UV REALTIME
TECHNICAL DOCUMENTATION

VERSION 1.9.1.0, DAN WILSON, FEBRUARY 2012

INTRODUCTION

This document is targeted at the intermediate to advanced computer user who would like more information on the U-Verse® implementations of IP Multicast, IGMP, and the manner in which UV Realtime gathers this information from the STB units.

I make no representation that this information is correct or complete. This is only what my research has shown and should not be used as a general reference for IP Multicast, IGMP, or the U-Verse® implementation of SSDP.

The first several sections of this document retain the description of IP Multicast, IGMP, and UV Realtime's interaction from version 1.2.x.0. These are here for historical and educational purposes, but UV Realtime, as of version 1.3.0.0, uses a different method to gather information from the STBs. This description is covered after these sections, in the section entitled "U-Verse®'s Pseudo-SSDP".

The Stream Analyzer feature introduced in v1.6.0.0 is covered in a later section.

IP MULTICAST OVERVIEW

IP multicast is a mechanism to send IP packets to a group of interested hosts without sending multiple copies of the data from the source. The source sends a single packet, which is then duplicated by the routers along the path to the hosts that have joined the group. Multicast is implemented at layer 3 of the OSI model and is part of the IP specification. Both IPv4 and IPv6 support multicast, but this document will deal strictly with the IPv4 implementation.

MULTICAST ADDRESS SPACE

Multicast address space is defined by IANA as 224.0.0.0/4. Most of this address space is only loosely defined or is reserved by IANA, so it will not be discussed exhaustively here. There are two address spaces we're interested in from the U-Verse® perspective:

224.0.0.0/24 This address space is for multicast housekeeping messages on the local subnet. This address space is never forwarded by routers.

239.0.0.0/8	This address space is locally administered within any organizational scope. It is the multicast equivalent of the 192.168.0.0/16, 172.16.0.0/16, and 10.0.0.0/8 unicast private address spaces defined by IANA. This is the subnet that AT&T is using for U-Verse®.

LAYER 2 DELIVERY

When an IP multicast packet directed to a certain group needs to be transmitted on Ethernet, there is a translation mechanism to formulate the destination MAC address from the destination IP address. This translation is as follows:

- The first 3 octets of the destination MAC address are assigned as 01:00:5E
- The next bit in the MAC address is assigned to be 0.
- The final 23 bits of the MAC address are copied from the lower order 23 bits of the IP multicast address.

This mechanism can result in some overlap of the multicast IP space in layer 3 (which can comprise up to 28 unique bits) when transmitted in the layer 2 space (where only 23 unique bits are available). This means that there may be a (rare) occasion where the end host's NIC may have to specifically look at the layer 3 IP address to determine if the packet belongs to a group it's interested in, rather than simply relying on the layer 2 MAC address.

Consumer-level layer 2 switches on the network typically do not treat IP multicast traffic any differently than broadcast traffic. Since the destination MAC address represents a group of hosts, the switch has no choice but to forward an IP multicast frame to all ports (except the ingress port). As U-Verse® can bring more than 20 Mbps of multicast traffic into the local network, switches can be very taxed, and this much multicast/broadcast traffic can easily overwhelm devices that utilize slower Ethernet hardware. The router used for U-Verse® installations (the 2Wire 3800HG-V) mitigates this problem using IGMP snooping, covered later in this document.

EFFECT ON UPPER PROTOCOLS

Because IP multicast is unidirectional, connection-oriented transport protocols like TCP cannot generally be used. U-Verse® sends all IPTV multicast transmissions via UDP at layer 4. As such, corrupted, late, or missing packets cannot be retransmitted, and will result in a video glitch.

INTERNET GROUP MANAGEMENT PROTOCOL (IGMP) OVERVIEW

For a host to join or leave a multicast group, the host must have the ability to tell a router on the local network that it wishes to receive multicast traffic from that group. The router, in turn, must inform upstream routers to begin sending traffic from that multicast group to it so that it can be forwarded to the host that wants to receive it. A protocol exists for the host to inform the router of its wish to join/leave a group, that protocol is Internet Group Management Protocol (IGMP).

Several versions of IGMP exist. U-Verse® uses IGMP version 3, defined in RFC 3376. The primary difference between version 3 and the more commonly deployed version 2 is that version 3 allows a host to specify particular source addresses that it will accept or reject the multicast traffic from.

There are two main packets in the IGMP protocol that are of interest: The query packet and the membership report packet.

IGMP QUERY PACKET

One router on a subnet assumes the role of a querier, and is responsible for keeping track of which hosts have joined which multicast groups. In the U-Verse® system, the 2Wire 3800HG-V functions as the querier. By RFC 3376 specifications, there can only be one querier on a subnet. Other routers must stop issuing query packets if they discover that another querier is already on the subnet.

An IGMP query packet asks all hosts to report their current IP multicast membership status to the router. IGMP Membership queries are multicast to 224.0.0.1 (all multicast-capable hosts).

