

Port Forwarding op een Netgear

1. Inleiding

Netgear routers zijn standaard uitgerust met een dubbele firewall: de NAT en de SPI. Deze twee firewalls beschermen aangesloten PC's en de daarop aanwezige data tegen inbraak van "hackers" via het internet. Intern heeft de Netgear router 65535 poorten (=registers) die gebruikt kunnen worden voor communicatie met internet en andere computers. Hiervan staat standaard maar een klein aantal open voor het hoogstnodzakelijke verkeer. De firewall staat dusdanig ingesteld dat slechts via deze zeer specifieke poorten verkeer mogelijk is. De overige poorten zijn afgesloten om misbruik van een open, onbewaakte poort te voorkomen.

Doordat slechts enkele poorten open staan kan het dus voorkomen dat bepaalde software of hardware applicaties niet met het internet kunnen communiceren, terwijl ze dit eerder zonder aangesloten router wel konden. De Netgear router blokkeert dan waarschijnlijk de poorten die deze applicatie wil gebruiken.

De oplossing is dan meestal de router zodanig te configureren dat de poorten alsnog worden geopend. De poorten openen en/of uitschakelen in de firewall kan op 5 manieren worden gedaan.

Hieronder worden de methoden beschreven.

2. Login

Als eerste dient men in te loggen op het routermenu van de router. Dit doet men via een internetbrowser zoals Firefox, Netscape of Internet Explorer. Op de adresbalk van de browser typt men voor een ongeconfigureerde router (direct na een reset): <http://192.168.1.1/basicsetting.htm> of <http://www.routerlogin.com/basicsetting.htm>



Voor een al werkende en/of geconfigureerde router tikt men <http://192.168.1.1> of <http://www.routerlogin.com> in. De iets oudere Netgear routers hebben nog het toegangsadres <http://192.168.0.1> of <http://192.168.0.1/basicsetting.htm>

Het kan zijn dat men na de login gevraagd wordt om een gebruikersnaam en een wachtwoord.

Deze zijn normaal:

	Standaard router	UPC	@home
Gebruikersnaam	admin	admin	admin
Wachtwoord	password	UPC	draadloos

Na een succesvolle inlog ziet men dan het scherm "Basic Settings" verschijnen met de vraag:

"Does Your Internet Connection Require A Login" of het menu "Router Status". Dit scherm laat men voor wat het is en men gaat hieronder verder.

3. Methoden

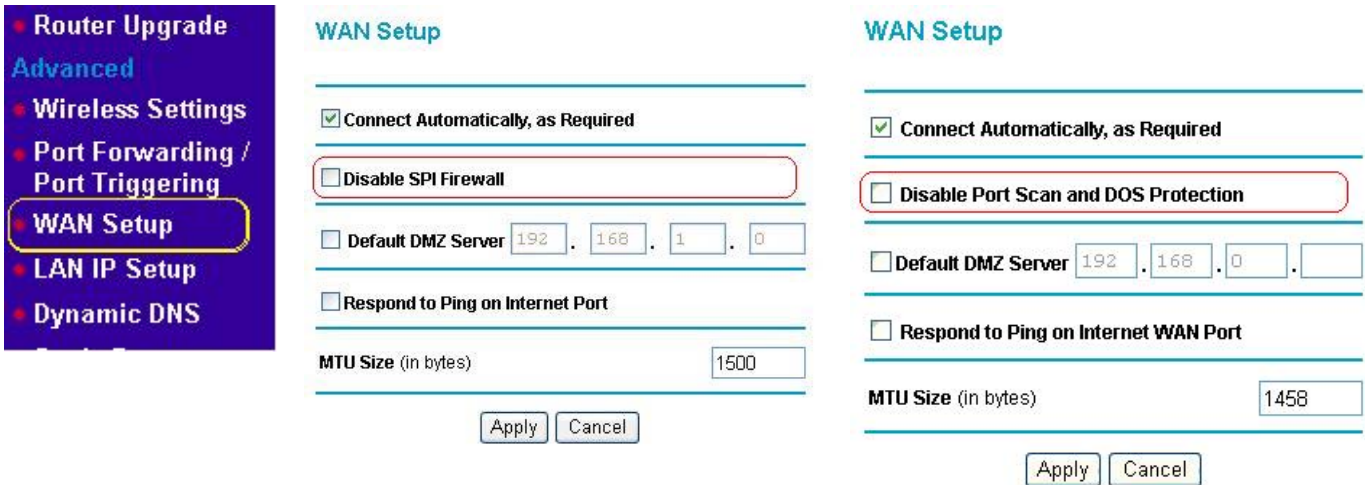
Voor het openen van poorten in de router's SPI firewall zijn er 5 methoden beschikbaar. Hieronder zullen deze worden behandeld.

