ZyXEL-Produkte im Einsatz mit IPTV

Verteilung von IPTV-Daten über das Internet Group Management Protokoll

IPTV stellt spezielle Anforderungen an die verwendete Hardware. Das IGMP-Protokoll (Internet Group Management Protokoll) stellt eine effiziente Verteilung der IPTV-Datenpakete sicher. Spezielle Gruppierungs-Benachrichtigungen steuern den Multicast-Stream so, dass jede beteiligte Netzwerkkomponente vom Provider bis zur STB (Set-Top-Box) weiss, welche Ports die Daten des ausgewählten Kanals benötigen. Wird ein TV-Stream von mehreren Ports angefordert, werden die Datenpakete am entsprechenden Knotenpunkt nach Bedarf dupliziert. Dadurch muss der Provider die Daten nicht für jede STB einzeln senden, was eine enorme Datenmenge verursachen würde, die Daten werden vielmehr auf dem Weg zu den Boxen vervielfacht.

Voraussetzungen für den Betrieb einer Set-Top-Box mit einem VDSL-Router

Damit die IGMP-Benachrichtigungen der Set-Top-Box korrekt zum Provider gelangen, muss der zur Internet-Anbindung eingesetzte Router IGMP unterstützen. Aktuelle IPTV-Angebote setzen mindestens IGMP v2 voraus. Alle VDSL-Router von ZyXEL unterstützen IGMP v2, benötigen aber zum Teil eine entsprechende Konfigurationsanpassung.

Die folgenden Informationen gelten für die IPTV-Lösung der Provider Sunrise und Swisscom, welche auf Multicast und IGMP aufsetzen. IPTV-Lösungen wie Zattoo, Wilmaa oder Teleboy nutzen normale Unicast-Datenübertragungen. Sie sind nicht so effizient, dafür weniger anspruchsvoll an die technischen Voraussetzungen.

Einsatz-Szenarien für Sunrise-TV

ZyXEL-VDSL-Router mit Sunrise-TV

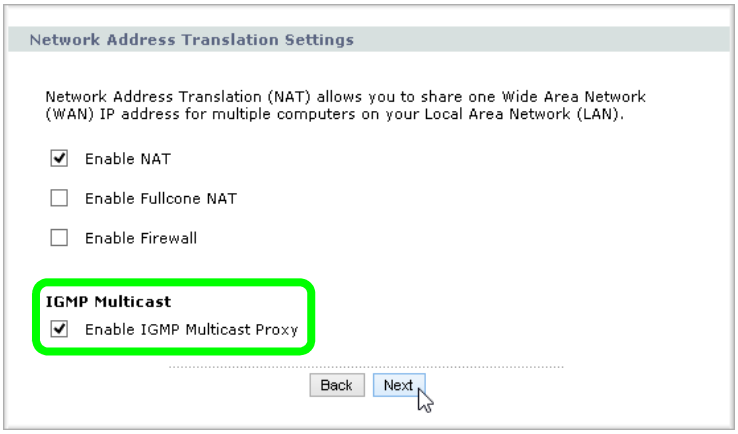
- Die Set-Top-Box benötigt zur Provisionierung zwingend den vom Provider zur Verfügung gestellten VDSL-Router. Der Ersatz durch ein Modell von ZyXEL-Router ist technisch nicht möglich.

Einsatz-Szenarien für Swisscom-TV

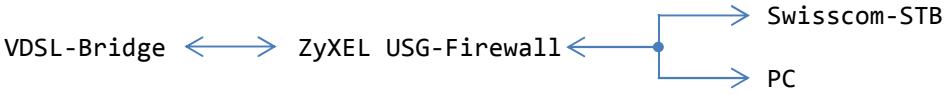
ZyXEL-VDSL-Router mit STB

- Der SBG3300 und der VMG8924 funktionieren "out of the box", das bedeutet ohne weitere Konfigurations-Anpassung.
- Ein Router der P870Hx-Serie benötigt eine Konfigurationsanpassung. Im Menü "Network > WAN > Internet Connection > ptm0.1" muss auf der dritten Konfigurationsseite des Assistenten die Option

"*Enable IGMP Multicast Proxy*" aktiviert werden.

