

Funktionale Empfehlungen an eine KNX-IT Infrastruktur
Erhöhte Anforderungen, Bereich Smart Home, Small Office, HomeOffice,
ab 30 IP-Netzwerkteilnehmer

Version 2018_03_13

Die folgende Beschreibung definiert die Ausführungsart einer KNX-IT Infrastruktur bezüglich des Einsatzes in oben genannten Bereichen. In einem solchen Gebäude werden diverse Anwendungen über Gewerkegrenzen hinweg per KNX-, wie auch IP-Datennetzwerk betrieben. Anhand der folgenden Anforderungen soll gemäß DIN ISO/IEC 27000 die

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Kontrollierbarkeit

der über diese Netzwerke übertragenen Daten und Informationen gewährleistet bzw. verbessert werden.

Den Anforderungen ist vollständig zu folgen, Ausnahmen bedürfen der Begründung gegenüber der Bauleitung bzw. den Bauherrn.

1. Allgemeines

Sämtliche zentralen Netzwerkelemente (Switch, Router, NAS etc.) sind nach Bedarf und Anforderung in einem abschließbaren Netzwerkschrank unterzubringen

Datenleitungen (IP, KNX etc.) sind im Außenbereich geschützt zu verlegen. Netzwerkanschlüsse jeglicher Art sind dort zu vermeiden. Die in diesem Bereich an die genannten Netzwerke angeschlossenen Geräte, sind gesondert gegen Zugriff, d.h. Demontage zu sichern. Sollte diese Empfehlungen auch in einem quasi-öffentlichen Umfeld angewandt werden (z.B. im Hotelzimmer), erstreckte sich diese Anforderung im übertragenen Sinn auch auf KNX-Geräte innerhalb des Gebäudes.

Gebäudeserver sind so einzurichten, dass vom Nutzer eingegebene Daten (z.B. Schaltzeiten der Uhren, sog. Remanentdaten) nach einer Aktualisierung der Software-Applikation bzw. einem Firmware-Update unverzüglich wieder zur Verfügung stehen.

Die Datennetzverkabelung ist entsprechend DIN EN50173-1 (Anwendungsneutrale Kommunikationskabelanlage) in Kategorie 6 augmented (Cat-6 bzw. Cat-6A) auszuführen und zu zertifizieren. Darüber hinaus sind Datenleitungen getrennt nach Gewerken bzw. Diensten auf Patchpanels aufzulegen.

Es sind nach Kundenanforderung und der dadurch notwendigen Dimensionierung hinsichtlich der Performanz und Datensicherheit des Netzwerks, Gigabit Switche (Manageable Layer 3 und evtl. Layer 2 Switche) zu nutzen.

