Nieuwe Netwerkvoorzieningen Rijkswaterstaat

Aansluitvoorwaarden

Datum 24 maart 2015
Status Definitief

© 2015 RWS CIV. Alle rechten voorbehouden. Geen enkel deel van dit document mag worden vermenigvuldigd in welke vorm of door welke middelen dan ook zonder schriftelijke toestemming van DID. Dit document is vertrouwelijk en mag alleen worden gebruikt voor de doeleinden waarvoor het is vrijgegeven.

Nieuwe Netwerkvoorzieningen Rijkswaterstaat

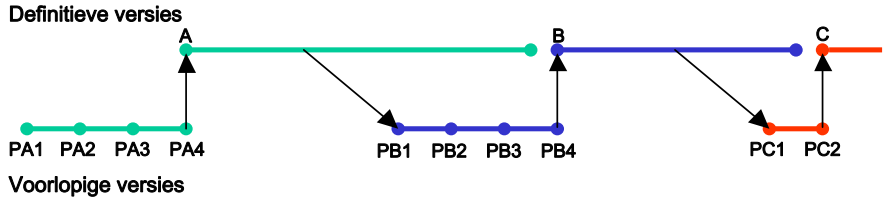
Aansluitvoorwaarden

Datum 24 maart 2015
Status Definitief

Colofon

Uitgegeven door	Productmanager Netwerken
Informatie	did-iap-gi-nti@rws.nl
Telefoon	
Fax	
Uitgevoerd door	RWS CIV IRN ICT Infra
Opmaak	Productmanager Netwerken
Datum	24-3-2015 15:31:00
Status	Definitief
Versienummer	E

Revisieschema



Revisiehistorie

Versie	Status	Datum	Auteur	Wijzigingen
A	Definitief	23-4-2007	Ir. M. de Bruyn	Accoord SM
B	Definitief	21-7-2008	Ir. M.F.E. Sibering	Naamswijziging DID Doorgevoerd
C	Definitief	11-5-2009	Ir. M.F.E. Sibering	Inclusie in PDC Nieuwe huisstijl
D	Definitief	2-5-2013	Ing. M. Klok	Toevoeging LAN
E	Definitief	16-12-2013	ir. M.A.A. Koolen	Toevoeging externe koppelingen, consolidatie met richtlijnen cybersecurity
E	Definitief	23 dec 2013	Ido Vlaminckx	Toevoeging bestaande LAN diensten, niet zijnde kantoorlocaties.
E	Definitief	24 maart 2015	ir M.P. van Wettum	Toevoeging trunking voor VOIP toestellen.

Datum van volgende revisie : jan 2016

Goedkeuring

Dit document vereist de volgende goedkeuringen. De getekende goedkeuringslijst wordt bewaard in het managementdossier.

Naam	Handtekening	Uitgiftedatum	Versie
Product manager		**24 mrt 2015**	E
Account Manager		**24 mrt 2015**	E

Distributielijst

Dit document is verspreid naar de volgende personen:

Naam	Uitgiftedatum	Versie
Product management	**24 mrt 2015**	E
Account management	**24 mrt 2015**	E
Service Management	**24 mrt 2015**	E

Inhoud

1 Inleiding 7
1.1 Doelstelling 7
1.2 Doelgroep 7
1.3 Voorkennis 7
1.4 Scope 7
1.4.1 Afbakening 7
1.4.2 Toepasselijkheid 7

2 Aansluitvoorwaarden NNV dienstverlening 8
2.1 Algemeen 8
2.2 Algemene aansluitvoorwaarden 9
2.3 Aansluitvoorwaarden “VPN aansluiting LAN” 10
2.3.1 Algemeen 12
2.3.2 OSI-laag 1 13
2.3.3 OSI-laag 2 14
2.3.3.1. VLANs 14
2.3.4 OSI-laag 3 15
2.3.5 Toegestaan verkeer 16
2.3.6 Toegestane IP unicast adressen 16
2.3.7 Toegestane IP multicast adressen 17
2.4 Aansluitvoorwaarden “LAN Aansluitingen” 18
2.4.1 Algemeen 18
2.4.2 OSI-laag 1 20
2.4.3 OSI-laag 2 22
2.4.3.1. VLANs 22
2.4.3.2. Trunking 22
2.4.4 OSI-laag 3 23
2.4.5 Toegestaan verkeer 24
2.4.6 Toegestane IP unicast adressen 24
2.4.7 Toegestane IP multicast adressen 25
2.5 Aansluitvoorwaarden “LAN Omgeving Draadloos” 25
2.5.1 Algemeen 26
2.5.2 OSI-laag 1 26
2.5.3 OSI-laag 2 26
2.5.4 OSI-laag 3 27
2.5.5 Toegestaan verkeer 27
2.6 Beveiliging 28
2.7 Beheer 29
2.8 Externe Toegang 29
2.8.1 Individuele Netwerktoegang door Derden 29
2.8.2 Locatie gebonden Netwerktoegang door Derden 29

Bijlage A NNV aansluitprocedure 30
A.1 Stap 1: Aanspreekpunt 30
A.2 Stap 2: Documentatie 30
A.3 Stap 3: Inventarisatie 30
A.4 Stap 4: Beveiliging en stabiliteit 30

A.5 Stap 5: Gereedmaken lokale situatie 30
A.6 Stap 6: Netwerk audit 30
A.7 Stap 7: Acceptatietest door NNV en afnemer 31
A.8 Optie 8: Acceptatietest: Fail 31

Bijlage B Checklist 32

Bijlage C Enkelvoudige aansluiting “VPN aansluiting LAN” 34

Bijlage D Redundante aansluiting “VPN aansluiting LAN” 36

Bijlage E Enkelvoudige aansluiting “VPN aansluiting LAN” + standaard “LAN omgeving bedraad” 39

Bijlage F Missiekritische aansluiting “VPN aansluiting LAN” + speciaal “LAN omgeving bedraad” 41

Bijlage Referenties 44

1 Inleiding

1.1 Doelstelling

Dit document geeft een gedetailleerde uitwerking van de voorwaarden waaronder het is toegestaan te worden aangesloten aan het NNV netwerk. Deze aansluitvoorwaarden hebben betrekking op de volgende producten:

1. VPN aansluiting LAN
2. LAN Omgeving Draadloos [WIFI]
3. LAN Aansluiting type Rekencentrum, -Gebouwen, -CVR/VOR en Weg-/ Waterkant
4. LAN omgeving bedraad t.b.v. gebouwen met kantoorfunctie

1.2 Doelgroep

De aansluitvoorwaarden zijn bestemd voor medewerkers van System Integrators (zowel interne als externe partijen die een rol spelen bij de aanbesteding, aanbieding, ontwerp, realisatie, beheer of audits van netwerkinfrastructuur) en Rijkswaterstaat organisatieonderdelen, die de NNV dienstverlening gebruiken als onderdeel van de eigen dienstverlening.

Dit document kan als bijlage worden bijgevoegd bij aanbestedingsdocumentatie[1].

1.3 Voorkennis

Dit document beschrijft netwerkdienstverlening. Kennis van netwerktechnologie wordt in beperkte mate bekend verondersteld.

1.4 Scope

1.4.1 Afbakening

De NNV aansluitvoorwaarden geven aan onder welke voorwaarden een koppeling mogelijk is met lokale netwerkdiensten en centraal aangeboden voorzieningen[2]. De invulling van deze netwerkdiensten en voorzieningen is afhankelijk van de betreffende klant[3].

1.4.2 Toepasselijkheid

Klantomgevingen die voldoen aan de NNV aansluitvoorwaarden worden binnen de in de PDC genoemde levertijd aangesloten op het NNV netwerk.

Klantomgevingen die niet voldoen aan de NNV aansluitvoorwaarden, maar toch wensen te worden aangesloten op NNV, vallen onder een speciaal traject. Hierbij kunnen afwijkingen plaatsvinden op o.a. prijs, servicevoorwaarden, doorlooptijden, benodigde (hard)- en software, etc.

[1] Onder een afnemer van NNV dienstverlening wordt verstaan een VPN eigena(a)r(ren) en een eventueel daarmee verbonden beheerorganisatie.
[2] Centrale netwerkdiensten worden in principe niet lokaal gehost, maar in een rekencentrum.
[3] De rechten van een eindgebruiker worden door de klant bepaald.

2 Aansluitvoorwaarden NNV dienstverlening

2.1 Algemeen

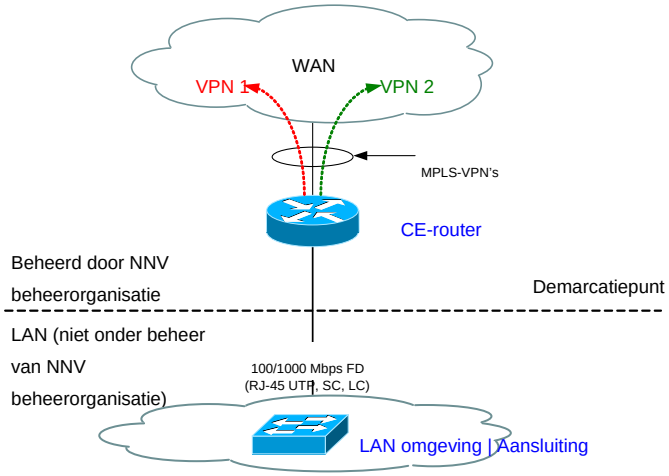
De NNV aansluitvoorwaarden maken deel uit van de Service Level Agreement (SLA) die zowel door de dienstverlener als de afnemer wordt ondertekend en nageleefd. Indien blijkt dat door de afnemer niet aan de aan haar gestelde voorwaarden wordt voldaan, heeft de dienstverlener de mogelijkheid om de dienstverlening op te schorten.

De NNV dienstverlening voorziet in de volgende typen aansluitingen:

- NNV WAN op basis van de bouwsteen “VPN aansluiting LAN”
- NNV LAN Aansluiting op basis van de bouwstenen:
  1. “LAN Omgeving Draadloos (WIFI)
  2. “LAN Omgeving Bedraad” (RWS locaties met Kantoorfunctie)
  3. “LAN Aansluiting type Rekencentrum, -Gebouwen, -CVR/VOR en Weg-/ Waterkant”

Op Rijkswaterstaat locaties, waarbij het lokale LAN wordt beheerd door een externe partij, anders dan de NNV beheerorganisaties, kan een “VPN aansluiting LAN” worden aangevraagd.

In onderstaande afbeelding is het product “VPN aansluiting LAN” te zien, waarbij het demarcatiepunt tussen de NNV dienstverlener en de afnemer ligt op de interface tussen de WAN router en de LAN switch.

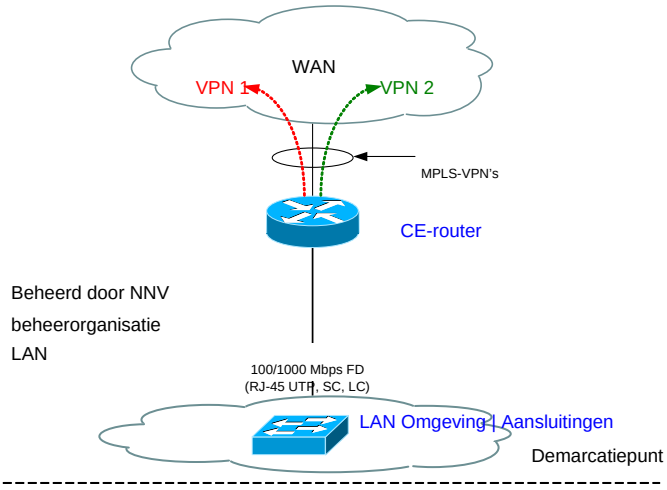


Figuur 1: Functiescheiding op locatie op basis van alleen een “VPN aansluiting LAN”

Alle LAN’s binnen RWS zijn onder beheer gebracht van de outsourcingspartner netwerken van RWS, zijnde KPN CT-RWS (NNV Beheer), tenzij het een contractuele demarcatie betreft, waarbij het LAN door derden wordt onderhouden.

Als er op een Rijkswaterstaat locatie een LAN wordt ontsloten dat ook door de NNV beheerorganisatie wordt beheerd, zal dit zijn gebaseerd op de bouwstenen “VPN aansluiting LAN” en de eerder genoemde LAN vormen

In onderstaande afbeelding zijn de producten “VPN aansluiting LAN” en “LAN Aansluiting” te zien, waarbij het demarcatiepunt tussen de WAN- en LAN dienstverlening zichtbaar is gemaakt.



