Residential IPv6 at Swisscom, an overview

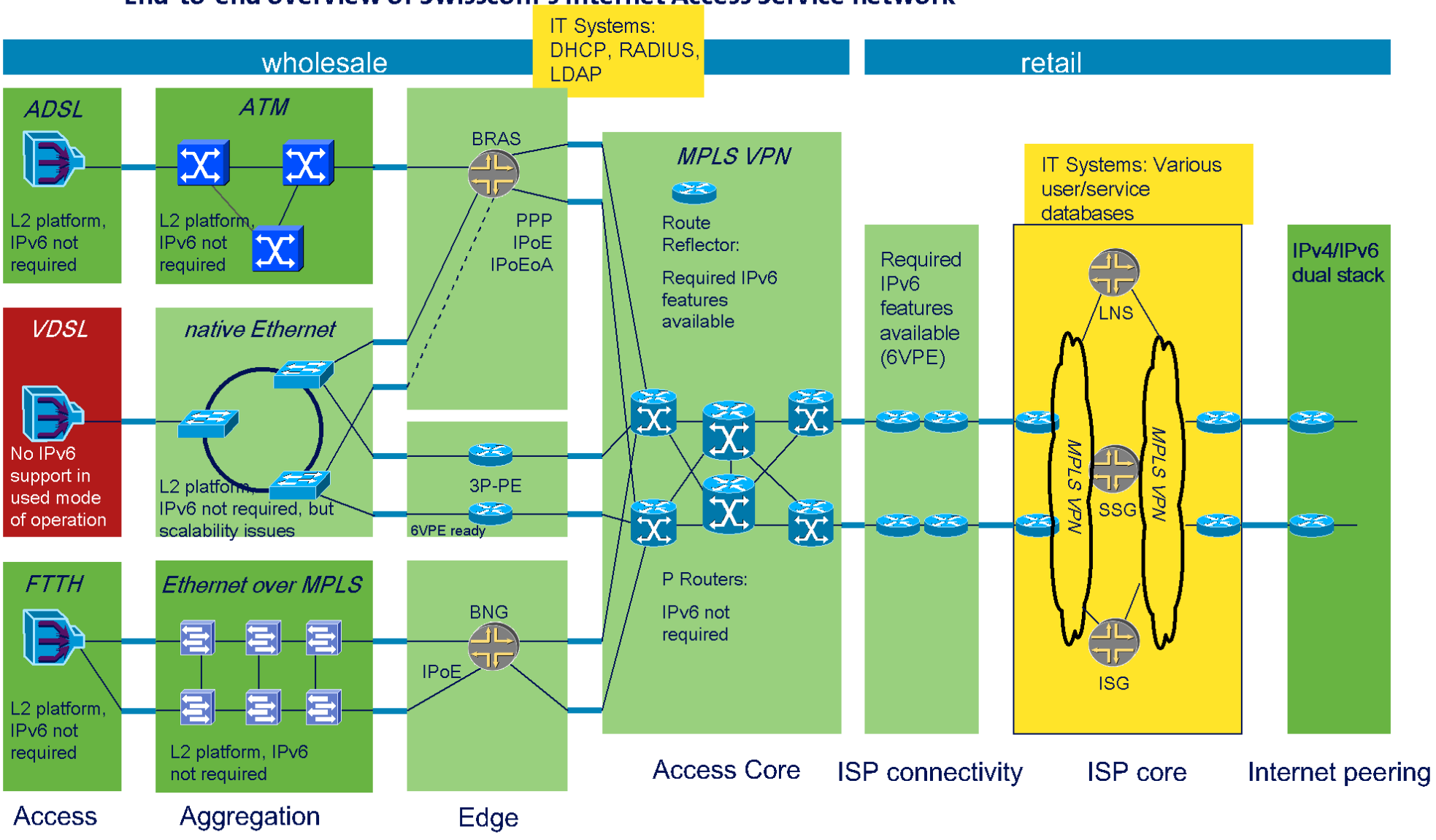
Martin Gysi

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.