IGMP QUERY PACKET STRUCTURE

An IGMP query packet (the IGMP layer only), is as follows:

	Bits 0-7	Bits 8-15	Bits 16-23	Bits 24-31
Bit Offset 0	Type = 0x11	Max Resp Code	Checksum	
Bit Offset 32	Multicast Group IP Address being Queried for Membership			
Bit Offset 64	Resv / S / QRV	QQIC	Number of Sources	
Bit Offset 96	Source Address 1 (if Number of Sources >0)			
Bit Offset 128	Additional Source Addresses …			

- **Type**: Defined in the IGMP protocol as 0x11 for a query packet.
- **Max Resp Code**: The Max Resp Code field specifies the maximum time allowed before sending a responding report. The actual time allowed, called the Max Resp Time, is represented in units of 1/10 second and is derived from the Max Resp Code as follows:
  - If Max Resp Code < 128, Max Resp Time = Max Resp Code
  - If Max Resp Code >= 128, Max Resp Code represents a floating-point value with the most significant bit = 1, the next 3 bits representing an exponent, and the least significant 4 bits representing a mantissa, with the final value of Max Resp Code = (mant | 0x10) << (exp + 3)
- **Checksum**: The 16-bit one's complement of the one's complement sum of the whole IGMP message (the entire IP payload). For computing the checksum, the Checksum field is set to zero. When receiving packets, the checksum MUST be verified before processing a packet.
- **Multicast Group IP Address**: The Group Address field is set to zero (0.0.0.0) when sending a General Query, and set to the IP multicast address being queried when sending a Group-Specific Query or Group-and-Source-Specific Query.
- **Resv (Reserved)**: The Resv field is set to zero on transmission, and ignored on reception. Res is 4 bits long.
- **S Flag (Suppress Router-Side Processing)**: When set to one, the S Flag indicates to any receiving multicast routers that they are to suppress the normal timer updates they perform upon hearing a Query. It does not, however, suppress the querier election or the normal "host-side" processing of a Query that a router may be required to perform as a consequence of itself being a group member. The S flag is 1 bit.
- **QRV (Querier's Robustness Variable)**: If non-zero, the QRV field contains the [Robustness Variable] value used by the querier, i.e., the sender of the Query. If the querier's [Robustness Variable] exceeds 7, the maximum value of the QRV field, the QRV is set to zero. Routers adopt the QRV value from the most

recently received Query as their own [Robustness Variable] value, unless that most recently received QRV was zero, in which case the receivers use the default [Robustness Variable] value specified in section 8.1 of RFC 3376 or a statically configured value.

- **QQIC (Querier's Query Interval Code)**: The Querier's Query Interval Code field specifies the query interval used by the querier. The actual interval, called the Querier's Query Interval (QQI), is represented in units of seconds and is derived from the Querier's Query Interval Code as follows:
    - If QQIC < 128, QQI = QQIC
    - If QQIC >= 128, QQIC represents a floating-point value with the most significant bit = 1, the next 3 bits representing an exponent, and the least significant 4 bits representing a mantissa, with the final value of Max Resp Code = (mant | 0x10) << (exp + 3)
- **Number of Sources**: The Number of Sources (N) field specifies how many source addresses are present in the Query. This number is zero in a General Query or a Group-Specific Query, and non-zero in a Group-and-Source-Specific Query. This number is limited by the MTU of the network over which the Query is transmitted. For example, on an Ethernet with an MTU of 1500 octets, the IP header including the Router Alert option consumes 24 octets, and the IGMP fields up to including the Number of Sources (N) field consume 12 octets, leaving 1464 octets for source addresses, which limits the number of source addresses to 366 (1464/4).

U-VERSE® USE OF THE IGMP QUERY PACKET

The U-Verse® 2Wire 3800HG-V router sends IGMP query packets every 125 seconds onto the local subnet. The actual packet sent is as follows (IGMP layer only):

	Bits 0-7	Bits 8-15	Bits 16-23	Bits 24-31
Bit Offset 0	Type = 0x11	Max Resp = 0x64	(varies)	
Bit Offset 32	Multicast IP = 0x00000000 (General Query)			
Bit Offset 64	0x02	0x7d (QRV = 125)	0x0000 (No sources)	

IGMP MEMBERSHIP REPORT PACKET

In response to the IGMP query packets that the U-Verse® 2Wire 3800HG-V is sending out, the U-Verse® STBs send an IGMP Membership Report Packet back to the router. This packet tells the router what IP Multicast groups the STB wants to be a member of, and therefore what IP multicast traffic it will receive.

The STBs also send this packet to the U-Verse® router when their multicast membership changes, such as when the STB channel is changed.

IGMP Membership report packets are sent to IP Multicast group 224.0.0.22 (IGMP v3 report address).

IGMP MEMBERSHIP REPORT PACKET STRUCTURE

An IGMP Membership Report packet is structured as follows (IGMP layer only):

	Bits 0-7	Bits 8-15	Bits 16-23	Bits 24-31
Bit Offset 0	Type = 0x22	Reserved	Checksum	

Bit Offset 32	Reserved		Number of Group Records	
Bit Offset 64	Group Records (if 1 or more)			

- **Type**: Defined in the IGMP protocol as 0x22 for an IGMP v3 membership report packet.
- **Reserved**: The reserved field is set to zero on transmission and ignored on reception.
- **Checksum**: The 16-bit one's complement of the one's complement sum of the whole IGMP message (the entire IP payload). For computing the checksum, the Checksum field is set to zero. When receiving packets, the checksum MUST be verified before processing a packet.
- **Reserved**: The reserved field is set to zero on transmission and ignored on reception.
- **Number of Group Records**: This field specifies the number of group records present in this report.
- **Group Record**: Each Group Record is a block of fields containing information pertaining to the sender's membership in a single multicast group on the interface from which the Report is sent.

