Zeitschrift: bulletin.ch / Electrosuisse
Herausgeber: Electrosuisse
Band: 96 (2005)
Heft: 1

Artikel: Wenn Voice-over-IP nicht funktioniert
Autor: Goldstein, Peter
DOI: https://doi.org/10.5169/seals-857759

Wenn Voice-over-IP nicht funktioniert

Konzeptionelle Fehler in IP-Anwendungen – NAT ist nicht das Problem

Das Internet basiert auf einem geschichteten Protokoll-Stack – analog den 7 OSI-Schichten. Die Anwendung arbeitet in der Regel mit der URL, zum Beispiel http://www.electrosuisse.ch oder sip:absender@sender.net. Die Netzwerkschicht dagegen mit einer IP-Adresse wie 82.195.225.102. Einige Anwendungen, darunter Voice-over-IP, nutzen die IP-Adresse aber auch in der Anwendungsschicht und übergeben diese Adressinformation der Netzwerkschicht für das Routing. Mit der Folge, dass die Anwendung nicht funktioniert, wenn ein NAT-Server die Adressen auf der Netzwerkschicht wechselt.

Peter Goldstein

Immer häufiger beschliessen Unternehmen, ihr IP-basiertes Firmennetz an das Internet anzuschliessen. Dies ist aber nicht immer so ohne weiteres möglich – häufig gibt es einen Adressenkonflikt, denn in Firmennetzen werden oft beliebige oder die von der IANA für Unternehmensnetze reservierten IP-Adressen[1] vergeben. Im Internet sind aber nur die von der Internet Assigned Numbers Authority (IANA)[2] zugewiesenen, öffentlichen IP-Adressen zulässig. Diese muss man in der Regel bei seinem Internet Service Provider (ISP) beantragen. Da die Anzahl IP-Adressen im heutigen Internet (IPv4) begrenzt ist, stellt sich für ein Unternehmen die Frage, ob jeder Host des Firmennetzes eine öffentliche IP-Adresse braucht oder nicht. In der Regel kann dies verneint werden, denn das Problem lässt sich elegant mit Network Address Translation (NAT) lösen. NAT in Kombination mit einer Firewall schützt zudem das Firmennetz gegen Angriffe von aussen. Nicht alle Anwendungen kommen aber mit NAT zurecht, wie das Beispiel mit Voice-over-IP zeigt.

