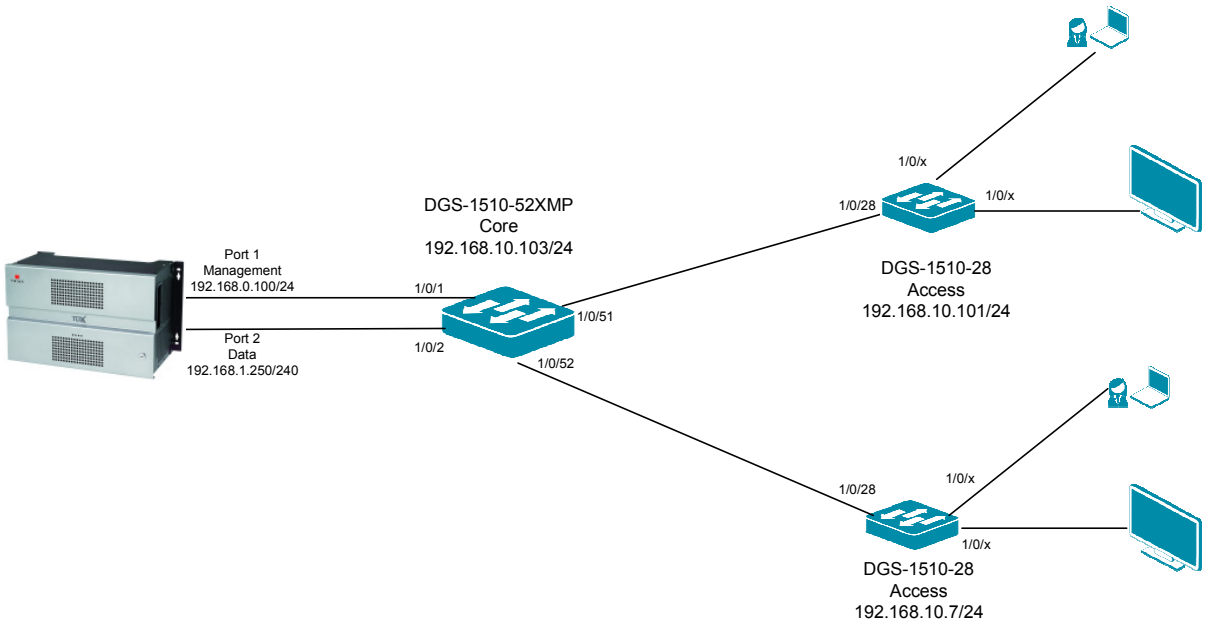
D-Link –Triax IPTV Solution
Installationshinweise für den DGS-1510-xx

[Voraussetzungen]

1. DGS-1510-xx mit aktueller Firmware 1.50B13 und höher

[Topologie]



[Vorbereitung]

- ⇨ Der DGS-1510-xx hat im Auslieferungszustand die Standard IP 10.90.90.90/8
- ⇨ Bitte ändern Sie dies bei der Ersteinrichtung (Integration in Ihre bestehende Infrastruktur) des DGS-1510-xx in Ihrem Netzwerk, für die genaue Vorgehensweise der Einstellung der IP & des Benutzernamens schlagen Sie bitte im Handbuch (z.B.: ftp://ftp.dlink.de/dgs/dgs-1510-52XMP/documentation) nach
- ⇨ Die aktuelle Firmware können Sie jederzeit von unserem FTP-Server (z.B. ftp://ftp.dlink.de/dgs/dgs-1510-52XMP/driver_software) herunterladen.

[Hinweis]

In diesem Testaufbau werden keine VLANs (alle Daten werden im VLAN 1 übertragen) verwendet um die jeweiligen IP-Subnetze voneinander zu trennen. Sollten Sie in Ihrem Aufbau VLANs verwenden, so können Sie diese Anleitung für Ihre VLAN-Definition anpassen.

[IP Adresse des Switches anpassen]

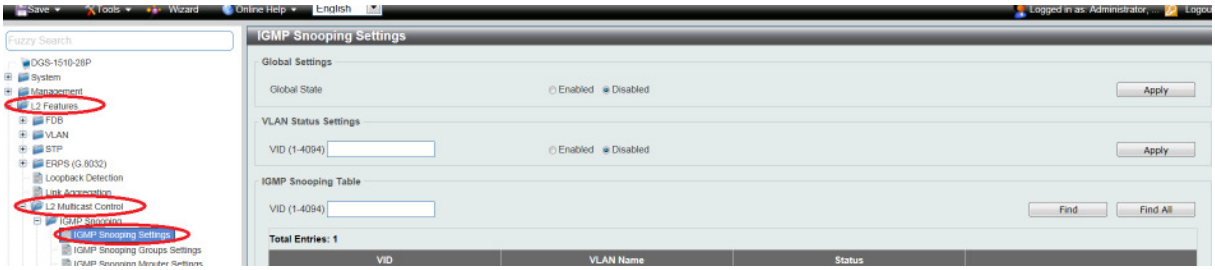
1.) **laden Sie von unserem FTP-Server den D-Link Network Assistant (DNA) sowie die jeweilige Firmware herunter und installieren Sie den DNA auf Ihrem Client**
   a. ftp://ftp.dlink.de/dgs/dgs-1510-20/driver_software/DGS-1510-20_sw_Network-Assistant_2-0-2-4_all_en_20151019.zip

2.) **folgen Sie der Anleitung zur Einrichtung der Management-IP Adresse (VLAN1) des DGS-1510**
   a. ftp://ftp.dlink.de/dgs/dgs-1510-20/documentation/DGS-1510-Series_HowTo_Anpassen_der_IP_Adresse_via_DNA.pdf
   b. Verbinden Sie sich anschließend per Webbrowser auf den Switch mit der von Ihnen vergebenen IP Adresse und speichern diese Einstellungen ab. (z.B. IP 192.168.10.103, Subnetzmaske 255.255.255.0, Gateway 192.168.10.1)

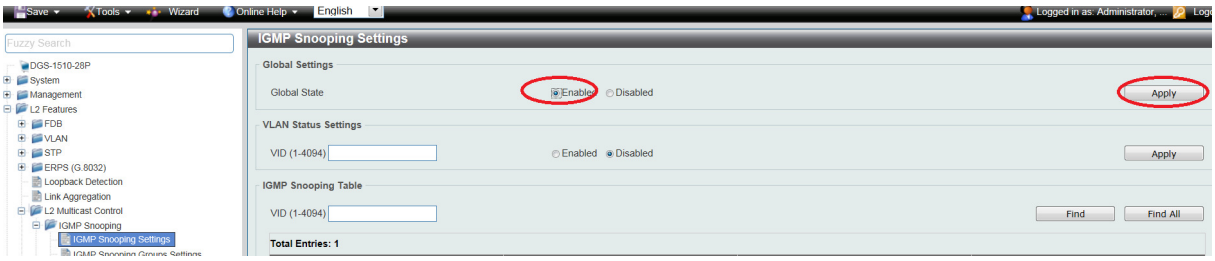
3.) **folgen Sie bei Bedarf der Anleitung zum Firmwareupdate des DGS-1510**
   a. ftp://ftp.dlink.de/dgs/dgs-1510-20/documentation/DGS-1510-Series_HowTo_Firmware-Update_via_DNA.pdf

