



# **Securing Service Provider Networks**

*Technology Overview*



## Introduction

***ECI Telecom's ShadeTree™ software's service delivery architecture incorporates an extensive set of security features to ensure all aspects of the system and services remain secure.***

## Thinking of Security in Planes

There are three operational planes in a data service network, the management plane, the control plane, and the data plane. The management plane is used to access network elements for network management purposes. The management plane can be an overlay on the data plane (in-band management) or use a separate network (out-of-band management). The control plane includes the network protocols, such as routing, signaling, and link management protocols that are used for communication between network elements. The control plane typically shares links with customer data. The data plane is where customer traffic is carried on the network and is comprised of the collection of network elements and links between network elements.

Security in the management and control planes is absolutely critical to network stability. A break in management plane security exposes network elements to an attacker who take can control of the network, reconfiguring or even shutting down devices. A break in control plane security allows a hacker to introduce false information about the network topology and potentially redirect customer traffic or even disable portions of the network.

The data plane is nearly impossible to secure completely since it carries customer traffic. What is most critical in the data plane is ensuring that each customer's traffic is carried securely across the network.

## Management Plane Security

Securing the management plane requires different approaches for in-band and out-of-band management. Out-of-band management is inherently more secure since the management traffic does not share links with customer data. With in-band management, precautions must be taken to prevent a network user from accessing the management processes on routers.



ECI's ST™200 ensures secure in-band management through a series of security features including:

- TACACS+ or RADIUS authentication
- Encrypted sessions using Secure Shell
- Access control lists
- Traffic policers to limit management
- Prioritization of management traffic relative to customer data traffic

In general, the management network should not be exposed to customers. For private services such as switched services and MPLS IP VPNs, the customer's traffic is secured (and isolated from the in-band management traffic) in the data plane using dedicated routing tables and connections. The customer therefore has limited or no access to the management network. For Internet services, however, all customer interfaces share a routing table with the in-band management network, opening a potential security hole. This can be secured using a combination of the features listed above.

In addition to in-band management, the ST200 provides a separate management interface for out-of-band management. Unlike most Internet routers that connect the management interface to the same IP stack used for the Internet data plane, the ST200 management interface utilizes a separate IP stack to provide enhanced security. This completely isolates the management interface onto its own secure IP management network and eliminates access to the management processes on the ST200 from any customer network interface.

## **Control Plane Security**

The control plane is critical to the operation of the network. If the control plane is compromised, it could lead to significant network outages or a potential compromise of the data plane, rendering customer traffic insecure. There are two aspects to control plane security – ensuring that the information received by control protocols (particularly at the network edge) is coming from a trusted source, and ensuring that the protocols operate in a consistent stable state. The latter is more difficult to achieve than the former.

The ST200 provides authentication and encryption on all control protocols to ensure secure communication. This prevents untrusted users from accessing the control plane; however, it does not prevent a trusted user from injecting invalid information into the control plane. Routing policies, secure routing protocol instances, and secure routing and switching tables are provided by the ST200 to control the reception and distribution of information on trusted protocol sessions.



The following features ensure that each protocol session is secure:

- MD5 encryption on all routing and signaling protocols including BGP4, IS-IS, OSPF, RSVP-TE, and LDP
- Extensive BGP import and export policies
- Import and export policies on IGP protocols including OSPF, IS-IS, and RIP

Compromises in the control plane are more likely to be the result of strenuous network conditions, bugs in network elements, heavy network load, or denial of service attacks on the control plane. The ShadeTree architecture is designed to prevent all of these conditions from introducing instability into the system. Several key features protect the control plane, including:

- Multi-threaded software architecture – critical tasks are separated into high priority threads to ensure that they receive sufficient processing time under strenuous load.
- Distributed software architecture – link protocols are separated from routing and signaling protocols and run on dedicated processors on each line card.
- Policing, shaping, and prioritization of protocol sessions – hardware policers, shapers, and priority queues control protocol traffic to the central RCPs in the ST200. This ensures that a misbehaving protocol session (due to a bug in attached equipment or a malicious attack) cannot impact performance of other well-behaved protocol sessions.
- Prioritization of network control traffic relative to customer data traffic – sophisticated QoS ensures that control protocols remain up even under extreme congestion in the data plane.

