

1 Klant Router Requirements

1.1 Inleiding

In dit hoofdstuk worden de requirements beschreven waaraan de Klant Router dient te voldoen wil de klant met succes een verbinding maken met de KPN Zakelijk Internet dienst Corporate Internet.

Aangezien de klant verantwoordelijk is voor zijn eigen apparatuur staat hem dan ook vrij te doen en te laten wat hij wil met deze apparatuur. De klant dient er wel van bewust te zijn dat als NIET aan de verplichte requirements voldaan wordt de door hem afgenomen dienst waarschijnlijk NIET gaan werken.

Als de klant een router uit de "white-list" gebruikt zijn er voorbeeld configuraties beschikbaar van de Cisco router die door KPN getest zijn. Met deze configuraties als leidraad zal een klant dus zonder veel problemen zijn aansluiting werkend kunnen krijgen.

Feit is wel dat de klant ZELF verantwoordelijk is voor het werkend krijgen van zijn verbinding met een eigen router. KPN zal bij oplevering de verbinding testen met een KPN router en deze router na verificatie van de correcte werking van de verbinding weer meenemen zodat daarna de klant zelf zijn apparatuur kan aansluiten.

In onderstaande paragrafen staan meerdere requirements. Deze requirements zijn in de volgende gradaties ingedeeld:

Verplicht:	Deze requirements zijn absoluut vereist voor correcte werking.
Zeer sterk aanbevolen:	Deze requirements zijn niet absoluut noodzakelijk, maar de klant doet er wel ZEER verstandig aan deze te implementeren voor bijv. de veiligheid van zijn LAN
Aanbevolen:	Deze requirements zijn niet absoluut noodzakelijk, de klant kan naar eigen inzicht wel of niet aan deze requirements voldoen.

1.2 Verkorte verplichte requirements lijst

In de volgende paragrafen staan ALLE requirements in meer detail weergegeven. In deze paragraaf volgt een korte lijst met de VERPLICHTE requirements:

- Ethernet IEEE 802.3 (2005) ondersteuning van 10Base-T en 100Base-T (of 1000BaseT en 1000Base-SX indien bandbreedte dat vereist)
- PPPoE (RFC 2516, 1661)
- PPP IPCP netmask request (Cisco implementatie RFC 1332)
- PPP PAP Authenticatie (RFC 1334)
- IP subnet zero
- TCP mss aanpassing voor op elkaar afstemmen van Etherneten PPPoE MTU waarden

1.3 Connectiviteit requirements

1.3.1 Ethernet / IEEE 802.3-2005

a). 10Base-T/100Base-T full duplex (**verplicht**)

Zie: (<http://en.wikipedia.org/wiki/Ethernet>) en (http://en.wikipedia.org/wiki/IEEE_802.3-2005)

Aansluiten op Corporate Internet NT geschiedt via Ethernet Cat5e (of hoger) kabel, De WAN poort van de klant router (waarop de NT aangesloten wordt) dient minimaal de 10BaseT full duplex aansluit snelheid te ondersteunen. Voor Corporate Internet verbindingen van 10 Mbit/s en hoger dient minimaal 100BaseT full duplex ondersteund te worden.

b). 1000Base-T full duplex of 1000Base-SX (**verplicht bij snelheden boven 80Mb/s**)

Zie: (http://en.wikipedia.org/wiki/Gigabit_Ethernet)

Voor Corporate Internet verbindingen boven 80 Mb/s is aansluiting op gigabit snelheid benodigd. Met 100Base-T kan "slechts" tot 80 Mb/s gegarandeerd worden (bij versturen/ontvangen enkel kleine IP pakketen)

Dus voor snelheden boven 80 Mb/s kan men kiezen tussen 1000Base-T en 1000Base-SX (fiber) aansluiting als WAN poort.

