

# **21c3 NOC Overview**

## ***Concepts, Implementation and Hardware***

Christian Carstensen, Sebastian Werner & The 21c3 NOC Crew

## ● Overview

- Networking terms
- Recall 20c3 - Situation
- Recall 20c3 - Consequences
- Recall 20c3 - Reasons
- Solution strategy
- Special demands
- Network Services
- BCC Network Layout - Logical
- BCC Network Layout - OSPF
- Hardware
- Implementation
- Internet uplink
- IP Uplink Topology
- IPSEC Realisation
- Using and abusing the network
- Sponsors

## What will we cover:

- Routing Terms explained
- Recall 20c3
- Solving the Problems
- Networking requirements
- BCC Networklayout how it should be
- Networklayout reality

- Overview
- Networking terms
- Recall 20c3 - Situation
- Recall 20c3 - Consequences
- Recall 20c3 - Reasons
- Solution strategy
- Special demands
- Network Services
- BCC Network Layout - Logical
- BCC Network Layout - OSPF
- Hardware
- Implementation
- Internet uplink
- IP Uplink Topology
- IPSEC Realisation
- Using and abusing the network
- Sponsors

- **Layer 2 OSI Data Link Layer.** e.g. Ethernet or 802.11a
- **Switch** Layer 2 based interconnection device between physical networks
- **Layer 3 OSI Network Layer.** e.g. IP or IPX
- **Router** Layer 3 device that connects Layer 2 segments logically
- **Layer 4 OSI Transport Layer.** e.g. UDP or TCP
- **LAN** Provides physical network connectivity.
- **VLAN** Divides a LAN into several logical/virtual LANs using the same physical link.
- **Flow based routing** Routing Switching on Layer 2 after a route lookup using MAC instead of IP

- Overview
- Networking terms
- Recall 20c3 - Situation
- Recall 20c3 - Consequences
- Recall 20c3 - Reasons
- Solution strategy
- Special demands
- Network Services
- BCC Network Layout - Logical
- BCC Network Layout - OSPF
- Hardware
- Implementation
- Internet uplink
- IP Uplink Topology
- IPSEC Realisation
- Using and abusing the network
- Sponsors

- New Building with unknown problems...
- about 20 different rooms with specific access profile
- 4 floors interconnected through floor D
- different network hardware arrived
- lack of facility documentation
- rogue services (dhcp) and hardware (access points!!)

- Overview
- Networking terms
- Recall 20c3 - Situation
- Recall 20c3 - Consequences
- Recall 20c3 - Reasons
- Solution strategy
- Special demands
- Network Services
- BCC Network Layout - Logical
- BCC Network Layout - OSPF
- Hardware
- Implementation
- Internet uplink
- IP Uplink Topology
- IPSEC Realisation
- Using and abusing the network
- Sponsors

- Layer3 networks connected via L2 backbone
- 2 routers did all routing work
- Initial cabling insufficient
- WLAN got flaky
- DHCP became unreliable
- A lot of extra work

- Overview
- Networking terms
- Recall 20c3 - Situation
- Recall 20c3 - Consequences
- Recall 20c3 - Reasons
- Solution strategy
- Special demands
- Network Services
- BCC Network Layout - Logical
- BCC Network Layout - OSPF
- Hardware
- Implementation
- Internet uplink
- IP Uplink Topology
- IPSEC Realisation
- Using and abusing the network
- Sponsors

- Many VLANs that got “trunked“
- Attacks on flow based routing equipment (TCAM full!)
- Hardware (HP, Foundry) got overload
- Patching cables on undocumented panels is hard
- Too many nodes in the WLAN and too powerful transceivers
- Lack of network monitoring
- Lack of user (available) documentation
- Finally: fatigued NOCpeople...

- Overview
- Networking terms
- Recall 20c3 - Situation
- Recall 20c3 - Consequences
- Recall 20c3 - Reasons
- **Solution strategy**
- Special demands
- Network Services
- BCC Network Layout - Logical
- BCC Network Layout - OSPF
- Hardware
- Implementation
- Internet uplink
- IP Uplink Topology
- IPSEC Realisation
- Using and abusing the network
- Sponsors

### Keep it simple!

- Smaller collision domains (Layer2 segments)
- Avoiding tagged (dot1q) / trunked (isl) vlans
- Routing not on L3 switches but on real full-featured routers
- Reduced trust in 802.11b (Do **NOT** expect it to work!)
- Focus on 802.11a
- Explicit effort to ensure documentation
- **NOC Help Desk**

