IPv6 bei der Post

Step by Step zu IPv6

Robert Bürk, IT221

Agenda

Wer sind wir **Projektteam, Projekt**	Vom User zur Post **Wo stehen wir heute**
Die Post **National und international**	Erfahrungen **Hindernisse zu überwinden**
Post Domain Verwaltung **ca. 700 Domains in ca. 70 Ländern**	Masterplan (Engineering) **Unsere Entscheidungsgrundlage**
Adresskonzept **Unsere ersten Erfahrungen**	Tools und Prozesse **Wie weit sind wir**
Dual Stack **Sicherheit nicht unterlaufen**	Intranet und Datacenter **Im Lifecycle IPv6 ready werden**

Wer sind wir
Projektteam, Projekt

Robert Bürk
Projektleitung, Adressierung

Thom Hofmann
Mail, Bluecoat

Daniel Eyholzer
Stv. PL, Netzwerk

Ronald Meier
Netzwerk

Urs Elmer
Firewall

Hans Scheurer
DNS, GSLB, Tools

Daniel Gisler
Security

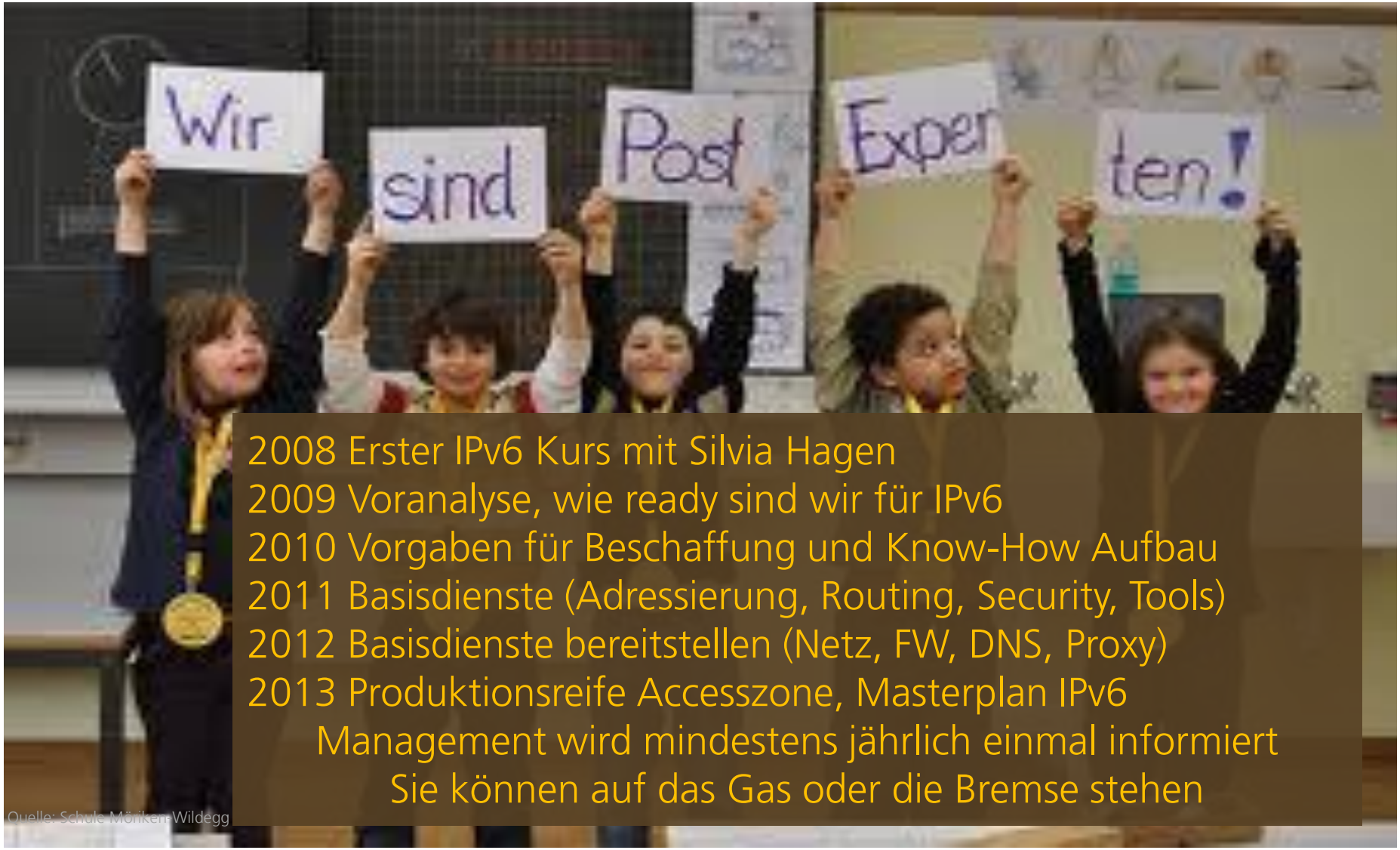
Stephan Badertscher
Adressverwaltung, Tools