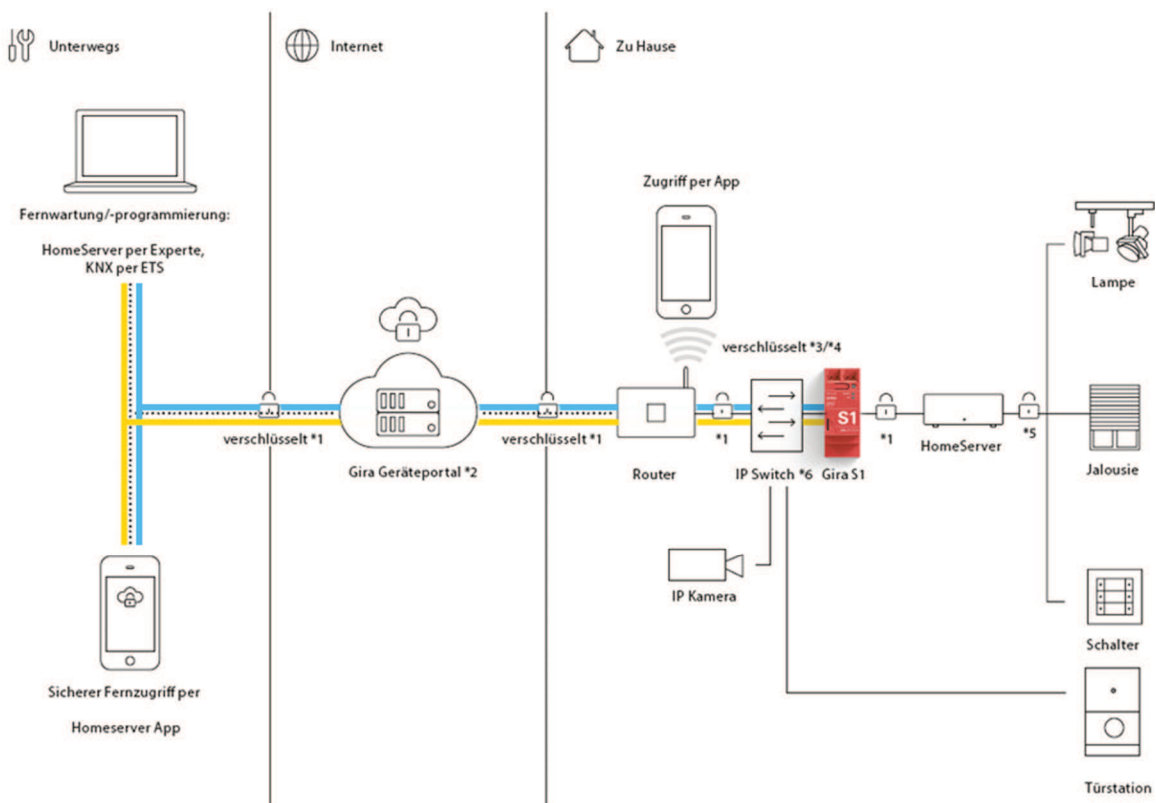
Die Dimensionierung eventuell erforderlicher POE (Power over Ethernet) Anschlüsse ist zu belegen. (Notwendig für z. B. die Versorgung von Netzwerkkameras.)

Im Bereich des hauseigenen Intranets (VLAN) ist zwingend das Internet Protocol Version 4 (IPv4) zu nutzen.

2. KNX-Koppler Programmierung

Die KNX-Koppler sind entsprechend der KNX-Topologie korrekt physikalisch zu adressieren. Filtertabellen sind zu setzen und sind sinnhaft zu nutzen. Eine Weiterleitung von inkorrekten Quelladressen in eine übergeordnete Linie ist auszuschließen. Punkt zu Punkt Verbindungen (z. B. für eine Geräteprogrammierung) über Koppler hinweg sind nach Abnahme der Anlage zu blockieren. Das Setzen eines BAU-Schlüssels (Passwort zur Sicherung des Zugriffs auf KNX-Geräte) wird dringend empfohlen.

3. IP-Topologie für erhöhte Anforderungen, Empfehlung ab 30 IP-Netzwerkteilnehmer



Quelle: Gira

Folgende Geräte wurden auf die im Weiteren dargestellten Anforderungen getestet:

Fernzugriff: Gira S1: Fa. Gira, Bestell-Nr.: 208900

Router: Fa. Netgate, z.B. Typ: SG2440 mit pfsense Paket

Switch: Fa. Cisco, Serie SG350-xx bzw. SG 500-xx entspricht einem xx-Port Switch

WLAN Accesspoint: Fa. Cisco, Typ WAP371

4. Programmierung der Switche

Der prinzipielle Aufbau des VLAN-Netzwerkes ist nach Diensten und Anwendungen getrennt auszuführen.

Die Layer 3-Switches sind grundsätzlich nach IEEE 802.1q, d.h. als sogenanntes Tagged VLAN, zu betreiben. Eventuell notwendige Untagged Ports der Switches sind zu dokumentieren.

Die Anwendung von dynamischen VLAN bzw. rein (Anschluss)Port-basierenden VLAN ist nur nach Absprache mit der Bauleitung zulässig.

Anmerkung:

In der Betriebsart Tagged VLAN stehen an jedem beliebigen Anschlusspunkt des IP-Netzwerks die individuellen Dienste des angeschlossenen Geräts zur Verfügung.

