UniLock
System 10

Manual til
Låsecomputer
LS10-IP

Projekt	PRJ189
Version	1.0
Revision	240716

LS10-IP er en sammensmeltning af en LS10 låsecomputer og en CV72 højsikker Ethernet konverter, polling sker via Ethernet.

UniLock programmet kommunikerer direkte med enten en CV72 eller en LS10-IP i lokaliteten via en TCP/IP forbindelse, der er sikret efter højeste krypteringsstandarder mod aflytning, manipulation, replay og hijacking.

LS10-IP kan forsynes via Power over Ethernet (PoE) og den dynamiske effektbegrænsning sikrer at det tilladte PoE forbrug ikke kan overskrides, eksempelvis under opladning af backup batteri.

LS10-IP har ikke brug for anden konfiguration end et ID nummer.

Indholdsfortegnelse

1. Produktbeskrivelse

Anvendelse

Låsecomputerens anvendes til, helt decentralt, at styre adgangskontrollen i et kontrolpunkt (dør), også kaldet et k-punkt.

Låsecomputeren er en selvstændigt fungerende enhed, som indeholder alle nødvendige informationer for at styre kontrolpunktet. Informationer modtages via kommunikationsforbindelsen fra UniLock pc-programmet.

Der kan tilsluttes både indlæser og udlæser, med overvågning af op til 8 læsere på samme tid. Det er muligt at parallelkoble flere læsere, så mange forskellige læseteknologier kan anvendes samtidigt i samme k-punkt.

Alle hændelser logges i låsecomputeren, hvorfra UniLock pc-programmet henter logningerne og gemmer dem til senere brug.

Beskrivelse

Låsecomputeren er robust opbygget, har stor immunitet over for elektrisk støj, og er derved meget velegnet til brug i industrielle miljøer. Printet er testet og CE-mærket efter de strengeste krav i EMC-direktivet.

Via låsecomputerens kommunikationsport kan op til 65.000 enheder udveksle data med hinanden og en pc. Låsecomputere fås med kommunikationsforbindelse til RS485 eller både RS485 og Ethernet.

Som standard kan låsecomputeren indeholde op til 2.500 nøgler (personer) og dette kan udvides til 65.000 nøgler.

Låsecomputeren indeholder egen strømforsyning, som kan forsyne både lås, læsere og andet eksternt udstyr samt oplade det tilsluttede backupbatteri. Ved totalt strømsvigt beskytter et indbygget batteri data i op til 10 år.

Låsecomputeren kan leveres i metalkasse eller på aluminiumsplade til tavlemontage og til DIN-skinnemontage i fx enUG12 el-tavle. Alle forbindelser er forsynet med aftagelige kvalitets-klemmer.

Enheden anvender Ethernet kommunikation og forsynes via PoE. RS485 kommunikation og 12 VDC forsyning er også mulig.

Alle låsecomputerens forbindelser er galvanisk adskilt fra Ethernet forbindelsen, så der ikke opstår problemer med fejlstrømme.

Strømforsyningen indeholder en automatisk justerende strømbegrænser, som modvirker at der trækkes mere strøm end PoE switchen tillader. Alternativt vil man kunne risikere at switchen lukker for PoE forsyningen. Er der tilsluttet et backupbatteri til LS10-IP, vil det blive brugt som ekstra energikilde hvis eksternt udstyr kræver mere forsyning end PoE switchen kan levere..

Låsecomputeren identificeres alene på baggrund af dens ID-nummer og kræver således ingen IP-opsætning.

Udover at fungere som et k-punkt, kan LS10-IP også fungere som gateway for pc-programmet til andre LS10-IP og LS10-230V (CV72 funktionalitet).

LS10-IP har egen hjemmeside, som indeholder værktøjer til hjælp ved installation og driftsover-vågning.

Krav til pc-software

IP-delen af LS10-IP indeholder nyeste højteknologiske krypteringsalgoritmer og modtager automatisk softwareopdateringer fra UniLock pc-program, blandt andet derfor anbefales det at holde pc-programmet opdateret.

Krav:

UniLock version 2.0 minimum revision 2017-03-07, dog anbefales altid nyeste.

CV-Config revision 2016-09-02 eller nyere.

2. Installations-vejledning

Dette afsnit indeholder information om konfiguration af LS10-IP.

2.1 ID-nummer

Før PC'en kan overføre og læse data i LS10, skal LS10 tildeles et entydigt ID-nummer. Som ID-nummer kan der frit vælges et 4 cifferet hex-tal mellem $0101 og $FFFF. Tal der begynder eller ender på "00" ($00nn, $nn00) må ikke benyttes.

ID-nummeret kan indtastes med loaderen (tast <A1>) eller fra tastaturet på en læser. Tænd for strømmen til LS10 og tast <*nnnn#> (tast ”*1001#” ved ID-nummer: ”1001”) på læser-tastaturet inden 20 sekunder. På LS10-IP kan ID-nummer også indtastes i 20 sekunder efter tryk på printets SW1 knap. Alle "gamle" data i låsecomputeren slettes automatisk når læseren anvendes til at give ID-nummer.

2.2 Gateway

For hver IP-lokalitet skal der være gateway mellem Polleren på installations-pc og de enkelte K-punkter. Gateway kan være CV72 eller LS10-IP med monteret jumper W1.

Er LS10-IP gateway kan IP konfigureres med CV-Config programmet (se afsnit 2.2 – 2.5).

Er LS10-IP ikke gateway er der ikke behov for yderligere IP-konfiguration.

2.3 Valg af IP opsætning

Inden LS10-IP kan fungere som gateway i pc-netværket, skal den være konfigureret korrekt.

Konfiguration af IP-delen og eventuelle ændringer i DHCP- og/eller DNS-serveren, bør altid foregå i samarbejde med den netværksansvarlige. Forkert opsætning kan i værste fald få alvorlige konsekvenser for pc-netværket i form af tabte data og driftsstop.

Inden der ændres i opsætningen for IP, skal nedenstående skema udfyldes. En detaljeret beskrivelse af de enkelte felter findes i de efterfølgende afsnit.

Identifikation		
Hostnavn		
Domæne		(Valgfri)
Registreringsadresse		(Valgfri)
Netværk		
	☐ Fast IP-adresse ☐ Dynamisk IP-adresse	
IP-adresse		(Kun ved fast IP-adresse)
Netmaske		(Kun ved fast IP-adresse)
Gateway adresse		(Kun ved fast IP-adresse)
DNS-server	Primær:	(Kun ved fast DNS adresse)
	Sekundær:	(Kun ved fast DNS adresse)
Port nummer		(default 7211)

Indtil det er fastlagt, hvordan skemaet skal udfyldes, er der ingen grund til at gå videre.

