

Sicherheitsmechanismen für Voice over IP

von

Dr. Behrooz Moayeri

6.2 Schutz für Quality of Service (QoS)

Dieser Abschnitt befasst sich mit dem Zusammenhang zwischen QoS für VoIP und VoIP-Sicherheit.

6.2.1 QoS als Sicherheits- und Vertrauensfrage

In vielen IPT-Umgebungen wird das Netz so konfiguriert, dass zur Sicherstellung der Quality of Service (QoS) die Voice-Pakete priorisiert werden und für sie Ressourcen im Netz reserviert wird. In diesen Fällen stellt sich auch die Sicherheits- und Vertrauensfrage, denn mit einer Manipulation der Paketmarkierung (zum Beispiel des DSCP-Feldes im IP-Header) kann unberechtigten Benutzern eine privilegierte Behandlung ihrer Pakete durch das Netz ermöglicht werden. So kann neben „Theft of Service“ auch „Denial of Service“ die Folge sein, wenn durch die Manipulation die Ressourcen ausgeschöpft werden und die legitime Voice-Applikation nicht mehr funktioniert.

Dagegen helfen zwei Kategorien von Maßnahmen:

- Implementierung von Richtlinien am Rand des Netzes UND
- Sicherheit und Integrität der gesamten Netzinfrastruktur.

Die entscheidende Frage in diesem Zusammenhang ist, ob allen oder ob nur einem Teil der Endgeräte vertraut werden kann. Abhängig von dieser Frage kann es erforderlich sein, die Ports im Netz unterschiedlich zu konfigurieren, zum Beispiel als vertrauenswürdige und nicht vertrauenswürdige Ports.

Einige der wichtigsten Sicherheitsanforderungen an eine QoS-Architektur besteht darin, dass die Nutzung von WAN-Kapazitäten für VoIP dort, wo Überkapazitäten unwirtschaftlich sind, einem Admission-Control-Mechanismus unterzogen wird, d.h. verhindert wird, dass zu viele priorisierte Paketströme in das WAN gelassen werden. Um die unkontrollierte Nutzung der für VoIP vorgesehenen Netzkapazität an der zentralen Kontrollinstanz vorbei zu verhindern, darf die zu VoIP passende Markierung der IP-Pakete nur für „offizielle“ VoIP-Anwendungen eingesetzt werden. Dies setzt eine strikte Kontrolle über die Endgeräte voraus, wenn die IP-Header von den Endgeräten gesetzt werden.

Ist dies nicht sichergestellt, muss eine nachträgliche Modifizierung der Header durch das Netz eingeleitet werden, indem die dafür erforderlichen Veränderungen der Netzarchitektur und des Betriebskonzeptes vorgenommen werden.

Im Zusammenhang mit der Kontrolle über die Endgeräte ist zu erwähnen, dass dies in einem Unternehmensnetz aus Sicherheitsgründen ohnehin erforderlich ist, sodass in vielen Unternehmen die Endgeräte in den Vertrauensbereich für die Zuordnung zu Prioritätsklassen einbezogen werden können.

6.2.2 Denkbare Vertrauensgrenzen

Die Abbildung 6.18 zeigt denkbare Modelle für die Festlegung der Vertrauensgrenzen bzw. für die Durchführung der Klassifizierung/Markierung im Zusammenhang mit VoIP.

