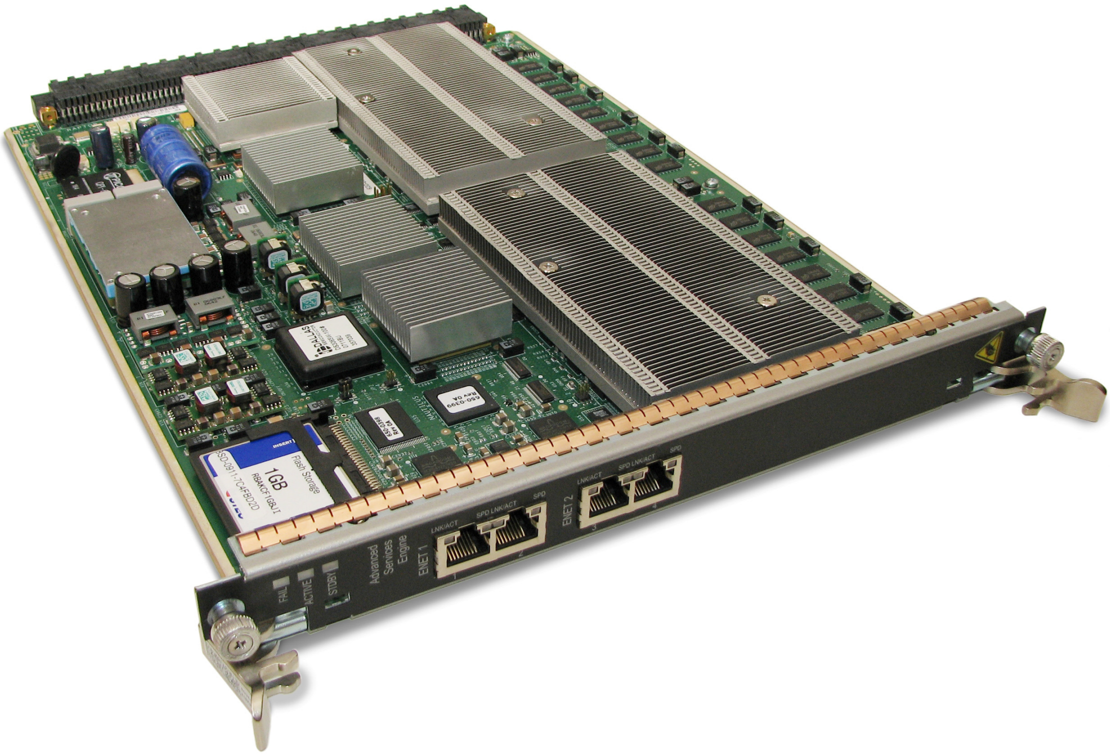
SMARTEDGE® ADVANCED SERVICES ENGINE - ASE

Provides Carrier-class Security and Application Identification for Secure, Efficient Operation of Your Network



Key benefits

- Supported in SmartEdge 400/800/1200
- Carrier-Grade Design: fault-tolerant ACTIVE/STANDBY or ACTIVE/ACTIVE operation Engineered – NEBS compliant
- Highly scalable architecture with multiple ASE cards in one chassis, each with 4 gbps throughput, 16,000 tunnels and 2 million P2P connections
- High performance processors for deep packet inspection: Cavium Octeon (16 cores @ 600 MHz)
- Designed with high performance processors and high speed RAMs; parallel processing of multiple flows for optimal performance
- Application-aware engine capable of pattern look-up in specific sections of an incoming packet
- IPSec services for remote office and mobile backhaul networks
- Parallel processing of multiple flows on the processors on board for optimal performance
- Compatible with SmartEdge two generations of Cross-connect Routing Processors boards (XCRP3 and XCRP4)
- ASE functionality is independent of layer2 encapsulations (ATM, Ethernet, etc)

Ericsson has enhanced its SmartEdge MultiService Edge Router with a high performance Advanced Services Engine (ASE) card that will redefine the role of edge routers in carriers' network. With the functionalities that are provided in ASE, the SmartEdge product line is now capable of six functions: IP/MPLS Edge Router, High Density Ethernet Aggregation, Broadband Remote Access Server (B-RAS), Session Border Controller, Network Security and Application Detection. Specifically, the ASE card enables advanced security functions to protect the network right at its edge closer to subscribers, for maximum effect. Security is provided via IPSec. With the ability to carry out Deep Packet Inspection, the ASE card can identify and process P2P applications, and provide a more efficient and secure network operation. Example of an application is detection of leading instant messaging (IM) services.

