IPv6 Security

Wie das neue Protokoll auf Ihre IT-Sicherheit wirkt

SWITCH

Serving Swiss Universities

Frank Herberg
frank.herberg@switch.ch

Security-Zone – Zürich, 18. September 2012

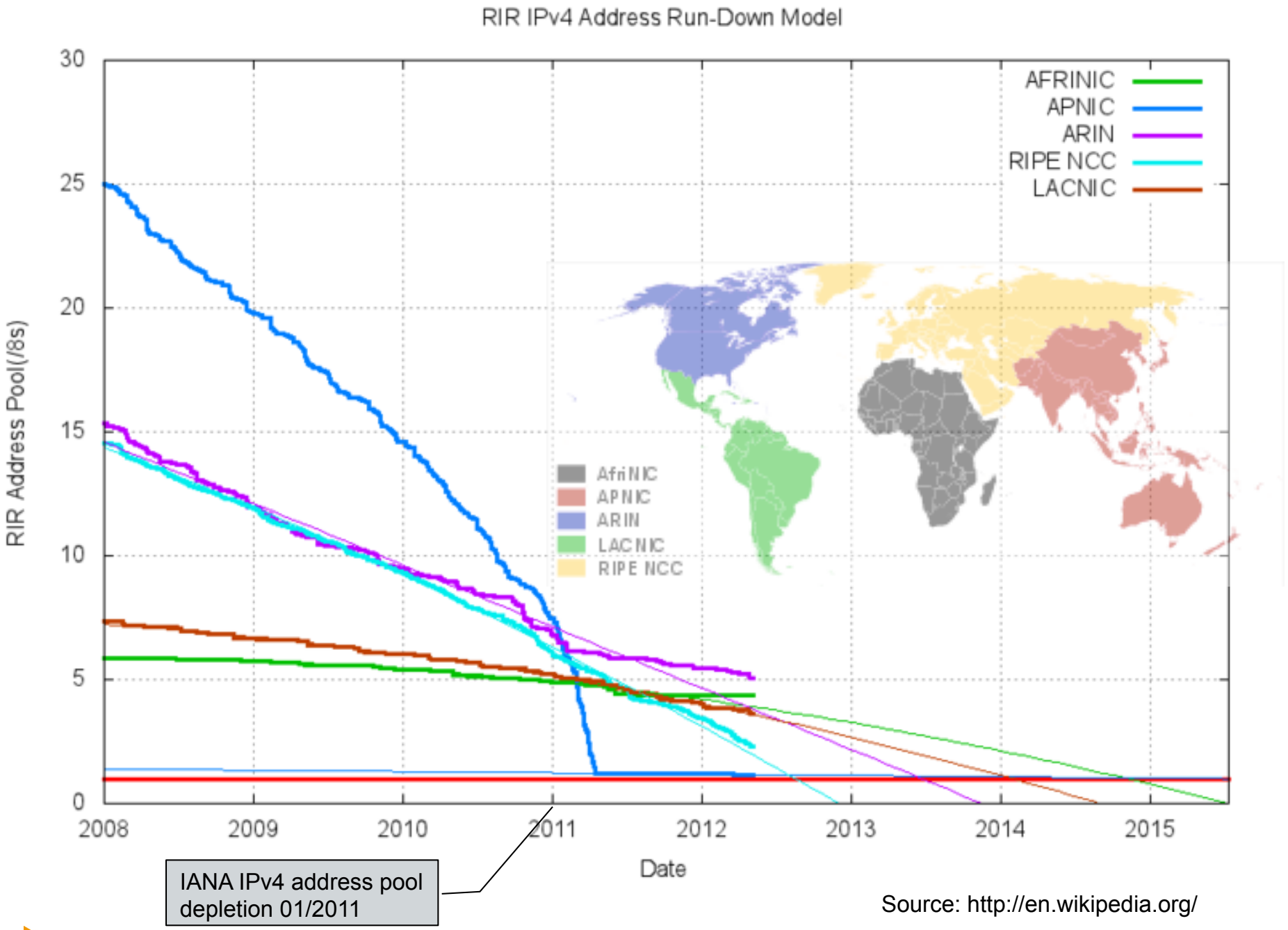
Übersicht

- Warum mit IPv6 beschäftigen?
- Welche Dimension hat das Thema?
- Wie wirkt IPv6 auf Ihre IT-Sicherheit?
- Anregungen für Ihre IPv6-Security-Strategie

© 2012 SWITCH

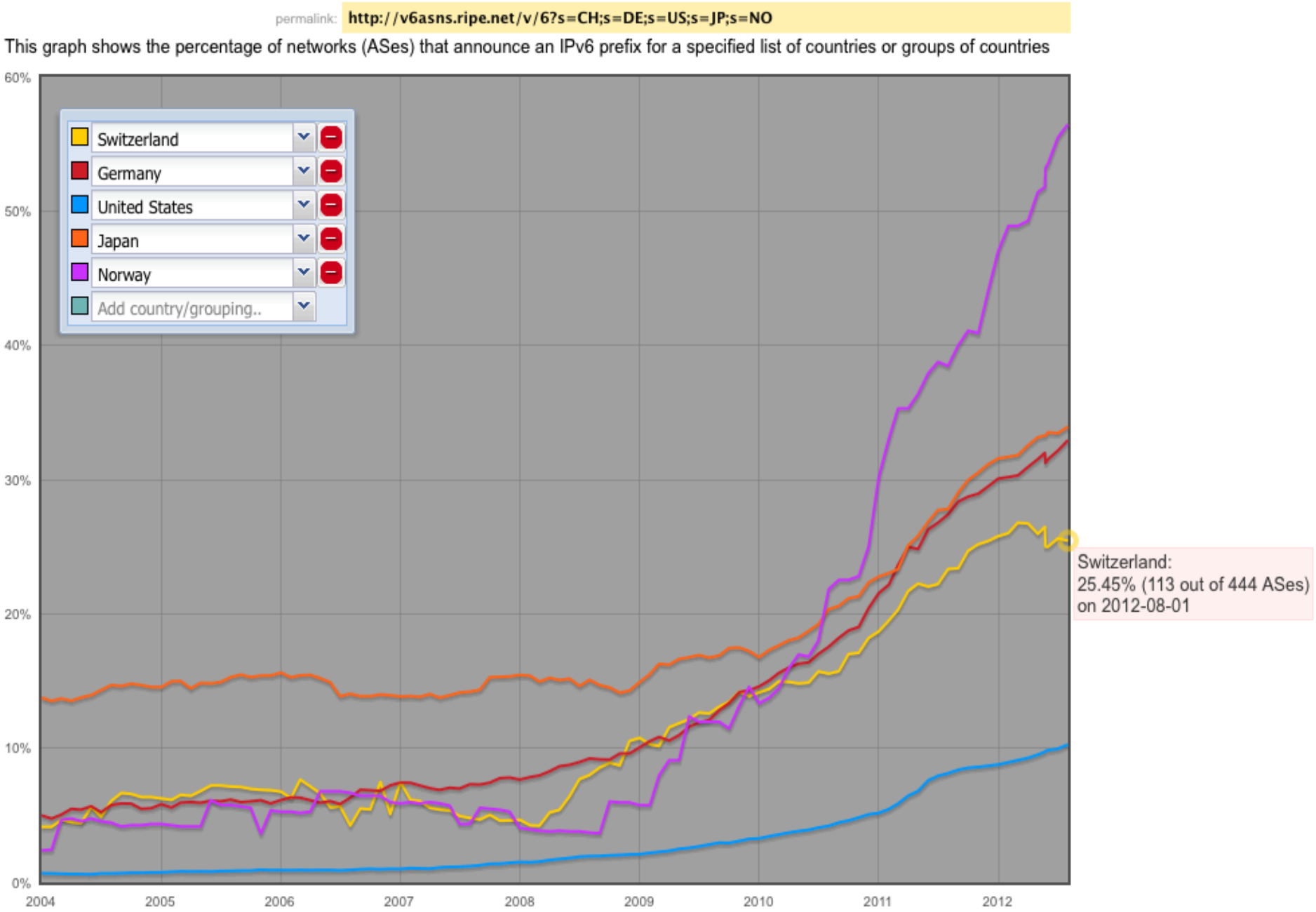
IPv6 - ist da!