Identifikation

Enheden kan identificeres på netværket ved hjælp af et hostnavn enten gennem NetBIOS eller DNS.
Et NetBIOS-navn (hostnavn) kan kun anvendes indenfor samme subnet, det kræver ingen DNS-server, der skal blot vælges et hostnavn til enheden.
Et DNS-navn (hostnavn.domæne) kan anvendes i hele domænet på tværs af subnet, men det kræver en DNS-server, som skal være kendt og åben for registrering. Foruden hostnavnet bør domæne og eventuelt registreringsadresse angives. Afhængig af den aktuelle installation kan det dog udelades, hvis den primære eller sekundære DNS-server skal anvendes til registrering.

Hostnavn

Hostnavn kan bruges i stedet for en fast IP-adresse til at identificere enheden på netværket ved hjælp af NetBIOS eller DNS. Default Hostnavn er: ”CV72LS10-xxxxxx”, hvor xxxxxx er de sidste 6 cifre i enhedens MAC-adresse.

Et NetBIOS-navn kan maksimalt være på 15 karakterer. Indtastes et hostnavn på mere end 15 karakterer, anvendes enhedens default hostnavn som NetBIOS-navn og det indtastede hostnavn som DNS-navn. (max 63 karakterer).

Domæne

Domænet bruges når enheden skal registrere sit hostnavn i en DNS-server, og angiver hvilket domæne, enheden skal være en del af.

Angives intet domæne, vil enheden automatisk forsøge, at anvende det samme domæne som den primære eller sekundære DNS-server tilhører (omvendt DNS opslag).

Registreringsadresse

Som noget helt specielt har enheden mulighed for, at registrere sig i en anden DNS-server end den primære eller sekundære DNS-server. Dette kan anvendes i de situationer, hvor enheden skal installeres i en lokalitet med en anden DNS-opsætning end i ”hovedafdelingen”, og hvor enhedens hostnavn skal anvendes af fx Polleren.

Angives intet, bruges den primære eller sekundære DNS-server.

Netværk

Enheden kan anvende en fast netværkskonfiguration, eller automatisk hente den fra en DHCP-server.

Skal netværkskonfiguration automatisk hentes fra en DHCP-server, skal parametrene IP-adresse, Netmaske og Gateway-adresse ikke udfyldes. Ligeledes kan DNS-serveradresserne udelades, hvis disse tildeles af DHCP-serveren.

DHCP-serveren kan tildele LS10-IP en tilfældig IP-adresse indenfor sit adresseområde, eller en fast IP-adresse, hvis den ønskede IP-adresse er låst til enhedens MAC-adresse (statisk DHCP).

Hvis der i routeren anvendes port mapping (port forwarding) for at gøre enheden tilgængelig fra internet, kan det være nødvendigt at tildele enheden en fast IP-adresse, hvis den anvendte router ikke understøtter hostnavne.

IP-adresse
Hvis der vælges en fast IP-adresse skal (bør) denne ligge udenfor det område som DHCP-serveren tildeler IP-adresser ud fra.

Netmaske
Skal normalt være den samme som for andre ”apparater” på samme subnet. I et almindeligt klasse C netværk er netmasken 255.255.255.0.

Gateway-adresse
Den adresse der skal sendes til, hvis der sendes til en IP-adresse der ligger uden for subnettets adresseområde. Skal enheden anvendes på samme subnet som UniLock pc-programmet, er det ikke nødvendigt at konfigurere gateway adressen.

DNS-serveradresse
IP-adresse for den primære og den sekundære DNS-server, hvis ikke de tildeles af DHCP-serveren.

Port nummer
Den port som benyttes til at kommunikere på. Som default anbefales det at anvende port nummer 7211, men det kan i princippet være alle tal mellem 1024 og 65535. Det valgte port nummer, skal normalt være det samme som er valgt i det program der kommunikeres med (UniLock).

2.4 Konfiguration af LS10-IP

Opsætning af LS10-IP netværksdel udføres med Windows programmet CV-Config. CV-Config kan downloades fra Uniteks hjemmeside. Programmet kan afvikles direkte uden at installere noget software på pc’en.

Når enheden er konfigureret skal programmet ikke bruges mere. Det er derfor sjældent nødvendigt at installere det. Ønskes det alligevel at installere programmet, gøres det ved manuelt at kopiere programfilen til det ønskede drev/mappe.

2.4.1 Tilslutning

Den LS10-IP der skal konfigureres, skal tilsluttes det samme subnet som den pc hvorpå CV-Config afvikles.

CV-Config kommunikerer med enheder via broadcast, hvorved der kommunikeres uden brug af IP-adresser. Dette gør det muligt, at konfigurere LS10-IP på et andet netværk end der hvor den efterfølgende skal anvendes.

2.4.2 Søgning med CV-Config

Når CV-Config programmet startes, søges der automatisk efter enheder på netværket. Alle fundne enheder vises i en sorteret liste. Som udgangspunkt er listen sorteret efter enhedernes oppetid, så den enhed der sidst blev tændt, står øverst på listen. Listen over fundne enheder kan opdateres ved at trykke på knappen [Søg].

Har pc'en flere netværkskort vælges det korrekte netværkskort i listen.

Bemærk at firewall på pc'en kan begrænse CV-Config programmets adgang til netværket og ændringer i pc'ens netværkskonfiguration automatisk vil genstarte pc'ens netværksstack, hvilket kræver genstart af CV-Config programmet.

2.4.3 Rediger indstillinger

For at ændre parametrene for en enhed, vælges den på listen, hvorefter der trykkes på knappen [Rediger indstillinger], eller der kan dobbeltklikkes på den i listen. Derved fremkommer en dialog hvor de ønskede parametre kan angives. Når der vælges [OK] sendes de nye parametre til enheden.

Når parametre er ændret i enheden, opdateres listen automatisk med de nye parametre. Parametre i listen er alle modtaget fra enhederne, så man kan være sikker på, at de viste parametre, også rent faktisk er de parametre, der er i de respektive enheder.

2.4.4 Adgangskode

LS10-IP kan beskyttes med en adgangskode på op til 32 karakterer. Adgangskoden gør det umuligt at ændre parametrene medmindre adgangskoden er kendt.

Et kort tryk på knappen i enheden nulstiller adgangskoden (adgangsnøgle).

For optimalt sikkerhed bør enheden tildeles en adgangskode på et lukket netværk, før den eventuelt flyttes til et offentligt netværk.

2.5 Konfiguration af pc-netværk

Afhængigt af netværkets opbygning og konfiguration kan der være behov for at ændre opsætningen af router og/eller DNS-server.

2.5.1 Opsætning af router

Kommunikationen mellem UniLock pc-programmet og gateway LS10-IP foregår på den brugervalgte IP-port, default 7211. Det er pc-programmet, der skaber forbindelse til LS10-IP. Det er derfor nødvendigt, at der kan kommunikeres med LS10-IP på den valgte port. Det vil sige, hvis LS10-IP og pc-programmet er adskilt af routere, firewalls og lignende, skal der i disse åbnes for den valgte IP-port, så pc-programmet kan få forbindelse til LS10-IP.

Port mapping

LS10-IP tildeles normalt ikke en "offentlig" IP-adresse. Er LS10-IP og pc-programmet adskilt af fx en router, kan den lokale IP-adresse ikke bruges direkte, da lokale IP-adresser ikke kan routes over internet.