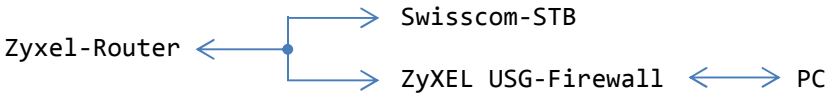


Betrieb von STB hinter USG-Firewall



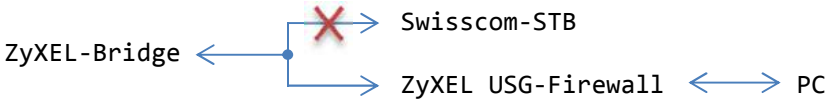
- Aktuelle Firewall-Modelle der ZyXEL USG-Serie unterstützen das IGMP-Protokoll, erfordern aber eine Konfigurationsanpassung. Mit den Grundeinstellungen bricht der TV-Stream einer direkt hinter einer USG-Firewall eingesetzten STB nach jedem Kanalwechsel nach wenigen Sekunden ab. Der Knowledge-Base-Artikel KB-3583 'IPTV mit Multicast und IGMP (USG-Serie FW 4.x)' beschreibt das Einrichten der Firewall für den Betrieb mit Multicast-IPTV.

ZyXEL-Router als Router und USG-Firewall



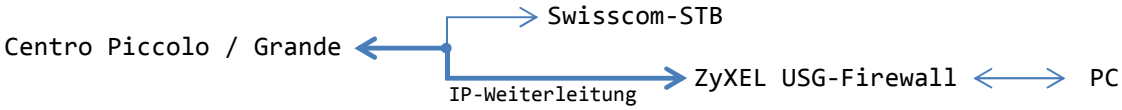
- Der Einsatz einer Firewall hinter einem VDSL-Router von Zyxel ist grundsätzlich möglich, jedoch verkompliziert das zweifach durchgeführte NAT das Einrichten von Port-Weiterleitungen und VPN-Verbindungen.

ZYXEL-Router als Bridge für Parallelbetrieb von STB und USG-Firewall

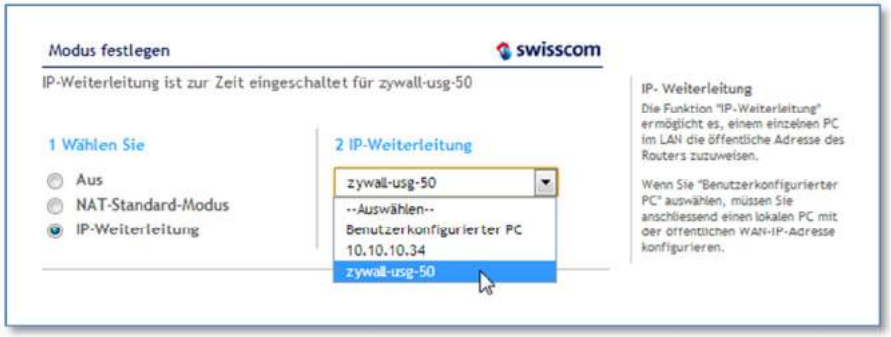


- Der direkte Parallel-Betrieb von STB und USG-Firewall hinter einem zur Bridge umkonfigurierten VDSL-Router ist aufgrund der dazu benötigten Mehrfachanmeldung beim Provider nicht möglich. Die STB bricht die Anmeldung mit der Fehlermeldung "konnte IP beziehen aber keine Internet-Verbindung herstellen" ab.

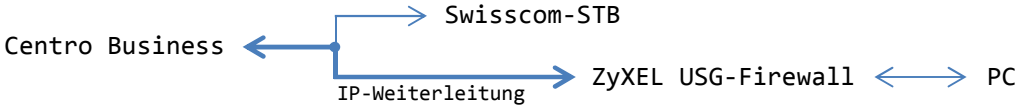
Swisscom Router Centro Piccolo oder Grande für Parallelbetrieb von STB und USG-Firewall



