Marconi Service Edge Routers
(BXR-1000 and BXR-5000)
Security Target

Version 1.0
February 8, 2006

Prepared for:
Marconi Corporation plc.
2000 Marconi Drive
Warrendale, PA USA

Prepared By:
Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The Marconi service edge routers primarily provide network traffic management and control. The products enforce information flow control policies to provide its services. In support of network traffic management, the products ensure that security-relevant events are audited, ensure that their own functions are protected from potential attacks, and provide security tools to manage all of the security functions.

The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security Environment (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8)

1.1 Security Target, TOE and CC Identification

ST Title – Marconi Service Edge Routers (BXR-1000 and BXR-5000) Security Target

ST Version – Version 0.7

ST Date – February 8, 2006

TOE Identification – The TOE consists of the following Marconi service edge router models (BXR-1000 and BXR-5000, running ShadeTree Routing Control Software ver 3.1.1).

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.2, Revision 256, January 2004.

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.2, Revision 256, January 2004.
    - CC Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.2, Revision 256, January 2004.
    - CC Part 3 Conformant
    - Evaluation Assurance Level 3 (EAL3)

1.3 Strength of Environment

The Marconi service edge routers provide combined switching and routing solutions for connected networks. They are called “Service Edge Routers” in that they are normally used to provide services such as B-RAS (Broadband Remote Access Server) and DSLAM (Digital Subscriber Line Access Management) on WAN connections for

customer networks at the edge of a service provider network, or to connect small departmental networks to an enterprise backbone network. Thus the Marconi service edge routers provide features such as traffic prioritization, filtering, route summarization, VPNs (Virtual Private Networks), and MPLS (MultiProtocol Label Switching) LER (Label Edge Router) services for the service provider's customers, or for the internal networks of an enterprise or government agency. In order to successfully maintain control over the routing and switch configuration in a volatile network environment, these appliances must remain physically connected to the networks that they route or switch. The appliances must be appropriately placed in a network infrastructure, protected from physical attacks, and direct logical access must be restricted to authorized users. To ensure that the design of the IT networks is acknowledged and that the risks to the target environment are adequately addressed, the assurance requirements for EAL3, and the minimum strength of function, SOF-Basic, were chosen.

1.4 Conventions, Terminology and Acronyms

This section specifies the formatting information used in the Security Target.

1.4.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.4.2 Terminology

Core routers	software-based core routers are often connected to hardware-accelerated layer 2 switches (historical). These layer 2 switches typically use/used ASICs to provide the needed throughput, but lacked the intelligence required for layer 3 routing, which the core routers provide.
Service Edge Routers	a new and evolving class of routers aimed at transitioning carriers to a single, multi-service network. Based on design requirements similar to those of core routers, this type of router must support continually evolving requirements and aggregate a range of network and traffic types. Service edge routers must support layer 2 traffic (which requires interoperability with frame relay and ATM devices) with the same level of guarantees as layer 2 devices (switches), as well as new, IP-based services. A carrier-class service-edge router must include routing as robust as that found in Internet core routers.
Switch router	an appliance that combines both switching and routing capability; the TOE appliances. Also referred to as a "switch/router".

1.4.3 Acronyms

The acronyms used within this Security Target:

ACL	Access Control Lists
ATM	Asynchronous Transfer Mode
ASIC	Application Specific Integrated Circuits
CC	Common Criteria
CD-ROM	Compact Disk Read Only Memory
CLI	Command Line Interface
CM	Control Management
CPU	Central Processing Unit
DO	Delivery Operation
EAL	Evaluation Assurance Level
HTTP	HyperText Transfer Protocol
I/O	Input/Output
MIB	Management Information Bases
MPLS	MultiProtocol Label Switching
NPB	Network Processor Board
PDF	Portable Document Format
PP	Protection Profile
PXF	Packet Switching Fabric
RCP	Route Control Processor
RCS	Routing Control Software
SF	Security Functions
SFR	Security Functional Requirements
SIO	System Input/Output
SSH	Secure Shell (protocol)
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
TSC	TSF Scope of Control
VPN	Virtual Private Network

2. TOE Description

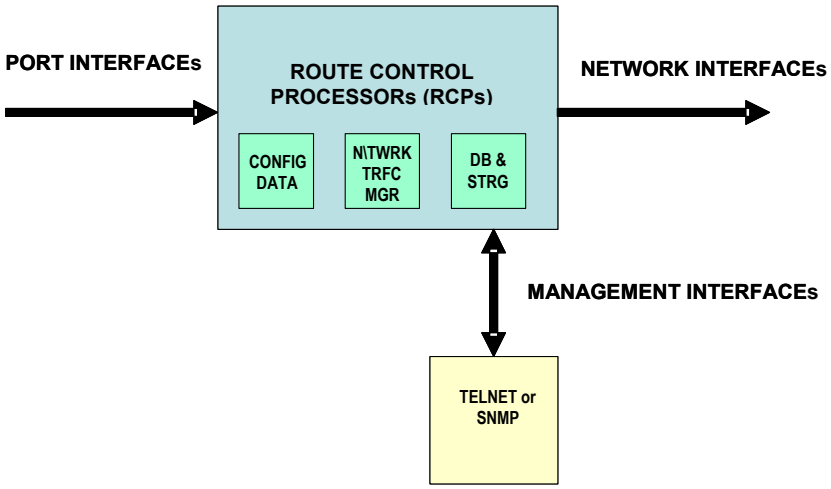
The TOE consists of a Marconi service edge router appliance from model numbers: BXR-1000 and BXR-5000. Each of these models has essentially the same security features. The primary differences between the models are performance and form factor. The products are designed by Marconi Corporation PLC, located at 2000 Marconi Drive, Warrendale, PA 15086.

