
| | Length of FIFO Queue | 1024 | 1024 | 1024 |
| | Length of PQ Queue | 1024 | 1024 | 1024 |

Annexure - IX

| Sl. No. | Specification | MSR 20 Series | MSR 30 Series | MSR 50 Series |
|---|---|---|---|---|
| | Length of CQ Queue | 1024 | 1024 | 1024 |
| | Length of WFQ Queue | 1024 | 1024 | 1024 |
| | Length of CBQ Queue | 512 | 512 | 512 |
| | Length of RTPQ Queue | 50 | 50 | 50 |
| | Max. Number of PQ Queue | 4 | 4 | 4 |
| | Max. Number of CQ Queue | 16 | 16 | 16 |
| | Max. Number of WFQ Queue | 4096 | 4096 | 4096 |
| | Max. Number of CBQ Queue | 4096 | 4096 | 4096 |
| | Max. Length of all Queue. | 10000 | 10000 | 10000 |
| | Max. Number of CAR policy | System 1000/Per Interface 135 | System 1000/Per Interface 140 | System 1000/Per Interface 142 |
| | Max. Number of GTS policy | 100 | 100 | 100 |
| | Max. Number of CAR on a single interface | 100 | 100 | 100 |
| | Max. Number of GTS on a single interface | 100 | 100 | 100 |
| 3.9 | VoIP | | | |
| | Max. Delay | 400ms | 400ms | 400ms |
| | Max. Jitter | 60ms | 60ms | 60ms |
| 3.10 | Application | | | |
| 3.10.1 | NQA | | | |
| | Max. simultaneous detect | 5 | 5 | 5 |
| | Max. Number of configurable detect target (group) | 30 | 30 | 30 |
| | Supported protocol | TCP,UDP, Jitter, ICMP | TCP, UDP, Jitter, ICMP, HTTP, FTP, DHCP, DLSw, SNMP | TCP, UDP, Jitter, ICMP, HTTP, FTP, DHCP, DLSw, SNMP |

Annexure - IX

| Sl. No. | Specification | MSR 20 Series | MSR 30 Series | MSR 50 Series |
|---|---|---|---|---|
| | Supported test packet size | CMP,UDP test packet size: 1Byte-8100Bytes. (In the case of ICMP test, if the size value configured is smaller than 20 bytes, the system will automatically stuff the test packet with the padding character string to 20 bytes.) | CMP,UDP test packet size: 1Byte-8100Bytes. (In the case of ICMP test, if the size value configured is smaller than 20 bytes, the system will automatically stuff the test packet with the padding character string to 20 bytes.) | CMP,UDP test packet size: 1Byte-8100Bytes. (In the case of ICMP test, if the size value configured is smaller than 20 bytes, the system will automatically stuff the test packet with the padding character string to 20 bytes.) |
| | Min. interval of test packet | Min. 10ms interval for Jitter detection | Min. 10ms interval for Jitter detection | Min. 10ms interval for Jitter detection |

