Customer Case Study

Airport Uses Network Virtualization to Consolidate and Scale Operations

EXECUTIVE SUMMARY

CUSTOMER NAME

Unique, operator of Zurich Airport

INDUSTRY

Transportation

BUSINESS CHALLENGE

- Offer reliable network service to all tenants on airport ground
- Meet increasing demand for client connectivity be it wired or wireless
- Support airport operation applications with a highly reliable network
- Provide video transmission over a converged network
- Keep pace with data center growth and demanding cluster applications

NETWORK SOLUTION

- MPLS VPN to replace network wide layer 2 VLANs
- Multicast VPN (mVPN) for efficient multicast traffic distribution
- Catalyst 6500 Switches with Supervisor Engine 720-3BXL
- WLAN integration

BUSINESS VALUE

- Consolidate multiple networks into one highly available network
- Provide security by keeping customer networks logically separated
- Help ensure flexibility of network connectivity across the whole airport
- Establish a scalable foundation to accommodate future growth needs

Flexible connectivity options and the ability to keep closed user groups isolated led Unique to design MPLS VPNs for Zurich Airport with Cisco Catalyst 6500 Series Switches.

BUSINESS CHALLENGE

Zurich Airport is located in the center of Switzerland and plays a distinct role in the European airport space. Unique is the operator of Zurich Airport and offers a broad service portfolio to about 180 other companies, which also reside on the airport. Zurich Airport offers work for about 20,000 individuals and transports around 18 million passengers per year.

Like many other enterprises, Unique faces the diverging business needs of providing the highest availability of operations while offering maximum flexibility to accommodate the ever changing needs of their business environment.

Airport applications like air-control and tower communication demand highest uptime and need to be separated from operations like baggage distribution, business administration, video surveillance, and public WLAN traffic. Besides airlines and other third parties, the airport also hosts conferences, exhibitions, and other events that require a very flexible architecture where network connection can easily be established and removed without affecting other groups.

NETWORK SOLUTION

The need for network virtualization—having multiple groups on the same physical network infrastructure, while keeping them logically separate to a degree that they have no “knowledge” of other groups—is not new. Multiple approaches are possible, as briefly outlined below.

Campuswide VLANs

The most common approach to this problem was to introduce a Layer 2 domain—that is, a VLAN for every single closed user group. These VLANs would then be configured to span across the whole campus. This was also known as “campuswide VLANs.” Although the approach seemed to be simple to implement, it turned out to suffer from some downsides.

The main drawbacks of campuswide VLANs are:

- Limited network scalability due to spanning tree
- Reduced client and network performance due to high broadcast and multicast level
- Complexity of troubleshooting
- Risk of problem propagation

Spanning Tree Protocol (STP) represented the limiting factor from a Layer 2 topology point of view. With the number of bridges in a Layer 2 domain, the risk of a Layer 2 loop (also known as broadcast storm) increased. Also the network diameter could become a limiting factor in mid-size to large topologies.

