Multicasting White Paper

**Executive Summary**
Multicasting is a type of communication between computers in a network that enables a computer to send one stream of data to many interested receivers without interrupting computers that are not interested. For these reasons, multicasting has become the favoured transmission method for most multimedia and triple play applications, which are typically large and use up a lot of bandwidth.

Multicasting not only optimises the performance of your network, but also provides enhanced efficiency by controlling the traffic on your network and reducing the loads on network devices.

This white paper includes the following sections:

**A. What is multicasting?**
Provides an overview and introduction to multicasting.

**B. How do multicast addresses work?**
Provides more detail about multicast addresses and architecture.

**C. How is multicast traffic managed?**
Discusses some of the protocols that facilitate the transmission of multicast traffic across and within networks.

**D. How is multicast traffic routed?**
Discusses some of the multicast routing protocols used in networks.

**E. How does QoS fit with multicasting?**
Explains how QoS works with multicasting.

**F. How do Allied Telesis products support multicasting?**
Outlines how Allied Telesis products provide multicasting support.
Multicasting White Paper

Contents

A. WHAT IS MULTICASTING? 3
   Introduction 3
   What is multicasting? 3
   What are the benefits of multicasting? 4

B. HOW DO MULTICAST ADDRESSES WORK? 5
   How are IPv4 multicast addresses organised? 5
   How are IPv6 multicast addresses organised? 5
   How are IPv4 multicast addresses mapped to MAC multicast addresses? 6
   How are IPv6 multicast addresses mapped to MAC multicast addresses? 8

C. HOW IS MULTICAST TRAFFIC MANAGED? 10
   Multicast host-router signalling 10
   IPv4 - Internet Group Management Protocol (IGMP) 10
       IGMPv2 11
       IGMPv3 11
       IGMP Snooping 11
   IPv6 - Multicast Listener Discovery (MLD) 11
       MLD snooping 12

D. HOW IS MULTICAST TRAFFIC ROUTED? 13
   Multicast Routing Protocols 13
       Dense mode protocols 13
       Sparse mode protocols 14
       Interoperability 14

E. HOW DOES QOS FIT WITH MULTICASTING? 16

F. HOW DO ALLIED TELESIS PRODUCTS SUPPORT MULTICASTING? 17
   Hardware Support 17
   Software Support 17
A. What is Multicasting?

Introduction

Hello, … how a …re ….yο …u?

Is there anything more frustrating than a telephone line with a time delay or live video footage with breaks and pauses?

The phenomenal complexity of the applications used to create film, multimedia and triple play applications, which combine sound, graphics, text and video means that these files are large. Their size and complexity makes them tricky to send across networks without interruptions, without taking up huge amounts of network bandwidth, and without interrupting other data being sent on the network. However, multicasting is proving to be a useful and cost effective alternative to traditional methods of sending large multimedia files across networks. Multicasting has the unique ability to send out a single data stream to multiple clients and has become the favoured transmission method for most multimedia applications.

Multicasting is able to provide broadcast-quality television channels over IP-based networks to home users, and is also enabling service providers to supply triple play solutions—integrated voice, video and data—over IP-based xDSL or fibre networks.

Multicasting is already successfully used in a variety of locations, including hospitals, hotels, schools and universities. Hospitals can use multicasting to provide television and video channels to patients’ bedsides. Multicasting can also enable doctors and students to watch surgery being performed live while in other locations, either within the hospital or, in an external lecture situation. More and more hotels are also using multicasting to provide television and movie channels in guest rooms. Schools and universities can also use multicasting to provide live links to lectures that are delivered either across campus or from another campus location. In addition, internal technical support departments can use multicasting file transfer software to simultaneously send software updates to multiple users at a site.

What is multicasting?

There are three types of communication between computers in a network:

Unicast - one computer talks directly to another computer
Broadcast - one computer talks to all computers
Multicast - one computer talks to a select group of others

In a conventional Ethernet network, most Internet Protocol (IP) packets are sent using unicast (host-to-host) transmission. Every computer in a network can transmit and receive packets, which in unicast transmission are labelled with the address of the receiving computer. Each computer listens to all the other packets that are sent in the network and looks for packets that are addressed to itself. When a computer encounters a packet that is addressed to itself, it interrupts the processor and hands the packet to the operating system to process.

