

Geavanceerde gebruikershandleiding internet



Welkom bij Internet van Ziggo

Van harte welkom bij Internet van Ziggo. Met deze geavanceerde handleiding kunt u de instellingen wijzigen van uw Wi-Fi modem.



Let op

Het aanpassen van de geavanceerde instellingen is op eigen risico. Ziggo heeft uw Wi-Fi modem standaard zo ingesteld dat het Wi-Fi modem goed werkt bij normaal gebruik. Mocht het Wi-Fi modem niet goed werken nadat u de geavanceerde instellingen gewijzigd heeft, dan adviseren wij u de standaardinstellingen te herstellen. Dit kan via de basisinstellingen of via een hard reset (zie de Gebruikershandleiding Internet). De reguliere Ziggo helpdesk kan u niet adviseren over de geavanceerde instellingen. Mocht u hier toch advies over willen, neem dan contact op met onze aanvullende dienst Service+ (0900-1876, € 0,65 per minuut).

Veel plezier met Internet van Ziggo!

Opmerkingen over de installatie en het gebruik van Internet van Ziggo

Internet van Ziggo is bedoeld voor persoonlijk gebruik. Het gebruik en de installatie van Internet van Ziggo zijn gebonden aan de Algemene Basisvoorwaarden Ziggo en de Aanvullende Voorwaarden Ziggo Internet. De meest recente versies kunt u vinden op: www.ziggo.nl/voorwaarden.

Inhoudsopgave

	Welkom bij Internet van Ziggo	1
	Inhoudsopgave	2
1	Internet van Ziggo	4
1.1	Symbolen	4
1.2	Ziggo Internet	4
2	Inloggen op de gebruikersomgeving	5
2.1	Geavanceerde instellingen.	5
3	Basic	6
3.1	Docsis	6
3.2	Firmware	6
3.3	Status	7
3.4	Security	8
3.5	Factory defaults	9
4	Gateway	10
4.1	Setup	10
4.2	DHCP	12
4.3	DDNS	14
4.4	Backup	16
4.5	Time	17
4.6	Options	18
4.7	Static Lease	20
4.8	IP Filtering	21
4.9	MAC Filtering	22
4.10	Port Filtering	23
4.11	Forwarding	24
4.12	Port Triggering	25
4.13	DMZ Host	27
4.14	RIP setup	28



5	Firewall	30
5.1	Web Content Filter	30
5.2	Local Log	32
5.3	Remote Log	33
6	Parental Control	35
6.1	User Setup	36
6.2	Basic Settings	39
6.3	ToD filter	41
6.4	Local Log	42
7	Wireless	43
7.1	Radio	43
7.2	Primary Network	48
7.3	Advanced	53
7.4	Access Control	56
7.5	Wi-Fi Multimedia (WMM)	57
7.6	Bridging	60
8	VPN	61
8.1	Basic	62
8.2	IPsec	63
8.3	Event Log	69
9	Overzicht van LED lampjes	70

1

Internet van Ziggo

Deze handleiding leidt u stap voor stap door de geavanceerde instellingen van Internet van Ziggo. Wij adviseren u om deze handleiding op uw computer op te slaan in verband met het eventueel wegvallen van de internetverbinding.

Heeft u hulp nodig? Stel uw vraag aan onze Online Assistent op www.ziggo.nl/klantenservice of bekijk het portal op www.ziggo.nl/WiFimodem.

De afbeeldingen in deze handleiding kunnen afwijken van de werkelijkheid.

1.1 Symbolen

In deze handleiding komt u de volgende symbolen tegen:



Let op

... geeft u extra uitleg over mogelijkheden of situaties.



Tip

... geeft u handige informatie over de toepassing van een functie.

1.2 Ziggo Internet

U heeft gekozen voor internetten via de kabel. Een goede keuze! Met internet van Ziggo bent u onbeperkt online. U krijgt gratis een spamfilter voor uw e-mail programma en anti-virus ter bescherming van uw computer.

2

Inloggen op de gebruikersomgeving

In de gebruikersomgeving kunt u geavanceerde instellingen van uw Wi-Fi modem wijzigen. Om op de gebruikersomgeving in te loggen volgt u de volgende stappen:

1. Open een internet browser op uw PC.
2. Typ het adres ***http://192.168.178.1*** in de adresbalk en druk op ***Enter***. Het login venster waarin wordt gevraagd om een gebruikersnaam en wachtwoord verschijnt.



3. Voer uw gebruikersnaam en wachtwoord in en klik op ***Inloggen***. Standaard is de gebruikersnaam ***ziggo*** en het wachtwoord ***draadloos***.

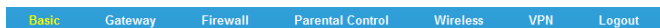
2.1 Geavanceerde instellingen

Na het inloggen verschijnt de startpagina van de gebruikersomgeving. Op deze startpagina staat basisinformatie van uw Wi-Fi modem weergegeven. De uitleg over de basisinformatie vindt u in de Gebruikershandleiding Internet.

Via de knop ***Geavanceerde instellingen*** kunt u geavanceerde instellingen wijzigen.

3

Basic



In dit hoofdstuk worden de basisinstellingen van de geavanceerde instellingen beschreven. De instellingen kunt u onder het menu **Basic** wijzigen.