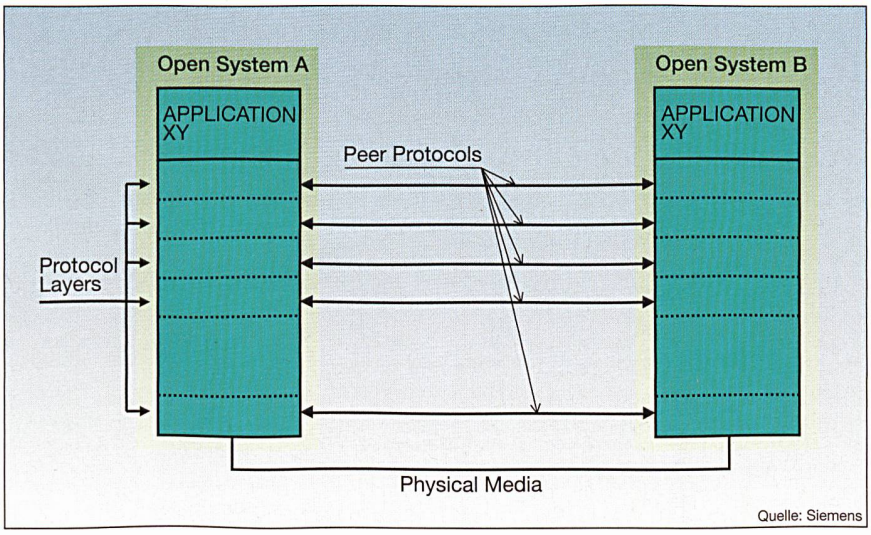

Bild 1 Referenzmodell für geschichtete Protokoll-Architektur

Protokoll-Architektur

Das Internet-Protokoll (IP) besteht aus einem geschichteten Protokoll-Stack. IP selbst ist ein Protokoll der Netzwerkschicht (Layer 3) und erbringt Dienste für die Protokolle TCP, UDP oder auch SCTP. IP seinerseits beansprucht die Dienste der unteren Schichten, zum Beispiel Ethernet (LAN) oder ATM[3]. Die Referenz für geschichtete Protokoll-Stacks ist der OSI-Stack[4] mit seinen 7 Schichten. Andere Beispiele für geschichtete Protokoll-Stacks sind der SS7- oder der ATM-Stack[5]. Die konzeptionelle Idee der geschichteten Protokoll-Stacks liegt darin, dass die Schicht (n) einen Service für die darüber liegende Schicht (n+1) erbringt. Neben den eigentlichen Protokolldaten werden an der Schnittstelle zwischen den Schichten, den so genannten Boundaries (upper and lower boundary), auch weitere Informationen ausgetauscht, zum Beispiel Adressinformationen. Eine Client-Anwendung ermittelt zum Beispiel aus der URL via DNS die IP-Adresse des Servers, den sie ansprechen will, und übergibt diese zusammen mit den zu übertragenden Daten an die Netzwerkschicht. Die Daten können unter anderem die IP-Adresse des Client beinhalten. Dies geht auch in umgekehrter Richtung: Die Netzwerkschicht kann die empfangene Netzwerkadresse über die Schichten des Protokoll-Stacks hinweg der Anwenderschicht übergeben, wo sie gespeichert und beim Senden einer Antwort wieder genutzt wird.

Das OSI-Modell wurde in Zusammenarbeit zwischen ISO und ITU-T erarbeitet. Einige grundsätzliche Aspekte sind sowohl als ISO/IEC International Standards (7498-1 und 10731) als auch als ITU-T Recommendations (X.200 und X.210) publiziert. Ein wesentlicher Aspekt des Modells ist das Konzept der geschichteten Architektur. Es müssen nicht zwingend alle 7 Schichten implementiert

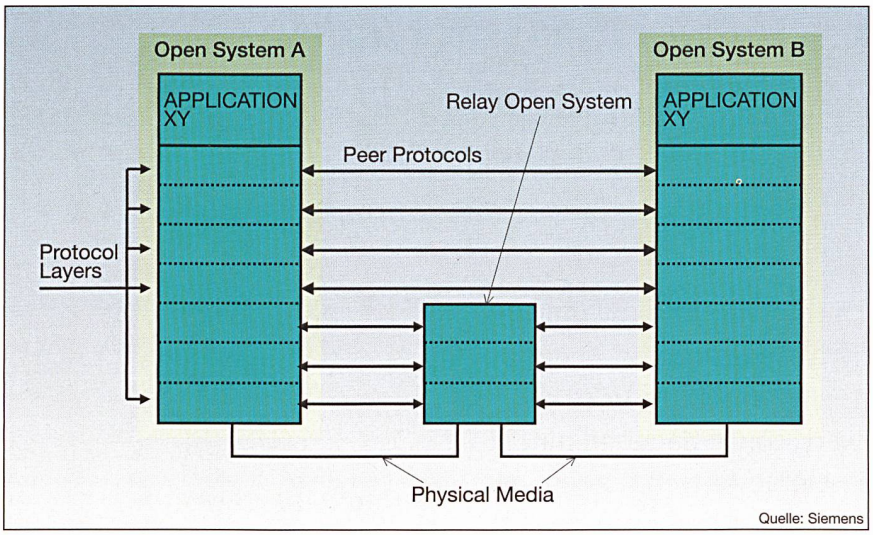

Bild 2 Netzszenario mit Relay

sein. Dies wird oft aus Gründen der Vereinfachung oder des Kosten/Nutzen-Verhältnisses ausgenützt. Beispiele für geschichtete Protokoll-Architekturen, die nicht alle Schichten des OSI-Modells realisieren sind SS7 und ATM aus der Telekommunikation und IP aus der Datenwelt.