Beispielhafte Zuordnung der Dienste und Anwendungen auf die VLAN Segmente:

- VLAN10: Haustechnik (KNX; Home/FacilityServer, X1, andere Bus Systeme)
- VLAN20: Voller Internetzugang für Firewall und andere Zwecke
- VLAN30: Daten-Netz für PC, Drucker, Tablets etc.
- VLAN40: Heizung/Klima/Lüftung, für z.B. Wartungszwecke
- VLAN50: Audio/Video/Multimedia Anwendungen
- VLAN60: IP-Kameras für z.B. die Gebäudeaußenüberwachung
- VLAN70: IP Gastzugang (für z.B. WLAN und reglementierte Zugänge)
- VLAN80: Internet-Telefonie, Voice over IP
- VLAN90: unbenutztes VLAN für unbenutzte physikalische Ports

Das administrative VLAN1 ist getrennt von anderen VLAN eingerichtet. Um ein Routing zwischen den VLAN zu ermöglichen, ist mit getrennten IP-Kreisen (Sub-Net) zu arbeiten. Die Vergabe von statischen IP-Adressen ist zu bevorzugen. DHCP Funktionalitäten innerhalb des Netzwerks sind nur in eingeschränkter Weise zu realisieren. Diese Vorgabe ist mit den gerätespezifischen Anforderungen der eingesetzten Systeme abzustimmen.

Der Zugriff auf die Konfigurationsschnittstellen des Switches und des Routers sind über entsprechend sichere Passwörter (siehe Punkt 9) zu sichern.

5. Sicherheitstechnisch wichtige Spezifikationen der Switches

Unterstützung des Spanning Tree Protocol. Hiermit sind bei der Verbindung von Switchen untereinander redundante Verbindungen möglich.

Bei Verwendung von Layer 2 Switches wird eine volle CLI (Command Line Interface) Unterstützung empfohlen.

Unbelegte physikalische Ports sind einzeln abzuschalten oder freien VLAN Segmenten zuzuweisen.

Der Failopen Mode ist zu deaktivieren, wenn dieser sich nicht automatisch selbst abschaltet. D.h. der Switch schaltet nicht selbstständig in den Hub-Modus, wenn die internen MAC Adressen Tabellen zum Überlaufen gebracht worden sind. (MAC Flooding)

Bei aktiven Ports ist die Autotrunking Funktion nach IEEE 802.1q abzuschalten (802.1q Negotiation).

Für eine definierte Anzahl physikalischer Ports ist eine feste Zuordnungen zu einer zugelassenen MAC-Adresse zu definieren. (Port Security Feature)

Die internen Routen zwischen den VLAN Netzen und der Firewall sind bedarfsgerecht zu programmieren. Da hier grundlegende Sicherheitsmechanismen der Anlage festgelegt werden, ist in Abhängigkeit der Anlagengröße zu entscheiden, ob das Routing im Layer 3 Switch oder in einer entsprechenden Firewall gelöst wird.

Der Umfang der Umsetzung dieser Spezifikationen geschieht nach Absprache mit der Bauleitung und muss entsprechend dokumentiert werden (vergl. 10.).

6. Externe Zugriffe auf das IP-Datennetzwerk

Um dem Nutzer des Gebäudes eine Möglichkeit zu geben, von außen über geeignete Anwendungen (Apps) in die Anlage eingreifen zu können, ist das Vorgehen differenziert nach Anwendung und deren Möglichkeiten auszuführen.

6.1 Ausführung der Fernzugriffs- und Fernwartungsfunktion am Beispiel Gira S1

Der Gira S1 ist Teil des IP-Netzwerks der Kundenanlage. Das Gerät verbindet sich automatisch, ohne weitere Änderungen an der Firewall des Routers, über das Internet mit dem Gira-Geräteportal. Die Kommunikation zwischen S1 und Portal ist AES verschlüsselt und mit digitalen Zertifikaten gesichert.

In Abhängigkeit von dem jeweiligen Gerät unterstützten Netzwerkprotokoll, erfolgt der Zugriff auf das Gerät direkt über das Gira Geräteportal oder über den Gira S1 Windows Client.

Die KNX-Installation ist mit dem S1 direkt zu verbinden und auf dem Wege von außerhalb im Zugriff und von der Ferne wartbar.

