Teknisk beskrivelse

TDC AlarmNet

Kapitel A, oversigt

Marts 2008

TDC A/S
Teglholmsgade 1
0900 København C
tdc.dk

1. Overblik

Generelt

Dette dokument beskriver på oversigtsform opbygningen af AlarmNettet, De tekniske beskrivelser erstatter det tidligere gældende Cirkulære 29 og publikationen "Tilslutning til AlarmNettet" version 2.1 udgivet af Tele Danmark Erhverv 1996.
Teknisk Beskrivelse består af 3 kapitler

Version

4.01 Marts 2009 / MTA

Forfatter

Mogens Tolberg Andersen / mta@tdc.dk

Indhold

1. OVERBLIK 2

Generelt 2
Version 2
Forfatter 2
Indhold 3

2. ALARMNETTET - SET UDEFRA. 5

AlarmNettets anvendelse 5
AlarmUdstyr (AU) 7
AlarmTerminal (ATU) 7
AlarmTerminal (IP-ATU) 7
VagtCentral (VC) 7
DistriktCenter (DC) 8
AlarmNettet 8

3. LOGISK NETSTRUKTUR 9

AlarmNettets struktur 9
AmuxServer 9
Alarm-MUltipleXer (AMUX) 10
IP-Alarm-MUltipleXer (IP-AMUX) 10
VCServer 10

4. FYSISK NETSTRUKTUR. 11

Transportnet 11
Centerby 11
TSby 12
Oplandsby 12
AMUX 12
IP-AMUX 12
VagtCentral 12

5. ALARMNET ADRESSERING 13

Oversigt ADSL-access 13
Oversigt PSTN /ISDN access 14
AlarmNet adresse 14
Macroadresse 15
Microadresse 15

6. OVERVÅGNING 16

Overvågning 16
Knudetest 16
Overvågning af PSTN/ISDN ATU 17
Overvågning af IP-ATU 17
Statusalarm 18
Logning 19

7. ALARMTERMINAL 20

Generelt 20

8. SIKKERHED (ATU) 21

Generelt 21
Simpelt angreb 21
Intelligent angreb 21
Sådan er det implementeret 23
Sikkerhed ved udskiftning af ATU 24

9. SIKKERHED (IP-ATU) 25

Generelt 25
Net-topologi 26
Simpelt angreb 28
Intelligente angreb 28

10. VAGTCENTRAL 29

Tilslutning via leased line (modem) 29
Tilslutning via LanLink (IP) 30

11. ALARMNETTETS MEDDELELSER. 31

Meddelelsestyper 31
Alarmernes vej fra alarmterminal til vagtcentral 31
Den primære vagtcentral 32
Alternative vagtcentraler 32
Backup-vagtcentraler 32

12. AFVISTE ALARMDATA OG LOGNING. 33

13. REMOTE LANACCESS 35

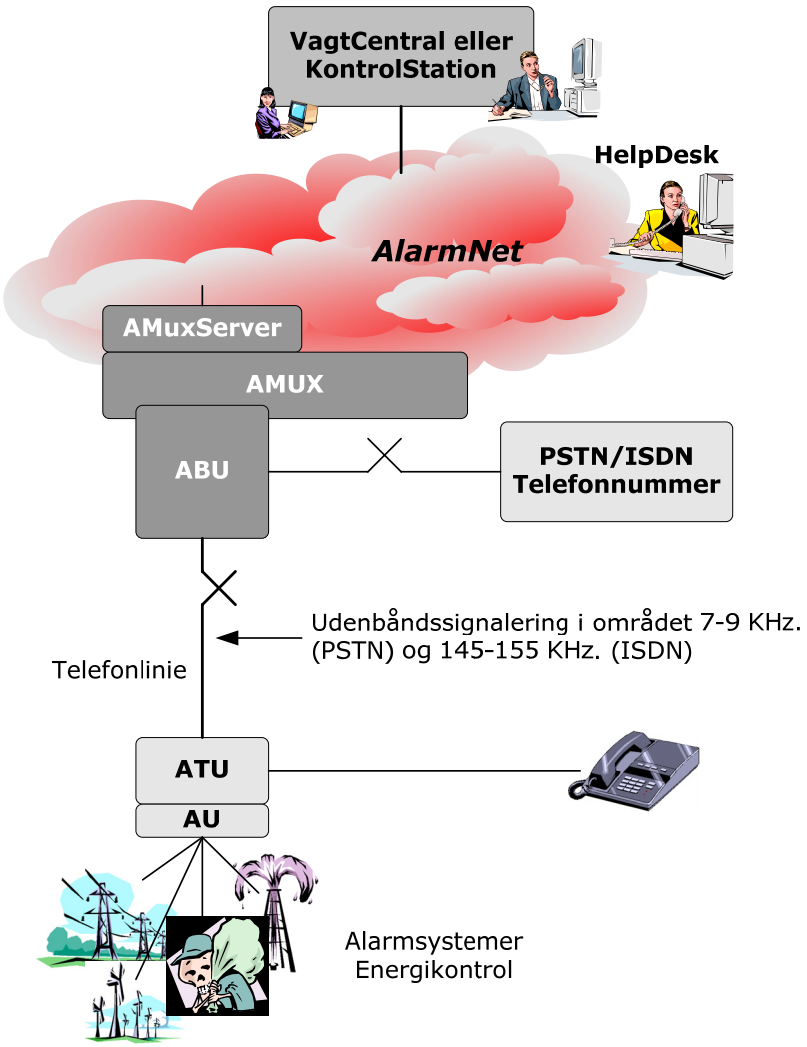
2. AlarmNettet - set udefra.

AlarmNettets anvendelse

Typisk anvendes AlarmNettet til overførsel af opsamlede data mellem en VagtCentral og den enkelte installation, som f.eks. tyverialarmer og måledata. Vagtcentralen kan afgive forskellige former for styring via det opsamlende udstyr (AU) som f.eks. lukning af branddøre, fjernbetjening af pumper og dataopdateringer. Generelt omtales disse data som henholdsvis alarmdata og styringsdata.

Tilslutning af installationer til AlarmNettet kan ske på 2 måder:

- Udenbåndstilslutning på eksisterende PSTN/ISDN kabelforbindelse

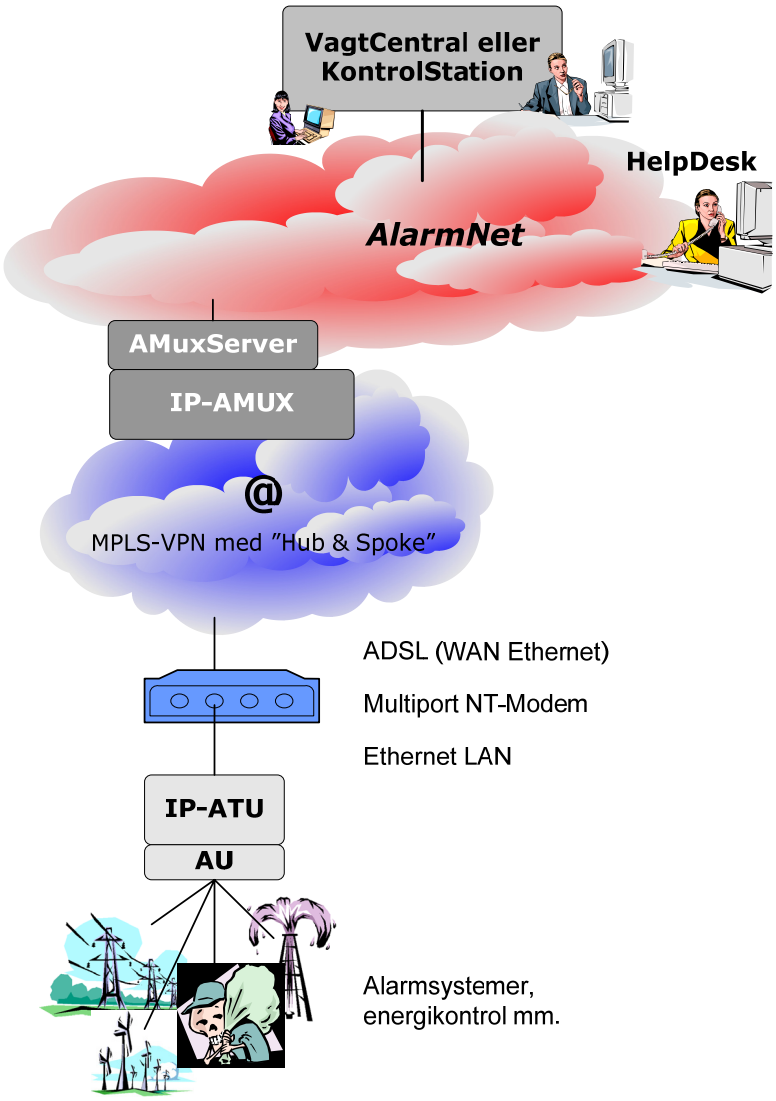


Figur 2.0

fortsættes …

... fortsat

- Ethernet via MPLS-VPN og "Hub & Spoke"



Figur 2.1

Fordelen ved anvendelse af AlarmNettet er en større sikkerhed for fremkommelighed og løbende kontrol af forbindelse/udstyr end den, en traditionel anvendelse af telefonnettet (DialUP) eller internet vil give.
Etableringen er baseret på eksisterende telekabler og installationer.