Anwendungen sollten möglichst unabhängig von Netzwerktechnologien sein, was gerade durch das Modell der geschichteten Protokoll-Architektur unterstützt wird. Die Anwendungsinstanzen benützen Protokoll-Stacks um miteinander zu kommunizieren (Bild 1). Ein Szenario mit einem Relay Open System zwischen den beiden offenen Systemen zeigt Bild 2. Beispiele für solch ein Relay sind der Signal Transfer Point (STP) des SS7 in Telekommunikationsnetzen oder die Router[6] in IP-Netzen. Ein Relay ist bloss für die Weiterleitung der Protokoll-Nachrichten besorgt und kommt mit einem reduzierten Protokoll-Stack aus. Der Aufbau einer Schicht ist aus Bild 3 ersichtlich. Dabei bezeichnet Layer (n) Entity im Wesentlichen die Protokoll-Maschine der Schicht (n), die das Peer-to-Peer-Protokoll abwickelt. Die Umsetzung der Primitives (Modellierung der Kommunikationsschnittstelle zwischen den Protokoll-Schichten) des Service Users durch den Service Provider zeigt Bild 4. Die Primitives sind durch Namen (Generic Name) und Typus (Specific Name) beschrieben und können neben den Anwender-Daten zusätzliche Parameter beinhalten, zum Beispiel die Adresse des Ursprungs und Ziels[7]. Die Tabelle zeigt in allgemeiner Form die Beschreibung der Primitives.

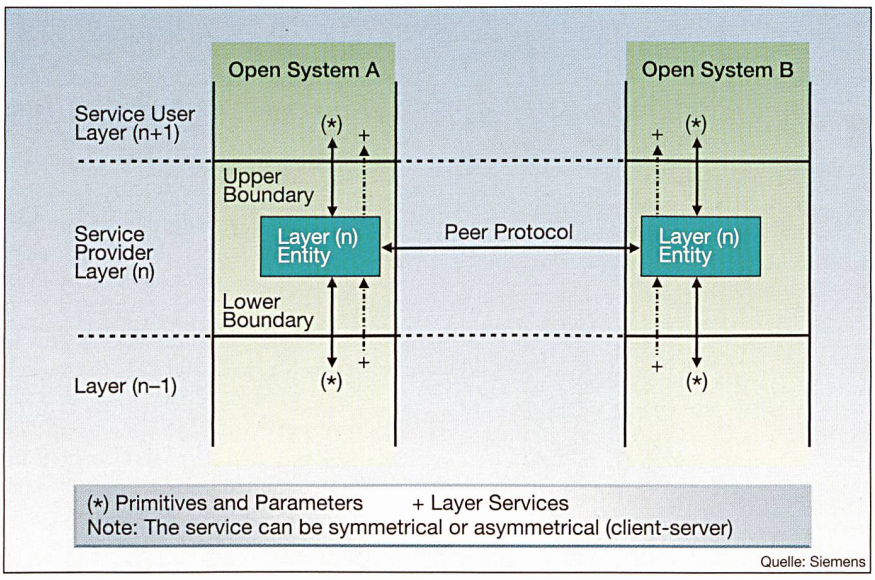

Bild 3 Protokollschicht

Die IP-Adresse

Anders als in einem leitungsvermittelten Telekommunikationsnetz, wo die Netzknoten zum Beispiel eine SS7-Adresse besitzen und die Telefone/Faxgeräte eine E.164-Adresse, umfasst im Internet die Adressierung auf der Netzwerkschicht auch die IP-basierten Endgeräte. Ein IP-basiertes Endgerät erhält mindestens eine IP-Adresse; die IP-Adresse für die Signalisierung (Control Plane) kann eine andere sein als die IP-Adresse für Sprache, Daten oder Video (User Plane). Die IP-Adresse ist der Schicht 3 (Network Layer) zuzuordnen, das heisst, sie erlaubt das zielgerichtete Weiterleiten der Protokoll-Nachrichten im Netz End-zu-End. Damit hat man im Internet solange kein Problem, als man

Abkürzungen

ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
DNS	Domain Name System
DoS	Denial of Service
DPC	Destination Point Code (SS7)
IETF	Internet Engineering Task Force
IP	Internet Protokoll (v4: Version 4, v6: Version 6)
ISO	International Standardization Organization
ITU-T	International Telecommunication Union, Telecommunication Standardization Sector
LAN	Local Area Network
NAT	Network Address Translation
MTP	Message Transfer Part (SS7)
OPC	Origination Point Code (SS7)
OSI	Open Systems Interconnection
PC	Personal Computer
SCTP	Stream Control Transmission Protocol
SIP	Session Initiation Protocol
STP	Signal Transfer Point (SS7)
SS7	Signalling System No.7 (ITU-T)
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VoIP	Voice over IP

nur mit öffentlichen IP-Adressen operiert. Da aber einerseits jede Einrichtung mit öffentlicher IP-Adresse den Gefahren des Internet (DoS-Attacken, Hacker-Angriffe, Viren) ausgesetzt ist und andererseits IP-Adressen unter Umständen nur beschränkt verfügbar sind (Adressraum und/oder Kosten), haben Unternehmen ihre IP-Netze mit privaten IP-Adressen aufgebaut, wie einleitend beschrieben. Sie erhalten nur über Firewalls/NAT Zugang zum Internet. Diese privaten IP-Adressen sind im Internet, d.h. den Routern, nicht bekannt.