© 2012 SWITCH



Source: http://en.wikipedia.org/

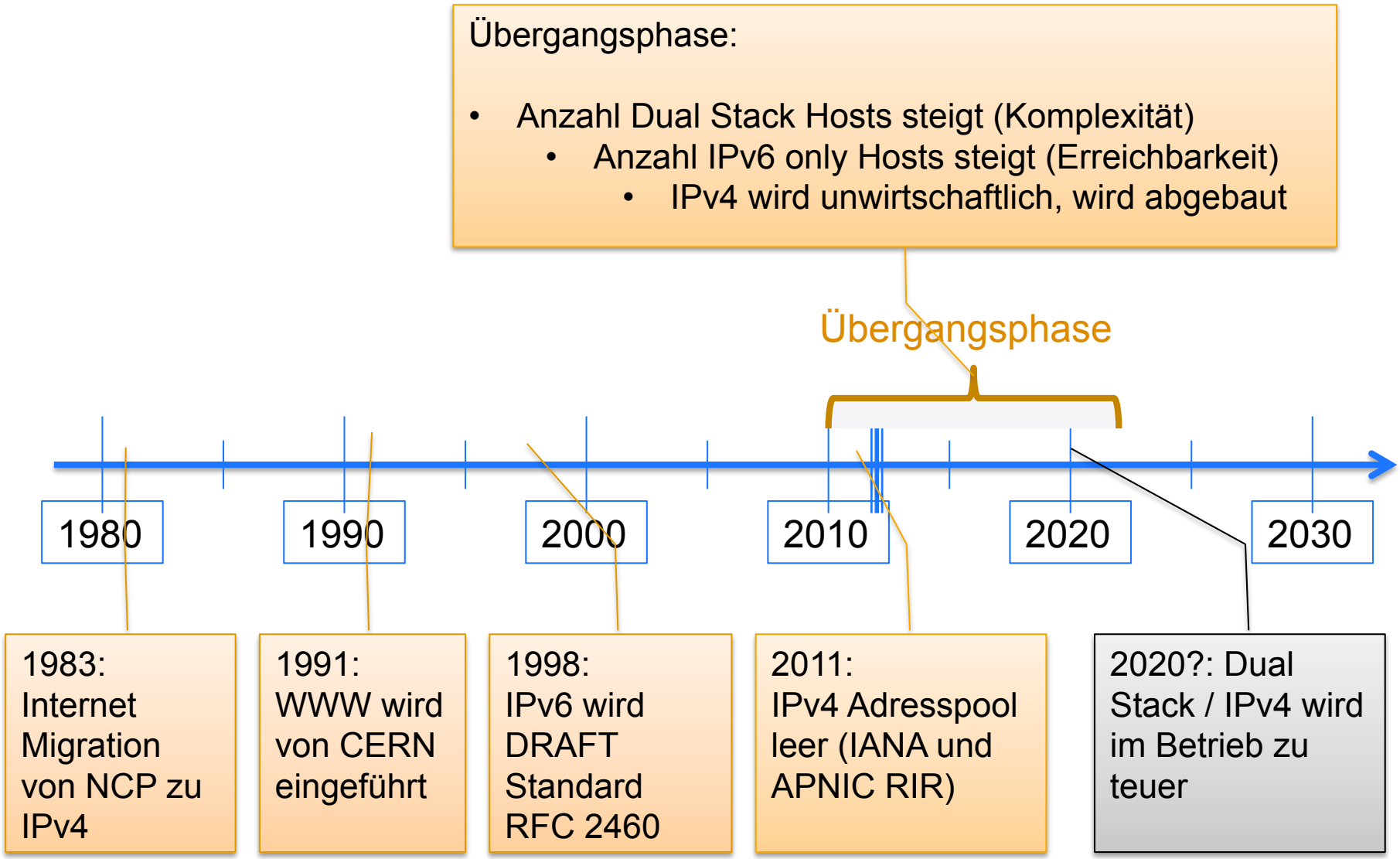
© 2012 SWITCH



Source: ripe.net

© 2012 SWITCH

IPv4/6 Timeline (50 Jahre)



© 2012 SWITCH

Mögliche Treiber für IPv6-Integration

- IP-Adressmangel (BYOD**s**, Internet der Dinge)
- Erreichbarkeit (IPv6-only / Asien)
- Neue Applikationen (End-to-End, IPv6 only, Mobile)
- Veraltete Infrastruktur / nachhaltige Neu-Investitionen
- Konsolidierungsbedarf im Netzbereich (Adresskonzept)
- Angebot von IPv6-Dienstleistungen / Technologie-Image

© 2012 SWITCH

"Porsche überholt auf der Datenautobahn

Die Dr. Ing. h.c. F. Porsche AG, Stuttgart, startet ins Internet der Zukunft: Ab sofort verwendet der Sportwagenhersteller das Internet Protocol Version 6 (IPv6) und schafft damit die Basis für den zukunftsweisenden Netzzugriff für Kunden und Besucher… "