Hans-Jörg Leuenberger
DDoS, IPS

Andreas Haisch
Postfinance

weitere Personen bei Bedarf
Client- und Serverbereich

Wer sind wir
Projektteam, Projekt

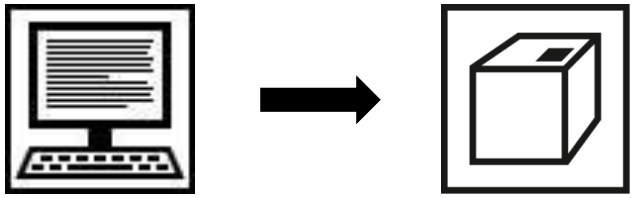


2008 Erster IPv6 Kurs mit Silvia Hagen
2009 Voranalyse, wie ready sind wir für IPv6
2010 Vorgaben für Beschaffung und Know-How Aufbau
2011 Basisdienste (Adressierung, Routing, Security, Tools)
2012 Basisdienste bereitstellen (Netz, FW, DNS, Proxy)
2013 Produktionsreife Accesszone, Masterplan IPv6
Management wird mindestens jährlich einmal informiert
Sie können auf das Gas oder die Bremse stehen

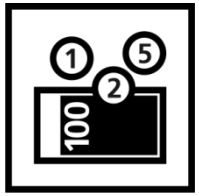
Quelle: Schule Möriken-Wildegg

Wo der Mischkonzern Post tätig ist
Vier Märkte

- **Logistikmarkt**

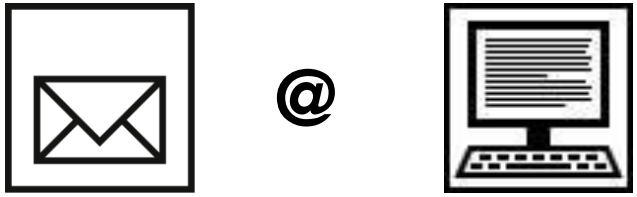


- **Retailfinanzmarkt**



- **Markt für öffentlicher Personenverkehr**

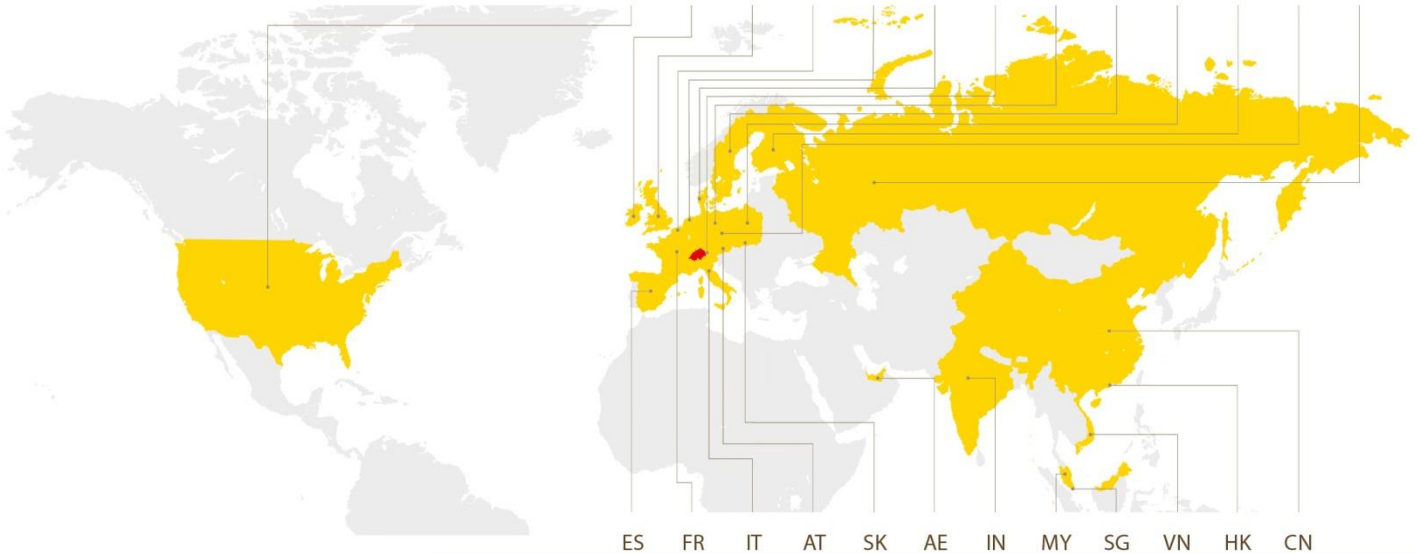
- **Kommunikationsmarkt**



Was die Post Geschäftskunden bietet
Leistungen rund um den Globus

Märkte | Die Schweizerische Post im Ausland

2011



	US	IE	UK	BE	NL	DK	FL	DE	SE	PL	FI	CZ	RU
Briefe international	■		■	■	■	■		■	■		■		
Dialoglösungen			■ 2					■ 2	■ 2	■ 2		■ 2	■ 2
Dokumentenlösungen	■	■	■			■ 1	■	■	■ 1	■ 1			
Personenverkehr							■						
E-Business-Lösungen			■					■					

	ES	FR	IT	AT	SK	AE	IN	MY	SG	VN	HK	CN
Briefe international	■	■	■	■			■	■	■		■	■
Dialoglösungen		■ 2										
Dokumentenlösungen	■	■	■	■	■	■ 1			■	■		
Personenverkehr		■										
E-Business-Lösungen									■			

1 Partner
2 Länder in denen Gesellschaften des Joint Venture MEILLERGHP GmbH tätig sind.

Post Domain Verwaltung
ca. 700 Domains in ca. 70 Ländern

DIE POST

PostFinance

PostAuto

+

Quelle: Zerigo, Inc.,

2013 Post wird zur AG

Domain Einträge müssen angepasst werden
Synergie nutzen IPv6 Adressen der DNS Systeme eintragen

Kosten werden vom Konzern getragen.
Die ganzen Mutationen benötigen mehr als ein Jahr Zeit

Quelle: Ripe

Adresskonzept
Unsere ersten Erfahrungen

Einteilung	Subnetierung IPv6 (classless)	Anzahl Subnetze	Vergleich IPv4 (Anzahl Subnetze)
Post weltweit	**/32**	**4,3 Mia**	**65‘536 x A-Class**
Post Schweiz	**/35**	**596.8 Mio**	**8192 x A-Class**

Einteilung	Subnetierung IPv6 (classless)	Anzahl Subnetze	Vergleich IPv4 (Anzahl Subnetze)
Country Aggregation	/40	16,7 Mio	256 x A-Class
Region Aggregation	/48	65‘536	A-Class
Local Aggregation	/56	256	B-Class

Adresskonzept
Unsere ersten Erfahrungen