2.1 Product Type

The Marconi service edge routers are network appliances that provide network traffic management and control. The Marconi service edge routers are highly scalable and flexible. They support any type of switched or routed data service for virtually any interface; they can manage traffic over essentially any type of network, with the different models providing varying level of performance speed and scalability of the traffic volume. All packets and traffic flows on the monitored network are scanned and then compared against a set of rules to determine whether the traffic should be switched or routed, and then it is passed to the appropriate destination. While the appliances function primarily as routers, they can also switch cells over ATM virtual circuits or Ethernet packets within VLANs (Virtual LANs) as needed. Since routing is their primary functionality in normal network operations, they will henceforth be described as "routers" or "service edge routers" unless switching functions are specifically referenced.

2.2 Product Description

The Marconi service 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 potentially redundant System Input/Output interfaces (SIOs), Route Control Processors (RCPs), Packet Switching Fabrics (PXFs), power supplies, and the device management interface. The TOE is managed by the ShadeTree Routing Control Software (RCS), which controls the TOE's operation. SIOs are the physical network interfaces that allow the TOE to be customized to the intended environment. In the BXR-1000 model of the TOE, the SIO functionality and interfaces are incorporated into the RCPs, while in the BXR-5000 model of the TOE, the SIO functionality and interfaces are contained in a separate card.



The service edge routers are powered by RCPs running the ShadeTree RCS, which are included in the TOE and which manage all network traffic management functions including cell, packet, and IP routing functions. The appliances support numerous routing and 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 Telnet/SSH.

Additionally, they may be monitored via SNMP using standard GET commands, although configuration changes may not be made via SNMP. (SNMP operates in Read-Only mode in managing the TOE.)

2.3 Security Environment TOE Boundary

The TOE appliance houses the software and hardware components necessary to perform all switching and routing functions. The TOE includes both physical and logical boundaries. The TOE is a self-contained network appliance that provides physical and logical connections for network management access.

2.3.1 Physical Boundaries

The TOE physical boundaries encompass all components that are managed by the RCPs that power the Marconi service edge routers. These components include the network management component, the administrative network component, and telnet/ssh and SNMP interfaces.

The network management component controls network traffic. This component groups the RCPs, SIOs, and all the optical interfaces and/or port cards used for all switching and routing functions, including connecting the TOE to all the environment networks, and providing address filtering services.

The administrative local network component is used to configure, manage and overall administer the appliance through a command line interface (CLI), for which the TOE controls access. The TOE provides several methods for accessing the CLI.

Remote administrator users can access the CLI using Telnet to access the CLI commands and directories (grouping of commands). Remote administrator users can also monitor but not otherwise manage the TOE using the SNMP interface.

2.3.2 Logical Boundaries

The logical boundaries of the TOE include the security functions implemented at the TOE interfaces. These functions include Security Audit, Information Flow Control, Identification and Authentication, Security Management and TSF Protection.

2.3.2.1 Security Audit

The TOE provides an audit feature that provides the ability to audit user actions related to authentication attempts and administrator actions.

2.3.2.2 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.

2.3.2.3 Identification and Authentication

The TOE requires administrative 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 such users via “profiles”, providing administrative flexibility by allowing highly granular assignment of management rights down to the level of individual commands or entire “directories” of commands. Only authorized administrators may access the TOE. Note, however, that for the purposes of this ST, any user that is defined such that they can directly authenticate to the TOE is considered to be an administrator though the specific authorizations may vary with the profile of the individual TOE user (administrator). End users whose traffic may traverse the TOE via its switching and routing functions do not need to be authenticated to use these services since they have no

control over the TOE. Thus the term "user" as applied to the TOE should be understood to refer to administrators unless otherwise specified by terms such as "end users."

2.3.2.4 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. Additionally, many of the TOE's functions can be monitored remotely via SNMP GET. Through the CLI, authorized administrators can configure and manage all TOE functions, including configuring the TOE and managing administrative user accounts (if authorized by their profile).

2.3.2.5 Protection of Security Functions

The TOE provides protection mechanisms for its security functions. One of the protection mechanisms is that administrative users must authenticate before any administrative operations can be performed on the system, whether those functions are related to the management of administrative user accounts or the configuration of of the switching and routing functions. 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.

3. Security Environment

The TOE security environment describes the security aspects of the intended environment in which the TOE is to be used and the manner in which it is expected to be employed.

The statement of TOE security environment defines the following:

- threats that the product is designed to counter and
- assumptions made on the operational environment and the method of use intended for the product.

3.1 Threats to Security

The following are threats identified for the TOE.

3.1.1 TOE Threats

T.ACCOUNT	An administrator might perform authentication or security management related 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	An user might intentionally misconfigure TOE security policy mechanisms.
T.NETFLOW	A user might be able to gain inappropriate access to information or network resources that should be restricted.
T.PROTECT	The TOE might be subject to malicious tampering or bypass of its security mechanisms by untrusted subjects.

3.2 Secure Usage Assumptions

The following usage assumptions are made about the intended environment of the TOE.

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.

4. Security Objectives

This section defines the security objectives of the TOE and its supporting environment. Security objectives, categorized as either security objectives for the TOE or Security Objectives for the TOE environment, reflect the stated intent to counter all identified threats and cover all identified assumptions. The security objectives for the TOE environment must be satisfied in order for the TOE to fulfill its own security objectives. All identified threats and assumptions are addressed by one or more of the objectives defined below.

4.1 Security Objectives for the TOE

The following security objectives are intended to be satisfied by the TOE.

O.AUDIT	The TOE shall generate audit records for TOE access attempts and administrator actions.
O.AUTH	The TOE shall require users to be identified and authenticated before any management functions can be performed.
O.CONFIG	The TOE shall ensure that authorized administrators, and only authorized administrators can configure the TOE security policy mechanisms.
O.FLOW	The TOE shall control the flow of information among its network connections.
O.PROTECT	The TOE shall protect itself from tampering and bypass of its security mechanisms.

