

Münchner Flughafengesellschaft vermietet Netzanschlüsse Horst Müller

Im neuen Terminal 2 des Münchner Flughafens sorgt seit wenigen Monaten ein Virtuelles Privates Netz (VPN) auf Basis der MPLS-Technik für sicheren und schnellen Datenaustausch. Die mandantenfähige Gigabit-Ethernet-Installation wird heute von den unterschiedlichsten Nutzergruppen in Anspruch genommen, denen der Flughafen als Dienstanbieter gegenübertritt. Jeder Anwender verfügt trotz gemeinsamer Infrastruktur über ein abgeschottetes Netz.

Im Terminal 2 des Münchner Flughafens, das am 29. Juni 2003 eröffnet wurde, übernehmen mit der Flughafen München Gesellschaft und der Lufthansa erstmals ein Airportbetreiber und eine Luftverkehrsgesellschaft gemeinsam die unternehmerische Verantwortung für den Betrieb eines Abfertigungsgebäudes. Im so genannten Hub Control Center wird dies besonders deutlich: Dort haben beide Partner eine gemeinsame Arbeitsplattform aufgebaut, von der aus alle Abfertigungsvorgänge – wie etwa Be- und Entladung des Gepäcks, Frischwasserversorgung, Betankung, Kabinenreinigung oder Catering – übergreifend gesteuert werden. Im Keller des Terminals sorgt eine weit verzweigte Gepäckförderanlage dafür, dass das Umsteigen von einem Flug zum nächsten reibungslos funktioniert und im Idealfall innerhalb von 30 Minuten zu bewältigen ist.

Bereits seit 1992 betreibt der Flughafen auf seinem Gelände ein Datennetz, das im Laufe der Jahre immer wieder modernisiert und erweitert wurde. „Im Jahr 2000 erreichten wir damit allerdings die Leistungsgrenzen und konnten die Anforderungen unserer Kunden immer schwerer erfüllen“, berichtet Michael Zaddach, Leiter der Hauptabteilung Informatik und Kommunikation der Flughafen München GmbH. Deshalb entschloss man sich, das vorhandene Netzgebilde durch eine einheitliche Infrastruktur abzulösen und das Bestandsnetz zu erneuern. Gleichzeitig war zu diesem Zeitpunkt aber auch schon klar, dass „auf der grünen Wiese“ mit dem geplanten Terminal 2 ein vollkommen neues Netz aufzubauen war. Beide Projekte wurden zeitlich synchronisiert, und aus den Erfahrungen mit dem Bestandsnetz konnten zahlreiche Anforderungen für die Ausschreibung des neuen Netzes in Terminal 2 abgeleitet werden.

Entscheidung für Gigabit-Ethernet

Schon relativ früh entschieden sich die Verantwortlichen für eine Lösung auf Basis der Gigabit-Ethernet-Technik. Sie bot neben technischen Vorteilen auch die geforderte Ausfallsicherheit und ein effizientes Bandbreitenmanagement bei gleichzeitig hoher Verfügbarkeit bis zum Arbeitsplatz im gesamten LAN. Da in einem Flughafen eine Vielzahl unterschiedlicher Nutzer und Dienstleister an das Netz angeschlossen werden müssen, war eine äußerst zuverlässige IT-

Infrastruktur mit getrennten, nutzerspezifischen Kommunikationskanälen gefordert. Denn nur durch diese Kanaltrennung konnte nach Meinung der Verantwortlichen im Flughafen der notwendige Datenschutz gewährleistet werden. Als optimale Lösung kam deshalb zu diesem Zeitpunkt nur ein Virtuelles Privates Netz (VPN) auf Basis von Multiprotocol Label Switching (MPLS) in Betracht.

Realisiert wurde diese Infrastruktur durch die Münchner Niederlassung des IT-Lösungsanbieters NK Networks & Services mit Hauptsitz in Köln, der in einer Ausschreibung den Zuschlag als Generalunternehmer erhielt. Dabei spielten

Auf einen Blick

Mit einem mandantenfähigen VPN auf MPLS-Basis kann der Flughafen München im neuen Terminal 2 den unterschiedlichsten Kundengruppen voneinander komplett abgeschottete Netze anbieten. Trotz der gemeinsam genutzten Infrastruktur, die leicht und kostengünstig zu verwalten ist, verfügt so jeder Anwender über ein eigenes Netz.

auch die Erfahrungen eine wichtige Rolle, die in erfolgreich abgeschlossenen Netzprojekten auf den Flughäfen in Köln/Bonn und Frankfurt/M. gesammelt werden konnten. Außerdem ist NK Networks & Services als zertifizierter Cisco-Goldpartner mit den Produkten des Netzkomponentenherstellers bestens vertraut, die in dem Projekt vorrangig verwendet werden sollten.

