Neues vom DV-Netzwerk in Hamburg

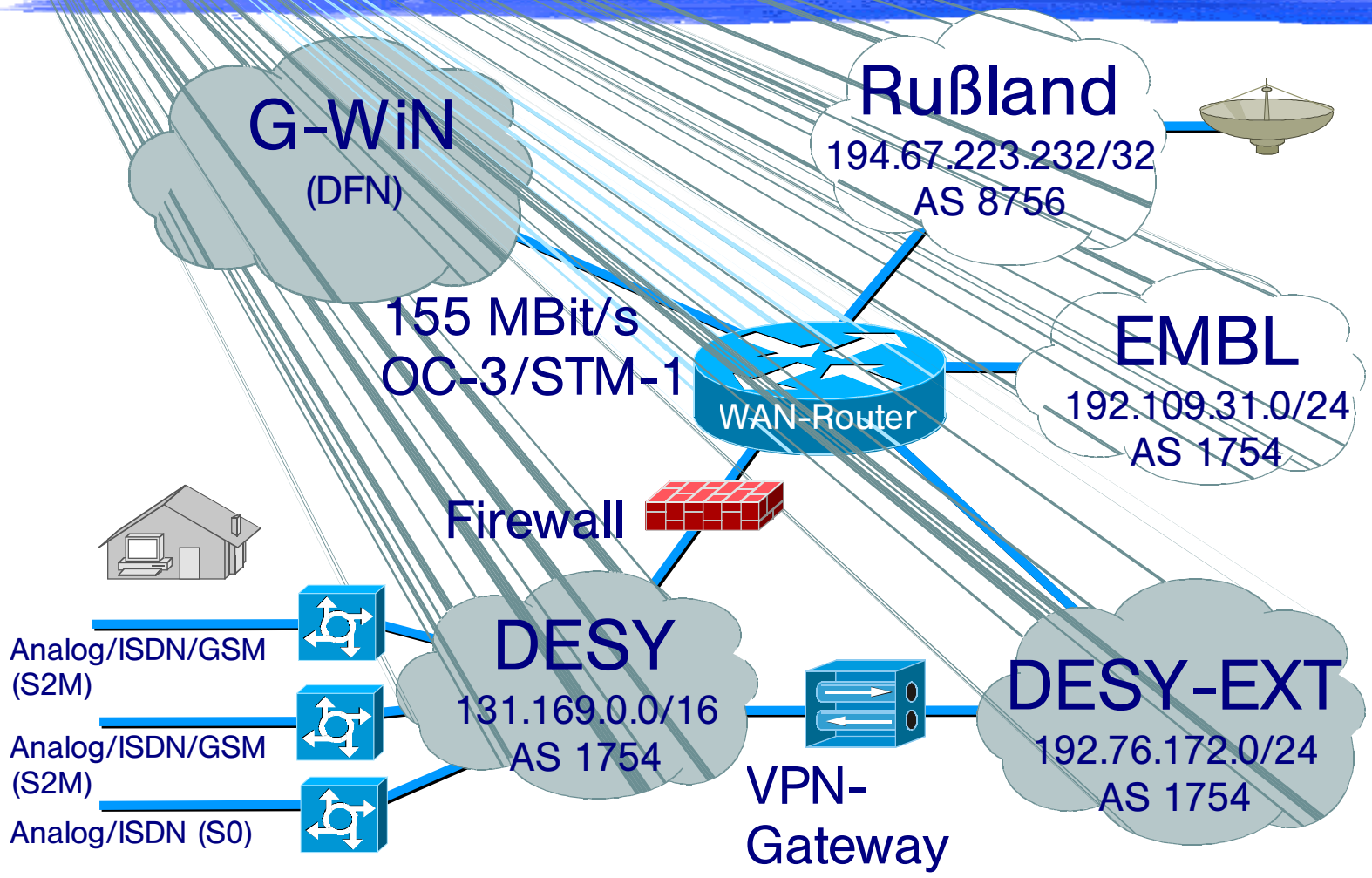
Inhalt

- Das DESY HH Datennetz
  - Design, Status
- Services
  - dynamic VLANs, DHCP, WLAN, VPN
  - Remote Access
- Netzwerk Management
  - QIP, SPECTRUM, Network Health, Cisco Works
- Zukunft

Die Herausforderung

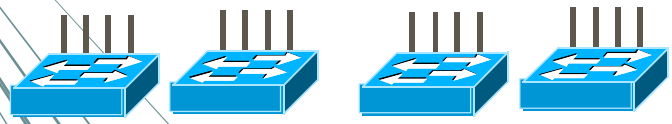
- Verfügbarkeit und Sicherheit
- Steigender Bandbreitenbedarf (Gigabit, …)
- Multimediadienste
  - Voice over IP, Videokonferenzen, ...
- Daten-, Sprach- und Video-Integration
- Echtzeitfähigkeit, Quality of Service
- Mobiles Computing