3.1 Uitzetten SPI firewall

Een van de eenvoudigste mogelijkheden is de Netgear firewall compleet uit te schakelen zodat alle verkeer ongehinderd naar alle randapparatuur kan doorgaan. Dit is voornamelijk van toepassing wanneer alle PC's en randapparatuur al beschermd worden door een ander type firewall (Windows, McAfee, Norton, Zonealarm, etc).

Het uitschakelen van de SPI firewall doet men in het menu "WAN Setup" onder het kopje "Disable SPI firewall" of "Disable Port Scan and DOS Protection".

Men krijgt dan een scherm te zien dat lijkt op het onderstaande.

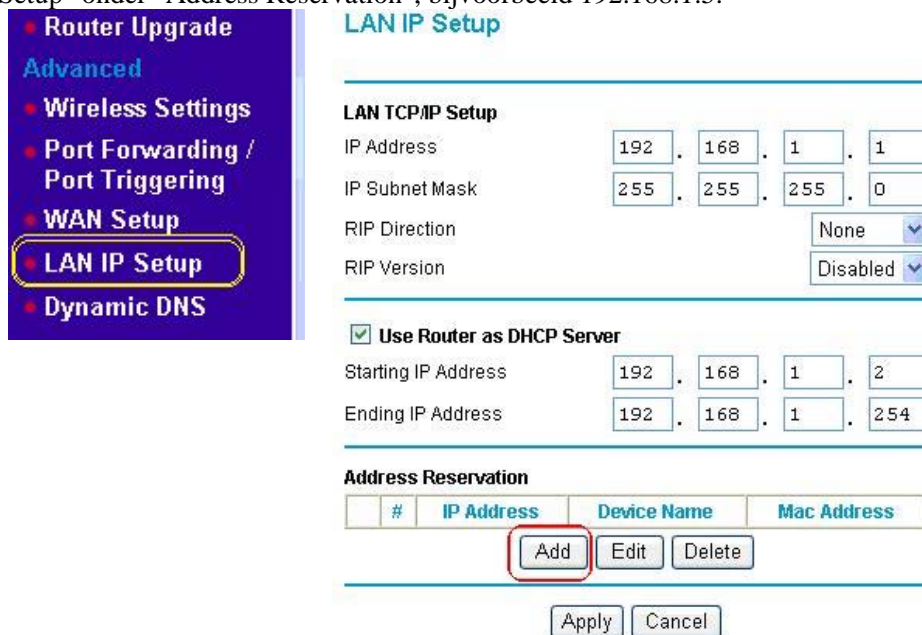


Wanneer men een vinkje plaatst in het geselecteerde veld en vervolgens “Apply” klikt, wordt de Netgear SPI firewall uitgeschakeld. Voor deze functie hoeft men geen verdere instellingen te doen.

3.2 DMZ

DMZ staat voor “Dé Militarized Zone”. De DMZ doet ongeveer hetzelfde als het uitschakelen van de firewall, maar slechts voor in totaal één randapparaat. Voor de andere aangesloten apparaten blijft de firewall dus actief.

Men geeft het specifieke apparaat waarmee men de DMZ- wil gaan gebruiken een vast (statisch) IP adres in het menu "LAN IP Setup" onder "Address Reservation", bijvoorbeeld 192.168.1.5.



Men heeft hiervoor wel het MAC-adres nodig van de betreffende netwerkkaart die de verbinding maakt met de router. Dit MAC adres kan men o.a. vinden door via de MS-DOS prompt het commando "IPCONFIG /ALL" te geven of door het aflezen van het apparaat aangezien het vaak ook op de zijkant wordt afgedrukt. Het MAC adres ziet er uit als een reeks van 12 cijfers en letters, zoals: "00A0732F7B11"