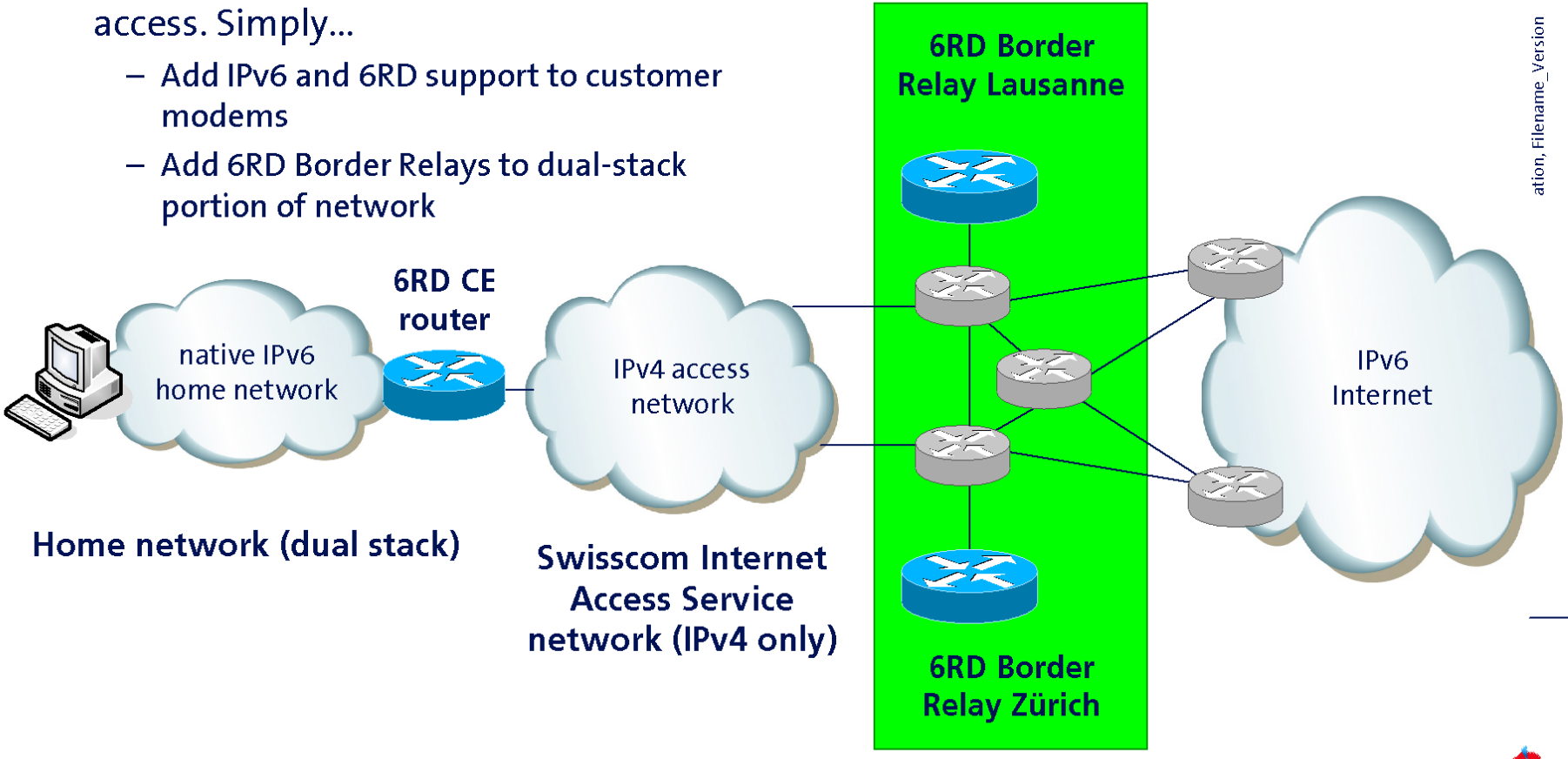
End-to-end overview of Swisscom's Internet Access Service network



Using 6RD, IPv6 Internet Access is an Incremental Upgrade.

