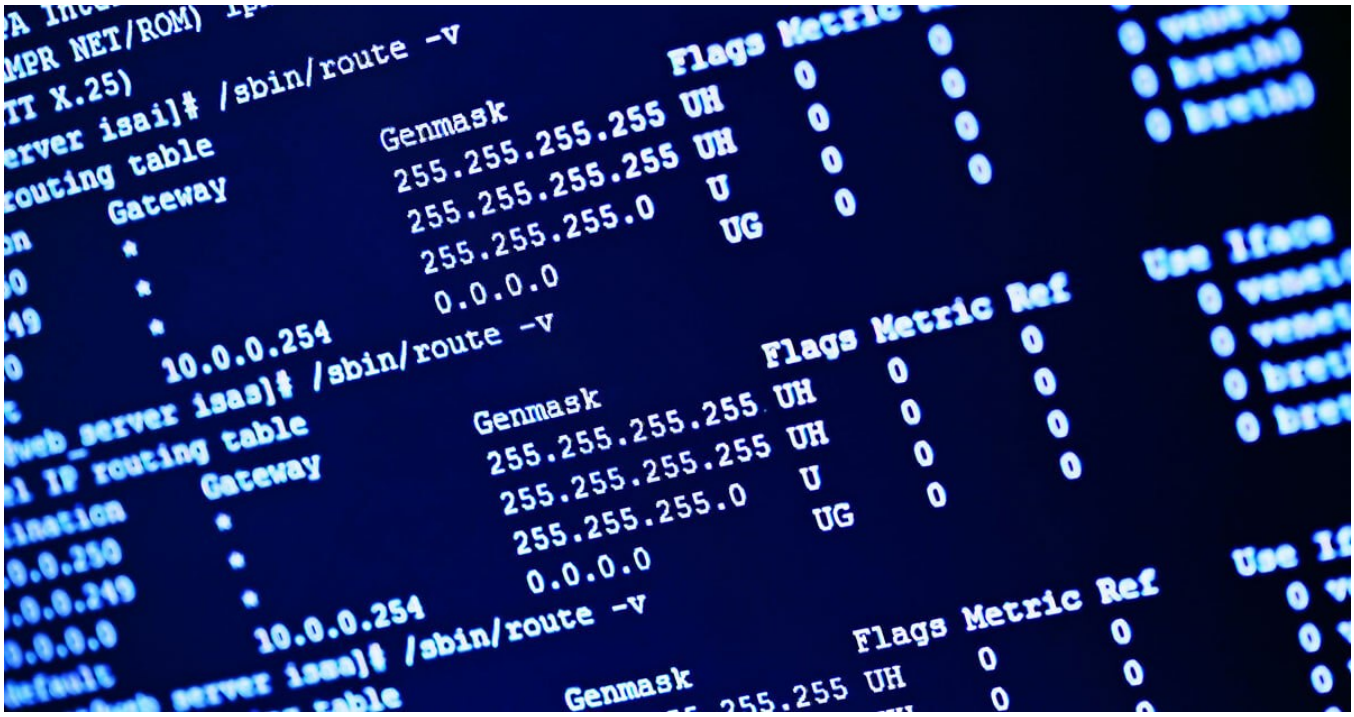



# TCP/IP – IGMP , Unicast + Multicast, Streaming Protokolle einfach erklärt! *TCP/IP … streaming protocols for dummies!*

Sie sind eine der **Grundlagen des Internets**: Ohne die TCP/IP-Protokolle wäre das tägliche Surfen durchs Netz nicht denkbar. Über die Protokolle – der Begriff fasst gleich mehrere Regelwerke zusammen – werden Datenpakete im Local Area Network (LAN) oder Wide Area Network (WAN) übertragen, also auch im World Wide Web bzw. dem Internet.

*They are one of the foundations of the Internet: without the TCP/IP protocols, daily surfing the net would be inconceivable. The protocols - the term summarizes several sets of rules - are used to transmit data packets in the Local Area Network (LAN) or Wide Area Network (WAN), i.e. also in the World Wide Web or the Internet.*

**Inhaltsverzeichnis / ToC of this chapter**



## Was ist TCP/IP? / What is TCP/IP?

**Definition: TCP/IP**

TCP/IP: Bei TCP/IP handelt es sich um eine Gruppe von Protokollen, die die Grundlage für das Internet und andere Netzwerke bilden. *TCP/IP: TCP/IP is a group of protocols that form the basis for the Internet and other networks.*

Der Name TCP/IP setzt sich aus den beiden für die Internetkommunikation entscheidenden Protokollen zusammen: dem Transmission Control Protocol (TCP) und dem Internet Protocol (IP). Dabei werden eigentlich sogar noch mehr Protokolle unter diesem Begriff zusammengefasst: Auch das Internet Control Message Protocol

(ICMP) und das User Datagram Protocol (UDP) zählt man zu dieser Gruppe. Bei TCP/IP selbst handelt es sich demnach nicht um eine bestimmte Technik, sondern um die Gruppierung von ausgewählten Protokollen. Allen gemeinsam ist, dass sie zu Standards bei der Kommunikation in Netzwerken geworden sind.

*The name TCP/IP is composed of the two protocols that are crucial for Internet communication: the Transmission Control Protocol (TCP) and the Internet Protocol (IP). Actually, even more protocols are combined under this term: The Internet Control Message Protocol (ICMP) and the User Datagram Protocol (UDP) also belong to this group. TCP/IP itself is therefore not a specific technology, but a grouping of selected protocols. What they all have in common is that they have become standards for communication in networks.*

Hinweis */ Note*
Wenn man von TCP/IP spricht, meint man manchmal auch die komplette Internetprotokollfamilie. Hierzu werden ca. 500 Protokolle gezählt, die im Internet eingesetzt werden.
*When one speaks of TCP/IP, one sometimes also means the complete Internet protocol family. There are about 500 protocols that are used on the Internet.*

## Wie funktioniert TCP/IP? / *How does it work?*

Die Protokolle des TCP/IP-Modells haben einen großen Vorteil: Sie funktionieren **losgelöst von der Hardware und der zugrundeliegenden Software**. Egal welches Betriebssystem man verwendet und welches Gerät man für die Kommunikation über das Netzwerk einsetzt, die Protokolle sind so standardisiert, dass sie in jedem Kontext funktionieren. *The protocols of the TCP/IP model have one major advantage: they work independently of the hardware and the underlying software. No matter what operating system you use and what device you use to communicate over the network, the protocols are standardized to work in any context.*

Im OSI-Modell nehmen die Protokolle die Schichten 3 und 4 ein. Transport- und Vermittlungsschicht kümmern sich direkt um die **Verbindung zwischen zwei Geräten über ein Netzwerk**. So wird beispielsweise mithilfe der IP-Adresse und dem Internetprotokoll das Datenpaket an den richtigen Empfänger gesendet. TCP hingegen ist dafür verantwortlich, eine Verbindung zwischen den beiden beteiligten Geräten aufzubauen und für die Übertragung aufrechtzuerhalten. Sollte der Transport der Datenpakete gestört worden sein, sorgt das Protokoll für einen erneuten Übermittlungsversuch. *In the OSI model, the protocols occupy layers 3 and 4. The transport and network layers deal directly with the connection between two devices via a network. For example, the IP address and the Internet protocol are used to send the data packet to the correct recipient. TCP, on the other hand, is responsible for establishing a connection between the two devices involved and maintaining it for transmission. If the transport of the data packets has been disturbed, the protocol ensures a new transmission attempt.*

## TCP/IP-Modell

Da es sich bei TCP/IP nur um einen Sammelbegriff handelt, der im Kontext der für das Internet wichtigsten Protokolle genannt wird, nutzt man den Terminus auch in weiteren Situationen. So gibt es auch ein **Referenzmodell mit Bezug auf TCP/IP**. Ähnlich wie beim OSI-Modell soll das System alle Aspekte der Kommunikation in Netzwerken abbilden. Das TCP/IP-Modell besteht allerdings aus vier verschiedenen Schichten, statt wie das OSI-Modell aus sieben Ebenen. Den Schichten im TCP/IP-Modell werden verschiedene Aufgaben und damit Protokolle zugesprochen. *Since TCP/IP is only a collective term used in the context of the most important protocols for the Internet, the term is also used in other situations. Thus there is also a reference model with reference to TCP/IP. Similar to the OSI model, it is intended to represent all aspects of communication in networks. However, the TCP/IP model consists of four different layers instead of seven layers like the OSI model. The layers in the TCP/IP model are assigned different tasks and thus protocols.*

- **Netzzugangsschicht**: Diese Schicht ist im Referenzmodell zwar vorgesehen, es wird aber kein bestimmtes Protokoll definiert. In der Praxis kommen vor allem Ethernet (Kabel) und IEEE 802.11 (Funk) zum Einsatz. Die Netzzugangsschicht sorgt für die Verknüpfung von verschiedenen Subnetzen und verbindet so beispielsweise das heimische WLAN per Router mit dem Internet. - ***Network access layer:*** *This layer is provided for in the reference model, but no specific protocol is defined. In practice, Ethernet (cable) and*

*IEEE 802.11 (radio) are the most commonly used. The network access layer provides the link between different subnets and thus connects, for example, the home WLAN with the Internet via a router.*

- **Internetschicht**: Auf dieser Schicht arbeitet das Internet Protocol und sorgt dafür, dass die transportierten Daten auch das richtige Ziel erreichen. Über die IP-Adresse werden die Datenpakete durch das Netzwerk geroutet. - ***Internet layer:*** *The Internet Protocol operates at this layer and ensures that the transported data reaches the correct destination. The data packets are routed through the network via the IP address.*
- **Transportschicht**: Für den Transport sorgt im Referenzmodell TCP. Das Protokoll ermöglicht die Ende-zu-Ende-Kommunikation, ist also verantwortlich für die Verbindung zwischen zwei Geräten. Neben TCP gehört auch UDP in diese Ebene. - ***Transport layer:*** *TCP is responsible for transport in the reference model. The protocol enables end-to-end communication, i.e. it is responsible for the connection between two devices. In addition to TCP, UDP also belongs in this layer.*
- **Anwendungsschicht**: Die Kommunikation der Programme über das Netzwerk wird in der obersten Schicht geregelt. Maßgeblich sind hier z. B. HTTP und FTP. Aber auch die E-Mail-Kommunikation (mit POP oder SMTP) funktioniert auf dieser Ebene. - ***Application layer:*** The communication of the programs via the network is regulated in the top layer. The decisive factors here are, for example, HTTP and FTP. But e-mail communication (with POP or SMTP) also functions at this level.