[IGMP Snooping konfigurieren & aktivieren]

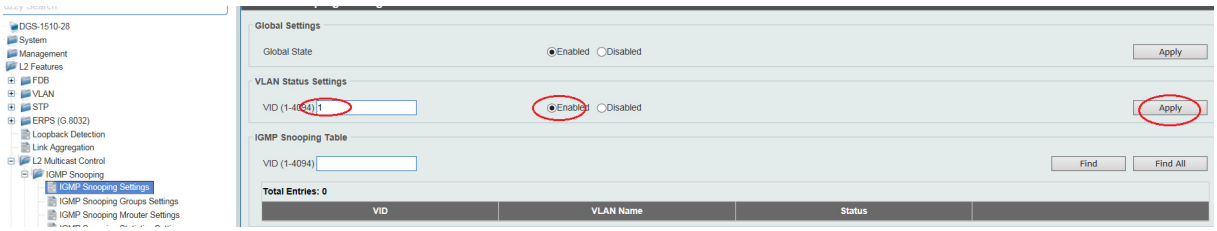
1.) **Verbinden zu den Switches (z.B. 192.168.10.7/101/103)**
   a. **L2 Features -> L2 Multicast Control -> IGMP Snooping Settings**



   b. **Aktivieren Sie den „Global State“ und bestätigen dies mit „Apply“**



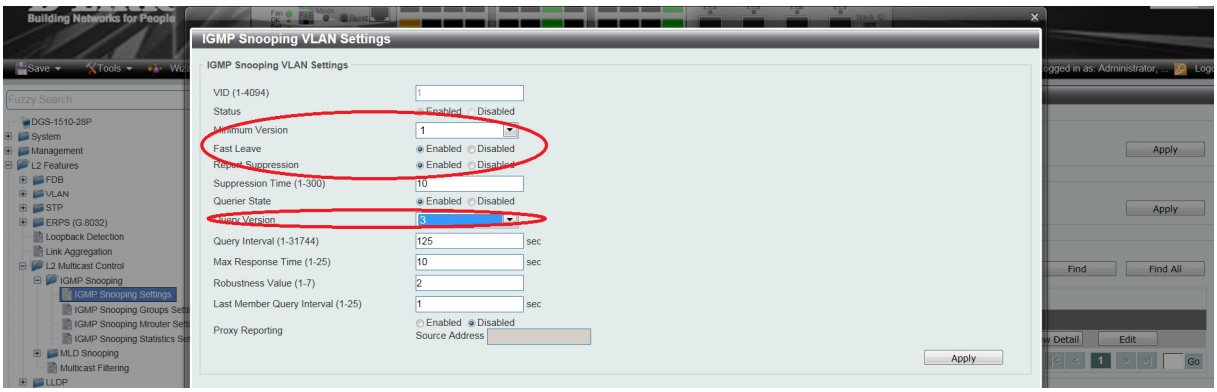
   c. **Tragen Sie im VLAN Status Settings Feld „VID“ die VLAN ID „1“ ein und Aktivieren Sie IGMP-Snooping für das VLAN und bestätigen dies mit „Apply“**



d. **Wählen Sie das VLAN 1 aus und passen die IGMP-Snooping Einstellungen an, indem Sie auf „Edit“ klicken**

i. **Minimum Version = definiert auf welche minimale IGMP Snooping Version das Gerät reagiert**
ii. **Fast Leave = beschleunigt das „Verlassen“ der IGMP-Gruppe durch den Client bei der Benutzung von IGMPv2 und/oder IGMPv3,**
iii. **Report Supression = verringert die Anzahl der IGMP-Meldungen an den Router bei IGMPv2 und/oder IGMPv3**
iv. **Querry Version = definiert die Zusammenfassung der einzelnen Multicast Gruppen, bitte die Version 3 auswählen**
v. **mittels „Apply“ bestätigen Sie Ihre Eingabe**

e. **Tragen Sie somit folgende Werte ein:**
i. **Minimum Version = 2**
ii. **Fast Leave = Enabled**
iii. ***Querier State = Enabled***
iv. ***Query Version = 3***
v. **mittels „Apply“ bestätigen Sie Ihre Eingabe**

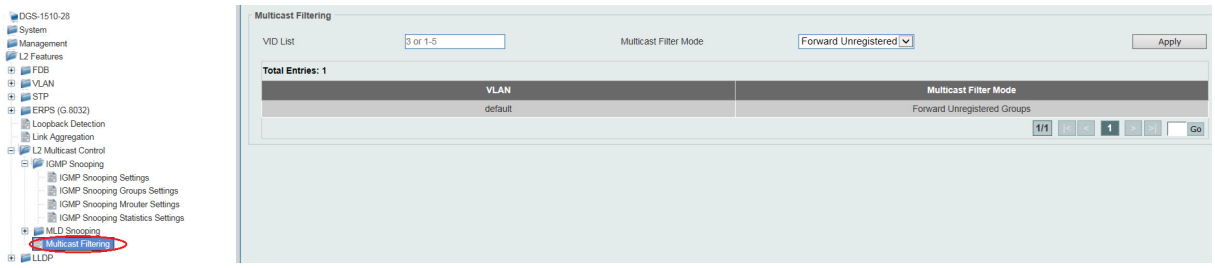


Die Option „Querier State“ darf nur am DGS-1510-52XMP Core (192.168.10.103/24) in diesem Beispielaufbau aktiviert werden, da es im IGMP-Snooping nur einen Querrier geben darf.

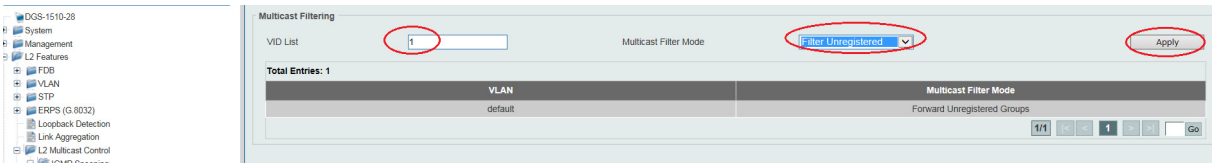
Sollte Ihr Design vom Testaufbau abweichend sein, so empfiehlt sich das Gerät, an welchem die IGMP-Quellen anliegen als Querrier zu definieren.