Each group record has the following structure:

	Bits 0-7	Bits 8-15	Bits 16-23	Bits 24-31
Bit Offset 0	Record Type	Aux Data Length	Number of Sources	
Bit Offset 32	IP Multicast Address			
Bit Offset 64	Source Addresses (if 1 or more)			
Bit Offset 96	Additional sources addresses …			
Bit Offset 128	Auxiliary Data (if present)			

- **Record Type**: One of 6 different values can be used for the Record Type.
  - "Current state records," which are sent in response to an IGMP query packet.
    - 0x01 = Filter mode is Include (not joined to the group).
    - 0x02 = Filter mode is Exclude (joined to the group).
  - "Filter mode change records", which are sent when a group's join/leave status changes.
    - 0x03 = Change filter mode to Include (leave the group).
    - 0x04 = Change filter mode to Exclude (join the group).
  - "Source list change records", which are sent when the group membership hasn't changed, but the desired sources that the host wants to listen to has changed.
    - 0x05 = Allow new sources. Source list contains additional sources to listen to for this group.
    - 0x06 = Block old sources. Source list contains previous sources that should no longer send multicast packets for the designated group.
- **Aux Data Length**: The Aux Data Len field contains the length of the Auxiliary Data field in this Group Record, in units of 32-bit words. It may contain zero, to indicate the absence of any auxiliary data.
- **Number of Sources**: The Number of Sources (N) field specifies how many source addresses are present in this Group Record.
- **Multicast Address**: The Multicast Address field contains the IP multicast address to which this group record pertains.
- **Source Addresses**: The Source Address [i] fields are a vector of n IP unicast addresses, where n is the value in this record's Number of Sources (N) field.
- **Auxiliary Data**: The Auxiliary Data field, if present, contains additional information pertaining to this Group Record. IGMP v3 does not specify any auxiliary data, so none should be present.

U-VERSE® USE OF THE IGMP MEMBERSHIP REPORT PACKET

The U-Verse® STBs send an IGMP Membership Report packet in response to an IGMP query packet from the U-Verse® 2Wire 3800HG-V router. A typical response packet is as follows (IGMP layer only):

	Bits 0-7	Bits 8-15	Bits 16-23	Bits 24-31
Bit Offset 0	0x22	0x00	(varies)	
Bit Offset 32	0x0000		0x0003 (3 Group Records)	

	Bits 0-7	Bits 8-15	Bits 16-23	Bits 24-31
Bit Offset 0	0x02 (In Group)	0x00	0x0000 (No Sources)	
Bit Offset 32	239.195.4.10			
	Bits 0-7	Bits 8-15	Bits 16-23	Bits 24-31
Bit Offset 0	0x02 (In Group)	0x00	0x0000 (No Sources)	
Bit Offset 32	239.192.1.17			
	Bits 0-7	Bits 8-15	Bits 16-23	Bits 24-31
Bit Offset 0	0x02 (In Group)	0x00	0x0000 (No Sources)	
Bit Offset 32	239.255.255.250			

This IGMP Membership report packet contains a report that the STB is currently joined to 3 groups.

- **239.255.255.250**: This is the Universal Plug-and-Play (UPnP) / Simple Service Discovery Protocol (SSDP) multicast group. This group is used to advertise the STB's services on the network. It is currently used in the implementation of Media Share, and this packet is how computers running Windows Media Player (or other media streaming server like TVersity) know that the STBs are on the network.
- **239.192.1.17**: This is the multicast IP address of an IPTV channel. All U-Verse® channels seen to date are in 239.192.0.0/16. Most national channels are in 239.192.0.0/24, 239.192.1.0/24, 239.192.5.0/24, and 239.192.7.0/24. Local channels are in other /24 subnets, with a single subnet per local market.
- **239.195.4.10**: This multicast IP address varies from market to market, but the ones I've seen are generally in 239.195.0.0/16. I don't know for sure what this group is used for, but I suspect this is the control channel used to tell the STB about subscription information and other housekeeping tasks. The STBs join this group as soon as they start up, and stay joined to it at all times, irrespective of whether the STB is turned on or not or tuned to other channels or not.

UV REALTIME'S INTERACTION ON THE NETWORK

UV Realtime gathers information from the STBs by inspecting the IGMP Membership Report packets and the SSDP packets from the DVR.

To do this, two obstacles must be overcome:

1. The 4-port Ethernet switch included in the 2Wire 3800HG-V router uses IGMP snooping to keep IP multicast traffic only on switch ports where the multicast traffic is needed. Because of this, the IGMP

Membership Report packets will not be sent to other ports on the switch since the only device that needs to receive them in a normal setup is the 2Wire 3800HG-V.