## Fakt (*we won't translate Fact* 😉)

Das TCP/IP-Modell gibt es bereits länger als das OSI-Modell: Das ältere System wurde bereits bei der Weiterentwicklung vom Arpanet zum Internet entwickelt. Die Erfahrungen, die man damals machte, sind dann auch in das inzwischen populärere OSI-Modell eingeflossen. Deshalb kann man die beiden Systeme auch parallel verwenden. Die Struktur von OSI ist zwar kleinteiliger, verwendet aber den gleichen Aufbau. Die Schichten des OSI-Modells lassen sich deshalb den Schichten von TCP/IP zuordnen. *The TCP/IP model has been around longer than the OSI model: The older system was already developed during the evolution from Arpanet to the Internet. The experience gained at that time was then also incorporated into the OSI model, which is now more popular. This is why the two systems can be used in parallel. Although the structure of OSI is more detailed, it uses the same structure. The layers of the OSI model can therefore be assigned to the layers of TCP/IP.*

# TCP- & UDP-Ports: Liste der wichtigsten Ports

TCP und UDP sorgen für die Verbindung zwischen zwei Geräten über das Internet oder andere Netzwerke. Damit Datenpakete allerdings einen Eingang beim PC oder Server auf der anderen Seite der Verbindung finden können, müssen hier Türen geöffnet sein. Solche **Öffnungen in das System** nennt man Ports. Für die beiden Protokolle gibt es einige bekannte und wichtige Ports, die man bei der Entwicklung von Web-Anwendungen kennen sollte. *TCP and UDP provide the connection between two devices via the Internet or other networks. However, in order for data packets to find an entrance at the PC or server on the other side of the connection, doors must be opened here. Such openings into the system are called ports. For both protocols, there are some well-known and important ports that should be known when developing web applications.*

**Inhaltsverzeichnis**



## Wofür sind Ports gedacht? *What are ports good for?*

Bei der Kommunikation über das Internet sorgen die beiden Protokolle TCP und UDP für den Verbindungsaufbau, setzen Datenpakete nach der Übermittlung wieder zusammen und übergeben sie dann an die adressierten Programme beim Empfänger. Damit diese Übergabe funktionieren kann, muss das Betriebssystem Eingänge schaffen und diese auch für die Übertragung öffnen. **Jeder Eingang hat eine spezifische Kennziffer**. Nach der Übertragung weiß das empfangende System mithilfe der Portnummer, wohin die Daten geliefert werden müssen. Im Datenpaket sind immer zwei Portnummern enthalten, die des Senders und die des Empfängers. *When communicating via the Internet, the two protocols TCP and UDP take care of establishing the connection,*

*reassembling data packets after transmission and then handing them over to the addressed programs at the recipient. For this transfer to work, the operating system must create inputs and also open them for transmission. Each input has a specific identification number. After the transfer, the receiving system knows where to deliver the data with the help of the port number. The data packet always contains two port numbers, that of the sender and that of the receiver.*

Ports sind fortlaufend durchnummeriert – von 0 bis 65536. Einige von diesen Kennziffern sind **standardisiert und damit bestimmten Anwendungen zugeordnet**. Diese Standard-Ports nennt man auch Well Known Ports, da die Kennzahlen für alle bekannt und vor allem fest sind. Daneben gibt es noch Registered Ports. Hier haben Organisationen bzw. Hersteller von Software einen Port für ihre Anwendung angemeldet. Für die Registrierung ist die Internet Assigned Numbers Authority (IANA) zuständig. Darüber hinaus gibt es aber auch einen großen Bereich von Portnummern, die dynamisch vergeben werden. Ein Browser verwendet beispielsweise einen solchen Port für die Zeit eines Website-Besuchs. Danach ist die Nummer wieder frei. *Ports are numbered consecutively - from 0 to 65536. Some of these codes **are standardized and thus assigned to specific applications**. These standard ports are also called Well Known Ports, since the codes are known to everyone and, above all, are fixed. In addition, there are also Registered Ports. Here, organizations or manufacturers of software have registered a port for their application. The Internet Assigned Numbers Authority (IANA) is responsible for the registration. In addition, there is also a wide range of port numbers that are assigned dynamically. For example, a browser uses such a port for the time of a website visit. After that, the number is free again.*

## Liste der wichtigsten Ports / *List of essentiel ports*

Es gibt unter den über 65.000 Ports einige Kennziffern, die sehr wichtig für die Kommunikation im Internet sind. Wir stellen jeweils wichtige Well Known Ports und Registered Ports vor. Teilweise sind Ports nur für eins der beiden Protokolle (TCP oder UDP) zugelassen. Außerdem gibt es Ports, die nicht offiziell für den genannten Dienst reserviert wurden, sich aber inoffiziell etabliert haben. Teilweise sind Ports doppelt belegt. *Among the more than 65,000 ports, there are some codes that are very important for communication on the Internet. We present important Well-Known Ports and Registered Ports respectively. In some cases, ports are only allowed for one of the two protocols (TCP or UDP). In addition, there are ports that have not been officially reserved for the named service, but have established themselves unofficially. In some cases, ports are assigned twice.*

### Well Kown Ports

| Port | TCP | UDP | Name | Beschreibung |
|---|---|---|---|---|
| 1 | ✔ | ✔ | tcpmux | TCP Port Multiplexer |
| 5 | ✔ | ✔ | rje | Remote Job Entry (Jobferneingabe) |
| 7 | ✔ | ✔ | echo | Echo-Service |
| 9 | ✔ | ✔ | discard | Null-Service für Prüfzwecke |
| 11 | ✔ | ✔ | systat | Systeminformationen |
| 13 | ✔ | ✔ | daytime | Zeit- und Datumsangaben |
| 17 | ✔ | ✔ | qotd | Sendet Zitat des Tages |
| 18 | ✔ | ✔ | msp | Übermittelt Textnachrichten |
| 19 | ✔ | ✔ | chargen | Sendet eine endlose Zeichenkette |
| 20 | ✔ | | ftp-data | FTP-Datenübertragung |
| 21 | ✔ | ✔ | ftp | FTP-Verbindung |
| 22 | ✔ | ✔ | ssh | Secure Shell Service |
| 23 | ✔ | | telnet | Telnet-Service |
| 25 | ✔ | | smtp | Simple Mail Transfer Protocol |
| 37 | ✔ | ✔ | time | Maschinenlesbares Zeitprotokoll |
| 39 | ✔ | ✔ | rlp | Resource Location Protocol |
| 42 | ✔ | ✔ | nameserver | Name-Service |

| Port | TCP | UDP | Name | Beschreibung |
|---|---|---|---|---|
| 43 | ✔ | | nicname | WHOIS-Verzeichnisservice |
| 49 | ✔ | ✔ | tacacs | Terminal Access Controller Access Control System |
| 50 | ✔ | ✔ | re-mail-ck | Remote Mail Checking |
| 53 | ✔ | ✔ | domain | Namensauflösung per DNS |
| 67 | | ✔ | bootps | Bootstrap Protocol Services |
| 68 | | ✔ | bootpc | Bootstrap Client |
| 69 | | ✔ | tftp | Trivial File Transfer Protocol |
| 70 | ✔ | | gopher | Dokumentensuche |
| 71 | ✔ | | genius | Geniusprotokoll |
| 79 | ✔ | | finger | Liefert Kontaktinformationen von Benutzern |
| 80 | ✔ | | http | Hypertext Transfer Protocol |
| 81 | ✔ | | | Torpark: Onion-Routing (inoffiziell) |
| 82 | | ✔ | | Torpark: Control (inoffiziell) |
| 88 | ✔ | ✔ | kerberos | Netzwerkauthentifizierungssystem |
| 101 | ✔ | | hostname | NIC Host Name |
| 102 | ✔ | | Iso-tsap | ISO-TSAP-Protocol |
| 105 | ✔ | ✔ | csnet-ns | Mailbox-Mailserver |
| 107 | ✔ | | rtelnet | Remote Telnet |
| 109 | ✔ | | pop2 | Post Office Protocol v2 für die E-Mail-Kommunikation |
| 110 | ✔ | | pop3 | Post Office Protocol v3 für die E-Mail-Kommunikation |
| 111 | ✔ | ✔ | sunrpc | RPC-Protokoll für NFS |
| 113 | | ✔ | auth | Authentifizierungsservice |
| 115 | ✔ | | sftp | Simple File Transfer Protocol (einfache Version von FTP) |
| 117 | ✔ | | uucp-path | Dateiübertragung zwischen Unix-Systemen |
| 119 | ✔ | | nntp | Übertragung von Nachrichten in Newsgroups |
| 123 | | ✔ | ntp | Dienst zur Zeitsynchronisierung |
| 137 | ✔ | ✔ | netbios-ns | NETBIOS Name Service |
| 138 | ✔ | ✔ | netbios-dgm | NETBIOS Datagram Service |
| 139 | ✔ | ✔ | netbios-ssn | NETBIOS Session Service |
| 143 | ✔ | ✔ | imap | Internet Message Access Protocol für E-Mail-Kommunikation |
| 161 | | ✔ | snmp | Simple Network Management Protocol |
| 162 | ✔ | ✔ | snmptrap | Simple Network Management Protocol Trap |
| 177 | ✔ | ✔ | xdmcp | X Display Manager |
| 179 | ✔ | | bgp | Border Gateway Protocol |
| 194 | ✔ | ✔ | irc | Internet Relay Chat |
| 199 | ✔ | ✔ | smux | SNMP UNIX Multiplexer |
| 201 | ✔ | ✔ | at-rtmp | AppleTalk Routing |
| 209 | ✔ | ✔ | qmtp | Quick Mail Transfer Protocol |
| 210 | ✔ | ✔ | z39.50 | Bibliographisches Informationssystem |
| 213 | ✔ | ✔ | ipx | Internetwork Packet Exchange |
| 220 | ✔ | ✔ | imap3 | IMAP v3 für die E-Mail-Kommunikation |
| 369 | ✔ | ✔ | rpc2portmap | Coda Filesystem Portmapper |
| 370 | ✔ | ✔ | codaauth2 | Coda Filesystem Authentication Service |
| 389 | ✔ | ✔ | ldap | Lightweight Directory Access Protocol |
| 427 | ✔ | ✔ | svrloc | Service Location Protocol |

| Port | TCP | UDP | Name | Beschreibung |
|---|---|---|---|---|
| 443 | ✔ | | https | HTTPS (HTTP über SSL/TLS) |
| 444 | ✔ | ✔ | snpp | Simple Network Paging Protocol |
| 445 | ✔ | | microsoft-ds | SMB über TCP/IP |
| 464 | ✔ | ✔ | kpasswd | Passwortänderung für Kerberos |
| 500 | | ✔ | isakmp | Sicherheitsprotokoll |
| 512 | ✔ | | exec | Remote Process Execution |
| 512 | | ✔ | comsat/biff | Mail-Client und -Server |
| 513 | ✔ | | login | Anmeldung an Remote-Computer |
| 513 | | ✔ | who | Whod User Logging Daemon |
| 514 | ✔ | | shell | Remote Shell |
| 514 | | ✔ | syslog | Unix System Logging Service |
| 515 | ✔ | | printer | Line Printer Daemon-Druckservices |
| 517 | | ✔ | talk | Talk Remote Calling |
| 518 | | ✔ | ntalk | Network Talk |
| 520 | ✔ | | efs | Extended Filename Server |
| 520 | | ✔ | router | Routing Information Protocol |
| 521 | | ✔ | ripng | Routing Information Protocol für IPv6 |
| 525 | | ✔ | timed | Zeitserver |
| 530 | ✔ | ✔ | courier | Courier Remote Procedure Call |
| 531 | ✔ | ✔ | conference | Chat über AIM und IRC |
| 532 | ✔ | | netnews | Netnews Newsgroup Service |
| 533 | | ✔ | netwall | Notfall-Broadcasts |
| 540 | ✔ | | uucp | Unix-to-Unix Copy Protocol |
| 543 | ✔ | | klogin | Kerberos v5 Remote Login |
| 544 | ✔ | | kshell | Kerberos v5 Remote Shell |
| 546 | ✔ | ✔ | dhcpv6-client | DHCP v6 Client |
| 547 | ✔ | ✔ | dhcpv6-server | DHCP v6 Server |
| 548 | ✔ | | afpovertcp | Apple Filing Protocol über TCP |
| 554 | ✔ | ✔ | rtsp | Steuerung von Streams |
| 556 | ✔ | | remotefs | Remote Filesystem |
| 563 | ✔ | ✔ | nntps | NNTP über SSL/TLS |
| 587 | ✔ | | submission | Message Submission Agent |
| 631 | ✔ | ✔ | ipp | Internet Printing Protocol |
| 631 | ✔ | ✔ | | Common Unix Printing System (inoffiziell) |
| 636 | ✔ | ✔ | ldaps | LDAP über SSL/TLS |
| 674 | ✔ | | acap | Application Configuration Access Protocol |
| 694 | ✔ | ✔ | ha-cluster | Heartbeat-Service |
| 749 | ✔ | ✔ | kerberos-adm | Kerberos v5 Administration |
| 750 | | ✔ | kerberos-iv | Kerberos v4 Services |
| 873 | ✔ | | rsync | rsync Dateitransfer-Services |
| 992 | ✔ | ✔ | telnets | Telnet über SSL/TLS |
| 993 | ✔ | | imaps | IMAP über SSL/TLS |
| 995 | ✔ | | pop3s | POP3 über SSL/TLS |