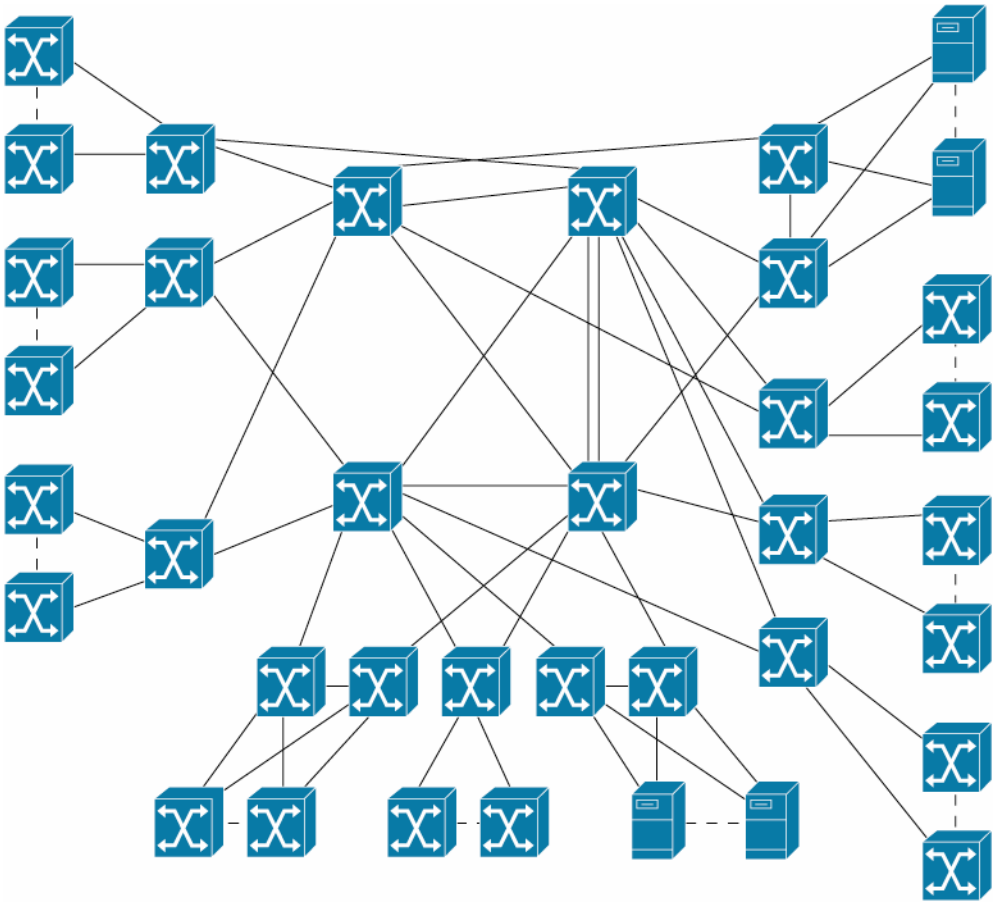
With the increasing number of clients in a VLAN, the level of broadcasts also increased. The impact of this could be seen in the higher CPU load of client and network devices as well as slower application performance. The purpose of Spanning Tree to provide a loop-free topology inherently prevented multiple active paths between any two destinations in the network and therefore limited the available network bandwidth. Although this did not represent a limiting factor at the network edge, for the core of the network this could become a problem.

Troubleshooting of large Layer 2 topologies required a significant amount of troubleshooting experience and often turned out to be time consuming. In the event of a Layer 2 loop, loss of client connectivity occurred, and remote network administration could be affected.

In addition, an STP-related issue was likely to affect all closed user groups (if not the entire network) and therefore represented a significant risk for all businesses making use of the network.

Unique's network was based on Alcatel Packet Engine switches and, where the majority of it operated, in Layer 2 mode. Figure 1 shows the network layout. Customer networks were implemented using campuswide VLANs. Unique's office network was Layer 2 in the access and Layer 3 switching on the core/distribution layer.

Figure 1. Old Layer 2-based Network



Layer 3 Campus

The use of Layer 3 switching in the core and distribution layer basically eliminated the scalability, performance, and troubleshooting drawbacks seen in the VLAN-based approach. Layer 3-based campus networks built over the past several years have proven to be scalable, robust, and high-performing.

However, the implicit “desire” of a Layer 3 switch to switch between all networks in the routing table, represented a challenge for the requirements for segmentation and closed user groups. Although access control lists (ACLs), policy-based routing (PBR), or overlay generic routing encapsulation (GRE) tunnels are possible approaches to segment traffic, the number of expected closed user groups and distribution zones are important factors to keep in mind. With an increasing number of closed user groups, the administrative/operational work would increase. A mistake of an ACL configuration in a single location could result in a “leak.” The consequence would be that one group could access data from others. In case of a worm or virus, propagation across multiple groups could happen.

