



**WL-351**

Wireless Gigabit Router 300N X3

**WL-368**

Wireless Gigabit Router 300N X2

**(802.11bgn)**



# Gebruikershandleiding

## INHOUDSOPGAVE

---

.....	1
.....	1
<a href="#"><u>1BELANGRIJKSTE KENMERKEN.....</u></a>	<a href="#"><u>4</u></a>
<a href="#"><u>2DE INHOUD VAN HET PAKKET.....</u></a>	<a href="#"><u>5</u></a>
<a href="#"><u>3AANSLUITPOORTEN.....</u></a>	<a href="#"><u>6</u></a>
<a href="#"><u>4NETWERK- EN SYSTEEMEISEN.....</u></a>	<a href="#"><u>8</u></a>
<a href="#"><u>5PLAATSING VAN DE WL-351/368.....</u></a>	<a href="#"><u>8</u></a>
<a href="#"><u>6LAN, WAN INSTELLEN.....</u></a>	<a href="#"><u>9</u></a>
<a href="#"><u>7INSTELLING PC-NETWERKADAPTER.....</u></a>	<a href="#"><u>10</u></a>
<a href="#"><u>8DE WL-351/368 OPSTARTEN.....</u></a>	<a href="#"><u>14</u></a>
<a href="#"><u>9 EERSTE INSTELLING VAN DE WL-351/368.....</u></a>	<a href="#"><u>14</u></a>
<a href="#"><u>10 CONFIGURATIEWIZARD.....</u></a>	<a href="#"><u>23</u></a>
<a href="#"><u>11 INSTELLINGEN DRAADLOZE VERBINDING.....</u></a>	<a href="#"><u>25</u></a>
<a href="#"><u>12 FIREWALL-INSTELLINGEN.....</u></a>	<a href="#"><u>36</u></a>
<a href="#"><u>13 GEAVANCEERDE INSTELLINGEN.....</u></a>	<a href="#"><u>42</u></a>
<a href="#"><u>14 INSTELLINGEN GEREEDSCHAP.....</u></a>	<a href="#"><u>53</u></a>

# Inleiding

Gefeliciteerd met uw aankoop van de WL-351/368 Wireless Gigabit Router 300N. De WL-351/368 is conform 802.11n en tot 6 keer sneller dan de standaardrouters die zijn gebaseerd op 802.11g, maar zijn ook nog steeds compatibel met 802.11g & 802.11b-apparaten. De WL-351/368 is niet alleen een Wireless Access Point, maar functioneert ook nog eens als een full-duplex Gigabit-switch met 4 poorten die uw bekabelde Ethernet-apparaten aan elkaar koppelt met een snelheid van 10/100/1000 Mbps.

Met een draadloze transmissiesnelheid van 300 Mbps maakt het Access Point in de router gebruik van geavanceerde MIMO (Multi-Input, Multi-Output)-technologie om in één enkel draadloos kanaal meerdere gegevensstromen te verzenden, waardoor u naadloos toegang hebt tot multimedia-inhoud. Het robuuste RF-signaal reist verder, elimineert "dead spots" en vergroot het netwerkbereik. Voor beveiliging en privacy van gegevens codeert WL-351/368 alle draadloze transmissies met WEP-, WPA- of WPA2-encryptie.

Met de ingebouwde DHCP-server en krachtige SPI-firewall worden door de WL-351/368 uw computers tegen indringers en de meeste internetaanvallen beschermd en wordt een veilige VPN Passthrough mogelijk gemaakt. Met de ongelooflijke snelheid en QoS-functie van 802.11n is de WL-351/368 ideaal voor allerlei mediatoepassingen, zoals streaming video, gaming en VoIP-telefonie, om tegelijkertijd door het netwerk meerdere media-intensieve gegevensstromen mogelijk te maken, zonder dat de prestatie achteruitgaat.

# 1 Belangrijkste kenmerken

---

Mogelijkheden	Voordelen
Ongelooflijke transmissiesnelheid tot 300 Mbps*	<b>Intensieve gegevensstromen zoals MPEG video streaming</b>
Conformiteit met IEEE 802.11n en achterwaartse compatibiliteit met 802.11b/g	<b>Volledige interoperabiliteit met IEEE 802.11b / IEEE802.11g-conforme apparaten en bescherming van oudere systemen</b>
Vier switchpoorten van 10/100/1000 Mbps gigabit (Auto-Crossover)	<b>Schaalbaarheid, vergroot uw netwerk</b>
Firewall ondersteunt virtuele server Mapping, DMZ, IP-filter, ICMP Blocking, SPI	<b>Voorkomt aanvallen van hackers of virussen vanaf het internet</b>
Ondersteuning voor 802.1x authenticator, 802.11i (WPA/WPA2, AES), VPN Passthrough	<b>Voorziet in wederzijdse authenticatie (sleutels voor client-encryptie en dynamische encryptie om beveiliging te vergroten)</b>
WDS (Wireless Distribution System)	<b>Maakt draadloze AP- en Bridge-modus tegelijkertijd tot een draadloze repeater</b>

*\* Theoretische snelheid van draadloos signaal gebaseerd op de gebruikte chipset van de IEEE-standaard 802.11a, b, g, n. Feitelijke doorvoer kan variëren. Netwerkomstandigheden en omgevingsfactoren verlagen de feitelijke doorvoersnelheid. Alle specificaties zijn zonder kennisgeving onderhevig aan wijziging.*

## **2 De inhoud van het pakket**

---

Open het pakket voorzichtig en controleer of alle hieronder genoemde onderdelen aanwezig zijn. Gooi verpakkingsmateriaal niet weg. U hebt het nodig als u het product moet retourneren; het product moet worden geretourneerd in de originele verpakking.

1. De WL-351/368 Router
2. Een 220V~240V netadapter
3. Een beknopte installatiehandleiding
4. Een CD (gebruikershandleiding)
5. Een garantiekaart
6. Een UTP-kabel

### 3 Aansluitpoorten

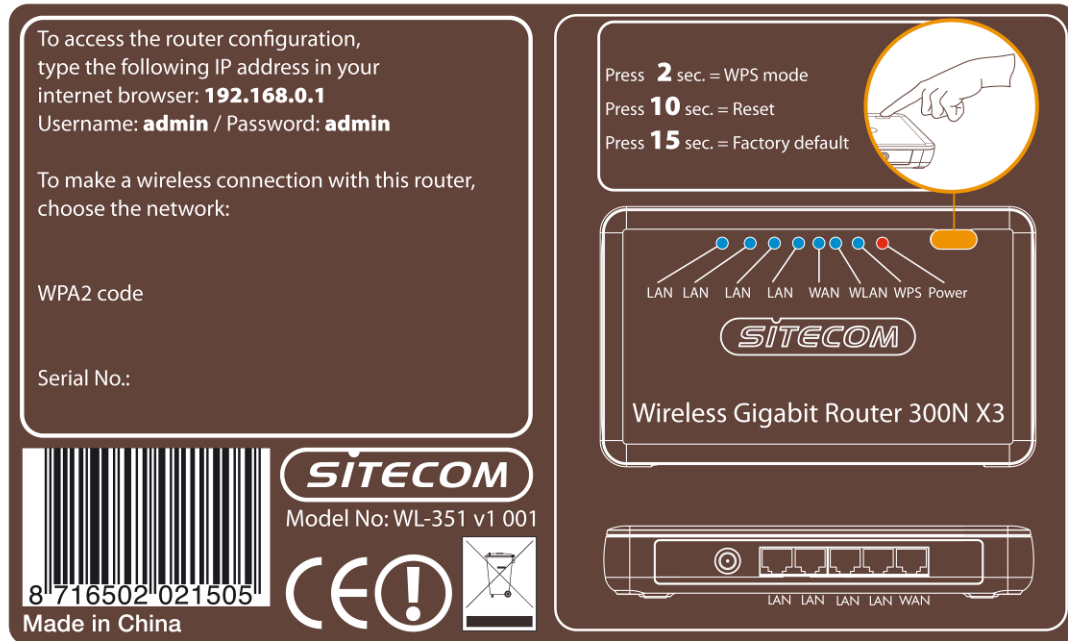
---



Poort	Beschrijving
Voedingspoort	Sluit de 12V DC-adapter aan op deze poort
LAN (Geel)	Sluit uw PC's of netwerkapparaten aan op deze poort
WAN (Blauw)	Sluit uw ADSL/kabelmodem aan op deze poort

## Label aan achterzijde

Het label aan de achterzijde beschrijft het IP-adres, de inloggegevens, SSID, beveiligingscode en functies van de WPS-knop.



Knop	Beschrijving
WPS-knop	2 seconden indrukken voor de WPS-modus 10 seconden indrukken om de router te resetten 15 seconden indrukken om de router te resetten naar de fabrieksinstelling.

## **4 Netwerk- en systeemeisen**

---

Controleer of uw systeem aan de hieronder genoemde eisen voldoet voordat u de WL-351/368 in gebruik neemt:

- PC/notebook.
- Besturingssysteem – Microsoft Windows XP/2000/VISTA
- 1 vrije Ethernet-poort.
- WiFi-kaart/USB-dongle (802.11 b/g/n) – optioneel.
- Extern xDSL (ADSL)- of kabelmodem met een Ethernet-poort (RJ-45).
- PC met een webbrowser (Internet Explorer, Safari, Firefox, Opera)
- Ethernet-compatibele CAT5-kabels.

## **5 Plaatsing van de WL-351/368**

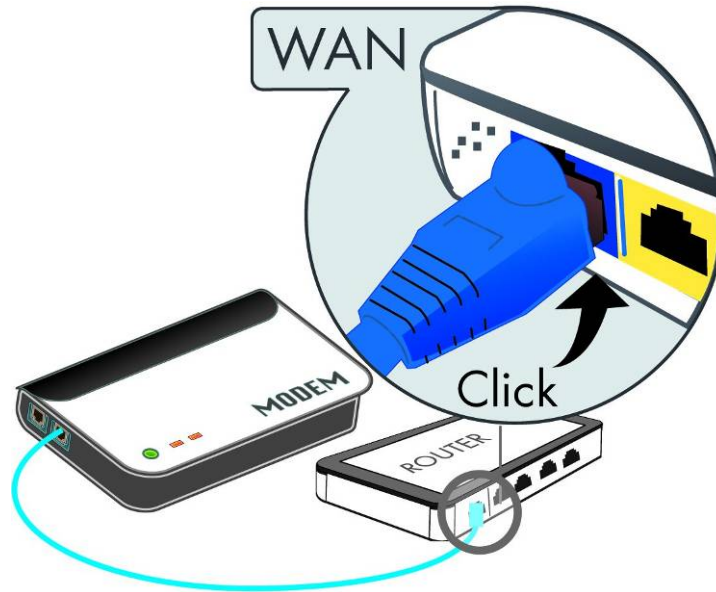
---

U kunt de WL-351/368 op een bureau of ander plat oppervlak plaatsen, of op een muur monteren. De WL-351/368 presteert optimaal als u de Wireless Broadband Router in het midden van uw kantoor (of uw huiskamer) plaatst, uit de buurt van mogelijke interferentiebronnen, zoals een metalen wand of een magnetron, in de buurt van een voedingsaansluiting en uw ADSL/kabelmodem.