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

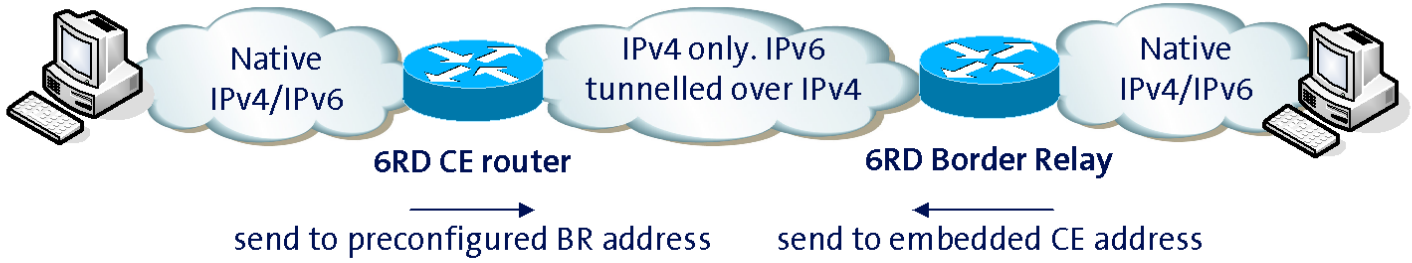


swisscom

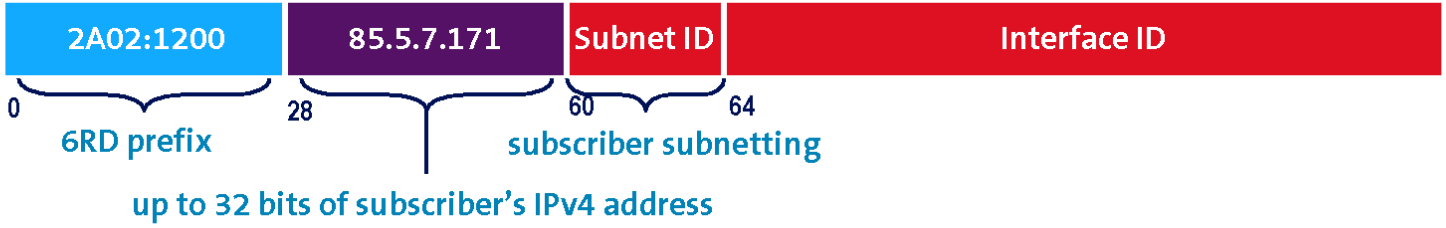
6RD is a Stateless Tunnel Technology, Embedding the CE's IPv4 Address into the IPv6 Prefix.

IPv6 Rapid Deployment on IPv4 Infrastructures (RFC 5969)

