

Residential IPv6 at Swisscom, an overview

Martin Gysi

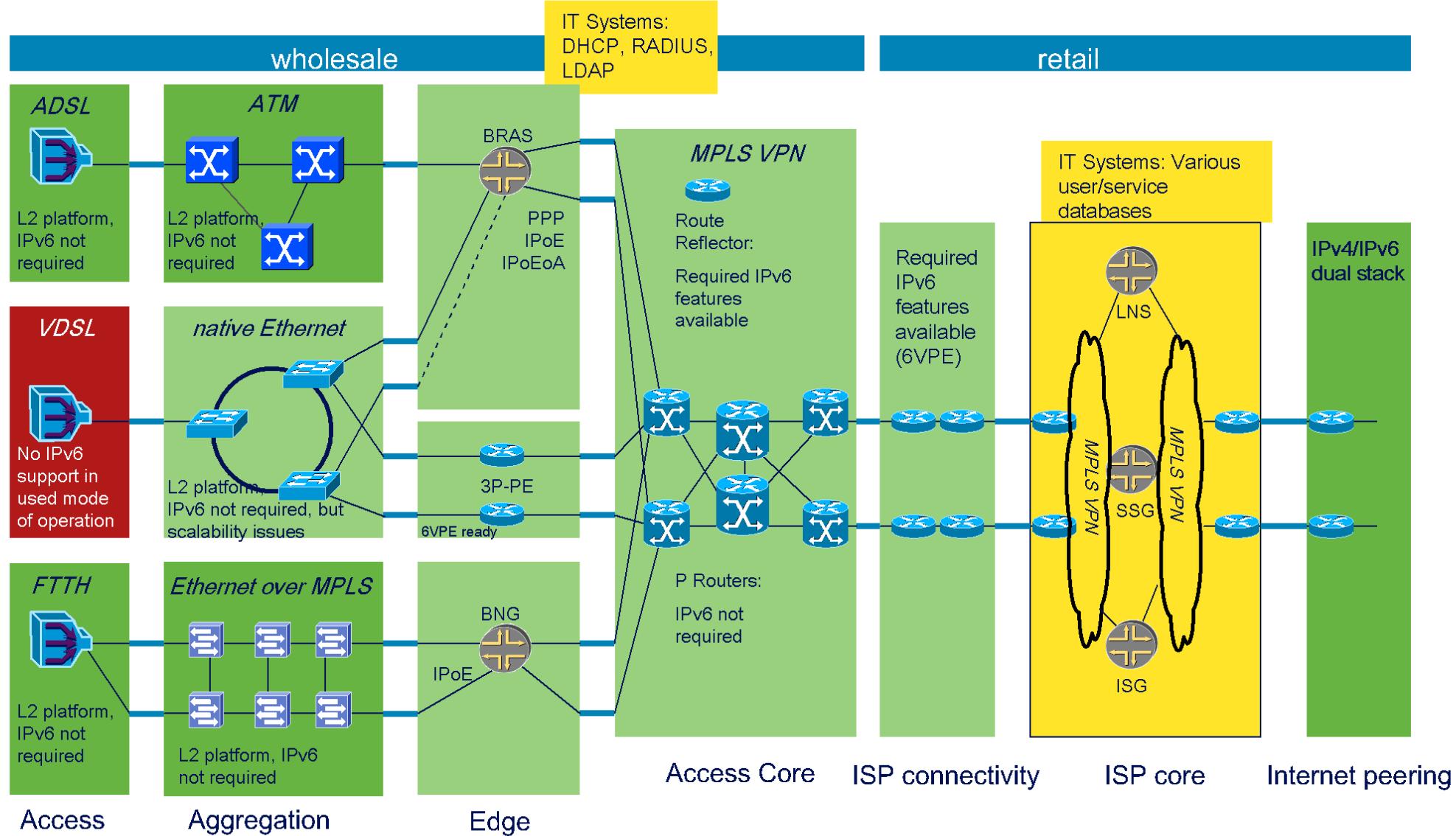


What is Required for an IPv6 Internet Access Service?