[Unterbinden des Weiterleitens der unregistierten Gruppen an die Engeräte]

a. L2 Features -> L2 Multicast Control -> Multicast Filtering



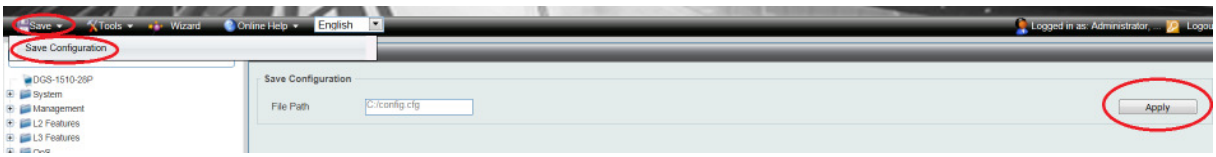
a. Tragen Sie im VLAN List Feld die VLAN ID „1“ ein und stellen den Modus auf „Filter Unregistered Groups“ und bestätigen dies mit „Apply“



Mit dieser Anpassung werden keine Multicast Datenströme mehr unangefordert an die Endgeräte mehr weitergeleitet.

Einzig an Clients, welche per IGMP Join nach dedizierten Datenströmen anfragen, werden genau diese übertragen.

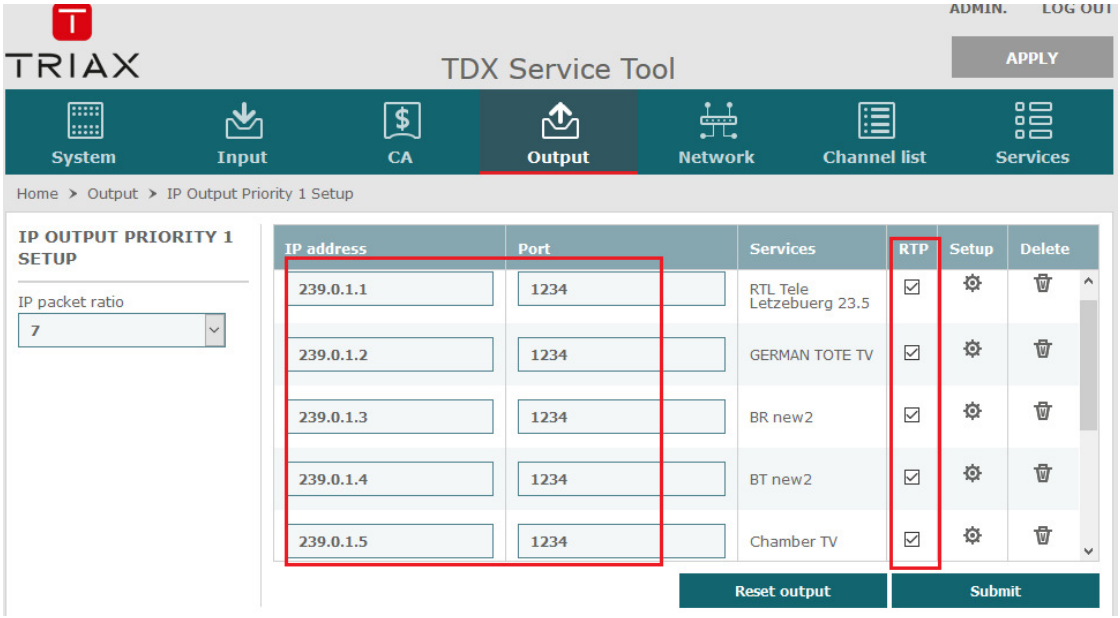
Bitte beachten Sie, dass Sie alle Anpassungen entsprechend speichern.



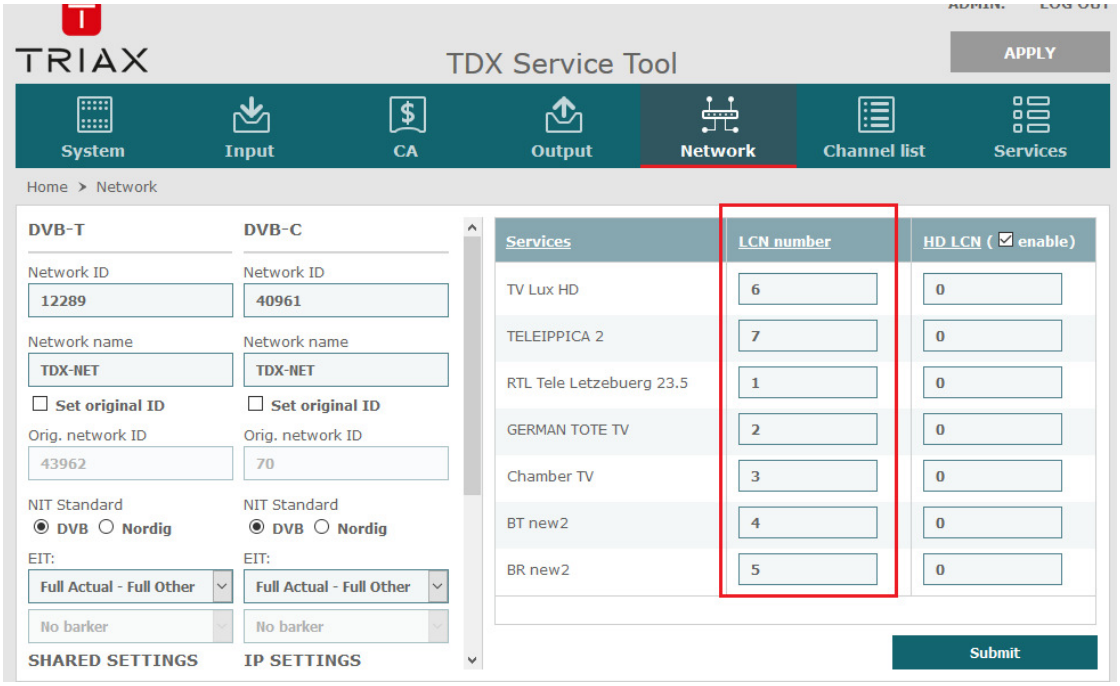
[Triax TDX Multicast Streams definieren.]

Für die Konfigurationen der TDX nutzen Sie sich bitte die verfügbare Dokumentation des Triax-Support, oder kontaktieren Sie diesen direkt.