1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 **/64 FFFF FFFF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 111 **/63 7FFF FFFF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 11 **/62 3FFF FFFF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1 **/61 1FFF FFFF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 **/60 FFF FFFF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 111 **/59 7FF FFFF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 11 **/58 3FF FFFF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1 **/57 1FF FFFF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 **/56 FF FFFF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 111 **/55 7F FFFF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 11 **/54 3F FFFF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1 **/53 1F FFFF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 **/52 F FFFF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 111 **/51 7 FFFF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 11 **/50 3 FFFF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1 **/49 1 FFFF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 **/48 FFFF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 111 **/47 7FFF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 11 **/46 3FFF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1 **/45 1FFF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 **/44 FFF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 111 **/43 7FF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 11 **/42 3FF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1 **/41 1FF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 **/40 FF FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 111 **/39 7F FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 11 **/38 3F FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1 **/37 1F FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 **/36 F FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 111 **/35 7 FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 11 **/34 3 FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1 **/33 1 FFFF FFFF**
1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 **/32 FFFF FFFF**

- **Adresskonzept ist optimiert auf schlankes Routing.**
- **Es ist geographisch aufgebaut. Jedes Land hat seine eigene Gesetzgebung. Es wird nach Möglichkeit über eine Schnittstelle angebunden.**
- **Internetangebote werden ausschliesslich über Internet erreicht. Alles andere wird intern geroutet.**
- **Default Gateway auch Link local sind standardisiert.**

