Brought to you by BLANKOM

IGMP-Snooping: Das Abhörverfahren für Multicast-Traffic

Multicast-Verbindungen stellen eine hervorragende Möglichkeit dar, um ein und dasselbe Datenpaket in IP-Netzwerken an **viele verschiedene Empfängergeräte** zu verschicken, ohne jedes dieser Geräte separat adressieren und beliefern zu müssen. Der Sender des Pakets verteilt diese Aufgabe auf die diversen Knoten der involvierten **Subnetze** und spart dadurch wertvolle Ressourcen. Insbesondere **Internet-Echtzeitanwendungen**, die von zahlreichen Nutzern verwendet werden, profitieren von dieser Form von **Mehrpunktverbindungen**, die mithilfe spezieller Multicast-Gruppen geschaffen werden.

Einen großen Anteil an der Organisation dieser Gruppen hat das Protokoll IGMP, das Grundstein für die reibungslose **IPv4-Multicast-Kommunikation** zwischen Sender, Routern und Empfängern ist. Darüber hinaus lässt sich der **Multicast-Verkehr** über **IGMP-Nachrichten filtern**, um die einzelnen Zielnetzwerke zu entlasten. Man spricht in diesem Fall auch von sogenanntem IGMP-Snooping.

Inhaltsverzeichnis

Hinweis

IGMP steht für „**Internet Group Management Protocol**“ – das IPv4-Protokoll zur Verwaltung von Multicast-Gruppen. Das Pendant für IPv6-Verbindungen ist das Protokoll „**Multicast Listener Discovery**“ (**MLD**).

Was ist IGMP-Snooping?

Multicast-Pakete durchlaufen auf ihrem Weg zu den Ziel-Hosts häufig mehrere Stationen. **Router** verwenden dabei das Verfahren **Protocol Independent Multicast (PIM)**, um die optimale Route zu errechnen und so den Datenstrom möglichst effizient weiterzuleiten. Netzwerk-Switches oder die multifunktionalen Internet-Router in Privathaushalten tun sich bei der Übermittlung von Multicast-Paketen hingegen deutlich schwerer: Da der Versuch scheitert, die Pakete wie gewohnt anhand der ausgewiesenen MAC-Adresse zuzuordnen (funktioniert nur bei Unicast-Verbindungen), leiten die Geräte die ankommenden Pakete mangels Alternativen an alle verfügbaren Geräte im jeweiligen Subnetz weiter.

An dieser Stelle kommt IGMP-Snooping (manchmal auch als „Multicast-Snooping“ bezeichnet) ins Spiel: Dieses Verfahren, das frei übersetzt so viel wie „IGMP-Schnüffeln“ heißt, macht seinem Namen alle Ehre und **belauscht sämtlichen IGMP-Traffic**, der zwischen Multicast-Routern und Hosts ausgetauscht wird. Switches oder Internet-Router, die IGMP-Snooping beherrschen und aktiviert haben, sind also in der Lage, die **Multicast-Aktivitäten der einzelnen Netzwerk-Teilnehmer zu überwachen**. Konkret bedeutet dies, dass die Geräte erfahren, wenn ein Host einer Multicast-Gruppe beitritt („Multicast-Query“) oder diese verlässt („Leave-Message“; erst ab IGMPv2). Auf Basis dieser Informationen kann dann in der MAC-Adresstabelle ein Eintragfür die mit dem Host verbundene Netzwerk-Schnittstelle angelegt bzw. entfernt werden.

Hinweis

IGMP-Snooping ist in RFC 4541 spezifiziert, wobei dieser Request for Comments nur den **Status „Informational“** hat. Das ist darauf zurückzuführen, dass gleich zwei Organisationen als verantwortliche Standardisierungsinstanzen für die Technik in Frage kommen – das **IEEE** (Institute of Electrical and Electronics Engineers), das Ethernet-Switches standardisiert, und die **IETF** (Internet Engineering Task Force), die u. a. für den IP-Multicasting-Standard verantwortlich ist.

