ERICSSON

# SmartEdge System Description

## DESCRIPTION

10/221 02-CRA 119 1170/1 Uen B

# Contents

# 1 Overview

This document describes the SmartEdge® router, and its usage, services, and architecture.

## 1.1 Scope

This description covers the logical and functional aspects of the product, but does not describe the hardware. For information about SmartEdge hardware, see the SmartEdge Hardware Library.

## 1.2 Audience

This document is intended to introduce the router to anyone who is not familiar with the platform.

# 2 Introduction

The SmartEdge multiservice edge routers (MSERs) combine multiple functionalities into a single platform that provides Layer 3 (IP) edge routing, Layer 2 (Ethernet) network aggregation, broadband network gateway (BNG) services for subscribers, and other advanced services.

The SmartEdge services provide carrier-class reliability, scalability and performance, have minimal power requirements, and include the following:

- Support for a comprehensive range of interior and exterior gateway routing protocols and high-performance multicast routing with predictable and sustained performance
- Support for peering, edge aggregation, and services routing applications where high-performance IP routing is an absolute requirement
- Advanced traffic management with hierarchical quality of service (H-QoS), comprehensive traffic shaping, and subscriber management
- Direct connection to an access layer of the network, such as a DSLAM, eliminating unnecessary network layers and reducing complexity

- Support for up to 256,000 subscribers per physical device and all methods of subscriber encapsulation for DHCP or IP-access clients, including PPP over Ethernet (PPPoE)

The router can be used in solutions that combine Layer 2, Layer 3, and BNG solutions.

Using the router in conjunction with other Ericsson solutions requires the following composite implementations:

- Mobile Packet Backbone Network (MPBN)—Layer 2 and Layer 3
- Mobile Backhaul (MBH)—Layer 2 and Layer 3
- IP Radio Access Network (RAN)—Layer 3
- Converged Packet Gateway—Layer 2, Layer 3, and BNG
- Border Gateway Function (BGF)—Layer 2, Layer 3, and BNG

For a description of each of these solutions, including diagrams and the configuration requirements, see Layer 2 Network, Layer 3 Network, BNG solutions, and SmartEdge Router in Other Ericsson Solutions.

Figure 1 illustrates the possible combinations and where other Ericsson solutions fit with the router.

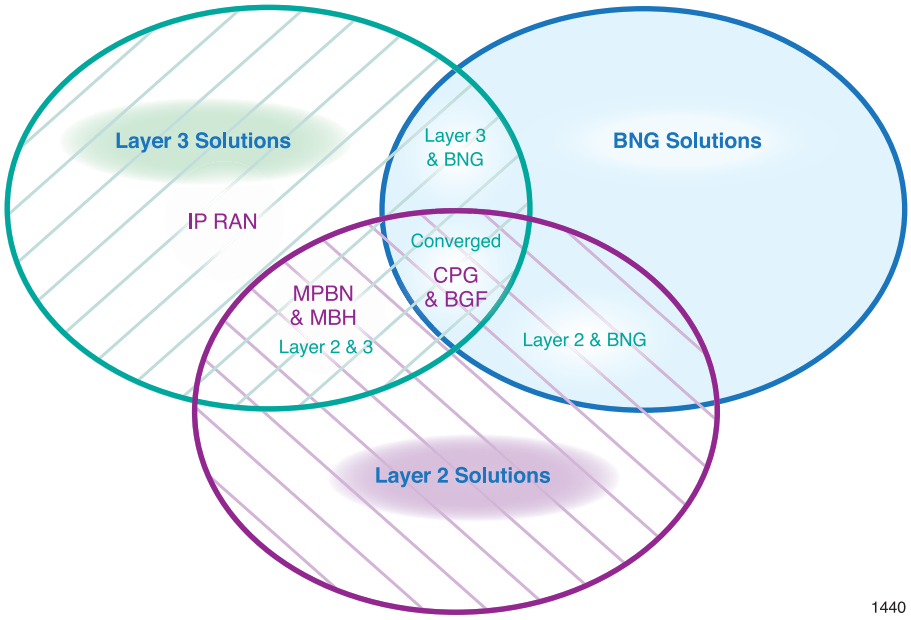


*Figure 1 Possible Service Combinations*

# 3 SmartEdge Use Cases

## 3.1 Layer 2 Network

The router can be used to provide services for Ethernet traffic such as the following:

- Layer 2 Virtual Private Network (L2VPN)—Provides end-to-end Layer 2 connection over IP and MPLS core networks
- Layer 2 frames over an MPLS network
- VPLS—Includes MAC learning, used to create a hierarchy using H-VPLS
- XC VLL-based transport (does not support MAC learning)
- Layer 2 applications—Enterprise VPN (Ethernet based) and Metro Ethernet Transport, including transporting residential access to BNG.

Figure 2 illustrates the router in a Layer 2 network.

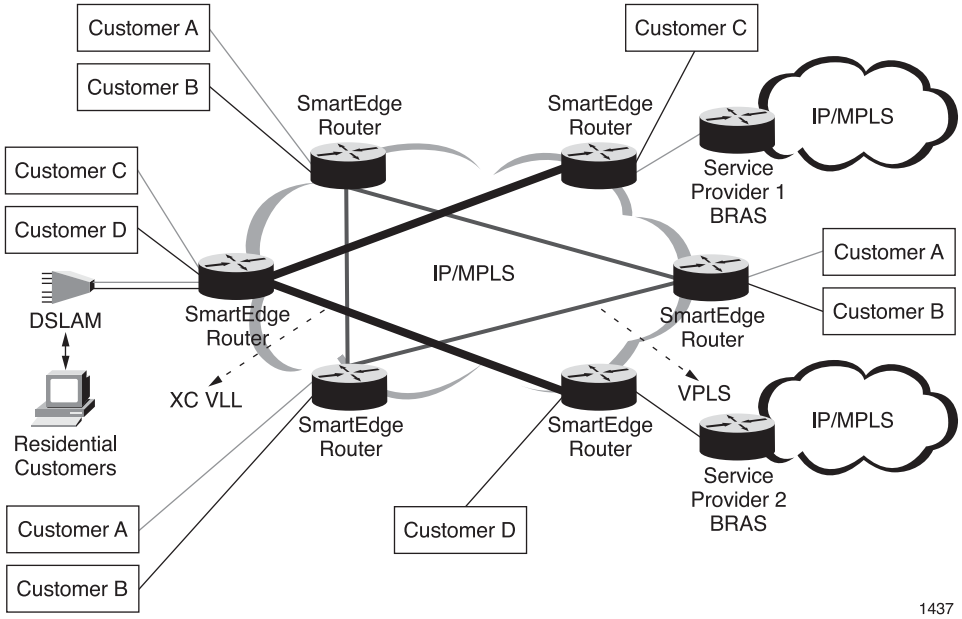


*Figure 2 Layer 2 Network*

Table 1 lists the features that can be configured for Layer 2 solutions.

*Table 1 Features Configured for Layer 2 Solutions*

| Business Application | L2 Transport Method | Routing and Forwarding Options | Services |
|---|---|---|---|
| Integrated Metro Ethernet and BNG | L2VPN VLL<br>L2VPN VPLS | LDP or RSVP<br>ISIS or OSPF | IPoE over PW |
| Metro Ethernet backhaul | L2 bridging | Pure bridging | QoS<br>MAC rate-limiting<br>MAC filtering |
| | L2 XC | Ethernet-to-Ethernet<br>Ethernet-to-ATM Bridge1483<br>Ethernet-to-ATM Route1483 | QoS |
| | L2VPN VLL | One of the following combinations:<br>LDP, ISIS<br>LDP, OSPF<br>RSVP, ISIS<br>RSVP, OSPF | QoS |
| | L2VPN VPLS or H-VPLS | One of the following combinations:<br>T-LDP(FEC Dist), LDP, ISIS<br>T-LDP (FEC Dist), LDP, OSPF<br>T-LDP( FEC Dist), RSVP-TE, ISIS<br>T-LDP( FEC Dist), RSVP-TE, OSPF<br>BGP, LDP, ISIS<br>BGP, LDP, OSPF<br>BGP, RSVP-TE, ISIS<br>BGP, RSVP-TE, OSPF | QoS<br>Multicast services<br>MAC filtering<br>MAC rate-limiting |

## 3.2 Layer 3 Network

The router can be used in many IP topologies, including networks providing the following L3VPN services:

- End-to-end Layer 3 connection over an IP/MPLS core network
- Business VPNs, such as BGP/MPLS Layer 3 VPNs, GRE VPNs, or IPsec VPNs
- BNG with Layer 3 VPN services, such as remote business VPNs and wholesale service offerings

Figure 3 illustrates the router in a Layer 3 network.

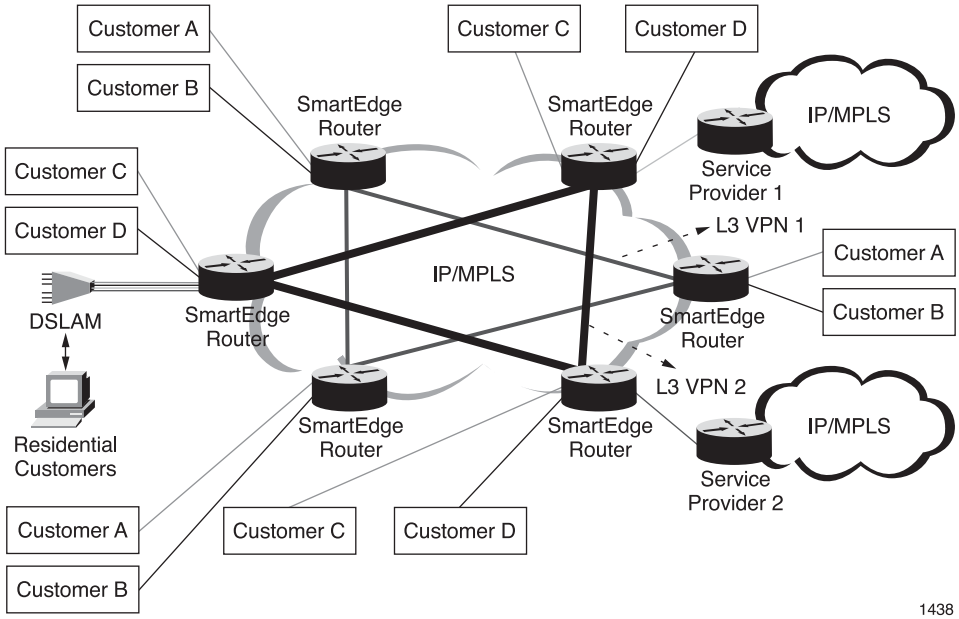


*Figure 3 Layer 3 Network*

Table 2 lists the features that can be configured for Layer 3 solutions.

*Table 2 Features Configured For Layer 3 Solutions*

| Business Application | Access Options | Routing Options | Services |
|---|---|---|---|
| Integrated BNG/L3VPN | PTA<br>L2TP<br>CLIPS<br>DHCP<br>Static Circuits | One of the following combinations:<br>BGP, MPLS, LDP, ISIS<br>BGP, MPLS, LDP, OSPF<br>BGP, MPLS, RSVP-TE, ISIS<br>BGP, MPLS, RSVP-TE, OSPF<br>BGP, MPLS, LDP over 1-hop RSVP, ISIS<br>BGP, MPLS, LDP over 1-hop RSVP, OSPF | QoS<br>CE-PE Routing Options<br>Route Filters |
| Backhaul Applications Such as MPBN | Static Circuits | One of the following combinations:<br>BGP, MPLS, LDP, ISIS<br>BGP, MPLS, LDP, OSPF<br>BGP, MPLS, RSVP-TE, ISIS<br>BGP, MPLS, RSVP-TE, OSPF<br>BGP, MPLS, LDP over 1-hop RSVP, ISIS<br>BGP/, MPLS, LDP over 1-hop RSVP, OSPF | QoS |

## 3.3 BNG Solutions

The router can provide the following BNG services:

- Broadband Remote Access Server

  - PTA: PPP terminated access
  - PPP (over Ethernet, over ATM)
- L2TP terminated access
  - L2TP LAC
  - L2TP LNS
  - L2TP LTS
- DHCP terminated access
  - DHCP
  - CLIPS
- 3-Play service model
  - Broadcast TV, video-on-demand, VoIP, high speed Internet
- Dedicated VLAN per subscriber – Service based VLANs

Figure 4 illustrates the router in a network providing BNG services.

