

Sonderdruck für MAGELLAN Netzwerke

IP-ROUTING-ANALYSE IN GROSSEN NETZEN

Eine Aufgabe für Spezialisten

Große Konzernnetze sowie immer mehr Carrier-Netzwerke basieren heute auf dem IP-Protokoll. Ohne die Verfügbarkeit spezialisierter Routing-Protokolle wie OSPF, EIGRP, IS-IS oder BGP4 jedoch wäre der Betrieb solcher Strukturen bis hin zum "World Wide Web" undenkbar. Diese Routing-Verfahren bergen allerdings auch Probleme und Fehlerquellen, die mit geeigneten Diagnose- und Managementwerkzeugen gelöst werden können.

Router dienen zur Konfiguration von Netzen und Subnetzen und sind für eine möglichst intelligente Paketvermittlung zuständig. Router für große Netze beispielsweise können autark die Erreichbarkeit verfügbarer Netze feststellen und selbstständig entscheiden, ob sie ein Datenpaket versenden oder nicht. Fallen Verbindungen oder Netzsegmente aus, werden Nachbarsysteme über solche Statusänderungen informiert.

In vielen Grafiken sind IP-Netzwerke als "IP-Wolken" dargestellt, wobei es unerheblich ist, welchen genauen Weg die Datenpakete nehmen – es sei denn, es kommt zu Problemen, etwa zu verringertem Datendurchsatz, zu sporadischen Verzögerungen oder gar zu einem Totalausfall.

Solche Störungen können für die Fehlersuche zur Herausforderung werden. Zunächst stellt der Techniker fest, dass vermehrt Routing-Protokolle aufgetreten sind:

Routing-Updates, Prefix-Changes, Neighbour-Loss sowie eine Fülle von speziellen Nachrichtentypen und Events, die die Router im Netz untereinander austauschen. Trotz unbestreitbarer Vorteile moderner Linkstate-Protokolle bergen sie auch Gefahren insbesondere für große IP-Netze. Statistisch gesehen sind Ausfälle zu rund 30 Prozent den OSI-Layern 1 und 2 zuzuordnen, auf Fehler innerhalb der Schicht 3 entfallen jedoch weit mehr als die Hälfte. Und hier spielen die Routing-Protokolle eine entscheidende Rolle.

FEHLERQUELLEN Eine Ursache für die hohe Fehlerquote liegt in den Komfortmerkmalen wie

Redundanz, Load-Balancing oder Load-Sharing. Denn diese sind anfällig für fehlerhafte Konfigurationen. Außerdem sind ältere, nicht kompatible aktive Komponenten wie unmanaged Hubs oder Alt-Router häufig der Grund für Netzwerkausfälle, weil Netzmanagementsysteme sie nicht ohne weiteres erkennen können. Auch falsch gesetzte Router-Parameter, die nicht den realen Anforderungen entsprechen, führen zu Störungen und fallen zudem nicht immer sofort auf. Beispielsweise ist manchmal die Link-Speed höher konfiguriert als die physikalischen Gegebenheiten es zulassen. Zudem erfordern der Umbau und die Wartung von Netzen mit zunehmender Größe und Komplexität höchste Aufmerksamkeit, da zum Beispiel nach einer Firmware-Aktualisierung nicht der gesamte Netzapparat mit allen programmierten Verhaltensweisen durchgeprüft werden kann.

Bei redundanten Verbindungen treten zum Beispiel Link-Flapping und Adjacency-Flapping auf. Damit ist ein ständiges Wechseln von Verbindungen oder von logischen Tunneln zwischen Routing-Domäne

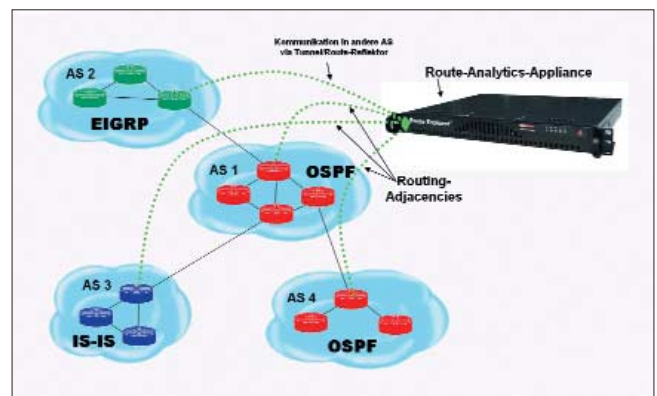


Bild 1. Integration einer IP-Routing-Analyse-Appliance in die Netzwerkinfrastruktur
Quelle: Magellan/Packet Design

und Appliance gemeint. Denn redundante Hauptverbindungen ermöglichen im Fehlerfall, dass der Router automatisch einen Ersatzweg für diese Verbindung wählt. Durch Falscheinstellung oder bei ungünstigem Lastverhalten kann es passieren, dass die Verbindung ständig zwischen diesen Wegen hin und her wechselt. Eine mögliche Folge ist dann, dass Datenpakete, die gerade auf der Verbindung unterwegs sind, durch Buffer-Clearing gelöscht werden oder dass bestehende logische Verbindungen von Applikationen zurückgesetzt werden. Das führt zu Performance-Einbußen, "Leitungshängern" und Neuanmeldungen.

