LF3

Network infrastructure of

GEEK-Fitness GmbH

Written by

Max Heilmann (IT4L), Ben Wambold (IT4L), Muhammed-Ali Dogan (IT4L)

Documentation for

System-Administrators & Co-Workers

Hamburg, 16.04.2025

Table of Contents

Introduction

Target Audience and Perspective

This documentation is prepared by GeekedOut GmbH for the management and relevant IT personnel at GEEK-Fitness GmbH. It provides an analysis of the current network infrastructure based on the provided Cisco Packet Tracer simulation and outlines planned modifications and evaluations as requested.

Project Scope and Objectives

The primary scope of this project is to:

1. Analyze and thoroughly document the existing network infrastructure simulated in Packet Tracer.
2. Plan and document the integration of a new PC workstation and a wireless tablet into the Purchasing department (Einkauf).
3. Plan and document the creation of a new, segregated subnet/VLAN for the Controlling department.
4. Provide clear, actionable documentation for the client.

Client Information

The client for this project is GEEK-Fitness GmbH. A fitness center.

1. Network plan

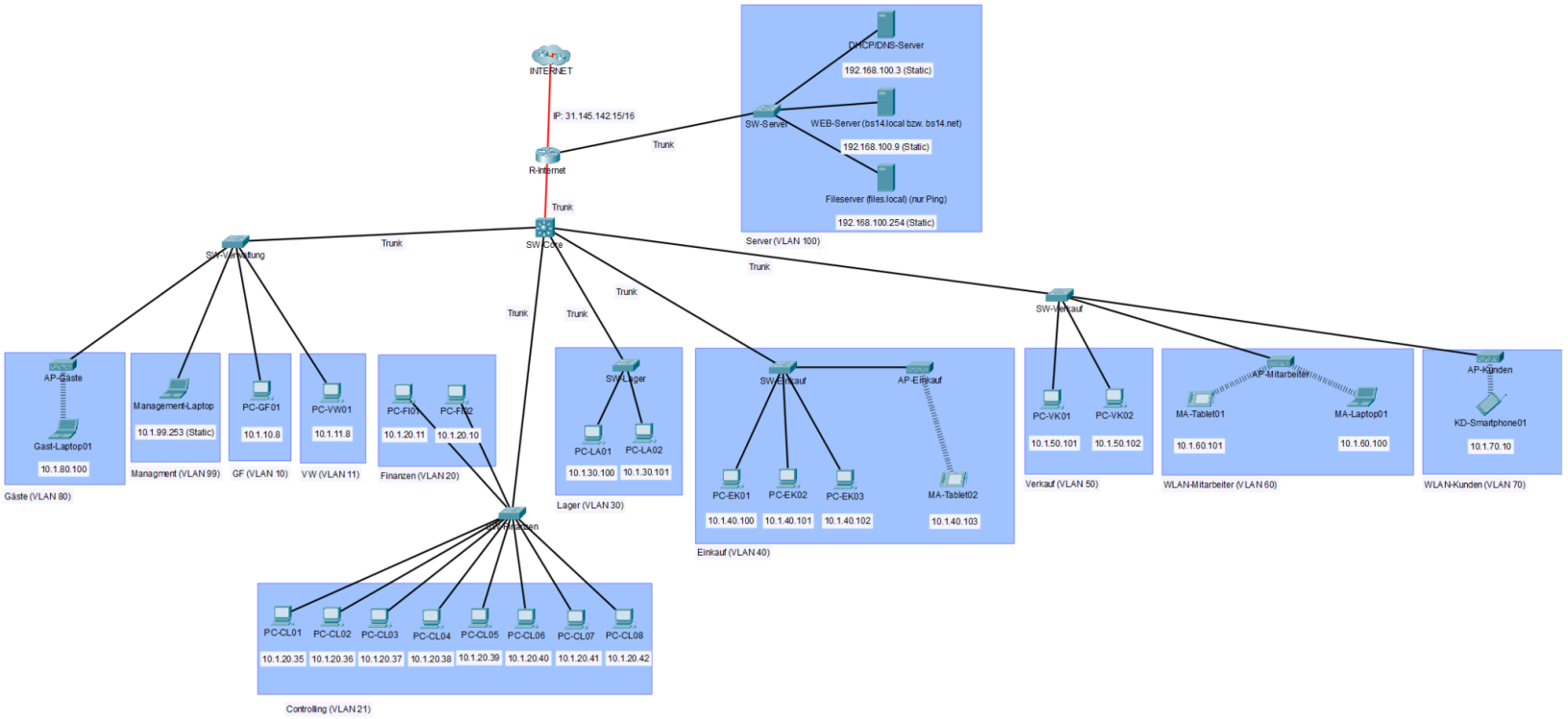

Figure 1: *GEEK-Fitness GmbH Network Topology (Packet Tracer Simulation)*

Legend:

- Trunk: Trunk port
- SW-*: Network Switch
- R-Internet: Router
- AP-*: Wi-Fi Access Point
- Server-*: Computers Running Server Software

Brief Explanation

The diagram shows the central R-Internet router, connecting the internal network segments (via SW-Core and SW-Server) to the INTERNET. SW-Core acts as the backbone, linking the departmental access switches (SW-Verwaltung, SW-Finanzen, etc.). Each access switch connects respective end devices (PCs) and potentially Access Points. The server farm connects directly to SW-Server, which links to R-Internet. Wireless devices connect via the appropriate APs. We decided to leave out port numbers as they can already be found in the port assignment table and would only clutter the network topology plan and therefore bring no real benefit.