4.2 Security Objectives for the Environment

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

5. IT Security Requirements

This section provides a list of all security functional requirements for the TOE.

5.1 TOE Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the TOE. All SFRs are drawn from the CC Part 2. This section organizes the SFRs by CC class. Table 1 identifies all SFRs implemented by the TOE.

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit data generation
FDP: User data protection	FDP_IFC.1: Subset information flow control
	FDP_IFF.1: Simple security attributes
FIA: Identification and authentication	FIA_ATD.1: User attribute definition
	FIA_UAU.1: Timing of authentication
	FIA_UID.1: Timing of identification
FMT: Security management	FMT_MOF.1: Management of security functions behaviour
	FMT_MSA.1: Management of security attributes
	FMT_MSA.3: Static attribute initialization
	FMT_MTD.1: Management of TSF data
	FMT_SMF.1: Specification of management functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_RVM.1: Non-bypassability of the TSP
	FPT_SEP.1: TSF domain separation
	FPT_STM.1: Reliable time stamps

Table 1 TOE Security Functional Components

5.1.1 Security Audit (FAU)

5.1.1.1 Audit data generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [***not specified***] level of audit; and

c) [**user authentication attempts and administrator actions**].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**no additional content**].

5.1.2 Information Flow Control (FDP)

5.1.2.1 Subset information flow control (FDP_IFC.1)

FDP_IFC.1.1 The TSF shall enforce the [**Router information flow control SFP**] on

[**subjects: IT entities that send information through the TOE;**

information: network traffic; and,

operations: switching and routing of information].

5.1.2.2 Simple security attributes (FDP_IFF.1)

FDP_IFF.1.1 The TSF shall enforce the [**Router information flow control SFP**] based on the following types of subject and information security attributes:[

a. subject security attributes:

- **the presumed address**

b. informationflow security attributes:

- **presumed address of the source subject;**
- **presumed address of the destination subject;**
- **transport layer protocol;**
- **application layer protocol;**
- **TOE network interface on which traffic information arrives and departs].**

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- **For switching and routing configurations, information is allowed to flow between TOE network interfaces only if:**
  - **a virtual circuit has been established between the inbound TOE interface and some other ATM interface (in which case the information is forwarded to the associated outbound TOE ATM interface) OR**
  - **the presumed destination address of the information identifies a subject associated with an outbound TOE interface (in which case the information is forwarded to the identified outbound TOE interface) OR**
  - **the presumed destination address of the information identifies a subject that is not associated with any TOE interface AND the TOE has been configured to broadcast traffic when it doesn't recognize the presumed address of the destination subject (in which case the information is broadcast out to all TOE interfaces that are not configured as part of a virtual circuit OR discarded).**
- **If the TOE has been configured to filter (drop) traffic when it doesn't recognize the presumed address of the destination subject, then traffic containing information intended for such unknown destination addresses is not allowed to flow between TOE network interfaces.**
- **For switch router configurations the following ADDITIONAL rules are applied such that information is allowed to flow between TOE network interfaces only if:**
  - **all the information flow security attribute values are unambiguously permitted by the information flow control SFP rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator**].

FDP_IFF.1.3 The TSF shall enforce the [**no additional information flow control SFP rules**].

FDP_IFF.1.4 The TSF shall provide the following: [**no additional SFP capabilities**].

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [**no additional information flow control SFP rules**].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [**no additional information flow control SFP rules**].

5.1.3 Identification and authentication (FIA)

5.1.3.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

- **User role and profile**
- **UserID**
- **Password**
- **Access privileges**].

5.1.3.2 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow [**information flow, subject to the Router information flow SFP**] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.3.3 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow [**information flow, subject to the Router information flow SFP**] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.4 Security Management (FMT)

5.1.4.1 Management of security functions behavior (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to [***enable, disable, determine and modify the behavior of***] the functions [**the Router Information Flow Control SFP Rules**] to [**authorized administrator**].

5.1.4.2 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the [**Router information flow control SFP**] to restrict the ability to [***change_default, modify or delete***] the security attributes [**ACLs on the switch router**] to [**authorized administrators**].

5.1.4.3 Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the [**Router information flow control SFP**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**authorized administrator**] to specify alternative initial values to override the default values when an object or information is created.

5.1.4.4 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to [***modify, delete,* [create]**] the [**user profiles**] to [**authorized administrators**].

5.1.4.5 Specification of management functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [

- **Router Information Flow control SFP and**
- **Maintain users and profiles**].

5.1.4.6 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [**super-user, read-only, operator, unauthorized, and custom**].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.5 Protection of the TOE Security Functions (FPT)

5.1.5.1 Non-bypassability of the TSP (FPT_RVM.1)

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.5.2 TSF domain separation (FPT_SEP.1)

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.5.3 Reliable Time Stamp (FPT_STM.1)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.2 IT Environment Security Functional Requirements

There are no environmental security functional requirements.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level (EAL) 3 components as specified in Part 3 of the Common Criteria. The minimum strength of function for mechanisms used within the TOE is SOF-Basic. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ACM: Configuration management	ACM_CAP.3: Authorisation controls
	ACM_SCP.1: TOE CM coverage
ADO: Delivery and operation	ADO_DEL.1: Delivery procedures
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1: Informal functional specification
	ADV_HLD.2: Security enforcing high-level design

	ADV_RCR.1: Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance
ALC: Life cycle support	ALC_DVS.1: Identification of security measures
ATE: Tests	ATE_COV.2: Analysis of coverage
	ATE_DPT.1: Testing: high-level design
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_MSU.1: Examination of guidance
	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.1: Developer vulnerability analysis

