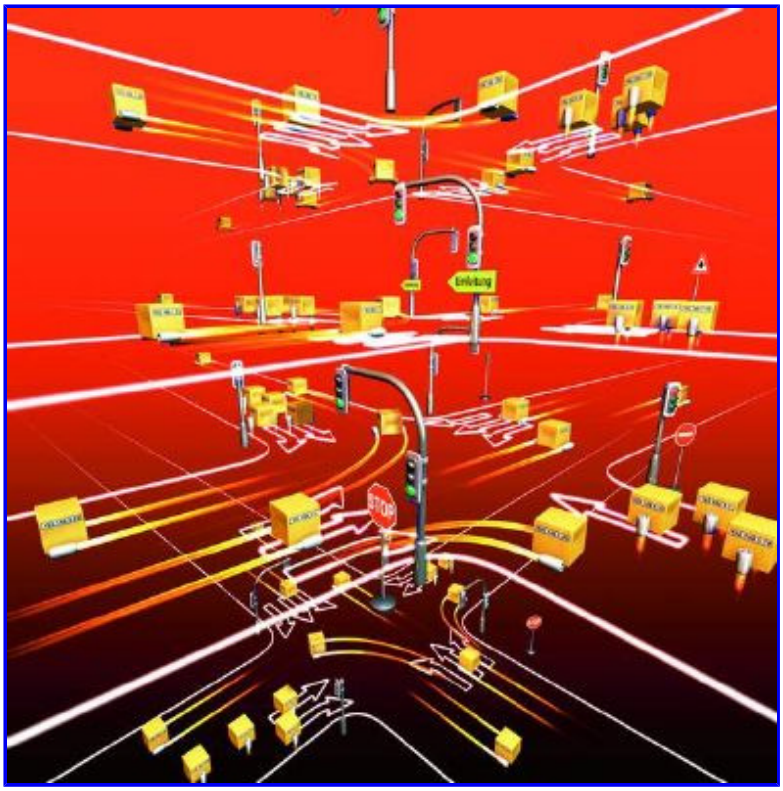


Stefan Dierichs, Prof. Norbert Pohlmann

Geordnetes Chaos

Wie Routing dem Internet seine Selbstheilungskräfte verleiht

Nach jedem Ausfall eines zentralen Verkehrsknotenpunkts im Internet flammt die Debatte um eine mögliche Verwundbarkeit des weltumspannenden Netzverbunds neu auf. Doch bisher beweist das Netz der Netze stets, dass es Pannen locker abfedern kann. Routing-Mechanismen zwischen den Teilnetzen sorgen blitzschnell für Umleitungen ohne Datenstau - und das ganz ohne menschlichen Eingriff.

Unterthema: Looking Glass: Routing-Informationen im Web
Unterthema: Surftipps

Das Internet dient mehr und mehr als Transportmedium für kritische Dienste. Bankverbünde transferieren Geld über VPN-Tunnels, Großunternehmen steigen zunehmend vom Festnetz auf Internet-Telefonie um. Und auch bei staatlichen Institutionen steigt die Abhängigkeit vom weltumspannenden IP-Netzwerk. Im gleichen Maße wächst die Angst, das Internet könnte vielleicht doch nicht so stabil sein, wie es die Mär vom atomkriegfesten Rechnerverbund suggeriert.

Immer wieder, zuletzt beim Weltgipfel der Informationsgesellschaft in Tunis, monieren Kritiker, dass ökonomische Zwänge das Netz der Netze grobmaschiger und damit anfälliger für Pannen und Angriffe werden lassen. Die Betreiber von weltumspannenden Backbones lassen sich in der Tat an zwei Händen abzählen. Ein erklecklicher Teil des IP-Traffics durchläuft große Knoten. Was, wenn einer oder mehrere dieser zentralen Punkte in der dezentralen Struktur ausfallen?

Die Antwort auf diese Frage gibt das Internet in kurzen Abständen selbst: Als beispielsweise im Oktober 2005 der größte deutsche Internet-Austauschpunkt DE-CIX in Frankfurt teilweise ausfiel, nahm kaum jemand Notiz davon. Fast alle Netzbetreiber halten für den Ernstfall Redundanz-Bandbreiten vor und schaffen es, ihren Traffic binnen weniger Minuten automatisiert umzuleiten. Dabei kommen ihnen die Routing-Protokolle zur Hilfe. Sie sind so gestaltet, dass Verbindungsunterbrechungen automatisch erkannt und umgangen werden können.

Autonom und vermascht

Ein genauerer Blick auf die logische Infrastruktur des Internet zeigt, dass der weltweite IP-Netzwerkverbund derzeit klaffende Wunden selbst schließen kann. Das Internet besteht aus einer stetig wachsenden Anzahl voneinander unabhängiger Netze, den autonomen Systemen (AS). Zurzeit sind rund 40 000 AS-Netzwerke registriert, etwa 21 000 sind aktiv. Gemeinsamer Nenner ist die dort verwendete Sprache, nämlich das TCP/IP-Protokoll. Ein AS wiederum kann aus vielen Teilnetzen zusammengesetzt sein, die über Router miteinander verbunden sind, aber einer einzigen administrativen Instanz unterstehen.