- Overview
- Networking terms
- Recall 20c3 - Situation
- Recall 20c3 - Consequences
- Recall 20c3 - Reasons
- Solution strategy
- Special demands
- Network Services
- BCC Network Layout - Logical
- BCC Network Layout - OSPF
- Hardware
- Implementation
- Internet uplink
- IP Uplink Topology
- IPSEC Realisation
- Using and abusing the network
- Sponsors

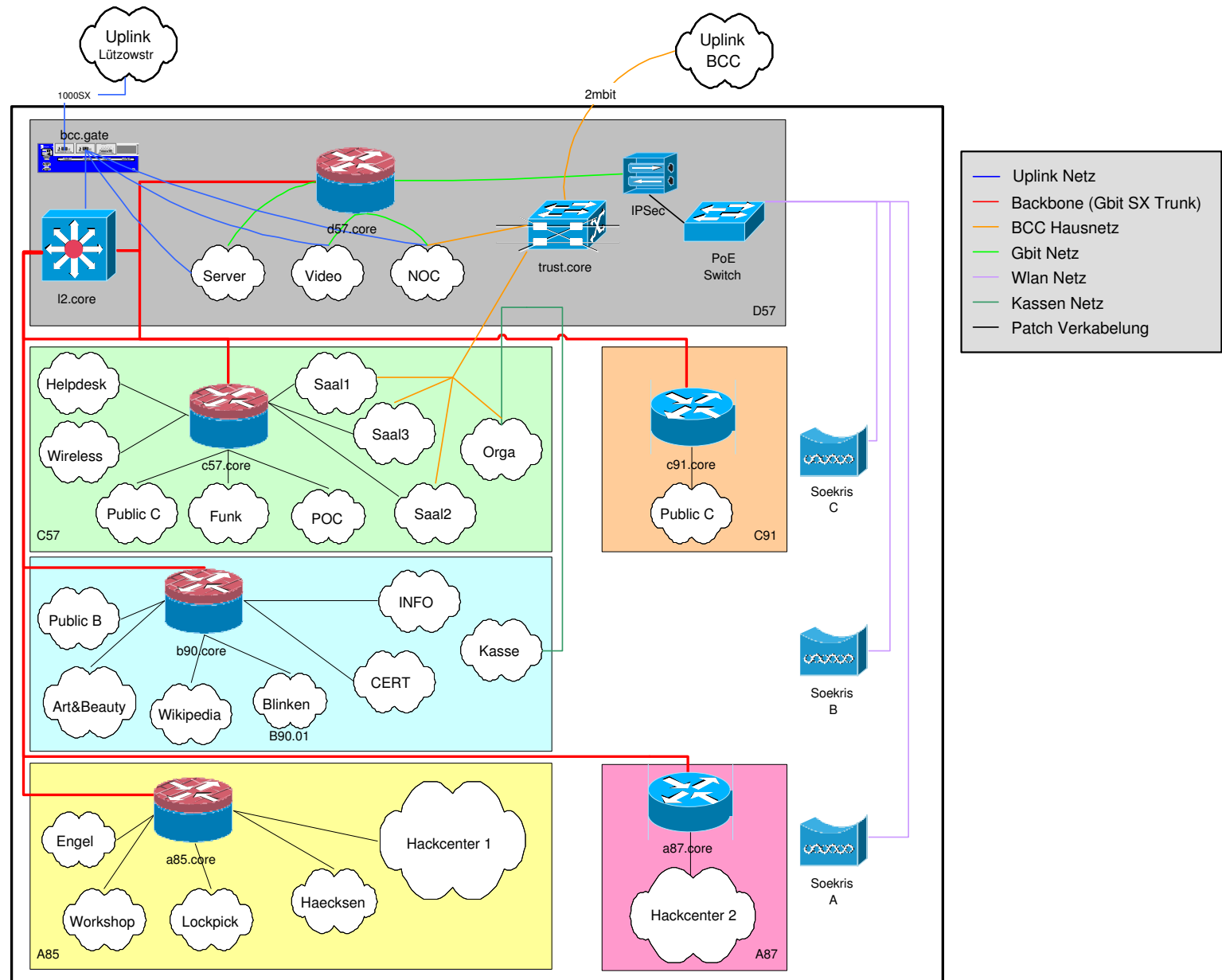
- Entrance needs to be exclusively linked to the Orga Area
- Network-Jacks for speakers need highly-available uplink
- WLAN (Soekris) need dedicated cabling (PoE!)
- Helpdesk and Public Terminals should have high-available uplink
- Video streams should be privileged
- Projects need “dynamic VLANing”
- Wireless Mesh needs WLAN Channel 10 *exclusively*
- Server storage/housing for projects