## **Data Plane Security**

The data plane is where customer traffic is carried on the network. It includes routing tables, connections, physical ports, sub-interfaces, channels, and logical interfaces. Securing the data plane is perhaps the most important area of security in provider networks since it is essential to ensure secure delivery of customer traffic. There are three primary areas of concern for data plane security:

- Ensuring secure delivery of customer traffic end-to-end
- Preventing a misbehaving customer or site from affecting other customers
- Preventing a malicious attack from impairing network services

The ST200 incorporates technology to address all areas of data plane security. The ST200 is specifically designed to create services for many customers simultaneously.



The ST200 ensures secure transport of customer traffic by first creating secure connections or tunnels across the provider's private IP/MPLS backbone network. Within these tunnels, the ST200 creates dedicated MPLS connections for each customer and service.

Switched services are secured using the MPLS connections by directly mapping ATM circuits, Frame Relay circuits, POS interfaces, or Ethernet VLANs:

- One-to-one mapping of Ethernet VLANs to MPLS connections
- One-to-one mapping of ATM or FR circuits to MPLS connections
- Port-to-LSP mapping for ATM, FR, PPP/POS, or Ethernet port services

Because these mappings occur directly on the customer interface, all customer traffic is securely delivered across the network using dedicated connections. The use of end-to-end connections eliminates the possibility of spoofing, redirection, or other techniques used in connectionless public data networks like the Internet.

Private routed services, such as IP VPNs, are secured using a combination of dedicated forwarding tables and connections for each customer VPN. At the edge of the network, each customer interface is tied to a secure forwarding table. The dedicated per-customer forwarding tables are interconnected across the network using secure MPLS connections (LSPs). This ensures that each customer's traffic is isolated to the customer's interfaces and, therefore, cannot be compromised by another customer.

ST200 hardware and software enhances security further through per-customer resource allocation. This allows resources to be allocated on a per-customer basis to ensure secure and reliable end-to-end carriage of customer traffic, including:

- Virtual Routing and Forwarding (VRF) tables dedicated to each customer
- Per-customer routing protocol instances secured with MD5 encryption
- Per-customer traffic queues and buffer allocation isolate each customer's traffic
- Per-customer rate-limiting and policing protect the network and other customers from a misbehaving user

ST200 wire-speed packet filters can be used to create access control lists. Traffic can be filtered according to:

- IP Type of Service (TOS) byte
- IP or TCP flag
- IP protocol (EGP, ICMP, IPv6, OSPF, PIM, RSVP, TCP, UDP, etc.)
- Source or destination address or port
- ICMP code or type



The ST200 incorporates additional features to secure public routed services such as Internet access, Internet transit, and Internet peering. These features also prevent malicious attacks from a customer on a private switched or routed service. The most important of these features is a comprehensive suite of Denial of Service (DoS) attack prevention features including:

- Source address verification
- Rate limiting and policing of control protocols
- MD5 authenticated and encrypted control protocol sessions
- Hardware filtering of all control traffic
- Prioritization of traffic to the main route control processor
- Multi-threaded architecture prevents critical tasks from being starved of compute resources

With these features enabled, the ST200 has been certified by leading ISPs to prevent a range of DoS attacks while maintaining wire-speed throughput, including:

land	fraggle	Nestea	syndrop	blurp	jolt 2	teardrop	arnudp	opentear
pingodeath	smurf	octopus	synful	killwin	jolt	papasmurf	kod	synk5
boink	bloop	pepsi	ssping	misfrag	bonk	newtear		

## Privacy vs. Security

The ST200 is designed for carriers to enable secure data services. All customer traffic switched or routed by the ST200 is ensured secure end-to-end delivery. However, some customers may wish to further secure the data-plane using encrypted tunnels. Encrypting data traffic provides privacy in addition to the security inherent in the ST200 service delivery architecture.