3.1 Docsis

Deze pagina is alleen van belang voor Ziggo en wordt niet toegelicht in deze handleiding.

3.2 Firmware

Op deze pagina kunt u de standaard Ziggo instellingen van het Wi-Fi modem bekijken.



**Hardware
Version**

Uitlezing van het versienummer van de hardware.

Software Version	Uitlezing van het versienummer van de software.
Cable Modem Serial Number	Uitlezing van het serienummer van het Wi-Fi modem.
CM certificate	Uitlezing of het Cable Modem (CM) certificaat geïnstalleerd is.

3.3 Status

Op deze pagina kunt u de status van het Wi-Fi modem bekijken.



System Up Time	Uitlezing van de uptime van het Wi-Fi modem sinds de laatste reset of inschakeling.
Network Access	Uitlezing van de status van de netwerktoegang.
Cable Modem MAC	Uitlezing van het Media Access Control (MAC) adres van het Wi-Fi modem.
CPE MAC	Uitlezing van het MAC adres van de ingebouwde Media Terminal Adapter (MTA) voor telefonie van Ziggo.

3.4 Security

Op deze pagina kunt u de inloggegevens van het Wi-Fi modem wijzigen.



- New Username** Veld voor het instellen van de nieuwe gebruikersnaam.
- New Password** Veld voor het instellen van het nieuwe wachtwoord.
- Re-Enter New Password** Veld om het nieuwe wachtwoord te herhalen.
- Current Password** Veld om het huidige wachtwoord in te geven.
- Apply** Knop om de ingestelde waarden door te voeren.



Tip

Noteer uw nieuwe wachtwoord op het Wi-Fi modem of in de handleiding wanneer u deze gewijzigd heeft.

3.5 Factory defaults

Op deze pagina kunt u de standaard Ziggo instellingen herstellen.



Restore Factory Defaults Instelling om de standaard Ziggo instellingen te herstellen.

Apply Knop om de ingestelde waarde door te voeren.

4

Gateway

Basic **Gateway** Firewall Parental Control Wireless VPN Logout

In dit hoofdstuk worden de gateway instellingen beschreven. De instellingen kunt u onder het menu **Gateway** wijzigen.

4.1 Setup

Op deze pagina kunt u verschillende instellingen van de LAN en WAN wijzigen.

Zigo modemrouter **ubee**

Basic **Gateway** Firewall Parental Control Wireless VPN Logout

Setup

Gateway

Setup

This page allows configuration of the basic features of the broadband gateway related to your ISP's connection.

Network Configuration

LAN

IP Address: 192 168 178 1

MAC Address: 88:9f:fe:c1:34:2b

WAN

IP Address: 83.82.197.115

MAC Address: 88:9f:fe:c1:34:29

Duration: 05 H, 19 M, 41 S, 20

Expires: Tue Apr 12 03:22:19 2011

IPv4 DNS Servers: 212.54.40.25, 212.54.35.25

Release WAN Lease Renew WAN Lease

WAN Connection Type: DHCP

MTU Size: 0 (256-1500 octets, 0 = use default)

Spoofed MAC Address: 00 00 00 00 00 00

Apply

©2010 Ubee Interactive. All rights reserved.

LAN (Local area network)

IP address

Veld voor het instellen van het LAN IP adres van het Wi-Fi modem. Dit is tevens het default gateway address en het IP adres om in te loggen op de gebruikersomgeving. Het standaard IP adres is **192.168.178.1**.

**Let op**

Als u andere routers aansluit op het Wi-Fi modem dan mag het default gateway address van de andere routers niet hetzelfde zijn als dat van het Wi-Fi modem.

MAC Address

Uitlezing van het MAC adres van het Wi-Fi modem.

WAN (Wide Area Network)

IP Address

Uitlezing van het IP adres dat is toegekend.

MAC Address

Uitlezing van het MAC adres.

Duration

Uitlezing van de geldigheidsduur van het IP adres dat is toegekend.

Expires

Uitlezing van de verloopdatum van het toegekende IP adres.

Release WAN Lease

Knop voor het vrijgeven van het WAN IP adres.

Renew WAN Lease

Knop voor het vernieuwen van het WAN IP adres.

Wan connection type

Instelling van de methode om een WAN IP adres te verkrijgen. Standaard gebeurt dat via Dynamic Host Configuration Protocol (DHCP).

**Let op**

Ziggo ondersteunt alleen de standaard waarde. Het veranderen van de waarde kan problemen geven.

MTU size

Veld voor het instellen van de grootte van netwerkframes. Standaard is deze waarde 0 om de standaard Maximum Transmission Unit (MTU) grootte te kiezen.

Spoofed MAC address

Veld voor het instellen van het MAC adres van de router aan de WAN zijde.

**Let op**

Ziggo ondersteunt alleen de standaard waarde. Het veranderen van de waarde kan problemen geven.

Apply

Knop om de ingestelde waarden door te voeren.

4.2 DHCP

Op deze pagina kunt u de **DHCP Server** instellingen van het Wi-Fi modem instellen en bekijken. De **DHCP Server** kent IP adressen toe aan de apparaten die verbonden zijn met het Wi-Fi modem.

Ziggo modemrouter **ubee**

Basic **Gateway** Firewall Parental Controls Wireless VPN Logout

Gateway

DHCP

This page allows configuration and status of the optional internal DHCP server for the LAN.