Die autonomen Systeme unterscheiden sich in Größe und räumlicher Ausdehnung immens voneinander. Das bedeutet auch, dass jeder Betreiber seine eigene Strategie hat, mit der er mit Hilfe von Routing-Protokollen die Kommunikation der IP-Pakete in seinem Netz organisiert. Er muss die Wegstrecken ständig neu austarieren. Sicher sollen sie sein, dabei möglichst preisgünstig und außerdem kurz. Die physischen Leitungen sind in der Regel so ausgelegt, dass das reale Datenvolumen 50 Prozent des theoretischen möglichen nicht übersteigt, um Datenstaus zu vermeiden [1].

Betrieben werden die AS-Netze von Internet Service Providern (ISPs), Webhostern, großen Unternehmen und von öffentlichen Internet-Austauschpunkten. Für die Koordination der autonomen Systeme zeichnet die zentrale Internet Assigned Numbers Authority (IANA) verantwortlich. Diese wiederum delegiert die konkrete Administration an die jeweiligen Regional Internet Registries (RIR). Möchte etwa ein deutscher Provider ein AS anmelden, wendet er sich an die europäische Registry, also an das Reseaux IP Européens (RIPE) [2].

Mautstrecken

Ziel der AS-Betreiber ist, ihre eigenen Systeme möglichst redundant mit dem Internet zu verknüpfen. Dabei verfolgt jeder Provider unterschiedliche Strategien, abhängig vom Kerngeschäft des Unternehmens und der Größe und Ausdehnung des autonomen Systems. Kleinere Systeme werden meist über einen IP-Transitvertrag mit Backbones größerer Carrier verbunden. In diesem Fall spricht die Branche von "Uplinks". Der Kleinere zahlt für das hochgeleitete Datenaufkommen.

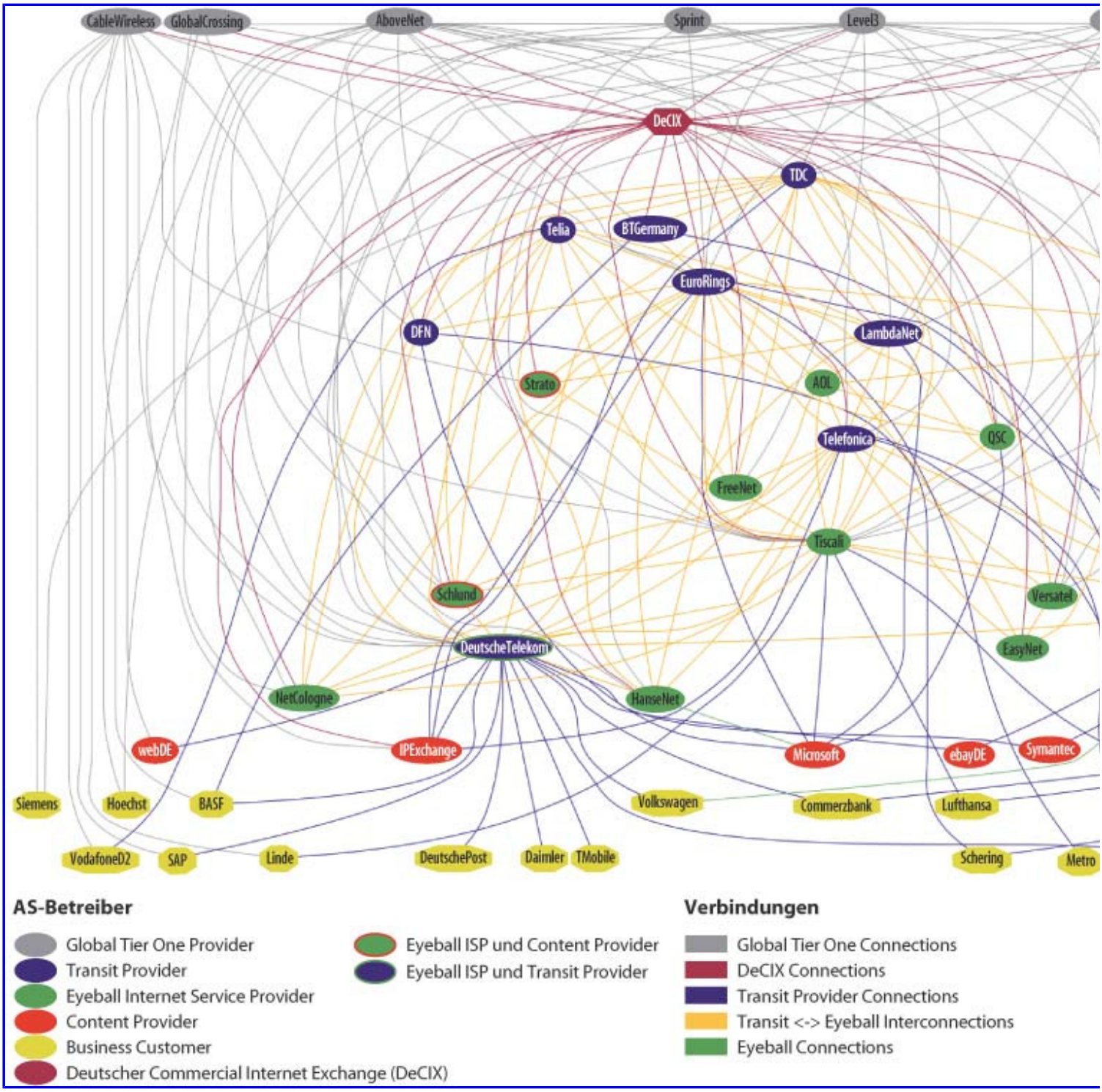
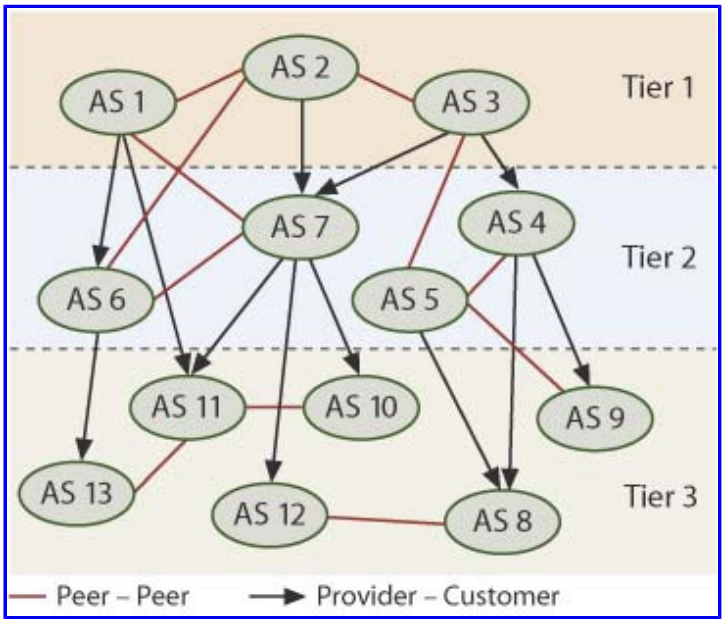