Figuur 2: Functiescheiding op locatie op basis van een “VPN aansluiting LAN” en “LAN”

De volgende twee paragrafen behandelen de aansluitvoorwaarden voor de bouwstenen “VPN aansluiting LAN” en “LAN” in haar diverse uitvoeringsvormen.

2.2 Algemene aansluitvoorwaarden

Er dienen voor de bouwstenen “VPN aansluiting LAN” en “LAN Aansluiting” voorzieningen te worden getroffen zodat WAN netwerkcomponenten van NNV in afgesloten stalen systeemkasten kunnen worden geplaatst. Deze kasten dienen 19” rack formaat te ondersteunen, voorzien te zijn van voldoende ventilatie, aarding vanaf een centraal aardpunt en van 230V 50 Hz wisselspanning aansluiting, zoals gedefinieerd in NEN1010.

In het geval van een redundante NNV “VPN aansluiting LAN” dient deze in twee kasten te worden ondergebracht. Beide kasten dienen voorzien te zijn van twee spanningsgroepen. Tussen de kasten moet een single mode glasvezelkabel met een lengte van minimaal 10 meter aanwezig zijn. Deze moet door de klant worden geleverd.

De NNV netwerkcomponenten dienen voor een storingsvrije werking te worden geplaatst in ruimtes die binnen extreme waardes vallen volgens ETSI norm 300 019-1-3 class 3.1 (stationair gebruik in een gesloten ruimte die beschermd is tegen externe weersomstandigheden met permanente temperatuurcontrole). De volgende zaken zijn hierbij o.a. van belang:

- Voor luchtvochtigheid i.c.m. omgevingstemperatuur gelden de volgende waardes.
    - Voor een relatieve vochtigheid tussen 10 en 50% dient de omgevingstemperatuur tussen de 10 en 40°C te liggen
    - Voor een relatieve vochtigheid tussen 50 en 85% dient de omgevingstemperatuur tussen de 10 en 30°C te liggen.
- Het stofgehalte mag de volgende waarden niet overschrijden.
    - stofdeeltjes < 10 micron: 10-100 microgr./m^3
    - stofdeeltjes > 10 micron: 20-200 microgr./m^3
- De afnemer dient alle voorzorgen te nemen om waterspatten te vermijden;
- De NNV componenten mogen niet rechtstreeks worden blootgesteld aan zonnestralen;
- etc.

Ruimtes waarin NNV netwerkcomponenten worden geplaatst dienen te zijn voorzien van een locatie-aanduiding t.b.v. referentie.

De afnemer is verantwoordelijk voor het patchen, en het onderhouden van de fysieke infrastructuur en de computerruimtes, tenzij expliciet anders overeengekomen.

2.3 Aansluitvoorwaarden “VPN aansluiting LAN”

Een klantomgeving in de vorm van een LAN wordt via de dienst “VPN aansluiting LAN” aangesloten op het NNV backbone (WAN) netwerk. Deze “VPN aansluiting LAN” dienst is voor de klant op maat gemaakt door het vaststellen en vastzetten van optiewaarden en het geven van een eigen naam in de PDC van de klant.

De NNV dienstverlening via een “VPN aansluiting LAN” wordt geleverd op NNV WAN apparatuur op de klantlocatie. Dit worden Customer-Edge routers (CE-router) genoemd. Op een CE-router zijn één of meerdere LAN switches aangesloten, afhankelijk van de grootte en type van een klantlocatie. Als deze switches onder beheer vallen van de NNV dienstverlener, dan gebeurt dit in de vorm van een aanvraag van een van de bouwstenen:

1. “LAN Omgeving Draadloos (WIFI) (via de LAN Omgeving Bedraad)
2. “LAN Omgeving Bedraad” (RWS locaties met Kantoorfunctie)
3. “LAN Aansluiting type Rekencentrum, -Gebouwen, -CVR/VOR en Weg-/ Waterkant”

De CE-router levert IPv4 gebaseerde OSI-laag 3 netwerkfunctionaliteit, waarbij NNV de achterliggende infrastructuur als een OSI-laag 2 (LAN) netwerk aanbiedt. Het is niet toegestaan dat klantnetwerken naast de CE router ook nog eigen routers hebben aangesloten op het LAN, omdat routering en verkeersscheiding worden afgehandeld door de CE-router. Op deze wijze wordt een beveiligingspolicy centraal beheerd en afgedwongen.

De structuur van NNV VPNs (Virtual Private Networks) wordt doorgetrokken naar de aangesloten LAN infrastructuur. Hierbij wordt per VPN één of meer VLANs (Virtual LAN) gebruikt die op de CE-router worden gekoppeld aan een NNV VPN. Zowel op laag 2 als laag 3 blijven de verkeersstromen gescheiden.

Vanuit het oogpunt van beheerbaarheid wordt er door de NNV beheerorganisatie naar gestreefd dat de VLAN-IDs op alle locaties gelijk zijn. Gebruikers die logisch onderdeel uitmaken van een VPN worden geplaatst in een bijbehorend VLAN. Dit is weergegeven in Figuur 3.

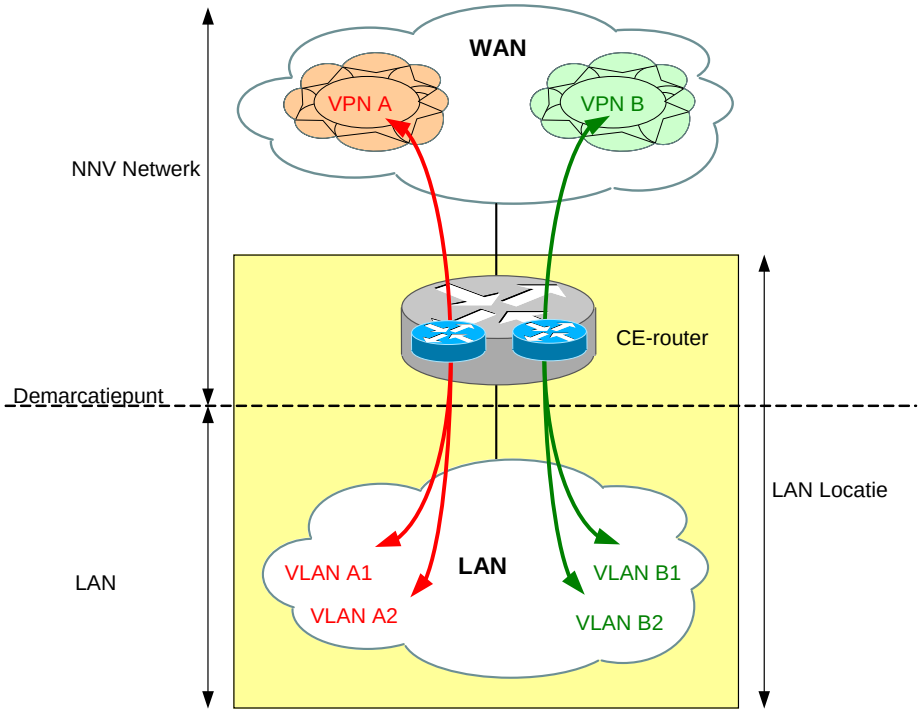
Er wordt een viertal type NNV WAN aansluitingen ondersteund voor het koppelen van het bijbehorende LAN op een locatie, te weten:

- **enkelvoudig**: Een enkelvoudige ontsluiting bestaat uit één CE-router die een enkele koppeling onderhoudt met de rest van het NNV netwerk (beschikbaarheid van 99,5%. Het koppelvlak met het LAN bestaat dan uit één fysieke interface (zie ook Bijlage C).

- **dubbel**: Een dubbelvoudige ontsluiting bestaat uit één CE-router die dubbele koppeling onderhoudt met de rest van het NNV netwerk (beschikbaarheid van 99,8%). Het koppelvlak met het LAN bestaat dan uit één fysieke interface (zie ook Bijlage C).

- **redundant**: Een redundante ontsluiting bestaat uit twee CE-routers die elk een eigen koppeling met de rest van het NNV netwerk onderhouden. Deze oplossing biedt een koppelvlak bestaande uit twee fysieke interfaces, te weten één interface per CE-router. Hierdoor kan aan het LAN een hogere beschikbaarheid worden geboden (zie ook Bijlage D).

- **missiekritisch**: Een missiekritische ontsluiting bestaat uit twee CE-routers die elk een eigen koppeling met een aparte PE router op het NNV netwerk onderhoudt. Deze oplossing biedt een koppelvlak bestaande uit twee fysieke interfaces, te weten één interface per CE-router. Hierdoor kan aan het LAN een hogere beschikbaarheid worden geboden (zie ook Bijlage D).



Figuur 3: Functiescheiding op LAN locatie

In de volgende paragrafen worden de specifieke voorwaarden weergegeven waaraan de aansluitingen op de “VPN Aansluiting LAN” zullen moeten voldoen. Hierbij worden de volgende aspecten per paragraaf behandeld:

- Algemeen
- OSI-laag 1
- OSI-laag 2
- OSI-laag 3

2.3.1 Algemeen

De NNV aansluitvoorwaarden maken deel uit van de Service Level Agreement (SLA) die zowel door de dienstverlener als de afnemer wordt ondertekend en nageleefd. Indien blijkt dat door de afnemer niet aan de aan haar gestelde voorwaarden wordt voldaan, heeft de dienstverlener de mogelijkheid om de dienstverlening op te schorten.

De afnemer dient aan de NNV beheerorganisatie kenbaar te maken wat de totale benodigde bandbreedte voor het VPN dient te zijn (afgesproken bandbreedte). De NNV beheerorganisatie kiest daar vervolgens een passende drager bij. Het is daarbij mogelijk dat meerdere klanten van dezelfde drager gebruik maken. Hierdoor kan efficiënt van bandbreedte gebruik gemaakt worden en kan in uitzonderlijke gevallen en indien ongebruikt door andere klanten, tijdelijk meer bandbreedte worden geboden dan initieel afgesproken. Statistisch is de kans dat partijen die een verbinding delen elkaar negatief beïnvloeden uitermate klein.

Aangesloten systemen (en daarop draaiende operating systemen [OS] en applicaties) dienen zodanig geconfigureerd en *hardened* te zijn dat zij geen onnodige netwerkbelasting veroorzaken in de vorm van broadcast verkeer of andere netwerkbevuiling.
Het is niet toegestaan om op de routers t.b.v. “VPN aansluiting LAN” routers en Wifi Access-points aan te sluiten die niet door de NNV beheerorganisatie worden beheerd. Het is tevens niet toegestaan om op de switches, die niet door de NNV organisatie worden beheerd, andere routers en Wifi-access points aan te sluiten. Voort is het niet toegestaan dat er werkstations en/of laptops worden aangesloten op de routers en/of switches als deze niet door een Rijkswaterstaat beheerorganisatie of andere door Rijkswaterstaat onderkende beheerpartij worden beheerd.

Indien vreemd of onnodig verkeer wordt geconstateerd, heeft de NNV beheerorganisatie het recht om de verbinding met onmiddellijke ingang op te schorten om de dienstverlening naar andere klanten niet in gevaar te brengen, zulks ter beoordeling van de NNV beheerorganisatie.

2.3.2 OSI-laag 1

Bij een redundante “VPN aansluiting LAN” dienen de bijbehorende NNV componenten verdeeld te zijn over verschillende MER’s (Main Equipment Rooms). Alleen indien een locatie niet de beschikking heeft over gescheiden MER ruimtes kunnen NNV componenten in dezelfde MER worden geplaatst. De geboden beschikbaarheid wordt dan negatief bijgesteld.

Bij een redundante “VPN aansluiting LAN” dienen de bijbehorende NNV componenten in verschillende kasten in verschillende computerruimtes te worden geplaatst. Hierbij dient er minimaal 10 meter tussen beide kasten aanwezig te zijn.

Een redundante “VPN aansluiting LAN” dient op fysiek gescheiden LAN componenten te worden ontsloten. Deze LAN componenten maken onderdeel uit van dezelfde redundante OSI-laag 2 infrastructuur die onafhankelijk is van de OSI-laag 3 infrastructuur.