**Registered Ports**

| Port | TCP | UDP | Name | Beschreibung |
|---|---|---|---|---|
| 1080 | ✔ | | socks | SOCKS Proxy |
| 1433 | ✔ | | ms-sql-s | Microsoft SQL Server |
| 1434 | ✔ | ✔ | ms-sql-m | Microsoft SQL Monitor |
| 1494 | ✔ | | ica | Citrix ICA Client |
| 1512 | ✔ | ✔ | wins | Windows Internet Name Service |
| 1524 | ✔ | ✔ | ingreslock | Ingres DBMS |
| 1701 | | ✔ | l2tp | Layer 2 Tunneling Protocol / Layer 2 Forwarding |
| 1719 | | ✔ | h323gatestat | H.323 |
| 1720 | ✔ | | h323hostcall | H.323 |
| 1812 | ✔ | ✔ | radius | RADIUS-Authentifikation |
| 1813 | ✔ | ✔ | radius-acct | RADIUS-Zugang |
| 1985 | | ✔ | hsrp | Cisco HSRP |
| 2008 | ✔ | | | Teamspeak 3 Accounting (inoffiziell) |
| 2010 | | ✔ | | Teamspeak 3 Webliste (inoffiziell) |
| 2049 | ✔ | ✔ | nfs | Network File System |
| 2102 | ✔ | ✔ | zephyr-srv | Zephyr Server |
| 2103 | ✔ | ✔ | zephyr-clt | Zephyr Client |
| 2104 | ✔ | ✔ | zephyr-hm | Zephyr Host Manager |
| 2401 | ✔ | | cvspserver | Concurrent Versions System |
| 2809 | ✔ | ✔ | corbaloc | Common Object Request Broker Architecture |
| 3306 | ✔ | ✔ | mysql | MySQL Datenbankservice (auch für MariaDB) |
| 4321 | ✔ | | rwhois | Remote Whois Service |
| 5999 | ✔ | | cvsup | CVSup |
| 6000 | ✔ | | X11 | X Windows System Services |
| 11371 | ✔ | | pgpkeyserver | Öffentlicher Keyserver für PGP |
| 13720 | ✔ | ✔ | bprd | Symantec/Veritas NetBackup |
| 13721 | ✔ | ✔ | bpdbm | Symantec/Veritas Database Manager |
| 13724 | ✔ | ✔ | vnetd | Symantec/Veritas Network Utility |
| 13782 | ✔ | ✔ | bpcd | Symantec/Veritas NetBackup |
| 13783 | ✔ | ✔ | vopied | Symantec/Veritas VOPIE |
| 22273 | ✔ | ✔ | wnn6 | Kana/Kanji-Konvertierung |
| 23399 | | | | Skype (inoffiziell) |
| 25565 | ✔ | | | Minecraft |
| 26000 | ✔ | ✔ | quake | Quake und andere Mehrspieler-Games |
| 27017 | | | | MongoDB |
| 33434 | ✔ | ✔ | traceroute | Netzwerk-Tracking |

**Hinweis*/Note***

Ab den Ports mit der Nummer 49152 handelt es sich um dynamische Ports. Diese werden nicht von der IANA vergeben. Jede Anwendung kann einen solchen Port lokal oder auch dynamisch global verwenden. So kann es leicht vorkommen, dass einer dieser Ports bereits belegt ist. *Ports with the number 49152 and higher are dynamic ports. These are not assigned by IANA. Every application can use such a port locally or also dynamically globally. Thus, it can easily happen that one of these ports is already in use.*

# Unicast: Gezielte Verbindung zwischen zwei Punkten

Die Netzwerktechnik kennt verschiedene Methoden, um eine Nachricht vom Adressaten zu dem oder den Empfängern zu bekommen. Während man bei einem Broadcast seine Daten an alle Teilnehmer eines Netzes richtet, hilft der Unicast bei einer gezielten Ansprache. Ähnlich funktioniert der Multicast, doch bei diesem geht die Nachricht gleich an mehrere spezifische Empfänger. Was versteht man genau unter einem Unicast und wie unterscheiden sich Unicast und Multicast voneinander?

*Network technology knows different methods to get a message from the addressee to the recipient(s). While a broadcast directs its data to all participants of a network, the unicast helps with a targeted address. Multicast works similarly, but in this case the message goes to several specific recipients at once. What exactly is a unicast and how do unicast and multicast differ from each other?*

**Inhaltsverzeichnis /***TOC*



## Was ist Unicast? *Whats that?*

Wenn Sie einen Telefonanruf tätigen, wählen Sie eine bestimmte Nummer, um **mit einer spezifischen Person** sprechen zu können. Es käme Ihnen nicht in den Sinn, den Namen des Adressaten in den Hörer zu sprechen mit der Hoffnung, von diesem eine Antwort zu erhalten. Dies unterscheidet auch den Broadcast, bei dem alle Netzteilnehmer die Nachricht erhalten, vom Unicast.

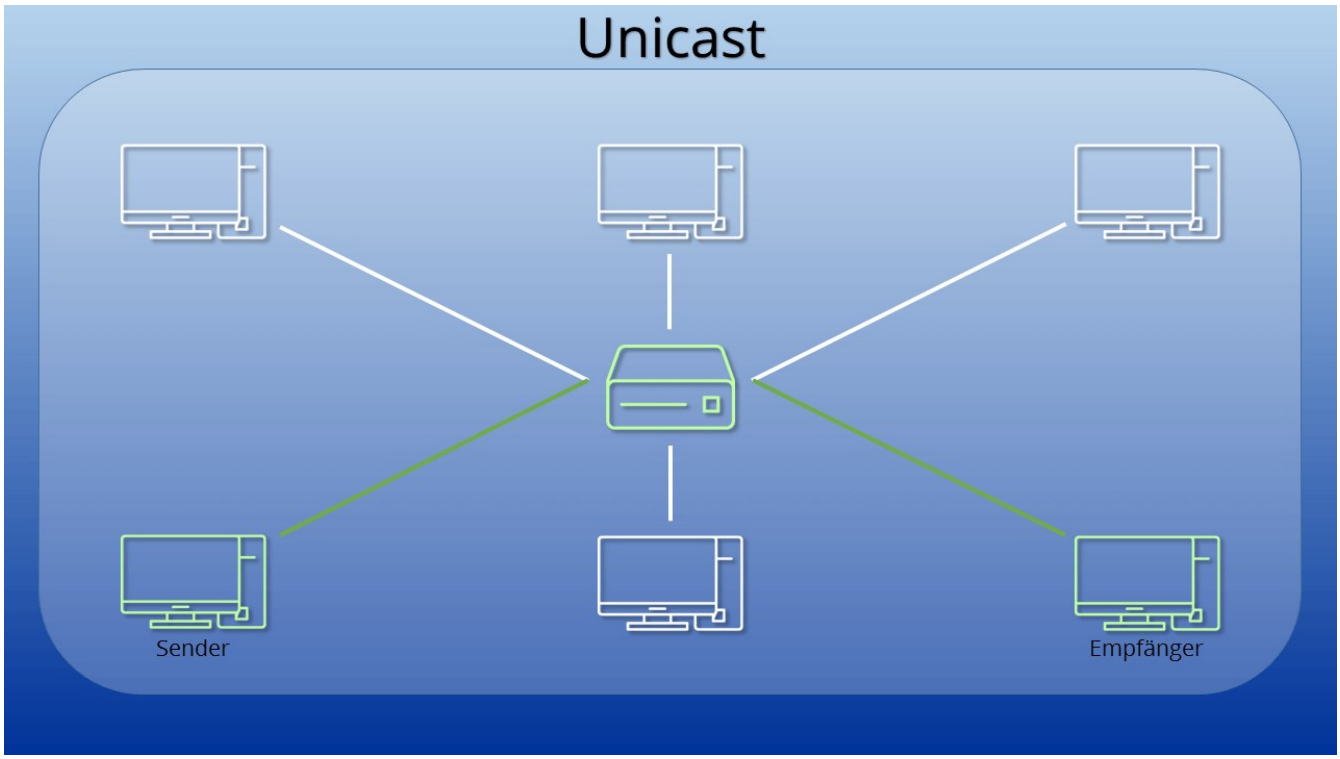
*When you make a phone call, you dial a specific number to be able to talk to a specific person. It would not occur to you to speak the name of the addressee into the receiver with the hope of getting an answer from him. This also distinguishes broadcast, where all network subscribers receive the message, from unicast.*

Letztere Verbindungsart stellt den Kontakt nur zwischen genau zwei Teilnehmern her. Dabei ist es nicht entscheidend, ob der Transfer in beide Richtungen funktioniert: Ob der Adressat selbst zu einem Sender wird, Daten also hin und her geschickt werden (bidirektional), oder es sich um eine Verbindung in nur eine Richtung (unidirektional) handelt, ist unerheblich. Solange man einen **Informationsfluss zwischen nur zwei Netzteilnehmern** hat, spricht man von einem Unicast.

*The latter type of connection establishes contact only between exactly two participants. It does not matter whether the transfer works in both directions: Whether the addressee itself becomes a sender, i.e. data is sent back and forth (bidirectional), or it is a connection in only one direction (unidirectional) is irrelevant. As long as **one has a flow of information between only two network participants**, one speaks of a unicast.*

Der größte Teil des Datenverkehres im Internet funktioniert über das Prinzip Unicast. Jedes Mal, wenn eine Website vom Nutzer aufgerufen wird, findet eine direkte Verbindung zwischen Client und Server statt. Auch der **E-Mail-Versand** funktioniert in der Regel per Unicast. Ein Beispiel ist auch der direkte Dateitransfer: Wenn Sie eine Datei herunterladen oder auf einen Server hochladen, geschieht dies per Unicast. Nur in bestimmten Szenarien – beispielsweise Streaming – finden andere Methoden wie etwa Multicast Verwendung.

