Residential IPv6 at Swisscom, an overview
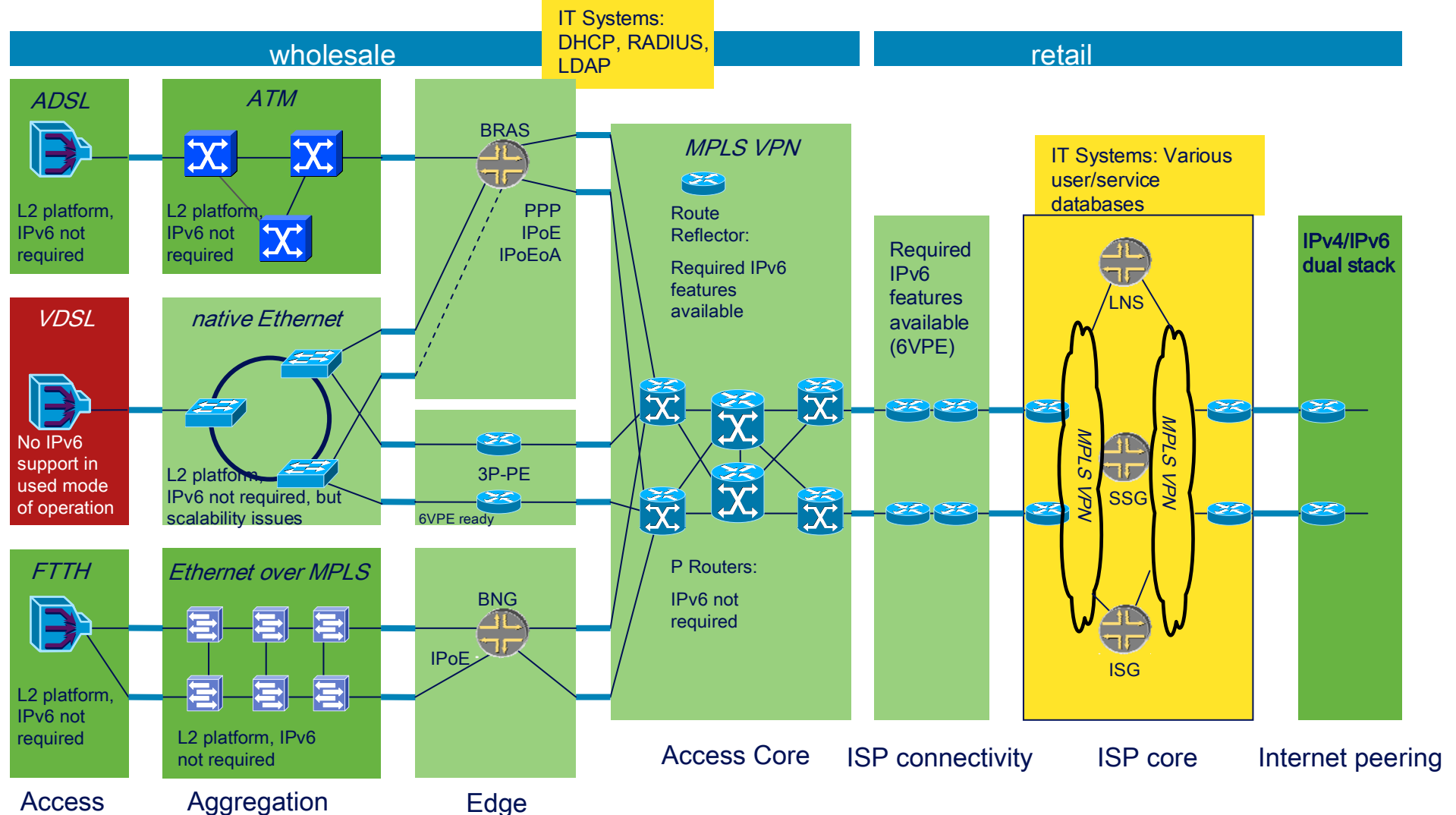
Martin Gysi

swisscom

What is Required for an IPv6 Internet Access Service?

Complex Infrastructure is Barrier to Cost-efficient IPv6 Deployment. Legacy Infrastructure Cannot be Upgraded Easily.