Das DESY-HH Datennetz



Modulares Netzwerk Design

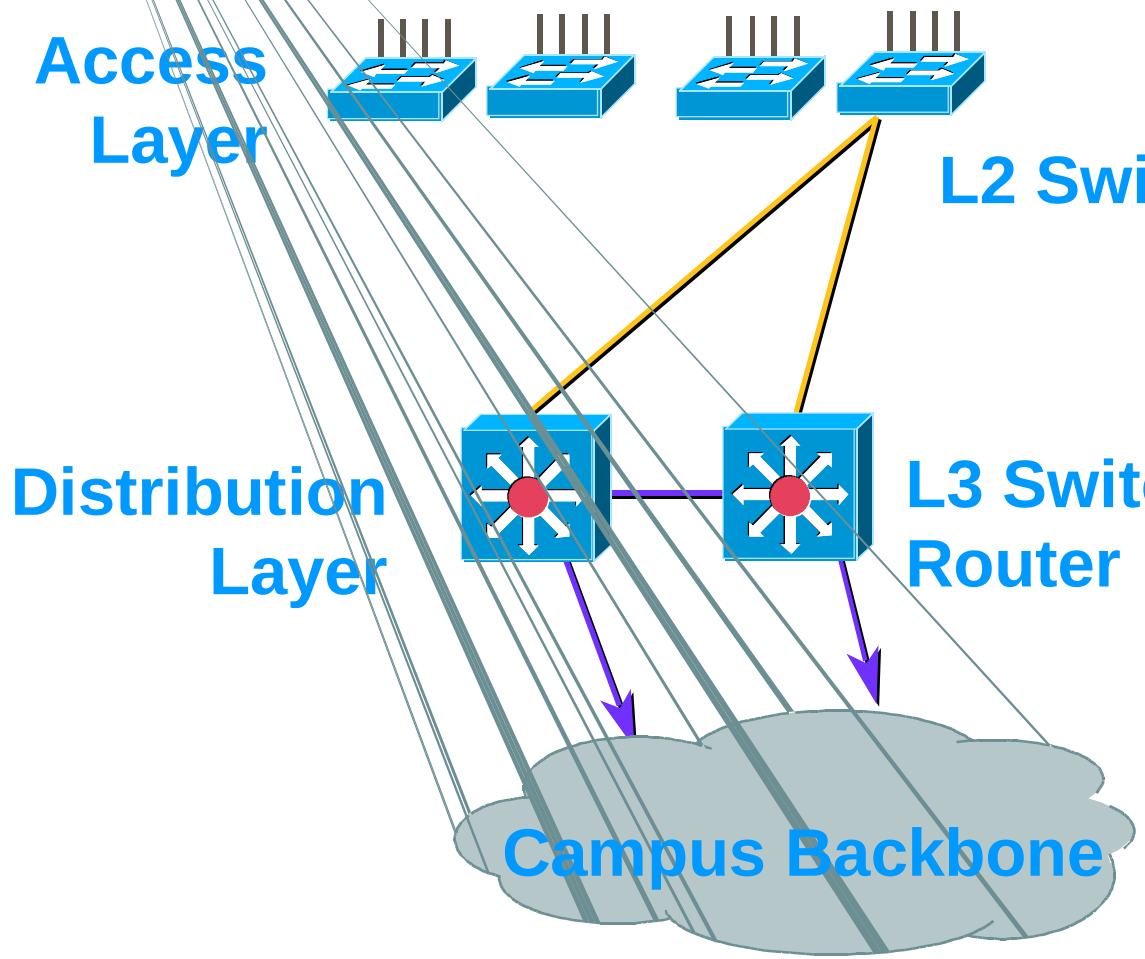
Access Layer



L2 Switch

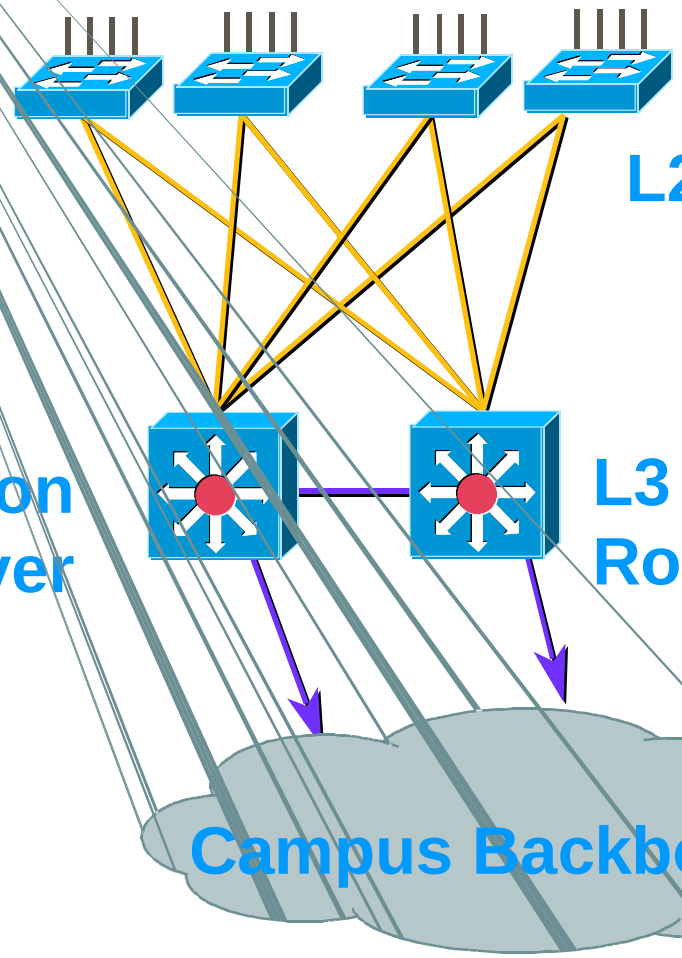
Campus Backbone

Modulares Netzwerk Design



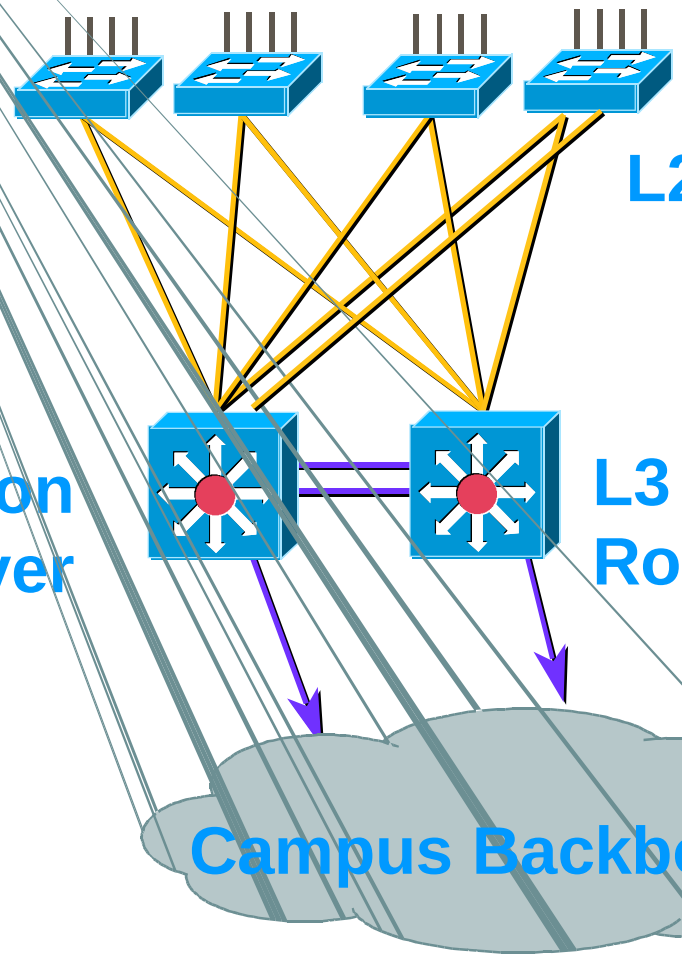
- Load Balancing und Redundanz zum Verteiler

Modulares Netzwerk Design



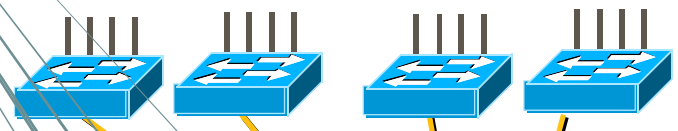
- Load Balancing und Redundanz zum Verteiler

Modulares Netzwerk Design



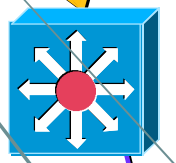
- Load Balancing und Redundanz zum Verteiler
- L2 Switch
- Scalable Trunking FE, FEC, GE, GEC
- L3 Switch, Router

