

Sonderdruck für NK Networks & Services

MPLS-NETZWERK DES FLUGHAFENS MÜNCHEN

Daten auf Reisen am Terminal 2

Der Neubau des Terminal 2 am Münchner Flughafen erforderte ein ausfallsicheres, flexibel erweiterbares Netzwerk für den schnellen und sicheren Datenverkehr. Noch während der Bauarbeiten entstand ein stark vermaschtes Gigabit-Ethernet-Netz auf Basis von MLPS (Multi-Protocol Label Switching). Zeitgleich modernisierte der Airport die Vernetzung des Terminal 1. Mit dieser Infrastruktur tritt der Flughafen München heute als Service-Provider für die zahlreichen vor Ort ansässigen Unternehmen und Einrichtungen auf.

Am Münchner Flughafen kümmert sich eine umfangreiche Reihe von Organisationen und Unternehmen um die Bedürfnisse der Passagiere. Dazu zählen neben der Flughafen München Gesellschaft (FMG) selbst die Fluggesellschaften, staatliche Behörden und Einrichtungen sowie zahlreiche Dienstleister, Hotel- und Gaststättenbetriebe, Banken, Geschäfte und Autovermieter. Sie alle sind – teils in erheblichem Maße – abhängig vom reibungslosen und unterbrechungsfreien Funktionieren ihrer Datenkommunikation. Die Anbindung der Clients und Server verläuft über das Flughafenetzwerk, das die FMG als Service-Provider bereitstellt. Zugleich sind die IT-Spezialisten des Airports zuständig für eine Reihe weiterer Systeme, die das Netz zum Datenaustausch nutzen. Dazu zählen so unterschiedliche Infrastrukturbestandteile wie das Fluginformations-

system, das Funk-LAN mit seinen Wireless Access Points, die TK-Anlagen, die Sicherheitseinrichtungen oder die Anlagen für Lautsprecherdurchsagen.

HOHE ANFORDERUNGEN Als IT-Basis für den neuen Terminal 2 (T2) forderte

der Flughafen München ein mandantenfähiges, skalierbares und hochverfügbares Netzwerk (siehe Kasten "T2-Netzwerk des Flughafens München"). Ein wichtiges Kriterium für die neue Infrastruktur war die absolute Isolation der Mandanten. Schließlich befinden sich zahlreiche am Flughafen ansässige Unternehmen in Konkurrenz, so die Fluggesellschaften oder die Reisebüros. Zudem galt es, im Fall eines etwaigen Missbrauchs der Netzwerkkapazität störende Auswirkungen für andere Netzteilnehmer möglichst gering zu halten.

Das Netz sollte hochgradig flexibel konfigurierbar und leicht zu verwalten sein. Als besondere Hürde erwiesen sich die SLA-Anforderungen (Service-Level-Agreement) einiger zu versorgender Kundenunternehmen. Von Anfang an bestanden Forderungen nach dreifacher Redundanz auf den OSI-Layern 1, 2 und 3. Zu den Vorgaben in Sachen Hochverfügbarkeit zählte zudem, dass das Flughafenetzwerk im Katastrophenfall nach nur drei Minuten wieder funktionsfähig zu sein hat. Für diese Ausfallsicherheit hält der Flughafen München auf seinem Gelände zwei Rechenzentren vor.

MPLS-NETZ AM T2

Lufthansa und FMG gründeten speziell für den T2-Neubau die FM Bau als gemeinsame Beteiligungsgesellschaft. Über ein Ausschreibungsverfahren erhielt das Planungsbüro NCB Informationstechnik aus Gärtringen den Zuschlag für die Pla-

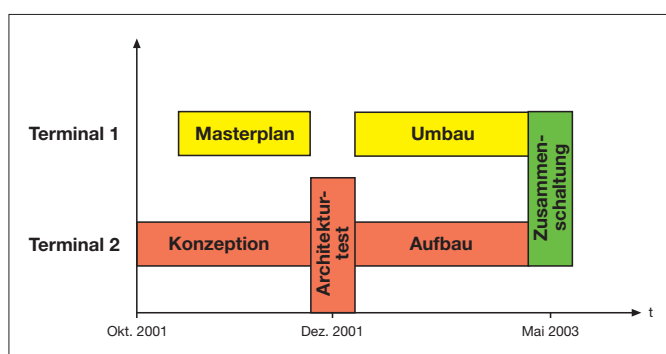


Bild 1. Die Projekte für den Neubau des Terminal 2 und die Modernisierung der IT-Infrastruktur des Terminal 1 liefen parallel ab