Auch Schleifenbildungen innerhalb der Routing-Protokolle sind potenzielle Störungsursachen. Oft werden diese durch rekursive Routenkonstruktion ausgelöst, die erst zu Tage tritt, wenn Ersatzwege eingeschlagen werden. Mit rekursiver Routenkonstruktion ist gemeint, dass BGP (Border Gateway Protocol) im Fehlerfall einen Ersatzweg einschlägt, der über einen Zwischen-Hop wieder auf dem Ursprungs-Router landet, weil das für die Zwischenstation der bevorzugte Datenweg ist. Solche Schleifenbildungen können ganze Netze oder Netzsegmente in Schach halten und sind zudem schwer vorhersehbar und nachvollziehbar. Man müsste beim Testen einer Verbindung automatisch die Ersatzwege mit überprüfen können. Häufig beruht dieses Verhalten auf Netzen mit Komponenten unterschiedlicher Hersteller.

Und schließlich treten beim Routing sogar schwarze Löcher auf. Sie erscheinen ebenfalls bei dynamischen Umschaltungen in Verbindung mit kleinen Konfigurationsfehlern. Dabei verschwinden Daten ohne nachvollziehbare Rückmeldung. Die Suche nach der Ursache (oft einzelne Router, deren Konfiguration/Betriebsmodus fehlerhaft ist) gestaltet sich oft schwierig.

HERKÖMMLICHES TROUBLESHOOTING
Fehlererkennung und -analyse sind insbesondere in großen Netzen kritische Faktoren. Eine Stunde Netzwerk-Downtime kann bei entsprechender Anzahl betroffener Nutzer katastrophale Folgen haben. Die meiste Zeit geht in diesen Fällen für die Isolation/Eingrenzung der Fehlerursachen verloren (Root-Cause-Analyse).

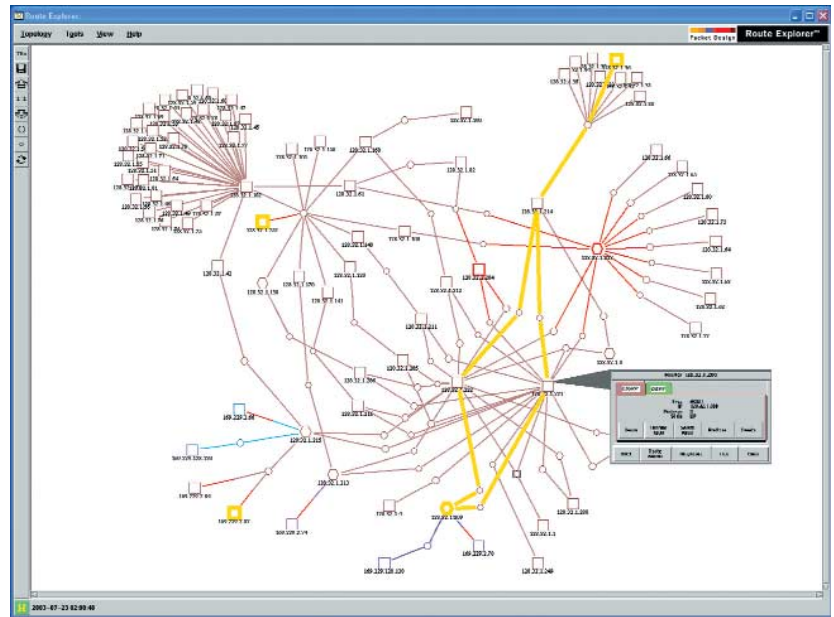


Bild 2. Visualisierung der realen IP-Verbindungswege

Quelle: Packet Design

So bietet die CLI-Diagnose (CLI: Console-Line-Interface) eine pragmatische, wenn auch archaisch anmutende Methode zur Fehlereingrenzung: Per Telnet-Konsole loggt sich ein IP-Experte oft gleichzeitig in mehrere zentrale oder betroffene Router ein und versucht, die Fehlersituation durch prüfenden Vergleich der Konfigurationen aufzuklären. Debugging-Tools bringen eventuell weitere Zusammenhänge ans Licht. Grundsätzlich handelt es sich dabei um einen manuellen Konsolen-Check. In einem komplexen Netzwerk mit zum Beispiel weltweit 100 verteilten Core-Routern ist diese Methode deshalb nicht sehr viel versprechend.

