

Aansluitvoorwaarden

Generiek Toegangsnetwerk GTN

T.b.v. randapparatuur in hostingszones.

Intern

Van	ProRail - ICT Infravoorzieningen - Netwerken
Auteur	Marco de Heuvel/Hans van der Spek/Joeri Bos
Kenmerk	
Versie	1.3
Datum	5 augustus 2021
Bestand	Aansluitvoorwaarden Generiek Toegangsnetwerk GTN v1.3.docx
Status	Definitief

Inhoudsopgave

1	INLEIDING	3
1.1	AANLEIDING	3
1.2	DOELSTELLING	3
1.3	SCOPE	3
1.4	STATUS.....	3
1.5	VERSIEBEHEER	4
1.6	DEFINITIES, TERMEN EN AFKORTINGEN LIJST	5
1.7	REFERENTIES.....	6
2	AANSLUITVOORWAARDEN	7
2.1	ALGEMEEN	7
2.2	SYSTEEM INTERFACE.....	7
2.3	KOPPELVAKKEN.....	8
2.4	BEVEILIGING	8
2.5	PROTOCOLLEN	8
2.6	QoS	9
2.7	ADRESSERING	9
2.8	OMVANG VAN VERKEER	9
2.9	KOPPELINGEN EXTERNE PARTIJEN	9

1 Inleiding

1.1 Aanleiding

ProRail ICT levert een Generiek Toegangsnetwerk (GTN). Dit GTN is het koppelvlak van de interne ICT-infrastructuur met externe partijen en internet. Daarnaast is het ook het koppelvlak tussen de verschillende Functionele Netwerken. Uitzondering hierop zijn koppelingen die interne Functionele Netwerken onderhouden met de Cloud. Binnen de GTN-infrastructuur kan randapparatuur worden aangesloten in de verschillende hostingzones mits deze voldoet aan bepaalde aansluitvoorwaarden. Dit document beschrijft voor deze systemen de voorwaarden waaronder deze mogen worden aangesloten.

1.2 Doelstelling

Dit document heeft tot doel om de aansluitvoorwaarden te beschrijven voor systemen welke geplaatst worden in een van de verschillende security-zones van het Generieke Toegangsnetwerk (GTN). De aangesloten randapparatuur en toegepaste applicaties dienen aan deze aansluitvoorwaarden te voldoen.

Op basis van dit document moeten o.a. systeemmanagers, productbeheerders en projectleiders in staat zijn de juiste randapparatuur te selecteren. Voor het koppelen van systemen en of netwerken aan de externe kant van het GTN zijn de aansluitvoorwaarden van derden van toepassing [AVD]. Op de koppelingen van de functionele netwerken aan de interne zijde van het GTN zijn de vigerende standaarden van toepassing.

1.3 Scope

Dit document beschrijft alleen de fysieke aansluitvoorwaarden voor systemen welke geplaatst dienen te worden in een van de verschillende security-zones van het Generieke Toegangsnetwerk.

Deze aansluitvoorwaarden zijn van toepassing op nieuwe systeeminfrastructuur welke dient te worden gekoppeld met een van de hostingzones van het GTN. Dit document kan niet worden gebruikt om te bepalen in welke securityzone randapparatuur kan worden ondergebracht. Daarvoor dient het securitybeleid te worden geraadpleegd. Als richtlijn kan hiervoor de 'beslisboom GTN' worden gebruikt. [BBGTN]

1.4 Status

Dit is een definitieve versie maar niet uitontwikkeld. Dit document zal t.z.t. worden samengevoegd met de aansluitvoorwaarden die van toepassing zijn van het ontsluiten van randapparatuur op ProRail datacenters.

1.5 Versiebeheer

Versie	Status	Datum	Omschrijving
0.1	Concept	27-01-2019	Eerste Concept versie
0.3	Concept	1-10-2019	Diverse aanpassingen
1.0	Definitief	3 maart 2020	Versie definitief gemaakt.
1.1	Definitief	13 juli 2020	Aanpassing m.b.t. OOBM
1.2	Definitief	11 januari 2021	Toevoegen beperking trunk/zone.
1.3	Definitief	5 augustus 2021	Aanpassing management interfaces en eis statisch IP

1.6 Definities, termen en afkortingen lijst

Onderstaande lijst bevat een lijst met afkortingen en termen die in dit document worden gebruikt.

