SENETAS

Security without compromise

SECURE MULTICAST TRANSMISISON

TECHNICAL PAPER

SECURE MULTICAST TRANSMISSION

This Technical-Paper discusses the encryption of multicast data traffic at Layer 2 to provide secure data transmission through high-speed networks.

Senetas CypherNET (CN) encryptors are devices that secure information transmitted at wire speeds across wide area Ethernet services.

Encrypting multicast traffic is difficult because of the nature of the data flow. This paper describes how multicast traffic can be transmitted simply and securely by encrypting at Layer 2 in the OSI model.

Multicast applications

Multicast transmission sends information simultaneously to interested receivers in a single transmission. This bandwidth saving technology delivers the same information efficiently to a group instead of individually to each member.

The growth of video-based applications as well as real-time information feeds and content delivery systems has led to increased multicast traffic volumes.

Multicast delivery across Layer 2 networks

Figure 1 shows data transmission for the unicast, broadcast and multicast cases. Unicast delivery requires a source to transmit a single copy of the data to one receiver. Broadcast delivery sends a single copy of the data to all members of a group; multicast delivery sends data to selected members of a group.

Efficient multicast delivery requires all network devices between transmitter and receivers to know the selected group members and to deliver packets only where they are needed.

Multicast transmission uses various protocols and reserved network addresses. At Layer 3, the class D range of IP addresses is reserved for multicast protocols. At Layer 2, the low order bit of the high-order byte in the destination MAC address distinguishes unicast addresses from multicast addresses.

For example:

- 00:80:C8:F9:76:EF is a Unicast address – indicated by 00 in the first octet of the MAC address.
- 01:00:5E:00:00:05 is a Multicast address –indicated by 01 in the first octet of the MAC address.

Multicast group membership is implemented using the Internet Group Management Protocol (IGMP) for IPv4 networks or Multicast Listener Discovery (MLD) Messages for IPv6 networks. Both protocols dynamically register individual hosts in a particular multicast group with a multicast router.

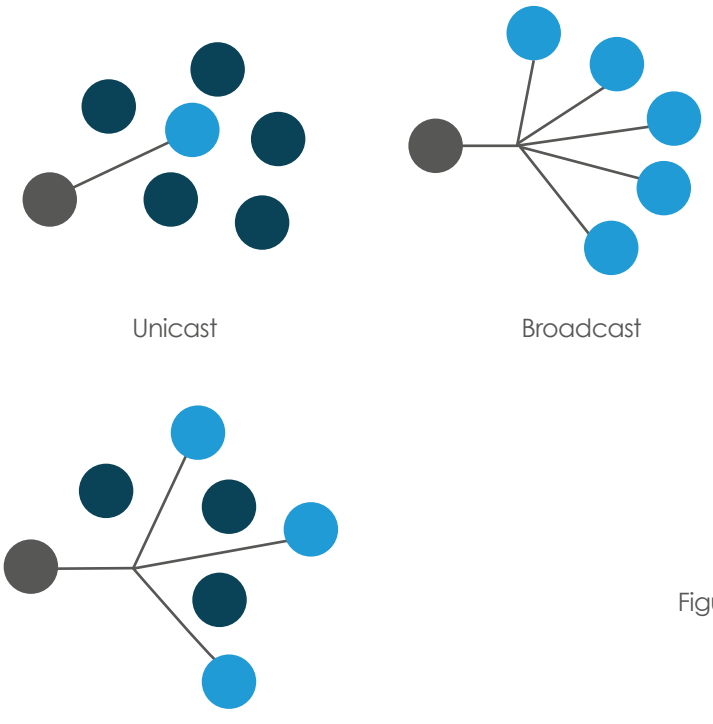


Figure 1

By default, a Layer 2 switch broadcasts multicast traffic from all destination ports. More efficient delivery of multicast traffic requires Layer 2 switches to learn which ports are associated with each multicast group. This is achieved by IGMP/MLD snooping - "listening in" on IGMP network traffic as it passes through the switch.

Figure 2 shows a Layer 2 switch in the path between a multicast router and the participating hosts. IGMP snooping requires the switch to eavesdrop on the information in the IGMP packets sent between the hosts and the multicast router. In this way the switch learns when hosts join a group (using IGMP join) or leave the group (using IGMP leave), therefore multicast data is only transmitted out of the relevant ports.