Bild: Institut für Internet-Sicherheit, Fachhochschule Gelsenkirchen

Die autonomen Systeme in Deutschland sind eng miteinander vermascht. Einige große Carrier wie Sprint oder die Telekom verzichten auf ein öffentliches Peering am DE-CIX.

Anders ist dies bei einer privaten Peering-Vereinbarung. Hier treffen zwei Provider ein Abkommen, ohne Berechnung Daten zwischen ihren Netzen auszutauschen. Beim Peering geben die beiden AS-Netze nur ihren Traffic aneinander weiter. Damit ein AS sämtlichen Verkehr eines anderen AS weiterleitet, muss zusätzlich ein Transit-Abkommen bestehen. Ein autonomes System erlaubt im Regelfall beispielsweise keinen Durchgangsverkehr von einem Peering-Partner zu dessen eventuell vorhandenen Transit-Providern. Diese Vereinbarungen werden vorab in Routing-Richtlinien (Policies) gegossen.

Das Zustandekommen eines Peering-Vertrags ist abhängig von vielen Faktoren. Eine wesentliche Rolle spielt die Größe der potenziellen Partner. Eher informell hat sich eine Einteilung der Provider in drei Schichten etabliert: Autonome Systeme, die keine Kunden mehr "unter" sich haben, also keinen Transit verkaufen, sondern ausschließlich Endkunden versorgen, werden als Edge-Networks bezeichnet und bilden die unterste Schicht (Tier 3).



Je nach Größe ihres autonomen Systems teilen sich IP-Provider selbst in "Tiers", also Klassen ein. Danach richtet sich, ob sie kostenneutral Traffic tauschen oder Transit untereinander verkaufen.

Große autonome Systeme, die keinen Transit mehr hinzukaufen, sondern nur mit anderen großen autonomen Systemen Peering-Verbindungen betreiben, bilden die Oberschicht (Tier 1). Von diesen Carrier-Riesen gibt es höchstens ein Dutzend weltweit. Dazu zählen MCI, Level3, AT&T und Sprint, aber auch Mischkonzerne wie AOL. Alle anderen AS bilden die mittlere Stufe (Tier 2).

Große Tiere

Sowohl bei der Entscheidung über AS-Verknüpfungen als auch beim Routing der Pakete selbst stehen ökonomische Belange im Vordergrund. Es ist durchaus möglich, dass große Provider (Tier 1) mit kleineren Providern (Tier 2) peeren, wenn sie sich einen Vorteil durch dieses Abkommen erhoffen. So kann es etwa vorkommen, dass der kleinere Partner über eine große Anzahl von Endkundenanschlüssen verfügt, die der große unbedingt erreichen will.

