# Dienstgüte und Resilience in ethernetbasierten Access Aggregation Netzwerken

Dietmar Tölle, Markus Zeller, Rudi Knorr
Fraunhofer-Einrichtung für Systeme der Kommunikationstechnik ESK
Hansastrasse 32, 80686 München
[toelle, zeller, knorr]@esk.fraunhofer.de

**Keywords**
Carrier Grade Ethernet, Resilience, Netzwerkdesign, QoS

## I. EINFÜHRUNG

Ethernet wird in den nächsten Jahren ATM als bevorzugte Technologie in Zugangsnetzen ablösen, da es einfach, schnell und kostengünstig zu realisieren ist. Der Datenverkehr mehrerer Kunden wird in den Zugangsknoten des Providers aggregiert. Diese auch Access Nodes genannten Knoten sind zum Beispiel DSLAMs für DSL und Wireless Access Points für WLAN oder WiMAX. Anschließend werden die Daten über den Uplink dieser Access Nodes an ein ausschließlich ethernetbasiertes Access Aggregation Netzwerke (AAN) weitergeleitet. Diese AAN werden häufig auch Next Generation Access Networks (NGAN) genannt.. Der Vorteil von Ethernet liegt in der Kosten- und Bandbreiteneffizienz, dem großen Bandbreitenbereich von Ethernet-Links und der geringen Komplexität in Bezug auf Betrieb, Management und Wartung. Allerdings weisen Ethernet und MAC Bridging in den aktuell standardisierten Versionen noch einige Mängel auf, die den Einsatz als Provider-Technologie einschränken. Neben der Problematik der Bereitstellung von Dienstgüte (Quality of Service, QoS) ist ein weiterer wichtiger Faktor die Zuverlässigkeit der Netzknoten und Verbindungen (Links) sowie die Fähigkeit der Fehlererkennung und Fehlerbehebung. Eine Möglichkeit der schnellen Fehlerbehebung ist ein fehlertolerantes Netzdesign, also die Nutzung redundanter Netzressourcen zur Sicherstellung des Netzbetriebs trotz auftretender Fehler im Netzwerk. Um sowohl QoS als auch eine hohe Verfügbarkeit zu erreichen, ist eine kombinierte Betrachtung beider Aspekte notwendig.