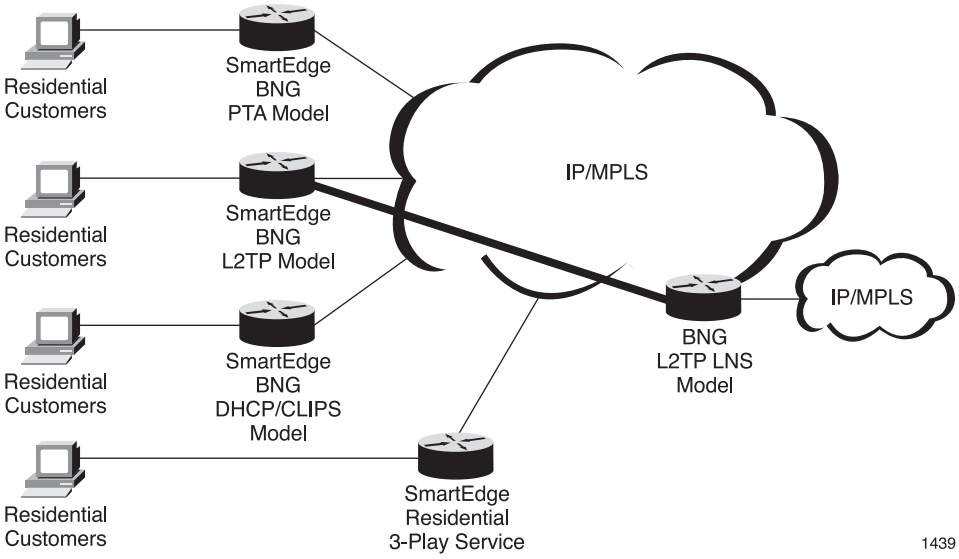


*Figure 4 SmartEdge Router With BNG Solutions*

Table 3 lists the features that can be configured for BNG solutions.

*Table 3 Features Configured for BNG Solutions*

| Business Application | Access Technology | Transport Options | Services |
|---|---|---|---|
| PTA | PPPoE | Single and double VLANs, CCOD, link groups | ACL<br>QoS<br>HTTP-Red<br>LI<br>VoIP<br>Multicast applications<br>NAT<br>Flow services |
| | ML PPPoE | Single and double VLANs, CCOD | |
| | PPPoEoA | ATM PVCs, ATM APS, CCOD | |
| | PPPoA | ATM PVC, ATM APS, CCOD | |
| | ML PPPoA | ATM PVC, ATM APS | |
| L2TP | LAC | Single and double VLANs, CCOD, link groups, ATM PVC, ATM APS | ACL<br>QoS<br>HTTP-Red<br>LI<br>VoIP<br>Multicast applications<br>NAT<br>Flow services |
| | LTS | Routed IP, ECMP IP, link groups, MPLS | |
| | LNS | Routed IP, ECMP IP, link groups, MPLS | |
| | MLPPP/LNS | Routed IP, ECMP IP, link groups, MPLS | |
| CLIPS | Static CLIPS | Single and double VLANs, link groups, ATM PVC, ATM APS | ACL<br>QoS<br>HTTP-Red<br>LI<br>VoIP<br>Multicast applications<br>NAT<br>Flow services |
| | Dynamic CLIPS | Single and double VLANs, CCOD, link groups, ATM PVC, ATM APS, | |
| DHCP | DHCP server | Single and double VLANs, CCOD, link groups, ATM PVC, ATM APS | ACL<br>QoS<br>HTTP-Red<br>LI<br>VoIP<br>Multicast applications<br>NAT<br>Flow services |
| | DHCP relay | Single and double VLANs, CCOD, link groups, ATM PVC, ATM APS | |
| | DHCP proxy | Single and double VLANs, CCOD, link groups, ATM PVC, ATM APS | |

*Table 3 Features Configured for BNG Solutions*

| Business Application | Access Technology | Transport Options | Services |
|---|---|---|---|
| Static | Bridge 1483 | ATM PVC, ATM APS | ACL |
| | Route 1483 | ATM PVC, ATM APS | QoS |
| | IPoE | Single and double VLANs | HTTP-Red |
| | | | LI |
| | | | VoIP |
| | | | Multicast applications |
| | | | NAT |
| | | | Flow services |

## 3.4 Other Ericsson Solutions

The router can also be used in other Ericsson solutions, such as Border Gateway Function (BGF), Converged Packet Gateway (CPG), IP Radio-Access Network (RAN), Mobile Backhaul (MBH) or Mobile Packet Backbone Network (MPBN).

For example, Figure 5 illustrates the router in a topology using IP RAN, MBH, MPBN solutions.

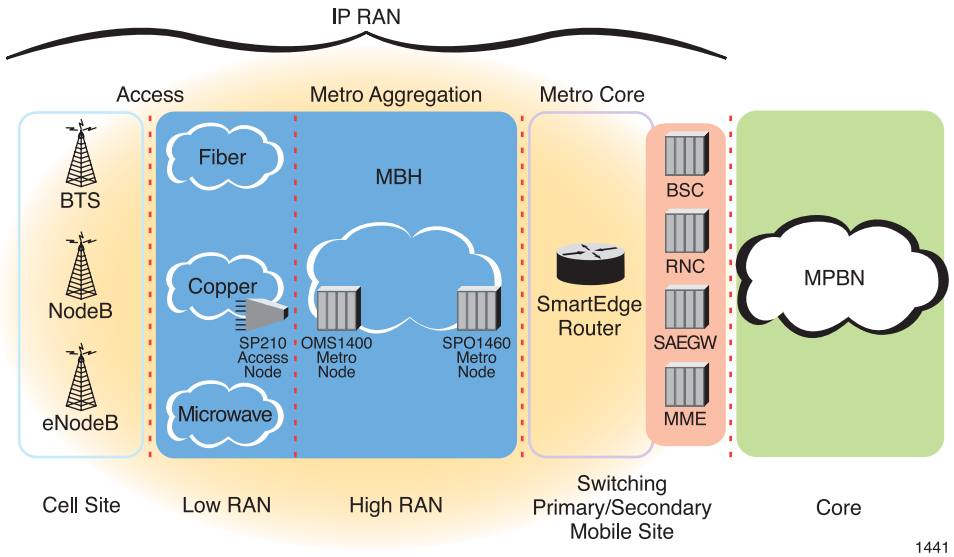


*Figure 5 Router in IP RAN, MBH, and MPBN Solutions*

Table 4 lists the features that can be configured for use with mobile solutions.

*Table 4 Features Configured for Use With Mobile Solutions*

| Business Application | Access or Transport Technologies | Routing Options | Service Options / Features |
|---|---|---|---|
| SmartEdge and MPBN | Ethernet 802.1Q LAG<br>POS LAG<br>ML PPP LAG<br>Gigabit Ethernet ports<br>10 Gigabit Ethernet ports | MPLS and LDP or RSVP<br>IS-IS, OSPF, or static routing<br>BGP<br>CSPF | L2VPN<br>L3VPN<br>Inter-AS VPNs<br>6VPE<br>IPSEC VPN<br>VPLS<br>BGF<br>Bridging<br>QoS marking and queuing<br>BGP NH trigger<br>Fast-convergence<br>P2P interfaces<br>RSTP/BVI<br>BFD<br>VRRP |
| SmartEdge and IP RAN (also with CPG) | Ethernet dot1q LAG<br>ML PPP LAG<br>Gigabit Ethernet ports<br>10 Gigabit Ethernet ports | MPLS and LDP or RSTP<br>IS-IS, OSPF or Static routing | VRRP<br>BVI<br>ICR<br>IPSEC<br>Bridging<br>CES<br>SAToP<br>QoS marking and queuing<br>BFD |
| SmartEdge and MBH | Ethernet dot1q LAG<br>POS LAG<br>ML PPP LAG<br>Gigabit Ethernet ports<br>10 Gigabit Ethernet ports | MPLS and LDP or RSVP<br>OSPF or IS-IS<br>BGP<br>MPLS fast-reroute | L2VPN<br>L3VPN<br>VPLS<br>XC VLL<br>QoS marking and queuing<br>CES<br>SAToP<br>Ethernet OAM<br>BFD<br>VRRP |

For information about using the router with the BGF solution see *SmartEdge Border Gateway Function*; and for using it with the CPG solution, see http://cpistore.internal.ericsson.com/alexserv?ac=LINKEXT&li=EN/LZN7040099R1E&FN=5_22102-AXB25020Uen.B.html

# 4 Features

## 4.1 Routing

The router supports standard network routing that moves information across an internetwork from a source to a destination, typically passing through one or more intermediate nodes along the way.

The SmartEdge OS routing table stores routes to directly attached devices, static IP routes, and routes learned dynamically from Routing Information Protocol (RIP), Constrained Shortest Path First (CSPF), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Intermediate System-to-Intermediate System (IS-IS).

When a network event causes routes to go down or become unavailable, routers distribute routing update messages that are propagated across networks, causing a recalculation of optimal routes. Routing algorithms that converge slowly can cause routing loops or network outages. Many algorithms can quickly select next-best paths and adapt to changes in network topology.

### 4.1.1 Routing Protocol Support

Methods for implementing IP routing, and the supported routing protocols on the router, are described in the following sections.

#### 4.1.1.1 Static Versus Dynamic Routing

The SmartEdge implementation of static routing involves packet forwarding on the basis of static routes configured by the system administrator. Static routes work well in environments where network traffic is predictable and network topology is relatively simple.

It also supports dynamic routing algorithms, which adjust to changing network circumstances by analyzing incoming routing update messages. RIP, OSPF, BGP, and IS-IS all use dynamic routing algorithms. A dynamic routing algorithm can also be supplemented with static routes where appropriate.

Some routing algorithms operate in a flat, hierarchy-free space, and others use routing hierarchies. In a flat routing system such as RIP, all routers are peers of all other routers. As networks increase in size, flat routing systems encounter scaling limitations. To address this, some routing protocols allow the administrator to partition the network into hierarchical levels, which facilitates the summary of topology information for anyone located outside the immediate level or area. For example, the OSPF protocol supports a two-level hierarchy in which area 0 is the backbone area that interconnects all other areas.

#### 4.1.1.2 IGPs Versus EGPs

SmartEdge routers support Interior Gateway Protocols (IGPs) to optimize network performance. RIP, OSPF, and IS-IS optimize the route between points within a network.

Exterior Gateway Protocols (EGPs) support route information exchange between different networks. SmartEdge OS supports BGP-4. The choice of an optimal path is made based on the cost of the path measured by metrics associated with each link in the network.

IGPs and EGPs have slightly differing administrative designs. An IGP typically runs in an area under a single administrative control; this area is referred to as an autonomous system (AS) or a routing domain. In contrast, an EGP allows two different autonomous systems to exchange routing information and send data across the AS border. Policy decisions in EGPs can be shaped to determine which routing information crosses the border between the two autonomous systems.

The SmartEdge routers support the following routing protocols:

- **Basic IP Routing**

  Basic IP routing on the router includes static IP routing and other basic routing features not covered by any routing protocol, including router IDs, static routes for multicast reverse path forwarding (RPF) lookup, IP Martian addresses, unicast RPF checks, maximum IP routes, and intercontext static routing among nonlocal contexts. For more information, see *Configuring Basic IP Routing*.

- **Virtual Router Redundancy Protocol (VRRP)**

  VRRP eliminates the single point of failure that is common in the default static routed environment and provides a higher availability default path without requiring dynamic routing or router discovery protocols on every end host.

  VRRP works by dynamically assigning responsibility for a virtual router to one of the VRRP routers on a LAN. A virtual router is defined by its virtual router ID (VRID) and a set of IP addresses. There are two types of VRRP routers—owner and backup. The VRRP router controlling the IP addresses associated with a virtual router is called the owner, and it forwards packets sent to the IP addresses. For more information, *Configuring VRRP*.

- **Routing Information Protocol (RIP)**

  RIP is a distance-vector protocol that uses hop count as its metric that can be used in small homogeneous networks. The router supports RIP Version 2 and provides for multiple RIP instances. Each instance maintains its own routing table and set of interfaces. Each interface can be assigned to at most one RIP instance. For more information, see *Configuring RIP*.