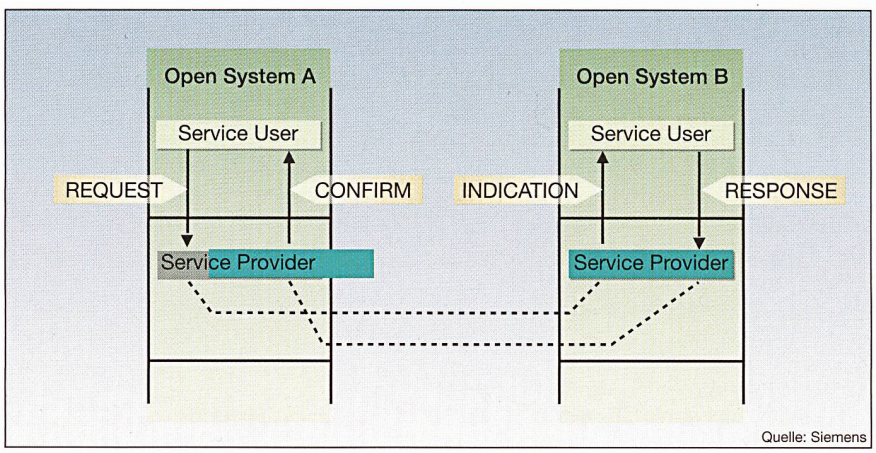

Bild 4 Interaction Primitives

Der konzeptionelle Fehler

Bei einem Zugriff eines Rechners (PC-Client) des privaten IP-Netzes auf eine Website wird in der Regel mittels Adressen-Auflösungsmechanismen, beispielsweise des Domain Name Systems (DNS), aus dem URL die öffentliche IP-Adresse des entsprechenden Servers ermittelt und als Ziel-IP-Adresse auf der Netzwerkschicht eingesetzt. Die eigene IP-Adresse wird sowohl auf der Anwendungsschicht als auch auf der Netzwerkschicht eingefügt (da ja IP dem End-zu-End-Paradigma folgt). Beim Einsatz einer NAT geht diese End-zu-End-Beziehung auf der Netzwerkschicht aber verloren, da die private IP-Adresse auf der Netwerkschicht im Internet nicht bekannt ist. Sie wird von der NAT auf der Netzwerkschicht gegen die öffentliche IP-Adresse des NAT-Servers ausgetauscht. Da IP einen verbindungslosen Dienst bietet, ist es Sache einer höheren Protokoll-Schicht (z. B. TCP), eine Verbindung zu erstellen, falls es die Anwendung erfordert. Beim Empfang der Nachricht darf nun die Anwendungsinstanz im Server mit der angesprochenen Website die PC-Client-Adresse nicht aus dem Datenfeld der Anwenderschicht entnehmen und ihrerseits für das Senden von Paketen benützen, da sie wie erwähnt nicht öffentlich bekannt ist und damit von den Routern nicht weitergeleitet werden kann, beziehungsweise vom NAT nicht akzeptiert wird. Analog verhält es sich mit den Signalisierprotokollen für VoIP, zum Beispiel H.323 oder SIP. Sie übertragen die IP-Adressen (z. B. Adresse des rufenden Endgerätes) in der Anwendungsschicht. Falls die Partner-Anwendungsinstanz diese IP-Adresse zusammen mit ihren Daten der Netzwerkschicht übergibt, haben die Router, beziehungsweise die NAT des rufenden Endgerätes, keine Chance, beim Empfang dieses Paketes die private IP-Adresse zu bearbeiten, da sie nicht der öffentlichen IP-Adresse der NAT entspricht.

Auf einem ähnlichen Missverständnis beruhen Anwendungen, die beim Empfang von IP-Paketen, die zu einer Antwort auf eine vorgängige Anfrage gehören, die IP-Source-Adresse im IP-Header überprüfen und, wenn nicht bekannt, die IP-Pakete verwerfen.

