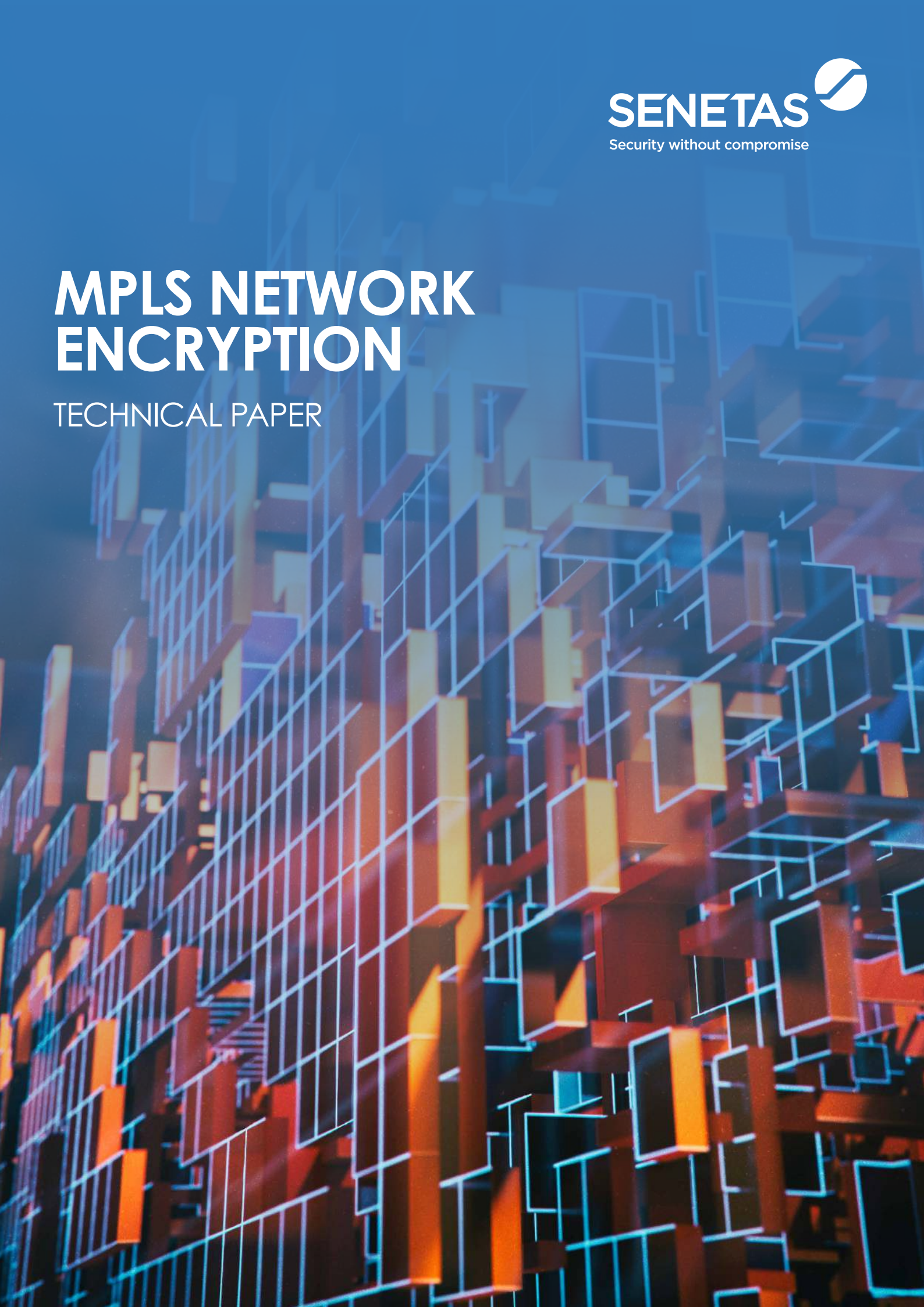
SENETAS
Security without compromise

MPLS NETWORK ENCRYPTION

TECHNICAL PAPER



Senetas high-assurance encryptors provide the most efficient means of encrypting data across modern metro or wide area Ethernet networks.

By encrypting the payload of Ethernet traffic, sensitive data (including all IP addresses) is kept completely private whilst the frame headers are left unencrypted so that traffic can still be switched across the network.

Senetas encryptors provide extremely high performance encrypted throughput and can operate at wire speed at rates up to 100 Gbps. By using a dedicated hardware encryption engine and a non-blocking architecture, the encryption process adds additional latency of less than 10 microseconds; ensuring that performance sensitive network applications such as video or voice traffic are not impacted.