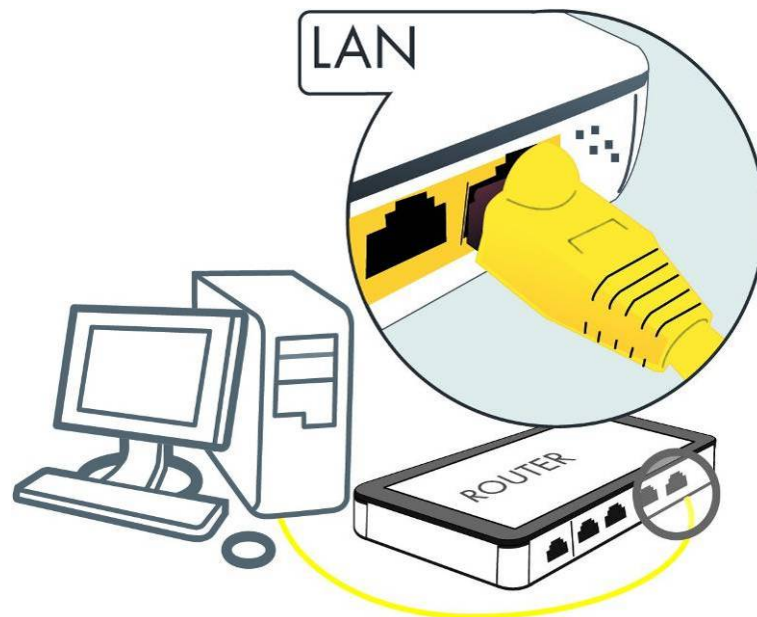
## 6 LAN, WAN instellen

---

WAN-verbinding:



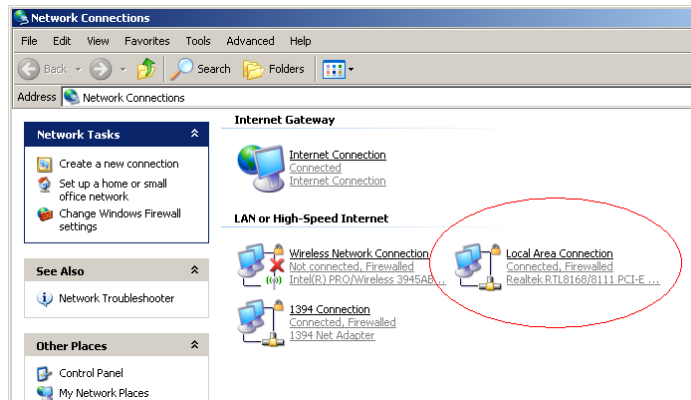
LAN-verbinding:



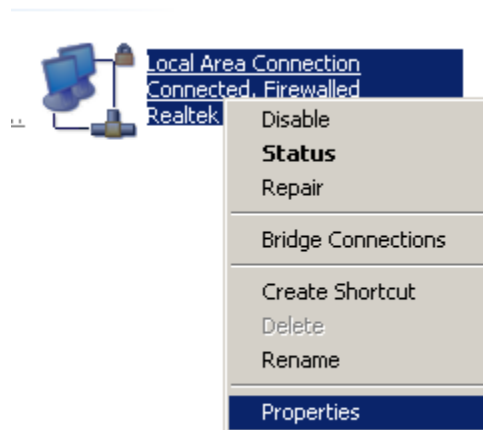
# 7 Instelling PC-netwerkadapter

## Windows XP

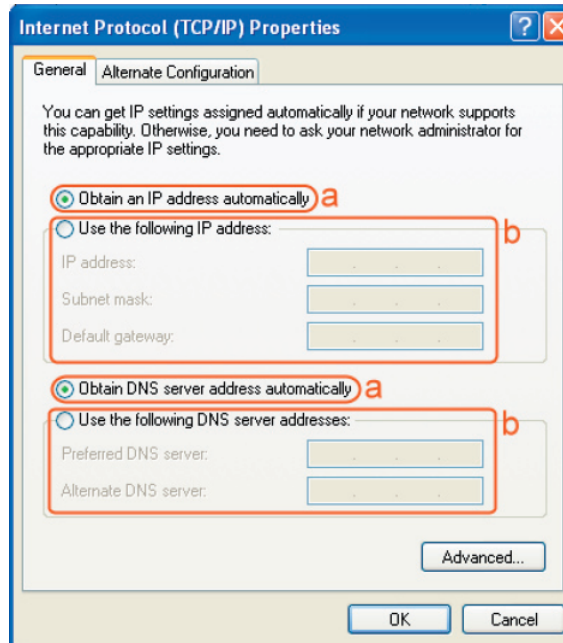
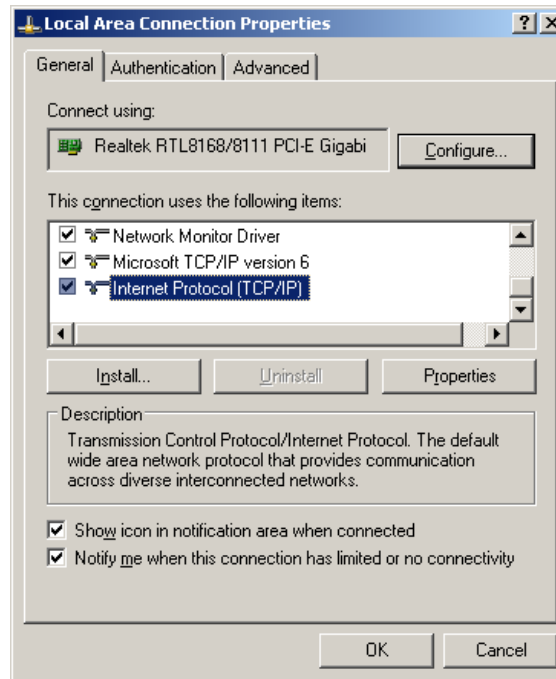
- Ga naar het menu [start] → selecteer [Configuratiescherm] → selecteer [Netwerkverbindingen].



- Selecteer het pictogram [LAN-verbinding])=>selecteer [Eigenschappen]



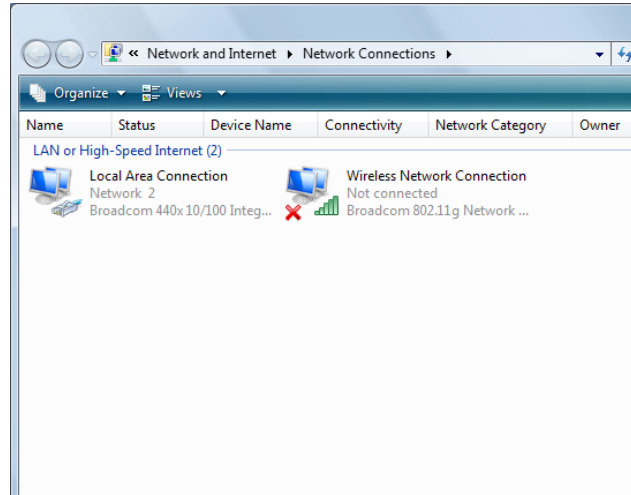
- Selecteer [Internet Protocol (TCP/IP)] =>Klik op [Eigenschappen].



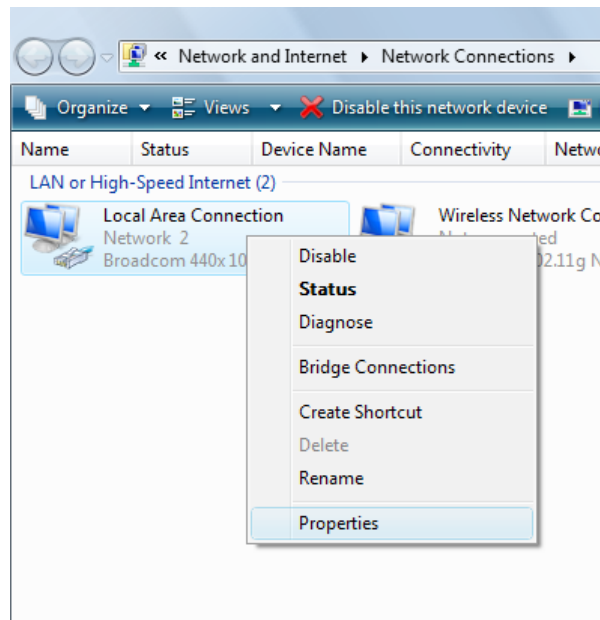
- Selecteer de tab [Algemeen].
  - a. De WL-351/368 ondersteunt de [DHCP]-functie; selecteer zowel [Automatisch een IP-adres laten toewijzen] als [Automatisch een DNS-serveradres laten toewijzen].

## Windows Vista

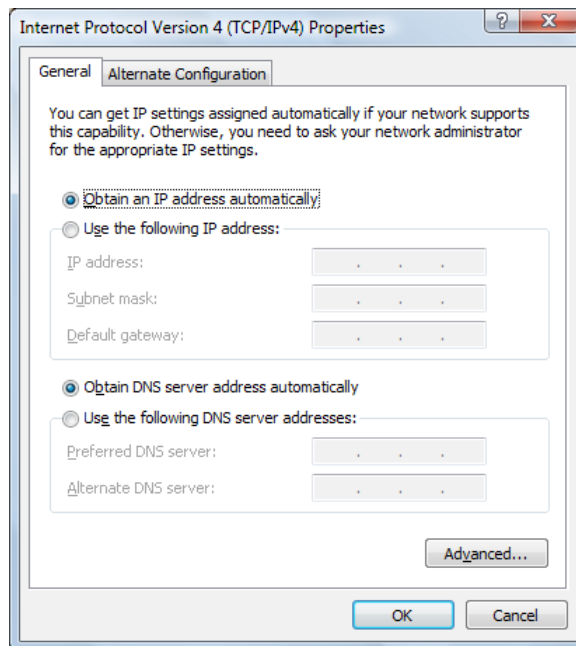
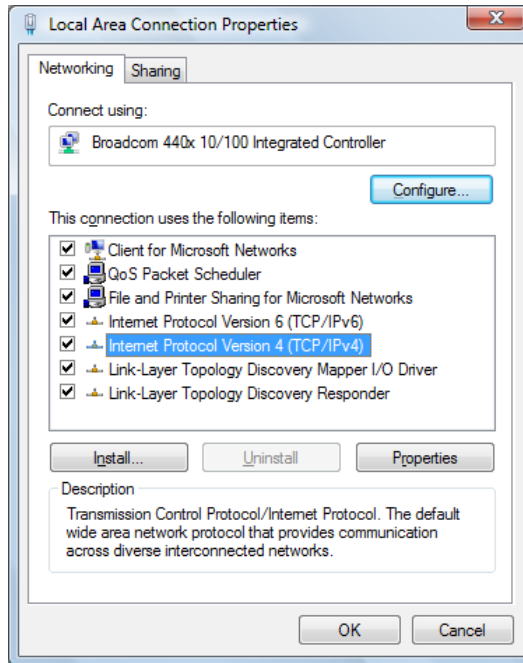
- Ga naar het menu [Starten] → selecteer [Configuratiescherm] → selecteer [Netwerkstatus en -taken weergeven] → selecteer [Netwerkverbindingen beheren].



- Selecteer het pictogram [LAN-verbinding])=>selecteer [Eigenschappen]



- Selecteer [Internet Protocol versie 4 (TCP/IPv4)] =>Klik op [Eigenschappen].



- Selecteer de tab [Algemeen].

De WL-351/368 ondersteunt de [DHCP]-functie; selecteer zowel [Automatisch een IP-adres laten toewijzen] en [Automatisch een DNS-serveradres laten toewijzen].

## 8 De WL-351/368 opstarten

---

Sluit de bijgeleverde netadapter aan op de voedingspoort en sluit de adapter aan op een stopcontact. De WL-351/368 komt vervolgens automatisch in de zelftestfase. Tijdens de zelftestfase brandt de voedings-LED continu om aan te geven dat dit product normaal werkt.