Term / Afkorting	Toelichting / Omschrijving
ACI	Application Centric Infrastructure (Cisco SDN oplossing voor in datacenters)
COM	Centraal Out-of-Band Management netwerk. Specifiek voor netwerkbeheer en ook alleen t.b.v. het GTN en ACI.
Delay	Delay of netwerkvertraging is de (gemiddelde) tijd die een data pakket erover doet om de bestemming te bereiken. Delay wordt uitgedrukt in ms
DHCP	Dynamic Host Configuration Protocol. Dynamic Host Configuration Protocol is een computerprotocol dat beschrijft hoe een computer dynamisch zijn netwerkinstelling van een DHCP-server kan verkrijgen. Het DHCP-protocol is gebaseerd op het Internet Protocol IP en werkt met UDP-pakketten.
Fides	Fides is het, generieke landelijke netwerk voor alle IP WAN connectiviteit van ProRail. Op Fides worden meerdere Functionele Netwerken gerealiseerd
Functioneel Netwerk	een specifiek domein (VPN) voor een klantgroep of toepassingsgebied en op logisch niveau gescheiden.
GTN	Generiek ToegangsNetwerk; Generieke infrastructuur van ProRail om veilig en gecontroleerd te kunnen communiceren tussen de verschillende interne netwerken onderling en/of tussen interne en externe netwerken.
ICT-O	ICT-Operations is de operationele beheer afdeling van ProRail
IP	Internet Protocol (RFC 791)
Jitter	Jitter in IP-netwerken is de variërende vertraging in het afleveren van data pakketten en wordt uitgedrukt in ms.
Klantlocatie	Met klantlocatie wordt binnen deze context een eindlocatie bedoeld waar de randapparatuur van een gebruikersgroep zich bevindt.
LAN	Local Area Network
Link Aggregation	Engelse benaming voor het samenvoegen van meerdere netwerkverbindingen met het doel een hogere doorvoersnelheid en/of een hogere beschikbaarheid te realiseren.
MMF	Multi Mode Fiber
Packet Loss	Packet loss (pakket verlies) is wanneer een verstuurd data pakket zijn bestemming niet bereikt. Packet Loss wordt uitgedrukt in het percentage van verloren data pakketten en opzichte van het totaal aantal verstuurde data pakketten.
Productbeheerder	Functie binnen ICT-Services; draagt zorg voor life cycle management van informatiesystemen ten behoeve van een continue beschikbaarheid van deze systemen die aansluiten bij de wensen van de klant en de beheerder.
Randapparatuur	Apparaten die bestemd zijn om te worden aangesloten op een netwerk ten behoeve van de overbrenging, verwerking of ontvangst van informatie en die eigendom zijn van Klant.
RTO	Recovery Time Objective

SIL	Safety Integrity Level
Stack	Combineren van meerdere fysieke switches naar 1 logische switch Een stack wordt ook wel virtual-chassis genoemd
Systeem	Zie randapparatuur
SpoorLAN	het SpoorLAN is een generieke LAN-infrastructuur op Spoorgebonden locaties.
Systeemmanager	Functie binnen AM; adviseert en ondersteunt management ten aanzien van technisch beleid, technische systeemvelden en technische systemen en draagt zorg voor de inzet en optimalisatie (performance en kosten) daarvan, teneinde bij te dragen aan een efficiënte en effectieve inzet van de railinfrastructuur voor klanten.
Trunking	Trunking is het transporteren van meerdere virtuele verbindingen (VLAN's) over één fysieke verbinding.
UTP	Unshielded Twisted Pair
Verkeersmatrix	Overzicht van de verkeerstromen voor een bepaald netwerk of systeem. Hierbij wordt aangegeven welke systemen met elkaar communiceren en wat daarvan de omvang en frequentie is.
VLAN	Virtual Local Area Network
VPN	Virtual Private Network, zie functioneel netwerk
WAN	Wide Area Network

1.7 Referenties

Ref	Versie	Status	Datum	Auteur	Titel
[AVD]	1.0	Definitief	Jan 2016	Paul Ram	Aansluitvoorwaarden derden
[IBB]	1.1	Definitief	Maart 2011	Stoffel Bos	Informatiebeveiligingsbeleid
[BBGTN]	1.0	Definitief	Nov 2014	Marco de Heuvel	Beslisboom GTN
[COM]	0.91	Concept	Dec 2020	Hans van der Spek	GO ProRail COM Netwerk