Modulares Netzwerk Design



Access Layer

L2 Switch



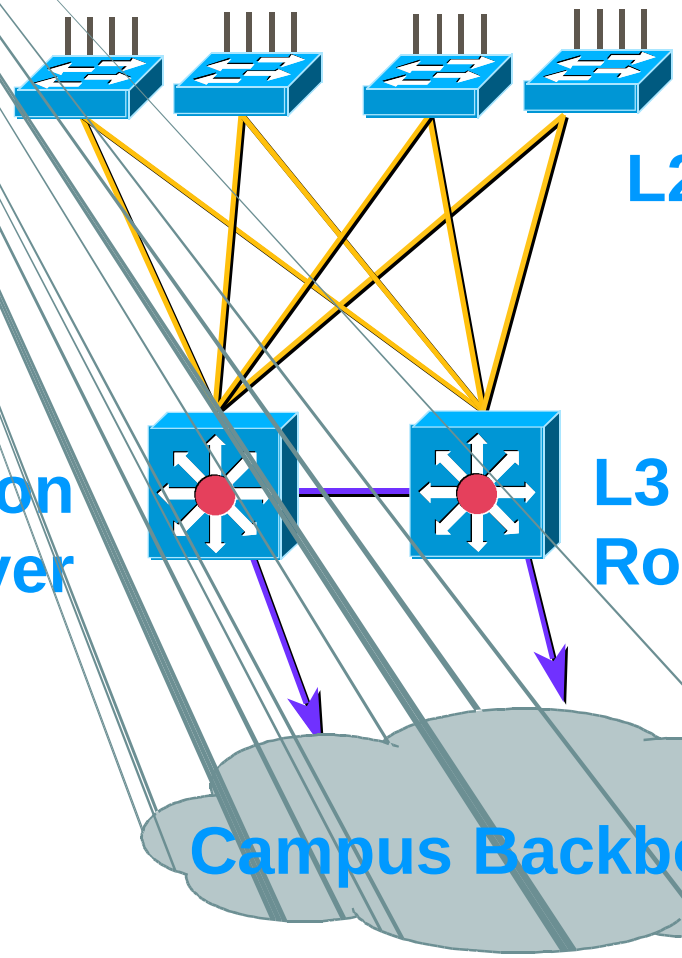
Distribution Layer

L3 Switch, Router

Campus Backbone

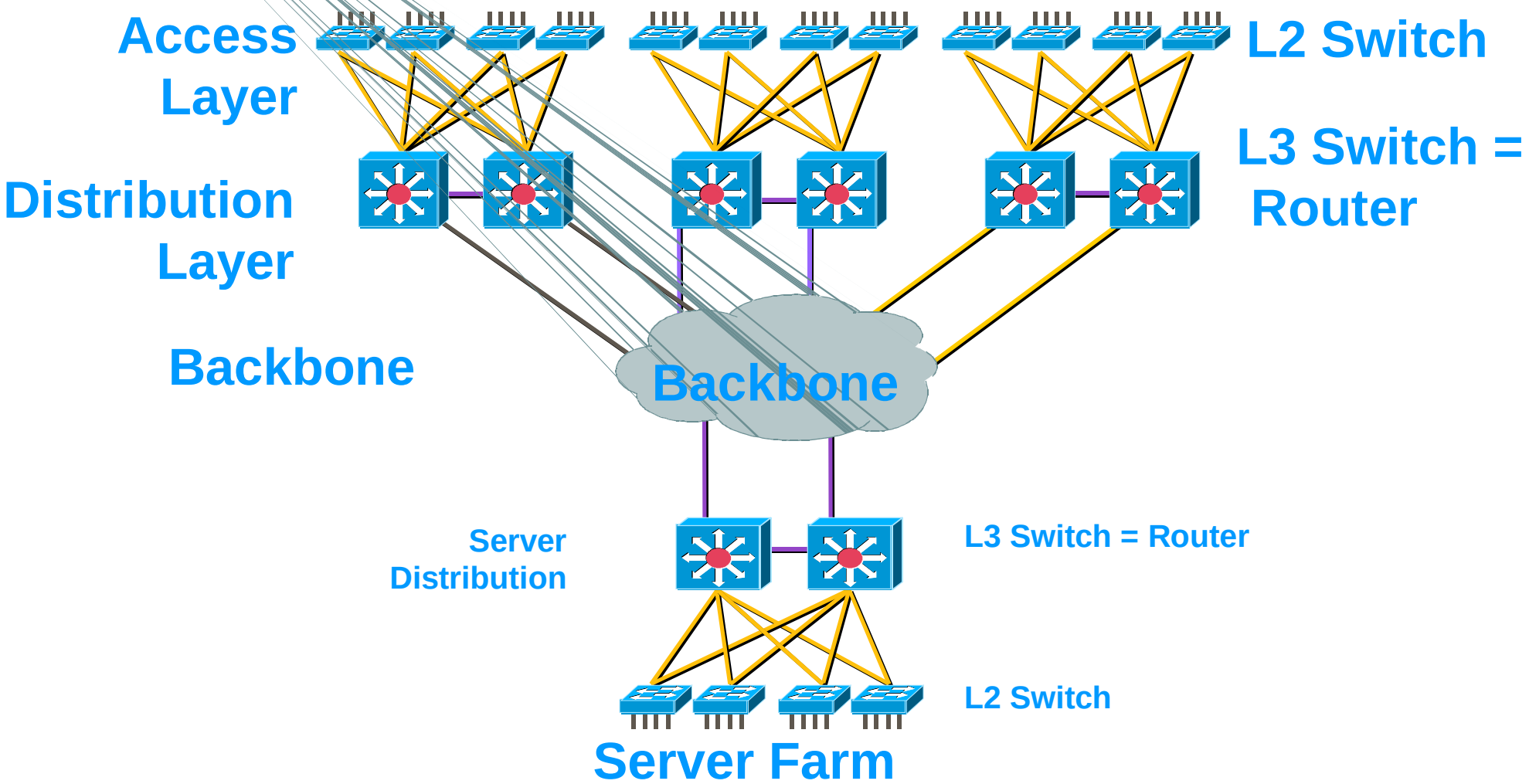
- Load Balancing und Redundanz zum Verteiler
- Scalable Trunking FE, FEC, GE, GEC
- Fast Failover mit HSRP

Modulares Netzwerk Design



- Load Balancing und Redundanz zum Verteiler
- Scalable Trunking FE, FEC, GE, GEC
- Fast Failover mit HSRP

Modulares Netzwerk Desing



Status Datennetz DESY-HH

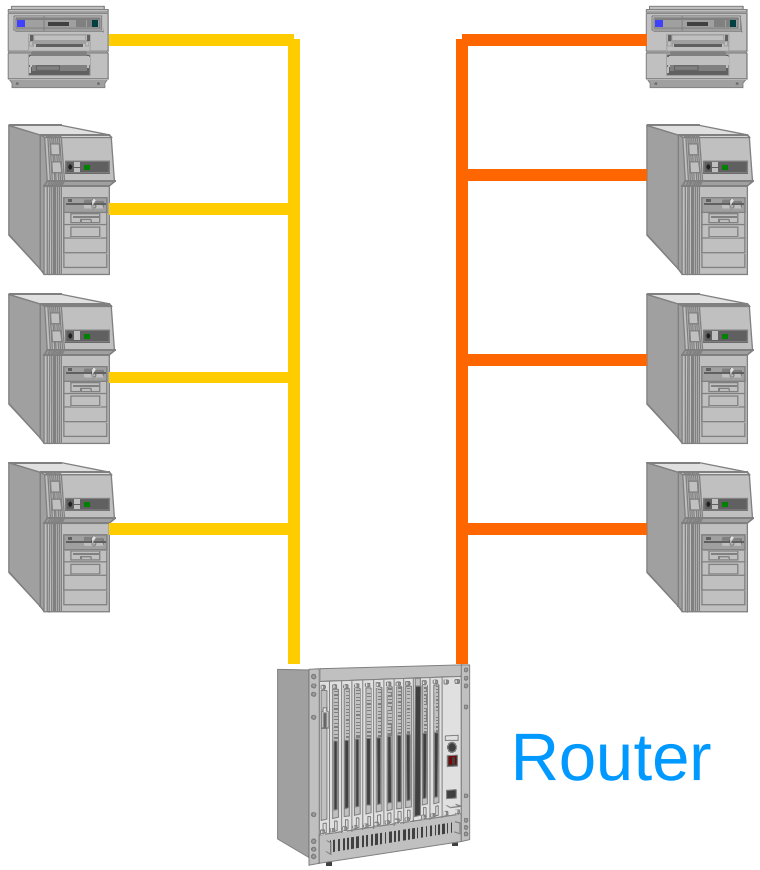
- Migration nahezu abgeschlossen
  - 5274 10/100 Ports
  - 287 GE - Ports (235 SX, 52 LX)
  - 8 GE - Kupferports
    - Spezialanwendung, nicht im Büroumfeld vorgesehen
- Nächste Migrationen
  - Universitätsinstitute
  - TTF