- **Open Shortest Path First (OSPF)**

  OSPF is an IGP that uses link-state advertisements (LSAs) to inform other routers of the state of the sender's links. In a link-state routing protocol, each router distributes information about its interfaces and neighbor relationships. The collection of the link states forms a database that describes the autonomous system (AS) topology. As OSPF routers accumulate link-state information, they use the Shortest Path First (SPF) algorithm to calculate the shortest path to each node, which forms the basis for developing routing information for that AS. For more information, see *Configuring OSPF*.

- **Bidirectional Forwarding Detection (BFD)**

  BFD is a simple Hello protocol that is similar to the detection components of some routing protocols. A pair of routers periodically transmits BFD packets over each path between the two routers, and if a system stops receiving BFD packets after a predefined time interval, some component in that particular bidirectional path to the neighboring router is assumed to have failed.

  A path is only declared operational when two-way communication has been established between systems.

  BFD provides low overhead, short-duration detection of failures in the path between adjacent forwarding engines, including the interfaces, data links, and to the extent possible, the forwarding engines themselves.

  The legacy Hello mechanism run by routing protocols takes more than one second to detect a failure.For some applications, more than one second caises a great deal of lost data at gigabit rates. BFD provides the ability to detect communication failures in less than one second. For more information, see *Configuring BFD*.

- **Border Gateway Protocol BGP)**

  BGP, an EGP based on distance-vector algorithms, uses the Transmission Control Protocol (TCP) as its transport protocol; it operates between exactly two BGP nodes, or BGP speakers. After a TCP connection is established, the two BGP speakers exchange dynamic routing information over the connection. The exchange of messages is a BGP session between BGP peers. For more information, see *Configuring BGP*.

- **Intermediate System-to-Intermediate System Routing (IS-IS)**

  IS-IS is an IGP that makes routing decisions based on link-state information.

  IS-IS is defined in ISO 10589, *Intermediate System to Intermediate System Intra-Domain Routing Exchange Protocol for Use in Conjunction with the Protocol for Providing the Connectionlessmode Network Service (ISO 8473), ISO DP 10589, February 1990*, and RFC 1195, *Use of OSI IS-IS*

*for Routing in TCP/IP and Dual Environments*. For more information, see *Configuring IS-IS*.

- **IP Multicast**

  IP multicast communication enables a source host to send IP packets to any number of hosts, anywhere within an IP network; it is one-to-any communication. That is, multicast communication is not limited to sending packets to a single destination host, or sending packets to every host on the network. Instead, multicast enables a source host to send IP packets to as many destination hosts as necessary, but no more than that. Configuration of multicast protocols is described in *Configuring IP Multicast* .

  The main challenge for multicast communication is developing a method for determining which hosts will receive multicast traffic and which will not. The SmartEdge OS supports the following multicast protocols:

  – Internet Group Management Protocol (IGMP)

  – Protocol Independent Multicast Sparse Mode (PIM-SM)

  – Multicast Source Discovery Protocol (MSDP)

- **Routing Policies**

  SmartEdge routing policies allow network administrators to enforce various routing policy decisions onto incoming, outgoing, and redistributed routes. The tools used to configure routing policies include BGP AS path lists, BGP community lists, IP prefix lists, and route maps with match and set conditions. For more information, see *Configuring Routing Policies*.

### 4.1.2 MPLS Networking

The SmartEdge OS supports MPLS to efficiently forward packets through a network. MPLS operates across an interface in an MPLS-enabled context.

In a conventional IP network, routers forward packets through the network, from one router to the next, with each router making an independent forwarding decision by analyzing the packet header; packet processing often causes considerable forwarding delay. With MPLS, the complete analysis of the packet header is performed only once, when it enters an MPLS-enabled network. For more information, see *Configuring MPLS*.

#### 4.1.2.1 Label Distribution

To communicate labels and their meanings among label switched routers (LSRs), MPLS uses the Resource Reservation Protocol (RSVP) or the label distribution protocol (LDP).

- **Resource Reservation Protocol (RSVP)**

Enables dynamic label allocation and distribution in an MPLS network. You can specify the ingress LSR and the egress LSR, but the next hops through the network are determined according to labels derived from existing routing protocols. The router supports the ability to configure route redundancy using RSVP; in this topology, a standby RSVP LSP serves as a backup to a primary LSP, or to another standby LSP in a backup-to-backup LSP configuration. For more information, see *Configuring MPLS*.

- **Label Distribution Protocol (LDP)**

  Enables dynamic label allocation and distribution in an MPLS network. An LSR enabled with LDP can establish LSPs to other LSRs in the network. LDP creates label bindings by assigning labels to connected routers and by advertising the bindings to neighbors. LDP also assigns labels to label bindings learned from neighbors, and readvertises the binding to other neighbors. When an LSR advertises a label binding for a route, the LSR is advertising the availability of an LSP to the destination of that route. LDP can learn several LSPs from different neighbors for the same route. LDP must be configured with an IGP, such as IS-IS or OSPF; LDP assigns a label only to routes selected by the underlying IGP. For more information, see *Configuring LDP*.

### 4.1.3 MPLS-Based Solutions

The router supports solutions using MPLS networks in which customer connectivity among multiple remote sites is deployed across a shared central infrastructure, and still provides the same access or security as a private network. For example, it supports L2VPNs, L3VPNs, port pseudowire (PW) connections, and Virtual Private LAN Services (VPLS) in MPLS network topologies.

- **Layer 2 Virtual Private Networks (L2VPNs)**

  L2VPNs, in which customer edge (CE) routers send Layer 2 traffic to provider edge (PE) routers over Layer 2 circuits, are configured between the PE and the CE routers. The router serves as a PE router and supports the following Layer 2 circuits:

  - Ethernet port
  - 802.1Q virtual LAN (VLAN)
  - Frame Relay permanent virtual circuit (PVC)
  - Asynchronous Transfer Mode (ATM) PVC

  You can configure the L2VPN on PE routers and use it to cross-connect a local Layer 2 circuit with a corresponding remote Layer 2 circuit through an LSP tunnel that crosses the network backbone. For more information, see *Configuring L2VPNs*.

- **L3VPNs**

Border Gateway Protocol/Multiprotocol Label Switching Virtual Private Networks (BGP/MPLS VPNs) are a collection of policies that control connectivity among a set of sites. A customer site is connected to the service provider network, often called a backbone, by one or more ports, where the service provider associates each port with a VPN context.

A BGP/MPLS VPN allows you to implement a wide range of policies; for example, within a VPN, you can allow every site to have a direct route to every other site (full mesh), or you can restrict certain pairs of sites from having direct routes to each other (partial mesh). For more information, see *Configuring BGP/MPLS VPN*.

- **Port Pseudowire (PW) Connections**

  MPLS PWs provide point-to-point (P2P) connections between pairs of provider edge (PE) routers, enabling you to connect Layer 2 networks to Layer 3 networks for routing and forwarding. Like physical Ethernet ports in the router, port PWs (supporting untagged Ethernet circuits) can be bound to IP interfaces in the local context or a VPN context (one port PW bound to one interface). This enables you to combine two Layer 2 routers into one. You can view and configure SmartEdge OS port PWs in much the same way as physical ports.

  In a typical deployment, port PW connections are used to transport fixed IP traffic from the ingress Layer 2 PE device to the egress Layer 3 PE router. In this deployment, traffic from customer premises equipment (CPE) devices in the broadband access or other network topologies behind the Layer 2 PE node is forwarded by the Layer 2 PE device (which can be a SmartEdge router) through the port PW to the router (where the port PW is configured), where it is routed and forwarded into the Layer 3 IP/MPLS network and the Internet. For more information, see *Configuring Port Pseudowire Connections*.

- **VPLS**

  VPLS enables networks at separate geographical locations to communicate with each other across a wide area network (WAN) as if they were directly attached to each other in a LAN. With VPLS PWs, the WAN becomes transparent.

  A VPLS pseudowire (PW) emulates the attributes and function of Ethernet connectivity over a WAN. Pseudowires are carried over MPLS tunnels on the network, and the MPLS signaling protocols are used to automatically provision the service on the pseudowire end-to-end, so you can provision a pseudowire by pointing to its two endpoints. In forwarding packets, MPLS automatically negotiates the path. For more information, see *Configuring VPLS*.

## 4.2 BNG Features

In the SmartEdge OS, subscribers are the end users of broadband network gateway (BNG) services, which include DHCP, CLIPS, L2TP, PPP, and PPPo*X* models.

Subscriber records are configured as part of a context, either locally on the router or on a RADIUS server. Subscriber records contain the information necessary to bind a subscriber to the correct interface, and to the correct network context and services. Subscriber records can also contain other configuration information, such as authentication, access control, rate-limiting, and policing information. For more information, see *Configuring Subscribers* and the documents in the Subscriber Management folder: *Configuring Authentication, Authorization, and Accounting*, *Configuring Bindings*, *Configuring IPV6 Subscriber ServicesConfiguring CLIPS*, *Configuring PPP and PPPoE*, *Configuring L2TP*, *Configuring RADIUS*, and *RADIUS Attributes*.

The number of active subscribers depends on licensing, configuration, memory, processing power, and desired per-subscriber bandwidth. Each software and hardware variant has a maximum active subscriber figure, which may or may not be achieved in different deployment scenarios.

The SmartEdge OS system supports the following subscriber management services:

- Dynamic service selection dynamically binding subscriber sessions to services
- Access functions that traditional routers were not designed to provide, such as subscriber management, provisioning, authentication, and accounting
- Routing of subscriber traffic based on Layer 3 addressing
- Translations necessary to convert subscriber traffic to IP, relieving the service provider backbone routers of frame translations that can cause congestion on high-volume routers
- Grooming of individual subscriber data streams into simplified IP flows for routers connecting to the Internet backbone

## 4.3 IP Protocol Support

The SmartEdge OS supports the following IP service protocols.

- **Address Resolution Protocol (ARP)**

  The SmartEdge OS implementation of the ARP is consistent with RFC 826, *An Ethernet Address Resolution Protoco*l, also called *Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*. In addition, the SmartEdge OS provides a configurable

ARP entry-age timer and the option to automatically delete expired dynamic ARP entries.

For more information about ARP on the router, see *Configuring ARP*.

- **Neighbor Discovery Protocol (ND)**

  SmartEdge routers use the ND protocol for IP Version 6 (IPv6) to determine the link-layer addresses for neighbors known to reside on attached links and to quickly purge cached values that become invalid. The IPv6 ND protocol corresponds to a combination of the IPv4 ARP and Internet Control Message Protocol (ICMP) Router Discovery. The ND protocol is described in RFC 2461, *Neighbor Discovery for IP Version 6 (IPv6)*. IPv4 and IPv6 ND can co-exist.

  The changes from IPv4 to IPv6 include:

  – Increase in address size from 32 bits to 128 bits

  – Simplified header

  – Extensible header with optional extension headers

  – Multicast addresses instead of broadcast addresses

  For more information about ND on the router, see *Configuring ND*.

- **Network Time Protocol (NTP)**

  The SmartEdge OS supports versions 1, 2, and 3 of the Network Time Protocol (NTP). On the router, NTP operates in client mode only; the router can be synchronized by a remote NTP server, but the remote server cannot be synchronized by the router.

  **Note:** Before using NTP, the router must first be configured with the IP address of one or multiple NTP servers.

  For more information about NTP on the router, see *Configuring NTP*.

- **Dynamic Host Configuration Protocol (DHCP)**

  The router provides four types of DHCP support:

  – External DHCP relay server

  – External DHCP proxy server

  – Internal DHCP server

  – Internal DHCPv6 PD server

  For more information about DHCP and DHCPv6 on the router, see *Configuring DHCP*.

- **Access Node Control Protocol (ANCP)**

  ANCP is a communications control protocol that allows the router to communicate with an access node and gather information about the parameters for the individual access lines on the access node.

  The ANCP is an out-of-band control protocol that does not interfere with the subscriber sessions that are carried on the access lines. Beneath the ANCP, the router uses the General Switch Management Protocol (GSMP) version 3 (GSMPv3) to communicate with the ANCP neighbor peers; GSMPv3 messages are encapsulated using the Transmission Control Protocol (TCP).

  For more information about ANCP on the router, see *Configuring ANCP*.