## Variations in SR series routers and representative unit of the series tested at CCTL

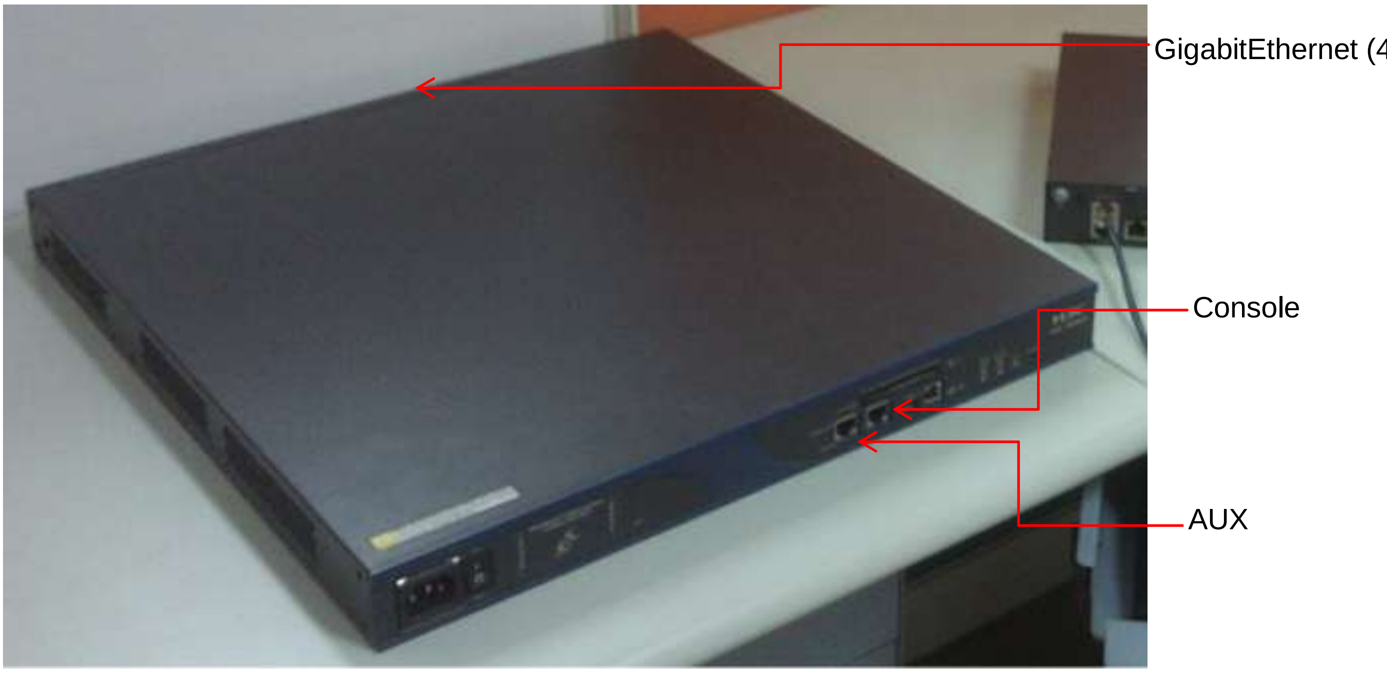

**Figure 4: SR6602**

Across the series, models (SR6602, SR6604, SR6608 and SR6616) vary in following parameters:

- Processor
- Memory size
- CF card size
- Main routing engine
- USB interfaces
- AUX
- Console
- Number of fixed Ethernet interfaces
- Built-in hardware based encryption engine
- Backplane bandwidth
- FIP slots
- HIM slots
- Real time clock
- Power input and consumption
- RPS
- Hot swappable control engine, service engine and power supply