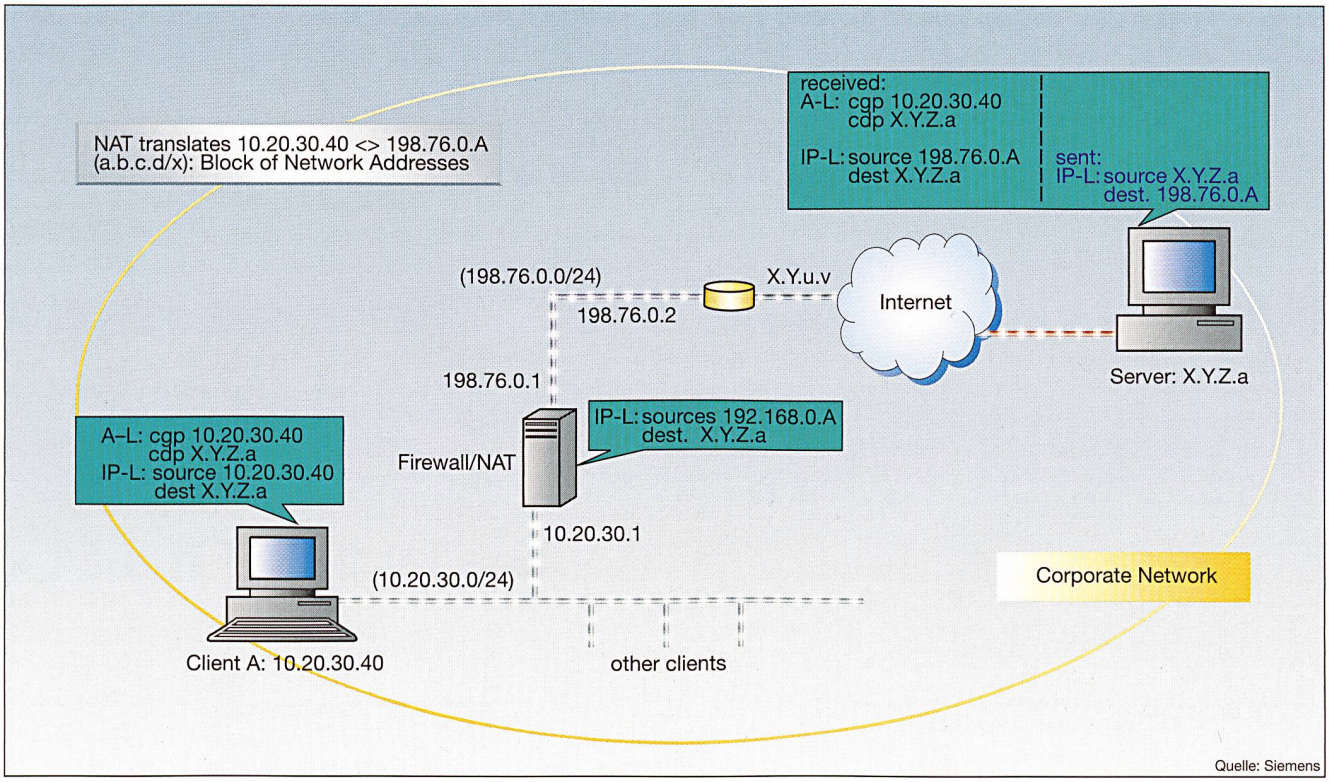

Bild 5 Adressmanipulation bei Zugriff auf einen Server im Internet

Der grundlegende Fehler liegt also darin, dass nicht beachtet wird, dass die Adressen auf der Anwendungsschicht und der Netzwerkschicht verschieden sein können. Beim Weg durch das Internet können IP-Adressen (Netzwerkadressen) beim Weiterleiten von Paketen verändert werden, ohne dass in den Daten der Anwendungsschicht eine entsprechende Anpassung der IP-Adresse erfolgt, beziehungsweise gar nicht erfolgen darf. Das richtige Vorgehen wäre also:

a) bei Empfang eines IP-Paketes die Übergabe der Ursprungsadresse, wie sie auf der Netzwerkschicht verwendet wird, durch die Netzwerkschicht an die Anwendungsschicht und
b) beim Senden einer Nachricht die Übergabe der gespeicherten Ursprungsadresse durch die Anwendungsschicht an die Netzwerkschicht zur Verwendung als Zieladresse.