Pressemitteilung von Porsche 11.6.2012

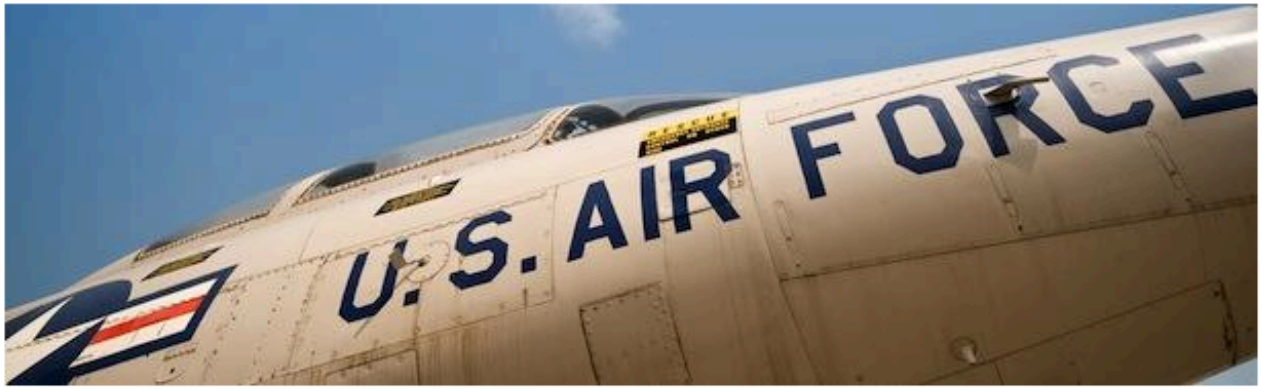
Source: http://www.porsche.com/germany/aboutporsche/pressreleases/?pool=germany&id=2012-06-11

© 2012 SWITCH

How the Air Force Is Flying Toward IPv6

DAVID STROM · AUGUST 20TH, 2012

Like 6 people like this.



The United States Air Force is one very high-tech organization, and we're not just talking about jet fighters. The Air Force's latest mission is a high-stakes, high-speed migration to Internet Protocol v6 (IPv6). Chances are most corporate networks aren't as extensive or complex as the Air Force's, but the service's planning operations offer worthwhile lessons for many organizations.

The Air Force began its transition to IPv6 earlier this summer, and expects to have its entire network migrated by the end of September 2014, the deadline self-imposed by the US government for all of its network operations. The move to IPv6 will also let the Air Force support more ad hoc networks in the field - making it them more operationally agile and better able to support machine-to-machine communications.

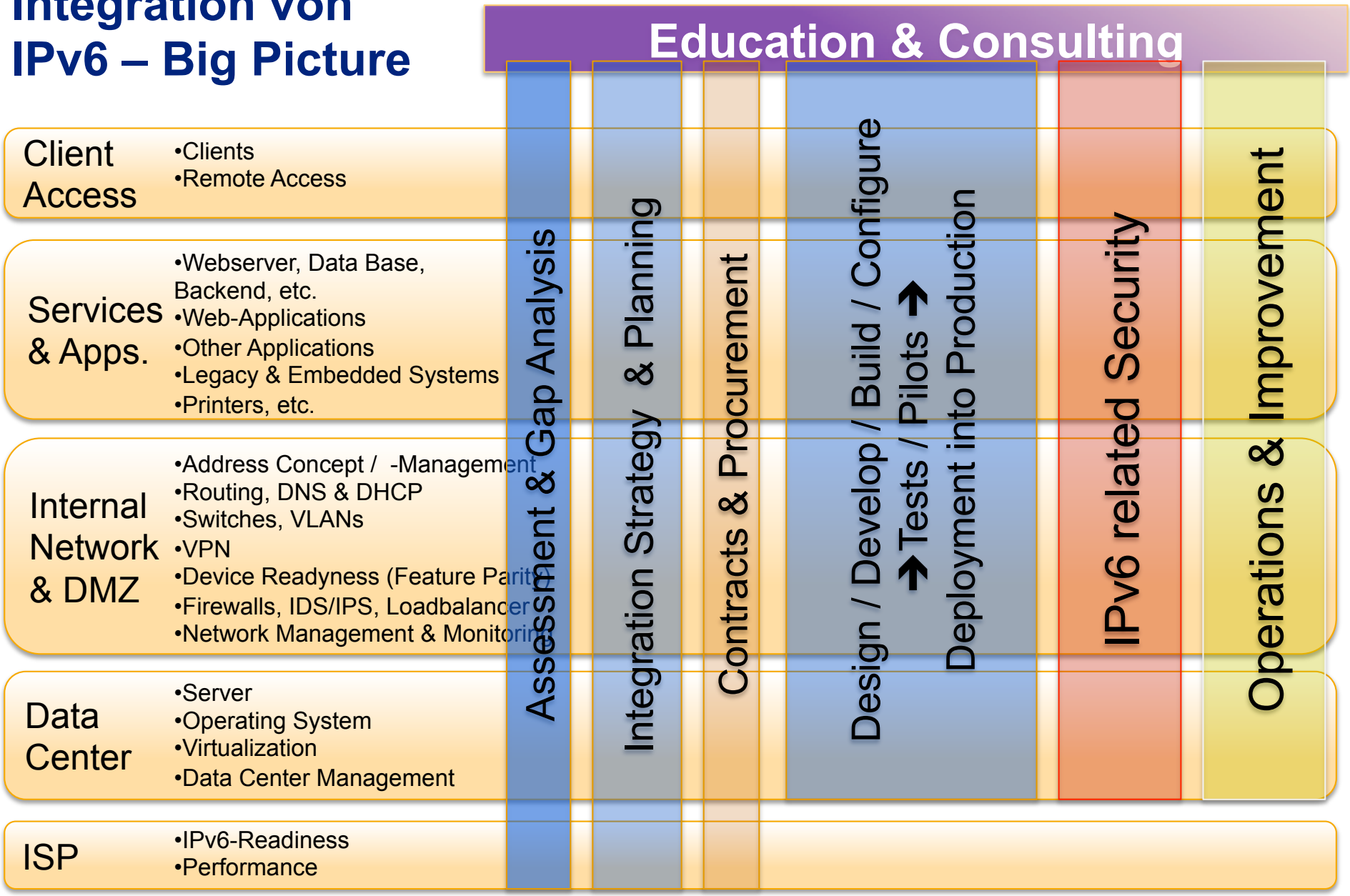
Source: http://www.readwriteweb.com/enterprise/2012/08/how-the-air-force-is-flying-toward-ipv6.php

© 2012 SWITCH

Welche Dimension hat das Thema IPv6?