## 9 Eerste instelling van de WL-351/368

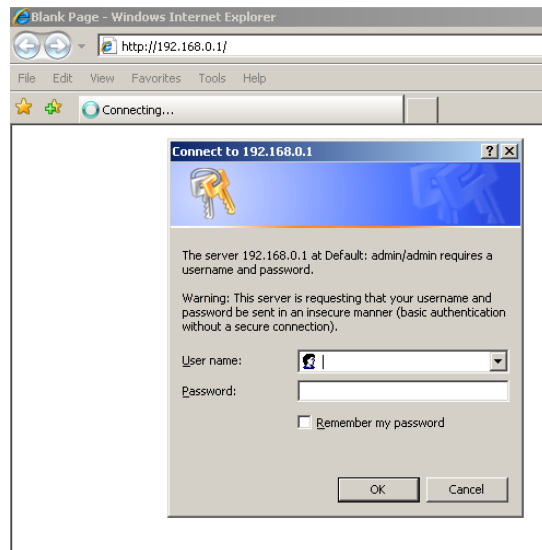
---

### Inlogprocedure


1. Open uw browser (bijv. Internet Explorer).



2. Typ <http://192.168.0.1> in de adresbalk en druk op [Enter]



3. Typ de gebruikersnaam en het wachtwoord (standaard is dit admin/admin).



Connect to 192.168.0.1

The server 192.168.0.1 at Default: admin/admin requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name:

Password:

Remember my password

OK Cancel

4. Klik op **OK**.
5. De home page van de WL-351/368 wordt vervolgens geopend.



**300N WIRELESS ROUTER** **SITECOM**

Status Wizard Wireless Settings Firewall Advanced Settings Toolbox Choose your language

System Status DHCP Server Device Status Internet Status DHCP Status Log Statistics

You can use the Status page to monitor the connection status for the WAN/LAN interfaces, firmware and hardware version numbers, any illegal attempts to access your network and information on all DHCP client PCs currently connected to your network.

**System**

Model :	Wireless Network Broadband Router
Uptime :	5 min 36 sec
Hardware Version :	Rev. A
Serial Number :	000000001
Boot Code Version :	0.7
Runtime Code Version :	0.1

Met de tab "System status" kunt u de huidige status van uw router bekijken.

Hier worden de verbindingstijd, hardware-informatie, het serienummer en informatie over de firmwareversie getoond.

## LAN-instellingen

Met de tab "DHCP-server" kunt u de IP-instellingen van de WL-351/368 wijzigen.

The screenshot shows the configuration interface for a 300N ROUTER WIRELESS. The page title is "300N ROUTER WIRELESS" with the "SITECOM" logo. The navigation menu includes "Status", "Wizard", "Wireless Settings", "Firewall", "Advanced Settings", and "Toolbox". The "DHCP Server" tab is selected. Below the navigation, there are tabs for "System Status", "DHCP Server", "Device Status", "Internet Status", "DHCP Status", "Log", and "Statistics". A note states: "You can enable the Broadband routers DHCP server to dynamically allocate IP Addresses to your LAN client PCs. The broadband router must have an IP Address for the Local Area Network." The "LAN IP" section contains the following fields: "IP Address" (192.168.0.1), "IP Subnet Mask" (255.255.255.0), "802.1d Spanning Tree" (Disabled), "DHCP Server" (Enabled), and "Lease Time" (Forever). The "DHCP Server" section contains: "Start IP" (192.168.0.100), "End IP" (192.168.0.200), and "Domain Name" (sitecomw341). "Apply" and "Cancel" buttons are at the bottom right.

Klik op **<Toepassen>** aan de onderzijde van dit scherm om wijzigingen op te slaan.

**IP-adres** 192.168.0.1. Dit is het IP-adres van de LAN van uw router (het standaard-IP-adres van de gateway van uw LAN-clients).

**IP Subnet Masker** 255.255.255.0 Geef voor uw LAN-segment een subnetmasker op.

**802.1d Spanning Tree** is standaard uitgeschakeld. Als de functie 802.1d Spanning Tree ingeschakeld is, gebruikt deze router het spanning tree-protocol om netwerklussen te voorkomen.

**DHCP-server** is standaard ingeschakeld. U kunt de DHCP-server inschakelen of uitschakelen. Als DHCP uitgeschakeld is, worden aan clients geen IP-adressen

toegewezen en moet u statische IP-adressen gebruiken. Als DHCP-server ingeschakeld is, wordt aan uw computers automatisch een IP-adres toegewezen totdat de "Lease tijd" verloopt.

**Lease tijd** Altijd. Bij de optie "Lease tijd" kunt u opgeven hoe lang de DHCP een IP-adres aan uw LAN-clients leent. De DHCP zal het IP-adres van uw LAN-client wijzigen als deze tijddrempel wordt overschreden.

**IP adres pool** U kunt voor uw DHCP-server een bepaald IP-adresbereik selecteren om aan uw LAN-clients IP-adressen uit te geven.

**Opmerking: *het standaard-IP-bereik is 192.168.0.100 ~ 192.168.0.200. Als u wilt dat uw PC('s) een statisch/vast IP-adres hebben, dan moet u een IP-adres kiezen dat buiten deze IP-adrespool ligt***

**Domein naam** U kunt voor uw LAN een domeinnaam opgeven. Of gewoon de standaardinstelling behouden (sitecomwl351).

## Apparaat Status

Bekijk de huidige configuratie-instellingen van de breedbandrouter. "Apparaat Status" toont de configuratie-instellingen die u hebt gekozen in de "Instel hulp" / Basisinstellingen / Instellingen draadloze verbinding.



The screenshot shows the web interface of a 300N WIRELESS ROUTER by SITECOM. The page title is "300N WIRELESS ROUTER" and the SITECOM logo is in the top right. A navigation bar includes "Status", "Wizard", "Wireless Settings", "Firewall", "Advanced Settings", and "Toolbox". A language selection dropdown is set to "Choose your language". Below the navigation bar, a secondary menu highlights "Device Status" among other options: "System Status", "DHCP Server", "Internet Status", "DHCP Status", "Log", and "Statistics".

View the current setting status of this device.

**Wireless Configuration**

Mode :	AP
ESSID :	Sitecom8C0008
Channel :	6
Security :	WPA2 pre-shared key
Associated Clients :	0
BSSID :	00:FF:52:8C:00:08

**LAN Configuration**

IP Address :	192.168.0.1
Subnet Mask :	255.255.255.0
DHCP Server :	Enabled
MAC Address :	00:FF:52:8C:00:08

## Internet status

Op deze pagina wordt getoond of de WAN-poort aangesloten is op een kabel/DSL-verbinding. Hier worden ook het IP-adres van het WAN, subnetmasker en ISP-gateway evenals het MAC-adres en de primaire DNS van de router getoond. Druk op de knop **Vernieuwen** om het IP-adres van het WAN te vernieuwen.



**300N WIRELESS ROUTER** **SITECOM**

Status Wizard Wireless Settings Firewall Advanced Settings **Toolbox** Choose your language ▾

System Status DHCP Server Device Status **Internet Status** DHCP Status Log Statistics

View the current internet connection status and related information.

<b>Attain IP Protocol :</b>	Dynamic IP Address
<b>IP Address :</b>	---
<b>Subnet Mask :</b>	---
<b>Default Gateway :</b>	---
<b>MAC Address :</b>	00:EE:52:8C:00:02
<b>Primary DNS :</b>	---

Renew

## Status DHCP-clients

**DHCP** Deze pagina toont alle DHCP-clients (LAN-PC's) die momenteel op uw netwerk zijn aangesloten. De tabel toont het toegewezen IP-adres, MAC-adres en de verstreken tijd voor elke DHCP-leaseclient. Gebruik de knop "Vernieuw" om de beschikbare informatie te updaten.

U kunt **IP van statische DHCP inschakelen** selecteren. Het is mogelijk om meer statische DHCP-IP's toe te voegen. Deze staan vermeld in de tabel **Tabel van huidige statische DHCP**. IP kan, indien gewenst, uit de tabel worden verwijderd.

Klik op de knop **Toepassen** om de gewijzigde configuratie op te slaan.

**300N WIRELESS ROUTER** **SITECOM**

Status Wizard Wireless Settings Firewall Advanced Settings **Toolbox** Choose your language ▾

System Status DHCP Server Device Status Internet Status **DHCP Status** Log Statistics

This table shows the assigned IP address, MAC address and expiration time for each DHCP leased client.

IP address	MAC address	Expiration Time
No DHCP.		

Refresh

Enable Static DHCP IP

IP address	MAC address
<input type="text"/>	<input type="text"/>

Add Reset

**Current Static DHCP Table:**

NO.	IP address	MAC address	Select
-----	------------	-------------	--------

Delete Selected Delete All Reset Apply Cancel

## Log van de WL-351/368

Bekijk het gegevenslog van de WL-351/368. Deze pagina toont het huidige systeemlog van de breedbandrouter. Dit log toont gebeurtenissen die zich na het opstarten van het systeem hebben voorgedaan. Aan de onderzijde van de pagina kan het systeemlog met **<Opslaan>** worden opgeslagen als een lokaal bestand voor verdere verwerking of het systeemlog kan met **<Legen>** worden geleegd of het kan worden vernieuwd met **<Vernieuw>** om de nieuwste informatie op te halen. Als het systeem wordt uitgeschakeld, zal het systeemlog verdwijnen indien het niet als een lokaal bestand is opgeslagen.



**300N WIRELESS ROUTER** **SITECOM**

Status Wizard Wireless Settings Firewall Advanced Settings **Toolbox** Choose your language

System Status DHCP Server Device Status Internet Status DHCP Status **Log** Statistics

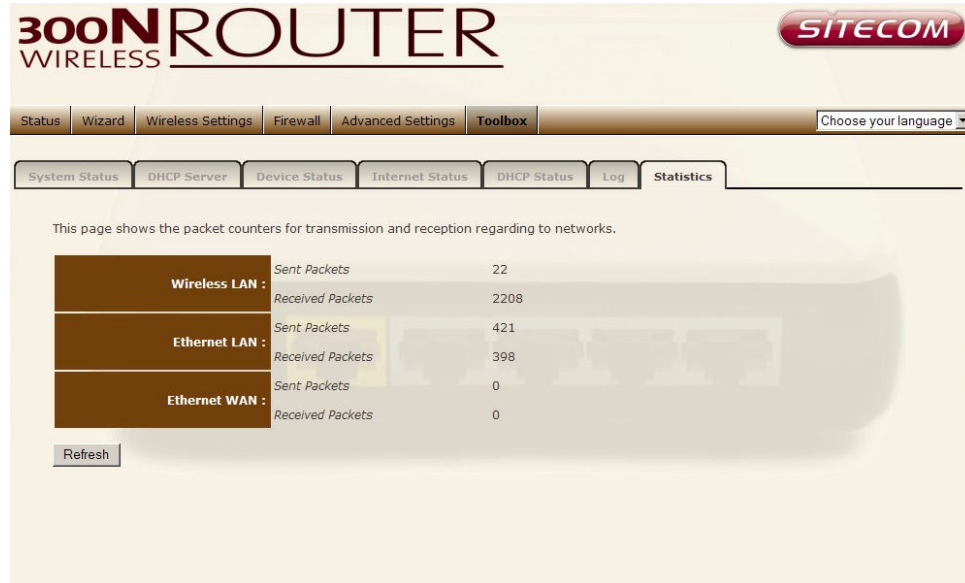
View the system operation information. You can see the system start up time, connection process...etc. here.

```
day 1 00:00:06 [SYSTEM]: WAN, No PHY Link
day 1 00:00:06 [SYSTEM]: WAN, start DHCP mode
day 1 00:00:04 [SYSTEM]: WAN, stop DHCP mode
day 1 00:00:03 [SYSTEM]: WAN, stop DHCP mode
day 1 00:00:02 [SYSTEM]: HTTP, start
day 1 00:00:01 [SYSTEM]: NET, start Firewall
day 1 00:00:01 [SYSTEM]: NET, start NAT
day 1 00:00:01 [SYSTEM]: NTP, start NTP Client
day 1 00:00:01 [SYSTEM]: DNS, start DNS Proxy
day 1 00:00:01 [SYSTEM]: DHCP, start DHCP Server
day 1 00:00:01 [SYSTEM]: WAN, No PHY Link
day 1 00:00:01 [SYSTEM]: WAN, start DHCP mode
day 1 00:00:01 [SYSTEM]: WAN, stop DHCP mode
day 1 00:00:01 [SYSTEM]: WLAN, Channel = 11
day 1 00:00:00 [SYSTEM]: LAN, IP address=192.168.0.1
day 1 00:00:00 [SYSTEM]: LAN, start
day 1 00:00:00 [SYSTEM]: BR, start
day 1 00:00:00 [SYSTEM]: Start Log Message Service!
```

Save Clear Refresh

## Statistiek van de WL-351/368

Toont de tellers van pakketten die via WAN, LAN & WLAN zijn verzonden en ontvangen.