Warum und in welchen Fällen lohnt sich IGMP-Snooping?

Multicast-Snooping hilft Switches und Internet-Routern dabei, **Multicast-Datenströme besonders effizient** an das gewünschte Ziel bzw. die gewünschten Ziele zu bringen. Wie wertvoll diese Unterstützung ist, wird deutlich, wenn eine derartige Filterungsmethode von Mehrpunktübertragungen fehlt: Die ankommenden Multicast-Pakete werden dann an alle Hosts des Netzwerks geschickt, die der Switch bzw. Internet-Router erreicht. Insbesondere in größeren Netzen sorgt diese Vorgehensweise für unnötig hohen Traffic, der sogar zu einer Überlastung des Netzes führen kann. Kriminelle können sich diesen Umstand sogar zunutze machen und einzelne Hosts oder das gesamte Netzwerk gezielt mit Multicast-Paketen überfluten, um diese wie bei einer klassischen DoS-/DDoS-Attacke in die Knie zu zwingen.

Mit eingeschaltetem IGMP-Snooping lassen sich derartige Überlastungsprobleme und Angriffsszenarien ausschließen. Alle Hosts des Netzwerks erhalten lediglich **Multicast-Traffic**, für den sie sich zuvor per Gruppenanfrage **angemeldet** haben. Der Einsatz der „Lausch“-Technik lohnt sich also überall dort, wo auf Applikationen zurückgegriffen wird, die sehr viel Bandbreite für sich beanspruchen. Beispiele hierfür sind **IPTV-** und andere **Streaming-Services** sowie **Webkonferenz-Lösungen**. Netzwerke, in denen nur wenige Teilnehmer und kaum Multicast-Verkehr vorhanden sind, profitieren allerdings nicht von dem Filter-Verfahren. Selbst wenn der Switch bzw. Router das Multicast-Snooping-Feature bietet, sollte es in diesem Fall ausgeschaltet bleiben, um unnötige Abhöraktivitäten zu unterbinden.

Das Internet Group Management Protocol (IGMP)

Normalerweise hat jedes Gerät in Ihrem Heimnetzwerk sein eigenes Sende- und Empfangsprofil. Das eine Gerät ruft gerade ein Update ab, das zweite ist mit einem Online Gameserver verbunden, etc. . Mit der Verbreitung von IP-TV steigt die Wahrscheinlichkeit das mehrere Geräte in Ihrem Haushalt das gleiche zur gleichen Zeit empfangen möchten. Sowohl für das Zugangsnetz Ihres Internetanbieters als auch Ihr Heimnetzwerk wäre es eine unnötige Verwendung von Bandbreite das gleiche Programm über einen jeweils separaten Stream zu verschiedenen Endgeräten zu übertragen.

Hier setzt das Prinzip des Multicasting an. Ein Datenstrom wird einmal gesendet, verteilt und gleichzeitig von mehreren Geräten empfangen.

Mit IP-TV gibt es wie über das Kabel- oder das Terrestrische Fernsehen ein Vielzahl von Programmen im Angebot. Alle Programme einfach auf Verdacht in einem Netzwerk zu senden, würde die Kapazität der Netzwerke sprengen. Effizienter wäre es das ein Gerät welches ein bestimmtes Programm empfangen möchte erst sein Interesse daran bekundet. Und nur wenn ein oder mehrere Geräte in Ihrem Heimnetzwerk Interesse an einem Programm haben wird es auch zu Ihrem Heimnetzwerk und an Ihr

Endgerät gesendet. Wird der Empfang von z.B. des ZDF an dem letzten Gerät in Ihrem Heimnetzwerk beendet, dann muß auch die Sendeaktivität zu und in Ihrem Netzwerk eingestellt werden.

