Discover Console Open IPTV – Requirements & Limitations

(LF ISBU TSS department – 2017-03-29 v02)

Dear customer IT/IPTV Specialist,

This document will additionally support in setting up the network where the Life Fitness Discover Open IPTV consoles will be connected to.

The consoles are able to work with Open (not encrypted) IPTV streams nicely, but because the consoles are not specifically made to just do that (like commercial grade/hospitality IPTV Set Top Boxes or PC/MAC laptops), they need some additional support from the network. The following few pages will give you additional info on how to setup the network.

To start, we want to highlight some crucial requirements which are inevitable to show the Open IPTV channels correctly on the consoles:

- **The network must have a Layer 3 device included which includes the IGMP Querier functionality (based on the IGMPv3 protocol).**
- **There may only be one device in the network which has the IGMP Querier functionality enabled**
- **All other devices in the network (switches) must support the IGMP Snooping functionality (This part of the IGMPv2 protocol).**
- **The IPTV streams offered to our consoles must be in UDP or RTP format. HTTP, HTTPLIVE and RTSP network protocols are not supported.**
- **It's strongly advised to thoroughly review the Multicast settings of each of the network devices (routers/switches) to make sure they're setup correctly to stream the IPTV channels to the consoles, adhering to the requirements indicated in this document.**
- **Not following these requirements can cause the following symptoms:**
  - **not able to show any of the IPTV channels (black screens)**
  - **Only channel audio is heard, no video is seen**
  - **Channels are shown with pixelated images**
  - **Only a static image of the channel is shown**
  - **Channels are only shown 20-60 seconds after selecting the channel**
- **Life Fitness or any of its affiliates are not responsible for setting up, managing, maintaining, changing or updating the customers network.**

UNVERIFIED DRAFT

We understand that these requirements are maybe beyond a normal network setup and appreciate your cooperation in setting up the network as indicated so that our consoles will be able to show the IPTV content seamlessly, creating the best user experience possible.

Thank you!

PS: Items marked with a will give additional online info about that specific item when clicking on this icon. Also check out the Q&A section at the end of this document.

Discover Open IPTV Console requirements & limitations

- Discover SE Console SW version: 2.30.66 or later
- Discover SE3(hd) Console version: 3.04.41 or later
- Network connected through LAN only (WLAN/Wifi not supported for Open IPTV)
- Console only support one LAN or VLAN connection at a time. It can not switch between 2 different network LANs/VLANs
- Console can only support a single network interface at the same time. It can not be configured to support LAN and WLAN/Wifi at the same time
- Console does not support any encryption schemes (i.e., Pro:Idiom, HDCP, etc.)
- Each Discover Open IPTV console must have a valid TCP/IPv4 IP address. DHCP-based or static IP assignments are both supported
- The internal console wired network interface adapter is a 100Mbps (100BASE-T) version

Customer Network requirements & limitations

- Network connected through LAN only (WLAN/Wifi not supported for Open IPTV)
- At least one “Layer 3” (L3) switch (or router) must be present within the network
- This Layer 3 piece of hardware needs to support and have “IGMPv3” enabled
- Only one Layer 3 piece of hardware needs to act as and enable “IGMP Querier” functionality (AKA IGMP Proxy or IGMP Host) (IGMPv3 protocol) This can be a switch or a router.
- All other switches (Layer 2 or 3) need to support and enable “IGMP Snooping” (IGMPv2 protocol)
- All switches need to support Gigabit Ethernet speeds of at least 1Gbps (1000BASE-T)
- VLAN trunking is not supported
- the IPTV network and the Internet (when applicable) need to be combined into a single LAN towards the consoles

UNVERIFIED DRAFT

See also the Network Configuration examples below

Other suggestions (unconfirmed!!):

- *All switches in the network should be “non-blocking” switches, preferably*
- *Have only one IGMP Querier activated within the network (or set to Auto when supported in the hardware, so that it detects other Querier(s) and auto turns itself off). Having 2 devices acting as Queriers will cause IPTV streaming issues*
- *All network hardware should have the correct date, time and time zone*
- *IPTV headend and ISP internet source should both preferably be directly connected to the L3 switch/router which has the IGMP Querier functionality enabled*
- *When available turn on "Immediate Leave" function within IGMP snooping setup (IGMPv2 protocol option)*
- *When available turn on IGMP Querier “Election” in the IGMP Querier device*
- *Make the "Query Max response interval” setting in IGMP VLAN settings as low as possible (in seconds) to improve channel switching timing (IGMP Querier device))*
- *“Multicast Router Port” setting should be set to "Static" (or turned on or equivalent) for the port in the L3 IGMP Querier device which sends the IPTV channels to the other switches in the network. the rest of the ports should have turned it off/none*
- *"Forward All" setting should be set to "Static" (or turned on or equivalent) for the port in the L3 IGMP Querier device which sends the IPTV channels to the other switches in the network. the rest of the ports should have turned it off/none*