Unicasting is great for communicating directly with one or a few other computers. However if you want to communicate with a number of computers, unicasting becomes inefficient because a copy of each packet must be sent to every receiving unicast address. Unicasting uses up bandwidth fast, especially when sending large multimedia files, which already take up a lot of
Multicasting optimises the performance of your network. Because only one multicast data stream is sent out, multicasting preserves bandwidth on your network and eliminates traffic redundancy. In contrast, the unicast environment sends out a separate copy of the data to each receiver.

Multicasting also provides enhanced efficiency by controlling the traffic on your network and reducing load on network devices. The clients on your network are able to decide whether or not to listen to a multicast address, so packets are only sent to where they are required.

In addition, multicasting is scalable across different sized networks, but is particularly suited to WAN environments. It gives people in different locations access to streaming data files, like a video, film or live presentation without taking up excessive bandwidth or broadcasting the data to all users on the network.
B. How do Multicast Addresses Work?

Because multicast addresses identify a transmission session rather than a specific physical destination or host, all of the receivers in a multicast group are identified by a single IP address. This section outlines how multicast IP and MAC addresses are structured.

How are IPv4 multicast addresses organised?

IPv4 multicasting uses class D addresses. A class D address starts with 1110 higher order bits in the first octet, followed by a 28-bit group address. The last 28 bits of a class D address are unstructured, unlike the class A, B and C IP addresses. These 28 bits identify the multicast group identity, which is a single address in the range of 224.0.0.0 to 239.255.255.255.

Some IPv4 multicast addresses are reserved for particular purposes. These addresses are assigned by the Internet Assigned Numbers Authority (IANA). Table 1 outlines some of the well-known IPv4 multicast addresses.

<table>
<thead>
<tr>
<th>IPv4 Address</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.0.0.1</td>
<td>All hosts on a subnet</td>
</tr>
<tr>
<td>224.0.0.2</td>
<td>All routers on a subnet</td>
</tr>
<tr>
<td>224.0.0.4</td>
<td>All Distance Vector Multicast Routing Protocol (DVMRP) routers</td>
</tr>
<tr>
<td>224.0.0.5</td>
<td>All Open Shortest Path First (OSPF) routers</td>
</tr>
<tr>
<td>224.0.0.6</td>
<td>All OSPF designated routers</td>
</tr>
<tr>
<td>224.0.0.9</td>
<td>All Routing Information Protocol version 2 (RIPv2) routers</td>
</tr>
<tr>
<td>224.0.0.13</td>
<td>All Protocol-Independent Multicast (PIM) routers</td>
</tr>
</tbody>
</table>

Table 1: Well-known IPv4 multicast addresses

How are IPv6 multicast addresses organised?

An IPv6 multicast address is an IPv6 address that has the following higher order bits in the first octet: 11111111 in binary notation, or FF in hexadecimal notation. In the second octet, the first three bits are reserved and are set to 0. The next bit in the octet defines the lifetime of the multicast address. A multicast address that has the lifetime parameter set to 0 is permanent and an address that has the lifetime parameter set to 1 is temporary. The next four bits in the octet indicate the scope of the multicast address. The scope can be set to the following parameters: 1 = node-local scope, 2 = link-local scope, 5 = site-local scope, 8 = organisation-local scope, E = global scope.
For example, a multicast address with the prefix FF02 is a permanent multicast address with a link local scope. By setting the scope, it is possible to limit how far a packet can go in a much more reliable way than with IPv4. Routers must know when links cross scope boundaries in order to implement this properly, which is easy for node-local and link-local scope, but requires configuration for site-local and organization-local scope. The following figure outlines the IPv6 multicast address format.

![IPv6 multicast address format](image)

Some IPv6 multicast addresses are reserved for particular purposes. Table 2 outlines some of the well-known IPv6 multicast addresses.

<table>
<thead>
<tr>
<th>IPv6 Address</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>FF02:0:0:0:0:0:1</td>
<td>All nodes (hosts and routers) multicast group</td>
</tr>
<tr>
<td>FF02:0:0:0:0:0:2</td>
<td>All routers multicast group</td>
</tr>
<tr>
<td>FF02:0:0:0:0:0:9</td>
<td>All Routing Information Protocol version 2 (RIPv2) routers</td>
</tr>
<tr>
<td>FF02:0:0:0:0:0:D</td>
<td>All Protocol-Independent Multicast (PIM) routers</td>
</tr>
</tbody>
</table>

Table 2: Well-known IPv6 multicast addresses

**How are IPv4 multicast addresses mapped to MAC multicast addresses?**

All Ethernet packets have a 48-bit destination MAC address field. For multicast IP packets, the destination MAC addresses are automatically determined from the destination IP addresses. This avoids the need for the Address Resolution Protocol (ARP) to map multicast IP addresses to MAC addresses. All multicast MAC addresses fit into the range of 01:00:5e:00:00:00 to 01:00:5e:7fff:ff. Figure 3 shows how multicast IPv4 addresses are mapped to MAC addresses.