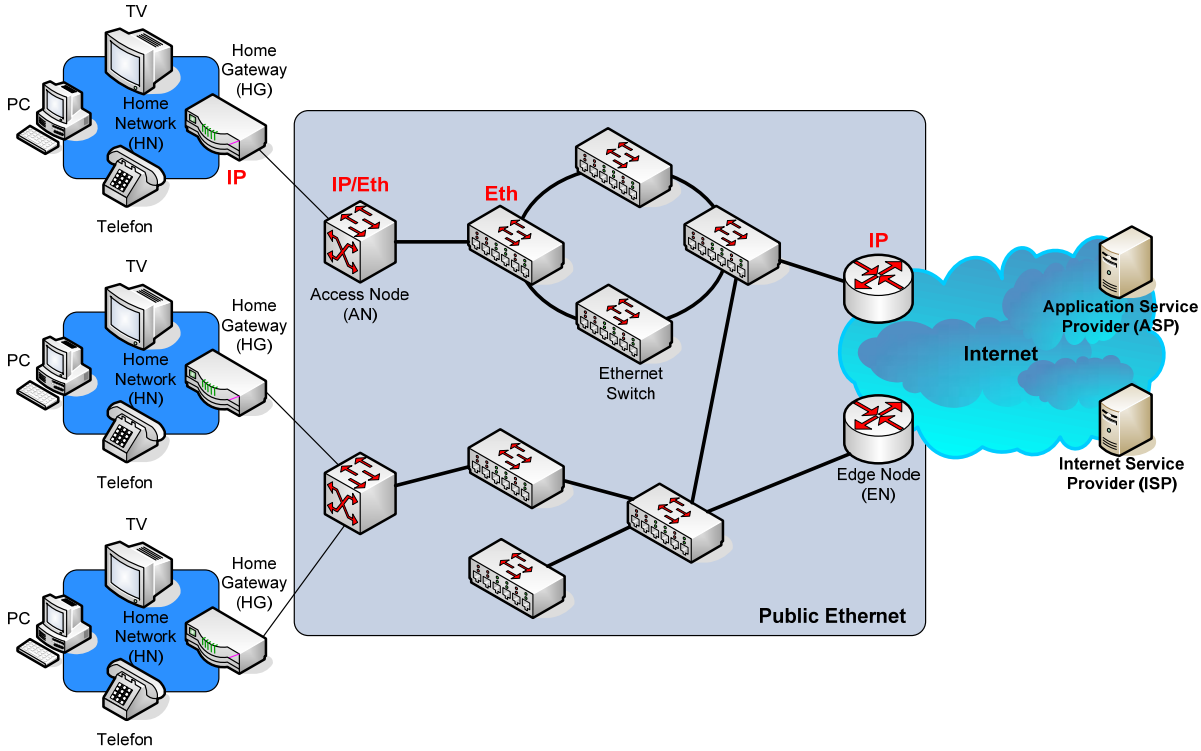


Abbildung 1: Struktur eines ethernetbasierten Access Aggregation Netzwerks

## II. QOS-FÄHIGES NETZDESIGN FÜR ETHERNET

Abbildung 1 zeigt ein typisches Beispiel für ein ethernetbasiertes AAN. Da dies im Normalfall von Netzbetreibern bereitgestellt wird, spricht man auch von Public Ethernet (öffentliches Ethernet), das dann aber auch strengen landesspezifischen Richtlinien in Bezug auf Sicherheit, Verfügbarkeit und eben QoS genügen muss. Das AAN beginnt an den Access Nodes, die die Kunden mit dem AAN verbinden, und endet an den Edge Nodes, den Übergängen ins IP-basierte Internet. Alle im hellblauen Feld befindlichen Netzelemente kommunizieren über Ethernet-Schnittstellen. Die Access Nodes können IP-Routing-Funktionalität besitzen oder ausschließlich auf Ethernet-Switching basieren. Die Edge Nodes sind IP-

basierte Router. Die Anbindung der Access Nodes an das Internet und die Aggregation des Datenverkehrs übernehmen Ethernet Switche, die für AAN über spezielle Funktionen verfügen müssen, die im Folgenden erläutert werden.
Diese Realisierungsform des AAN funktioniert zwar auch mit Standard-Ethernet-Switchen, diese können dann aber keine Dienstgüte bereitstellen, sondern nur Best Effort-Dienste. Das Hauptproblem diesbezüglich resultiert bei Ethernet, wie auch bei IP, aus der fehlenden Kontrollschicht (Control Plane). ISDN zum Beispiel hat diese Control Plane – der Zugriff darauf erfolgt über den D-Kanal – und nutzt diese, um mit der Wahl der Telefonnummer jeden beteiligten Netzknoten abzufragen, ob noch genügend freie Ressourcen für diese Verbindung zur Verfügung stehen. Bei einer positiven Rückmeldung wird ein fest reservierter Kanal durch das gesamte Netz geschaltet. Dies nennt man explizite Ressourcenreservierung. Erst wenn dieser Kontrollvorgang abgeschlossen ist, steht die Verbindung auf dem B-Kanal mit hoher Dienstgüte zur Verfügung.
Bei Ethernet und IP wird eine solche explizite Ressourcenreservierung standardmäßig nicht durchgeführt, die Datenpakete werden einfach nach Bedarf gesendet. Somit kann aber auch nicht vorausgesagt werden, wem wann welche Ressourcen zur Verfügung stehen. Diese nicht-deterministische Vergabe der Ressourcen führt dazu, dass keine QoS bereitgestellt werden kann.
Auch wenn Ethernet und IP über keine dedizierte Control Plane verfügen, kann man über erweiterte Management-Funktionen diese Control Plane integrieren. Sowohl Ethernet-Rahmen als auch IP-Pakete verfügen über Kontrollinformationen im Header. Neben der Quell- und Zieladresse gibt es noch Informationsfelder über den Typ und die Priorität der Daten. Diese Daten werden im Access Node ausgewertet (siehe Abbildung 2).