© 2012 SWITCH

Integration von IPv6 – Big Picture

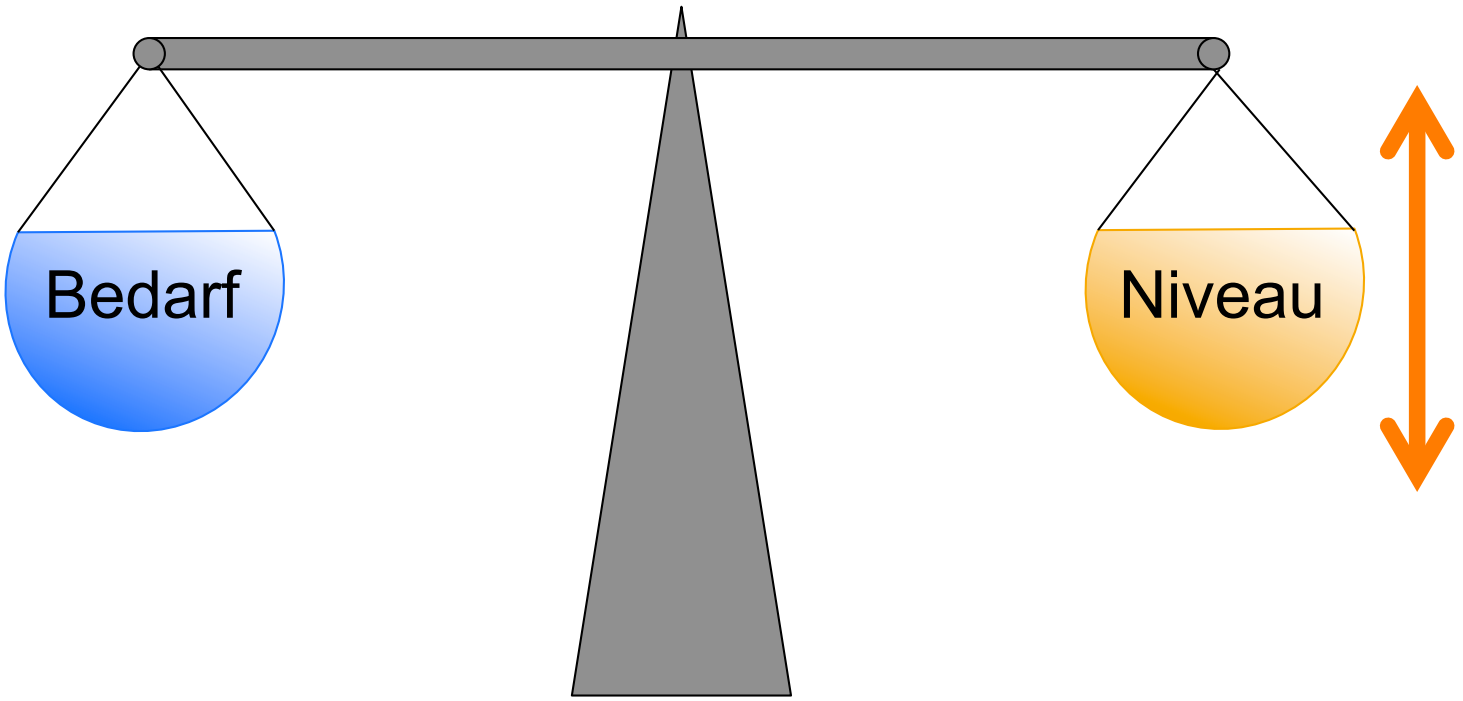


© 2012 SWITCH

Wie wirkt IPv6 auf Ihre IT-Sicherheit?

© 2012 SWITCH

➔ IPv6 bringt viel in Bewegung



IT-Sicherheit

© 2012 SWITCH

Latent Threat – IPv6 ungemanaged aktiv

- IPv6 ist auf allen gängigen Betriebssystemen per default "im Hintergrund" aktiviert…
- …und kann durch Autokonfiguration (SLAAC) ohne manuelles Eingreifen konfiguriert werden (Routing, Globale IP-Adresse)
- Missbrauch für DOS- und MITM-Angriffe
- ein fehlkonfigurierter Client kann Netz lahmlegen
- Durch Tunnel-Autokonfiguration können Verbindungen durch Firewall hindurch aufgebaut werden (TEREDO, ISATAP)

