

# National Information Assurance Partnership



## Common Criteria Evaluation and Validation Scheme Validation Report

### **Marconi Corporation plc**

Marconi Multiservice Switches and Switch Router  
(ASX-200BX, ASX-1000, ASX-1200, TNX-210, TNX-  
1100, ASX-4000, ASX-4000M, and BXR-48000) with  
ForeThought 8.3.1 and BXR ForeThought 2.0.1

**Report Number:** CCEVS-VR-05-0101  
**Dated:** 03 June 2005  
**Version:** 0.3

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

National Security Agency  
Information Assurance Directorate  
9800 Savage Road STE 6740  
Fort George G. Meade, MD 20755-6740

VALIDATION REPORT  
Marconi Multiservice Switches and Switch Router

**ACKNOWLEDGEMENTS**

**Validation Team**

**Victoria A. Ashby  
The MITRE Corporation  
McLean, VA**

**Alton (Spike) Lewis  
NSA  
Columbia, MD**

**Common Criteria Testing Laboratory**

**Science Applications International Corporation  
Columbia, Maryland**

VALIDATION REPORT  
Marconi Multiservice Switches and Switch Router

## Table of Contents

1	Executive Summary .....	1
1.1	Interpretations .....	2
1.2	Threats to Security .....	2
2	Identification .....	3
3	Security Policy .....	4
4	Assumptions.....	5
5	Architectural Information .....	5
6	Documentation .....	6
	Design documentation .....	6
	Guidance documentation .....	7
	Configuration Management documentation .....	8
	Delivery and Operation documentation .....	9
	Life Cycle Support documentation .....	11
	Test documentation.....	11
	Vulnerability Assessment documentation.....	11
	Security Target.....	12
7	IT Product Testing .....	12
7.1	Developer Testing.....	12
7.2	Evaluation Team Independent Testing .....	12
7.3	Evaluation Team Penetration Testing.....	13
8	Evaluated Configuration .....	13
9	Results of the Evaluation .....	13
10	Validator Comments/Recommendations .....	14
11	Annexes.....	15
12	Security Target.....	15
13	Glossary .....	15
14	Bibliography .....	15

VALIDATION REPORT  
Marconi Multiservice Switches and Switch Router

## **1 Executive Summary**

The evaluation of the Marconi Multiservice Switches and Switch Router (ASX-200BX, ASX-1000, ASX-1200, TNX-210, TNX-1100, ASX-4000, ASX-400M, and BXR-48000) with ForeThought 8.3.1 and BXR ForeThought 2.0.1 was performed by Science Applications International Corporation (SAIC) in the United States and was completed on 13 April 2005. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.2 and the Common Methodology for IT Security Evaluation (CEM), Version 1.0.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.2). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the Marconi Multiservice Switches and Switch Router (ASX-200BX, ASX-1000, ASX-1200, TNX-210, TNX-1100, ASX-4000, ASX-400M, and BXR-48000) with ForeThought 8.3.1 and BXR ForeThought 2.0.1 product by any agency of the US Government and no warranty of the product is either expressed or implied.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 3) have been met.

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) Part 1 (non-proprietary) produced by SAIC.

## 1.1 Interpretations

This evaluation used the Common Criteria for Information Technology Security Evaluation Parts 2 and 3, Version 2.2, Revision 256, January 2004, which incorporated all applicable interpretations at the time the evaluation started.

## 1.2 Threats to Security

The Security Target identified the following threats that the evaluated product addresses:

T.ACCOUNT	An administrator might perform actions for which they are not accountable.
T.AUTH	A user might be able to gain unauthorized access to TOE functions.
T.CONFIG	An administrator might not be able to configure the TOE security policy mechanisms.
T.DETECT	A user's attempts to violate TOE authentication and security management security mechanisms may go undetected.
T.MISCONFIG	A user might intentionally mis-configure TOE security policy mechanisms.
T.NETFLOW	A user might be able to access information or network resources that should be restricted.
T.PROTECT	The TOE might be subject to malicious tampering or bypass of its security mechanisms.