Zur Absicherung existieren in den Peering-Verträgen meist Vereinbarungen über maximale Datenvolumen, die in die jeweilige Richtung geschickt werden. Übersteigt ein Provider diese Grenzen, werden Kosten fällig, wie etwa jüngst der Streit zwischen den IP-Carriern Cogent und Level3 deutlich machte [3].

Peeren können zwei AS-Netze auch an diversen öffentlichen Peering-Punkten (Internet Exchange Points, IXP), in Deutschland beispielsweise am bei weitem größten, dem DE-CIX, und regionalen wie dem Münchner INXS und dem Berliner B-CIX. Diese Knoten bestehen aus riesig dimensionierten Switches, mit denen sich IP-Provider über einen Router verbinden können. Das DE-CIX beispielsweise verfügt über drei redundant ausgelegte Cisco Catalyst 6509-NEB-A-Switches mit 10-GBit-Glasfaser-Ports. Jedes angeschlossene AS kann ohne Traffic-Berechnung Daten mit jedem anderen vorhandenen AS austauschen. Die Peering-Kunden zahlen stattdessen einen monatlichen Festbetrag für den Switch-Port.

Früher waren es die gegenüber Transit-Verträgen geringeren Kosten, die die Provider veranlasst haben, Peering-Vereinbarungen an öffentlichen Internetaustauschpunkten einzugehen. Dieses Argument ist angesichts ins Bodenlose fallender Transitpreise heute kaum noch relevant. Arnold Nipper, der technische Leiter des DE-CIX erläutert, dass die Provider unterschiedliche Motivationen haben, teilzunehmen. Zum einen spielen demnach die kürzeren Wege und die dadurch geringere Verzögerung eine Rolle, zum anderen die vom CIX-Betreiber gut gewartete Anbindung des AS am Switch.

Umgekehrt gibt es auch Provider, die bewusst die Anbindung an öffentliche Austauschpunkte meiden. Damit wollen sie zeigen, dass sie selbst eine Größe erlangt haben. Sie kalkulieren anders und peeren nicht öffentlich am DE-CIX. Das prominenteste Beispiel ist hierzulande wohl die Deutsche Telekom. Aber auch global agierende Tier-1-Carrier wie Sprint machen um das DE-CIX einen großen Bogen. Sie setzen darauf, dass viele Provider ohnehin nicht darum herum kommen, Verbindungen zu ihnen zu unterhalten. Und dann möchten sie dafür gerne Geld sehen.

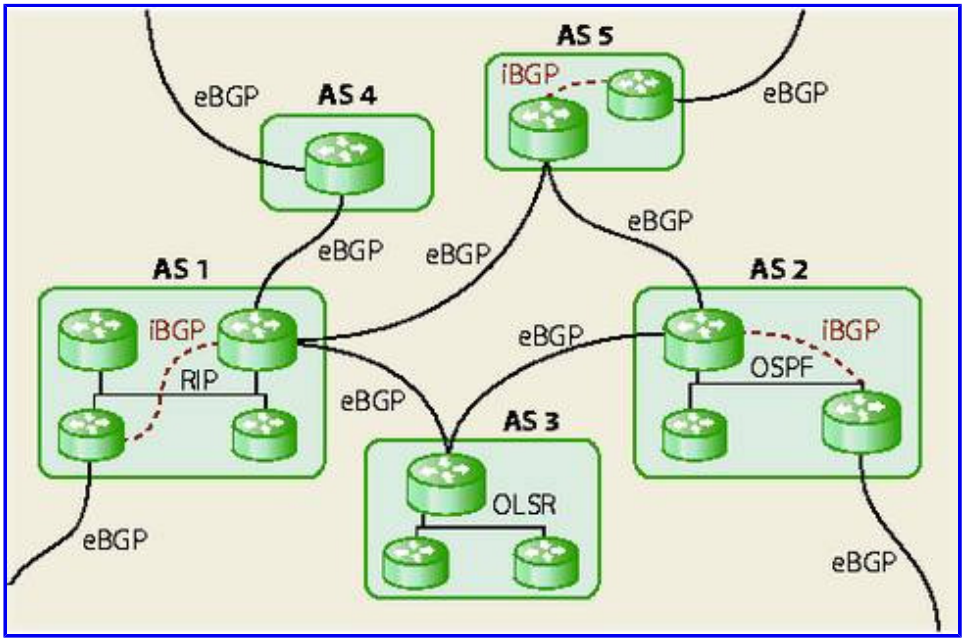
Navigationssysteme

Die große Kunst für Netzplaner bei den großen Carriern ist es, in ihrem AS optimale Wegstrecken für den IP-Datenverkehr in alle Richtungen festzulegen. Das beste Netz nutzt wenig, wenn niemand weiß, wie die einzelnen Rechner am effizientesten zu erreichen sind. Routing dient in einem Netz dazu, die logischen Wege zu definieren, auf denen die Datenpakete übertragen werden können.