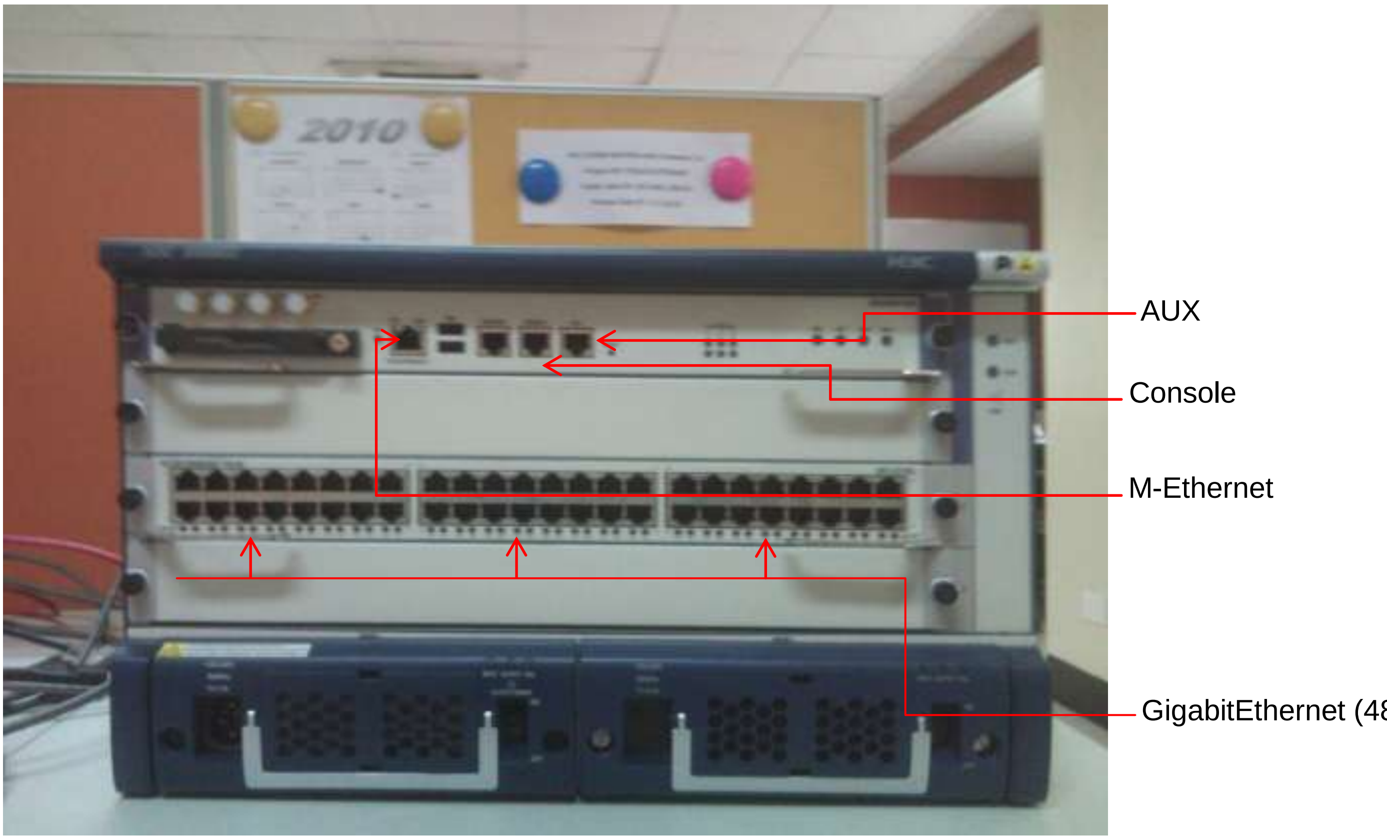

**Figure 5: SR8802, tested at CCTL**

Across the series, models (SR8802, SR8805, SR6608 and SR8812) vary in following parameters:

- Number and orientation of slots
- Packet switching capability
- Packet forwarding performance
- Power supply
- Fan structure
- Weight and dimension

**Details of Hardware variations (SR6600 Series)**

| Sl. No | Specification | SR6602 | SR6604 | SR6608 | SR6616 |
|---|---|---|---|---|---|
| 1 | Processor | MIPS Multicore,1GHZ | MIPS Multicore,1GHZ | MIPS Multicore,1GHZ | MIPS Multicore,1GHZ |
| 2 | Memory (default/max.) | DDR2, 2GB/4GB | DDR2,<br>1GB/2GB | DDR2,<br>1GB/2GB | DDR2,<br>1GB/2GB |
| 3 | CF (default/max.) | 1+1; 256M/2GB | 1+1; 256M/1GB | 1+1; 256M/1GB | 1+1; 256M/1GB |
| 4 | FLASH (default/max.) | 4MB/4MB | 4MB/4MB | 4MB/4MB | 4MB/4MB |
| 5 | USB | 2 | 2 | 2 | 2 |
| 6 | AUX | 1 | 1 | 1 | 1 |
| 7 | Configuration port | 0 | 1 | 1 | 1 |
| 8 | Fixed Ethernet port (L3) | 4 | 2 per line-card | 2 per line-card | 2 per line-card |
| 9 | Fixed switching port (L2) | 0 | 0 | 0 | 0 |
| 10 | Other fixed port | 0 | 0 | 0 | 0 |
| 11 | Interface-card slot | 2 | 2 or 4 per line-card | 2 or 4 per line-card | 2 or 4 per line-card |