Encrypting IGMP/MLD packets prevents snooping and causes multicast traffic to be broadcast. For this reason, Senetas encryptors' policy control permits them to selectively encrypt OR bypass IGMP/MLD packets through the encryptor. This allows switch snooping and efficient network delivery.

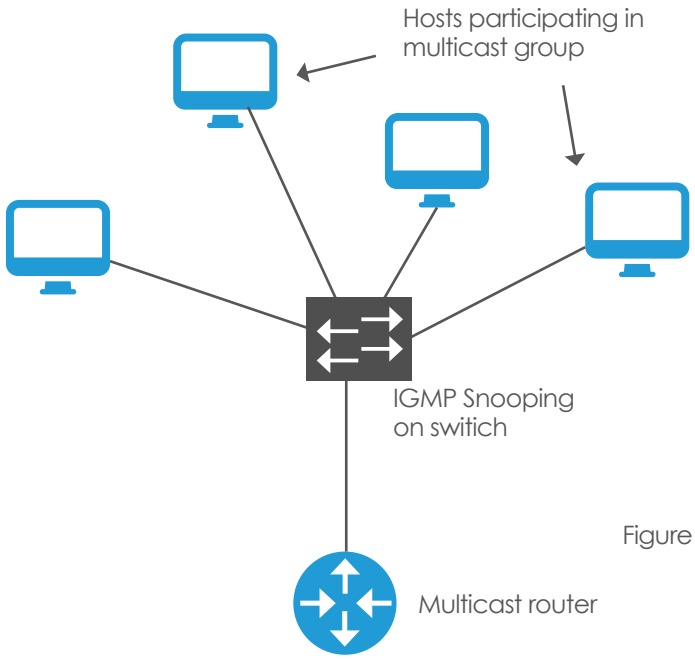


Figure 2

Security of multicast traffic

The risk to multicast communication is similar to, or greater than, that for unicast transmission and includes eavesdropping as well as unauthorised modification or destruction of data.

Multicast distribution has vulnerabilities that unicast traffic does not have. For example, because multicast group membership is open and unauthenticated, anyone is able to join a multicast group so that they can receive the traffic stream or maliciously insert data into the group (senders need not be members).

By using widely available webinar and video conferencing tools, businesses increasingly use multicast technologies to reduce the number and frequency of face-to-face meetings. Recent research demonstrates that insecure video conferencing systems can be 'the bug in the boardroom', allowing hackers to listen to confidential discussions. This risk can be mitigated by encrypting multicast sessions thus ensuring confidential network traffic.

Encryption of multicast traffic is challenging because a single sender must synchronise the encryption state with multiple receivers. Each receiver requires secure knowledge of the encryption key, the encryption state and must be able to receive and send traffic to other members of the group.

Using a group key system solves this problem. Every member of the shared community (for example, a multicast group or a VLAN) has a common key with which to encrypt and decrypt traffic. By contrast, unicast encryption uses a unique key per connection between a single sender and a single receiver.

One method of group key implementation uses a dedicated key server (Figure 3) that pushes encryption keys to all members.