Mit Routing-Protokollen tauschen sich Provider über Wegstrecken-Informationen aus. Innerhalb eines autonomen Systems sorgt die Gruppe der Interior Gateway Protocols (IGPs) für die Routing-Infos, zwischen autonomen Systemen übertragen Router die Infos mit den Exterior Gateway Protocols (EGPs). Bekannteste Protokolle der IGP-Familie sind das Open Shortest Path First (OSPF) und das Routing Information Protocol (RIP).

Das Routing selbst erfolgt anhand unterschiedlicher Entscheidungskriterien, die sich mit den Protokollen definieren lassen. Genau dabei unterscheiden sich die beiden genannten Protokollfamilien. Bei den IGPs ist das Ziel klar: Finde den günstigsten Weg durch das Netz! Je nach Situation muss der günstigste Pfad allerdings nicht immer der kürzeste oder schnellste sein. Die Verwaltung von EGP-Regeln gestaltet sich für Netzplaner komplexer, da die IP-Pakete die Unternehmensgrenzen verlassen und damit wirtschaftliche und firmenpolitische Aspekte bei der Wegewahl eine größere Rolle spielen.

Das Border Gateway Protocol (BGP) trägt, als De-facto-Standard unter den Routing-Protokollen zwischen autonomen Systemen, wesentlich zum Funktionieren des Gebildes Internet bei. Es gehört zu den Path-Vektor-Protokollen, verwaltet also in seiner Routing-Tabelle den kompletten Pfad bis zum entsprechenden Zielnetz. Dabei listet es alle autonomen Systeme auf, die auf dem Weg zum Ziel durchquert werden.



Innerhalb von autonomen Systemen kommt die iBGP-Protokollfamilie zum Einsatz. Untereinander sprechen die AS mit eBGP.

An jeder Schnittstelle ihres AS-Netzes zu anderen betreiben die Provider einen so genannten Border-Router. Dort findet die Übergabe von IP-Paketen von einem AS zum fremden Border-Router statt. Die beiden tauschen untereinander permanent Routing-Informationen aus. Jeder Border-Router spricht auch ein AS-internes BGP (iBGP) zu allen anderen BGP-Routern im eigenen AS. Das BGP-Prokoll für die Kommunikation zwischen AS-Netzen wird daher zur Unterscheidung externes BGP (eBGP) genannt. Border-Router schicken eBGP-Informationen im Regelfall nur an ihren direkten Nachbarn.

Grenzposten

Wenn nun zwei autonome Systeme einander ihre Routen mitteilen möchten, bauen die Border-Router an den Grenzen der Netze eine BGP-Session auf. Zu Beginn dieser Session übermitteln die beiden Nachbarn einander ihre kompletten Routing-Informationen. Anschließend werden nur noch Änderungen ausgetauscht.

In bestimmten Zeitabständen senden sich die Border-Router außerdem via BGP Nachrichten zum Aufrechterhalten der Session. Bei Cisco-Routern etwa geschieht das standardmäßig im 60-Sekunden-Intervall. Dieser Mechanismus ist immens wichtig für die Stabilität des gesamten Internet. Erhält ein Border-Router nämlich nach einer bestimmten Zeit

keine neue BGP-Nachricht von seinem Nachbar-Router, beendet er die Session und streicht dessen Routen aus seiner Tabelle. Auf diese Weise überwachen BGP-Nachbarn selbst die Verfügbarkeit ihrer Gegenstellen.

Aus den Routen-Informationen von anderen Routern baut sich jeder BGP-Router selbst eine Datenbank für die Routen zu allen Internet-Netzen auf. Derzeit umfasst eine solche Tabelle mit kompletten Routen-Informationen rund 185 000 Pfade. Am Ende einer Route befindet sich immer das Zielnetz. Sie dient zur Adressierung des Kommunikationspartners auf IP-Ebene und ist immer einem autonomen System zugeordnet.

Router-Politik

Beim Routing selbst gelten in jedem AS eigene Regeln, die so genannten Routing-Policies. Entscheidungskriterien für die Wegewahl sind beispielsweise die Länge eines AS-Pfads oder unterschiedliche Nutzungspreise der Verbindungen. So kommt es oft vor, dass ein Paket einen längeren Weg durchs Internet zurücklegt als eigentlich nötig, weil der absendende Provider wegen der höheren Kosten eine teure Transit-Abkürzung meidet und stattdessen den Weg über ein Peering wählt.