Genau diese Funktion des “Interesse bekunden” und das Auswerten der Interessen übernimmt das Internet Group Management Protocol (IGMP) für das Internet Protokoll Version 4 (IPv4). IGMP kann für verschiedenste Anwendungen eingesetzt werden, IP-TV diente Eingangs als praxisnahes Beispiel. Im folgenden eine Grafik, welche die prinzipielle Architektur von IGMP für ein Heim- und Internetzugangsnetzwerk illustriert.

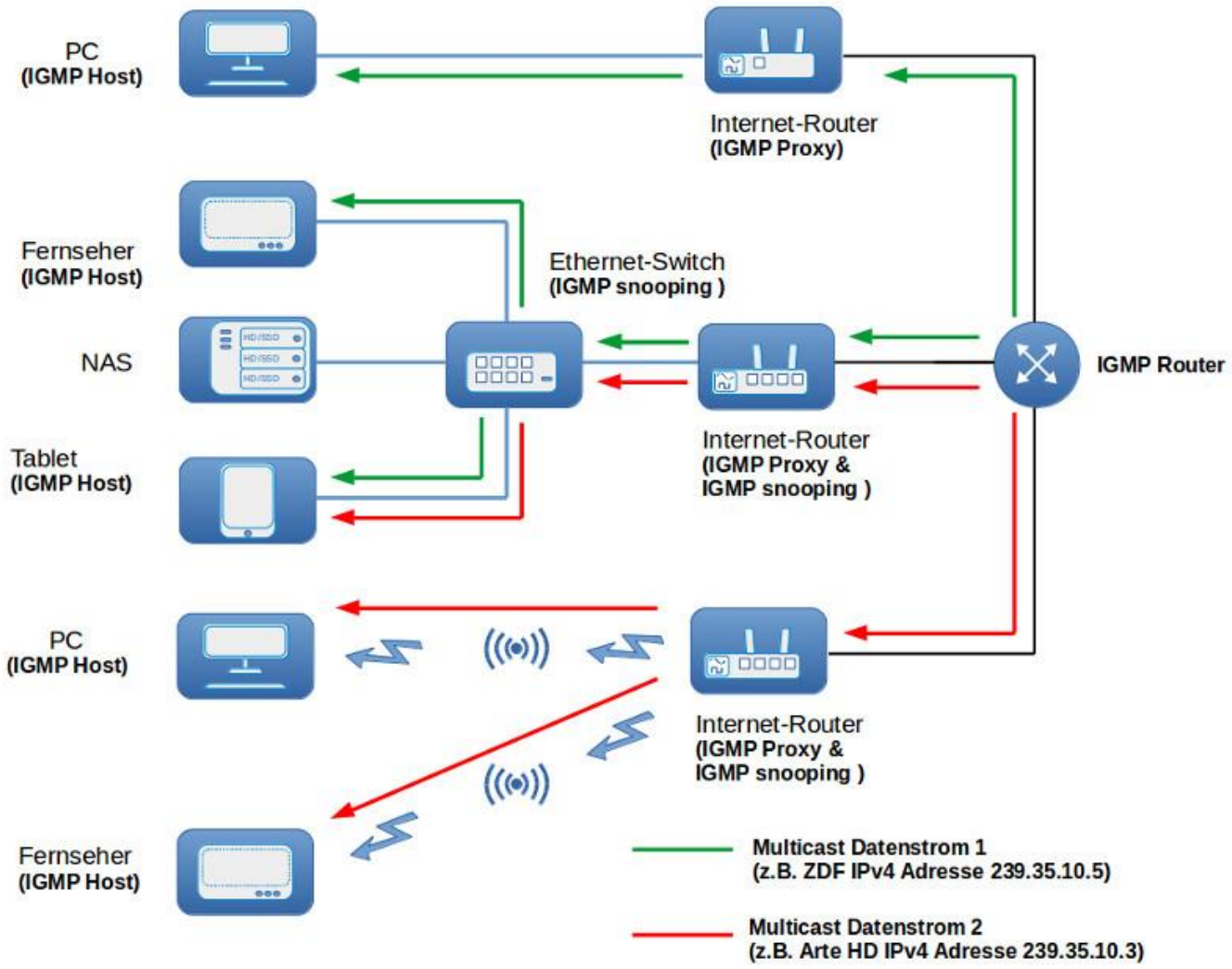


Bild: Internet Group Management Protocol Architektur (IGMP)