Voor het koppelen van een LAN omgeving aan “VPN aansluiting LAN” kan van de volgende typen aansluitingen gebruik worden gemaakt:

- 10 GE en Gigabit Ethernet over RJ45
- 10GBASE-SR over MMF / OM3
- 1000Base-[SX, LX] over LC/PC multimode

De gebouwenbekabeling is gespecificeerd volgens de volgende richtlijn:

De voorzieningen moeten voldoen aan het Handboek ICT-huisvesting en Bekabeling (HIB) versie 1.0 van de Rijksgebouwendienst. Het handboek is te downloaden vanaf de website van de Rijksgebouwendienst:
http://www.rgd.nl/zoeken/?tx_solr%5Bq%5D=Handboek%20ICT-huisvesting%20en%20Bekabeling%20%28HIB%29%20versie%201.0%20van%20de%20Rijksgebouwendienst

De bekabeling dient aangelegd te worden met goedkeuring van de gebouweigenaar. De toegepaste type glasvezelbekabeling en gebruikte connectoren (LC/PC) dienen afgestemd te zijn met de NNV beheerorganisatie.

2.3.3 OSI-laag 2

De afnemer dient interfaces waarop NNV componenten worden aangesloten zodanig te configureren dat bij het actief worden van de interface het spanning tree protocol (STP) op de betreffende interface direct van blocking mode over gaat naar forwarding mode.

Het NNV koppelvlak tussen een NNV WAN router en een LAN switch (wel of geen NNV) is een trunk-verbinding op basis van 802.1Q.

Een VLAN kan slechts aan één VPN worden toegewezen. Het is daarbij mogelijk om meerdere VLANs aan één VPN toe te wijzen.

De NNV leverancier maakt aan de afnemer kenbaar welke VLANs er op welke LAN poorten van de NNV router beschikbaar zijn voor het aansluiten van LAN apparatuur. Deze VLANs kunnen niet ter beschikking staan voor LAN beheer doeleinden en mogen door de afnemer enkel op access-poorten worden geconfigureerd. De betreffende VLANs dienen daarvoor op trunk-verbindingen tussen de NNV WAN router en de LAN switch(es) te worden doorgelaten.
Voor het beheer van een LAN switch zal een separaat VLAN worden gebruikt dat niet ter beschikking mag worden gesteld als access-poorten op een NNV LAN switch.

NNV maakt aan de afnemer van het LAN kenbaar welke VLANs (lees: VLAN-ID) en volgens welke indeling deze gebruikt kunnen worden op het LAN. Hieronder vallen zowel isolated en non-isolated VLANs.

Ter bescherming van de router, die voor de ontsluiting van de “VPN aansluiting LAN” zorgt, en het achterliggende netwerk infrastructuur dienen door de afnemer de volgende laag 2 maatregelen op de eigen switch omgeving te worden genomen:

- VLAN filtering op basis van MAC filtering
- RSTP of MSTP
- UDLD

Indien door vreemd verkeer door de NNV beheerorganisatie wordt geconstateerd dat bovengenoemde laag 2 maatregelen niet door de afnemer zijn geïmplementeerd, heeft de NNV beheerorganisatie het recht om de verbinding met onmiddellijke ingang op te schorten om de dienstverlening naar andere klanten niet in gevaar te brengen, zulks te beoordeling van de NNV beheerorganisatie.

2.3.3.1. VLANs

Indien wordt gekozen voor het toepassen van een trunk met daarin op 802.1q gebaseerde virtuele LANs (VLANs), zijn de VLAN ranges niet vrij te kiezen. De beschikbare VLANs per VPN zijn bij het configureren van het VPN vastgelegd.

Er zijn standaard 10 VLANs per VPN beschikbaar.

Indien noodzakelijk kunnen aanvullende VLAN ranges beschikbaar worden gesteld.

2.3.4 OSI-laag 3

NNV levert voor het LAN OSI-laag 3 functionaliteit op basis van het IPv4 protocol en in de toekomst tevens op basis van het IPv6 protocol. Hiervoor levert NNV voor elk LAN IP subnet een default gateway. Voor het correct functioneren is er een aantal IP adressen per LAN subnet gereserveerd t.b.v. het NNV netwerk. Deze gereserveerde IP adressen worden door NNV aan de afnemer bekend gemaakt. Het is voor de afnemer niet toegestaan deze IP adressen voor eigen gebruik in te zetten.

Per VLAN is slechts één IP subnet actief. Er zal geen overlap van een IP subnet over verschillende VPN's worden geboden.

Ieder aan te sluiten IP subnet op een LAN dient uniek te zijn binnen het gehele VPN, m.a.w. het IP subnet mag niet op andere locaties voorkomen die ook op hetzelfde VPN zijn aangesloten. Het is mogelijk om hetzelfde IP subnet te gebruiken binnen verschillende VPNs[4].

Het is op het aangesloten LAN niet toegestaan om een gerouteerde verbinding tussen IP segmenten te creëren. Een aansluiting op het LAN mag dan ook slechts op één segment worden aangesloten. Inter VLAN routering binnen de locatie, zonder tussenkomst van de NNV WAN router(s) wordt wel toegestaan voor routering van het verkeer van en naar (blade)servers die zich in de MER bevinden, mits de bijbehorende VLAN's tot hetzelfde VPN behoren.

Bij de toepassing van meerdere VLAN's toebehorend aan één VPN vindt de routering tussen deze VLAN's via de router van de locatie ontsluiting plaats (de router t.b.v. de "VPN LAN aansluiting"), zonder tussenkomst van de routeringsfunctionaliteit in de Centrale Voorzieningen.
Indien er tussen VPN's moet worden gerouteerd, moet er wel gebruik worden gemaakt van de routeringsfunctionaliteit binnen de Centrale Voorzieningen, aangevuld met firewall ruling.

Bijgaande networkservices worden per VPN geboden en mogen worden afgenomen. Als dergelijke diensten nodig zijn, dienen ze vanuit NNV te worden afgenomen.

- DHCP
- DNS
- NTP
- Internet Access
- Extranet Access (site 2 site toegang op basis van vaste externe toegang)
- Remote Access Service (indivuele toegang op basis van een verstrekt token)

Op alle NNV VPN's is de NNV beheerorganisatie verantwoordelijk voor de uitgifte van IP subnetten. De afnemer dient voor deze segmenten bij de NNV beheerorganisatie een IP subnet aan te vragen o.b.v. van een aanvraag PDC dienst. De afnemer dient daarbij aan de NNV beheerorganisatie kenbaar te maken voor welk LAN deze

[4] Het gebruik van dezelfde IP adressen op verschillende VPNs heeft tot gevolg dat het verkeer tussen VPNs wordt beperkt of dat er extra NAT maatregelen noodzakelijk zijn. Er dient daarom gebruik te worden gemaakt van uniek geregistreerde IP adressen.

bedoeld is en voor welk VPN. Voor LAN segmenten behorend tot andere VPNs dient de afnemer aan de NNV beheerorganisatie kenbaar te maken welke IP subnetten hiervoor worden gebruikt en zelf zijn gereserveerd.

De afnemer dient per VPN vooraf aan de NNV beheerorganisatie kenbaar te maken of Quality-of-Service (QoS) m.b.t. IP verkeer noodzakelijk is (dit gebeurt bij het aanvragen of wijzigen van het VPN PDC item). Hiertoe zal de NNV beheerorganisatie aan de afnemer kenbaar maken welke QoS modellen er door de NNV beheerorganisatie worden geboden. De afnemer dient vervolgens aan te geven welk QoS model er dient te worden gehanteerd, en welk type IP verkeer in welke klasse dient te worden ondergebracht. Bij voorkeur vindt de QoS markering van het verkeer plaats door de applicatie of het LAN. QoS zal vervolgens globaal worden uitgerold voor de afnemer.

Indien de afnemer gebruik wenst te maken van QoS en het LAN of eindapplicatie geen markering ondersteunt, zal deze functionaliteit door de CE-router worden geboden (op vLAN/ IP reeks/IP nummer of poort niveau)

2.3.5 Toegestaan verkeer

De NNV VPN dienst is bedoeld voor IP versie 4 verkeer conform rfc 791 [i]. In de toekomst zal ook IP versie 6 verkeer worden ondersteund.

Om de integriteit van het netwerk te beschermen zijn de volgende verkeerssoorten niet toegestaan:

- ICMP redirects
- ICMP unreachables
- ICMP mask request/reply
- IP directed broadcast
- Proxy arp

Indien bovenstaande verkeerssoorten door de NNV beheerorganisatie worden gedetecteerd, kan als maatregel de dienstverlening voor de betreffende dienst worden opgeschort.
Aanvullende maatregelen kunnen worden genomen naarmate de beveiliging dit vereist. In dat geval zal dit document worden aangepast.

2.3.6 Toegestane IP unicast adressen

Martian IP adres space zoals gedefinieerd in rfc 3330 [ii] is niet toegestaan voor subnetten die door de gebruiker zelf worden aangedragen, met uitzondering van de volgende IP adresreeksen zoals gedefinieerd in rfc1918 [iii]:

- 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

Een aantal IP subnetten is gereserveerd voor intern NNV gebruik. Een dubbel gebruik van deze IP subnetten leidt tot routeringconflicten op het NNV netwerk. Dit geldt voor alle over NNV gedefinieerde VPNs. Om deze reden is het niet toegestaan om de volgende IP subnetten op routeerbare LAN segmenten te gebruiken:

- 10.x.0.0 /24
- 10.x.128.0 /24
- 10.x.253.0 /24
- 10.x.254.0 /24

RWS IP hosts dienen bij voorkeur gebruik te maken van de hierboven aangegeven private address space. Voor toegang van systemen in een RWS VPN tot het Internet wordt in de NNV Centrale Voorzieningen - Internet dienst [iv] Netwerk Adres Translatie (NAT) toegepast op een voor de gebruiker transparante manier. Voor RWS systemen die vanaf het Internet bereikbaar moeten zijn, is de NNV Centrale Voorzieningen - DMZ [v] dienstverlening beschikbaar. In deze dienst wordt uit de publieke adresruimte die aan Rijkswaterstaat is toegewezen, ruimte gereserveerd voor proxies die toegang geven tot deze systemen.

2.3.7 Toegestane IP multicast adressen

Er kan alleen gebruik van Source Specific (SSM) of limited scope adressen worden gemaakt.

Dit betekent dat alleen IP multicast verkeer met destination adressen uit de onderstaande range zijn toegestaan en door de afnemer van de dienst kunnen worden gebruikt:

- 232.0.0.0 – 232.255.255.255
- 239.0.0.0 – 239.255.255.255

De source adressen van IP multicast verkeer dienen te voldoen aan de regels voor IP unicast verkeer.

2.4 Aansluitvoorwaarden “LAN Aansluitingen”

De LAN dienstverlening van NNV bestaat uit:

1. NNV LAN Omgeving Bedraad
2. NNV LAN Omgeving Draadloos
3. NNV LAN Aansluiting type Rekencentrum, -Gebouw, -CVR/VOR en –Weg-/Waterkant

In de volgende paragrafen worden de voor deze type LAN’s de aansluitvoorwaarden beschreven.

Er wordt een tweetal type NNV RWS LAN aansluitingen ondersteund voor het koppelen van eindapparaten via de genoemde LAN producten. te weten:

- **standaard**: Een standaard ontsluiting bestaat uit een koppeling tussen een eindapparaat en NNV via één NNV LAN switch, die op zijn beurt een enkele of dubbele koppeling onderhoudt met de rest van het NNV netwerk via een VPN aansluiting LAN koppeling. Het koppelvlak tussen het eindapparaat met de LAN omgeving bestaat dan uit één fysieke interface. De beschikbaarheid van deze standaard LAN aansluiting is 99,5%. (Zie ook Bijlage E).

- **Redundant**: Een speciale ontsluiting bestaat uit twee koppelingen tussen een eindapparaat en NNV via twee NNV LAN switches, die op hun beurt elk een eigen koppeling met de rest van het NNV netwerk onderhouden via een VPN aansluiting LAN koppeling. Deze oplossing biedt een koppelvlak bestaande uit twee fysieke interfaces, te weten één interface per NNV LAN switch. Hierdoor kan aan het LAN een hogere beschikbaarheid aan NNV dienstverlening worden geboden aan servers en blade servers in MER’s (Main Equipment Rooms) met een beschikbaarheid van 99,95% (Zie ook Bijlage F).

