



Interception Of IP Multicast Traffic

A VERINT SYSTEMS TECHNICAL BRIEF

September 2007

Table of Contents

Preface: An Introduction to IP Multicast	1
Addressing the Challenges of IP Multicast Interception	2
The Role of Internet Group Management Protocol (IGMP)	2
A Typical Interception Solution	3
Verint Lawful Interception Solutions	4
About STAR-GATE.....	4
About RELIANT.....	4

Unauthorized use, duplication, or modification of this document in whole or in part without the written consent of Verint Systems Inc. is strictly prohibited.

By providing this document, Verint Systems Inc. is not making any representations regarding the correctness or completeness of its contents and reserves the right to alter this document at any time without notice.

All marks referenced herein with the ® or TM symbol are registered trademarks or trademarks of Verint Systems Inc. or its subsidiaries. All rights reserved. All other marks are trademarks of their respective owners.

© 2007 Verint Systems Inc. All rights reserved worldwide.

ACSTG441007U

Preface: An Introduction to IP Multicast

IP Multicast is a technology that enables a single data stream to be simultaneously delivered to multiple, specific destinations over an IP infrastructure. IP Multicast conserves network bandwidth, even as the data is delivered to thousands of endpoints. Alternatives such as broadcast do not scale well and are therefore usually limited to the local network.

In most multicast implementations, an IP packet is sent only once over the same link. A spanning tree needed to reach each multicast client (a destination of a multicast packet) is calculated by multicast protocol messages between IP routers at the IP level.

To enable multicasting, the IP header of a multicast datagram is different from a regular IP packet. While it contains a regular source IP address, the destination IP address is an IP address of the Multicast Group to which the packet is sent and does not correlate to a specific host, and the destination MAC address is derived from the IP address and does not correlate to a physical address.

This technical brief addresses the challenges and solutions associated with intercepting IP Multicast traffic in law enforcement applications.

Practical Applications of IP Multicast Technology

Interception of IP Multicast traffic may be important for law enforcement applications because IP Multicast is used in many real-time applications, such as:

- IPTV
- Internet video streaming (e.g. webcams)
- Internet audio streaming (e.g. Internet radio)
- Audio/video conferencing
- Stock-quote delivery
- News feeds
- Online gaming

IP Multicast is also effective in non-real-time applications, especially when eliminating data duplication in the delivery of large amounts of data can conserve significant bandwidth.

Examples of such non-real-time applications are:

- File mirroring/replication
- Database replication
- Software distribution

Verint. Powering Actionable Intelligence.®

Verint® Systems Inc. is a leading global provider of analytic software-based solutions for enterprise optimization and security. Verint solutions help organizations make sense of the vast voice, video, and data available to them, transforming this information into *actionable intelligence™* for better decisions and highly effective performance.

Since 1994, Verint has been committed to developing innovative solutions that help global organizations achieve their most important objectives. Today, organizations in over 100 countries use Verint solutions to enhance security, boost operational efficiency, and fuel profitability.

Addressing the Challenges of IP Multicast Interception

The unique characteristics of the IP Multicast datagram present several challenges when intercepting by IP address (referred to as the IP Target). While it is not problematic to intercept Multicast IP packets sent *from* the IP Target, incoming multicast traffic *to* the IP Target would not carry the IP address of the target and would consequently be ignored. An IP subscriber could thus receive packets that are not properly monitored.

Although some multicast applications, such as IPTV and Internet Radio, may be of minimal interest to law enforcement agencies, other multicast traffic may contain information important to an investigation; for example, an Internet subscriber watching a child pornography video stream using multicast technology or a suspected terrorist watching Internet webcam images of locations he is planning to visit.

The problem of not intercepting incoming multicast traffic affects not only targets directly intercepted by IP address, but also targets intercepted by login name, calling line identity, MAC address, and similar identities used by such protocols as RADIUS and DHCP for authentication and dynamic IP allocation. A lawful interception solution that analyzes RADIUS and DHCP for target IP addresses will likely fail to intercept incoming multicast traffic to the target.

The Role of Internet Group Management Protocol (IGMP)

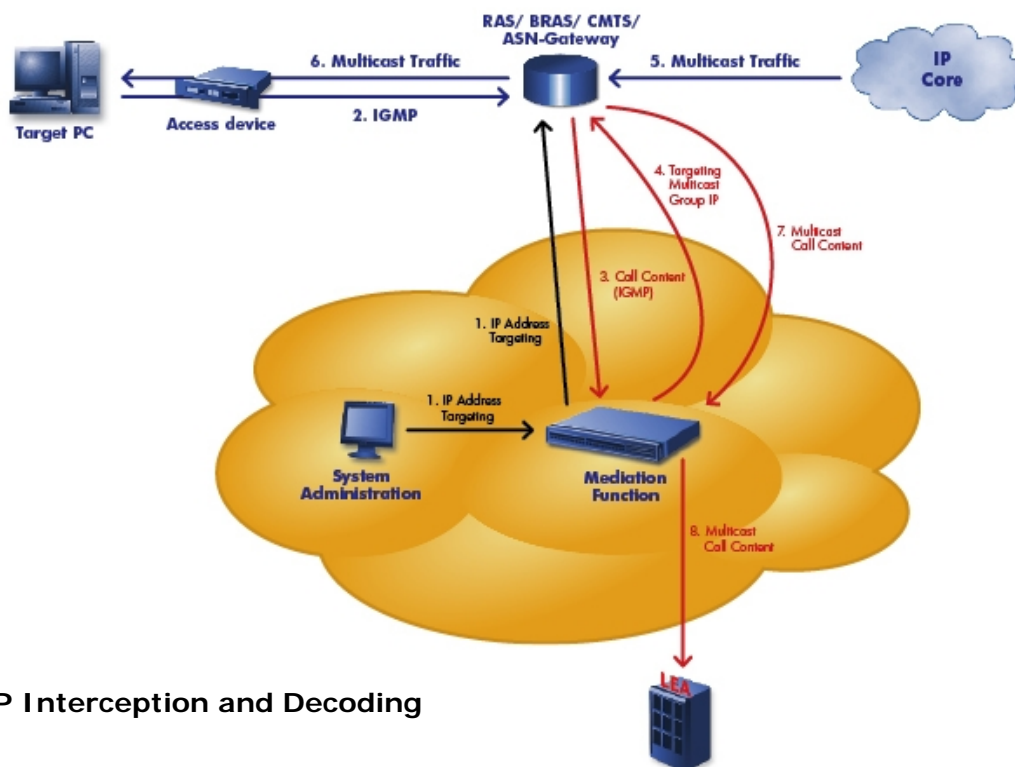
In order to address these multicast challenges, it is important to first understand how a client becomes a member of Multicast Group. A client needs to register with all Multicast Groups it wishes to be part of. This registration is part of the process of building the spanning tree for routing multicast datagrams. Registration with a Multicast Group is generally performed using Internet Group Management Protocol (IGMP) messages. The protocol enables a client to join and leave a Multicast Group. The Multicast Group is referred to by its IP Multicast address.