The network-addressing structure should be carefully considered when using ACLs or PBR. Although a smart choice of address ranges used per group can simplify the configuration significantly, it presents a drawback because the addressing of the end system often needs to be changed. Making this change not only involves the network group within an organization but also the client/server administrators of individual closed user groups.

Layer 3 VPNs

There are basically two type of VPNs related to Layer 3: IP Security (IPSec) VPNs and Multiprotocol Label Switching (MPLS) VPNs. While IPSec VPNs are mainly focused on encryption of point-to-point connections (or point-to-multipoint in the case of Dynamic Multipoint VPN), MPLS VPNs serve the need to form logically separated networks on a common physical infrastructure. This document exclusively relates to MPLS VPNs unless mentioned otherwise.

Service providers have made use of MPLS technology for several years. Most enterprises were not embracing it, mainly due to the lack of availability on LAN switches. Only carrier-class systems such as the Cisco 12000 series routers would satisfy the performance requirements in the enterprise space. With the introduction of MPLS VPN support on the Cisco Catalyst® 6500 Series Switches in late 2003, MPLS technology became affordable for enterprises at up to multi 10 Gb Ethernet speeds.

MPLS VPNs basically offer all benefits of the previously mentioned Layer 3 campus solution, with the additional benefit of segmentation as an implicit part of the technology. Therefore closed user groups are defined using different VPNs. These VPNs are transported independently over the core of the network using labels. The networkwide benefit is that any VPN can be configured to be present at any location in the network without any compromises in performance or network design.

Flexibility of network addressing is also addressed due to the fact that the user groups are completely autonomous. Each VPN makes use of its own virtual routing and forwarding (VRF) table. This can be viewed as a separate routing table for each VPN. Therefore addressing across VPNs is completely independent and can even be overlapping. If shared or common services (for example, Domain Name System, e-mail, and Internet access) are used, Network Address Translation (NAT) would need to be used on a per VRF basis.

Table 1 outlines the benefits and limitations of each solution.

Table 1. Comparison Chart of Design and Virtualization Solutions

Requirement	Campuswide VLANs	Layer 3 Campus	Layer 3 VPNs
Network Scalability	-	+	+
Network Performance	-	+	+
Troubleshooting	-	+	+

Requirement	Campuswide VLANs	Layer 3 Campus	Layer 3 VPNs
Group Dependency	-	+	+
Secure Separation	+	-	+
Flexible Addressing	+	-	+

TECHNOLOGY AND PRODUCT BENEFITS

While being separated from other parties, customers of Unique would span all over the airport grounds, requiring any-to-any connectivity. Although Layer 2 VLANs would suffer from scalability and a pure Layer 3 network could not offer scalable and secure separation, MPLS VPN as a technology turned out to be a well-suited solution. Performance, network robustness, and scalability needs could be addressed using this technology that had proven to be working in demanding service provider networks. Consolidating multiple networks represented additional operational und business benefits.

Each Unique customer would be put in a separate VPN. The customer, however, would not (need to) know about the underlying architecture. Any-to-any connectivity would be achieved using VRFs. Speed requirements would range from a few Mbps up to connections using multiple GE ports.

The Cisco Catalyst 6500 Series Switch with Supervisor Engine 720 could easily accommodate connectivity requirements like the following:

- Network access across multiple distribution zones (such as operations of Unique itself, customs, baggage claim, travel agencies, etc.)
- Internet access for Internet kiosks that are scattered throughout airport terminals
- Building automation such as badge readers, parking meters, air conditioning, etc. spread all over the airport and connected to a central operations center
- Airline networks to gates, lounges, and check-in infrastructure
- Integration of SITA airport infrastructure and connectivity to the global SITA network
- Video surveillance and x-ray scanners with multicast requirements
- Public WLAN (PWLAN) infrastructure covering all of the passenger area