De komponenter, der indgår, beskrives i det følgende.

AlarmUdstyr (AU)

Alarmudstyret er det kundeudstyr, der opsamler de data, der ønskes overført. Det kan dreje sig om rumfølere, dørkontakter, brandalarmer mm, eller hvad der ellers måtte være brug for. Endvidere er det alarmudstyret, som er i stand til at udføre de handlinger, som ved hjælp af styringer ønskes iværksat.
Alarmudstyret leveres af en lang række leverandører, og der kan være tale om specialudviklet udstyr.

AlarmTerminal (ATU)

Alarmterminalen er den enhed, der sammenbinder alarmudstyret til AlarmNettet via PSTN/ISDN eller basislinie. ATU'en tilsluttes direkte telefonlinien og virker som et filter overfor den eksisterende telefoninstallation. Den vil fysisk befinde sig i nærheden af – eller eventuelt være sammenbygget med - alarmudstyret.
Alarmterminalen leveres i dag kun af TDC i abonnement.

AlarmTerminal (IP-ATU)

IP-Alarmterminalen er den enhed, der sammenbinder alarmudstyret til AlarmNettet via TDC bredbånd. IP-ATU'en tilsluttes en specifik port på et multiport ADSL-modem. Den vil fysisk befinde sig i nærheden af – eller eventuelt være sammenbygget med - alarmudstyret.

VagtCentral (VC)

Vagtcentralen / kontrolstationen er det udstyr, der modtager/sender data til alarmudstyr (alarmer/styringer). Tilslutning til AlarmNettet sker med en seriel forbindelse enten via modem (9600 b/s) eller IP (LanLink).

Vagtcentraler udvikles af en række leverandører, og der findes adskillige muligheder for udbygning med forskellige faciliteter til overvågning, bl.a. grafisk præsentation, samt faciliteter til reaktioner på de modtagne alarmdata, f.eks. i form af automatiseret afsendelse af styringsdata.

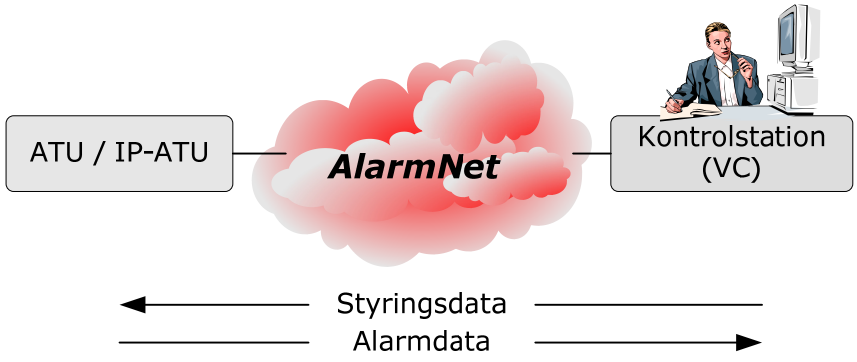


Fig. 2.2: Alarmdata og styringsdata

DistriktCenter (DC)

DC betjenes fra TDC's døgnbemandede HelpDesk. Ved hjælp af DC overvåges AlarmNettet, således at det er muligt at gribe ind, hvis en vagtcentral ikke fungerer eller hvis der opstår fejl i selve AlarmNettet. Det er også HelpDesk, der står for oprettelser, test og idriftsættelse af nye kunder.

AlarmNettet

AlarmNettet er et datatransparent net, der transmitterer henholdsvis alarmdata og styringsdata. Imidlertid er et grundigere kendskab til AlarmNettets opbygning en forudsætning for, at forstå AlarmNettets mere avancerede faciliteter. Dette gennemgås i det følgende.

3. Logisk netstruktur

AlarmNettets struktur

Logisk set er AlarmNettet et IP-net med DC i toppen som den administrative enhed og vagtcentraler, alarmudstyr/alarmterminaler i bunden.

Skematisk kan AlarmNettets logiske struktur tegnes på følgende måde (fig. 3.0):

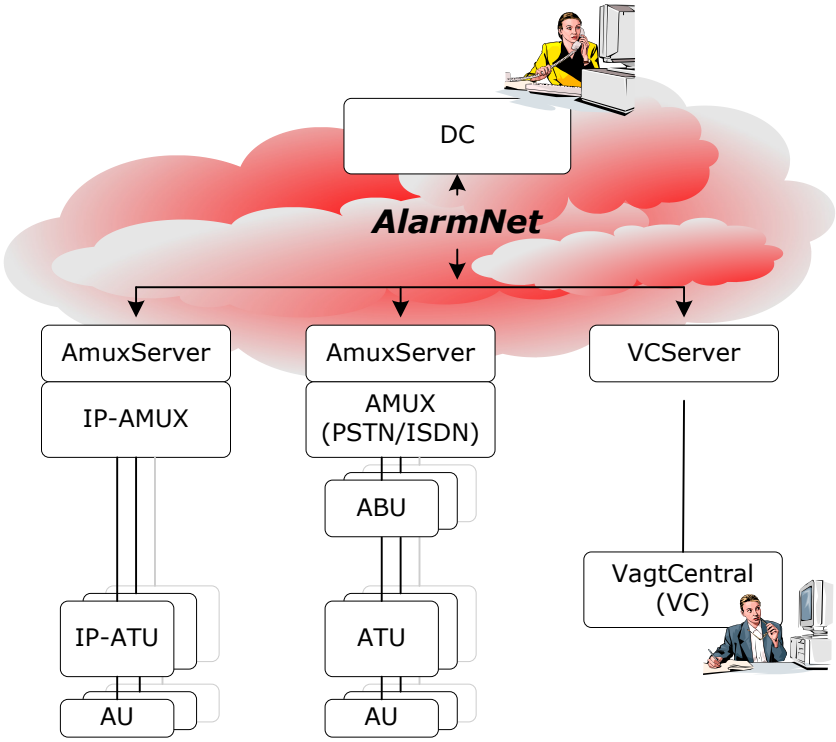


Fig. 3.0: AlarmNettets logiske opbygning

Alle ATU/VC tilslutninger sker gennem en AmuxServer eller VCServer. Serverne tilvejebringer en IP baseret forbindelse mellem alle andre Amux / VCServere og DC.

AmuxServer

AmuxServeren varetager kommunikationen med alarmmultiplekseren (AMUX) og er en del af systemovervågningen i AlarmNettet.

Hver AmuxServer har én alarmmultiplekser tilsluttet.

Alarm-MUltipleXer (AMUX)

Alarmmultiplekseren varetager kommunikationen med PSTN/ISDN alarmterminalerne. Der kan pr. AMUX tilsluttes 72 alarmterminaler via lokalt modem (ABU).

IP-Alarm-MUltipleXer (IP-AMUX)

IP-Alarmmultiplekseren varetager kommunikationen med alarmterminaler tilsluttet ADSL. Der kan pr. IP-AMUX tilsluttes 72 alarmterminaler.