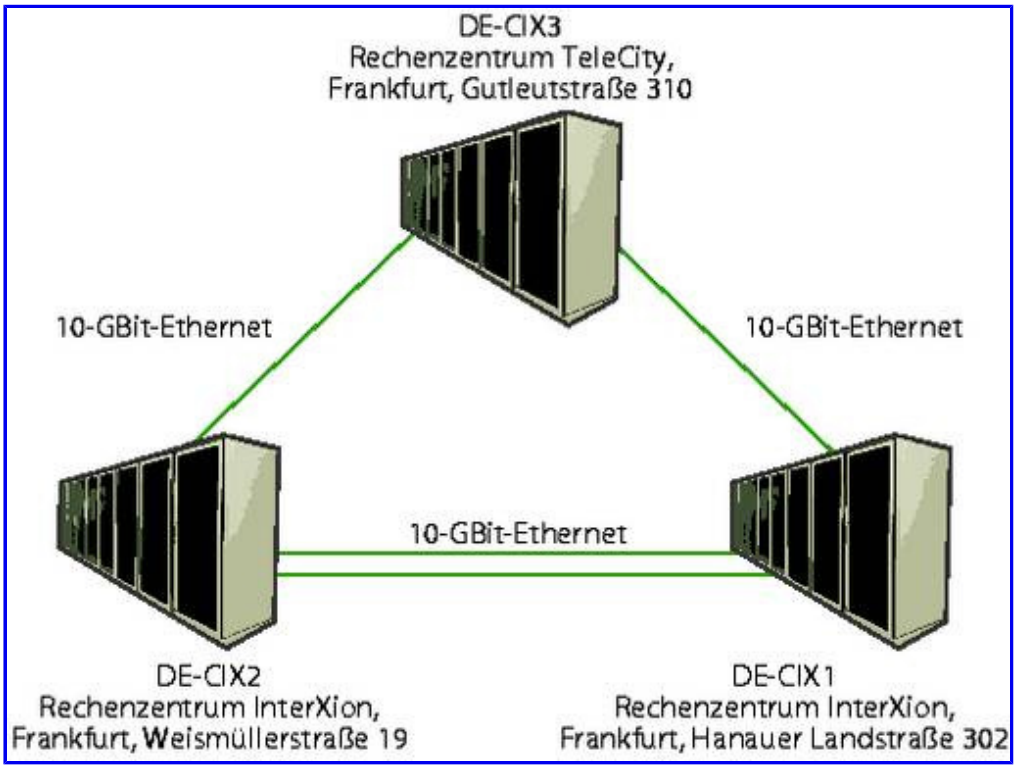
Die aus den Routing-Strategien resultierenden Regeln bestimmen den Weg von IP-Paketen über mehrere Netze hinweg. Bei der gängigen Hot-Potato-Strategie ist der Provider darauf aus, den Durchgangsverkehr rasch wieder los zu werden, um die eigenen Ressourcen zu schonen. Er routet den Verkehr möglichst schnell zu anderen autonomen Systemen weiter, fasst ihn also wie eine heiße Kartoffel an.

Das Cold-Potato-Routing verfolgt den umgekehrten Ansatz. Hier möchte der Provider möglichst lange die Kontrolle über den Traffic behalten, um Quality-of-Service-Anforderungen gerecht werden zu können. Jeder Provider tariert seine Strategie zwischen Hot- und Cold-Potato-Prinzip individuell aus. Er bewegt sich dabei im Spannungsfeld zwischen Dienstgüte und Kosten.

Dieser Konflikt wird größer, je mehr die breite Masse Echtzeit-Anwendungen wie IP-Telefonie oder Video-Streaming nutzt. Allgemein gefasste Qualitätszusicherungen reichen da oft nicht mehr aus. Die Übermittlung nach dem Best-Effort-Prinzip, das heißt der Gleichbehandlung aller IP-Pakete, wird daher an Bedeutung verlieren. In Zukunft spielen neben der puren ausgetauschten Datenmenge auch Qualitätszusicherungen, etwa bezüglich Paketverlustrate, Verzögerung und Schwankungen (Jitter) eine größere Rolle.

Pannensicher

Der Blick hinter die Routing-Kulissen zeigt, dass das Internet gegen Ausfälle von Geräten oder ganzen autonomen Systemen gut gewappnet ist. Als Beispiel kann hier noch einmal der Eingangs erwähnte Teilausfall des deutschen Peering-Punkts DE-CIX dienen: Als am 17. Oktober letzten Jahres einer von drei DE-CIX-Switches plötzlich den Dienst verweigerte, konnten viele der angeschlossenen autonomen Systeme ad hoc ohne manuellen Eingriff auf dieses Ereignisse reagieren. Die Auswirkungen der Panne waren kaum spürbar.



Die drei DE-CIX-Switches sind an unterschiedlichen Orten im Frankfurter Stadtgebiet untergebracht. Fällt eine der Verbindungen aus, wird die Kommunikation untereinander noch nicht gestört.

Die Peering-Switches des DE-CIX befinden sich, verteilt auf zwei Rechenzentrumsbetreiber, in drei unterschiedlichen Gebäuden im Frankfurter Stadtgebiet. Sie sind über Glasfaserleitungen miteinander verknüpft (siehe Grafik auf S. 165). Ein solcher Drei-Knoten-Cluster sorgt auch dann für die Erreichbarkeit jedes Geräts, wenn eine der Glasfaserverbindungen unterbrochen ist. Etwa 30 der 163 momentan am DE-CIX angeschlossenen Provider haben Ports an zwei unterschiedlichen Switches belegt. Die anderen mieten zwar zum Teil auch mehrere Ports an, diese aber alle gebündelt an einer der drei Cisco-Maschinen.