**Details of performance variations(SR6600 Series)**

| Sl. No. | Specification | SR6602 | SR6604 | SR6608 | SR6616 |
|---|---|---|---|---|---|
| 1 | Network Size | 500 -1000 | 1000 -2000 | 2000 -5000 | 5000 -10000 |
| 2 | Physical and Logical Interface | | | | |
| | Max. Number of L3 FE port | 16 | 32 | 64 | 128 |
| | Max. Number of L3 GE port | 20 | 36 | 72 | 144 |
| | Max. Number E1/CE1 port | 16 | 64 | 128 | 256 |
| | Max. Number of Synchronous serial ports | 16 | 64 | 128 | 256 |
| | Max. Number of CPOS port | 4 | 8 | 16 | 32 |
| | Max. Number of POS port | 8 | 16 | 32 | 64 |
| | Max. Number of 10G Ethernet port | 2 | 4 | 8 | 16 |
| 3 | LAN Protocol | | | | |
| 3.1 | Switch Ethernet | Not support | Not support | Not support | Not support |
| 3.2 | WAN Protocol | | | | |
| | Max. PPPoE Connection | 18000 | 16000 | 32000 | 32000 |
| 3.3 | Network Layer Protocol | | | | |
| 3.3.1 | ARP | | | | |
| | Static ARP | 2K | 4K | 4K | 4K |
| | Dynamic ARP | 16K | 16K | 16K | 16K |
| 3.3.2 | DHCP Server | | | | |
| | Address Pool Size | 254 | 254 | 254 | 254 |
| 3.3.3 | IPv4 | | | | |
| | Overall Throughput (pps) | 4.5Mpps | 9Mpps | 18Mpps | 36Mpps |
| 3.4 | Routing Protocol | | | | |
| 3.4.1 | Static Routing | | | | |
| | Routing table | 30,000 | 30,000 | 30,000 | 30,000 |
| | Max. ECMP (load-balance) | 8 | 8 | 8 | 8 |
| 3.4.2 | RIP | | | | |
| | Max. Number of Route Entrance | 10000 | 10000 | 10000 | 10000 |
| 3.4.3 | OSPF | | | | |
| | Max. Number of Route | 500,000 | 500,000 | 500,000 | 500,000 |

| Sl. No. | Specification | SR6602 | SR6604 | SR6608 | SR6616 |
|---|---|---|---|---|---|
| | Entrance | | | | |
| 3.4.4 | BGP | | | | |
| | Max. Number of Route Entrance | 500,000 | 500,000 | 500,000 | 500,000 |
| 3.4.5 | IS_IS | | | | |
| | Max. Number of Route Entrance | 500,000 | 500,000 | 500,000 | 500,000 |
| 3.5 | MPLS | | | | |
| 3.5.1 | LDP | | | | |
| | Max. Number of Dynamic LSP | 30,000 | 30,000 | 30,000 | 30,000 |
| | Max. Number of Static LSP | 1024 | 1024 | 1024 | 1024 |
| | Max. Number of MPLS supported interface | 2048 | 2048 | 2048 | 2048 |
| | Max. Number of Local Peer | 200 | 200 | 200 | 200 |
| | Max. Number of Remote Peer | 200 | 200 | 200 | 200 |
| 3.5.2 | L3VPN | | | | |
| | Max. Number of VRF | 1024 | 1024 | 1024 | 1024 |
| | Max. Number of interface bounded by a single VRF | 1024 | 1024 | 1024 | 1024 |
| | Max. Number of VRF bounded interface of the system | 2048 | 2048 | 2048 | 2048 |
| | Max. Number of route Entrance for a single VRF | 100,000 | 100,000 | 100,000 | 100,000 |
| 3.6 | Multicast | | | | |
| | Multicast Route | 4096 | 4096 | 4096 | 4096 |
| | IGMP Group | 16384 | 16384 | 16384 | 16384 |
| 3.7 | Security Function | | | | |
| 3.7.1 | NAT | | | | |
| | Number of Address Pool | 32 | 32 | 32 | 32 |
| | Size of a single address pool | 255 | 255 | 255 | 255 |
| | Concurrent connections | 1,000,000 | 1,000,000 per line-card | 1,000,000 per line-card | 1,000,000 per line-card |
| | Session established Rate (session/second) | >40,000 | >40,000 per line-card | >40,000 per line-card | >40,000 per line-card |