6.1.1 Benutzerverwaltung über das Gira Geräteportal

Die Verwaltung der Benutzer und deren Zugriffsrechte auf geeignete Netzwerkgeräte im Sinne der Fernbedienung bzw. Fernwartung der Anlage muss durch den Endkunden möglich sein. Dies kann in Verbindung mit dem GIRA S1 über das Gira Geräteportal (<https://geraeteportal.gira.de>) erfolgen.

Dem Nutzer der Anlage ist dort ein eigenes Konto einzurichten, über welches er selbstständig in der Lage ist, sämtliche Benutzerrechte bezüglich des Zugriffs von außen zu administrieren. Das Geräteportal speichert keine übertragenen Daten und wird auf Servern in Deutschland unter Einhaltung der deutschen Datenschutzrichtlinien betrieben.

6.2 Ausführung des Fernzugriffs auf die restlichen Netzwerkgeräte

Sollte ein Gerät/System nicht über den Weg des Gira S1 von außen erreichbar sein, so ist dieser Fernzugriff über VPN einzurichten. Bevorzugt ist hierbei der Aufbau des VPN auf Basis von IPSec, richtet sich aber auch nach den Möglichkeiten der zu nutzenden VPN Clients auf z.B. den SmartPhones.

Die Ausführung einer VPN Zuweisung an z.B. VLAN 10 (z.B. die Haustechnik) wird empfohlen.

7. Prinzipielle Anforderungen an das WLAN

Zur Durchgängigkeit des oben beschriebenen Konzepts sind für den Aufbau des WLAN ausschließlich Multi-Access Points einzusetzen (durchgängige VLAN Unterstützung). Die genannten VLAN 10, 30, 50, 70, 80 sind in der WLAN Planung zu berücksichtigen und getagged an die Accesspoints zu übertragen.

Übertragungs-Bandbreite in den Kernbereichen des Gebäudes 108 Mbit/s, ansonsten 36Mbit/s.
Minimale Sendefeldstärke im abzudeckenden Bereich: -85dBm

Eine Auslastungsplanung, die Kanalüberlappungen und Interferenzen berücksichtigt, ist anzufertigen und mit einer HeatMap auf Basis des Gebäude-Grundrisses zu dokumentieren. Unter Berücksichtigung regionaler Funkgegebenheiten ist zu dem Zeitpunkt eine bewusste Entscheidung für das 2,4 GHz und 5 GHz-Band zu treffen. Auf Grundlage von Vorgaben der Bauleitung zur maximal möglichen WLAN-Datenübertragungsrate, ist eine Kanalbandbreite von 20 MHz, 40 MHz oder mehr festzulegen.

Die Access Points müssen nach IEEE802.11.r arbeiten oder das WLAN-Roaming (= nahtloser Wechsel eines Teilnehmers von einer Funkzelle in eine andere, ohne dass eine bestehende Funkverbindung abgebrochen wird) durch herstellerspezifische Mechanismen realisieren. In diesem Fall sind diese Geräte von einem Hersteller zu wählen.

Das vereinfachte Authentifizierungs-Verfahren WPS (Wi-Fi Protected Setup) ist nach Einlernen der Endgeräte sofort wieder zu deaktivieren.

8. Sicherheitsmaßnahmen im WLAN Bereich

Um das Risiko versehentlich bekannt gewordener WPA2-Passwörter zu vermeiden, ist (soweit es der WLAN-Client zulässt) die Anmeldung am WLAN Netzwerk über eine Einzelbenutzer-Authentifizierung, mittels einer RADIUS Server Funktion, zu realisieren.

Dies gilt allgemein für alle betroffenen VLAN.

Als Verschlüsselungsstandard zwischen den WLAN Access Points und den mobilen Endgeräten WPA2-Enterprise nach IEEE802.1X, in Verbindung mit Algorithmus AES, zu nutzen.

Für Heimgeräte wie ebook-Reader (z.B. Kindle) oder Streaming -Lösungen (z.B. Firestick) kann eine WPA2-Personal Anmeldung vorgesehen werden.