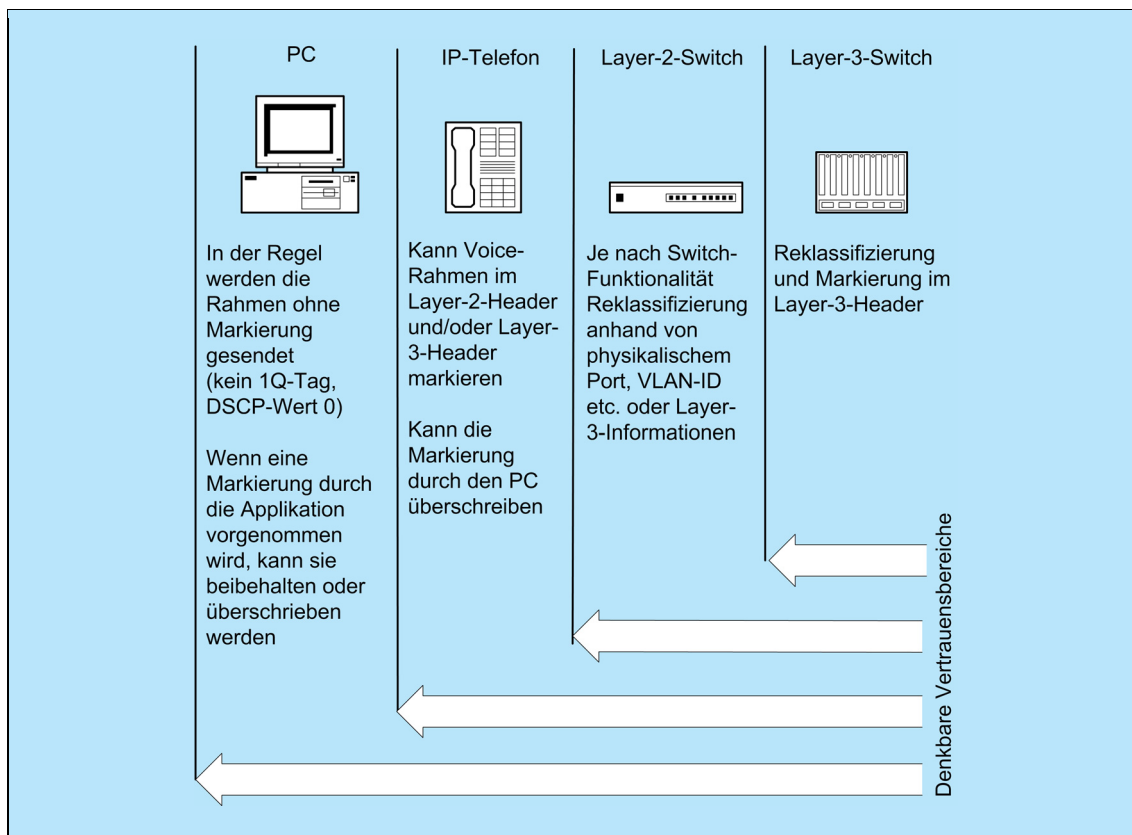


Abbildung 6.18: Denkbare Vertrauensgrenzen

Das erste Modell besteht darin, nur den Layer-3-Switchs zu vertrauen und auf der Layer-3-Instanz für alle Pakete eine Reklassifizierung und Markierung aller Pakete vorzunehmen. Dazu müssen auf dem Layer-3-Switch entsprechende Regeln eingestellt werden.

Weitet man den Vertrauensbereich auf alle Netzkomponenten aus und schließt damit auch die Layer-2-Switchs im LAN in diesen Bereich ein, kann man eine Reklassifizierung der Pakete je nach Produkt anhand verschiedener Kriterien wie zum Beispiel dem physikalischen Port, der VLAN-ID oder auch der Layer-3-Informationen im Paket vornehmen.

Schließt der vertrauenswürdige Bereich neben den Netzkomponenten auch noch die IP-Telefone ein, kann man je nach Telefontyp die Pakete der hinter den Telefonen angeschlossenen Endgeräte neu markieren.

Alternativ können alle Endgeräte in den vertrauenswürdigen Bereich einbezogen werden. Dann können zum Beispiel bestimmte Applikationen wie Softpho-

nes eine QoS-Markierung vornehmen.

Die Abbildung 6.19 zeigt unterschiedliche Modelle für die Behandlung von LAN-Ports, an die PCs und Telefone angeschlossen werden.