Senetas encryptors provide strong authenticated key management using industry standard X.509 certificates that are installed in each encryptor from a trusted root Certificate Authority.

The encryptors automatically exchange credentials across the network for authentication and to securely exchange the AES data encryption keys that are used to encrypt network traffic.

MPLS Network Encryption

Senetas high-assurance encryptors are designed to be transparent across any layer 2 network such as point-point dark fiber, WDM links, metro Ethernet, VPLS or any layer 2 MPLS services.

Senetas encryptors can also be used across a layer 3 MPLS network (one in which Ethernet headers are not preserved end-end) with the following two conditions:

- The encryptor must be configured to preserve MPLS labels and/or IP addresses in the clear so that they are visible across the core for network forwarding
    - This is a standard encryptor configuration item and can be enabled via the CLI or remotely using Senetas CM7 or Safenet Management Centre(SMC).
- The second condition is that a layer 2 broadcast domain must be available for the encryptor's key management traffic which is sent as Ethernet frames.
    - This can be provisioned as either a physically separate network
    - Or across the MPLS network itself depending upon its capabilities

Layer 2 domain provisioned across the MPLS network

This can be provisioned across the MPLS core itself.

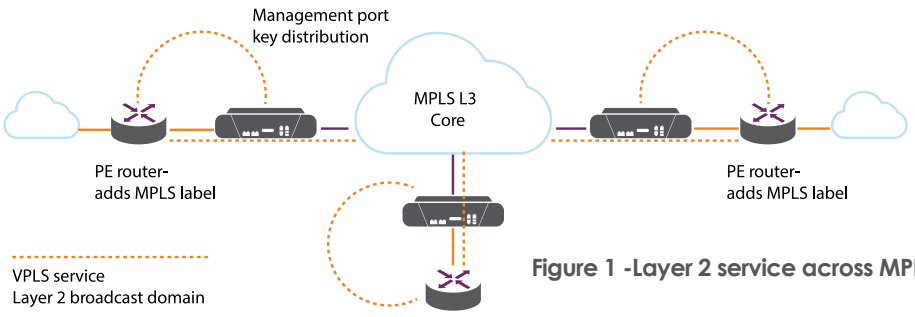


Figure 1 -Layer 2 service across MPLS core

Figure 1 shows one way of achieving this. In this example the encryptors require out-of-band key management (a dedicated port on the encryptor) where the encryptor's management port is connected to a PE router on the protected side of the network. The network operator must configure a VPLS (layer 2 broadcast domain) service across the MPLS core that connects all the router ports that are connected to the encryptor's administration interface.

MPLS networks can generally be configured to pass either layer 2 or layer 3 traffic end-to-end. Provisioning the VPLS service where it is needed allows the encryptors to exchange keys and establish secure connections across the MPLS core.

Once a secure connection has been established, the Senetas high-assurance encryptors will secure traffic at 100% line rate. The frame header can be left unencrypted ensuring that it can be switched across the network.

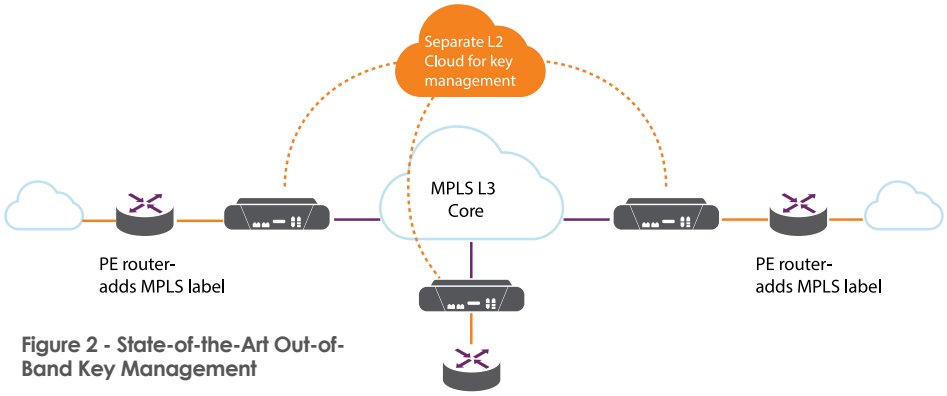


Figure 2 - State-of-the-Art Out-of-Band Key Management

To bypass this issue, Senetas encryptors have a standard mechanism to allow key management traffic to be sent out the administration (management) interface instead of out the normal network facing port; this is called out-of-band key management.

