

# **Netzwerkdesign-Wettbewerb 2009**

**von**

**Dipl.-Inform. Petra Borowka-Gatzweiler**

## 2 RFI: Die Redesign-Anforderungen

Das Ausgangsnetzwerk sowie die Anforderungen wurden an ein konkretes Planungsprojekt angelehnt und um einige Aspekte im Sicherheits- und Mobilitätsbereich erweitert. Die Lösungsanfrage wurde als Request for Information (RFI) formuliert und an die Hersteller versendet. Eine Empfehlung oder Einschränkung hinsichtlich einzusetzender Komponenten oder Komponententypen wurde nicht vorgegeben, jeder Hersteller hatte bei der Erarbeitung der Lösung Wahl- und Entscheidungsfreiheit über die eingesetzten Produkte.

### 2.1 Beschreibung

Sie sehen den zentralen Standort der Behörde FutureWorld mit circa 3800 Anschlüssen (Teilnehmer ohne TK-Anschlüsse) und circa 150 Servern (zukünftig 300) auf zwei Gebäude verteilt. Das bestehende geschichtete Ethernet-Netzwerk ist inzwischen 5-8 Jahre alt und entspricht in vielen Bereichen nicht mehr einem modernen Netzwerkdesign. Die eingesetzten Ethernet-Layer-2- und Layer-3-Switches eines etablierten Herstellers sind erstens teilweise End-of-Life und zweitens sind mit wachsender Netzgröße und Anzahl der angebotenen Anwendungen Leistungs-Engpässe (schlechte Antwortzeiten) aufgetreten. Aus beiden Gründen ist ein Redesign des Netzwerkes notwendig, das die Leistungsmerkmale und Potenziale moderner Netzwerkprodukte ausschöpfen soll.

Kernziele des Redesign sind:

- Beseitigung von Leistungsengpässen, besonders serverseitig
- Nutzung moderner Design-Ansätze und neuer Produkt-Leistungsmerkmale für ein zukunftsorientiertes Design unter streng wirtschaftlichen Rahmenbedingungen
- Schaffung eines hohen Verfügbarkeits-Niveaus mit folgenden Verfügbarkeitswerten in Prozent pro Jahr im produktiven, wartungsfreien Betrieb
  - 99,999% zwischen den Gebäuden und in der Anbindung kritischer Server
  - 99,99% in der Anbindung wichtiger Server
  - 99,95% für wichtige Dienste im Gebäudehauptverteiler
  - 99,9% für wichtige Dienste im Endgerätebereich für jeweils 24 Anschlüsse
- Umsetzung von Sicherheitslösungen bereits auf Netzwerkebene
  - Stufe 1: nur authentifizierte Geräte haben Zugang
  - Stufe 2: nur authentifizierte Benutzer auf authentifizierten Geräten haben Zugang
  - Stufe 3: wie 2, zusätzlich haben nur Geräte Zugang, die einen ausreichenden Grad an Sicherheit aufweisen

## 2.2 Anforderungen

### 2.2.1 Funktionalität

- Beseitigung von Leistungsengpässen unter folgender Vorgabe: mittelfristiges Lastwachstum von insgesamt 100% (nicht mehr Systeme sondern mehr Last je System)
- Redundanzkonzept unter folgenden Verfügbarkeits-Vorgaben:
  - 99,999% zwischen den Gebäuden und in der Anbindung kritischer Server
  - 99,99% in der Anbindung wichtiger Server
  - 99,95% wichtiger Dienste im Gebäudehauptverteiler
  - 99,9% wichtiger Dienste im Endgerätebereich für jeweils 24 Anschlüsse
- Servervorgaben:
  - Zukünftig soll jeder standalone Server mit 3 NIC angebunden werden: 2 NIC ins Produktiv-LAN, 1 Admin NIC, Nutzung von Adapter Teaming für die NICs ins Produktivnetz
  - Je Bladeserver sind 2 NIC (Teaming) ins Produktivnetz zu planen
  - Aufteilung der Server auf beide RZ
  - Die 14 VMware Cluster sowie die 145 zusätzlichen Server werden in insgesamt 14 Bladeserver-Chassis betrieben
  - Berücksichtigung der Layer-2-Verbindungen zwischen Cluster-Servern und Bladeserver-Clustern
  - Berücksichtigung der Bladeserver / Bladeserver-Chassis, inkl. Anbindung der 145 neuen Bladeserver (BL 460c) an das SAN
  - Migration des SAN: Aufteilung auf beide RZ
- Voice-Readiness und Voice Stufe 1:
  - Anschluss von 100 Telefonen (Avaya Telefone, 100 Mbit, PoE Kl. 2) an singuläre Switch-Ports in Gebäude 1, 3.OG + 4.OG
  - Anschluss von 250 Telefonen (Avaya Telefone, 100 Mbit, PoE Kl. 2) an singuläre Switch-Ports in Gebäude 2, 1.OG + 2.OG
  - als optionale Erweiterung: flächige Anschaltung von Telefonen inklusive Stromversorgung
- Sicherheitsfunktionalität als Anforderung aus dem Anwendungsbereich Telefonie und Wireless in mehreren Stufen
  - Stufe 1: nur authentifizierte Geräte haben Zugang
  - Stufe 2: nur authentifizierte Benutzer auf authentifizierte n Geräten haben Zugang

