Trusted Cyber Technologies

THALES

Secure Multicast Transmission

White Paper

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

Thales CN series 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.

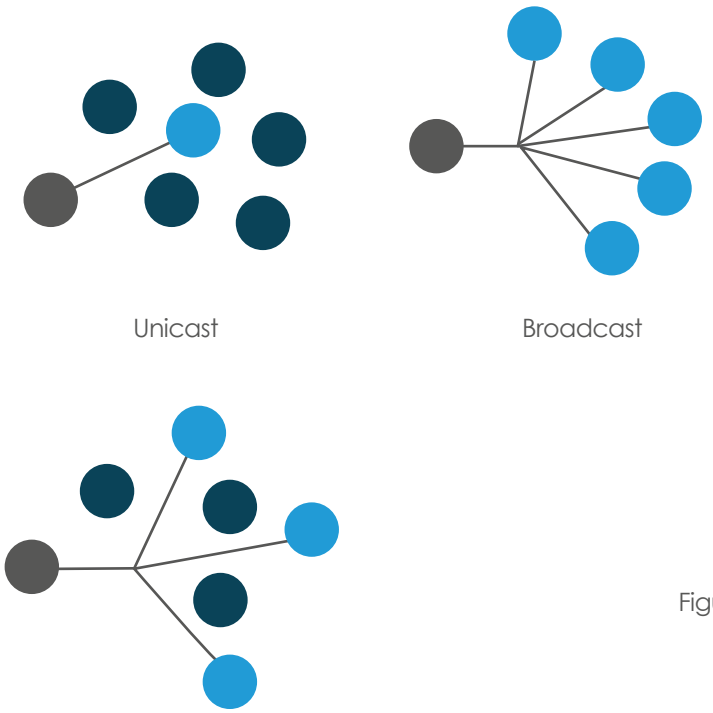

Figure 1

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.

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, Thales encryptors' policy control permits them to selectively encrypt OR bypass IGMP/MLD packets through the encryptor. This allows switch snooping and efficient network delivery.

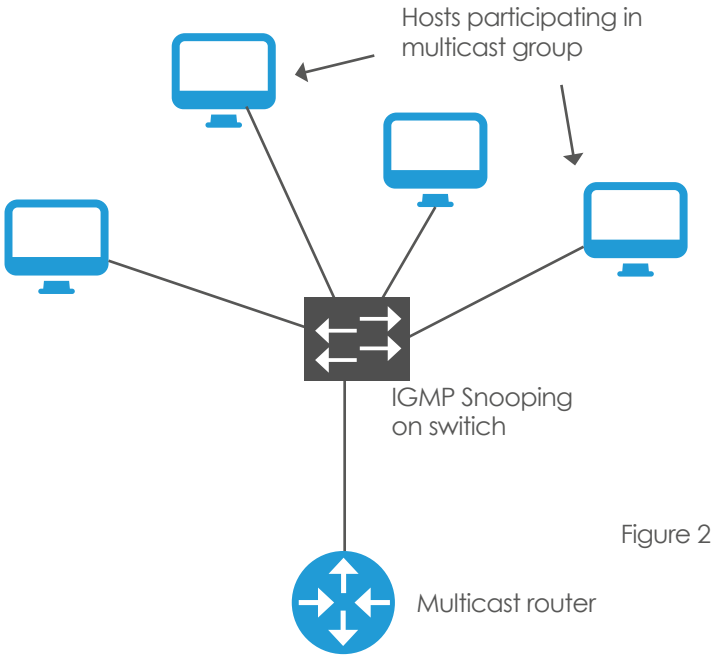

Figure 2

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.