Some of the customer networks would be local to the airport and have no need for external connectivity. Others, however, might need access from inside the network to the Internet (PWLAN, Internet kiosks, lounges). A third scenario would be represented by tenants that need to grant IPSec VPN access from the Internet to their network (for remote support of third-party applications such as SAP, etc.). Finally the Unique network would also serve as a “transit” network for larger networks, where PE nodes not only offer connectivity to access switches but rather learn routes from adjacent Layer 3 switches or routers with large customer networks behind them. An example for that is the use of inter-AS routing on redundant Gigabit Ethernet trunks that face the SITA airport hub. Over these links, individual VPNs from the SITA network could be connected to the MPLS VPNs on Unique’s side.

Although the Cisco Catalyst 6500 Series Switch with Supervisor Engine 2 could offer MPLS VPN support with the additional use of Optical Services Modules (OSMs), the Supervisor Engine 720 with integrated PFC3[1] introduced MPLS VPN support on LAN interfaces. All LAN ports in the system can make use of the hardware-based MPLS forwarding (PE or P router). Fabric enabled line cards can make use of optional DFC3s, which increases the performance to support switching local to the line card, satisfying the highest levels of performance in the enterprise space.

The rich options of interface types, as well as the density of GE interfaces, presented a nice fit for the core, distribution, and data center access layer. Since servers of customers as well as Unique would be hosted in two physically separated data centers, high port density was a prerequisite. Also optional service modules like the Wireless LAN Service Module (WLSM) and Firewall Service Module (FWSM), or service carrier cards such as the SSC-400 and the IPSec SPA, positioned the Cisco Catalyst 6500 Series Switch to accommodate future security and client roaming needs in the network edge, data center, and (P)WLAN space.

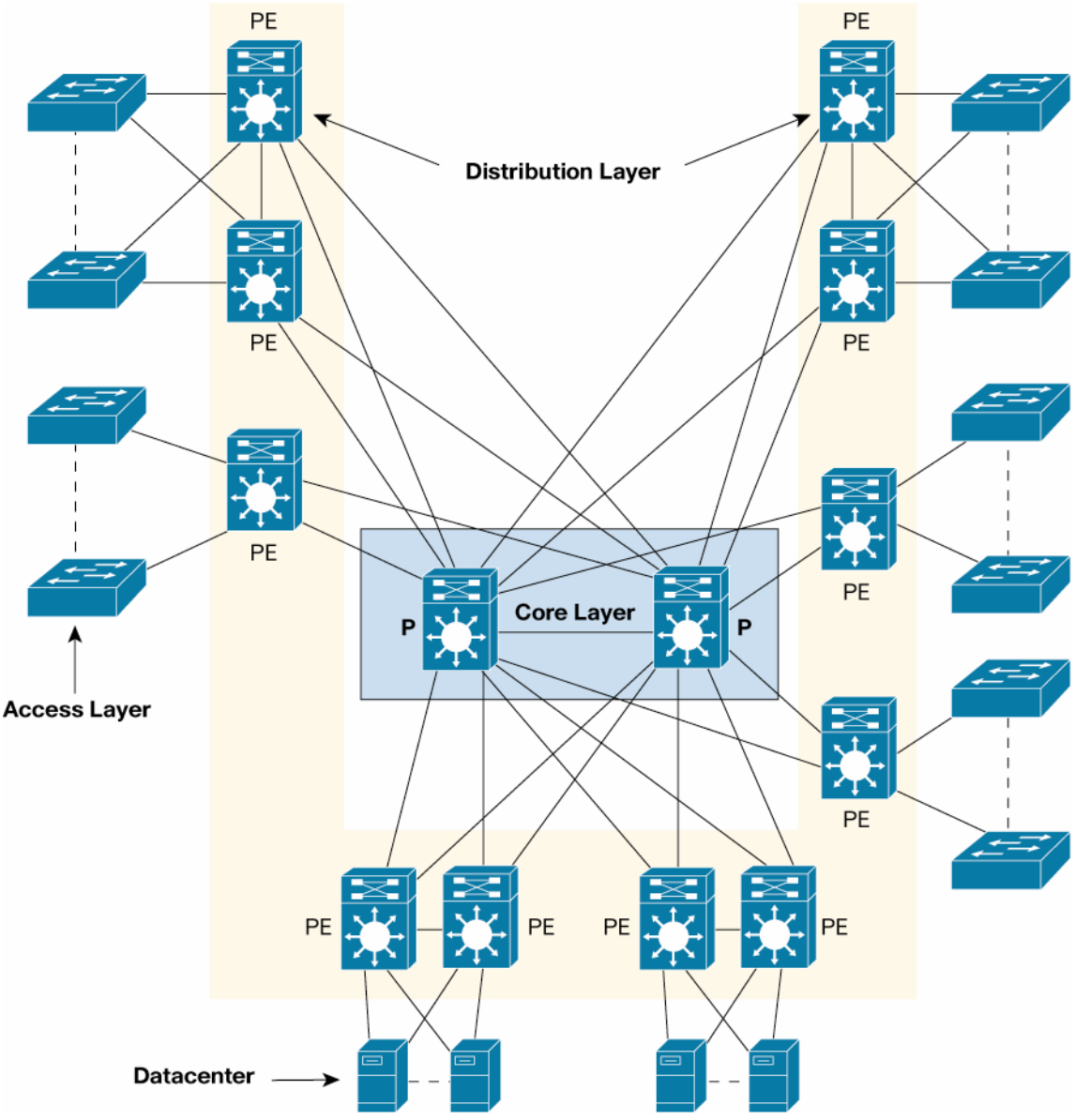
[1] PFC3B/3BXL and later support MPLS VPNs