## 2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant;
- The organizations and individuals participating in the evaluation.

**Table 1: Evaluation Identifiers**

Item	Identifier
<b>Evaluation Scheme</b>	United States NIAP Common Criteria Evaluation and Validation Scheme
<b>TOE:</b>	Marconi Multiservice Switches (ASX-200BX, ASX-1000, ASX-1200, TNX-210, TNX-1100, ASX-4000, and ASX-4000M) with ForeThought 8.3.1, and  Marconi Switch Router BXR-48000 with BXR ForeThought 2.0.1
<b>Protection Profile</b>	Not applicable.
<b>ST:</b>	<i>Marconi Multiservice Switches and Switch Routers (ASX-200BX, ASX-1000, ASX-1200, TNX-210, TNX-1100, ASX-4000, ASX-4000M, and BXR-48000) Security</i>

VALIDATION REPORT  
Marconi Multiservice Switches and Switch Router

<b>Item</b>	<b>Identifier</b>
	<i>Target</i> , Version 1.0, April 10, 2005.
<b>Evaluation Technical Report</b>	<i>Evaluation Technical Report for Marconi Router/Switches</i> , Version 1.0, April 1, 2005
<b>CC Version</b>	Common Criteria for Information Technology Security Evaluation, Version 2.2, Revision 256, January 2004
<b>Conformance Result</b>	CC Part 2 conformant, CC Part 3 conformant
<b>Sponsor</b>	Marconi Corporation plc
<b>Developer</b>	Marconi Corporation plc
<b>Common Criteria Testing Lab (CCTL)</b>	SAIC, Columbia, MD
<b>CCEVS Validator</b>	Vicky Ashby, The MITRE Corporation  Alton (Spike) Lewis, National Security Agency

### 3 Security Policy

The TOE provides the following security functions: Security Audit, Information Flow Control, Identification and Authentication, Security Management and TSF Protection. Each is discussed in more detail as follows:

- **Security Audit** - The TOE provides an audit feature that provides the ability to audit user actions related to authentication attempts and administrator actions.
- **Information Flow Control** - In general, network devices exchange valuable information among themselves. To mitigate threats of spoofing, replay attacks, unauthorized access and DoS attacks among others, the TOE provides an Information Flow Control mechanism that supports control of the flow of traffic generated by the network devices. The Information Flow Control Policies are configured on each network devices to allow traffic to only flow between the authorized sources and authorized destinations.
- **Identification and Authentication** - The TOE requires users to provide unique identification and authentication data before any administrative access to the system is granted. The TOE provides the ability to define levels of authority for users via “profiles”, providing administrative flexibility by allowing granular assignment of management rights down to the level of individual commands or entire “directories”

VALIDATION REPORT  
Marconi Multiservice Switches and Switch Router

of commands. Authorized users may also be assigned to different profiles depending on how they access the TOE (via local terminal console, telnet, HTTP, or SNMP).

- **Security Management** - The TOE is managed through a Command Line Interface (CLI) that can be accessed locally using the terminal console, or remotely using telnet or a web browser. The web browser interface is basically an HTML rendering of the CLI command set, so it has identical functionality to the telnet or terminal console CLI. Additionally, many of the TOE's functions can be managed remotely via SNMP GET and SET commands. Through the CLI, authorized administrators can configure and manage all TOE functions, including configuring the switch router devices and manage user accounts.
- **Protection of Security Functions** - The TOE provides protection mechanisms for its security functions. One of the protection mechanisms is that users must authenticate before any administrative operations can be performed on the system, whether those functions are related to the management of user accounts or the configuration of routers. Another protection mechanism is that the TOE is self-contained and therefore maintains its own execution domain. All TOE security functions are confined to the device.

