

Vorhandene Infrastruktur des Netzwerkes

Ist-Stand LAN

Verkabelungsstrukturen:

- Glasfaser- Backbones zwischen den Liegenschaften bzw. innerhalb der einzelnen Liegenschaften zwischen den Gebäuden

liegenschaftsübergreifend: → LWL-Singlemodestrecken 9/125 µm, abgelegt auf E2000-APC-Kupplung

innerhalb einer Liegenschaft: → LWL-Strecken 9/125 µm abgelegt auf E2000-APC-Kupplung
→ zum Teil auch noch LWL-Multimode 50/125 µm abgelegt auf ST-Kupplung)

- Glasfaserstrecken im Sekundärbereich (von den Gebäudeeintrittspunkten zu den Etagenverteilern)
(LWL-Strecken 9/125 µm (abgelegt auf E2000-APC bzw. SC-Kupplung) sowie 50/125 µm (abgelegt auf SC- bzw. ST-Kupplung))
- Die Anbindung der Arbeitsplätze (Tertiärbereich) auf einer Etage ist mindestens als Kat-5 (in der Regel Kat-5+, Kat-6 oder besser) Verkabelung ausgeführt (Bestand). Die Neuverkabelungen erfolgen nach Kat. 7 mit PIMF- Kabeln (paarweise geschirmte Kabel). Angestrebt wird eine strukturierte Verkabelung, d.h. ein gemeinsames Netz für TK und Daten, die erforderlichen Anschlüsse werden im Datenschränk gepatcht. Datenverkabelung in Kupfer nach Kat.6 oder besser.
- Die für den Betrieb des flächendeckenden WLAN-Netzes (primär am Standort „Zentralklinikum“) wurden die entsprechenden Verkabelungsstrukturen auf Basis einer VoIP-ready-WLAN-Ausleuchtung (Frequenzband: 2,4 GHz; 802.11 b/g; VoIP-tauglich) innerhalb der Neubau- bzw. Sanierungsmaßnahmen realisiert. (Auslass für WLAN-AP's / Kupfer nach Kat.5+ oder besser / POE nach IEEE 802.3at zum Teil auch noch IEEE 802.3af)

Erstellt:	Machacek, Roger - 15.03.2022	15.03.2022	ID: 34392
Inhaltlich geprüft:	Schulz, Uwe - 13.05.2022	13.05.2022	Revision: 002/05.2022
Formal geprüft:	Ruback, Alexander - 16.05.2022	16.05.2022	Wiedervorlage: 23.05.2026
Freigegeben:	Weitemeyer, Christian - 16.05.2022	16.05.2022	Seite 1 von 6

L2/L3-Struktur des LAN:

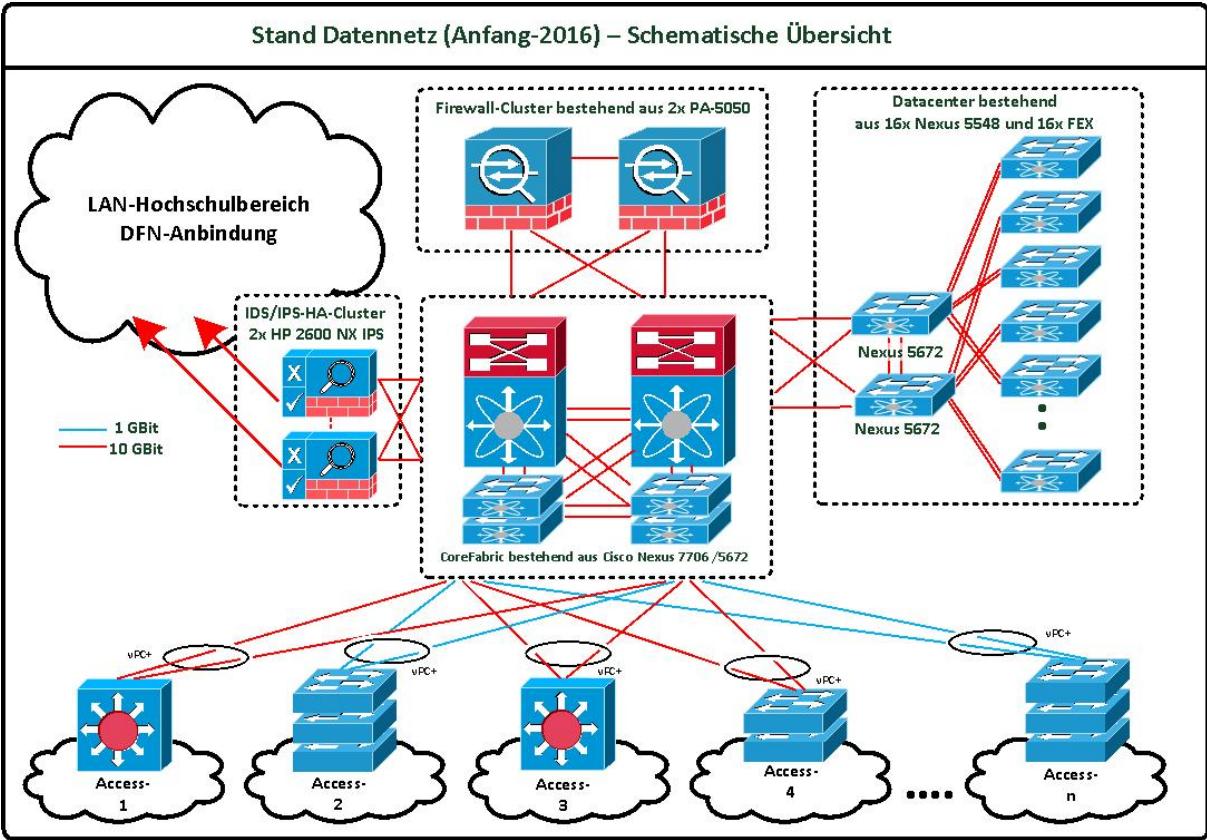


Abbildung-1: Schematischer Aufbau des Netzwerkes

• Im Backbone-Bereich

→ 10Gigabit- bzw. Gigabit- Ethernet mit folgenden Charakteristika:

- Basis-Design: Meshed HA-Design (Spine/Leaf-Architektur) auf Basis Cisco Fabric-Path im Core und Distribution Bereich (2x Nexus 7706 / 10x Nexus 5672, full-redundant, full-ISSU-fähig); Anbindung der Access-Bereiche auf Basis Cisco VPC+ (LACP-Based über Nexus 5672)
- eingesetzte Komponenten: 2x Cisco Nexus 7706
- VLANs: VLANs nach IEEE 802.1q
- L2-Redundanz: Cisco Fabric-Path / VPC+
- L3-Redundanz: auf Basis Cisco HSRP
- Quality of Service: QOS-Tagging nach IEEE 802.1p / TOS und DiffServ
- Device Discovery Protocol: CDP bzw. LLDP nach IEEE-802.1ab
- Netzwerkmanagement: SNMPv2/v3 / RMON / sshv2

Erstellt:	Machacek, Roger - 15.03.2022	15.03.2022	ID: 34392
Inhaltlich geprüft:	Schulz, Uwe - 13.05.2022	13.05.2022	Revision: 002/05.2022
Formal geprüft:	Ruback, Alexander - 16.05.2022	16.05.2022	Wiedervorlage: 23.05.2026
Freigegeben:	Weitemeyer, Christian - 16.05.2022	16.05.2022	Seite 2 von 6

- Stromversorgung Redundant (mind 1x USV, 1x SV)

- **Im Distribution-Bereich**

→ Gigabit- Ethernet mit folgenden Charakteristika:

- Basis-Design: Meshed HA- (Spine/Leaf-Architektur) auf Basis Cisco Fabric-Path im Core und Distribution Bereich (2x Nexus 7706 / 10x Nexus 5672, full-redundant, full-ISSU-fähig);
Anbindung der Accessbereiche auf Basis Cisco VPC+ (LACP-Based über Nexus 5672)
- eingesetzten Komponenten: 2x Cisco Nexus 5672
- VLANs: LANs nach IEEE 802.1q incl. GARP VLANs
- L2-Redundanz: Cisco Fabric-Path / VPC+
- Quality of Service: QOS-Tagging nach IEEE 802.1p / TOS und DiffServ
- Trunks: VPC+, LACP, ggf. auch Etherchannel
- Device Discovery Protocol: LLDP nach IEEE-802.1ab
- Netzwerkmanagement: SNMPv2/v3 / sshv2
- Stromversorgung: Redundant (mind 1x USV, 1x SV)