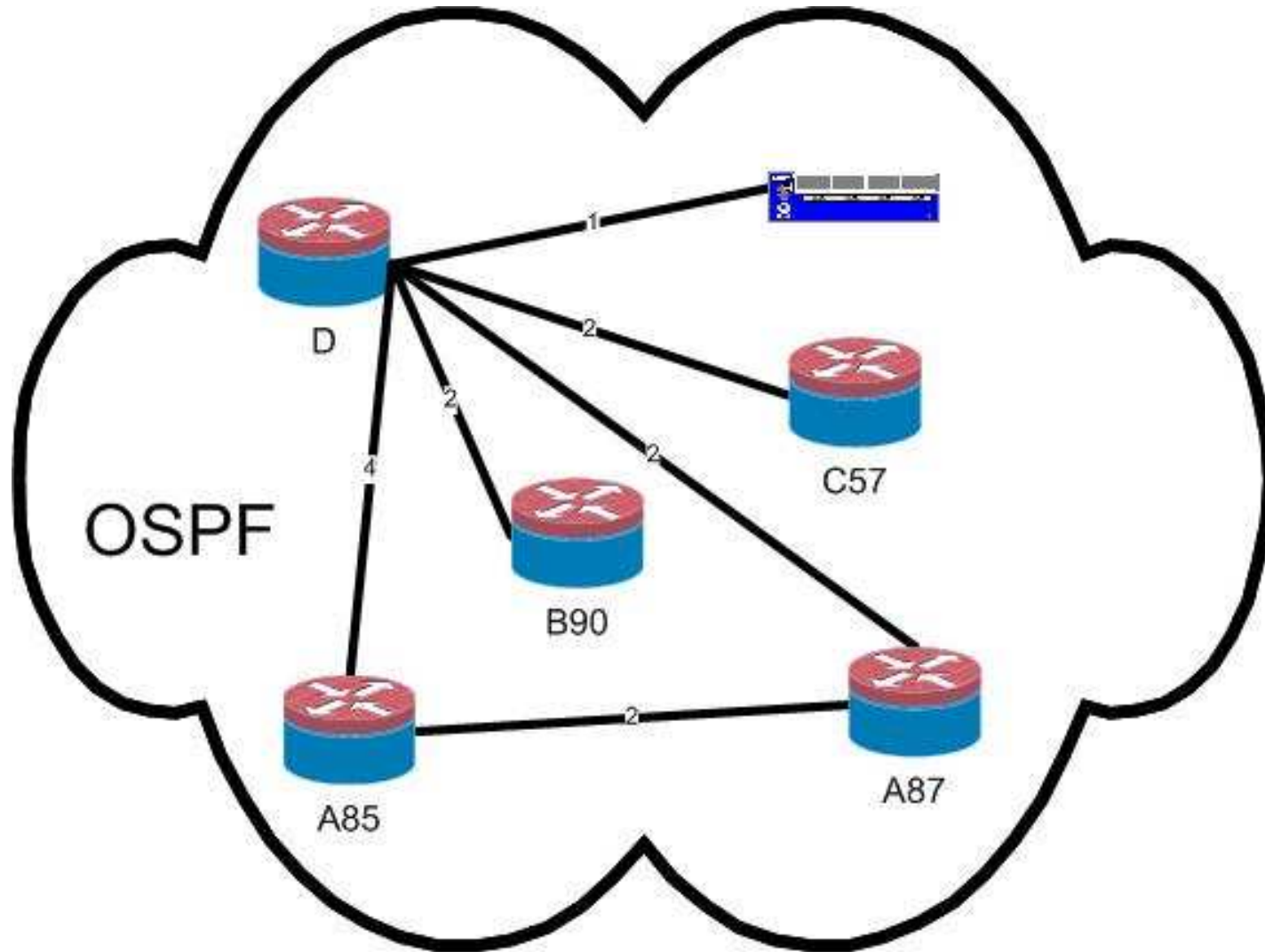
- Overview
- Networking terms
- Recall 20c3 - Situation
- Recall 20c3 - Consequences
- Recall 20c3 - Reasons
- Solution strategy
- Special demands
- Network Services
- BCC Network Layout - Logical
- BCC Network Layout - OSPF
- Hardware
- Implementation
- Internet uplink
- IP Uplink Topology
- IPSEC Realisation
- Using and abusing the network
- Sponsors

- DomainNameService (recursive & authoritative) *82.130.23.35*
- User DNS Registration  
`https://yourname.congress.ccc.de`
- DHCP Service `https://yourname.congress.ccc.de`
- IPSEC Frontend  
`https://illuminatheros.congress.ccc.de`