Mit Hilfe des IGMP Protokolls kann ein Endgerät sein Interesse bekunden einer oder auch mehreren bestimmten Multicast Gruppen beizutreten. Eine Multicast Gruppe definiert sich durch Ihre spezifische IPv4 Adresse aus dem Adressbereich 224.0.0.0 /4. Dieses Beitrittsersuchen wird von dem nächsten Router, in diesem Fall Ihrem Internet-Router empfangen und dann wiederum an den nächsten Router Ihres Internetanbieters weitergeleitet. Wenn der Router Ihres Internetanbieters keine Gründe sieht eine Anfrage zu verweigern, fängt dieser an den angeforderten Datenstrom zu senden. Falls ein zweites Endgerät der gleichen Multicast Gruppe beitreten möchte, dann kann Ihr Internet-Router dem Beitrittsersuchen direkt stattgeben und den schon empfangenen Datenstrom einfach weiter verteilen. Von Zeit zu Zeit erkundigt sich der Router Ihres Internetanbieters bei Ihrem Internet-Router ob und an welchen Multicast Gruppen noch Interesse besteht. Dieser Antwortet mit dem Status, welchen er selbst

durch seine Abfragen und entsprechende Reports der Endgeräte unterhält. Hat das letzte Endgerät eine Multicast Gruppe verlassen, bekommt das der Router Ihres Internetanbieters durch einen Report Ihres Internet-Routers mit und stellt die Sendeaktivität ein.

Ihr Internet-Router agiert dabei in der Rolle eines IGMP Proxy. Das bedeutet aus der Sicht Ihrer Endgeräte übernimmt der Internet-Router die Rolle des IGMP Multicast Routers, welcher Beitrittsgesuche empfängt und stattgibt und den Status der Multicast Mitgliedschaften über Abfragen unterhält. Aus Sicht des Routers Ihres Internetanbieters ist Ihr Internet-Router wiederum das Endgerät, welches Multicast Gruppen beitreten möchte und auf Anfragen antwortet ob Mitgliedschaften noch aktuell sind.

Notiz: Die aktuelle Version von IGMP ist die Version 3. Diese wird z.B. für die Realisierung des “Entertain” IP-TV Angebots der Telekom genutzt."

Wenn Sie in Ihrem Heimnetzwerk Ethernet-Switches einsetzen (auch wenn in einem Internet-Router integriert) , dann gibt es noch einen weiteren wichtigen Punkt zu beachten. Ein Ethernet-Switch arbeitet nach dem Prinzip das es ein Datenpaket dessen Ziel es nicht kennt, an alle ausgehenden Schnittstellen verteilt, außer an der Schnittstelle über welche das Datenpaket empfangen wurde. Normalerweise lernt ein Ethernet-Switch die verschiedenen angeschlossenen Ziele durch das Untersuchen der Quelladressen in den empfangenen Datenpaketen. Mit Hilfe dieser Untersuchung unterhält ein Ethernet-Switch eine Tabelle mit der Information hinter welcher Schnittstellen welche Ziele angebunden sind. Das Problem mit Multicasting ist, das eine Multicast Adresse nicht als Quelleadresse benutzt wird. Ein Ethernet-Switch kann damit nicht lernen welches Gerät welche Multicast Datenströme empfangen möchte und sendet im Endresultat Multicast Datenströme immer an alle ausgehenden Schnittstellen. Das kann zu einer Überlastung von Endgeräten und Netzwerkverbindungen führen. Um diese Problem zu Umgehen gibt es das sogenannte IGMP snooping. Das Prinzip ist einfach. Ein Ethernet-Switch belauscht den Datenverkehr. Werden IGMP Nachrichten an einer Schnittstelle entdeckt, dann werden diese mitgelesen und entsprechende Mitgliedschaften vermerkt. Ein Multicast Datenstrom wird danach nur an Schnittstellen weitergeleitet an welchen Mitglieder angeschlossen sind.