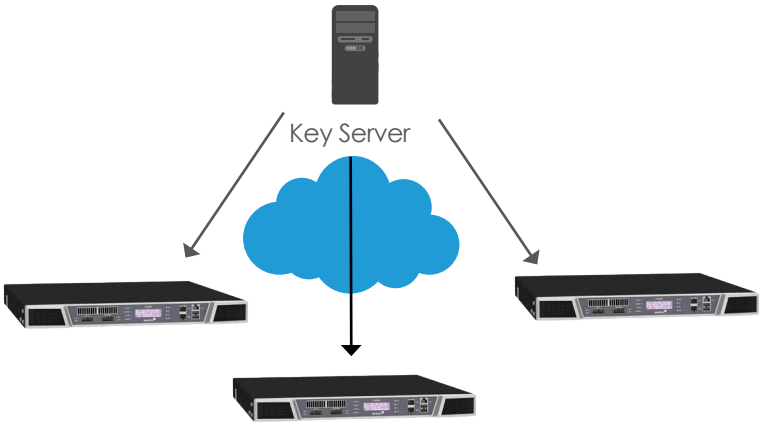

Figure 3

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)

Thales Network Encryption

Thales 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).

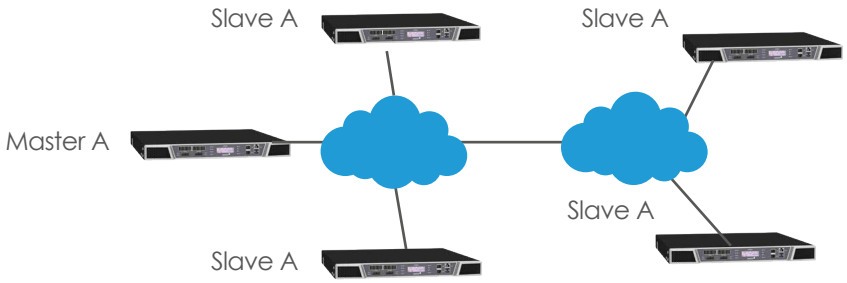

Figure 4

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.

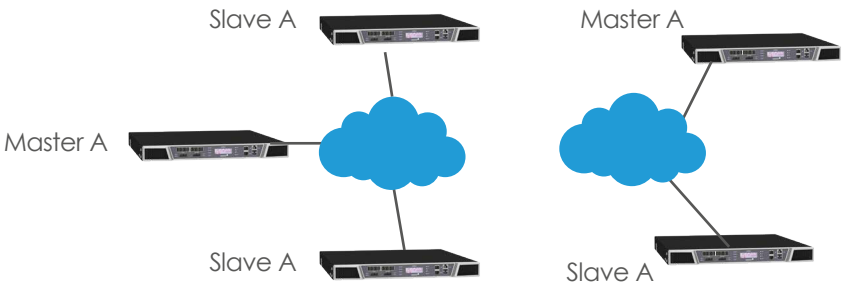

Figure 5 - Network split with 2 key masters

Policy control

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

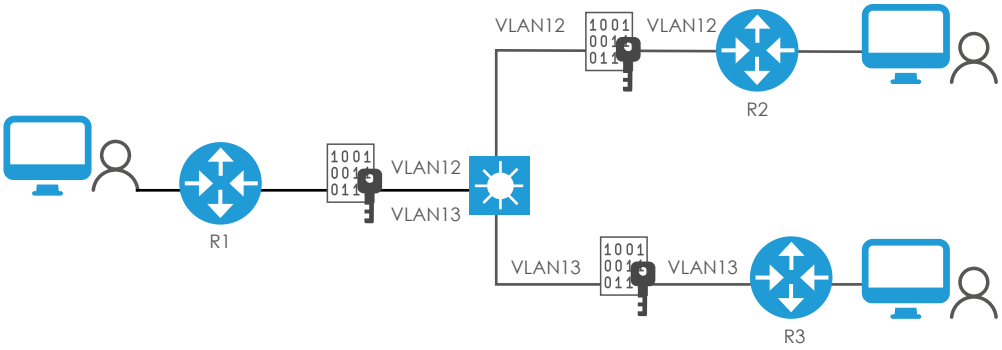

Figure 6 - Multicast group that spans VLANs

Thales GUI management tool 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.

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.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com