DHCP Server ☒ Yes ☐ No

Starting Local Address **192.168.178**

Number of DHCPs

Lease Time

DHCP Clients

Mac Address	IP Address	Lease Time	Expires	Expires	Expires
0024060ac874	192.168.178.01255255255.0000	00 H:01 M:00 S:00	Fri Apr 08 11:45:01 2011		
002123444444	192.168.178.017285255255.0000	00 H:01 M:00 S:00	Fri Apr 08 11:50:46 2011		
001x9223777	192.168.178.019255255255.0000	00 H:01 M:00 S:00	Fri Apr 08 11:47:03 2011		

Current System Time: Fri Apr 08 10:51:05 2011

©2010 Ubee Interactive. All rights reserved.

DHCP Server

Instelling om de DHCP Server in- of uit te schakelen. Wanneer u de DHCP Server uitschakelt worden de overige instellingen genegeerd. Als u statische IP adressen wilt gebruiken zet u deze functie op **No**.

Starting Local Address

Veld voor het instellen van het startadres van de DHCP pool. Standaard is de DHCP pool **192.168.178.10**.

**Let op**

Het startadres mag niet hetzelfde zijn als het default gateway address van het Wi-Fi modem.

Number of CPE's

Veld voor het instellen van het aantal apparaten dat aan het Wi-Fi modem gekoppeld mag worden (maximaal 200 apparaten).

Lease Time

Veld voor het instellen van de lease tijd in minuten (tussen 1 en 71582788). De lease tijd is de tijd dat een (via DHCP verkregen) IP adres gebruikt kan worden door een netwerkkapparaat. Is de lease tijd verstreken? Dan vraagt het netwerkkapparaat opnieuw een IP adres aan.

Apply

Knop om de ingestelde waarden door te voeren.

DHCP Clients

In de DHCP Clients lijst staan de apparaten die met het Wi-Fi modem verbonden zijn. Per apparaat staan de volgende gegevens weergegeven:

MAC Address

Uitlezing van het MAC adres van de client.

IP Address

Uitlezing van het IP adres van de client.

Subnet Mask

Uitlezing van het gebruikte Subnet masker.

Duration

Verstreken tijd sinds het IP adres is verstrekt. Indien het om een gereserveerd IP adres gaat, staat hier **Statis IP Address**.

Expires

Uitlezing van de geldigheidsduur van de IP adressen die zijn uitgegeven.

- Select** Instelling om het toegekende IP adres als statisch IP adres te reserveren.
- Current System Time** Uitlezing van de actuele systeemtijd.
- Force Available** Knop om wijzigingen in de router en bij de aangesloten apparaten te forceren.

4.3 DDNS

Wanneer u via een andere internetaansluiting (zonder gebruik te maken van het WAN IP adres van het Wi-Fi modem) op het Wi-Fi modem wilt inloggen heeft u een Dynamic Domain Name Service (DDNS) nodig. Een geregistreerde hostname kan dynamisch worden gekoppeld aan het publieke WAN IP adres. Ondersteunende DDNS diensten zijn te vinden op www.dyndns.org.



- DDNS Service** Instelling van de gewenste DDNS Service.
- User Name** Veld voor het instellen van de gebruikersnaam voor de geselecteerde DDNS Service.
- Password** Veld voor het instellen van het wachtwoord voor de geselecteerde DDNS Service.
- Host Name** Veld voor het instellen van de hostname voor de geselecteerde DDNS Service.

<i>IP Address</i>	Uitlezing van het IP adres van de DDNS server.
<i>Status</i>	Uitlezing van de status van de DDNS server.
<i>Apply</i>	Knop om de ingestelde waarden door te voeren.

4.4 Backup

Op deze pagina kunt u een backup van de instellingen maken of terugzetten.



Bestand kiezen Knop om het bestand te selecteren waarin de instellingen zijn opgeslagen.

Restore Knop om eerder opgeslagen instellingen terug te plaatsen in het Wi-Fi modem.

Backup Knop om huidige instellingen in een bestand op te slaan.
Het bestand wordt automatisch gedownload naar de browserapplicatie waarmee u toegang heeft verkregen tot de gebruikersomgeving.

4.5 Time

Op deze pagina kunt u de instellingen van de manier waarop de systeemtijd wordt verkregen wijzigen.

**Enable SNTP**

Instelling om de Simple Network Time Protocol (SNTP) / systeemtijd te synchroniseren met een timeserver op het internet.

Current Time

Uitlezing van de huidige systeemtijd.

System Start Time

Uitlezing van de verstreken tijd vanaf het moment dat het systeem opgestart is.

Time Server 1-3

Veld voor het instellen van het IP adres of domeinnaam van de eerste, tweede en derde timeserver.

Timezone Offset

Instelling van de gewenste tijdzone.

Apply

Knop om de ingestelde waarden door te voeren.

Reset Values

Knop om de huidige instellingen naar de standaard Zigo terug te zetten.

4.6 Options

Op deze pagina kunt u geavanceerde gateway instellingen wijzigen.



WAN Blocking Instelling om connection requests vanaf de WAN zijde te blokkeren.



Let op

Inloggen op het Wi-Fi modem vanuit een andere internetlocatie wordt hiermee onmogelijk.