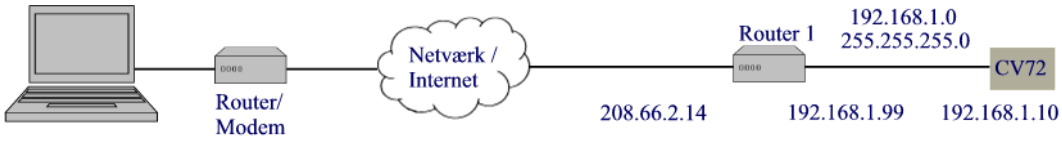
For at løse dette problem, kan der bruges en funktion i routeren som kaldes port mapping eller port forwarding. Port mapping er en funktion under NAT (Network Address Translation).

NAT giver mulighed for, at flere lokale IP-adresser kan deles om én offentlig IP-adresse, men her skal alle forbindelser startes af den lokale enhed.

Port mapping betyder, at udefra kommende trafik der sendes til routeren på en specifik port, altid videresendes til én specifik lokal IP-adresse, der vælges i routeren.

Routeren har altså en offentlig IP-adresse (WAN adresse), som bruges til at komme i kontakt med routeren. I routeren sættes port mapping op sådan, at når der kommer kommunikation til en bestemt IP-port på WAN-siden, oversættes den til en ny adresse på LAN-siden. Det er WAN adressen, der skal indtastes i Adgangseditoren.

Eksempel:



1. Gateway LS10-IP (med CV72) skal placeres i et ”internt” netværk med netværksadresse 192.168.1.0 og netmaske 255.255.255.0.
2. Pc’en sidder i et andet netværk med en vilkårlig netværksadresse.
3. Router 1 har en offentlig WAN IP-adresse 208.66.2.14.
4. IP-adressen for lokaliteten i UniLock pc-programmet sættes så til 208.66.2.14 og port 7211
5. Port mapping i router 1 sættes sådan, at kommunikation der kommer til adresse 208.66.2.14 på port 7211 routes til den interne IP-adresse 192.168.1.10 på port 7211.

LS10-IP opsættes til:

- IP-adresse: 192.168.1.10
- Netmaske: 255.255.255.0
- Gateway adresse: 192.168.1.99
- Port: 7211

Gateway adressen skal være den gateway adresse som router 1 er konfigureret til. I eksemplet er det 192.168.1.99, men det kan være andre adresser, blot skal adressen være indenfor netværkets adresseområde.

I pc-programmet opsættes LS10-IP data til:

- IP-adresse: 208.66.2.14
- Port: 7211

Bemærk at den IP-adresse der opsættes i pc-programmet, ikke er den samme som den IP-adresse der opsættes for LS10-IP.

2.6 Registrering af hostnavn i DNS-server

LS10-IP kan registrere sit Hostnavn i en DNS-server (hostnavn.domæne). Dette giver mulighed for at tilgå CV72 med hostnavnet uden nødvendigvis at være på samme subnet som LS10-IP.

Registrering af hostnavnet i DNS-serveren kan enten foretages automatisk af enheden eller manuelt af den IT-ansvarlig.

Vær opmærksom på, at det kan tage lang tid, før hele netværket er opdateret med tilføjelser og ændringer af navne. Korrekt rækkefølge er yderst vigtig for at minimere tiden, inden de korrekte navne er anvendelige.

Tiden, inden netværket er fuldt opdateret med ændringer skyldes, at svar fra en DNS-server gemmes (caches) af DNS-klienter (pc, mellemliggende DNS-servere og routere) i en given tid, hvorefter de automatisk slettes igen. Svarer en DNS-server, at det forespurgte DNS-navn ikke findes, gemmer DNS-klienter dette svar i en given tid, fra få sekunder til flere døgn afhængig af DNS-serverens konfiguration.

Dette betyder, at man skal være særligt opmærksom på, at navnet er registreret inden det anvendes af en pc, da der ellers kan gå yderligere tid, inden pc'en kan finde enheden.

Almindeligvis sænker man levetiden for svar (time to live) i DNS-serveren i god tid inden, der foretages ændringer. Ved at sænke levetiden, skal man vente kortere tid på, at ugyldige informationer udløber.

2.6.1 Automatisk registrering

LS10-IP kan automatisk registrere sit navn i en DNS-server (A-record). Til denne registrering er det nødvendigt at kende navnet på domænet. Hvis domænet ikke er angivet, eller ikke kan hentes gennem DHCP, er automatisk registrering ikke mulig.

Hentes IP-adressen automatisk via DHCP forsøger LS10-IP at foretages registreringen gennem DHCP-serveren (option 81). Er det ikke muligt at registrere gennem DHCP-serveren så forsøges det i stedet at foretage registreringen direkte i DNS-serveren.

Hvis der er angivet et domæne ved konfiguration af LS10-IP anvendes dette, alternativt bruges det domæne som DHCP-serveren angiver.

Anvendes en fast IP-adresse er det kun muligt, at registrere navnet direkte i DNS-serveren med det angivne domæne.

Registreringer direkte i DNS-serveren forudsætter at DNS-serveren tillader [Ikke sikrede dynamiske opdateringer] for den pågældende [Forward Lookup Zone].

Registrering foretages eller fornyes på baggrund af følgende kriterier:

- Ved opstart af enheden
- Ved ændring af enhedens opsætning.
- Ved fornyelse af dynamisk IP-adresse eller en gang i døgnet for en statisk IP-adresse.

2.6.2 Manuel registrering

Manuel registrering anvendes typisk hvis automatisk registrering ikke er muligt fx hvis DNS-serveren ikke tillader dynamiske opdateringer.

Ved manual registrering kan enheden ikke selv holde registreringen opdateret, og den IT-ansvarlige er derfor ansvarlig for dette. DNS-registreringen holdes nemmest korrekt opdateret ved, at tildele enheden en fast IP-adresse eller via statisk DHCP.

Vær opmærksom på, at enhedens statushjemmeside kun angiver status for registreringer, som enheden selv har anmodet om eller udført. Det vil sige, at statushjemmesiden i dette tilfælde vil

angive fejl under registrering af hostnavn, da enheden ikke selv har kendskab til den manuelle registrering.

2.6.3 Test af DNS-registrering

For at teste registreringen i DNS-serveren kan bruges følgende fremgangsmåde:

1. Åbn statushjemmesiden med IP-adressen (http://ip-adresse) og verificer at det registrerede DNS-navn er korrekt.
2. Åbn hjemmesiden med DNS-navnet (http://hostnavn.domæne). Giver dette den samme statushjemmeside som i pkt. 1, er navnet registreret korrekt og klar til brug.
3. Indtast nu hostnavnet i UniLock programmet.

2.7 Kommunikation med andre enheder

Til kommunikation med andre IP-enheder (LS10-IP og CV72v2) anvendes multicast på IP-adresse 239.255.72.11, UDP-port 7211 med default TTL=2, hvorved enheder kan kommunikere på tværs af lokale netværk adskilt af max en router (forudsat korrekt router-konfiguration).