2. The STBs only send IGMP Membership Report packets in response to an IGMP Query packet issued by the 2Wire 3800HG-V router, which only occurs once every 125 seconds. It is desirable for UV Realtime to update the STB status more often than this.

IGMP SNOOPING

As mentioned earlier, most consumer-level switches do not treat IP multicast specially, and instead treat it the same as other broadcast traffic. When an IP multicast frame is received, the switch forwards the frame to all ports. The switch has no choice but to do this, since destination MAC addresses are a derivation of the IP address, thus the internal MAC address-to-port table cannot be used to determine which ports to send the traffic to. This behavior can result in flooding of traffic to ports that don't need it, especially in the IPTV environment where the multicast bandwidth is large.

To combat this, switches can employ a mechanism called IGMP snooping. The switch will listen for and parse the IGMP packets on the network to determine which ports should receive which multicast traffic. The switch will then build an internal table of multicast IP addresses-to-ports, and use this table to forward multicast traffic. This mechanism does violate a central principal of the OSI model, namely that a layer X device should not be looking at or inspecting a protocol in a higher layer. In this case, the switch (a layer 2 device) is looking at layer 3 (IP) and 4 (IGMP) data inside the packet to make a layer 2 (Ethernet) forwarding decision.

The U-Verse® router, the 2Wire 3800HG-V employs IGMP snooping on its internal 4-port Ethernet switch. This prevents ports that don't need to receive the IPTV multicast traffic from receiving them. Unfortunately, it also introduces complication #1 above.

WAYS TO COMBAT OBSTACLE #1 – IGMP SNOOPING

In an IGMP snooping switch, there are only 3 mechanisms that will cause the switch to forward multicast traffic to a port:

1. A host on that port sends an IGMP Membership Report packet that joins a multicast group.
2. A multicast-capable router on that port begins issuing IGMP Query packets.
3. An administrator configures the switch such that a given port is not subject to IGMP snooping.

For UV Realtime, the first obvious solution would be to use method #1 – send an IGMP join packet for group 224.0.0.22, which is the IGMP v3 reporting group. Unfortunately, this doesn't work. 224.0.0.22 is not a group that can be joined – the address is reserved for IGMP membership reports, and the switch will not add this group membership to its port forwarding table.

Another option would be method #3, but the U-Verse® 2Wire 3800HG-V router does not offer any administrative mechanism to turn off IGMP snooping, either for the entire router or for a specific port.

The only method left is #2, which does work to turn off IGMP snooping. The switch in the 2Wire 3800HG-V sees the query packet and begins to forward all multicast traffic to that port, believing that port to be a link to another multicast-capable router. The problem is that IGMP specifically requires that only one querier be present on a subnet. What will happen if you try to construct and send your own query packets is that the STBs on the network will begin expecting your host station to be the source of multicast streams. The STBs will eventually have picture freezes and glitches as they become confused as to who the true querier on the network is supposed to be.

WAYS TO COMBAT OBSTACLE #2 – SLOW UPDATES

The U-Verse® router sends IGMP Query packets every 125 seconds. For showing the STB status in a "realtime" application, we would desire the update rate to be faster than this. However, the only mechanism available that will cause the STBs to report their membership status is the IGMP Query packet. As discussed above, sending your own IGMP Query packet will interfere with the STBs.

UV REALTIME'S SPECIAL IGMP QUERY PACKET

The trick to getting STB reports 1) often enough, and 2) without causing the STBs to become confused about the network querier, is to construct an illegal query packet that does what we want.

UV Realtime does this by sending an IGMP query packet with the wrong source IP address. Instead of the host station, the IP address of the 2Wire 3800HG-V is used.

The full special IGMP Query packet (for a 192.168.1.0/24 network) is as follows:

Ethernet Layer	Bits 0-7	Bits 8-15	Bits 16-23	Bits 24-31
Word 0	Destination MAC Address			
Word 1	Continuation of Destination MAC		Source MAC Address	
Word 2	Continuation of Source MAC Address			
Word 3	Type			

IP Layer	Bits 0-7	Bits 8-15	Bits 16-23	Bits 24-31
Word 0	Version/Hdr Length	Differentiated Svcs	Total Length	
Word 1	Packet Identification Number		Flags / Fragment Offset	
Word 2	TTL	Protocol	Header Checksum	
Word 3	Source IP Address			
Word 4	Destination IP Address			
Word 5	IP Options			

IGMP Layer	Bits 0-7	Bits 8-15	Bits 16-23	Bits 24-31
Word 0	IGMP Type	Max Response Code	Checksum	
Word 1	Multicast IP Address			
Word 2	Res / S / QRV	QQIC	Number of Sources	

- **Destination MAC Address**: Set to 00:01:5E:00:00:01, which is the MAC address for IP multicast group 224.0.0.1 (all multicast-capable hosts)
- **Source MAC Address**: Set to the actual MAC address of the source station. Normally, because the MAC address here in the layer 2 (Ethernet) header and the IP address in the layer 3 header (IP) do not match, this would cause severe problems on the network with end hosts because it would essentially poison their

ARP cache (mismatched IP and MAC). But, since the packet is multicast and not unicast, end stations do not use this packet for populating their ARP cache. Also, this packet does not interfere with the switches on the network, because the source MAC address is correct, allowing the switch to populate its MAC-to-port table as intended.

