Ingentive Fall Studie

LAN Netzwerkdesign eines mittelständischen Unternehmens mit HP ProCurve

Februar 2009

ingentive.networks©

Kundenprofil

- Mittelständisches Beratungsunternehmen
- Schwerpunkt in der betriebswirtschaftlichen Beratung und Softwareentwicklung
- 450 Mitarbeiter
- Zentraler Hauptsitz und 10 Ländervertretungen in Europa und USA
- Umzug der Zentrale an neuen Standort erfordert Neudesign eines Netzwerks

Anforderungen

- Zwei neue Gebäude mit je 6 Etagen werden bezogen
- Zentraler Serverraum redundant ausgelegt
- 420 Gigabit Ports auf allen Etagen
- 420 dedizierte PoE Ports für IP Telefonie
- 200 Gigabit Ports im Serverraum
- Wireless LAN Zugang für Mitarbeiter, Gäste, Partner
- VoIP fähige Infrastruktur für eine Avaya Telefonielösung
- Zentrale Managementlösung

Sicherheitsanforderungen

- Netzwerkzugangskontrolle gegenüber allen Mitarbeitern (802.1x Port Authentisierung)
- Active Directory als Benutzer Datenbank
- MAC Authentisierung bei nicht-802.1X fähigen Geräten
- Zentrale Administration aller WLAN Access Points
- Abgeschotteter Gastzugang für WLAN und LAN
- Zeitlich limitierte Benutzer für WLAN bei Gästen und Partnern

Lösung mit HP ProCurve

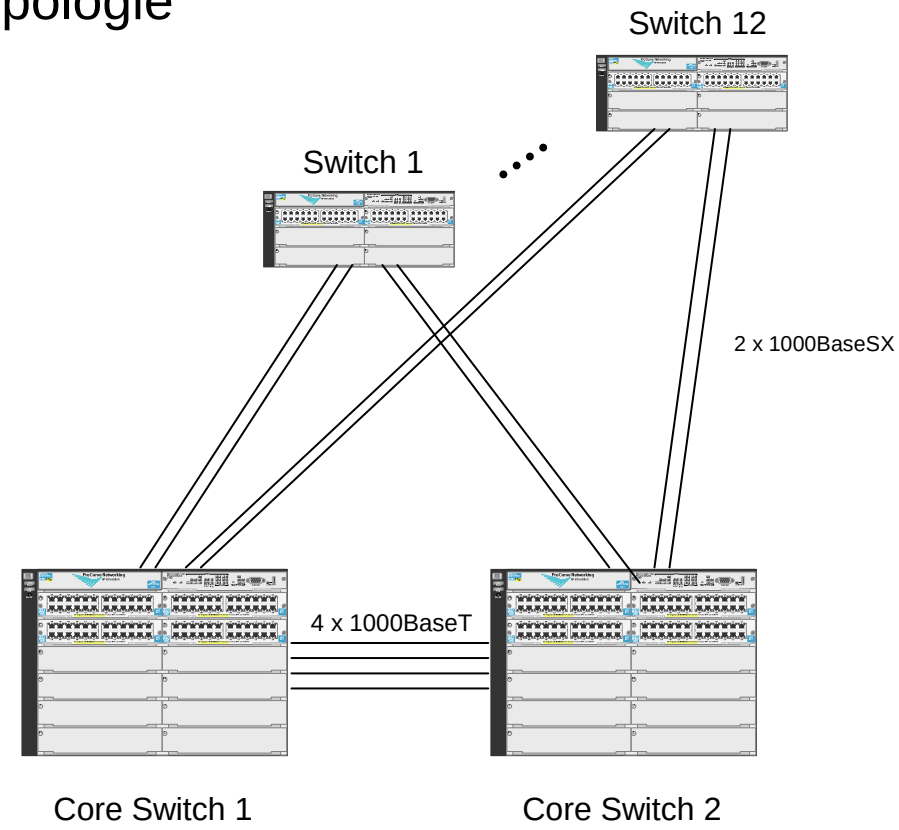
- 12 x ProCurve 5406 Switches als Etagen Switch
- 2 x ProCurve 5412 als Core Switches
- WESM als zentraler WLAN Controller
- 24 x Radio Ports RP230
- ProCurve Manager+ als zentrale Management Plattform
- Windows 2008 NPS als RADIUS Server