The multicast needs from the video surveillance and X-ray infrastructure also could be satisfied using the mVPN (multicast VPN) functionality offered on the Cisco Catalyst 6500 Series Switch with Supervisor Engine 720.

PROPOSED DESIGN

The proposed design was to build a small MPLS core consisting of two Cisco Catalyst 6500 Series Switches equipped with Supervisor Engine 720-3BXLs acting as P routers. For each distribution layer zone, either a single or redundant Cisco Catalyst 6500 Series Switch (also Sup720-3BXL) would be placed acting as PE routers. The PE routers would also act as distribution-layer switches, terminating all user/customer VLANs and mapping these into the respective VPNs. In the data center, the Cisco Catalyst 6500 Series Switches would also be used as access-layer switches for servers to accommodate the increasing demand of 10/100/1000 Ethernet interfaces.

Figure 2. Proposed Design with Two MPLS P Routers and Adjacent PE Routers



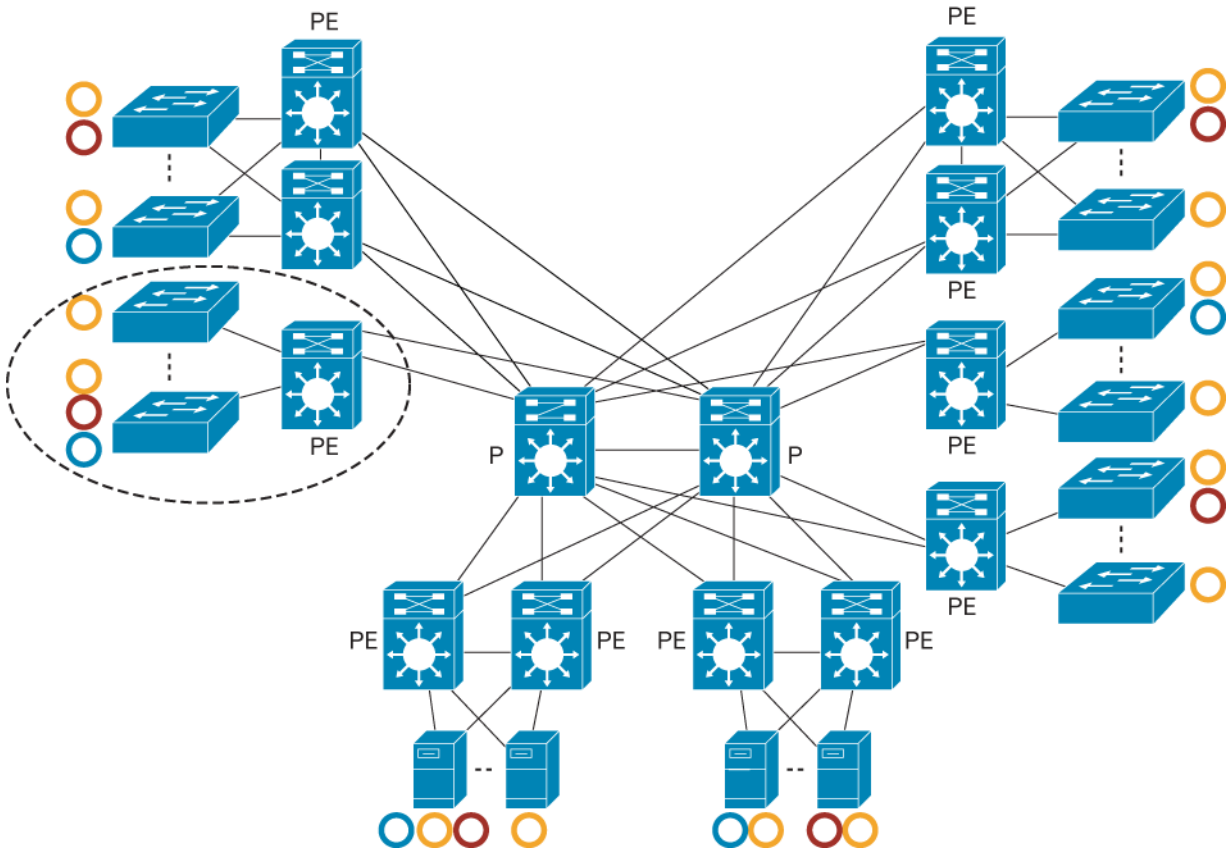
MIGRATION

As an airport, Unique had stringent requirements towards the migration process. Although the Alcatel-based Layer 2 network did suffer from the earlier mentioned limitations, not all customers could be migrated over night. Therefore a parallel network based on Cisco Catalyst 6500 switches and Supervisor Engine 720-3BXLs was put in place. The Cisco network was first set up as a commonly known campus network with a Layer 3 core and distribution layer[2].

"Unique operations" was then migrated to the new network as a first customer still residing in the global routing table. For this migration the Unique VLAN in the old layer 2 network was connected to a Cisco Catalyst 6500 Series Switch, which acted as a (default) gateway to the new subnets created for each distribution zone. This part of the migration was done in multiple steps, since the whole access layer infrastructure also had to be replaced. Although this process took some time (Unique itself employs close to 1500 network users), this change offloaded the old Alcatel network significantly.

The next step was to add the MPLS configuration to the core and distribution switches. The addition of label-switching infrastructure did not cause any traffic disruption of the Layer 3 campus network, since forwarding in the global routing table would still continue. This way, the infrastructure to accommodate VPNs could be introduced in a smooth, nondisruptive manner.