- Zu jedem VDSL-Anschluss mit IPTV stellt Swisscom einen Router bereit. Die Modelle der Centro-Serie bieten die Option der IP-Weiterleitung. Damit lässt sich ein paralleler Betrieb der STB und einer USG-Firewall realisieren. Die STB wird so mit einer internen IP-Adresse aus dem Bereich des Centro-Routers betrieben, während die IP-Weiterleitung der USG-Firewall am WAN-Anschluss die öffentliche IP-Adresse des Centro-Routers zur Verfügung stellt.
- Das lokale Subnetz 192.168.1.0 ist in der Grundkonfiguration sowohl auf dem Centro-Router als auch auf der USG-Firewall vorkonfiguriert. Mindestens eines der beiden Netze muss angepasst werden. Zum Beispiel indem auf dem Centro-Router die LAN-IP auf 10.10.10.1 geändert wird.
- Der Empfang von IPTV über die STB und der Internetzugang über die USG-Firewall funktionieren so bereits. Damit die USG-Firewall die öffentliche IP-Adresse des Centro-Routers erhält, ist ein weiterer Schritt notwendig.
- Im Menü *IP-Weiterleitung* des Centro-Routers lässt sich im Schritt 1 die Weiterleitung auswählen. Im Schritt 2 wird die eingesetzte USG-Firewall für die IP-Weiterleitung bestimmt. Ein Neustart von Router und Firewall sorgt dafür, dass die Firewall nun per DHCP vom Router direkt die WAN-IP-Adresse zugeteilt bekommt.



Swisscom Router Centro Business für Parallelbetrieb von STB und USG-Firewall



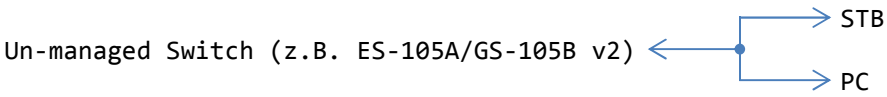
- Die Modelle der Centro-Business-Serie bieten eine weniger transparente Option der IP-Weiterleitung. Damit lässt sich zwar ein paralleler Betrieb der STB und einer USG-Firewall realisieren. Die IP-Weiterleitung auf die USG-Firewall muss aber zwingend über das Subnetz 172.31.255.4/30 erfolgen. Siehe Swisscom-Dokument 'IP Passthrough Local Security Gateway'.
- Weitere Varianten bieten die Konfigurationsarten 'PPPoE-Passthrough' und 'DMZ-Mode'. Diese erfordern eine fixe öffentliche IP-Adresse, erlauben aber deren Verwendung direkt am WAN-Interface der Firewall.
- Details zu Möglichkeiten und zur Einrichtung sind im Knowledge-Base-Artikel KB-3617 'USG mit Centro Business Router' aufgeführt.

Einsatz von Switchs mit IPTV

Einfache, nicht konfigurierbare (un-managed) Switchs wissen mit dem IGMP-Protokoll nichts anzufangen. Sie erkennen aber in Regel, dass es sich bei den empfangenen Daten um einen Multicast-Stream handelt und verteilen die Daten auf sämtliche aktiven Ports. Dies führt auf einem Netzwerk zu einer stetigen Grundlast, welche in den meisten Fällen aber aufgrund der wesentlich höheren Bandbreite des Switches zu keinen nennenswerten Einschränkungen führen sollte. Etwas anders sieht es aus, wenn die IGMP-Daten so zu einem Access-Point gelangen. Ohne entsprechende IGMP-Unterstützung wird auch dieser versuchen, die Daten an sämtliche verbunden Clients zu senden, was das WLAN-Netzwerk komplett auslasten kann.

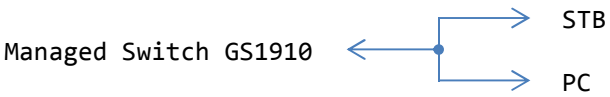
In einem Netzwerk mit IPTV setzt man daher vorzugsweise mindestens einen einfachen, konfigurierbaren (managed) Switch ein, welcher den Weg des Multicast-Streams steuern lässt.