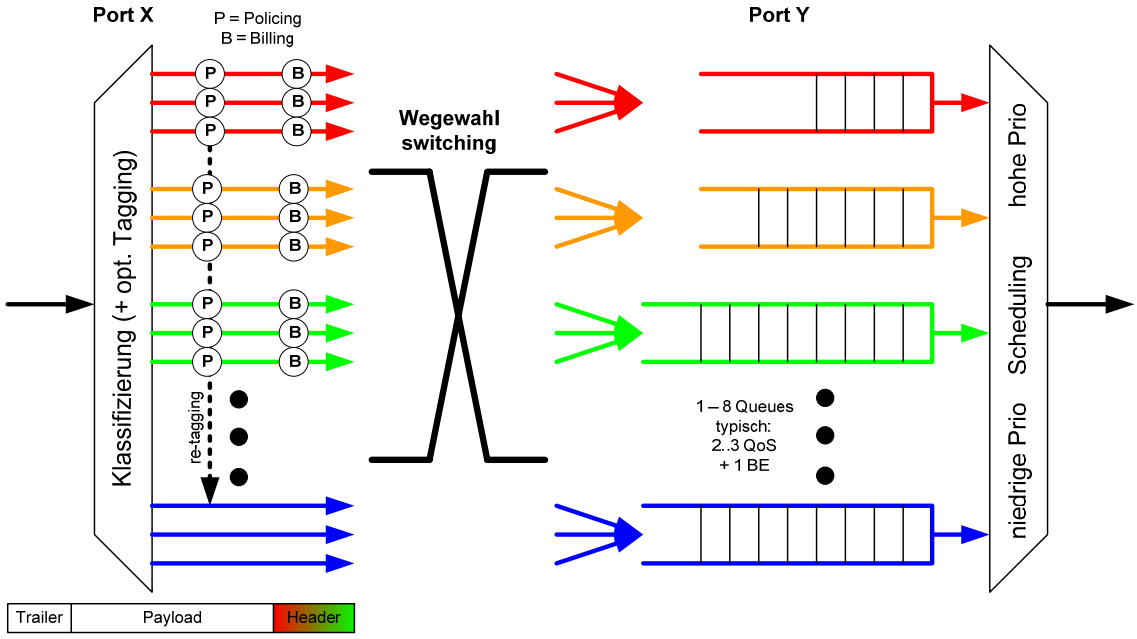

Abbildung 2: Klassifizierung im Access Node

Zunächst muss sich jeder Kunde, der einen Dienst anfordern will, beim Access Node authentifizieren. Bei ethernetbasierten Netzen erfolgt dies zum Beispiel über IEEE 802.1X, der so genannten Port Authentication. Nach erfolgreicher Authentifizierung kann der Kunde bei einem Service Provider einen Dienst per Signalisierungsprotokoll anfordern, zum Beispiel über SIP oder H.323. Verbunden mit dem Signalisierungsprotokoll oder vom Service Provider initiiert, wird mit der Anforderung des Diensts eine Ressourcenanforderung gestartet (siehe Abbildung 3). Sind sowohl Dienstanforderung als auch Ressourcenbereitstellung erfolgreich, so kann der Kunde den Dienst mit der jeweiligen Dienstgüte nutzen, das heißt der Netz-Provider garantiert die Dienstgüte gemäß den festgelegten Verkehrsparametern (siehe Textbox).
Am Eintrittspunkt des Datenverkehrs der Kunden – im Access Node – wird dieser zunächst klassifiziert und entsprechend seiner Wichtigkeit gekennzeichnet (tagging). Das Policing dient zur Lastkontrolle am Eingangsport ins Netz und kontrolliert, ob der Kunde nicht mehr Verkehr als für diesen Dienst vereinbart ins Netz sendet. Wird zuviel Verkehr gesendet oder kann das Netz die Verkehrsmenge nicht abarbeiten, so kann die Priorität für bestimmte Dienste reduziert werden (re-tagging).
Anschließend erfolgt die Abrechnung des Dienstes (Billing) entsprechend der Priorität des Dienstes, da von nun an die Priorität in diesem Netzabschnitt nicht mehr geändert wird und die Dienste mit höherer

Priorität Dienste mit niedrigerer verdrängen können. Dementsprechend sind Dienste mit höherer Priorität auch teurer.