- **Im Tertiärbereich**

→ Fast-Ethernet bzw. Gigabit- Ethernet mit folgenden Charakteristika:

- Basis-Design: Access-Switches in den klinischen Bereichen mit redundanter Stromversorgung, redundanter Anbindung; über VPC+/LACP mit redundantem Management und ISSU-fähig;
Access-Switches in den nichtklinischen Bereichen: redundante Stromversorgung wird angestrebt; redundante Anbindung über LACP/VPC+ wird angestrebt;
- eingesetzten Komponenten: diverse Switches der Cisco Catalyst-Series in den klinischen Bereichen schwerpunktmäßig: Cisco Catalyst 4507 und Cisco Catalyst 3850 Series
- VLANs: VLANs nach IEEE 802.1q für ausgewählte Anschlüsse (z.B. VoIP-Apparate, Server, WLAN-AP's...)
- Quality of Service: QOS-Tagging nach IEEE 802.1p / TOS und DiffServ z.Z. für ausgewählte Endgeräte (z.B. VoIP, ...)

Erstellt:	Machacek, Roger - 15.03.2022	15.03.2022	ID: 34392
Inhaltlich geprüft:	Schulz, Uwe - 13.05.2022	13.05.2022	Revision: 002/05.2022
Formal geprüft:	Ruback, Alexander - 16.05.2022	16.05.2022	Wiedervorlage: 23.05.2026
Freigegeben:	Weitemeyer, Christian - 16.05.2022	16.05.2022	Seite 3 von 6

- Trunks: Trunking nach IEEE 802.3ad ggf. auch Etherchannel für ausgewählte Endgeräte (z.B. Server, Med.Tech....)
- Device Discovery Protocol: LLDP-MED nach IEEE-802.1ab für VoIP-Anschlüsse und WLAN-AP's
- Stromversorgung in den klinischen Bereichen → in der Regel redundant (mind 1x USV, 1x SV)
- Power over Ethernet: USV-gestützte POE-Anschlüsse nach 802.11at (z.T. auch nur 802.11at) für ausgewählte Endgeräte (z.B. VoIP-Apparate und WLAN-AP's)

Hinweis: In den klinischen Bereichen wird im Access-Bereich in der Regel eine der beiden folgenden Standardvarianten eingesetzt:

- a) Cisco Catalyst 4507 (ISSU-fähig) mit redundanten Powersupplies, redundanten Supervisor-Engines; angebunden über 10 GE Ethernet LACP-Trunk (10 GE-LACP-Ports auf beide Supervisor-Engines aufgeteilt)
- b) Cisco Catalyst 3850 Stack (Stack mit jeweils zwei Switches / ISSU-fähig / inkl. Power-Stacking) angebunden über 10 GE Ethernet LACP-Trunk (10 GE-LACP-Ports auf beide Stack-Member aufgeteilt)

Netzwerkprotokolle:

- Im Core- und im Distribution-Bereich wird ausschließlich Cisco-Fabric-Path als Basis eingesetzt (IS-IS basiert). Darauf aufsetzend wurde eine VLAN / VRF-basierte IPv4 Subnetzstruktur aufgesetzt.
- Sämtliche Switches im Access-Bereich werden redundant an die Distribution-Layer auf Basis VPC+ / LACP angebunden (z.Z. noch in Umsetzung)
- zentrale Firewall- bzw. IDS/IPS-Systeme sind direkt über VPC+ / LACP an die Coreswitches angeschlossen
- zentrale Server werden in der Regel redundant über Bladecenter FEX-Extender direkt an die Cisco-Fabric-Path-basierten Core- und Distribution-Layer angeschlossen
- Produktiv wird zurzeit ausschließlich IPv4 unterstützt. Für alle neuen LAN-, WLAN-, bzw. Server-Komponenten wird zwingend IPv6 Unterstützung gefordert.
- Zurzeit gibt es mehrere IPv4, IGMPv2 basierte Multicast-Anwendungen (Ackermann-Patientenruf-System, Dräger-mobiles-Monitoring, voraussichtlich ab Q4/2018 Multicast basiertes IP-TV)
- Als Netzwerkmanagement-Protokoll wird zur Zeit SNMPv2/v3 zzgl. RMON unterstützt. Für alle neuen Komponenten wird neben SNMPv2 auch zwingend eine SNMPv3 Unterstützung gefordert.