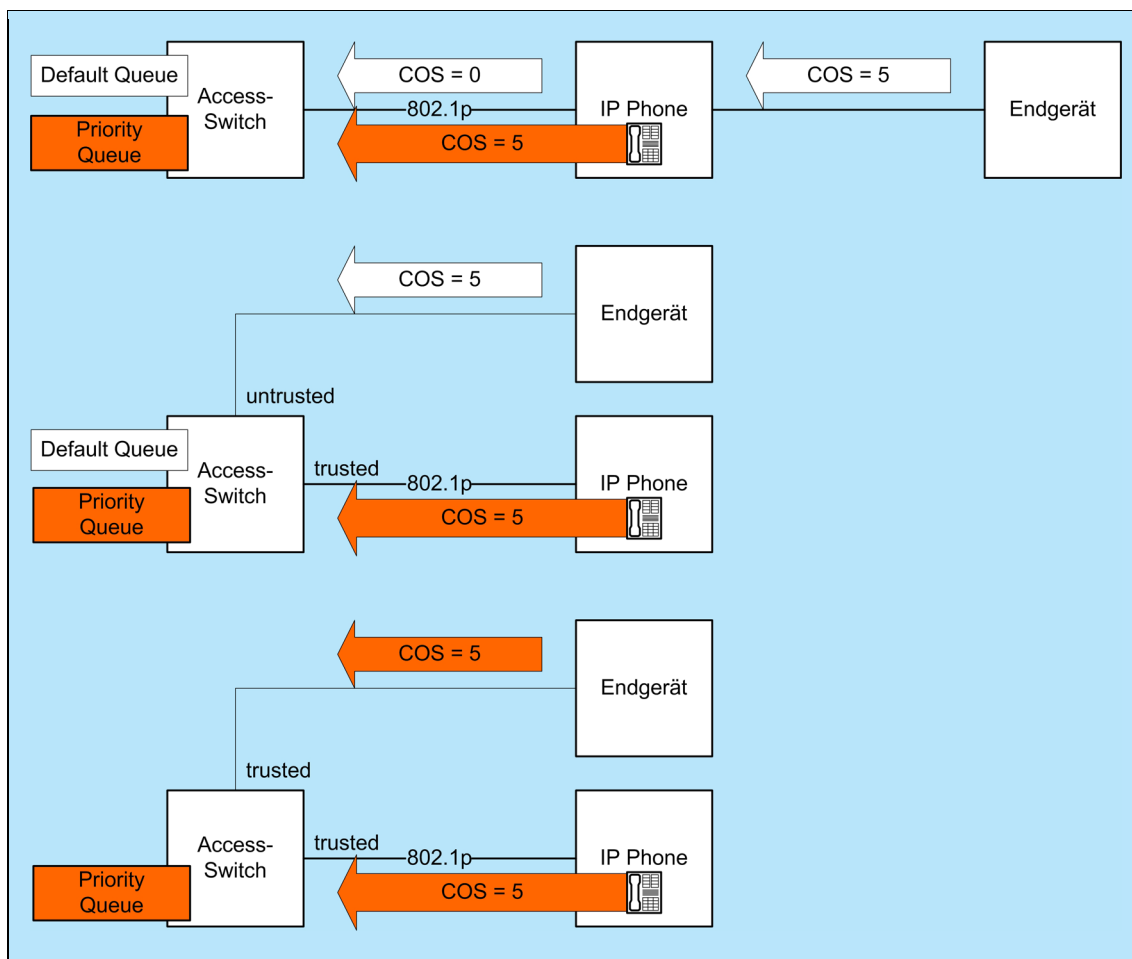


Abbildung 6.19: Trusted und Untrusted Ports am Switch

Im obersten Modell gemäß der Abbildung 6.19 überschreibt das IP-Telefon alle Markierungen, die das an den Miniswitch des Telefons angeschlossene Endgerät in den Paket-Header schreibt, sodass die Pakete des PCs als nicht zu priorisierende Pakete beim Access-Switch ankommen.

Der Priorisierung durch den PC wird im mittleren Modell nicht vertraut, sodass der Access-Switch die Markierung des PCs überschreibt. Der Port, an den das Telefon angeschlossen ist, wird jedoch als trusted Port konfiguriert, sodass die vom Telefon vorgenommene Markierung übernommen wird.

Im unteren Modell werden alle Ports als vertrauenswürdig konfiguriert, sodass nicht nur der Markierung durch die Telefone, sondern auch den entsprechenden Angaben der PCs vertraut wird. In diesem Modell werden Soft- und Hardphones gleich behandelt.

6.2.3 Denkbare QoS-Architektur

Die Grundzüge einer denkbaren QoS-Architektur können wie folgt sein:

- VoIP-Pakete werden im DSCP-Feld des IP-Headers markiert.
- Jene IP-Router an der Übergabestelle zwischen LAN und MAN/WAN, die VoIP übertragen müssen, priorisieren die VoIP-Pakete gegenüber allen anderen Paketen mit Ausnahme der Netzsteuerungspakete (Routing Updates etc.) bis zu der für VoIP vorgesehenen Netzkapazität.
- Die Nutzung von WAN- und MAN-Kapazitäten für VoIP muss dort, wo Überkapazitäten unwirtschaftlich sind, einem Admission-Control-Mechanismus unterzogen werden. Ein möglicher standardisierter Ansatz hierfür ist der H.323-Gatekeeper. Der Einsatz eines H.323-Gatekeepers oder eines entsprechenden Mechanismus auf anderen zentralen Komponenten der VoIP-Umgebung (Telefonieserver, Gateways) ist unerlässlich.
- Um die unkontrollierte Nutzung der für VoIP vorgesehenen Netzkapazität am Gatekeeper bzw. anderweitiger Kontrollinstanz vorbei zu verhindern, darf die zu VoIP passende Markierung der IP-Pakete nur für VoIP eingesetzt werden. Dies setzt eine strikte Kontrolle über die Endgeräte voraus, da die IP-Header von den Endgeräten gesetzt werden. Eine nachträgliche Modifizierung der Header durch das Netz ist nur durch wesentliche Veränderungen der LAN-Architektur und des Betriebskonzeptes möglich. Die strikte Kontrolle über die Endgeräte ist aus Sicherheitsgründen ohnehin erforderlich, sodass die Endgeräte in den Vertrauensbereich für die Zuordnung zu Prioritätsklassen einbezogen werden können.
- Eine statische Priorisierung von VoIP-Paketen ohne Bitratenbegrenzung könnte die anderen WAN-Anwendungen beeinträchtigen. Daher muss am Rand des WAN eine Obergrenze des Voice-Verkehrs festgelegt werden, der über das IP-WAN übertragen wird. Sinnvoll ist eine Begrenzung der Bitrate für priorisierten VoIP-Verkehr, welcher vom LAN in das WAN übertragen wird. Diese Bitratengrenze muss in Korrelation mit der Zahl der Verbindungen stehen, welche die lokale Kontrollinstanz über das IP-WAN erlaubt. Wird diese maximal Zahl von Verbindungen erreicht, muss eine Routing-Funktion am Standort die Route über das PSTN wählen.
- In WAN mit langsamen Verbindungen, die sowohl Daten als auch Sprache übertragen, müssen Pakete fragmentiert werden, damit ein VoIP-Paket nicht auf die vollständige Übertragung eines langen Datenpakets warten muss und zwischen den Fragmenten eines solchen Paketes übertragen werden kann.

Auf einige Einzelheiten der Implementierung wird in den folgenden Abschnitten eingegangen.