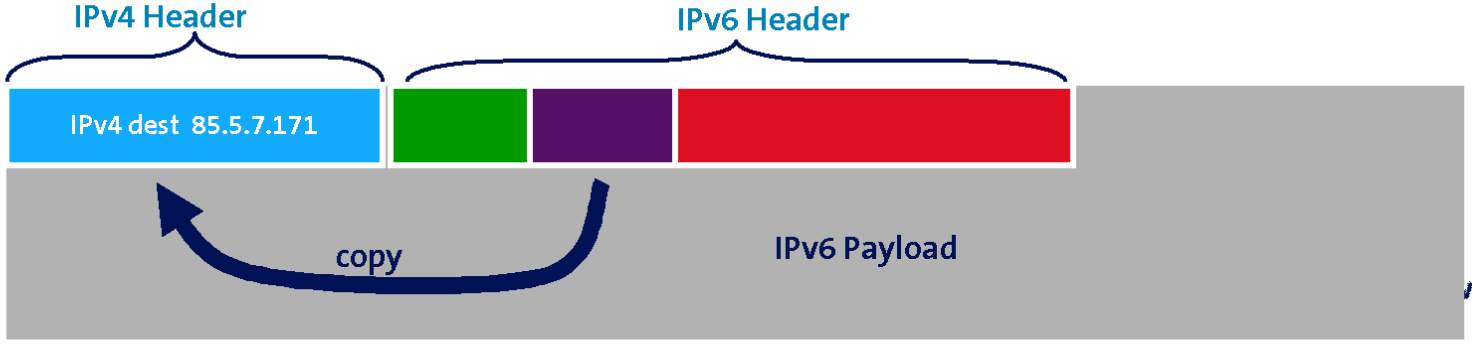
Network topology



IPv6 address format for 6RD

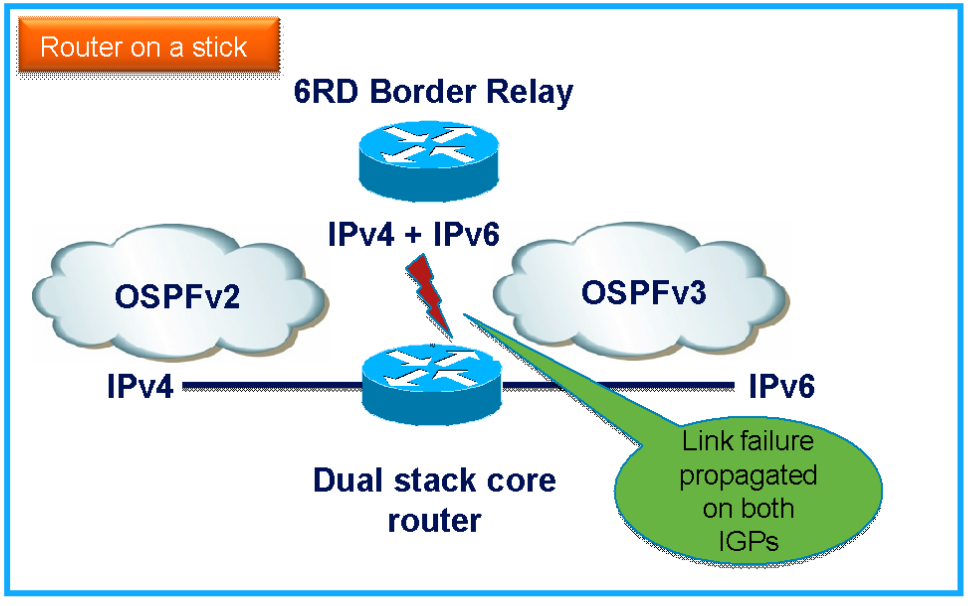


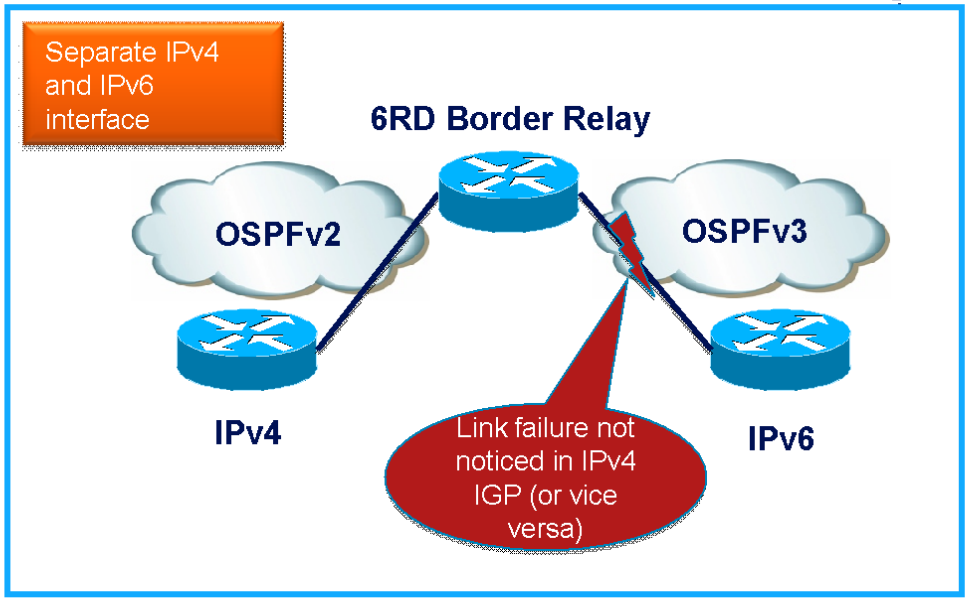
IPv4 header & encapsulated IPv6 packet (downstream)



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.