2 Aansluitvoorwaarden

2.1 Algemeen

Het GTN is het koppelvlak tussen de verschillende Functionele Netwerken onderling en tussen de Functionele Netwerken en netwerken buiten de invloedssfeer van ProRail. Het GTN is geo-redundant opgebouwd in twee fysiek gescheiden locaties, waarbij per locatie ook een bepaalde mate van redundantie aanwezig is. Het GTN levert een hosting omgeving voor systemen welke in het GTN worden ondergebracht. Dit zijn alleen systemen/toepassingen die diensten leveren ten behoeve van het veilig uitwisselen van data tussen systemen op verschillende Functionele en/of externe netwerken. In het GTN zullen geen toepassingen worden gehost welke een directe invloed kunnen hebben op de treinenloop of gerelateerd zijn aan safety (geen SIL 1-4 toepassingen). Ook zal het GTN geen applicaties en of systemen hosten die, over de datacenters heen, gebruik willen maken van VLAN of Laag 2 stretching en daarnaast is het GTN niet geschikt voor toepassingen die specifieke en strikte RTO eisen stellen. Het GTN is een generieke infrastructuur en zal daarom een 'best-practice' recovery dienst leveren.

2.2 Systeem Interface

Het GTN is zo opgebouwd dat uitval van één component niet mag leiden tot uitval van functionaliteit. Storing in één component of uitschakelen van één component in verband met onderhoud moet mogelijk zijn zonder functionele impact. Dit stelt wel eisen aan alle aangesloten randapparatuur.

- Alle randapparatuur moet redundant aangesloten worden op de GTN-infrastructuur om beschikbaarheid te garanderen. Dit betekent dat een systeem met minimaal twee interfaces, verdeelt over twee switches, aangesloten moet worden;
- NIC-bonding, portchannels of teaming (het configureren van fysieke interfaces alsof het één logische interface is) wordt ondersteund;
- LACP (alleen met slow-timers) is het protocol wat ondersteund wordt (PaGP wordt niet ondersteund);
- GTN biedt geen ondersteuning aan static mac-adressen of static arp-entries;
- Het GTN is beveiligd tegen het ontvangen van BPDU-pakketten. Interfaces van het GTN worden dan ook geblokkeerd bij de ontvangst van BPDU's;
- Het GTN ondersteund alleen MAC-adressen welke conform de IEEE standaard zijn uitgegeven;
- DOT1Q wordt ondersteund. VLAN-indeling dient te worden afgestemd met ICT-O netwerkbeheer;
- In een trunk mogen alleen VLAN's van dezelfde subzone worden gecombineerd. Het is dus niet toegestaan om VLAN's van verschillende (sub)zones in dezelfde trunk te combineren;
- Bonding/Portchannels/Etherchannels worden toegepast voor netwerkredundantie en niet voor uitbreiding van bandbreedte. De beheerder van randapparatuur welke gebruik maakt van deze technieken is verantwoordelijk voor het voorkomen van functionele degradatie bij het wegvallen van een redundante access verbinding;
- Om interferentie met het GTN te voorkomen is het toepassen van virtuele netwerk infrastructuur alleen mogelijk na toestemming van de netwerkbeheerder;
- Geo-redundantie op het hosting deel van het GTN wordt alleen geleverd via Laag3 en in combinatie met DNS services.

2.3 Koppelvlakken

Voor het aansluiten van randapparatuur op het GTN kunnen verschillende koppelvlakken worden toegepast. Alle koppelvlakken zijn op basis van Ethernet (IEEE 802.3). De onderstaande verschijningsvormen zijn beschikbaar.

Type	Maximale Bandbreedte	Connector	Medium	Opmerking
STANDAARD				
1Gbps UTP	1Gbps	RJ45	CAT6A	UTP Standaard aansluiting
10Gbps Glas	10Gbps	LC/PC	MMF 850nm	Standaard

- Het GTN ondersteund geen 10Mbps of 100 Mbps koppelvlakken.
- Indien een enclosure in meerdere zones aanwezig is, dan dient er per zone 2 uplinks beschikbaar te zijn, exclusief koppelingen met andere omgevingen (bv. Backup, vmotion, etc.)
- Een server mag maximaal onderdeel uitmaken van 1 zone of subzone binnen het GTN. Dual-homing tussen zones is niet toegestaan.
- Op alle koppelvlakken wordt 'auto-negotiation' toegepast.