## 4.4 IP Services

The SmartEdge OS provides the IP services:

- **Domain Name System( DNS)**

  DNS enables subscribers to access devices using hostnames instead of IP addresses. When a command refers to a hostname, the SmartEdge OS consults the local host table for mappings. If the information is not in the table, the router generates a DNS query to resolve the hostname. DNS is enabled on a per-context basis, with one domain name allowed per context.

  For more information about DNS on the router, see *Configuring DNS*.

- **HTTP Redirect**

  HTTP redirect enables service providers to interrupt subscriber HTTP sessions and redirect them to a preconfigured URL. Applications can require customer registration, direct customers to web sites to download virus protection software, and advertise new services or software updates. An HTTP redirect profile containing a redirect URL is attached to subscriber records, and a forward policy redirects HTTP traffic to the lightweight HTTP server on the controller card attached to the subscriber circuit. The forward policy that performs the redirection is removed through a subscriber reauthorization mechanism.

  For more information about HTTP redirect policies, see *Configuring HTTP Redirect*.

- **Access Control Lists (ACLs)**

  The SmartEdge OS supports IP filtering access control lists (ACLs) and policy ACLs (for both IPv4 and IPv6 traffic), which work in collaboration with QoS to manage traffic flow.

  – IP filtering ACLs

IP ACLs are lists of packet filters. Based on the criteria specified in the IP ACLs associated with the packet, the SmartEdge OS decides whether the packet should be forwarded or dropped. IP ACLs filter packets by using **`deny`** and **`permit`** statements. IP ACLs can be applied to interfaces and contexts and affect packets on all circuits bound to the interface or all administrative packets on a context.

– Policy ACLs

  Policy ACLs are lists of packet filters, packet classifications, or both. Based on criteria specified in the policy ACLs associated with the packet, the SmartEdge OS decides whether the packet should be forwarded, dropped, or assigned a class name. Policy ACLs filter packets, classify packets, or both by using **`permit`** statements. Policy ACLs can be applied to forward, NAT, and QoS metering and policing policies.

For more information about ACLs, see *Configuring ACLs*.

### 4.4.1 Mobile IP (Wireless) and Hotlining

Mobile IP services enable the router to act as one or more foreign agents (FAs). Each communicates with its associated home-agent (HA) peers that support mobile subscribers, which are referred to as mobile nodes (MNs). Each FA has a care-of address (CoA) that the system uses as the termination address for the tunnel to an HA peer.

The MNs connect to the FA through one or more base transceiver stations (BTSs) using Ethernet circuits. MNs can move to different BTSs, depending on their locations.

MNs communicate with the router (the FA) over Ethernet-based circuits, using a context that you configure for the FA. The system routes the MN traffic to each external HA peer using a Generic Routing Encapsulation (GRE) tunnel circuit or an IP-in-IP tunnel. Each HA peer uses a different tunnel. Traffic from an HA peer is routed back to the MNs associated with that HA peer using the same tunnel circuit.

Hotlining enables the SmartEdge OS to redirect subscribers to a portal controlled by a service provider. This portal can be used for service registration, updates, and service advertisements, and to address issues that require immediate attention, such as virus attacks and missed payments. When hotlining is complete, the subscriber is released from the hotlined state (released from the portal) and directed to the original destination.

For more information about Mobile IP services, see *Configuring Mobile IP for a Foreign Agent*, *Configuring Mobile IP for a Home Agent*, *Configuring Hotlining for a Foreign Agent*, and *Configuring Hotlining for a Home Agent*.

## 4.5 IP Service Policies

The SmartEdge OS provides the following IP service policies:

- **Forward Policies**

  Forward policies support IP traffic mirroring, redirect, and drop. IP traffic mirroring copies packets traveling across a circuit and forwards the duplicated packets to a designated outgoing port. IP traffic redirect forwards IP packets to IP addresses that are different than their original destination. IP traffic drop determines which particular packets should be dropped, rather than forwarded.

  For more information about SmartEdge forward policies, see *Configuring Forward Policies*.

- **Network Address Translation (NAT) Policies**

  Through NAT policies, hosts using unregistered IP addresses on private networks can connect to hosts on the Internet and vice versa. NAT translates the private (not globally unique) addresses in the internal network into legal addresses before packets are forwarded onto another network. ISPs can place NAT devices between end users and the public Internet to suppress global IPv4 address consumption.

  Traditional NAT (CPE NAT) – exists at the edge of the customer network, where it connects to a service provider and translates between private IPv4 addresses within the customer network and a public address assigned by the provider.

  Carrier Grade NAT (CGN) exists within the service provider network.

  Both types of NAT translate between private and public IPv4 addresses.

  For more information about NAT on the router, see *Configuring NAT Policies*.

- **Service Policies**

  Service policies determine the context or contexts that Point-to-Point Protocol (PPP) and PPP over Ethernet (PPPoE) subscribers can access by verifying the domain or context name associated with subscriber records.

  A service policy can be attached to any PPP- or PPPoE-encapsulated subscriber circuit, including PPP-encapsulated Layer 2 Tunneling Protocol (L2TP) tunnels.

  For more information about service policies, see *Configuring Service Policies*.

## 4.6 Quality of Service

The Internet provides only best-effort service, offering no guarantees packet delivery. The SmartEdge router offers QoS differentiation based on traffic type and application.

### 4.6.1 Configuring QoS on Circuits

You can attach both metering (ingress) and policing (egress) policies to the following:

- Ports or channels
- ATM PVCs
- 802.1Q PVCs
- Subscriber sessions
- Link groups

For details on configuring ports, channels, circuits, subscribers, and link groups for QoS, see *Configuring Circuits for QoS*.

### 4.6.2 Rate-Limiting and Class-Limiting

The SmartEdge OS classifies, marks, and rate-limits incoming packets:

- Priority groups

  A priority group number assignment enables you to classify all traffic, including non-IP traffic, on an ingress circuit. A priority group is an internal value used by the router to determine into which egress queue the inbound packet should be placed. The type of service (ToS) value, Differentiated Services Code Point (DSCP) value, and Multiprotocol Label Switching (MPLS) experimental (EXP) bits are not changed by this command. The actual queue depends upon the number of queues configured on the circuit.

  For more information about traffic engineering using rate-limiting and class-limiting, see *Configuring Rate-Limiting and Class-Limiting*.

- Policy ACLs

  A classification filter is configured through a policy ACL. Each policy ACL supports up to eight unique classes. Packets can be classified according to IP precedence value, protocol number, IP source and destination address, ICMP attributes, Internet Group Management Protocol (IGMP) attributes, Transmission Control Protocol (TCP) attributes, and User Datagram Protocol (UDP) attributes.

A policy ACL can be applied to incoming or outgoing packets on a port, circuit, or for a subscriber profile. A policy ACL is applied to incoming packets through a QoS policing policy and to outgoing packets through a QoS metering policy.

- QoS Policing and Metering Policies

  A QoS policing policy marks, rate-limits, or performs both actions on incoming packets; a QoS metering policy does the same for outgoing packets. Both types of policies can be applied at one of two levels or at both levels simultaneously. One level of application applies to all packets on a particular circuit. Another level of application applies to only a particular class of packets traveling across the circuit. The class is configured through a policy ACL.

### 4.6.3 Queueing and Scheduling

After classification, marking, and rate-limiting occurs on an incoming packet, the packet enters an output queue for servicing by an egress traffic card's scheduler.

The SmartEdge OS supports up to eight queues per circuit. Queues are serviced according to a queue map scheme, a QoS scheduling policy, or both.

For more information about traffic engineering using queueing and scheduling, see *Configuring Queuing and Scheduling*.

### 4.6.4 Flow Admission Control

A flow is a unidirectional object that identifies related data packets and enables you to apply a set of services to a portion of a circuit. Without flows, you could only apply services to an entire group of subscriber traffic mapped to a separate circuit. All attributes on a flow inherit from the services applied to the circuit to which the flow applies.

All attributes applied using flow features reside in a flow admission control (FAC) profile, which is the basic unit of flow configuration. You create a FAC profile and then apply it to an existing circuit in circuit configuration mode.

For more information about flow admission control, see *Configuring Flow Admission Control*.

## 4.7 Application Traffic Management

When implemented with an ASE card and properly configured, the router can apply control policies to types of application traffic. When the router detects application traffic, it applies a DPI traffic management policy that classifies and maps it to one or more classes. Depending on the traffic control levels that you configure, each class is associated with a set of actions that applies to all

traffic mapping for that class. You can apply classes to traffic associated with individual subscribers, groups of subscribers, or all the subscribers managed by a router. For more information, see *Application Traffic Management Configuration and Operation*.

# 5 System Architecture

Figure 6 illustrates the SmartEdge OS architecture.

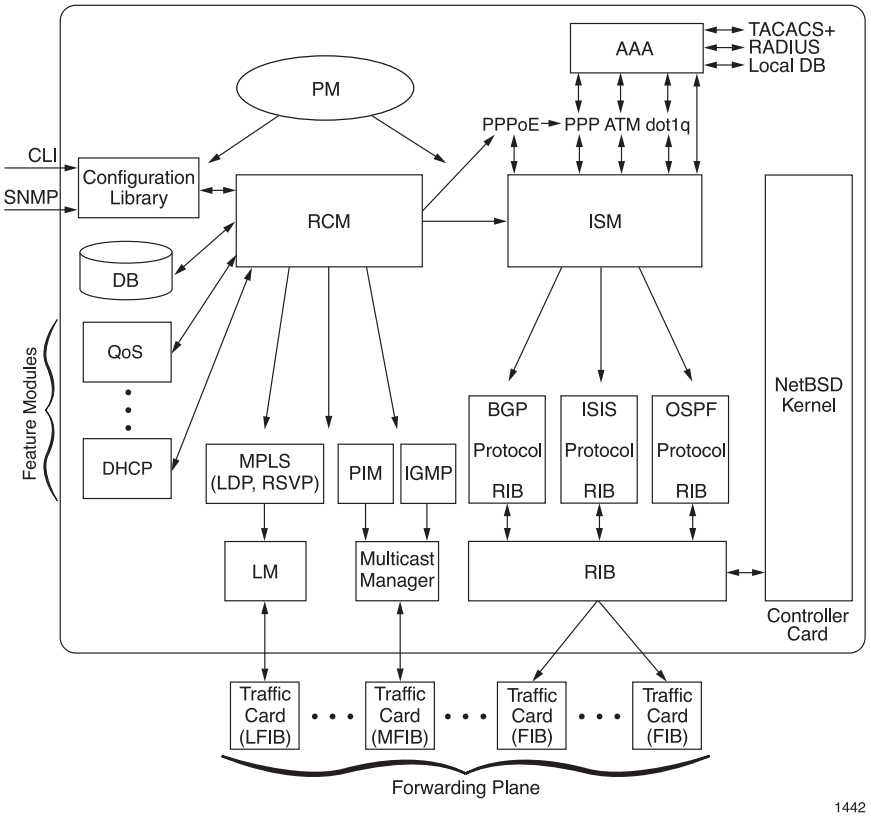


*Figure 6 SmartEdge OS Architecture*

# 6 Router Components

The SmartEdge OS running on the XCRP controller cards performs route processing and other control functions. Packet forwarding is performed in collaboration with Packet Processing ASICs (PPAs) on the individual traffic cards.

## 6.1 SmartEdge OS

Figure 7 illustrates the SmartEdge OS software component relationships.

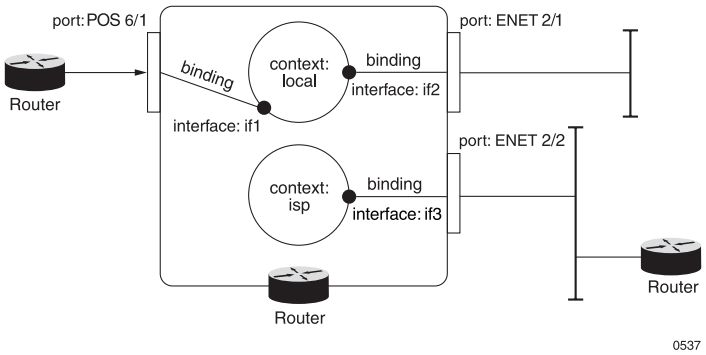


*Figure 7 SmartEdge OS Software Component Interrelationships*

## 6.2 Contexts

Most networking products are designed so that the entire set of ports, circuits, and protocols operate together as one global instance. The SmartEdge OS supports an advanced feature called multiple contexts. Each context is a virtual router instance running within a single physical device. A context operates as a separate routing and administrative domain, with separate routing protocol instances, addressing, authentication, accounting, and so on, and does not share this information with other contexts. By separating the address and name spaces in this way, you can use multiple contexts to provide direct access to customers, or to provide different classes of services for customers. You use a single physical device to implement this, with one or more contexts assigned to each service provider or service class. Implementing this with equipment from other vendors requires multiple devices.