Neben der physischen Verbindung der autonomen Systeme bietet DE-CIX den Providern auch die Möglichkeit, die neu gewonnenen Routen bekanntzumachen. Dazu betreibt der DE-CIX-Eigner eco einen Routeserver. ISPs nutzen diesen, um Routen beim DE-CIX zu annoncieren und vom DE-CIX zu empfangen. Der Routeserver fungiert als eine Art Vermittlungsstelle, indem er die Routen eines Peer annimmt und an die anderen weitergibt.

Zum Zeitpunkt des Ausfalls waren an dem betroffenen Switch etwa 40 Provider ohne Redundanz-Port angeschlossen. Die Panne bewirkte zuerst einen Abbruch der BGP-Sessions zwischen den Border-Routern der Provider. Die Router konnten keine Nachrichten zum Aufrechterhalten der Verbindung mehr senden. Sie kappten, nachdem ihr Timer abgelaufen war, die Verbindungen und strichen die DE-CIX-Routen aus ihren Tabellen. Sodann suchten die Router in den betroffenen autonomen Systemen automatisch nach Alternativ-Routen. In dieser Situation machten sich vorherige Überlegungen der Netzplaner in Richtung möglichem DE-CIX-Ausfall und diesbezüglicher Redundanzen bezahlt. Viele Provider leiteten ihren Traffic binnen weniger Sekunden über ihre Anschlüsse am Amsterdamer AMS-IX oder am Londoner LINX um. Aber auch innerhalb Deutschlands standen regionale Internet-Austauschpunkte zur Verfügung. Der öffentliche Peering-Knoten INXS in München etwa verzeichnete sofort einen Durchsatzanstieg von etwa 2,8 auf rund 3,8 GBit/s.

Der Hoster und Provider Schlund beispielsweise verfügt über Ports an zwei der drei DE-CIX-Switches. Stefan Mink, Leiter des WAN-Management bei Schlund, berichtete, dass es vom Zeitpunkt des Ausfalls weniger als 90 Sekunden dauerte, bis die so genannte Rekonvergenz einsetzte, die Schlund-internen Nachbar-Router des vom Ausfall betroffenen Routers Alternativpfade vorschlugen. "Aus denen wurde dann der jeweils beste für jedes Ziel nach dem 'BGP Decision Process' ausgewählt. Das dauert in unserem Netz meist keine Minute mehr, eher deutlich drunter." Das Schlund-AS leitete seinen IP-Traffic sodann automatisch über den niederländischen AMSIX, den britischen LINX und den Münchener INXS. Als sich die vom Ausfall abgetrennten Gegenstellen zurückmeldeten, beendete das AS sein Alternativ-Routing automatisch.

Einige Provider, die neben dem öffentlichen DE-CIX-Peering hauptsächlich über Upstream-Transits verfügen, konnten den Ausfall nicht komplett über andere öffentliche Peerings ausgleichen. So kann eine länger andauernde

Panne viel Geld kosten, nämlich dann, wenn sie beispielsweise auf Ausweich-Transitstrecken vereinbarte Datenvolumina kurzfristig überschreiten.

Ausblick

Jede Panne am DE-CIX oder bei anderen zentralen Knotenpunkten des Internet ist ein Proof-of-Concept für die Stabilität des Internet. Bisher erweist sich die physische und logische Infrastruktur als überaus robust. Das Institut für Internet-Sicherheit (ifis) an der Fachhochschule Gelsenkirchen [4] hat anhand von Informationen über autonome Systeme die Vermaschung des deutschen Internet-Teils näher analysiert. Eine Netzkarte, die die wichtigsten Datenautobahnen in Deutschland darstellt, zeigt Verknüpfungen großer Systeme untereinander (siehe Abbildung auf S. 162).

Das Institut erfragte Kennzahlen bei deutschen DSL-Providern, die auch Privathaushalte versorgen. Demnach verbraucht jeder DSL-Nutzer durchschnittlich zehn GByte IP-Traffic (30 KBit/s) pro Monat. So kommt allein durch die rund zehn Millionen privaten DSL-Kunden in Deutschland ein monatliches Datenvolumen von etwa 100 000 TByte (im Durchschnitt 300 GBit/s) zu Stande.

Unternehmen verbrauchen Schätzungen des Instituts zufolge dann monatlich ein Datenvolumen von rund 75 000 TByte (im Durchschnitt 225 GBit/s). In der Summe laufen also 175 000 TByte IP-Daten auf, die die Provider ihren Kunden in Deutschland zuführen. Ausgehend von der Annahme, dass 20 Prozent davon im jeweils eigenen Netz bleibt, müssen 140 000 TByte Traffic über Transit und Peerings zwischen den AS-Netzen in Deutschland ausgetauscht werden. Allein das DE-CIX schaufelt zurzeit monatlich 22 000 TByte (im Durchschnitt 36 GBit/s) durch die Switches, das wären dann rund 15,7 Prozent des Gesamtvolumens in Deutschland.

Der physische Austausch von Daten zwischen autonomen Systemen, sei es mittels Peering oder Transit, findet zumeist in den hiesigen Rechenzentren statt und ist somit auf eine relative geringe Zahl von Standorten begrenzt - eine potenzielle Schwachstelle des Internet. Bislang vermaschen fast alle Provider im eigenen Interesse ihre AS-Netze eng und haben damit größere Auswirkungen von Ausfällen vermieden.