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

2

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

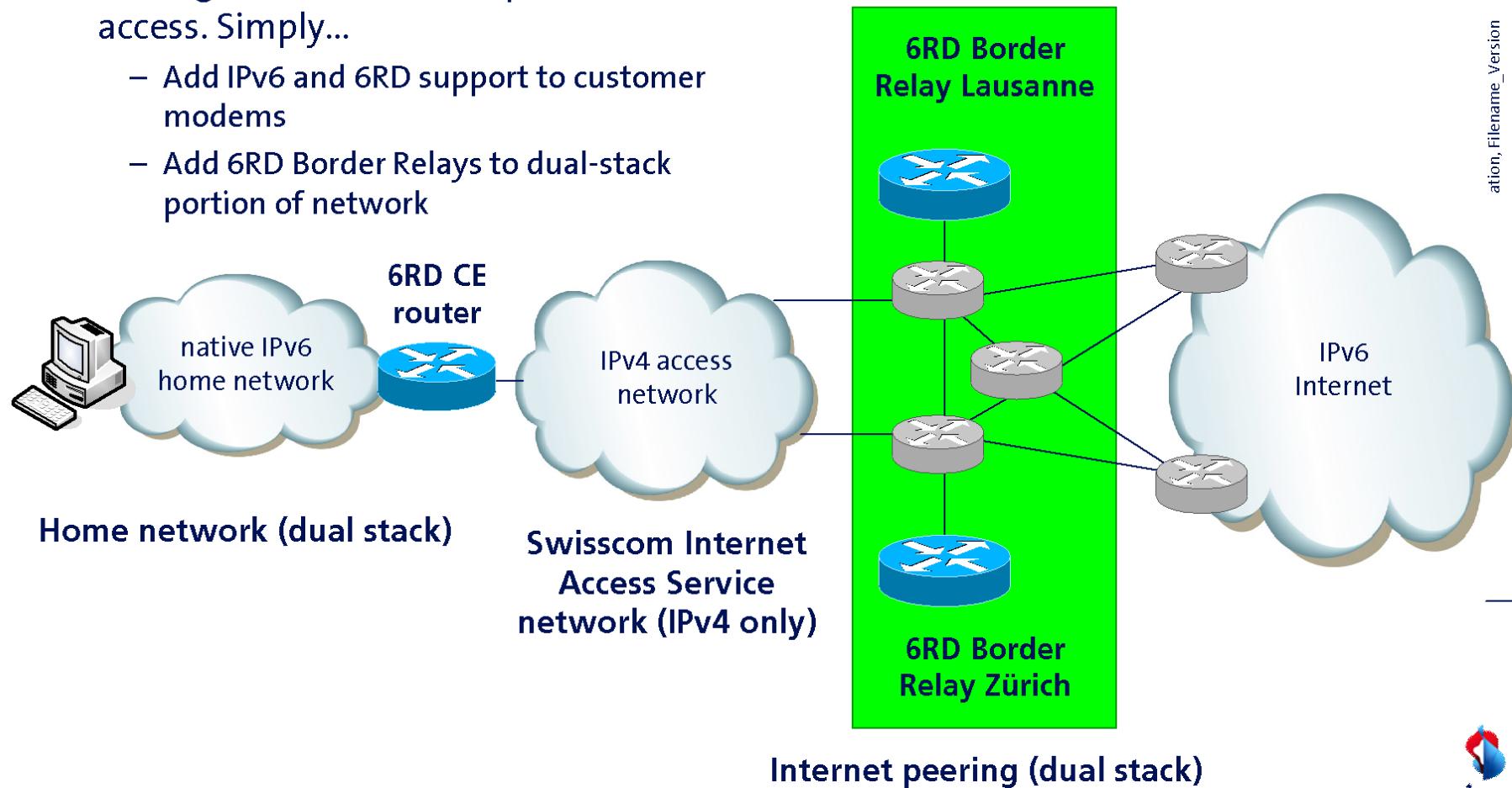


Using 6RD, IPv6 Internet Access is an Incremental Upgrade. Production-quality IPv6 Internet Access at a Fraction of the Costs