---

6 The complete IPv6 address model is specified in RFC3513 – IPv6 Addressing Architecture
The multicast MAC address prefix is always 01:00:5e, which identifies the frame as a multicast frame, and the next bit is always 0. This leaves 23 bits for the remainder of the MAC multicast address. Because IPv4 multicast addresses are 28 bits long (32 bits minus the designated 4 bits for the class D prefix 1110) and MAC multicast addresses only have a remaining 23 bits, the mapping cannot be one to one. Therefore only the 23 least significant bits of the IPv4 multicast address are placed in the frame and the remaining five high-order bits are ignored. This means that 32 different multicast addresses can be mapped to the same MAC address, so the address is not unique.

Because the multicast MAC address is not unique, a computer set up to receive multicasts needs to filter out any extra multicast packets that are sent with the same MAC multicast address.

To recap, the high order nine bits of the IPv4 multicast address are not mapped to the MAC multicast address. Because the top nine bits of the IPv4 multicast address are not used in the MAC multicast address, the mapping correlates 32 IPv4 multicast addresses into one MAC multicast address. Figure 4 shows how the IPv4 host group addresses 224.8.8.5 and 229.136.8.5 have the same MAC address of 01-00-5E-08-08-05.

Figure 3: Mapping an IPv4 multicast address to a MAC multicast address

The multicast MAC address prefix is always 01:00:5E, which identifies the frame as a multicast frame, and the next bit is always 0. This leaves 23 bits for the remainder of the MAC multicast address. Because IPv4 multicast addresses are 28 bits long (32 bits minus the designated 4 bits for the class D prefix 1110) and MAC multicast addresses only have a remaining 23 bits, the mapping cannot be one to one. Therefore only the 23 least significant bits of the IPv4 multicast address are placed in the frame and the remaining five high-order bits are ignored. This means that 32 different multicast addresses can be mapped to the same MAC address, so the address is not unique.

Because the multicast MAC address is not unique, a computer set up to receive multicasts needs to filter out any extra multicast packets that are sent with the same MAC multicast address.

To recap, the high order nine bits of the IPv4 multicast address are not mapped to the MAC multicast address. Because the top nine bits of the IPv4 multicast address are not used in the MAC multicast address, the mapping correlates 32 IPv4 multicast addresses into one MAC multicast address. Figure 4 shows how the IPv4 host group addresses 224.8.8.5 and 229.136.8.5 have the same MAC address of 01-00-5E-08-08-05.
If two multicast streams on the same network share the same MAC address, usually the higher-layer protocols interpret which packets are for the application.

**How are IPv6 multicast addresses mapped to MAC multicast addresses?**

In IPv6, the multicast MAC address header is always 33.33 and the remaining 32 bits are mapped directly from the lower 32 bits of the IPv6 multicast address. The IPv6 address has an extra 88 bits that are ignored when mapping to MAC addresses. These extra bits could result in $2^{88}$ IPv6 addresses using the same MAC address. A computer set up to receive multicasts needs to filter out any extra multicast packets that are sent with the same MAC multicast address. Usually the higher-layer protocols interpret which packets are for the application. See Figure 5 for an example of how IPv6 multicast addresses are mapped to MAC addresses.
Figure 5: Mapping an IPv6 multicast address to a MAC multicast address
C. How is Multicast Traffic Managed?

On a single physical segment in a network, multicasting is relatively simple. The sender provides a specific multicast destination address and the device driver converts this address to the corresponding MAC address and sends the package out on the network. The receiving devices on the network must indicate if they want to receive the multicast data.

However, complications arise when multicasting is extended beyond a single physical network and multicast packets pass through routers. All devices that participate in the multicast, such as the server, the host, the router and the switch, must coordinate their operations. Establishing a path between source and destination devices and forwarding multicast data through a network are also issues that need to be considered when managing multicast traffic.

Multicast traffic is transmitted from the source to a multicast group by means of a distribution tree, which connects all of the hosts in the group. There are a number of different multicast routing protocols that use different techniques to construct these trees, but before the multicast traffic can travel on the network, routers need to know which hosts want to join a multicast group.