Die auf der Anwendungsschicht verwendeten Adressen sind, im Fall von privaten Adressen, nicht für das Routing im Internet bestimmt. Bild 5 zeigt den Zugriff, insbesondere die Verwendung der Adressen auf den verschieden Protokollschichten, von einem Client in einem Unternehmensnetz auf einen Server im Internet.

Oder ein Beispiel aus dem VoIP-Bereich: Das SIP-Telefon 1 (10.10.10.117) in einem Unternehmen baut eine Verbindung auf zu einem weiteren SIP-Telefon 2 (sip: 1060@194.90. 133.116) im Internet. Die Anbindung des Unternehmensnetzes an das Internet erfolgt über eine Firewall/NAT mit der öffentlichen IP-Adresse 194.90.133.115. Der SIP-Proxy hat die Adresse 194.90.133.116.

Tabelle Primitive und Parameter

Eine Primitive (Generic Name) kann in der Form genau eines Typs (Specific Name) oder in der Form mehrerer Typen existieren. A, B,... sind Parameter, z. B. Adressen, Sequenznummer oder Priorität.

Primitives		Parameter
Generic Name	**Specific Name**	
N-XYZ	Request, Indication	A, B, C, User Data
N-RST	Indication	E
N-OPQ	Request, Indication, Response, Confirmation	A, F, G, H, I

Die erste Meldung im Verbindungsaufbau ist INVITE: SIP-Telefon 1 → Firewall/NAT → SIP-Proxy → SIP-Telefon 2. NAT ersetzt auf dem IP-Layer die Source-Adresse des SIP-Telefons 1 (10.10.10.117) durch die eigene öffentliche Adresse (194.90.133.115). Die Adressen auf den verschieden Protokollschichten beim Empfang der Meldung INVITE im SIP-Proxy sind:

- IP-Layer: Source: 194.90.133.115/ Destination: 194.90.133.116
- SIP-Layer: Via: 10.10.10.117/To: 1060 @194.90.133.116

Während der IP-Layer also die öffentlichen IP-Adressen nutzt, arbeitet die Anwendungsschicht mit der SIP-Adresse, respektive mit der privaten IP-Adresse des ersten Telefons. Falls nun die Anwendung auf dem SIP-Proxy feststellt, dass die Verbindung nicht aufgebaut werden kann, muss eine entsprechende Fehlermeldung an die Firewall/NAT gesendet werden. Die entsprechende Adresse ist nicht die aus dem SIP-Layer (10.10. 10.117), sondern die aus dem IP-Layer (194.90.133.115). Da IP verbindungslos operiert, muss die IP-Adresse 194.90. 133.115 zusammen mit der INVITE über die Schichten des Protokoll-Stacks an die Anwenderschicht übergeben und hier gespeichert werden. Für die Fehlermeldung zum NAT muss diese dann wiederum zusammen mit den Daten (Failure Response Codes) an die Netzwerkschicht (IP-Layer) übergeben werden.

Schichten nicht verletzen!

Findige Köpfe haben mittlerweile Umgehungsmöglichkeiten entwickelt, womit sie die Adressen der Anwenderdaten in der Netzwerkschicht, dem Layer 3, manipulieren. Dies widerspricht natürlich dem Konzept des Schichtenmodells, denn eine Schicht (n) manipuliert Daten einer höheren Schicht und verletzt damit das Prinzip des unversehrten Transports der ihr anvertrauten Daten.

Mit IPv6 wirds einfacher

Für die Probleme bei Netzwerkszenarien mit NAT ist also der Verstoss gegen das Adressierungskonzept bei geschichteten Protokoll-Architekturen entscheidend. IP-Adressen sind für die Adressierung der Netzelemente bestimmt. Die Anwendungen in den Netzelementen (PC, Server, Call-Server/Softswitch, IP-Telefone,...) werden durch die TCP-, UDP- oder SCTP-Port-Nummern adressiert.