3

dd/mm/yyyy
ation,Filename_Version

- 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

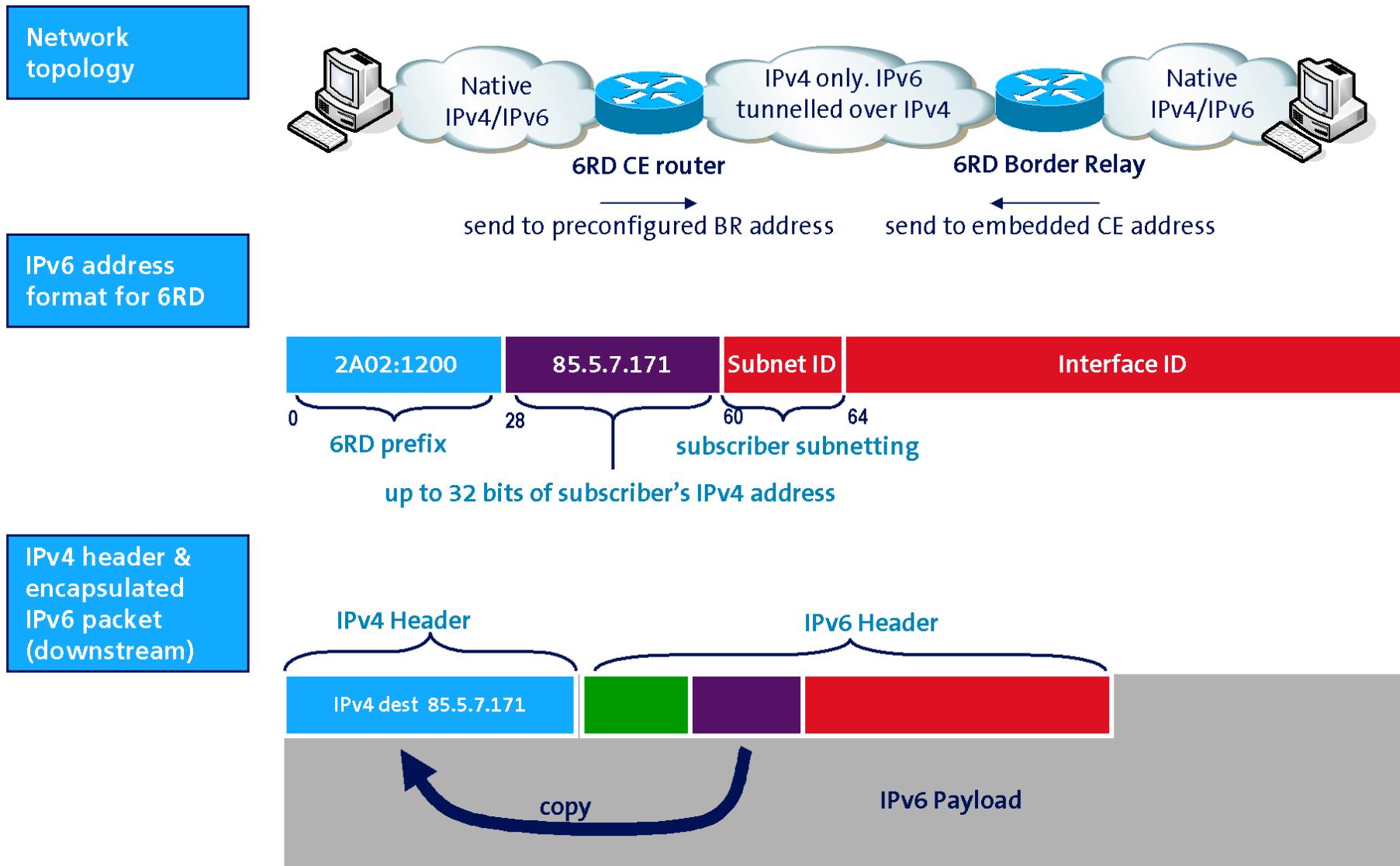


6RD is a Stateless Tunnel Technology, Embedding the CE's IPv4 Address into the IPv6 Prefix.