## 4 Assumptions

The following secure usage assumptions about the intended environment of the TOE are identified in the Security Target:

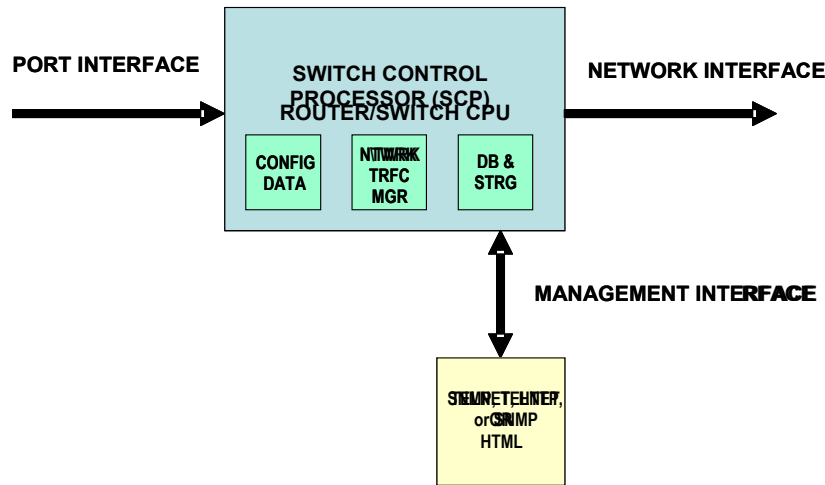
- |            |  |
|------------|--|
| A.ADMIN    | The administrators will be competent and will adhere to the applicable TOE guidance.   |
| A.CONNECT  | The TOE will be installed in a network infrastructure such that it can effectively control the flow of the applicable information. |
| A.NOEVIL   | The administrators of the TOE will not be willfully negligent or otherwise hostile.  |
| A.PHYSICAL | The TOE will be protected from unauthorized physical access.   |

## 5 Architectural Information



VALIDATION REPORT  
Marconi Multiservice Switches and Switch Router

The Marconi multiservice switch and switch router appliances are designed to provide transport devices for ATM and other types of Layer 2 networks to LAN and WAN environments. The TOE consists of the hardware appliance that contains the device specific port interfaces, Switch Control Processor (SCP), and the device management interface. Port cards are the physical network interfaces that allow the TOE to be customized to the intended environment.



**Figure 1 – Marconi Router/Switches**

The multiservice switches and switch routers are powered by the ForeThought 8.3.1 or BXR ForeThought 2.0.1 switch control software, which is included in the TOE and which manages all switch/router management functions including cell, packet, and IP routing/switching functions. The appliances support numerous routing/switching standards, allowing them to be flexible as well as scalable. The appliances are managed either through a locally connected terminal console or remotely via a web-based interface (HTTP) or via Telnet/SSH, or via SNMP using the SET/GET commands to access MIBs (Management Information Bases).

## 6 Documentation

### Design documentation

Document	Version	Date
ForeThought 8.3.1 and BXR FT 2.0.1 For ASX/TNX, ASX-4000, & BXR-48000 Multiservice Switches - Functional Specification Document (FT&BXR_FS_1.8.doc)	1.8	09 March 2005

VALIDATION REPORT  
Marconi Multiservice Switches and Switch Router

ForeThought 8.3.1 and BXR 2.0.1 For ASX/TNX, ASX-4000, & BXR-48000 Multiservice Switches - High Level Design Document (FT&BXR_HLD_1.4.doc)	1.4	07 January 2005
ForeThought 8.3.1 and BXR ForeThought 2.0.1 Common Criteria Certification TSF Representation Correspondence (BBRS-CK-002_FT&BXR_RepCorrespondence_1.1.doc)	1.1	08 February 2005

### Guidance documentation

User Documents for ASX™, TNX™, ASX™-4000 Multiservice Switches and ForeThought® 8.3.1