- *"Unregistered Multicast" setting should be set to "Forwarding" (or turned on or equivalent) for the port in the L3 IGMP Querier device which sends the IPTV channels to the rest of the switches in the network. the rest of the ports should have turned it off/set to "Filtering"*
- *"Jumbo frames" setting should be turned off in all switches*
- *Turn on "Flow control" only when the consoles are getting flooded with too much data and then turn it on only within the switch(es) directly connected to the consoles*
- *As the cost of a Layer 3 IGMP Querier device is significantly higher than a Layer 2 device and the Layer 3 switch pricing increases rapidly when going beyond 10 ports, we advice to setup the network with a small Layer 3 IGMP Querier device, which can handle all the incoming streams as well as one outgoing stream, which is connected to a Layer 2 device. This much cheaper Layer 2 device distributes the streams to all Consoles. (see examples below)*
- *When an IPTV channel is broadcasting its video content in MPEG4, we believe that the broadcast is most stable and in sync when its setup with the RTP network protocol and less with the UDP network protocol. MPEG 1 & 2 streams can be broadcasted through the UDP protocol*

Life Fitness network hardware requirements & limitations (optional)

- If using a Life Fitness-provided gateway, the gateway must act as the DHCP server and all internet traffic must be routed through it.
- Life Fitness-provided gateways do not support the functionality to combine both internet and IPTV services. (only pass-through both services)

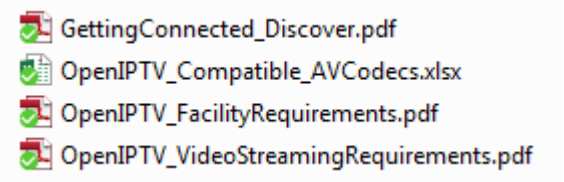
IPTV Streaming requirements & limitations

UNVERIFIED DRAFT

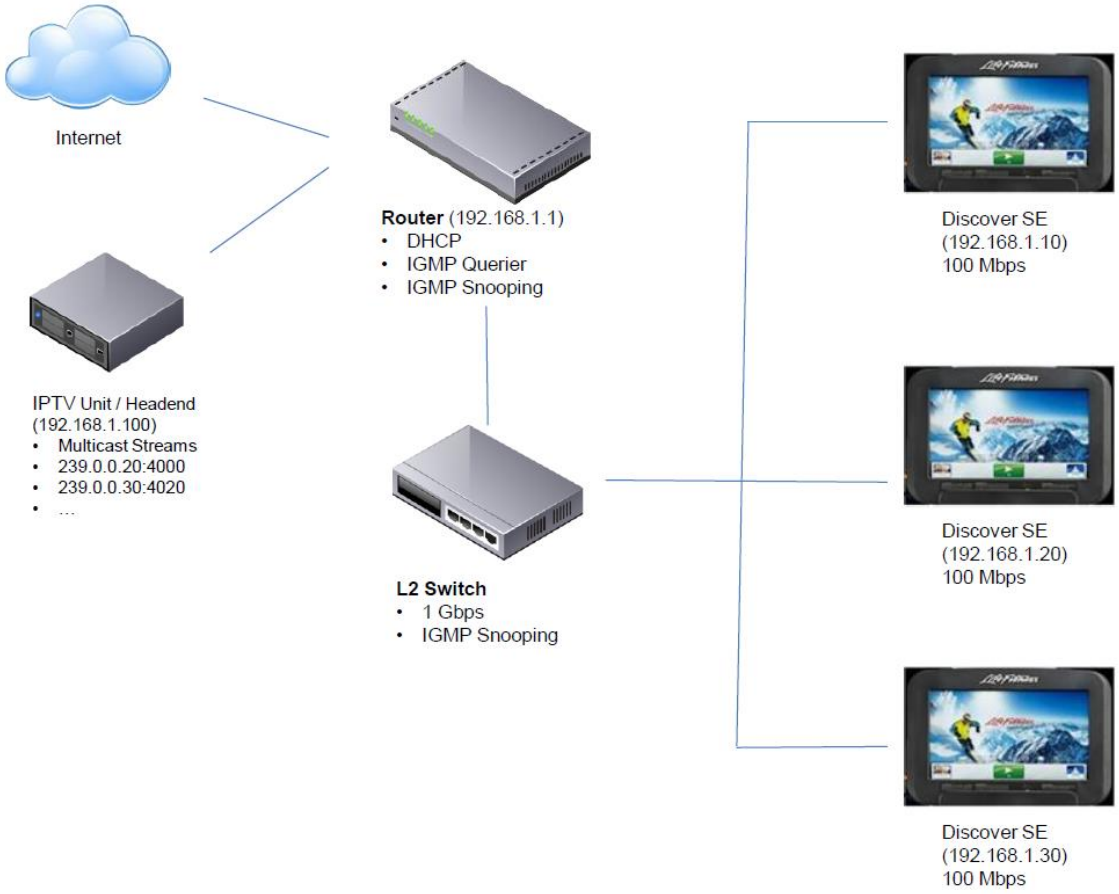
- Input Bitrate – the maximum supported bitrate is 12Mbps per IPTV channel
- The recommended total bandwidth is based on the number of channels and the expected channel bandwidth. For example, if there are 20 channels of 10Mbps video streams, the network will require (20x10) 200 Mbps support
- Each IPTV channel must be setup as unique IP Multicast address and is composed of a SPTS (Single Program Transport Stream) Eg: MPTS (Multi Program Transport Stream) is not supported
- the Multicast address range the IPTV channels should have is between 224.0.0.0 and 239.255.255.255 (Class D Multicast IP addresses)
- Captive Portal functionality (i.e., a special page shown to Wi-Fi clients forcing them to authenticate or pay for internet access) is not supported.