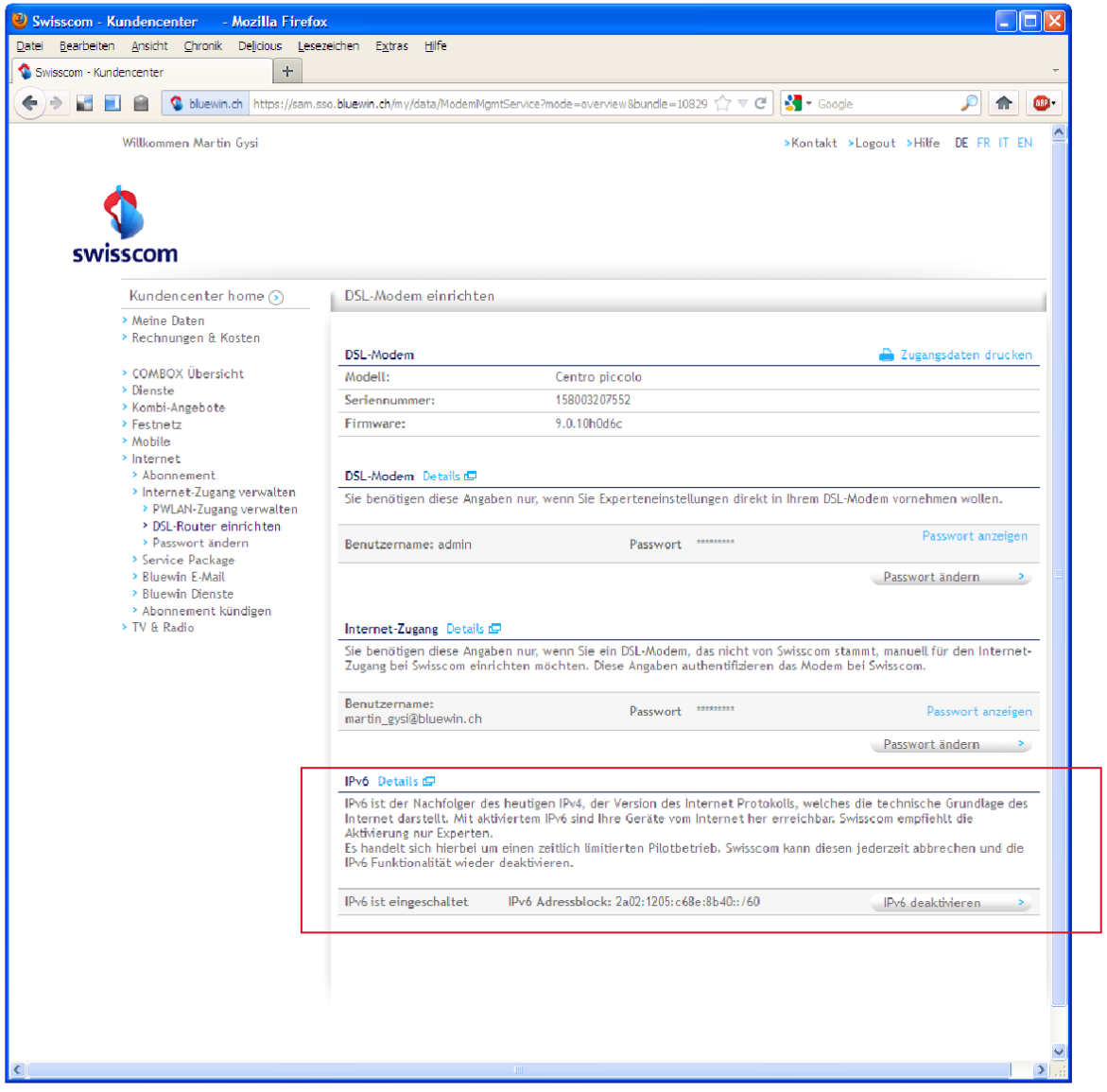
6RD CPE Routers

Implementation Details

- **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**

swisscom

IPv6 enabled by customer on “customer centre” website



swisscom

Pilot customer feedback

- 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.

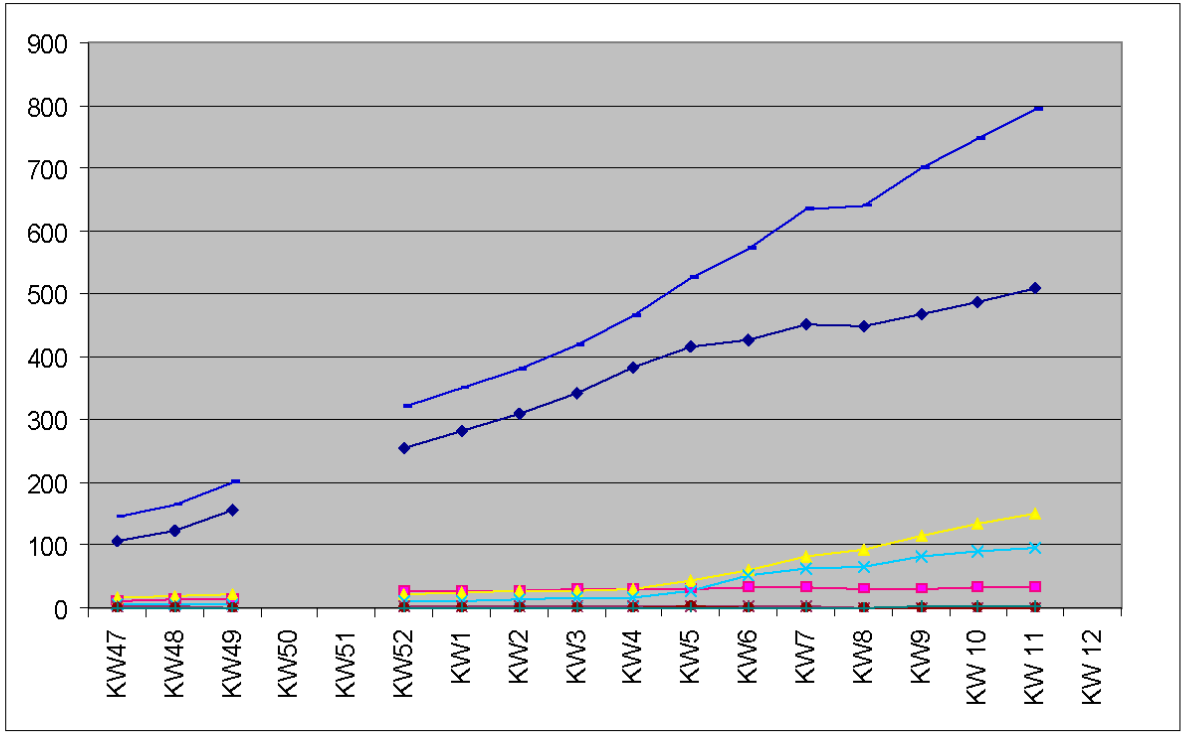
Das Centro Grande braucht dringend eine einfache Firewall, um die Kunden PCs, iPads, Smartphones, Playstations, Drucker, Set Top Boxes etc. vor dem Internet zu schützen.