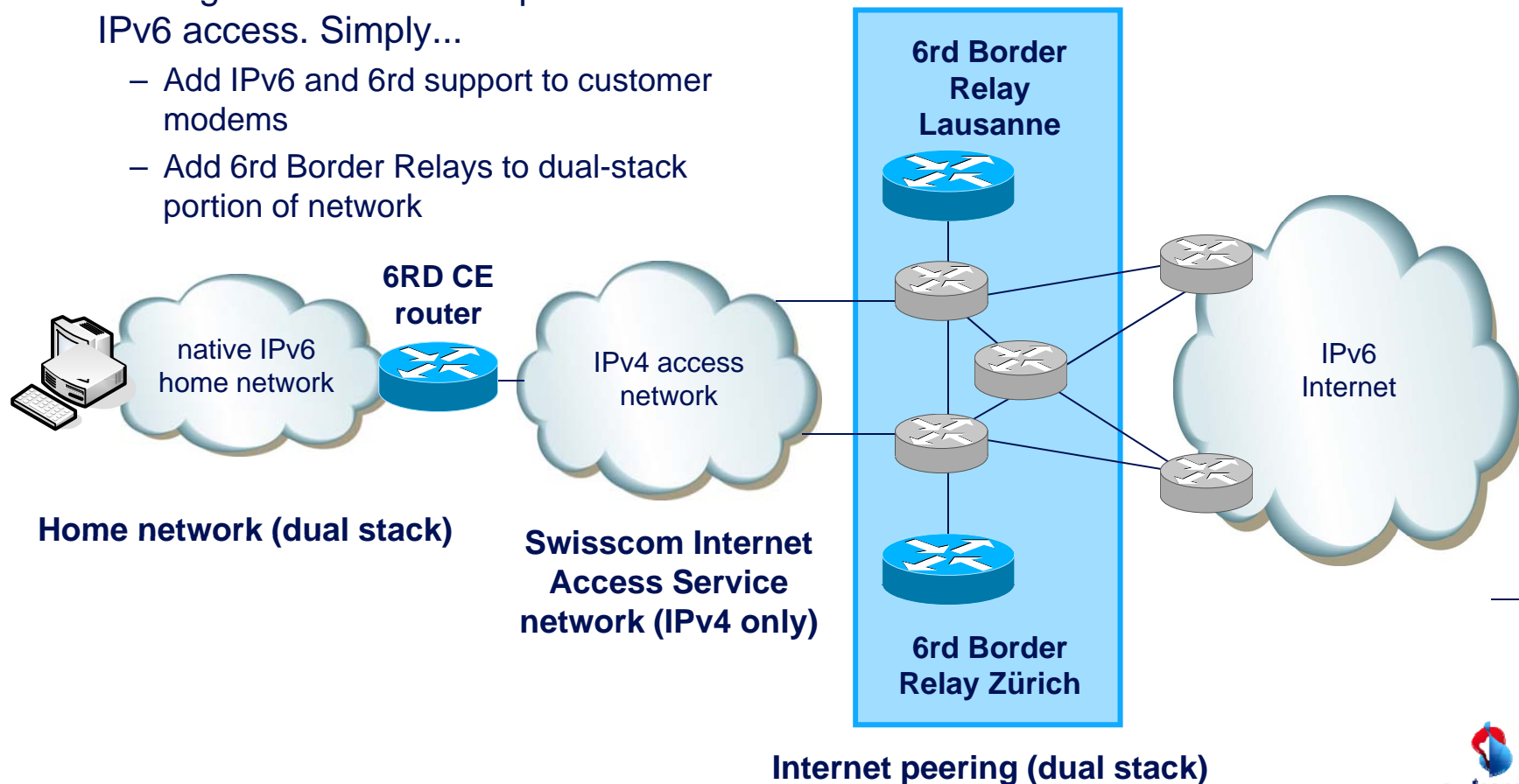**End-to-end overview of Swisscom's Internet Access Service**

wholesale

retail

IT Systems: DHCP, RADIUS, LDAP

ADSL

L2 platform, IPv6 not required

ATM

L2 platform, IPv6 not required

VDSL

No IPv6 support in used mode of operation

native Ethernet

L2 platform, IPv6 not required, but scalability issues

FTTH

L2 platform, IPv6 not required

Ethernet over MPLS

L2 platform, IPv6 not required

BRAS

PPP
IPoE
IPoEoA

3P-PE

6VPE ready

BNG

IPoE

MPLS VPN

Route Reflector:

Required IPv6 features available

P Routers:

IPv6 not required

Required IPv6 features available (6VPE)

IT Systems: Various user/service databases

LNS

MPLS VPN

SSG

MPLS VPN

ISG

IPv4/IPv6 dual stack

Access Core

ISP connectivity

ISP core

Internet peering

Access

Aggregation

Edge

6rd benefits
Production-quality IPv6 Internet Access at a Fraction of the Costs

- No complex upgrade of infrastructure, leverage IPv4 network to provide IPv6 access. Simply...
  - Add IPv6 and 6rd support to customer modems
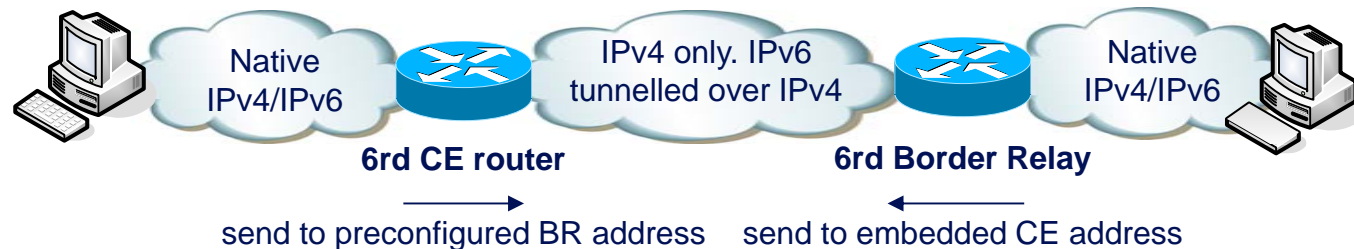 - Add 6rd Border Relays to dual-stack portion of network

6rd Border Relay Lausanne

6RD CE router

native IPv6 home network

IPv4 access network

IPv6 Internet

Home network (dual stack)

Swisscom Internet Access Service network (IPv4 only)

6rd Border Relay Zürich

Internet peering (dual stack)

swisscom

IPv6 Rapid Deployment on IPv4 Infrastructures (RFC 5969) 6RD is a Stateless Tunnel Technology, Embedding the CE's IPv4 Address into the IPv6 Prefix.
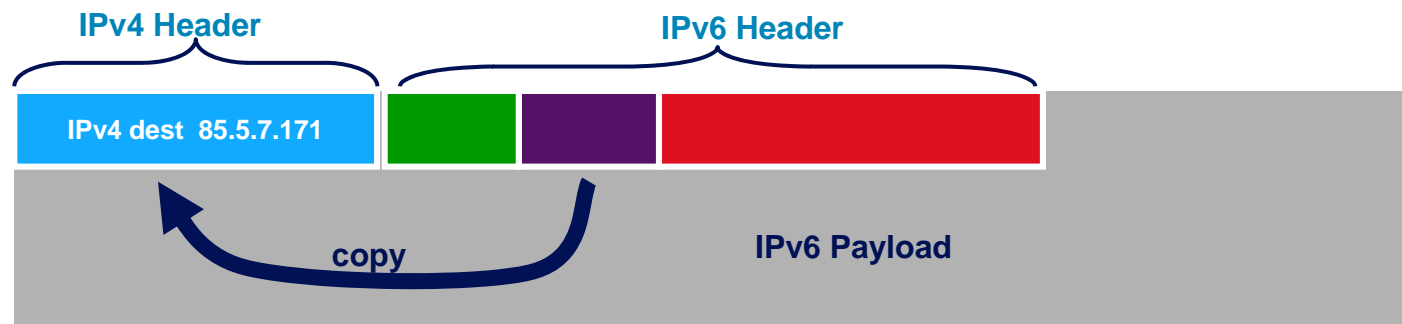
Network topology