- **Type**: The Ethernet type field is set to 0x0800, which indicates IP.
- **Version/Header Length**: Set to 0x46, indicating IPv4, and a length of 6 words (24 bytes)
- **Differentiated Services**: This is set to 0xC0. This is done to mirror what the U-Verse® router sends in its query packets.
- **Total Length**: Set to the total length of the packet, from the start of the IP layer.
- **Packet Identification Number**: Set sequentially starting from 0x0001. Each query packet sent by UV Realtime increments this value.
- **Flags / Fragment Offset**: Flags is 3 bits, including a reserved bit (set to 0), the don't fragment flag (set to 0), and the more fragments flag (set to 0). The fragment offset is 13 bits, set to 0.
- **Time to Live (TTL)**: Set to 1, since this packet is not intended to cross a router.
- **Protocol**: Set to 0x02 = IGMP.
- **Header Checksum**: The 16-bit one's complement of the one's complement sum of the whole IP message (the entire IP payload). For computing the checksum, the Checksum field is set to zero. When receiving packets, the checksum MUST be verified before processing a packet.
- **Source IP Address**: Would normally be set to the source station, but in this case is forged to the IP address of the 2Wire 3800HG-V. This causes STBs to believe that the query packet came from the U-Verse® router.
- **Destination IP Address**: Set to 224.0.0.1 (all multicast-capable hosts).
- **IP Options**: Set to 0x94040000 to mirror what the U-Verse® router sends in its query packets. These options specify that every router should examine this packet.
- **Type**: Set to 0x11 = IGMP Query packet.
- **Max Response Code**: Set to 0x0A = 1 second for all stations to respond.
- **Checksum**: The 16-bit one's complement of the one's complement sum of the whole IGMP message (the entire IGMP payload). For computing the checksum, the Checksum field is set to zero. When receiving packets, the checksum MUST be verified before processing a packet.
- **Multicast IP Address**: Set to 0.0.0.0 to indicate that this is a general query.
- **Reserved / S Flag / QRV**: Set to 0x02 to mirror what the U-Verse® router sends in its query packets.
- **QQIC**: Set to 0x3C indicating a query interval of 60 seconds.
- **Number of Sources**: Set to 0 (no source IP addresses in the query).

This packet is sent out on the network every 20 seconds by UV Realtime. The packet does two things:

1. It causes the switch in the U-Verse® 2Wire 3800HG-V router to believe that another multicast-capable router is on the network on this Ethernet port. The 3800HG-V will turn off IGMP snooping on this port so that the new "router" will receive all IGMP and multicast packets.
2. It causes the STBs to respond with an IGMP Membership report packet, which will contain the IP multicast groups they are a member of. UV Realtime analyzes these IGMP Membership packets from the STBs to find out what multicast groups they have joined.

The side effect of this packet is that all multicast traffic is now delivered to the port that the query was issued on, including all IPTV streams. This is why it is highly recommended that no intervening switch is used between the query host and the U-Verse® router, as such a switch would receive many Mbps of traffic and would flood it to all ports.

Under some circumstances, the query host could also be overwhelmed if the NIC in the host is a low-end 100Mbps interface.

MICROSOFT .NET FRAMEWORK RESTRICTIONS

UV Realtime is written in Visual Basic in the Microsoft .Net Framework. The .Net framework does not allow arbitrary construction of illegal network packets like the query packet above. To send this packet, UV Realtime uses WinPcap to place this packet on the network.

U-VERSE®'S PSEUDO-SSDP PACKETS

The U-Verse® DVR and STB units periodically send out a packet that contains useful information. These packets are a variant of SSDP. UV Realtime v1.3.0.0 and higher now use these packets to gather all STB/DVR channel/stream information rather than the IGMP join packets. This has several advantages:

1. It is no longer necessary to construct and send the illegal IGMP Query packet described in the previous section. This results in not turning off IGMP Snooping on the 2Wire 3800HGV's switch, thus the large amount of network traffic from the IPTV streams no longer comes to the computer running UV Realtime.
2. More information, including which streams are being watched and recorded, and individual detection of Off, VOD, and Recorded TV is now possible.
3. UV Realtime is now mostly a passive network application, simply listening on the network for the SSDP packets that the STB/DVR units send out.
4. The requirement that the UV Realtime computer is directly connected to the RG is no longer required, since the large IPTV network traffic that would overwhelm connected switches and other devices is no longer present.

WHAT IS SSDP?

SSDP stands for Simple Service Discovery Protocol. It is based on an expired IETF draft proposal from Microsoft and HP, and was intended to be used so that network clients can discover other network services with little or no configuration. SSDP eventually became the basis for Universal Plug and Play (UPnP).

Microsoft operating systems (including the Windows CE implementation in the STBs) still use SSDP to advertise some of their services on the network.

SSDP advertisements are sent to the multicast address of 239.255.255.250, on UDP port 1900.