1.3.2 PPPoE / PPP

c). RFC 2516 PPPoE (<http://tools.ietf.org/html/rfc2516>) (**verplicht**)

Voor Corporate Internet wordt gebruik gemaakt van PPPoE zoals beschreven in RFC 2516

d). RFC 1661 PPP (<http://tools.ietf.org/html/rfc1661>) (**verplicht**)

Onderliggend aan PPPoE wordt PPP volgens RFC 1661 gebruikt.

e). RFC 1332 PPP Internet Protocol Control Protocol (<http://tools.ietf.org/html/rfc1332>) (**verplicht**)

Bij Zakelijk Internet van KPN krijgt de klant niet 1 IP adres zoals gebruikelijk is voor internet diensten voor particulieren, maar een blok van IP adressen (8, 16, 32, enz. IP adressen). Om tijdens de opbouw van de PPP sessie een IP blok aan de klant router uit te delen dient de klant router een speciaal verzoek te doen. Dit is de zogenaamde "ipcp netmask request", de implementatie van deze feature kan voor iedere fabrikant verschillend zijn. De klant router is verplicht dit verzoek van het netmask werkend te hebben voor de Cisco implementatie aan de Acces Router zijde. Dit wil niet zeggen dat de klant router een Cisco router moet zijn, maar deze moet wel compatible zijn met de Cisco implementatie van de IPCP netmask request.

Zie: (http://www.cisco.com/en/US/docs/ios/12_1/12_1dc/feature/guide/ipcp_msk.html)

f). QOS op IP nivo (**zeer sterk aanbevolen**)

De klant router dient de volgende mogelijkheden te hebben om bepaalde in te stellen verkeerstypen (VOIP verkeer bijv.) voorrang te geven op overig verkeer.

- QOS dient handmatig instelbaar te zijn op basis van source & destination IP, IP protocol en TCP/UDP poort nummers.
- Scheduling van QOS regels.

g). Shaping van upstream verkeer (**aanbevolen**)

De klant router dient een vorm van traffic-shaping te ondersteunen. D.m.v. traffic shaping kan de klant de hoeveelheid verkeer dat per tijdseenheid richting internet verstuurd wordt afstemmen op de afgenomen bandbreedte, hierdoor verkrijgt de klant een “netter” verkeers patroon en hoeft excessief upstream klant verkeer niet door het EVPN netwerk ge-policed (weggegooid) te worden.

1.3.3 Authentication Support

a. RFC 1334 PPP PAP Authenticatie (<http://tools.ietf.org/html/rfc1334>) (**verplicht**)

Corporate Internet maakt gebruik van PPP PAP om de PPP sessie te authenticeren en zodoende de klant router van het juiste ip adres en subnet masker voorzien. Hiervoor moet de klant router tijdens de PPP authenticatie een request met een username EN password doen, geen van beide velden mogen leeg zijn.

De username en password zijn in principe vrij te kiezen, maar men doet er verstandig aan geen vreemde tekens te gebruiken. Gebruik bijvoorbeeld voor username: <bedrijfsnaam> (zonder spaties en zonder “<” en “>”) en password: KPN

1.3.4 Performance

Belangrijk punt is natuurlijk de performance van de router. De klant dit zelf rekening te houden of zijn router wel over voldoende performance beschikt om de afgenomen internet bandbreedte te kunnen behappen.

Richtwaarden van de door KPN geleverde routers (up- en downstream synchroon verkeer):

Siemens 5880 series:	20Mb/s max
Cisco 87x series:	20Mb/s max
Cisco 18xx series:	60Mb/s max
Cisco 28xx series:	60Mb/s max
Cisco 38xx series:	120Mb/s max

1.4 Features requirements

1.4.1 Security Support

a). Anti-spoofing Internet -> klant (**aanbevolen**)

Binnen Corporate Internet wordt gespoofed (vervalste IP pakketen) verkeer vanuit de klant lokatie geblokt naar het internet (een klant kan alleen verkeer sturen met een source ip adres die aan de klant behoort). Verkeer blokkeren vanaf het internet met destination ip address anders dan die van het klantnetwerk is een anti-spoofing maatregel die op de klant router moet gebeuren.

b). Access-lists / Firewall opties (**zeer sterk aanbevolen**)

Met behulp van Firewall opties en Access-Lists moet het klant netwerk verder beveiligd worden. Als de klant geen publieke servers heeft staan moeten sessies alleen gestart kunnen worden vanaf het klantdomein. Als een klant wel publieke servers heeft staan (mailserver, webserver, ...) dan moeten sessies vanaf het internet alleen worden toegestaan naar deze publieke servers. Uitgebreidere security mogelijkheden worden vaak mogelijk als er naast de klant router nog een volledige Firewall wordt ingericht.

c.) Geïntegreerde Firewall (**zeer sterk aanbevolen**)