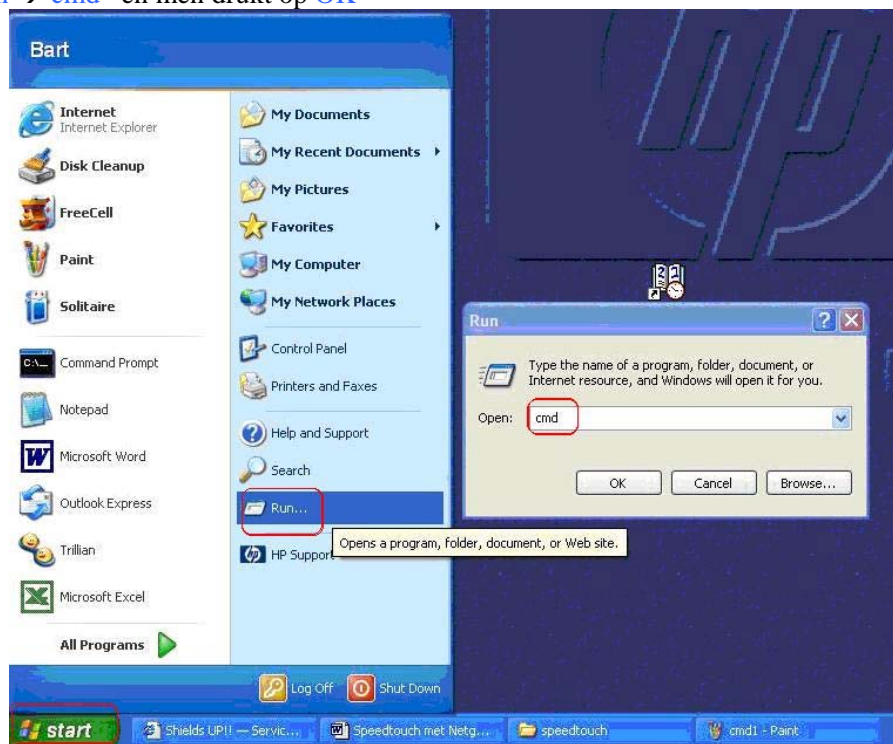
Address Reservation

Address Reservation Table

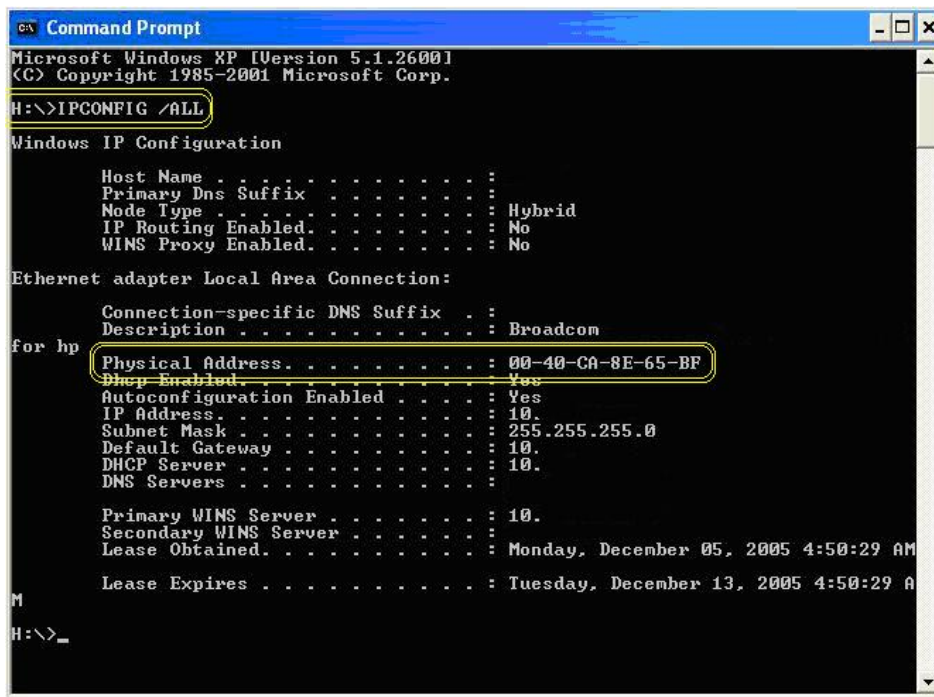
	#	IP Address	Device Name	MAC Address
IP Address		192 . 168 . 1 . 5		
MAC Address				00A0732F7B11
Device Name			maguzelfbepalen	

Indien u het MAC-adres van de netwerkkaart niet bekend is dan gaat men naar:

Start → Uitvoeren → cmd en men drukt op OK



In het scherm MS-DOS scherm dat zich nu opent tikt men dan het commando: **“IPCONFIG /ALL”**.



