Network concept for Kraftwerk1

Version	Status	date	Author:in
0.1	First draft	20.12.2023	Felix Köppel
0.2	Revision	09.01.2024-11.01.2024	Felix Köppel
0.3	Addition after measurements	12.01.2024 & 15.01.2024	Felix Köppel
0.4	Additions	17.01.2024 & 18.01.2024	Felix Köppel
0.5	Small additions	24.01.2024 & 25.01.2024	Felix Köppel
0.6	Additions to firewall, switch and devices	02.02.2024	Felix Köppel
0.7	Additions and channel allocation	06.02.2024	Felix Köppel, Fabio Pagotto
0.8	Further additions and planning update, setting up network PVID8	07.03.2024 & 14.03.2024	Felix Köppel
0.81	Status update for internet subscription	02.05.2024	Felix Köppel
1.0	Last finalisations and final version	PENDING	Egil Rüefli, Felix Köppel, Fabio Pagotto

This network concept was created by the project team of Rafisa Informatik GmbH.

Client: Building and housing co-operative Kraftwerk1

Hardturmstrasse 134
8005 Zurich

Your name	Position	e-mail address	Phone number
Andreas Engweiler	Managing Director	andreas.engweiler@kraftwerk1.ch	044 446 40 66
Alex Hafner	Administration & Management	alex.hafner@kraftwerk1.ch	044 446 40 64
David Müller	Client representative (Müller Schnörringer Architects sia)	dm@muellerschnoerringer.ch	044 545 10 66
Andreas Knecht	CEO Electrical installation company (Züri Elektro AG)	andreas.knecht@zueri-elektro.ch	044 209 92 90

Location of the property to be equipped

Hardturmstrasse 269
8005 Zurich

Project team: Rafisa Informatik GmbH

Bernstrasse 88
8953 Dietikon

Your name	Position	eMail	Phone number
Fabio Pagotto	Responsible for Firewall and LAN	f.pagotto@rafisa.ch	+41 76 306 71 51
Felix Köppel	Responsible for LAN, Firewall and WiFi	f.koeppel@rafisa.ch	+41 78 713 43 65
Egil Rüefli	Project Manager	e.rueefli@rafisa.ch	+41 78 767 84 04

VLAN and IP address concept

This concept specifies the VLAN IDs, VLAN names and IP addresses including the subnet mask, the DHCP lease time and the functions of the VLANs. The access authorisations of the VLANs are also specified.

VLAN concept & DHCP configuration concept

This concept contains the VLAN information and DHCP configurations. Please note that VLAN 10 cannot be used, as this VLAN may be required for the Swisscom Internet connection. VLAN 9 is reserved for the fallback Internet connection. It should also be noted that this VLAN is only designed as a „virtual cable“ from the server room to the top floor and is also optional.

PVID	VLAN name	IP subnet	Subnet mask	Lease	Hosts (Range)	Function
1	VLAN01_MGMT	10.1.1.0	255.255.255.0	30 days	154 (.100 - .254)	Management VLAN → Management of all devices
2	VLAN02_IOT-WR	10.1.2.0	255.255.255.128	30 Days	30 (.30 - .60)	Network only for inverters and automatic mailbox
3	VLAN03_IOT-MOB	10.1.3.0	255.255.255.0	1 Day	250 (.3 - .253)	For mobility (Tesla etc.), e-mobile charging station
4	VLAN04_IOT	10.1.4.0	255.255.255.0	30 days	250 (.3 - .253)	All IoT devices
5	VLAN05_GAST	10.1.5.0	255.255.255.0	1 Hour	250 (.3 - .253)	For guests. Has content filter (parental control and more)
6	VLAN06_Jugend	10.1.6.0	255.255.255.0	1 Hour	250 (.3 - .253)	For all minors. Has content filter (parental control)
7	VLAN07_ERW	10.1.7.0	255.255.255.0	1 Hour	250 (.3 - .253)	For adults
8	VLAN08_FAIRCUS	10.1.8.0	255.255.255.0	1 Day	250 (.3 - .253)	Fair Customer Network
9	VLAN09_FALLBACK	-	-	-	-	Virtual cable from top floor to firewall for LTE/5G fallback

Filter information

Parental control filter includes NSFW filters and other things that young people are not allowed to

access.