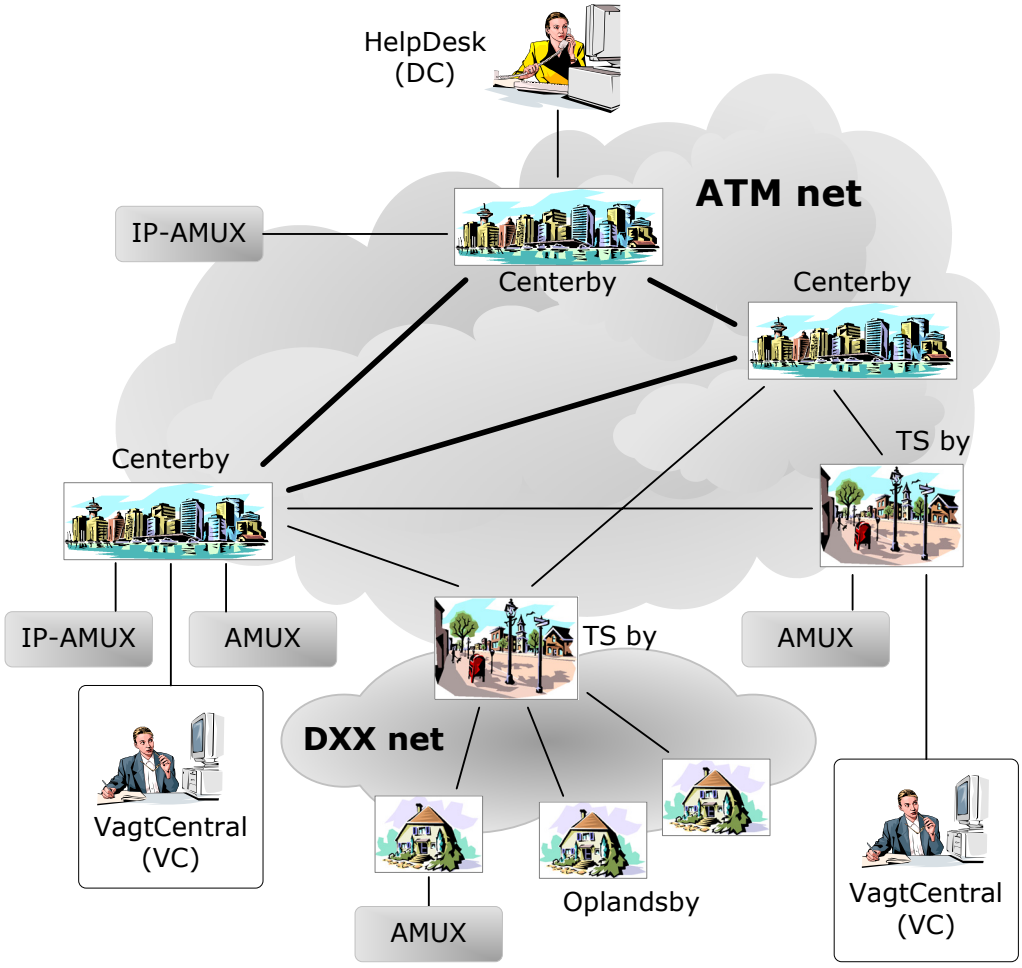
VCServer

VCServeren varetager den serielle kommunikation med VagtCentralen enten via modem eller LanLink og er en del af systemovervågningen i AlarmNettet.
Hver VCServer har én vagtcentral tilsluttet.

4. Fysisk netstruktur.

Transportnet

AlarmNettet er et overordnet lukket separat IP net med egne routere mm og fysisk benyttes ATM som transportnet mellem Centerbyer og TSbyer.



Figur 4.0 herover viser IP-AlarmNettet i simplificeret form.

Centerby

Der er i AlarmNettet 12 "Centerbyer", monteret som redundante komponenter med alternative dataveje, fordelt geografisk i Danmark og i overensstemmelse med TDC's overordnede SDH net (Standard for synchron datatransmission over fibernet - **S**ynchronous **D**igital **H**ierarchy) "Centerby" er i denne sammenhæng et begreb.

TSby

"TSbyer" er stort set placeret i alle støre provinsbyer. Der er alternativitet til en anden ”Centerby” udover ens egen ”Centerby”.
”TSby” er i denne sammenhæng et begreb.

Oplandsby

En "Oplandsby" er en landcentral eller et teknikhus.
Alle ”oplandsbyer” har alternativ ISDN forbindelse til en ”TSby”.
”Oplandsby” er i denne sammenhæng et begreb.

AMUX

Amux'er tilsluttes i ”Centerbyer”, ”TSbyer” eller ”Oplandsbyer”.

IP-AMUX

IP-Amux'er tilsluttes i ”Centerby” eller ”TSby”.

VagtCentral

Vagtcentraler tilsluttes kun i ”Centerbyer” eller ”TSbyer”.

5. AlarmNet adressering

Oversigt ADSL-access

Alle komponenter i en AlarmNetstilslutning har en AlarmNetadresse, som er sammensat af en macro og en microadresse. Ved ADSL er der derudover i accessvejen frem til IP-AMUX'en en IP adressering. IP-ATU'en får tildelt en fast IP-adresse via en dedikeret DHCP.

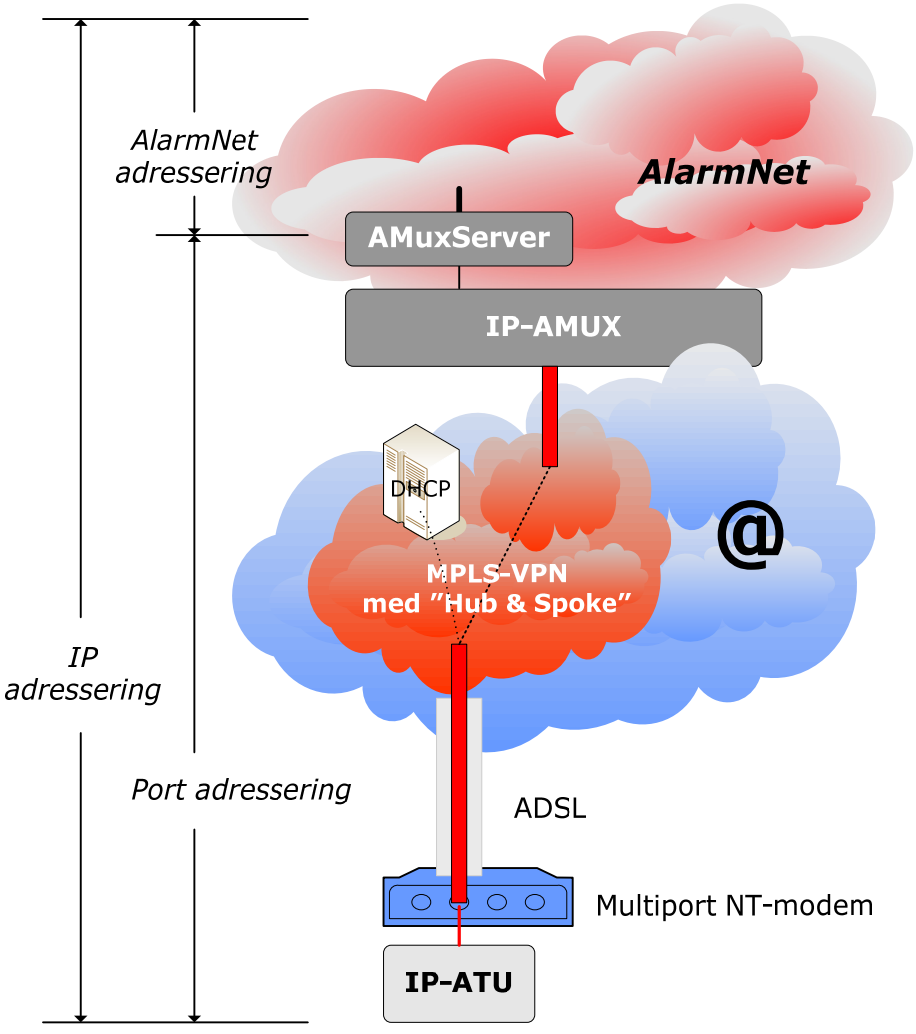


Fig. 5.0 Adressering ved ADSL access

Oversigt PSTN /ISDN access

Alle komponenter i en AlarmNetstilslutning har en AlarmNetadresse, som er sammensat af en macro og en microadresse. Ved PSTN/ISDN access dækker AlarmNetadresseringen til og med ATU. Internt sker det via porte som vist herunder.

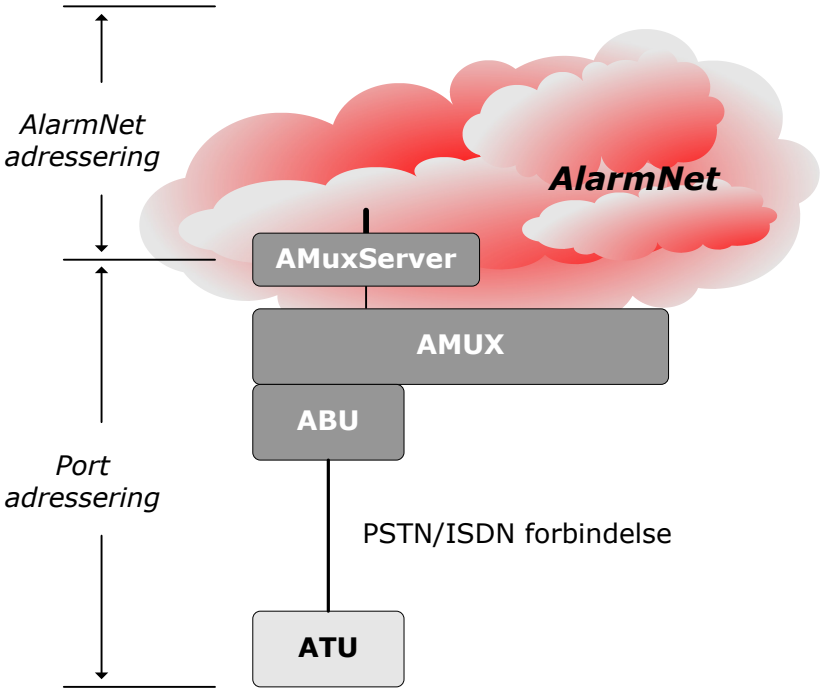


Fig. 5.1 Adressering ved PSTN/ISDN access

AlarmNet adresse

En AlarmNetadresse består af en micro og en macroadressse og afspejler den hirakiske opbygning (se afsnit 6)

fortsættes ...