Native IPv4/IPv6

IPv4 only. IPv6 tunnelled over IPv4

Native IPv4/IPv6

6rd CE router

6rd Border Relay

send to preconfigured BR address

send to embedded CE address

IPv6 address format for 6rd

2A02:1200	85.5.7.171	Subnet ID	Interface ID

0   28   60   64

6RD prefix

subscriber subnetting

up to 32 bits of subscriber's IPv4 address
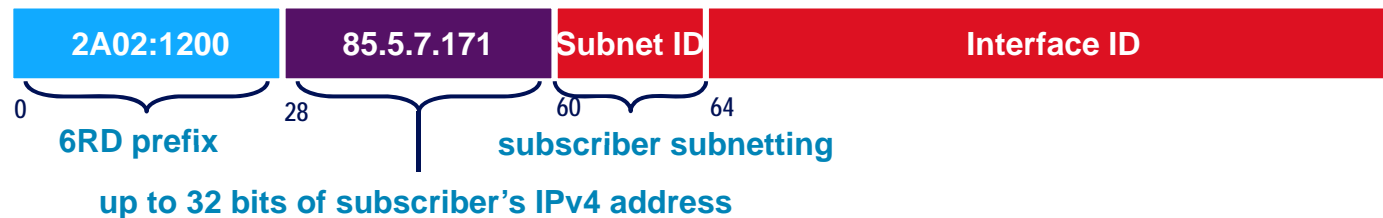
IPv4 header & encapsulated IPv6 packet (downstream)

IPv4 Header

IPv6 Header

IPv4 dest 85.5.7.171

IPv6 Payload

copy

6rd Border Relay
Implementation Details

- Cisco ASR1002-ESP10
  → scales up to 10 Gb/s per box (tested)

- Using anycast IPv4 address, geographically distributed → scale by adding more boxes

- Topology: "Router on a stick"
  → No danger of black hole routing, as IPv4 and IPv6 interface status is inherently coupled.

Router on a stick

6RD Border Relay

IPv4 + IPv6

OSPFv2

OSPFv3

IPv4

IPv6

Dual stack core router

Link failure propagated on both IGPs

Separate IPv4 and IPv6 interface

6RD Border Relay

OSPFv2

OSPFv3

IPv4

IPv6

Link failure not noticed in IPv4 IGP (or vice versa)
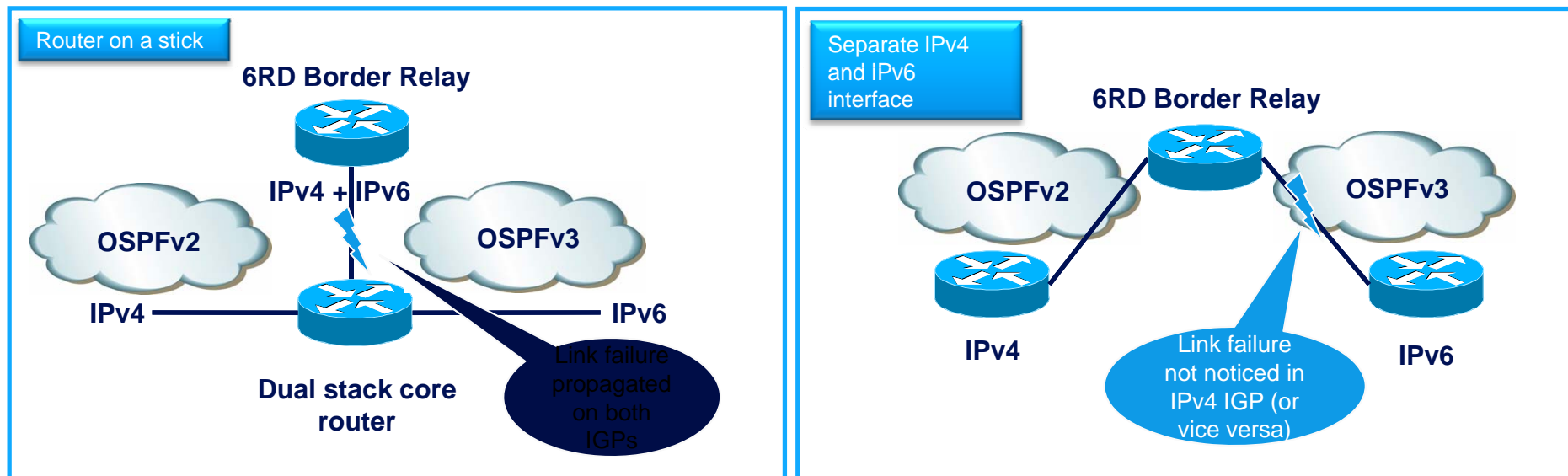
6rd CPE Routers