In de volgende paragrafen worden de specifieke voorwaarden weergegeven waaraan de omgeving zal moeten voldoen. Hierbij worden de volgende aspecten per paragraaf behandeld:

- Algemeen
- OSI-laag 1
- OSI-laag 2
- OSI-laag 3

2.4.1 Algemeen

De NNV aansluitvoorwaarden maken deel uit van de Service Level Agreement (SLA) die zowel door de dienstverlener als de afnemer wordt ondertekend en nageleefd. Indien blijkt dat door de afnemer niet aan de aan haar gestelde voorwaarden wordt voldaan, heeft de dienstverlener de mogelijkheid om de dienstverlening op te schorten.

Aangesloten systemen (en daarop draaiende operating systemen [OS] en applicaties) dienen zodanig geconfigureerd en *hardened* te zijn dat zij geen

onnodige netwerkbelasting veroorzaken in de vorm van broadcast verkeer of andere netwerkbevuiling. Het is eveneens niet toegestaan om op de switches t.b.v. “LAN omgeving bedraad” andere, niet door de NNV beheerorganisatie beheerde switches, routers en Wifi Access-points aan te sluiten.
Voort is het niet toegestaan dat er werkstations en/of laptops worden aangesloten op de routers en/of switches als deze niet door een Rijkswaterstaat beheerorganisatie of andere door Rijkswaterstaat onderkende beheerpartij worden beheerd.

Indien vreemd of onnodig verkeer wordt geconstateerd, heeft de NNV beheerorganisatie het recht om de verbinding met onmiddellijke ingang op te schorten om de dienstverlening naar andere klanten niet in gevaar te brengen, zulks ter beoordeling van de NNV beheerorganisatie.

Bekabeling toegepast voor Weg- en Waterkant LANs zijn gespecificeerd in de daarvoor opgestelde documenten, zijnde:

<u>Aanleg en verleggingen RWS glasvezelinfrastructuur</u>

- Montage Specificaties Aanleg Glasvezelkabelnetwerk
- Specificaties Documentatie RWS datanetwerken
- Impact Analyse Gepland werk aan RWS Glasvezelinfrastructuur

Los van de normale eisen die RWS stelt tav tekeningen e.d. (zie K&L binnen Werkwijze Aanleg)

<u>Aanleg en Wijziging wegkantgebonden PDC Items</u>

Voor wegkantgebonden PDC items zijn PDC items die veelal geconfigureerd door KPN CT-RWS aan ON worden aangeleverd en door de ON worden geïnstalleerd. PDC items waarvoor dat betreft zijn:

1. Wegkant LAN aansluiting,
2. Analoge camera aansluiting en
3. Draadloze VPN aansluiting

Hiervoor zijn de volgende documenten en richtlijnen van toepassing:

1. Projecteringsrichtlijnen RWS Datanetwerken en
2. Montage specificatie Wegkant LAN Aansluitingen
3. Montage specificatie Analoge Camera Aansluiting en
4. Montage specificatie Draadloze VPN aansluiting

2.4.2 OSI-laag 1

Bij redundant "LAN's dienen de bijbehorende LAN componenten verdeeld te zijn over verschillende MER's (Main Equipment Rooms) en eventueel SER's. Alleen indien een locatie niet de beschikking heeft over gescheiden MER en SER ruimtes kunnen de LAN componenten in dezelfde MER worden geplaatst. De geboden beschikbaarheid wordt dan negatief bijgesteld.

De kasten dienen hierbij minimaal 10 meter van elkaar gescheiden te zijn.

De LAN componenten binnen een "LAN" maken onderdeel uit van dezelfde redundante OSI-laag 2 infrastructuur die onafhankelijk is van de OSI-laag 3 infrastructuur.

<u>LAN Omgeving bedraad</u>

Op de aansluitingen van de switches t.b.v. "LAN omgeving bedraad"kunnen de volgende typen eindapparatuur worden aangesloten:

- Rijkswaterstaat desktops/laptops, op basis van 10/100/1000Base-T, full- of half-duplex, RJ45
- Rijkswaterstaat High Performance deskstops op basis van 1000Base-X, RJ45 of LC/PC multimode glasvezel
- Servers en bladeservers in de MER op basis van 1000Base-SX, LC/PC multimode glasvezel
- VoIP telefoontoestellen
- Power injectors t.b.v. het voeden van VoIP telefoontoestellen en/of Wifi Accesspoints
- WiFi AccessPoints, die door de NNV beheerorganisatie worden beheerd

Voor de bovengenoemde eindapparatuur zal de NNV beheerorganisatie de poorten op de switches voor de "LAN omgeving bedraad" configureren als "access" poort. Het is niet toegestaan om andere apparaten anders dan bovengenoemd, of niet onder beheer van de NNV beheerorganisatie vallend, aan te sluiten op de switches voor "LAN omgeving bedraad". Ter bescherming van het NNV netwerk kan Network Admission Control (NAC) op basis van het 802.1X en EAP protocol op deze access-poorten zijn toegepast. Aangesloten apparatuur, die niet door het Network Admission Control protocol wordt herkend, zal dan geen of beperkte toegang tot het NNV netwerk krijgen.

De beschikbaarheid van bepaalde functies en koppelvlakken is gebaseerd op de volgende 4 typen RWS LAN's:

- Kleine locatie
- Middelgrote locatie
- Grote locatie
- Campus locatie (combinatie van vorige typen)

Voor een **kleine locatie** zijn de volgende typen LAN aansluitingen te verkrijgen:

- 10/100 Base-T LAN poorten t.b.v. Rijkswaterstaat desktops en laptops

Een **kleine locatie** levert aan de aangesloten eindapparatuur een beschikbaarheid, die is gebaseerd op een standaard "LAN omgeving bedraad", namelijk 99,5%.

Voor een **middelgrote locatie** zijn de volgende typen LAN aansluitingen te verkrijgen:

- 10/100 Base-T full- [half] duplex LAN aansluitingen t.b.v. Rijkswaterstaat desktops en laptops
- Enkele 1000 Base-T full- [half] duplex aansluitingen t.b.v. desktops
- Enkele 1000 Base-SX aansluitingen t.b.v. servers in de MER

Een **middelgrote locatie** levert aan de aangesloten eindapparatuur een beschikbaarheid, die is gebaseerd op een standaard “LAN omgeving bedraad”, namelijk 99,5% of een speciaal “LAN omgeving bedraad” variant, met een beschikbaarheid van 99,95%.

Voor een **grote locatie** zijn de volgende typen LAN aansluitingen te verkrijgen:

- 10/100 Base-T full- [half] duplex LAN aansluitingen t.b.v. Rijkswaterstaat desktops/laptops
- Meerdere 1000 Base-T full- [half] duplex aansluitingen t.b.v. desktops
- Meerdere 1000 Base-SX aansluitingen t.b.v. servers en bladeservers in de MER

Een **grote locatie** levert aan de aangesloten eindapparatuur een beschikbaarheid, die is gebaseerd op een standaard “LAN omgeving bedraad”, namelijk 99,5% of een speciaal “LAN omgeving bedraad” variant, met een beschikbaarheid van 99,95%.

De bekabeling is gespecificeerd volgens de volgende richtlijn:

De voorzieningen moeten voldoen aan het Handboek ICT-huisvesting en Bekabeling (HIB) versie 1.0 van de Rijksgebouwendienst [vi].

De bekabeling dient aangelegd te worden met goedkeuring van de gebouweigenaar. De toegepaste type glasvezelbekabeling en gebruikte connectoren (LC/PC) dienen afgestemd te zijn met de NNV beheerorganisatie.

<u>LAN Aansluitingen type Rekencentrum, en - Gebouw</u>

Hiervoor gelden de aansluitvoorwaarden zoals beschreven in de onderhavige PDC’s. Aanvullend geldt dat niet actieve LAN poorten worden gesloten.

Voor wat betreft bekabeling en kasten geldt hetzelfde als hiervoor beschreven.

LAN Aansluitingen type Weg- en Waterkant en type CVR/VOR
Hiervoor gelden de aansluitvoorwaarden zoals beschreven in de onderhavige PDC’s. Aanvullend geldt dat niet actieve LAN poorten worden gesloten.

Voor bekabeling en kasten gelden de specificaties zoals genoemd in paragraaf 2.4.1

2.4.3 OSI-laag 2

Ter bescherming van de infrastructuur voor de “LAN’s” zullen door de NNV beheerorganisatie de volgende maatregelen worden genomen op de access-poorten:

- MAC filtering
- RSTP of MSTP
- UDLD
- BPDU Guard

Indien op grond van bovengenoemde maatregelen vreemd of onnodig verkeer door de NNV beheerorganisatie wordt geconstateerd, heeft de NNV beheerorganisatie het recht om de verbinding met onmiddellijke ingang op te schorten om de dienstverlening naar andere klanten niet in gevaar te brengen, zulks ter beoordeling van de NNV beheerorganisatie.

Een VLAN kan slechts aan één VPN worden toegewezen. Het is daarbij mogelijk om meerdere VLANs aan één VPN toe te wijzen.

De NNV beheerorganisatie maakt aan de afnemer kenbaar welke VLANs er op welke LAN poorten van de NNV router beschikbaar zijn voor het aansluiten van LAN apparatuur. Deze VLANs kunnen niet ter beschikking staan voor LAN beheer doeleinden door de NNV beheerorganisatie en mogen door de afnemer enkel op access-poorten worden geconfigureerd. De betreffende VLANs dienen daarvoor door de NNV beheerorganisatie op trunk-verbindingen tussen de NNV WAN router en de LAN switch(es) te worden doorgelaten.
Voor het beheer van een LAN switch zal een gescheiden VLAN worden gebruikt dat niet ter beschikking mag worden gesteld als access-poorten op een NNV LAN switch.

NNV maakt aan de afnemer van het LAN kenbaar welke VLANs (lees: VLAN-ID) en volgens welke indeling deze gebruikt kunnen worden op het LAN. Hieronder vallen zowel isolated en non-isolated VLANs.

2.4.3.1. VLANs

Indien wordt gekozen voor het toepassen van een trunk met daarin op 802.1q gebaseerde virtuele LANs (VLANs), zijn de VLAN ranges niet vrij te kiezen. De beschikbare VLANs per VPN zijn bij het configureren van het VPN vastgelegd.

Er zijn standaard 10 VLANs per VPN beschikbaar.

Indien noodzakelijk kunnen aanvullende VLAN ranges beschikbaar worden gesteld.

2.4.3.2. Trunking

Trunking op basis van 802.1q met VLAN tags kan vanuit de Bouwstenen “LAN Omgeving bedraad”, LAN Aansluitingen type Gebouw en type Rekencentrum uitsluitend worden toegepast naar:

- Server aansluitingen
- Switch uplink aansluitingen
- VOIP telefoontoestellen

Alle VLAN's binnen een trunk naar een server dienen toe te behoren uitsluitend één VPN.

Aanvullend geldt:
LAN Aansluitingen type Weg- en Waterkant zijn bedoeld om einddevices aan te sluiten en daarom is Sticky MAC Address filtering van toepassing. Alleen met een exceptie is het mogelijk hierop uit te zonderen. Niet gebruikte LAN poorten zijn gesloten.

LAN Aansluitingen type CVR/VOR zijn bedoeld of om enddevices aan te sluiten of om LAN's type Weg- en Waterkant aan te sluiten conform de PDC Netwerken.
Niet gebruikte LAN poorten zijn gesloten.

2.4.4 OSI-laag 3

De NNV beheerorganisatie levert voor het LAN OSI-laag 3 functionaliteit op basis van het IPv4 protocol en in de toekomst tevens op basis van het IPv6 protocol. Hiervoor levert de NNV beheerorganisatie voor elk LAN IP subnet een default gateway. Voor het correct functioneren is er een aantal IP adressen per LAN subnet gereserveerd t.b.v. NNV. Deze gereserveerde IP adressen worden door de NNV beheerorganisatie aan de afnemer bekend gemaakt. Het is voor de afnemer niet toegestaan deze IP adressen voor eigen gebruik in te zetten.

Per VLAN is slechts één IP subnet actief. Er zal geen overlap van een IP subnet over verschillende VPN's worden geboden.

Ieder aan te sluiten IP subnet op een LAN dient uniek te zijn binnen het gehele VPN, m.a.w. het IP subnet mag niet op andere locaties voorkomen die ook op hetzelfde VPN zijn aangesloten. Het is mogelijk om hetzelfde IP subnet te gebruiken binnen verschillende VPNs[5].