Auch für die Analyse von mitgeschnittenen Routing-Datenpaketen ist Expertenwissen gefragt: Hat der Netzwerkexperte zunächst die Fehlersituation sondiert und weiß, welche Knoten betroffen sind, zeichnet er dort den Datenverkehr über Probes und einen Protokollanalysator auf. Das geschieht entweder über den Mirror-beziehungsweise Span-Port des Routers oder über ein dazwischen geschaltetes Analyse-Tap, das den Traffic über einen Splitter ohne Eingriff in den Datenverkehr auf einen Tap-Port abbildet. Durch den Protokolldecoder kann er nun Auffälligkeiten und Unregelmäßigkeiten innerhalb der Routing-Daten analysieren, den Fehler sichtbar

machen und korrigieren. Doch der Mitschnitt von Inter-Router-Konversationen bedeutet, dass der Analysator tausende von Routing-Paketen in kürzester Zeit empfängt und der Protokolldecoder blitzschnell Ursache und Wirkung unterscheiden muss. Zudem ist die Datenaufzeichnung technisch aufwändig, da die Datenbeziehungen in viele Richtungen weisen. Auch Span-Port-Konfiguration und Tap-Einbindung erfordern viel Know-how.

Eine auf den ersten Blick einfache Möglichkeit zur Fehlersuche, ist die Nutzung des vorhandenen Managementsystems, die in der Regel auch Layer-3-Verbindungen erkennen und visualisieren können. Durch optionale MIB-Erweiterungen (etwa auf Basis der OSPF-MIB/RFC2370 und der BGP-MIB/RFC1657) lassen sich die Systeme so anpassen, dass sie auch die Vitalparameter der Routing-Protokolle sammeln und die Situation des IP-Netzwerks aus den MIB-Details rekonstruieren. Aus den Daten leiten sie mathematisch auftretende Fehlersituationen ab und korrelieren Zusammenhänge.

Hier besteht das Problem, dass nicht der tatsächliche Schicht-3-Verkehr analysiert wird, sondern dass Gerätemeldungen der Router mathematisch ausgewertet werden. Zudem kann ein Layer-2-Event fatale Auswirkungen auf die Schicht-3-Verhaltens-

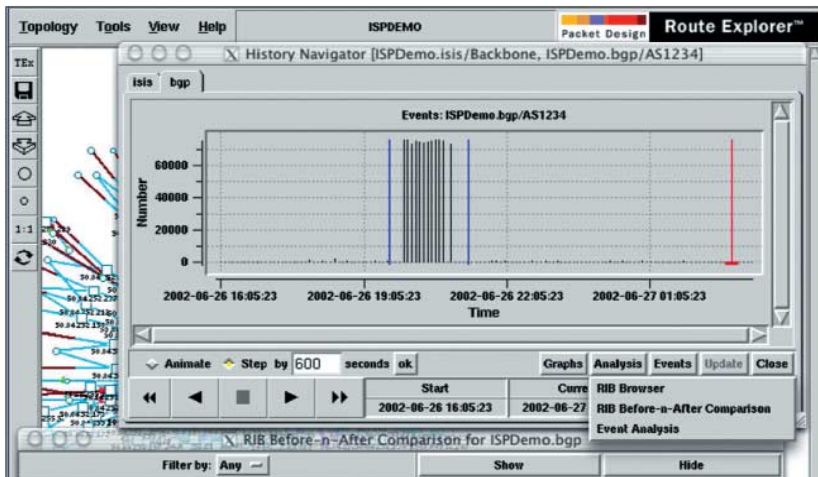


Bild 3. Ähnlich wie bei Videoaufzeichnungen kann der Administrator in der Routing-Historie hin- und herspulen und die Konfigurationen nachbearbeiten. Die Änderungen werden in der Topologiefgrafik visualisiert. Quelle: Packet Design

weise eines Netzes haben. Das heißt, bei großen Netzen besteht die Gefahr, dass der Manager im Fehlerfall vor lauter Event-Meldungen den Überblick verliert. Hinzu kommt, dass SNMP-Polling nicht echtzeitfähig ist, weil die zentrale Polling-Engine die Daten sequenziell aus den betroffenen Systemen anfordert. Doch die Autonomie und Eigendynamik der intelligenten Routing-Protokolle erfordern oft eine gleichzeitige und schnelle Analyse, um die Zusammenhänge und Hintergründe einer Fehlersituation aufdecken zu können.

