

# 12 Network Troubleshooting

## 12.1 Network Documentation

- Network Topology Diagrams
  - Physical Topology: Device Name, Device location, Interface, ports used, cable type
  - Logical IPv4 Topology: Device id, IP/SM, Interface Id, Routing Protocols, Static routes, L2: VLANs, trunks, Etherchannel)
  - Logical IPv6 Topology: evtl. eigenes Diagramm
- Network Device Documentation
  - Router
  - Switch
  - End-system
- Network Baseline (normal network utilization)
  1. Determine What Types of Data to Collect (z.B. interface utilization, CPU utilization)
  2. Identify Devices and Ports of Interest (uplink-ports, server, key-user)
  3. Determine the Baseline Duration (2 bis 4 Wochen)

## 12.2 Troubleshooting Process

- Seven-Step Troubleshooting Process
  1. Define the Problem
  2. Gather Information
  3. Analyze information
  4. Eliminate Possible Causes
  5. Propose Hypothesis
  6. Test Hypothesis
  7. Solve the problem
- Question End Users
- Gather Information
  - ping, traceroute, telnet, ssh
  - show ip(v6) interface brief
  - show ip(v6) route
  - show protocols
  - debug
- Structured Troubleshooting Methods
  - Bottom-Up: OSI-Layer 1-7
  - Top-Down: OSI-Layer 7-1
  - Divide-and-Conquer: OSI-Layer 3
  - Follow-the-Path: traffic path from source to destination
  - Substitution: swap-the-component
  - Comparison: spot-the-differences (Vergleich mit funktionierenden Geräten, Konfigurationen)
  - Educated Guess: shoot-from-the-hip

## 12.3 Troubleshooting Tools

- Software Troubleshooting Tools: Network Management System Tools, Knowledge Bases, Baselining Tools
- Protocol Analyzers: Wireshark
- Hardware Troubleshooting Tools
  - Digital Multimeters
  - Cable Testers
  - Cable Analyzers (NEXT: near-end crosstalk, RL: return loss)
  - Portable Network Analyzers
  - Cisco Prime Network Analysis Module (NAM)
- Syslog server

## 12.4 Symptoms and Causes of Network Problems

### Physical Layer Troubleshooting

- Symptoms
  - Performance lower than baseline
  - Loss of connectivity
  - Network bottlenecks or congestion
  - High CPU utilization rates
  - Console error messages
- Problem Cause
  - Power-related
  - Hardware faults
  - Cabling faults
  - Attenuation (Dämpfung)
  - Noise (EMI: electromagnetic interference)
  - Interface configuration errors
  - Exceeding design limits
  - CPU overload

### Data Link Layer Troubleshooting

- Symptoms
  - No functionality or connectivity at the network layer or above
  - Network is operating below baseline performance levels
  - Excessive broadcasts
  - Console messages
- Problem Cause
  - Encapsulation errors
  - Address mapping errors
  - Framing errors
  - STP failures or loops

## Network Layer Troubleshooting

- Symptoms
  - Network failure
  - Suboptimal performance
- Problem Cause
  - General network issues
  - Connectivity issues
  - Routing table
  - Neighbor issues
  - Topology database

## Transport Layer Troubleshooting - ACLs

- Symptoms
  - Connectivity issues
  - Access Issues
- Problem Cause
  - ACL configurations
  - NAT configurations
- Common ACL Misconfigurations
  - Selection of traffic flow
  - Order of access control entries
  - Implicit deny any
  - Addresses and IPv4 wildcard masks
  - Selection of transport layer protocol
  - Source and destination ports
  - Use of the established keyword
  - Uncommon protocols
  - Hilfreich: log keyword

## Transport Layer Troubleshooting - NAT for IPv4

- Common interoperability areas
  - BOOTP and DHCP
  - DNS and WINS
  - SNMP
  - tunneling and encryption protocols

## Application Layer Troubleshooting

- SSH/Telnet, HTTP, FTP, TFTP, SMTP, POP
- SNMP
- DNS
- Network File System (NFS)

## 12.5 Troubleshooting IP Connectivity

- ping, traceroute (für ipv4, ipv6)
- show interfaces G0/0/0
  - input/output queue drops / errors
  - Full-duplex/Half-duplex
- MAC-Adressen, VLANs
  - Windows: arp -a, netsh interface ipv6 show neighbor
  - show ipv6 neighbors, show mac address-table
- Default Gateway, Routing
  - show ip route, show ipv6 route
  - show ipv6 interface GigabitEthernet 0/0/0
  - Windows: ipconfig, route print
- Transport-Layer: telnet mit anderen Ports
- ACLs: show ip access-lists, show ip interface

**PT 12.5.13** Troubleshoot Enterprise Networks

**PT 12.6.1** Troubleshooting Challenge - Document the Network

**PT 12.6.2** Troubleshooting Challenge - Use Documentation to Solve Issues