Adresskonzept
Unsere ersten Erfahrungen

- **Mit Dual Stack stehen weiterhin nur die IPv4 Subnetze zur Verfügung die wir bereits haben.**
- **Keine Merkmale verwenden in der IPv6 Adresse wie Telefon Länderkennung, VLAN (neu 16 Mio) etc.**
- **Keine dezimalen Kennungen in einer hexadezimalen Adresse verwenden.**

Dual Stack
Sicherheit nicht unterlaufen

- Gleiche Sicherheitsstandards wie bei IPv4 erreichen.
- Sicherheitssysteme zuerst ausgiebig testen.
- Start mit getrennten Firewalls für IPv6.
- Konfigurations- und Betriebsdokumente anpassen.
- Ersichtlich, welche Services auch über IPv6 zu erreichen sind.
- Entscheide und Ausnahmen dokumentieren.

Der Weg vom Home User zur Post
Wo stehen wir heute

User *(Home User)*
Ready OS, Browser

DNS *(Domain Name Server)*
Ready seit 2012

ISP Home User *(Internet Service Provider)*
Ready Schweiz ca. 10 %

GSLB *(Global Server Load Balancer)*
Ready, Ersatz im Lifecycle

ISP Post *(Internet Service Provider)*
Ready seit 2012

NTP (*Network Time Protocol)*
Ready seit September 2013

DDos Abwehr beim ISP
Ready Swisscom, Sunrise später

LSLB *(Local Server Loadbalancer)*
Ready seit 2012

Netz *(Access Zone / DMZ)*
Ready seit 2012

Web Server *(Testserver)*
Ready seit 2012

IPS / Firewall *(Intrusion Prevention System)*
Ready seit 2012

XML GWY *(Extensible Markup Language)*
Ready seit 2013

Was es sonst noch braucht
Wo stehen wir heute

Adressverwaltung *(IPAM/Inventar)*
Ready seit 2013

Outgoing Proxies *(IPv6 Sites erreichen)*
Ready seit Herbst 2013

Prozesse *(Workflow Tool)*
Ready seit September 2013

Mail (*Contentfilter)*
Not ready, geplant 2014

ADS *(Access Detection System)*
Ready seit 2012

Homepage Post *(Internetauftritt Post)*
Not ready, Projekt für Ablösung

NetViz *(Network Visualization)*
Ready seit 2013

Management *(Server/Network)*
Not ready, zur Zeit auf IPv4

MRTG/Cacti *(Messen, Statistik)*
Not Ready MIB's fehlen

Schulung *(Know How)*
30 MA drei Tage Schulung

Wir stellen uns den Herausforderungen

Erfahrungen
Hindernisse zu überwinden

DDoS Abwehr bei den Providern

- Arbor System ready, detektierte den IPv6 Launchday als Anomalie Verkehrsanstieg um 100 %
- Swisscom geplant Oktober 2012 aufgeschaltet im Juni 2013 Herausforderung Netzinfrastruktur
- Test durch Post Herbst 2013
- Sunrise geplant April 2013 der Termin ist noch offen Herausforderung Netzinfrastruktur

Die Post geht nicht in die Produktion bevor DDoS IPv6 die gleiche Funktionalität erfüllt wie bei IPv4

NTP

- In der Testumgebung stellt sich heraus, dass das NTP System nur im gleichen Subnetz funktioniert (nur mit Link local Adressen)
- Major Release mit dem Fix kommt nach 15 Monaten
- Intern benötigen wir weitere 9 Monate um die Tests erneut in Angriff zu nehmen. Test erfolg-reich inkl. Management mit IPv6

Die Post will Major Releases einsetzen

Erfahrungen
Hindernisse zu überwinden

Loadbalancer

- Die alten Loadbalancer sind nicht IPv6 fähig
- Alle Loadbalancer Services müssen auf die neue Umgebung migriert werden
- Die Migration sollte bis ende Jahr abgeschlossen sein
- Die Internet Accesszone ist bereit für IPv6 Services

Der Migrationsaufwand ist nicht zu unterschätzen
Je ein Service für IPv4 und IPv6 ist zu implementieren