Figure 3 shows how this feature can be enabled using the SafeNet CM7 management platform. The feature functions similarly in SMC. Alternatively the CLI command to enable this is shown in Figure 4.

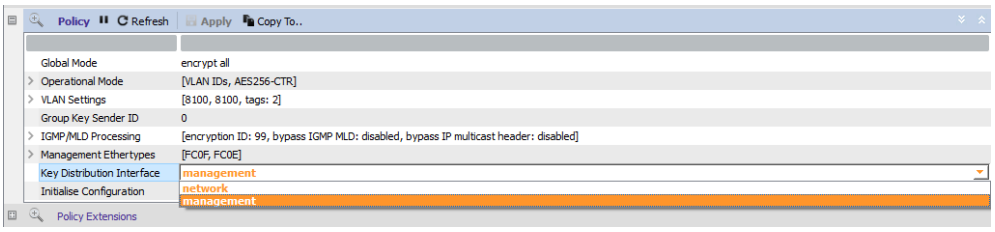


Figure 3 - Enabling management interface key distribution via CM7

Format

controlplaneif<CR>	Display current status
[net/man]	Set key distribution port to Network port or Management port

Figure 4 - CLI command

In this topology, the encryptors will authenticate each other and exchange encryption keys across the separate layer 2 network. Once this is complete, data across the MPLS WAN will be fully encrypted and the MPLS/IP headers left in the clear to allow switching in the WAN. There is no degradation of performance or impact on the security of the network.

GLOBAL SUPPORT

Senetas encryption solutions are distributed and supported internationally (outside Australia and New Zealand) by Thales

Thales is the world leader in digital security and defence, servicing over 30,000 customers across 180 countries. Senetas products are sold by Thales under its brand.

ANZ PARTNER COMMUNITY

Senetas works directly with customers and their service providers across Australia and New Zealand. We provide technical consultancy and support to data networks providers, systems integrators and cloud service providers. Visit our **ANZ Partner Page** for full details.

www.senetas.com

Senetas is a leading developer of end-to-end encryption security solutions; trusted to protect enterprise, government, defence, Cloud and service provider network data in over 40 countries.

From certified high-assurance hardware and virtualised encryption, to secure file sharing and collaboration with data sovereignty control, all are based on the same crypto-agile platform and deliver security without compromise.

Regional Contacts:

Asia	**T:** +65 8307 3540	**E:** infoasia@senetas.com
Australia & New Zealand	**T:** +61(03) 9868 4555	**E:** info@senetas.com
Europe, Middle East & Africa	**T:** +44 (0)1256 345 599	**E:** infoemea@senetas.com
The Americas	**T:** +1 949 436 0509	**E:** infousa@senetas.com

GET IN TOUCH

Are you looking for a service provider to help you select and implement a network data encryption or secure file sharing and collaboration solution? Contact Senetas and we'll help you find the right one.

Senetas works with IT infrastructure service providers and systems integrators across the globe, to help specify the optimal cybersecurity solution for their customers' needs.

Customers may contact Senetas directly to discuss their requirements; or ask their service provider to speak to us on their behalf.

NETWORK DATA SECURITY WITHOUT COMPROMISE

Whatever your network security needs, Senetas has a network independent encryption solution to suit. Our multi-certified high-assurance encryptors protect data across networks operating at speeds from modest 100Mbps to ultra-fast 100Gbps and support all network topologies.

Our virtualised encryption solution, for virtual CPE and virtualised WAN, supports bandwidths of up to 15Gbps. It provides policy-based, end-to-end encryption across multi-Layer networks.

Senetas encryptors are recognised globally for delivering maximum data security and crypto-agility, without compromising network or application performance.

They are trusted to protect much of the world's most sensitive government, defence and commercial data.

SECURE COLLABORATION

SureDrop offers all the flexibility of a drop-box style solution, with the added benefit of best-in-class encryption security and 100% control over data sovereignty.

For customers seeking additional layers of content security, SureDrop is also available with the Votiro Secure File Gateway extension.

DISARM MALICIOUS CONTENT

Votiro Secure File Gateway leverages patented Content Disarm & Reconstruction (CDR) technology to protect your files from the most advanced, persistent cyber-attacks. It sanitises incoming files, eliminating the risks associated with zero-day or undisclosed attacks, whilst preserving 100% file functionality.

SENETAS