- Stufe 3: wie 2, zusätzlich haben nur Geräte Zugang, die einen ausreichenden Grad an Sicherheit aufweisen
- Stufe 4: Zusatzlösung für Fremdgeräte (Drop-Bereich für nicht authentifizierte Geräte, Guest-VLAN für Geräte, die mit einem Tagespasswort für Gäste, über Web-Passwort o.ä. authentifiziert sind)
- Stufe 5: Anomalien im Betrieb werden erkannt (Detection)
- Stufe 6: es erfolgen automatische Reaktionen auf Anomalien (Prevention)
- Einbindung von 650 Wireless Benutzern in Gebäude 1 und 2 mit 54 Mbit/s (bitte Angabe des unterstützten Verfahrens 802.11 b/a/g/h); Je Nutzer sollen 7 Mbit bereitgestellt werden ( $650 * 7M = 4550M$ ; 27 Mbit Nutzrate je AP ergeben circa 170 APs, unter Berücksichtigung von Einbußen aufgrund der Gebäudetechnik: 176 APs; Ausstattung für Redundanz mit Faktor 1,5: 264 APs insgesamt)
  - 88 APs in Gebäude 1, EG und 1.OG
  - 176 APs in Gebäude 2, EG, 7. und 8.OG
  - Einsatz einer Controller-basierenden Lösung
  - Migrierbarkeit auf IEEE 802.11n für AP und Controller
- Integriertes Management für alle Netzwerkkomponenten
- Vermeidung einer überdimensionierten Lösung unter streng wirtschaftlichen Rahmenbedingungen

### **2.2.2 Spezielle Randbedingungen zur Beachtung:**

- Skalierbarkeit
- Erweiterbarkeit auf flächendeckende Ausstattung mit Voice over IP
- Kommunikationsbeziehungen und Dienste
- Serverstandorte
- Subnetz-Bildung
- Fehlereingrenzung auf Layer-2 und Layer-3
- Lastentkopplung
- Trennung von Benutzergruppen gebäudetechnisch, gerätetechnisch oder logisch
- Quality of Service soweit erforderlich
- Aufbau von Steigbereichen
- Aufbau des Gelände-Backbones
- Layer-2/Layer3 Funktionalität
- Umzugshäufigkeit der Nutzer von 30 Prozent pro Jahr

- **Von einer kurzfristigen Änderung der FTTO-Verkabelung ist nicht auszugehen, die mittelfristige Planung ist hier offen. Für die Lösung gibt es entsprechend eingeschränkte Varianten:**
  - Beibehaltung der (alten) Microsens Switches
  - Ggf. Planung neuer Mini- / Office-Switches in den Büros
  - Ggf. Einsatz neuer Konverter

## 4.5 Hewlett Packard

### Access-Bereich

In Gebäude 1 kommen als neue Office-Switches die ohne PoE lüfterlosen Procurve 2610er 24-Port-100Base-TX-Switches zum Einsatz. Diese verfügen über zwei 1000Base-TX-Ports, so dass in Zukunft auch einzelne Anbindungen von Gigabit-Endgeräten in den Büros möglich sind. Die 24-Port/12Port-PoE-Switches der P2610 Linie haben einen Lüfter (Lautstärke als PC-Lüfter).

In Gebäude 2 kommen ebenfalls Office-Switches der P2610er Linie, jedoch mit 48 Ports zum Einsatz. Diese sind nicht mehr lüfterlos, was bei einem Einbau in den vorhandenen Etagenverteiler-Räumen jedoch nicht stört.

Für die PoE-Versorgung der Telefone und Access Points wurden ausreichend viele PoE-Ports in den entsprechenden Stockwerken dimensioniert.

In den Gebäuden werden mit modularen Procurve 5400 Switches jeweils eigene Distribution-Bereiche geschaffen. Jeder Access-Switch wird redundant mit 1000Base-SX an zwei Distribution-Switches im Gebäudehauptverteiler angeschaltet. Die Distribution / Konzentration-Switches eines Gebäudes erhalten eine zweifache 10-Gbit-LAG als Querverbindung.

### Backbone

Als Core kommen zwei vollredundant ausgelegte Procurve 8212zl Switches mit redundanter CPU (Management-Modul) zum Einsatz. Die beiden Core-Switches werden mit 10 Gbit sternförmig vollredundant an alle Distribution-Layer-Switches angebunden.

Die Core-Switches und Distribution-Switches leisten das Routing. Per dynamischem OSPFv2-Routing und ECMP wird eine Lastverteilung über den Core hinweg gewährleistet.

Übersichten der Lösung sind in Abbildung 4.24 bis Abbildung 4.27 gezeigt.