Adressverwaltung

- Tools sind vorhanden
- Zur Zeit keine vollständige Integration Inventar und Adressverwaltung bei IPv6
- Zu hohe Kostenfolge der post-spezifischen Anforderungen
- Noch zu viele händische Eingriffe bei IPv6 notwendig damit der User die gleiche Sicht wie bei IPv4 hat

Die Post will auf Standardprodukte setzen

Erfahrungen
Hindernisse zu überwinden

Outgoing Proxies

- Ziel 1: Die IPv4 Clients im Postnetz sollen jede IPv6 Webseite im Internet abrufen können
- Ziel 2: Dual Stack Webseiten sollen über IPv6 erreicht werden
- Bug: Dual Stack über IPv6 funktioniert bei Facebook und Google. Bei anderen Sites noch nicht
- Volle IPv6 Funktionalität seit 10.10.2013

Die Post will Major Releases einsetzen

Mail / Contentscanner

- Ein erster Prerelease des Contentscanners ist für Herbst 2013 angekündigt
- Wenn dieser stabil läuft, wird er in der Testumgebung eingesetzt
- Die Testumgebung ist Backup für die Produktion. Szenarien für ein Downgrade auf IPv4 festlegen

Die Post geht nicht in die Produktion bevor der Contentscanner die gleich Funktionalität erfüllt wie bei IPv4

Erfahrungen
Hindernisse zu überwinden

IPv6 Unterstützung im Netz

- Cisco bringt mit dem Release IOS 15.2 / NX-OS 7.1 die IPv6 Unterstützung, die über den Layer 3 hinausgehen
- Learnings: IPv6 Unterstützung auf Feature Ebene sind Musskriterien bei 2 WTO Ausschreibungen

Die Post will nur noch Produkte beschaffen, die IPv6 unterstützen

IPv6 Unterstützung beim Mgmt

- 50 % der eingesetzten ILO unterstützen kein IPv6
- Die Server werden im Lifecycle ersetzt
- Learnings: Die Ablösung der heute eingesetzten Mgmt Hard- und Software muss IPv6 unterstützen

Die Post will nur noch Produkte beschaffen, die IPv6 unterstützen

Erfahrungen
Wo lauern die Gefahren

- Eigenheiten Security im IPv6 Protokoll.
- Die (noch) fehlende Unterstützung der Endpoint Security der Hersteller.
- Welche sind von Bedeutung für die Access Zone Post?
- RA Guard und Destination Guard

Sicherheitsherausforderung

Router Advertisement

Problem: Fremde Geräte können den Verkehr ableiten

Lösung: RA Guard einsetzen

Problem: Cisco unterstützt RA Guard erst im 1. Quartal 2014 (Nexus)

Einschätzung: Der Zutritt zu den entsprechenden Räumen ist gut gesichert. Die Zutritte werden registriert.

Accesszone mit Auflagen freigegeben
Für Produktion RA Guard notwendig

Neighbor Cache Exhaustion

Problem: Neighbor Cache kann überlaufen

Lösung: Destination Guard einsetzen. Subnetze verkleinern

Problem: Cisco unterstützt Destination Guard erst im 1. Quartal 2014 (Nexus)