Table 2 EAL 3 Assurance Components

5.3.1 Configuration management (ACM)

5.3.1.1 Authorisation controls (ACM_CAP.3)

ACM_CAP.3.1d The developer shall provide a reference for the TOE.
ACM_CAP.3.2d The developer shall use a CM system.
ACM_CAP.3.3d The developer shall provide CM documentation.
ACM_CAP.3.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.3.2c The TOE shall be labelled with its reference.
ACM_CAP.3.3c The CM documentation shall include a configuration list and a CM plan.
ACM_CAP.3.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.3.5c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.3.6c The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.3.7c The CM system shall uniquely identify all configuration items.
ACM_CAP.3.8c The CM plan shall describe how the CM system is used.
ACM_CAP.3.9c The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.3.10c The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
ACM_CAP.3.11c The CM system shall provide measures such that only authorised changes are made to the configuration items.
ACM_CAP.3.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.2 TOE CM coverage (ACM_SCP.1)

ACM_SCP.1.1d The developer shall provide a list of configuration items for the TOE.
ACM_SCP.1.1c The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.
ACM_SCP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and operation (ADO)

5.3.2.1 Delivery procedures (ADO_DEL.1)

ADO_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2d The developer shall use the delivery procedures.

ADO_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1d The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1c The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

ADO_IGS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2e The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

5.3.3.1 Informal functional specification (ADV_FSP.1)

ADV_FSP.1.1d The developer shall provide a functional specification.

ADV_FSP.1.1c The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2c The functional specification shall be internally consistent.

ADV_FSP.1.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4c The functional specification shall completely represent the TSF.

ADV_FSP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.2 Security enforcing high-level design (ADV_HLD.2)

ADV_HLD.2.1d The developer shall provide the high-level design of the TSF.

ADV_HLD.2.1c The presentation of the high-level design shall be informal.

ADV_HLD.2.2c The high-level design shall be internally consistent.

ADV_HLD.2.3c The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5c The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6c The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8c The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9c The high-level design shall describe the separation of the TOE into TSPenforcing and other subsystems.

ADV_HLD.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.2.2e The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1d The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1c For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

ADV_RCR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Guidance documents (AGD)

5.3.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1d The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1c The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2c The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3c The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4c The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5c The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6c The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7c The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8c The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

AGD_ADM.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.

AGD_USR.1.1c The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2c The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3c The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4c The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5c The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6c The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

AGD_USR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5 Life cycle support (ALC)

5.3.5.1 Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1d The developer shall produce development security documentation.

ALC_DVS.1.1c The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ALC_DVS.1.2c The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.
ALC_DVS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ALC_DVS.1.2e The evaluator shall confirm that the security measures are being applied.

5.3.6 Tests (ATE)

5.3.6.1 Analysis of coverage (ATE_COV.2)

ATE_COV.2.1d The developer shall provide an analysis of the test coverage.
ATE_COV.2.1c The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_COV.2.2c The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.
ATE_COV.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.2 Testing: high-level design (ATE_DPT.1)

ATE_DPT.1.1d The developer shall provide the analysis of the depth of testing.
ATE_DPT.1.1c The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.
ATE_DPT.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.3 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.
ATE_FUN.1.2d The developer shall provide test documentation.
ATE_FUN.1.1c The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2c The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3c The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4c The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5c The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.
ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.4 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.
ATE_IND.2.1c The TOE shall be suitable for testing.
ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2e The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.7 Vulnerability assessment (AVA)

5.3.7.1 Examination of guidance (AVA_MSU.1)

AVA_MSU.1.1d The developer shall provide guidance documentation.
AVA_MSU.1.1c The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AVA_MSU.1.2c The guidance documentation shall be complete, clear, consistent and reasonable.
AVA_MSU.1.3c The guidance documentation shall list all assumptions about the intended environment.
AVA_MSU.1.4c The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).
AVA_MSU.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_MSU.1.2e The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.
AVA_MSU.1.3e The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

5.3.7.2 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1d The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.
AVA_SOF.1.1c For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.
AVA_SOF.1.2c For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.
AVA_SOF.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.3.7.3 Developer vulnerability analysis (AVA_VLA.1)

AVA_VLA.1.1d The developer shall perform a vulnerability analysis.
AVA_VLA.1.2d The developer shall provide vulnerability analysis documentation.
AVA_VLA.1.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.
AVA_VLA.1.2c The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.
AVA_VLA.1.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.
AVA_VLA.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VLA.1.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

The TOE implements the following security functions:

- Security Audit
- Information Flow Control
- Identification and Authentication
- Security Management
- TSF Protection

6.1.1 Security Audit

The Security Audit function provides for auditing user logon attempts, administrator actions, TOE shutdown and TOE startup events. The TOE includes an audit feature that can be configured to generate records of events related to attempts to login to the appliance and subsequently administrator actions. Note that logging is always enabled while the TOE is in operation.

The TOE can generate audit records of all the events indicated in section 5.1 as part of the definition of FAU_GEN.1.1. Audit records include at least event time and date, event type, subject identity and outcome (success or failure). The TOE also provides a means of storing and reviewing audit records either via its local file storage and viewing capabilities or by sending audit records as SYSLOG messages to an administrative system on the TOE's secure management network.

The Security Audit security function instantiate the following security functional requirements:

- FAU_GEN.1 is addressed by generating records of users actions specified within the definition of the security requirement.

6.1.2 Information Flow Control

The Information Flow Control security function provides for controlling network traffic. It implements an information flow security policy that controls how information moves through the system and regulates exchange of information between devices connected to the network.

In all appliances, the TOE enforces a relatively simple information flow policy. When the TOE receives network traffic, it associates subjects (based on their presumed source address as indicated in the received traffic) with TOE interfaces. Subsequently, when the TOE receives network traffic it will use the (subject) destination address in the traffic to identify whether an outbound TOE interface is associated with the destination address. If an outbound TOE interface is identified, that is where the traffic will be sent. Otherwise, the traffic will either be discarded or broadcast on all TOE interfaces (not associated with a virtual circuit), depending on how the administrator has configured the TOE.