Other available documents

Next to this document you also should've received the following documents to complete the information about Open IPTV and the Discover Consoles:

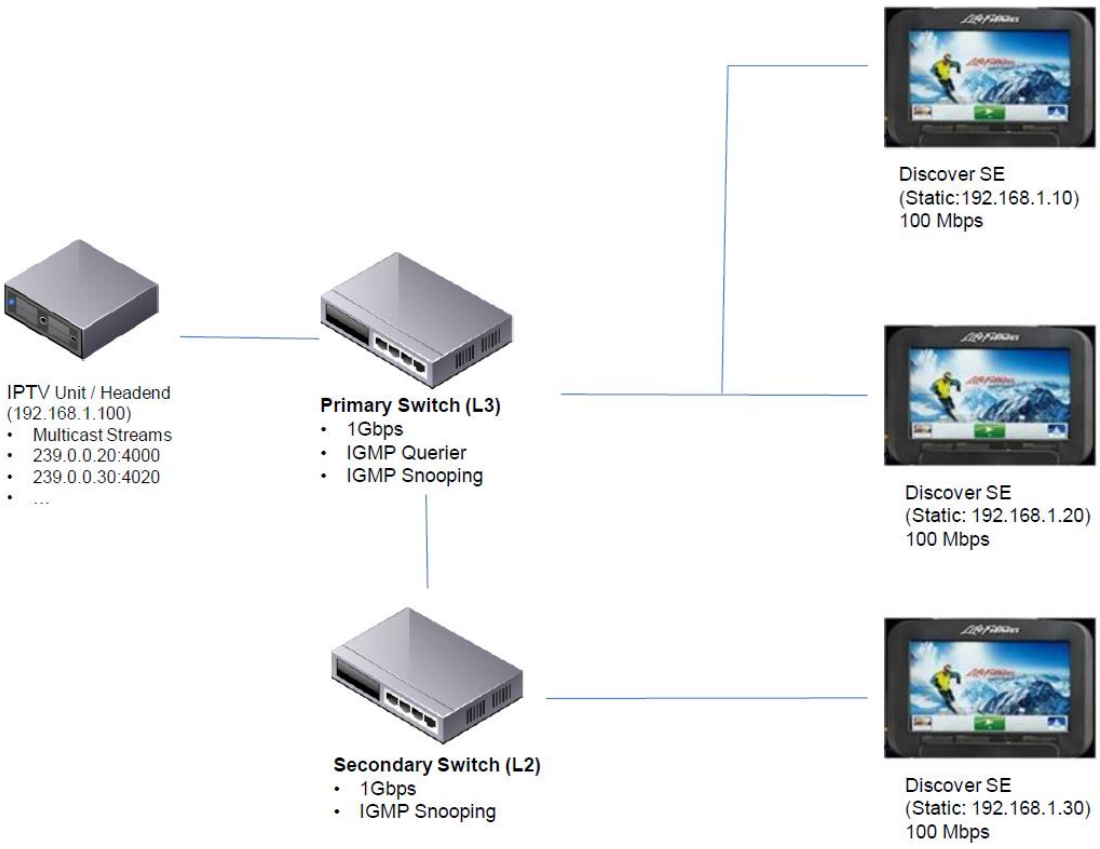


Example Network Configuration 1

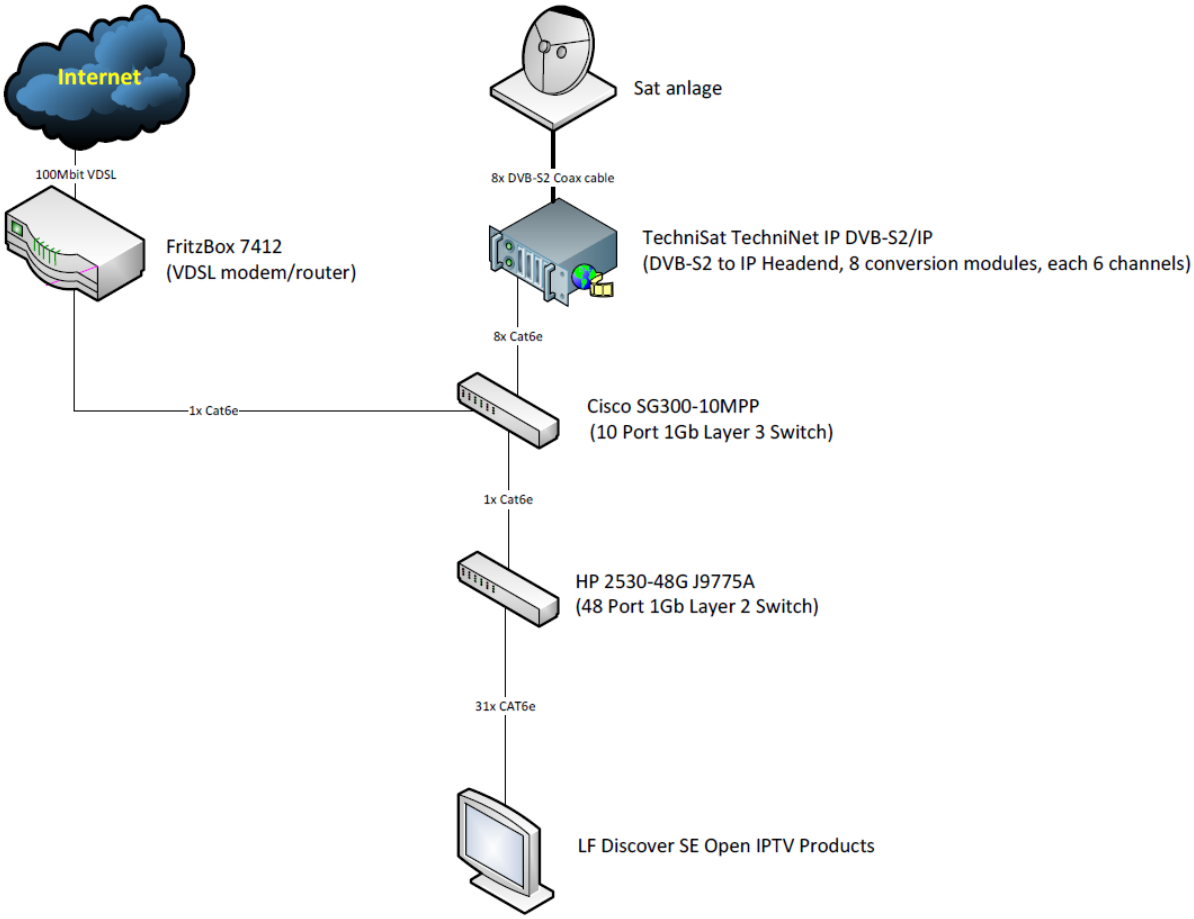


UNVERIFIED DRAFT

Example Network Configuration 2



Example Network Configuration 3



Q & A

(unconfirmed resources)

What is IGMP Querying and IGMP Snooping and why would I need it on my network?
IGMP is a network layer (Layer 3) protocol used to establish membership in a Multicast group and can register a router to receive specific Multicast traffic. (Refer to RFC 1112 and RFC 2236 for information on IGMP versions 1 and 2.)

Multicast aware switches are slowly making their way into the network cores for businesses and universities that have heavy traffic to move through their networks. Multicast filtering is achieved by dynamic group control management. By default, all Multicast traffic should be blocked until requested by a Multicast group member. (Default behavior depends on switch manufacturer.) The master of the IGMP filter lists is the router or switch that is configured to act as the IGMP Querier. The responsibility of the Querier is to send out IGMP group membership queries on a timed interval, to retrieve IGMP membership reports from active members, and to allow updating of the group membership tables.

