Residential Access @Init7

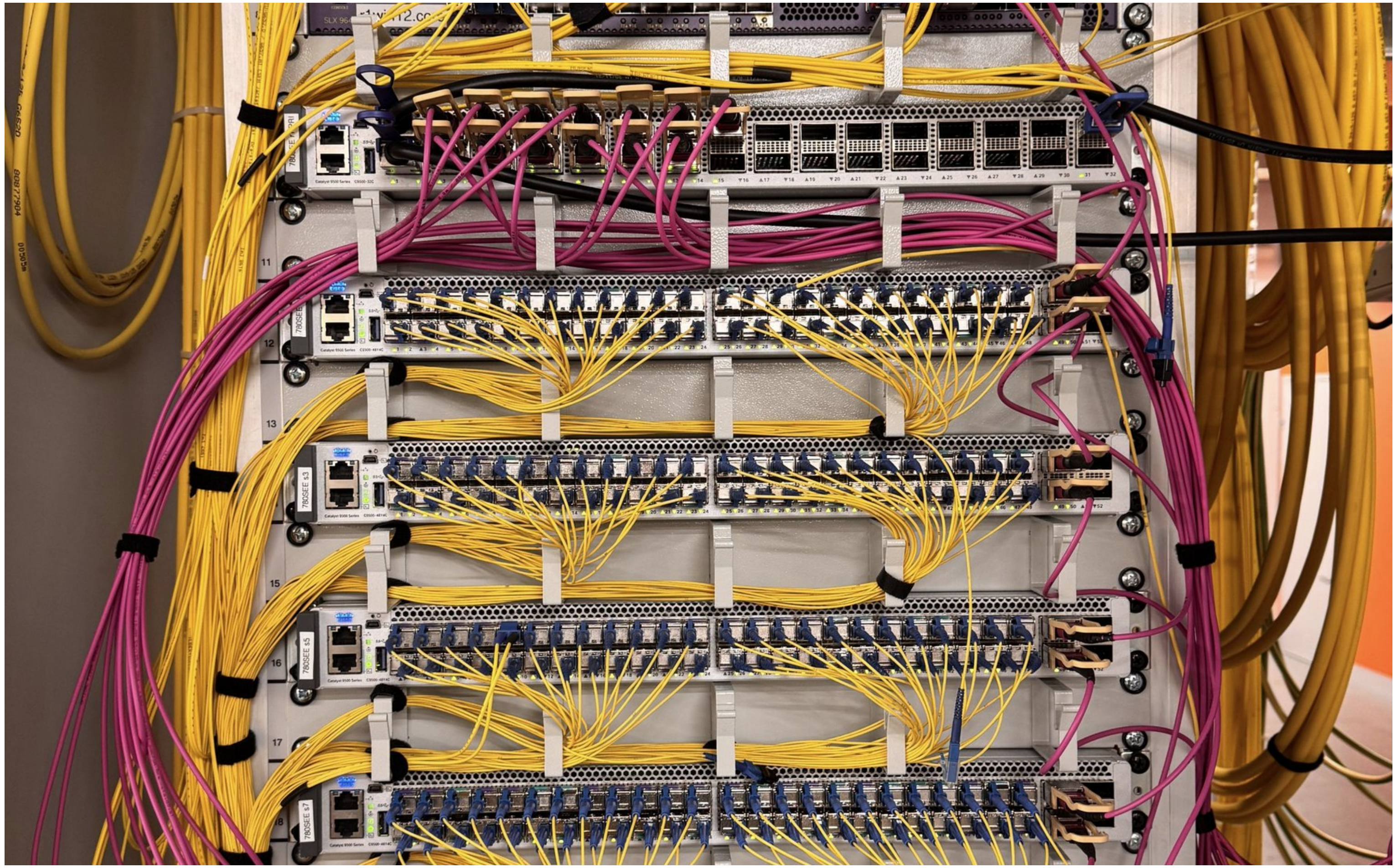
First Hop Security at the customer network edge

Init7

Residential Access @Init7

- Dark fiber last mile is provided by our infrastructure partners
- Our access switches are Cisco Catalyst C9500-48Y4C
- That box has 48x SFP28 slots and 4x QSFP28 slots
- 1G, 10G and 25G BiDi LR transceivers to connect customers
- 2x 100G used for the backhaul
- A pair of Cisco Catalyst C9500-32C collect the backhauls in PoPs with more than 2 access switches

Residential Access @Init7



Residential Access @Init7

- The PoPs are typically backhauled in chains to 2 core routers
- Layer3 termination is already in the PoP
- Addresses delivered by DHCPv4/v6 to customers
- No Broadband Network Gateway (BNG) involved
- Optimal routing and no added delay
- But: All customers at a PoP are in the same Layer2 domain
- First Hop Security necessary!

First Hop Security: Client Isolation

- Do not permit Ethernet frames from customer to customer directly
  - **Private VLAN** with an **Isolated Secondary VLAN**
  - **Promiscuous Port** of that Private VLAN is the Layer3 Interface
- Same IPv4 subnet customer to customer traffic possible due to **Local Proxy ARP** and is Layer3 switched
- IPv6 is different in that respect:
  - DHCPv6 assignes a /128 netmask to the customers CPE WAN interface
  - Default Gateway (`FE80::FF:FE00:F7`) is sent out by local IPv6 Router Advertisment (RA)
  - The customer CPE thinks, it is just him and the router in that LAN segment
  - Again, data to other local customers is Layer3 switched

First Hop Security: Spoofing mitigation

- Ciscos "**Switch Integrated Security Feature (SISF)**"
- "**Gleans**" the DHCPv4/v6 packets
- Creates switch port <—> Address binding

```
    Network Layer Address   Link Layer Address   Interface  vlan  prlvl  age    state      Time left
DH4 192.0.2.77              abcd.dead.beef       Twe1/0/48  100   0024   19mn   REACHABLE  661 s
DH6 2001:db8:777::57        abcd.dead.beef       Twe1/0/48  100   0024   3mn    REACHABLE  1601 s
DH6 2001:db8:777:42::/48    abcd.dead.beef       Twe1/0/48  100   0024   3mn    REACHABLE  (2590000 s)
```

- Source for the spoofing mitigation features
- IPv4/v6 source guard: packets from spoofed addresses get dropped
- Limit the number of addresses a customer can use
- All rogue packets just hit the Layer3 interface

First Hop Security: Protecting the switch

- Rate limiting of ARP, Neighbor Discovery, DHCPv4/v6
- Storm control shuts down the interface for 120 seconds
- More than 100Mbps of incoming Broadcast-, Multicast- or Unknown Unicast (BUM) Frames is considered a Packet Storm by us
- Switch port Access List to filter out unwanted protocols like PIM, OSPF and EIGRP
- IGMP is only allowed from our "own" mulitcast range 233.50.230.0/24

Questions?

Init7