Vorteile der HP Lösung

- Einheitliche Plattform im Etagen und Core Bereich bringt Flexibilität und spart Kosten
  (z.B. bei eigener Ersatzteilbevorratung)
- Modulare Switches im Etagenbereich bringen weitere Vorteile:
  - Flexibilität bei der Bestückung
  - Preisvorteil bei der redundanten Ausstattung der Netzteile (kein externes RPS notwendig)
  - Keine Notwendigkeit von Stacking
  - Skalierbarkeit für eventuelle Aufrüstung auf 10 Gigabit
  - Zukunftssichere Investition durch 345.6 Gbps Switch Fabric
- 30 Jahre Herstellergarantie auf alle HP ProCurve Geräte

Netzwerktopologie

Physikalische Topologie

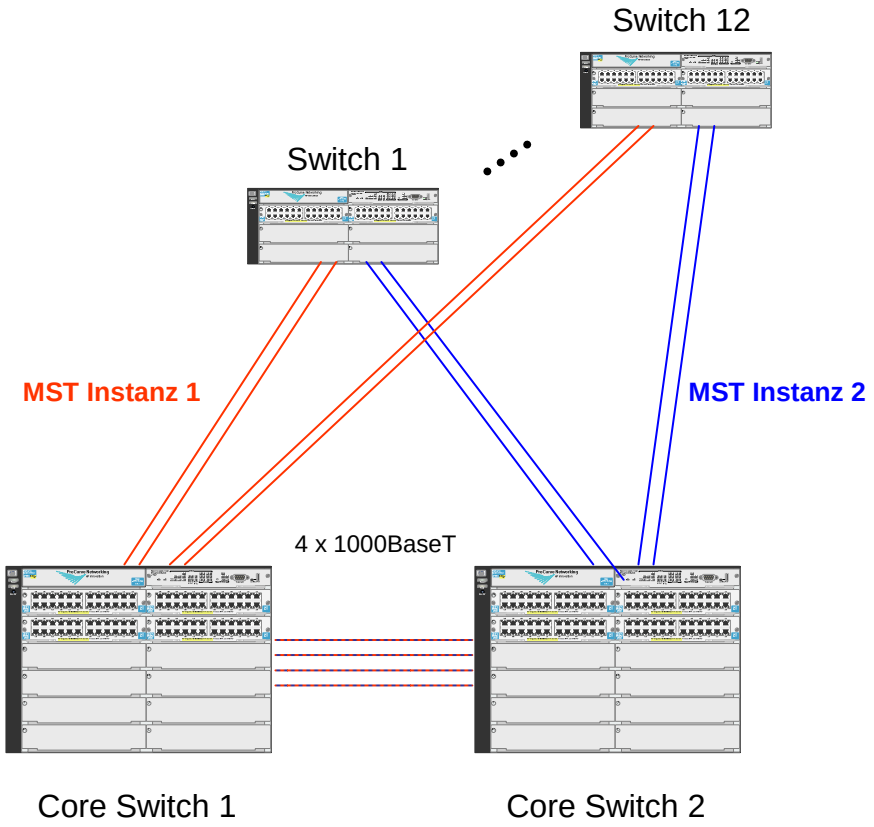


ingentive.networks

Logische Topologie

- Bündelung der Uplinks zu 2 Gbit/s durch Trunks
- Einsatz von Multiple Instanz Spanning Tree (MST)
- Zwei Instanzen zur Lastverteilung
  - Ungerade VLANs für Instanz 1
  - Gerade VLANs für Instanz 2
- VRRP als redundante Routinginstanz