Furthermore, all appliances with ATM network interfaces allow administrators to define ATM virtual circuits which essentially bind two TOE ATM interfaces together. Any traffic received on one of the associated TOE ATM interfaces is simply forwarded to the other associated TOE ATM interface.

In addition to these simple switching information flow rules, the service edge router appliances impose rules based on additional traffic content. Specifically, they allow the administrator to configure filters based on presumed source and destination addresses, transport and application layer protocols, and inbound and outbound TOE interfaces. The

administrator can specify essentially any combination of the attributes identified above to define allowable information flows.

Note that the information flow rules are permissive by default and hence, will allow traffic to flow freely. The administrator can subsequently choose to establish virtual circuits, to disallow broadcast of switched traffic with an unknown destination interface, and to establish more specific filters based on specific addresses, protocols, and interfaces.

The Information Flow Control security function instantiates the following security functional requirements:

- FDP_IFC.1 is addressed by enforcing an information flow control policy to control traffic.
- FDP_IFF.1 is addressed by specifying strict rules under the information flow policy.

6.1.3 Identification and Authentication

The Identification and Authentication security function provides for user logon.. The TOE maintains a user list for each individual user that includes a userID, a password used for authentication, and other user-specific information such as allowed applications, lockout status, etc. Only the authorized administrators can create, update, and delete the user lists..

The logon process ensures that users are identified and authenticated before they can access any TSF-mediated functions in the TOE that are not associated with the flow of information among TOE network interfaces. When users connect to the TOE either via the local console or remotely using telnet, they are presented with a login dialog that requests their username and password. The TOE authenticates the users by comparing the information received at the login dialog against the security attributes in the user list stored in the TOE. If users utilize SNMP GET requests to discover, monitor, manage, or configure the TOE, they must also include the appropriate community strings (for SNMPv1 or 2) or username and password (for SNMPv3 only).

The identification and authentication satisfies the following security functional requirements:

- FIA_ATD.1 is addressed with the system creating and maintaining user lists for each potential TOE user.
- FIA_UAU.1 is addressed with a logon process that requires identification and authentication information as the first step for TOE access.
- FIA_UID.1 is addressed with a logon process that requires identification and authentication information as the first step for TOE access.

6.1.4 Security Management

The Security Management security function provides interfaces for the appropriate management of the TOE information flow and identification and authentication policies. In every case, the administrator functions are restricted to authorized administrators by virtue of the identification and authentication mechanisms, since only authorized administrators are given login accounts which give them direct access to TOE administration functions. Each user is assigned to a specific user profile that determines which CLI commands the user can access and which TOE functions the user can perform. A user may be assigned to only one user profile on the TOE, no matter which access method they use. Only the authorized administrators can create, update, and delete the user profiles.

The TOE maintains a number of roles: ‘super-user’, ‘read-only’, ‘operator’, ‘unauthorized’, and ‘custom’. Throughout the TOE guidance documentation and the CLI, a role is referred to as a “class”.

1) The super-user role or class has all administrative level access privileges and thus can access all areas of the TOE. Administrative users in this class can use all CLI commands to configure all administrator-accessible TOE features, including configuring the device, configuring the TOE audit and information flow control policies, and creating new user profiles.
2) The read-only role or class has no administrative level access privileges. Users in this class can only view the current TOE configuration and information flow policies but cannot change them.

3) The operator role or class defines a limited set of rights for other administrative users to perform specific information flow policy management functions. The operator role or class, as with any of the other pre-defined classes, cannot be modified by an authorized administrator to grant specific rights to specific command directories. By default, users assigned to the 'operator' class are allowed to execute the 'clear,' 'network,' 'trace,' and 'reset' commands, as well as all 'view' commands that allow the viewing of all other TOE configuration information. This prevents a userid assigned to this role from performing such TSF-mediated functions as creating or deleting users, changing other users' passwords, shutting down or rebooting the TOE, changing the TOE's operating system software or firmware, modifying the TOE's auditing functions, etc.

4) The unauthorized role or class defines a severely limited set of rights for TOE administrative users. Users assigned to the 'unauthorized' class may login to the TOE but cannot view or change any of the TOE configuration.. An 'unauthorized' user can display a list of audit log files, but cannot view, copy, change, or delete them. With such limited rights, the 'unauthorized' class may be most useful as a method of preserving a valid userid without allowing that user any rights to view or change the TOE configuration. For example, if a userid is suspected of being responsible for unwarranted or undesired changes to the TOE configuration, or if it is suspected that it has been "hijacked" for use by an unauthorized person, that userid may be assigned to the 'unauthorized' role as a protective measure until further investigation can be completed. Since there is no other means of "disabling" a user account, the 'unauthorized' role fulfills this purpose.

5) A "custom" role or class may be created and assigned specific permissions to allow users in this role to perform various duties on the TOE. Since the other four classes have predefined permissions assigned to them that may not be altered, even by a 'super-user' administrator, only these custom (administrator-created) classes may be assigned specific permissions to perform a variety of tasks. For example, a user in the 'super-user' class could create a new "netops" class and assign it permissions such as 'configure', 'view', 'network-control', 'routing-control', 'forwarding-control', and 'interface-control', then create userids and assign them to this 'netops' class. These userids would then be able to configure, manage, and monitor all information flow control functionality on the TOE as allowed by these permissions, but would not be able to access or configure TOE security, authentication, or auditing features.

For the purposes of this Security Target, however, all of these roles should be considered to be part of the 'administrator' role regardless of the fact that their actual capabilities may vary.

While the TOE allows the administrators to manage its policies, the TOE enforces no information flow restrictions by default and, given the login restrictions, allows only an administrator to change the initial default settings.