IPv6 Rapid Deployment on IPv4 Infrastructures (RFC 5969)

4

Classification, First name & surname, Organization, Filename_Version_dd/mm/yyyy



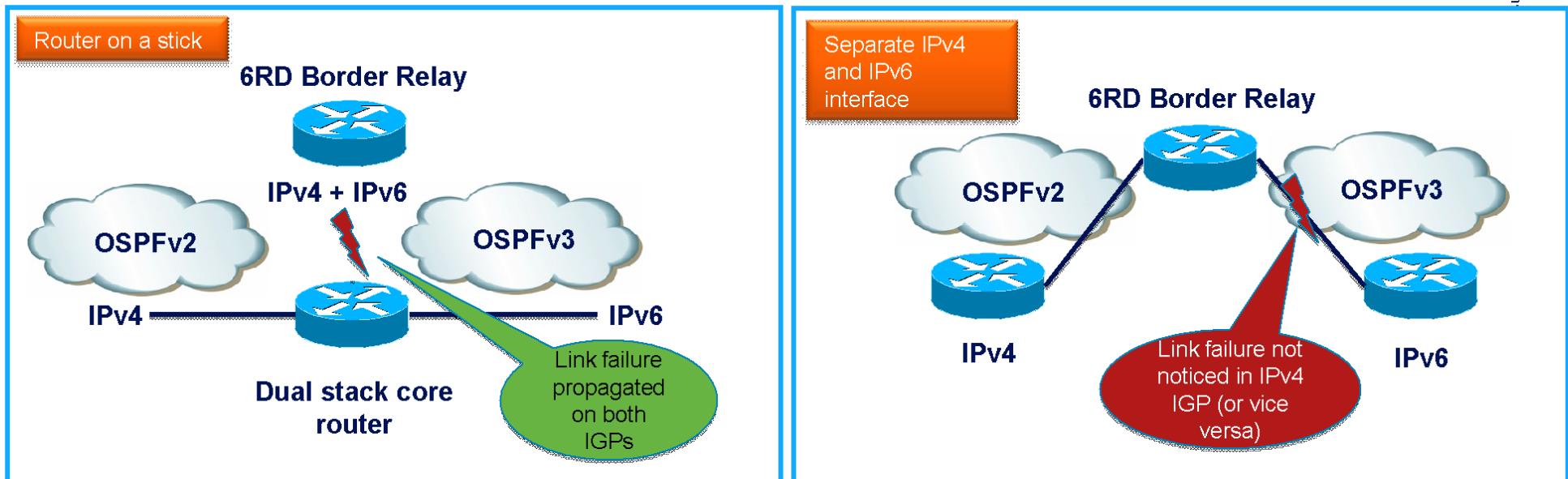
6RD Border Relay

Implementation Details

5

username, Organization, Filename_Version dd/mm/yyyy

- 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.