Figure 3. Clients of Different VPNs Distributed Across Access Switches

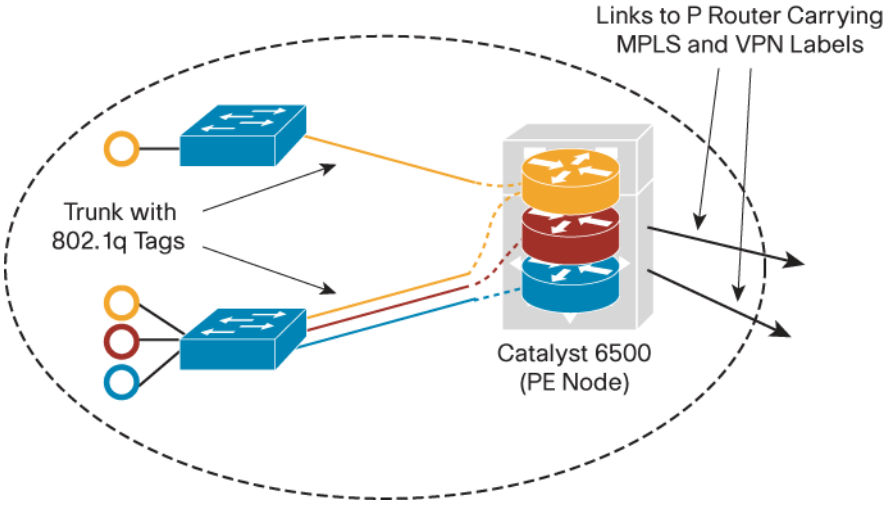


[2] Check the Solution Reference Network Design guides under http://www.cisco.com/go/srnd

A first test VPN was then created, and tests for that VPN were performed. It became apparent that the migration of customers into their respective VPN would be a straightforward task. Customers running legacy applications (non-IP or not supporting Layer 3 IP networks) were chosen to be migrated last. Clear guidelines on application requirements and migration timeframes were given to the customers several months in advance. With this, all customers residing in either entirely separate networks or in a VLAN on the Alcatel infrastructure would get migrated bit by bit. Also the Unique operations network was then put into a dedicated VPN.

The video surveillance solution from VisioWave (acquired by GE Security) as well as the X-ray equipment represented two special types of client VPNs. These VPNs would make heavy use of multicast. While multiple video streams would need to be viewable in multiple locations, the X-ray application also asked for live distribution of X-ray data to a central operations center. Although the previous network was not designed to meet large multicast requirements, multicast VPN (mVPN), an extension to MPLS VPNs, allowed an efficient transport of multicast traffic across an MPLS core.

Figure 4. Detail on VLAN to VRF Mapping



Another significant application in the airport vertical is WLAN. While applications like PWLAN in passenger areas and WLAN access for office purposes are obvious, WLAN is heavily used in the airfield/gate area. Applications from various organizations—such as handling agents, fueling, baggage logistics, and plane maintenance—make intense use of WLAN applications. These operations are usually also led by individual companies, which therefore ask for “dedicated” networks. On a WLAN layer, this could be achieved using individual SSIDs, which then are mapped into VLANs and VRFs at the distribution layer.

Since some applications need to seamlessly roam between terminals, the WLSM presented a good fit for Unique. Airport authority and handling agent cars with integrated PCs would require non-stop IP connectivity without changing the IP address while driving on the airport grounds. The WLSM would form an mGRE tunnel to the access points and therefore provide seamless roaming. This is also used for the PWLAN infrastructure to offer Layer 3 roaming to passengers commuting between terminals (that is, different distribution-layer zones) without any special need from a WLAN client driver perspective.

Remote access using IPSec VPNs was implemented based on the existing infrastructure with individual PIX firewalls and VPN 3000 Concentrators series. These would connect into the respective MPLS VPN and therefore connect users directly into their closed environment.

“The Catalyst 6500 based MPLS VPN network at Zurich Airport allows us to offer “carrier grade” network services to our Zurich Airport customers including airlines, airport operations and additional services; a typical service provider technology at the price point of an enterprise network.”

—Peter Zopfi, Head of Communication Engineering, Unique

Concerning network management, the approach would be to manage all devices using the global routing table. Although not optimal this solution offered the best level of compatibility with all used device types. From an application point of view, the CiscoWorks2000 LMS bundle was used. The VPN provisioning was done manually, since the number of P/PE devices was relatively low, and the majority of the customers would present a static environment. VPNs for events could either be preconfigured or would not take a lot of time to establish or remove.