Einfacher, nicht konfigurierbarer Switch und IPTV

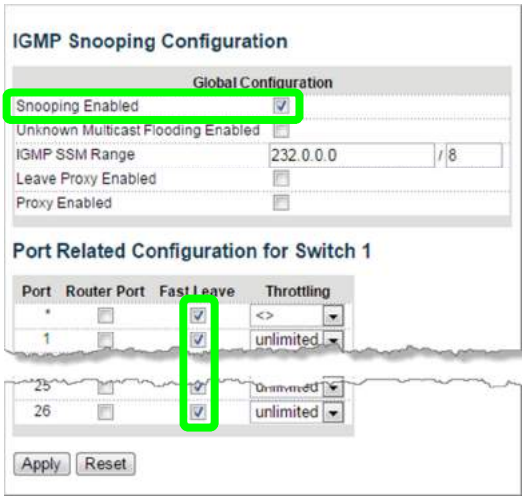


- Empfang von IPTV und Internet-Zugang funktioniert.
- Der Switch signalisiert auf allen aktiven Ports eine hohe Aktivität (= Multicast Flooding).

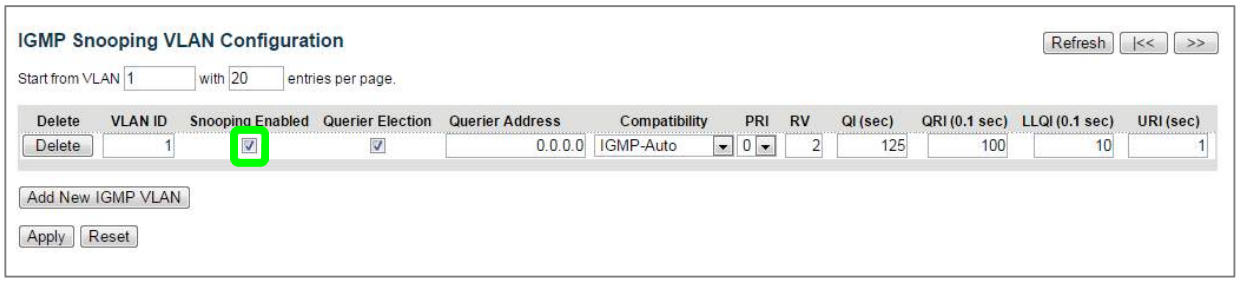
Managed Switch der GS1910-Serie (ab 2012)



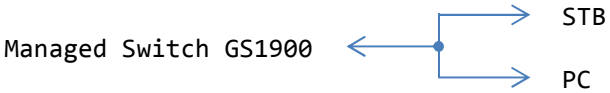
- Empfang von IPTV und Internet-Zugang funktioniert.
- Der Switch signalisiert auf allen aktiven Ports eine hohe Aktivität (= Multicast Flooding).
- Lösung: Unter "*IPMC > IGMP Snooping > Basic Configuration*" das IGMP Snooping aktivieren. Deaktivieren von "*Unknown Multicast Flooding*" verhindert, dass der Switch unbekannten Multicast-Traffic auf alle Ports weiterleitet. Je nach Provider kann die Option "*Fast Leave*" den schnellen Kanal-Wechsel begünstigen.



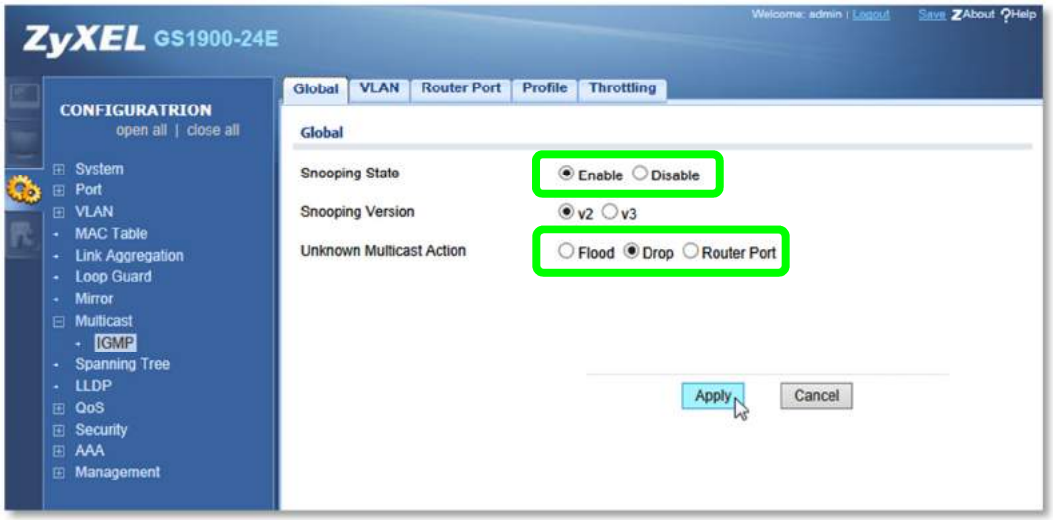
- Im Menü "*IPMC > IGMP Snooping > VLAN Configuration*" über "*Add New IGMP VLAN*" ein neues Profil mit *VLAN ID* "*1*" erstellen und "*Snooping*" aktivieren.