Implementation Details

- Vendors: Motorola, ADB Broadband (formerly Pirelli Broadband)
- 6rd parameters configured using TR-069 (home device management standard)
  - Swisscom 6rd prefix and length (2a02:1200::/28)
  - IPv4 bits suffix length (all 32 bits)
  - 6rd Border Relay anycast IPv4 address (6rd.swisscom.com)
  - IPv6 flag (enable/disable)
- Third-party modems (AVM Fritz Box and others) work, but need manual configuration

http://supportcommunity.swisscom.ch/t5/media/gallerypage/user-id/63/image-id/3981iF940048F58D2E93C

Pilot and service feedback

No negative experience, but security as a concern

Pilot experience

Security as a concern for initial (Swisscom-internal) pilot users

- 20% of pilot users did not activate IPv6, because
  - They had security concerns
  - They didn't have time to do so
- 10% turned IPv6 off again after having it turned on:
  - More than half cited security concerns

Service experience

IPv6 service running since October 2011
- No network issues detected
- Customers activate IPv6 themselves
- 10% of traffic over IPv6

Active users

1200
1000
800
600
400
200
0

KW47 KW49 KW51 KW1 KW3 KW5 KW7 KW9 KW 11 KW13 KW15 KW17

Aggregate - 6RD BR

IPv6 Throughput

10 M
8 M
6 M
4 M
2 M
0
-2 M
-4 M
-6 M
-8 M
-10 M

in-> [bps] <-out

May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr
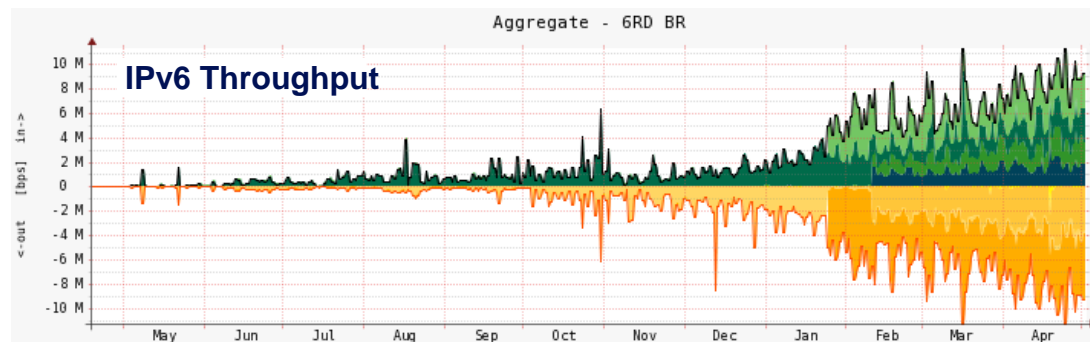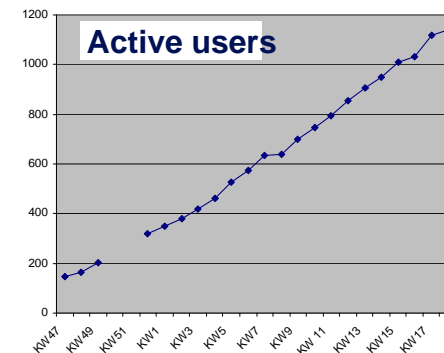
swisscom

Service activation
IPv6 enabled by customer on "customer centre" website

https://sam.sso.bluewin.ch/my/data/ModemMgmtService?mode=overview

What happens when IPv6 is turned on?

Centro router starts advertising IPv6 prefix, end devices construct complete IPv6 address and start using them where possible

Mode of operation

Assingment of IPv6 addresses
- Centro router generates prefix and announces it into the LAN
- Attached devices generate complete address
- IPv6 address is used if DNS query returns an IPv6 address
- IPV4 address is used if DNS query returns an IPv4 address

before

Internetzugang		⊕
Internetverbindung		OK
DSL synchronisiert		OK
DSL-Leitungsmodus		VDSL2
DSL-Verbindungstyp		DHCP
DNS server		195.186.4.162
		195.186.1.162
IP-Adresse im Internet		85.4.218.45
DynDNS		Inaktiv
Messwerte		
Geschwindigkeit	Upstream	11012 kbps
	Downstream	33031 kbps
Leitungsdämpfung	Upstream	10.6 dB
	Downstream	11.0 dB
Signal-Rausch-Abstand	Upstream	20.7 dB
	Downstream	27.0 dB