nung des Terminal 2, später auch für die parallel dazu fällige Modernisierung der T1-Infrastruktur. Für den T2 war ursprünglich ein Layer-2-Netz vorgesehen, doch die Einführung eines Layer-3-Cores erwies sich in der Konzeptionsphase als sinnvoller, da als mandantenfähiges Netzwerk effektiver managebar. Ebenfalls aus Gründen der Verwaltbarkeit setzte das Planungsteam auf MPLS. MPLS hat inzwischen in zahlreiche Carrier- und Service-Provider-Netze Eingang gefunden und wird als wichtige Zukunftstechnologie für den paketorientierten Datentransport der Provider gehandelt. Denn MPLS bietet eine flexible Transporttechnologie für den immer stärker IP-lastigen Datenverkehr sowie effiziente Traffic-Engineering-Mechanismen im Provider-Core. Dennoch war im Jahr 2002 die von NCB konzipierte MPLS-Installation ein sehr anspruchsvolles Unterfangen: Die Ausschreibungsanforderungen der FMG beinhalteten über 100 VPNs (Virtual Private Networks), über 1000 VLANs (Virtual LANs) sowie rund 5500 Clients.

Mittels VLANs und VPNs sollte der MPLS-Backbone des Flughafenetzes die vollständige Trennung des Datenverkehrs der einzelnen Kunden garantieren. Nicht umsonst kommt diese Vorgehensweise auch bei diversen Carriern zum Einsatz. Um den Störgrad bei Missbrauch – zum Beispiel durch Broadcast-Floods – minimal zu halten, teilte der Flughafen sein Netzwerk in sehr kleine Segmente. So wären im Falle einer Broadcast-Flood typischerweise lediglich zwei Access-Switches betroffen. Die Fehlerdomänen sind somit sehr klein.

ZWEI PROJEKTE PARALLEL Während der Planung des T2-Netzes stand auch die Renovierung der T1-Infrastruktur an. Denn dessen historisch gewachsene Landschaft zahlreicher Systeme mit Ethernet- und ATM-Transport war zu groß und unübersichtlich geworden, um noch effektiv verwaltbar zu sein. Für die Erneuerung des T1-Netzwerks konnte das Projektteam Erkenntnisse aus der T2-Konzeption nutzen. Ziel war ein gemeinsames Netz für beide Terminals.

Die Erneuerung der IT-Infrastruktur im T1 wurde zwar später geplant als das Netz des Terminal 2, kam aber schnell zur Um-

setzung. So konnte der Flughafen wiederum Ideen aus dem Masterplan des T1-Netzes in das T2-Projekt einfließen lassen (Bild 1). Das erleichterte letztlich auch die Zusammenschaltung der beiden Netzwerke.

AUSSCHREIBUNG Schon im Rahmen der Ausschreibung der Core- und Access-Switches im Oktober 2001 erfolgte ein gründlicher Test der in Frage kommenden Geräte unterschiedlicher Hersteller. Angesetzt war die Teststellung der Core-Switches für Dezember 2001 – also nur zwei Monate nach der Ausschreibung. Lediglich drei Hersteller sahen sich damals in der Lage, ein anspruchsvolles Netzwerk mit diesen Anforderungen und Umfängen zu stemmen: Angebote kamen von Alcatel, Cisco und Extreme. Aufgrund der Anforderungs-Checkliste entschied sich das Projekt-

team für einen Test des zur Testphase "Eagle Switch" genannten Routing-Switches von Alcatel und des Cisco Catalyst 6500.

Für das Testszenario bildete das Team die geplante T2-Netzwerkstruktur nach und prüfte die Geräte-Features der beiden Anbieter jeweils fünf Tage lang auf Management-, Performance-, VLAN- und QoS-Features (Quality of Service). Alcatel scheiterte letztlich daran, dass sie die geforderte Deadline für die Lieferbarkeit in Stückzahlen – Mitte Januar 2002 – nicht einhalten konnte. Doch auch Cisco als einzig verbleibender Anbieter erfüllte zwar alle "Must"-Kriterien, einige gewünschte Eigenschaften jedoch nur zu 80 Prozent. Deshalb schickte die FMG Fachkräfte zu Cisco nach San José, um die verbleibenden Problemfelder vor Ort mit Cisco-Entwicklern zu klären. "Das Risiko, ganz auf den einen verbleibenden Lieferanten zu setzen, konnten wir eingehen," so Marc Lindike, Leiter der Abteilung Systembetrieb beim Flughafen München, "da die wesentlichen Features funktionierten." Nachzurüsten galt es spezielle QoS-Features wie Bandbreiten Garantien innerhalb einer Prioritäts-Queue. Außerdem sollte der Catalyst die geforderte Zahl von 1000 VLANs ohne Performance-Einbußen unterstützen. Hier hatte der Switch angesichts der ungewöhnlich hohen Anforderung zunächst Performance-Schwächen. Den dafür verantwortlichen Bug im Cisco-Betriebssystem IOS konnte der Hersteller aber sofort beheben.