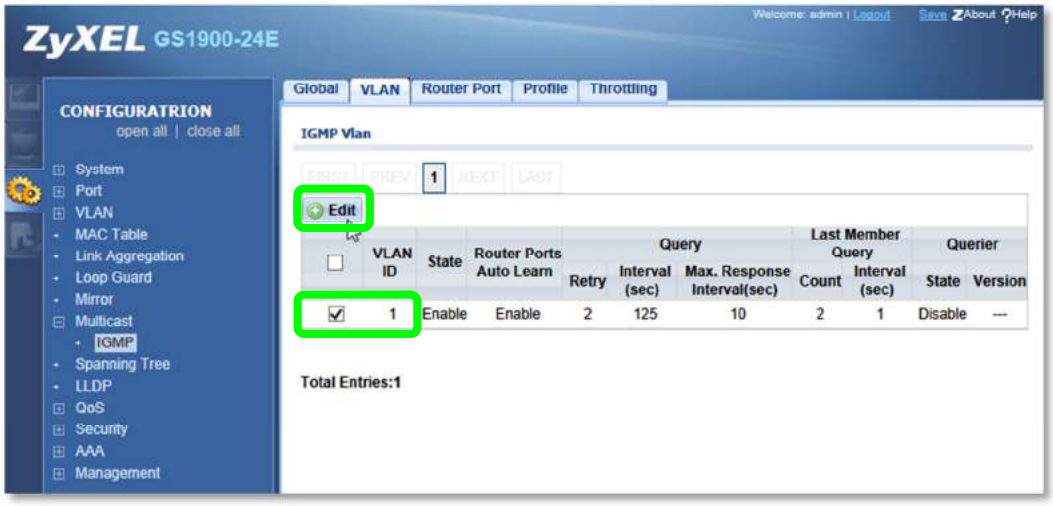
Managed Switch der GS1900-Serie (ab 2014)



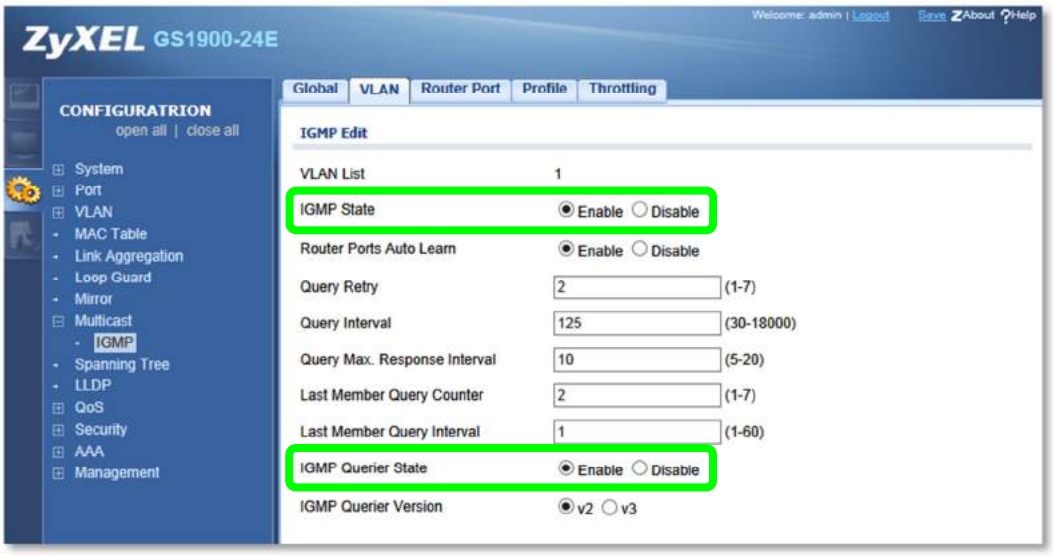
- Empfang von IPTV und Internet-Zugang funktioniert.
- Der Switch signalisiert auf allen aktiven Ports eine hohe Aktivität (= Multicast Flooding).
- Lösung: Über das Menü "*Configuration > Multicast > IGMP > Global*" die globale IGMP-Unterstützung aktivieren.