’Besonderheiten’ im Datennetz DESY-HH

- Dynamische VLANs
  - zentrale Registrierung aktiver Komponenten
  - ermöglichen Gästenetzwerk
- Fokus auf Mobilität
  - Nutzung Dynamischer VLANs
  - Alle linken Anschlussdosen sind aktiv/gepatcht und laufen im dynamischen Modus
  - Rechte Anschlussdosen werden nach Bedarf geschaltet

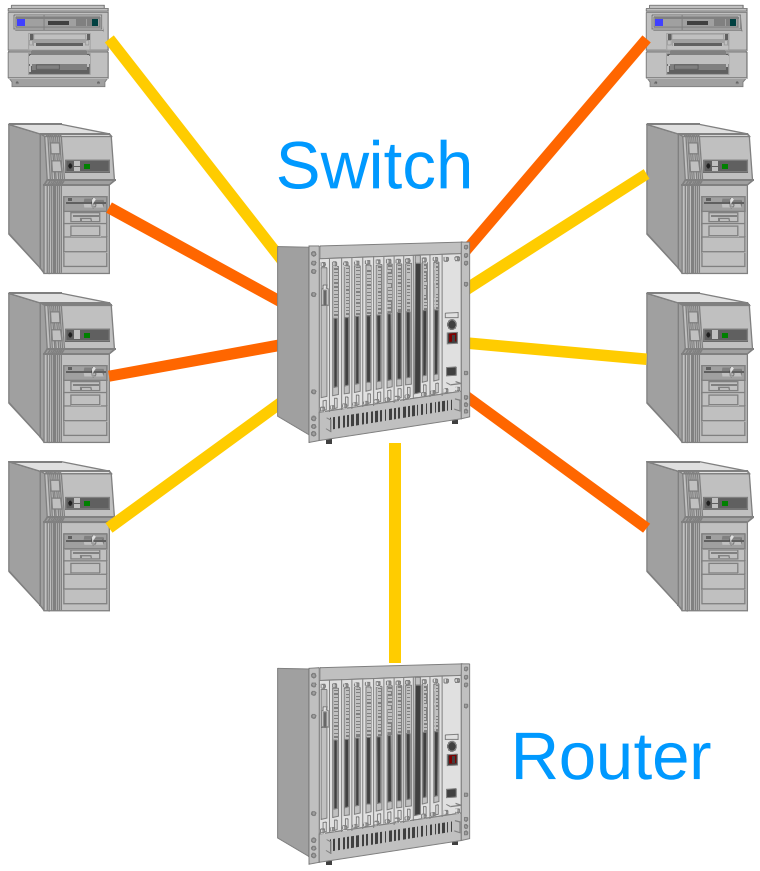
Virtual LANs (VLANs)

- In klassischen Datennetzwerken wird das Subnetz über die physikalische Topologie festgelegt



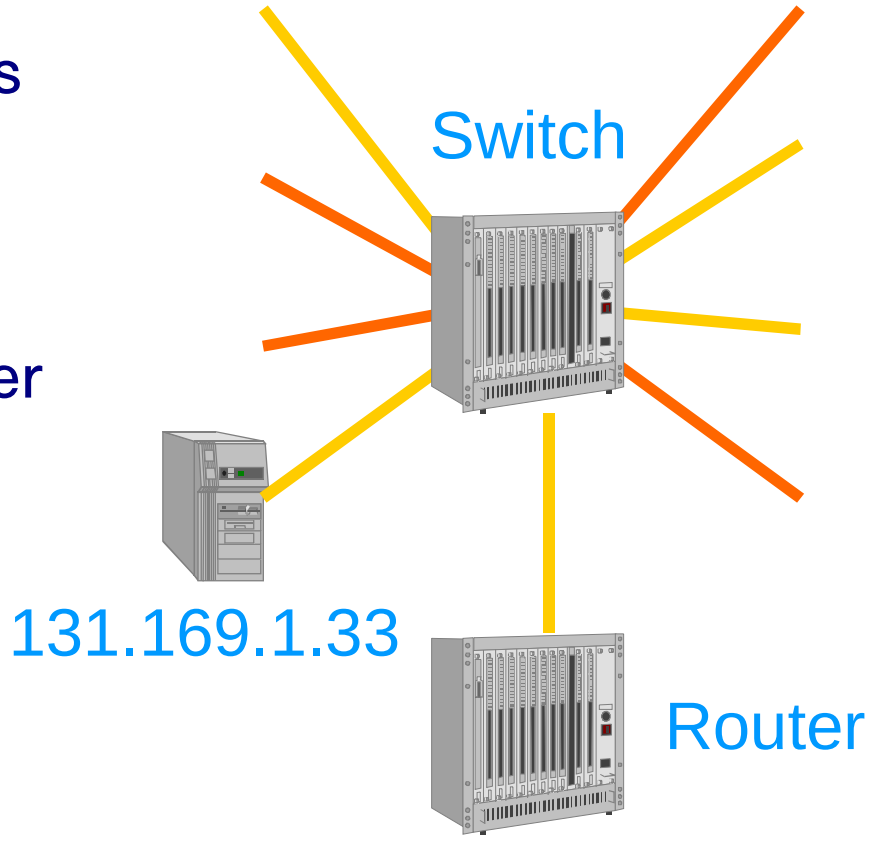
Virtual LANs (VLANs)

- In geswitchten Netzwerken erfolgt die Subnetzzugehörigkeit über eine logische Segmentierung
  - Standard IEEE 802.1Q
- VLAN Zuweisung über
  - Switch Port (Layer 1)
  - MAC Address (Layer 2)
  - Protocol Type (Layer 2)
  - IP Subnet Address (Layer 3)
  - Application (Layer 4)