**Definieren Sie die zu verwendenden IP-Multicast IP Adressen und Ports.
Zudem stellen Sie sicher, dass die Option RTP aktiviert ist, da diverse IPTV TV-Endgeräte (z.B. Panasonic TV) nur dieses Protokoll unterstützen.**



Weiterhin ist es für diverse Endgeräte (z.B. Panasonic TV) notwendig die Reihenfolge (LCN) in der M3U-Playlist zu definieren.



Mittels Submit & Apply übernehmen Sie diese Einstellungen.

Die für IPTV TV's notwendige M3U-Playlist können Sie direkt von der TDX herunterladen.

Passen Sie hierzu die URL folgendermaßen an:

<http://Management-IP Ihrer TDX>/satip.m3u

In diesem Beispiel lautet die URL somit „ http://192.168.0.100/satip.m3u ". Speichern Sie die M3U-Datei um diese dann auf den TV-Geräten einzuspielen.

In unserem Beispiel sieht die M3U-Datei folgendermaßen aus.

„

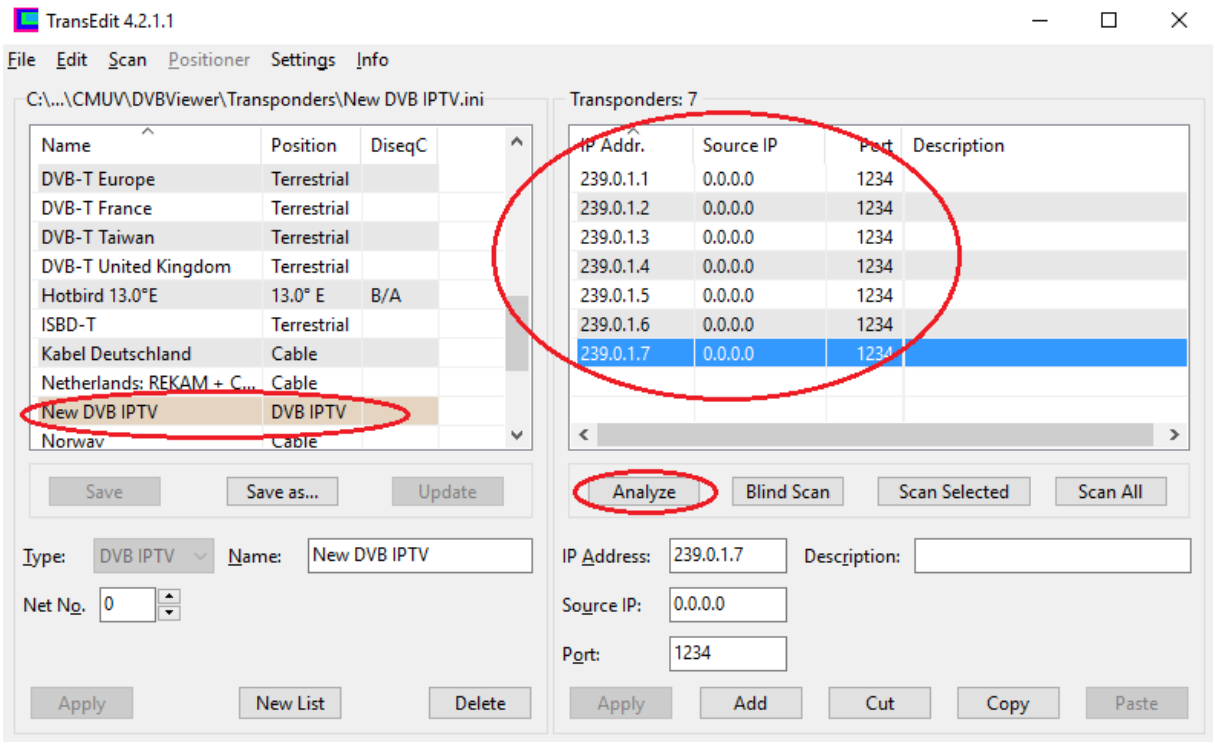
```
#EXTM3U
#EXTINF:0,1. RTL Tele Letzebuerg 23.5
rtp://239.0.1.1:1234?stype=1&onid=43962&tsid=0&svcid=6
#EXTINF:0,2. GERMAN TOTE TV
rtp://239.0.1.2:1234?stype=1&onid=43962&tsid=0&svcid=3
#EXTINF:0,5. BR new2
rtp://239.0.1.3:1234?stype=1&onid=43962&tsid=0&svcid=2
#EXTINF:0,4. BT new2
rtp://239.0.1.4:1234?stype=1&onid=43962&tsid=0&svcid=1
#EXTINF:0,3. Chamber TV
rtp://239.0.1.5:1234?stype=1&onid=43962&tsid=0&svcid=5
#EXTINF:0,7. TELEIPPICA 2
rtp://239.0.1.6:1234?stype=1&onid=43962&tsid=0&svcid=7
#EXTINF:0,6. TV Lux HD
rtp://239.0.1.7:1234?stype=1&onid=43962&tsid=0&svcid=4
```

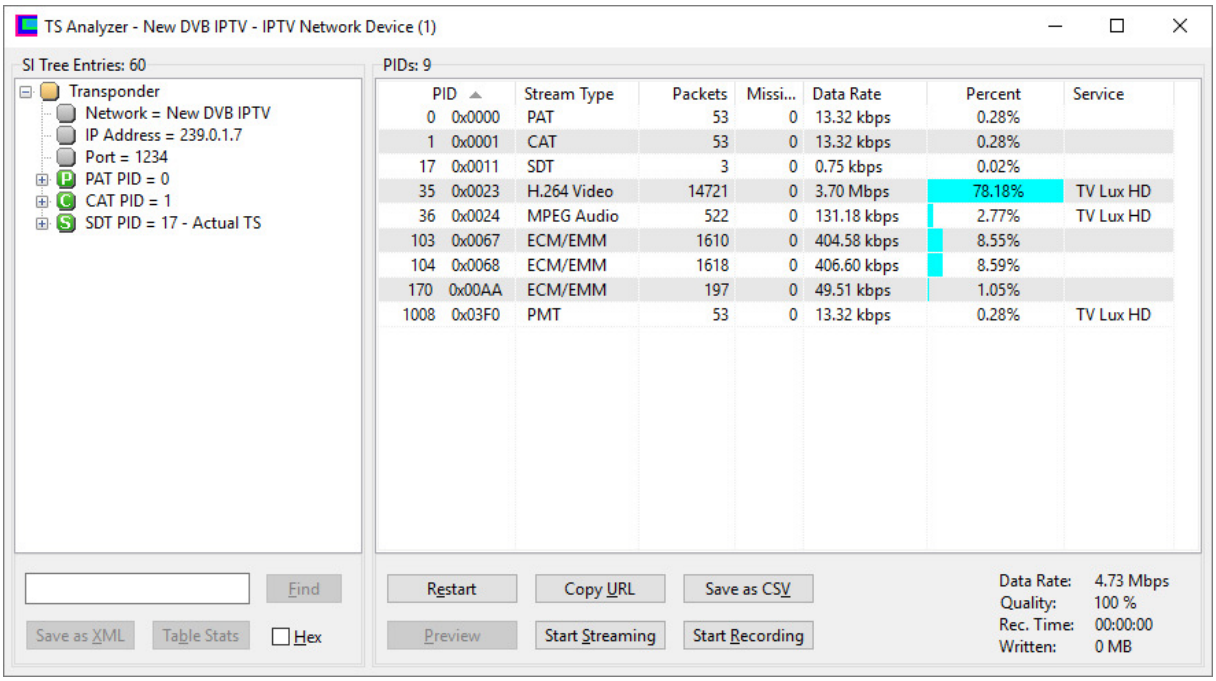
"