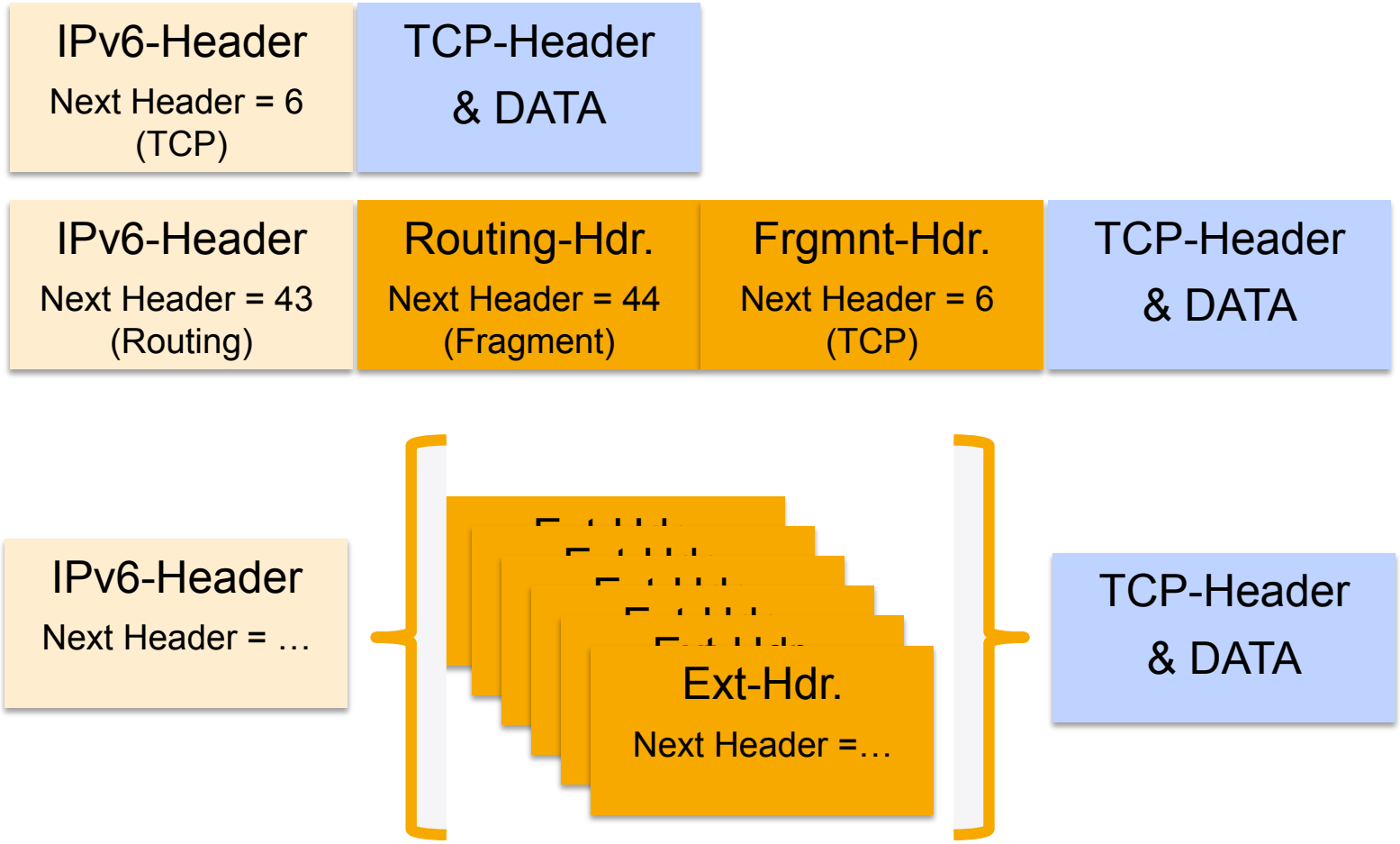
© 2012 SWITCH

Höhere Komplexität – im Protokoll

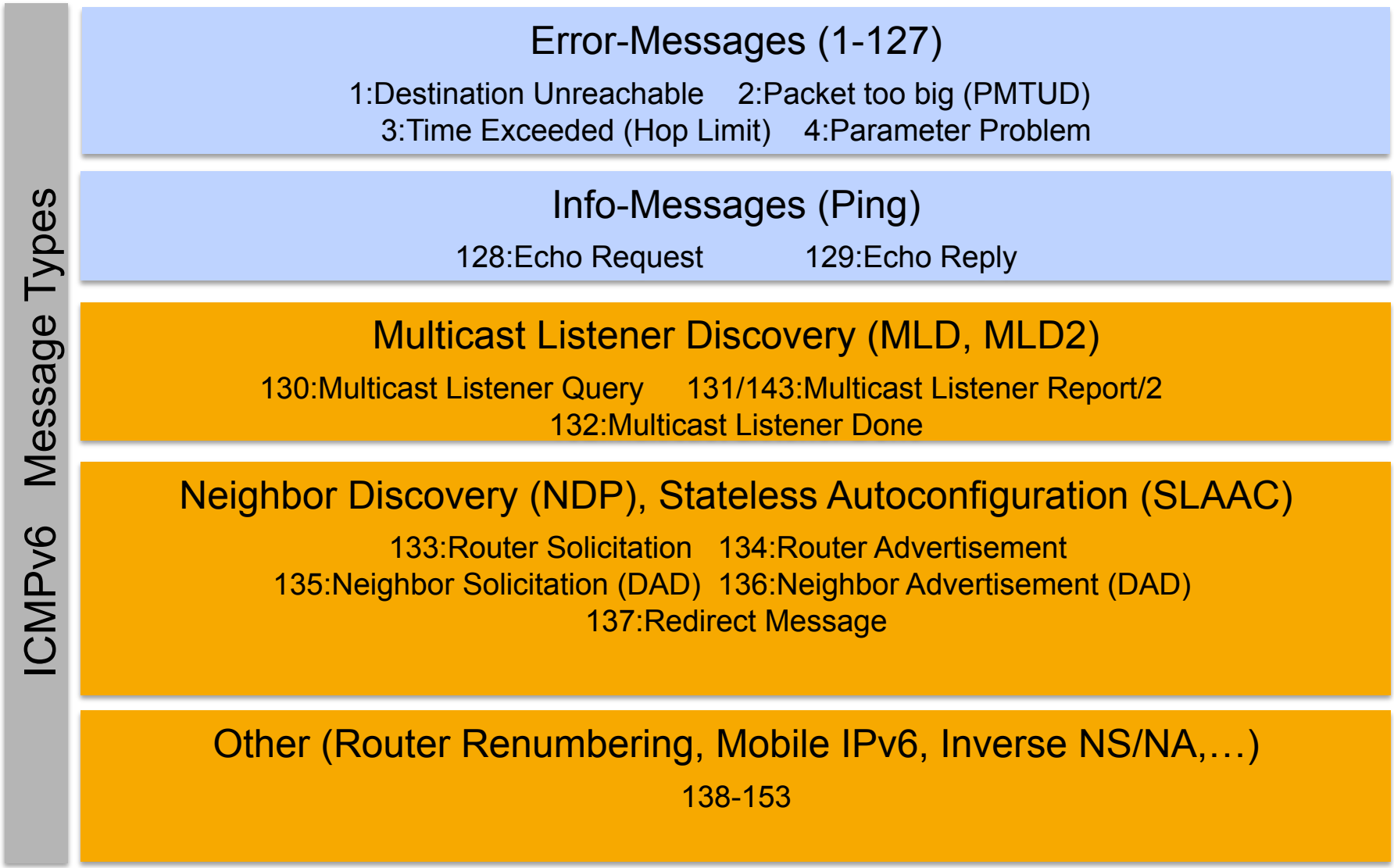
- IPv6 ist sehr komplex!
- Beispiele:
  - Extension Header
  - ICMPv6 (Autokonfiguration, etc.)
  - Adressen

© 2012 SWITCH

Protokollkomplexität: Extension Header



Protokollkomplexität: ICMPv6



© 2012 SWITCH

Protokollkomplexität: IPv6-Adressen

- Mehrere IP-Adressen pro Interface

Link Local	fe80::3e07:54ff:fe5d:abcd
Global	2001:610::41:3e07:54ff:fe5d:abcd
Privacy	2001:610::41:65d2:e7eb:d16b:a761