6RD CPE Routers

Implementation Details

6

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



Classification, First name & surname, Organization, Filename_Version dd/mm/yyyy

IPv6 enabled by customer on “customer centre” website

7

The screenshot shows a Mozilla Firefox browser window with the title "Swisscom - Kundencenter - Mozilla Firefox". The URL in the address bar is <https://sam.sso.bluewin.ch/my/data/ModemMgmtService?mode=overview&bundle=10829>. The page content is titled "DSL-Modem einrichten". It displays information about a "Centro piccolo" modem, including its model number (Centro piccolo), serial number (158003207552), and firmware version (9.0.10hd6c). Below this, there are sections for "DSL-Modem Details" and "Internet-Zugang Details". The "Internet-Zugang Details" section contains fields for "Benutzername" (admin) and "Passwort" (*****). At the bottom of the page, there is a section titled "IPv6 Details" which is highlighted with a red box. This section contains text explaining IPv6 as the successor to IPv4, stating that Swisscom recommends activating it for expert users, and noting that it is currently in a pilot phase. It also shows the IPv6 address block (2a02:1205:c68e:8b40::/60) and a link to deactivate it.

Classification, First name & surname, Organization, Filename_Version dd/mm/yyyy



Pilot customer feedback

8

- 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
- Security _is_ a concern for our customers. Feedbacks:

„Meine Bedenken waren v.a. punkto Sicherheit/Firewall etc.“

„Zeit knapp und bedenken wegen eigenem Netzwerk innerhalb des Hauses mit fixen IP Adressen“

Sicherheitsbedenken da keine HW Firewall dazwischen ist. Keine grossen Vorteile, da einzelne Dienste mit NAT auch von aussen erreichbar sein können. Ich möchte auch wählen können, welche Geräte von aussen erreichbar sein können, mit IPv6 sind einfach alle.

Das Centro Grande braucht dringend eine einfache Firewall, um die Kunden PCs, iPads, Smartphones, Playstations, Drucker, Set Top Boxes etc. vor dem Internet zu schützen.

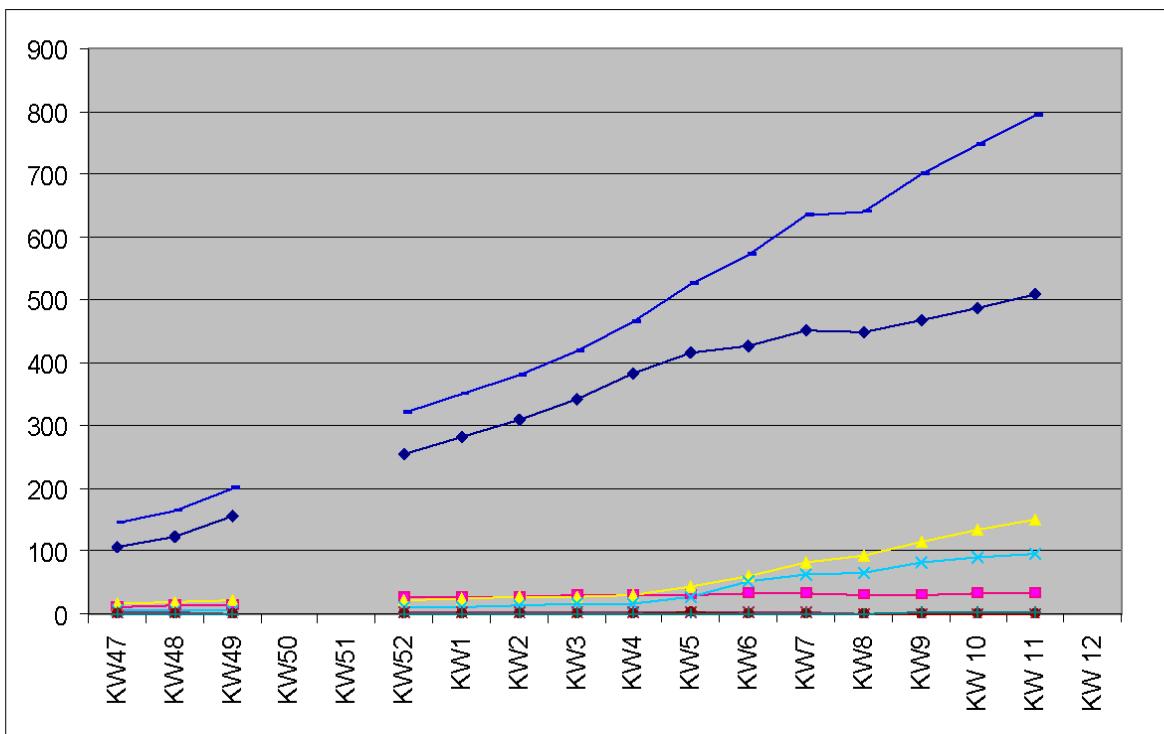
Die Firewall muss im Router integriert werden

...