Die rot-Markierte Nummer ist die LCN Nummer, welcher der Nummerierung der Streams in den Endgeräten dient.

[IP-Multicast Datenstrom prüfen]

Auf der Webseite www.dvbviewer.com ist kostenpflichtig der DVB-Viewer erhältlich. Mittels des dort verfügbaren Tools „Transedit“ kann die Qualität des Streams relativ leicht geprüft werden.

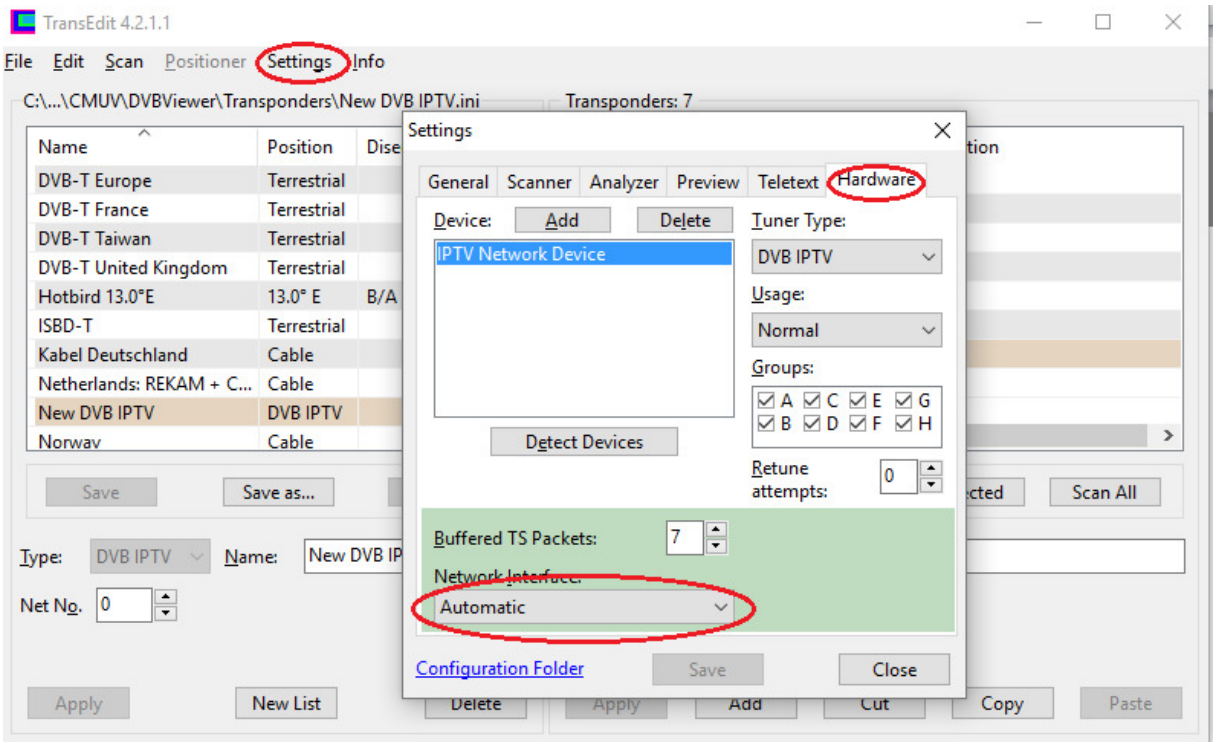




Für die genaue Anleitung zur Benutzung des Tools „Transedit“ konsultieren Sie bitte den Anbieter oder das verfügbare Handbuch.

TIPP:

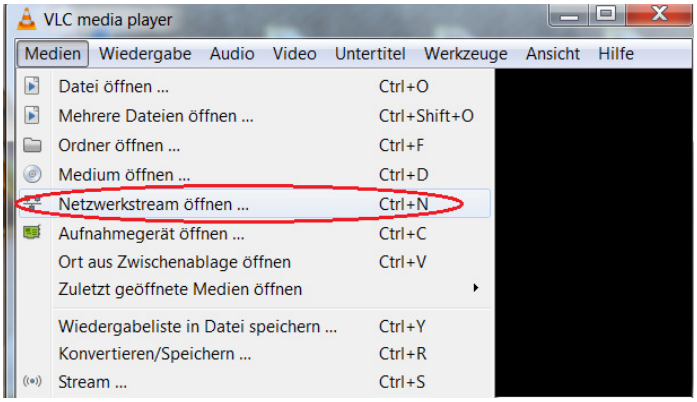
Bei Verfügbarkeit von mehreren NIC oder IP-Adressen an Ihrem Test-Client empfiehlt es sich dem Tool „Transedit“ manuell das zu verwendende Interface/IP-Adresse mitzuteilen.



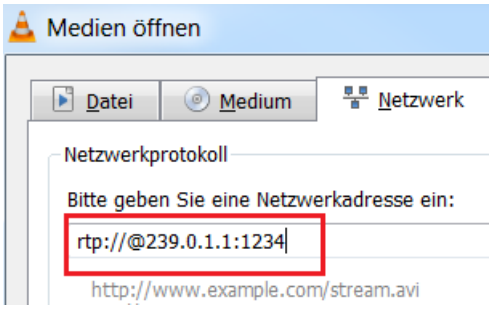
Auf der Webseite www.videolan.org ist der VLC-Mediaplayer erhältlich.
Mit diesem kann auch die Qualität eines Multicast-Streams geprüft werden.