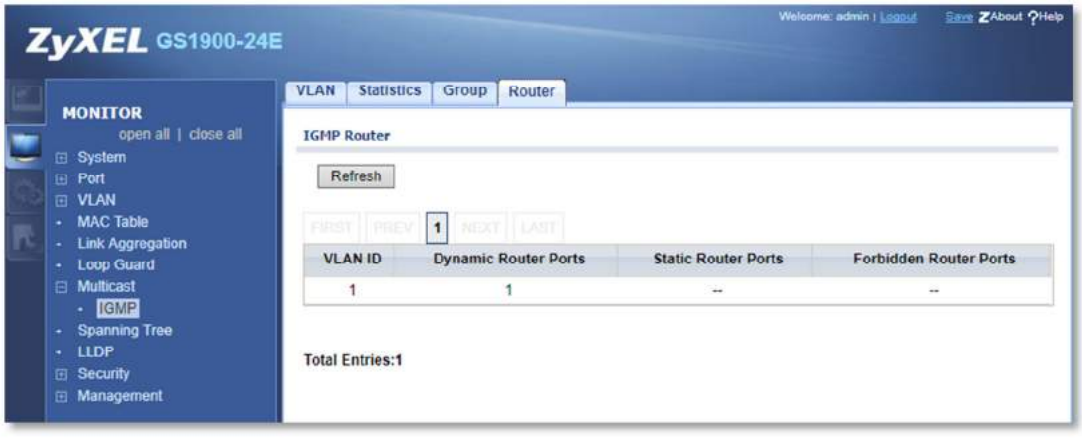
- Im Register "*VLAN*" das VLAN1 auswählen, editieren und...



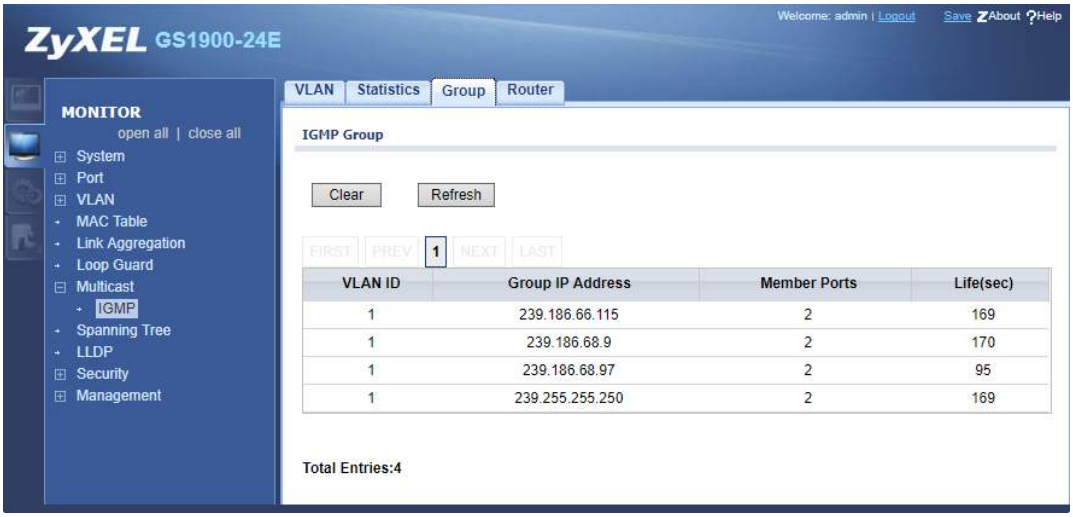
...die Optionen "*IGMP State*" und "*IGMP Querier State*" aktivieren. So verfolgt der Switch die Gruppierungs-Informationen und verteilt Multicast-Pakete nur noch an in IPTV involvierte Ports.