- Overview
- Networking terms
- Recall 20c3 - Situation
- Recall 20c3 - Consequences
- Recall 20c3 - Reasons
- Solution strategy
- Special demands
- Network Services
- BCC Network Layout - Logical
- BCC Network Layout - OSPF
- Hardware
- Implementation
- Internet uplink
- IP Uplink Topology
- IPSEC Realisation
- Using and abusing the network
- Sponsors



- Overview
- Networking terms
- Recall 20c3 - Situation
- Recall 20c3 - Consequences
- Recall 20c3 - Reasons
- Solution strategy
- Special demands
- Network Services
- BCC Network Layout - Logical
- **BCC Network Layout - OSPF**
- Hardware
- Implementation
- Internet uplink
- IP Uplink Topology
- IPSEC Realisation
- Using and abusing the network
- Sponsors



- Overview
- Networking terms
- Recall 20c3 - Situation
- Recall 20c3 - Consequences
- Recall 20c3 - Reasons
- Solution strategy
- Special demands
- Network Services
- BCC Network Layout - Logical
- BCC Network Layout - OSPF
- **Hardware**
- Implementation
- Internet uplink
- IP Uplink Topology
- IPSEC Realisation
- Using and abusing the network
- Sponsors

- Inhouse Internet Uplink: Juniper M7i
- D57 (Core): Cisco Catalyst 6509
- C57 (Ebene C): Cisco Catalyst 4507
- B90 (Ebene B): Cisco Catalyst 4506
- A85 (HackCenter 1): Cisco Catalyst 6513
- A87 (HackCenter 2): Cisco Catalyst 4006
- Access Layer: HP ProCurve 5308xl, Cisco 3750, Cisco 3550, Cisco 4908

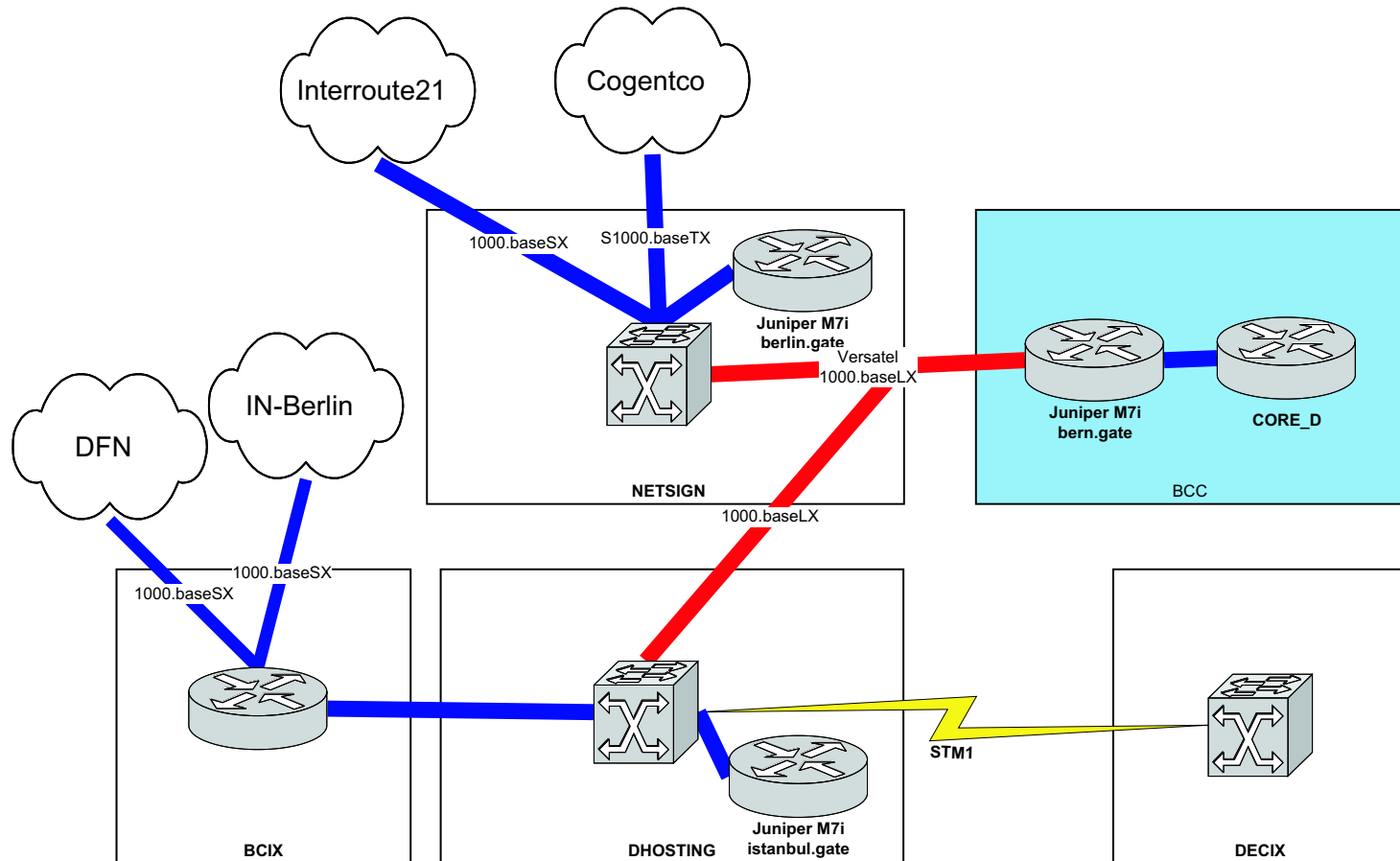
- Overview
- Networking terms
- Recall 20c3 - Situation
- Recall 20c3 - Consequences
- Recall 20c3 - Reasons
- Solution strategy
- Special demands
- Network Services
- BCC Network Layout - Logical
- BCC Network Layout - OSPF
- Hardware
- Implementation
- Internet uplink
- IP Uplink Topology
- IPSEC Realisation
- Using and abusing the network
- Sponsors