Multicast host-router signalling

There are a number of protocols that facilitate the transmission of multicast traffic across and within networks, but the first step in the process is to define who receives the multicast data.

IPv4 - Internet Group Management Protocol (IGMP)

IGMP\(^1\) is used with IPv4 to automatically control and limit the flow of multicast traffic through a network. IGMP manages multicast groups and traffic through the use of query and report messages. Routers periodically send out IGMP query messages to interfaces on their network to see if any group members exist. These messages are not forwarded on to other networks. If a host wants to join a multicast group, it sends out an IGMP report message in response to the query and depending on the reports that a router receives from the interfaces on a network, it works out where to forward the multicast packets.

If a router does not receive a response to its query messages after a number of queries, it assumes that there are no group members on that network. Hosts do not have to wait for a query before joining a multicast group, they can send out a message requesting to receive a multicast stream.

Note: Routers are not interested in the specific hosts that are requesting multicast data; they are only interested in the interfaces in a network that want to receive multicast traffic because multicast traffic is sent to an entire cable segment, not a single host.

To maintain multicast groups and ensure that the hosts on a network still want to receive the multicast data, routers periodically send membership queries to the all-hosts group address (224.0.0.1). Only one member per group responds to the query, saving bandwidth on the network and processing by the hosts.

IGMPv1 does not define any special leave mechanism, so hosts can leave a multicast group at any time without notifying the router. This can mean that bandwidth is taken up sending multicast data when it is not actually wanted.

1. IGMP version 1 is defined in RFC 1112 “Host Extensions for IP Multicasting.”
IGMPv2

Most of the differences between version 1 and version 2 of IGMP deal with the limitations of joining and leaving multicast groups in version 1. IGMPv2 includes a procedure for electing the multicast querier for each segment of a network based on IP addresses. Initially every router believes that it is the querier for all the interfaces that are multicast enabled and transmits query messages. However, if a router receives a query message from a numerically lower IP address, it stops being the querier on that interface and the router with the numerically lower IP address takes over.

In IGMPv2, a host can receive both general and group specific queries. A group specific query enables routers to query membership in one group instead of all groups, which speeds up the process of finding out if any members are left in a specific group without asking all groups for a report.

For faster pruning, IGMPv2 also includes explicit leave messages. When someone ends a multicast session, the host transmits a leave group message to the all-routers (224.0.0.2) group, with the group field indicating the group that the host is leaving. When the member leaving is the last member of the group, the leave latency for the group on that segment of the network is reduced. However, there is still a time delay of around two seconds before the IGMPv2 router stops forwarding traffic, because it still sends a group-specific query to check that the host that sent the leave message was the last host connected to the group.

IGMPv3

IGMPv3 provides support for source filtering. Source filtering enables a host to report interest in receiving packets from specific source addresses ‘only’, or from ‘all but’ specific source addresses. This information is used by multicast routing protocols to avoid delivering multicast packets from specific sources to networks where there are no interested receivers.

IGMP Snooping

IGMP snooping enables switches to intelligently forward multicast packets to hosts that want to receive the packets instead of sending them to all ports on a virtual LAN (VLAN). IGMP snooping can passively snoop on IGMP Query, Report and Leave packets that are sent between IP multicast routers and hosts to learn the multicast group membership of the packets. IGMP snooping checks packets as they move around a network, picking out group registration information and then configuring the multicast stream so that multicast traffic is only sent to ports that have members of the particular multicast group or groups. IGMP snooping does not generate any extra network traffic and significantly reduces the multicast traffic passing through your switches.

IPv6 - Multicast Listener Discovery (MLD)

In the same way that IGMP manages multicast groups for IPv4, MLD works with IPv6 to define who receives the multicast data in a network. MLD automatically controls the flow of traffic in a network by using multicast queriers and hosts. A querier is a network device that sends query messages to work out which network devices are members of a given multicast group. A host is a receiver that sends report messages to inform the querier of its membership in a multicast group. Queries and hosts use MLD reports to join and leave multicast groups and to begin receiving group traffic.

---

2 IGMPv2 is defined in RFC 2236 “Internet Group Management Protocol, Version 2”. Allied Telesis products are compliant with RFC 2236.