Erstellt:	Machacek, Roger - 15.03.2022	15.03.2022	ID: 34392
Inhaltlich geprüft:	Schulz, Uwe - 13.05.2022	13.05.2022	Revision: 002/05.2022
Formal geprüft:	Ruback, Alexander - 16.05.2022	16.05.2022	Wiedervorlage: 23.05.2026
Freigegeben:	Weitemeyer, Christian - 16.05.2022	16.05.2022	Seite 4 von 6

Das Datennetz ist zur besseren Absicherung vor unberechtigtem Zugriff und zum Schutz vor Viren, Trojanern und anderer Malware wie in Abbildung-2 schematisch dargestellt, in mehrere Sicherheitszonen segmentiert.

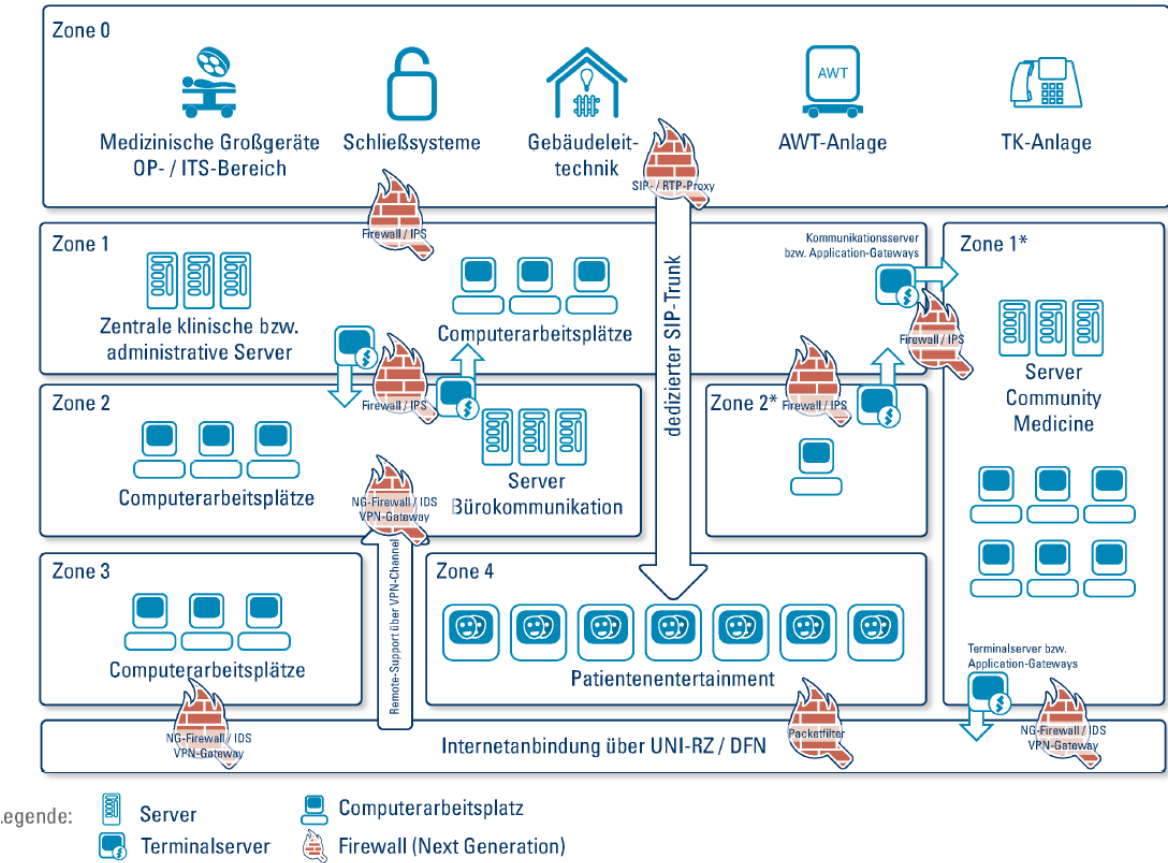


Abbildung 2: Schematischer Aufbau Sicherheitszonen im Datennetz

Durch diese Segmentierung werden die zentrale Bereiche der Patientenversorgung sowie andere technische Anlagen (welche aus Sicht eines 24/7 Routinebetriebes als besonders kritisch einzustufen sind) besonders geschützt. Gleichzeitig wird trotzdem ein Zugriff auf Dienste im Internet sowie die klinischen Daten von jedem Arztarbeitsplatz aus ermöglicht. Dieser ist nur über die zwischen den Zonen 1 und 2 bzw. 1* und 2* etablierten Terminalserver möglich. Die Nutzer einer Zone können über ein sogenanntes Terminalserverfenster auf die Basis-Dienste der jeweils anderen Zone zugreifen. Dateitransfers sind explizit ausgeschlossen!!!

Sämtliche Kernkomponenten dieser mehrstufigen Security-Architektur sind bzw. werden zurzeit redundant ausgelegt.

Die Anbindung externer Dienstleister, Institutionen und Krankenhäuser erfolgt nur über einen abgesicherten, klar definierten Zugangspunkt auf Basis einer Firewall / VPN-Struktur (Cisco-ASA-5525-Cluster basiert).

Erstellt:	Machacek, Roger - 15.03.2022	15.03.2022	ID: 34392
Inhaltlich geprüft:	Schulz, Uwe - 13.05.2022	13.05.2022	Revision: 002/05.2022
Formal geprüft:	Ruback, Alexander - 16.05.2022	16.05.2022	Wiedervorlage: 23.05.2026
Freigegeben:	Weitemeyer, Christian - 16.05.2022	16.05.2022	Seite 5 von 6

Netzwerk-Basis-Dienste und Dienste der Bürokommunikation