A Layer 2 switch supporting IGMP Snooping can passively snoop on IGMP Query, Report, and Leave (IGMP version 2) packets transferred between IP Multicast routers/switches and IP Multicast hosts to determine the IP Multicast group membership. IGMP snooping checks IGMP packets passing through the network, picks out the group registration, and configures Multicasting accordingly.

Without IGMP Querying/Snooping, Multicast traffic is treated in the same manner as a Broadcast transmission, which forwards packets to all ports on the network. With IGMP Querying/Snooping, Multicast traffic is only forwarded to ports that are members of that Multicast group. IGMP Snooping generates no additional network traffic, which significantly reduces the Multicast traffic passing through your switch.

UNVERIFIED DRAFT

What is IGMP Snooping? (explained by a different resource -1)
Internet Group Management Protocol (IGMP) Snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch. Multicast IP traffic is traffic that is destined to a host group. Host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request the multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly affecting network performance.
A traditional Ethernet network may be separated into different network segments to prevent placing too many devices onto the same shared media. Bridges and switches connect these segments. When a packet with a broadcast or multicast destination address is received, the switch will forward a copy into each of the remaining network segments in accordance with the IEEE MAC Bridge standard. Eventually, the packet is made accessible to all nodes connected to the network. This approach works well for broadcast packets that are intended to be seen or processed by all connected nodes.
In the case of multicast packets, however, this approach could lead to less efficient use of network bandwidth, particularly when the packet is intended for only a small number of nodes. Packets will be flooded into network segments where no node has any interest in receiving the packet. While nodes will rarely incur any processing overhead to filter packets addressed to unrequested group addresses, they are unable to transmit new packets onto the shared media for the period of time that the multicast packet is flooded.
The problem of wasting bandwidth is even worse when the LAN segment is not shared, for example in full-duplex links. Allowing switches to snoop IGMP packets is a creative effort to solve this problem. The switch uses the information in the IGMP packets as they are being forwarded throughout the network to determine which segments should receive packets directed to the group address.

What is IGMP Snooping? (explained by a different resource -2)
IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations, the switch maintains a map of which links need which IP multicast streams.
Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic. A switch will, by default, flood multicast traffic to all the ports in a broadcast domain (or the VLAN equivalent).

Multicast can cause unnecessary load on host devices by requiring them to process packets they have not solicited. When purposefully exploited, this can form the basis of a denial-of-service attack. IGMP snooping is designed to prevent hosts on a local network from receiving traffic for a multicast group they have not explicitly joined. It provides switches with a mechanism to prune multicast traffic from links that do not contain a multicast listener (an IGMP client).

IGMP snooping allows a switch to only forward multicast traffic to the links that have solicited them. Essentially, IGMP snooping is a layer 2 optimization for the layer 3 IGMP. IGMP snooping takes place internally on switches and is not a protocol feature. Snooping is therefore especially useful for bandwidth-intensive IP multicast applications such as IPTV.

What is an IGMP Querier? (explained by a different resource -1)
IGMP snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the IGMP querier. The IGMP query responses, known as IGMP reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicasts to the port where the end device is located.

What is an IGMP Querier? (explained by a different resource -2)
In order for IGMP, and thus IGMP snooping, to function, a multicast router must exist on the network and generate IGMP queries. The tables created for snooping (holding the member ports for each a multicast group) are associated with the querier. Without a querier the tables are not created and snooping will not work. Furthermore, IGMP general queries must be unconditionally forwarded by all switches involved in IGMP snooping. Some IGMP snooping implementations include full querier capability. Others are able to proxy and retransmit queries from the multicast router.

What is RTP?
RTP stands for Real-time Transport Protocol. It is normally sent via UDP. It does not ensure “real time” but is a protocol that enhances the control and synchronization of real time stuff (like streaming video). Here is where it gets interesting: with MPEG-1 and MPEG-2, RTP is unnecessary because MPEG itself provides synchronization.
Like so many standards, there are several ways to implement it. For example, you can split apart the MPEG-1 stream and send audio on one IP address and video on another, or you can send both audio & video on the same address. RTP provides timestamps that will provide audio/video sync.
In the case of MPEG-4, the only meaningful way to send audio/video is via RTP (there is nothing like a “MPEG-1 System Stream” nor a “MPEG-2 Transport Stream”). In other words, for MPEG-4, a/v sync is provided via RTP.
Analogy: RTP is like an orchestra leader, keeping all the musicians in sync.

UNVERIFIED DRAFT