Rollout strategy

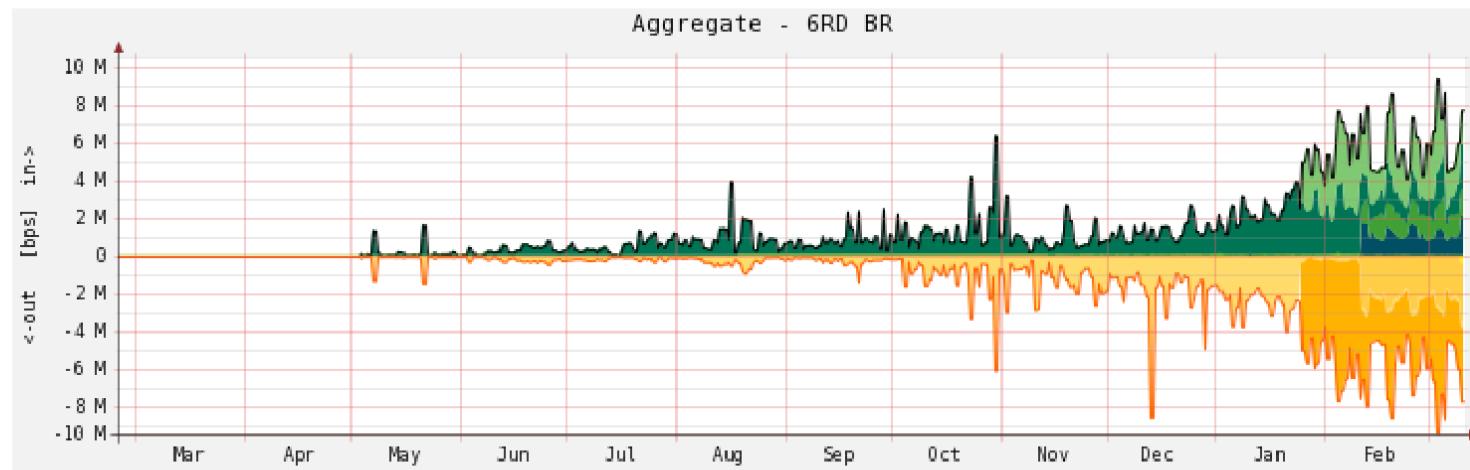
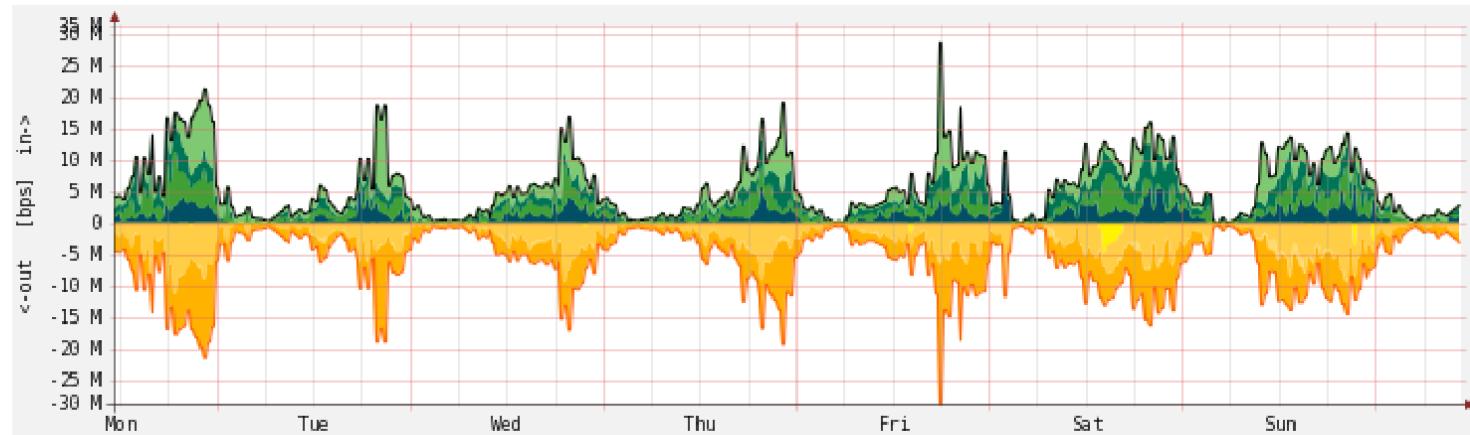
9