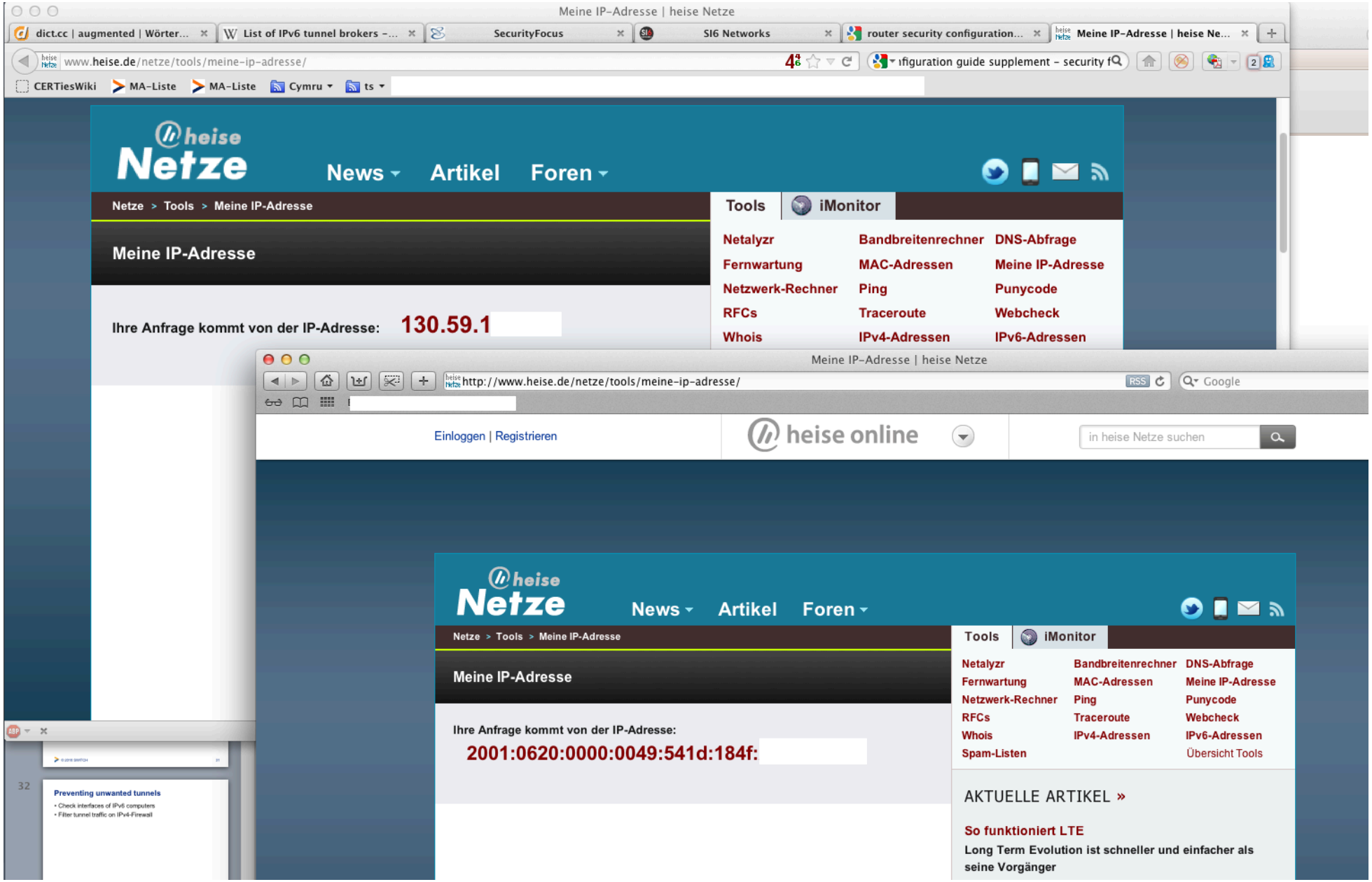
(Privacy Extensions = random / temporär)

IPv4	173.194.32.119

(Dual Stack: IPv4 & IPv6)

- Schreibweise nicht eindeutig (Nullen)
- Adresswahl nicht klar

© 2012 SWITCH


Meine IP-Adresse | heise Netze
www.heise.de/netze/tools/meine-ip-adresse/
heise Netze
News
Artikel
Foren
Netze > Tools > Meine IP-Adresse
Meine IP-Adresse
Ihre Anfrage kommt von der IP-Adresse: 130.59.1
Tools
iMonitor
Netalyzr
Bandbreitenrechner
DNS-Abfrage
Fernwartung
MAC-Adressen
Meine IP-Adresse
Netzwerk-Rechner
Ping
Punycode
RFCs
Traceroute
Webcheck
Whois
IPv4-Adressen
IPv6-Adressen
Meine IP-Adresse | heise Netze
http://www.heise.de/netze/tools/meine-ip-adresse/
Einloggen | Registrieren
heise online
in heise Netze suchen
heise Netze
News
Artikel
Foren
Netze > Tools > Meine IP-Adresse
Meine IP-Adresse
Ihre Anfrage kommt von der IP-Adresse:
2001:0620:0000:0049:541d:184f:
Tools
iMonitor
Netalyzr
Bandbreitenrechner
DNS-Abfrage
Fernwartung
MAC-Adressen
Meine IP-Adresse
Netzwerk-Rechner
Ping
Punycode
RFCs
Traceroute
Webcheck
Whois
IPv4-Adressen
IPv6-Adressen
Spam-Listen
Übersicht Tools
AKTUELLE ARTIKEL »
So funktioniert LTE
Long Term Evolution ist schneller und einfacher als seine Vorgänger
32
Preventing unwanted tunnels
• Check interfaces of IPv6 computers
• Filter tunnel traffic on IPv4-Firewall