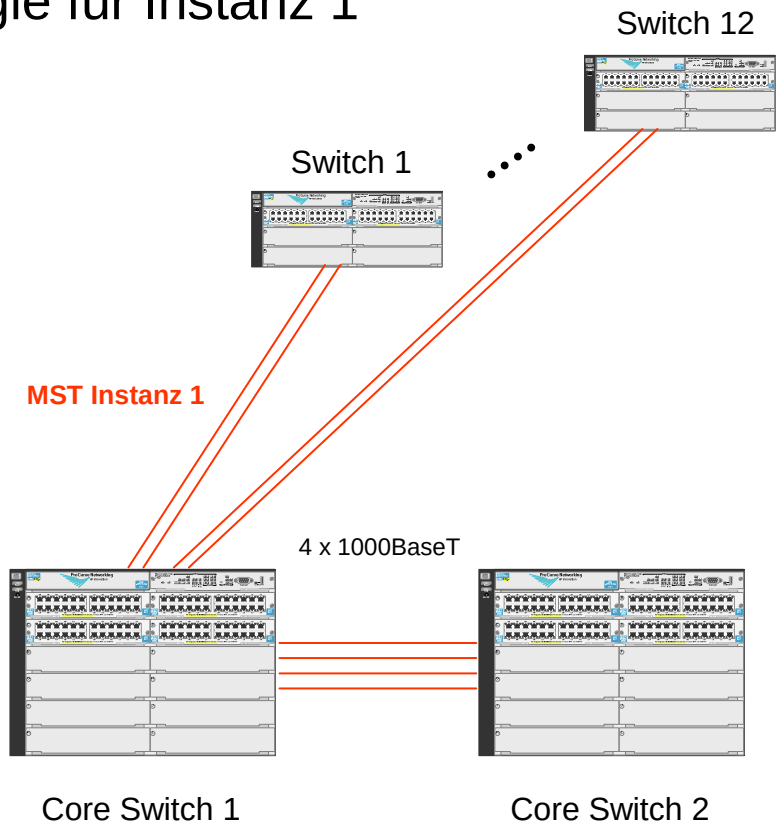
Logische Topologie



ingentive.networks

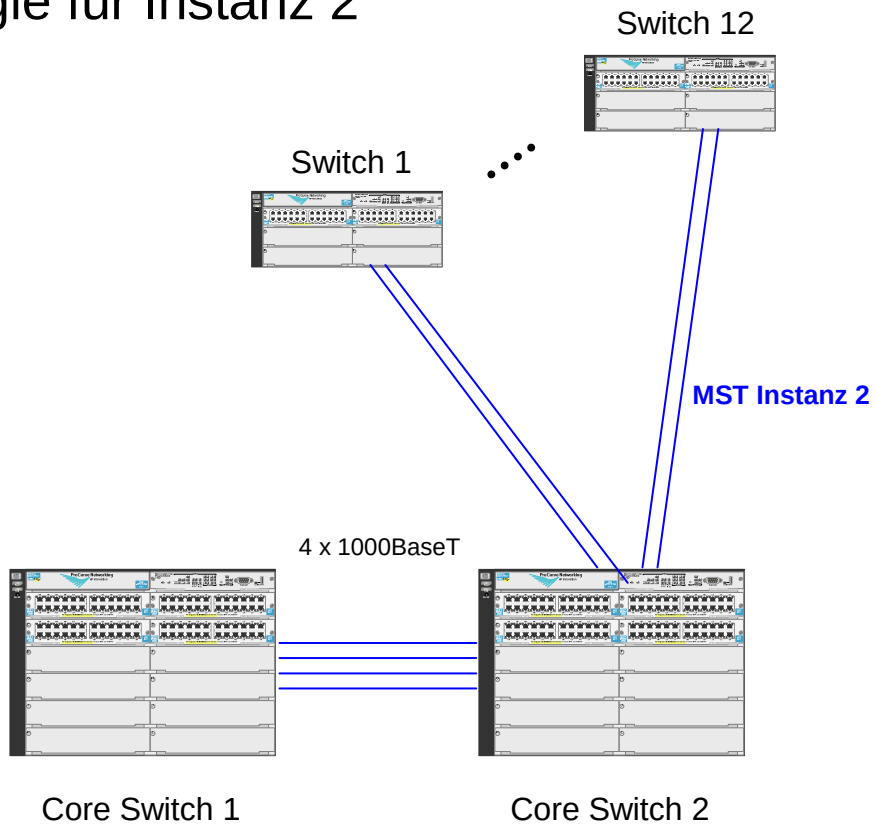
Logische Topologie

Logische Topologie für Instanz 1



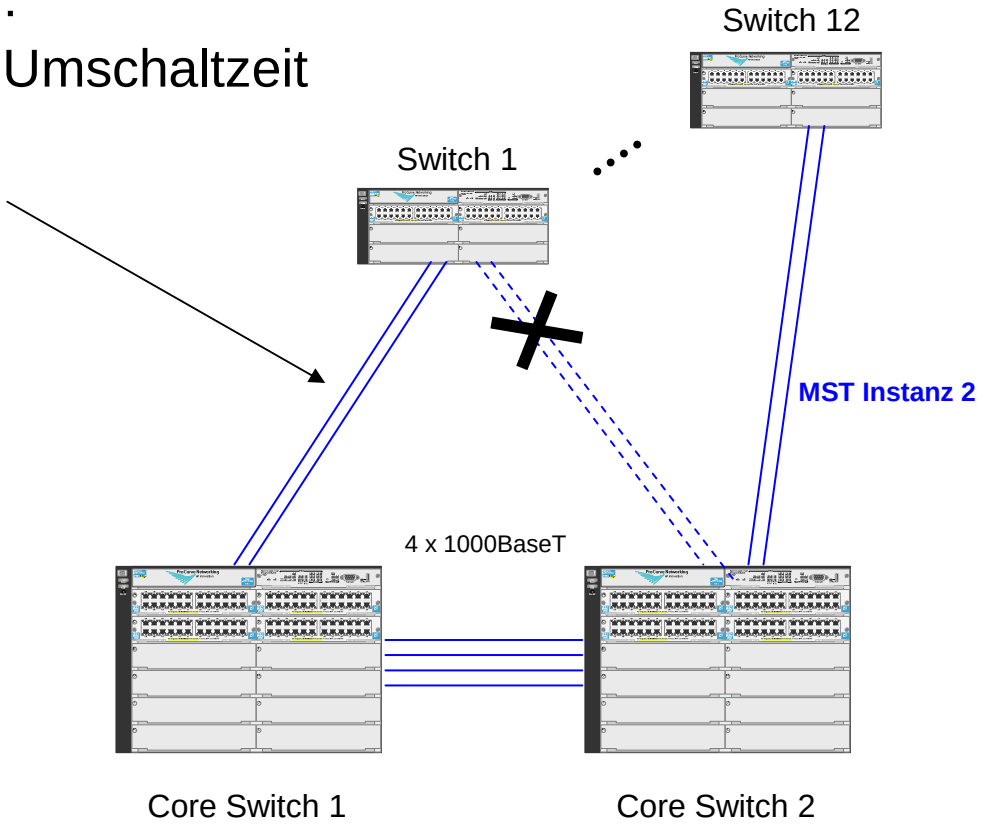