2. IPv4 Addressing Scheme (IPAM)

The network utilizes private IPv4 addressing, primarily in the 10.x.x.x range, segmented by VLANs. The server network uses the 192.168.100.0/24 range. Addressing is managed centrally via DHCP for most client devices, with static IPs assigned to servers and network infrastructure management interfaces. A new VLAN and address space is expected to be created by us for the new “Controlling” division.

VLAN	Name	Network	Subnet Mask	Usable Host Range (DHCP)	Gateway	Purpose
10	Geschäftsführung	10.1.10.0/28	255.255.255.240	10.1.10.2 to 10.1.10.14	10.1.10.1	Management /Executive
11	Verwaltung	10.1.11.0/28	255.255.255.240	10.1.11.2 to 10.1.11.14	10.1.11.1	Company Admin
20	Finanzen	10.1.20.0/27	255.255.255.224	10.1.20.2 to 10.1.20.30	10.1.20.1	Finance
21	Controlling	10.1.20.32/28	255.255.255.240	10.1.20.34 to 10.1.20.42	10.1.20.33	Controlling
30	Lager	10.1.30.0/24	255.255.255.0	10.1.30.2 to 10.1.30.254	10.1.30.1	Warehouse/ Logistics
40	Einkauf	10.1.40.0/24	255.255.255.0	10.1.40.2 to 10.1.40.254	10.1.40.1	Purchasing
50	Verkauf	10.1.50.0/24	255.255.255.0	10.1.50.2 to 10.1.50.254	10.1.50.1	Sales
60	WLAN-MA	10.1.60.0/24	255.255.255.0	10.1.60.2 to 10.1.60.254	10.1.60.1	Employee Wi-Fi
70	WLAN-KD	10.1.60.0/24	255.255.255.0	10.1.70.2 to 10.1.71.254	10.1.70.1	Customer Wi-Fi
80	WLAN-GA	10.1.70.0/23	255.255.254.0	10.1.80.2 to 10.1.80.254	10.1.80.1	Guest Wi-Fi
99	Managment	10.1.99.192/26	255.255.255.192	*- No DHCP -*	10.1.99.254	Network Device Management
100	Server	192.168.100.0/24	255.255.255.0	192.168.100.1 to 192.168.100.253	192.168.100.254	Servers

*Fields marked in **green** are to be newly added.*

3. Port Assignment Tables

The following tables detail the significant port configurations for each access switch based on the simulation file. Unused ports are generally configured in VLAN 1 (default) and are administratively shut down for security. Trunk ports carry tagged traffic for multiple VLANs, while access ports carry untagged traffic for a single assigned VLAN.

*Changes are marked in **green**.*

SW-Verwaltung

Port	Status	Mode	Assigned VLAN(s)	Connected Device
Fa0/1	Up	Access	10	PC-GF01
Fa0/2 - Fa0/10	Down	Access	1	-
Fa0/11	Up	Access	11	PC-VW01
Fa0/12 - Fa0/19	Down	Access	1	-
Fa0/20	Up	Access	80	AP-Gäste
Fa0/21 - Fa0/23	Down	Access	1	-
Fa0/24	Up	Access	99	-
Gi0/1	Up	Trunk	10, 11, 80, 99	SW-Core
Gi0/2	Up	Access	99	Management-Laptop

SW-Lager

Port	Status	Mode	Assigned VLAN(s)	Connected Device
Fa0/1	Up	Access	30	PC-LA01
Fa0/2	Up	Access	30	PC-LA02
Fa0/3 - Fa0/23	Down	Access	1	-
Fa0/24	Up	Access	99	-
Gi0/1	Up	Trunk	30, 99	SW-Core
Gi0/2	Down	Access	1	-

SW-Finanzen

Port	Status	Mode	Assigned VLAN(s)	Connected Device
Fa0/1	Up	Access	20	PC-FI01
Fa0/2	Up	Access	20	PC-FI02
Fa0/3 - Fa0/16	Down	Access	1	-
Fa0/17	Up	Access	21	PC-CL01
Fa0/18	Up	Access	21	PC-CL02
Fa0/19	Up	Access	21	PC-CL03
Fa0/20	Up	Access	21	PC-CL04
Fa0/21	Up	Access	21	PC-CL05
Fa0/22	Up	Access	21	PC-CL06
Fa0/23	Up	Access	21	PC-CL07
Fa0/24	Up	Access	21	PC-CL08
Gi0/1	Up	Trunk	20, 99	SW-Core
Gi0/2	Down	Access	1	-