Ein harter Verdrängungswettbewerb sorgt aber derzeit für einen Konzentrationsprozess unter den IP-Carriern. Immer weniger Tier-1- und Tier-2-Systeme versorgen den Markt mit immer mehr Transit-Bandbreite. Der Ausfall eines großen AS könnte also bald wesentlich mehr Schaden anrichten, als es bisher zu beobachten war. Kritische Stimmen, auch aus dem Internet-Mutterland USA, bezweifeln vermehrt, ob die reine Marktwirtschaft nicht auf Dauer zur Destabilisierung des Netzverbunds führen könnte.

Sie fordern staatliche Eingriffe in die Vernetzungsstrategien der IP-Carrier, sogar staatlich verordnete Zwangs-Peerings werden diskutiert. Noch existiert nicht einmal eine Instanz, die die Themen Ausfallsicherheit und Redundanz-Anbindungen regelmäßig überwacht und bei kritischen Veränderungen auf Probleme aufmerksam machen kann. Reibereien um konsequentere staatliche Regulierung der kritischen Internet-Infrastruktur auf dem UNO-Gipfel zur Informationsgesellschaft könnten schon bald in scharf geführte Debatten münden. (hob)

Prof. Dr. Norbert Pohlmann ist Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie Leiter des Instituts für Internet-Sicherheit an der FH Gelsenkirchen.

Stefan Dierichs ist Mitarbeiter im Bereich Internet-Forschung des Instituts für Internet-Sicherheit an der FH Gelsenkirchen sowie bei T-Systems International GmbH angestellt.

Literatur

[1] Holger Bleich, Die Bosse der Fasern, Die Infrastruktur des Internet, c't 7/05, S. 88

[2] Reseaux IP Européens (RIPE): http://ripe.net

[3] Monika Ermert, Knirschen im Internet-Gebälk, Preisverfall bei IP-Bandbreite sorgt für Krach unter den Carriern, c't 23/05, S. 64

[4] Institut für Internet-Sicherheit: www.internet-sicherheit.de

Kasten 1

Looking Glass: Routing-Informationen im Web

Das Web bietet eine Menge Einblicke in die Vernetzung von autonomen Systemen. Ein idealer Einstiegspunkt ist der Routing-Information-Service des Reseaux IP Européens (RIPE). Hier kann man beispielsweise durch den Service RISWhois die Zugehörigkeit von IP-Adressen und IP-Präfixen zu autonomen Systemen recherchieren. Generell sind die Webseiten des RIPE erste Anlaufstelle, um Informationen über Autonome Systeme, IP-Adressen oder auch Routing-Policies zu erhalten. Hier findet man über die WHOIS-Datenbank auch die AS-Nummer seines ISP heraus, mit der dann weitere Informationen über das AS zu recherchieren sind.

Informationen, wie die Dauer von BGP-Sessions, die aktuelle Größe der globalen Routing-Tabelle oder die Verbindungen und Präfixe des eigenen DSL-Providers können zumeist auf dessen Website online recherchiert werden. Über den jeweiligen Looking-Glass-Service kann man sich die Routing-Informationen ansehen.

Oft ist es möglich, einen Traceroute-Befehl vom jeweiligen Router aus abzusetzen. Der Service zeigt den Weg, den ein IP-Paket vom AS des Providers zum Ziel durchläuft. Die Anzahl der Router (Hops) auf diesem Weg ist ein wichtiges Kriterium für die Bewertung der Übertragungsqualität, die ein Provider bietet. Als Faustregel gilt: Je mehr direkte Verbindungen zu autonomen Systemen, desto geringer die Anzahl der Hops. Über ein "BGP-Summary" erhält man überdies bei vielen Providern Informationen über Dauer und Anzahl der BGP-Sessions der einzelnen Router.

Kasten 2

Surftipps

Site	Beschreibung	URL
RIPE Routing Information Service	Online-Tools, um Routing-Informationen zu erhalten	www.ripe.net/projects/ris/tools/index.html
RIPE Whois	Online-Suche nach RIPE-Objekten	www.ripe.net/whois
Potaroo	Grundlagen zu BGP und Co.	www.potaroo.net
CAIDA-Project	Infos zur Internet-Infrastruktur	www.caida.org
Traceroute.org	URLs zu Looking Glasses und mehr	www.traceroute.net
DTAG Routing Information Services	Looking Glass fürs IP-Netz der Deutschen Telekom	https://f-lga1.f.de.net.dtag.de/index.php
University of Oregon Route Views Project	Info-Sammlung zum Thema Routing und dessen Visualisierung	http://www.routeviews.org
Opte Project	künstlerischer Ansatz zur Visualisierung des Internet	http://opte.org
Network Explorer	Informationen zu Interconnects eines wählbaren AS	www.robtex.com/netexp
BGB-Play	Visualisierung von BGP	http://www.ris.ripe.net/bgpplay/