

ENERGYHUB INTERN-NÄTVERK

Vid inkoppling av flera EnergyHub enheter installeras ett internt nätverk. Detta används för att systemet ska kunna synkronisera styrparametrar samt att aggregera mätdata från samtliga enheter. Den aggregerade mätdata visas på den interna displaymodulen och skickas upp till Ferroamp Portal. Detta nätverk är tänkt att vara isolerat och representerat som en nod i kundens nätverk. När EnergyHub-systemet är installerat kan någon inte fysiskt komma åt den interna nätverksutrustningen utifrån såvida lås till dörrar är låsta med medföljande nycklar. Detta dokument beskriver nätverkskonfigurationen för dessa nätverk.

1 Överblick

Illustration visar det interna nätets uppbyggnad. Nätverket innehåller en router som har NAT-funktion samt DHCP för att hantera den interna nätverksrymden. System förberedda för fler än tre enheter består även av en icke konfigurerbar switch.

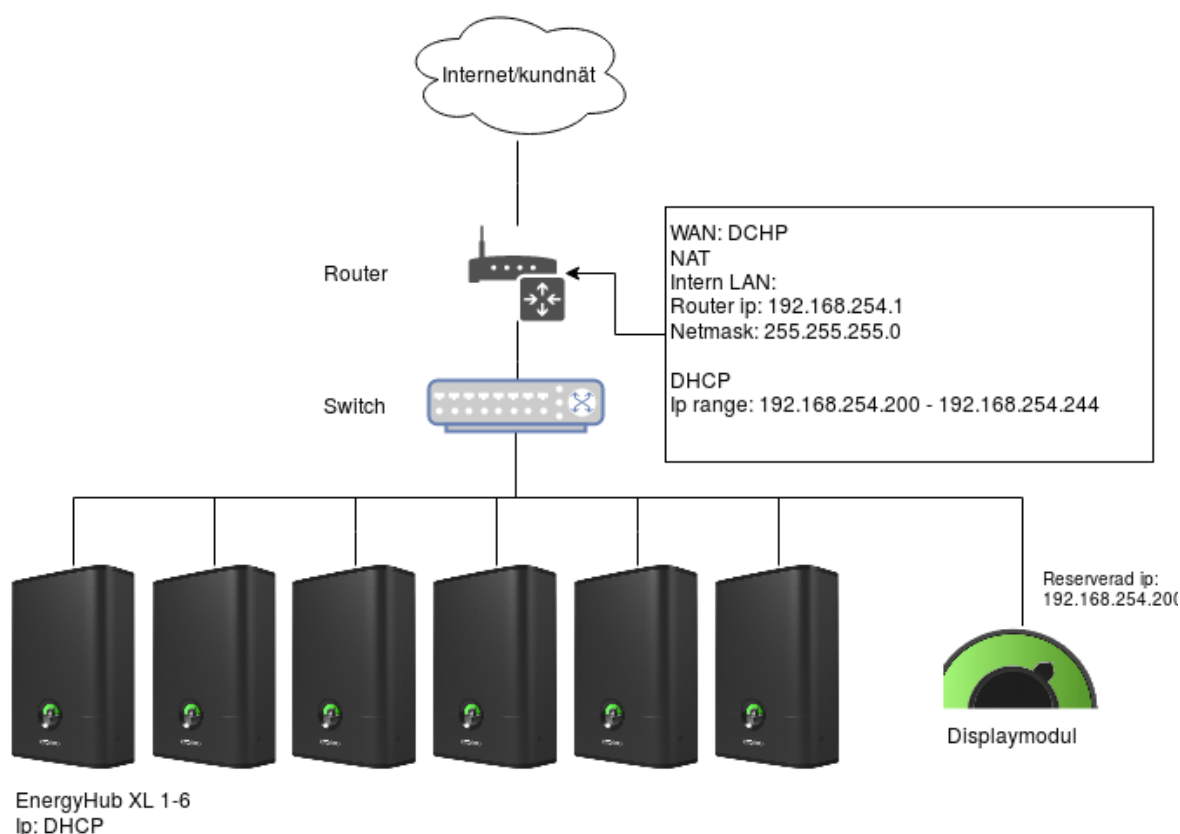


ILLUSTRATION 1: NÄTVERKSDIAGRAM

2 Nätverkskonfiguration

2.1 WAN

WAN i detta fall syftar till kundens nätverk eller internet uppkoppling. Detta kopplas in på WAN-porten på den interna routern.