- OSPF between core layer devices
- Multiple gigabit (etherchannel) interconnects
- VLAN Trunking for access layer devices
- DHCP forwarding from every VLAN to the DHCP via 'ip-helper'

- Overview
- Networking terms
- Recall 20c3 - Situation
- Recall 20c3 - Consequences
- Recall 20c3 - Reasons
- Solution strategy
- Special demands
- Network Services
- BCC Network Layout - Logical
- BCC Network Layout - OSPF
- Hardware
- Implementation
- Internet uplink
- IP Uplink Topology
- IPSEC Realisation
- Using and abusing the network
- Sponsors

- 1000.baseLX uplink (Thanks to Versatel!)
- Own AutonomousSystemNumber (temp. AS34254)
- Everyone gets a world reachable IP (temp. 82.130.0.0/18)
- 3 Juniper Network M7i routers
- internal BGP between those
- external BGP sessions from 2 routers
- Native peerings with interroute21, Cogentco

- Overview
- Networking terms
- Recall 20c3 - Situation
- Recall 20c3 - Consequences
- Recall 20c3 - Reasons
- Solution strategy
- Special demands
- Network Services
- BCC Network Layout - Logical
- BCC Network Layout - OSPF
- Hardware
- Implementation
- Internet uplink
- IP Uplink Topology
- IPSEC Realisation
- Using and abusing the network
- Sponsors



- Overview
- Networking terms
- Recall 20c3 - Situation
- Recall 20c3 - Consequences
- Recall 20c3 - Reasons
- Solution strategy
- Special demands
- Network Services
- BCC Network Layout - Logical
- BCC Network Layout - OSPF
- Hardware
- Implementation
- Internet uplink
- IP Uplink Topology
- IPSEC Realisation
- Using and abusing the network
- Sponsors

- IPv4 *and* IPv6
- Based on OpenBSD isakmpd
- X.509/ssh cert-/key-based authentication
- Anonymised users
- Non platform specific
- Work in progress



- Overview
- Networking terms
- Recall 20c3 - Situation
- Recall 20c3 - Consequences
- Recall 20c3 - Reasons
- Solution strategy
- Special demands
- Network Services
- BCC Network Layout - Logical
- BCC Network Layout - OSPF
- Hardware
- Implementation
- Internet uplink
- IP Uplink Topology
- IPSEC Realisation
- Using and abusing the network
- Sponsors

- Statically add MAC of *your* gateway
- Have you *ever* thought about ICMP route redirects?
- Contact NOC Helpdesk for network problems: Phone 1234-NONET
- Spanning tree *HAS* a purpose - *YOU* destroy *YOUR* network!

- Overview
- Networking terms
- Recall 20c3 - Situation
- Recall 20c3 - Consequences
- Recall 20c3 - Reasons
- Solution strategy
- Special demands
- Network Services
- BCC Network Layout - Logical
- BCC Network Layout - OSPF
- Hardware
- Implementation
- Internet uplink
- IP Uplink Topology
- IPSEC Realisation
- Using and abusing the network
- Sponsors



Internet routers



Backbone routers



Routing equipment



Switches



Upstream connectivity

■ Interroute21 - Upstream connectivity



Upstream connectivity



Internet uplink