Dass Adressen spezifisch nach der Protokollschicht sind, gilt auch für IPv6, der neuen Version 6 des Internet-Protokolls. Die schier grenzenlos verfügbaren IP-Adressen in IPv6 machen zwar den Einsatz von NAT zwecks Einsparung von IP-Adressen obsolet, es sind aber nach wie vor Adressen der Netzwerkschicht und dürfen nicht zur Adressierung von Anwendungsinstanzen verwendet werden. Auch wenn man nun argumentieren kann, dass auf Grund der riesigen Anzahl die Vergabe von IPv6-Adressen pro Anwendung bzw. sogar pro Anwendungsinstanz möglich ist. Es gilt also auch hier: Gemäss der Protokoll-Architektur muss die Adresse auf der Netzwerkschicht unabhängig von der Adresse auf der Anwendungsschicht gehandhabt werden. Auch für die Sicherheit muss in IPv6 kein NAT betrieben werden, da das neue Protokoll auch umfassendere Sicherheitslösungen bietet als IPv4.

Weiterführende Literatur

ISO/IEC 7498-1 bzw. ITU-T Rec.X.200 Open Systems Interconnection – Basic Reference Model: The Basic Model

ISO/IEC 10731 bzw. ITU-T Rec. X.210 Open Systems Interconnection – Basic Reference Model: Conventions for the Definition of OSI Services

ITU-T Rec.Q.700, Introduction to CCITT Signalling System No. 7

ITU-T Rec.I.361 B-ISDN ATM layer specification

ITU-T Rec.H.323 Packet based multimedia communications systems

IETF RFC 791 IPv4

IETF RFC 1918 Address Allocation for Private Internets

IETF RFC 3022 Traditional IP Network Address Translator

IETF RFC 1631 Network Address Translator

Angaben zum Autor

Peter Goldstein, Dipl. El.-Ing. ETH, arbeitet in der HW/SW-Entwicklung der Siemens Schweiz AG auf dem Gebiet der Telekommunikation. Er war Consultant für Intelsat und arbeitet in der Standardisierung der ITU-T (SS7, Signal Processing, Rapporteur Q.10/11, Protocols and Network functions for Signal Processing Equipment).

Siemens Schweiz AG, 8047 Zürich, peter.goldstein@siemens.com

[1] 10.0.0.0/8, 172.16.0.0/12 und 192.168.0.0/16, siehe auch RFC 1918

[2] Heute: Internet Corporation for Assigned Names and Numbers (ICANN)

[3] Bei IP over ATM, ATM steht für Asynchronous Transfer Mode

[4] OSI: Open Systems Interconnection, definiert von der International Standardization Organization (ISO)

[5] Der ATM-Stack wurde definiert von der International Telecommunication Union, Telecommunication Standardization Sector (ITU-T)

[6] Sofern sie denn keine Bewertung/Manipulation von/an Informationen der höheren Schichten vornehmen

[7] Bei SS7 (MTP): OPC und DPC, bei IP: Ursprungs- und Zieladresse, die IP-Adressen

Quand Voice-over-IP ne fonctionne pas

Défauts de conception dans les applications IP – et NAT n'est pas le problème

Internet se base sur un empilage de protocoles à plusieurs niveaux – un peu comme les 7 couches OSI. L'application opère en général avec l'URL, par exemple http://www.electrosuisse.ch ou sip:absender@sender.net. La couche réseau en revanche travaille avec une adresse IP comme 82.195.225.102. Quelques applications, comme Voice-over-IP, utilisent cependant l'adresse IP également au niveau application et transmettent cette information d'adresse au niveau réseau pour le routing. Conséquence: l'application ne fonctionne pas lorsqu'un serveur NAT change les adresses au niveau réseau.

Für die Mitglieder da.

Der Schweizer Automatik Pool (SAP) positioniert sich neu als Swiss Technolgie Network ***(swissT.net)***.

Das Netzwerk des Schweizer Technologiesektors ***swissT.net*** *wird von den Mitgliedern getragen und ist für die Mitglieder da.* ***swissT.net*** *bündelt die Interessen und Kräfte eines lebendigen Schweizer Industriezweiges und bildet als Interessenverbund die Schnittstelle nach aussen.*

Der 1976 gegründete Wirtschaftsverband umfasst rund 350 Mitgliedfirmen und 100 Sympathiemitglieder in 27 marktorientierten Sektionen. ***Weitere sind herzlich willkommen.***

swissT.net
swiss technology network

Wirkt im Kleinen, bewegt im Grossen.

swissT.net · Postfach · CH-8022 Zürich · www.swisst.net
Tel. +41 44 307 70 07 · Fax +41 44 307 70 10