Document	Version	Date
ASX™ -4000 Series Switch Installation and Maintenance Manual - ForeThought 8.3.1, 081-0014-05 (8101405a.pdf)	Issue A	05-14-2004
ASX™ Multiservice Broadband Switch Installation and Maintenance Manual - ForeThought 8.3.1, 081-0015-05, (8101505a.pdf)	Issue A	05-14-2004
TNX™ Multiservice Broadband Switch Installation and Maintenance Manual - ForeThought 8.3.1, 081-0016-05, (8101605a.pdf)	Issue A	05-14-2004
Multiservice Broadband Switch Diagnostics and Troubleshooting Manual - ForeThought 8.3.1, 083-0001-05 (8300105a.pdf)	Issue A	05-14-2004
AMI Configuration Commands Reference Manual, Part 1 - ForeThought 8.3.1, 084-0017-05 (8401705a.pdf)	Issue A	May 2004
AMI Configuration Commands Reference Manual, Part 2 - ForeThought 8.3.1, 084-0018-05, (8401805a.pdf)	Issue A	May 2004
AMI Configuration Commands Reference Manual, Part 3 - ForeThought 8.3.1, 084-0019-05, (8401905a.pdf)	Issue A	May 2004
ForeThought® Software for ASX™ and TNX™ Switches Release Notes - Version 8.3.1, 085-0035-06, (8503506a.pdf)	Issue A	06-23-2003

VALIDATION REPORT  
Marconi Multiservice Switches and Switch Router

Document	Version	Date
ASX™-4000 Series Switch Network Module Carrier Quickstart Guide, 086-0013-04, (8601304a.pdf)	Issue A	06-23-2003
SCP-P5 Series Quickstart Guide, 086-0021-01 – (8602101a_P5-SCP_Quickstart_Guide.pdf)	Issue A	06-23-2003

User Documents for BXR™ -48000 Multiservice Switch Router and BXR™ ForeThought® 2.0.1

Document	Version	Date
BXR™-48000 Multiservice Switch Router Installation and Maintenance Manual, Release 2.0.1, 081-0007-05, (8601905b.pdf)	Issue B	5-14-2004
BXR™-48000 Multiservice Switch Router AMI Configuration Commands Reference Manual: Part 1, 084-0007-04, (8400704b.pdf)	Issue B	5-14-2004
BXR™-48000 Multiservice Switch Router AMI Configuration Commands Reference Manual: Part 2, 084-0008-04, (8400804b.pdf)	Issue B	5-14-2004
BXR™-48000 Multiservice Switch Router AMI Configuration Commands Reference Manual: Part 3, 084-0009-04, (8400904b.pdf)	Issue B	5-14-2004
BXR™-48000 Multiservice Switch Router Release Notes, ForeThought BXR 2.0.1, 085-0028-03, (8502803b.pdf)	Issue B	5-14-2004
BXR™-48000 Multiservice Switch Router Commissioning and Turn Up Guide, Release 2.0.1, 086-0019-05, (8601905b.pdf)	Issue B	5-14-2004
BXR™-48000 Multiservice Switch Router Site and Equipment Preparation Guide, 086-0020-05 - Release 2.0.1 (8602005b.pdf)	Issue B	5-14-2004

**Configuration Management documentation**

Document	Version	Date
Configuration Management Plan (003-0001-01.doc)	Revision A	05/30/2001