Nach der Wahl des richtigen Ausgangsports (Switching) wird der gesamte Datenverkehr entsprechend seiner Priorität in Queues einsortiert. Das Queueing dient zur Lastkontrolle am Ausgang. Der Scheduler sorgt für die richtige Reihenfolge beim Aussenden der Daten aus den verschiedenen Queues. Dabei werden die Daten in den Queues mit höherer Priorität bevorzugt behandelt.

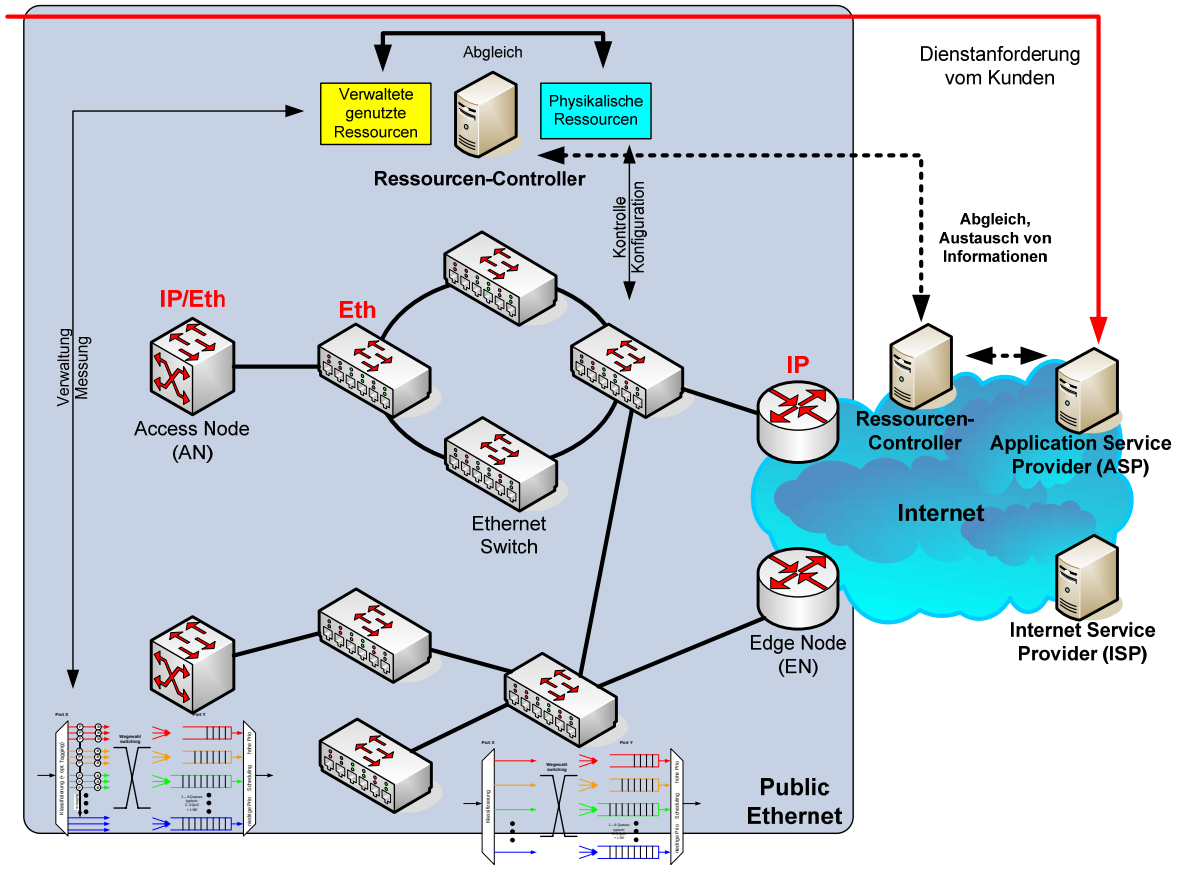

Abbildung 3: Dienstanforderung und Ressourcenbereitstellung

Diese erweiterte Behandlung des Verkehrs erfolgt einmalig in den Access Nodes. Optional kann diese auch in den Edge Nodes erfolgen, um den Datenverkehr in oder aus dem Internet erneut zu überprüfen und bewerten. In den Netzknoten zur Aggregation entfällt Tagging, Policing und Billing, der Rest der Prozedur bleibt gleich. Das Queueing und Scheduling ist in diesen Netzknoten wichtig, da der Verkehr von mehreren Access Nodes aggregiert wird und sich so die Reihenfolge der Datenpakete wieder ändern kann. Jeder dieser Netzknoten muss sicherstellen, dass die Verkehrsparameter eingehalten werden, wobei jeder Netzknoten einen Einfluss auf alle Verkehrsparameter hat. So kann sich in jedem Netzknoten die Ursache für die Verschlechterung der Dienstqualität ergeben. Bei jeder Aggregation ist die Dienstgüte potenziell gefährdet.
Die Hauptursachen für diese QoS-Einbrüche sind:

- Paketverlust: Überlast über einen längeren Zeitraum, fehlerhafte Übertragung
- Verzögerung: Ungünstiges Netzdesign, Topologie
- Jitter: Kurzzeitige Überlast (Bursts), Wegewahl bei Umschaltung und Lastverteilung
- Datenrate: Policing, Überlast

Um QoS zu gewährleisten, ist es erforderlich, dass im Netz ein Ressourcen-Controller existiert, der das Fehlen der Control Plane kompensiert. Dieser Ressourcen-Controller verwaltet zum einen die physikalischen Ressourcen im Netz, zum anderen verwaltet er die Ressourcennutzung durch die Dienste der Kunden und kombiniert diese miteinander. Der Ressourcen-Controller stellt also die aktuelle Ressourcennutzung durch Messung und Signalisierung fest, prüft die aktuellen physikalischen Ressourcen im Netz und legt fest, welcher Dienst welche Ressource nutzen darf.