Logische Topologie

Logische Topologie für Instanz 2



Logische Topologie

Vorteile MST:
Im Fehlerfall Umschaltzeit
< 1 Sekunde

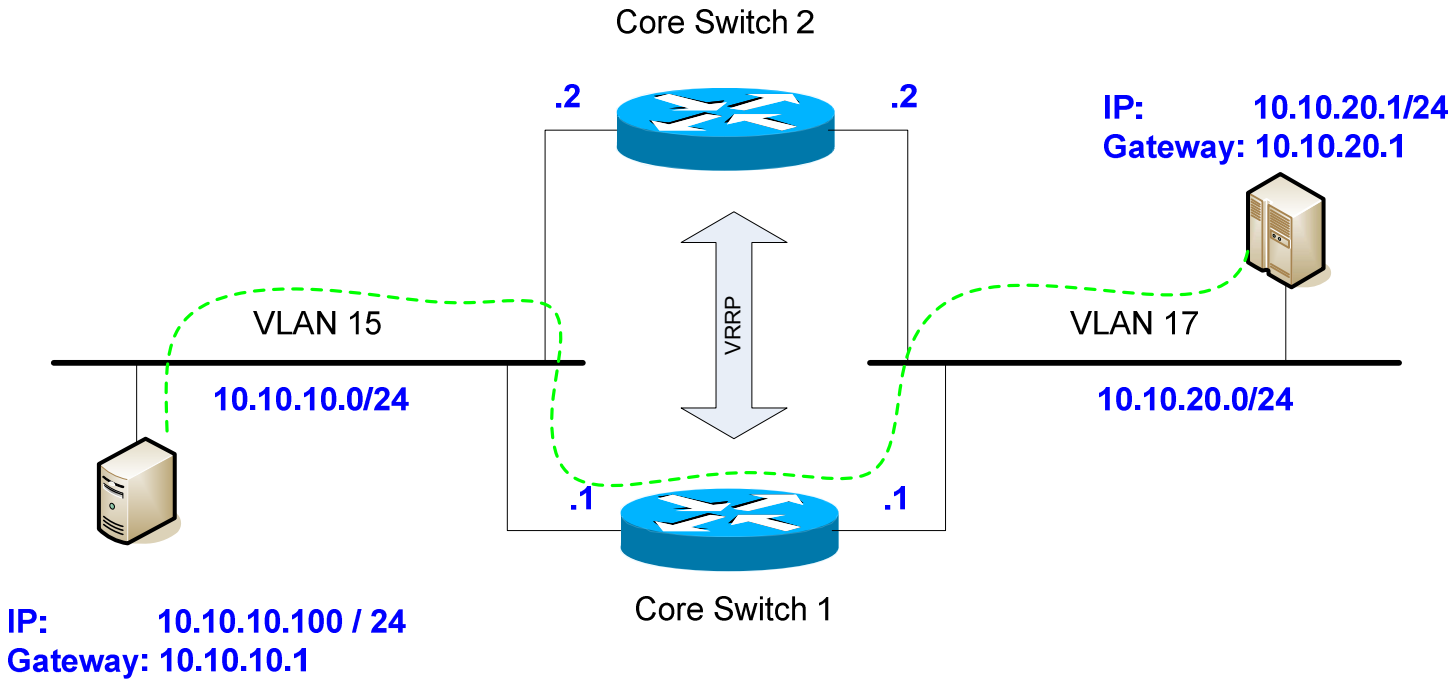


IP Design

- 30 verschiedene IP Subnetze
- Etagenübergreifende VLANs
- Neue Definition von IP Adress Bereichen
- Server IP Netze werden teilweise migriert (Lizensierung auf IP Adresse)
- Unsichere Netzwerke werden auf Firewall terminiert