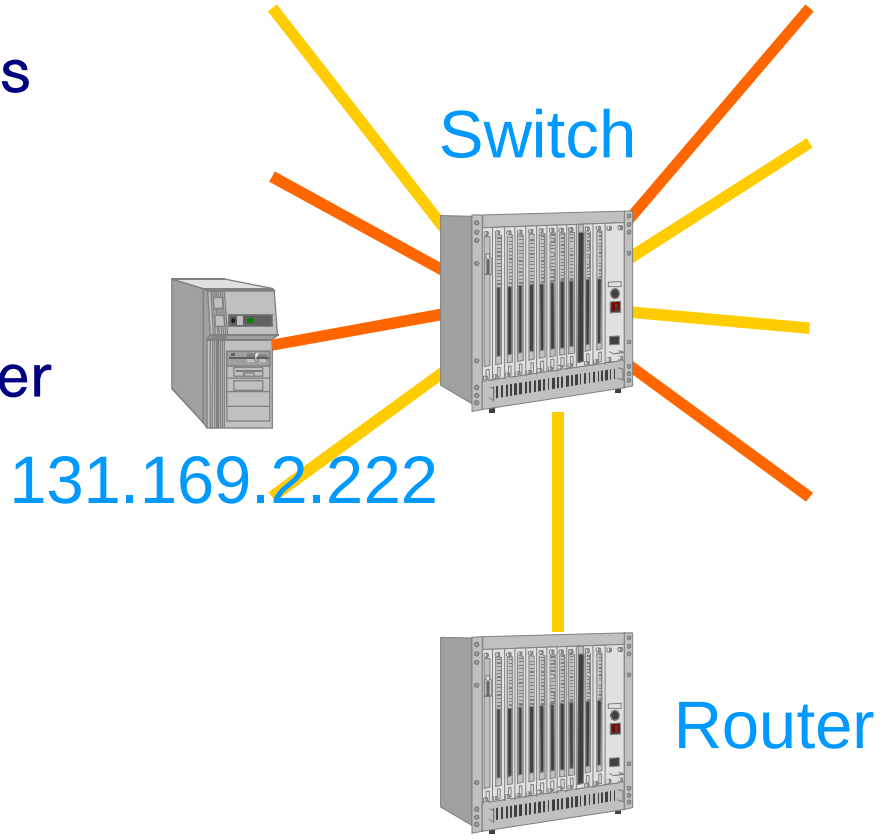
Mobile User

- Über DHCP
  - IP-Adresse des Gerätes ändert sich
  - Einfach zu implementieren
  - Security Policies schwer umzusetzen



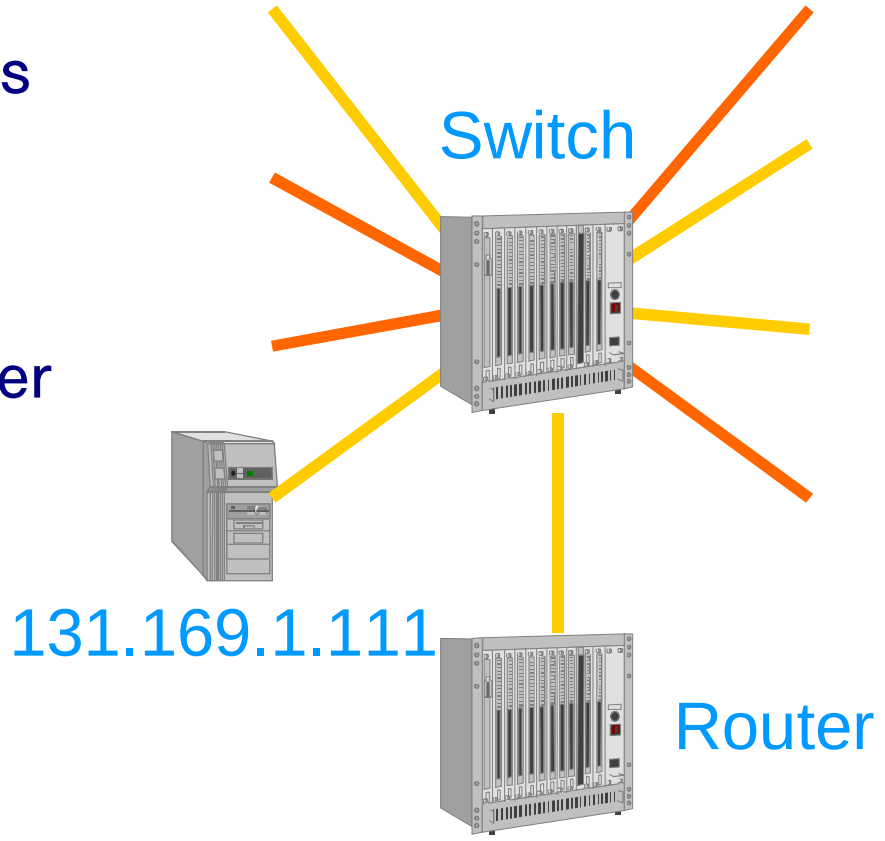
Mobile User

- Über DHCP
  - IP-Adresse des Gerätes ändert sich
  - Einfach zu implementieren
  - Security Policies schwer umzusetzen



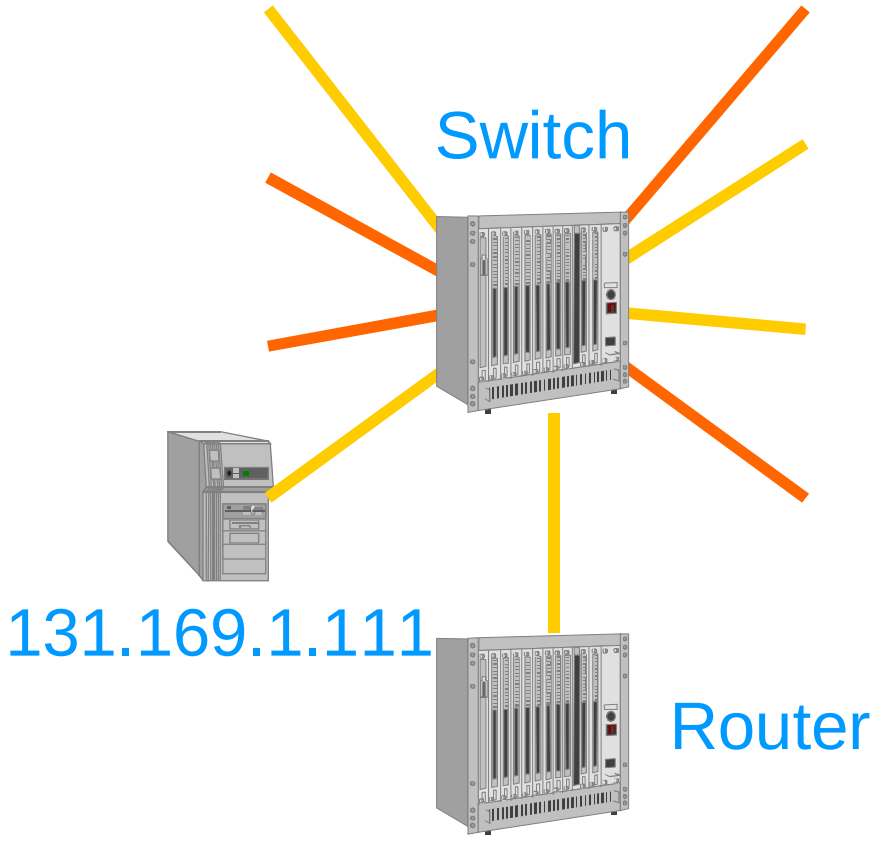
Mobile User

- Über DHCP
  - IP-Adresse des Gerätes ändert sich
  - Einfach zu implementieren
  - Security Policies schwer umzusetzen