- 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. 794 today.



Traffic

10



Rollout plans for 2012

11

- Firewall firmware to be rolled out by July (Mot), November (ADB)
- IPv6 turned on by default
- If possible, 40'000 pilot devices before June 6th (world IPv6 launch)
- About 500'000 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.

Classification, First name & surname, Organization, Filename_Version dd/mm/yyyy

IPv6 Firewall with three levels

12

dd/mm/yyyy

Classification, First name & surname, Organization, Filename_Version

Router Configuration

The screenshot shows the Swisscom Router Configuration interface. The top navigation bar includes links for DE, FR, IT, EN, and a swisscom logo. Below the navigation is a menu bar with Network, Phone Number(s), Router, and Security tabs. The Router and Security tabs are highlighted with red boxes. The main content area has tabs for Overview, Settings, Diagnostics, Security, IPv6 Firewall, and Expert Mode. The Security tab is active. The IPv6 Firewall tab is also highlighted with a red box. On the left, there's a sidebar with Network, Phone Number(s), Router, and Security sections. The Router and Security sections are highlighted with red boxes. The main content area displays 'IPv6 Firewall Mode Settings' with three options: Off (radio button), Medium (radio button, selected), and High (radio button). Below these are Save and Cancel buttons. To the right, there's a Help section with detailed descriptions for Off, Medium, and High modes.

DE | FR | IT | EN Logout

Network
Phone Number(s)
Router
Security

Security

IPv6 Firewall **Expert Mode**

IPv6 Firewall Mode Settings

Off
 Medium
 High

Save Cancel

Help

Off
Only basic sanitation checks to protect from invalid and malicious traffic are enabled.

Medium
Passes IPv6 traffic in both directions, except for a set of Standard Protocols and "Custom Rules" that you define. Basic sanitation checks to protect from invalid and malicious traffic are also enabled.

High
IPv6 Traffic is allowed to be initiated only in the outbound direction, except for a set of Standard Protocols and "Custom Rules" that you define. Basic sanitation checks to protect from invalid and malicious traffic are also enabled.

Firewall level „medium“: Default behaviour is „permit“

13

- Firewall passes all traffic except for a defined set of protocols (including the sanitation checks from firewall setting “off”).
 - LAN protocols: Dropped in both inbound and outbound direction
 - Remote management protocols: Outbound only. Inbound TCP connection establishment prohibited by blocking inbound TCP packets with only the SYN flag set.
- User can allow inbound remote management protocols with a single click
- Incorporates the sanitation rules of the „off“ level

Classification, First name & surname, Organization, Filename_Version dd/mm/yyyy

Firewall level „high“: Default mode is „deny“ in inbound direction. Stateful firewall using connection tracking.

14

- Drops all inbound traffic except for traffic belonging to a session established from the inside, using connection tracking
- This stateful firewall mimics the firewall behaviour of an IPv4 NAT device.