Trotz aller Vorkehrungen gegen Broadcast-Floods sollte ein Multicasting in alle Kundennetze funktionieren. "Seitens Cisco hieß es an-

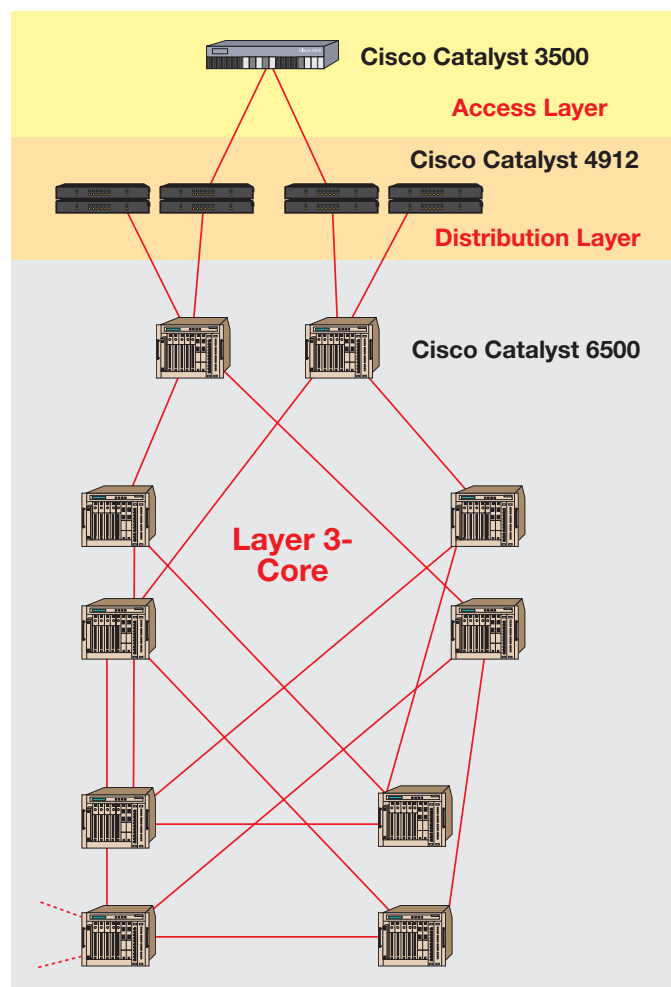


Bild 2. Schematische Darstellung des MPLS-Cores am Flughafen München

fangs, dies sei nicht möglich", so Marc Lindike. "Unsere Gespräche mit Cisco ebneten aber den Weg dafür, diese Funktionalität freizuschalten." Auf der Basis der NCB-Planung und der überarbeiteten Cisco-Switches implementierte die Münchener Niederlassung des Netzwerkspezialisten NK Networks & Services unter Leitung des Projektmanagers Horst Müller den stark vermaschten Gigabit-Ethernet-Backbone als reines Layer-3-Netzwerk, also ohne Layer-2-Tunneling.

Spezielle Industrial-Ethernet-Anforderungen bestanden nicht, da die Maschinensteuerung – zum Beispiel für die Gepäckförderbänder – anders als deren Anzeige nicht über das MPLS-Netz erfolgt. Einen Sonderfall bildete lediglich der Vorfeldbereich (also der "Flugzeugparkplatz"): Hier befinden sich die Access-Switches in Containern, die nicht isoliert sind und somit die Switches hohen Temperaturen aussetzen. In diesen 29 Containern griff NK Networks auf HMA-RS2-FX/FX Rail-Switches von Hirschmann zurück.