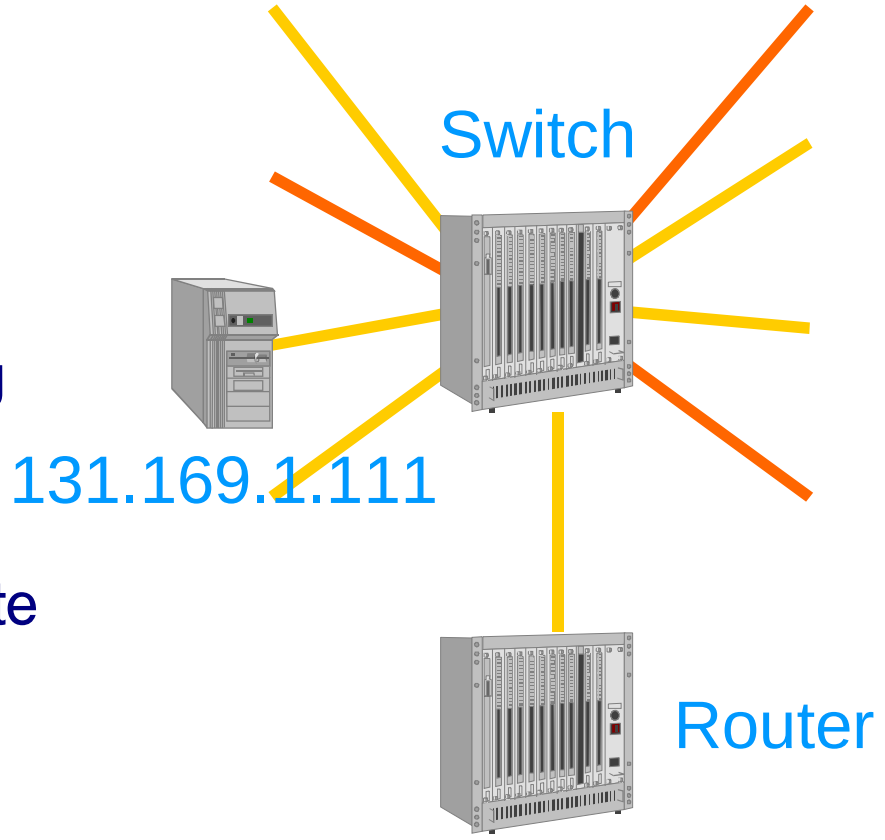
Mobile User

- Über Dynamic VLANs
  - IP-Adresse ist statisch
  - Filter auf IP-Ebene können angewandt werden



Mobile User

- Über Dynamic VLANs
  - IP-Adresse ist statisch
  - Filter auf IP-Ebene können angewandt werden
  - Erfordert Registrierung von Geräten
    - ‘Zugangskontrolle‘
    - Unregistrierte Geräte bekommen ‘Default VLAN‘ -> Gästesubnetz



Mobilität, dVLANs

- Produktiv seit Februar 2001
- Beste Erfahrungen, keine Ausfälle
- Zentrale Datenbank mit registrierten MAC-Adressen, 2 Server (Switches)
- Policies möglich, bisher nicht im Einsatz
- Wichtige Dienste werden über statische Ports gefahren
- Alle linken Anschlussdosen aktiv
- VLAN Modus ist pro Port definierbar

DHCP

- Zunächst im Gästenetzwerk eingesetzt
- Produktionsbetrieb auf allen Netzen seit 1.5.
  - Mobile Geräte leichter zu administrieren
- Verwaltung erfolgt über QIP
- Bisher nur Statisches DHCP erlaubt
- DHCP Template beinhaltet
  - Domain, DNS-Server, WINS-Server, Netzmaske, Gateway, Broadcast Adresse
  - Mailsserver, Timeserver, etc bisher nicht berücksichtigt

WLANs @ DESY

- Bisher abgedeckte Bereiche
  - Seminarräume 1b
  - Hörsaal inklusive Foyer
- Produktionsbetrieb seit 1.4.2002
- Kartenausleihe über UCO
  - Unterschrift des Accountsupervisor
  - Zeitliche Befristung der Ausleihe (1 Monat)
  - Generelle Beschaffung über BAs

WLANs @ DESY

- Technische Details
  - 802.11b Standard (6 - 7 MBit/s effektiv)
  - Je 2 Accesspoints entsprechend 2er Netze
    - Gästenetzwerk, keine Registrierung, keine ‘SSID‘, IP-Adresse über DHCP
    - Subnet 12, Registrierung erforderlich, ‘SSID‘, IP-Adresse über DHCP
    - keine Verschlüsselung
- Nächste Bereiche
  - Phase 1:Öffentliche Seminarräume
  - Phase 2: Experimentierhallen

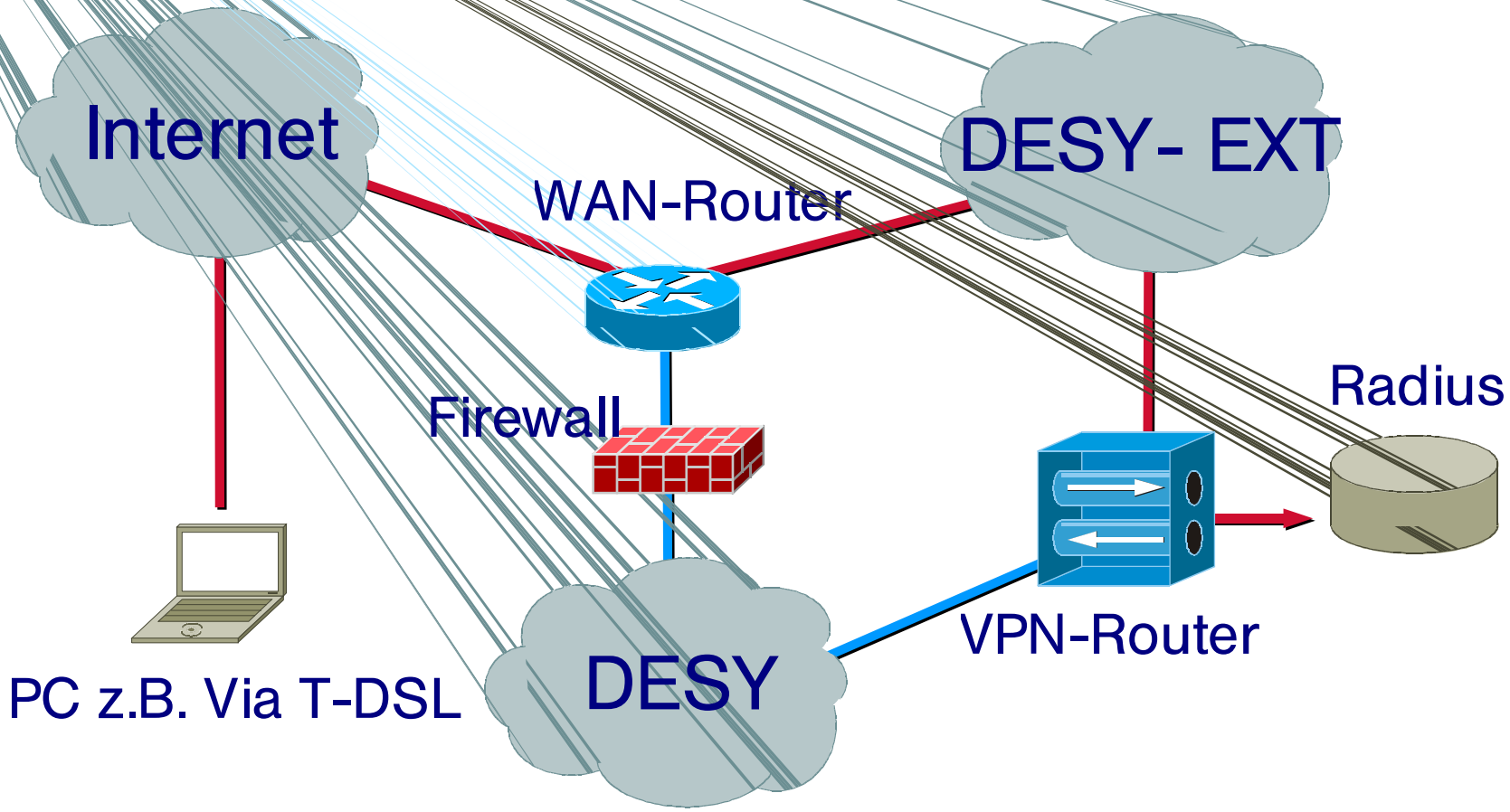
WLANs @ DESY

- Kantine (3x)
- Lab. 1 (Kopfbau, Direktorium, 292)
- Seminarraum 2
- RZ
- Videokonferenzräume (2x)
- 30b (4. + 5. Stock)
- 30 5.Stock
- HASYLAB (25f-456, 25b-113, 25f Foyer)
- 55-204, 55a-110
- TTF Reinraum