The screenshot shows the web interface of a 300N WIRELESS ROUTER. The page title is "300N WIRELESS ROUTER" with the SITECOM logo. The navigation menu includes Status, Wizard, Wireless Settings, Firewall, Advanced Settings, and Toolbox. A language selection dropdown is set to "Choose your language". The "Statistics" tab is selected, showing packet counters for three network types: Wireless LAN, Ethernet LAN, and Ethernet WAN. The data is as follows:

Network Type	Category	Count
Wireless LAN :	Sent Packets	22
	Received Packets	2208
Ethernet LAN :	Sent Packets	421
	Received Packets	398
Ethernet WAN :	Sent Packets	0
	Received Packets	0

A "Refresh" button is located below the table.

## 10 Configuratiewizard

---

Klik op **Instel hulp** om de router te configureren. De "Instel hulp" verschijnt; controleer of de modem aangesloten is en klik op **Volgende**.



Selecteer uw land bij "Land". Selecteer uw internetprovider. Klik op **Volgende**.



Afhankelijk van de provider die u kiest, kan het nodig zijn dat u uw gebruikersnaam en wachtwoord, MAC-adres of hostnaam moet invullen in het volgende venster. Nadat u de juiste informatie hebt ingevuld, klikt u op **Volgende**.

# 300N WIRELESS ROUTER

SITECOM

Status **Wizard** Wireless Settings Firewall Advanced Settings Toolbox Choose your language ▾

Please, enter the data which is supplied by your ISP.

Hostname :	<input type="text"/>	(Alleen voor oudere @home verbindingen)
MAC Address :	<input type="text" value="000000000000"/>	Clone MAC address

Previous Apply Cancel



# 300N WIRELESS ROUTER

SITECOM

Status **Wizard** Wireless Settings Firewall Advanced Settings Toolbox Choose your language ▾

Please, enter the data which is supplied by your ISP.

Login Method :	PPP over Ethernet	
Username :	<input type="text"/>	
Password :	<input type="text"/>	
Service :	<input type="text"/>	
MTU :	<input type="text" value="1452"/>	(512<=MTU Value<=1492)
Connection Type :	<input type="text" value="Keep connection"/>	<input type="button" value="Connect"/> <input type="button" value="Disconnect"/>
Idle Time :	<input type="text" value="10"/>	(1-1000 Minutes)

Previous Apply Cancel



Klik op **Toepassen** om de configuratie te voltooien.

## 11 Instellingen draadloze verbinding

U kunt parameters instellen die voor de draadloze stations worden gebruikt om verbinding te maken met deze router. De parameters omvatten "Modus", "ESSID", "Kanaal nummer" en "Verbonden client".

### Draadloze functie



Schakel de draadloze functie hier in of uit. Klik op **Toepassen** en wacht totdat de module gereed & geladen is.

## Basisinstellingen

**300N WIRELESS ROUTER** **SITECOM**

Status Wizard **Wireless Settings** Firewall Advanced Settings Toolbox Choose your language

Enable **Basic** Advanced Security ACL WPS

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode : AP

Band : 2.4 GHz (B+G+N)

ESSID : Sitecom8C0008

Channel : 11

Apply Cancel

**Modus** Stelt u in staat de AP- of WDS-modus te kiezen.

**Band** Stelt u in staat om de AP vast in te stellen op de modus 802.11b of 802.11g. U kunt ook de modus B+G selecteren om tegelijkertijd 802.11b- en 802.11g-clients toe te staan.

**SSID # inschakelen** Stelt u in staat om voor deze router maximaal vier SSID's in te schakelen.

**ESSID** Dit is de naam van het draadloze signaal dat wordt uitgezonden. Alle apparaten in hetzelfde draadloze LAN moeten dezelfde ESSID hebben.

**Kanaal** Het kanaal dat wordt gebruikt door het draadloze LAN. Alle apparaten in hetzelfde draadloze LAN moeten hetzelfde kanaal gebruiken.

Enable **Basic** Advanced Security ACL WPS

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode : AP

Band : 2.4 GHz (B+G+N)

Enable SSID# : 1

SSID1 : om5B8808

Channel : 11

Apply Cancel

## Geavanceerd

Met deze tab kunt u de geavanceerde draadloze opties instellen. De opties omvatten "Beveiligings type", "Fragmentdrempel", "RTS-drempel", "Beacon-interval" en "Preamble Type". Deze parameters moet u niet veranderen tenzij u weet welke gevolgen deze wijzigingen hebben voor uw breedbandrouter.



The screenshot shows the configuration interface for a 300N GIGABIT ROUTER XR. The page is titled "300N WIRELESS GIGABIT ROUTER XR" and features the SITECOM logo. The navigation menu includes Status, Wizard, **Wireless Settings**, Firewall, Advanced Settings, and Toolbox. A language selection dropdown is set to "Choose your language".

Under the "Wireless Settings" section, the "Advanced" tab is selected. A warning message states: "These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Broadband router."

The configuration options are as follows:

Authentication Type :	<input checked="" type="radio"/> Open System	<input type="radio"/> Shared Key	<input type="radio"/> Auto
Fragment Threshold :	2346	(256-2346)	
RTS Threshold :	2347	(1-2347)	
Beacon Interval :	100	(20-1024 ms)	
DTIM Period :	1	(1-255)	
Data Rate :	Auto		
N Data Rate :	Auto		
Channel Bandwidth :	<input checked="" type="radio"/> Auto 20/40 MHZ	<input type="radio"/> 20 MHZ	
Preamble Type :	<input type="radio"/> Long Preamble	<input checked="" type="radio"/> Short Preamble	
CTS Protection :	<input checked="" type="radio"/> Auto	<input type="radio"/> Always	<input type="radio"/> None
Tx Power :	100 %		

Buttons for "Apply" and "Cancel" are located at the bottom right of the settings area.

**Beveiligings type** Er zijn twee beveiligingstypes: "Systeem openen" en "Gedeelde sleutel". Als u "Systeem openen" selecteert, kunnen draadloze stations zich associëren met deze draadloze router zonder WEP-encryptie. Als u "Gedeelde sleutel" selecteert, moet u ook een WEP-sleutel instellen op de pagina "Encryptie". Nadat dit is gebeurd, moet u ervoor zorgen dat de draadloze clients die u met het apparaat wilt verbinden, ook met dezelfde encryptiesleutel worden ingesteld.

**Fragmentdrempel** "Fragmentdrempel" specificeert de maximale grootte van een pakket tijdens de fragmentatie van gegevens die moeten worden verzonden. Als u deze waarde te laag instelt, resulteert dit in een slechte prestatie.

**RTS-drempel** Als de pakketgrootte kleiner is dan de RTS-drempel, zal de draadloze router het RTS/CTS-mechanisme niet gebruiken om dit pakket te verzenden.

**Beacon-interval** geeft aan om de hoeveel tijd deze draadloze router een baken uitzendt. Een Beacon wordt gebruikt om het draadloze netwerk te synchroniseren.

**Data snelheid** De "Data snelheid" is de snelheid die dit Access Point gebruikt om gegevenspakketten te verzenden. Het Access Point gebruikt de hoogst mogelijke geselecteerde transmissiesnelheid om de gegevenspakketten te verzenden.

**N Data Rate** De "N Data Rate" is de snelheid die dit Access Point gebruikt om gegevenspakketten te verzenden voor draadloze knooppunten die N-conform zijn. De hoogste tot de laagste datasnelheid kan vast worden ingesteld.

**Channel Bandwidth** is het frequentiebereik dat wordt gebruikt.

**Preamble Type** De "Long Preamble" kan een betere compatibiliteit van het draadloze LAN geven terwijl de "Short Preamble" een betere prestatie van het draadloze LAN kan geven.

**CTS Protection:** Het verdient aanbeveling om het protectiemechanisme in te schakelen. Dit mechanisme kan de mate van gegevensbotsingen tussen draadloze 802.11b- en 802.11g-stations verlagen. Als de protectiemodus ingeschakeld is, zal de doorvoer van de AP enigszins lager zijn vanwege het grote frame-netwerkverkeer.

**Zend vermogen** kan worden ingesteld op een absoluut minimaal of maximaal vermogen.

## Beveiliging

Dit Access Point voorziet in complete beveiligingsfuncties voor een draadloos LAN, waaronder WEP, IEEE 802.11x, IEEE 802.11x met WEP, WPA met vooraf gedeelde sleutel en WPA met RADIUS. Met deze beveiligingsfuncties kunt u illegale toegang tot uw draadloos LAN voorkomen. Zorg ervoor dat uw draadloze stations dezelfde beveiligingsfunctie gebruiken, en worden ingesteld met dezelfde beveiligingsleutel.

**SSID Selection** Hier kiest u de SSID waarvoor u de beveiliging wilt instellen.

**ESSID uitzenden** Als u "ESSID uitzenden" hebt ingeschakeld, kan elk draadloos station dat zich binnen de dekking van dit Access Point bevindt, dit Access Point gemakkelijk lokaliseren. Als u een openbaar draadloos netwerk bouwt, wordt aanbevolen deze functie in te schakelen. Uitschakeling van "ESSID uitzenden" kan een betere beveiliging bieden.

**WMM** WiFi Multi Media, indien ingeschakeld, ondersteunt QoS voor een betere ervaring van audio, video en spraak in toepassingen.

The screenshot shows the configuration interface for the Sitecom 300N Wireless Gigabit Router XR. The page is titled "300N WIRELESS GIGABIT ROUTER XR" and features the Sitecom logo. The navigation menu includes Status, Wizard, Wireless Settings (selected), Firewall, Advanced Settings, and Toolbox. A language selection dropdown is set to "Choose your language".

Under the "Wireless Settings" tab, the "Security" sub-tab is active. The page contains the following configuration options:

- SSID Selection:** Sitecom5FA5C4
- Broadcast ESSID:** Enable
- WMM:** Enable
- Encryption:** WPA pre-shared key
- WPA Type:**  WPA(TKIP)  WPA2(AES)  WPA2 Mixed
- Pre-shared Key Type:** Passphrase
- Pre-sharedKey:** V0VQWPTFE8D1

Buttons for "Apply" and "Cancel" are located at the bottom right of the configuration area.

## Uitschakelen

Als u encryptie uitschakelt, dan is het erg onveilig om met de WL-351/368 te werken.



The screenshot shows a web interface for wireless security configuration. At the top, there are tabs: 'Enable', 'Basic', 'Advanced', 'Security' (selected), 'ACL', and 'WPS'. Below the tabs, a message states: 'This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.' The 'Encryption' dropdown menu is set to 'Disable'. There is an unchecked checkbox for 'Enable 802.1x Authentication'. At the bottom right, there are 'Apply' and 'Cancel' buttons.

## 802.1x-authenticatie inschakelen

IEEE 802.1x is een authenticatieprotocol. Elke gebruiker moet een geldige account gebruiken om bij dit Access Point in te loggen voordat toegang mogelijk is tot het draadloze LAN. De authenticatie wordt verwerkt door een RADIUS-server. Deze modus authenticceert gebruikers alleen met IEEE 802.1x, maar versleutelt tijdens communicatie geen gegevens.



The screenshot shows the configuration page for enabling 802.1x authentication. The 'Enable 802.1x Authentication' checkbox is checked. Below it, there are three input fields: 'RADIUS Server IP Address' (empty), 'RADIUS Server Port' (set to 1812), and 'RADIUS Server Password' (empty). At the bottom right, there are 'Apply' and 'Cancel' buttons.

## WEP

Als u de 64-bit of 128-bit WEP-sleutel selecteert, moet u WEP-sleutels invoeren om gegevens te versleutelen. U kunt de sleutel zelf genereren en invoeren. U kunt vier WEP-sleutels invoeren en één hiervan selecteren als een standardsleutel. De router kan vervolgens pakketten ontvangen die door één van de vier sleutels is versleuteld.