- FMT_MOF.1 is enforced by ensuring that only authorized administrators have the ability to manage and modify the applicable functions.
- FMT_MSA.1 is enforced by ensuring that only authorized administrators have the ability to manage and modify the applicable functions.
- FMT_MSA.3 is enforced by enforcing a permissive default information flow policy and ensuring that only authorized administrators have the ability to manage and modify the default policy.
- FMT_MTD.1 is enforced by ensuring that only authorized administrators have the ability to manage and modify the applicable functions.
- FMT_SMF.1 is enforced by offering interfaces to allow only authorized administrators the ability to manage information flow and identification and authentication related information.
- FMT_SMR.1 is enforced by assigning every user of the TOE a role supporting the administrator role for the management of TOE policies.

6.1.5 TSF Protection

The TOE TSF Protection security function provides for non-bypassability of the TSF, domain separation and time stamp.

The TOE has complete access control to its resources. All administrators and users that access TOE data and functions must be identified and authenticated. The TOE enforces an information flow control security policy that controls network traffic and covers all exchanges of information that occurs in the TOE. The TOE implements audit functionality to monitor administrator and user actions.

The TOE is an appliance in which all operations are self-contained, with all administration and configuration operations performed within the physical boundary of the TOE. These functions include the creation and maintenance of routing and switching tables as well as the routing/switching of packets, frames, or cells themselves. The control software within the TOE controls all operations. The TOE operates solely as a service edge router and neither performs nor supports other non-switch/router related functions.

The Marconi service edge routers include a time clock which is used to stamp all records generated by the TOE.

The TSF Protection security function is designed to satisfy the following TOE security requirements:

- FPT_RVM.1 is enforced by ensuring that the TOE allows only authorized administrators the ability to manage and modify its information flow and identification and authentication rules at the applicable interfaces.
- FPT_SEP.1 is enforced by instantiation of the TOE in an appliance that protects itself at its external interfaces.
- FPT_STM.1 is enforced by providing a time stamp for use in creating audit records.

6.2 TOE Security Assurance Measures

The following assurance measures are applied to satisfy the Common Criteria EAL3 assurance requirements:

- Process Assurance;
- Delivery and Guidance;
- Design Documentation;
- Tests; and
- Vulnerability Assessment.

6.2.1 Process Assurance

6.2.1.1 Configuration Management

The configuration management measures applied by Marconi ensure that there is a CM Plan, configuration items are uniquely identified, a configuration list is maintained, that only authorized changes are made, and that documented procedures are used to control and track changes that are made to the TOE. Marconi ensures changes to the implementation representation are controlled and that TOE associated configuration item modifications are properly controlled. Marconi performs configuration management on the TOE implementation representation, design, tests, user and administrator guidance, delivery and installation documentation, and the CM documentation. Note that the TOE is also labeled appropriately with its identification. These activities are documented in:

- Marconi CM Procedures
- Marconi CMM Processes
- Marconi Lifecycle Management Process

The Configuration Management assurance measure satisfies the following assurance requirements:

- ACM_CAP.3
- ACM_SCP.1

6.2.2 Delivery and Guidance

Marconi provides delivery documentation that explains how the TOE is delivered and procedures to identify the TOE, allow detection of unauthorized modifications of the TOE and installation and generation instructions at start-up. Marconi's delivery procedures describe the steps to be used for the secure installation, generation, and start-up of the TOE along with configuration settings to secure the TOE privileges and functions. The delivery procedures are documented in:

- Product Configuration Management Request Forms (ECN's, CUP's, DEV's) CMFM-4490-001 | REV. D
- PRFC-1062 Distribution Material Flow
- PRST-4150-001 Handling, Storage, Preservation, and Delivery of Products
- PRWI-1099 Material Flow Guide
- PROP-4155-001 Pre-Pack Boxing and Labeling Procedure

Marconi provides administrator guidance in the installation and initialization procedures. The installation and generation procedures, included in the administrator guidance, describe the steps necessary to install and operate Marconi products in accordance with the evaluated configuration, detailing how to establish and maintain the secure configuration. Since only an administrator can access TOE configuration commands, that is the only guidance

provided. Administrators can create other administrative users with rights to defined command directories and non-administrative read-only users who have no direct access to the TOE security or systems commands, only using it as a generic network connection component when communicating across connected networks.

The installation and administrator guidance is documented in:

- BXR-5000 and BXR-1000 User Guide, Volumes 1 to 9
- BXR-1000 Hardware Installation Guide
- BXR-5000 Hardware Installation Guide
- BXR-5000 and BXR-1000 Service Edge Router Release Notes, v3.1.1
- BXR-5000 and BXR-1000 CC Evaluated Configuration Guide

The Delivery and Guidance assurance measure satisfies the following Assurance requirements:

- ADO_DEL.1
- ADO_IGS.1
- AGD_ADM.1
- AGD_USR.1

6.2.3 Development

The Design Documentation provided for BXR-1000/5000 service edge router Products is provided in the following documents:

- Marconi BXR-1000 and BXR-5000 Functional Specification
- Marconi BXR-1000 and BXR-5000 High-level Design

These documents are internally consistent and serve to describe the security functions of the TOE, its interfaces both external and between subsystems, the architecture of the TOE (in terms of subsystems), and correspondence between the available design abstractions (including the ST). The high-level design describes the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate. The Design Documentation security assurance measure satisfies the following security assurance requirement:

- ADV_FSP.1
- ADV_HLD.2
- ADV_RCR.1

6.2.4 Life-Cycle Support

Marconi has development security documentation that describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Marconi's development security documentation can be found in:

- BBRS-PO-001_Marconi Information Security Program ver 2.1

The Life-cycle assurance measure satisfies the following assurance requirements:

- ALC_DVS.1

6.2.5 Tests

The Test Documentation is found in the following documents:

- Marconi BXR-1000 and BXR-5000 Test Plan
- Actual BXR-1000 and BXR-5000 Test Results

These documents provide an analysis of the test coverage depth and demonstrate correspondence between the tests identified and the security functions in the functional specification, describe the overall test plan, testing procedures, the tests themselves, including expected and actual results. In addition, these documents describe how the functional specification has been appropriately tested.