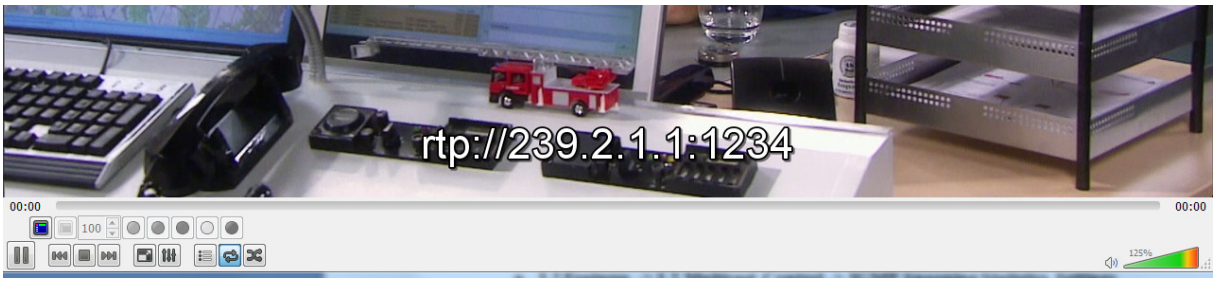
Rufen Sie einen Multicast Stream z.B. über die Multicast IP Adresse 239.0.1.1 Port 1234 ab

a. Starten des VLC und Abrufen eines Netzwerkstream

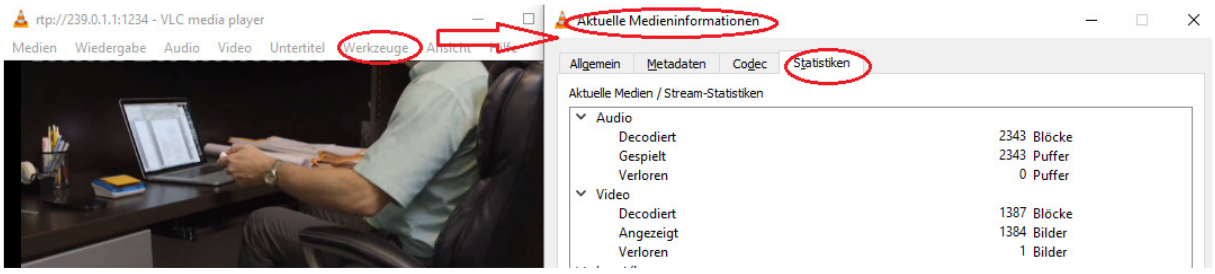


b. Abrufen der Multicast Adresse via RTP Protokoll (rtp://@239.0.1.1:1234)





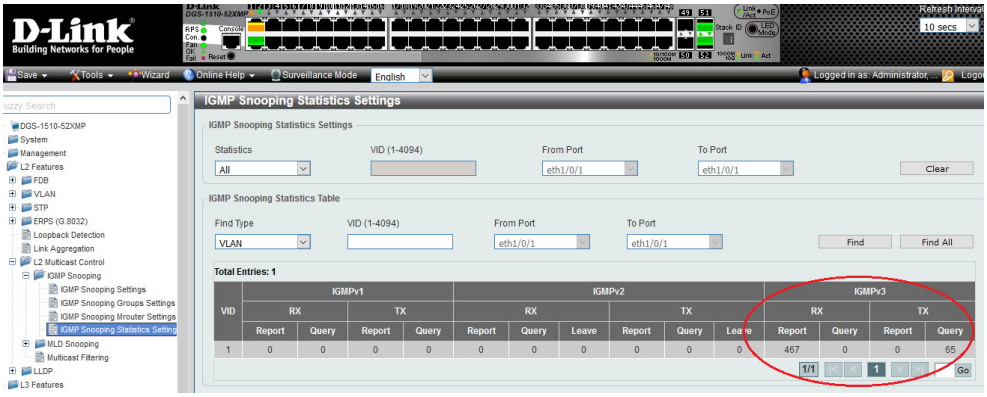
Über die Option „Werkzeuge“ können Sie sich die „Medieninformationen“ oder „Codec-Informationen“ anzeigen lassen.



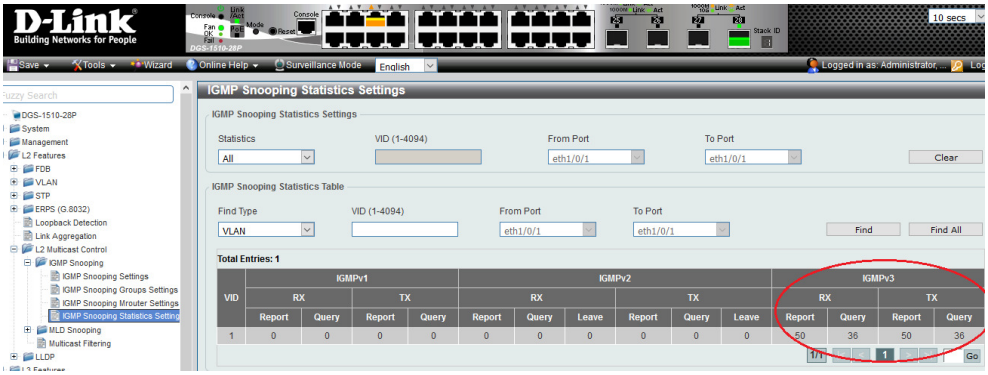
[IP-Multicast Datenstrom prüfen]

Um die korrekte Funktion von IGMP zu prüfen können Sie folgendermaßen vorgehen.

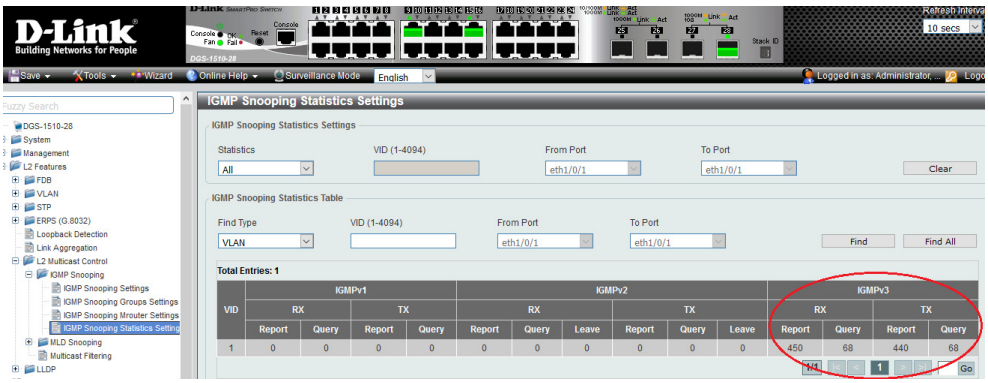
1.) **Verbinden zum Switch (z.B. 192.168.10.103/101/7)**
   a. **L2 Features -> L2 Multicast Control -> IGMP Snooping Statistics Settings**
      i. **IGMP-Snooping Statistics am Querrier (192.168.10.103)**
         An diesem Switch ist kein Endgerät angeschlossen.