The additional filter in the guest network only makes mail, social media (youtube, instagram, Facebook and co.), web browsing, video platforms (Netflix and co.) available.

Authorisation matrix of the VLANs

VLAN	01	02	03	04	05	06	07	08	09	WAN
01_MGMT	✔	✔	✔	✔	✔	✔	✔	✔	✘	✔
02_IOT-WR	✘	✔	✘	✘	✘	✘	✘	✘	✘	✔
03_IOT-MOB	✘	✘	✔	✘	✘	✘	✘	✘	✘	✔
04_IOT	✘	✘	✘	✔	✘	✘	✘	✘	✘	✔
05_GAST	✘	✘	✘	✘	✔	✘	✘	✘	✘	✔
06_JUGEND	✘	✘	✘	✘	✘	✔	✘	✘	✘	✔
07_ERW	✘	✘	✘	✘	✘	✘	✔	✘	✘	✔
08_FAIRCUS	✘	✘	✘	✘	✘	✘	✘	✔	✘	✔
09_FALLBACK	✘	✘	✘	✘	✘	✘	✘	✘	✔	✘

Network plan TARGET

The two network diagrams are intended to illustrate our concept. The logical plan shows how the devices communicate with each other. The Layer3 plan shows the structure of the proposed VLANs.

Logical network plan

Will be added after Internet Package upgrade

Layer 3 network plan

Will be added after internet package upgrade

Network devices

Quantity	device	Device manufacturer	Model	Note
1	Modem			Supplied by Init7
1	Firewall	Hunsn	RS41	
1	Controller	Ubiquiti Networks	Cloud Key Gen2 Plus	
1	Switch	Ubiquiti Networks	USW-24-PoE	
1	Switch	Ubiquiti Networks	USW-Flex	Attic
1	PoE Injector	Ubiquiti Networks	U-POE-AT	for switch top floor
2	Access Point	Ubiquiti Networks	U6-Pro	Top floor / slipper bar, for ultra high density
4	access point	Ubiquiti Networks	U6-Plus	all remaining rooms, for low/medium density

Quantity	device	Device manufacturer	Model	Note
2	access point	Ubiquiti Networks	UAP-AC-Lite	Garage (WiFi 5 Only for better device compatibility)
1	Access Point	Ubnt (ubiquiti networks)	UAP	Legacy device for server room only - reuse from before rebuild
1	PoE Passive Injector	Ubnt (ubiquiti networks)	24 passive poe	Legacy device for server room only - reuse from before conversion

Network components Connection information

In order to have a better overview of all devices, a table was created with the devices, including IP address allocation and VLAN access.

Device name	Host name	PVID	PVID Tagged	IP address	Connection type	Location	Notes
U6-Pro	ap-kw1-dg	1	3, 4, 5, 6, 7, 8	10.1.1.13	LAN	Attic floor	
U6-Pro	ap-kw1-pb	1	3, 4, 5, 6, 7, 8	10.1.1.12	LAN	Slipper bar	
U6-Plus	ap-kw1-kr	1	3, 4, 5, 6, 7, 8	10.1.1.11	LAN	Creative room	
U6-Plus	ap-kw1-jr	1	3, 4, 5, 6, 7, 8	10.1.1.10	LAN	Youth room	
U6-Plus	ap-kw1-kd	1	3, 4, 5, 6, 7, 8	10.1.1.9	LAN	Consumer depot	
U6-Plus	ap-kw1-gz	1	3, 4, 5, 6, 7, 8	10.1.1.8	LAN	Guest room	
UAP-AC-Lite	ap-kw1-gn	1	3, 4, 5, 6, 7, 8	10.1.1.7	LAN	Garage (North)	(WiFi 5 Only)
UAP-AC-Lite	ap-kw1-gs	1	3, 4, 5, 6, 7, 8	10.1.1.6	LAN	Garage (South)	(WiFi 5 Only)
UAP	ap-kw1-edv	1	7	10.1.1.5	LAN (24passive)	IT room	LEGACY device
USW-Flex	sw-kw1-02		1, 2, 3, 4, 5, 6, 7, 8, 9	10.1.1.4	LAN TRUNK	Top floor	
USW-24-PoE	sw-kw1-01		1, 2, 3, 4, 5, 6, 7, 8, 9	10.1.1.3	LAN TRUNK	RK-KW1-01	
Cloud Key Gen2	uck-kw1-01	1		10.1.1.2	LAN	RK-KW1-01	
devices Fair Customer		8		DHCP	LAN & WiFi	Office ()	
devices adults		7		DHCP	WiFi		
devices youth		6		DHCP	WiFi		
devices guests		5		DHCP	WiFi		
IoT end devices		4		DHCP	WiFi		
TV attic		4		DHCP	LAN	Top floor	