The router is always configured with the special local context. This context is always present on the system and cannot be deleted. In a single-context configuration, the local context is the only context on the system.

## 6.3 Interfaces

The concept of an interface in the SmartEdge OS differs from that in traditional networking devices. In traditional devices, the term interface is often used synonymously with port, channel, or circuit, which are physical entities. In the SmartEdge OS, an interface is a logical construct that provides higher-layer protocol and service information, such as Layer 3 addressing. Interfaces are configured as part of a context and are independent of physical ports, channels, and circuits. The decoupling of the interface from the physical layer entities enables many of the advanced features offered by the SmartEdge OS.

For the higher-layer protocols to become active, an interface must be associated with a physical port, channel, or circuit. This association is referred

to as a binding in the SmartEdge OS. For more information, see Section 6.6 on page 26.

## 6.4 Ports, Channels, and Circuits

Ports, channels, and circuits in the SmartEdge OS represent the physical connectors and paths on the SmartEdge traffic and controller cards. Physical port, channel, and circuit configurations include both hardware and software parameters that allow the behavior of the port, channel, or circuit to be specified for a specific router.

Before any higher-layer user data can flow through a physical port, channel, or circuit, that port, channel, or circuit must be associated with an interface within a context. This association is referred to as a binding in the SmartEdge OS. The configuration for each port, channel, and circuit includes binding information. For more detailed information on ports, channels, and circuits, see *Configuring ATM, Ethernet, and POS Ports*, *Configuring Cards*, and *Configuring Circuits*.

## 6.5 Cross-Connections

The SmartEdge OS supports cross-connections that perform Layer 2 switching in the router; this is also referred to as a bypass. In cross-connection, the forwarding process switches an ATM or 802.1Q packet on an ingress circuit to an egress circuit, and performs actions on the Layer 2 header, which can include stripping or preserving the original header or adding new Layer 2 headers, according to the configuration of the PVC. For more information, see *Configuring Cross-Connections*.

## 6.6 Bindings

Bindings form the association in the SmartEdge OS between the ports, channels, or circuits and the higher-layer routing protocols configured for a context. No user data can flow on a port, channel, or circuit until some higher-layer service is configured and associated with it. After a port, channel, or circuit is bound to an interface, traffic flows through the context as it would through any IP router. For more information, see *Configuring Bindings*.

Bindings are either statically mapped during configuration or dynamically created based on subscriber characteristics defined in the local database, or on a RADIUS server as described in the following sections.

With static bindings, a port, channel, or circuit is bound directly to an interface. In this case, the port, channel, or circuit is hard-wired to the higher-layer protocols defined for the interface. Multiple ports, channels, or circuits can be bound to a single interface.

Dynamic binding occurs when a circuit is bound to the higher-layer protocols based on session information. For example, a PPP-encapsulated session can

be bound to a particular context and interface by examining the authenticated structured subscriber name in the form ***sub-name@ctx-name***.

## 6.7 Bridges

The SmartEdge OS supports transparent, self-learning bridges (as described in IEEE 802.1D) that support restricted (very secure) circuits. Bridging on the router is context-specific, and a context can support multiple bridges. Circuits that can be bridged include Ethernet ports with 802.1D or 802.1Q encapsulation, 802.1Q permanent virtual circuits (PVCs), and Asynchronous Transfer Mode (ATM) PVCs with RFC 1483 bridged encapsulation. IP- and Point-to-Point Protocol (PPP)-encapsulated circuits cannot be bridged; however, bridging of IP over Ethernet (IPoE)-encapsulated circuits and PPP over Ethernet (PPPoE)-encapsulated circuits is supported at the medium access control (MAC) layer. The router implements the Rapid Spanning Tree Protocol (RSTP) and MAC moves monitoring to provide path redundancy and prevent bridging loops. Additional information on RSTP is available in IEEE 802.1d and IEEE 802.1w (RSTP is not supported over ATM). In addition, the SmartEdge OS supports Virtual Private LAN Service (VPLS) to provide Ethernet bridging over MPLS pseudowires. For more information, see *Configuring Bridging*.

## 6.8 Tunnels

The SmartEdge OS supports the following tunnel types:

- **IP-in-IP Tunnels**

  IP-in-IP tunneling transports IP payload packets encapsulated inside an outer IP header. This tunneling mode allows the multicast backbone to set up tunnels between sites to exchange IP multicast traffic over the Internet.

  Mobile IP services also use IP-in-IP tunnels to transport packets from a mobile node (MN), when it is forwarded from the foreign agent (FA) to the home agent (HA), and optionally in the reverse direction. For more information, see *Configuring Single Circuit Tunnels*

- **GRE Tunnels and VPNs**

  Generic Routing Encapsulation (GRE) is a simple, stateless protocol that allows for tunneling of IP in IP. GRE allows you to connect remote sites using private IP addresses over a public network that uses publicly routable IP addresses.

  Using GRE tunneling, you can create VPNs to connect to remote sites. Multiple SmartEdge OS contexts and GRE tunnel circuits, one for each VPN, demultiplex traffic for each VPN into its own IP address space. Thus each context acts as a dedicated virtual router for a VPN, where the IP address space (for example, private addresses as described in RFC

1918, *Address Allocation for Private Internets*) and routing databases are maintained separately from other contexts.

For more information, see *Configuring GRE Tunnels*.

- **L2TP Tunnels**

  L2TP tunnels are User Datagram Protocol (UDP)/IP-encapsulated circuits that carry subscriber Point-to-Point Protocol (PPP) sessions to another router.

  For more information, see *Configuring L2TP*.

  The router is designated as an LNS or a LAC, depending on its tunnel function:

  – As an LNS, the router accepts IP packets from LACs in the network and terminates them.

  – As a LAC, the router terminates subscriber PPP sessions and tunnels these sessions to a number of LNSs.

  In each context configured on the system, the router can function as a LAC to one or more LNSs, as an LNS to one or more LACs, or as both a LAC and an LNS.

- **IPsec Tunnels**

  The IP Security (IPsec) Virtual Private Network (VPN) application provided by the security service on the ASE card enables support of IPsec on site-to-site tunnels between two security gateways. You can create IPsec tunnels between two SmartEdge routers or between one managed router and an unmanaged device (referred to as an extranet device), such as Customer Premises Equipment (CPE) or a remote special-purpose server.

# 7 System Processes

## 7.1 Independent System Processes

Implementation of the major software components as independent processes provides several benefits:

- Processes in the system can be independently stopped, restarted, and upgraded without reloading the entire system or individual traffic cards.

- The system continues to operate in the event of a failure or disruption to any single component.

The separation of the route processing and control functions (performed by the SmartEdge OS software running on the controller card) from the forwarding function (performed on the individual traffic cards) also provides several benefits:

- Dedicated route processing functions are not affected by heavy traffic; dedicated packet forwarding is not affected by routing instability in the network.
- The architecture enables line-rate forwarding on all traffic cards. New features can be added to the control software on the controller without affecting forwarding performance.
- The architecture provides nonstop forwarding during system upgrades or reloads; the traffic cards continue to forward packets.

## 7.2 SmartEdge OS Processes

The SmartEdge OS major system components run as separate processes; see Table 5 for some examples.

*Table 5 SmartEdge OS Processes*

| **Module** | **Descriptions** |
|---|---|
| Address Resolution Protocol (ARP) | Manages IPv4 IP-to-MAC address resolution for ARP as described by RFC 826. IP ARP and XC ARP are supported, storing ARP entries in a database residing on the control plane. XC ARP is used for interworking cross-connects to manage MAC information for the Layer 2 portions of bypass connection. |
| Chassis Management (CM) | Manages system, card, port configuration, card/port state event communication, alarm reporting, hardware diagnostics, and hardware state retrieval. |
| Interface and Circuit State Manager (ISM) | Monitors and disseminates the state of all interfaces, ports, and circuits in the system. |
| Line Cards | Includes the PPA ASICs, which contain the Forwarding Information Base (FIB) and perform forwarding functions. |

*Table 5 SmartEdge OS Processes*

| Module | Descriptions |
|---|---|
| ND | The ND process provides five main functions, chiefly for IPv6 address resolution:<br>• Address resolution<br>• Stateless Address Auto-Configuration (SLAAC)<br>• Duplicate Address Detection (DAD)<br>• Neighbor Unreachability Detection (NUD)<br>• Multibind IPv6 and dual-stack subscriber support<br>ND is supported on multiple link types, including Ethernet, trunk LAG, access LAG, L2TP LNS tunnels, and ATM. |
| Process Manager (PM) | Monitors and controls the operation of the other processes in the system. |
| Quality of Service (QoS) | Provides different priorities to different applications, users, or data flows, and enforces forwarding throughput limits in individual data flows and aggregations of flows. Implements resource reservation control (RSVP) mechanisms and configures forwarding that implements QoS. |
| Router Configuration Module (RCM) | Controls all system configurations using a transaction-oriented database. |
| Simple Network Management Protocol (SNMP) | Performs monitoring and management of network devices using the Simple Network Management Protocol (SNMP). Communicates trap and inform notifications and manages SNMP requests according to the Management Information Bases (MIBs). |

Many more feature processes run as independent processes. For examples, see the following sections.

## 7.3 Layer 2 Processes

### 7.3.1 Asynchronous Transfer Mode (ATM) Process

The Asynchronous Transfer Mode (ATM) process manages ATM circuits. These include explicitly configured PVCs (and ranges of PVCs), as well as PVCs created on demand. Unlike Ethernet circuits, ATM circuits do not only handle PPA management, but also segmentation and reassembly (SAR) management. The ATM process supports circuit creation on demand (CCOD) and the following encapsulations:

- Multiprotocol encapsulation

- RFC 1483 bridged encapsulation—Supports Ethernet over ATM
- PPPoA—Supports VC-multiplexed encapsulation and the following PPP encapsulations: auto-detect, Logical Link Control-Subnetwork Access Protocol (LLC-SNAP), Network Layer Protocol Identifier (NLPID), and Serial High-Level Data Link Control (HDLC)
- PPPoEoA—Uses RFC 1483 bridged encapsulation

### 7.3.2 Bridge Process

The Bridge process handles bridge-related configurations (used to configure the forwarding plane) such as defining circuits belonging to a bridge instance, communicating configured bridge-related routes to RIB, and setting bridge instance attributes such as:

- Enabling or disabling RSTP
- Enabling or disabling MAC learning
- Configuring the aging time for learned MAC-circuit associations

The bridge process also participates in RSTP PDU exchanges (termination/origination) with other RSTP-enabled bridges and switches in the network.

### 7.3.3 dot1q (802.1Q) Process

The dot1q (802.1Q) process manages circuits with 802.1Q single and double-tagged encapsulation. These include explicitly configured circuits and circuit ranges, as well as circuits created on demand. For double-tagged packets, there may be a circuit corresponding to both tags, or to just the outer tag (a tunnel).

### 7.3.4 Tunnel Manager Process

The tunnel process implements “soft” tunnels in the SmartEdge OS; adding only an encapsulation without a tunnel entry endpoint in the forwarding plane. Handles tunnels according to the next-hop types in the FIB, including:

- GRE tunnels
- IP-in-IP tunnels
- IPsec tunnels (used with the ASE card)

Unlike these tunnels, L2TP tunnel functionality is managed by the L2TP process.

### 7.3.5 Cross-Connect (XC) Process

Manages cross-connections, running on the active XCRP card. It communicates statically configured cross-connects to the forwarding plane in such a way that a packet received on an ATM or 802.1Q PVC on ingress is switched to a particular egress circuit. The Layer 2 cross-connect feature in the SmartEdge OS enables Layer 2 switching between the following types of permanent virtual circuits (PVCs):

- ATM PVC to ATM PVC
- ATM PVC to single-tagged 802.1Q PVC
- ATM PVC to double-tagged 802.1Q PVC
- Single-tagged 802.1Q PVC to single-tagged 802.1Q PVC
- Single tagged 802.1Q PVC to double-tagged 802.1Q PVC
- Double-tagged 802.1Q PVC to double-tagged 802.1Q PVC

## 7.4 BNG Processes

BNG functions are managed by modules, such as the following samples.