| Sl. No. | Specification | SR6602 | SR6604 | SR6608 | SR6616 |
|---|---|---|---|---|---|
| | Total number of Nat Servers in a system | 1024 | 1024 | 1024 | 1024 |
| 3.7.2 | ACL | | | | |
| | Number of Basic ACL | 32000 | 32000 | 32000 | 32000 |
| | Number of Advanced ACL | 32000 | 32000 | 32000 | 32000 |
| | Total Number of ACL | 32000 | 32000 | 32000 | 32000 |
| | ACL forwarding performance | Impaction on forwarding performance < 10% | Impaction on forwarding performance < 10% | Impaction on forwarding performance < 10% | Impaction on forwarding performance < 10% |
| 3.7.3 | IPSec | | | | |
| | encryption performance | 3Gbps<br>@1400bytes | 3Gbps<br>@1400bytes, per line-card | 3Gbps<br>@1400bytes, per line-card | 3Gbps<br>@1400bytes, per line-card |
| | Max Tunnel | 6000 | 6000 | 6000 | 6000 |
| 3.7.4 | SSL VPN | Not support | Not support | Not support | Not support |
| 3.7.5 | L2TP | | | | |
| | Max. Number of L2tp Tunnel | 18000 | 18000 | 18000 | 18000 |
| | Session established Rate (session/second) | 50 | 50 | 50 | 50 |
| 3.7.6 | GRE | | | | |
| | Max. Number of Tunnels | 4094 | 16384 | 16384 | 16384 |
| 3.7.7 | FW | | | | |
| | Throughput (Mbps) | 1Gbps | 1Gbps per line-card | 1Gbps per line-card | 1Gbps per line-card |
| | Max. Number of Concurrent Connections | 1 million | 1 million per line-card | 1 million per line-card | 1 million per line-card |
| 3.7.8 | Portal Authentication | | | | |
| | Number of concurrent connections | 100 | 100 | 100 | 100 |
| | Max. Number of Client | 10,000 | 10,000 | 10,000 | 10,000 |
| 3.8 | QoS | | | | |
| | Length of FIFO Queue | 1024 | 1024 | 1024 | 1024 |
| | Length of PQ Queue | 1024 | 1024 | 1024 | 1024 |
| | Length of CQ Queue | 1024 | 1024 | 1024 | 1024 |

| Sl. No. | Specification | SR6602 | SR6604 | SR6608 | SR6616 |
|---|---|---|---|---|---|
| | Length of WFQ Queue | 1024 | 1024 | 1024 | 1024 |
| | Length of CBQ Queue | 512 | 512 | 512 | 512 |
| | Max. Queue Number of PQ | 4 per interface | 4 per interface | 4 per interface | 4 per interface |
| | Max. Queue Number of CQ | 16 per interface | 16 per interface | 16 per interface | 16 per interface |
| | Max. Queue Number of WFQ | 4096 per interface | 4096 per interface | 4096 per interface | 4096 per interface |
| | Max. Queue Number of CBQ | 4096 per interface | 4096 per interface | 4096 per interface | 4096 per interface |

**Details of Hardware variations (SR8800 Series)**

| Sl. No | Specification | SR8802 | SR8805 | SR8808 | SR8812 |
|---|---|---|---|---|---|
| 1 | Processor | MPC7447A 1GHz | MPC7447A<br>1GHz | MPC7447A<br>1GHz | MPC7447A<br>1GHz |
| 2 | Memory (default/max.) | DDR2, 1GB/2GB | DDR2,<br>1GB/2GB | DDR2,<br>1GB/2GB | DDR2,<br>1GB/2GB |
| 3 | CF (default/max.) | 1+1; 256M/1G | 1+1;<br>256M/1G | 1+1;<br>256M/1G | 1+1;<br>256M/1G |
| 4 | FLASH (default/max.) | 128MB/128MB | 128MB/128MB | 128MB/128MB | 128MB/128MB |
| 5 | USB | 1 | 1 | 1 | 1 |
| 6 | AUX | 1 | 1 | 1 | 1 |
| 7 | Configuration port | 1 | 1 | 1 | 1 |
| 8 | Fixed Ethernet port (L3) | 0 | 0 | 0 | 0 |
| 9 | Fixed switching port (L2) | 0 | 0 | 0 | 0 |
| 10 | Other fixed port | 0 | 0 | 0 | 0 |
| 11 | Interface-card slot | 2 | 5 | 8 | 12 |

**Details of performance variations (SR8800 series)**

| Sl. No. | Specification | SR8802 | SR8805 | SR8808 | SR8812 |
|---|---|---|---|---|---|
| 1 | Network Size | 500 -1000 | 1000 -2000 | 2000 -5000 | 5000 -10000 |