Device name	Host name	PVID	PVID Tagged	IP address	Connection type	Location	Notes
Mobility devices		3		DHCP	WiFi	Garage	

Terminal list: Connectivity

List of end devices

The following table contains all the device types used with the possible connection options and those recommended by us (or determined in meetings).

Quantity	Brand name	Device name	Device type	IT functionality	Proposal Connection	Location
			Inverter	Ethernet/WiFi	Ethernet	
			E-mobile	WiFi	WiFi	Garage

Terminal list: Network connection

Device name/brand	Device type	Connection type	PVID	IP address assignment	Hostname
	Inverter	LAN	2	DHCP	-
	E-Mobile	LTE/WiFi	3	DHCP	-

Switch Port assignment VLAN

Changes possible, not final yet!

sw-kw1-01

Switch Model: USW-24-POE Ubiquiti Networks Switch 24 PoE Standard

PoE budget: 95 watts. Used in total: 75 watts.

Port	patch	PVID (native/[tagged]/{profile})	Device	MAC address	Power	Hostname / Note
1	-	1	Management laptop			Management only
2	-					FREE
3	UG04					
4	EC07					
5	EC05					
6	EC06					
7	EC04					
8	UG02					
9	-	1 - UCK	Cloud Key Gen2 Plus	70:a7:41:f9:65:63	13 Watt	uck-kw1-01 (RK-KW1-01)

Port	patch	PVID (native/[tagged]/{profile})	Device	MAC address	Power	Hostname / Note
10	UG03	1 [3, 4, 5, 6, 7, 8] {AP-Uplink}	UAP-AC-Lite	d8:b3:70:b6:a7:b8	6.5 Watt	ap-kw1-gs / Garage South (WiFi 5 Only)
11	UG01	1 [3, 4, 5, 6, 7, 8] {AP-Uplink}	UAP-AC-Lite	d8:b3:70:b6:a8:16	6.5 Watt	ap-kw1-gn / Garage North (WiFi 5 Only)
12	EG01	1 [3, 4, 5, 6, 7, 8] {AP-Uplink}	U6-Plus	d8:b3:70:e9:34:3c	9 watts	ap-kw1-gz / guest room
13	EC12	1 [3, 4, 5, 6, 7, 8] {AP-Uplink}	U6-Plus	d8:b3:70:e6:d9:40	9 Watt	ap-kw1-kd / consumer depot
14	EG11	1 [3, 4, 5, 6, 7, 8] {AP-Uplink}	U6-Plus	d8:b3:70:e9:06:68	9 watts	ap-kw1-jr / Youth room
15	EG02	1 [3, 4, 5, 6, 7, 8] {AP-Uplink}	U6-Plus	d8:b3:70:e9:4d:60	9 watts	ap-kw1-kr / creative room
16	EG03	1 [3, 4, 5, 6, 7, 8] {AP-Uplink}	U6-Pro	e4:38:83:6b:47:31	13 Watt	ap-kw1-pb / slipper bar
17	-	1 [7, 8] - AP-EDV	UAP	24:a4:3c:86:6c:e4	-	ap-kw1-edv / EDP-AP. 24v Passive PoE Injector
18	EG09				-	FAIR CUSTOMER
19	EG08				-	PACKAGE STATION
20	EG10				-	FAIR CUSTOMER
21	DG01				-	RESERVE ATTIC
22	DG02	TRUNK {UPLINK}	USW-Flex Port 1	ac:8b:a9:a5:ed:0e	-	PoE+ Injector powered, Uplink SW-KW1-02
23	-	TRUNK {UPLINK}	Firewall LAN2		-	Reserved - Link aggregation Firewall! - Disabled
24	-	TRUNK {UPLINK}	Firewall LAN1		-	Main uplink to the firewall

sw-kw1-02

Port	PVID (untagged/[tagged]/{profile})	Device	MAC address	Power requirement	Device name/note
1	TRUNK	Switch server room	d8:b3:70:5c:fd:77	Power Input	PoE+ Injector
2	7	indeterminate		-	unknown