Een klant router die uitgevoerd is met een geïntegreerde firewall geniet de voorkeur. De firewall dient het mogelijk te maken vrij instelbare poorten en protocollen te blokken/door te laten naar gelang wat van toepassing is.

d). Toegang tot klant router beperken (**zeer sterk aanbevolen**)

Relatief vaak zijn incorrect ingestelde klant routers vanaf de WAN kant te benaderen op http, snmp, telnet, ssh, etc. Toegang tot de klant router zou beperkt moeten worden toegestaan vanaf het LAN segment van de klant, of in het geval van de door een Business partner beheerde klant router, alleen vanaf de Business Partner.

e). Snmp community string instelbaar (**zeer sterk aanbevolen**)

Als een klant router uit te vragen is met snmp, blijkt de snmp community string vaak op public of private te staan. Via SNMP is het dan ook mogelijk om instellingen op te vragen en te wijzigen. Naast het punt beschreven in 4c, is er tevens het dringende advies om deze snmp community strings te wijzigen naar een andere instelling, zodat de klant router vanaf het internet niet of in elk geval niet zonder de juiste SNMP string te benaderen is.

f). Username/Password for login (**zeer sterk aanbevolen**)

Naast het punt beschreven in 1.3.1. c) (Toegang tot klant router beperken), is het zeer sterk aanbevolen om toegangsmogelijkheid voor login (http of telnet) verder te beveiligen. Dit kan o.a. met

SSH Tacacs gerealiseerd worden. Als dit niet ondersteund wordt zou in ieder geval het default password aangepast moeten worden.

g). De GUI dienst aan de volgende zaken te voldoen (**zeer sterk aanbevolen**)

- Interface dient volledig voor de eindgebruiker beschikbaar te zijn onder één inlog account (profiel).
- De diagnostic functie dient over duidelijke details te beschikken mbt tot de status van de verbinding. Deze moet onderscheid kunnen maken tussen verschillende fases in de opbouw van de PPPoE verbinding.
- Totale logging van connecties over firewall en routing van NAT verkeer met source & destination adres, port nummer en drop/accept.
- System summary en export/save van configuratie.

1.4.2 Netwerk gerelateerde zaken

a). NAT/PAT (**aanbevolen**)

De klant router zou NAT/PAT (Network Address Translation en Port Address Translation), multi-NAT (i.c.m. IPCP reeks) dienen te ondersteunen volgens RFC 1631, 2663, 3022 en 3027.

D.m.v. NAT/PAT kan een klant meer hosts aansluiten op zijn LAN dat het aantal vrije IP adressen die door Zakelijk Internet wordt aangeboden.

b) Priorisering (class based) IP verkeer (**aanbevolen**)

De klant router dient een prioriserings algoritme te hebben die bepaalde typen IP verkeer (bijv. VOIP) voorrang geeft t.o.v. van ander IP verkeer, deze prioriteiten dienen instelbaar te zijn en bij voorkeur voor meerdere typen IP verkeer. Bijv. Class Based Weighted Fair Queueing (CBWFQ), Link Fragmentation and Interleaving (LFI), Low Latency Queueing (LLQ) algoritmes.

De klant dient zelf te beslissen welk type verkeer prioriteit krijgt over andere typen verkeer.

1.4.3 Overig

a). Ip subnet-zero (**verplicht**)

De klant router moet om kunnen gaan met het 1^e subnet uit een reeks. Bv. 194.151.0.0/27 (historisch gezien is dit een probleem geweest in bij een aantal vendors). Voor meer info:
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080093f18.shtml

b). Wall mountable (**aanbevolen**)

In de praktijk is de ervaring opgebouwd dat apparatuur die aan de muur wordt vastgeschroefd (bv. Naast een ISDN centrale) minder snel wordt uitgeschakeld door de klant. Hierdoor kunnen een aantal storingen voorkomen worden.

c). Automatisch aan na stroomonderbreking (**zeer sterk aanbevolen**)

Enkele merken klant routers gaan na een stroomonderbreking niet automatisch aan. Voor de Corporate Internet dienst wordt zeer sterk aanbevolen om een router te selecteren die na een stroomonderbreking wel automatisch opstart.

Speciale features

a). MSS aanpassing (**verplicht**)

Hoewel deze feature niet absoluut vereist is, is hij wel dusdanig belangrijk dat men hem eigenlijk als verplicht dient te beschouwen. Zonder implementatie van deze feature in de klant router is het zeer waarschijnlijk dat het internet verkeer niet naar behoren gaat werken en kunnen er vage klachten ontstaan.