after

Internetzugang		⊕
Internetverbindung		OK
DSL synchronisiert		OK
DSL-Leitungsmodus		VDSL2
DSL-Verbindungstyp		DHCP
DNS server		195.186.4.162
		195.186.1.162
IP-Adresse im Internet		85.4.218.45
IPv6-Prefix		2a02:1205:504d:a2d0::/64
DynDNS		Inaktiv
Messwerte		
Geschwindigkeit	Upstream	11012 kbps
	Downstream	33031 kbps
Leitungsdämpfung	Upstream	10.6 dB
	Downstream	11.0 dB
Signal-Rausch-Abstand	Upstream	20.7 dB
	Downstream	27.0 dB

swisscom

Security of end devices

End devices communicate directly using IPv6 where possible.
Network layer security assured by IPv6 firewall. Content remains the same…

Protection against unauthorised access

IPv4

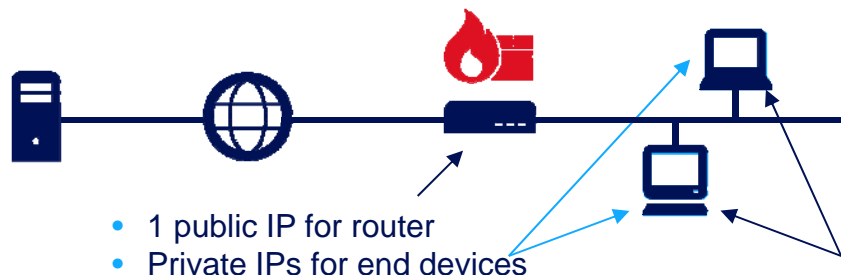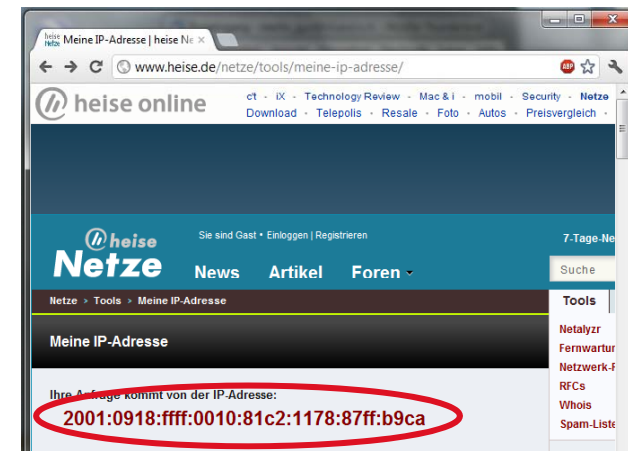**Implicit through NAT function**
- Private addresses not accessible from the outside

IPv6

Explizit through firewall
- End devices with public addresses
- Next firmware release: integrated IPv6 Firewall

- 1 public IP for router
- Private IPs for end devices

- 1 IPv6 prefix for router
- Public IPs for end devices

swisscom

Rollout strategy
IPv6 will be enabled on all capable devices until end of 2012

Today

IPv6 firmware is rolled out to all „centro" routers

- Current firmware contains no firewall yet
- Customers must activate IPv6 themselves on the customer portal web page. 1200 today.

World IPv6 launch

6.6.2012: Start of permanent IPv6 service of Google, Facebook – and Swisscom

- If possible, up to 40'000 pilot devices before June 6th (world IPv6 launch)
- www.swisscom.com over IPv6

World Pv6 Day

Next steps

Rollout plans for 2012

- Firewall firmware to be rolled out by July (Mot), November (ADB)
- IPv6 turned on by default
- About 600'000 devices today, forecast 650'000 eoy. Customer base 1.7 Mio.
- No active replacement due to IPv6
- Device exchange driven by business requirements, i.e. change from ADSL to VDSL or FTTH.

IPv6 Firewall: Easy to use, but customisable

Normal users can rely on firewall as-is, expert users have options to customise IPve firewall

Experte mode

Firewall

85.4.218.45/cgi-bin/firewall.ha

DSL-Modem (Router) Konfiguration

DE | FR | IT | EN   swisscom

Übersicht   Einstellungen   Diagnose   Logout

Netzwerk
Telefonnummer(n)
DSL-Modem (Router)
Sicherheit

Sicherheit

IPv6 Firewall   Expertenmodus

IPv6 Firewall Modus festlegen

Die IPv6 Firewall ist standardmässig auf "Mittel" eingestellt

○ Aus
◉ Mittel
○ Hoch

Speichern   Abbrechen

Hilfe

Aus
Nur grundlegende Datenverkehrs-Kontrollen sind aktiviert um vor ungültigem und schädlichem Datenverkehr zu schützen. Der restliche Datenverkehr wird durchgelassen.