IMPLEMENTIERUNG In der Implementierungsphase waren die auftretenden Probleme, wie bei Projekten dieser Größenordnung üblich, laut Lindike "zu 20 Prozent technischer und zu 80 Prozent organisatorischer Natur". Die technischen Hürden ergaben sich vorrangig aus dem Umstand, dass es das T2-Netzwerk bereits während der Bauphase des Terminalgebäudes zu implementieren galt: Mal fehlten Hinweisschilder zu Ortsangaben, mal waren IT-Räume noch nicht absperrbar. Mitunter war noch kein Strom vorhanden, dann stellte wieder die

staubhaltige Luft die empfindlichen IT-Systeme auf eine harte Probe. Ein Sanierungsunternehmen war permanent damit beschäftigt, die IT-Komponenten staubfrei zu halten. Das Team von Horst Müller war in seiner Funktion als Koordinator erheblich gefordert. So galt es zum Beispiel, mittels Schlüsseldienst sicherzustellen, dass Räume mit teurem Equipment nicht mehr frei betretbar waren. Diese Koordination von NK Networks funktionierte so gut, dass lediglich ein Cisco-3500-Access-Switch auf der Baustelle abhanden kam.

Dank der intensiven Tests bei der Ausschreibung traten laut Marc Lindike bei den Tests während der Implementierung nur noch triviale Probleme auf. Eine falsch dokumentierte Schalterstellung bei einem Cisco-Switch führte einmal zu einem Forwarding auf allen Ports – ein Software-Bug, für den schnell ein Workaround gefunden war. So konnte sich die FMG auf das Change-Management für den Umzug in den Terminal 2 konzentrieren. Jedes Großprojekt bildet jedoch seine eigene Dynamik aus. Im Falle des T2 ergab sich in den letzten drei Wochen vor Inbetriebnahme eine Flut von 1500 kurzfristigen Neuschaltungsanträgen: Mitarbeiter wollten zum Beispiel ihre Schreibtische an eine andere Stelle rücken und benötigten dafür dort eine Anschlussbuchse. All diese Änderungen waren im Kabelmanagement- und im Helpdesk-System zu hinterlegen, um künftige Aufschaltungen effizient zu halten. Hier gab es laut Wilhelm Bicker von der Abteilung Kommunikationstechnik und -netze der FMG "harte Kämpfe", um zu vermeiden, dass Kabel "irgendwie verlegt" wurden. Insgesamt

samt schaltete die FMG im Rahmen des T2-Projekts 16.000 Leitungen für die unterschiedlichsten technischen Systeme von LAN und Telefonie bis zu Einbruchsmeldern frei.

Solche kurzfristigen Änderungen machten das Projekt zusammen mit der kurzen Planungszeit und der Implementierung während des Baus zu einem, so Lindike, "intensiven Prozess". Eine Ausdehnung des Projekts war nicht möglich, da das Netzwerk zur Eröffnung des Terminal 2 stehen musste. Ein Aufschub von März auf Juni 2003 entstand lediglich durch Verzug bei den Baumaßnahmen. So hatte das IT-Projekt ein Quartal mehr Luft. Am 22. Mai 2003 schaltete die FMG schließlich die Netze des ersten und des zweiten Terminals zusammen – rechtzeitig zur Eröffnung des neuen Terminals am 29. Juni 2003.

BETRIEB Die Neukonzeption des Netzwerks führte zu einer Neugliederung der IT-Aufgaben: Die von Marc Lindike geleitete Abteilung Systembetrieb ist verantwortlich für den aktiven, logischen Teil des Netzwerks sowie für Serverräume, Backend-Systeme und Security. Hier steuern heute von zentraler Stelle aus drei CCIEs (Cisco Certified Internetworking Expert) das Flughafenetzwerk. "Ohne MPLS wären dafür sechs oder acht Mitarbeiter nötig, zum Beispiel für die Pflege von Access-Control-Listen", schätzt Lindike. Administrationsaufgaben wie das Customizing erledigt der User Helpdesk neben seiner eigentlichen Arbeit. Wilhelm Bickers Abteilung Kommunikationstechnik und -netze, verantwortlich für Verteilerräume, passive Komponenten sowie Verkabelung, erledigt mit mehreren Mitarbeitern die vor Ort anfallenden Arbeiten (Field-Services).