VALIDATION REPORT  
Marconi Multiservice Switches and Switch Router

Document	Version	Date
Control of Unreleased Product (CUP) Procedure (005-0185-01.pdf)	Revision C	August 2000
Interchangeability Guideline (060-0001-01.pdf)	Revision C	5/8/00
Initial Configuration / New Product Release ECN Requirements Checklist (064-0001-01.htm)	Revision B	
Released Product Change ECN Requirements Checklist (064-0002-01.htm)	Revision A	
Part Number and Manufacturer Release and Change Procedure (CMOP-4430-001.pdf)	Revision D	11/21/97
Engineering Change Notice Procedure (CMOP-4490-002.pdf)	Revision H	6/21/00
Lifecycle Document Change, Approval and New Release Procedure (LCPD-0011 ApprovalProcessDoc.doc)	Revision 2	August 2002
BBRS Process Documentation Procedure (LCPD-0012 BBRSProcessDocControl.doc)	Revision 2	August 2002
Product Identification Specification (MEOP-4800_001.doc)	Revision G	11 February 2005
PAW 4.2.3 BBRS Document Control Process v3.1 (PAW_4.2.3-Documents_Control_Process_v3.1.doc)	Revision 3.1	
PAW 4.2.3.1 BBRS E*Tools Document Management Tool v1.1 (PAW_4.2.3.1-ETools_Document_Mgmt_v1.1.doc)	Revision 1.1	
PAW 4.2.3.2 BBRS Software Configuration Management v1.1 (PAW_4.2.3.2-Software Configuration Management_v1.1.doc)	Revision 1.1	
Procedure for Initiating, Controlling, and Revising Controlled Documents (QAOP-1017.doc)	Revision D	November 15, 2002

**Delivery and Operation documentation**

Document	Version	Date
Product Outer Packaging Labeling Guidelines (MEGL-4154_001)	Revision E	3/1/02
Packaging Specification for Incoming and Outgoing Shipments (MEOP-4154_001)	Revision B	23 August 2002

VALIDATION REPORT  
Marconi Multiservice Switches and Switch Router

<b>Document</b>	<b>Version</b>	<b>Date</b>
Marconi Part Conversion Procedure (MEWI-4103-191)	Revision D	04-June-02
Volume Operations Flow Chart (PRFC-1030)	Revision C	20-MAR-03
Distribution Material Flow (PRFC-1062)	Revision B	January 31, 2003
ASX-1000, ASX-1200, & TNX-1100 Configuration Checklist (PRFM-1160)	Revision B	4/5/2005
ASX-200BX & TNX-210 Configuration Checklist (PRFM-1162)	Revision B	4/5/2005
ASX-4000 Blanks Visual Checklist (PRFM-1165)		4/5/2005
ASX-4000 Chassis Visual & Functional Checklist (PRFM-1166)	Revision B	4/5/2005
ASX-4000 Fabric Visual & Functional Checklist (PRFM-1167)	Revision B	4/5/2005
ASX-4000 Port Card Visual & Functional Checklist (PRFM-1168)	Revision B	4/5/2005
ASX-4000 SCP Visual & Functional Checklist (PRFM-1170)	Revision B	4/5/2005
Netmod Visual & Functional Checklist (PRFM-1172)	Revision B	4/5/2005
SCP Visual & Functional Checklist (PRFM-1175)	Revision B	4/5/2005
Power Supply Visual & Functional Checklist (PRFM-1204)	Revision A	4/5/2005
BXR-48000 Chassis Visual & Functional Checklist (PRFM-1213)	Revision A	4/5/2005
BXR-48000 Card Visual & Functional Checklist (PRFM-1214)	Revision A	4/5/2005
Pre-Pack Boxing and Labeling Procedure (PROP-4155_001)	Revision D	12-February-2003
Handling, Storage, Preservation, and Delivery of Products (PRST-4150-001)	Revision C	September 5, 2002
Packing and Shipping Training Guide and Work Instructions (PRWI-1022_RevA)	Revision A	17 MAR 05
Final Inspection Procedure (QAOP-1104)	Revision C	3/24/03

VALIDATION REPORT  
Marconi Multiservice Switches and Switch Router

Document	Version	Date
Common Criteria Certification (CCC) Evaluated Configuration Guide, ForeThought 8.3.1 and BXR FT 2.0.1, (082-0015-01)	Revision 1.5	31 March 2005

### Life Cycle Support documentation

Document	Version	Date
Marconi Information Security Program (MISPV2.1.doc)	Version 2.1	7/11/2001