Tipp: Kurz zusammengefasst. Falls Sie IP-TV nutzen und Ethernet-Switches in Ihrem Netzwerk verwenden, dann ist es empfehlenswert darauf zu achten das diese IGMP snooping bis zur Version 3 unterstützen. Das gilt selbstverständlich auch für einen in einem Internet-Router integrierten Ethernet-Switch.

And now in english:

Brought to you by BLANKOM

IGMP Snooping: The Listening Method for Multicast Traffic

Multicast connections are an excellent way to send one and the same data packet in IP networks to many different recipient devices without having to address and deliver to each of these devices separately. The sender of the packet distributes this task among the diverse nodes of the involved subnets, thus saving valuable resources. In particular, real-time Internet applications used by numerous users benefit from this form of multipoint connections, which are created with the help of special multicast groups.

The IGMP protocol, which is the cornerstone for smooth IPv4 multicast communication between senders, routers and receivers, plays a major role in organising these groups. In addition, multicast traffic can be filtered via IGMP messages in order to relieve the individual target networks. In this case, one also speaks of so-called IGMP snooping.

Table of contents

Note

IGMP stands for "Internet Group Management Protocol" - the IPv4 protocol for managing multicast groups. The counterpart for IPv6 connections is the protocol "Multicast Listener Discovery" (MLD).

What is IGMP snooping?

Multicast packets often pass through several stations on their way to the destination hosts. Routers use the Protocol Independent Multicast (PIM) method to calculate the optimal route and thus forward the data stream as efficiently as possible. Network switches or the multifunctional internet routers in private households, on the other hand, have a much more difficult time transmitting multicast packets: Since the attempt to assign the packets as usual on the basis of the designated MAC address fails (only works with unicast connections), the devices forward the incoming packets to all available devices in the respective subnet for lack of alternatives.

This is where IGMP snooping (sometimes also called "multicast snooping") comes into play: This procedure, which loosely translates as "IGMP snooping", lives up to its name and eavesdrops on all IGMP traffic exchanged between multicast routers and hosts. Switches or Internet routers that are capable of IGMP snooping and have activated it are therefore able to monitor the multicast activities of the individual network participants. In concrete terms, this means that the devices learn when a host joins a multicast group ("multicast query") or leaves it ("leave message"; only from IGMPv2). Based on this information, an entry for the network interface connected to the host can then be created or removed in the MAC address table.

Note

IGMP snooping is specified in RFC 4541, whereby this Request for Comments only has the status "Informational". This is due to the fact that two organisations can be considered as responsible standardisation bodies for the technology - the IEEE (Institute of Electrical and Electronics Engineers), which standardises Ethernet switches, and the IETF (Internet Engineering Task Force), which is responsible for the IP multicasting standard, among other things.

Why and in which cases is IGMP snooping worthwhile?

Multicast snooping helps switches and Internet routers to bring multicast data streams particularly efficiently to the desired destination or destinations. The value of this support becomes clear when such a filtering method of multipoint transmissions is missing: The incoming multicast packets are then sent to all hosts of the network that the switch or Internet router reaches. Especially in larger networks, this procedure causes unnecessarily high traffic, which can even lead to an overload of the network. Criminals can even take advantage of this circumstance and deliberately flood individual hosts or the entire network with multicast packets in order to bring them to their knees as in a classic DoS/DDoS attack.