Encryption :	WEP
Key Length :	64-bit
Key Type :	ASCII (5 characters)
Default Key :	Key 1
Encryption Key 1 :	
Encryption Key 2 :	
Encryption Key 3 :	
Encryption Key 4 :	

**Sleutel lengte** U kunt voor encryptie de lengte van de WEP-sleutel selecteren: 64-bit of 128-bit. Hoe groter de sleutel hoe hoger het gebruikte beveiligingsniveau, maar de doorvoer zal kleiner zijn.

**Sleutel type** U kunt ASCII-karakters (alfanumeriek formaat) of hexadecimale cijfers (binnen het bereik "A-F", "a-f" en "0-9") selecteren als WEP-sleutel.

**Sleutel 1 - Sleutel 4** De WEP-sleutels worden gebruikt om gegevens te versleutelen die in het draadloze netwerk worden verzonden. Gebruik de volgende regels om op het apparaat een WEP-sleutel in te stellen. 64-bit WEP: voer 10-cijferige Hex-waarden (binnen het bereik "A-F", "a-f" en "0-9") of 5-cijferige ASCII-waarden in als encryptiesleutel. 128-bit WEP: voer 26-cijferige Hex-waarden (binnen het bereik "A-F", "a-f" en "0-9") of 13-cijferige ASCII-waarden in als encryptiesleutels.

Klik op <Toepassen> aan de onderzijde van het scherm om bovengenoemde configuraties op te slaan. U kunt nu andere onderdelen configureren door "Continue" te kiezen, of kies "Toepassen" om de instellingen toe te passen en start het apparaat opnieuw op.

## Vooraf gedeelde WPA-sleutel

Wi-Fi Protected Access (WPA) is een geavanceerde beveiligingsstandaard. U kunt een vooraf gedeelde sleutel gebruiken om draadloze stations te authenticeren en tijdens communicatie gegevens te versleutelen. Deze sleutel gebruikt TKIP of CCMP (AES) om de encryptiesleutel vaak te wijzigen. De encryptiesleutel is door hackers daardoor niet gemakkelijk te kraken. Dit is de best mogelijke beveiliging die beschikbaar is.



The screenshot shows a configuration window for WPA. The 'Encryption' dropdown is set to 'WPA pre-shared key'. The 'WPA Type' section has three radio buttons: 'WPA(TKIP)' is selected, 'WPA2(AES)' is unselected, and 'WPA2 Mixed' is unselected. The 'Pre-shared Key Type' dropdown is set to 'Passphrase'. The 'Pre-sharedKey' text input field is empty. At the bottom right, there are 'Apply' and 'Cancel' buttons.

## WPA-Radius

Wi-Fi Protected Access (**WPA**) is een geavanceerde beveiligingsstandaard. U kunt een externe RADIUS-server gebruiken om draadloze stations te authenticeren en de sessiesleutel te leveren waarmee tijdens communicatie gegevens worden versleuteld. Deze sleutel gebruikt **TKIP** of CCMP (**AES**) om de encryptiesleutel vaak te wijzigen. Druk op de knop **Toepassen** als u klaar bent.



The screenshot shows a configuration window for WPA. The 'Encryption' dropdown is set to 'WPA RADIUS'. The 'WPA Type' section has three radio buttons: 'WPA(TKIP)' is selected, 'WPA2(AES)' is unselected, and 'WPA2 Mixed' is unselected. The 'RADIUS Server IP Address' text input field is empty. The 'RADIUS Server Port' text input field contains the value '1812'. The 'RADIUS Server Password' text input field is empty. At the bottom right, there are 'Apply' and 'Cancel' buttons.

## ACL

Deze draadloze router ondersteunt MAC Address Control, waarmee wordt voorkomen dat onbevoegden toegang krijgen tot uw draadloze netwerk.



The screenshot shows the configuration interface for a 300N WIRELESS ROUTER. The page title is "300N WIRELESS ROUTER" with the SITECOM logo. The navigation menu includes Status, Wizard, Wireless Settings (selected), Firewall, Advanced Settings, and Toolbox. There is a language selection dropdown. Below the navigation, there are tabs for Enable, Basic, Advanced, Security, ACL (selected), and WPS. A note states: "For security reason, the Access Point features MAC Address Filtering which only allows authorized MAC Addresses to associate with the Access Point." The main section is titled "MAC Address Filtering Table" and contains a table with columns: NO., MAC address, Comment, and Select. Below the table are buttons for "Delete Selected", "Delete All", and "Reset". There is a checkbox labeled "Enable Wireless Access Control". Below this, there is a "New:" section with input fields for "MAC address" and "Comment", and buttons for "Add" and "Reset". At the bottom right, there are "Apply" and "Cancel" buttons.

**Toegangs controle aanzetten** Schakelt de functie voor controle van draadloze toegang in

**Een adres toevoegen aan de lijst** Voer het "MAC adres" en "Commentaar" in van het toe te voegen draadloze station en klik vervolgens op "Toevoegen". Het draadloze station wordt vervolgens toegevoegd aan de "Current Access Control List" hieronder. Als u moeilijkheden ondervindt met het invullen van de velden, klik dan op "Legen" waarna in zowel het veld "MAC-adres" als "Commentaar" de ingevoerde gegevens worden gewist.

**Een adres uit de lijst verwijderen** Als u een MAC-adres wilt verwijderen uit de "Current Access Control List", selecteer dan het MAC-adres dat u uit de lijst wilt verwijderen en klik vervolgens op "Selectie verwijderen". Als u alle MAC-adressen uit de lijst wilt verwijderen, klik dan op de knop "Alles verwijderen". Klik op "Reset" als u de huidige selecties wilt wissen.

Klik op <Toepassen> aan de onderzijde van het scherm om bovengenoemde configuraties op te slaan. U kunt nu andere onderdelen configureren door

“Continue” te kiezen, of kies “Toepassen” om de instellingen toe te passen en start het apparaat opnieuw op.

## **WPS**

Wi-Fi Protected Setup (WPS) is de eenvoudigste manier om een verbinding tot stand te brengen tussen de draadloze clients en de draadloze router. U hoeft niet elke keer wanneer u een draadloze verbinding tot stand wilt brengen, de encryptiemodus te selecteren en een lang encryptiewachtwoord in te vullen. U hoeft alleen maar een knop in te drukken op zowel de draadloze client als de draadloze router, en WPS doet de rest voor u.

De draadloze router ondersteunt twee WPS-types: “WPS via drukknop” en “WPS via PIN”. Als u de drukknop wilt gebruiken, moet u op de draadloze client of in de utility van de draadloze client een specifieke drukknop indrukken om de WPS-modus te starten, en de draadloze router in de WPS-modus zetten. Het is heel eenvoudig. Druk op de WPS-knop van de draadloze router, of klik op de knop “Start verwerking” in de webconfiguratie-interface. Als u de PIN-code wilt gebruiken, moet u de PIN-code van de draadloze client weten en deze in de WPS-modus zetten. Voer vervolgens de PIN-code van de draadloze client in via de webconfiguratie-interface van de draadloze router.

300N WIRELESS ROUTER SITECOM

Status Wizard **Wireless Settings** Firewall Advanced Settings Toolbox Choose your language ▾

Enable Basic Advanced Security ACL **WPS**

**WPS :**  Enable

**Wi-Fi Protected Setup Information**

**WPS Current Status :** unConfigured

**Self Pin Code :** 91750488

**SSID :** Sitecom8C0008

**Authentication Mode :** Disable

**Passphrase Key :**

**WPS Via Push Button :**

**WPS Via PIN :**

**WPS** Selecteer het vakje om de WPS-functie in te schakelen en deselecteer het vakje als u de WPS-functie wilt uitschakelen.

**Huidige status WPS** Als de draadloze beveiligingsfunctie (encryptie) van deze draadloze router op de juiste wijze ingesteld is, ziet u hier het bericht "Configured". Anders ziet u "UnConfigured".

**Zelfpincode** Dit is de WPS-PIN-code van de draadloze router. U hebt deze informatie mogelijk nodig als u verbinding maakt met andere draadloze apparaten waarop WPS ingeschakeld is.

**SSID** Dit is de uitzendnaam (SSID) van het netwerk van de router.

**Authenticatiemodus** Deze optie toont de actieve authenticatie voor de draadloze verbinding.

**Wachtwoordsleutel** Deze optie toont de wachtwoordsleutel die tijdens het WPS-proces door de draadloze router willekeurig wordt gegenereerd. U hebt deze informatie mogelijk nodig als u een apparaat gebruikt dat geen ondersteuning biedt voor WPS.

**WPS via drukknop** Druk op de knop om het WPS-proces te starten. De router wacht tot 2 minuten op het WPS-verzoek vanaf de draadloze apparaten.

**WPS via PIN** U kunt de PIN-code van het draadloze apparaat invullen en op de knop drukken om het WPS-proces te starten. De router wacht tot 2 minuten op het WPS-verzoek vanaf het draadloze apparaat.

## 12 Firewall-instellingen

---

De breedbandrouter biedt via een firewall een uitgebreide beveiliging door verbindingsparameters te beperken. Dit verkleint het risico van aanvallen door hackers en biedt bescherming tegen een groot aantal bekende internetaanvallen. Bij gebruik van toepassingen die onbeperkte toegang tot het internet vereisen, kunt u echter een specifieke client/server configureren als een Demilitarized Zone (DMZ).

**Opmerking:** Als u de Firewall-instellingen wilt inschakelen, selecteer dan **Inschakelen** en klik op **Toepassen**



## DMZ

Indien u een client-PC hebt die achter een NAT-firewall niet op correcte wijze een internettoepassing (bijv. games) kan draaien, dan kunt u de firewall-bependingen wijzigen in onbeperkte 2-weg internettoegang door een DMZ-host te definiëren. De DMZ-functie stelt u in staat om alle pakketten die naar het IP-adres van uw WAN-poort gaan, om te leiden naar een specifiek IP-adres in uw LAN. Het verschil tussen de virtuele server en de DMZ-functie is dat de virtuele server een specifieke service/internettoepassing (bijv. FTP, websites) omleidt naar een specifieke LAN-client/server, terwijl DMZ alle pakketten (ongeacht om welke service het gaat) die naar het IP-adres van uw WAN gaan, omleidt naar een specifieke LAN-client/server.

**300N WIRELESS ROUTER** SITECOM

Status Wizard Wireless Settings **Firewall** Advanced Settings Toolbox Choose your language ▼

Enable **DMZ** DoS Access URL block

If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, you can open unrestricted two-way Internet access for this client by defining a Virtual DMZ Host.

Enable DMZ

Public IP Address	Client PC IP Address
<input type="radio"/> Dynamic IP Session 1 ▼	<input type="text"/>
<input type="radio"/> Static IP <input type="text"/>	<input type="text"/>

Add Reset

**DMZ table:**

NO.	Public IP Address	Client PC IP Address	Select
-----	-------------------	----------------------	--------

Delete Selected Delete All Reset

Apply Cancel

**DMZ aanzetten** Schakel DMZ in of uit

**Publiek IP Adres** Het IP-adres van de WAN-poort of andere publieke IP-adressen die door uw ISP aan u zijn verstrekt.

**Client PC IP Adres** Vul het IP-adres in van een specifieke host in uw LAN die alle pakketten ontvangt die oorspronkelijk naar de WAN-poort of het publieke IP-adres hierboven gingen.

Klik op **<Toepassen>** aan de onderzijde van het scherm om bovengenoemde configuraties op te slaan.

## Denial of Service (DoS)

De firewall van de breedbandrouter kan algemeen bekende hackeraanvallen blokkeren, waaronder Denial of Service, Ping of Death, Port Scan en Sync Flood. Als zich internetaanvallen voordoen, kan de router de gebeurtenissen registreren in een log.



**Ping of Death** Beschermingen tegen Ping of Death-aanval

**Ping op WAN negeren** De WAN-poort op uw router zal niet reageren op Ping-verzoeken

**Poort scan** Beschermt de router tegen poortscans

**Sync-flood** Beschermt de router tegen Sync Flood-aanvallen

## Toegang

U kunt instellen dat gebruikers geen toegang hebben tot bepaalde internettoepassingen/services (bijv. websites op het internet, e-mail, FTP, etc.). Met toegangsregeling kunnen gebruikers het verkeerstype definiëren dat in uw LAN is toegestaan. U kunt instellen welke PC-client toegang tot deze services heeft.