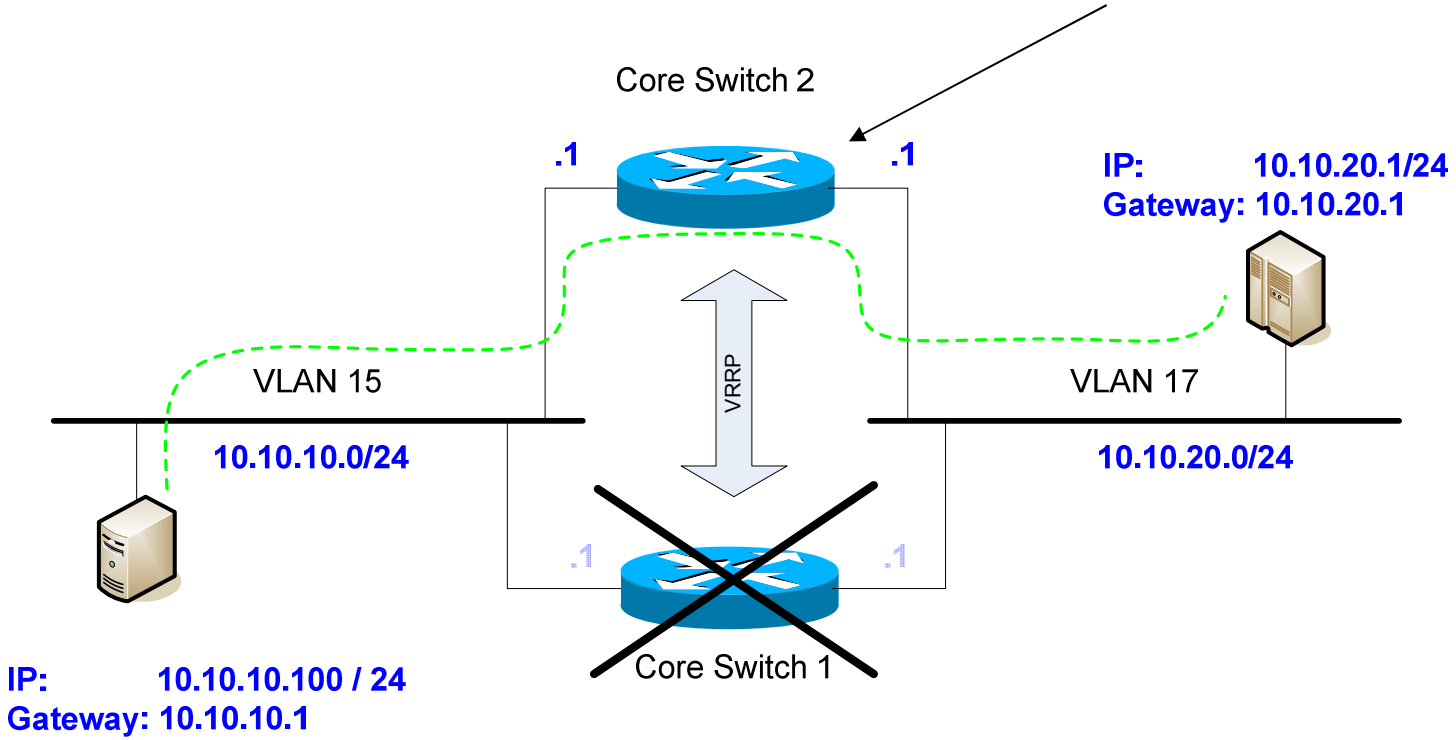
IP Design

VRRP Instanz für jedes VLAN



IP Design

Im Fehlerfall < 3 Sekunden Umschaltzeit auf zweiten Router

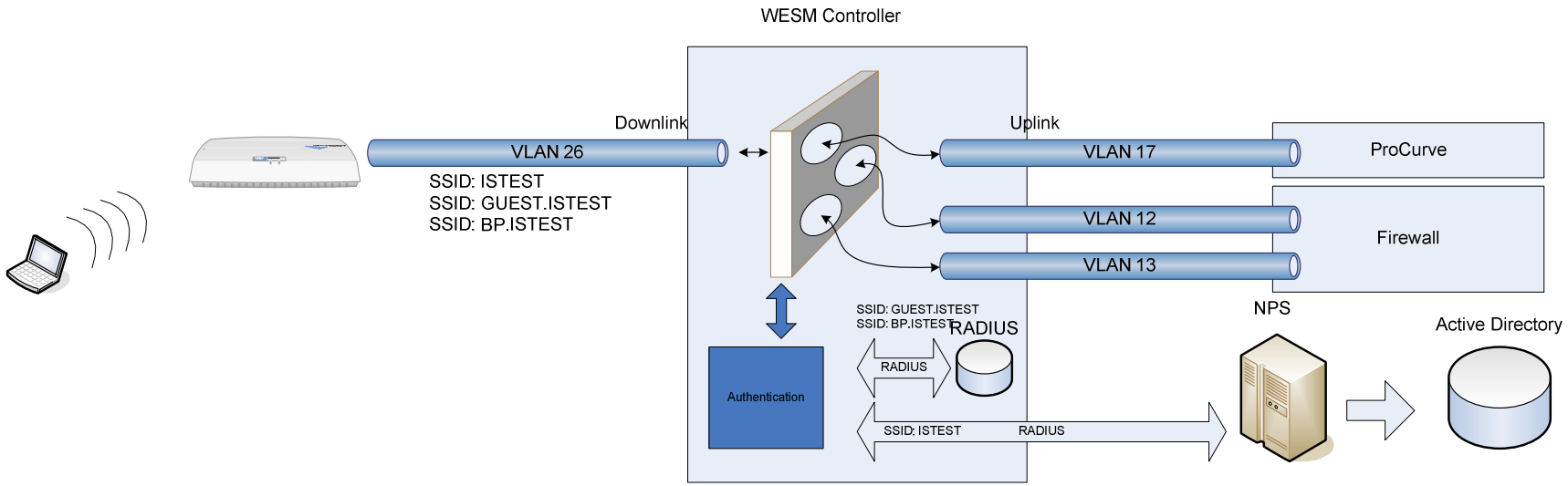


WLAN Zugang

- WESM Controller kontrolliert und verwaltet die Radio Ports
- Zentrales Management aller Radio Ports
- Verschiedene SSID für unterschiedliche Profile
  - Mitarbeiter
  - Schnurlose IP Telefone
  - Gäste mit zeitlich limitiertem Zugang
  - Businesspartner mit zeitlich limitiertem Zugang

WLAN Zugang

Authentisierung und Routing abhängig der SSID



WLAN Zugang

Rezeption kann Gastzugänge eigenständig generieren

Username und Passwort können automatisch generiert werden und timen nach definierter Zeit automatisch aus

802.1X Port Authentisierung

- Zugangskontrolle durch 802.1X Protokoll
- Windows 2008 NPS dient als RADIUS Server
- VLAN wird dynamisch durch RADIUS zugewiesen
- Geringer Verwaltungsaufwand: Benutzername und Passwort liefert Active Directory
- Bei fehlgeschlagener Authentisierung nur Gast VLAN Zugriff
- Authentisierung geschieht im Windows Anmeldeprozess und ist somit für Benutzer transparent

MAC Authentisierung

- Zugangskontrolle durch Nicht-802.1x fähige Geräte (z.B. Drucker)