U-VERSE® IMPLEMENTATION OF SSDP/UPNP

The U-Verse® STBs advertise their services using a pseudo-SSDP packet. The packet is multicast to 239.255.255.250, just like a standard SSDP/UPnP packet, but uses port 8082 instead of 1900. In addition, there are approximately 49 bytes of proprietary unknown information in the payload of the packet before usable information is found.

UV Realtime parses the information contained in these SSDP packets to gather information about the STBs.

SSDP NOTIFY MESSAGE

The U-Verse® SSDP packets have usable information beginning 49 bytes into the UDP payload (57 bytes including the 8-byte UDP header), which starts with a “NOTIFY” message in ASCII. Following the NOTIFY message are several x-xxxx MIME headers which give some information about the STB, and then data in XML format.

An example SSDP message from a DVR that is currently off is:

```
NOTIFY * HTTP/1.1
X-TYPE: DVR
X-LOCATION: HTTP://192.168.1.75:8080/DVRFS/INFO.XML
X-DEVICE: C560C1AD-40F0-4E61-854B-FB15632F49A7
X-DEBUG: HTTP://192.168.1.75:8080
X-FILTER: B6F20B27-E8DB-4BB0-A662-1169B38756C2
X-LASTUSERACTIVITY: 6/26/2010 3:55:24 AM

<NODE COUNT='136460'>
        <ACTIVITIES>
                <RECORDVER VER='82' SIZE='207232172032' FREE='83751862272' />
                <X/>
                <SCHEDVER DVER='2' VER='6135' PENDCAP='TRUE' />
                <X/>
        </ACTIVITIES>
</NODE>
```

Here it can be seen that following the NOTIFY message is an X-Type: DVR message, indicating that this packet came from the DVR. The STB (non-DVR) units use X-Type: display.

The <Activities> section of the XML data is where useful information is obtained. Several different record types can be present in the Activities section, but the important ones that UV Realtime looks for are <RecordVer> (for DVR space information), <RecReq> (for recorded streams), and <Tune> (for watched streams).

DETECTING DVR SPACE INFORMATION

Within the XML data for the <RecordVer> record from the DVR, there are two strings of text that are useful:

- size=’########’
- free=’########’

The number signs are replaced with digits in the XML data. The values given are the size of the DVR’s hard drive in bytes, and the amount of free space on the DVR in bytes.

UV Realtime parses these values to determine DVR space information. HD and SD time remaining are computed based on assumed bitrates of 5610 Kbps for HD and 2050 Kbps for SD.

DETECTING DVR RECORDING INFORMATION

To detect whether the DVR is recording or not, a <RecReq> record is searched for in the DVR's XML data contained in the SSDP packet.

Within the XML data for each <RecReq> record, there is a parameter of the following form:

- st='0x########'

For streams that the DVR is tuned to but not recording, the numerical data in this tag is a single digit 0. For a stream that the DVR is recording, the numerical data in the tag is a hex representation of the program start time.

UV Realtime looks for this tag throughout the <RecReq>, and if a non-zero numerical value is found, the recording light is turned on in the UV Realtime interface.

Sometimes, the amount of XML data in the SSDP packet exceeds what can be encapsulated within 1500 bytes on the Ethernet network. In this case, the DVR sends this packet as two or more IP fragments that have to be reconstructed together. In previous versions of UV Realtime, these fragments were ignored. Because v1.3.0.0 of UV Realtime is dependent on the entire content of the UDP payload to accurately get information from the STBs, UV Realtime v1.3.0.0 now buffers fragments and performs packet reconstruction to get access to the entire UDP payload.

DETECTING STREAMS BEING WATCHED

To detect what streams are being watched, <Tune> records are searched for STBs, and <RecReq> records are searched for the DVR.

An example packet where the STB is watching a live stream is:

```
NOTIFY * HTTP/1.1
X-TYPE: DISPLAY
X-LOCATION: HTTP://192.168.1.66:8080/DVRFS/INFO.XML
X-DEVICE: 43F2F0F0-8D4A-418C-864C-1C3DDFAB6B39
X-DEBUG: HTTP://192.168.1.66:8080
X-FILTER: B6F20B27-E8DB-4BB0-A662-1169B38756C2
X-LASTUSERACTIVITY: 6/24/2010 4:09:40 PM

<NODE COUNT='816776'>
        <ACTIVITIES>
                <SCHEDVER DVER='2' VER='6135' PENDCAP='FALSE' />
                <X/>
                <TUNE SRC='UDP://239.192.7.63:7534:52E37116-F14D-426B-AB38-B60D83D7E4AA'
PIPE='FULLSCREEN' CT='0XCFD0A680AB43C47A' PIL='0X0' RATE='0X559A10' STOPPED='FALSE'/>
        </ACTIVITIES>
</NODE>
```

You can see that in the <Tune> record, the multicast IP address of 239.192.7.63 is present, which is then translated via the channel database to a channel number and description. The key entry in the <Tune> record that indicates which stream is actually being watched (if there is more than one <Tune> record), is the PIPE='FULLSCREEN' tag.

For VOD, the multicast IP address in the SRC field is replaced with "VOD".