Die VPN-Funktion von MPLS ermöglicht es mit vertretbarem Aufwand, zahlreiche private Netze für viele Kunden mit ausreichender Sicherheit einzurichten. Dadurch können beliebig viele geschlossene Benutzergruppen über die gleiche Infrastruktur kommunizieren,



Im Backbone wurden auf der Primärebene fünf „Primäre Konzentrationspunkte“ (PKP) mit Cisco-Switches der Produktfamilie Catalyst 6509 installiert

ohne dass zwischen ihnen ein direkter Datenaustausch möglich ist. Sämtliche Verbindungen zwischen diesen Benutzergruppen laufen über eine Firewall, die mit ihrem Regelwerk sicherstellt, dass nur berechtigte Nutzer auf die für sie bestimmten Daten zugreifen können. Um den einzelnen Anwendern in den Benutzergruppen Zugriff auf das jeweilige VPN zu ermöglichen, wurden auf dem Layer 2 so genannte VLAN (Virtual Local Area Networks) installiert.

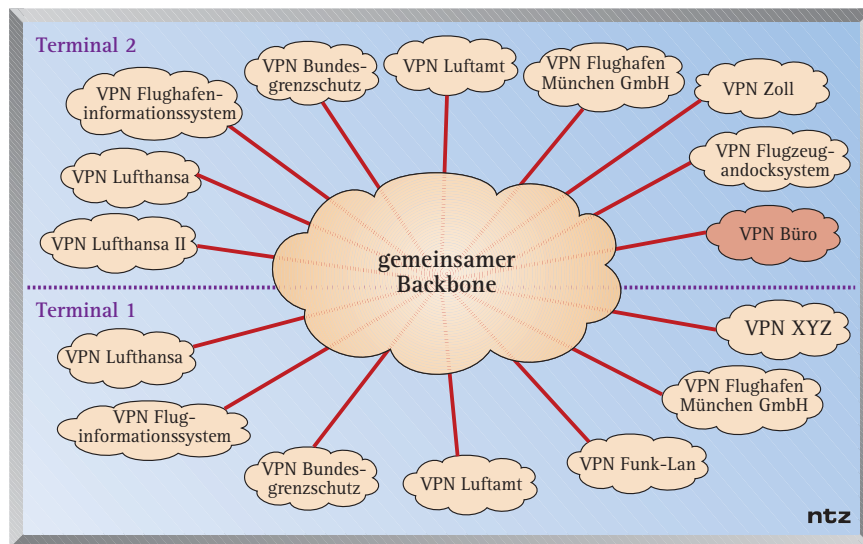
Redundante Architektur sichert Hochverfügbarkeit

Die grundsätzliche Realisierungsstrategie basiert auf einem sternförmigen Primär-, Sekundär- und Tertiärnetz für verschiedene modulare Teilgewerke, zu denen unter anderem das Hauptgebäude des Terminal 2 mit seinen beiden Piers, die Gepäcksortierhalle und das neue Parkhaus zählen. Im Backbone-Bereich wurden auf der Primärebene insgesamt fünf „Primäre Konzentrationpunkte“ (PKP) mit Cisco-Switches der Produktfamilie Catalyst 6509 installiert. Diese sind jeweils redundant auf die „Sekundären Konzentrationpunkte“ (SKP) geführt, die ebenfalls aus dem gleichen Switchtyp bestehen.

Zusammen bilden sie den in verschiedene Teilbereiche segmentierten Backbone. Die Zugangsbereiche oder „Tertiären Konzentrationpunkte“ (TKP) wurden jeweils redundant an zwei SKP angebunden und decken datentechnisch die gesamte Fläche des Terminal 2 ab. Verwendet wurden dafür die Switchtypen Catalyst 3550-24 und 3550-48. Eine Ausnahme sind einige Bereiche, die extremen Temperaturschwankungen ausgesetzt sind. Hier mussten spezielle Industrial-Ethernet-Switches (Hirschmann RS2-FX/FX) eingebaut werden.