ICMP Blocking Instelling om Internet Control Message Protocol (ICMP) berichten te blokkeren.

Ipsec PassThrough Instelling om Virtual Private Network (VPN) tunnels transparant te kunnen doorgeven. De VPN tunnels beginnen of eindigen hierbij niet in het Wi-Fi modem, maar in een randapparaat.

**PPTP
PassThrough**

Instelling om Point to Point Tunneling Protocol (PPTP) tunnels transparant te kunnen doorgeven. Hierdoor kan een apparaat aan de LAN zijde van het Wi-Fi modem een VPN verbinding opzetten met een apparaat aan de WAN zijde.

**Multicast
Enable**

Instelling om multicast pakketten tussen LAN en WAN zijde van het Wi-Fi modem door te geven.

UPnP Enable

Instelling om de UPnP agent in het Wi-Fi modem te activeren. Door middel van UPnP worden netwerkapparaten automatisch met elkaar verbonden.

Apply

Knop om de ingestelde waarden door te voeren.

**PassThrough
MAC addresses**

Instelling om MAC adressen in de PassThrough tabel, buiten het Wi-Fi modem om (via Network Address Translation (NAT) of DHCP), naar de WAN zijde doorgeven. Bijvoorbeeld bij een Bridge mode.

**Let op**

Deze optie moet uit staan.

**Add MAC
Address**

Knop om MAC adressen toe te voegen.

**Remove MAC
Address**

Knop om geselecteerde MAC adressen te verwijderen.

Clear All

Knop om alle MAC adressen uit de lijst te verwijderen.

4.7 Static Lease

Op deze pagina kunnen statische IP adressen worden toegekend aan apparaten in het LAN netwerk binnen een bepaald adresbereik.

Ziggo modemrouter **ubee**

Basic **Gateway** Firewall Parental Control Wireless VPN Logout

Setup
DHCP
DNS
Backup
Time
System
Static Lease
IP Filtering
MAC Filtering
Port Filtering
Forwarding
Port Triggers
DMZ Host
NAT Setup

Gateway

Static Lease

This page allows configuration of static lease in order to create the IP reservation with MAC address.

LAN IP Address range 192.168.178.10 – 192.168.178.73

Static Lease											
MAC Address								IP Address		Enabled	
00	:	00	:	00	:	00	:	00	:	00	<input type="checkbox"/>
00	:	00	:	00	:	00	:	00	:	00	<input type="checkbox"/>
00	:	00	:	00	:	00	:	00	:	00	<input type="checkbox"/>
00	:	00	:	00	:	00	:	00	:	00	<input type="checkbox"/>
00	:	00	:	00	:	00	:	00	:	00	<input type="checkbox"/>
00	:	00	:	00	:	00	:	00	:	00	<input type="checkbox"/>
00	:	00	:	00	:	00	:	00	:	00	<input type="checkbox"/>
00	:	00	:	00	:	00	:	00	:	00	<input type="checkbox"/>
00	:	00	:	00	:	00	:	00	:	00	<input type="checkbox"/>
00	:	00	:	00	:	00	:	00	:	00	<input type="checkbox"/>
00	:	00	:	00	:	00	:	00	:	00	<input type="checkbox"/>
00	:	00	:	00	:	00	:	00	:	00	<input type="checkbox"/>
00	:	00	:	00	:	00	:	00	:	00	<input type="checkbox"/>
00	:	00	:	00	:	00	:	00	:	00	<input type="checkbox"/>

Apply

MAC Address Veld voor het instellen van het MAC adres van het apparaat waaraan een statisch IP adres moet worden toegekend.

IP Address Veld voor het instellen van het statische IP adres.

Enabled Instelling om het statische IP adres te activeren.

Apply Knop om de ingestelde waarden door te voeren.

4.8 IP Filtering

Op deze pagina kunnen IP filters worden gedefinieerd om dataverkeer naar apparaten met specifieke IP adressen te blokkeren. Elk filter kan voor een reeks van apparaten worden ingesteld. Een reeks bestaat uit een begin en een eind IP adres.

Start Address	End Address	Enabled
192.168.178.	192.168.178.	<input type="checkbox"/>
192.168.178.	192.168.178.	<input type="checkbox"/>
192.168.178.	192.168.178.	<input type="checkbox"/>
192.168.178.	192.168.178.	<input type="checkbox"/>
192.168.178.	192.168.178.	<input type="checkbox"/>
192.168.178.	192.168.178.	<input type="checkbox"/>
192.168.178.	192.168.178.	<input type="checkbox"/>
192.168.178.	192.168.178.	<input type="checkbox"/>
192.168.178.	192.168.178.	<input type="checkbox"/>
192.168.178.	192.168.178.	<input type="checkbox"/>

Start Address Veld voor het instellen van het eerste IP adres van een reeks apparaten.

End Address Veld voor het instellen van het laatste IP adres van een reeks apparaten.

Enabled Instelling om het IP filter te activeren. Hierbij wordt het dataverkeer van, naar en tussen de opgegeven IP adressen geblokkeerd.

Apply Knop om de ingestelde waarden door te voeren.

4.9 MAC Filtering

Op deze pagina kunnen MAC filters worden gedefinieerd om dataverkeer naar apparaten in het LAN netwerk, met specifieke MAC adressen, te blokkeren. De MAC adressen worden opgeslagen in een Black list.