For recorded TV, the multicast IP address in the SRC field is replaced with the IP address of the DVR unit on the local network. This is why the <Tune> record is not used for determining what the DVR is watching, because if the DVR has buffered the stream and the program is being watched delayed, the <Tune> record indicates that Recorded TV is being watched. In this case, UV Realtime looks at the <RecReq> records, looking for the stream with the ST='0x0' tag, which is the buffered stream.

DETECTING STREAMS BEING RECORDED

To detect what streams are being recorded, <RecReq> records are searched. These are only present on the DVR's packets.

An example packet where the DVR is recording multiple streams is:

```
NOTIFY * HTTP/1.1
X-TYPE: DVR
X-LOCATION: HTTP://192.168.1.75:8080/DVRFS/INFO.XML
X-DEVICE: C560C1AD-40F0-4E61-854B-FB15632F49A7
X-DEBUG: HTTP://192.168.1.75:8080
X-FILTER: B6F20B27-E8DB-4BB0-A662-1169B38756C2
X-LASTUSERACTIVITY: 6/26/2010 5:00:06 PM

<NODE COUNT='137905'>
        <ACTIVITIES>
                <RECORDVER VER='84' SIZE='207232172032' FREE='83751862272' />
                <X/>
                <SCHEDVER DVER='2' VER='6139' PENDCAP='TRUE' />
                <X/>

                <RECREQ SRC='UDP://239.192.7.149:7534:64A32D5C-E907-47BC-80D3-
7FA7AB2C8F0D?R=5610000&AMP;P=1&AMP;SSRC0=1882976137&AMP;R0=5610000&AMP;CH=120
3&AMP;PROFILE=MULTICASTICC&AMP;ST=0XCFD0A244&AMP;ET=0XCFD0B108'
ST='0XCFD0A24400000000' ET='0XCFD0B10800000000' POSTPAD='120' RATE='5610000' PRI='32'/>

                <RECREQ SRC='UDP://239.192.34.18:7534:A4317A30-EC38-4C96-9C22-
F34CD2B072B8?CH=1002&AMP;P=1&AMP;PROFILE=MULTICASTICC&AMP;R=7500000&AMP;R0=750
0000&AMP;SSRC0=1174677020' ST='0X0' ET='0XFFFFFFFFFFFFFFFF' POSTPAD='0' RATE='7500000'
PRI='1'/>

                <TUNE SRC='UDP://239.192.34.18:7534:A4317A30-EC38-4C96-9C22-
F34CD2B072B8' PIPE='FULLSCREEN' CT='0XCFD0B0A725F61C51' PIL='0X0' RATE='0X7270E0'
STOPPED='FALSE'/>

                <TUNE SRC='UDP://239.192.7.149:7534:64A32D5C-E907-47BC-80D3-
7FA7AB2C8F0D' RATE='0X559A10'/>
```

```
                    <RECORD URL='HTTP://192.168.1.75:8080/DVRFS/V112'
SRC='UDP://239.192.7.149:7534:64A32D5C-E907-47BC-80D3-7FA7AB2C8F0D' PRI='1'
ST='0XCFD0A276DED96791' ET='0XCFD0B0A7E84FA463' STOPPED='FALSE'/>
                    <RECORD URL='HTTP://192.168.1.75:8080/DVRFS/V108'
SRC='UDP://239.192.7.149:7534:64A32D5C-E907-47BC-80D3-
7FA7AB2C8F0D?ST=0XCFD0A244&AMP;ET=0XCFD0B108' PRI='32' ST='0XCFD0A2466E7A186A'
ET='0XCFD0B0A7E84FA463' STOPPED='FALSE'/><TUNE SRC='UDP://239.192.34.18:7534:A4317A30-
EC38-4C96-9C22-F34CD2B072B8' RATE='0X7270E0'/>
                    <RECORD URL='HTTP://192.168.1.75:8080/DVRFS/V92'
SRC='UDP://239.192.34.18:7534:A4317A30-EC38-4C96-9C22-F34CD2B072B8' PRI='1'
ST='0XCFD0B0951D389C8F' ET='0XCFD0B0A742236AEE' STOPPED='FALSE'/>
          </ACTIVITIES>
</NODE>
```

Here there are two <RecReq> records indicating recording. The first one has a valid start time in the ST='' tag, indicating that stream is actually recording. The second <RecReq> record has a start time of ST='0x0', indicating that the stream is buffering (and therefore being watched). The <Record URL> records are not used by UV Realtime, but they indicate to the STB units what recordings are available for the current streams on the DVR, and what URL to connect to if the STB wants to watch one of those streams.

For VOD and Recorded TV, UV Realtime uses the RATE='' tags to determine if the stream is SD or HD. The RATE='' tag contains the assigned bitrate of the stream in bits per second, in hexadecimal representation. Bitrates greater than 4 Mbps are assumed to be HD.

DETECTING CHANNELS NOT IN THE DATABASE

UV Realtime normally uses the multicast IP address retrieved from the <RecReq> record or the <Tune> record to make a lookup in the channel database. This allows UV Realtime to show the channel number and description to the user.