Die Firewall muss im Router inegriert werden

...

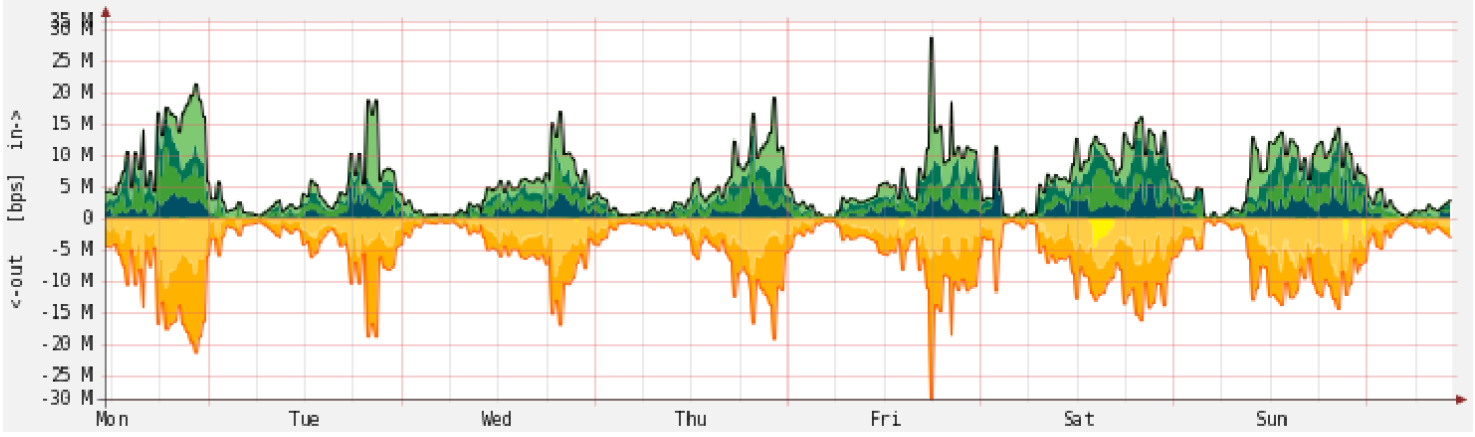
Rollout strategy

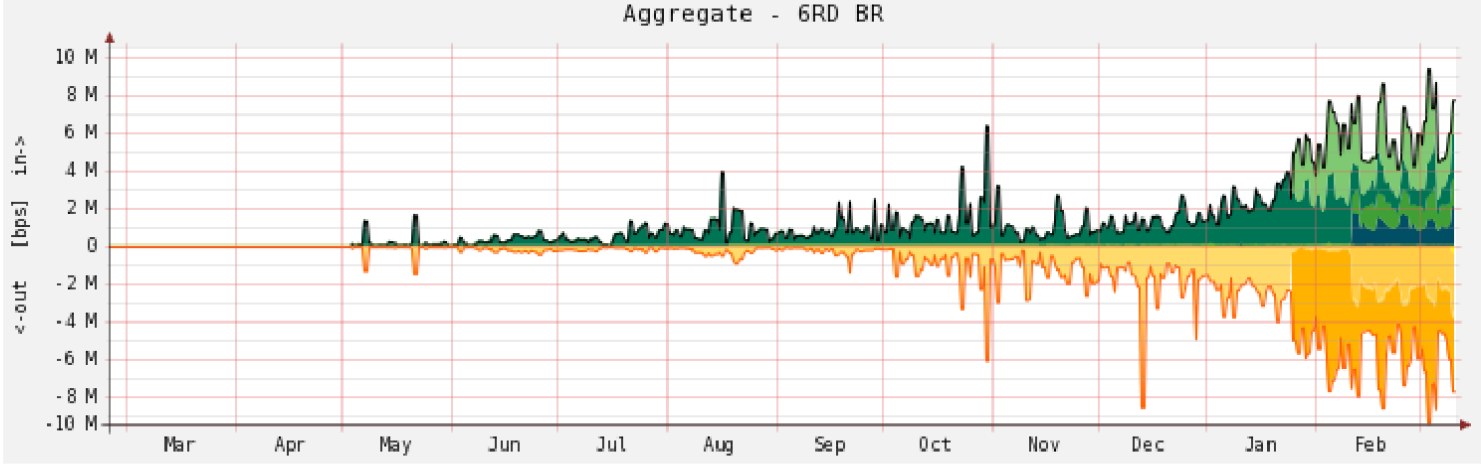
- IPv6 firmware is rolled out to all „centro“ routers
- Current firmware contains no firewall yet
- Customers must activate IPv6 themselves on the customer portal web page. 794 today.