| Sl. No. | Specification | SR8802 | SR8805 | SR8808 | SR8812 |
|---|---|---|---|---|---|
| 2 | Physical and Logical Interface | | | | |
| | Max. Number of L3 FE port | 20/slot | 20/slot | 20/slot | 20/slot |
| | Max. Number of L3 GE port | 20/slot | 20/slot | 20/slot | 20/slot |
| | Max. Number E1/CE1 port | 32/slot | 32/slot | 32/slot | 32/slot |
| | Max. Number of CPOS port | 4/slot | 4/slot | 4/slot | 4/slot |
| | Max. Number of POS port | 1/slot | 1/slot | 1/slot | 1/slot |
| | Max. Number of 10G Ethernet port | 2/slot | 2/slot | 2/slot | 2/slot |
| 3 | LAN Protocol | | | | |
| 3.1 | Switch Ethernet | support | support | support | support |
| 3.2 | WAN Protocol | | | | |
| | Max. PPPoE Connection | Not support | Not support | Not support | Not support |
| 3.3 | Network Layer Protocol | | | | |
| 3.3.1 | ARP | | | | |
| | Static ARP | 4K | 4K | 4K | 4K |
| | Dynamic ARP | 64K | 64K | 64K | 64K |
| 3.3.2 | DHCP Server | | | | |
| | Address Pool Size | 128 | 128 | 128 | 128 |
| 3.3.3 | IPv4 | | | | |
| | Overall Throughput (pps) | 146 Mpps | 244Mpps | 391Mpps | 586Mpps |
| 3.4 | Routing Protocol | | | | |
| 3.4.1 | Static Routing | | | | |
| | Routing table | 100,000 | 100,000 | 100,000 | 100,000 |
| | Max. ECMP (load-balance) | 8 | 8 | 8 | 8 |
| 3.4.2 | RIP | | | | |
| | Max. Number of Route Entrance | 10000 | 10000 | 10000 | 10000 |
| 3.4.3 | OSPF | | | | |
| | Max. Number of Route Entrance | 512K | 512K | 512K | 512K |
| 3.4.4 | BGP | | | | |
| | Max. Number of Route Entrance | 1G Engine Memory : 1 M, | 1G Engine Memory : 1M, 2G Engine | 1G Engine Memory : 1M , | 1G Engine Memory : 1M , |

| Sl. No. | Specification | SR8802 | SR8805 | SR8808 | SR8812 |
|---|---|---|---|---|---|
| | | 2G Engine Memory：3 M | Memory：3M | 2G Engine Memory：3M | 2G Engine Memory：3M |
| 3.4.5 | IS_IS | | | | |
| | Max. Number of Route Entrance | 1000,000 | 1000,000 | 1000,000 | 1000,000 |
| 3.5 | MPLS | | | | |
| 3.5.1 | LDP | | | | |
| | Max. Number of Dynamic LSP | 32K | 32K | 32K | 32K |
| | Max. Number of Static LSP | 1010 | 1010 | 1010 | 1010 |
| | Max. Number of MPLS supported interface | 16K | 16K | 16K | 16K |
| | Max. Number of Local Peer | 256 | 256 | 256 | 256 |
| | Max. Number of Remote Peer | 256 | 256 | 256 | 256 |
| 3.5.2 | L3VPN | | | | |
| | Max. Number of VRF | 1024 | 1024 | 1024 | 1024 |
| | Max. Number of interface bounded by a single VRF | SPE-1010-E/SPE-1020-E<512K， SPE-1010/SPE-1020<128K | SPE-1010-E/SPE-1020-E<512K，SPE-1010/SPE-1020<128K | SPE-1010-E/SPE-1020-E<512K，<br>SPE-1010/SPE-1020<128K | SPE-1010-E/SPE-1020-E<512K，<br>SPE-1010/SPE-1020<128K |
| 3.6 | Multicast | | | | |
| | Multicast Route | 32 K | 32 K | 32 K | 32 K |
| | IGMP Group | 1024 | 1024 | 1024 | 1024 |
| 3.7 | Security Function | | | | |
| 3.7.1 | NAT | | | | |
| | Number of Address Pool | 255 | 255 | 255 | 255 |
| | Size of a single address pool | 1. 64 IP addresses per PAT address pool<br>2. 255 IP addresses per NAT address pool<br>3. 255 NAT | 1. 64 IP addresses per PAT address pool<br>2. 255 IP addresses per NAT address pool<br>3. 255 NAT address pools | 1. 64 IP addresses per PAT address pool<br>2. 255 IP addresses per NAT address pool<br>3. 255 NAT | 1. 64 IP addresses per PAT address pool<br>2. 255 IP addresses per NAT address pool<br>3. 255 NAT |