Finally the data center would not only be able to host servers from Unique operations but also offer:

- Hosting space for servers of customers
- Shared services for multiple customers

Hosting space for customers is straightforward, meaning a VPN would just get extended to the data center and mapped into an individual VLAN. Shared services, however, would be of particular interest, since Unique’s service offering was not limited to network connectivity, but also range from client to server administration and maintenance. Also a central Internet and e-mail service should be offered to customers. In a first phase, the data center was used for Unique’s servers only, but the second phase would allow hosting of other parties’ servers. Also the concept of a shared services area would help Unique in offering cost-effective services to their customers.

NEXT STEPS

With the consolidation of networks and addition of more customers per distribution zone, the need for higher port density and availability will justify the addition for a second distribution layer switch (PE node) in each location. Multicast traffic sourced by the X-ray scanners is transported over mVPN already; the IP video surveillance part (currently running on a separate network) will be migrated to the MPLS based network.

Also the remote access solution will be addressed using a VRF-aware IPSec (ASWAN) solution with the goal to centralize configuration for IPSec VPNs. To protect the server farm and consolidate the extranet firewall infrastructure, a pair of Firewall Service Modules will be introduced. Since the airport is spanning across a large geographical area, and not all access switches are fully access protected, the introduction of IEEE 802.1x port authentication is considered. It will also allow users to be placed to their respective VPN based on their login credentials (username and password).

NETWORK VIRTUALIZATION IN OTHER VERTICALS

Although this solution represented a good fit for an airport environment, the benefits of network virtualization using Layer 3 VPNs could be mapped to customer networks of other industry verticals. Some examples for different verticals are listed in Table 2.

Table 2. Application Examples of Network Virtualization in Individual Verticals

Vertical	Examples of Cases for Network Virtualization
Manufacturing	Production plants (robots, automation of production environment, and so on), administration, sales, video surveillance.
Finance	Trading floors, administration, mergers.
Government	Shared buildings and facilities supporting different departments. In some countries the law mandates separate networks between such departments.
Healthcare	General trend toward hotel service with medical treatment. Separation among medical staff, magnetic resonance imaging (MRI) and other technical equipment, Internet access for patients, media services such as radio and television for patients.
Commercial Real Estate: Multibusiness Campus	Some resources are shared among groups. Multiple companies on the same campus where different buildings belong to different groups, but all rely on the same core and Internet access. Building automation is administered by the owner and spans across all buildings.
Retail	Kiosks, public wireless LAN (PWLAN) in branches, RF identification, WLAN devices (for example, older WLAN barcode readers that do not support any WLAN security).
Education	Separation among students, professors, administrators, and external research groups. Alternatively, individual departments that spread across multiple buildings might require access to their respective server areas. Some resources (Internet, e-mail, and news, for example) might be shared or accessed through a services zone. Building automation, too, must be separated.

SUMMARY

The Cisco Catalyst 6500 Series Switch with Supervisor Engine 720-3BXL enabled Unique at Zurich Airport to successfully implement network virtualization using MPLS VPN technology. By moving away from the legacy approach using campuswide Layer 2 VLANs, the following requirements were met:

- Smooth migration without long network disruptions
- Segmentation between the different customers
- Central service zone for shared services
- Accommodation of advanced multicast requirements
- Integration of technologies like WLAN into the network while keeping PWLAN usage separated from operational WLAN traffic

Consolidating multiple physical customer networks allows Unique to reduce operational costs and make use of a single, scalable and easy-to-manage platform in Zurich Airport. This new IP infrastructure will also serve as a base for future applications to be introduced at the airport.

FOR MORE INFORMATION

To find out more about the Cisco Catalyst 6500 Series Switches, go to: http://www.cisco.com/go/catalyst6500

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA C36-347444-00 05/06