Die klinikumsweite Verfügbarkeit von zentralen Netzwerk-Basis-Diensten bildet eine wichtige infrastrukturelle Voraussetzung für die Realisierung und den Routinebetrieb komplexer DV-Projekte.

Folgende Basisdienste werden ausschließlich zentral bereitgestellt:

- IP-Basisdienste (DNS, DHCP, zentraler Syslog-Service, Time-Service (NTP) , LDAP-Verzeichnisdienst), Monitoring via. SNMP, RMON und WMI. Die Implementation separater DNS, DHCP und NTP-Server-Strukturen ist nicht zulässig.
Jegliche Arten von NetzwerkdDiscovery / Netzwerkmonitoring durch Dritte mit Weiterleitung der erhobenen Daten an externe Systeme ist nicht zulässig.
- abgesicherter Zugang zu den Diensten des Internet über ein mehrstufiges zentrales Firewallsystem inkl. Intrusion Detection-/ Präventionsystem und mit integrierter Virusscan-Engine entsprechend den Empfehlungen des BSI (vgl. Abbildung-2)
- abgesicherter Zugang zum WLAN über zentrale Radius-Server
- zentrale Terminalserver für den sicheren Zugriff auf die Ressourcen einer anderen Zone,
- zentrales Active-Directory mit mehreren AD-Servern, Einführung von AD-Sites (für eine bessere Verwaltung der einzelnen Sicherheitszonen) in Vorbereitung
- zentraler SMTP / IMAP basierter E-Mail-Server (inkl. WEB-Mail und Groupware-Frontend) – Ablösung durch Microsoft-Exchange in Umsetzung
- Bürokommunikation mit zentralen Datei- und Printservern, zentraler System-Update-Service,
- zentrale Installations- und Updatedienste für ausgewählte Clients und Server (Schwerpunktmäßig in Zone-1)
- zentrales Backup,
- Intranet Server für hausinterne Informationsrecherchen,

Erstellt:	Machacek, Roger - 15.03.2022	15.03.2022	ID: 34392
Inhaltlich geprüft:	Schulz, Uwe - 13.05.2022	13.05.2022	Revision: 002/05.2022
Formal geprüft:	Ruback, Alexander - 16.05.2022	16.05.2022	Wiedervorlage: 23.05.2026
Freigegeben:	Weitemeyer, Christian - 16.05.2022	16.05.2022	Seite 6 von 6