Um QoS zu gewährleisten, müssen immer genug freie Ressourcen vorhanden sein. Ist dies nicht mehr der Fall, muss eine Dienstanforderung entweder abgelehnt werden oder der Dienst wird ohne QoS bereitgestellt. Die verfügbaren physikalischen Ressourcen spielen auch eine Rolle bei der Resilience.

## III. Fehlertolerantes Netzdesign für Ethernet

Mit Hochverfügbarkeit von Netzen bezeichnet man die Eigenschaft der Netze, die Funktionsfähigkeit idealer Weise in 100 Prozent der Zeit zu gewährleisten und damit die beauftragten Netzverbindungen und Dienste auch tatsächlich zu realisieren. Leider lässt sich eine Verfügbarkeit von 100 Prozent aufgrund der beschränkten Lebensdauer der Netzelemente und Verbindungen nicht erreichen, so dass mit Hochverfügbarkeit die Nähe zur hundertprozentigen Verfügbarkeit gemeint ist. Das oft genannte Ziel ist die 99,999-prozentige Verfügbarkeit, realistische Werte liegen zwischen 99 und 99,99 Prozent.
Um die Hochverfügbarkeit von Zugangsnetzen sicherzustellen, gibt es drei verschiedene Ebenen des Netzdesigns, die weitgehend unabhängig voneinander betrachtet und optimiert werden können: Geräteebene, Verbindungsebene und Netzebene.

### Geräteebene

Eine Lösung zur Sicherstellung der Verfügbarkeit ist die weitest mögliche Vermeidung von Fehlern und Ausfällen in den Netzknoten oder die redundante Auslegung betriebskritischer Einzelkomponenten innerhalb eines Gerätes.

### Verbindungsebene

Die Verfügbarkeit muss auch auf Verbindungsebene, den so genannten Netzkanten, so hoch wie möglich sein. Auch auf dieser Ebene hat man zwei Möglichkeiten, die Verfügbarkeit zu erhöhen: Erhöhung der Sicherheit einer Einzelverbindung oder redundante Auslegung der Verbindung.