Ausnahme: Der IP-Gastzugang in VLAN70

Dieses ist als virtuelles, isoliertes Gastnetz zu erstellen. Dieses Netz erlaubt z.B. Gästen ausschließlich die Internet- und Email-Nutzung. Die Anmeldung zum Gastnetz erfolgt über ein Captive-Portal.

9. Vorgaben zur Gestaltung sicherer Passwörter

Es gelten im Maßnahmenkatalog M2.11 des IT-Grundschutzkatalogs, veröffentlicht vom BSI (Bundesamt für Sicherheit in der Informationstechnik), definierten Gestaltungsregeln. (Stand 2016)

Siehe unter:

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html

Dies sind unter anderem:

- Das Passwort darf nicht leicht zu erraten sein. Namen, Kfz-Kennzeichen, Geburtsdatum usw. dürfen deshalb nicht als Passwörter gewählt werden.
- Ein Passwort sollte aus Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen bestehen. Es sollten mindestens zwei dieser Anforderungen umgesetzt sein.
- Wenn für das Passwort alphanumerische Zeichen gewählt werden können, sollte es mindestens 8 Zeichen lang sein.

10. Spezielle Anforderungen an die Dokumentation der IT-Infrastruktur

Steuerung, Kontrolle und Notfallvorsorge bei IT-Systemen basieren auf einer aktuellen Dokumentation der vorhandenen IT-Infrastruktur. Nur eine aktuelle Dokumentation der Systemkonfiguration ermöglicht im Notfall einen geordneten Wiederanlauf.

Dies beinhaltet folgender Inhalte:

- physikalische Netzkonfiguration
- logischen Netzkonfiguration
- Beschreibung des internen Routings zwischen den VLAN-Netzen.
- Zugriffsrechte der einzelnen Benutzer
- Stand der Datensicherung
- eingesetzte Applikationen und deren Konfiguration (bezgl. der aktiven Netzwerkkomponenten)
- Die Internet-Zugangsdaten, bereitgestellt vom Internet-Provider, sind Teil der Anlagendokumentation.

Es ist auf Aktualität und Verständlichkeit der Dokumentation zu achten, damit auch ein Vertreter die Administration jederzeit weiterführen kann. Die Dokumentation ist so aufzubewahren, dass sie im Bedarfsfall jederzeit verfügbar ist. Wenn sie in elektronischer Form geführt wird, sollte sie entweder regelmäßig ausgedruckt oder auf einem transportablen Datenträger gespeichert werden. Der Zugriff auf die Dokumentation ist auf den Bauherren zu beschränken.

In der Dokumentation sollten alle Schritte aufgeführt sein, die beim Herauf- bzw. Herunterfahren des IT-Systems zu beachten sind.

11. Betreuung und Systempflege

Die vorab beschriebene KNX-IT Infrastruktur bedarf, um sie technisch und funktional auf einem aktuellen Stand zu halten, der dauerhaften Betreuung und Systempflege. Dabei sind Nutzungsanpassungen, Updates und aktuelle Sicherheitsvorgaben zu berücksichtigen.

Vergl. jährlicher Lagebericht des BSI zur IT-Datensicherheit:

<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.html>

Eine vertraglich gesicherte und zyklisch ausgeführte Systempflege wird empfohlen.

12. Support und weitergehende Unterstützung

Bei Fragen zur Umsetzung der Empfehlungen, bezugnehmend auf die Programmierung des Switches, wenden Sie sich bitte an den offiziellen Support des Herstellers:

http://www.cisco.com/c/de_de/support/index.html

Tel.: 0800 503 0017

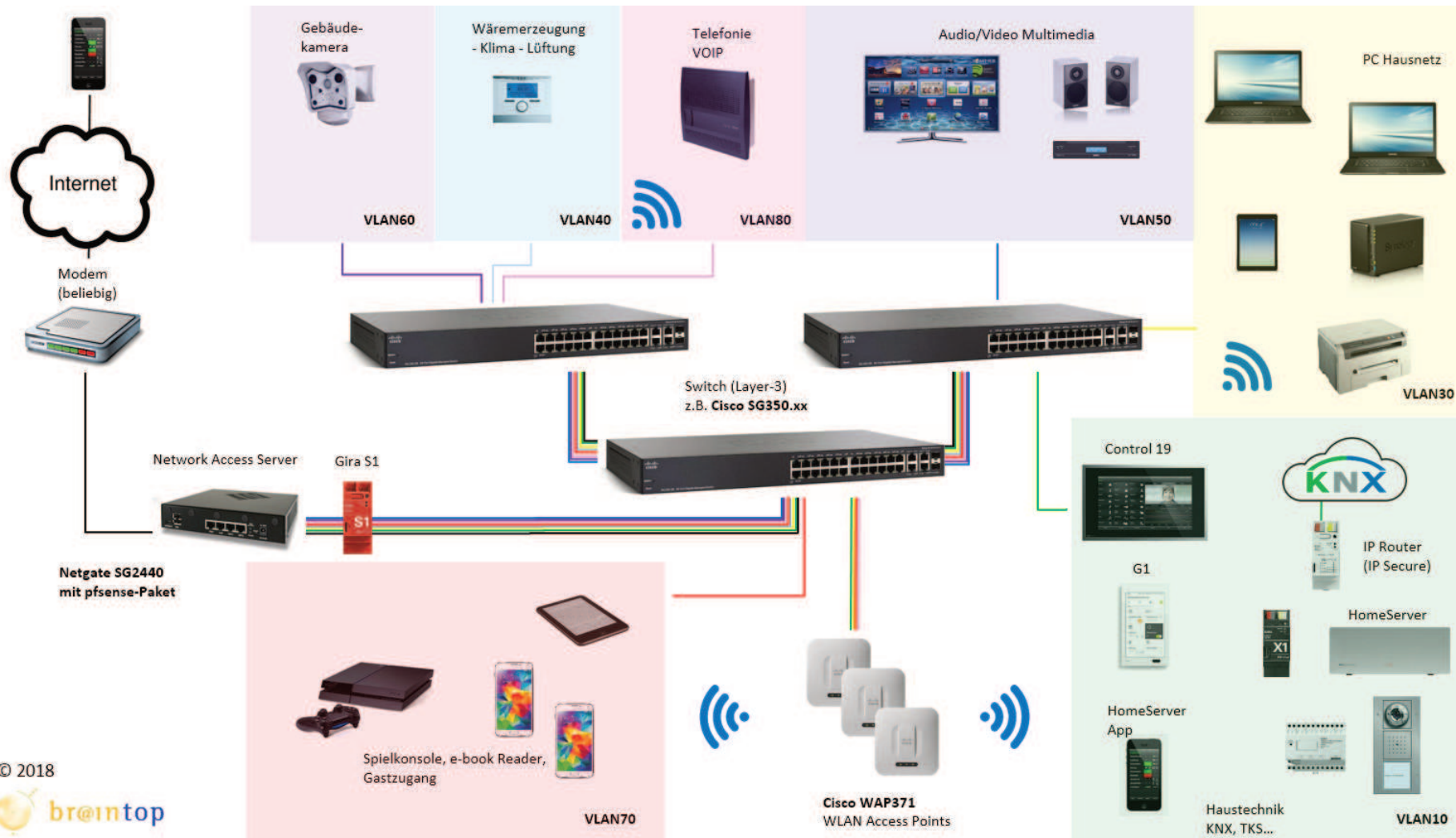
Bei ähnlich gelagerten Fragen zum Network Access Server, wenden Sie sich an den Hersteller unter <https://netgate.com>

Bei Fragen zum Gira S1

Support des Herstellers: Tel.: 02195-602-123 / hotline@gira.de

Diese Empfehlungen sind mit hoher Sorgfalt erstellt worden, es kann jedoch nicht ausgeschlossen werden, daß im Einzelfall davon abgewichen werden muss. Somit kann keine Gewährleistung vom Ersteller dieser Empfehlung übernommen werden. Ebenso sind weitergehende Ansprüche ausgeschlossen.

Beispielhafter Aufbau: (Anzahl der Layer-3 Switche nach Bedarf)



Anmerkung:

Die aufgeführten Geräte dienen ausschließlich der beispielhaften Darstellung und bedürfen im realen Fall einer fach- und funktionsgerechten Planung.