*Most of the data traffic on the Internet works on the principle of unicast. Every time a website is called up by the user, a direct connection takes place between client and server. Sending e-mails also usually works via unicast. Direct file transfer is another example: When you download a file or upload it to a server, this is done via unicast. Only in certain scenarios - streaming, for example - do other methods such as multicast find use.*




Bei einer Unicast-Verbindung nehmen immer nur genau zwei Endpunkte an der Kommunikation teil.
*With a unicast connection, only exactly two endpoints ever participate in the communication.*

## Technischer Ablauf: IPv4, IPv6 & Unicast */ How does it work:*

Egal, um welche Form von Kommunikation es sich handelt: Wenn man einen konkreten Ansprechpartner erreichen möchte, muss man wissen, wie dieser anzusprechen ist. Name, Telefonnummer, Postadresse – alle helfen uns, unsere Informationen an den korrekten Empfänger zu richten. Auch in der Netzwerktechnik ist dies nicht anders. Hier helfen **IP- und MAC-Adresse** bei der Identifizierung der Empfänger. *No matter what form of communication is involved: If you want to reach a specific contact person, you need to know how to address them. Name, phone number, postal address - all help us direct our information to the correct recipient. This is no different in network technology. Here, IP and MAC addresses help identify recipients.*

Im **OSI-Modell** liegt der Unicast auf der **Vermittlungsschicht (Layer 3)** und ist damit ein Routingschema. Der Information, die verschickt werden soll (egal ob E-Mail, Datei oder einfache Website-Anfrage), wird ein Header hinzugefügt, in dem die Adressdaten untergebracht sind. Soweit handelt es sich um einen recht einfachen Vorgang: Im Header befindet sich die Adresse des Empfängers im Netzwerk. Das Paket wird genau in diese Richtung gesendet. *In the **OSI model**, the unicast is located on the **network layer (Layer 3)** and is thus a routing scheme. A header is added to the information that is to be sent (whether e-mail, file or simple website request), in which the address data is placed. As far as it is concerned, the process is quite simple: the header contains the address of the recipient in the network. The packet is sent exactly in this direction.*

Allerdings findet die Kommunikation nicht immer nur innerhalb eines geschlossenen Netzwerks statt, wo der Router jeden Endpunkt direkt erreichen kann. Auch zwischen verschiedenen (Sub-)Netzen sind Unicasts möglich. Dafür setzt man auf **IP-Routing-Technologie**. Diese stellt sicher, dass jeder Knotenpunkt weiß, welchen Weg das Datenpaket einschlagen muss, damit es den rechtmäßigen Empfänger erreicht. Router (die Netzwerkknoten) verwenden dafür Routingtabellen. Um diese zu erstellen, werden vor allem die beiden Protokolle OSPF und RIPv2 eingesetzt. *However, communication does not always take place only within a closed network, where the router can reach every endpoint directly. Unicasts are also possible between different (sub)networks. IP routing technology is used for this. This ensures that each node knows which path the data packet must take in order to reach the rightful recipient. Routers (the network nodes) use routing tables for this purpose. The two protocols OSPF and RIPv2 are primarily used to create these.*

Im Gegensatz zu den bislang noch üblichen IPv4-Adressen hat das neuere **IPv6** für Unicast eine Besonderheit vorgesehen: Bestimmte Adressbereiche sind für die unterschiedlichen Kommunikationsarten reserviert. Multicast-Adressen befinden sich in einem anderen Adressbereich als Unicast-Adressen. Dabei unterscheidet man zudem verschiedene Arten von Unicast-Adressen, die durch ein **Präfix** am Anfang der Adresse dargestellt werden. *In contrast to the IPv4 addresses still in use up to now, the newer **IPv6** has provided a special feature for unicast: Certain address ranges are reserved for the different types of communication. Multicast addresses are located in a different address range than unicast addresses. A distinction is also made between different types of unicast addresses, which are represented by a **prefix** at the beginning of the address.*

### Link-Local-Unicast-Adressen

Link Local bezeichnet lokale, in sich **geschlossene Netzwerke**. Hierbei ist keine Weiterleitung durch einen Router in andere Netzwerke nötig; der Bereich *fe80::/10* ist hierfür reserviert. Die ersten 10 Bits der Adresse sind für das Präfix vorgesehen. Es folgen 64 Bits, die alle auf 0 gestellt sind. Abgeschlossen wird die Adresse von einem 54-Bit langen Bereich. Darin befindet sich die Schnittstellen-ID, die den Client eindeutig im lokalen Netz identifiziert. *Link Local refers to local, self-contained networks. Here, no forwarding by a router to other networks is necessary; the range fe80::/10 is reserved for this. The first 10 bits of the address are reserved for the prefix. This is followed by 64 bits, which are all set to 0. The address is concluded by a 54-bit long area. This contains the interface ID that uniquely identifies the client in the local network.*

**Fakt**
Auch unter IPv4 gibt es einen Adressbereich, der für Link Local Unicast reserviert ist: 169.254.0.0/16.
Also under IPv4 there is an address range reserved for Link Local Unicast: 169.254.0.0/16.

### Unique Local Unicast

Im Gegensatz zu den Link-Local-Adressen kann ein Unique Local Unicast **durch einen Router weitergeleitet** werden. Dennoch sind diese Adressen intern (in einem festgelegten Netzwerkbereich; z. B. das Netzwerk eines großen Unternehmens) einmalig vergeben. Die Internet Engineering Task Force (IETF) hat hierfür den Bereich *fc00::/7* vorgesehen. Derzeit ist allerdings nur der Teil *fd00::/8* konkret für den Unique Local Unicast vergeben, über den Bereich *fc00:/8* wurde noch nicht entschieden. Nach dem Präfix folgt ein 40-Bit-Teil, in dem eine zufällig zu generierende Site-ID steht. Das Ende bildet eine 16-Bit lange Subnet-ID. *In contrast to link local addresses, a unique local unicast can be forwarded by a router. Nevertheless, these addresses are assigned once internally (in a defined network area; e.g., the network of a large company). The Internet Engineering Task Force (IETF) has designated the range fc00::/7 for this purpose. At present, however, only the part fd00::/8 has been specifically assigned for the Unique Local Unicast; no decision has yet been made about the range fc00:/8. The prefix is followed by a 40-bit part containing a randomly generated site ID. The end is a 16-bit long subnet ID.*

**Fakt**
Der Unique-Local-Unicast-Adressbereich entspricht in seinen Eigenschaften dem IPv4-Private-Adressbereich. Es handelt sich damit also um Adressen, die jeder Nutzer innerhalb seines Netzwerks vergeben darf, ohne dies durch eine außenstehende Organisation genehmigen zu lassen. *The unique local unicast address range has the same properties as the IPv4 private address range. This means that each user can assign addresses within his or her network without having to obtain approval from an outside organization.*

### Global Unicast

Durch den Global Unicast ist es auch mit IPv6 möglich, **Unicasts weltweit über das Internet** zu versenden. Die Adressen sind global einmalig vergeben. So ist es möglich, jemanden ganz gezielt zu erreichen. Dies ist quasi der Standardfall einer IPv6-Adresse. Den ersten Teil der Adresse bezeichnet man als Standortpräfix oder öffentliche Topologie; er hängt vom Internetanbieter ab. Anschließend folgen Informationen zum Teilnetz und zum eigentlichen Client. Wie beim **Subnetting** darf auch hier der letzte Teil der Adresse (Schnittstellen-ID) innerhalb des Teilnetzes nur einmal vergeben werden. Nur so kann sichergestellt sein, dass ein Unicast auch tatsächlich das korrekte Ziel erreicht. *Global Unicast makes it possible to send unicasts worldwide over the Internet even with*

*IPv6. The addresses are assigned once globally. This makes it possible to reach someone specifically. This is more or less the standard case of an IPv6 address. The first part of the address is called the location prefix or public topology; it depends on the Internet provider. This is followed by information about the subnet and the actual client. As with subnetting, the last part of the address (interface ID) may only be assigned once within the subnet. This is the only way to ensure that a unicast actually reaches the correct destination.*

**Fakt**
Ein Teil des Global-Unicast-Adressraums (*0:0:0:0:0:ffff::/96*) ist für die Umwandlung von IPv4 zu IPv6 (IPv4 mapped IPv6 addresses) gedacht. Hierbei enthalten die letzten 32 Bits der IPv6-Adresse die Informationen des älteren Formats. So ist es möglich, einen Unicast im alten System auch über das neue Protokoll zu erreichen. *Part of the global unicast address space (0:0:0:0:ffff::/96) is intended for the conversion from IPv4 to IPv6 (IPv4 mapped IPv6 addresses). Here the last 32 bits of the IPv6 address contain the information of the older format. So it is possible to reach a unicast in the old system also over the new protocol.*

## Unicast vs. Multicast

Die beiden Kommunikationsarten Unicast und Multicast haben klare Ähnlichkeiten, vor allem wenn man sie dem Broadcast gegenüberstellt. Den Broadcast sendet man an eine hierfür reservierte Adresse. Alle Teilnehmer im Netz erkennen dies und können so auf das Datenpaket reagieren. Unicast und Multicast hingegen werden an **spezifische Ziele** gerichtet; die anderen Teilnehmer im Netz nehmen keine Notiz von den Daten bzw. reagieren auf diese nicht. *The two communication types unicast and multicast have clear similarities, especially when compared to broadcast. The broadcast is sent to an address reserved for this purpose. All participants in the network recognize this and can thus respond to the data packet. Unicast and multicast, on the other hand, are directed to specific destinations; the other participants in the network take no notice of the data or do not react to it.*

Unicast und Multicast unterscheiden sich ziemlich offensichtlich darin, dass man den Unicast nur an einen einzelnen Empfänger sendet, während man mit einem Multicast eine ganze Gruppe von Zielen adressieren kann. Dabei ist der Multicast aber nicht einfach nur eine Sammlung von einzelnen Unicasts. Stattdessen erfolgt der Versand über eine Multicast-Adresse. Diese veranlasst die Weiterleitung über einen Router oder Server an alle Mitglieder der **Multicast-Gruppe**. Diese Gruppe muss also bereits vor Datentransfer bestehen und kann nicht im Moment des Versendens durch den Quellknoten festgelegt werden. *Unicast and multicast are quite obviously different in that you send the unicast only to a single receiver, while with a multicast you can address a whole group of destinations. However, the multicast is not simply a collection of individual unicasts. Instead, it is sent via a multicast address. This initiates forwarding via a router or server to all members of the multicast group. This group must therefore already exist before the data is transferred and cannot be defined by the source node at the moment of sending.*

Der Vorteil des Multicasts im Gegensatz zum **Multiple Unicast** – also dem Transfer an mehrere Unicast-Adressen – liegt im einmaligen Versand des Datenpakets. Nutzt man mehrere Unicasts, wird das Paket jedes Mal erneut ins Netz gesendet. Der Multicast verschickt das Paket nur einmal. Erst am Verteiler werden die Daten multipliziert – das spart Bandbreite. Deshalb sind vor allem beim Multimedia-Streaming Multicasts beliebt. Da eine große Gruppe von Clients genau die gleichen Daten verlangt, ist es sehr viel praktikabler, diese nur einmal zu senden. Würden die gleichen Daten zeitgleich an viele Empfänger per Unicast versendet, käme es zu Geschwindigkeitseinbußen. *The advantage of multicast over multiple unicast - i.e. transfer to multiple unicast addresses - is that the data packet is sent only once. If multiple unicasts are used, the packet is sent to the network again each time. Multicast sends the packet only once. The data is only multiplied at the distribution point - this saves bandwidth. This is why multicasts are particularly popular for multimedia streaming. Since a large group of clients requires exactly the same data, it is much more practical to send it only once. If the same data were sent to many recipients at the same time via unicast, there would be a loss of speed.*