### Netzebene

Die beiden oben angesprochenen Ebenen haben den signifikanten Nachteil, dass sie lediglich explizite Redundanz bereitstellen. Jede installierte redundante Netzressource dient zum Schutz einer ganz bestimmten Netzressource und keiner anderen. Dies erhöht die Kosten zum Teil erheblich, der Netzbetreiber kann aber hierbei sehr gut planen und steuern, ob und welche Redundanzen integriert werden.
Wesentlich flexibler erweist sich da die Redundanz auf Netzebene. Dieses Konzept sieht die Nutzung von ungeschützten Netzkomponenten und -verbindungen vor, die Ausfallsicherheit wird durch die gegenseitige Absicherung erhöht. Man spricht von einer verteilten Redundanz. Bei diesen Verfahren sind die Fehlererkennung und die Steuerung der Netzressourcen essentiell für Hochverfügbarkeit. Die Fehlererkennung und Netzsteuerung wird entweder zentral von einem Netzmanagement-System übernommen oder autonom durch die Netzelemente mittels eines geeigneten Protokolls.
Ein Grund für die hohe Kosteneffizienz von Ethernet ist die Fähigkeit, auf einfache und effiziente Weise Redundanz auf Netzebene bereitzustellen. Ethernet lässt sich prinzipiell zu jeder beliebigen Topologie zusammenschalten, allerdings ist es sehr anfällig für Schleifenbildung, die bei redundanten Netzen immer auftreten. Die Netzelemente unterstützen aber in der Regel zahlreiche Protokolle zur Schleifenvermeidung bei gleichzeitiger Bereitstellung von Redundanz. Die folgende Tabelle vergleicht die wichtigsten ethernetbasierten Verfahren hinsichtlich Einsatzzweck und Umschaltzeiten.

| Protokoll | Nutzbar für: | Fehlerreaktion | Initialisierung |
|---|---|---|---|
| STP (Spanning Tree Protocol) | Baumstrukturen | 15 - 50 Sekunden | 10 - 30 Sekunden |
| RSTP, MSTP (Rapid, Multiple STP) | Baumstrukturen | ca. 0,6 Sekunden | ca. 0,4 Sekunden |
| EAPS (Ethernet Automatic Protection Switching) | Ringstrukturen | 0,1 - 0,25 Sekunden | 0,1 Sekunden |

Tabelle 1: Vergleich ethernetbasierter Redundanzverfahren

## IV. Strategien zum fehlertoleranten QoS-Netzdesign

Die obigen Kapitel zeigen gängige Varianten des fehlertoleranten Netzdesigns für ethernetbasierte Netze, die zudem auch QoS bieten sollen. Bei der Bereitstellung von Redundanz auf der Geräte- bzw. Verbindungsebene ist zu beachten, dass diese explizite Redundanz sehr kostspielig sein kann. Die Systemhersteller sehen für viele ihrer Netzelemente Redundanz vor, der Betreiber kann den Grad der eingesetzten Redundanz auch sehr gut steuern. Bei der Verbindungsredundanz ist es sehr schwierig und kostenintensiv, ein hohes Maß bereitzustellen. Außerdem verhindern die Randbedingungen häufig eine

gezielte Bereitstellung von Redundanz. Die Möglichkeiten von Ethernet zur Bereitstellung von Redundanz auf Netzebene sind eine ideale Ergänzungsmöglichkeit, um Hochverfügbarkeit sicher zu stellen.
Der Ressourcen-Controller muss auch die redundanten Netzressourcen mitverwalten, damit ein Einzelfehler nicht zum Einbruch der QoS führt. Dazu werden nicht alle physikalischen Ressourcen für QoS-Dienste zur Verfügung gestellt. Die übrigen Ressourcen können Best Effort-Diensten zur Verfügung gestellt werden. Fällt eine Netzkomponente durch einen Fehler aus, können die Dienste mit hoher Priorität, also diejenigen die dem Provider den meisten Gewinn bringen, weiterhin bedient werden. Lediglich der Anteil der Ressourcen für die Best Effort-Dienste wird geringer. So kann der Netzbetreiber trotz Fehler im Netz den Gewinnausfall minimieren.
Die im Ressourcen-Controller ablaufenden Prozesse sind allerdings komplex, was insbesondere bei großen Netzen leistungsstarke Rechner benötigt. Die Fraunhofer-Einrichtung für Systeme der Kommunikationstechnik ESK arbeitet an Lösungen zur Optimierung dieser Verfahren. Dabei wird auf autonome, verteilte Prozesse gesetzt, die in den Netzelementen direkt ablaufen können. Außerdem können diese die Redundanzverfahren direkt mit einbeziehen, so dass die Ausfallsicherheit ein integraler Bestandteil dieses Verfahrens ist.