swisscom

Traffic



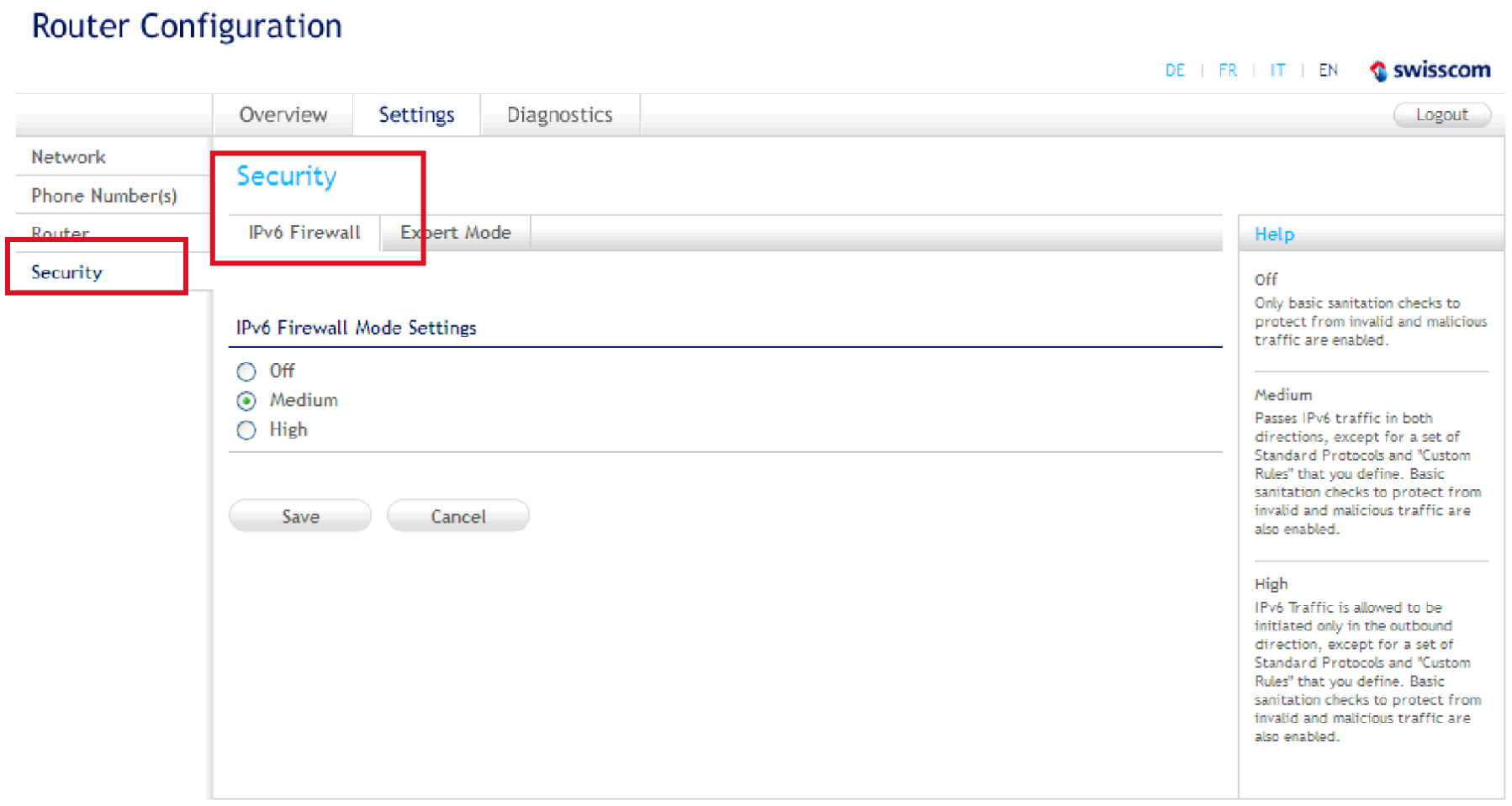


swisscom

Rollout plans for 2012

- 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.