**Fazit**
Sollen vertrauliche Daten nur einen Empfänger erreichen, ist der Unicast die richtige Wahl. Website-Aufrufe und E-Mails werden so tagtäglich gesendet. Sollen aber mehrere Empfänger die gleichen Daten erhalten, ist ein

Multicast effizienter. *If confidential data is to reach only one recipient, unicast is the right choice. Website calls and e-mails are sent like this every day. But if several recipients are to receive the same data, multicast is more efficient.*

## Basic zu IGMP:

**Anwendungsbereiche des Internet Group Management Protocols** *Application areas of the Internet Group Management Protocol*

Das Internet Group Management Protocol kommt für verschiedene Anwendungen zum Einsatz. Die Verwendung ist immer dann sinnvoll, wenn Daten in Form von Multicasts nur an einen bestimmten Empfängerkreis übertragen werden sollen. *The Internet Group Management Protocol is used for various applications. It is always useful when data is to be transmitted in the form of multicasts to a specific group of recipients only.*
Typische Anwendungsbereiche sind beispielsweise: *Typical application areas are for example:*

- IPTV (Fernsehen über das Internet Protokoll) *IPTV (television via the Internet Protocol)*
- Videokonferenzen über IP-Netze *Video conferencing over IP networks*
- Streaming in IP-Netzen *Streaming in IP networks*
- Routingprotokolle wie Open Shortest Path First (OSPF) oder Routing Information Protocol Version 2 (RIPv2) *Routing protocols such as Open Shortest Path First (OSPF) or Routing Information Protocol Version 2 (RIPv2)*

Das Internet Group Management Protocol ist ein Protokoll aus der TCP/IP-Welt zur Realisierung und Organisation von Multicast-Übertragungen in einem IP-Netz. Per IGMP können Clients einem Router mitteilen, dass sie ein bestimmtes Multicast empfangen möchten. Auf Layer 2 nutzen Switches das so genannte IGMP-Snooping, um Multicasts effizienter zu verteilen.
*The Internet Group Management Protocol is a protocol from the TCP/IP world for realizing and organizing multicast transmissions in an IP network. Via IGMP, clients can inform a router that they want to receive a specific multicast. On Layer 2, switches use so-called IGMP snooping to distribute multicasts more efficiently.*

Das Internet Group Management Protocol arbeitet im ISO/OSI-Schichtenmodelle auf **Layer3** (Vermittlungsschicht). Hauptaufgabe des Protokolls ist die Verwaltung der verschiedenen IP-Multicast-Übertragungen und -Gruppen auf den Routern.
*The Internet Group Management Protocol operates in the ISO/OSI layer model on Layer3 (network layer). The main task of the protocol is to manage the various IP multicast transmissions and groups on the routers.*

Die Router empfangen von den Multicast-Sendern die Multicast-IP-Pakete und leiten diese an die Empfänger weiter, die sich zuvor per IGMP für einen bestimmten Multicast angemeldet haben. Sind mehrere Router beteiligt, tauschen sie untereinander ebenfalls IGMP-Nachrichten aus. Multicast reduziert die Bandbreite für die gleichzeitige Übertragung von IP-Paketen an mehrere Empfänger drastisch, da der Sender die IP-Pakete nur einmal verschicken muss. Erst die Router duplizieren die Pakete in Richtung der Empfänger und senden sie an die Mitglieder einer Multicast-Gruppe.
*The routers receive the multicast IP packets from the multicast senders and forward them to the receivers that have previously registered for a specific multicast via IGMP. If multiple routers are involved, they also exchange IGMP messages among themselves. Multicast drastically reduces the bandwidth needed to transmit IP packets to multiple recipients simultaneously, since the sender only needs to send the IP packets once. Only the routers duplicate the packets in the direction of the receivers and send them to the members of a multicast group.*

Das Internet Group Management Protocol kommt beispielsweise für IPTV, Videokonferenzen oder Routingprotokolle zum Einsatz. IGMPv1 wurde im Jahr 1989 im RFC 1112 spezifiziert. IGMPv2 ist im RFC 2236 und IGMPv3 in den RFCs 3376 und 4604 beschreiben. Die Versionen sind abwärtskompatibel. Das bedeutet, dass ein Gerät das IGMPv3 unterstützt auch mit den Versionen 1 und 2 kompatibel ist.
*The Internet Group Management Protocol is used, for example, for IPTV, video conferencing or routing protocols. IGMPv1 was specified in RFC 1112 in 1989. IGMPv2 is described in RFC 2236 and IGMPv3 in RFCs 3376 and 4604.*

*The versions are backward compatible. This means that a device that supports IGMPv3 is also compatible with versions 1 and 2.*

**Grundsätzliches zum Multicasting in IP-Netzen** *Basic information on multicasting in IP networks*
IP-Netze kennen grundsätzlich drei verschiedene Übertragungsarten. Dies sind:
*IP networks basically know three different transmission types. These are:*

- **IP-Unicasts:** ein Sender schickt Pakete an einen Empfänger *IP unicasts: one sender sends packets to one receiver*
- **IP-Broadcasts:** ein Sender schickt Pakete an alle erreichbaren Empfänger *IP-Broadcasts: one sender sends packets to all reachable receivers*
- **IP-Multicast:** ein Sender schickt Pakete an eine Gruppe von Empfängern *IP multicast: a sender sends packets to a group of receivers*

IP-Multicasts sind eine besondere Form von Mehrpunktverbindungen. Sie bieten den Vorteil, dass der Sender nicht für jeden Empfänger eigene IP-Pakete versenden muss und sich seine Datenübertragungsrate mit der Anzahl der Empfänger nicht multipliziert. Der Sender schickt die IP-Pakete hier nur einmalig mit einer speziellen IP-Multicast-Adresse. Die Verteilung der Pakete und Zustellung an die Empfänger übernehmen die Router auf dem Weg zum Ziel. Für Multicasts sieht IPv4 den Adressraum von 224.0.0.0 bis 239.255.255.255 vor.
*IP multicasts are a special form of multipoint connections. They offer the advantage that the sender does not have to send separate IP packets for each recipient and its data transmission rate is not multiplied by the number of recipients. The sender sends the IP packets here only once with a special IP multicast address. The distribution of the packets and delivery to the recipients is handled by the routers on the way to the destination. For multicasts, IPv4 provides the address space from 224.0.0.0 to 239.255.255.255.*

Über das Internet Group Management Protocol signalisieren Clients einem Router, dass sie ein bestimmtes Multicast empfangen möchten. Die höchste Effizienz bietet die Multicast-Übertragung, wenn alle Router auf dem Weg vom Sender zum Empfänger das Internet Group Management Protocol unterstützen.
*Using the Internet Group Management Protocol, clients signal a router that they want to receive a particular multicast. Multicast transmission provides the highest efficiency when all routers on the path from the sender to the receiver support the Internet Group Management Protocol.*

**Funktionsweise des Internet Group Management Protocols** *How the Internet Group Management Protocol works*

Das Internet Group Management Protocol erlaubt die dynamische Verwaltung von Multicast-Gruppen. Ein Client, der einen Multicast empfangen möchte, sendet eine spezielle IGMP-Nachricht an den Router. Dieser trägt den Client in die entsprechende Multicast-Gruppe ein und merkt sich die Schnittstelle, über die der Client erreichbar ist. *The Internet Group Management Protocol allows dynamic management of multicast groups. A client that wants to receive a multicast sends a special IGMP message to the router. The router enters the client into the appropriate multicast group and remembers the interface through which the client can be reached.*

Zum Anmelden oder Verlassen einer Multicast-Gruppe verwenden die Clients so genannte Join- oder Leave-Nachrichten. Die IP-Pakete eines empfangenen Multicasts dupliziert der Router und sendet sie auf all seinen Schnittstellen, über die die zuvor angemeldeten Clients erreichbar sind. Der eigentliche Sender des Multicasts kennt die Empfänger nicht und hat keine Informationen darüber, wie viele Clients seinen Multicast empfangen. Die Verteilung des Multicasts und die Verwaltung der Teilnehmer übernehmen vollständig die IGMP-Router. *To join or leave a multicast group, the clients use so-called Join or Leave messages. The IP packets of a received multicast are duplicated by the router and sent on all its interfaces through which the previously registered clients can be reached. The actual sender of the multicast does not know the receivers and has no information about how many clients receive its multicast. The distribution of the multicast and the management of the subscribers are completely handled by the IGMP routers.*

Auf dem Layer 2 arbeiten Switches mit dem so genannten IGMP-Snooping, um Multicast-Daten effizienter zu verteilen. Dank Snooping werden IP-Multicast-Pakete nur auf den Switchports ausgegeben, hinter denen sich

Clients befinden, die diesen Multicast empfangen möchten. Dadurch verhindert der Switch, dass Multicasts auf all seinen Ports gesendet werden müssen und der Switch oder angeschlossene Netzwerke überlastet werden. *At Layer 2, switches work with so-called IGMP snooping to distribute multicast data more efficiently. Thanks to snooping, IP multicast packets are only output on the switch ports behind which there are clients that want to receive this multicast. This prevents the switch from having to send multicasts on all its ports and overloading the switch or connected networks*

IGMP-Snooping erlaubt Layer-2-Geräten das Mitlesen und verstehen der IGMP-Nachrichten des Layers 3. Der Switch belauscht den Datenverkehr nach IGMP-Nachrichten. Erkennt er Nachrichten des Internet Group Management Protocols, merkt sich der Switch, welches Endgerät an welchem Port welchen Multicast empfangen möchte. Dank dieser Information muss der Switch die Multicast-Daten nur auf den Ports senden, über die Gruppenmitglieder eines Multicasts erreichbar sind. *IGMP snooping allows Layer 2 devices to read and understand IGMP messages from Layer 3. The switch listens to the data traffic for IGMP messages. If it detects Internet Group Management Protocol messages, the switch remembers which end device on which port wants to receive which multicast. Thanks to this information, the switch only needs to send the multicast data on the ports through which group members of a multicast are reachable.*