Begriffsdefinition Quality of Service (QoS):
Dienstqualität bzw. Dienstgüte

QoS bezeichnet den messbaren Erreichungsgrad der für einen Dienst festgelegten Verkehrsparameter. Dieser Grad sollte immer möglichst nahe an 100 Prozent liegen. Letzten Endes will man mit QoS die Garantie der vereinbarten Verkehrsparameter erreichen.
Verschiedene Dienste, die über Netzwerke bezogen bzw. in Anspruch genommen werden können, benötigen eine gewisse Dienstgüte.

Die Dienstgüte wird anhand von Verkehrsparametern spezifiziert.
Die Verkehrsparameter sind dabei:

- Minimal benötigte bzw. erwartete Datenrate (Überschreitung möglich)
- Maximale Ende zu Ende Verzögerung (Unterschreitung möglich)
- Verzögerungsvarianz $\Rightarrow$ Jitter
- Maximale Paketverluste (Unterschreitung möglich)

Bei dieser Betrachtung wird zunächst davon ausgegangen, dass die Verfügbarkeit A des Netzes bei 100 Prozent liegt bzw. das Netz gerade verfügbar ist.

Ist ein bestimmter Dienst aktiv, zum Beispiel Internet TV, wird erwartet, dass die Datenpakete entsprechend der festgelegten Verkehrsparameter beim Empfänger des Dienstes ankommen, also zum Beispiel 2,5 MBit/s Datenrate, 250 Millisekunden Verzögerung, 30 Millisekunden Verzögerungsvarianz und 1 Prozent Paketverlust. Werden diese Verkehrsparameter eingehalten, erhält der Kunde den Dienst in der erwarteten Qualität. Aufgrund der Eigenheiten der Netze ist dies aber nicht immer der Fall.
Mit QoS wird beschrieben, wie gut die Verkehrsparameter über die Zeit des Dienstes eingehalten werden, also eine prozentuale Übersicht des Erreichungsgrades der Verkehrsparameter.
Wie im Beispiel zu erkennen ist, ist es durchaus vertretbar, dass Datenpakete des Dienstes verloren gehen, aber nur bis zu einem Wert von 1 Prozent. Gehen mehr als 1 Prozent der Pakete verloren, so reduziert sich die Qualität des Dienstes. Natürlich kann ein Parameter deutlich in positiver Richtung vom vereinbarten Wert abweichen, zum Beispiel eine deutlich kleinere Verzögerung, darf aber die anderen Parameter nicht ungünstiger beeinflussen.

QoS wird häufig gleichgesetzt oder sogar verwechselt mit Maßnahmen zur Sicherung der Dienstqualität. So sind etwa die Klassifizierung und Priorisierung, der so genannten Class of Service (CoS), oder die Ressourcenreservierung Maßnahmen zur Sicherung der QoS, nicht QoS selbst.

Da die Dienstqualität sehr subjektiv ist, ist QoS häufig nicht ausreichend zur Beschreibung, und so wird der Begriff Quality of Experience (QoE) immer bedeutsamer. Hier sollen auch subjektive Werte einfließen. Hierzu jedoch nur ein kleiner Vergleich:
Beim Surfen im Internet wird meist keine Dienstqualität festgelegt, womit aus QoS-Sicht die Verkehrsparameter beliebig sein können. Bei QoE kommen jetzt noch die Reaktionszeit und die Datenrate ins Spiel. Der Eindruck ist schlecht, wenn man viele Sekunden auf den Seitenaufbau warten muss, weil die Datenrate so gering ist – also: die QoS ist OK, die QoE ist es nicht!