Ein Mitarbeiter der Abteilung Systembetrieb kümmert sich ausschließlich um Firewall- und Security-Fragen. Denn die FMG fungiert sofern gewünscht auch als Managed-Security-Service-Provider. Der Verkehr zwischen den Teilnetzen läuft hierbei über ein Firewall-Cluster verschiedener Hersteller mit mehrstufiger Infrastruktur. Neben Firewalling und VPNs gehören auch Antivirus-Scans sowie aktive Codeinterpretation wie Spam-Filter und Content-Scanner zum Leistungsspektrum. Außerdem bietet die FMG einen weiteren Service: Für "Freistil-Surfen" – also für nicht-

Flughafen München

Seit Mai 1992 ist der "Flughafen München Franz Josef Strauß" nahe Erding knapp 30 Kilometer nordöstlich von München in Betrieb, seit Juni 2003 mit zwei Terminals. Die Gesellschafter der Flughafen München GmbH (FMG) sind der Freistaat Bayern, die Bundesrepublik Deutschland und die Stadt München. Im Jahr 2003 setzte die FMG nach vorläufigen Zahlen 618 Millionen Euro um, im Vergleich zum Vorjahr ist dies trotz schwieriger Rahmenbedingungen ein Plus von 7,7 Prozent. Das Passagieraufkommen lag bei knapp 24,2 Millionen, ein Plus von 4,4 Prozent gegenüber 2002. Damit belegt München nach Frankfurt den Rang 2 unter den deutschen Flughäfen und Rang 8 in Europa. 2003 verzeichnete der Airport über 343.000 Flugbewegungen im gewerblichen Verkehr, der Luftfrachtumschlag betrug über 246.500 Tonnen. Der Flughafen München beschäftigt knapp 4900 Mitarbeiter, mit Konzerntöchtern fast 7650. Insgesamt sind am Airport über 22.000 Personen beschäftigt. Den Terminal 2 will die FMG verstärkt nutzen, um die Position Münchens als Flugdrehscheibe auszubauen, der Terminal 1 dient vor allem für Punkt-zu-Punkt-Verbindungen.

kritischen, ungeschützten Webzugriff – hat Lindikes Mannschaft in der DMZ (Demilitarized Zone) der Internetanbindung einen Metaframe-Server mit Internet-Explorern aufgesetzt. Der Server wird jeden Tag neu aufgesetzt. Da Dateitransfers von diesem Bereich aus verboten sind, stellt der Flughafen seinen Kunden einen CD-Brennservice bereit.

Das Netzwerk ist hochverfügbar ausgelegt. Allein die beiden zirka zwei Kilometer voneinander entfernten Rechenzentren sind laut Wilhelm Bicker durch ungefähr 300 Kilometer Glasfaser miteinander verbunden. Schon in der Installationsphase hatte das Projektteam Gelegenheit, die eingebauten Redundanzen “intensiv zu testen”, so Horst Müller von NK Networks: Stromausfälle traten wiederholt auf. Um das Funktionieren des Ausfallsicherheitskonzepts auch im laufenden Betrieb sicherzustellen, schaltet Lindikes Abteilung routinemäßig einmal wöchentlich von einem Rechenzentrum auf das zweite um. Dies veranlasst der jeweils zuständige Systemmanager vom Dienst. Lange Entscheidungswege entfallen also. Seine Bewährungsprobe musste das Redundanzkonzept im Sommer 2002 bestehen: Der Bruch eines Feuerlöschrohrs setzte einen Backbone-Verteilerraum im Terminal 1 unter Wasser. Trotz Stromausfalls war die Netzwerkunterbrechung aber nach zwei Minuten behoben.

Hardwareausfälle hatte die FMG bisher nicht zu verzeichnen: Alle Geräte arbeiten wie geplant. Auch bei den vier Upgrade- und Patch-Vorgängen verlief alles problemlos und ohne Nachwehen. Die Firmware-Stände hält der Flughafen mit Ciscos Management-Tool Ciscoworks synchron.

Für Event-, Performance- und Asset-Management kommt TNG Unicenter von Computer Associates zum Einsatz, für das Elementmanagement der Switches ist Ciscoworks auf Datenbankebene mit TNG synchronisiert. Helpdesk und Konfigurationsverwaltung laufen über Remedy, die Überwachung des Kabelbestands über das Kabelmanagementsystem C6000 im Zusammenspiel mit Remedy. Netzwerkneuschaltungen erfolgen teilautomatisiert: Alle Kabelwege sind in Remedy verfügbar, sodass aus dem System heraus ein Großteil der Konfigurationsaufgaben bei Neuanschlüssen zu bewerkstelligen ist. Dieser Status war nur dank straffer Organisation auf der Großbaustelle T2 zu erzielen, befinden

sich doch auf dem Flughafengelände mit seinen 2,5 Kilometern Durchmesser über 20.000 Endnoten.