The only way a customer can ensure private delivery of traffic end-to-end is to encrypt the traffic prior to sending it into the carrier's network. This can be done on CPE equipment using IPSEC tunnels. It is important that these tunnels originate and terminate at the customer premises. If the traffic is delivered to the carried unencrypted, no privacy is ensured since the traffic has already traversed a public network on the access link between the CPE and provider point-of-presence (POP).



## **Conclusion**

The ST200 incorporates a service delivery architecture that ensures the highest level of security of any edge router in the industry. All aspects of service delivery are secured including the management plane, control plane, and data plane. Both providers and their customers can trust the ST200 to create and deliver secure public and private, switched or routed data services.



For more information on ST-series products and ShadeTree Management Suite, go to <http://www.ecitele.com/dnd> or contact one of ECI's local offices listed here:

**Corporate Headquarters/Research & Development Center**

ECI Telecom Ltd.  
30 Hasivim Street  
Petach Tikva, 49133 Israel  
Tel: +972 3926 6555  
Fax: +972 3928 7100

**US Research & Development Center**

ECI Data Networking Division  
Omega Corporate Center  
1300 Omega Drive  
Pittsburgh, PA 15205, USA  
Tel: +1 412 809 4200  
Fax: +1 412 809 4201

**Europe**

**ECI Telecom GmbH (Germany)**

Buopark Oberursel, In der Au 27,  
61 440 Oberursel, Germany  
Tel: +49 6171 6209 0  
Fax: +49 6171 6209 88

**ECI United Kingdom**

ISIS House, Reading Road, Chineham  
Basingstoke, Hampshire, RG24 8TW, UK  
Tel: +44 1256 388 000  
Fax: +44 1256 388 144

**ECI Telecom France**

Espace Velizy "Le Nungesser"

13 Avenue Morane Saulnier, 78140, Velizy,  
France

Tel: +33 (1) 3463 0480  
Fax: +33 (1) 3946 2118

**North America**

**ECI Telecom Inc., USA**

1201 West Cypress Creek Rd  
Fort Lauderdale, FL 33309, USA  
Tel: +1 954 772 3070  
Fax: +1 954 351 4404

**Latin America**

ECI Telecom do Brasil Ltda.  
Av. Dr. Cardoso de Melo, 1460 - cj. 101/2  
Vila Olimpia, 04548-005 - Sao Paulo - SP - Brasil  
Tel: +55 11 3512 1600  
Fax: +55 11 3512 1601

**Asia Pacific**

ECI Telecom Singapore  
150 Beach Road #28-07/08  
Gateway East, Singapore 189720  
Tel: +65 6297 7335  
Fax: +65 6299 2716

**ECI Telecom India**

301, Boston House  
Suren Road, Andheri - East  
Mumbai - 400 093  
Tel: +91 22 5675 8971  
Fax: +91 22 5675 8973

**About ECI Telecom**

ECI Telecom offers future-ready telecommunications solutions that leading carriers and service providers rely on for delivering revenue-generating services to their business and residential customers. With its current products, ECI can deliver a full complement of access-to-edge IP transport solutions today. Known for its ability to translate customer needs into scalable, flexible, cost-effective solutions, ECI helps companies increase the value of their network infrastructure and reduce operating expenses. The company's single-shelf networking systems simplify network deployment and enable Build-as-You-Grow™ next generation telecommunication networks.

**The Data Networking Division**

The Data Networking Division (DND) adds next-generation IP/MPLS edge routing technology to ECI Telecom's product and services portfolio. DND's edge routers offer full-featured, multi-service support and complete Internet routing in a carrier-class, IP-based platform. ECI's ST-series routers provide the automated subscriber management, reliability, and performance that service providers need to implement advanced, revenue-generating broadband applications, like video on demand or voice over IP.

---

© 2006 ECI Telecom DND, Inc. All rights reserved. ST and ShadeTree are trademarks ECI Telecom DND, Inc. All other trademarks, service marks, registered trademarks or registered service marks are the property of their respective owners. ECI Telecom assumes no liability for any inaccuracies in this document and reserves the right to change this document without prior notice.