# IGMP-Snooping: Das Abhörverfahren für Multicast-Traffic

***English as complete part after the whole chapter***

**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.

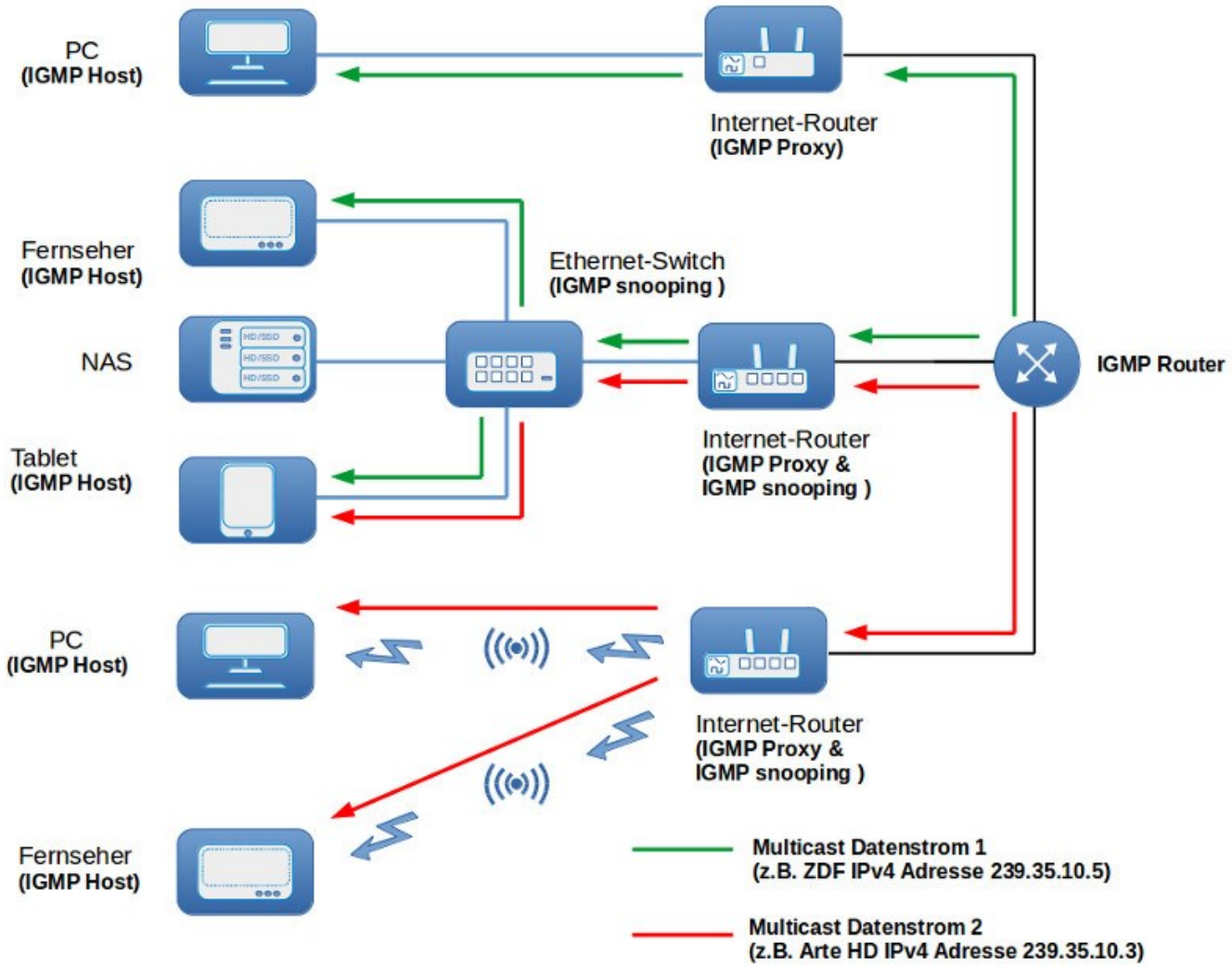



Bild: Internet Group Management Protocol Architektur (IGMP)

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:

# 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.

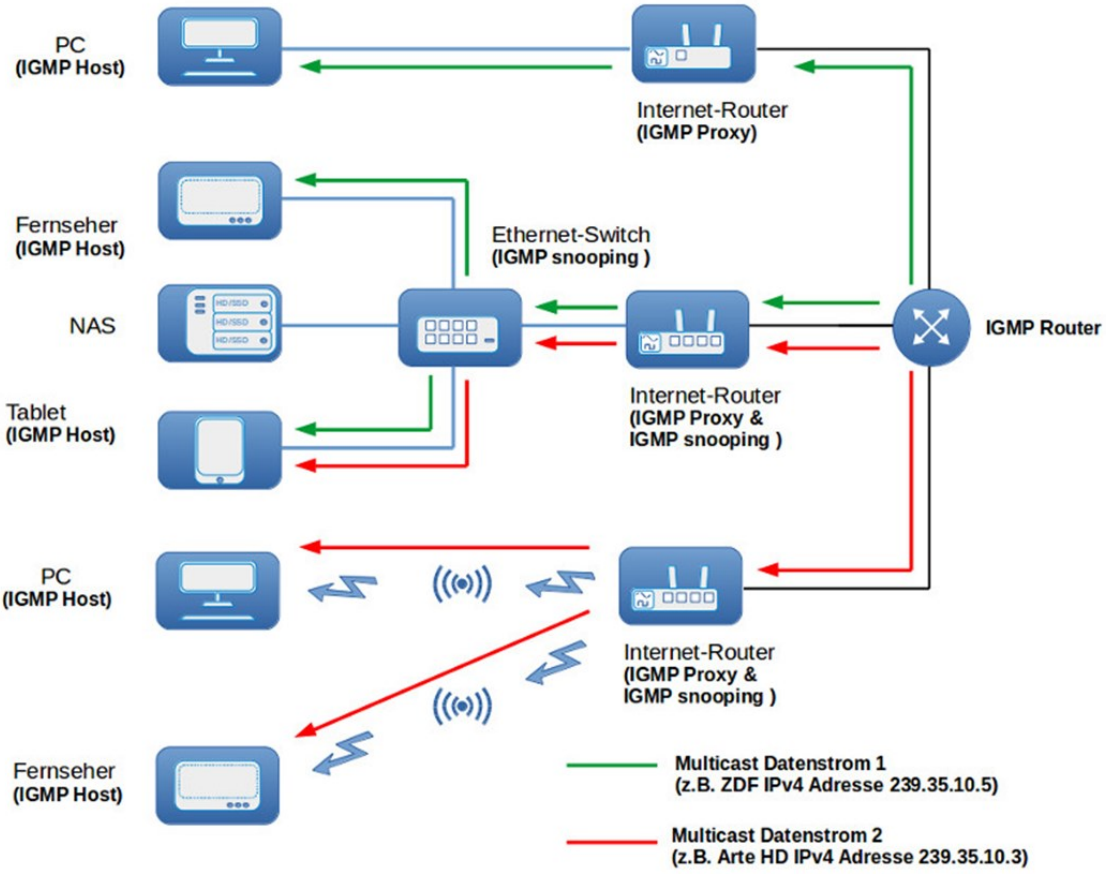
# The Internet Group Management Protocol (IGMP)

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.

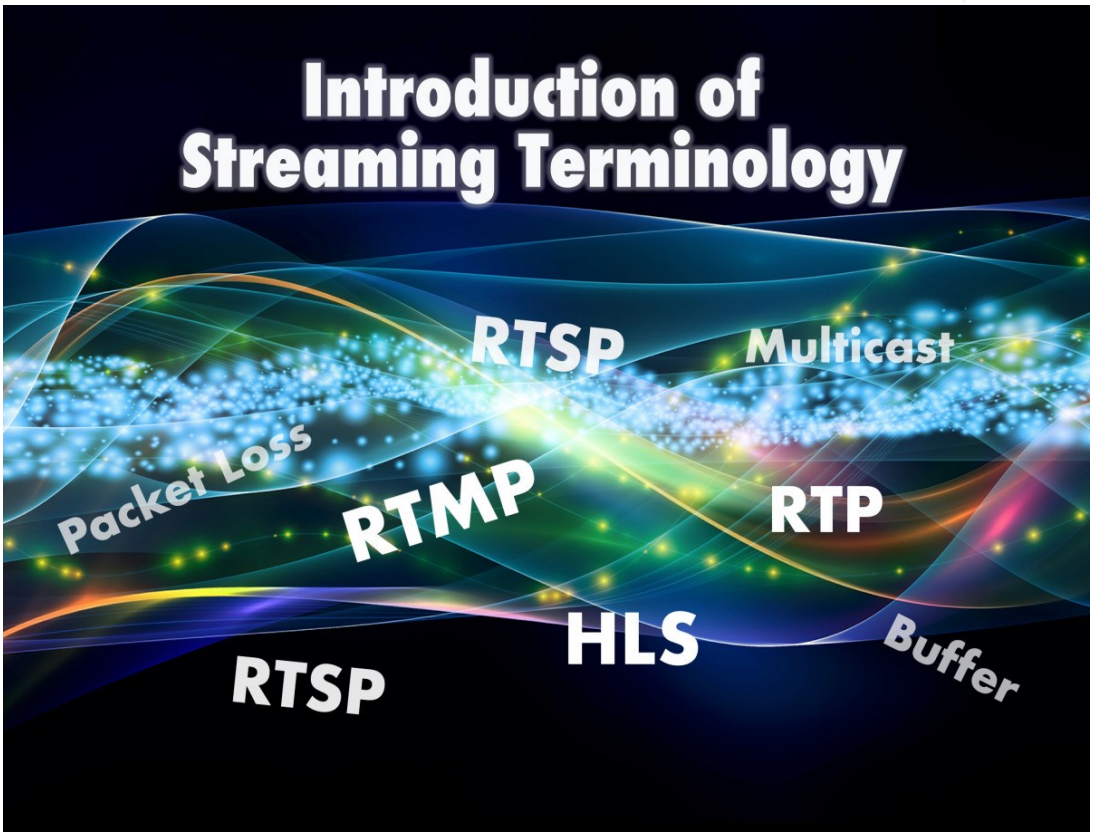
If you use Ethernet switches in your home network (even if integrated in an Internet router), there is another important point to note. An Ethernet switch works on the principle that it distributes a data packet whose destination it does not know to all outgoing interfaces, except to the interface via 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.

**Introduction of Streaming Terminology- What is UDP, TCP, Unicast, Multicast, RTP, RTSP, RTMP and more**

*Einführung in die Streaming-Terminologie - Was ist UDP, TCP, Unicast, Multicast, RTP, RTSP, RTMP und mehr*

many thanks to Datavideo




## Transmission protocols

### UDP

UDP stands for user datagram protocol and is an unreliable connectionless transmission protocol. The term connectionless means that the sender is not aware of the receiver(s): it is sending out data without knowing if the intended recipient is there as there is no handshake before sending data.
UDP is like sending out a letter in the post with a standard stamp; you won't get a confirmation that it's arrived you just hope it does.

*UDP steht für User Datagram Protocol und ist ein unzuverlässiges verbindungsloses Übertragungsprotokoll. Der Begriff "verbindungslos" bedeutet, dass der Absender den/die Empfänger nicht kennt: Er sendet Daten, ohne zu wissen, ob der vorgesehene Empfänger anwesend ist, da vor dem Senden der Daten kein Handshake stattfindet. UDP ist wie das Versenden eines Briefes mit einer Standardbriefmarke: Sie erhalten keine Bestätigung, dass der Brief angekommen ist, Sie hoffen nur, dass er angekommen ist.*

### TCP

TCP stands for transmission control protocol and is a reliable connection-based transmission protocol. As TCP is connection-based the sender is fully aware of the state of the intended recipients. A handshake must take place and a connection formed between sender and receiver before any data is sent.
TCP is like sending a letter using a recorded postal service, you get an acknowledgement that the letter has arrived and if it does not you can send it again.