Classification, First name & surname, Organization, Filename_Version dd/mm/yyyy

Medium firewall, expert mode

Router Configuration

15

DE | FR | IT | EN  swisscom

Logout

Overview Settings Diagnostics

Network Phone Number(s) Router Security

IPv6 Firewall Expert Mode

Security

Medium Firewall Mode

Add new custom rule

Add new custom rule Standard Rules Enable All Standard Rules

Remote Management Protocols

Enable Rule name Protocol Ports Block

<input checked="" type="checkbox"/>	Telnet	TCP	23	Inbound
<input checked="" type="checkbox"/>	Mac OS X Server Admin	TCP	311	Inbound
<input checked="" type="checkbox"/>	rlogin	TCP	513	Inbound
<input checked="" type="checkbox"/>	Mac OS X Server Administration	TCP	660	Inbound
<input checked="" type="checkbox"/>	Mac OS X Server Administration	TCP	687	Inbound
<input checked="" type="checkbox"/>	Samba Web Administration Tool	TCP	901	Inbound
<input checked="" type="checkbox"/>	Telnet over TLS/SSL	TCP	992	Inbound
<input checked="" type="checkbox"/>	QT Server Administration	TCP	1220	Inbound
<input checked="" type="checkbox"/>	VNC Listener	TCP	5500	Inbound
<input checked="" type="checkbox"/>	VNC over HTTP	TCP	5800	Inbound
<input checked="" type="checkbox"/>	VNC remote desktop protocol	TCP	5900	Inbound
<input checked="" type="checkbox"/>	TeamViewer remote desktop proto.	TCP	5938	Inbound
<input checked="" type="checkbox"/>	WBEM HTTP, Apple Remote Desktop	TCP	5988	Inbound

Enable Rule name Protocol Ports Block

<input checked="" type="checkbox"/>	WINS	Both	42	Inbound/Outbound
<input checked="" type="checkbox"/>	TACACS	Both	49	Inbound/Outbound

Help

Off
Only basic sanitation checks to protect from invalid and malicious traffic are enabled, because IPv6 Firewall is turned off. Turn on the firewall to use the features of Expert Mode.

Medium
When the IPv6 Firewall Level is Medium, the firewall passes IPv6 traffic in both directions, except for a set of Standard Protocols (grouped into "Remote Management Protocols" and "LAN Protocols"), and any "Custom Rules" that you define. TCP Ports that belong to the "Remote Management Protocols" category are not filtered in the inbound direction. UDP and TCP Ports that belong to the "LAN Protocols" category are blocked in the inbound and outbound directions.

Other basic sanitation checks to protect from invalid and malicious traffic are enabled.

When you disable a Rule, by unchecking its "Enable" checkbox, this means the Medium Firewall level default behavior will apply, allowing traffic in both directions to the port(s) specified.

High
When the IPv6 Firewall Level is set to High, traffic is allowed to be initiated only in the outbound direction, except for a set of standard "LAN Protocols", and any "Custom Rules" that you define. UDP and TCP Ports that belong to the "LAN Protocols" category are blocked in the inbound and outbound directions.

Other basic sanitation checks to protect from invalid and malicious traffic are enabled.

When you disable a Rule, by unchecking its "Enable" checkbox, this means the High Firewall Level default behavior will apply.

Classification, First name & surname, Organization, Filename_Version_dd/mm/yyyy



Defining a custom rule

16

- Choose port range or single port
- Then hit save

Add new custom rule

Rule name

Rule name Name, e.g. «MyRule»

Add ports for this rule

1 Protocol
Select the required protocol

2 Ports
Enter the required ports
--Choose--
Port numbers to Port numbers, e.g. 21

--Choose--
Both
Single port
Port range

1 Protocol
Select the required protocol

2 Ports
Enter the required ports
Single port
Port numbers Port numbers, e.g. 21