The Tests assurance measure satisfies the following assurance requirements:

- ATE_COV.2
- ATE_FUN.1
- ATE_IND.2

6.2.6 Vulnerability Assessment

Marconi has guidance documents that identify all possible modes of operation of the TOE, their consequences and implications for secure operation. The guidance documents also describe external security measures including physical and personnel security of the TOE development environment and developers. The applicable guidance and physical and personnel security procedures can be found in:

- BXR-5000 and BXR-1000 User Guide, Volumes 1 to 9
- BXR-5000 and BXR-1000 CC Evaluated Configuration Guide
- BBRS-PO-001_Marconi Information Security Program ver 2.1

Each probabilistic or permutational mechanism used by the TOE must satisfy the SOF-Basic requirements. The only probabilistic or permutational mechanism used in the TOE is the authentication mechanism. Marconi has performed a strength of function analysis that indicates that the authentication mechanism fulfills at least SOF-Basic. Similarly, Marconi performed a vulnerability analysis of the TOE to identify weaknesses that can be exploited in the TOE. Both the strength of function analysis and the vulnerability analysis are documented in:

- Marconi BXR-1000 and BXR-5000 SOF Analysis
- Marconi BXR-1000 and BXR-5000 Vulnerability Analysis

The Vulnerability Assessment assurance measure satisfies the following assurance requirements:

- AVA_MSU.1
- AVA_SOF.1
- AVA_VLA.1

7. Protection Profile Claims

There are no PP claims for this evaluation.

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- TOE Summary Specification;
- Security Functional Requirement Dependencies; and
- Internal Consistency.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption or threat.

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of threats and usage assumptions by the security objectives.

	T.ACCOUNT	T.AUTH	T.CONFIG	T.DETECT	T.MISCONFIG	T.NETFLOW	T.PROTECT	A.ADMIN	A.CONNECT	A.NOEVIL	A.PHYSICAL
O.AUDIT	X			X							
O.AUTH		X									
O.CONFIG			X		X						
O.FLOW						X					
O.PROTECT							X				
OE.ADMIN					X			X			
OE.CONNECT									X		
OE.NOEVIL										X	
OE.PHYSICAL											X

Table 3 Environment to Objective Correspondence

8.1.1.1 T.ACCOUNT

An administrator might perform authentication or security management related actions for which they are not accountable

This Threat is satisfied by ensuring that:

- O.AUDIT: The TOE must audit administrator actions.

8.1.1.2 T.AUTH

A user might be able to gain unauthorized access to TOE functions.

This Threat is satisfied by ensuring that:

- O.AUTH: The TOE must ensure that users are identified and authenticated before they can perform any management functions.

8.1.1.3 T.CONFIG

An administrator might not be able to configure the TOE security policy mechanisms.

This Threat is satisfied by ensuring that:

- O.CONFIG: The TOE must ensure that authorized administrators can configure the TOE security policy mechanisms.

8.1.1.4 T.DETECT

A user's attempts to violate TOE authentication and security management security mechanisms may go undetected.

This Threat is satisfied by ensuring that:

- O.AUDIT: The TOE must audit user attempts to access the TOE and use of administrator functions.

8.1.1.5 T.MISCONFIG

A user might intentionally misconfigure TOE security policy mechanisms.

This Threat is satisfied by ensuring that:

- O.CONFIG: The TOE must ensure that authorized administrators can configure the TOE security policy mechanisms.
- OE.ADMIN: It is assumed that administrators will adhere to applicable guidance when configuring security policies.

8.1.1.6 T.NETFLOW

A user might be able to gain inappropriate access to information or network resources that should be restricted.

This Threat is satisfied by ensuring that:

- O.FLOW: The TOE must control information flows among its network connections, thereby ensuring that users can access only information or other resources via those flows allowed by the TOE policies.

8.1.1.7 T.PROTECT

The TOE might be subject to malicious tampering or bypass of its security mechanisms by untrusted subjects.

This Threat is satisfied by ensuring that:

- O.PROTECT: The TOE must protect itself from tampering and bypass of its mechanisms.

8.1.1.8 A.ADMIN

The administrators will be competent and will adhere to the applicable TOE guidance.

This Assumption is satisfied by ensuring that:

- OE.ADMIN: Both the assumption and objective indicate that the administrators will be competent and will adhere to the applicable TOE guidance.

8.1.1.9 A.CONNECT

The TOE will be installed in a network infrastructure such that it can effectively control the flow of the applicable information.

This Assumption is satisfied by ensuring that:

- OE.CONNECT: Both the assumption and objective indicate that the TOE will be installed in a network infrastructure such that it can effectively control the flow of the applicable information.

8.1.1.10 A.NOEVIL

The administrators of the TOE will not be willfully negligent or otherwise hostile.

This Assumption is satisfied by ensuring that:

- OE.NOEVIL: Both the assumption and objective indicate that the administrators of the TOE will not be willfully negligent or otherwise hostile.

8.1.1.11 A.PHYSICAL

The TOE will be protected from unauthorized physical access.

This Assumption is satisfied by ensuring that:

- OE.PHYSICAL: Both the assumption and objective indicate that the TOE will be protected from unauthorized physical access.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that the following table indicates the requirements that effectively satisfy the individual objectives. .

8.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

	O.AUDIT	O.AUTH	O.CONFIG	O.FLOW	O.PROTECT
FAU_GEN.1	X				
FDP_IFC.1				X	
FDP_IFF.1				X	
FIA_ATD.1		X			
FIA_UAU.1		X			
FIA_UID.1		X			
FMT_MOF.1			X		
FMT_MSA.1			X		
FMT_MSA.3			X		
FMT_MTD.1			X		
FMT_SMF.1			X		
FMT_SMR.1			X		
FPT_RVM.1					X
FPT_SEP.1					X

FPT_STM.1	X				

Table 4 Objective to Requirement Correspondence

8.2.1.1 O.AUDIT

The TOE shall generate audit records for TOE access attempts and administrator actions.