| Sl. No. | Specification | SR8802 | SR8805 | SR8808 | SR8812 |
|---|---|---|---|---|---|
| | | address pools | | address pools | address pools |
| | Concurrent connections | 1,000,000 | 1,000,000 per line-card | 1,000,000 per line-card | 1,000,000 per line-card |
| | Session established Rate (session/second) | > 200,000/s per line-card | > 200,000/s<br>per line-card | > 200,000/s per line-card | > 200,000/s per line-card |
| | Total number of Nat Servers in a system | 1024 | 1024 | 1024 | 1024 |
| 3.7.2 | ACL | | | | |
| | Number of Basic ACL | SPE-1010:16K, SPE-1020:2*16K ,<br>SPE-1010-E:64K,<br>SPE-1020-E:64K, 64K/System | SPE-1010:16K, SPE-1020:2*16K， SPE -1010-E:64K, SPE-1020-E:64K, 64K/System | SPE-1010:16K, SPE-1020:2*16K, SPE-1010-E:64K,<br>SPE-1020-E:64K, 64K/System | SPE-1010:16K, SPE-1020:2*16K, SPE-1010-E:64K,<br>SPE-1020-E:64K, 64K/System |
| | Number of Advanced ACL | SPE-1010:16K, SPE-1020:2*16K ,<br>SPE-1010-E:64K,<br>SPE-1020-E:64K, 64K/System | SPE-1010:16K, SPE-1020:2*16K,<br>SPE-1010-E:64K,<br>SPE-1020-E:64K, 64K/System | SPE-1010:16K, SPE-1020:2*16K,<br>SPE-1010-E:64K,<br>SPE-1020-E:64K, 64K/System | SPE-1010:16K, SPE-1020:2*16K,<br>SPE-1010-E:64K,<br>SPE-1020-E:64K, 64K/System |
| | Total Number of ACL | SPE-1010:16K, SPE-1020:2*16K ,<br>SPE-1010-E:64K,<br>SPE-1020-E:64K, 64K/System | SPE-1010:16K, SPE-1020:2*16K,<br>SPE-1010-E:64K,<br>SPE-1020-E:64K, 64K/System | SPE-1010:16K, SPE-1020:2*16K,<br>SPE-1010-E:64K,<br>SPE-1020-E:64K, 64K/System | SPE-1010:16K, SPE-1020:2*16K,<br>SPE-1010-E:64K,<br>SPE-1020-E:64K, 64K/System |
| 3.7.3 | IPSec | | | | |
| | encryption performance | 64Bytes：300Mbps, | 64Bytes：300Mbps, | 64Bytes：300 Mbps, | 64Bytes：300 Mbps, |

| Sl. No. | Specification | SR8802 | SR8805 | SR8808 | SR8812 |
|---|---|---|---|---|---|
| | | 1500Bytes：1Gbps | 1500Bytes：1Gbps | 1500Bytes：1 Gbps | 1500Bytes：1 Gbps |
| | Max Tunnel | 6000 | 6000 | 6000 | 6000 |
| 3.7.4 | SSL VPN | Not support | Not support | Not support | Not support |
| 3.7.5 | L2TP | | | | |
| | Max. Number of L2tp Tunnel | 8192 | 8192 | 8192 | 8192 |
| 3.7.6 | GRE | | | | |
| | Max. Number of Tunnels | 4096 | 4096 | 4096 | 4096 |
| 3.7.7 | FW | | | | |
| | Throughput (Mbps) | 64Bytes：1 Gbps, 1500Bytes：6Gbps<br>64-byte frames: 1 Gbps; 1500-byte frames: 6 Gbps | 64Bytes：1Gbps , 1500Bytes：6Gbps<br>64-byte frames: 1 Gbps; 1500-byte frames: 6 Gbps | 64Bytes：1Gbps, 1500Bytes：6 Gbps<br>64-byte frames: 1 Gbps; 1500-byte frames: 6 Gbps | 64Bytes：1Gbps, 1500Bytes：6 Gbps<br>64-byte frames: 1 Gbps; 1500-byte frames: 6 Gbps |
| | Max. Number of Concurrent Connections | 1 M | 1 M | 1 M | 1 M |
| 3.7.8 | Portal Authentication | | | | |
| | Number of concurrent connections | 100 | 100 | 100 | 100 |
| | Max. Number of Client | 2000 | 2000 | 2000 | 2000 |
| 3.8 | QoS | | | | |
| | Max. Queue Number of PQ | 16K | 16K | 16K | 16K |
| | Max. Queue Number of CQ | 16K | 16K | 16K | 16K |
| | Max. Queue Number of WFQ | 16K | 16K | 16K | 16K |
| | Max. Queue Number of CBQ | 16K | 16K | 16K | 16K |