Anvender netværket IGMP snooping til at minimere netværkstrafik, skal der være konfigureret en IGMP querier til periodisk at sende forespørgsler om at opretholde multicast IP-adresse registreringer til IP-enheder. Dette er et krav i IGMP for at sikre at netværkstrafik altid routes korrekt. Det henvises til undervisningsmateriale for IGMP snooping.

En søgefunktionalitet findes på enhedernes hjemmesides fane [Find enheder], hvor søgningen kan synliggøre hvilke andre enheder, den enkelte enhed kan kommunikere med.

I større IT-installationer kan der være behov for at overstyre TTL-værdien hvis:

1. Enheder kan ikke finde hinanden pga. for mange routere mellem dem. TTL hæves.
2. Enheder kan finde hinanden få tværs af for mange routere. TTL sænkes.

Overstyring af multicast TTL gøres med en producentspecifik DHCP-option:

DHCP Vendor Class:	”UniLock” (Hexadecimal: 55 6E 69 4C 6F 63 6B)
Option Code:	1
Option Datatype:	1 byte
Option Value:	TTL-værdien (1-255)

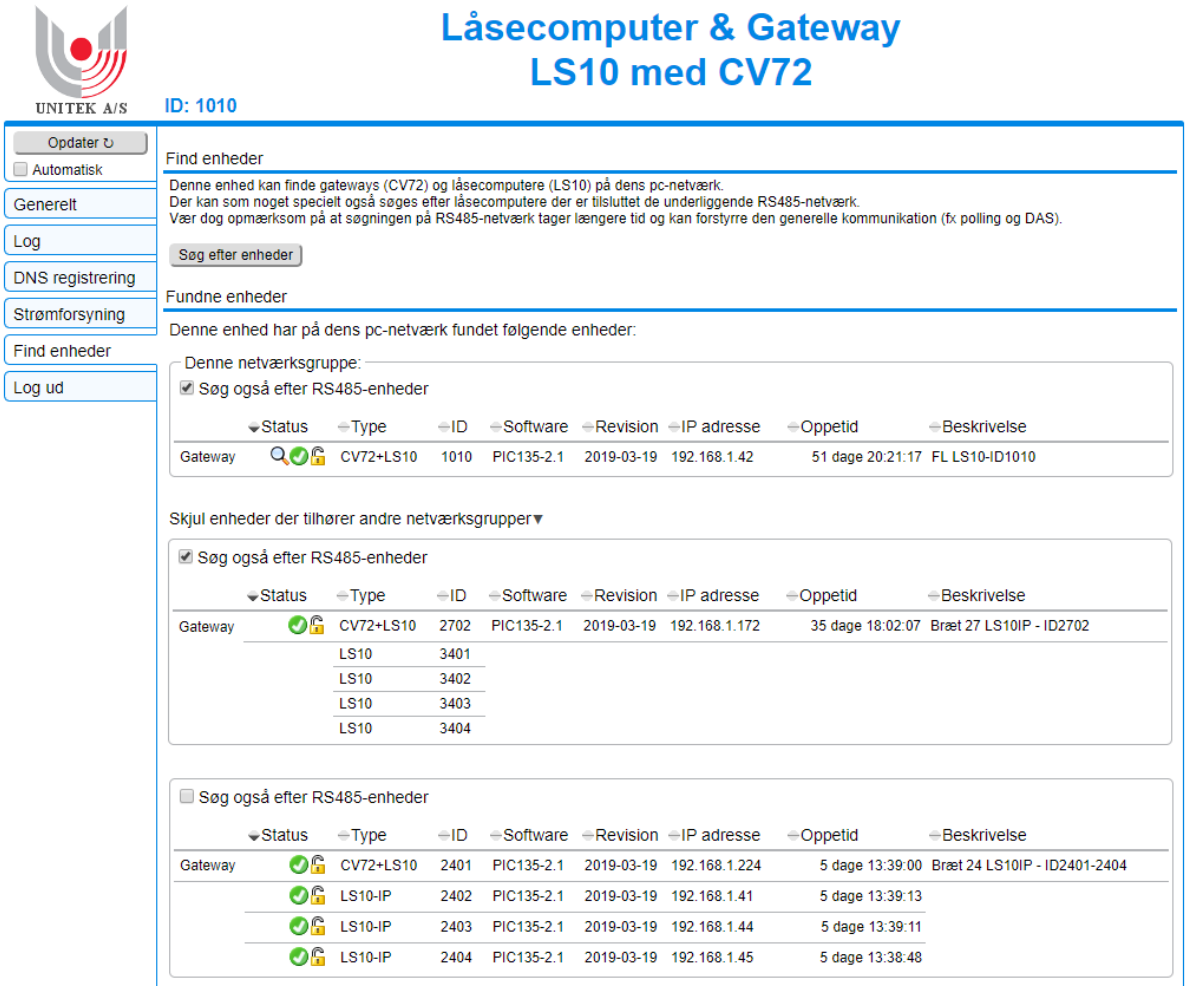
2.8 Hjemmeside

LS10-IP har en indbygget hjemmeside, hvorfra man kan se status og søge efter andre enheder på Ethernet (CV72, LS10-IP) og RS485 (LS10-230V). Med hjemmesiden kan man således verificere at denne LS10-IP kan se andre enheder, samt finde andre enheders IP-adresse og ID-numre.

Adgang på standard web port 80 testes med web-browser ved at skrive IP-adressen for enheden (http://[adresse]).

Adgang på den valgte kommunikationsport testes med web-browser ved at skrive adressen og port-nummeret for enheden (http://[adresse]:[port]).

Er enheden placeret bag en router med port-mapping, kan der oprettes en http-forbindelse ved at skrive "http://[adresse]:[port]", hvor [adresse] angiver routerens adresse, og [port] angiver den port på routeren der er mappet til kommunikationsporten på enheden (default 7211).


UNITEK A/S
Låsecomputer & Gateway
LS10 med CV72
ID: 1010
Opdater
Automatisk
Generelt
Log
DNS registrering
Strømforsyning
Find enheder
Log ud
Find enheder
Denne enhed kan finde gateways (CV72) og låsecomputere (LS10) på dens pc-netværk.
Der kan som noget specielt også søges efter låsecomputere der er tilsluttet de underliggende RS485-netværk.
Vær dog opmærksom på at søgningen på RS485-netværk tager længere tid og kan forstyrre den generelle kommunikation (fx polling og DAS).
Søg efter enheder
Fundne enheder
Denne enhed har på dens pc-netværk fundet følgende enheder:
Denne netværksgruppe:
Søg også efter RS485-enheder
Status Type ID Software Revision IP adresse Oppetid Beskrivelse
Gateway CV72+LS10 1010 PIC135-2.1 2019-03-19 192.168.1.42 51 dage 20:21:17 FL LS10-ID1010
Skjul enheder der tilhører andre netværksgrupper▼
Søg også efter RS485-enheder
Status Type ID Software Revision IP adresse Oppetid Beskrivelse
Gateway CV72+LS10 2702 PIC135-2.1 2019-03-19 192.168.1.172 35 dage 18:02:07 Bræt 27 LS10IP - ID2702
LS10 3401
LS10 3402
LS10 3403
LS10 3404
Søg også efter RS485-enheder
Status Type ID Software Revision IP adresse Oppetid Beskrivelse
Gateway CV72+LS10 2401 PIC135-2.1 2019-03-19 192.168.1.224 5 dage 13:39:00 Bræt 24 LS10IP - ID2401-2404
LS10-IP 2402 PIC135-2.1 2019-03-19 192.168.1.41 5 dage 13:39:13
LS10-IP 2403 PIC135-2.1 2019-03-19 192.168.1.44 5 dage 13:39:11
LS10-IP 2404 PIC135-2.1 2019-03-19 192.168.1.45 5 dage 13:38:48

2.9 Tilslutning

Diagram over tilslutning kan ses på Figur 1 og Figur 2.