300N WIRELESS ROUTER SITECOM

Status Wizard Wireless Settings **Firewall** Advanced Settings Toolbox Choose your language

Enable DMZ DoS **Access** URL block

Access Control allows users to define the traffic type permitted or not permitted in your LAN. You can control which PC uses what services or has access to.  
If both MAC filtering and IP filtering are enabled, the MAC filtering table will be checked first.

Enable MAC filtering  Deny  Allow

Client PC MAC Address	Comment
<input type="text"/>	<input type="text"/>

Add Reset

**MAC Filtering table:**

NO.	Client PC MAC Address	Comment	Select
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Delete Selected Delete All Reset

Enable IP Filtering Table (up to 20 computers)  Deny  Allow

NO.	PC Description	PC IP Address	Client Service	Protocol	Port range	Select
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Add Delete Selected Delete All

Apply Cancel

**Weigeren** Als u "Weigeren" selecteert, dan hebben alle clients toegang tot het internet behalve de clients in de lijst hieronder.

**Toestaan** Als u "Toestaan" selecteert, dan heeft geen enkele client toegang tot het internet behalve de PC's in de lijst hieronder.

**Client-PC's filteren op basis van IP** Vul de "IP filter tabel" in om clients te filteren op basis van IP.

**PC Toevoegen** U kunt op "PC Toevoegen" klikken om voor gebruikers een toegangsregel toe te voegen op basis van IP-adres.

**PC verwijderen** Als u uit de "IP filter tabel" een aantal PC's wilt verwijderen, selecteer dan in de tabel de PC die u wilt verwijderen en klik vervolgens op

"Selectie verwijderen". Als u alle PC's uit de tabel wilt verwijderen, klik dan op de knop "Alles verwijderen".

**Client-PC's filteren op basis van MAC** Selecteer "MAC filtering aan" om MAC-filtering in te schakelen.

**PC Toevoegen** Vul "Client PC MAC adres" en "Commentaar" in van de PC die toestemming heeft om het internet op te gaan, en klik vervolgens op "Toevoegen". Als u een spelfout ziet voordat u de instelling toevoegt en u de gegevens opnieuw wilt invoeren, klik dan op "Reset" waarna de inhoud in de velden wordt gewist.

**PC verwijderen** Als u uit de "MAC filtering tabel" een aantal PC's wilt verwijderen, selecteer dan in de tabel de PC die u wilt verwijderen en klik vervolgens op "Selectie verwijderen". Als u alle PC's uit de tabel wilt verwijderen, klik dan op de knop "Alles verwijderen". Als u de selectie wilt wissen en de optie opnieuw wilt selecteren, klik dan op "Reset".

Klik op <**Toepassen**> aan de onderzijde van het scherm om bovengenoemde configuratie op te slaan.

## URL blokkeren

Voor een bepaalde PC kunt u toegang tot sommige websites blokkeren door een volledig URL-adres of alleen maar trefwoorden van de website in te voeren.



The screenshot shows the configuration interface for the 300N WIRELESS ROUTER. The page is titled "300N WIRELESS ROUTER" and "SITECOM". The navigation menu includes "Status", "Wizard", "Wireless Settings", "Firewall", "Advanced Settings", and "Toolbox". The "Firewall" section is active, and the "URL block" tab is selected. The page contains a checkbox for "Enable URL Blocking", a text input field for "URL/keyword", and "Add" and "Reset" buttons. Below this is a table titled "Current URL Blocking Table" with columns for "NO.", "URL/keyword", and "Select". At the bottom of the table are buttons for "Delete Selected", "Delete All", and "Reset". At the bottom right of the page are "Apply" and "Cancel" buttons.

**URL blokkering aan** Schakel blokkering van URL in/uit

**URL-trefwoord toevoegen** Vul "URL/sleutelwoord" in en klik vervolgens op "Toevoegen". U kunt het volledige URL-adres of het trefwoord invullen van de website die u wilt blokkeren.

**URL-trefwoord verwijderen** Als u een aantal URL-trefwoorden wilt verwijderen uit de "Huidige URL blokkering tabel", selecteer dan in de tabel het URL-trefwoord dat u wilt verwijderen en klik op "Selectie verwijderen". Als u alle URL-trefwoorden uit de tabel wilt verwijderen, klik dan op de knop "Alles verwijderen". Als u de selectie wilt wissen en de optie opnieuw wilt selecteren, klik dan op "Reset".

Klik op <**Toepassen**> aan de onderzijde van het scherm om bovengenoemde configuraties op te slaan.

## 13 Geavanceerde instellingen

Network Address Translation (NAT) geeft u de mogelijkheid om meerdere lokale gebruikers te verbinden met internet via een of meerdere publieke IP-adressen. NAT geeft u tevens firewall-bescherming tegen hackeraanvallen en de flexibiliteit om specifieke "Lokaal IP"-adressen te koppelen aan "Publieke IP"-adressen voor services als Websites of FTP. Selecteer "Uitschakelen" om de NAT-functie uit te schakelen.



Hardware accelerator verhoogt uw netwerk prestaties. Schakel deze functie in om (internet)snelheden tot 400Mbps te kunnen behalen. (Let op: om optimale resultaten te kunnen behalen, worden de QoS en bandbreedte-beheer functies uitgeschakeld.)

## Port Forwarding

Met "Port Forwarding" kunt u een specifieke reeks servicepoortnummers (vanaf de internet/WAN-poort) omleiden naar een specifiek IP-adres van het LAN. Hiermee kunt u servers hosten achter de NAT-firewall van de router.

300N WIRELESS ROUTER SITECOM

Status Wizard Wireless Settings Firewall **Advanced Settings** Toolbox Choose your language

NAT Enable **Port forwarding** Virtual Server Special Applications Application Layer Gateway uPnP Quality of Service

Entries in this table allow you to automatically redirect common network services to a specific PC behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the local network.

Enable Port Forwarding

Local IP	Type	Port range	Comment
<input type="text"/>	Both	<input type="text"/> - <input type="text"/>	<input type="text"/>

Add Reset

**Current Port Forwarding Table:**

NO.	Local IP	Type	Port range	Comment	Select
-----	----------	------	------------	---------	--------

Delete Selected Delete All Reset

Apply Cancel

**Port forwarding aan** Schakel "Port Forwarding" in.

**Lokaal IP** Dit is de lokale IP van de server achter de NAT-firewall.

**Type** Dit is het protocoltype dat moet worden omgeleid. U kunt ervoor kiezen om alleen "TCP"- of "UDP"-pakketten om te leiden, of "Beide" selecteren om zowel "TCP"- als "UDP"-pakketten om te leiden.

**Poort bereik** Het bereik van de poorten die moeten worden omgeleid naar de lokale IP.

**Commentaar** Beschrijving van deze instelling.

**Port Forwarding toevoegen** Vul "Lokaal IP", "Type", "Poort bereik" en "Commentaar" in van de instelling die moet worden toegevoegd en klik

vervolgens op "Toevoegen". Deze "Port Forwarding"-instelling wordt toegevoegd aan de "Huidige Port Forwarding tabel" hieronder.

**Port Forwarding verwijderen** Als u een "Port Forwarding"-instelling wilt verwijderen uit de "Huidige Port Forwarding tabel", selecteer dan in de tabel de "Port Forwarding"-instelling die u wilt verwijderen en klik vervolgens op "Selectie verwijderen". Als u alle "Port Forwarding"-instellingen uit de tabel wilt verwijderen, klik dan op de knop "Alles verwijderen". Klik op "Reset" als u de huidige selecties wilt wissen.

## Virtuele server

Gebruik de functie "Virtual Server" als u wilt dat in uw LAN verschillende servers/clients verschillende service/internettoepassingstypes vanaf het internet afhandelen (bijv. e-mail, FTP, Webserver, etc.). Computers gebruiken getallen, die poortnummers worden genoemd, om een specifiek service/internettoepassingstype te herkennen. De virtuele server stelt u in staat om een specifiek servicepoortnummer (vanaf de internet/WAN-poort) om te leiden naar een specifiek lokaal IP-adres van het LAN en het servicepoortnummer hiervan.

300N WIRELESS ROUTER SITECOM

Status Wizard Wireless Settings Firewall **Advanced Settings** Toolbox Choose your language

NAT Enable Port forwarding **Virtual Server** Special Applications Application Layer Gateway uPnP Quality of Service

You can configure the router as a Virtual Server allowing remote users to access services such as Web or FTP at your local PC. Depending on the requested service (TCP/UDP) port number, the router will redirect the external service request to the appropriate internal server (located at one of your local PCs).

Enable Virtual Server

Local IP	Local Port	Type	Public Port	Comment
<input type="text"/>	<input type="text"/>	Both	<input type="text"/>	<input type="text"/>

Add Reset

**Current Virtual Server Table:**

NO.	Local IP	Local Port	Type	Public Port	Comment	Select
-----	----------	------------	------	-------------	---------	--------

Delete Selected Delete All Reset

Apply Cancel

**Virtual Server aan** Schakel de virtuele server in.

**Lokaal IP** Dit is het IP-adres van de LAN-client/host waarnaar het pakket van het publieke poortnummer wordt verzonden.

**Lokale poort** Dit is het poortnummer (van de bovengenoemde "Lokaal IP"-host) waarin het nummer van de hieronder genoemde

**Publieke poort** wordt gewijzigd wanneer het pakket uw **LAN** (naar de LAN-server/client-IP) binnenkomt

**Type** Selecteer het protocoltype (TCP, UDP of beide) van het poortnummer. Als u het niet zeker weet, laat deze optie dan staan op de standaardinstelling "Beide". **Publieke poort** Voer het poortnummer van de service

(service/internettoepassing) vanaf het internet in dat wordt omgeleid naar de host van bovengenoemde lokale IP-adres in uw LAN.

**Commentaar** De beschrijving van deze instelling.

**Virtuele server toevoegen** Vul "Lokaal IP", "Lokale poort", "Type", "Publieke poort" en "Commentaar" in van de instelling die moet worden toegevoegd en klik vervolgens op "Toevoegen". Deze instelling van de virtuele server wordt toegevoegd aan de "Tabel van huidige virtuele server" hieronder.

**Virtuele server verwijderen** Als u de instellingen van de virtuele server wilt verwijderen uit de "Tabel van huidige virtuele server", selecteer dan in de tabel de instellingen van de virtuele server die u wilt verwijderen en klik op "Selectie verwijderen". Als u alle instellingen van de virtuele server uit de tabel wilt verwijderen, klik dan op de knop "Alles verwijderen". Klik op "Reset" als u de huidige selecties wilt wissen.

Klik op <**Toepassen**> aan de onderzijde van het scherm om bovengenoemde configuraties op te slaan.

## Speciale toepassingen

Sommige toepassingen (zoals internetspelletjes, videoconferenties, bellen via internet en andere) hebben meervoudige verbindingen nodig. In dit hoofdstuk kunt u de router zo configureren dat voor dit soort toepassingen meerdere verbindingen worden ondersteund.

**Trigger poort aan** Schakel de functie "Special Applications" in.

**Trigger poort** Dit is het uitgaande (Outbound) poortnummerbereik voor deze specifieke toepassing.

**Trigger type** Selecteer of het protocol van de uitgaande poort "TCP", "UDP" of beide is.

**Publieke poort** Voer de inkomende (Inbound) poort of het inkomende poortbereik voor dit toepassingstype in (bijv. 2300-2400, 47624)

300N ROUTER WIRELESS SITECOM

Status Wizard Wireless Settings Firewall **Advanced Settings** Toolbox Choose your language

NAT Enable Port forwarding Virtual Server **Special Applications** Application Layer Gateway uPnP Quality of Service

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic.