### Test documentation

Document	Version	Date
SWTP-0001 - FT 8.3.1 AND BXR FT 2.0.1 Common Criteria Evaluation Test Plan, Procedures, & Results (SWTP-0001-FT&BXR_CC_Evaluation_Test_Plan_1.6.doc)	Version 1.6	28 March 2005
Syslog_ASX-200BX.txt - FT 8.3.1 Auditing Test Results on ASX-200BX (Syslog_ASX-200BX.txt)		21 March 2005
Syslog_ASX-1200.txt - FT 8.3.1 Auditing Test Results on ASX-1200 (Syslog_ASX-1200.txt)		21 March 2005
Syslog_ASX-4000.txt - FT 8.3.1 Auditing Test Results on ASX-4000 (Syslog_ASX-4000.txt)		21 March 2005
Syslog_BXR-4800.txt - FT 8.3.1 Auditing Test Results on BXR-48000(Syslog_BXR-48000.txt)		21 March 2005
Syslog_TNX-1100.txt - FT 8.3.1 Auditing Test Results on TNX-1100 (Syslog_TNX-1100.txt)		21 March 2005

Syslogs contain the actual results

### Vulnerability Assessment documentation

Document	Version	Date
CS-PAW-002 - CERT® Security Alert Management (CS-PAW-002 CERT Security Alerts.doc)		
ENDS-0001 ForeThought 8.3.1 and BXR FT 2.0.1 Strength of Function Analysis (ENDS-0001_FT-BXR_SOF_v1.1.doc)	Revision 1.1	March 15, 2005
ForeThought 8.3.1 and BXR FT 2.0.1 Vulnerability	Revision	March

VALIDATION REPORT  
Marconi Multiservice Switches and Switch Router

Analysis 1.1 (ENDS-0002_FT&BXRFT_Vulnerability_Analysis_v1.1.doc)	1.2	14, 2005
Marconi TACTics Online Alerts Web Page (TACTics_Alerts_Page.bmp)		

### Security Target

Document	Version	Date
Marconi Multiservice Switches and Switch Routers (ASX-200BX, ASX-1000, ASX-1200, TNX-210, TNX-1100, ASX-4000, ASX-4000M, and BXR-48000) Security Target	1.0	10 April 2005

## 7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

### 7.1 Developer Testing

The vendor ran the documented test procedures before the evaluation team's Independent Testing Activity began. The vendor provided a complete set of test results for analysis.

The evaluation team analyzed the vendor test procedures to ensure adequate coverage and to determine if the interfaces between subsystems were behaving as expected.

The Evaluation Team determined that the developer's actual test results matched the vendor's expected results.

The evaluation test team installed the TOE in the vendor's test lab. Some issues were noted during the set up and testing. Updates to the vendor documentation have corrected the cause of these issues.

SAIC and the developer consider the detailed test configuration to be proprietary information. However, the Evaluation Team has included a description of the vendor's test configurations in the ETR, Part 2.

### 7.2 Evaluation Team Independent Testing

The Evaluation Team chose to run a subset of the tests that the developer performed. The subset was chosen to ensure adequate coverage for all security functional requirements. This ensured that the Evaluation Team adequately addressed both security functions. The Evaluation Team used the developer's test configurations to perform the tests.

VALIDATION REPORT  
Marconi Multiservice Switches and Switch Router

In addition, the Evaluation Team also tested the installation, generation, and start-up procedures to determine, in accordance with ADO\_IGS.1.2E, that those procedures result in a secure configuration.

### **7.3 Evaluation Team Penetration Testing**

For its penetration tests, the Evaluation Team used a combination of open-source vulnerability documentation and a set of test procedures to identify penetration test cases based on the developer's vulnerability assessment documentation. The Evaluation Team used the developer's test configuration to successfully perform its penetration tests.

The Evaluation Team's ETR, Part 2, provides a detailed description of the tests, the results, and the effects, if any, on the information presented in the ST or other evaluation evidence.