With IGMP snooping switched on, such overload problems and attack scenarios can be ruled out. All hosts in the network only receive multicast traffic for which they have previously registered via group request. The use of "eavesdropping" technology is therefore worthwhile wherever applications are used that require a lot of bandwidth. Examples of this are IPTV and other streaming services as well as web conferencing solutions. Networks with only a few participants and hardly any multicast traffic, however, do not benefit from the filtering method. Even if the switch or router offers the multicast snooping feature, it should remain switched off in this case to prevent unnecessary eavesdropping activities.

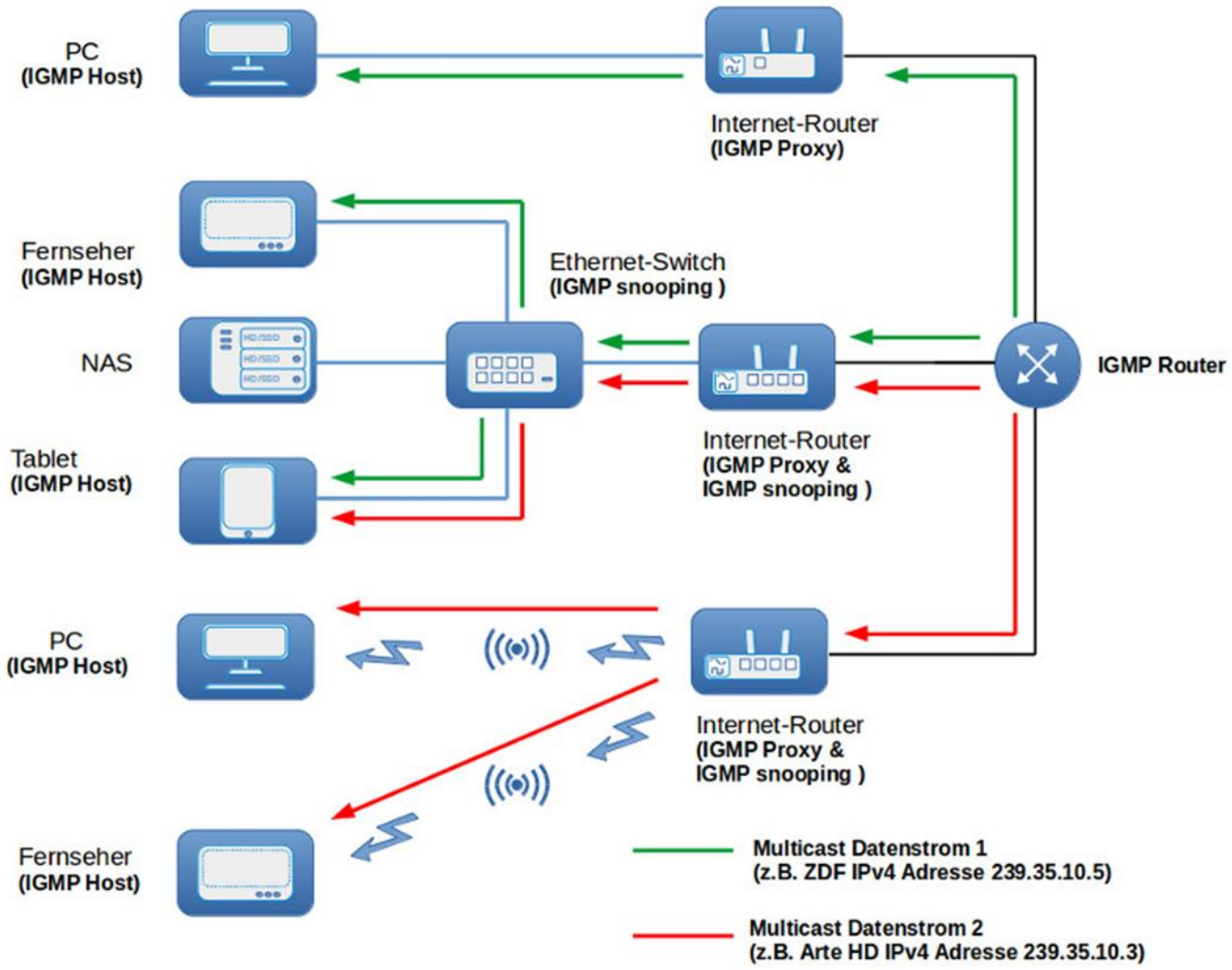
The Internet Group Management Protocol (IGMP)