Add MAC Address

Knop om MAC adressen toe te voegen.

Remove MAC Address

Knop om geselecteerde MAC adressen te verwijderen.

Clear All

Knop om alle MAC adressen uit de lijst te verwijderen.

4.10 Port Filtering

Op deze pagina kunnen Port filters worden gedefinieerd om specifieke internetdiensten voor alle LAN apparaten in het netwerk te blokkeren.

Gateway

Port Filtering

This page allows configuration of port filters in order to block specific internet services to all devices on the LAN.

Start Port	End Port	Protocol	Enabled
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>

Apply

©2011 Ubee Innovations. All rights reserved.

Start Port

Veld voor het instellen van het eerste poortnummer van een reeks poorten.

End Port

Veld voor het instellen van het laatste poortnummer van een reeks poorten.

Protocol

Instelling om het Transmission Control Protocol (TCP), User Datagram Protocol (UDP) of TCP en UDP te blokkeren.

Enabled

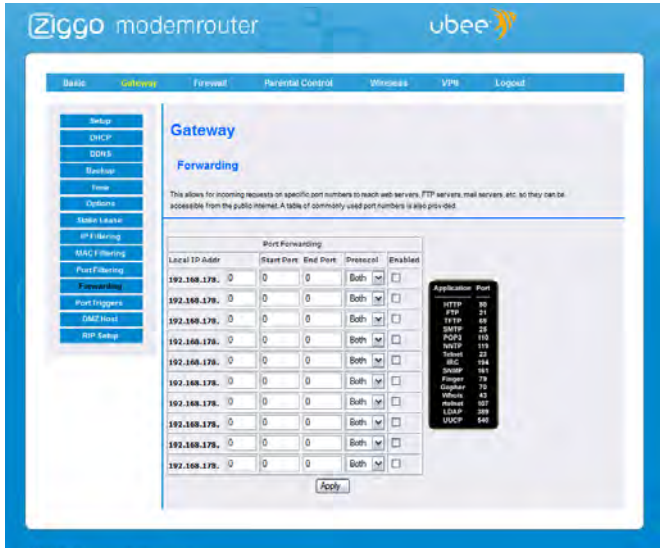
Instelling om het poort filter te activeren. Hierbij wordt het dataverkeer van, naar en tussen de opgegeven poorten geblokkeerd.

Apply

Knop om de ingestelde waarden door te voeren.

4.11 Forwarding

Op deze pagina kunnen connection requestes van de WAN zijde van het Wi-Fi modem worden doorgestuurd naar een specifiek apparaat aan de LAN zijde.



Let op

Forwarding werkt niet in combinatie met DMZ.



Tip

Bij **Forwarding** worden poortnummers gebruikt van een connection request. Bijvoorbeeld: een File Transfer Protocol (FTP) request wordt aan het poortnummer herkend en wordt doorgeleid naar een FTP server aan de LAN zijde.

**Tip**

*Kent u bij het opzetten van een **Forward** statische IP adressen toe aan de apparaten waar een connection request naar wordt doorgeleid. Hierdoor voorkomt u dat de **Forward** instellingen moeten worden aangepast, wanneer de lease tijd van een dynamisch verkregen IP adres verloopt.*

Local IP Addr	Veld voor het instellen van het IP adres van het apparaat waarvoor de Forward wordt opgezet.
Start Port	Veld voor het instellen van het eerste poortnummer van een reeks poorten.
End Port	Veld voor het instellen van het laatste poortnummer van een reeks poorten.
Protocol	Instelling om het protocol TCP, UDP of TCP en UDP te blokkeren.
Enabled	Instelling om de Forward te activeren.
Apply	Knop om de ingestelde waarden door te voeren.
Application port map	Uitlezing van veel gebruikte applicaties en de bijbehorende poortnummers.

4.12 Port Triggering

Op deze pagina kan dynamisch een tijdelijke **Forward** tussen apparaten aan de WAN zijde van het Wi-Fi modem en apparaten aan de LAN zijde worden opgezet. Hierdoor kan bi-directioneel dataverkeer op een correcte manier worden doorgeleid.

**Let op**

Port Triggering kan voor het correct functioneren van bijvoorbeeld videoconferenties, spraakconferenties, spellen en chatprogramma's nodig zijn.

Trigger Range

Trigger Range is een reeks poortnummers. Wanneer een lokaal netwerkapparaat een WAN apparaat probeert te bereiken met een poort in de **Trigger Range**, onthoudt het Wi-Fi modem het IP adres hiervan.

Target Range

Target Range is een reeks poortnummers. De **Target Range** wordt door WAN netwerkkapparaten gebruikt om data naar het LAN apparaat terug te sturen. Het Wi-Fi modem zal binnenkomende pakketten met deze poortnummers naar het betreffende LAN apparaat doorsturen.

Zigo modemrouter **ubee**

Basic **Gateway** Firewall Parental Control Wireless VPN Logout

Setup
DHCP
ODNS
Backup
Time
Options
Static Lease
IP Filtering
MAC Filtering
Port Filtering
Port Triggers
Forwarding
Port Triggers
DMZ Host
RIP Setup

Gateway

Port Triggers

This page allows configuration of dynamic triggers to specific devices on the LAN. This allows for special applications that require specific port numbers with bi-directional traffic to function properly. Applications such as video conferencing, voice, gaming, and some messaging program features may require these special settings.