Virtual Private Networking (VPN)

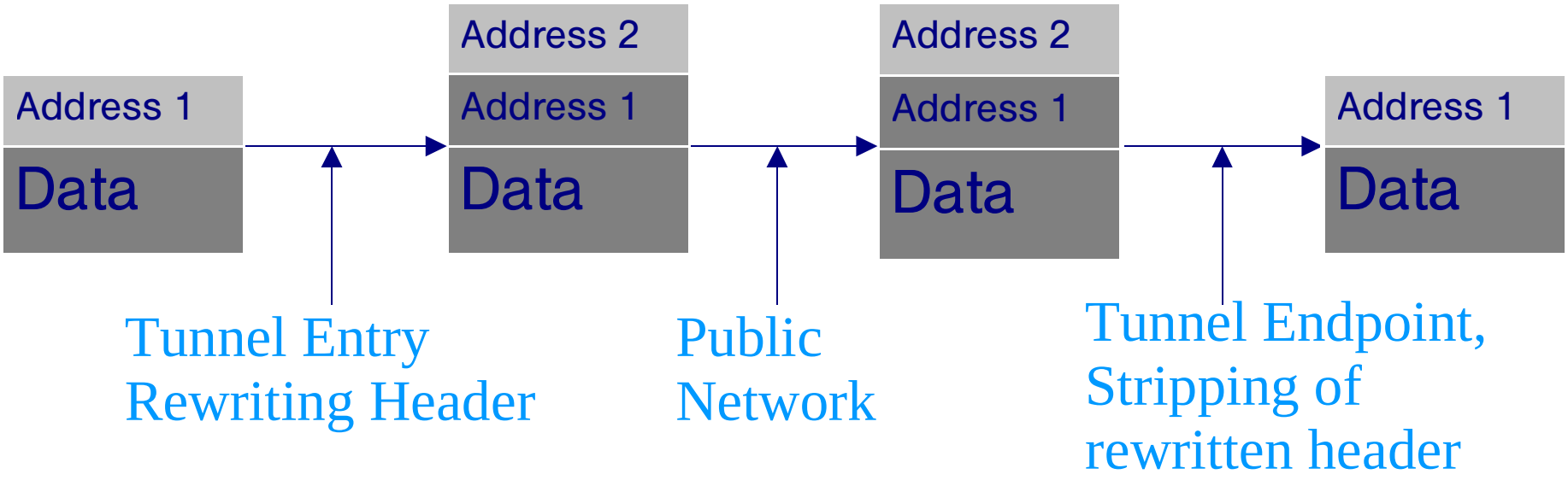
- Problem: DESY IP-Adressen sind nicht überall verfügbar, damit auch nicht immer Zugriff auf DESY-Intranet möglich (T-DSL)
- Lösung: Virtual Private Networks
  - Gerät bekommt virtuelle DESY IP-Adresse
  - sicherer verschlüsselter Tunnel über das Internet zum VPN-Gateway
  - Tunnelprotokoll IPSec (IPSec Group nötig)
- Autorisierung gegenüber Radius-Server (DESY RAS Account)

Virtual Private Networking (VPN)



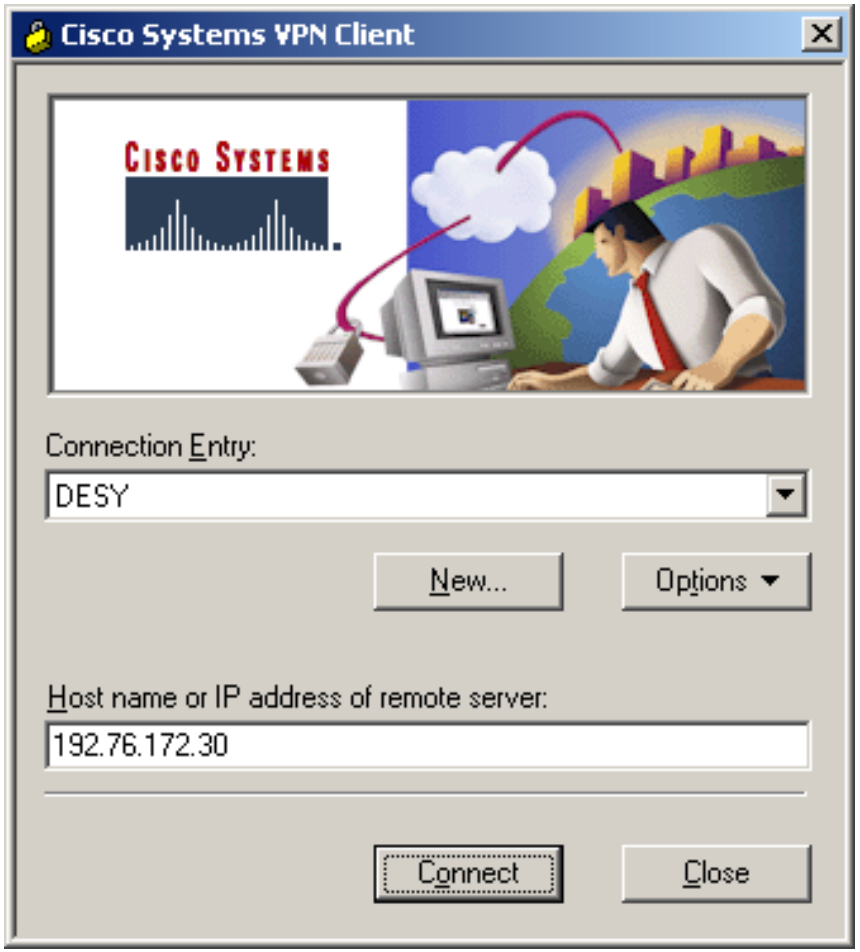
IP-Tunnel und VPNs

- Idee: Ein IP Paket wird in einem weiteren Paket ‘verpackt‘



IP-Tunnel und VPNs

- Ein VPN ist sehr einfach zu benutzen:
  - Gerät anschalten und IP Adresse konfiguriere (z.B. über DHCP, ...)
  - VPN Client Software starten und Authentifizierung durchführen
  - That‘s it!



DESY-HH VPN

- IT-interner Testbetrieb seit Anfang April
- VPN Client Software + RAS Account nötig
- Das öffentliche Netz wird als Erweiterung des privaten Netzes genutzt
- Ein VPN bietet zusätzliche Sicherheit durch
  - Authentifizierung
  - Autorisierung
  - Verschlüsselung
- IPv6 beinhaltet Mobile IP !!!