Normally, each device in your home network has its own send and receive profile. One device is downloading an update, the second is connected to an online game server, etc. . With the spread of IP-TV, the likelihood of several devices in your household wanting to receive the same thing at the same time increases. For both the access network of your Internet provider and your home network, it would be an unnecessary use of bandwidth to transmit the same programme via a separate stream to different end devices.

This is where the principle of multicasting comes in. A data stream is sent once, distributed and received simultaneously by several devices.

With IP-TV, as with cable or terrestrial television, there is a multitude of programmes on offer. Simply broadcasting all programmes on a network on a hunch would go beyond the capacity of the networks. It would be more efficient if a device that wants to receive a certain programme first expresses its interest in it. And only if one or more devices in your home network are interested in a programme will it be sent to your home network and to your end device. If the reception of e.g. ZDF is stopped at the last device in your home network, then the transmission activity to and in your network must also be stopped.

Exactly this function of "expressing interest" and evaluating the interests is taken over by the Internet Group Management Protocol (IGMP) for the Internet Protocol Version 4 (IPv4). IGMP can be used for a wide variety of applications; IP-TV served as a practical example at the beginning. The following is a diagram illustrating the principle architecture of IGMP for a home and internet access network.



Picture: Internet Group Management Protocol architecture (IGMP)

With the help of the IGMP protocol, an end device can express its interest in joining one or more specific multicast groups. A multicast group is defined by its specific IPv4 address from the address range 224.0.0.0 /4. This request to join is received by the next router, in this case your Internet router, and then in turn forwarded to the next router of your Internet provider. If your ISP's router sees no reason to deny a request, it will start sending the requested data stream. If a second terminal wants to join the same multicast group, then your Internet router can directly grant the request to join and simply redistribute the data stream already received. From time to time, the router of your Internet provider inquires with your Internet router whether and in which multicast groups there is still interest. The router responds with the status that it maintains itself through its queries and corresponding reports from the end devices. If the last end device has left a multicast group, the router of your Internet provider receives this through a report from your Internet router and stops the transmission activity.

Your Internet router acts in the role of an IGMP proxy. This means that from the point of view of your end devices, the Internet router assumes the role of the IGMP multicast router, which receives and grants membership requests and maintains the status of the multicast memberships via queries. From the point of view of your ISP's router, your Internet router is in turn the end device that wants to join multicast groups and responds to queries about whether memberships are still current.

Note: The current version of IGMP is version 3, which is used, for example, for the realisation of the "Entertain" IP-TV offer of Telekom.

If you use Ethernet switches in your home network (even if integrated in an Internet router), there is another important point to note. An Ethernet switch works on the principle that it distributes a data packet whose destination it does not know to all outgoing interfaces, except to the interface via which the data packet was received. Normally, an Ethernet switch learns the various connected destinations by examining the source addresses in the received data packets. With the help of this examination, an Ethernet switch maintains a table with the information behind which interfaces which destinations are connected. The problem with multicasting is that a multicast address is not used as a source address. An Ethernet switch cannot learn which device wants to receive which multicast data streams and as a result always sends multicast data streams to all outgoing interfaces. This can lead to an overload of end devices and network connections. To circumvent this problem, there is the so-called IGMP snooping. The principle is simple. An Ethernet switch listens in on the data traffic. If IGMP messages are detected at an interface, they are read and the corresponding memberships are noted. A multicast data stream is then only forwarded to interfaces to which members are connected.

Tip: In a nutshell. If you use IP-TV and Ethernet switches in your network, it is recommended to make sure that they support IGMP snooping up to version 3. Of course, this also applies to an Ethernet switch integrated in an Internet router.