### 7.4.1 Authentication, Authorization, and Accounting (AAA) Process

AAA performs authentication, authorization, and accounting of subscribers, tunnels, and circuits and the following tasks:

- In collaboration with other processes, provisions, manages, and retains subscriber sessions
- Implements AAA configuration and command processing
- Handles RADIUS services

### 7.4.2 Dynamic Host Configuration Protocol (DHCP) Process

DHCP passes configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap protocol (BOOTP), adding the capability of automatic collection of reusable network addresses and additional configuration options.

The SmartEdge router provides three types of Dynamic Host Configuration Protocol (DHCP) support:

- External DHCP relay server

  In relay mode, the router acts as an intermediary between the DHCP server and the subscriber. The router forwards requests from the subscriber's

PC to the DHCP server and relays the server's responses back to the subscriber PC.

- External DHCP proxy server

  In proxy mode, the router provides responses directly to the subscriber requests. Each subscriber sees the router as the DHCP server and sends all DHCP negotiations, including IP address release and renewal, to the router, which then relays the information to the DHCP server.

  The proxy feature enables the router to track IP address lease times and other DHCP information more closely. With RADIUS authentication, an accounting record is sent from the router to RADIUS every time an IP address is assigned or released.

- Internal DHCP server

  The router provides the functions of the DHCP server; no communications are sent to an external DHCP server.

  **Note:** Before using an external DHCP server, the SmartEdge OS must first be configured with the IP address or hostname of one or multiple external DHCP servers. DHCP servers are configured on a per-context basis, with a limit of one server per context.

The internal DHCP server is also used for Clientless IP Service Selection (CLIPS), interacting with the CLIPS daemon to appropriately configure the forwarding plane.

### 7.4.3 Layer 2 Tunneling Protocol (L2TP) Process

L2TP process facilitates the tunneling of PPP packets across an intervening network.

### 7.4.4 Point-to-Point Protocol (PPP) Process

The PPP process manages PPP subscriber sessions, including packet forwarding and handling PPP-related configuration and show commands.

### 7.4.5 PPP over Ethernet (PPPoE) Process

PPPoE transmits PPP traffic over Ethernet connections and learns the Ethernet address of the remote peer, and establishes a unique session identifier for all packets.

# 7.5 Routing Processes

On the SmartEdge router, route information is collected from the different routing protocols in the routing information base (RIB) (on the XCRP controller card), which calculates the best routes and downloads them to the forwarding information base (FIB) on the line cards.

Figure 8 illustrates the routing information flow.

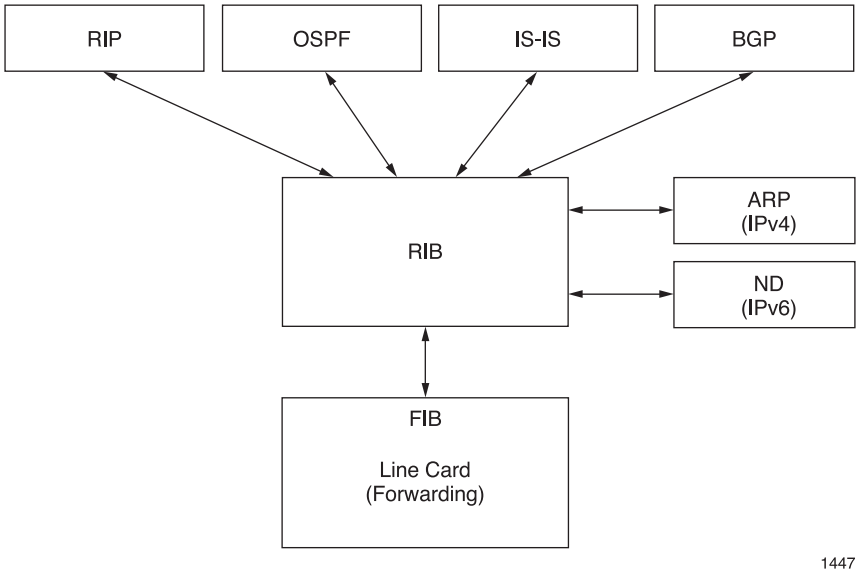


*Figure 8 Routing Information Flow*

## 7.5.1 Routing Information Protocol (RIP) Process

The RIP module implements RIP Version 2 as documented in RFC 1388. It also implements RIPv2 over a multibind interface, which is a SmartEdge OS proprietary feature.

## 7.5.2 Border Gateway Protocol (BGP) Process

The BGP process is responsible for installing both IPv4 and IPv6 routes in the RIB, installing Multicast Distribution Tree (MDT) routes into PIM, and downloading MPLS labels allocated by BGP to the Label Manager (LM).

## 7.5.3 Intermediate System-to-Intermediate System (IS-IS) Process

IS-IS performs the IS-IS routing protocol functions, including providing routes to the RIB and handling IS-IS configuration, show, and debug commands.

### 7.5.4 Open Shortest Path First (OSPF) Process

The OSPF process performs OSPF functions, including the following:

- Installing connected routes as well as best routes from LSPs in the RIB.
- Receiving redistributed routes from other routing instances (which may also be OSPF).
- Responding to events on interfaces where it is running.

### 7.5.5 Routing Information Base (RIB) Process

Running on the active XCRP, the RIB process is one of the most fundamental processes in the SmartEdge OS, RIB directly impacts how packets flow in and out of the box because it configures the routing tables in the forwarding plane and connectivity to the management interface. The RIB process is responsible for collecting routes from its clients, selecting the best path, and downloading the routes to each line card's forwarding information base (FIB). See Figure 8 for a diagram of RIB-related information flow.

The RIB process interacts with other SmartEdge OS modules, including the following:

- RCM
- Routing protocols or RIB clients such as the static routing, OSPF, OSPF3, ISIS, BGP, RIP, NAT, tunnel, L2TP, and bridge processes
- ISM
- ARP (IPv4)
- ND (IPv6)
- SNMP
- Forwarding

### 7.5.6 Multicast Processes

The Multicast manager process collects multicast groups and forwarding data from the PIM, IGMP, and MSDP processes, and forwards it to the line cards. It also logs multicast events.

Figure 9 illustrates the Multicast information flow.

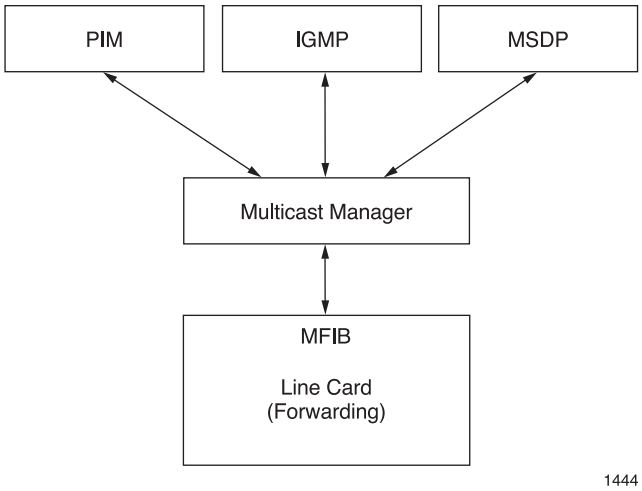


*Figure 9 Multicast Information Flow*

#### 7.5.6.1 Internet Group Management Protocol (IGMP) Process

The IGMP process manages IGMPv3 (as described in RFC 3376) and IGMPv2 (as described in RFC 2236). On SmartEdge OS interfaces, the process determines which IP multicast groups and, for IGMPv3, which sources have listeners on the network attached to the interface. Collected information is provided to Protocol Independent Multicast (PIM) to be advertised to other multicast routers.

#### 7.5.6.2 Multicast Source Discovery Protocol (MSDP) Process

The MSDP process manages MSDP as described in RFC 3618, advertising (S,G) entries (for groups that use a particular source address) from one PIM-SM domain to another. If the MSDP peer receiving the Source Advertisement (SA) is the Rendezvous Point (RP) for the (S,G) and there are receivers in the domain, it adds itself to the multicast distribution tree.

#### 7.5.6.3 Protocol Independent Multicast (PIM) Process

The PIM process maintains multicast information per group and per interface in the Multicast Forwarding Information Base (MFIB), which is downloaded to the Multicast Manager for installation on the line cards.

### 7.5.7 Multiprotocol Label Switching (MPLS) Processes

The MPLS process enables MPLS forwarding by downloading LSP configuration to the line cards.

Figure 10 illustrates the MPLS label information flow.

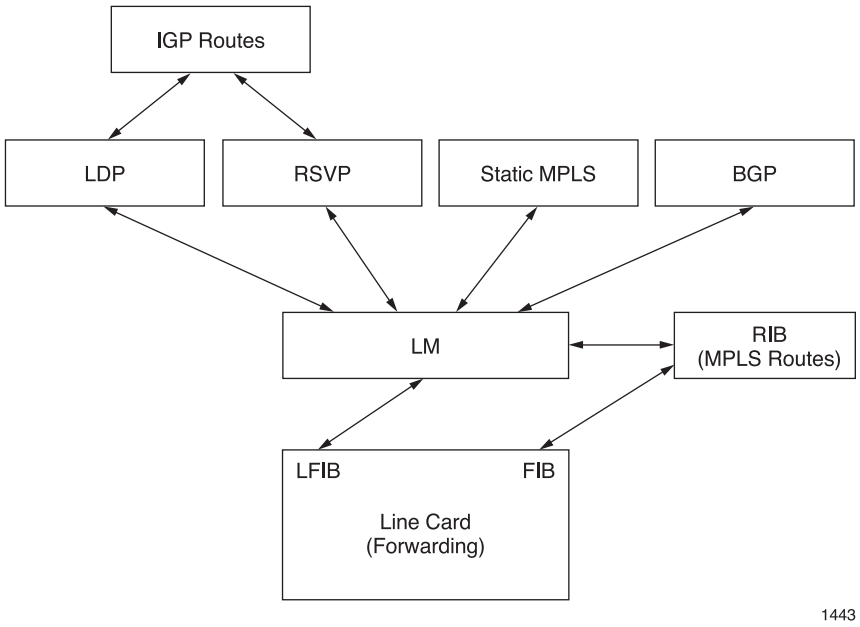


*Figure 10 MPLS Label Information Flow*

### 7.5.8 Label Manager (LM) Process

The LM process manages label requests and reservations from various MPLS protocols such as LDP and RSVP, and configures LSPs and PWs in the system. It installs LSPs and Layer 2 routes in the RIB and provisions MPLS-related data structures in the forwarding plane. It also handles MPLS-related configurations and functionality such as MPLS ping and traceroute. L2VPN functionality is handled in the LM process including configuration and PW setup. VPLS PWs and VLLs use a common framework for PW establishment.

### 7.5.9 LDP Process

The LDP process creates MPLS labels based on OSPF and IS-IS routes. It installs LSPs in LM and registers labels, routes, and prefixes in the RIB. The Update process sends LDP updates to neighbors.

### 7.5.10 RSVP Process

The RSVP process implements RSVP (as described in RFC 3031, RFC 3032, RFC 3209, and RFC 4090), providing LSPs to the LM process. It queries RIB for outgoing interfaces and next-hop information and registers BFD sessions in the RIB.

### 7.5.11 MPLS-Static Process

The MPLS-Static process manages static LSP configuration on the router (when serving as an ingress Label Edge Router (ingress-LER), a Label Switching Router (LSR), or egress LER) and communicates the details to the LM process.

## 7.6 Forwarding Process

SmartEdge OS forwarding is implemented on the set of installed line cards (each with a unique slot number), which perform both ingress and egress functions. The Forwarding process on each line card performs packet processing functions such as Forwarding Information Base (FIB) lookup for the longest prefix match with the destination IP address, and QoS classification for both fast data traffic and slower control traffic, such as ICMP, VRRP, or BFD messages.

## 7.7 System Redundancy and Synchronization

The router supports dual Cross-Connect Route Processor (XCRP) controller cards; one controller card acts as the active controller, and the other acts as its hot standby.