De vereiste voor de MSS aanpassing feature komt doordat er voor Corporate Internet gebruikt gemaakt wordt van PPPoE. In de RFC van PPPoE wordt er vanuitgegaan dat de maximale payload grootte van een Ethernet frame 1500 bytes is. Aangezien de PPP header zelf ook nog 8 bytes beslaat blijft er voor het IP pakket (in totaal) 1492 bytes over. Aangezien de IP header 20 bytes beslaat en de TCP header ook 20 bytes blijft er als TCP/IP payload 1452 bytes over.

Het huidige internetverkeer bestaat voor het overgrote deel van het verkeer uit IP/TCP verkeer.

Zie: (http://en.wikipedia.org/wiki/Transmission_Control_Protocol)

TCP heeft als mechanisme dat het bij het opzetten van een verbinding tussen 2 hosts op het internet wordt onderhandeld over de maximale packet grootte die de hosts naar elkaar kunnen verzenden en ontvangen. Dit is de zogenaamde MSS onderhandeling en hosts gebruiken over het algemeen de maximum waarde van hun LAN payload: 1500 bytes (Ethernet) – 20 bytes (IP header) – 20 bytes (TCP header) = 1460 bytes. Dit is dus voor een ethernet LAN de MSS waarde voor TCP.

Zie: (http://en.wikipedia.org/wiki/Maximum_segment_size)

Zoals eerder voorgerekend is de MSS waarde voor een PPPoE tunnel 1452 bytes. Als hosts van de klant verkeer richting internet versturen en uitgaan van een MSS waarde van 1460 bytes, zullen deze pakketten niet door de PPPoE tunnel passen en is de kans groot dat de verkeersstroom niet op gang komt en de klant dus bijvoorbeeld een opgevraagde webpagina niet te zien krijgt.

Er dient dus een mechanisme te zijn die de MSS onderhandeling tussen twee hosts op 1452 bytes "bemiddeld". Dit heet de MSS aanpassing feature en dient op de klant router te geschieden.

Op Cisco routers is de feature te activeren met het commando "ip tcp adjust-mss 1452" op het LAN interface. Hierdoor zullen alle MSS onderhandelingen door de router "bemiddeld" worden op 1452 bytes. Dit heeft tot effect dat TCP verkeerstromen zonder probleem door de PPPoE tunnel past.

Het is dus zeer belangrijk dat de klant router een vorm van MSS aanpassing ondersteund. Hoe dit bij het betreffende merk klant router geactiveerd dient te worden zal de klant zelf bij de fabrikant moeten achterhalen.

Bijlage A – “white-list” routers

De volgende routers zijn door KPN getest en met de juiste config zullen zij naar verwachting zonder problemen met de Corporate Internet en Internet Fiber diensten van KPN functioneren.

- Cisco 87x Series Router
- Cisco 18xx Series Router
- Cisco 28xx Series Router
- Cisco 38xx Series Router
- Cisco 720x VXR Series Router met NPE-G1 processor board

Hieronder volgt een uittreksel van een voorbeeld config met de belangrijkste punten om een Cisco router werkend op de Corporate Internet of Internet Fiber dienst aan te sluiten.

DHCP pool definitie

```
ip dhcp pool IAS
  import all
  origin ipcp
  dns-server 194.151.228.18 194.151.228.34
```

WAN interface config

```
interface FastEthernet0
  description WAN Link to EVPN CPE
  no ip address
  load-interval 30
  speed auto
  full-duplex
  pppoe enable
  pppoe-client dial-pool-number 1
  no shut
```

LAN interface config

```
interface FastEthernet1
  description LAN interface
  ip address pool IAS
  ip verify unicast reverse-path
  load-interval 30
  ip tcp adjust-mss 1452
  no shut
```

PPPoE dialer

```
interface Dialer1
  description Customer Traffic PPPoE Connection
no shut
  ip address negotiated
  ip verify unicast reverse-path
  encapsulation ppp
  mtu 1492
  dialer pool 1
  dialer-group 1
  ppp pap sent-username KPN password 0 KPN
  ppp ipcp mask request
  ppp ipcp address accept
```

Default route

```
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1
```