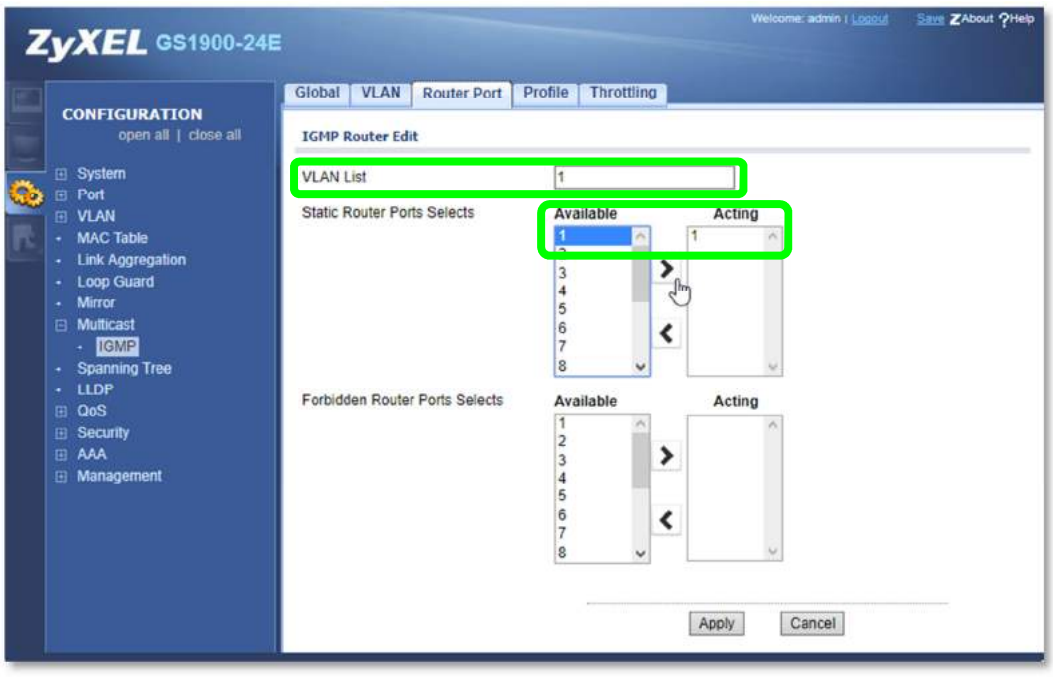
- **Optional:** Normalerweise erkennt der Switch über die IGMP-Snooping-Funktion automatisch, an welchem Port der Router für den Empfang der Multicast-Daten angeschlossen ist. Der Monitor führt dann diesen Port unter 'Dynamic Router Ports' auf.



An einigen wenigen Standorten brach der Multicast-IPTV-Stream trotz korrekter Konfiguration des Switch jeweils nach kurzer Zeit ab. Der IGMP-Monitor zeigte, dass der Switch die aktuellen IGMP-Streams lange vor Ablauf des Timers '*Life(sec)*' aus der Group-Tabelle entfernte.

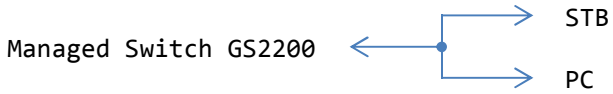


Abhilfe schafft das manuelle Festlegen des Router-Ports unter "*Configuration* > *Multicast* > *IGMP* > *Router Port*". Wählen Sie dazu das VLAN 1 und unter "*Static Router Ports Selects*" den Port aus, an dem der Router für den Internet-Zugang angeschlossen ist.



Der Switch lernt so den Router-Port nicht mehr automatisch an. Es ist daher wichtig, dass der Internet-Router auch am fix definierten Switch-Port angeschlossen ist.

Managed Switch der GS/XS1920 oder GS2200-Serie



- Empfang von IPTV und Internet-Zugang funktioniert.
- Der Switch signalisiert auf allen aktiven Ports eine hohe Aktivität (= Multicast Flooding).

Lösung: Unter "*Advanced Application* > *Multicast* > *Multicast Setting*" das IGMP Snooping aktivieren. Deaktivieren von "*Unknown Multicast Flooding*" verhindert, dass der Switch unbekannten Multicast-Traffic auf alle Ports weiterleitet. Je nach Provider kann die Option "*Fast Leave*" den schnellen Kanal-Wechsel begünstigen.