© 2012 SWITCH

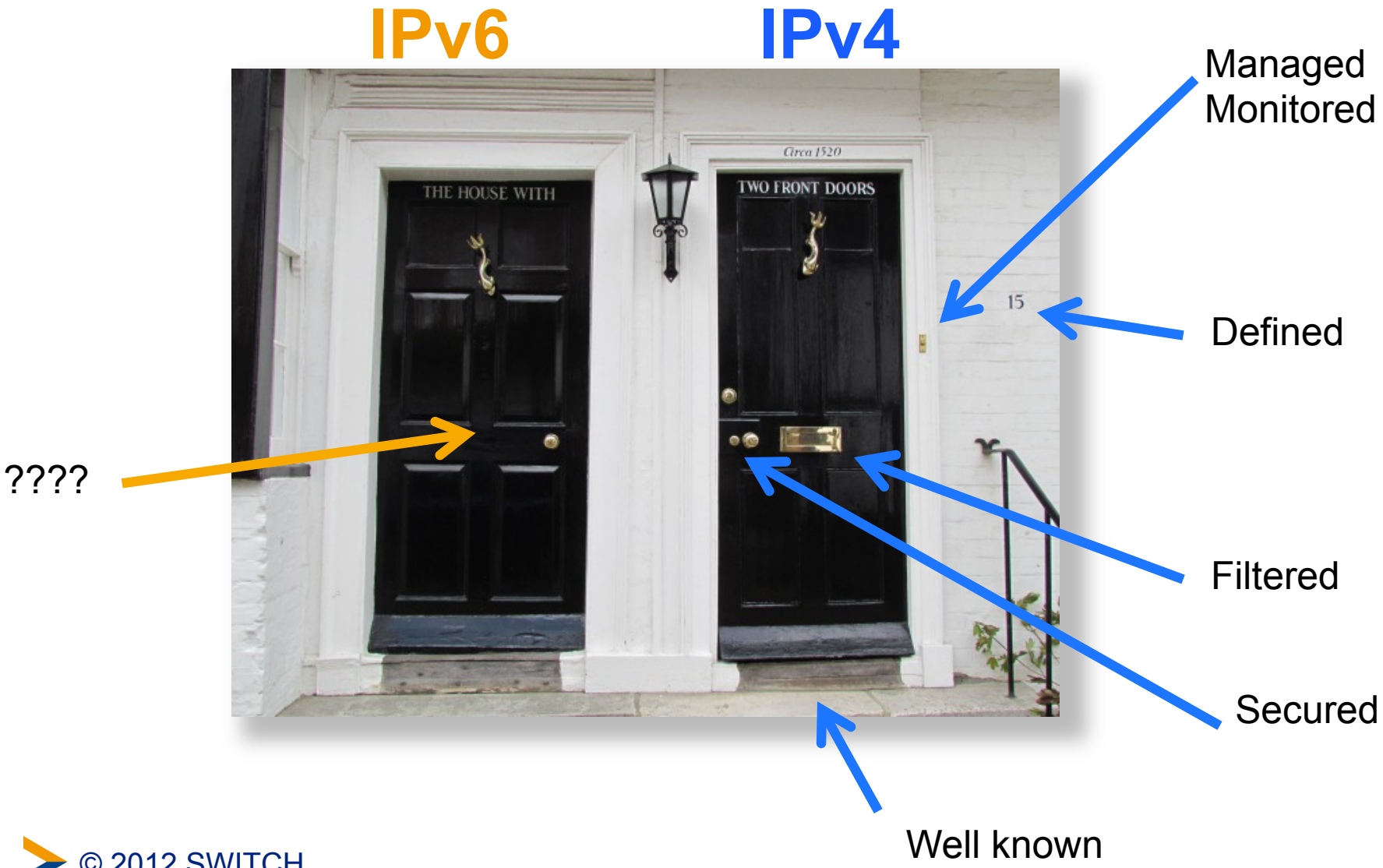
Höhere Komplexität – durch Dual Stack

- Zwei Protokolle parallel (Dual Stack) bedeutet deutlich mehr (doppelt so viel?) Komplexität auf Jahre
  - Doppelt so viele Firewall Policies (je nach FW)
  - Doppelt so viele IP basierte Access-Listen (ACLs)
  - Mehr Devices (wenn getrennt nach Protokoll)
  - usw…

➔ x2 Administrationsfehler
➔ x2 Schwachstellen

© 2012 SWITCH

Dual Stack: The House with two front doors



© 2012 SWITCH

Geringere Reife – im Design

- IPv6 ist immernoch in Teilen "Development in Progress"
- Beispiele:

  RFC 6564: April 2012

  "A Uniform Format for IPv6 Extension Headers"

  RFC 6555: April 2012

  "Happy Eyeballs: Success with Dual-Stack Hosts"

© 2012 SWITCH

Geringere Reife – in Implementierungen

- Situation der Hersteller
  - Es gibt keinen "IPv6-Standard" - sondern sehr viele RFCs
  - diese widersprechen sich teilweise
  - alle relevanten RFCs implementieren ist ggf. nicht sinnvoll

➔ Hersteller kämpfen mit Komplexität und Moving Target

© 2012 SWITCH

Geringere Reife – in Implementierungen

- Häufige Auswirkungen
  - benötigte **Features** nicht implementiert
  - **Performance** nicht gewährleistet
  - denn vieles ist (noch) nicht "in Hardware" realisiert
  - **Stabilität** nicht gewährleistet
  - dies bedeutet häufige Updates

© 2012 SWITCH

Monitoring ist oft blind für IPv6

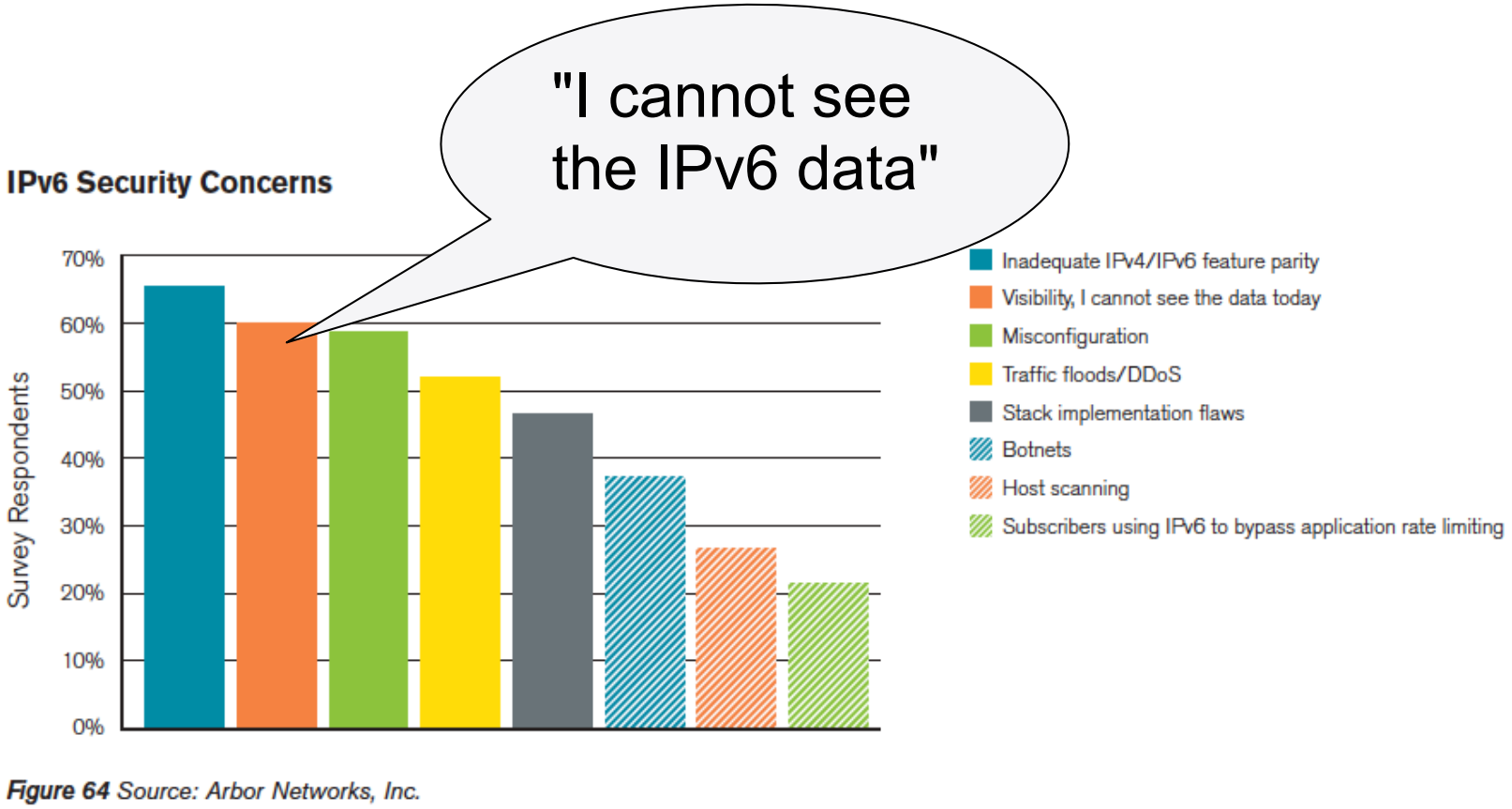


Figure 64 *Source: Arbor Networks, Inc.*

Source: Arbor Worldwide Infrastructure Security Report 2011

© 2012 SWITCH

Neue Angriffsmöglichkeiten

- Schwachstellen in Design oder Implementierung (Extension Header, Autoconfiguration,…)