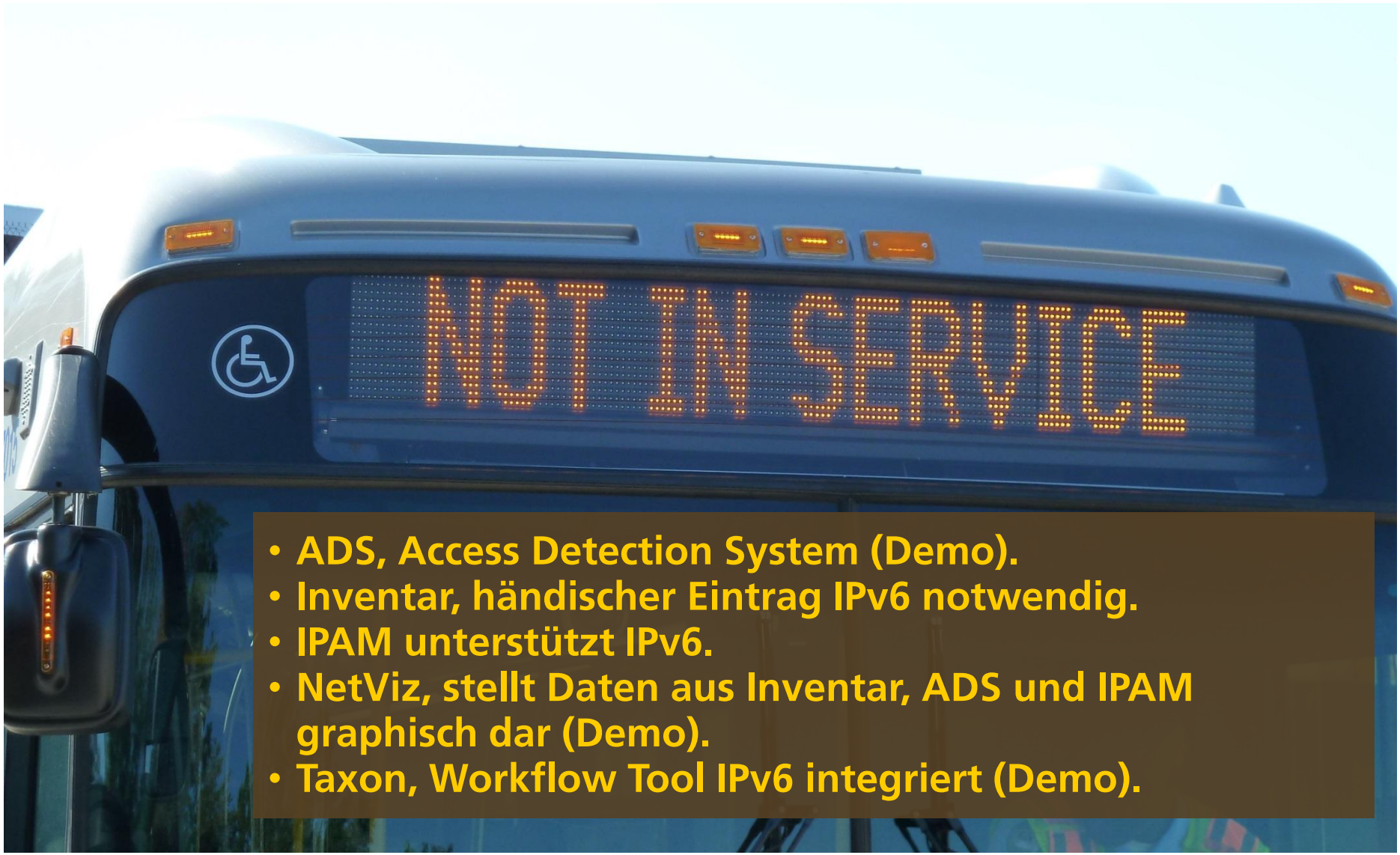
Einschätzung: In der Testphase kann bei einem Angriff IPv6 abgeschaltet werden.

Accesszone mit Auflagen freigegeben
Für Produktion Destination Guard notwendig

Masterplan (Engineering)
Unsere Entscheidungsgrundlage

- ca. 50 Einzelaktivitäten mit 18 Auftragnehmer, 7 Teams.
- Eigenverantwortung der Auftragnehmer.
- Messbarkeit des Fortschrittes, Kennzahl(en) in %.
- Teamleiter und Leitung werden vierteljährlich informiert.
- Teamleiter und Führung stehen in der Pflicht.

Tools und Prozesse
Wie weit sind wir



- ADS, Access Detection System (Demo).
- Inventar, händischer Eintrag IPv6 notwendig.
- IPAM unterstützt IPv6.
- NetViz, stellt Daten aus Inventar, ADS und IPAM graphisch dar (Demo).
- Taxon, Workflow Tool IPv6 integriert (Demo).

Intranet und Datacenter
Im Lifecycle IPv6 ready werden

- Im Rahmen des Lifecycle soll das Intranet und Datacenter den IPv6 Grammy Status erreichen.
- Backbone ist IPv6 ready und kann aktiviert werden.
- Firewall und Netzinfrastruktur sind bis 2015 ready.
- IPv4 Inseln sind bekannt (z.B. Paket- und Briefzentren).
- Wie sieht es bei den Applikationen aus?

Zukunft


Die Post ist im Internet mit DNS, Mail und Homepage Post unter IPv4 und IPv6 erreichbar
Wir wissen, wann und mit welchem Aufwand wir IPv6 im Intranet und Datacenter einführen können

Fragen
bringen uns weiter

robert.buerk@post.ch

Alle Photos: Robert Bürk


Vielen Dank für Ihre Aufmerksamkeit.