Insgesamt deckt das neue Netz im Terminal 2 eine Bruttogeschossfläche von 260 000 m² ab. Die strukturierte Verkabelung besteht im Primärbereich (Geländeverkabelung) aus mehr als 3 500 km Einmoden- und im Sekundärbereich (Steigzonenverkabelung) aus knapp 6 000 km Mehrmoden-Glasfasern. Dazu kommen im Tertiärbereich (Etagenverkabelung) mehr als 1 300 km Kupfer-Datenkabel.

Eine entscheidende Aufgabe zur Herstellung der Hochverfügbarkeit und Gewährleistung einer maximalen Ausfallsicherheit war die redundante Architek-



Das Konzept der Virtual Private Networks im Terminal 2 des Flughafen München

tur des gesamten Netzes. Jeder Anschluss-Switch ist dazu redundant am Backbone angeschlossen, auch die Backbone-Switches sind doppelt vorhanden. Teilweise wurden die Nutzer im Anschlussbereich zudem geräteredundant angeschlossen – etwa bei Nutzergruppen mit Terminals, die örtlich nebeneinander stehen. Die Stromversorgung ist ebenfalls dreifach gesichert: Neben dem Anschluss an das normale Elektronetz gibt es eine unterbrechungsfreie Stromversorgung und ein Diesel-Notstromaggregat.

Terminalbetreiber als Dienstanbieter

Das neue mandantenfähige MPLS-Netz im Terminal 2 stellt heute eine Integrationsplattform dar, auf der die unterschiedlichen Nutzer ihre diversen Systeme betreiben. Dazu zählen beispielsweise die Flughafen München Gesellschaft, die Deutsche Lufthansa, das Hauptzollamt München, der Bundesgrenzschutz Flughafen München, die Luftsicherheitsstelle des Luftamts Südbayern und zahlreiche Fluggesellschaften, Dienstleister, Hotel- und Gaststättenbetriebe, Banken, Modeboutiquen oder Autovermieter.

Gegenüber all diesen Nutzern, die Netzanschlüsse benötigen, tritt der Flughafen wie ein Dienstanbieter auf. „Die Möglichkeit, jedem Kunden dabei ein eigenes, abgeschottetes Netz anbieten zu können, ist ein wichtiges Verkaufsargument“, erläutert M. Zaddach. Insgesamt stehen im Terminal 2 derzeit rund 10 000 Ethernet-Ports zum Anschluss bereit. Wird die maximale Kapazität erreicht, ist das Netz dank der stufenlosen Skalierbarkeit der Lösung jederzeit problemlos erweiterbar. Im Backbone werden die Routing-Informationen über das OSPF-Protokoll (open shortest path first)

ausgetauscht, das eine dynamische Lastverteilung ermöglicht und nur einen geringen Overhead aufweist.

Für den Austausch von Routing-Informationen innerhalb der VPN wird das Multiprotocol BGP (Border Gateway Protocol) benutzt. Dieses ermöglicht die Verteilung der Routinginformation der beteiligten VPN, wobei die Routinginformationen der einzelnen virtuellen Netze strikt getrennt bleiben. Die gleichzeitige Verteilung der Daten aus dem Fluginformationssystem an diverse Endgeräte macht zusätzlich die Verwendung von IP-Multicast erforderlich. Im Netz des Terminals 2 wird heute nur TCP/IP als einziges Übertragungsprotokoll akzeptiert. Durch dieses einheitliche Design lassen sich vor allem die Betriebskosten gering gehalten. Grundsätzlich ist das Netz jedoch in der Lage, im Bedarfsfall auch andere Protokolle wie IPX oder SNA zu unterstützen.

Horst Müller ist Projektleiter in der Münchner Niederlassung von NK Networks & Services.

Mit dem VPN-Projekt im Terminal 2 des Münchner Flughafens konnte mit einem der ersten mandantenfähigen MPLS-VPN im Unternehmensbereich auf Switch-Basis erfolgreich Neuland betreten werden. Als digitales Nervensystem sowohl des neuen Abfertigungsgebäudes als auch der übrigen Bereiche des Flughafens trägt das neue Netz wesentlich dazu bei, dass die bayrische Landeshauptstadt im Wettbewerb der großen Luftverkehrsdrehscheiben bestens gerüstet ist und ihrem Anspruch als „umsteigefreundlichster Flughafen Europas“ optimal gerecht wird. ■