Het **Fysieke adres (Physical Address)** dat bij de LAN verbinding staat vermeld is het MAC-adres dat wordt gezocht. Let wel op dat hier het juiste adres wordt overgenomen en niet per ongeluk dat van een andere adapter, anders werkt het niet. Dit geldt zowel voor draadloze WLAN adapters als voor de vaste LAN adapters. Na de invoer van het fysieke adres ziet het menu “Lan IP Setup” er dan als volgt uit:

LAN IP Setup

LAN TCP/IP Setup

IP Address: 192 . 168 . 1 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

RIP Direction: None

RIP Version: Disabled

Use Router as DHCP Server

Starting IP Address: 192 . 168 . 1 . 2

Ending IP Address: 192 . 168 . 1 . 51

Address Reservation

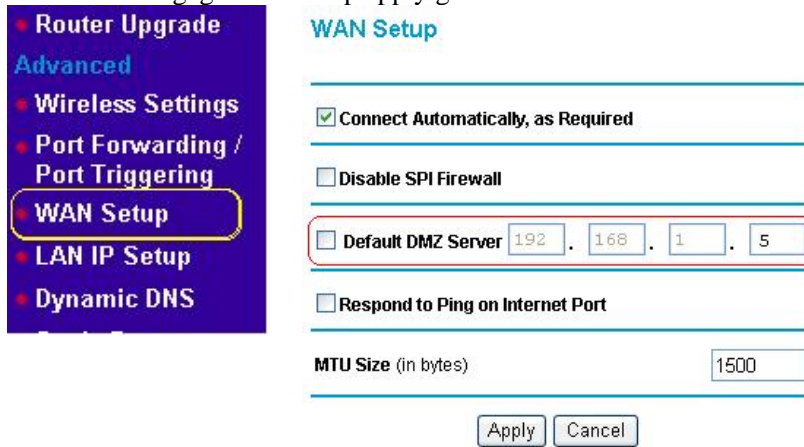
#	IP Address	Device Name	Mac Address
1	192.168.1.5	maguzelfbepalen	00:A0:73:2F:7B:11

Add Edit Delete

Apply Cancel

Hier klikt men op de knop “Apply”.

In het menu “WAN Setup” definieert men de DMZ naar het IP adres dat werd toegekend in het menu “LAN IP Setup”, zoals hieronder wordt weergegeven. Na op apply geklikt te hebben wordt de DMZ dan actief.

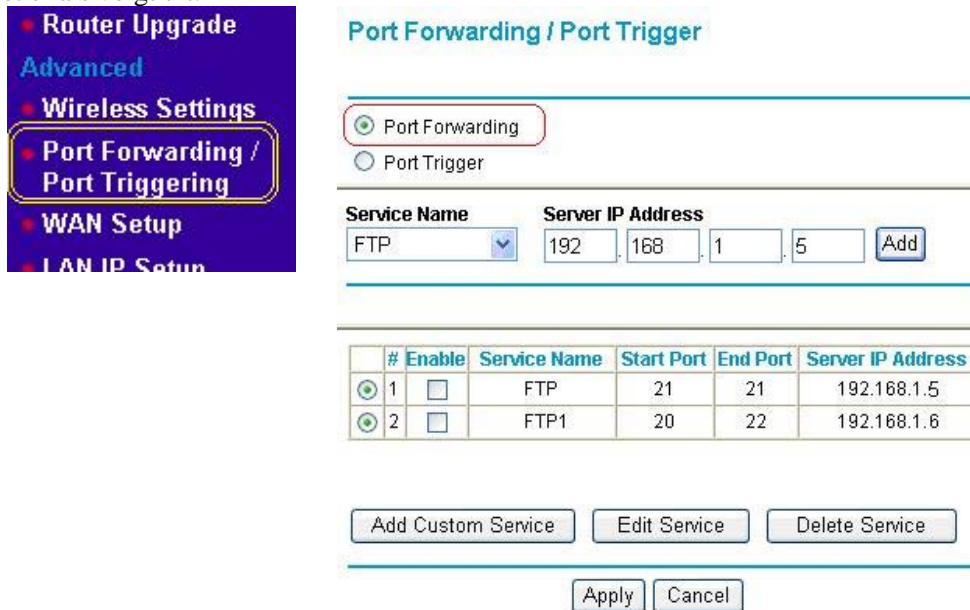


3.3 Port Forwarding

Ook bij deze functie wordt gebruik gemaakt van een statisch IP-adres uit de “Address Reservation” tabel van het menu “LAN IP Setup”.