Het is op het aangesloten LAN niet toegestaan om een gerouteerde verbinding tussen IP segmenten te creëren. Een aansluiting op het LAN mag dan ook slechts op één segment worden aangesloten.

Bij de toepassing van meerdere VLAN's toebehorend aan één VPN vindt de routering tussen deze VLAN's via de router van de locatie ontsluiting plaats (de router t.b.v. de "VPN LAN aansluiting"), zonder tussenkomst van de routeringsfunctionaliteit in de Centrale Voorzieningen.
Indien er tussen VPN's moet worden gerouteerd, moet er wel gebruik worden gemaakt van de routerings- en Firewall functionaliteit binnen de Centrale Voorzieningen.

De volgende additionele diensten kunnen worden afgenomen en indien ze benodigd zijn moeten ze middels de PDC Netwerken worden afgenomen:

- DHCP
- DNS

[5] Het gebruik van dezelfde IP adressen op verschillende VPNs heeft tot gevolg dat het verkeer tussen VPNs wordt beperkt of dat er extra NAT maatregelen noodzakelijk zijn. Er dient daarom gebruik te worden gemaakt van uniek geregistreerde IP adressen.

- NTP
- Internet Access
- Extranet Access
- Network Admission Control op basis van IEEE 802.1X en EAP

De afnemer dient per VPN vooraf aan de NNV beheerorganisatie kenbaar te maken of Quality-of-Service (QoS) m.b.t. IP verkeer noodzakelijk is. Hiertoe zal de NNV beheerorganisatie aan de afnemer kenbaar maken welke QoS modellen er door de NNV beheerorganisatie worden geboden. De afnemer dient vervolgens aan te geven welk QoS model er dient te worden gehanteerd, en welk type IP verkeer in welke klasse dient te worden ondergebracht. Bij voorkeur vindt de QoS markering van het verkeer plaats door de applicatie of het LAN. QoS zal vervolgens globaal worden uitgerold voor de afnemer.

Indien de afnemer gebruik wenst te maken van QoS en het LAN of eindapplicatie geen markering ondersteunt, zal deze functionaliteit door de CE-router worden geboden.

2.4.5 Toegestaan verkeer

De “LANs” zijn bedoeld voor IP versie 4 verkeer conform rfc 791[i]. In de toekomst zal ook IP versie 6 verkeer worden ondersteund. Voorwaardelijk is dat er gebruik wordt gemaakt van een “VPN aansluiting LAN”.

Om de integriteit van het netwerk te beschermen zijn de volgende verkeerssoorten niet toegestaan:

- ICMP redirects
- ICMP unreachables
- ICMP mask request/reply
- IP directed broadcast
- Proxy arp

Indien bovenstaande verkeerssoorten door de NNV beheerorganisatie worden gedetecteerd, kan als maatregel de dienstverlening voor de betreffende dienst worden opgeschort.
Aanvullende maatregelen kunnen worden genomen naarmate de beveiliging dit vereist. In dat geval zal dit document worden aangepast.

2.4.6 Toegestane IP unicast adressen

Martian IP adres space zoals gedefinieerd in rfc 3330 [ii] is niet toegestaan voor subnetten die door de gebruiker zelf worden aangedragen, met uitzondering van de volgende IP adresreeksen zoals gedefinieerd in rfc1918 [iii]:

- 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

Een aantal IP subnetten is gereserveerd voor intern NNV gebruik. Een dubbel gebruik van deze IP subnetten leidt tot routeringconflicten op het NNV netwerk. Dit

geldt voor alle over NNV gedefinieerde VPNs. Om deze reden is het niet toegestaan om de volgende IP subnetten op routeerbare LAN segmenten te gebruiken:

- 10.x.0.0 /24
- 10.x.128.0 /24
- 10.x.253.0 /24
- 10.x.254.0 /24

RWS IP hosts dienen bij voorkeur gebruik te maken van de hierboven aangegeven private address space. Voor toegang van systemen in een RWS VPN tot het Internet wordt in de NNV Centrale Voorzieningen - Internet dienst [iv] Netwerk Adres Translatie (NAT) toegepast op een voor de gebruiker transparante manier. Voor RWS systemen die vanaf het Internet bereikbaar moeten zijn, is de NNV Centrale Voorzieningen - DMZ dienstverlening [v] beschikbaar. In deze dienst wordt uit de publieke adresruimte die aan Rijkswaterstaat is toegewezen, ruimte gereserveerd voor proxies die toegang geven tot deze systemen.

2.4.7 Toegestane IP multicast adressen

Er kan alleen gebruik van Source Specific (SSM) of limited scope adressen worden gemaakt.

Dit betekent dat alleen IP multicast verkeer met destination adressen uit de onderstaande range zijn toegestaan en door de afnemer van de dienst kunnen worden gebruikt:

- 232.0.0.0 – 232.255.255.255
- 239.0.0.0 – 239.255.255.255

De source adressen van IP multicast verkeer dienen te voldoen aan de regels voor IP unicast verkeer.

2.5 Aansluitvoorwaarden “LAN Omgeving Draadloos”

Er wordt een drietal typen NNV Aansluitingen ondersteund voor het koppelen van eindapparaten via het product “LAN Omgeving Draadloos”, te weten:

- **RWS intern**: RWS devices met RWS account credentials, beide lid van RWS Active Directory domein(en). Dit type aansluiting geeft toegang tot het VPN RWS:RWS. De beschikbaarheid van dit type aansluiting is 99,5% per wireless Access-Point.

- **RWS BYOD**: RWS AD accounts met non managed devices (BYOD). Dit type aansluiting geeft toegang tot een beperkte set van applicaties waaronder Inter- en Intranet. De beschikbaarheid van dit type aansluiting is 99,5% per wireless Access-Point.

- **RWS GAST**: RWS AD Accounts die via Self Service portal een tijdelijk gastaccount aanmaken voor hun gast(en) of zichzelf om toegang te verlenen voor een ‘non managed device (BYOD)’ via WIFI tot uitsluitend het publieke internet. De beschikbaarheid van dit type aansluiting is 99,5% per draadloos Access-Point.

In de volgende paragrafen worden de specifieke voorwaarden weergegeven waaraan de omgeving zal moeten voldoen. Hierbij worden de volgende aspecten per paragraaf behandeld:

- Algemeen
- OSI-laag 1
- OSI-laag 2
- OSI-laag 3

2.5.1 Algemeen

De NNV aansluitvoorwaarden maken deel uit van de Service Level Agreement (SLA) die zowel door de dienstverlener als de afnemer wordt geaccepteerd bij eerste ingebruikname en nageleefd. Indien blijkt dat door de afnemer niet aan de aan haar gestelde voorwaarden wordt voldaan, heeft de dienstverlener de mogelijkheid om de dienstverlening op te schorten.

Aangesloten systemen (en daarop draaiende operating systemen [OS] en applicaties) dienen zodanig geconfigureerd en hardened te zijn dat zij geen onnodige netwerkbelasting veroorzaken in de vorm van broadcast verkeer of andere netwerkbevuiling.

Indien vreemd of onnodig verkeer wordt geconstateerd, heeft de NNV beheerorganisatie het recht om de verbinding met onmiddellijke ingang op te schorten om de dienstverlening naar andere klanten niet in gevaar te brengen, zulks ter beoordeling van de NNV beheerorganisatie.

2.5.2 OSI-laag 1

De LAN componenten binnen een “LAN Omgeving Draadloos” maken onderdeel uit van dezelfde redundante OSI-laag 2 infrastructuur die onafhankelijk is van de OSI-laag 3 infrastructuur.

Op de aansluitingen van de draadloze Access-Points t.b.v. “LAN Omgeving Draadloos” kunnen de volgende typen eindapparatuur worden aangesloten:

- RWS Intern: RWS devices met RWS account credentials, beide lid van RWS Active Directory domein(en)
- RWS BYOD: RWS AD accounts met non managed devices (BYOD)
- RWS GAST: RWS AD Accounts die via een Self Service portal een tijdelijk gastaccount aanmaken voor hun gast(en) of zichzelf om toegang te verlenen voor een ‘non managed device (BYOD)’ via WIFI tot uitsluitend het publieke internet

Ter bescherming van het NNV netwerk zal altijd Network Admission Control (NAC) op basis van het 802.1X en EAP protocol op alle draadloze aansluitingen zijn toegepast. Aangesloten apparatuur, die niet door het Network Admission Control protocol wordt herkend, zal dan geen of beperkte toegang tot het NNV netwerk krijgen.

2.5.3 OSI-laag 2

Ter bescherming van de infrastructuur voor de “LAN Omgeving Draadloos” zullen door de NNV beheerorganisatie de volgende maatregelen worden genomen op de Access-Points t.b.v. het draadloze netwerk voor RWS Gast apparaten:

- MAC filtering
- AAA servers
- Allow AAA override enabled
- NAC state Radius NAC

Ter bescherming van de infrastructuur voor de “LAN Omgeving Draadloos” zullen door de NNV beheerorganisatie de volgende maatregelen worden genomen op de Access-Points t.b.v. het draadloze netwerk voor RWS Intern en RWS BYOD apparaten:

- WPA2 met AES encryptie
- 802.1X authenticatie
- Allow AAA override enabled
- NAC state Radius NAC

Indien op grond van bovengenoemde maatregelen vreemd of onnodig verkeer door de NNV beheerorganisatie wordt geconstateerd, heeft de NNV beheerorganisatie het recht om de verbinding met onmiddellijke ingang op te schorten om de dienstverlening naar andere klanten niet in gevaar te brengen, zulks ter beoordeling van de NNV beheerorganisatie.

2.5.4 OSI-laag 3

De NNV beheerorganisatie levert voor het LAN OSI-laag 3 functionaliteit op basis van het IPv4 protocol en in de toekomst tevens op basis van het IPv6 protocol.

Het is op het aangesloten draadloze LAN niet toegestaan om een gerouteerde verbinding tussen IP segmenten te creëren. Een aansluiting op het draadloze LAN mag dan ook slechts op één segment worden aangesloten.

De volgende additionele diensten zullen voor de "LAN Omgeving Draadloos" standaard worden afgenomen:

- DHCP
- DNS
- NTP
- Internet Access
- (Beperkte) Extranet Access
- Network Admission Control op basis van IEEE 802.1X en EAP

Op de VPN’s t.b.v. de "LAN Omgeving Draadloos"is de NNV beheerorganisatie verantwoordelijk voor de uitgifte van IP subnetten middels DHCP.

Ten behoeve van de priorizering van het draadloos verkeer zijn er op basis van QoS maatregelen genomen. Deze maatregelen zijn als volgt ingeregeld:

- RWS Intern verkeer heeft te allen tijde voorrang op RWS BYOD verkeer
- RWS BYOD verkeer heeft te allen tijde op RWS Gast verkeer

2.5.5 Toegestaan verkeer

De “LAN Omgeving Draadloos” is bedoeld voor IP versie 4 verkeer conform rfc 791[i]. In de toekomst zal ook IP versie 6 verkeer worden ondersteund. Voorwaardelijk is dat er gebruik wordt gemaakt van een “VPN aansluiting LAN”.

Om de integriteit van het netwerk te beschermen zijn de volgende verkeerssoorten niet toegestaan vanuit de bouwsteen “VPN aansluiting LAN” en daarmee de bouwsteen “LAN Omgeving Draadloos”:

- ICMP redirects
- ICMP unreachables
- ICMP mask request/reply
- IP directed broadcast
- Proxy arp

Indien bovenstaande verkeerssoorten door de NNV beheerorganisatie worden gedetecteerd, kan als maatregel de dienstverlening voor de betreffende dienst worden opgeschort.
Aanvullende maatregelen kunnen worden genomen naarmate de beveiliging dit vereist. In dat geval zal dit document worden aangepast.

2.6 Beveiliging

Voor algemene richtlijnen met betrekking tot beveiliging van netwerkinfrastructuur wordt verwezen naar de meest recente versies van de documenten “Cybersecurity Implementatierichtlijn Objecten – RWS” en de “Baseline Informatiebeveiliging Rijksdienst (BIR)”.