Both controller cards contain compact-flash cards that store the operating system image, its associated files, and the configuration database. A synchronization process ensures that the standby XCRP card is always ready to become the active XCRP card:

- When either the software release or the firmware on the active XCRP card is upgraded, the standby XCRP card automatically synchronizes its software or firmware version to that of the active controller.
- When a user modifies the contents of the compact-flash card (for example, by saving a configuration to a file, copying a file, or deleting a file), the change is propagated to the compact-flash card of the standby controller.
- The configuration databases of the active and standby XCRP cards are always synchronized.

To guard against system inconsistency, the synchronization process is protected during system load and XCRP card reload. At that time, while the synchronization is in progress, switchover from the active to the standby XCRP card is not allowed. If the active card should fail during synchronization, the standby XCRP card does not become active. If the user attempts to force a switchover during this synchronization period, the system warns the user that the standby is not ready. However, during the normal running state, an XCRP card switchover can occur at any time, and the standby XCRP card has the data required to take the active role.

The synchronization process is not affected by traffic card installation and removal. The active XCRP card continues to forward control traffic and detect and notify the administrator of any faults that occur while the standby XCRP card is being synchronized (the FAIL LED is blinking).

After the synchronization is complete, the standby controller is ready to become the active controller card if the active card fails.

Besides redundant XCRP controller cards, the router also supports many other redundancy features, including:

- Ethernet resiliency in L2VPN topologies using redundant Ethernet ports or XCs
- Slot redundancy for Layer 2 Tunneling Protocol (L2TP) sessions
- Inter-chassis redundancy for PPPoE, CLIPS, and DHCP subsessions (with PPA2-based line cards)
- Link redundancy with link groups
- APS protections for ATM cards
- MPLS route redundancy using RSVP
- VPLS redundant PWs
- Redundant RADIUS servers, including CoA servers
- Bridge redundancy in meshed network configurations and other network configurations running RSTP
- Redundant SSE cards
- Redundant timing systems
- Dual power connections

# 8 User Interface

The router provides three interfaces to access, manage, and configure the SmartEdge OS, as well as access node state information:

- The command line interface (CLI)
- Network Element Management System interface (NetOp EMS)

- Simple Network Management Protocol interface (SNMP)

For information about configuring the router using NetOp EMS, see the NetOp EMS Library.

For information about using SNMP to manage the router, see *Configuring RMON and SNMP*.

The primary user interface to the SmartEdge OS is the CLI, which can be accessed as follows:

- Ethernet management port connection to a local management workstation

  Requires a PC-type workstation running Windows 7, Vista, XP, NT, 2000, 98, 95, 3.01, or DOS with an Telnet or SSH client, and a shielded Ethernet crossover cable.

- Ethernet management port connection to a remote management workstation

  Requires a PC-type workstation running Windows 7, Vista, XP, NT, 2000, 98, 95, 3.01, or DOS with a Telnet or SSH client.

  Requires a shielded Ethernet straight cable (shipped with the system) or a router or bridge

- Craft 2 port connection to a local console terminal

  For a local terminal, choose one of the following:

  – ASCII/VT100 console terminal or equivalent that runs at 9600 baud, 8 data bits, no parity, 1 stop bit

  – PC-type workstation running Windows 7, Vista, XP, NT, 2000, 98, 95, 3.01, or DOS with a terminal emulator, in the same configuration as the ASCII/VT100 terminal.

    A terminal server and a craft console cable (shipped with the system)

- Craft 2 port connection to a remote console terminal

  For a local terminal, choose one of the following:

  – ASCII/VT100 console terminal or equivalent that runs at 9600 baud, 8 data bits, no parity, 1 stop bit

  – PC-type workstation running Windows 7, Vista, XP, NT, 2000, 98, 95, 3.01, or DOS with a terminal emulator, in the same configuration as the ASCII/VT100 terminal.

    A terminal server cable

We recommend that you have two access methods available, such as a remote workstation connected to the Ethernet management port and a remote console terminal with connection to a terminal server. Many administrative tasks should be carried out from the CLI when connected through a terminal server, because some processes, such as reloading or upgrading the software, may sever an Ethernet management port connection.

## 8.1 Command Modes and Prompts

In the SmartEdge CLI, the two primary modes are exec and global configuration. When a session is initiated, the CLI is set to the exec mode by default. The exec mode allows you to examine the state of the system and perform most monitoring, troubleshooting, and administration tasks using a subset of the available CLI commands.

Exec mode prompts can be one of the following forms, depending on the user privilege level (see Section 8.3 on page 45).

```
[local]hostname#

[local]hostname>
```

In this example, **local** is the context in which commands are applied and **hostname** is the currently configured hostname of the router. When you exit exec mode using the **exit** command, the entire CLI session ends.

Global configuration mode is the top-level configuration mode; all other configuration modes are accessed from this mode. These modes allow you to interactively configure the system through the CLI, or to create and modify a configuration file offline by entering configuration commands using any text editor. After you have saved the file, you can then load it to the operating system.

To access global configuration mode, enter the **configure** command (in exec mode).

Configuration mode prompts are of the following form:

```
[local]hostname(mode-name)#
```

In the example, **local** is the context in which commands are applied, **hostname** is the currently configured hostname of the router, and **mode-name** is a string indicating the name of the current configuration mode.

The prompt (in global configuration mode), assuming the factory default hostname of **Redback** and the **local** context, is as follows:

```
[local]Redback(config)#
```

Each feature supported through the SmartEdge OS can have one or more configuration modes, some of which you access using a command (in global configuration mode). Table 6 lists the configuration modes for the commands described in this document and the commands that you enter to access them.

## 8.2 Command Mode Hierarchy

Command modes exist in a hierarchy. You must access the higher-level command mode before you can access a lower-level command mode in the same chain. As an example, Figure 11 shows the hierarchy of the command modes used to configure some basic system features.

For the modes required for specific commands, see the command in *Command List*.

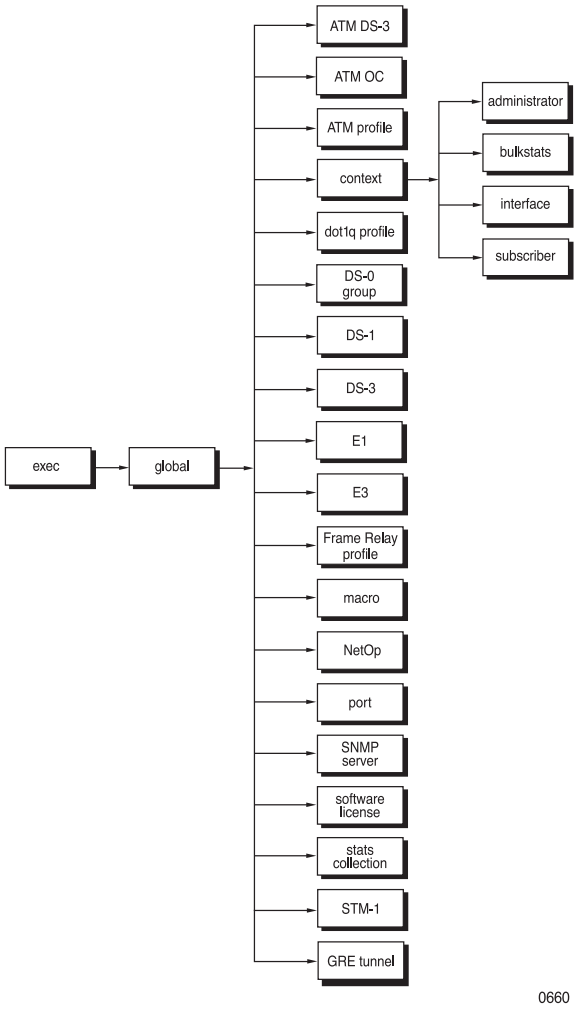


*Figure 11 Command Mode Hierarchy for Basic System Commands*

Table 6 lists a sample of the command modes (in alphabetical order) for the SmartEdge basic system features. This is not a comprehensive list and is provided only as a sample. For more information about the command modes, see *Command List*.

*Table 6 Basic System Features: Command Modes and System Prompts*

| Mode Name | Commands Used to Access | Command-Line Prompt |
|---|---|---|
| exec | (user logon) | # or > |
| administrator | **`administrator`** command from context configuration mode | (config-administrator)# |
| ATM OC | **`port atm`** command from global configuration mode | (config-atm-oc)# |
| ATM profile | **`atm profile`** command from global configuration mode | (config-atm-profile)# |

| Mode Name | Commands Used to Access | Command-Line Prompt |
|---|---|---|
| bulkstats | **bulkstats policy** command from context configuration mode | (config-bulkstats)# |
| context | **context** command from global configuration mode | (config-ctx)# |
| dot1q profile | **dot1q profile** command from global configuration mode | (config-dot1q-profile)# |
| Frame Relay profile | **frame-relay profile** from global configuration mode | (config-fr-profile)# |
| global | **configure** command from exec mode | (config)# |
| interface | **interface** command from context configuration mode | (config-if)# |
| macro | **macro** command from global configuration mode | (config-macro)# |
| netOp | **netop** command from global configuration mode | (config-netop)# |
| port | **port channelized oc-12**, **port ethernet**, and **port pos** commands from global configuration mode | (config-port)# |
| snmp server | **snmp server** command from global configuration mode | (config-snmp-server)# |
| software license | **software license** command from global configuration mode | (config-license)# |
| stats-collection | **stats-collection** command from global configuration mode | (config-stats-collect)# |
| STM-1 | **port channelized-stm1** command from global configuration mode | (config-stm1)# |
| subscriber | **subscriber** command from context configuration mode | (config-sub)# |

For initial configuration of a router, see *Performing Basic Configuration Tasks*, *Managing Configuration Files*, *Configuring Contexts and Interfaces*, *Configuring Cards*, *Configuring ATM, Ethernet, and POS Ports*, and *Configuring Subscribers*.

For configuring other SmartEdge features, see the configuration files in the SmartEdge OS library Operation and Maintenance > Configuration Management folder.

For more information about using CLI commands, see *Using the CLI* and for information about specific commands, see the *Command List*.

## 8.3 Privilege Levels

The SmartEdge OS supports 16 different privilege levels for administrators and commands. By default, administrators are assigned an initial privilege level of 6; administrators can only issue commands that are assigned at the same level as their own privilege level or lower than their privilege level. Each command in the CLI is assigned a default privilege level. At a privilege level of 6 or higher, the prompt in the CLI displays a number sign (#) instead of an angle bracket (>).

There are three types of administrators:

- Local—An administrator authenticated to the local context. The local administrator has a structured administrator name of the form ***admin-name*@local**.
- Nonlocal—An administrator authenticated to any context other than the local context. An example of a nonlocal administrator that has a administrator name of the form ***admin-name@ctx-name*** is **joe@vpn1**, where **vpn1** is the name of the context.

  **Note:** The separator character between the ***sub-name*** and the ***ctx-name*** arguments is configurable and can be any of %, -, @, _, \\, #, and /. The default character is @. For information about configuring the separator character, see *Configuring Authentication, Authorization, and Accounting*.

When setting up users on the system, the administrator assigns privilege levels to each of the users. If no level is assigned, the default is 6. Users can then access any command at or below their assigned privilege level.

An administrator authenticated to the local context, with appropriate administrator privileges, can configure all functions on the router, including functions for each context and global entities, such as ports, port profiles, SNMP, and so on. Nonlocal administrators have no configuration mode privileges and have restricted exec mode privileges.

To configure administrator privilege levels, see *Configuring Contexts and Interfaces*.

Each command has a default privilege level (15 for administrators, who can do anything) that determines who can enter the command. The majority of commands (in exec mode) have a default privilege level of 3, while commands in any configuration mode have a default privilege level of 10. Exceptions are noted in parentheses ( ) in the Command Mode section in any command description; for example, “exec (15)”.

Command privilege levels are configurable; to change the default privilege level for a command, see *Restricting Access to the CLI*.

## 8.4 No and Default Forms of Commands

Many configuration commands support the **no** keyword. Entering the **no** keyword in front of a command disables the function or removes the command from the configuration. For example, to create a message that is displayed after a user logs on to the system, enter the **banner exec** command (in global configuration mode). To subsequently disable the command from the configuration, enter the **no banner exec** command (in global configuration mode).