*TCP steht für Transmission Control Protocol und ist ein zuverlässiges verbindungsbasiertes Übertragungsprotokoll. Da TCP verbindungsbasiert ist, kennt der Absender den Zustand des Empfängers genau. Es muss ein Handshake stattfinden und eine Verbindung zwischen Sender und Empfänger aufgebaut werden, bevor Daten gesendet*

*werden. TCP ist vergleichbar mit dem Versenden eines Briefes per Einschreiben: Sie erhalten eine Bestätigung, dass der Brief angekommen ist, und wenn dies nicht der Fall ist, können Sie ihn erneut versenden.*

## Communication Types / *Kommunikations-Arten*

### Unicast

Unicast is a one-to one connection between the client and the server (In most cases the server is the video encoder). Unicast uses IP delivery methods such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). The client has a direct relationship to the server. Each unicast client that connects to the server takes up additional bandwidth. For example, if you have 10 clients all playing 100-kilobits per second (Kbps) streams, those clients as a group are taking up 1,000 Kbps. If you have only one client playing the 100 Kbps stream, only 100 Kbps is being used.

*Unicast ist eine Eins-zu-Eins-Verbindung zwischen dem Client und dem Server (in den meisten Fällen ist der Server der Video-Encoder). Unicast verwendet IP-Übermittlungsmethoden wie das Transmission Control Protocol (TCP) und das User Datagram Protocol (UDP). Der Client steht in einer direkten Beziehung zum Server. Jeder Unicast-Client, der sich mit dem Server verbindet, beansprucht zusätzliche Bandbreite. Wenn Sie beispielsweise 10 Clients haben, die alle Streams mit 100 Kilobit pro Sekunde (Kbps) abspielen, verbrauchen diese Clients als Gruppe 1.000 Kbps. Wenn Sie nur einen Client haben, der den 100-Kbps-Stream abspielt, werden nur 100 Kbps verwendet.*

### Multicast

Multicast is a true broadcast. There is no direct relationship between the clients and server. This is similar to tuning into a station on a radio. Each client that listens to the multicast adds no additional overhead on the server. In fact, the server sends out only one stream. The same load is experienced on the server whether only one client or 1,000 clients are listening.

It's the job of the network switch or router to receive this single stream from the encoder and send it out to all the clients.

Please Note: Multicast on the Internet is generally not practical because only small sections of the Internet are multicast-enabled.

Even on a local network you need to be careful with multicast as routers and switches that are not capable of handling multicast correctly will treat it as a BROADCAST message. What this means is that if your encoder is connected to an un-configured Ethernet switch and sends out a multicast message it will broadcast this message out on all ports and flood the entire network with your stream. If the network is dedicated to that stream this is no big problem however it the network is used for other things it will cause performance issues.

The solution to this problem is to use switches that are IGMP compatible, these switches will forward multicast traffic only on ports connected to devices that are subscribed to that multicast group. In other words, the switch will only forward the stream out on ports that are connected to devices that are trying to tune in to your multicast stream.

*Multicast ist ein echter Broadcast. Es besteht keine direkte Beziehung zwischen den Clients und dem Server. Dies ist vergleichbar mit dem Einstellen eines Radiosenders. Jeder Client, der dem Multicast zuhört, verursacht keinen zusätzlichen Overhead für den Server. Tatsächlich sendet der Server nur einen Stream aus. Die Belastung des Servers ist dieselbe, egal ob nur ein Client oder 1.000 Clients zuhören. Es ist die Aufgabe des Netzwerk-Switches oder Routers, diesen einzelnen Stream vom Encoder zu empfangen und an alle Clients zu senden.*

*Bitte beachten Sie: Multicast im Internet ist im Allgemeinen nicht praktikabel, da nur kleine Teile des Internets multicastfähig sind. Selbst in einem lokalen Netzwerk müssen Sie mit Multicast vorsichtig sein, da Router und Switches, die Multicast nicht richtig verarbeiten können, es als BROADCAST-Nachricht behandeln. Das heißt, wenn Ihr Encoder an einen un-konfigurierten Ethernet-Switch angeschlossen ist und eine Multicast-Nachricht sendet, wird er diese Nachricht an alle Ports senden und das gesamte Netzwerk mit Ihrem Stream überfluten. Wenn das Netzwerk nur für diesen Stream verwendet wird, ist das kein großes Problem, aber wenn das Netzwerk auch für andere Zwecke verwendet wird, führt das zu Leistungsproblemen. Die Lösung für dieses Problem ist die Verwendung von IGMP-kompatiblen Switches, die den Multicast-Datenverkehr nur an Ports weiterleiten, die mit Geräten verbunden sind, die diese Multicast-Gruppe abonniert haben. Mit anderen Worten, der Switch leitet den*

*Datenstrom nur an Ports weiter, die mit Geräten verbunden sind, die versuchen, Ihren Multicast-Stream zu empfangen.*

## Broadcast

Broadcast is a type of communication where data is sent from one computer once and a copy of that data will be forwarded to all the devices. In Broadcast, there is only one sender and the data is sent only once. But the Broadcast data is delivered to all connected devices.
Switches by design will forward the broadcast traffic and routers by design will drop the broadcast traffic. In other words, Routers will not allow a broadcast from one LAN to cross the Router and reach another Network Segment. The primary function of a Router is to divide a big Broadcast domain to multiple smaller broadcast domains.
*Broadcast ist eine Art der Kommunikation, bei der Daten von einem Computer einmal gesendet werden und eine Kopie dieser Daten an alle Geräte weitergeleitet wird. Bei Broadcast gibt es nur einen Absender und die Daten werden nur einmal gesendet. Die Broadcast-Daten werden jedoch an alle angeschlossenen Geräte weitergeleitet. Switches leiten den Broadcast-Verkehr weiter, während Router den Broadcast-Verkehr nicht weiterleiten. Mit anderen Worten: Router lassen nicht zu, dass ein Broadcast von einem LAN den Router durchquert und ein anderes Netzwerksegment erreicht. Die Hauptfunktion eines Routers besteht darin, eine große Broadcast-Domäne in mehrere kleinere Broadcast-Domänen zu unterteilen.*

## Other Common Terminology

### Packet Loss

Packet loss occurs when one or more packets of data travelling across a computer network fails to reach its destination. Typically packet loss on an Ethernet network is non-existent, packet loss on WiFi is moderate if signal strength is good and packet loss over the internet is heavily dependent on the carrier's paths but can be heavy with poor internet connections.

*Paketverluste treten auf, wenn ein oder mehrere Datenpakete, die über ein Computernetz übertragen werden, ihr Ziel nicht erreichen. In der Regel gibt es keine Paketverluste in einem Ethernet-Netzwerk, die Paketverluste in einem WiFi-Netzwerk sind mäßig, wenn die Signalstärke gut ist, und die Paketverluste über das Internet hängen stark von den Übertragungswegen ab, können aber bei schlechten Internetverbindungen sehr hoch sein.*

### Buffer

A buffer or cache is the amount of video that is stored in memory before playback begins. A large buffer results in more delay but gives more stability when jitter and packet loss are present.

*Ein Puffer oder Cache ist die Menge an Videomaterial, die vor Beginn der Wiedergabe im Speicher abgelegt wird. Ein großer Puffer führt zu einer größeren Verzögerung, bietet aber mehr Stabilität, wenn Jitter und Paketverluste vorhanden sind.*

### Jitter

Jitter is the variation in the time between packets arriving, caused by network congestion, timing drift, or route changes. Jitter is a very important factor when streaming as if the delay over network path is constantly changing it could cause a packet to arrive late, the decoder must have a buffer big enough to continue playback while waiting for delayed packets.

*Jitter ist die Schwankung in der Zeit zwischen den ankommenden Paketen, die durch Netzüberlastung, Zeitverschiebung oder Routenänderungen verursacht wird. Jitter ist ein sehr wichtiger Faktor beim Streaming, denn wenn sich die Verzögerung über den Netzwerkpfad ständig ändert, kann dies dazu führen, dass ein Paket zu spät ankommt.*

## Streaming Protocols

The most commonly used streaming protocols, how they work and where they work best.

*Die am häufigsten verwendeten Streaming-Protokolle, wie sie funktionieren und wo sie am besten funktionieren.*

**RTP/RTSP**

RTP and RTSP are two completely different protocols that are commonly used together, although RTP can be used on its own RTSP cannot be used without RTP, this means if you see the term RTSP it always means RTP/RTSP.
RTP stands for real-time transport protocol and is used to carry the actual media stream, in most cases H264 or MPEG4 video is inside the RTP wrapper. RTSP is short for real-time streaming protocol and is used to establish and control the media stream.

*RTP und RTSP sind zwei völlig unterschiedliche Protokolle, die häufig zusammen verwendet werden. Obwohl RTP allein verwendet werden kann, kann RTSP nicht ohne RTP verwendet werden, d. h. wenn Sie den Begriff RTSP sehen, bedeutet er immer RTP/RTSP. RTP steht für Real-Time Transport Protocol und wird für die Übertragung des eigentlichen Medienstroms verwendet. In den meisten Fällen befindet sich H264- oder MPEG4-Video innerhalb des RTP-Wrappers. RTSP ist die Abkürzung für Real-Time Streaming Protocol und wird für die Einrichtung und Steuerung des Medienstroms verwendet.*

**What does this mean in practice?**

RTP on its own is a push protocol. This means that if a encoder wants to send video to a decoder using RTP, the encoder would need to know the decoder's IP address and would push the video to the listening decoder. RTP/RTSP is a pull protocol, this means the decoder connects to the encoder using the RTSP protocol the encoder then sends video to the decoder using the RTP protocol. Multiple decoders can connect to one RTSP server (this is called multi-unicast). RTSP also supports multicast.

*RTP ist an sich ein Push-Protokoll. Das bedeutet, dass ein Encoder, der ein Video über RTP an einen Decoder senden möchte, die IP-Adresse des Decoders kennen muss und das Video an den zuhörenden Decoder schieben muss. RTP/RTSP ist ein Pull-Protokoll, d. h. der Decoder verbindet sich mit dem Encoder über das RTSP-Protokoll, und der Encoder sendet dann das Video über das RTP-Protokoll an den Decoder. Mehrere Decoder können sich mit einem RTSP-Server verbinden (dies wird als Multi-Unicast bezeichnet). RTSP unterstützt auch Multicast.*

**Is it TCP or UDP based?**

Actually, it can be either. Usually, RTSP works over TCP and the actual RTP video stream is sent over UDP; the video and audio are sent over a pair of UDP ports. This is fine for streaming over a LAN but can be troublesome if used over the internet as it requires multiple ports. Also, as video and audio are sent separately, we rely on the timestamps in the RTP headers for synchronization.

So, when using RTSP over the internet we can interleave the RTP video and audio streams over the same TCP connection used for RTSP. Everything works over port 554 TCP.

*Eigentlich kann es beides sein. Normalerweise arbeitet RTSP über TCP und der eigentliche RTP-Videostream wird über UDP gesendet; Video und Audio werden über ein Paar UDP-Ports gesendet. Dies ist für das Streaming über ein LAN in Ordnung, kann aber bei der Verwendung über das Internet problematisch sein, da mehrere Ports benötigt werden. Da Video und Audio getrennt gesendet werden, sind wir für die Synchronisierung auf die Zeitstempel in den RTP-Headern angewiesen. Bei der Verwendung von RTSP über das Internet können wir also die RTP-Video- und Audioströme über dieselbe TCP-Verbindung verschachteln, die für RTSP verwendet wird. Alles funktioniert über Port 554 TCP.*

**What's it suitable for?**

RTSP is great for streaming to multiple devices on a local network where jitter and packet loss are minimal. RTSP works with almost all decoders and software players.