Mittel
Lässt IPv6 Datenverkehr in beide Richtungen zu, mit Ausnahme einer Gruppe von Standardprotokollen und benutzerdefinierten Regeln, welche Sie definieren. Die grundlegende Datenverkehrs-Kontrolle ist ebenfalls aktiviert um vor ungültigem und schädlichem Verkehr zu schützen.

Hoch
IPv6 Datenverkehr darf nur in abgehender Richtung initiiert werden. Davon ausgenommen ist eine Gruppe von Standard Protokollen und benutzerdefinierten Regeln, welche Sie definieren. Die grundlegende Datenverkehrs-Kontrolle ist ebenfalls aktiviert um vor ungültigem und schädlichem Verkehr zu schützen.

Copyright Swisscom AG 2012 | Alle Rechte vorbehalten
Über

Sicherheit

IPv6 Firewall   Expertenmodus

Mittel Firewall Modus

Neue benutzerdef. Regel hinzufügen

Neue benutzerdef. Regel hinzufügen
Standardregeln   Alle Standardregeln aktivieren
Fernwartungs-Protokolle   Fernwartung nie zulassen   Fernwartung immer zulassen

Aktivieren	Dienst	Protokoll	Ports	Blockieren
☑	Telnet	TCP	23	Eingehend
☑	Appleshare IP Web Admin	TCP	311	Eingehend
☑	rlogin	TCP	513	Eingehend
☑	Mac OS X Server Admin	TCP	660	Eingehend
☑	ASIP Registry	TCP	687	Eingehend
☑	Samba Web Administration Tool	TCP	901	Eingehend
☑	Telnet over TLS/SSL	TCP	992	Eingehend
☑	QT Server Administration	TCP	1220	Eingehend
☑	VNC Listener	TCP	5500	Eingehend
☑	VNC over HTTP	TCP	5800	Eingehend
☑	VNC remote desktop protocol	TCP	5900	Eingehend
☑	TeamViewer remote desktop proto.	TCP	5938	Eingehend
☑	WBEM HTTP, Apple Remote Desktop	TCP	5988	Eingehend

LAN Protokolle

Aktivieren	Dienst	Protokoll	Ports	Blockieren
☑	WINS	Beide	42	Ankommend/Abgehend
☑	TACACS	Beide	49	Ankommend/Abgehend

Hilfe

Aus
Es ist nur eine grundlegende Datenverkehrs-Kontrolle aktiviert um vor ungültigem und schädlichem Verkehr zu schützen, da die IPv6 Firewall ausgeschalten ist. Schalten Sie die Firewall ein um sämtliche Funktionen des Experten Modus zu benützen.

Mittel
Falls die IPv6 Firewall Stufe ""Mittel"" aktiviert ist, wird der IPv6 Datenverkehr in beide Richtungen (ankommend und abgehend) zugelassen. Davon ausgenommen ist eine Gruppe von Standard Protokollen (Gruppiert in ""Fernwartungs-Protokolle"" und ""LAN-Protokolle"") und alle benutzerdefinierten Regeln, welche Sie definieren. TCP Ports, welche zur Kategorie ""Fernwartungs-Protokolle"" gehören, werden nicht aus dem ankommenden Datenverkehr gefiltert. UDP und TCP Ports, welche zur Kategorie "LAN-Protokolle" gehören werden im abgehenden und ankommen Datenverkehr blockiert.

Andere grundlegende Datenverkehrs-Kontrollen sind aktiviert um vor ungültigem und schädlichem Verkehr zu schützen.

Falls Sie eine Regel durch deaktivieren des Kontrollkästchens ausschalten, wird automatisch der Firewall-Status "Mittel" angewendet, welcher für die spezifizierten Ports den Datenverkehr in beiden Richtungen (ankommend und abgehend) erlaubt.

Hoch
Falls die IPv6 Firewall Stufe ""Hoch"" aktiviert ist, wird der IPv6 Datenverkehr nur in abgehende Richtungen zugelassen. Davon ausgenommen sind ""LAN-Protokolle"" und benutzerdefinierte Regeln, welche Sie definieren. UDP und TCP

swisscom