Standard är routern konfigurerad till att ta emot ip-adress samt DNS via DHCP automatiskt.

Detta kan omkonfigureras av oss på Ferroamp på begäran av kund.

2.2 LAN

LAN i detta fall syftar till det interna nätverket inuti t.ex. rackskåp. Detta nätverk är konfigurerat att innehålla en intern DHCP för att hantera de interna enheternas ip-adresser.

Den interna DHCP servern är konfigurerad som följer:

IP-adressrymd	192.168.254.200-192.168.254.244
Nätmask	255.255.255.0
Gatewayadress/routeripadress	192.168.254.1
DHCP-lån	24h
IP-reservation till display	192.168.254.200

2.3 NAT

Routern innehåller NAT mellan LAN och WAN för att representeras som en enhet på kundens nätverk. Det finns inga portar öppna in till någon av enheterna i standardfallet.

Om kunden vill aktivera modbus TCP eller ExtAPI kommunikation in till EnergyHub systemet så kommer även en eller flera port-forward att aktiveras i NAT konfigurationen.

3 Portar

3.1 Inkommande portar

I standard konfiguration är inga inkommande portar öppna in till systemet. All kommunikation initieras inifrån systemet. Fjärrstyrning går via portalen eller av Ferroamps personal via Ferroamp service gateway.

Om kund vill använda modbus TCP eller ExtAPI så öppnas portar för detta vid konfigurationen. Dessa APIer kommer då att vara tillgängliga på systemets WAN ip-adress på port enligt API specifikation. (Port-forwards kommer att konfigureras enligt 2.3). Detta gör att systemets APIer blir exponerat till hela nätverket kopplat till WAN. Därför rekommenderar vi att kunden konfigurerar statiska adresser till de enheter som vill ansluta till APIerna så att dessa kan bli låsta i port-forward konfigurationen.

3.2 Utgående portar

För att systemet ska kunna kommunicera med Ferroamp Portal samt att kunna få nya mjukvaruuppdateringar eller få fjärrsupport av Ferroamps supportavdelning behöver systemet kunna ansluta till ett antal portar på Ferroamps servrar.

Dessa adresser kan komma att ändras utan förvarning.

Detta är de utgående portarna systemet kommer ansluta på:

Protokoll	Port	Adress
MQTT	1883,8883	Data2.ferroamp.se
Service gateway	2443	52.29.33.74
NTP	123	
DNS	53	8.8.8.8
Uppdateringar	80,443	Amazon S3 bucket eu-central-1 region

3.2.1 MQTT

Den mätdata och styrparametrar som kan ses eller styras i eller via ferroamp portal transporteras via MQTT protokollet till Ferroamps MQTT broker som hostas i vårt moln på Amazon AWS. Denna trafik autentiseras och krypteras med TLS v1.2.

3.2.2 Service gateway

Systemet öppnar en ssh-tunnel till Ferroamps service gateway. Denna används för att kunna supportera kunder vid frågor eller problem. Även för att manuellt initiera systemuppdateringar.

3.2.3 NTP

Systemet synkroniserar tiden till NTP-servrar online. Detta kan konfigureras på kunds begäran.

Systemets tid måste vara korrekt för att data ska presenteras korrekt i Ferroamp Portal.

3.2.4 DNS

Systemet använder den DNS som tilldelas via DHCP som standard men har också googles DNS server som backup. Detta kan konfigureras på begäran av kund.

3.2.5 Mjukvaruuppdateringar

Uppdateringspaket hämtas via HTTP samt HTTPS. Om brandvägg eller annan nätverksutrustning manipulerar SSL certifikaten finns risk för att automatiska uppdateringar misslyckas.

Uppdateringspaketen hämtas från Amazons S3 bucket i region eu-central-1. Ip-adresser för dessa kan hittas på Amazons hemsida, <https://ip-ranges.amazonaws.com/ip-ranges.json>.