IPv6 Firewall with three levels



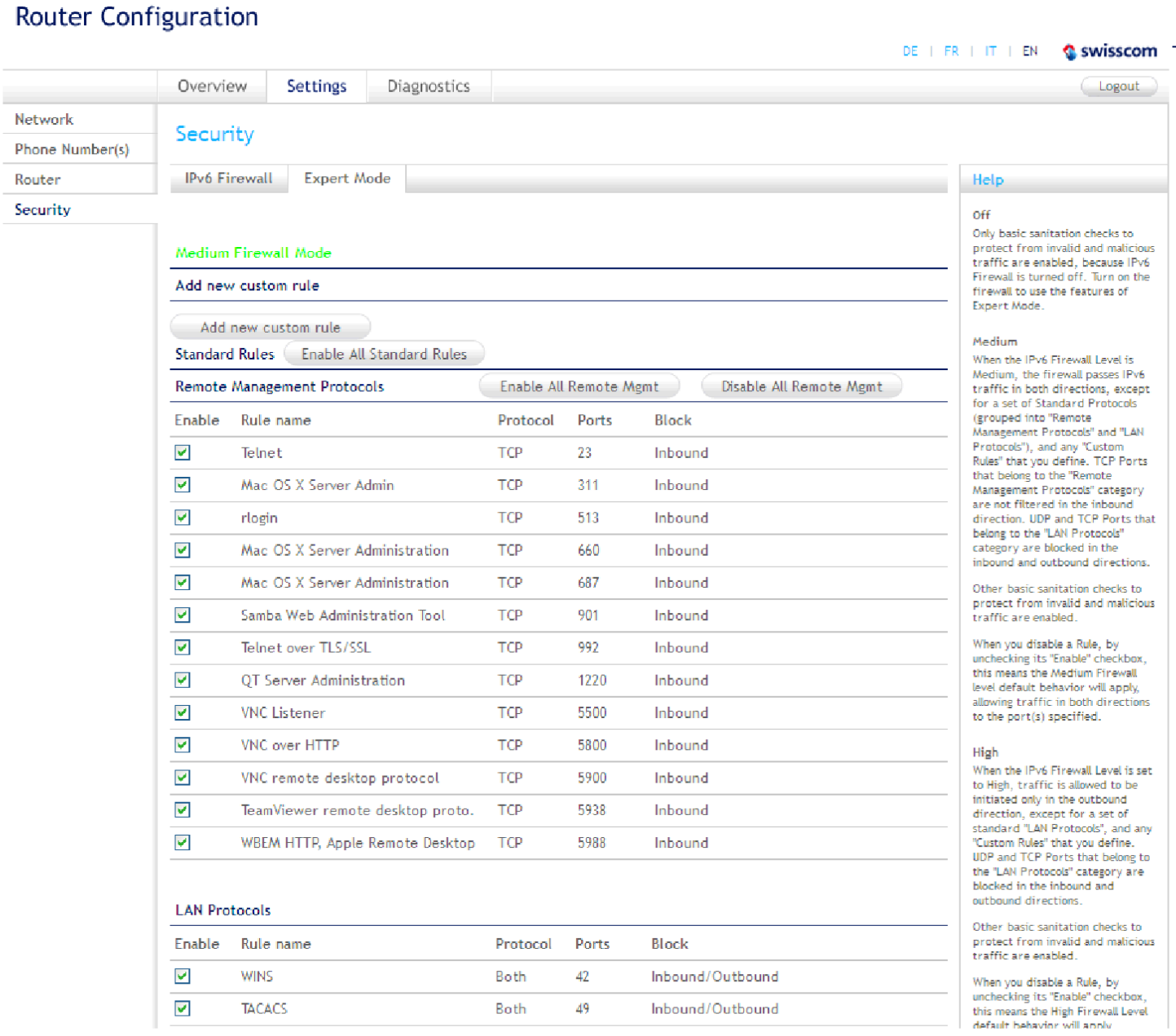
Firewall level „medium“: Default behaviour is „permit“

- 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

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

- 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.

Medium firewall, expert mode



swisscom

Defining a custom rule

- Choose port range or single port
- Then hit save