... fortsat

Macroadresse

AlarmNetadressen består af en makroadresse, som entydigt identificerer et DC-nummer og netgruppenummer. For vagtcentraler, alarmmultipleksere og alarmterminaler består AlarmNet-adressen udover makroadressen også af en mikroadresse.

Makroadressen, der skrives på formatet **d-nn-tt**, er opbygget på følgende måde:

- **d**: DC-nummer, skal ligge i intervallet 1..9
- **nn**: netgruppenummer, skal ligge i intervallet 0..63
- **tt**: terminalstationsnummer, skal ligge i intervallet 0..63

Microadresse

Mikroadressen, der skrives på formatet **mmmm**, tolkes på følgende måde:

- for vagtcentraler skal mikroadressen ligge i intervallet 32..255
- for alarmmultipleksere skal mikroadressen ligge i intervallet 1..38 multipliceret med 256 (dvs. en af værdierne 256, 512, 768 .. 9728)
- for alarmterminaler skal mikroadressen være større end 256, og ligge i intervallet mellem mikroadressen på den alarmmultiplekser, den er tilknyttet, og mikroadressen på den efterfølgende alarmmultiplekser.

EKSEMPEL:
For eksempel vil AlarmNet-adressen 6-01-02-0310 angive adressen på en alarmterminal under DC nummer 6, netgruppenummer 1 og 02 vil sammen med 0310 udpege AmuxServer og tilknyttet Alarmmultiplexer svarende til adressen 6-01-02-0256. Ofte udelades de foranstillede nuller og/eller bindestregerne. Det vil sige, at adressen på den førnævnte alarmterminal skrives som 6 01 02 0310, 6-1-2-310 eller 6 1 2 310.

---

6. Overvågning

Overvågning

AlarmNettet indeholder en række overvågnings- og diagnosticeringsværktøjer. Det drejer sig bl.a. om løbende overvågning af AmuxServer, VCServer, telefonlinieforbindelsen til ATU, DSL forbindelse til IP-ATU, alarmudstyr (AU) og logning.

Knudetest

Alle AlarmNettets komponenter fra DC til AMUX og vagtcentral deltager i en forbindelsestest (knudetest), som løbende finder sted. Ved forbindelsestest anvendes AlarmNettets nettopologiske struktur, dvs. at der testes, om der er forbindelse mellem de enkelte komponenter, som vist i fig. 6.0.

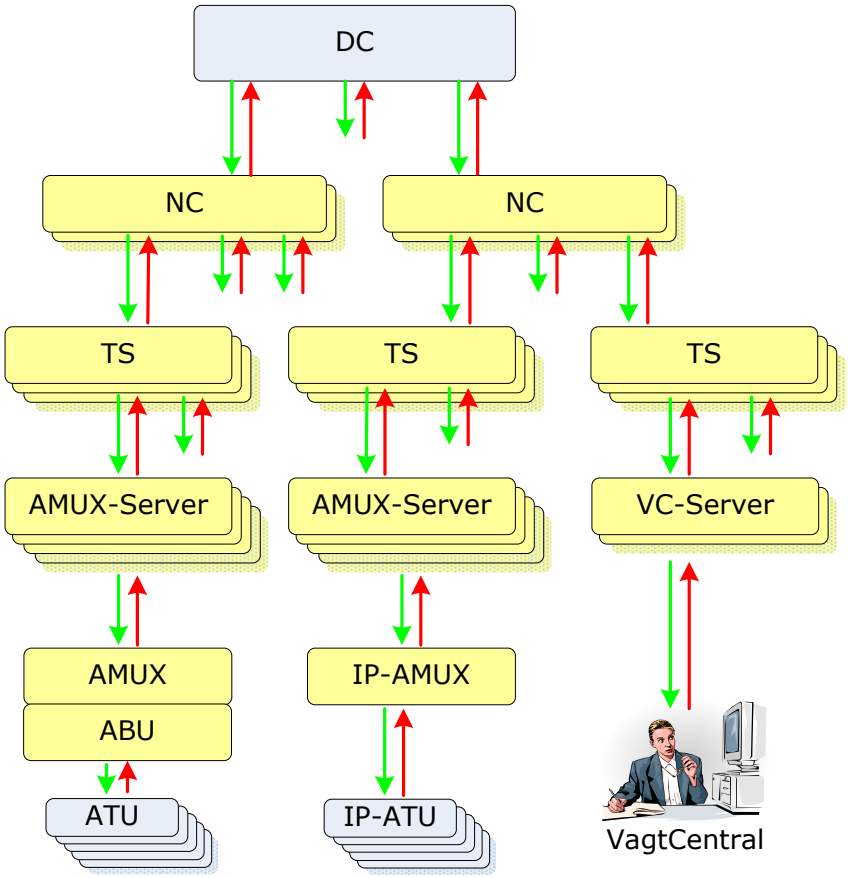


Fig. 6.0 Knudetest foretages på de pilemarkerede forbindelser.

fortsættes ...

... fortsat

For DC, NC, TS og AMUX gælder, at den underliggende komponent forventer efter en knudetest, at næste knudetest ankommer inden for en periode af 2 min. Sker det ikke, dømmes den overordnede komponent nede.

Første gang, der atter kommer svar fra en komponent, der er dømt nede, dømmes komponenten oppe igen.

Hver gang en komponent dømmer en anden komponent oppe eller nede, meddeles dette videre i form af broadcasts, der sendes til alle tilgængelige over- og underliggende til og AMUX/VC-server. Ligeledes videresendes alle modtagne broadcasts til alle tilgængelige komponenter, bortset fra den komponent, der har afsendt den pågældende broadcast.

Dømmes en AMUX nede, vil der ved PSTN/ISDN ske det, at:

- AMUX ophører med at polle sine underliggende ATU'er
- ATU'erne vil pga. manglende poll sænke HW-signalet ATOK som tegn på, at der ikke mere er forbindelse til AlarmNettet.

Dømmes en IP-AMUX nede af en overliggende komponent, vil IP-AMUX, hvis muligt:

- sende en meddelelse til IP-ATU'erne om at sænke HW-signalet ATOK som tegn på, at der ikke mere er forbindelse til AlarmNettet.

Overvågning af PSTN/ISDN ATU

For PSTN/ISDN er forbindelsen mellem AMUX og alarmterminal normalt kundens almindelige telefonledning. Udover knudetest foregår der løbende en overvågning fra AMUX (poll) af forbindelsen således, at der i tilfælde af en afbrydelse vil blive sendt en liniealarm til vagtcentralen og DriftCenteret.

Perioden mellem hvert poll er 2 sekunder. Forudsætningen for en liniealarm er 3 på hinanden følgende ubesvarede poll. Liniealarmen genereres ved afsendelse af fjerde poll (8 sek.)

Hvis kvaliteten af forbindelsen er så dårlig, at den ikke kan anvendes forsvarligt til dataoverførsel, vil der til Driftcenteret blive sendt Service og måske StopPoll alarm.
Service alarm indikerer, at forbindelsen er anvendelig, men der forekommer en del retransmissioner.
StopPoll alarm indikerer, at kun få data overføres. Forbindelsen er meget dårlig.
Service- og StopPoll alarmer er kun aktuelle, når der ikke samtidigt er sendt liniealarm.

Overvågning af IP-ATU

Overvågning af forbindelsen mellem IP-AMUX og IP-ATU sker som en dobbeltrettet funktion. IP-ATU bliver knudetestet af IP-AMUX hvert andet minut og IP-ATU forbindelsestester sin IP-AMUX hvert andet sekund.

fortsættes ...

fortsat ...

Denne forbindelsestest fra IP-ATU bruges som "Keep alivetrafik". Hvis IP-AMUX ikke har modtaget noget fra IP-ATU i 8 sekunder, sendes en linie-alarm til kontrolcentralen og DC.
Der sendes også liniealarm i tilfælde af kommunikationsfejl .
HW-signalet ATOK sænkes som tegn på, at der ikke mere er forbindelse til AlarmNettet.
Serveice- og StopPoll alarmer anvendes ikke ved IP-ATU.

Statusalarm

Endelig findes der en type alarmdata (statusalarmer), der melder om ændringer eller fejl i ATU/IP-ATU, spændingsforsyning eller fejl i kommunikationen mellem ATU/IP-ATU og alarmudstyr (AU). Statusalarmer sendes til DC samt til kontrolcentraler, som har valgt at modtage de pågældende alarmdata.

Mulige statusalarmer for ATU og IP-ATU:

Statusfejl \ **Interface**	Async.	Parif	Serif.	RS232 ALC	RS232	Lokal ether-net
ACO: Fejl i hovedstrømforsyning (Digital indgang)	√	√	√	√	√	√
BAO: Fejl i backup-strømforsyning (Digital indgang)	√	√	√	√	√	√
Restart: ATU er genstartet. Tidligere statusinformation er væk	√	√	√	√	√	√
Handshakefejl: Fejl i kommunikation mellem ATU og tilsluttet udstyr	√	√	√	√	√	-
AU fejl: Det tilsluttede udstyr har meddelt, at det er upålideligt. (Digital indgang)	√	√	√	√	√	√
Kommunikationsfejl: Protokolfejl i kommunikationen mellem ATU og tilsluttet udstyr	-	-	√	√	√	√
Timeout:	√	√	√	√	√	√
ATU: ATU er ikke blevet pollet normalt i > 8 sek.						
IP-ATU: Manglende forbindelse mellem IP-AMUX og AlarmNettet meddelt IP-ATU eller manglende TCP forbindelse i > 8 sek.						