For channels not in the database, UV Realtime as of version 1.7.0.0 automatically submits them to a central server for inclusion in the next channel database update. The information submitted consists of the multicast IP address detected from the <RecReq> record, the city, state, and zip code detected from IP Geolocation, and the declared channel number which is present in the <RecReq> record. This is sufficient information to find out what channel goes with what multicast IP address.

Channel numbers are only present in <RecReq> records, so UV Realtime can only do channel submissions using information from the DVR. Since STB's do not use <RecReq> records, but instead only use <Tune> records, there is not enough information to make a channel submission when an STB has tuned to a channel that is not in the database.

UV REALTIME SSDP JOIN PACKET

For UV Realtime to receive the SSDP packets, UV Realtime sends an IGMP join packet to the RG every 60 seconds, joining the 239.255.255.250 multicast group. This ensures that the SSDP packets reach the UV Realtime computer.

For most Windows installations, this actually isn't necessary because Windows sends Universal Plug-and-Play packets that are nearly identical, which achieves the join of the 239.255.255.250 group. UV Realtime sends them anyway in case the user's computer is using firewall software that blocks the outbound UPnP packets.

STREAM ANALYZER

As of version 1.6.0.0, UV Realtime contains a network IPTV stream analyzer component. This section will briefly discuss how the stream analyzer works.

Because the U-Verse® IPTV stream is multicast and delivered via UDP, there is no opportunity for error correction or retransmission of corrupted or missing packets. In addition, UDP does not provide connection-oriented delivery, resulting in the possibility that IPTV packets may arrive out-of-order.

Because of these restrictions, the network delivering IPTV must be error-free in order to receiver error-free video and audio. Errors introduced on the network that result in corrupted, missing, or out-of-order packets will have a direct impact on video and audio quality, resulting in picture freezes, glitches, pixilation (blocks of color resulting from a decode of an MPEG stream containing errors), and potentially audio cut-outs or noise.

The stream analyzer can analyze an IPTV stream and determine if there are missing, corrupted, or out-of-order packets arriving at the U-Verse® STB, confirming problems within the network.

U-VERSE® IPTV UDP PACKET

The full structure of a U-Verse® IPTV packet is shown below.

Ethernet Layer	Bits 0-7	Bits 8-15	Bits 16-23	Bits 24-31
Word 0	Destination MAC Address (Multicast)			
Word 1	Continuation of Destination MAC		Source MAC Address	
Word 2	Continuation of Source MAC Address			
Word 3	Type (IPv4)			

IP Layer	Bits 0-7	Bits 8-15	Bits 16-23	Bits 24-31
Word 0	Version/Hdr Length	Differentiated Svcs	Total Length	
Word 1	Packet Identification Number		Flags / Fragment Offset	
Word 2	TTL	Protocol (UDP)	Checksum	
Word 3	Source IP Address			
Word 4	Destination IP Address (Multicast)			

UDP Layer	Bits 0-7	Bits 8-15	Bits 16-23	Bits 24-31
Word 0	Source Port		Destination Port (7534)	
Word 1	Length		Checksum (Optional, but used by U-Verse®)	
Word 2	IPTV Header (0x8021 or 0x9021)		IPTV Packet Sequence Number	

Word 3+	Additional Packet Payload (IPTV Data / MPEG Transport Stream)

Shown in yellow are the fields used by UV Realtime to determine what category a packet falls in.

COUNTING AND CLASSIFYING PACKETS

UV Realtime's Stream Analyzer begins counting packets when the "Start Analysis" button is pressed, and counts packets until the analysis timer expires. For each packet, the packet integrity is checked using the UDP checksum and IP layer checksum, and the packet identification in the IPTV stream is retrieved from the UDP payload data.

The packet is then classified as follows:

- **Total Packets in Stream:** The difference between the first IPTV packet sequence number that was seen when analysis started and the most recent IPTV packet sequence number that was seen.
- **Good Packets:** The sum of how many IPTV packets were received with valid IP and UDP layer checksums, and had proper packet integrity, addressing, and other options.
- **Out of Order Packets:** If a packet is received with an IPTV packet sequence number that is less than the most recently seen IPTV packet sequence number on the network, the packet is considered out-of-order and this total is incremented.
- **Corrupted Packets:** Any packet received that had a bad checksum or failed the packet integrity check increments this total.
- **Missing Packets:** The difference between the total number of packets expected in the stream and the sum of good, out-of-order, and corrupted packets.

RESULTS

Normally, a perfectly intact IPTV stream (100.0 % good packets) should reach the DVR/STB unit. Any accumulation of out-of-order, corrupted, or missing packets indicates network problems that will adversely affect video and audio performance. These problems are nearly always hardware-related, and can be caused by:

- Bad cabling, which is especially common with coax, even if all coax PHY rates show 112 Mbps (128 Mbps on i3812V/3801HGV).
- Bad Ethernet cabling is less common, but crossed pairs or poor termination can cause the problem.
- Bad Ethernet switches will definitely cause issues. Even a properly working, but low-powered switch may drop packets and cause problems.
- Bad RG can also be the issue.

CONCLUSION

With this information, those who have an interest in the underlying protocols and network operation of both the U-Verse® system and UV Realtime can further research the system and attempt to discover additional possibilities to retrieve information from the system.