  THC IPv6 Attack Toolkit (> 30 Tools)

  SI6 Networks IPv6 Toolkit (12 Tools)

- Fuzzing - Ausprobieren, wie (neue) Implementierung auf Unvorhergesehenes reagiert
- Covert Channel – Versteckter Informationskanal im Protokoll
- mehr Source-IP-Adressen zur Auswahl (Blacklisting)

© 2012 SWITCH

Weniger Know-how

- Weniger oder kein Know-how
  - Netzwerk-Staff, Sysadmins, Security-Staff
  - Management
- Lernkurve IPv6
  - braucht viel Zeit (Jahre)
  - braucht freie Ressourcen / Budget
  - braucht Praxis
  - führt am Anfang zu Fehlern

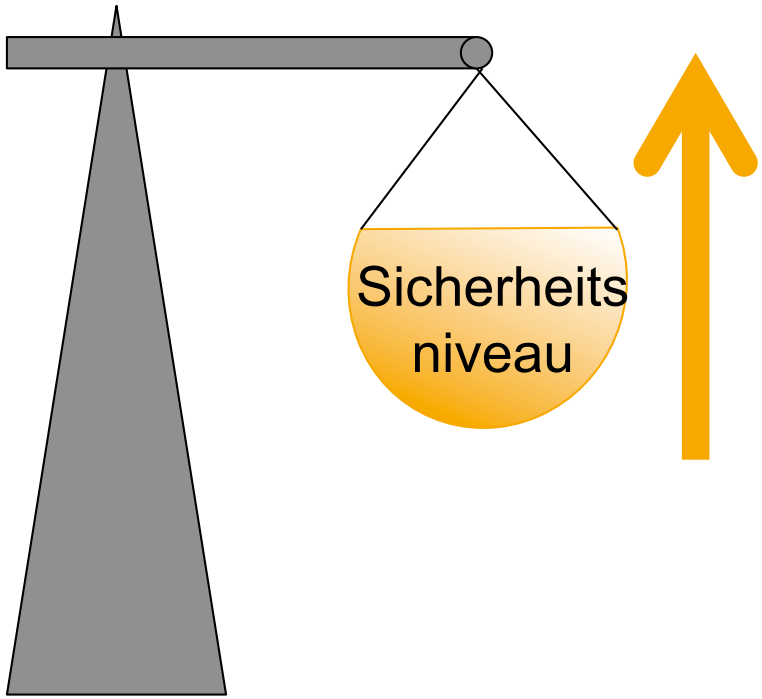
© 2012 SWITCH

Chancen für verbesserte IT-Sicherheit

- Review des vorhandenen Sicherheitsniveaus
- Konsolidierung im Netzwerk-Design
- IPv6 Adressplan - mehr oder weniger Policy-freundlich
- (Besseres) Adressmanagement - IPAM
- NAT vs. Sicherheit (RFC 4864)
- Vorbereitung für kommende Sicherheitsfeatures vs. Legacy-Technologie

© 2012 SWITCH

Fazit: Wie IPv6 auf Ihre IT-Sicherheit wirkt



- Latent aktiv im "IPv4-only" Netz
- höhere Komplexität
- geringere Reife
- weniger Know-how
- neue / mehr Angriffs-Vektoren
- weniger Sichtbarkeit
- viele Veränderungen (bieten auch Chancen)

© 2012 SWITCH

5 Anregungen für eine sichere IPv6-Strategie

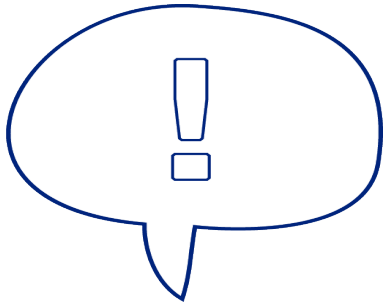
© 2012 SWITCH

1. Operativen Betrieb absichern

- Gibt es eine IPv6 Latent Threat Gefahr in Ihrem Netz?
- Wenn ja, ergreifen Sie Gegenmassnahmen

➔IPv6 oder SLAAC auf Systemen deaktivieren
➔Tunnel-Traffic am Perimeter filtern
➔Monitoring verbessern (Rogue Router Advrts.)

© 2012 SWITCH



2. Management sensibilisieren

- Ist IPv6 auf der IT-Management-Agenda angekommen?

  Priorität – Ressourcen – Budget

- Ist IPv6-Integrationsstrategie geplant?

  exist. Zyklen/Projekte nutzen – realistische Roadmap

  schrittweise und kontrolliert vorgehen

- Ist IT-Security in IPv6-Integrationsstrategie involviert?

  z.B. Security-Devices, Designentscheidungen, NAT, Adressplan, Update Security-Policy!

© 2012 SWITCH

3. Know-how aufbauen

- Trainingsplan definieren und durchführen
- Test-Labor aufbauen

  für Praxiserfahrung & Equipment-Tests

- Pilotprojekt durchführen und Erfahrungen sammeln
- Aktiv informieren und von anderen lernen

  Business-Events, Swiss IPv6 Council,…

- Nutzung von Beratungsangebot erwägen

© 2012 SWITCH

4. IPv6-Reife Ihres Security-Equipments berücksichtigen

- Bestandsaufnahme machen
- IPv6-Anforderungen für Equipment definieren

  RIPE-554, NIST USGv6, IPv6 Ready Logo
- IPv6-Roadmap der Hersteller kennen
- Testplan definieren
- Readyness der Security-Produkte in Gesamt-IPv6-Integrationsstrategie berücksichtigen

© 2012 SWITCH

5. Chancen erkennen und nutzen

- Früh anfangen = ohne Zeitdruck sicher umsetzen
- Investitionszyklen und vorhandene Projekte berücksichtigen (Investitionsschutz)
- Schrittweise IPv6-Integration bevorzugen
- Chance für Netzwerk Re-Design ggf. nutzen
- Sicherheitsaspekte rechtzeitig miteinbeziehen

© 2012 SWITCH

Fazit

- Es gibt keine Alternative zu IPv6
- IPv6 ist sicherheitsrelevant
- Nutzen Sie die Zeit!

© 2012 SWITCH

Empfohlene Informationsquellen

- IPv6-Strategie – kurz und gut

  Silvia Hagen – "Planning for IPv6" (O'Reilly)

- IPv6-Security – ausführlich und technisch

  S. Hogg / E. Vyncke – "IPv6 Security" (Cisco Press)

- Swiss IPv6 Council – Austausch, Events

  http://swissipv6council.ch

- SWITCH-Training "IPv6 Deployment & Security" ab Q1/13

  http://www.switch.ch/securitytraining/

© 2012 SWITCH

Fragen?

frank.herberg@switch.ch

© 2012 SWITCH