INHOUDSTAFEL

1 HET GEBRUIK VAN HET IP TELEMATICANETWERK 1
1.1 Inleiding 1
1.2 Algemeen 1
1.3 Verantwoordelijkheden netwerk 1
1.4 Verantwoordelijkheden aanneming 2
1.5 Beschikbare netwerkdiensten 3
1.6 Montage-aspecten 3
1.7 Informatie te leveren door de aanneming 3
1.8 Informatie te leveren door de netwerkbeheerder 4
1.9 Gebruik van eigen netwerkapparatuur 4
1.10 Aanvaardbaar gebruik 5

LIJST NORMEN EN DIENSTORDERS

1 HET GEBRUIK VAN HET IP TELEMATICANETWERK

1.1 Inleiding

Onderstaande tekst beschrijft de voorwaarden waaraan toepassingen moeten voldoen om gebruik te kunnen maken van het telematica IP netwerk. Specifieke vereisten kunnen steeds in onderling overleg besproken worden. Uittesten van de toepassing gebeurt in coördinatie met de aannemer en het netwerkteam.

1.2 Algemeen

Met telematicanetwerk wordt in deze tekst het telematica IP netwerk bedoeld, dat specifiek uitgebouwd is om technische toepassingen te laten communiceren. Daarnaast is er ook nog mogelijkheid tot verkrijgen van transparente ethernet of E1-connecties over SDH of WDM/OTN, waarop in deze tekst niet dieper ingegaan wordt. Het buroticanetwerk, waarvan in deze tekst sprake, is het netwerk dat de Vlaamse Overheid outgesourced heeft aan een externe firma, voor de communicatiebehoeften die eerder administratief gericht zijn.

Bij aanpassing van de IP adressering van de apparatuur van de toepassing zal er geen meerprijs gelden voor software-aanpassingen. Hiertoe kan eventueel gebruik gemaakt worden van de DNS functionaliteit die het telematicanetwerk aanbiedt. Op deze wijze wordt het mogelijk aanpassingen in de netwerkgegevens van de aangesloten apparatuur uit te voeren zonder de toepassingssoftware te moeten bijwerken.

De toepassing moet terugvallen op een veilige situatie bij wegvallen van het netwerk Het netwerk heeft weliswaar een zeer hoge beschikbaarheid; er kan echter altijd een uitval optreden.

Het telematicanetwerk voorziet steeds een UPS; de aannemer mag er echter niet van uitgaan dat deze UPS ook voor zijn toepassing mag gebruikt worden.

1.3 Verantwoordelijkheden netwerk

Het telematicanetwerk is verantwoordelijk voor:

- levering en installatie van de netwerkapparatuur;
- verbindingen tussen netwerkapparatuur binnen dezelfde site of tussen sites;
- instellingen op de netwerkapparatuur,
- verwerking van SNMP traps van de UPS van het telematicanetwerk met betrekking tot de afwezigheid en aanwezigheid van de voedingsspanning;
- toewijzing van IP adresseringsgegevens en aansluitpoorten;
- uitschakelen van niet-toegewezen poorten op de actieve netwerkapparatuur;
- ter beschikking stellen van RJ45 aansluitpoorten van type 10/100 BaseT (IEEE 802.3 & 802.3u) op alle sites;
- ter beschikking stellen van RJ45 aansluitpoorten van type 10/100/1.000 BaseT (IEEE 802.3 & 802.3u & 802.3ab) op een beperkt aantal sites, bedoeld voor het aansluiten van servers, wanneer snelheden boven 100 Mbps van/naar de aangesloten server(s) nodig zijn;
- ter beschikking stellen van Power over Ethernet (802.3af) op 10/100BaseT poorten indien gevraagd voor deze toepassing;
- dimensioneren, upgraden en uitbreiden van het netwerk waar nodig;
- ondersteuning van multicast indien gevraagd.

1.4 Verantwoordelijkheden aanneming

De aannemer van de toepassing is verantwoordelijk voor:

- levering van de apparatuur die aan het netwerk te koppelen is;
- levering van de netwerkaansluiting van de apparatuur (network interface card);
- instellen van de netwerkparameters op de network interface card;
- indien een of meerdere UPS systemen geleverd worden:
  - aansluiting van UPS op het netwerk;
  - netwerkinstellingen op de netwerk interface van de UPS;
  - SNMP traps naar meerdere centrale bewakingssystemen van het netwerk (gegevens die minimaal ingesteld moeten worden, worden door de netwerkbeheerder meegedeeld, zoals IP adressen, community strings e.d.);
  - SNMP traps minimaal voor het uitvallen en opkomen van de ingangsspanning van de UPS;
  - toegang tot de UPS via het netwerk met mogelijkheid tot verificatie van de toestand van de UPS, waaronder de ingangsspanning, en dit met één of meerdere van de volgende TCP/IP protocols: telnet, ssh, http, https, snmp.
    Bijkomende informatie hiervoor (login, paswoord, handleiding verificatie) wordt door de aannemer doorgegeven.
- uitsluitend gebruik van TCP/IP, UDP/IP en/of ICMP als communicatieprotocollen over het netwerk;
- verlies van datapakketten in het transport is voorzien in de toepassing (standaard TCP gedrag of toepassingsvoorzieningen bij gebruik van UDP);
- correcte werking van de toepassing over een gerouteerd netwerk;
- toepassing zonder gebruik van Windows broadcast protocollen (zoals netbios) tussen sites of aparte subnets binnen een site;
- toepassing zonder gebruik van broadcast;
- indien dit voor de toepassing echt gewenst is dienen voorafgaande besprekingen gehouden te worden over de haalbaarheid ervan: broadcast is niet mogelijk over een gerouteerd netwerk; een broadcast kan wel getransporteerd worden naar een verwijderd segment;
- geen IP layer 3 functionaliteit in de apparatuur die in het kader van de aanneming wordt aangesloten;
- gebruik van namen in de (centrale) toepassingssoftware, met gebruik van DNS functionaliteit om het IP adres te bepalen;
- toepassing zodanig opgebouwd dat er geen extra kost is bij het aanpassen van de gebruikte IP adressen als netwerkaanpassingen dit nodig maken. Dergelijke aanpassingen gebeuren hoogstens 1 maal per jaar per aangesloten apparaat;
- ondersteuning van statische instelling van IP adres, subnet mask en default gateway, eventueel ook van DHCP;
- instelling van de aangesloten apparatuur zodat deze reageert op een ICMP ping request (met een ICMP ping reply);
- indien DHCP gebruikt wordt:
  - eindapparatuur dient voldoende lang (5 minuten) DHCP requests te sturen om de opstartperiode van de lokale switch te overbruggen na bvb een stroomonderbreking.

1.5 Beschikbare netwerkdiensten

- DHCP door het netwerk, beperkt tot netwerkgegevens (IP adresgegevens, DNS gegevens).
- DHCP relay, waarbij DHCP requests doorgestuurd worden naar een DHCP server van de aanneming.
- NTP (Network Time Protocol).
- DNS (Name Server) – de aannemer mag ook zijn eigen DNS gebruiken.
- Beheer van een DNS subdomein is mogelijk voor de toepassing door de aannemer zelf ook wanneer geen eigen DNS hardware voorzien in voor de aanneming.
- Monitoring van toepassingsapparatuur (servers, eindapparatuur…) is mogelijk mits akkoord van het opdrachtgevend bestuur volgens af te spreken methodes en afhandeling.
- Toegang tot centrale apparatuur via het internet is mogelijk, beveiligd door middel van een geëncrypteerde verbinding, met authenticatie door een token (aan te vragen aan de netwerkbeheerder) op basis van een internet browser met ondersteuning van https.
- Hiertoe zal door de aannemer aangegeven worden welke TCP en/of UDP poorten nodig zijn voor de toegang tot de centrale apparatuur.
- Toegang tot het burotica netwerk is mogelijk via de VONET koppeling via standaard protocollen (http/https, ftp). Voor andere protocollen dient met burotica overlegd te worden. Hiertoe zal door de aannemer aangegeven worden welke TCP en/of UDP poorten nodig zijn voor de toegang tot de centrale apparatuur.

1.6 Montage-aspecten

De aannemer van de toepassing voorziet:

- de nodige plaats voor de montage van de UPS van het telematicanetwerk en de voorziene netwerkapparatuur. In een geconditioneerde ruimte is deze apparatuur in principe voorzien voor montage in een 19 inch rek. Andere opstellingswijzen dienen goedgekeurd te worden door de projectingenieur (bijvoorbeeld staande UPS, DIN-rail mountable netwerkapparatuur, opstelling in niet-geconditioneerde ruimtes);
- de elektrische voeding voor de netwerkapparatuur. De elektrische voeding gebeurt op netvoeding via een tweepolige automaat 16 A en 230 V;
- de verbinding tussen de toepassing en de netwerkapparatuur (UTP kabel, RJ-45 connectie) is de verantwoordelijkheid van de aannemer van de toepassing. De kabel is in principe een blauwe UTP-kabel. De nodige labeling moet voorzien worden.