Trigger Range		Target Range		Protocol	Enable
Start Port	End Port	Start Port	End Port		
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>

Apply

©2010 Libero Interactive. All rights reserved.

Start Port

Veld voor het instellen van het eerste poortnummer van een reeks poorten.

End Port

Veld voor het instellen van het laatste poortnummer van een reeks poorten.

Protocol

Instelling om het protocol TCP, UDP of TCP en UDP te blokkeren.

Enable

Instelling om de **Trigger Range** en **Target Range** te activeren.

Apply

Knop om de ingestelde waarden door te voeren.

4.13 DMZ Host

Op deze pagina kunnen apparaten uit de LAN zijde direct zichtbaar worden gemaakt aan de WAN zijde. Dit kan worden toegepast wanneer **Port Triggers** of **Port Forwards** niet gebruikt kunnen worden of voor specifieke instellingen.



Let op

Port Forwarding en **Port triggering** werken niet meer als Demilitarized Zone (DMZ) Host gebruikt wordt.



DMZ Address

Veld voor het instellen van het IP adres van het apparaat aan de LAN zijde dat direct zichtbaar wordt gemaakt aan de WAN zijde.

Apply

Knop om de ingestelde waarden door te voeren.

4.14 RIP setup

Op deze pagina kunnen Routing Information Protocol (RIP) parameters worden geconfigureerd. Deze RIP parameters zijn nodig voor authenticatie en identificatie het bestemmings IP adres, het masker en de interval rapportage. Het RIP zorgt automatisch voor de snelste routing naar iedere bestemming.



Tip

Het RIP wordt gebruikt tussen routers die meer dan 1 WAN aansluiting hebben. Omdat het Wi-Fi modem slechts 1 WAN aansluiting heeft, is het RIP hiervoor niet zinvol.

The screenshot shows the 'Gateway' configuration page for a Zigo modemrouter. The 'Routing Information Protocol Setup' section is active. It includes a sidebar with navigation links: Setup, DHCP, DNS, Backup, Time, Options, Static Leases, IP Filtering, MAC Filtering, Port Filtering, Forwarding, Port Triggers, DMZ Host, and WAN Setup. The main configuration area has the following fields:

- RIP Authentication:** ☒ Enable
- RIP Authentication Key:** [Text input field]
- RIP Authentication Key ID:** [Input field with value 0]
- RIP Reporting Interval:** [Input field with value 30] seconds
- RIP Destination IP Address:** [Input fields with values 0, 0, 0, 0]
- RIP Destination IP Subnet Mask:** [Input fields with values 255, 255, 255, 0]

An 'Apply' button is located at the bottom of the configuration area. The footer of the page reads: '©2010 Ubee Interactive. All rights reserved.'

RIP Authentication Instelling voor het aan- en uitschakelen van de RIP Authenticatie.

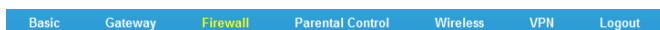
RIP Authentication key Veld voor het instellen van de RIP authenticatiesleutel.

RIP Authentication key ID Veld voor het instellen van het ID van de RIP authenticatiesleutel.

<i>RIP Reporting Interval</i>	Veld voor het instellen van de interval rapportage in seconden.
<i>RIP Destination IP Address</i>	Veld voor het instellen van het bestemmings IP adres.
<i>RIP Destination Subnet Mask</i>	Veld voor het instellen van het bestemmings Subnet masker.
<i>Apply</i>	Knop om de ingestelde waarden door te voeren.

5

Firewall



In dit hoofdstuk worden de firewall instellingen beschreven. De instellingen kunt u onder het menu **Firewall** wijzigen.

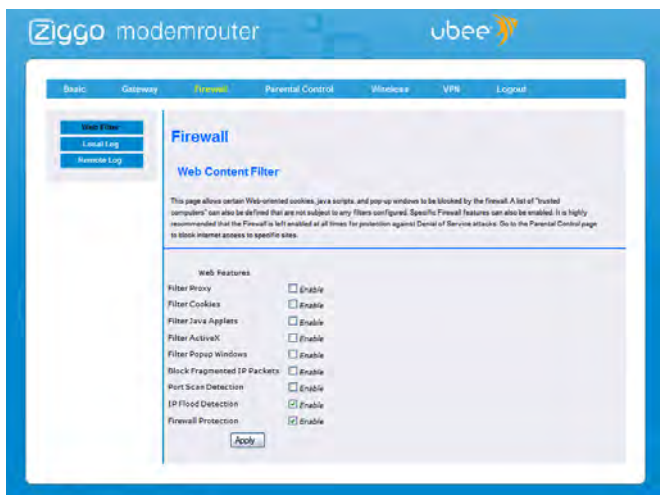


Let op

*Zorgt u ervoor dat de firewall altijd ingeschakeld is. De firewall beschermt u tegen Denial- of Service-aanvallen. Zie ook het hoofdstuk **Geavanceerde instellingen - Parental Control** om internettoegang tot bepaalde websites te blokkeren.*

5.1 Web Content Filter

Op deze pagina kunnen **Web Content Filters** worden geactiveerd voor het blokkeren van verschillende functies.