Logning

Alle væsentlige begivenheder i AlarmNettet gemmes på en logserver, så det senere er muligt i detaljer, at analysere et konkret handlingsforløb. Meddelelser, der logges, er bl.a. liniealarmer og broadcasts. Også alarmer fra alarmudstyret logges, hvorimod datatypen ”måledata” kan sendes både med og uden logning.

7. AlarmTerminal

Generelt

Der er gennem tiden udviklet et antal forskellige alarmterminaler med forskellige tilslutningsformer. Anvendelsen af de forskellige alarmterminaltyper vil fortsat blive understøttet af AlarmNettet, men i dag leveres kun terminaltype ATU-4B for tilslutning via PSTN/ISDN eller IP-ATU for tilslutning via xDSL.

ATU-4B (PSTN) findes med følgende fysiske interface:

- asynkron (async)
- parallel (parif)
- RS232 (via AddOn)
- RS422 (via AddOn)
- seriel (serif/strømstyret)
- kundespecifikt interface via AddOn-CPU

IP-ATU (xDSL) tilbyder udover ovenstående også:

- 10Mb ethernet (LAN)

Fysiske interface og HW er beskrevet i kapitel B og C

8. Sikkerhed (ATU)

Generelt

Ved anvendelse af ATU PSTN/ISDN, er det muligt at benytte faciliteter, som giver en stærkt forbedret sikkerhed mod angreb. Ud over den generelle overvågning (knudetest/polling), drejer det sig om:

- **autenticitetskontrol**, der entydigt sikrer, at det er den rette alarmterminal, der er tilsluttet. Herved fjernes risikoen for, at en 'fjendtlig' alarmterminal tilsluttes.
- **sikring mod replay**, således at det ikke vil være muligt at optage en sekvens af kommunikationen mellem AMUX og ATU og 'afspille' den senere og herved omgå autenticitetskontrollen.

Dette sikres ved hjælp af et sæt protokoller, der anvender MAC (Message Authentication Codes) værdier baseret på DES (Data Encryption Standard). Denne sikkerhedsfacilitet, som alene vedrører sikkerheden på forbindelsen mellem alarmterminal ATU og AlarmNettet, er transparent for brugeren.

Simpelt angreb

Forbindelsen mellem alarmterminal og AlarmNet, er overvåget, idet alarmterminalen polles hvert andet sekund. Hvis poll ikke besvares tre på hinanden følgende gange, sendes en liniealarm til vagtcentralen. Alarmnettet vil fortsat forsøge sig med poll af alarmterminalen, og hvis et poll atter besvares, afmeldes liniealarmen.

AlarmNettet sikre dermed mod angreb, der består i at afbryde forbindelsen til alarmterminalen og derved forhindre alarmer i at blive afsendt.

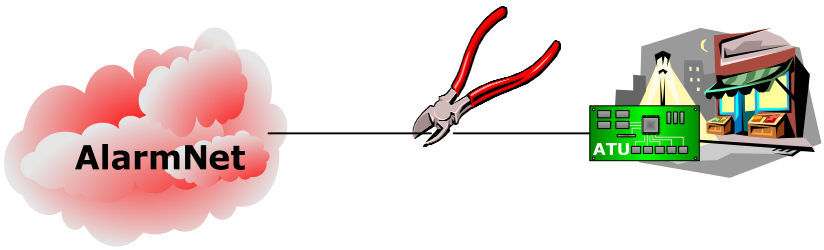


Fig. 8.0: Simpelt angreb

Intelligent angreb

ATU anvender autenticitetskontrol og sikring mod replay som et modsvar mod det, der kan kaldes "intelligente angreb", forstået som et angreb, der er baseret på kendskab til AlarmNettet og adgang til det nødvendige udstyr.

fortsættes …

fortsat …

"Intelligente angreb" kan være følgende:

I praksis kan periodiske fejl på linier/forbindelser af og til medføre linie-alarmer, der hurtigt vil blive afmeldt igen.

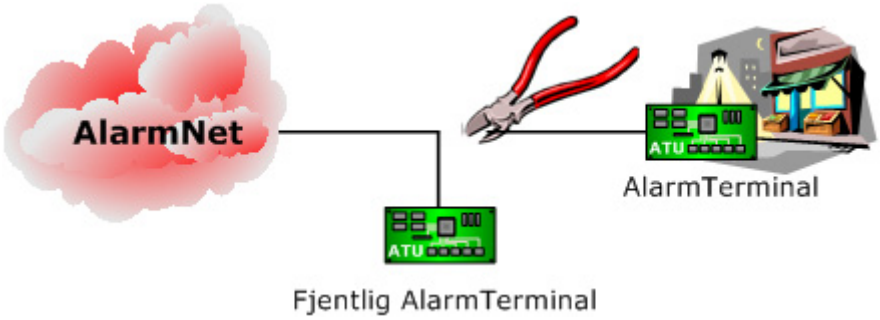


Fig. 8.1 Intelligent angreb: Indkobling af fjendtligt udstyr

Det vil være muligt at indkoble en anden "fjendtlig - alarmterminal", se fig. 8.1 ovenfor.
Indkoblingen af den fjentlige alarmterminal vil resultere i en liniealarm, men en hurtig indkobling af den fjendtlige alarmterminal vil bevirke, at liniealarmen er meget kortvarig.
Set fra vagtcentralen vil dette indgreb ligne en situation med en mulig periodisk forbindelsesfejl.
For at forhindre dette angreb, skal det sikres, at det er den korrekte alarmterminal, der svarer.

En anden og mere avanceret form for "intelligent angreb", der ikke kan afvises alene ved identitetskontrol, vil være at indkoble udstyr, der aflytter meddelelserne og forvansker dem. På denne måde vil alarmer kunne frasorteres og identitetskontrol besvares normalt.

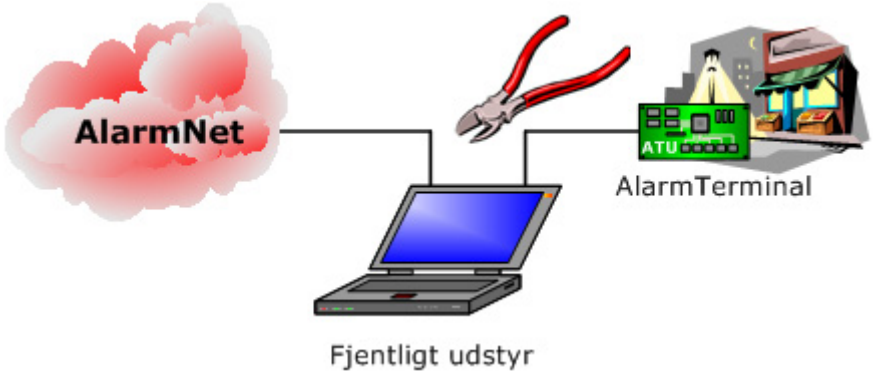


Fig. 8.2 Intelligent angreb: Indkobling af udstyr til aflytning /forvanskning

fortsættes …

fortsat …

En effektiv sikring kræver således både sikring af alarmterminalens identitet og af meddelelsernes ægthed (autenticitetskontrol) samt sikring mod gentagelser (replay). Disse to faciliteter er inkluderet i ATU.

AlarmNettet har integreret denne sikkerhed ved at gøre autenticitetskontrol og sikring mod replay til en facilitet, der tilbydes for al kommunikation på forbindelsen mellem alarmnettet og ATU, som netop er den mest sårbare strækning.

Selve dataindholdet (AlarmUdstyrsdata) er ved ATU ikke krypteret og sendes derfor som klar tekst

Kun nøglerne, som beskrives efterfølgende, skal hemmeligholdes.

Sådan er det implementeret

Hver ATU tildeles en entydig identifikation (nøglen). Nøglen bliver under produktion engangsprogrammeret.
Nøglen distribueres også til AMUX. Denne distribution sker fra et nøglecenter, som er en del af DC. Nøglerne opbevares og distribueres i krypteret form.
Den anvendte kryptering af nøgle er baseret på DES (Data Encryption Standard). Krypteringsalgoritmen er symmetrisk, hvilket betyder at både AMUX og ATU har samme nøgle.
Til den samlede meddelelsen tilføjes en MAC-værdi (Message Authentication Code). Meddelelse og MAC-værdi overføres, og modtageren kan derfor, ved at foretage den samme kryptering, sammenligne og kontrollere meddelelsens ægthed.

For at gøre de enkelte meddelelser unikke og derved imødegå replay-angreb, vælger begge sider ved opstart en tilfældig værdi, der udveksles (i klar tekst). På baggrund af ATU'ens nøgle beregnes nu to værdier, som kaldes challenges.