A possible solution for the problem of intercepting multicast traffic: when monitoring an IP target, automatically intercept all requests for joining and leaving a Multicast Group. With proper and timely decoding of these messages, more IP addresses (those of the Multicast Groups of which the client is a member) can be associated with the initial IP Target under inspection.

However, there is a limitation to this solution: IGMP traffic is usually not forwarded outside of the local LAN. Instead, protocols such as PIM, MOSFP, and MBGP are used between routers to build the multicast spanning tree outside the local LAN. These protocols are of little value to interception because they do not include the original IP address of the subscriber who requested to join the Multicast Group. Only the IGMP protocol includes the subscriber's IP address. Consequently, a practical solution requires access to the first access routers handling subscriber traffic.

A Typical Interception Solution

The following illustration depicts a typical interception solution, combining the power of interfacing with different network elements with passive analysis of IGMP messages.



IGMP Interception and Decoding

The target host is connected to the Internet network through DSLAM, modem, cable modem, or another access device. The above illustration shows an active solution where target traffic is accessed by provisioning its IP address to the first router to which it is connected (1), whether it is a RAS, BRAS, CMTS, or WIMAX ASN gateway. The IP address can be provisioned directly or by passively accessing and decoding RADIUS access messages or DHCP lease requests. Interception of non-multicast traffic from and to the target and multicast traffic from the target now begins.

When the target joins the Multicast Group, the target sends an IGMP message to the router indicating that it has joined the Multicast Group (2). The message carries the IP address of the Multicast Group. The source IP address of these IGMP packets will be the IP address of the target that is tapped. Therefore, the IGMP packets are replicated and sent to Mediation Function (3). The Mediation Function inspects packets and decodes IGMP packets. It extracts the IP address of the Multicast Group and provisions it to the router as a secondary IP address of the target (4). From that moment on, all of the Multicast Group's traffic that reaches the router (5) and is sent to the client (6) is also replicated by the router to the Mediation Function (7) and sent to the Law Enforcement Agency (8).

A similar process occurs when the client sends an IGMP message indicating it has left the Multicast Group. The IP of the Multicast Group is removed from the intercepted IP list of the router.

Verint Lawful Interception Solutions

Verint's industry-leading STAR-GATE™ and RELIANT™ solutions allow communication service providers and law enforcement agencies to access target traffic in virtually any network scenario. Verint mediation devices include optional support for IGMP decoding. This capability, combined with superior interoperability with router vendors and the dynamic IP address analysis capabilities offered by the Verint IP-Probe, is an essential element of these flexible, cost-effective solutions, designed to intercept every packet generated by or sent to the monitored targets.

About STAR-GATE

STAR-GATE is a comprehensive solution portfolio that promotes seamless service provider compliance with lawful interception and data retention mandates. STAR-GATE streamlines compliance-related activities and reduces the complexity of a rapidly expanding array of regulations, standards, and communication technologies. With STAR-GATE, service providers can access communications on virtually *any* type of network, retain communication data for as long as required, and query and deliver content and data in compliance with CALEA, ETSI, and other standards and regulations.

Designed to manage vast numbers of targets, concurrent sessions, call data records, and communications, STAR-GATE transparently accesses targeted communications without alerting subscribers or disrupting service. A single point of administration facilitates intercepts and queries on any combination of communication networks, and an intelligent wizard dramatically simplifies administration.

This portfolio of scalable, turnkey solutions helps service providers of virtually any size comply with lawful interception and data retention requirements efficiently and cost effectively.

About RELIANT

The RELIANT solution portfolio helps law enforcement agencies collect, retain, analyze, and distribute intercepted voice and data communications for conducting highly productive investigations and gathering evidence. RELIANT features:

- Interception of traditional telephony and fax transmissions and a wide range of broadband services and protocols, including both 3G and packet data messages
- Advanced analytic tools
- Active interception through a large number of switches, as well as passive collection of both telephony and IP transmissions
- Support for cross-departmental sharing of information
- Compliance with international delivery standards, including ETSI, CALEA, and SORM, and specific national regulations regarding interception and evidence
- A robust architecture and multi-level security

For more information, call 1-631-962-9600, email marketing.lis@verint.com, or contact your local Verint representative.