Remote Access Technologie

- Große Anzahl unterschiedlichster Technologien verfügbar um IP-Verbindungen herzustellen
  - ISDN, Analog, GSM, ISP, ...
  - Unterschiedlich bezüglich
    - Geschwindigkeit
    - Adressraum
    - Kosten
    - Sicherheit

ISDN, Analog

- Was wird benötigt
  - Modem
  - Remote Access Account (z.B. am DESY)
    - Username, Passwort, Telefonnummer
- Geschwindigkeit:
  - Analog: 56 kBit/s (~10 Sekunden für www.desy.de)
  - ISDN: 64/128 kBit/s (~10/5 seconds)
- Kosten:
  - 0,01-0,02 €/min, unabhängig vom Volumentransfer

ISDN, Analog (2)

- IP Adresse:
  - 131.169.X.X möglich, innerhalb DESY
- Sicherheit
  - Datenpakete werden über das öffentliche Telefonnetz und nicht das öffentliche Internet gesendet
  - Calling Line Identification (CLID)
- Andere Vorteile:
  - Access Service kann und wird am DESY angeboten
  - Callback möglich
  - Weltweite Verfügbarkeit, ein Telefonanschluss genügt

DSL

- Was wird benötigt:
  - DSL Modem
  - DSL-Provider (z.B. German Telekom)
  - ISP Account (z.B. T-Online)
- Geschwindigkeit:
  - 128 kBit/s upstream (< 1 Sekunde)
  - 768 kBit/s downstream (< 1 Sekunde)
- Kosten
  - Flatrate ~25 €/Monat oder 0,01 – 0,02 €/Min

DSL (2)

- IP Adresse
  - x.x.x.x, außerhalb DESY
- Sicherheit:
  - Daten werden über öffentliches Netz gesendet
- Bemerkungen:
  - Es wird keine Möglichkeit geben diesen Dienst am DESY anzubieten!

GSM, HSCSD

- Was wird benötigt
  - Mobiltelefon + Vertrag (T-D1, Vodafone, ...)
  - Remote Access Account (z.B. DESY)
- Geschwindigkeit
  - GSM: 9.6 kBit/s (~75 Sekunden)
  - HSCSD (High Speed Circuit Switched Data)
    - „GSM Kanalbündelung“
    - 14.4 kBit/s pro verfügbarem Kanal,
      typisch 3-4 mit modernen Geräten = 57,6 kBit/s

GSM, HSCSD (2)

- Kosten:
  - 0,15 €/Min (GSM, z.B. D1), HSCSD vergleichbar
- IP Adresse
  - 131.169.x.x möglich, innerhalb DESY
- Sicherheit:
  - Vergleichbar mit Analog oder ISDN Zugängen
- Bemerkungen:
  - Access Service wird vom DESY angeboten
  - Kein HSCSD von T-D1 verfügbar

GPRS (Global Packet Radio Service)

- Was wird benötigt
  - GPRS fähiges Mobiltelefon
  - Vertrag (z.B. T-D1, Vodafone, ...)
  - ISP Account
- Speed
  - 9,05/**13.4**/15,6/21,4 kBit/s pro Kanal (3-4)
- Kosten:
  - 0,01 €/kBytes (www.desy.de = 1 €)

GPRS (2)

- IP Adresse:
  - x.x.x.x, außerhalb DESY
- Sicherheit
  - Vergleichbar DSL
- Bemerkungen
  - Packet Switched Network
  - Bezahlung pro transferiertem Volumen, nicht über Verbindungsdauer, ”always on“
  - Trigger für IPv6

Internet Service Provider

- Was wird benötigt:
  - Account (z.B. AOL, T-Online, ...)
- Speed:
  - Abhängig von Verbindungstechnologie
- Kosten:
  - 1-2 Cent/Min, Flatrates

Internet Service Provider (2)

- IP Adresse:
  - x.x.x.x, definitiv außerhalb DESY
- Sicherheit:
  - Da das eigenen Gerät verwendet wird
    - Kontrolle über installierte Software
    - Benötigte Software kann installiert werden
    - Volle Konfigurationsmöglichkeit
  - IP Traffic läuft über öffentliche Netze

Internet Cafe, Konferenz

- Vergleichbar mit ISP aber
  - Unbekannte Gerät
    - Welche Software ist verfügbar?
  - Nicht alles konfigurierbar
  - Sicherheit:
    - Browser behält Historie besuchter Webseiten
    - Was bleibt in den Caches (Passwörter, Mails, etc.)
    - Tastatur Logging?

RAS Technologie Vergleich

	Speed (kBit/s)	Kosten (€/Min)	Am DESY verfügbar	IP Adresse
Analog/ISDN	56 Analog 64/128 ISDN	0,01 – 0,02	Yes	131.169.x.x
DSL	128 Upstream 768 Downstream	0,01 – 0,02 25€/Monat	No	x.x.x.x
GSM, HSCSD	9,6 GSM < 57,6 HSCSD	0,15	Yes	131.169.x.x
GPRS	< 53,6	0,01 €/kBytes	No	x.x.x.x
ISP	Unterschiedlich	0,01 – 0,02	No	x.x.x.x
Cafe	Unterschiedlich	2,5 – 5 €/h	No	x.x.x.x

RAS Technologien

- Unterschiedlichste Technologien für IP-Zugänge verfügbar
  - Geringe Bandbreite bei hoher Mobilität
  - Hohe Bandbreite bei geringer Mobilität
- Generelles Problem: Die benutzte IP-Adresse ist nicht im DESY Intranet
- Die beste Lösung für mobile Geräte ist ein VPN welches sich am DESY in der Testphase befindet

QIP

- Managementwerkzeug zur Verwaltung des IP-Adressraums benötigt
  - ca. 12.000 IP-Adressen in Benutzung
  - ca. 80 Segmentadministratoren verwalten Subnetze, macht Zugriffskontrolle nötig
  - Altes System nicht mehr wartbar
  - Wahl viel auf QIP von Lucent Technologies

QIP

- QIP seit 11.12.2001 produktiv
  - Support für DDNS
    - bisher nicht aktiv für desy.de
    - Tests laufen auf win2k.desy.de
  - erlaubt Verwaltung und Konfiguration des DHCP-Services
  - Registrierung der MAC-Adressen durch Segmentadministratoren

SPECTRUM

- Seit vielen Jahren im Einsatz
- Überwachung (Ping, SNMP) der zentralen Netzwerk und RZ-Komponenten
- Alarmierungssystem für das Operating
- Wird nicht mehr allen Anforderungen gerecht
  - Dienstüberwachung
  - Wartungszeiten
  - Eskalationen
- Status: Service wird eingefroren

Network Health

- SPECTRUM hat unbefriedigendes Reporting
- Wahl viel auf Networkhealth
  - Produktiv seit Mitte 2001
- Regelmäßiges Polling aller wichtigen Ports (RZ, Backbone) (> 1000), und CPUs
- Unbekannte Geräte werden innerhalb von 90 Tagen aufgenommen
- ‘Intelligenz‘ innerhalb der Health Reports
  - Trendreports, Trendanalysen
  - ‘Situations to Watch‘

Cisco Works

- Interessant für Konfigurations- und Softwaremanagement
  - Zentrale SW Konfiguration
  - Backup aller Konfigurationen
  - Software-/Konfigurationsverteilung
  - User Tracking
    - MAC, IP, Switchport, Wann gesehen?
- Userinterface unbrauchbar (Java, WWW)
    - langsam, instabil
- Abgeschaltet, warten auf neue Version

Zukünftige Themen

- Firewall
  - Umstieg auf Cisco PIX
- VPN HH <-> Zeuthen
- Konsolidierung NMS
  - Standalone Werkzeuge, Integration zwingend
- IP Telefone
- Accounting !
  - POF
- IPv6