Enable Trigger Port

Trigger port	Trigger type	Public Port	Public type	Comment
<input type="text"/>	Both	<input type="text"/>	Both	<input type="text"/>

Popular applications : Select an application Add

Add Reset

**Current Trigger-Port Table:**

NO.	Trigger port	Trigger type	Public Port	Public type	Comment	Select
-----	--------------	--------------	-------------	-------------	---------	--------

Delete Selected Delete All Reset

Apply Cancel

**Publiek type** Selecteer het protocoltype van de inkomende poort: "TCP", "UDP" of beide

**Commentaar** De beschrijving van deze instelling.

**Populaire applicaties** In dit gedeelte staat een lijst met de meer populaire applicaties die meerdere verbindingen vereisen. Selecteer een applicatie uit de selectie "Populaire applicaties". Selecteer na selectie van een applicatie een locatie (1-10) in het vak "Naar selectie kopiëren" en klik vervolgens op de knop "Kopiëren". Hierdoor wordt automatisch een lijst opgeroepen met publieke poorten die voor deze populaire applicatie zijn vereist in de door u opgegeven locatie (1-10).

**Special Application toevoegen** Vul de "Trigger poort", "Trigger type", "Publieke poort", "Publiek type", "Publieke poort" en "Commentaar" in van de toe te voegen instelling en klik vervolgens op "Toevoegen". De instelling van de Special Application wordt toegevoegd aan de "Huidige Trigger poort tabel" hieronder. Mocht u een fout maken, klik dan op "Legen", waarna de inhoud van de velden wordt gewist.

**Verwijderen** Als u instellingen van "Special Applications" wilt verwijderen uit de "Huidige Trigger poort tabel", selecteer dan de instellingen van de "Special Application" die u uit de tabel wilt verwijderen en klik vervolgens op "Selectie verwijderen". Als u alle instellingen van "Special Applications" uit de tabel wilt verwijderen, klik dan op de knop "Alles verwijderen". Klik op "Reset" als u de huidige selecties wilt wissen.

## ALG

U kunt toepassingen selecteren die "Application Layer Gateway"-ondersteuning nodig hebben.

300N WIRELESS ROUTER SITECOM

Status Wizard Wireless Settings Firewall **Advanced Settings** Toolbox Choose your language ▾

NAT Enable Port forwarding Virtual Server Special Applications **Application Layer Gateway** uPnP Quality of Service

Some applications require special support to function under NAT. Please select the applications which you are using.

Enable	Name	Select
<input type="checkbox"/>	H323	Support for H323/netmeeting.
<input type="checkbox"/>	MMS	Support for Microsoft Streaming Media Services protocol.
<input type="checkbox"/>	TFTP	Support for TFTP.
<input type="checkbox"/>	Egg	Support for eggdrop bot networks.
<input type="checkbox"/>	IRC	Allows DCC to work though NAT and connection tracking.
<input type="checkbox"/>	Amanda	Support for Amanda backup tool protocol.
<input type="checkbox"/>	Quake3	Support for Quake III Arena connection tracking and nat.
<input type="checkbox"/>	Talk	Allows netfilter to track talk connections.
<input type="checkbox"/>	IPsec	Support for IPsec passthrough
<input type="checkbox"/>	FTP	Support for FTP.

Apply Cancel

**Enable** Selecteer de toepassing onder "Application Layer Gateway", waarna de router de geselecteerde toepassing op correcte wijze door de NAT-gateway zal laten gaan.

## UPNP

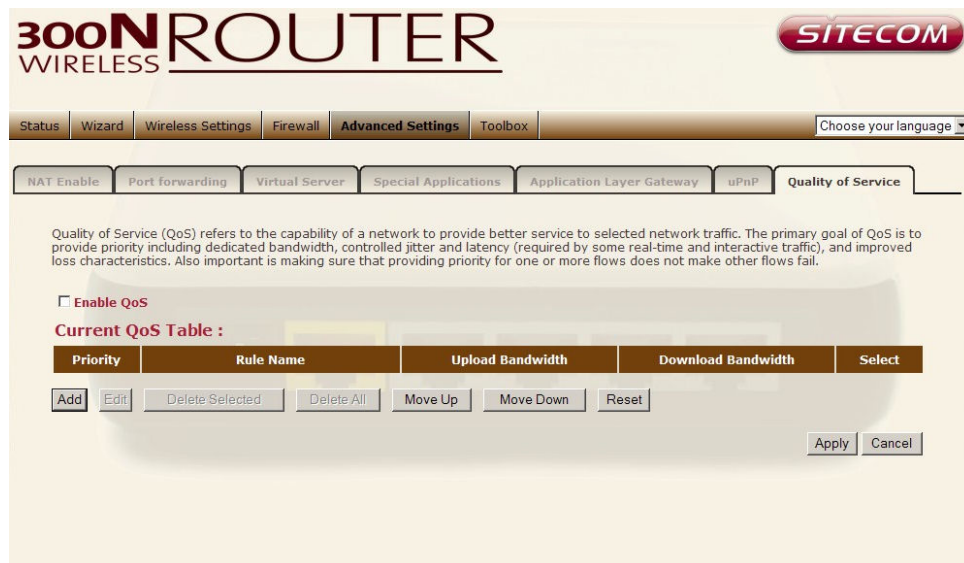
Met UPnP zullen alle PC's in uw intranet deze router automatisch detecteren. U hoeft uw PC dus niet te configureren en de PC kan via deze router gemakkelijk het internet op gaan.



**UPnP-functie** U kunt de UPnP-functie hier in- of uitschakelen. Nadat u de UPnP-functie hebt ingeschakeld, kunnen alle client-systemen die ondersteuning bieden voor UPnP, zoals Windows XP, deze router automatisch detecteren en via deze router het internet op gaan zonder dat iets hoeft te worden geconfigureerd. De NAT Traversal-functie die door UPnP wordt geboden, kan toepassingen die ondersteuning bieden voor UPnP, verbinding laten maken met het internet zonder dat het nodig is om de onderdelen van de virtuele server te configureren.

## QoS

Met QoS kunt u het verkeer van internettoepassingen classificeren op basis van het IP-adres en poortnummer van de bron of het doel. U kunt een prioriteit instellen voor elk toepassingstype en hiervoor bandbreedte reserveren. De toepassingspakketten met hogere prioriteit krijgen altijd voorrang. Toepassingen met lagere prioriteit krijgen bandbreedte nadat toepassingen met hogere prioriteit genoeg bandbreedte hebben gehad. Op deze wijze wordt de prestatie vergroot bij gebruik van kritieke real-time toepassingen zoals internettelefoon, videoconferenties, etc. Alle toepassingen die niet door u worden gespecificeerd, worden geclassificeerd onder de regelnaam "Overige". De regel met een kleiner prioriteitsnummer krijgt een hogere prioriteit; de regel met een groter prioriteitsnummer krijgt een lagere prioriteit. U kunt de prioriteit van de regels wijzigen door deze omhoog of omlaag te verplaatsen.



The screenshot shows the configuration interface for a 300N WIRELESS ROUTER. The page title is "300N WIRELESS ROUTER" with the SITECOM logo. The navigation menu includes Status, Wizard, Wireless Settings, Firewall, Advanced Settings (selected), and Toolbox. A language selection dropdown is set to "Choose your language".

Under the "Advanced Settings" tab, the "Quality of Service" option is selected. A descriptive text explains that QoS provides better service to selected network traffic by prioritizing bandwidth, jitter, and latency.

An "Enable QoS" checkbox is present. Below it, the "Current QoS Table" is shown as an empty table with the following headers:

Priority	Rule Name	Upload Bandwidth	Download Bandwidth	Select
----------	-----------	------------------	--------------------	--------

Below the table are several action buttons: Add, Edit, Delete Selected, Delete All, Move Up, Move Down, and Reset. At the bottom right, there are "Apply" and "Cancel" buttons.

**QoS in/uitschakelen** U kunt "Enable QoS" selecteren om QoS-functionaliteit in te schakelen voor de WAN-poort.

**Een QoS-regel toevoegen aan de tabel** Klik op "Toevoegen" en voer vervolgens een formulier van de QoS-regel in. Klik op "Toepassen" nadat u het formulier hebt ingevuld; de regel wordt vervolgens toegevoegd aan de tabel.

**QoS-regels uit de tabel verwijderen** Als u QoS-regels uit de tabel wilt verwijderen, selecteer dan de QoS-regels die u uit de tabel wilt verwijderen en klik vervolgens op "Selectie verwijderen". Als u alle QoS-regels uit de tabel wilt verwijderen, klik dan op de knop "Alles verwijderen". Klik op "Reset" als u de huidige selecties wilt wissen.

**Een QoS-regel bewerken** Selecteer de regel die u wilt bewerken en klik vervolgens op "Bewerken" en voer vervolgens het detailformulier van de QoS-regel in. Klik op "**Toepassen**" nadat u het formulier hebt bewerkt, waarna de regel wordt opgeslagen.

**Prioriteit van de QoS-regel wijzigen** U kunt de regel selecteren en op "Omhoog verplaatsen" klikken om de prioriteit hiervan te verhogen. Ook kunt u de regel selecteren en op "Omlaag verplaatsen" klikken om de prioriteit hiervan te verlagen.

## 14 Instellingen GEREEDSCHAP

---

### Opties voor wijzigen van wachtwoord

U kunt het wachtwoord wijzigen dat wordt gebruikt om in te loggen in het op het web gebaseerde beheer van het systeem van de breedbandrouter. Het standaardwachtwoord is: admin. Wachtwoorden kunnen 0 tot 12 alfanumerieke karakters bevatten en zijn hoofdlettergevoelig.



The screenshot shows the web interface of a Sitecom 300N Wireless Router. At the top, there is a navigation bar with tabs for Status, Wizard, Wireless Settings, Firewall, Advanced Settings, and Toolbox. Below this is a sub-menu with tabs for Password, Timezone, Remote, Firmware, Back-up, Reset, and DDNS. The main content area contains a text box explaining that the password can be changed and that it must be 0 to 30 alphanumeric characters and case sensitive. Below this are three input fields labeled 'Current Password', 'New Password', and 'Confirm Password'. At the bottom right of the form are 'Apply' and 'Cancel' buttons.

**Huidig wachtwoord** Vul het huidige wachtwoord in om daarna een nieuw wachtwoord te kunnen kiezen.

**Nieuw wachtwoord** Voer uw nieuwe wachtwoord in.

**Bevestig wachtwoord** Voer ter controle uw nieuwe wachtwoord opnieuw in.

Klik op **<Toepassen>** aan de onderzijde van het scherm om bovengenoemde configuraties op te slaan.

## Tijdzone

Met de tijdzone kan uw router zijn tijd baseren op de instellingen die door u zijn geconfigureerd, wat gevolgen heeft voor functies zoals logbestanden en firewall-instellingen.

300N WIRELESS ROUTER SITECOM

Status Wizard Wireless Settings Firewall Advanced Settings **Toolbox** Choose your language

Password **Timezone** Remote Firmware Back-up Reset DDNS

Set the time zone of the Broadband router. This information is used for log entries and firewall settings.

Set Time Zone : (GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

Time Server Address : europe.pool.ntp.org

Daylight Saving :  Enable From January 1 To January 1

Apply Cancel

**Stel Tijdzone in** Selecteer de tijdzone van het land waar u momenteel bent. De router bepaalt zijn tijd op basis van uw selectie.

**Tijd server adres** U kunt een NTP-serveradres instellen.

**Schakel zomertijd in** De router kan ook rekening houden met zomertijd. Als u deze functie wilt gebruiken, moet u het vak Enable selecteren om uw zomertijdconfiguratie in te schakelen (hieronder).

**Start zomertijd** Selecteer de periode waarin u de zomertijd wilt starten

**Eind zomertijd** Selecteer de periode waarin u de zomertijd wilt beëindigen

Klik op **<Toepassen>** aan de onderzijde van het scherm om bovengenoemde configuraties op te slaan.

## Beheer op afstand

De functie voor beheer op afstand stelt u in staat aan een host op het internet de mogelijkheid te geven om vanaf een locatie op afstand de breedbandrouter te configureren. Voer in het veld IP-hostadres het IP-adres van de toegewezen host in.