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN.1: The TOE is required to generate audit records for user authentication attempts and administrator actions.
- FPT_STM.1: The TOE is required to generate time stamps that can be used in creating audit records.

8.2.1.2 O.AUTH

The TOE shall require users to be identified and authenticated before any management functions can be performed.

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1: The TOE is required to maintain user attributes to support identification and authentication of authorized users.
- FIA_UAU.1: The TOE is required to authenticate users prior to offering access to administrator functions.
- FIA_UID.1: The TOE is required to identify users prior to offering access to administrator functions.

8.2.1.3 O.CONFIG

The TOE shall ensure that authorized administrators, and only authorized administrators can configure the TOE security policy mechanisms.

This TOE Security Objective is satisfied by ensuring that:

- FMT_MOF.1: The TOE is required to restrict the ability to manage information flow security function to an authorized administrator.
- FMT_MSA.1: The TOE is required to restrict the ability to manage information flow security attributes to an authorized administrator.
- FMT_MSA.3: The TOE is required to provide permissive default information flow values and to restrict the ability to modify the initial values to authorized administrators.
- FMT_MTD.1: The TOE is required to restrict the ability to manage authorized users to an authorized administrator.
- FMT_SMF.1: The TOE is required to provide administrator functions to manage the information flow rules and to manage authorized users.
- FMT_SMR.1: The TOE is required to provide an authorized administrator role.

8.2.1.4 O.FLOW

The TOE shall control the flow of information among its network connections.

This TOE Security Objective is satisfied by ensuring that:

- FDP_IFC.1: The TOE is required to control the flow of information among its network connections.
- FDP_IFF.1: The TOE is required to enforce the configured security policy rules for information flow.

8.2.1.5 O.PROTECT

The TOE shall protect itself from tampering and bypass of its security mechanisms.

This TOE Security Objective is satisfied by ensuring that:

- FPT_RVM.1: The TOE is required to ensure it security mechanisms cannot be bypassed.
- FPT_SEP.1: The TOE is required to protect itself from tampering.

8.3 Security Assurance Requirements Rationale

This ST contains the assurance requirements components of the EAL3 assurance package defined in the CC. The TOE environment will be exposed to a low level of attack risk. As such, the Evaluation Assurance Level Three (low to moderate level of assurance) and the strength of function claim SOF –basic are appropriate.

8.4 Requirement Dependency Rationale

The ST satisfies all the requirement dependencies of the Common Criteria, as indicated in the table below.

ST Requirement	CC Required Dependencies	ST Provided Dependencies
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FDP_IFC.1	FDP_IFF.1	FDP_IFF,1
FDP_IFF.1	FDP_IFC.1 and FMT_MSA.3	FDP_IFC.1 and FMT_MSA.3
FIA_ATD.1	none	none
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UID.1	none	none
FMT_MOF.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MSA.1	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_IFC.1
FMT_MSA.3	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1 and FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	none	none
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_RVM.1	none	none
FPT_SEP.1	none	none
FPT_STM.1	none	none
ACM_CAP.3	ALC_DVS.1	ALC_DVS.1
ACM_SCP.1	ACM_CAP.3	ACM_CAP.3
ADO_DEL.1	none	none
ADO_IGS.1	AGD_ADM.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1	ADV_RCR.1
ADV_HLD.2	ADV_FSP.1 and ADV_RCR.1	ADV_FSP.1 and ADV_RCR.1
ADV_RCR.1	none	none
AGD_ADM.1	ADV_FSP.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1	ADV_FSP.1

ALC_DVS.1	none	none
ATE_COV.2	ADV_FSP.1 and ATE_FUN.1	ADV_FSP.1 and ATE_FUN.1
ATE_DPT.1	ADV_HLD.1 and ATE_FUN.1	ADV_HLD.2 and ATE_FUN.1
ATE_FUN.1	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1
ATE_IND.2	none	none
AVA_MSU.1	ADO_IGS.1 and ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1	ADO_IGS.1 and ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1
AVA_SOF.1	ADV_FSP.1 and ADV_HLD.1	ADV_FSP.1 and ADV_HLD.2
AVA_VLA.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1	ADV_FSP.1 and ADV_HLD.2 and AGD_ADM.1 and AGD_USR.1

Table 5 Requirement Dependency Rationale

8.5 Explicitly Stated Requirements Rationale

There are no explicitly stated requirements.

8.6 Strength of Function Rationale

The password used at the logon process is the only probabilistic or permutational mechanism implemented in the TOE. This mechanism is associated with the Identification and Authentication security function and instantiates the FIA_UAU.1 security functional requirements. The password space is calculated in the Strength of Function analysis.

The system places the following restrictions on the passwords selected by the user:

- The password must be at least 6 characters long; and

The ST associates a SOF-Basic minimum strength of function level with the TOE security functional requirements and the TOE security functions.

8.7 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 6 Security Functions vs. Security Requirements Mapping**~~**Table 6 Security Functions vs. Security Requirements Mapping**~~ demonstrates the relationship between security requirements and security functions.

	SECURITY AUDIT	INFORMATION FLOW CONTROL	IDENTITY & AUTHENTICATION	SECURITY MANAGEMENT	TSF PROTECTION
FAU_GEN.1	X				
FDP_IFC.1		X			
FDP_IFF.1		X			
FIA_UAU.1			X		
FIA_ATD.1			X		
FIA_UID.1			X		
FMT_MOF.1				X	
FMT_MSA.1				X	
FMT_MSA.3				X	
FMT_MTD.1				X	
FMT_SMF.1				X	
FMT_SMR.1				X	
FPT_RVM.1					X
FPT_SEP.1					X
FPT_STM.1					X

Table 6 Security Functions vs. Security Requirements Mapping

8.8 PP Claims Rationale

See section 7, Protection Profile Claims.