IPv6 Client Networks

Benedikt Stockebrand
Wilhelm Boeddinghaus

RIPE75, Dubai

IPv6 Working Group

Why Client Networks?

- We have talked about
  - ISP Networks -> Design is done
  - Datacenter -> Design is done
  - WAN -> Design is done

Why Client Networks?

- We have talked about
  - Datacenter -> Design is done
  - WAN -> Design is done

- We have talked about
  - Applications (in the datacenter)

- Clients run the other side of the Application
  - Is that easier than in the Datacenter?

What have we today?

- IPv4 only
- Large Networks
  - 256 IPv4 Adresses
  - 512 IPv4 Adresses
  - Even larger ☹
- Layer2 Networks are
  - A Trust Domain
  - A Failure Domain

What do we have today?

- Mixed Networks
- Clients (Windows mostly) + Printers
- Clients (on the Desk) + Mobile PC (Laptops from Sales)
  - All Viruses from Hotel, Airport, Starbucks, etc.

Large Client Networks

- What can we do?
- Fix the Design
- Make Networks smaller

Large Client Networks

- What can we do?
- No, we introduce a new Protocol
- Private VLAN to the Rescue
- Add Complexity
  - Makes our jobs safe ☺

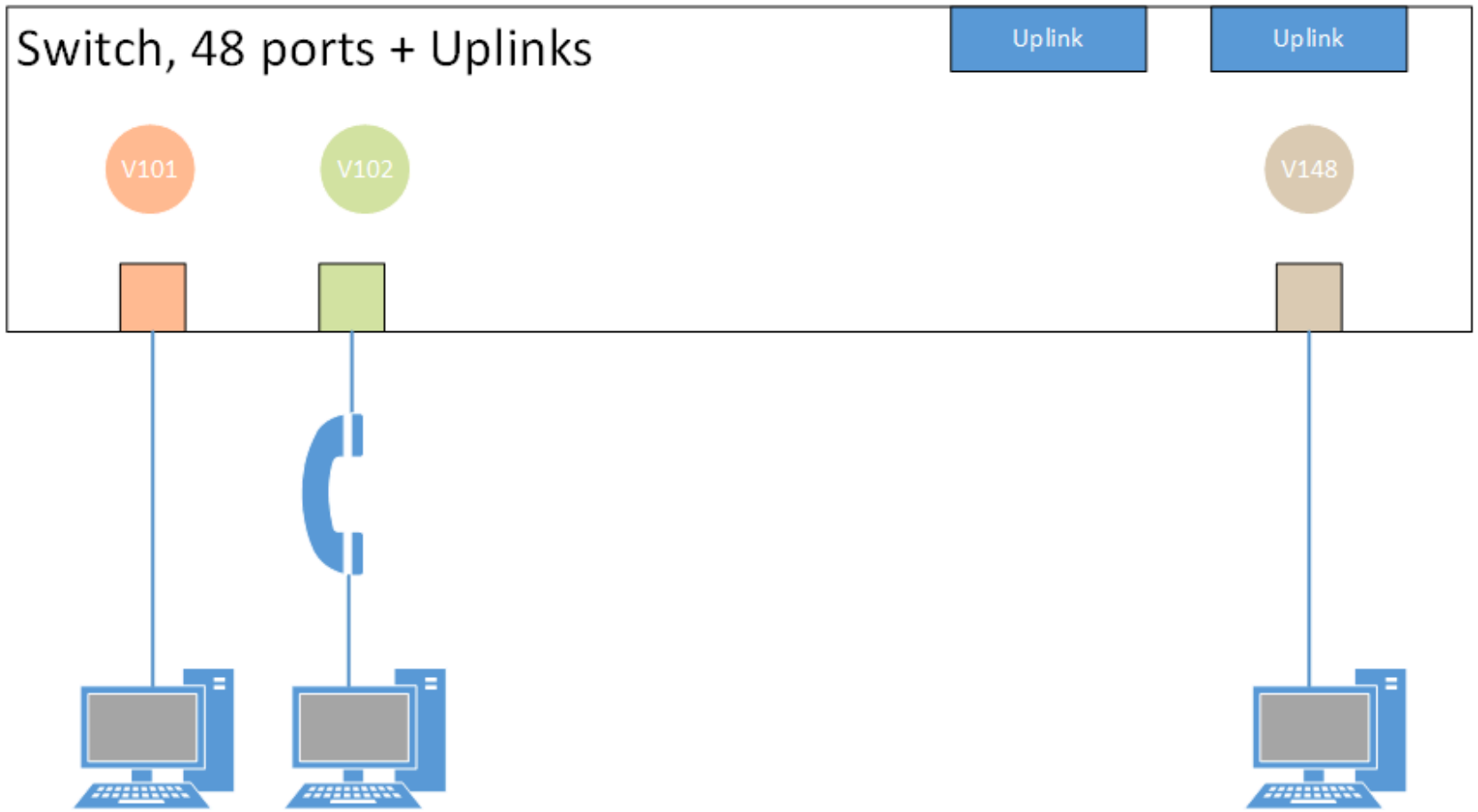
Todays Talk

- We want to discuss a design idea
- We want your input and your knowledge
- Special Thanks for providing us with a Testlab to

IPv6 only Client Networks

- Run IPv6 only on Ethernet
- Fix the large networks design flaw
- Run IPv4 as a Service
- Have a smooth migration

Network Diagram



48 VLANs?

- 48 Trust and Failure Domains
- One /64 network per Port
- Router Advertisement to the Client
  - O – Flag for some extra Infomation
- Aggregate on Uplinks (OSPFv3, IS-IS, BGP)

48 VLANs

- No need for Stateful DHCPv6
- Client registers in Domain and DNS via IPv6

- One /64 per User, we as admins know who uses what network
  - Authorization via IPv6 Address -> IPv6 Network

- Stateless DHCP on
  - small Router
  - Raspberry Pi Class Machine
  - Rackswitch

48 VLANs