LS10-IP kan forsynes af Power over Ethernet (PoE) eller af ekstern forsyning (VDC).

Data

Funktioner:	DHCP (inkl. option 81), Statisk IP, Hostnavn, NetBIOS, DNS, TCP, UDP, ARP, HTTP, IGMP (v1, v2, v3), LLDP (PoE power negotiation), ICMP (Ping), IP-firmware opdatering.
Sikkerhed:	Rabbit 128bit-kryptering, HMAC, SipHash, Password.
IP:	IPv4 (IPv6 forberedt).
Netværk (J1):	10/100BaseT (RJ45), galvanisk adskilt
Seriel (J5):	2-ledet RS485, half duplex, ikke galvanisk adskilt, transientbeskyttet
Forsyning ind:	
PoE/PoE+ (J1):	36-57 VDC (eget forbrug: 3,5W)
VDC (J6):	10-14,5 VDC (eget forbrug: 2,5W)
Forsyning ud ved (J6):	
PoE	12VDC, max 6W
PoE+	12VDC, max 15W
Størrelse:	217 x 112 x 28 mm, 0,3 kg

2.9.1 LS10-IP forsyning til eksterne enheder

Når LS10-IP forsynes med Power over Ethernet, kan den levere fuld galvanisk adskilt 12 VDC til eksterne enheder.

For at forhindre at switchen slukker for PoE forsyningen, begrænser LS10-IP som udgangspunkt effektforbruget fra PoE til enten 12.9W for en PoE switch (type 1) eller 25.5W for en PoE+ switch (type 2). Derudover justerer LS10-IP automatisk effektgrænsen mellem 12.9W og 25.5W hvis switchen angiver hvor meget effekt der er til rådighed via LLDP protokollen (LLDP-MED Advanced Power Management).

Hvis switchen begrænses til at levere mindre end 15,4W (12,9W) vil switchen slukke for PoE forsyningen inden enhedens effektbegrænsning aktiveres.

Begrænsningen sker ved at reducere output spændingen fx under opladning af et backupbatteri.

Når effektgrænsen er nået vises dette både på printet med en lysdiode og på enhedens hjemmesides faneblad [Strømforsyning]. På fanebladet rapporteres den tilgængelige effekt og det aktuelle effektforbrug automatisk.

Test altid inden drift.

PoE type	PoE effekt (PSE)	PoE effekt (PD)	Effekt eksternt
PoE	15,4 W	12,9 W	6 W
PoE+	30,0 W	25,5 W	15 W

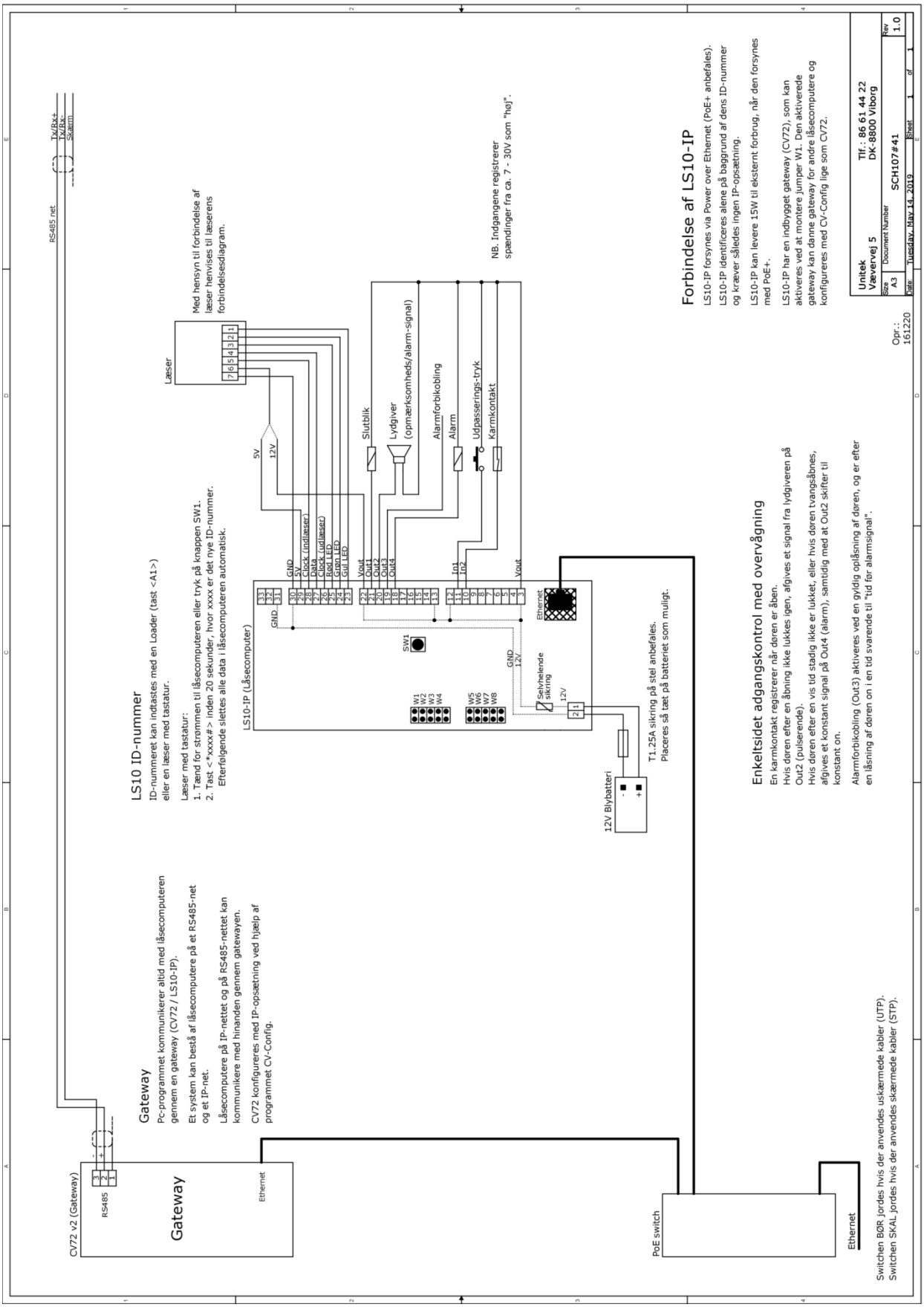
Det anbefales at anvende PoE+ for at sikre tilstrækkelig effekt til læsere og slutblik/el-lås.