Management aansluitingen

- Dergelijke aansluitingen hebben een afwijkende SLA (best effort) en mogen tijdens plannend maintenance altijd onderbroken worden (geen change request, maar een mededeling "onderhoudswerkzaamheden")
- Het COM-netwerk zal alleen worden ingezet voor netwerkbeheer en ook alleen t.b.v. het GTN en ACI. [COM]

Backup aansluiting

- Backupdata van randapparatuur geschiedt bij voorkeur via een fysiek of logisch afgescheiden infrastructuur. Ook hier kan gebruik worden gemaakt van een aparte tenant op Cisco ACI.

2.4 Beveiliging

- Randapparatuur binnen het GTN moet voldoen aan het [IBB].
- Randapparatuur moet voorzien zijn van een lokale en juist ingerichte firewall of filtering conform ProRail standaard, toegepast op alle interfaces die aangesloten zijn op infrastructuur van ProRail.
- Randapparatuur moet ingericht zijn conform de desbetreffende benchmark van de CIS organisatie (<https://www.cisecurity.org>)

2.5 Protocollen

Binnen het GTN wordt gebruik gemaakt van IPv4 (RFC 791) als Netwerk Protocol. Als Transport Protocol wordt TCP (RFC 675; RFC 793; RFC 1122 en RFC 2581) en UDP (RFC 768) gebruikt. Andere Transport Protocollen worden niet per definitie ondersteund, de mogelijkheid van de toepassing daarvan zal per geval moeten worden bekeken.

Het GTN is voorbereid op het gebruik van IPv6 (RFC2460). Deze functionaliteit is nog niet beschikbaar voor eindsystemen.

2.6 QoS

Het GTN ondersteunt beperkt QoS. QoS kan alleen geleverd worden op datastromen welke aan de interne zijde van het GTN kunnen worden afgehandeld. Typisch zijn dit datastromen tussen interne domeinen/Functionele netwerken.

2.7 Adressering

- Elk aan te sluiten randapparaat of virtueel systeem op dit randapparaat dient te worden voorzien van minimaal één uniek IP adres;
- IP adressen worden uitgegeven en beheerd door ICT-O netwerkbeheer. Het is niet mogelijk, noch toegestaan andere IP adressen te gebruiken.
- Binnen het GTN worden alleen private-space IPv4 adressen (RFC1918) toegestaan, met uitzondering van systemen in de Rode zone.
- IP adressen worden uitgegeven per NDC. Dit betekent dat IP adressen tussen GTN NDC's niet uitwisselbaar zijn.
- Aanvraag voor publieke IPv4 adressen dienen goed onderbouwd aangevraagd te worden bij ICT-O netwerken.
- Publieke IPv4 adressen mogen alleen voorkomen op systemen in de Rode zone van het GTN.
- Statische IP adressering is vereist; dynamische IP adressering (DHCP) is niet toegestaan.

2.8 Omvang van verkeer

De omvang en frequentie van de netwerkcommunicatie dient afgestemd te zijn op wat functioneel noodzakelijk is en technisch verantwoord. Hierbij is het streven om de frequentie laag en de omvang klein te houden. Dit dient in de vorm van een verkeersmatrix te worden afgestemd met ICT Infravoorzieningen - Netwerken.

2.9 Koppelingen externe partijen

Zoals beschreven is het GTN het koppelvlak tussen de interne infrastructuur en externe partijen en internet. Voor externe aansluitingen op het GTN (Internet, derde partijen) gelden de aansluitvoorwaarden zoals gesteld in [AVD].

Colofon

Titel	Aansluitvoorwaarden Generieke Toegangsnetwerk
Documentnummer	
Versie/Datum	1.3 / 5 augustus 2021
Status	Definitief
Van	ProRail ICT Infravoorzieningen - Netwerken
Auteur	Marco de Heuvel/Hans van der Spek/Joeri Bos
Projectleider	
Distributie	
Document	Aansluitvoorwaarden Generiek Toegangsnetwerk GTN v1.3.docx

Autorisatie

	Paraaf	datum
gecontroleerd prl	_____	_____
projectleider	_____	_____