IP-ROUTING-ANALYSE Konzerne und Carrier wenden die beschriebenen Verfahren meist in Mischform an, da alle Methoden ihren spezifischen Nutzen aufweisen. Darüber hinaus gibt es mittlerweile auch dedizierte Techniken zur Analyse des IP-Routing-Verhaltens in großen Netzen. Eine

davon entwickelte beispielsweise das amerikanische Unternehmen Packet Design. Dieses Verfahren basiert auf einer Appliance, die im Netzwerk installiert wird und in Echtzeit allein die Routing-Informationen zwischen den einzelnen Routing-Domänen (AS) über logische Routing-Tunnel (Routing-Adjacencies) und Route-Reflektoren sammelt, sich jedoch nicht aktiv am Protokollverkehr beteiligt (non-inversiv). Eine dahinter geschaltete, auf Routing spezialisierte Analyse-Engine interpretiert die aufgezeichneten Daten in Echtzeit und erstellt dem Anwender daraus ein reales Abbild der Layer-3-Struktur. Bild 2 zeigt die Layer-3-Strukturen einer amerikanischen Universität. Dabei sind die Router je nach Funktion oder unterstützten Routing-Protokollen mit unterschiedlichen Farben und Umrissen belegt. Die Grafik zeigt, wie sich der Ausfall zweier Router auf das Layer-3-

Netz auswirkt: Die betroffenen Systeme leuchten rot auf, die in diesem Fall vorhandenen Ersatzverbindungen zwischen zwei beliebig gewählten Endpunkten sind gelb.

Da die aufgezeichneten Daten abgespeichert sind, kann der Administrator sich auch Veränderungen im Netz anzeigen lassen (History-Analyse). Sind zum Beispiel bei einem Software-Update Routing-Probleme aufgetreten, kann der Administrator die gesamte Historie der "Routing-Wolke" nachvollziehen und nach verschiedenen Aspekten untersuchen.

Darüber hinaus bietet sich diese Technik als Simulationshilfsmittel an. Denn der IT-Verantwortliche kann sich aus den aufgezeichneten Daten der History-Datenbank Netzsituationen herausgreifen, dort Router-Konfigurationen verändern und die Auswirkungen auf andere Knoten testen. Die Veränderungen fließen direkt in die Grafiken ein (Bild 3). Im Vorfeld von Wartungsmaßnahmen wäre das ein wirkungsvolles Hilfsmittel, um mögliche Störungen vorab zu erkennen und zu umgehen. Damit würden sich Ausfälle deutlich reduzieren.

Da sich diese Technik allein auf das IP-Routing konzentriert, eignet sie sich als Ergänzung zu bestehenden Netzwerkmanagementsystemen, die sich in der Regel auf Layer 2 beschränken.

AUSBLICK Die Technik wird auf Wunsch von vielen Netzbetreibern in den Bereichen MPLS und VPLS (Multi-Protocol Label Switching und Virtual Private LAN-Segment) noch weiter ausgebaut. Darüber hinaus bietet sich die IP-Routing-Analyse-Appliance auch für die zentrale Administration von Routing-Domänen in Außernetzen an. Denn unabhängige Routing-Domänen werden häufig über Routing-Protokolle wie EIGRP, IS-IS oder OSPF konfiguriert. Und da die Appliance Routing-Adjacencies zum Sammeln der Routing-Daten aufbaut, kann der Administrator über diese auch Router in Außernetzen verwalten.

(Uli Weller/db)

Der Autor ist Mitbegründer von Magellan Netzwerke und verantwortlich für den Bereich Netzwerktelemetrie.

Glossar

| | |
|--------------|--|
| AS | Autonomous System, unabhängige Routing-Domäne |
| BGP | Border Gateway Protocol, meistgenutztes Routing-Protokoll zwischen Internet-Providern |
| CLI | Console-Line-Interface, Konfigurationszugang (seriell oder per Telnet) eines aktiven Netzwerksystems |
| EIGRP | Enhanced Interior Gateway Protocol, Erweiterung des IGP, Linkstate-Protokoll von Cisco |
| IS-IS | Intermediate-System – Intermediate-System, Layer-3-Routing-Protokoll nach ISO10589 |
| MPLS | Multi-Protocol Label Switching |
| OSPF | Open Shortest Path First, standardisiertes Linkstate-Routing-Protokoll |
| VPLS | Virtual Private LAN-Segment (gemäß RFC 2764) |