### RZ / Server

Das bestehende Rechenzentrum wird auf Gebäude 1 und Gebäude 3 aufgeteilt. Dabei ist aufgrund der Notwendigkeit einer Layer-2-Verbindung für die Clusterfunktionalität keine Layer-3-Trennung zwischen den beiden RZ-Standorten vorgesehen.

Die 115 normalen Server werden gleichmäßig (57/58) auf die beiden Rechenzentren in Gebäude 1 und Gebäude 3 aufgeteilt und jeweils mit drei 1000Base-TX-Anschlüssen an modulare Procurve 5412 als Server-Access-Switches angebunden.

Auch für die RZ-Gebäude hat HP einen Distribution-Bereich geplant, hierfür kommt je RZ ein modularer Procurve 5406 zum Einsatz. Die Server-Access-

Switches werden mit 10 Gbit sternförmig redundant an die Distribution-Switches beider RZs (Gebäude 1 und Gebäude 3) angeschaltet. Zusätzlich sind die beiden P5406 Distribution-Switches mit zweifachen 10 Gbit querverbunden, um die RZ-übergreifende Layer-2-Verbindung zu realisieren.

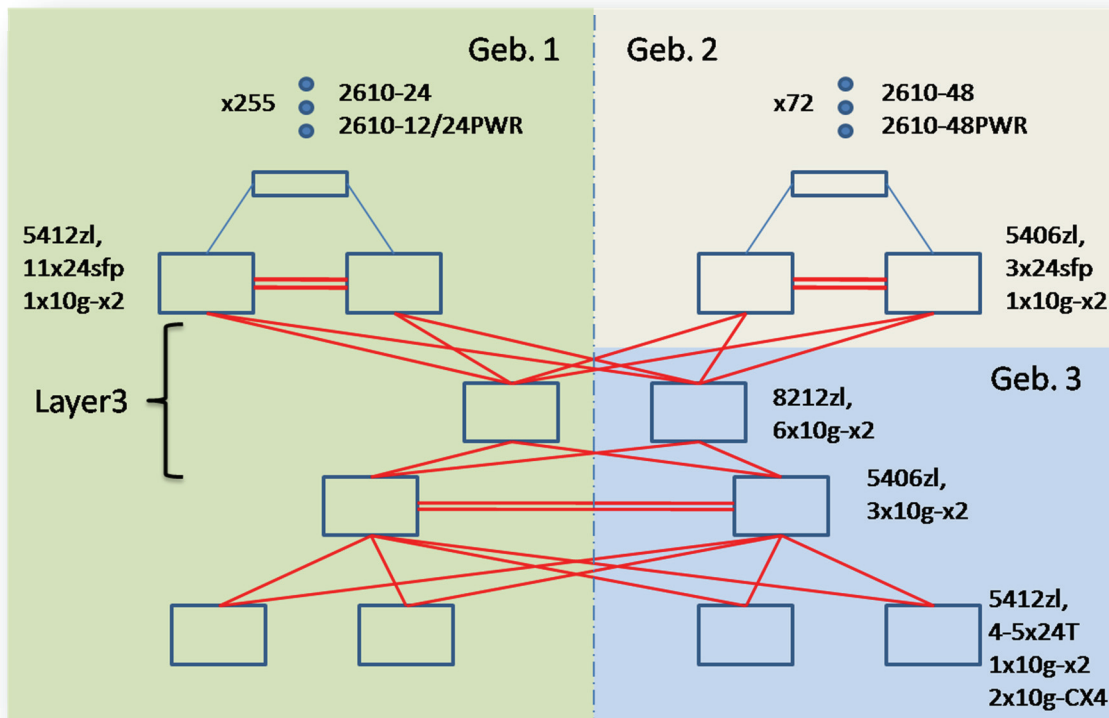


Abbildung 4.24: Übersicht der HP-Lösung

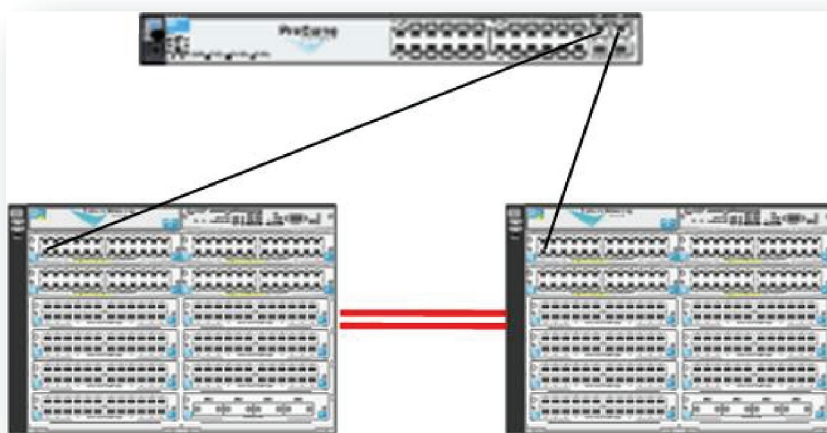


Abbildung 4.25: HP-Lösung für Gebäude 1