*RTSP eignet sich hervorragend für das Streaming an mehrere Geräte in einem lokalen Netzwerk, wo Jitter und Paketverluste minimal sind. RTSP funktioniert mit fast allen Decodern und Software-Playern.*

## MPEG-2 Transport Stream

MPEG-TS is probably the most commonly used streaming protocol in the broadcast industry, compatible with most set top boxes and decoders. MPEG-TS is commonly called a MPEG 2 Transport Stream even though the video inside the wrapper is actually H264 / MPEG 4 Part 10. MPEG TS is a usually a push protocol that takes audio and video over one stream.

*MPEG-TS ist wahrscheinlich das am häufigsten verwendete Streaming-Protokoll in der Rundfunkbranche und mit den meisten Set-Top-Boxen und Decodern kompatibel. MPEG-TS wird gemeinhin als MPEG 2 Transport Stream bezeichnet, obwohl das Video innerhalb des Wrappers eigentlich H264 / MPEG 4 Part 10 ist. MPEG TS ist in der Regel ein Push-Protokoll, das Audio und Video in einem Stream überträgt.*

**Is it TCP or UDP based?**

Typically, it is UDP based meaning if there is packet loss glitches will be seen in the stream as the lost data is not re-sent however high end encoders utilize a technology called FEC (Forward Error Correction) to combat this. FEC allows the decoder to make educated guesses as to what data was lost and fill the gaps back in.

Some equipment also supports MPEG-TS over TCP although this is not such a commonly used standard, Teradek equipment for example supports MPEG-TS over TCP.

*In der Regel handelt es sich um ein UDP-basiertes Verfahren, was bedeutet, dass bei einem Paketverlust Störungen im Datenstrom auftreten, da die verlorenen Daten nicht erneut gesendet werden. Hochwertige Encoder verwenden jedoch eine Technologie namens FEC (Forward Error Correction), um dies zu verhindern. FEC ermöglicht es dem Decoder, zu erraten, welche Daten verloren gegangen sind, und die Lücken wieder aufzufüllen. Einige Geräte*

*unterstützen auch MPEG-TS über TCP, obwohl dies kein weit verbreiteter Standard ist; Teradek-Geräte unterstützen beispielsweise MPEG-TS über TCP.*

## RTMP

This is original based on flash streaming and mainly used to get video into a CDN for distribution to large audiences online.

*Dabei handelt es sich original um Flash-Streaming, das hauptsächlich dazu verwendet wird, Videos in ein CDN zu übertragen, um sie an ein großes Online-Publikum zu verteilen.*

**What's it suitable for?**

RTMP(s) is reliable over the internet. Its low latency and low overhead have made it the standard for streaming into all major CDNs (YouTube Live, UStream, Wowza e.t.c). It can also be used for point-to-point connections with some encoders and decoders (Such as HDE / HDD – series from BLANKOM).

*RTMP(s) ist über das Internet zuverlässig. Die geringe Latenz und der geringe Overhead haben es zum Standard für das Streaming in alle großen CDNs (YouTube Live, UStream, Wowza usw.) gemacht. Es kann auch für Punkt-zu-Punkt-Verbindungen mit einigen Encodern und Decodern (z.B. HDE / HDD - Serie von BLANKOM) verwendet werden.*

**Is it TCP or UDP based?**

It's TCP-based. *TCB-basierend*

**HTTP Live Streaming (HLS)**

This stands for HTTP Live Streaming; this protocol is used to stream video IOS devices running the Safari web browser. Expect to see many seconds of delay as HLS downloads video in large chunks and the player always downloads one full chunk before starting playback.

*HLS steht für HTTP Live Streaming; dieses Protokoll wird zum Streamen von Videos auf IOS-Geräten mit dem Safari-Webbrowser verwendet. Rechnen Sie mit einer Verzögerung von mehreren Sekunden, da HLS Videos in großen Paketen herunterlädt und der Player immer ein ganzes Paket herunterlädt, bevor er mit der Wiedergabe beginnt.*

**What's it suitable for?**

HLS is usually used to stream to IOS devices when delay is not critical but stability is. HLS is now also becoming the standard protocol that most CDNs use to deliver video behind the scenes, however this is beyond the scope of this document.

*HLS wird in der Regel für das Streaming auf IOS-Geräte verwendet, wenn die Verzögerung nicht entscheidend ist, wohl aber die Stabilität. HLS wird nun auch zum Standardprotokoll, das die meisten CDNs für die Bereitstellung von Videos hinter den Kulissen verwenden, was jedoch den Rahmen dieses Dokuments sprengen würde. -> Siehe anderes Dokument bzgl. Latenzen und Protokollen. HLS ist dabei eines derjenigen mit den schlechtesten Latenz-Zeiten.*

**Is it TCP or UDP based?**

It uses HTTP which is a TCP based protocol. *Es verwendet HTTP, ein TCP-basiertes Protokoll.*

## Zixi

This protocol was specifically designed by Zixi to provide reliable delivery over extremely poor networks where packet loss and jitter are high (transatlantic for example). Zixi uses some very clever error correction to maintain a stable image even with huge packet loss.

*Dieses Protokoll wurde von Zixi speziell entwickelt, um eine zuverlässige Übertragung über extrem schlechte Netze zu gewährleisten, in denen Paketverluste und Jitter hoch sind (z. B. transatlantisch). Zixi verwendet eine ausgeklügelte Fehlerkorrektur, um auch bei großen Paketverlusten ein stabiles Bild zu erhalten.*

**What's it suitable for?**

Low latency streaming over extremely poor internet connections where MPEG-TS and RTMP fail to deliver.

*Streaming mit geringer Latenz über extrem schlechte Internetverbindungen, wo MPEG-TS und RTMP versagen.*

**Is it TCP or UDP-based?**

It is UDP-based but features forward error correction so achieves reliability similar to that of TCP-based protocols.

*Es ist UDP-basiert, verfügt aber über eine Vorwärtsfehlerkorrektur, so dass eine ähnliche Zuverlässigkeit wie bei TCP-basierten Protokollen erreicht wird.*

**But this is now more or less better solved by**

SRT – *this is documented in another PDF…*

*Aber das ist jetzt mehr oder weniger besser durch SRT gelöst - dies ist in einem anderen PDF dokumentiert...*

*Intro:*

SRT is a transport protocol that enables the secure, reliable transport of data across unpredictable networks, such as the Internet. While any data type can be transferred via SRT, it is particularly optimized for audio/video streaming.
SRT can be applied to contribution and distribution endpoints as part of a video stream workflow to deliver the best possible quality and lowest latency video at all times.
As packets are streamed from a source to a destination device, SRT detects and adapts to the real-time network conditions between the two endpoints. SRT helps compensate for jitter and bandwidth fluctuations due to congestion over noisy networks. Its error recovery mechanism minimizes the packet loss typical of Internet connections. And SRT supports AES encryption for end-to-end security.
SRT has its roots in the UDP-based Data Transfer (UDT) protocol. While UDT was designed for high throughput file transmission over public networks, it does not do well with live video. SRT is a significantly modified version that supports live video streaming.
Low latency video transmission across IP based networks typically takes the form of MPEG-TS unicast or multicast streams using the UDP protocol. This solution is perfect for protected networks, where any packet loss can be mitigated by enabling forward error correction (FEC). Achieving the same low latency between sites in different cities, countries or even continents is more challenging. While it is possible with satellite links or dedicated MPLS networks, these are expensive solutions. The use of cheaper public internet connectivity, while less expensive, imposes significant bandwidth overhead to achieve the necessary level of packet loss recovery.
Even though UDT was not designed for live streaming, its packet loss recovery mechanism provided an interesting starting point. The original version of SRT included new packet retransmission functionality that reacted immediately to packet loss to enable live streaming.
To achieve low latency streaming, SRT had to address timing issues. The characteristics of a stream from a source network are completely changed by transmission over the public internet, which introduces delays, jitter, and packet loss. This, in turn, leads to problems with decoding, as the audio and video decoders do not receive packets at the expected times. The use of large buffers helps, but latency is increased.

…

*SRT ist ein Transportprotokoll, das den sicheren und zuverlässigen Transport von Daten über unvorhersehbare Netzwerke wie das Internet ermöglicht. Obwohl jeder Datentyp über SRT übertragen werden kann, ist es besonders für Audio-/Video-Streaming optimiert.*

*SRT kann auf Beitrags- und Verteilungsendpunkte als Teil eines Videostream-Workflows angewendet werden, um jederzeit die bestmögliche Qualität und die geringste Latenz zu liefern.*

*Während die Pakete von einer Quelle zu einem Zielgerät gestreamt werden, erkennt SRT die Echtzeit-Netzwerkbedingungen zwischen den beiden Endpunkten und passt sich diesen an. SRT hilft, Jitter und Bandbreitenschwankungen aufgrund von Überlastung in verrauschten Netzwerken zu kompensieren. Sein Fehlerbehebungsmechanismus minimiert den für Internetverbindungen typischen Paketverlust. Und SRT unterstützt AES-Verschlüsselung für Ende-zu-Ende-Sicherheit.*

*SRT hat seine Wurzeln im UDP-basierten Datenübertragungsprotokoll (UDT). Während UDT für die Übertragung von Dateien mit hohem Durchsatz über öffentliche Netze entwickelt wurde, eignet es sich nicht für Live-Videos. SRT ist eine erheblich modifizierte Version, die Live-Video-Streaming unterstützt.*

*Die Videoübertragung mit geringer Latenz über IP-basierte Netze erfolgt in der Regel in Form von MPEG-TS-Unicast- oder Multicast-Streams unter Verwendung des UDP-Protokolls. Diese Lösung eignet sich perfekt für geschützte Netze, in denen Paketverluste durch die Aktivierung der Vorwärtsfehlerkorrektur (FEC) abgeschwächt werden können. Die gleiche niedrige Latenzzeit zwischen Standorten in verschiedenen Städten, Ländern oder sogar Kontinenten zu erreichen, ist eine größere Herausforderung. Zwar ist dies mit Satellitenverbindungen oder speziellen MPLS-Netzen möglich, doch handelt es sich dabei um teure Lösungen. Die Nutzung billigerer öffentlicher*

*Internetverbindungen ist zwar weniger kostspielig, erfordert aber einen erheblichen Bandbreiten-Overhead, um das erforderliche Niveau der Wiederherstellung von Paketverlusten zu erreichen.*

*Obwohl UDT nicht für das Live-Streaming konzipiert wurde, bietet sein Mechanismus zur Wiederherstellung von Paketverlusten einen interessanten Ansatzpunkt. Die ursprüngliche Version von SRT enthielt eine neue Funktion zur erneuten Übertragung von Paketen, die sofort auf Paketverluste reagierte, um Live-Streaming zu ermöglichen.*

*Um eine niedrige Latenzzeit beim Streaming zu erreichen, musste sich SRT mit Timing-Problemen befassen. Die Eigenschaften eines Streams aus einem Quellnetz werden durch die Übertragung über das öffentliche Internet völlig verändert, was zu Verzögerungen, Jitter und Paketverlusten führt. Dies wiederum führt zu Problemen bei der Dekodierung, da die Audio- und Videodekodierer die Pakete nicht zu den erwarteten Zeiten erhalten. Die Verwendung großer Puffer hilft, aber die Latenzzeit erhöht sich.*
*…*