Many configuration commands support the **default** keyword. Entering the **default** keyword in front of a command returns a parameter or feature to the default state.

# 9 Administration

The router has many features for managing security and performance and monitoring and reporting on status, and troubleshooting the system.

For information on data collection when submitting a customer service request (CSR) to Technical Support, see *Data Collection Guideline for the SmartEdge Router*.

## 9.1 Managing Security

The SmartEdge OS security implementation is a multilayered strategy that provides protection at various components and modules in the system. The strategy includes the following main aspects:

- **Secure operation, administration, and maintenance (OAM)**
  - **Access**—You can access the SmartEdge OS by a directly connected console port or by telnet or ssh sessions to the management port. Access is permitted only to successfully authenticated users, based on username and password. The user database used for authentication can be locally managed on the SmartEdge platform or centrally managed on a RADIUS or TACACS server.
  - **User Accounts**—You can manage local user accounts through the command-line interface (CLI). All user accounts must have a password, which is stored encrypted in the configuration file. After you log in the first time, you can change your password using CLI commands.

- **Privileges**—User privilege levels determine the set of commands accessible to a user. Users with the default privilege level (6) cannot configure the system but can modify some ACL rule conditions. Access to higher privilege levels is password protected. You can also configure TACACS+ authorization for commands of a specified level.

- **Administrator Sessions**—Logon is permitted only on successful authentication. Idle sessions are disconnected by default after 10 minutes. The idle timeout interval is configurable. To discourage brute-force login attempts, the session is terminated after three authentication failures. Successful and failed logins as well as logouts are logged to the system log to provide security trails.

- **Secure Access**—The OAM traffic can be both physically and logically separated from other traffic by using separate network interfaces. The SmartEdge platform supports secure protocols such as SSH, SCP, and SFTP. Traffic over line cards can be secured using IPsec by using the ASE card hardware.

- **Logging**—Event logs and alarms raised by different modules on the router are handled by the logging infrastructure. Logs can be filtered based on the log level and directed to multiple destinations such as the system console, local storage, and remote syslog servers. You can use tunnel mode IPsec to transmit logs to syslog servers securely. Malicious traffic logs are visible to the logging infrastructure, but ACL drop logs are not. The security audit trail logs successful logins, logouts, and failed login attempts.

- **SNMP**—The SmartEdge OS supports SNMPv1, SNMPv2, and SNMPv3. You can configure community strings only by using the CLI. DES encryption is supported for SNMPv3. For security reasons, use SNMPv3 whenever possible.

- **Secure Layer 2 traffic**

  - **Ports & VLANs**—All ports on the router are disabled by default and have to be explicitly enabled and bound to an interface or associated with a bridge instance to be functional. By default, routing protocols are not enabled on any interfaces. You must configure a VLAN explicitly by setting the port encapsulation to 802.1.Qand creating PVCs. Merely setting the encapsulation to 802.1Q does not result in a default VLAN being created.

  - **Bridging MAC flooding**—The SmartEdge platform has several mechanisms that protect against MAC flooding attacks.

  - **ARP**—By default, the router accepts gratuitous ARP messages and is vulnerable to ARP poisoning. You can mitigate this problem by enabling secure ARP. You can rate-limit ingress ARP messages by configuring a QoS rate-limit policy and applying the policy to relevant circuits.

- **Enable Packet filtering**

You can filter packets by configuring IP ACLs. When you apply an ACL to an interface, packets received and sent over the interface are subject to the rules specified in the ACL. ACLs applied at the context level are called administrative ACLs; only packets sent to the kernel are subject to those ACLs. The format and function of ACLs are the same regardless of whether they are applied to kernel-bound packets or traffic sent or received over interfaces.

You can also configure administrative ACLs in any context to protect the control plane from unwanted traffic.

- **Secure Layer 3 routing**

  We recommend that you use loopback interfaces for all routing protocols. However, no restriction exists for configuring routing protocols to use nonloopback interfaces. By default, routing protocols are not enabled on any interface. Manually distributed keys, stored encrypted in the configuration file, are used for authentication. Authentication is implemented for all unicast IPv4 protocols. BGP peers are authenticated using MD5. You can configure prefix lists. The maximum number of prefixes accepted is configurable by BGP peer or by peer group and address family. The BGP process receives packets only on sockets bound to a specific local address and connected to a particular destination address. You can configure administrative ACLs in the BGP context to provide additional security.

  For malicious traffic detection, some Layer 3 security checks are performed implicitly by the forwarding plane, and others are performed when enabled through configuration. Malicious traffic detection is performed using a combination of implicit and configured checks. The forwarding plane maintains counters for packets dropped due to implicit checks, ACLs, reassembly failures, and so on. Some counters are maintained at the circuit level, and others are maintained at the context level. The malicious traffic counters correspond to the malicious traffic alarms. Related counters are grouped into a counter group (category) for display purposes.

- **Enable Security protocols**

  – **Key Chains**—Key chains allow you to control authentication keys used by various routing protocols in the system. The SmartEdge OS supports the use of key chains with the Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), and Virtual Router Redundancy Protocol (VRRP) routing protocols. In the configuration process, you establish a name for each key chain, and an identification for each key within the key chain.

  – **IPsec**—IPsec tunnel mode is supported on ASE cards. Only traffic exchanged over line cards can be secured by IPsec; the NetBSD kernel does not support IPsec. However, SmartEdge OS control traffic can be secured by IPsec if the traffic travels over line-card ports. IPv4 VPN traffic encryption is supported, as are the AES and 3DES encryption algorithms. Detection of anomalies and attacks is not supported. The

SmartEdge IPsec implementation is fully compliant with RFCs 2403 and 2405 and partially compliant with RFCs 4301-4309.

– **TACACS+**—TACACS+ secures remote access to networks and network services and is based on a client/server architecture. The router can be configured to act as a TACACS+ client. TACACS+ replaces the need for local configuration of user records, although we recommend a local configuration in case the remote server is unreachable. The SmartEdge OS supports OPIE, S/Key, and secureID.

- **Enable Security alarms**

  You can enable malicious traffic alarms in a single context-wide alarm against the aggregate of all the drop category counters. You can configure a global alarm threshold that applies to all contexts. An alarm is raised when the context-wide aggregate drop counter reaches or exceeds the configured high watermark within the configured interval. A raised alarm is cleared when the counter reaches or falls below the configured low watermark.

- **Enable Security logging**

  Malicious traffic logging is disabled by default; however, you can configure the forwarding plane to log packets dropped due to the various implicit and configured checks. You can enable logging for each of the counter groups. You can enable forwarding plane malicious-traffic logging independently of ACL packet logging, service troubleshooting, and forwarding plane packet logging.

For more information about SmartEdge security, see *SmartEdge OS Hardening Guide* in the Initial Configuration folder, the files in the Security Management folder (*Configuring Key Chains*, *Configuring Malicious Traffic Detection and Monitoring*, *Configuring TACACS+*, and *Restricting Access to the CLI*) and *IPsec VPN Configuration and Operation Using the SmartEdge OS CLI*

## 9.2 Managing Performance

To manage performance, you can use RFlow, load balancing, and SNMP.

### 9.2.1 RFlow

The SmartEdge OS provides RFlow for performance management. You can use RFlow to collect a variety of IP traffic statistics, which are compiled in a record that can help you understand data traffic in your network and optimize the following:

- Network planning and analysis
- Network monitoring

- Troubleshooting
- Accounting and billing

For details, see *Configuring RFlow*

### 9.2.2 Load Balancing

For performance management, the router provides load balancing for Layer 3, equal-cost mult-ipath (ECMP), and Layer 4 traffic streams, as well as between link groups and pseudowire multi-paths. For more information, see *Load Balancing*.

### 9.2.3 Simple Network Management Protocol (SNMP)

You can enable SNMP on the router to monitor one or more network devices from a central location. An SNMP management system includes one or more SNMP agents, an SNMP Manager, and the protocols to communicate information between the SNMP agent and manager entities such as trap notifications—for example, traps and events, Get requests, Set requests, and Management Information Bases (MIBs). You can also configure a target for collecting SNMP data.

## 9.3 Monitoring, Reporting, and Troubleshooting Tools

### 9.3.1 Logging

The SmartEdge OS contains two log buffers: main and debug. Log files must be sent to Customer Support when submitting a support request. In large installations, we recommend enabling the logging of system events to a remote syslog server that is reachable by the current context.

By default, log messages for the local context are displayed in real time on the console; nonlocal contexts are not displayed in real time on the console. To change this behavior, and display log messages in real time, use the **`logging console`** command (in context configuration mode in the context of interest). However, log messages can be displayed in real time from any telnet session using the **`terminal monitor`** command (in exec mode).

For more logging information, see *Logging*.

The SmartEdge OS also supports dynamic random-access memory (DRAM) crash dump data collection, if failures occur. You can enable sending core dump files to a URL using the File Transfer Protocol (FTP) to save space in SmartEdge memory.

### 9.3.2 Statistics

To monitor router status, you can configure Bulkstats to gather large amounts of data and periodically send updates to a management station. The bulkstats feature frees both the router and the management station from the Simple Network Management Protocol (SNMP) polling processes and minimizes the amount of memory used by the router for statistics collection. The collection of data is governed by a named bulkstats policy. Bulkstats policies are context-specific, and multiple bulkstats policies can exist for each context. A bulkstats policy defines the collection information, such as the transfer interval, the server to which the data files are sent, and the sampling interval.

For more information, see *Configuring Bulkstats*.

### 9.3.3 Reporting

The SmartEdge OS provides **show** commands to display most system features and functions. For example, you can use the monitoring commands in Table 7. For information about specific commands, see *Command List*, and for more information about using **show** commands, see *Using the CLI*.

For more information about using **show** commands to display information related to specific features, see the Configuration Management files.

*Table 7 Types of Monitoring Commands*

| Type of Command | Example | Function |
|---|---|---|
| Monitor a system component | **show chassis**<br><br>**show hardware** | Displays status of cards installed in the chassis.<br><br>Displays detailed card hardware information. |
| | **show port perf-monitor** | Displays configuration and performance statistics for one or more ports. |
| | **show circuit counters** | Displays statistics for one or more circuits. |
| Monitor the status of a process and provide continuous updates | **monitor process** | Enter this command in exec mode. |
| Monitor files in memory | **directory**<br><br>**pwd** | Displays a list of files in the specified directory. Enter this command in exec mode.<br><br>Displays the current working directory. Enter this command in exec mode. |
| Monitor a process | **show process** | Displays current status of a process. Enter this command in all modes. |

*Table 7 Types of Monitoring Commands*

| Type of Command | Example | Function |
|---|---|---|
| Display a software release or version | **show release**<br><br>**show version** | Displays release and installation information. Enter this command in all modes.<br><br>Displays the version of the currently running OS. Enter this command in all modes. |
| Monitor an administrator session | **show privilege**<br><br>**show public-key** | Displays the current privilege level for the current session.<br><br>Displays the public keys for an administrator.<br><br>Enter these commands in all modes. |
| System monitoring | **show clock-source** | Displays clock source information. Enter this command in all modes. |
| | **show configuration** | Displays the configuration commands for a feature. Enter this command in all modes. |
| | **show memory** | Displays memory statistics. Enter this command in all modes. |
| | **show redundancy** | Displays state of the standby controller card. Enter this command in all modes. |
| | **show system alarm** | Displays system alarms at one or more levels. Enter this command in all modes. |

### 9.3.4 Data Collection

If you have an issue with your router, before attempting to troubleshoot, collect data to record the state of the router at the time the issue occurred. If you submit an issue to Technical Support, they will require this data for troubleshooting.

For information on data collection when submitting a customer service request (CSR) to Technical Support, see *Data Collection Guideline for the SmartEdge Router*.

### 9.3.5 Troubleshooting

For information on resolving problems with the router, see the following guides in the SmartEdge OS library Operation and Maintenance > Fault Management > Troubleshooting folder:

- *ASE Troubleshooting Guide*
- *Basic Troubleshooting Techniques*

- *BRAS Troubleshooting Guide*
- *Debugging*
- *General Troubleshooting Guide*
- *Troubleshooting MPLS*
- *Troubleshooting OSPF*
- *Troubleshooting IPv6 and Dual-Stack Subscriber Services*
- *Troubleshooting IS-IS*
- *Troubleshooting L3VPNs*
- *Troubleshooting VPLS*