SW-Einkauf

Port	Status	Mode	Assigned VLAN(s)	Connected Device
Fa0/1	Up	Access	40	PC-EK01
Fa0/2	Up	Access	40	PC-EK02
Fa0/3	Up	Access	40	PC-EK03
Fa0/4	Up	Access	40	AP-Einkauf
Fa0/5 - Fa0/23	Down	Access	1	-
Fa0/24	Up	Access	99	-
Gi0/1	Up	Trunk	40, 99	SW-Core
Gi0/2	Down	Access	1	-

SW-Verkauf

Port	Status	Mode	Assigned VLAN(s)	Connected Device
Fa0/1	Up	Access	50	PC-VK01
Fa0/2	Up	Access	50	PC-VK02
Fa0/3 - Fa0/19	Down	Access	1	-
Fa0/20	Up	Access	60	AP-Mitarbeiter
Fa0/21	Up	Access	70	AP-Kunden
Fa0/22 - Fa0/23	Down	Access	1	-
Fa0/24	Up	Access	99	-
Gi0/1	Up	Trunk	50, 60, 70, 99	SW-Core
Gi0/2	Down	Access	1	-

SW-Server

Port	Status	Mode	Assigned VLAN(s)	Connected Device
Fa0/1	Up	Access	100	DHCP/DNS-Server
Fa0/2	Up	Access	100	WEB-Server
Fa0/3	Up	Access	100	Fileserver
Fa0/4 - Fa0/23	Down	Access	1	-
Fa0/24	Up	Access	99	-
Gi0/1	Up	Trunk	1, 99, 100	R-Internet
Gi0/2	Up	Access	1	-

SW-Core

Port	Status	Mode	Assigned VLAN(s)	Connected Device
Gi1/0/1	Up	Trunk	10-11, 20, 30, 40, 50, 60, 70, 80, 99	SW-Verwaltung
Gi1/0/2	Up	Trunk	10-11, 20**, 21**, 30, 40, 50, 60, 70, 80, 99	SW-Finanzen
Gi1/0/3	Up	Trunk	10-11, 20, 30, 40, 50, 60, 70, 80, 99	SW-Lager
Gi1/0/4	Up	Trunk	10-11, 20, 30, 40, 50, 60, 70, 80, 99	SW-Einkauf
Gi1/0/5	Up	Trunk	10-11, 20, 30, 40, 50, 60, 70, 80, 99	SW-Verkauf
Gi1/0/6 - Gi1/0/24	Down	Access	1	-
Gi1/1/1	Up	Trunk	10-11, 20**, 21**, 30, 40, 50, 60, 70, 80, 99-100	R-Internet
Gi1/1/2 - Gi1/1/4	Down	Access	1	-
Vlan99 (SVI)	Up	-	99 (Management Interface)	IP: 10.1.99.100/24

4. Testing the Network

To verify network functionality after analysis and implementation:

- **Intra-VLAN Connectivity:** Ping between PC-EK01 to PC-EK02.
  Expected Result: Success.
- **Inter-VLAN Connectivity:** Ping from PC-GF01 in VLAN 10 to PC-VK01 in VLAN 50
  Expected Result: Success.
- **DNS Resolution:** From PC-LA01, use nslookup bs14.local.
  Expected Result: Correct IP addresses returned.
- **Internet Connectivity:** Ping 8.8.8.8 from PC-EK01.
  Expected Result: Success.
- **DHCP:** Verify PC-EK03 gets a correct IP address in the 10.1.40.x range.
- **Controlling Subnet Verification:** Verify PC-CL01 gets an IP in the 10.1.20.32/28 range.
- **Controlling Intra-VLAN:** Ping between PC-CL01 and PC-CL02.
  Expected Result: Success.
- **Controlling Inter-VLAN:** Ping from PC-CL01 to PC-LA01.
  Expected Result: Failure (due to ACL).
- **Controlling Inter-VLAN:** Ping from PC-VW01 to PC-CL03.
  Expected Result: Failure (due to ACL).
- **Customer WLAN DHCP:** Verify DHCP assigns an IP in the 10.1.70.0/23 range to KD-Smartphone01.
- **Customer WLAN Restrictions:** Attempt to ping internal file server.
  Expected Result: Failure (due to ACL).
- **Customer WLAN Restrictions:** Attempt DNS lookup (nslookup testnet.lo).
  Expected Result: Success (DNS allowed by ACL).

Summary

The existing network infrastructure of GEEK-Fitness GmbH is well-segmented using VLANs, providing a good foundation. Key services like DHCP and DNS are centralized. The analysis identified specific configurations for switches, the router, and wireless access points. VLANs with untrusted devices are isolated from other networks in order to restrict access to critical business infrastructure.

The documentation outlines clear steps for integrating the new PC and tablet for the Purchasing department and for creating a new, isolated subnet for the Controlling department, including necessary IP addressing, VLAN creation, router ACLs, and switch port configurations