<i>Filter Proxy</i>	Instelling voor het blokkeren van Proxy instellingen.
<i>Filter Cookies</i>	Instelling voor het blokkeren van web-georiënteerde cookies.
<i>Filter Java Applets</i>	Instelling voor het blokkeren van Java Applets.
<i>Filter Active X</i>	Instelling voor het blokkeren van ActiveX.
<i>Filter Popup Windows</i>	Instelling voor het blokkeren van pop-up vensters.
<i>Block Fragmented IP Packets</i>	Instelling voor het blokkeren van gefragmenteerde IP pakketten.
<i>Port Scan Detection</i>	Instelling voor het blokkeren van een poortscan. Een poortscan wordt aan de LAN en WAN zijde gedetecteerd en geblokkeerd.
<i>IP Flood Detection</i>	Instelling voor het blokkeren van een IP Floods pakketten. Een IP Flood wordt aan de LAN en WAN zijde gedetecteerd en geblokkeerd.
<i>Firewall Protection</i>	Instelling om de firewall in te schakelen of uit te schakelen.
<i>Apply</i>	Knop om de ingestelde waarden door te voeren.

5.2 Local Log

Op deze pagina kan een logboek van de firewall worden ingesteld. Het logboek kan naar een opgegeven e-mailadres verzonden worden.

Contact Email Address	Veld voor het instellen van het e-mailadres waarnaar het logboek verzonden moet worden.
SMTP Server Name	Veld voor het instellen van de Simple Mail Transfer Protocol (SMTP) server naam.
SMTP Username	Veld voor het instellen van de SMTP gebruikersnaam.
SMTP Password	Veld voor het instellen van het SMTP wachtwoord.
E-mail Alerts	Instelling om het logboek naar het opgegeven e-mailadres te verzenden.
Apply	Knop om de ingestelde waarden door te voeren.

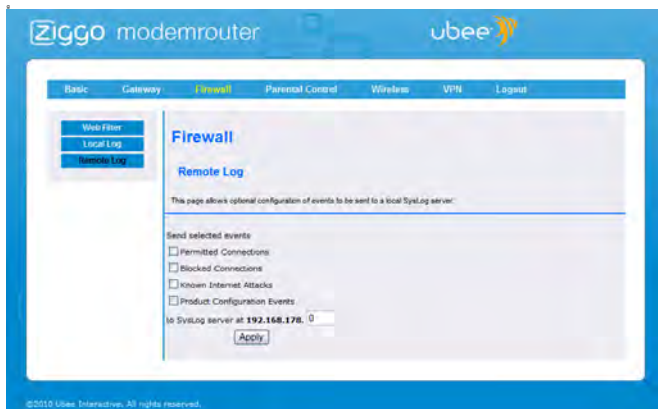
Log

In de tabel staan de events die reeds ingesteld zijn. Per event staan de volgende gegevens weergegeven:

Description	Uitlezing van de omschrijving van het event.
Count	Uitlezing van het aantal events.
Last Occurrence	Uitlezing van de laatste datum van het event.
Target	Uitlezing van de bestemming van het event.
Source	Uitlezing van de bron van het event.
E-mail Log	Knop om de instellingen toe te voegen.
Clear Log	Knop om alle events uit de lijst te verwijderen.

5.3 Remote Log

Op deze pagina kunnen events worden gekozen die naar een lokale syslog server worden gestuurd.



Permitted Connections	Instelling om een event te registreren voor elke toegestaaneverbinding.
Blocked Connections	Instelling om een event te registreren voor elk door de firewall geweigerde toeganspoging.
Known Internet Attacks	Instelling om een event te registreren voor elk bekende aanval vanaf het internet.

<i>Product Configuration Events</i>	Instelling om een event te registreren voor elke keer dat de Wi-Fi modem configuratie gewijzigd is door een gebruiker of beheerder.
<i>SysLog server</i>	Veld voor het instellen van het IP adres van de SysLog server.
<i>Apply</i>	Knop om de ingestelde waarden door te voeren.



Parental Control

Basic	Gateway	Firewall	Parental Control	Wireless	VPN	Logout
-------	---------	----------	------------------	----------	-----	--------

Dit hoofdstuk beschrijft de instellingen om bepaalde websites op het internet toegankelijk te maken (White List) of te blokkeren (Black List) voor specifieke gebruikers. De instellingen kunt u onder het menu **Parental Control** wijzigen.



Tip

De toegang van websites op het internet kan worden beperkt door een wachtwoord beveiliging, tijdsloten, website blokkades en blokkades op basis van sleutelwoorden.

6.1 User Setup

Op deze pagina kunnen gebruikersaccounts aangemaakt worden voor gebruikers aan de LAN zijde van het Wi-Fi modem.

User Configuration

Add User

Knop om een nieuwe gebruiker aan te maken.

User Settings

User Settings

Instelling van een gewenste gebruiker.

Instelling om een gebruiker te activeren.

Knop om een gebruiker te verwijderen.

Password

Veld voor het instellen van het wachtwoord voor de gebruiker.

Re-Enter Password

Veld voor het herhalen van het wachtwoord voor de gebruiker.

Trusted User

Instelling om de gebruiker **Trusted User** te maken.