2.9.2 Lysdioder

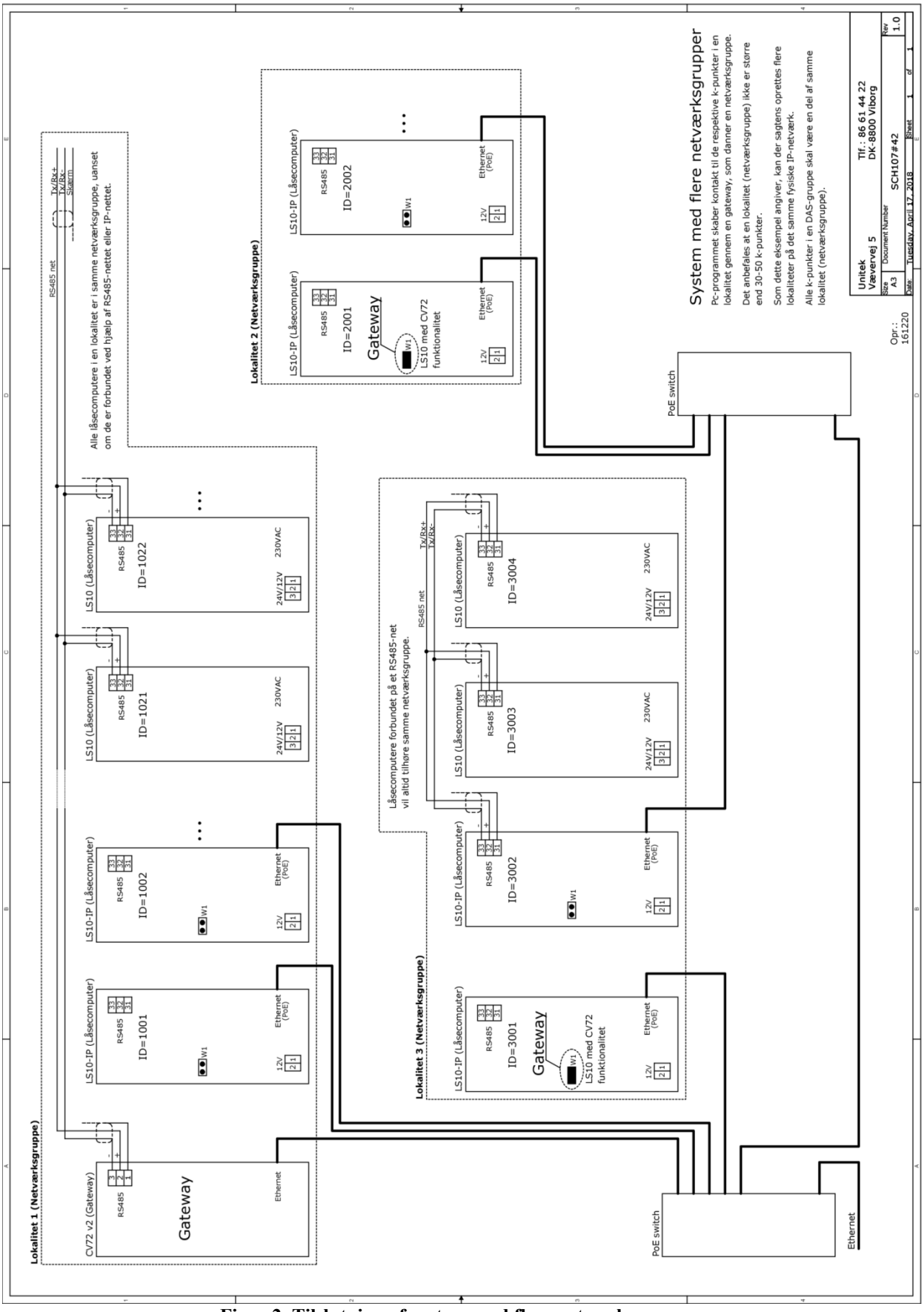
Lysdioderne viser driftsinformationer for enheden, som kan være en god hjælp ved installation og kontrol.

Lysdiode	Beskrivelse
[PoE Power] **D1**	Grøn konstant Power over Ethernet forsyning tilsluttet.
[PoE Max] **D2**	Gul konstant PoE ikke kan levere den nødvendige effekt. Output spændingen er reduceret for at begrænse effekten.
[Status] **D3**	Grøn = 0,025 sek. Off = 0,025 sek. Softwareopdatering i gang. Grøn = 0,1 sek. Off = 2,9 sek. IP fejl/ IP ikke klar. Grøn = 0,5 sek. Off = 0,5 sek. Klar Grøn konstant Der er etableret en TCP/IP forbindelse til Polleren
[Ethernet Link/Act] **D4**	Off konstant Der er ikke en Link forbindelse. Grøn konstant Der er en Link forbindelse til Ethernet. Grøn = 0,025 sek. Off = 0,025 sek. Der er aktivitet på Ethernet, uanset om data er til denne enhed.
[Ethernet Rx] **D5**	Lyser når der modtages data fra Ethernet adresseret til denne enhed eller dens netværksgruppe.
[Ethernet Tx] **D6**	Lyser når der sendes data ud på Ethernet på den valgte IP-port.
[Run] **D7 + D8**	Run lyser normalt rødt i ca 1 sek under opstart, hvorefter der skiftes til grønt. Rød konstant Låsecomputeren kører ikke. Grøn konstant Låsecomputeren kører.
[LS10 Rx/Tx] **D9**	Gul = 0,02 sek Gyldig streng modtaget Gul = 0,80 sek Sender besked
D10	Off konstant CPU kører ikke. Grøn = 0,1 sek. Off = 0,1 sek. i 3 sek. Enhed er netop nulstillet efter 5 sek. tryk på knap. Grøn = 0,1 sek. Off = 0,4 sek. CPU kører korrekt med default opsætning. Grøn = 0,1 sek. Off = 1,9 sek. CPU kører korrekt.
D11	Test lysdiode. (Lyser aktuelt, hvis enheden er tidsserver.)

2.9.3 Forbindelsesdiagramer



Figur 1. Tilslutning af LS10-IP



Figur 2. Tilslutning af system med flere netværksgrupper

3. Test og fejlfinding

Ved idriftsættelse eller kommunikationsproblemer bør forbindelsen til og opsætning af LS10-IP verificeres.