3 IGMPv3 is specified in RFC 3376 – “Internet Group Management Protocol, Version 3”.

4 See RFC 2710 – Multicast Listener Discovery (MLD) for IPv6 for more information. The Allied Telesis MLD implementation is based on Multicast Listener Discovery Version 2 (MLDv2) for IPv6 - draftvidia-mdlv2-00.txt.
MLD has three types of messages:

- **Query messages** - these include:
  - General query messages
  - Group specific messages
  - Multicast address specific messages
- **Report messages**
- **Done messages**

When MLD sends a general query, the multicast address field is set to 0 and the general query learns which multicast addresses have listeners on an attached link. Both group-specific and multicast-address-specific queries are the same—a group address is a multicast address. MLD report messages have their multicast address field set to that of the specific IPv6 multicast address that the sender is listening to. MLD done messages let the source know that the receiver no longer wants to receive the multicast data. MLD done messages have their multicast address field set to the specific IPv6 multicast address to which they are no longer listening.

Like IGMPv2, MLD version 1 pauses for around two seconds when group members want to leave a multicast session. When a host using MLDv1 sends a leave message, the router sends query messages to check that the host was the last MLDv1 host that was connected to the group before it stops forwarding traffic. MLDv2 provides the same features as IGMPv3, namely it provides support for source filtering.

**MLD snooping**

Like IGMP snooping, MLD snooping enables switches to forward multicast data to hosts that want to receive the data rather than to all ports regardless of whether or not they want to receive the data.

---

3 The recommendations for IGMP and MLD snooping are defined in Internet Draft draft-ietf-magma-snoop-10.txt - Considerations for IGMP and MLD Snooping Switches.
D. How is Multicast Traffic Routed?

Because a multicast address identifies a particular transmission session rather than a specific physical destination, routing multicast traffic is more complex than routing unicast or broadcast traffic. As there may be a large number of receivers wanting to receive a multicast stream, and the source does not need to know all the addresses of the receiving devices, the network routers have to translate multicast addresses into host addresses. The basic principle of multicast routing is that routers must interact with each other to exchange information about neighbouring routers.

In order to distribute the multicast data, the designated routers need to establish distribution trees and connect all of the members of a multicast group. The distribution trees specify the forwarding path from the source to each of the members of the multicast group. There are a number of different distribution trees, but the two most basic types are source specific trees and shared or centre specific trees.

Source specific trees find the shortest path from the source to the receivers. Source specific trees build multiple delivery trees, which emanate from the subnetworks that are directly connected to the source.

Shared or centre specific trees use distribution centres and build a single tree that is shared by all members of a group. In the shared tree approach, multicast traffic is sent and received over the same path regardless of the sources of the data.

Multicast routing protocols

Multicast routing protocols facilitate the exchange of information between routers and are responsible for constructing distribution trees and forwarding multicast packets. There are a number of different routing protocols, but they generally follow one of two basic approaches—dense mode or sparse mode.

Dense mode protocols

Dense mode protocols are based on the assumption that there are a number of multicast group members densely distributed across a network. Because of this, these protocols periodically flood the network with multicast traffic to establish and maintain the distribution tree. Dense mode protocols are best suited to environments where there is a number of hosts that want to or must receive the multicast data and the bandwidth to cope with the flooding of the network.

Distance Vector Multicast Routing Protocol (DVMRP)

There are a number of IPv4 dense mode protocols, but the oldest and most widely known is DVMRP. DVMRP uses reverse path flooding, so when a router receives a packet, it floods the packet out of all paths to reach all LANs except the one that leads back to the source of the packet. If a LAN does not want to receive packets from a particular multicast group, the router sends prune messages back up the distribution tree to stop any other packets from travelling to where there are no members. DVMRP has its own unicast routing protocol, based on hop counts, that determines which interface leads back to the data source, so the paths of multicast and unicast data may not be the same.

---

6 DVMRP is described in RFC 1075 - Distance Vector Multicast Routing Protocol. Allied Telesis products are compliant with draft-ietf-idmr-dvmrp-v3-10.txt, which comes after RFC 1075.
Protocol Independent Multicast Dense Mode (PIM-DM)

PIM-DM is both an IPv4 and an IPv6 routing protocol. PIM-DM operates in a similar fashion to DVMRP and is best suited to situations where there are numerous members for each multicast group, densely located. Like DVMRP, PIM-DM floods packets out to all routers in a network and then prunes routers that do not have group members attached. Protocol Independent means that it can use the existing unicast routing table content instead of building and maintaining its own separate multicast route table. It does not matter which unicast routing protocol is being used in the network to populate the existing unicast routing table.