Begge parter i kommunikationen vil nu kende både sin egen og modpartens challenge. Ved hver kryptering indgår egen - og ved sammenligningen modpartens - challengeværdi i den tegnfølge, der krypteres. For hver kryptering opdateres challengeværdierne ved at kryptere de tidligere benyttede challengeværdier. Da begge sider kan udføre dette, er der ingen grund til løbende at overføre de opdaterede challengeværdier.

Funktionen til opdatering af challengeværdier er udformet således, at en sekvens af værdier ikke vil gentage sig inden for en overskuelig tidshorisont. Det vil derfor ikke reelt være muligt at optage en sekvens for senere afspilning.

Sikkerhed ved udskiftning af ATU

Imidlertid er der også den menneskelige faktor at tage hensyn til, og derfor beskriver dette afsnit den procedure, der anvendes ved udskiftning af en eksisterende alarmterminal ATU med en ny.
Proceduren har til formål at sikre, at det ikke kan lade sig gøre at narre vagtselskab eller TDC til at gennemføre en udskiftning af en alarmterminal med en fjendtlig ATU.

Proceduren omfatter følgende trin:

- Den arbejdsudførende tekniker på adressen kontakter den aktuelle vagtcentral med oplysning om den nye ATU-nøgle.
- Vagtcentralens operatør kontakter telefonisk HelpDesk med anmodning om ændring af ATU-Nøgle på den givne adresse. (samtalen optages)
- Sammen med vagtcentralen foretages herefter ændringen. (StopPoll, ændring af ATU-nøgle, StartPoll)
- Til slut foretager HelpDesk en intern test af alarmterminalen for at sikre, at den nye ATU fungerer korrekt.

9. Sikkerhed (IP-ATU)

Generelt

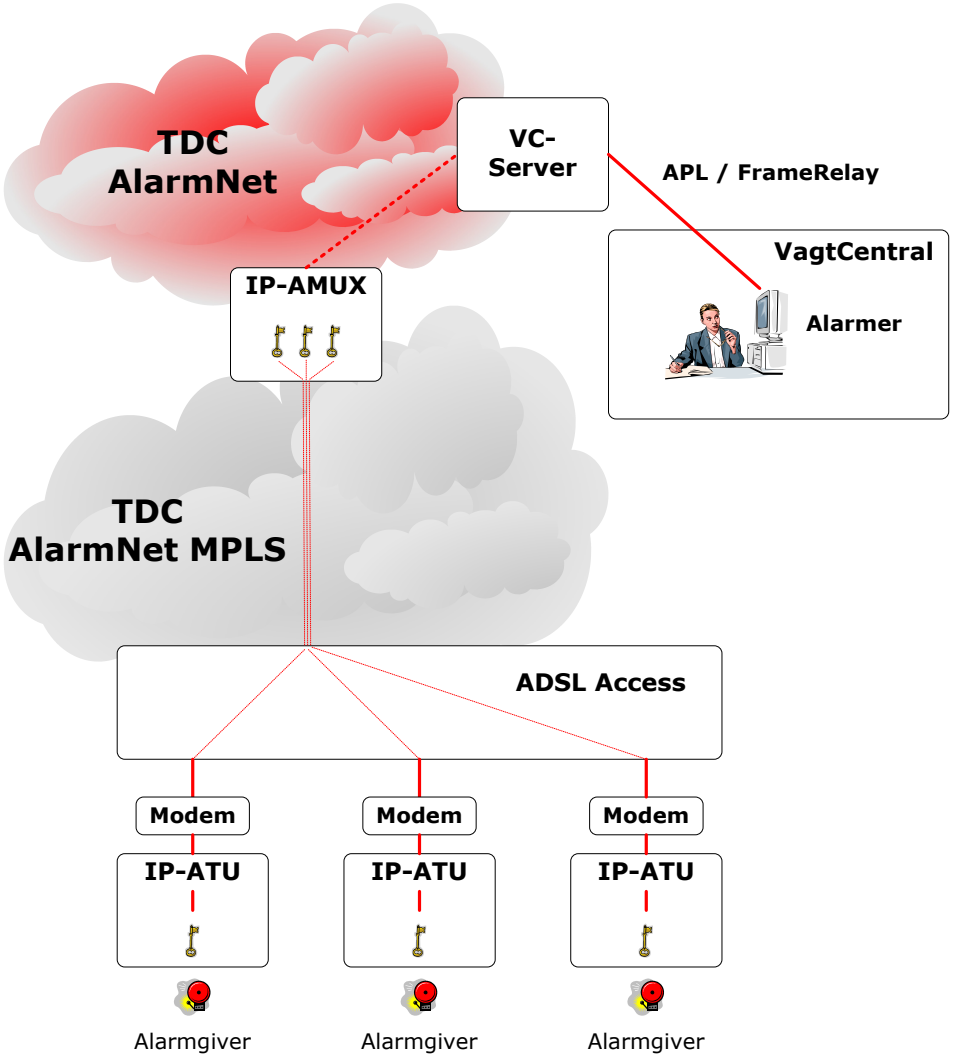
Ved anvendelse af IP-ATU benyttes faciliteter, som giver en meget stor sikkerhed mod angreb. Ud over den generelle overvågning (knude-test/polling), drejer det sig om:

- **Autenticitetskontrol**, der entydigt sikrer, at det er den rette alarm-terminal, der er tilsluttet. Herved fjernes risikoen for, at en 'fjendtlig' alarmterminal tilsluttes.
- **Sikring mod replay** således, at det ikke vil være muligt at optage en sekvens af kommunikationen mellem IP-AMUX og IP-ATU og 'afspille' den senere og herved omgå autenticitetskontrollen.
- **Kryptering af dataindhold,** hvilket sikrer, at dataindholdet hemmeligholdes.
- **Dedikeret PVC med QoS** giver garanti for fremkommelighed af alarmdata (prioriteret datatrafik)
- **Hub & Spoke,** hvilket sikrer en gensidig ”usynlighed” mellem de enkelte IP-ATU’er

Disse sikkerhedsfaciliteter, som alene vedrører sikkerheden på forbindelsen mellem alarmterminal og AlarmNettet, er transparent for brugeren.

Net-topologi

IP-ATU'en er forbundet til alarmnettet via TDCs ADSL platform.
ATU'en tilsluttes en dedikeret port på ADSL modem/router, som via et MPLS-VPN fremføres til IP-AMUX. Fremkommelighed er sikret gennem IP prioritering (QoS), således at AlarmNet-kommunikation har fortrinsret frem for almindelig IP trafik.

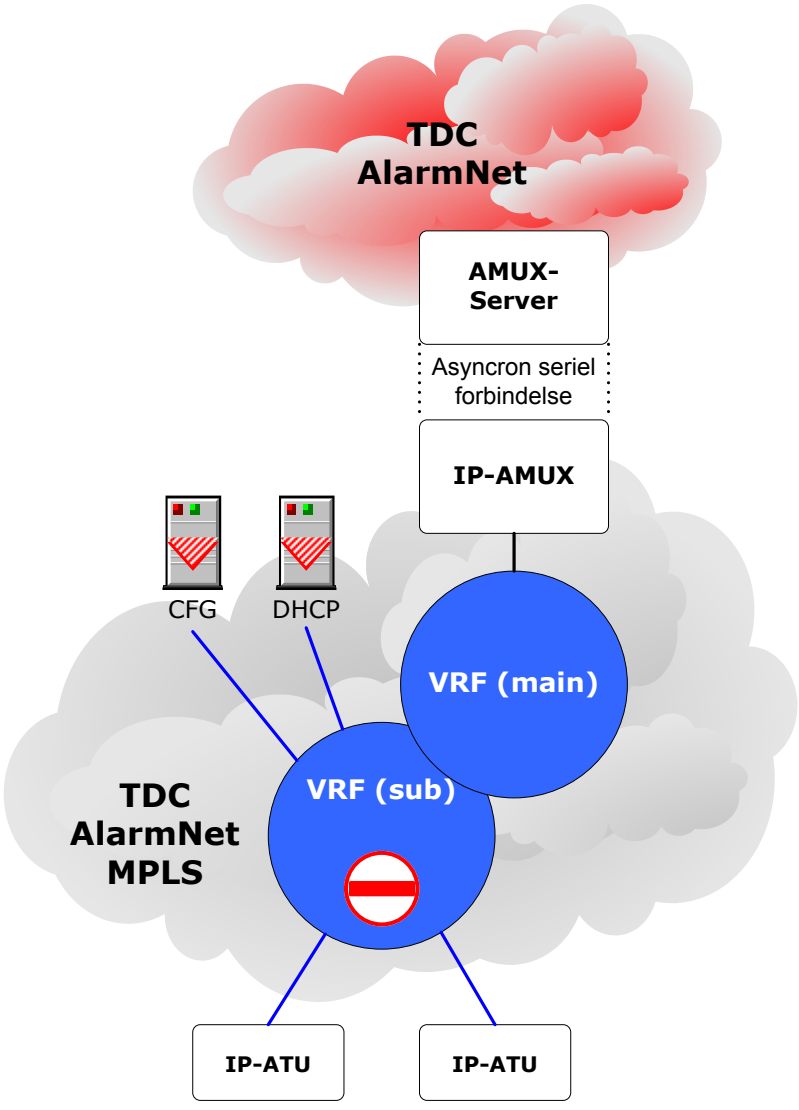


Figur 9.3

fortsættes ...

fortsat ...