LERNEFFEKT Welchen Lerneffekt hatte das Großprojekt für die Beteiligten? Laut NCB-Geschäftsführer Hartwig Bazzanella hat das T2-Projekt erneut bestätigt, wie wichtig es ist, bei der Planung die logische Kette von der Architektur über die Systeme und die aktiven bis zu den passiven Komponenten konsequent einzuhalten: “Die Planung muss in dieser Richtung verlaufen, sonst fallen bei den passiven Komponenten Neuplanungen an.” Als besonders nützlich erwies sich laut Bazzanella auch die dynamische Dokumentation, bei der die IP-Adressen in die Visio-Dokumente eingebunden sind. Denn manche Pläne waren schnell wieder veraltet.

RATIONELLE ABLÄUFE Nicht nur terminlich, sondern auch finanziell, so betont IT-Leiter Lindike, habe das Projekt den gesetzten Rahmen nicht überschritten. Das Netzwerk sei allerdings schneller als erwartet gewachsen. Einen erheblichen wirtschaftlichen Vorteil des neuen Netzes sieht Lindike im effizienten Beschaltungsprozess. Dieser ist Workflow-basiert und erlaubt nur wenige Varianten. So erfolgen Neubeschaltungen reibungslos, schnell und qualitätsgesichert. Bemerkbar macht sich das für die IT-Fachleute im Ausbleiben von negativem Feedback neuer Netzteilnehmer. In Einzelfällen gebe es Diskussionen mit Systemadministratoren von Kundenunternehmen, die ein Layer-2-Netzwerk bevorzugen würden. Hier leistet Lindikes Truppe

T2-Netzwerk des Flughafens München

Anforderungen

- Netzwerkerstellung für den Terminal 2
- hochverfügbares, ausfallsicheres Netzwerk
- leichte und schnelle Konfiguration
- Netzaufbau für 5500 10/100BaseX-Ports
- MPLS-Backbone
- Trennung zahlreicher Nutzergruppen über VPNs (Mandantenfähigkeit)
- Kopplung der LANs des alten und des neuen Terminals: Synchronisation der Erneuerung des Bestandsnetzes (Terminal 1) und der Anforderung an das neue Netzwerk (Terminal 2) sowie Zusammenschaltung in einer Nacht

Beim Terminal-2-Projekt eingesetzte Produkte

- Backbone: 20-mal Cisco Catalyst 6509, Optical Services Modules für MPLS
- Access: 137-mal Cisco Catalyst 3550-24, 121-mal Cisco Catalyst 3550-48, 12-mal Catalyst 4000, 29-mal Hirschmann Rail-Switch

Zeitlicher Ablauf des T2-Projekts

- Ausschreibung: Oktober 2001
- Testphase: Dezember 2001
- Auftragserteilung für die Installation: April 2002
- Installation: August 2002 bis Februar 2003
- provisorische Kopplung T1/T2: Oktober 2002
- Probebetrieb: 08.01.2003 bis 22.05.2003
- Zusammenschaltung beider Netze: 22.05.2003
- Eröffnung des Terminal 2: 29. Juni 2003

Aufklärung und Hilfestellung bis hin zu Layer-3-Schulungen für Administratoren und erzielt damit eine hohe Akzeptanz.

FAZIT Das Projektteam von FMG, NCB und NK Networks schaffte es, das aufwändige Netzwerkprojekt einschließlich Zusammenschaltung mit dem neu designten Netz des bestehenden Terminals rechtzeitig zur Eröffnung des Terminal 2 fertigzustellen. Dank des soliden MPLS-Netzwerks ist der Flughafen München als Service-Provider gut gerüstet, um den heute 6500 Clients des Flughafennetzes flexibel und schnell zusätzliche Teilnehmer hinzuzufügen. Mit den drei Mann für das Netzwerkmanagement kommt die Abteilung Systembetrieb laut Leiter Marc Lindike “gut klar”. Ihr Leistungsspektrum will die IT-Mannschaft weiter ausbauen. Dieses Jahr beginnen Tests für Voice-over-IP-Services. Außerdem erwägt die FMG-Truppe, eines Tages die Daten der 1500 Videoüberwachungskameras mittels Video über IP zu übertragen. (Dr. Wilhelm Greiner)