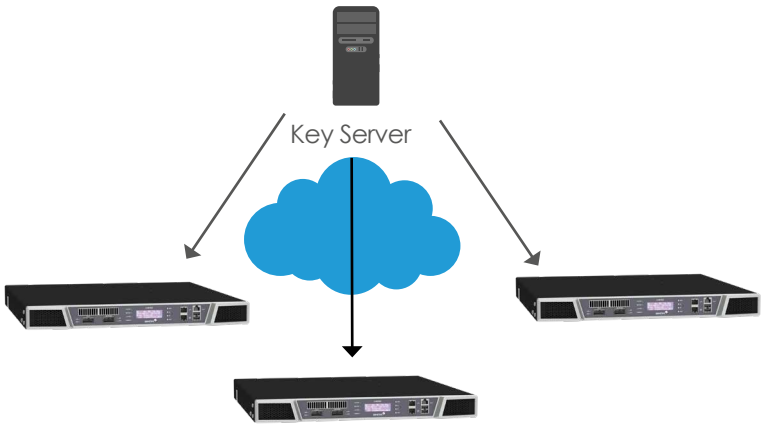
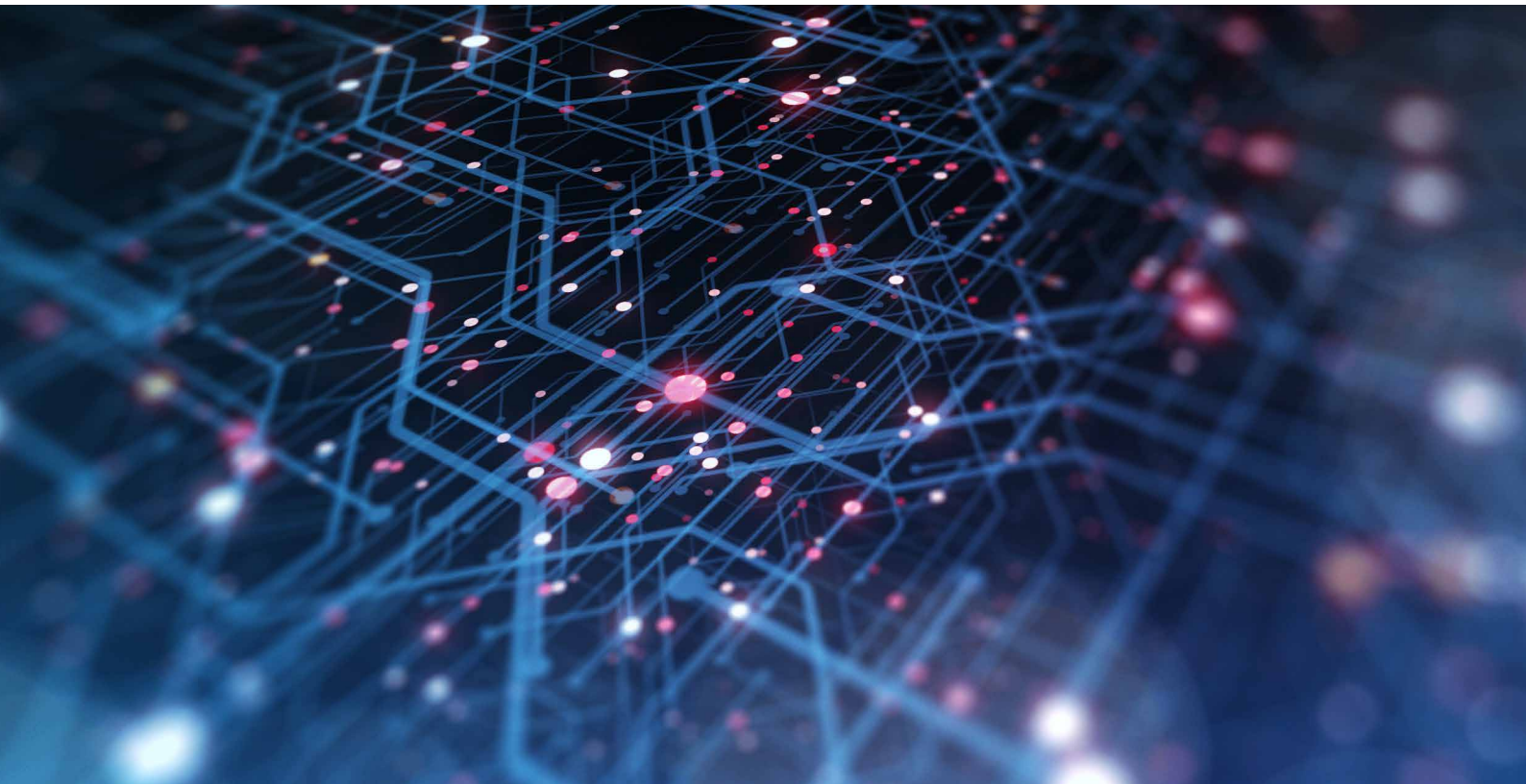


Figure 3

Limitations of this method include:

- Purchase & maintenance of another server in the network (more than one if load balancing / redundancy is needed)
- Server must be accessible by all group members
- Server always must be online or the keys are not refreshed
- A single point of compromise (redundant servers don't necessarily mitigate this because a compromise to one server is a compromise to all with shared keys)
- A single point of failure (redundant servers can mitigate this at additional expense)



Senetas group encryption

Senetas uses an alternate approach to group key distribution. Giving one encryptor in the group responsibility for generating and distributing keys to all other members avoids the need for a separate key server, (see Figure 4).