AlarmNet MPLS-VPN'et har tilknyttet 2 VRF's. (se figur 9.4)
IP-AMUX er medlem af Main-VRF og alle IP-ATU'er er medlem af Sub-VRF. Virtual Routing and Forwarding (VRF), som en del af VPN, er en teknologi, som sikre en effektiv adskillelse mellem AlarmNettrafik og andre internet-brugere (paths).



Figur 9.4

AlarmNet MPLS-VPN'et har indbygget "hub and spoke" (nav og eger som på en hjul) uden routnings mulighed (forbindelse) mellem de enkelte spokes (IP-ATU'er). Det betyder at den enkelte spoke kan se sin egen IP-AMUX (hub), men ikke de andre spoker. Omvendt kan huben se alle spoker.

fortsættes ...

... fortsat

Sikkerhedsmæssigt betyder det, at der ikke er adgang mellem de enkelte IP-ATU'er.
På netværkslag 2 er det TDCs ADSL mekanismer, der forhindrer sniffering m.m. mellem de enkelte ADSL forbindelser.

Der er til sub-VRF tilknyttet 2 specielle funktionsservere:

- DHCP, som bl.a. tildeler IP-ATU'en en AlarmNet specifik IP-Adresse og IP-adressen på dens aktuelle CFG server.
- CFG, som sørger for den korrekte konfiguration af IP-ATU f.eks. hvilken IP-AMUX, den tilhøre. IP-ATU'ens unikke serienummer er nøglen til information fra CFG serveren.

Simpelt angreb

Forbindelsen mellem IP-ATU og AlarmNet er overvåget, idet alarmterminalen poller AlarmNettet (IP-AMUX) hvert andet sekund og selv bliver pollet hvert andet minut. Hvis IP-AMUX ikke modtager poll tre på hinanden følgende gange, sendes en liniealarm til vagtcentralen. Modtager IP-AMUX igen poll fra IP-ATU og bliver et poll fra IP-AMUX atter besvaret, afmeldes liniealarmen.

Installationen overvåges derfor mod angreb, der består i at slukke for strømmen, afbryde linieforbindelsen til ADSL-modem eller ethernetforbindelse mellem modem og IP-ATU, og derved forhindre alarmer i at blive afsendt.

Intelligente angreb

IP-ATU anvender autenticitetskontrol og sikring mod replay som et middel mod angreb, der er baseret på kendskab til AlarmNettet og adgang til nødvendigt udstyr.

Implementeringen er identisk med PSTN/ISDN (se afsnit 9)

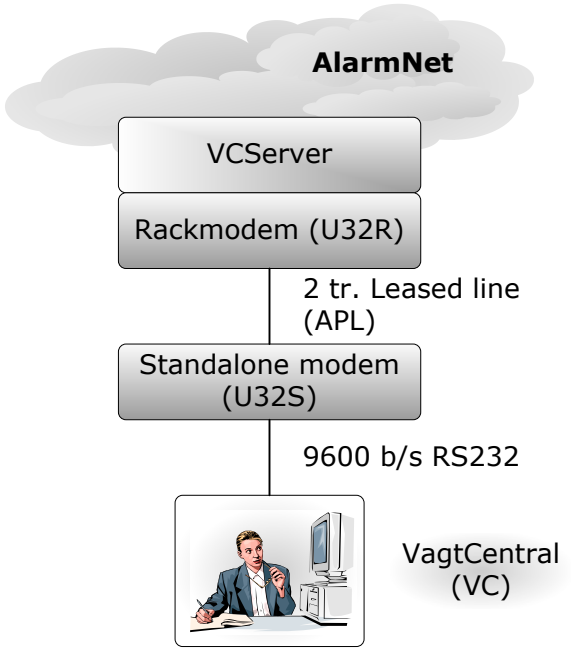
Alarmdata krypteres efter DES standard.

10. VagtCentral

Vagtcentraler tilsluttes AlarmNettet på to måder:

Tilslutning via leased line (modem)

- ALC-tilslutning

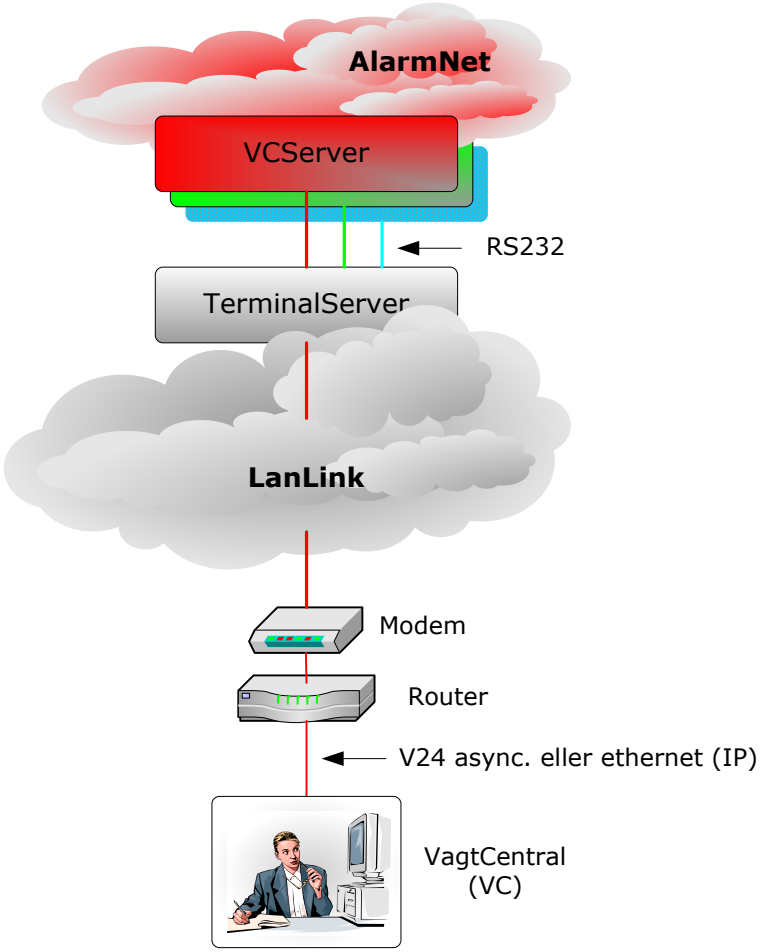


Ved ALC-tilslutning er tilslutningshastigheden 9600 bit/s. via et specielt V32 TDC modem. Vagtcentralen er fysisk tilsluttet en bestemt VCServer, og til kommunikation anvendes protokollen ALC.

Tilslutning via LanLink (IP)

- IP-tilslutning

  Fremføringen sker ved hjælp af et LanLink (F/R) kredsløb, afsluttet hos bruger gennem en router. Tilslutningen her kan være V24 eller Ethernet. Den maximale datahastighed er 57.6 kb/s.



ALC protokollen anvendes også her uanset om det sker direkte via V24 eller gennem en IP tilslutning.

11. AlarmNettets meddelelser.

Meddelelsestyper

Kommunikationen i AlarmNettet er tidligere omtalt som henholdsvis alarmdata og styringsdata, som identificeres ved hjælp af meddelelsestyper. Typerne tjener en lang række formål i AlarmNettet. En meddelelse i AlarmNettet er identificeret ved en operationskode, som består af to tal, adskilt af et punktum. Det første tal identificerer en hovedgruppe, mens det andet tal specificerer meddelelsen yderligere.

Disse operationskoder repræsenteres som et tocifret hexadecimalt tal, hvor første ciffer svarer til hovedgruppen. Det vil sige at meddelelsestype 3.0 er repræsenteret som H30, og meddelelsestype 3.15 som H3F. De enkelte meddelelsestyper til og fra alarmudstyr og vagtcentraler er beskrevet i detaljer i kapitel C.