I nogle af de efterfølgende afsnit skal enhedens adresse anvendes for at kontakte enheden. Feltet [adresse] kan være en af adressetyperne:

- IP-adresse i formatet "n.n.n.n"
- NetBIOS-navn i formatet "hostnavn"
- DNS-navn i formatet "hostnavn.domæne"

3.1 Test af forbindelse til enheden

Forbindelsen til LS10-IP kan testes med ping eller ved at åbne enhedens hjemmeside.

3.1.1 Hjemmeside

Adgang på standard web port 80 testes med web-browser ved at skrive IP-adressen for enheden (http://[adresse]).

Adgang på den valgte kommunikationsport testes med web-browser ved at skrive adressen og port-nummeret for enheden (http://[adresse]:[port]).

Er enheden placeret bag en router med port-mapping, kan der oprettes en http-forbindelse ved at skrive "http://[adresse]:[port]", hvor [adresse] angiver routerens adresse, og [port] angiver den port på routeren der er mappet til kommunikationsporten på enheden (default 7211).

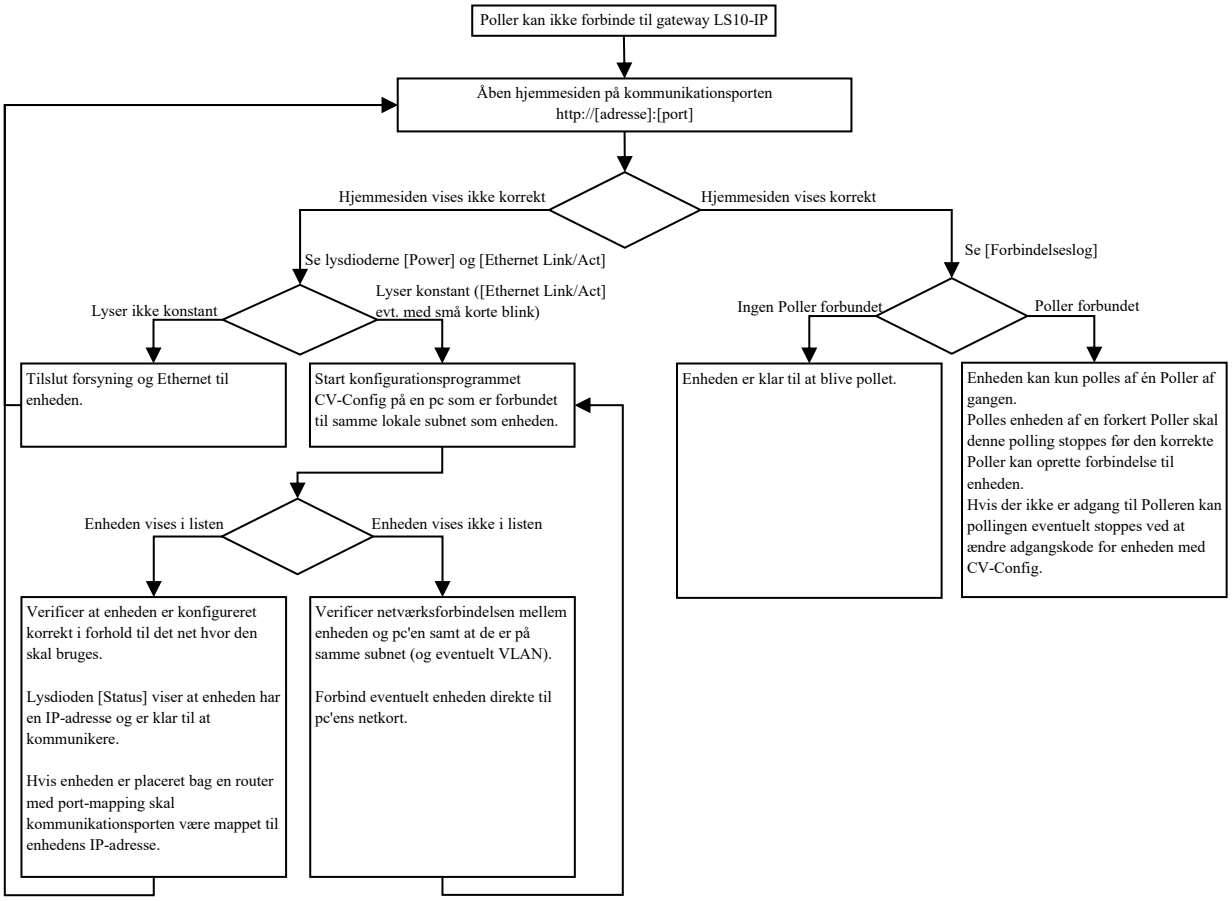
3.1.2 Ping

Start en kommandoprompt (”DOS vindue”) og skriv ”ping [adresse]” hvor [adresse] er adressen på enheden. Pinges et hostnavn vil Ping-kommandoen først oversætte dette til en IP-adresse, hvorefter den fundne IP-adresse anvendes.

Ping kan ikke anvendes til at teste forbindelsen til en enhed, hvis enheden er placeret bag en router med port mapping, da routeren selv vil svare på ping-forespørgsler.

3.2 Fejlfinding

Skulle der opstå problemer med kommunikation til LS10-IP, er det vigtigt at gå systematisk frem for lettest at lokalisere fejlen.



Med hensyn til opsætning af routere, switche, firewalls mv., er opsætningen af disse helt forskellig fra fabrikat til fabrikat, så der henvises til den enkelte fabrikats brugervejledning.

3.3 Specielt om udskiftning af LS10-IP

Hvis en LS10-IP skal udskiftes med en anden LS10-IP, er der en række netværksmæssige udfordringer man skal være opmærksom på, for hurtigst muligt at få den nye LS10-IP i drift.

De følgende afsnit beskriver hvad man skal være særligt opmærksom på afhængigt, af hvordan LS10-IP adresseres i fx UniLock.

Adresseret med IP-adresse

Bruger den nye LS10-IP samme IP-adresse som den tidligere LS10-IP, skal alle involverede pc'er, routere, mv. have deres ARP-tabeller opdateret.

ARP-tabellen bruges til at bestemme en MAC-adresse ud fra en IP-adresse.

Det er essentielt for korrekt kommunikation, at ARP-tabellen er opdateret, da al kommunikation på et Ethernet foregår ved hjælp af MAC-adresser og ikke ved hjælp af IP-adresser.

Routere, pc'er mv. vil normalt automatisk holde deres ARP-tabeller opdateret. Afhængig af deres opsætning kan der gå fra få sekunder til flere timer, før de opdaterer deres ARP-tabeller.

Hvis man ikke ved hvordan ARP-tabellen skal fornys i routere mv., må man vente til de automatisk opdaterer. På en pc kan ARP-tabellen tvangsopdateres ved at slettes tabellen med kommandoen ”arp -d” skrevet i kommandoprompten.

Alternativt kan den nye LS10-IP tildeles et andet IP-nummer, hvis IP-nummerplanen tillader dette.

Adresseret med hostnavn

Hvis den nye LS10-IP bruger samme Hostnavn (NetBIOS-navn eller DNS-navn) som den tidligere LS10-IP, og de ikke anvender samme IP-adresse, skal man være opmærksom på, at pc'en gemmer disse informationer i en cache i en given tid. Det betyder, at et gemt navn vil referere til den gamle IP-adresse og ikke den nye.