- Secure Neighbor Discovery is not used today
  - Microsoft and Apple do not implement it
- No ND Attacks are possible in small networks
  - No 2nd port in VLAN
  - Even a Misconfiguration on a Client does not hurt

48 VLANs

- Use Accesslist on VLAN Interfaces
  - Layer3 Boundaries make Security easier
- No layer2 Attacks possible
  - (Yes, the Voice VLAN)

48 VLANs

- No Spanning Tree
- No VRRP
- No HSRP

- Dynamic Routing from the Rackswitch
  - IPv6 can be aggregated easily

But wait, what about IPv4?

- Use a Tunnel into you datacenter
  - Datacenter runs Dualstack

- MTU is not an issue, it is inhouse

- Microsoft RAS ?
- openVPN ?
- Checkpoint VPN?
- Cisco Anyconnect ?

IPv4 Tunnel

- IPv4 runs as Service on top of IPv6
  - Does anyone remember 6over4?
- Tunnel can be turned off
  - IPv4 Sunset
- Microsoft VPN Clients come with the OS
  - Administrators trust in Microsoft
  - No extra cost for licence
- Microsoft RAS Server is included

IPv4 Tunnel

- Microsoft RAS can be deployed automatically on Client
  - It needs a CA
  - No strong Encryption needed, it runs inhouse
- Opensource (OpenVPN, tinc, Softether, etc.)
  - Extra Software, maybe not allowed
  - Security Policy demands closed source software ☺
- VPN Software may need licence

Migration

- Enable Routing on Rackswitch
- Keep your old Switched VLAN Structure

- Migrate Port by Port to the new Configuration

- If you have Printers or Video Conferencing on same Switch you need your old VLANs anyway

Summary

- Go directly to IPv6 only
- No Dualstack
- IPv4 is a Service

- Open Items:
  - VPN Client?
  - Can VPN Clients register in DNS?

Speakers

- Benedikt Stockebrand
- Stepladder IT Training + Consulting GmbH
- www.stepladder-it.com
- bs@stepladder-it.com

- Wilhelm Boeddinghaus
- iubari GmbH
- IPv6 Training and Consulting
- www.iubari.de
- boeddinghaus@iubari.de
- Linkedin: https://www.linkedin.com/in/boeddinghaus/

Testlab

- www.xantaro.net