ERICSSON

Peer to peer identification

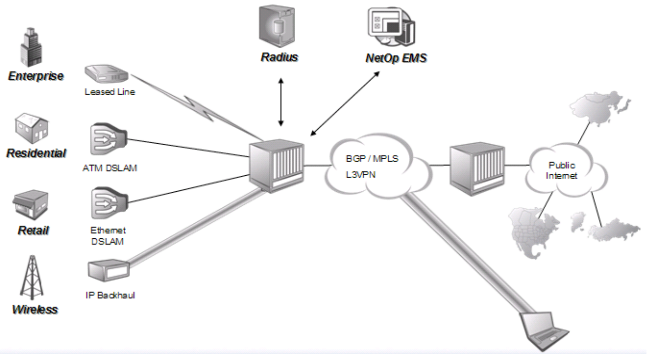
Powered by two Cavium Octeon (16 cores @ 600 MHz), the ASE card supports deep packet inspection (DPI) for identification of P2P applications. The DPI engine is also complemented with a heuristics based analysis engine. DPI implementation is stateful, and signature based. Therefore, the application state is maintained over the life of the logical connection while inspection is carried out on multiple packets simultaneously. Using Deterministic Finite Automata (DFA) graphs, raw packet analysis is conducted and the signature database is regularly updated by these same graphs. P2P identification capability enables operators to offer volume based billing even with high volume of P2P traffic as they can offer rate limits or tiered offering targeting P2P applications. Rate limiting profiles can be assigned per application or group of applications. Individual subscribers can be assigned composite profiles based on set of applications and per-application rate limits. With rate limiting P2P traffic, cost reductions, better customer experience and bandwidth efficiency can be obtained.

Example P2P applications that can be detected and processed are BitTorrent, eDoneky, Instant Messaging Services, Jabber, etc. Ericsson's NetOp product may be used to generate reports per P2P application, per subscriber, per node and per group of nodes.

Security (IPSec)

Security features are provided to ensure minimization of network disruption and offering personalized secure tunnels for end-user's applications. IPSec configuration, management and reporting can all be conducted via Ericsson NetOp Element Manager. The architecture is designed to optimize the performance of the card in the SmartEdge MSER. For example, no multicast packet will transit through the ASE card. Also, if a flow has not been signed up for specific secure services the traffic is bypassed by the ASE card.

The ASE card IPSec implementation offers secure tunnels for end-user's or business applications. IPSec services such as managed VPN for enterprise users or securing service provider's own data are classical examples of its usage. Ericsson's IPSec implementation also provides secure access to Layer 3 VPNs from locations that are outside of that VPN (figure below). Remote VPN access can be secured via L2TP (transport mode).



Device specifications for SmartEdge Advanced Services Engine - ASE

Hardware

- Takes one slot in a SmartEdge chassis
- Worst case power consumption: 178 Watts
- System clock speed – 600 MHz

Redundancy and high availability

- Active/Passive mode
- Active/Active Mode
- N:1 redundancy
- Inter- card and Inter-ASP redundancy

IPSec

- Supported RFC 2401, 2403-2410,2412,3706,3947,3948
- Route based VPN
- IKEv1 with pre-shared key
- Operating modes include:
  - IKE Main mode/Aggressive Mode
  - Quick mode for IPSec SA setup
- IPSec Encapsulation – ESP
- Encryption Methods
- DES-CBC (56 bits), 3DES-CBC (128 bits) , AES-128, AES-192, AES-256 bit
- Authentication and Hashing algorithms - HMAC-SHA1 and HMAC-MD5
- NULL encryption
- Dead Peer Detection
- Anti-Replay
- IPSec NAT traversal
- Perfect Forward Secrecy(DH Group Support) – Group 1,2,5

Performance and licensing

- Maximum concurrent sessions 2M flows
- New sessions/second 60K /second
- 3DES performance - 4G IMIX per card
- Concurrent tunnels - 16,000 per card

P2P

- Stateful – maintains application state over TCP session life
- Heuristics based application analysis
- Signature based
  - Raw Packet Analysis with DFA graphs
  - Hardware optimized to expedite DFA matching
  - Each P2P application has a dedicated engine
- Rate limiting per application or group of applications
- Rate limiting per subscriber
- Example P2P applications: BitTorrent, Skype , Kazaa Jabber

System management

- NetOp Policy Manager
- Command Line interface(console//ssh)
- SNMP (v2/v3)

Ericsson
100 Headquarters Drive
San Jose, CA 95134-1362 USA
Tel: +1 408 750 5000
Fax: +1 408 750 5599
www.ericsson.com