In het bijzonder geldt voor zowel de LAN netwerken die door een derde worden beheerd, als het product “LAN omgeving bedraad”, dat deze geen directe koppelingen mogen hebben met andere netwerken. Onder ‘andere netwerken’ wordt o.a. verstaan:

- Netwerken van externe partijen (incl. Internet)
- Inbelvoorzieningen
- WLANs (wanneer deze niet voldoen aan de beveiligingstandaard van RWS)
- etc.

Koppelingen naar externe netwerken zijn alleen indirect mogelijk via de in de centrale voorzieningen aangeboden standaardproducten met betrekking tot externe koppelingen (zie hiervoor ook paragraaf 2.7 “Externe Toegang”).

Er vindt geen directe routering plaats (lees: op de CE-router of binnen het KA LAN) tussen VLANs behorend tot verschillende VPNs. Routering tussen deze VPNs vindt plaats binnen een specifiek hiervoor geconfigureerde centrale omgeving. Voor RWS klanten zijn dit de Centrale Voorzieningen die door de NNV beheerpartij worden beheerd. In dat geval moeten routering- en filteringspecificaties hiervoor door de eigenaar van de betrokken VPNs aan de NNV beheerorganisatie kenbaar te worden gemaakt.

Hierop bestaat wel een uitzondering. Inter VLAN routering binnen de locatie, zonder tussenkomst van de NNV WAN router(s) wordt wel toegestaan voor routering van het verkeer van en naar (blade)servers die zich in de MER bevinden, mits de

bijbehorende VLAN's tot hetzelfde VPN behoren. Deze routering dient dan wel op de LAN router plaats te vinden.

2.7 Beheer

De toegang door (onderhouds)technici van of namens de NNV beheerorganisatie tot de technische ruimten en bijbehorende systeemkasten waarbinnen zich NNV componenten bevinden, moet zodanig worden geregeld dat aan de SLA eisen kan worden voldaan. Indien dit niet kan, wordt de hersteltijd in de storingsafhandeling stilgezet.

De NNV beheerorganisatie heeft het recht om gedurende de looptijd van de SLA technische audits uit te voeren op de locale infrastructuur van de afnemer.

2.8 Externe Toegang

Externe toegang tot het RWS netwerk is mogelijk via standaardproducten die hier specifiek voor zijn ontwikkeld, mits in het end-to-end ontwerp voor deze toegang duidelijk invulling wordt gegeven aan de eerder genoemde "Cybersecurity Implementatierichtlijn Objecten – RWS, versie 1.0".

Bij externe toegang wordt een tweetal toegangsvormen onderkend. Voor beide vormen geldt dat deze aangevraagd kunnen worden via een "Aanvraag Toegang Derden". In het bij het proces behorende "Intakewerkboek Toegang Derden" wordt o.a. met ontwerpvoorbeelden uitgelegd op welke manier deze toegangsvormen ingezet kunnen worden en welke protocollen daarbij worden ondersteund.

2.8.1 Individuele Netwerktoegang door Derden

Dit betreft toegang vanuit het internet met behulp van een RAS Token. In DMS-online bekend onder de producten RAS Profiel in combinatie met Wijziging Firewall Policy en RAS Gebruiker.

2.8.2 Locatie gebonden Netwerktoegang door Derden

Dit betreft toegang vanuit het internet met behulp van een IPsec koppeling of een vaste verbinding. In DMS-online bekend onder het product Vaste externe toegangsvoorziening in combinatie met Wijziging Firewall Policy.

Bijlage A NNV aansluitprocedure

A.1 Stap 1: Aanspreekpunt

Er is een lokaal aanspreekpunt beschikbaar voor het aanleveren van informatie en het coördineren van acties. De lokale contactpersoon is bij de afnemer projectverantwoordelijk en kwartiermaker voor het project (aansluiten op NNV infrastructuur) en als zodanig een volwaardig lid van het implementatieteam. Daarnaast is er voor elke aan te sluiten locatie een NNV contactpersoon beschikbaar van het NNV bouwteam.

A.2 Stap 2: Documentatie

De netwerkboekhouding van een locatie dient compleet en actueel te zijn. Deze netwerkboekhouding dient ter beschikking te kunnen worden gesteld aan het NNV bouwteam en indien nodig de NNV beheerorganisatie. De volgende zaken dienen binnen de netwerkboekhouding aanwezig te zijn:

- Netwerktekeningen (onderverdeeld in OSI-lagen)
- Lokaal IP nummerplan
- VLAN architectuur
- Routeringarchitectuur
- Overzicht applicaties
- Speciale benodigdheden (throughput, beschikbaarheid, QoS, etc.)

A.3 Stap 3: Inventarisatie

Aan de hand van de aangeleverde documentatie zal door de NNV beheerder worden gecontroleerd of de actuele situatie conform is met de aangeleverde documentatie. Indien dat niet het geval is dan dient de lokale contactpersoon deze documentatie *up-to-date* te maken. Tussen stap 2 en 3 zit een iteratieslag totdat aan alle voorwaarden is voldaan.

A.4 Stap 4: Beveiliging en stabiliteit

Op een NNV VPN aangesloten systemen en hosts dienen zich te conformeren aan de beveiligingsvoorwaarden van de VPN eigenaar.

De lokaal gebruikte OS'en en applicaties dienen zodanig te zijn geconfigureerd dat zij geen onnodige netwerkbelasting veroorzaken voor het NNV koppelvlak en de achterliggende NNV netwerk als geheel.

A.5 Stap 5: Gereedmaken lokale situatie

De omgeving dient te zijn opgeschoond van constructies die de functionaliteit, veiligheid of stabiliteit van het NNV netwerk in gevaar kunnen brengen, dan wel een koppeling onmogelijk maken.

A.6 Stap 6: Netwerk audit

Er wordt door NNV een netwerk audit uitgevoerd om te bepalen of aan alle voorwaarden voor aansluiting op het NNV netwerk is voldaan. Tussen stappen 4, 5 en 6 zit een iteratieslag totdat aan alle voorwaarden is voldaan.

A.7 Stap 7: Acceptatietest door NNV en afnemer

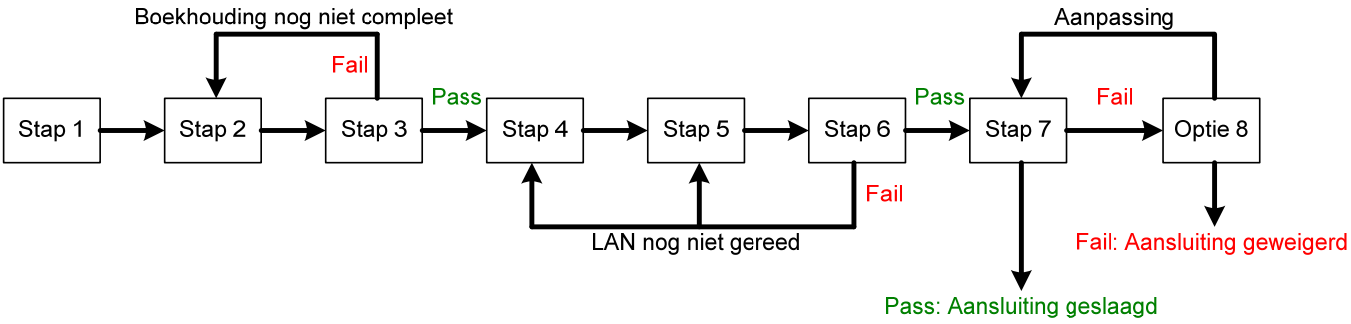
Zowel vanuit NNV als ook vanuit de afnemer wordt de aansluitprocedure afgesloten door een separate acceptatietest. Beide partijen stellen hiervoor hun benodigdheden en *pass/fail* criteria op. Er wordt pas van een geslaagde aansluiting gesproken als beide acceptatietests succesvol zijn afgesloten.

A.8 Optie 8: Acceptatietest: Fail

Indien de acceptatietest niet succesvol is, dan dient de implementatie onderworpen te worden aan binnen NNV en afnemer bekende troubleshoot en debug procedures. Deze werkzaamheden worden zowel door het NNV implementatieteam als ook door de afnemer uitgevoerd. Hierbij zijn er twee uitkomsten mogelijk:

- Het is mogelijk de implementatie binnen de randvoorwaarden aan te passen, waarna er opnieuw acceptatietests plaatsvinden. Tussen stappen 7 en 8 zit een iteratieslag totdat de koppeling met het NNV succesvol is.

- Het is niet mogelijk de implementatie binnen de randvoorwaarden aan te passen. Een NNV aansluiting zal dan door één of beide partijen worden geweigerd.



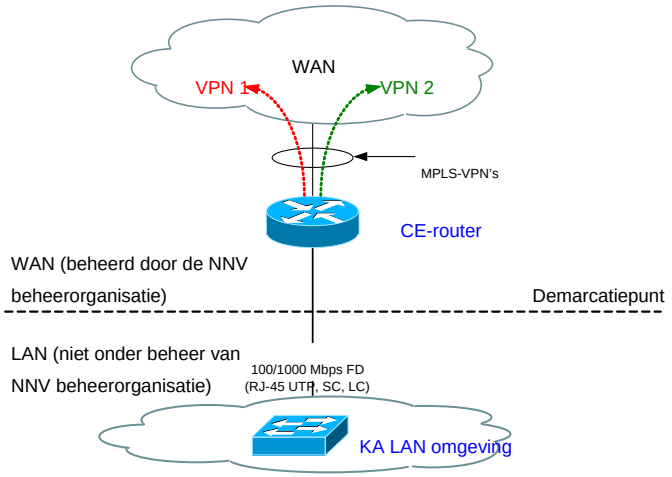
Figuur 4 :Flowchart aansluitprocedure NNV

Bijlage B Checklist

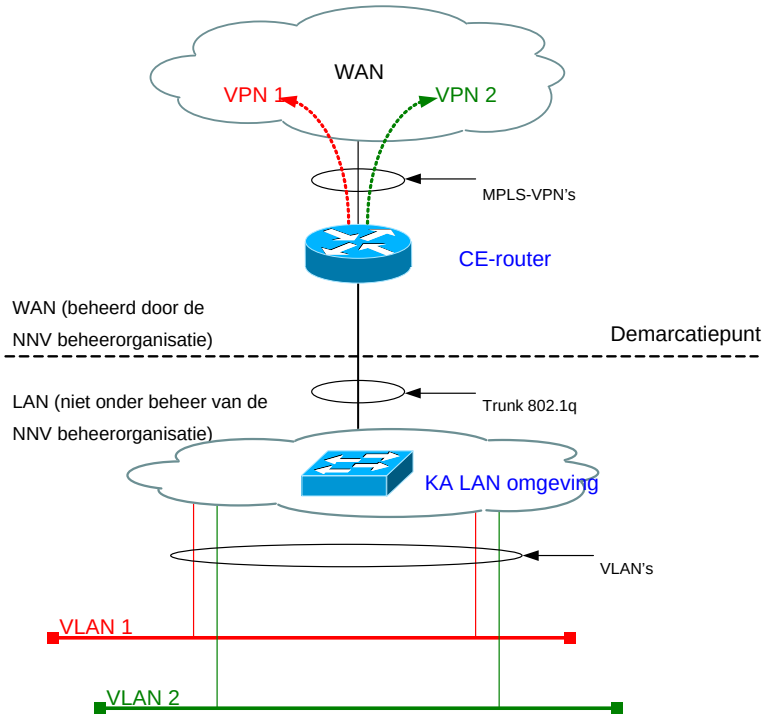
Eis	Korte omschrijving zoals gedefinieerd in NNV aansluitvoorwaarden	Voldaan		
		Ja	Nee	NVT
1	Het is de afnemer bekend dat NNV LAN aansluitingen onderhevig zijn aan een SLA, en dat het niet nakomen van de voorwaarden inhoudt dat de NNV beheerpartij zich het recht voorbehoud om de dienstverlening op te schorten.			
2	De afnemer heeft één van de standaard SLA modellen gekozen voor een “NNV VPN LAN aansluiting” of “LAN omgeving bedraad”.			
3	De afnemer heeft bandbreedtebehoefte van de uplink bepaald en heeft deze per VPN gespecificeerd.			
4	(Eind)systemen op het NNV LAN veroorzaken geen onnodige netwerkbelasting, zoals *broadcasts-stormen* en andere vormen van netwerkbevuiling.			
5	De afnemer heeft stalen 19” systeemkasten ter beschikking gesteld aan de NNV beheerpartij. Deze systeemkasten zijn afsluitbaar, bezitten voldoende ventilatie en zijn voorzien van 230V 50 Hz wisselspanning volgens de NEN1010 standaard.			
6	Ruimtes waarin NNV WAN en LAN componenten worden afgemonteerd voldoen aan ETSI norm 300 019-1-3 class 3.1. De afnemer heeft o.a. aan de volgende zaken voldaan: • correcte luchtvochtigheid i.c.m. omgevingstemperatuur • correct stofgehalte • afscherming tegen waterspatten • afscherming tegen zonlicht			
7	Ruimtes waarin NNV WAN en LAN componenten worden afgemonteerd zijn voorzien van een locatie-aanduiding.			
8	De verantwoordelijkheid voor patching en het onderhouden van de infrastructuur in de computerruimte(s) ligt bij de afnemer.			
9	Indien van toepassing: Er zijn meerdere MER ruimtes beschikbaar voor redundante NNV WAN en LAN componenten.			
10	Indien van toepassing: Er is 10 meter ruimte tussen kasten voor redundante NNV componenten in het geval van het ontbreken van meer dan één MER ruimte.			
11	Indien van toepassing: Het NNV LAN beschikt over een redundante OSI-laag 2 infrastructuur t.b.v. een redundante NNV WAN aansluiting.			
12	Indien van toepassing: Servers in de MER’s kunnen op basis van IEEE 802.1q worden aangesloten.			
13	Op VLANs op het LAN die exclusief zijn toegewezen aan NNV componenten zijn geen andere (eind)systemen binnen een pand aangesloten.			
14	De afnemer heeft aan NNV kenbaar gemaakt welke VLANs er op de CE-router dienen te worden ontsloten.			
15	Het door de afnemer aangeboden dataverkeer is op basis van IPv4 en in de toekomst op basis van IPv6. Er zijn binnen LAN subnetten gereserveerde IP adressen toegewezen aan NNV t.b.v. het leveren OSI-laag 3 functionaliteit. Deze IP adressen zijn niet toegewezen aan andere systemen op het LAN.			
16	Op elk VLAN binnen het LAN is slechts één IP subnet in gebruik.			
17	IP adresreeksen op het LAN zijn niet in gebruik elders binnen het VPN.			
18	Voor VPNs waarvoor de NNV beheerpartij IP adresbeheer uitvoert, heeft de afnemer voor de betreffende VLANs aan de NNV beheerpartij een IP adresruimte aangevraagd. Voor VLANs behorend tot overige VPNs heeft de afnemer aan de NNV beheerpartij kenbaar gemaakt welke IP adressen er worden toegepast.			