- Authentisierung erfolgt anhand der MAC Adresse
- Verwaltungsaufwand: MAC Adressen im AD einpflegen
- Mögliche Angriffsszenarien durch „MAC Address Spoofing“ wird durch Accesslisten auf Routing Switch gemildert

Weitere Features

Einsatz von weiteren Features zum Gewinn von Stabilität und Sicherheit:

- DCHP Snooping
- Accesslisten
- Bridge PDU Guard
- Loop Guard
- UDLD
- Port Security

Voice over IP

- Telefonielösung von Avaya
- PoE nach 802.3af Standard auf allen Ports
- Avaya Telefone markieren mit DSCP
- VoIP Codec nach G.711 Standard ~ 90kbps Datenstrom
- QoS Konfiguration mit 4 Hardware Queues
- 40 Telefone pro Etage

Zugesicherte Bandbreite für VoIP = 40 * 90 kbps = 3,6 Mbps

Managementlösung

- ProCurve Manager als zentrale Managementplattform
- Läuft in virtueller Maschine auf Windows 2003 Server
- Überwachung der Geräte
- Auswertung der Auslastung (Top Talker)
- Sammeln von Konfigurationsdateien
- Zentraler Firmware Update

Ingentive Networks

Ingentive Networks liefert

- Konzepterstellung und Herstellervergleich zwischen HP ProCurve© und Cisco Systems ©
- Feinkonzept zur Umsetzung
- Konzept für Testaufbau
- Implementierung des Testaufbaus
- Implementierung der Produktionsumgebung