The screenshot shows the configuration interface for a 300N WIRELESS ROUTER by SITECOM. The page has a navigation menu with options: Status, Wizard, Wireless Settings, Firewall, Advanced Settings, and Toolbox. Below this is a sub-menu with Password, Timezone, Remote, Firmware, Back-up, Reset, and DDNS. The 'Remote' tab is selected. A text box explains: 'The remote management function allows you to designate a host from the Internet to have management/configuration access to the router from a remote site. Enter the designated host IP Address in the Host IP Address field.' Below this is a table with three columns: Host Address, Port, and Enable. The 'Host Address' column has an empty input field. The 'Port' column has an input field containing '8080'. The 'Enable' column has a checkbox that is currently unchecked. At the bottom right of the table are 'Apply' and 'Cancel' buttons.

Host Address	Port	Enable
<input type="text"/>	<input type="text" value="8080"/>	<input type="checkbox"/>

**Hostadres** Dit is op het internet het IP-adres van de host die vanaf een locatie op afstand de breedbandrouter kan beheren/configureren. Als u het hostadres op 0.0.0.0 laat staan, dan betekent dit dat iedereen vanaf een locatie op afstand toegang krijgt tot de op het web gebaseerde configuratie van de router, mits zij het wachtwoord kennen.

**Poort** Het poortnummer van de webinterface voor beheer op afstand.

**Inschakelen** Selecteer **Inschakelen** om de functie voor beheer op afstand in te schakelen.

Klik op **<Toepassen>** aan de onderzijde van het scherm om bovengenoemde configuraties op te slaan.

## Firmware upgraden

Op deze pagina kunt u de firmware van de router upgraden.



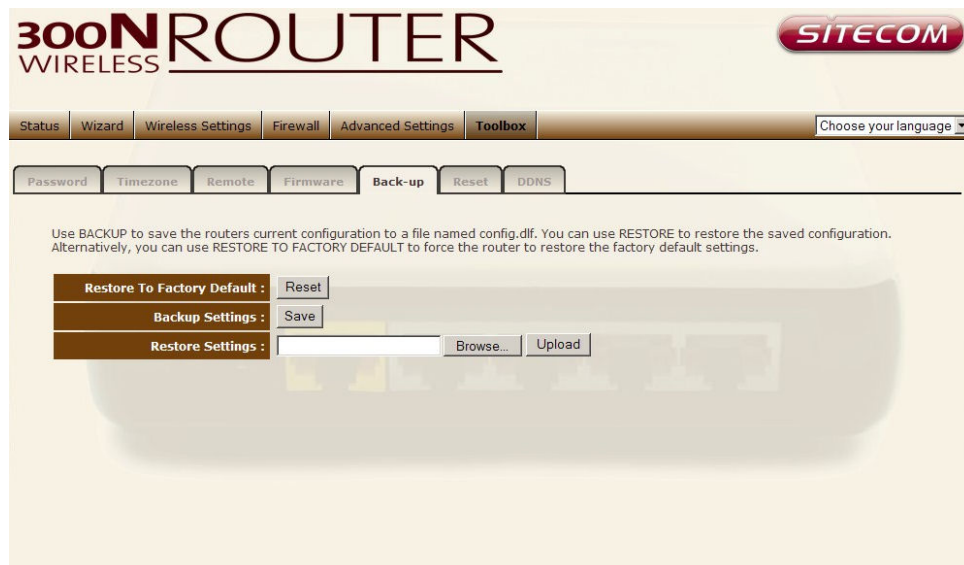
The screenshot shows the web interface of a Sitecom 300N Wireless Router. At the top, the text "300N WIRELESS ROUTER" is displayed in a large, stylized font, with the "SITECOM" logo to the right. Below this is a navigation menu with tabs for "Status", "Wizard", "Wireless Settings", "Firewall", "Advanced Settings", and "Toolbox". A "Choose your language" dropdown menu is located on the right side of the menu. Underneath the menu, there are several sub-tabs: "Password", "Timezone", "Remote", "Firmware", "Back-up", "Reset", and "DDNS". The "Firmware" tab is currently selected. The main content area contains the following text: "This tool allows you to upgrade the Routers firmware. Browse to and select the upgrade file and click APPLY. You will be prompted to confirm the upgrade." Below this text is a text input field with a "Browse..." button next to it. At the bottom right of the form, there are "Apply" and "Cancel" buttons. The background of the page features a faint image of the router's front panel.

**Firmware upgraden** Met deze tool kunt u de systeemfirmware van de breedbandrouter upgraden. Om de firmware van uw breedbandrouter te upgraden, moet u het firmwarebestand downloaden naar uw lokale harde schijf, en in het betreffende veld op deze pagina de bestandsnaam en het pad invoeren. U kunt ook de knop "Bladeren" gebruiken om op uw PC de firmware te lokaliseren.

Zodra u het nieuwe firmwarebestand hebt geselecteerd, klikt u op <**Toepassen**> aan de onderzijde van het scherm om het upgradeproces te starten.

## Backup-instellingen

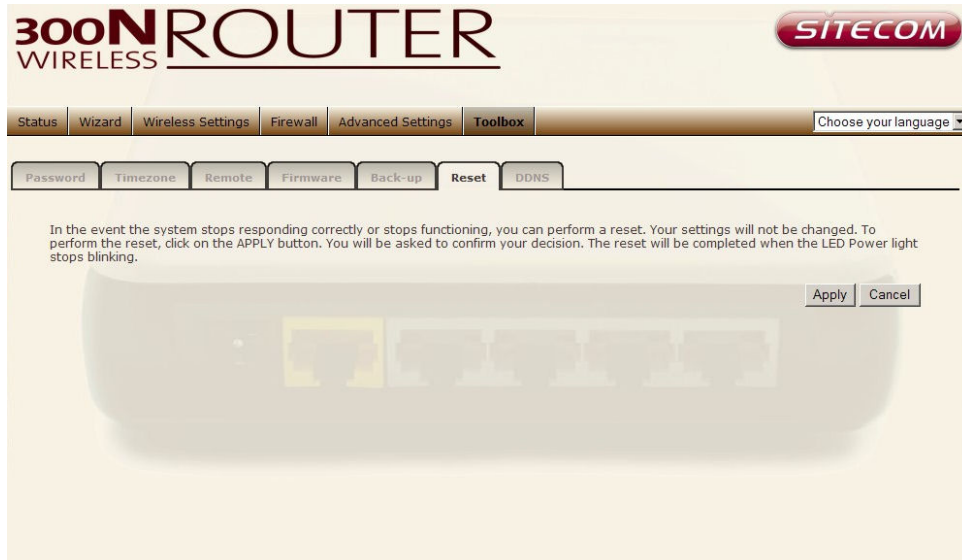
In het scherm Back-up kunt u de huidige configuratie-instellingen van de router opslaan (backup maken). Als u de configuratie-instelling opslaat (Backup), kunt u de opgeslagen configuratie via de optie "Instellingen terug zetten" weer oproepen. Als er zich extreme problemen voordoen, kunt u de optie "Naar fabrieksinstellingen" gebruiken om alle configuraties weer terug te stellen naar de standaardinstelling (zoals die was bij aankoop van de router).



Gebruik de tool "Back-up" om op uw PC de huidige configuratie van de breedbandrouter op te slaan in een bestand met de naam "**config.bin**". U kunt later de tool "Instellingen terug zetten" gebruiken om de opgeslagen configuratie weer terug te zetten naar de breedbandrouter. U kunt ook de tool "Naar fabrieksinstellingen" gebruiken om de breedbandrouter te dwingen het systeem te resetten en de standaardinstelling te herstellen.

## Reset

U kunt het systeem van de router resetten als zich problemen voordoen. In essentie zorgt de resetfunctie ervoor dat het systeem van uw router opnieuw wordt opgestart.



## DDNS

Met DDNS kunt u de statische domeinnaam aan een dynamisch IP-adres koppelen. U hebt een account, wachtwoord en een statische domeinnaam van de DDNS-serviceproviders nodig. Deze router ondersteunt DynDNS, TZO en andere veel voorkomende DDNS-serviceproviders.

300N WIRELESS ROUTER SITECOM

Status Wizard Wireless Settings Firewall Advanced Settings Toolbox Choose your language ▼

Password Timezone Remote Firmware Back-up Reset DDNS

DDNS allows users to map a static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service provider..

Dynamic DNS :  Enable  Disable

Provider : 3322(qdns) ▼

Domain Name :

Account/E-mail :

Password/Key :

Apply Cancel

**Inschakelen/Uitschakelen** Schakel de DDNS-functie van deze router in of uit

**Provider** Selecteer een DDNS-serviceprovider

**Domein naam** Vul de naam in van uw statisch domein dat DDNS gebruikt

**Abonnement/E-mail** De account die uw DDNS-serviceprovider aan u heeft toegewezen

**Wachtwoord/Sleutel** Het wachtwoord dat u instelt voor de bovengenoemde DDNS-serviceaccount

Klik op **<Toepassen>** aan de onderzijde van het scherm om bovengenoemde configuraties op te slaan.

Parts of the firmware of the WL-351/368 Wireless Broadband router are subject to the [GNU general public license](#).

## Appendix A: Licensing Information

This product includes third-party software licensed under the terms of the [GNU General Public License](#). You can modify or redistribute this free software under the terms of the [GNU General Public License](#). Please see Appendix B for the exact terms and conditions of this license.

Specifically, the following part of this product is subject to the GNU GPL:

#	Package name	Source
1	Linux v2.6.21	<a href="http://www.kernel.org">www.kernel.org</a>
2	Iptables v1.3.5	<a href="http://www.netfilter.org/">www.netfilter.org/</a>
3	Bridge-utils v1.2	<a href="http://bridge.sourceforge.net/">bridge.sourceforge.net/</a>
4	Busybox v1.7.5	<a href="http://www.busybox.net/">www.busybox.net/</a>
5	Rp-pppoe v3.8	<a href="http://freshmeat.net/projects/rp-pppoe/">freshmeat.net/projects/rp-pppoe/</a>
6	Pptp-client v1.7.1	<a href="http://pptpclient.sourceforge.net/">pptpclient.sourceforge.net/</a>
7	Ppp v2.4.3	<a href="http://ppp.samba.org/">ppp.samba.org/</a>
8	Udhcp v0.9.9-pre	<a href="http://udhcp.busybox.net/">udhcp.busybox.net/</a>
9	iproute2 v2.6.16-060323	<a href="http://www.linux-foundation.org/en/Net:Iproute2">www.linux-foundation.org/en/Net:Iproute2</a>
10	Dnsmasq v2.39	<a href="http://www.thekelleys.org.uk/dnsmasq/doc.html">www.thekelleys.org.uk/dnsmasq/doc.html</a>
11	Ez-ipupdate v3.0.11b8	<a href="http://ez-ipupdate.com/">ez-ipupdate.com/</a>
12	Libupnp v1.6.0	<a href="http://upnp.sourceforge.net/">upnp.sourceforge.net/</a>
13	Wireless-tools v28	RaLink SDK 3.1.0.0
14	U-boot v1.1.3	RaLink SDK 3.1.0.0
15	gcc-3.3.6	RaLink SDK 3.1.0.0
16	Uclibc-0.9.29	RaLink SDK 3.1.0.0

## Availability of source code

Sitecom Europe BV has made available the full source code of the GPL licensed software, including any scripts to control the compilation and installation of the object code [in the driver section of this product](#).

## No Warranty

The free software included in this product is distributed in the hope that it will be useful, but WITHOUT ANY LIABILITY OF OR ANY WARRANTY FROM THE LICENSOR.

## Appendix B: GNU GENERAL PUBLIC LICENSE

Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

### Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too. When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if

you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things. To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights. We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations. Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all. The precise terms and conditions for copying, distribution and modification follow.

## **TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION**

0.

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1.

You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2.

You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions: a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change. b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License. c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other

licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following: a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free

software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8.

If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9.

The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10.

If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

## **NO WARRANTY**

11.

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

## **END OF TERMS AND CONDITIONS**