Sparse mode protocols

The sparse mode protocols are based on the assumption that group members wanting to receive multicast data are sparsely distributed across a network and that bandwidth is not necessarily widely available. Because the group members are spread sparsely throughout the network, flooding would waste bandwidth and could cause performance problems. Sparse mode protocols therefore are more selective about how they distribute multicast data. They start with empty distribution trees and only add branches when they receive join requests. Core Based Trees and Protocol Independent Multicast Sparse Mode (PIM-SM) are two of the more common sparse mode protocols.

Protocol Independent Sparse Mode (PIM-SM)

PIM-SM is both an IPv4 and an IPv6 routing protocol. PIM-SM has been designed for environments where the receivers are widely distributed. PIM-SM uses a rendezvous point that sendsers direct their information to and receivers request information from. So, when a receiver wants to receive a multicast data stream, it registers with the rendezvous point and once the data starts to flow from the sender, the rendezvous point sends the data on. The routers automatically optimize the path to get rid of unnecessary hops. Because PIM-SM is protocol independent, it uses the data contained in the existing unicast routing protocol.

Interoperability

Both IPv4 and IPv6 implement RFC 2715 "Interoperability Rules for Multicast Routing Protocols". For IPv4, this means that PIM SM, PIM DM and DVMRP can operate at the same time on different interfaces, and for IPv6, this means PIM SM and PIM DM can operate at the same time on different interfaces.

---

7 Allied Telesis products using software release 2.5.1 or higher are compliant with Internet draft Protocol Independent Multicast – Dense Mode (PIM-DM) draft-ietf-pim-dm-new-v2-01.txt.
8 Core Based Trees are described in RFC 2201.
10 Allied Telesis products using software release 2.5.1 or higher are compliant with the following Internet Draft - Protocol Independent Multicast - Sparse Mode (PIM-SM) draft-ietf-pim-sm-v2-new-05.txt, which comes after RFC 2362.
11 Allied Telesis products using software release 2.5.1 or higher are compliant with RFC 2715.
Figure 6: Dense Mode vs. Sparse Mode

With dense mode routing, the source broadcasts data everywhere on the network and then prunes back when the data is unwanted. With sparse mode routing, the interested receiver requests the data from the source or the first router that receives the multicast.
E. How does QoS fit with Multicasting?

The most efficient and common method of delivering multicast data streams is User Datagram Protocol (UDP). UDP is a Layer 4 IP protocol that transmits packets from the source to receiver without requiring any acknowledgement from the receiver and without retransmitting packets if they are lost in the transmission. Because multimedia files must be transmitted in a continuous, real-time stream, there is no time to retransmit any lost packets, so any packet loss or delay caused by congestion affects the quality of the received data stream.

Applications that receive the multicast streams usually have some buffering built in so that minor delays or losses can be smoothed out. However, prolonged loss due to a congested network link or device will eventually disrupt the quality of the data stream that is seen by the end user in the form of broken video and/or voice streams.

To maintain an uninterrupted flow of data or Quality of Service (QoS), it is essential to avoid packet loss and delay in the multicast data stream. Applying QoS and giving multicast data packets priority over other packets when processed by the network switch or router can achieve this.

Allied Telesis QoS functions can classify and prioritise multicast packets, maintaining low latency and jitter, even when the there is congestion due to high levels of other non-real-time traffic. With QoS, bandwidth can be guaranteed for the multicast data, and other traffic can be bandwidth-limited so it does not compete with the essential multicast stream.
F. How do Allied Telesis Products Support Multicasting?

Most Allied Telesis Layer 3 switch and router products provide multicast support for both IPv4 and IPv6.

**Hardware support**

All Allied Telesis Layer 3 switches and routers provide hardware support for Layer 2 switching of multicast traffic. In addition, all Allied Telesis Layer 3 switches perform Layer 3 switching of multicast traffic, providing 100% wire speed forwarding of multicast data between VLANs from and to any number of ports.

**Software support**

Allied Telesis' routers provide Layer 3 routing of multicast traffic in their software.

Allied Telesis is able to provide a variety of multicast protocols for both IPv4 and IPv6. For IPv4, Allied Telesis supports IGMPv2, DVMRP, PIM-SM and PIM-DM. For IPv6, Allied Telesis supports MLDv2, PIM-SM and PIM-DM. Migrating from IPv4 to IPv6 is a simple process with Allied Telesis products, especially for network managers who are familiar with Allied Telesis' IPv4 implementation. Currently, all of the Allied Telesis IPv6 multicast functions are software based.

Allied Telesis' flexible options for multicast support are providing customers with an affordable and bandwidth efficient method of delivering multimedia and triple play applications.

For more information, please contact your local Allied Telesis representative.