      ii. **IGMP-Snooping am Access-Switch 1 (192.168.10.101)**
         An diesem Switch ist 1x Panasonic IPTV-TV Endgerät angeschlossen



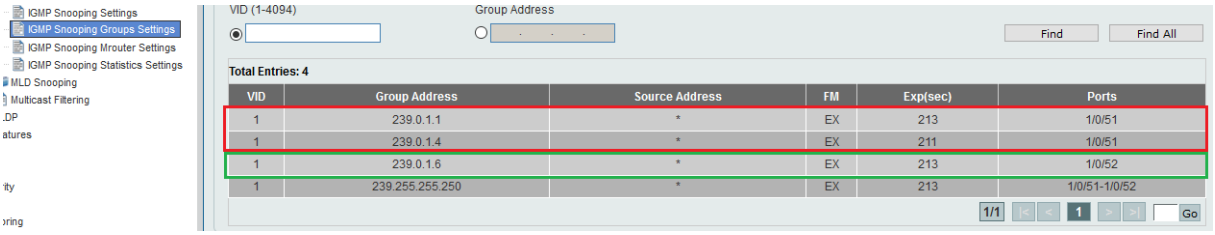
      i. **IGMP-Snooping am Access-Switch 1 (192.168.10.101)**
         An diesem Switch ist 1x Notebook mit VLC & DVB-Viewer angeschlossen



b. L2 Features -> L2 Multicast Control -> IGMP Snooping Group Settings

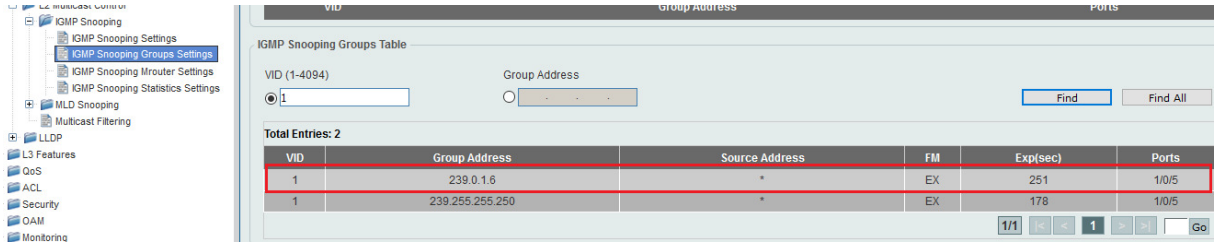
i. IGMP-Snooping Statistics am Querrier (192.168.10.103)

An diesem Switch ist kein Endgerät angeschlossen. Die Access-Switches (Port 1/0/51 & 1/0/52) fragen insgesamt 3 Streams ab (239.0.1.1 & 239.0.1.4 & 239.0.1.6)



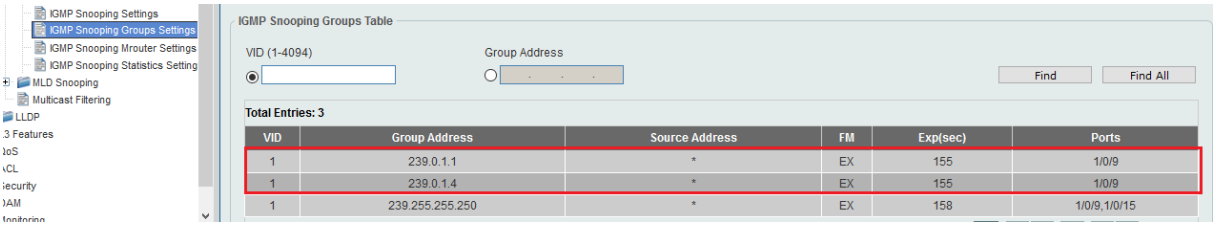
ii. IGMP-Snooping am Access-Switch 1 (192.168.10.101)

An diesem Switch ist 1x Panasonic IPTV-TV Endgerät angeschlossen (Port 1/0/5), dieses Endgerät ruft aktuell 1 Stream ab (239.0.1.6)



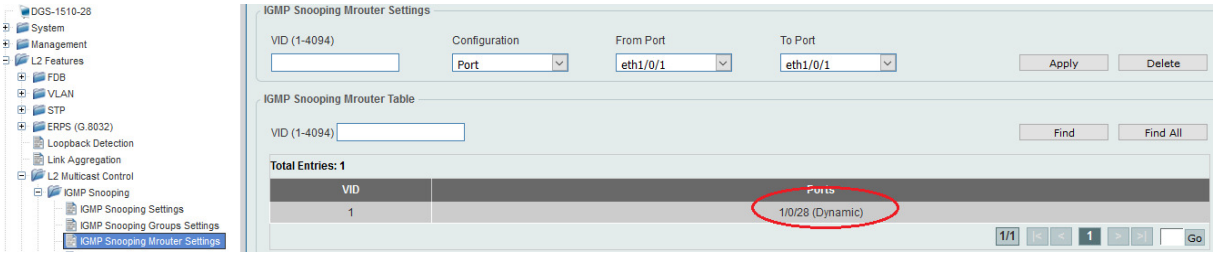
iii. IGMP-Snooping am Access-Switch 1 (192.168.10.101)

An diesem Switch ist 1x Notebook mit VLC & DVB-Viewer angeschlossen (Port 1/0/9), dieser Client ruft aktuell 2 Streams parallel ab (239.0.1.1 & 239.0.1.4)

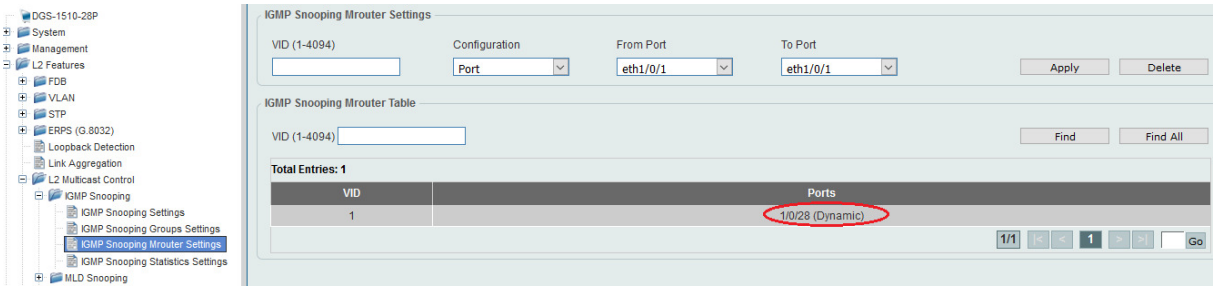


Mittels des IGMP-Snooping MRouter Port können Sie den Multicast Eingang an den Access-Switches prüfen:

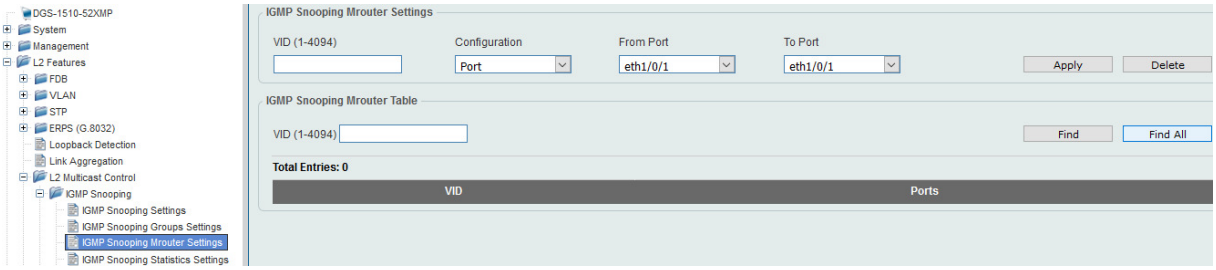
Access-Switch 192.168.10.7



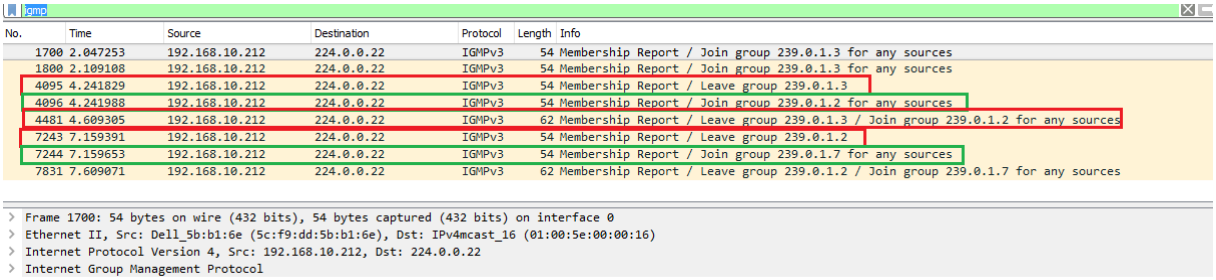
Access-Switch 192.168.10.101



Core-Switch 192.168.10.103



Die korrekte IGMP-Snooping Funktion eines Client können Sie bei einem Kanalwechsel am Client mit entsprechenden Tools (z.B. Wireshark) prüfen.



Bei einem entsprechend korrekt konfigurierten Endgerät werden IGMP-JOINS und IGMP-LEAVE bei jedem Kanalwechsel angezeigt.

[Konfiguration via CLI / Console (serieller Schnittstelle)]

Konfiguration des Switches per CLI

```
Switch#config terminal                                          || den Konfigurationsmodus des DGS-1510 betreten
Switch(config)#
Switch(config)#interface vlan 1                                 || das IP Interface für das VLAN 1 betreten
Switch(config-if)#ip address 192.168.0.103 255.255.255.0        || IP Adresse und Subnetzmaske für das VLAN 1
                                                                || IP Interface vergeben
Switch(config-if)#exit                                          || Verlassen des IP Interface Konfigurationsmodus
Switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.1             || je nach Bedarf das Default Gateway 192.168.0.1
                                                                || eintragen
Switch(config)#ip igmp snooping                                 || aktivieren von IGMP Snooping Global auf dem Switch
Switch(config)#vlan 1                                           || VLAN 1 betreten
Switch(config-vlan)#ip igmp snooping minimum-version 2          || IGMP Snooping Minimum Version 2 im VLAN 1
Switch(config-vlan)#ip igmp snooping query-version 3            || IGMP Snooping Querry Version 3
Switch(config-vlan)#ip igmp snooping querier                    || aktivieren IGMP Querrier im VLAN 1
Switch(config-vlan)#ip igmp snooping                            || aktivieren IGMP Snooping im VLAN 1
Switch(config-vlan)#multicast filtering-mode filter-unregistered || aktivieren des Filterns der unregistrierten Gruppen
Switch(config-vlan)#exit                                        || verlassen des VLAN Konfigurationsmodus
Switch(config)#exit                                             || verlassen des Switch Konfigurationsmodus
Switch#copy running-config startup-config                       || speichern der Konfiguration

Destination filename startup-config? [y/n]:  y
```

Den IGMP-Querrier dürfen Sie nur an einem Switch im Nerzwerk aktivieren.

Prüfen des IGMP-Snooping des Switches per CLI

Switch#sh ip igmp snooping groups

IGMP Snooping Connected Group Membership:

VLAN ID	Group address	Source address	FM	Exp(sec)	Interface
1	239.0.1.1	*	EX	157	1/0/51
1	239.0.1.4	*	EX	152	1/0/51
1	239.0.1.6	*	EX	157	1/0/52
1	239.0.1.7	*	EX	156	1/0/51
1	239.255.255.250	*	EX	158	1/0/51-1/0/52

Total Entries: 5

Switch#

Die IGMP-Empfänger timen automatisch nach 5 Minuten aus. Bei korrektem IGMP-Snooping wird der Timer nach der ½ Zeit (130 Sekunden) wieder auf die volle Zeit (260 Sekunden) zurückgesetzt.

Switch#sh ip igmp snooping groups

IGMP Snooping Connected Group Membership:

VLAN ID	Group address	Source address	FM	Exp(sec)	Interface
1	239.0.1.1	*	EX	260	1/0/51
1	239.0.1.4	*	EX	260	1/0/51
1	239.0.1.6	*	EX	259	1/0/52
1	239.0.1.7	*	EX	257	1/0/51
1	239.255.255.250	*	EX	259	1/0/51-1/0/52

Total Entries: 5

Switch#show ip igmp snooping statistics vlan 1

VLAN 1 Statistics:
IGMPv1 Rx: Report 0, Query 0
IGMPv2 Rx: Report 0, Query 0, Leave 0
IGMPv3 Rx: Report 691, Query 0
IGMPv1 Tx: Report 0, Query 0
IGMPv2 Tx: Report 0, Query 0, Leave 0
IGMPv3 Tx: Report 0, Query 88

Total Entries: 1