Port	PVID (untagged/[tagged]/{profile})	Device	MAC address	Power requirement	Device name/note
3	7	Mains connection cabinet		-	Connection in the cabinet
4	7	Mains connection table		-	Connection table
5	1 [3, 4, 5, 6, 7, 8] {AP-Uplink}	U6-Pro	e4:38:83:72:96:71	13 watts	ap-kw1-dg

You could set the TRUNK profile on port 4 and connect a USW-Flex Mini, which only consumes 2.5 watts, and configure it according to the requirements in order to have more Ethernet connections.

WiFi SSIDs, frequency bands and VLAN assignment

Felix has written down the WiFi SSIDs (WiFi network names), the encryption type, the VLAN allocation and the radio frequency bands here. Felix has also written down the bandwidth limitation for the network. The information is given from the client's point of view, i.e. 20/30 (up/dn) would be 20Mbit/s upload and 30Mbit/s download.

Shared Key is a new technology with which you have one SSID and several passwords. Depending on the password you enter, you can access one VLAN or the other. You can store several passwords and specify which VLAN they will be sent to.

SSID	PVID	Frequency band	Encryption	AP group	Devices	QoS (Mbit/s)	Other
KW1-DEBUG	1	2.4GHz & 5GHz	WPA3-SAE	All	Admins & test devices	unlimited	only active during debugging
KW1-Mobility	3	2.4GHz & 5GHz	WPA2-PSK	GARAGE	Cars, end devices Mobility	40/40 (up/dn)	Active
KW1	1, 4, 5, 6, 7, 8	2.4GHz & 5GHz	WPA2-PSK	All	All devices	50/50 (up/dn)	Active with shared key
KW1-EDV	7	2.4GHz	WPA2-PSK	EDV	Admins in the IT room	unlimited	Only active on AP in the EDV room!

Radio settings

		2.4GHz frequency band			5GHz frequency band			
AP host name	AP-Group	Channel	Bandwidth	TX power	Channel	Bandwidth	TX-Power	More
ap-kw1-edv	EDV	Auto	20MHz	23dBm	-	-	-	2.4GHz only
ap-kw1-gn	GARAGE, GN	9	20MHz	20dBm	48	80MHz	20dBm	WiFi 5 only

ap-kw1-gs	GARAGE, GS	5	20MHz	20dBm	64	80MHz	20dBm	WiFi 5 only
ap-kw1-kd	KD, All	13	20MHz	17dBm	64	40MHz	23dBm	
ap-kw1-gz	GZ, All	1	20MHz	17dBm	136	40MHz	23dBm	
ap-kw1-jr	JR, All	5	20MHz	26dbm	136	40MHz	26dBm	Relief KR
ap-kw1-kr	KR, All	1	20MHz	26dBm	52	80MHz	26dBm	PB relief
ap-kw1-pb	PB, All	5	20MHz	22dBm	128	80MHz	26dBm	Outdoor Mode
ap-kw1-dg	DG, All	5	20MHz	22dBm	128	80MHz	26dBm	Outdoor Mode

VPN configurations

Will be added later!

Internet connection

In realisation phase.

Upgrade to init7 fibre 1/1 gbit/s with media converter and TV subscription - confirmed! Order is not yet finalised.

Currently: Swisscom Fibre connection 40/40 mbit/s with Swisscom Internet Box Standard

Fallback solution

Mobile provider/subscription: Unknown 4G/5G modem: To be added!

To be completed!

IPTV

To be added!

Existing Blue TV with sports subscription

Documentation of the settings

https://wiki.rafisa.net/doku.php?id=de:intern:dokumentationen:log_unifi-cloud-key_access-point_konfigurieren