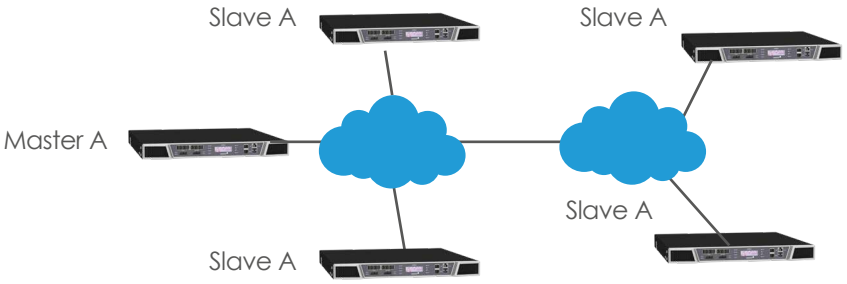


Figure 4

This model delegates the role of key master to one encryptor using an automatic election process amongst the visible encryptors in the network.

Features:

- Automatic discovery of multicast encryption groups and secure connections (manual configuration of MAC addresses or VLAN IDs is not required)
- Secure distribution and automatic updates of keys to all members of the group
- New members can securely join or leave the group at any time
- Automatic aging/deletion of inactive groups
- Fault tolerant to network outages and topology changes

In the event of a temporary isolation of network segments (caused by a network outage or reconfiguration as shown in Figure 5), the group key management scheme automatically maintains/establishes new group key managers within each visible network.

When the network segments rejoin, the network transparently re-elects a single group as key master. This 'split-rejoin' process does not disrupt network traffic provided the network is separated for less than two key update periods.

If the key update period is one hour, two split groups can use the same key for between one and two hours. Key updates allow the encryptor with keys to stay one key update period change ahead.

If two or more key updates occur while the networks are separate, the terminating group (controlled by the key master that terminates) synchronises with the remaining Master. This causes less than three seconds of disruption.

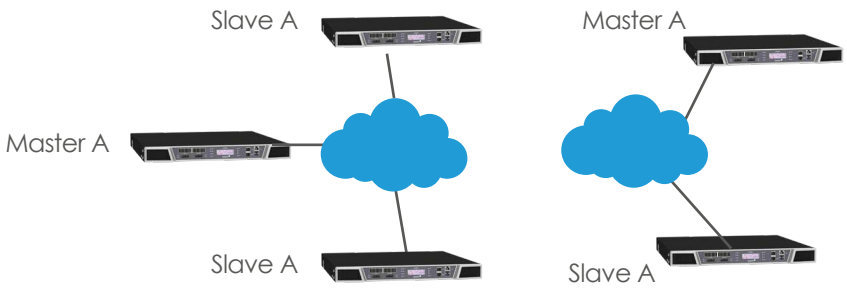


Figure 5 - Network split with 2 key masters

Policy control

Multicast encryption is supported by both MAC and VLAN modes of operation on Senetas encryption appliances.

i. In MAC mode the encryptor will establish both unicast and multicast connections based on the MAC address in each received Ethernet frame.

In this mode pairwise keys encrypt frames with unicast destination addresses. Dynamic multicast connections are established using group keys for frames with multicast destination addresses. Multicast connections can be automatically deleted when no traffic is present for a specified number of minutes.

ii. In VLAN mode the encryptor establishes an encrypted connection per VLAN using group keys only. The VLAN identifier in the frame distinguishes secure connections. VLAN connections are automatically discovered but do not age with inactivity.

Where one multicast group address spans multiple VLAN IDs (for example in Figure 6 where all hosts are part of the same multicast group), VLAN mode is required. This ensures that the encryptor's key management traffic is always on the same VLAN for a given connection.