## **8 Evaluated Configuration**

The evaluated configuration consists of a Marconi switch or switch router containing Marconi software, with the following designations:

- Marconi Multiservice Switches (ASX-200BX, ASX-1000, ASX-1200, TNX-210, TNX-1100, ASX-4000, and ASX-4000M) with ForeThought 8.3.1, and
- Marconi Switch Router BXR-48000 with BXR ForeThought 2.0.1

## **9 Results of the Evaluation**

The Evaluation Team conducted the evaluation based on the Common Criteria (CC) Version 2.2 and the Common Evaluation Methodology (CEM) Version 1.0 and all applicable National and International Interpretations in effect.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Verdicts were not assigned to assurance classes.

Section 5, Results of Evaluation, in the Evaluation Team's ETR, Part 1, states:



VALIDATION REPORT  
Marconi Multiservice Switches and Switch Router

“The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s performance of a subset of the vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.”

For further details, the reader is encouraged to consult the non-proprietary ETR, Part 1, for this product.

The validation team followed the procedures outlined in the Common Criteria Evaluation and Validation Scheme (CCEVS) publication number 3 for Technical Oversight and Validation Procedures. The validation team has observed the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validation team therefore concludes that the evaluation and its results of pass are complete.

## 10 Validator Comments/Recommendations

In addition to the information presented in other sections of this document, the validator has the following comments:

**Evaluated Configuration:** Marconi provides three different configurations for management of the switch with differing security implications. These three configurations include:

- High security – The console must be directly attached to the switch; remote administration is not allowed.
- Medium security – The console can be connected to a LAN that includes the switch, and the administrator can use telnet, HTTP, or SNMP to access the switch.
- Low security – The console can be connected to the switch using a network connection.

Only the first two are included in the evaluated configuration. That is, the console must be directly connected or connected through a local LAN to the switch to be in the evaluated configuration.

**Cryptography:** The security functional requirements claimed in the ST are not met by any cryptography. The Marconi products do include cryptography, but it is not used to meet any security functional requirement met by the TOE. The evaluation did not look at the cryptography included in the Marconi switches.

**Audit:** The TOE produces audit records, but they cannot be stored on the switch. The audit records must be moved to an audit collector outside of the TOE. Therefore, only audit data generation (FAU\_GEN.1) is claimed for the TOE.

**Documentation:** Marconi has provided documentation that clearly states what interfaces are security relevant, and therefore part of the TOE, and which are not.

## 11 Annexes

Not applicable.

## 12 Security Target

The Security Target is identified as *Marconi Multiservice Switches and Switch Routers (ASX-200BX, ASX-1000, ASX-1200, TNX-210, TNX-1100, ASX-4000, ASX-4000M, and BXR-48000) Security Target*, Version 1.0, April 10, 2005..

The document identifies the security functional requirements (SFRs) necessary to implement Information Flow Protection and TOE Self Protection security policies. These include TOE SFRs and IT Environment SFRs. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 3.

## 13 Glossary

The following definitions are used throughout this document:

*Hardware*: the physical equipment used to process programs.

*Software*: the programs and associated data that can be dynamically written and modified.

*Target of Evaluation (TOE)* - An information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

## 14 Bibliography

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

- *Common Criteria for Information Technology Security Evaluation*, Version 2.2, Revision 256, January 2004, Parts 1, 2, and 3.
- *Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.
- *Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model*, Version 0.6, 11 January 1997.
- *Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology*, Version 1.0, August 1999.

VALIDATION REPORT  
Marconi Multiservice Switches and Switch Router

- *Marconi Multiservice Switches and Switch Routers (ASX-200BX, ASX-1000, ASX-1200, TNX-210, TNX-1100, ASX-4000, ASX-4000M, and BXR-48000) Security Target*, Version 1.0, April 10, 2005.
- ETR Part 1 (Non-Proprietary), Version 1.1, 11 April 2005.