Alarmernes vej fra alarmterminal til vagtcentral

Når en alarmterminal oprettes i AlarmNettets database, fastlægges hvordan den pågældende alarmterminal skal kommunikere med en eller flere vagtcentraler. Herunder fastlægges, hvilke vagtcentraler alarmterminalen kan sende meddelelser til eller modtage fra. Hertil benyttes et begreb, som kaldes en adresseskiftkode, der er et tal i intervallet 0..255.
Når en alarmterminal oprettes på DC, oprettes der derfor en tabel med følgende udseende (fig. 11.1):

Adresse-skiftkode	VagtCentral	Backup vagtcentral	Meddelel-sestype
0	PVC	BVC	3.x
1	AVC 1	BVC a	3.x
:	AVC n	BVC b	3.x
255	AVC 255	BVC c	3.x

Fig.11.1

Når alarmudstyret via alarmterminalen vil aflevere alarmdata, afleveres der også en adresseskiftkode. Afleveres der ikke en adresseskiftkode, vil adresseskiftkode 0 blive anvendt.
Brugen af adresseskiftkoder giver en sikkerhed for at alarmdata kun sendes til de vagtcentraler, man ved oprettelsen eller senere planlagte ændringer ønsker at sætte som modtager. Det er altså ikke muligt at en alarmterminal - enten som følge af fejl i udstyret eller som følge af en bevidst fjendtlig handling - oversvømmer en fremmed vagtcentral med alarmdata.

Den primære vagtcentral

En alarmterminals primære vagtcentral (PVC) er den vagtcentral, der er udpeget for adresseskiftkode 0.
Den samme vagtcentral kan udmærket være udpeget for andre adresseskiftkoder. Med ATU/IP-ATU er det muligt at bruge samme adresseskiftkode til at sende meddelelser med forskellig størrelse. Tidligere har det været nødvendigt at definere en adresseskiftkode for hver kombination af modtager, meddelelsestype og længde (ATIS, ATIM, ATIA mm).

Alternative vagtcentraler

For adresseskiftkoderne fra 1 til 255 er det muligt at udpege andre vagtcentraler end den primære vagtcentral. Disse kaldes alternative vagtcentraler (AVC'er). Det skal understreges, at en alternativ vagtcentral ikke må opfattes som en backup-facilitet, men derimod et alternativ til den primære vagtcentral.
Det er muligt for den enkelte adresseskiftkode at specificere, at den primære vagtcentral skal modtage en kopi af alarmdata sendt til en alternativ vagtcentral.

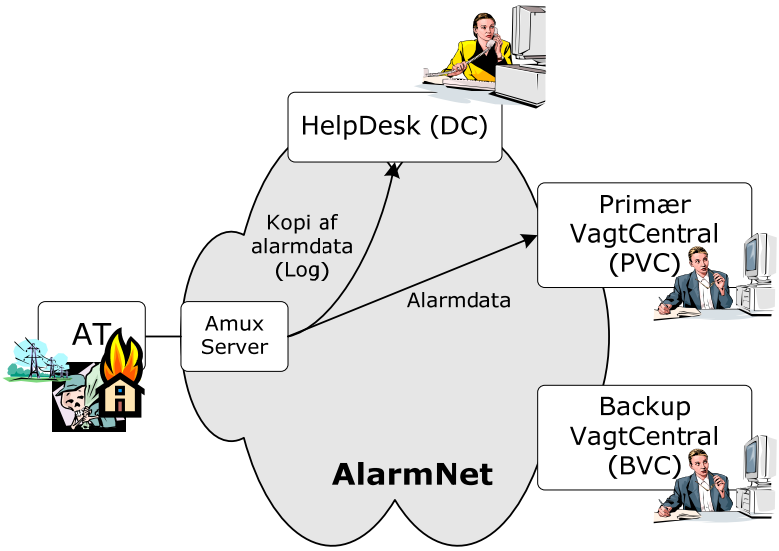
Backup-vagtcentraler

Som det ses af tabellen ovenfor (fig. 11.1), er det for hver enkelt adresseskiftkode muligt at angive en backup-vagtcentral (BVC). Hvis den netenhed, som alarmterminalen hører under, ikke kan aflevere alarmen til den specificerede vagtcentral (primær eller alternativ), sendes den i stedet til backup-vagtcentralen, såfremt en sådan er specificeret.
Backup-vagtcentral kan således specificeres for hver eneste af den enkelte alarmterminals adresseskiftkoder. Der er ikke tale om, at én vagtcentral er backup-vagtcentral for en anden vagtcentral.

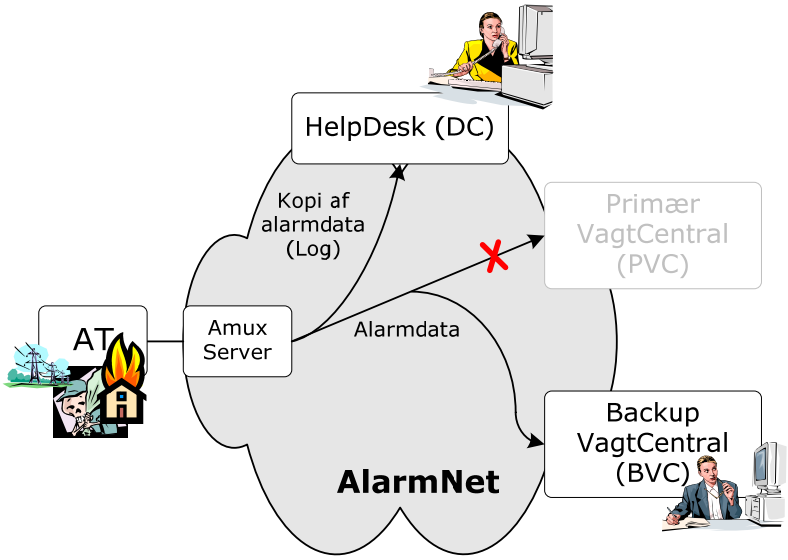
---

12. Afviste alarmdata og logning.

Nedenfor vises en mulig konfiguration med primær vagtcentral (PVC/AVC) og backup-vagtcentral (BVC) defineret for en alarmterminal (AT).



De pågældende alarmdata forsøges først sendt fra AT til PVC/AVC. Samtidig sendes en kopi af alarmdata som logmeddelelse til DC.

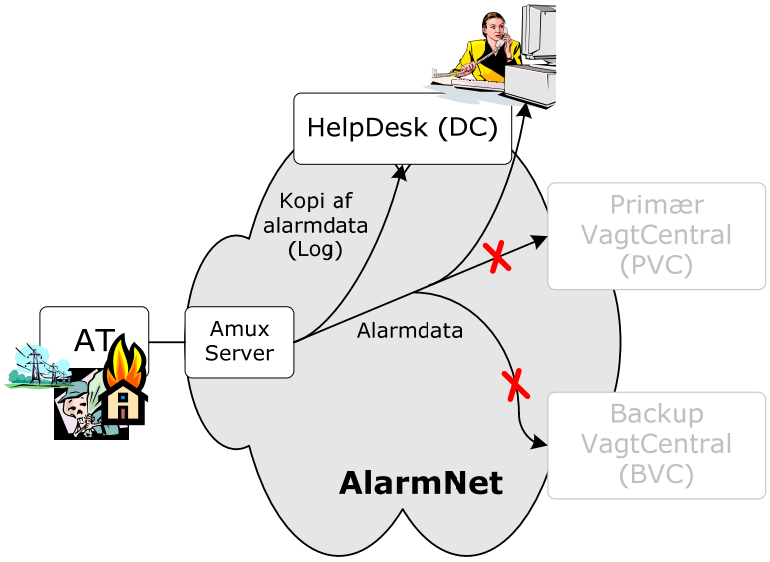


Er det ikke muligt at sende alarmdata fra AT til PVC/AVC, sendes alarmen i stedet til BVC. Når alarmdata er modtaget af PVC/AVC eller BVC, sendes en logmeddelelse til DC om, at alarmdata er afleveret.

fortsættes …

fortsat …

Hvis hverken PVC/AVC eller BVC kan nås, sendes alarmdata til DC og præsenteres som afvist alarm på operatørens skærm, så denne kan gribe ind og kontakte personalet på den pågældende vagtcentral.



Samtidig logges de omdirigerede alarmdata også i DC's log.

Virkemåden vil være den samme, hvis adresseskiftkoden i stedet udpeger en alternativ vagtcentral.
Foruden alarmdata, kan alarmudstyret også sende måleværdier med eller uden logning på distriktscentret. Hvordan de nævnte faciliteter kan anvendes for disse meddelelsestyper er vist nedenfor:

13. Remote LANaccess

Blank side

adresseskiftkode 32
alarmdata 6
Alarmmultiplekser 11
AlarmNetadresse..... 14;15;16
Alarmterminal..... 8
Alarmudstyr 8
ALC..... 31
ALC linedown..... 19
AT 8
ATM 12
ATOK 18;19
AU 8
autenticitetskontrol 22;26
AVC 33
BVC 33
Centerby..... 12
challenge 24
DES 24
HelpDesk 9
Hub & Spoke 7;26
Keep alivetrafik..... 19
knudetest 17
kontrolstation 8
Kryptering..... 26
LanLink 31
log 20
logserver 20
MAC 24
MAC-fejl 19
makroadresse..... 16
meddelelsestyper..... 32
mikroadresse 16
MPLS-VPN 7
Nøgle 24
Oplandsby..... 13
Service alarm 18
sikring mod replay 22;26
statusalarm..... 19
StopPoll alarm 18
styringsdata 6
TSby 12
Vagtcentral 8
VC 8

TDC Alarmnet