Port forwarding opent langdurig in de SPI firewall specifieke poorten naar één of meerdere IP adressen van aangesloten apparaten. Andere poorten dan degene toegewezen blijven hiermee gesloten en ongemoeid.

Het menu ziet er als volgt uit:



Men selecteert de benodigde “Service Name” en kent aan deze service naam het geregistreerde IP-adres toe. Heeft men geen geschikte “Service Name” of wil men een nieuwe functie toevoegen, dan creëert men een Service name door op “Add Custom Service” te klikken.

Onderstaand scherm laat zien hoe dit werkt:

Ports - Custom Services

Enable

Service Name

Starting Port (1~65535)

Ending Port (1~65535)

Server IP Address . . .

Wil men een tweede computer laten werken met precies dezelfde poorten, dan dient men voor dit nieuwe apparaat een "reeks" van poorten aan te maken. Eerst dient men dan nog een nieuwe "Service" te creëren met een nieuwe naam.

Vervolgens kent men dan aan deze nieuwe "Custom Service" een reeks toe. Gebruikte men voor het eerste apparaat poort 21, dan wordt voor het tweede apparaat de poorten geplaatst op Start port 20- End port 22, PC3 op 19-23, etc.

[3.4 Port Triggering](#)

Port triggering werkt op eenzelfde principe als Port Forwarding, maar echter voor een beperkte duur. Dat betekent dat na een bepaalde tijd (de Port Triggering Timeout) de poort automatisch weer wordt vrijgegeven voor een andere PC of randapparaat. Deze functie is bijvoorbeeld toepasbaar voor applicaties die maar voor korte duur specifieke poorten nodig hebben zodat ze daarna snel weer beschikbaar kunnen zijn voor andere gebruikers.



Port Forwarding / Port Triggering

Please select the service type

Port Forwarding

Port Triggering

Disable Port Triggering

Port Triggering Timeout (in minutes)

Port Triggering Portmap Table

#	Enable	Service Name	Service Type	Inbound Connection	Service User
<input type="radio"/> 1	<input checked="" type="checkbox"/>	starcraft	TCP:6112	TCP/UDP:6112	ANY
<input type="radio"/> 2	<input checked="" type="checkbox"/>	paltalk_1	TCP:2090	TCP/UDP:2090	ANY

Het toewijzen van een specifieke poort gaat via de knop “Add Service”. Men krijgt dan onderstaand scherm waarin men de juiste service kan toevoegen.

Voor deze functie hoeft men geen statisch IP adres te definiëren in het menu “LAN IP Setup” wanneer men “Service User: Any” kiest.

Port Triggering - Services

Service

Service Name

Service User

. . .

Service Type

Triggering Port (1~65535)

Required Inbound Connection

Connection Type

Starting Port (1~65535)

Ending Port (1~65535)

3.5 UPnP

UPnP staat voor “Universal Plug and Play”. Deze functie in de router staat het bij nieuwere routers toe dat randapparaten die UPnP ondersteunen de router zelf verzoeken om specifieke poorten te openen. Men dient hiervoor wel UPnP in de router te activeren door “Turn UPnP On” aan te vinken. De gebruiker hoeft op dit vlak niets te doen behalve de functie in te schakelen. De applicatie zal dan zelf de afhandeling regelen.

Advanced

- Wireless Settings
- Port Forwarding / Port Triggering
- WAN Setup
- LAN IP Setup
- Dynamic DNS
- Static Routes
- Remote Management
- **UPnP**

upnp

Turn upnp On

Advertisement Period (in minutes)

Advertisement Time To Live (in hops)

upnp Portmap Table

Active	Protocol	Int. Port	Ext. Port	IP Address

De “Advertisement Period” is de tijd dat de router zijn huidige status doorstuurt aan de aangesloten randapparaten. Een kortere tijd resulteert in actuelere informatie maar ook meer gegevens verkeer.

De “Advertisement Time To Live” is het maximale aantal stappen dat een UPnP pakket moet overbruggen voordat deze aankomt bij zijn doel. Voor thuisgebruik is de waarde “4” meestal voldoende.

4. Poorten

Op de Netgear website http://kbserver.netgear.com/kb_web_files/n100495.asp kan men van veel programma's en applicaties terugvinden welke geopende poorten ze nodig hebben. Men moet er daar wel op letten dat de lijst nooit geheel volledig kan zijn.

Vraag in het geval van twijfel de fabrikant van het produkt om de juiste poort gegevens.