Hvis man ikke har adgang til at opdatere cachen lokalt, og i eventuelle mellemliggende DNS-servere, sker det automatisk efter en given tid. Det vil typisk ske indenfor 20 min, men det afhænger af pc'ens konfiguration.

Den lokale cache kan manuelt tømmes for hostnavne ved at skrive en kommando i kommando-prompten. Kommandoen for at fjerne NetBIOS-navne er "nbtstat -R" og kommandoen for at fjerne DNS-navne er "ipconfig /flushdns".

Vær dog opmærksom på, at mellemliggende DNS-servere ligeledes vil gemme navnet i deres cache, hvorved vi vil få det samme gamle IP-adresse.

Alternativt kan den nye LS10-IP gives samme Hostnavn og IP-adresse som den tidligere LS10-IP, eller bare gives et andet hostnavn, hvorved disse problemstillinger elimineres.

Da et hostnavn relaterer til en IP-adresse kan det være nødvendigt at opdatere ARP-tabellen som beskrevet i forrige afsnit.

3.4 Nulstilling af opsætning

Tilhørsforhold til netværksgruppe, krypteringsnøgle og adgangsnøgle nulstilles hvis jumperen W1 sættes eller fjernes.

Adgangskoden (adgangsnøglen) nulstilles ved et kort tryk på knappen [SW1] på LS10-IP print.

Opsætningen kan nulstilles til fabriksindstilling, hvis knappen holdes nede i 5 sekunder indenfor de første 30 sekunder efter power-opstart.

Lysdioden D10 vil blinke (Grøn = 0,1 sek. Off = 0,1 sek.) i 3 sek. efter nulstilling af opsætning.

4. Sikkerhed

Dette afsnit beskriver overordnet hvordan kommunikation til og fra enheden beskyttes.

4.1 Netværkssikkerhed

For at sikre dataintegriteten, forhindre manipulation af data, replay af strenge og hijacking af enheder, er de vitale dele af kommunikationen sikret ved hjælp af kryptering og adgangskode.

Udover adgangskode og krypteringsnøgle anvendes yderligere en offentligt nøgle til overførsel af krypteringsnøglen i forbindelse med opstart af en enhed, dog kun hvis adgangskoden ikke allerede er sat i enheden.

For at forstærke krypteringen anvendes en ændringsnøgle i krypteringen. Populært sagt kan man sige, at ændringsnøglen sammen med krypteringsnøglen gør, at den samme krypteringsnøgle aldrig anvendes igen.

For at forhindre replay af en datastreng indsættes en tidskode (challenge), som krypteres i selve datastrengen.

For at verificere at en streng er dekrypteret korrekt, og at der ikke er manipuleret med data, beregnes et kryptografisk hashtal af alle data. Dette hashtal kan betragtes som en digital underskrift, der verificerer autenticiteten af en given datastreng.

4.1.1 Algoritmer

Til kryptering anvendes krypteringsalgoritmen Rabbit. Rabbit er en stream krypterings-algoritme med en 128 bit nøgle og en 64 bit ændringsnøgle (initialiseringsvektor). Ændringsnøg-len sikrer, at den samme streng krypteres forskelligt, hver gang den sendes.

Til integritetstjek anvendes en HMAC (Hash-based Message Authentication Code). Denne HMAC genereres vha. algoritmen SipHash, som er en kryptografisk 128 bit nøgleafhængig hash-algoritme (HMAC) der genererer et 64 bit hashtal. Dette hashtal er at betragte som en digital underskrift.

Begge overnævnte algoritmer anses for at være ubrydelige, og har ingen kendte svagheder. Et brute-force angreb mod en 128 bit symmetrisk krypteringsalgoritme vil ikke være praktisk muligt med nutidens computerteknologi, så det vil tage et par fantasiliarder år at prøve dem alle.

4.1.2 Adgangskode/adgangsnøgle

Ud fra brugerens adgangskode beregnes en adgangsnøgle i form af et hashtal, som efterfølgende anvendes og lagres i enhederne. Altså: Adgangskoden opbevares ikke i enheden eller sendes til enheden.

Adgangsnøglen bruges kun for at forhindre, at uautoriserede personer kan ændre i opsætningen af enheden, fx via pc-programmet CV-Config. Ligeledes beskytter adgangsnøglen mod, at en anden Poller kan overtage enheden (hijacking).

Altså: Adgangsnøglen låser enhederne til dette netværk, så enhederne ikke kan flyttes til et andet netværk uden at adgangsnøglen nulstilles eller videregives. Selv om der ikke er en adgangsnøg-le, så kan Polleren udmærket oprette en sikker krypteret kommunikationsforbindelse til enheden.

Et kort tryk på en knap i enheden nulstiller adgangsnøglen.

4.1.3 Krypteringsnøgle

Krypteringen sikrer, at data ikke kan aflyttes, og at data når sikkert og umanipuleret frem til enheden.
Krypteringsnøglen er den symmetriske nøgle, der anvendes af Polleren og enheder under normal drift.

4.1.4 Offentlig nøgle

Den offentlige nøgle anvendes kun i initialiseringsfasen til at kryptere overførslen af den første symmetriske krypteringsnøgle eller adgangsnøgle. Den offentlige nøgle anvendes ikke, og kan ikke anvendes, når der er sat en adgangsnøgle i enheden.

4.1.5 Ændringsnøgle

Formålet med ændringsnøglen (nonce) er at sikre, at de samme data aldrig giver samme krypterede resultat. Populært sagt kan man sige, at ændringsnøglen sammen med krypteringsnøglen gør, at den samme krypteringsnøgle aldrig anvendes igen.

4.1.6 Tidskode

For at forhindre replay af data indeholder hver streng en tidskode (challenge). Når den anvendte challenge er en tidskode, kan data overføres direkte uden forudgående kommunikation til overførsel af en challenge.
At anvende en tidskode som challenge giver endvidere mulighed for at anvende broadcast.
Hvis tiden i enheden ikke er kendt, eller den er ude af synkronisering, kan man bede enheden om at oplyse dens tid (challenge).

4.1.7 Integritetstjek

For at verificere at data er konsistente, indeholder strengen en digital underskrift i form af et kryptografisk hashtal (HMAC). Dette tal sikrer, at strengen er sendt fra en afsender, der er tillid til, og at der ikke er manipuleret med indholdet. Hashtallet beregnes ved hjælp af en kryptografisk nøgleafhængig hash-algoritme på baggrund af hele datastrengen. Altså: Såvel af den krypterede som den ukrypterede del.
Hashtallet krypteres efterfølgende ind i den krypterede del af datastrengen.

4.1.8 Reset knap

I enheden findes en trykknap. Ved et kort tryk nulstilles adgangsnøglen i enheden (altså ikke krypteringsnøglen).
Efterfølgende vil Polleren automatisk tildele enhederne den korrekte adgangsnøgle igen.