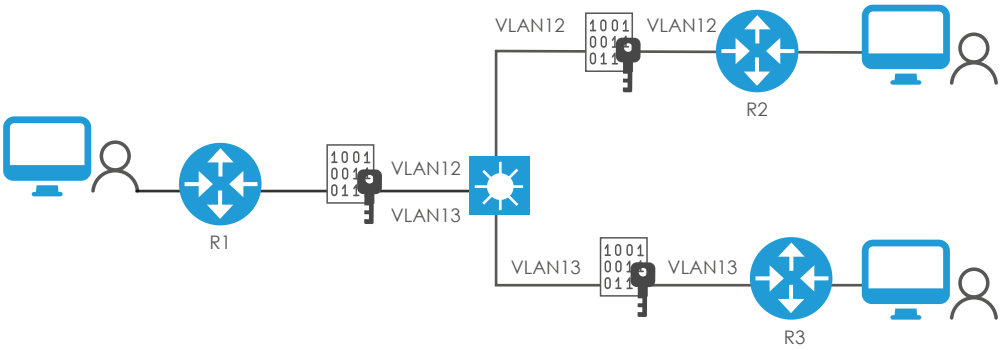


Figure 6 - Multicast group that spans VLANs

Senetas' GUI management tool, CypherManager, configures the encryptor policy. This provides detailed control of traffic processing and allows encryption policy to be set on a per Ethertype / per address class level of resolution as shown in Figure 7.

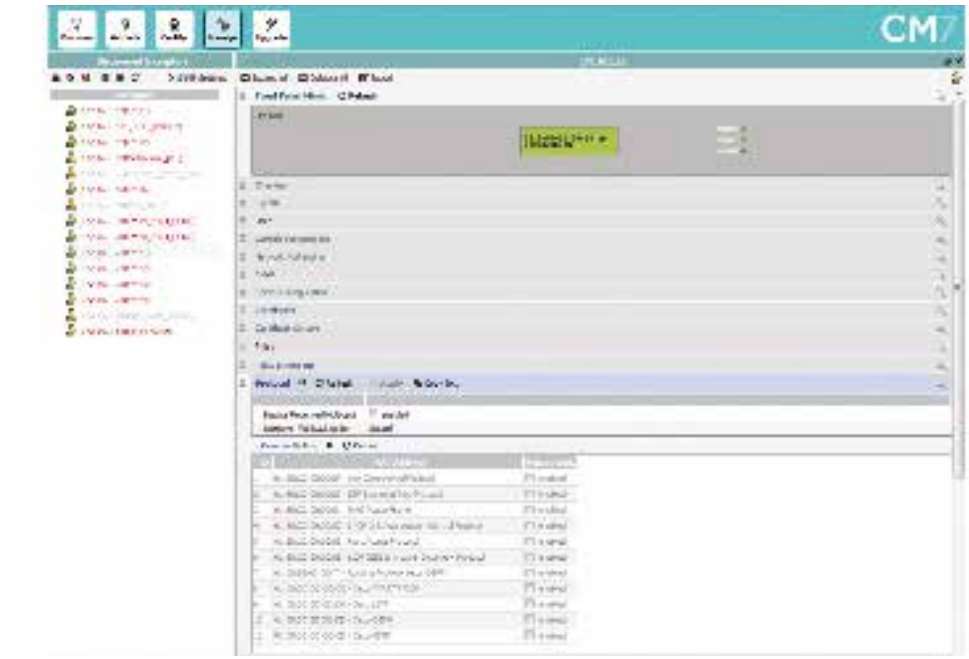


Figure 7

Performance

The CN encryption platform uses dedicated silicon for cut-through forwarding of data plane traffic. This allows wire speed processing of encrypted traffic at full line rate at up to 100Gbps.

Latency on the CN9120 Ethernet encryptor is less than 2 microseconds and is independent of packet size. Encryption introduces little or no jitter regardless of the network application or traffic profile.

Encryption uses the AES algorithm with 256 or 128 bit keys. In group encryption mode (VLAN or multicast MAC) CTR encryption is used. This introduces an additional eight bytes of data to every encrypted frame.

Summary

There is a growing need to securely and efficiently deliver multicast traffic across networks for a variety of applications.

Encryption at Layer 3 is problematic from a complexity and performance perspective. Encryption at Layer 2 is a simple, effective way of securing multicast traffic streams without compromising network performance.

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