1.7 Informatie te leveren door de aanneming

- Aantal nodige aansluitpoorten per site.
- Sites waar gigabit aansluitingen nodig zijn, aantal gigabit aansluitingen.
- Aanduiding of opdeling in subnets (gescheiden LANs) ongewenst/gewenst/nodig is, en dit per site.
- Prioriteit van het dataverkeer, op basis van type:
  - Voice (spraak);
  - Video;
  - Best-effort;
  - …
- Schatting debiet van vertrekkende/aankomende gegevens per site (in Kilobit per seconde of Megabit per seconde).

- Aantal aansluitpoorten per site waarvoor Power over Ethernet (PoE) nodig is.
- DNS gegevens (naam en IP adres) voor apparatuur, voor zover geen eigen beheer van een DNS subdomein gebeurt.
- IP adres van de DHCP server van de aanneming, voor zover gebruik gemaakt wordt van de DHCP relay functionaliteit van het netwerk.

1.8 Informatie te leveren door de netwerkbeheerder

- Identiteit van de aansluitpoorten per site en per subnet, dit laatste voor zover meerdere subnets in een site van toepassing zijn.
- Type van de aansluitpoorten per aansluitpoort (10/100 BaseT of 10/100/1.000 BaseT poort, al dan niet met Power over Ethernet).
- Per site en subnet: IP instellingen voor de aan te sluiten toepassingsapparatuur.
- (zo nodig) IP gegevens over DNS server(s).
- (zo nodig) IP gegevens over NTP server(s).
- (zo nodig) IP gegevens over DHCP relay points.

1.9 Gebruik van eigen netwerkapparatuur

Het is de aanneming toegestaan om eigen netwerkapparatuur te gebruiken mits rekening te houden met de volgende beperkingen:

- eigen netwerkapparatuur van een aanneming dat een aansluitend (netwerk)geheel vormt zal op één en slechts één poort van het telematicanetwerk gekoppeld worden (achtergrond hiervan : vermijden van rondlussen bij incoherente instellingen van STP tussen het telematicanetwerk en het netwerk van de aanneming);
- assistentie bij foutopsporing door de beheerder van het telematicanetwerk strekt zich niet uit tot het netwerkgeheel van de aanneming. Deze assistentie beperkt zich tot op de aansluitpoort van het netwerk van de aanneming op het telematicanetwerk;
- de aansluitingen op het telematicanetwerk zijn native ethernet aansluitingen;
- mits overleg met de beheerder van het telematicanetwerk kan hiervan afgeweken worden voor 802.1q (ook VLAN trunking genoemd) of LACP (voor aggregeren van meerdere aansluitpoorten tot 1 virtuele poort met hogere bandbreedte);
- er wordt geen gebruik gemaakt van routing protocols of statische routing tussen het telematicanetwerk en het netwerk van de aanneming (anders verwoord: geen Layer 3 functionaliteit);
- gebruik van andere IP subnets dan deze die door de netwerkbeheerder toegekend zijn gebeurt op eigen risico van de aanneming. Er is geen enkele garantie dat bestemmingen in deze andere subnets via het telematicanetwerk naar de netwerkapparatuur van de aanneming zal verstuurd worden;
- de monitoring van de netwerkapparatuur van de aanneming is (onder voorwaarden) weliswaar mogelijk, maar gebeurt niet standaard door het telematicanetwerk.

Bij gebruik van een eigen GPRS toestel is aanvullend het volgende nodig:

- gebruik van een IP subnet toegekend door Telematica;
- gebruik van een statische route in Telematica om (onversleuteld) te routeren naar het GPRS toestel van de aannemer ofwel een IP sec tunnel vanaf de GPRS doos naar de firewall van Telematica.

1.10 Aanvaardbaar gebruik

Om connectie te krijgen met het telematicanetwerk moeten een aantal regels in verband met de veiligheid nageleefd worden. Een aantal van deze regels over specifieke onderwerpen zijn vastgelegd in zogenaamde “security policies”. Zo bestaan er volgende security policies:

- beleid_Aanvaardbaar_Gebruik.doc;
- beleid_Analoge_en_ISDN_lijnen.doc;
- beleid_Draadloze_Communicatietoegang.doc;
- beleid_Extranet.doc;
- beleid_Toegang_vanop_afstand.doc;
- beleid_VPN.doc;
- audit beleid.

De aannemer kan deze policies op eenvoudig verzoek verkrijgen en is geacht zich hieraan te houden. Om toegang te verkrijgen vanuit externe locatie zal een standaard aanvraagformulier moeten ingevuld worden.

Hoofdstuk 48 werd opgemaakt door Werkgroep 7

Voorzitter

Koen Wardenier

Secretaris

Karen De Winne

Leden van de werkgroep

Etienne Avaux, Josef Hennissen, Hans Bonte