19	Afnemer geeft aan of QoS gewenst is. Zo ja, dan heeft de afnemer aangegeven welk NNV QoS model dient te worden toegepast en welk type IP verkeer in welke klasse dient te zijn ingedeeld.			
20	Indien van toepassing: Wanneer m.b.t. QoS het LAN geen markering ondersteund wordt dit uitgevoerd op de CE-router. De afnemer heeft hiervoor aan NNV kenbaar gemaakt op welke wijze verkeersstromen gemarkeerd dienen te worden.			
21	Er zijn geen koppelingen met andere (externe) netwerken op het LAN.			
22	De afnemer heeft aangegeven of er routerings- en filterspecificaties binnen de Centrale Voorzieningen (IK en/of EK) dienen te worden aangepast m.b.t. routering naar en van andere VPNs.			
23	De afnemer heeft geregeld dat personeel van de NNV beheerpartij fysiek toegang kan krijgen tot NNV componenten op de locatie.			
24	De afnemer staat toe dat de NNV beheerpartij technische audits kan uitvoeren op het LAN en het WAN.			

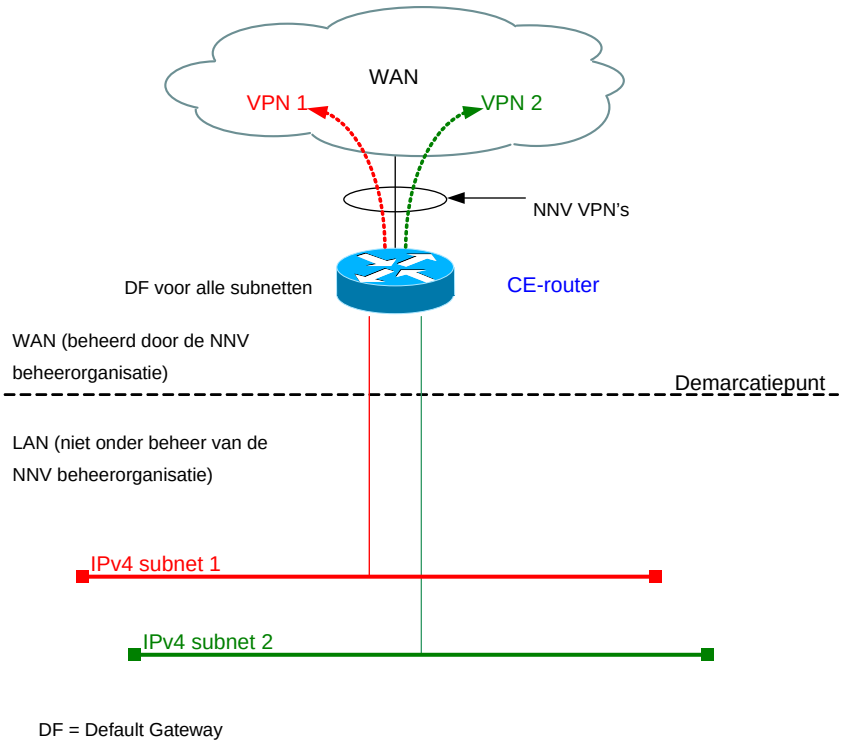
Bijlage C Enkelvoudige aansluiting “VPN aansluiting LAN”



Figuur 5: Laag 1 enkelvoudige “VPN aansluiting LAN”

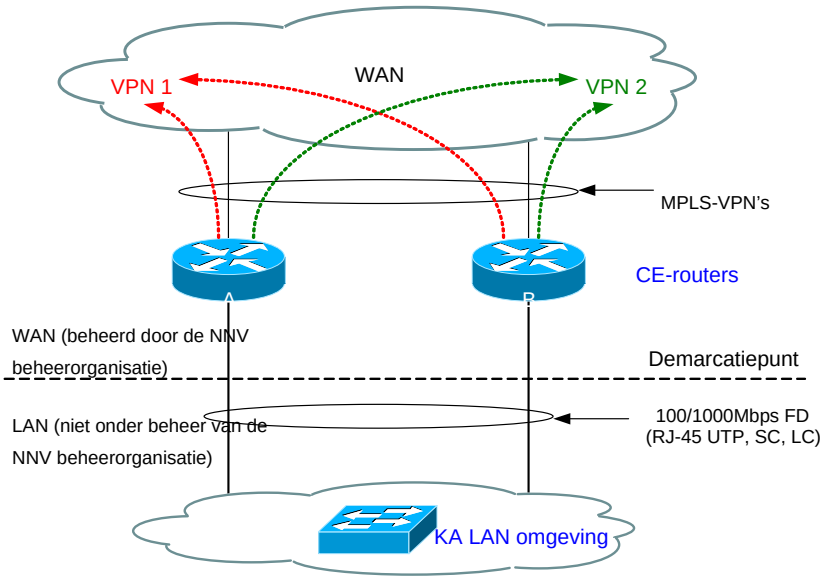


Figuur 6: Laag 2 enkelvoudige “VPN aansluiting LAN”

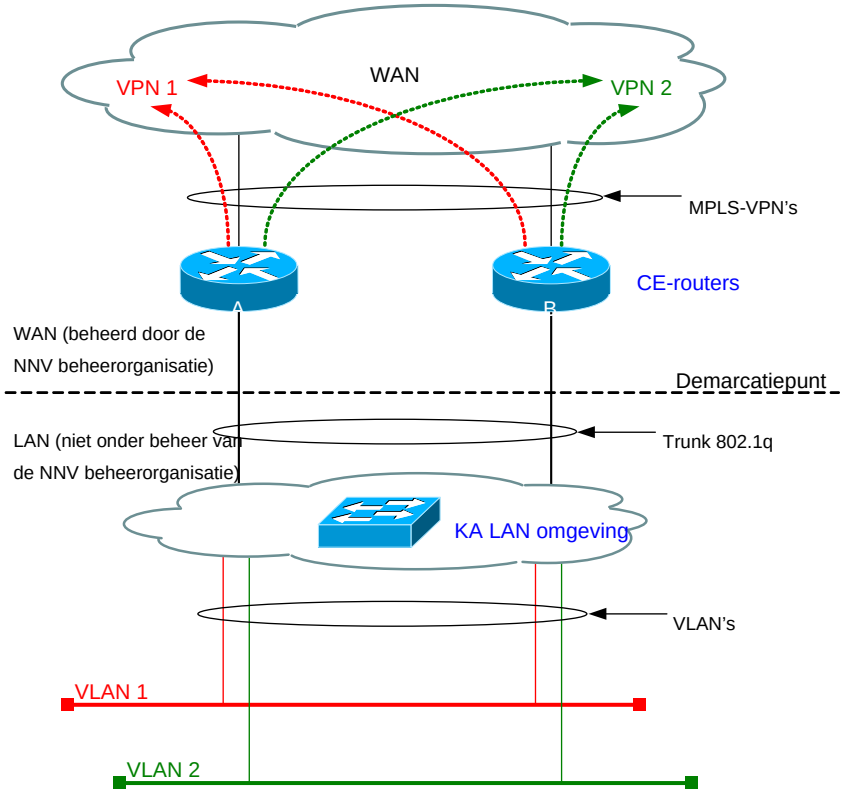


Figuur 7: Laag 3 enkelvoudige "VPN aansluiting LAN"

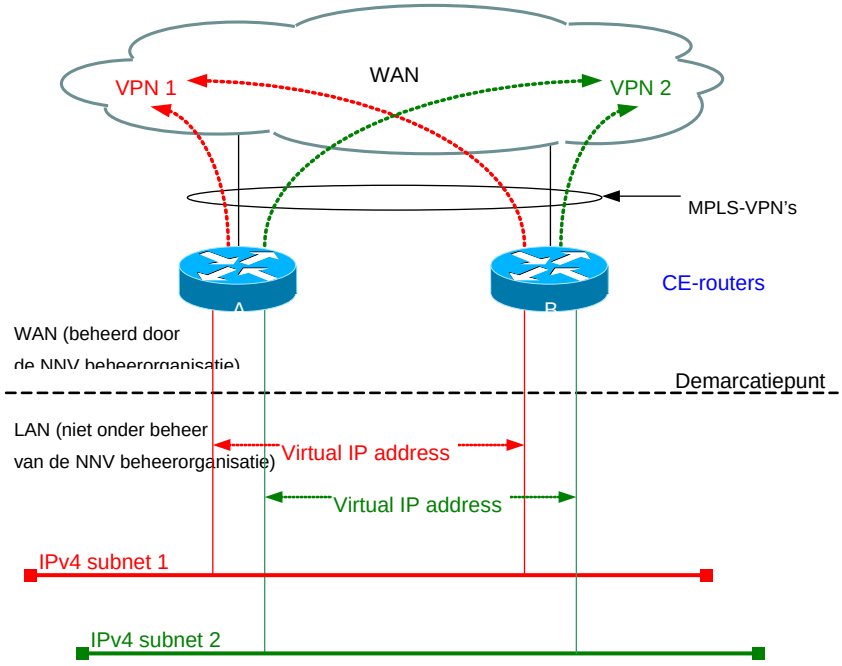
Bijlage D Redundante aansluiting “VPN aansluiting LAN”



Figuur 8: Laag 1 redundante “VPN aansluiting LAN”



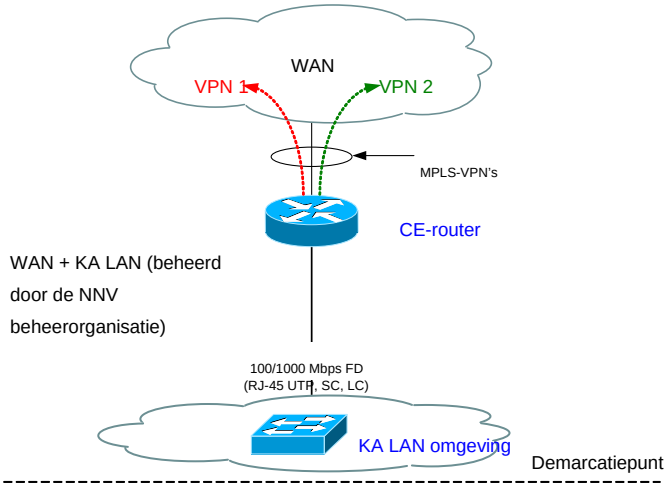
Figuur 9: Laag 2 redundante "VPN aansluiting LAN"



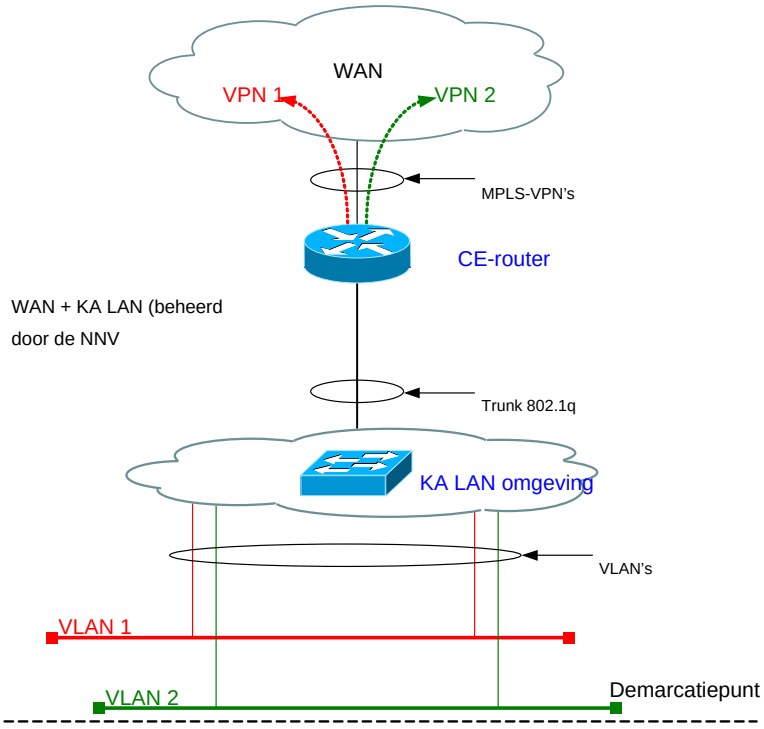
Virtual IP address dient als default-gateway voor subnets op VLAN's.

Figuur 10: Laag 3 redundante "VPN aansluiting LAN"

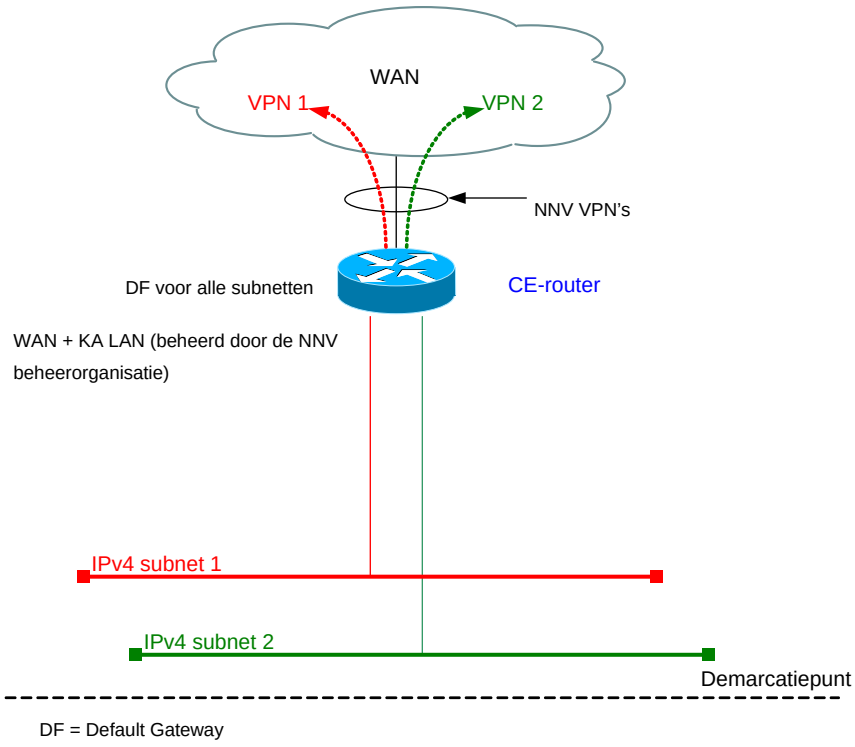
Bijlage E Enkelvoudige aansluiting “VPN aansluiting LAN” + standaard “LAN omgeving bedraad”



Figuur 11: Laag 1 enkelvoudige “VPN aansluiting LAN” + standaard “LAN omgeving bedraad”

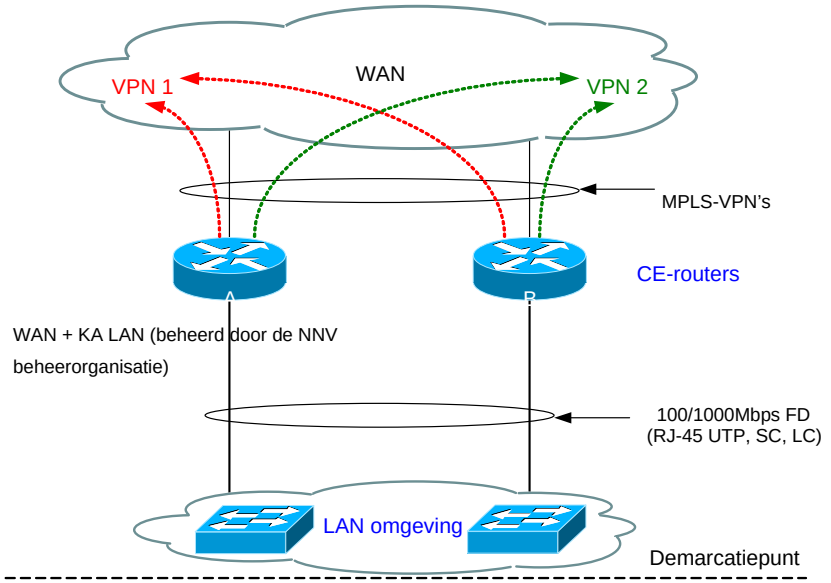


Figuur 12: Laag 2 enkelvoudige “VPN aansluiting LAN” + standaard “LAN omgeving bedraad”

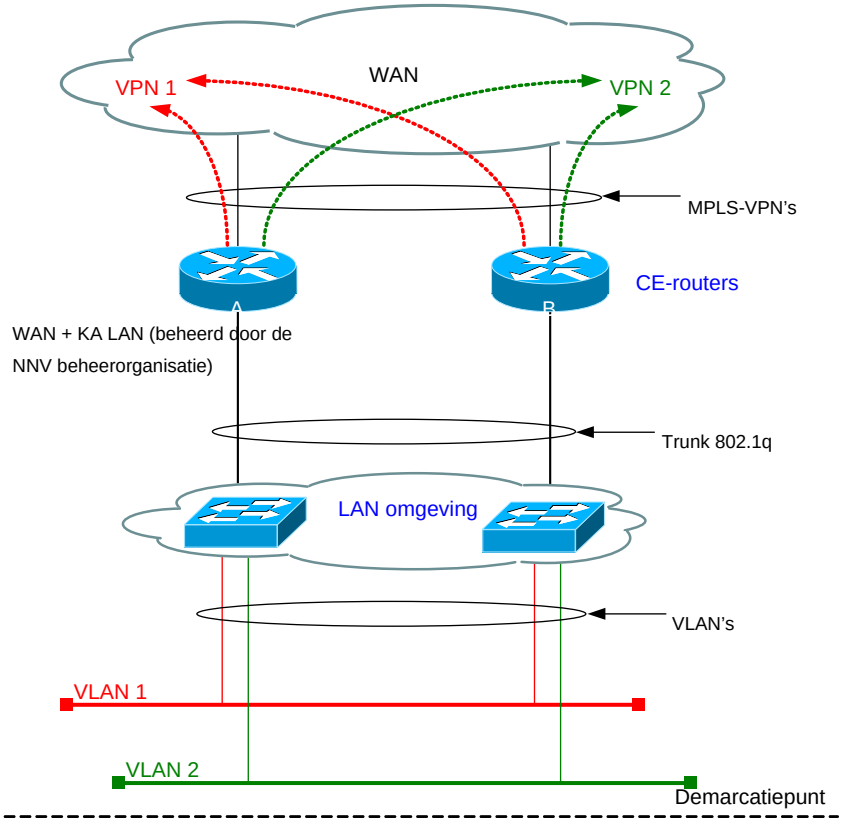


Figuur 13: Laag 3 enkelvoudige "VPN aansluiting LAN" + standaard "LAN omgeving bedraad"

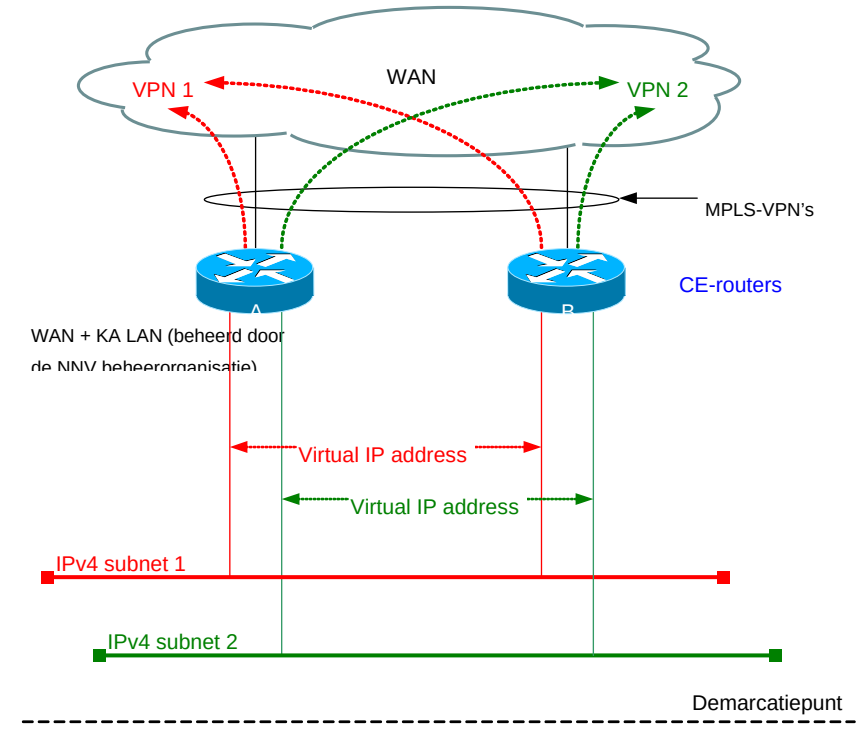
Bijlage F Missiekritische aansluiting “VPN aansluiting LAN” + speciaal “LAN omgeving bedraad”



Figuur 14: Laag 1 missiekritische “VPN aansluiting LAN” + speciale “LAN omgeving draadloos”



Figuur 15: Laag 2 missiekritische "VPN aansluiting LAN" + speciale "LAN omgeving draadloos"



Virtual IP address dient als default-gateway voor subnets op VLAN's.

Figuur 16: Laag 3 missiekritische "VPN aansluiting LAN" + speciale "LAN omgeving draadloos"

Bijlage Referenties

1. [i] rfc791: Internet Protocol; 1982; http://www.rfc-editor.org/rfc/rfc791.txt
2. [ii] rfc3330: Special use IPv4 Addresses; 2002; http://www.rfc-editor.org/rfc/rfc3330.txt
3. [iii] rfc1918: Address allocation for private Intranets; 1996; http://www.rfc-editor.org/rfc/rfc1918.txt
4. [iv] Productplan NNV Centrale Voorzieningen – Internet; Cluster Netwerken; 2006
5. [v] Productplan NNV Centrale Voorzieningen – DMZ; Cluster Netwerken; 2006
6. [vi] Handboek ICT-huisvesting en bekabeling (HIB) versie 1.0
7. NNV-NG - Globaal Ontwerp - v1.7 (definitief); 2012