**Tip**

***Trusted User** is handig bij tijdelijke situaties. De gedefinieerde filters worden hierbij overschreven en hoeven niet opnieuw aangemaakt te worden.*

Content Rule

Instelling van een gewenste content rule.

**Tip**

Wanneer de content rule White List en Black List toegangsdefinities bevat, zorgt een vinkje in de checkbox ervoor dat uitsluitend de vermelde websites in de White List websites toegestaan zijn.

Time Access Rule

Instelling van een tijdslot.

Session Duration

Veld voor het instellen van de maximale duur (minuten) van een gebruikerssessie. Bij het overschrijden van de maximale duur van de gebruikerssessie wordt de gebruiker uitgelogd. De gebruiker zal vervolgens opnieuw moeten inloggen.

Inactivity Time

Veld voor het instellen van de duur (minuten) van een gebruikerssessie waarbij de gebruiker inactief is. Bij het bereiken van de duur van een gebruikerssessie waarbij de gebruiker inactief is, wordt de gebruiker uitgelogd. De gebruiker zal vervolgens opnieuw moeten inloggen.

Apply

Knop om de ingestelde waarden door te voeren.

Trusted Computers

Add

Knop om het MAC adres van een **Trusted Computer** toe te voegen.

Remove

Knop om een geselecteerd **Trusted Computer** te verwijderen.

6.2 Basic Settings

Op deze pagina kunnen toegangsregels worden gedefinieerd.



Tip

Om er zeker van te zijn dat de laatste informatie getoond wordt, kunt u uw browser herladen.

Enable Parental Control Instelling om **Parental Control** in te schakelen.

Apply

Knop om de ingestelde waarden door te voeren.

Content Policy Configuration

In de content policy configuratievelden kan een nieuwe regel worden gedefinieerd.

Add New Policy Knop om een nieuwe toegangsregel aan te maken.

Content Policy List

Content Policy List Instelling van een gewenste toegangsregel.

Knop om een toegangsregel te verwijderen.

Keyword List Uitlezing van de sleutelwoorden die geblokkeerd zijn.

Add Keyword Knop om een sleutelwoord toe te voegen.

Remove Keyword Knop om een sleutelwoord te verwijderen.

Blockd Domain List Uitlezing van de domeinnamen die geblokkeerd zijn.

Add Domain Knop om een domeinnaam toe te voegen.

Remove Domain Knop om een domeinnaam te verwijderen.

Allowed Domain List Uitlezing van de domeinnamen die toegestaan zijn.

Add Domain Knop om een domeinnaam toe te voegen.

Remove Domain Knop om een domeinnaam te verwijderen.

Override Password

Met **Override Password** kan de toegang tot een geblokkeerde website worden geforceerd voor een ingestelde tijdsduur (seconden).

Password Veld voor het instellen van het wachtwoord voor een geblokkeerde website.

Re-Enter Password Veld voor het herhalen van het wachtwoord voor een geblokkeerde website.

**Access
Duration**

Veld voor het instellen van de tijdsduur (seconden) hoelang een geblokkeerde website geforceerd wordt.

Apply

Knop om de ingestelde waarden door te voeren.

6.3 ToD filter

Op deze pagina kunnen Time of Day (ToD) filters ingesteld worden. Een ToD filter blokkeert de toegang tot internet tijdens een bepaalde tijdsinterval op bepaalde dagen.

Parental Control

Time of Day Access Policy

This page allows configuration of time access policies to block all internet traffic to and from specific network devices based on time of day settings.

Time Access Policy Configuration

Create a new policy by giving it a descriptive name, such as "Weekend" or "Working Hours"

Time Access Policy List

No filters entered

Days to Block:

☐ Every day ☐ Sunday ☐ Monday ☐ Tuesday
☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday

Time to Block:

☐ All day

Start: 12 (hour) 00 (min) AM

End: 12 (hour) 00 (min) AM

©2010 Ubee Interactive. All rights reserved.

Add New Policy Knop om een nieuwe tijdsintervan aan te maken.

Time Access Policy List

**Time Access
Policy List**

Instelling van een gewenst tijdslot.

Instelling om een tijdslot te activeren.

Knop om een tijdslot te verwijderen.

- Days to Block** Instelling van de dagen waarop het tijdslot actief is.
- Time to Block** Instelling van de tijdsduur waarin de toegang tot internet geblokkeerd is.
- Apply** Knop om de ingestelde waarden door te voeren.

6.4 Local Log

Op deze pagina kan het logboek van de **Parental Control** events worden bekeken.



- Last Occurrence** Uitlezing van het laatste event.
- Action** Uitlezing welke actie de Parental Control heeft uitgevoerd, inclusief afwijzen en toekennen van toegangsverzoeken.
- Target** Uitlezing van het IP adres van de website die tot deze event heeft geleid.
- User** Uitlezing van de gebruiker die dit event heeft veroorzaakt.
- Source** Uitlezing van het Personal Identity Portal (PIP) adres van de gebruiker die dit event heeft veroorzaakt.
- Clear Log** Knop om het logboek leeg te maken.

7

Wireless

Basic Gateway Firewall Parental Control **Wireless** VPN Logout

In dit hoofdstuk worden de draadloze instellingen beschreven. De instellingen kunt u onder het menu **Wireless** wijzigen.

7.1 Radio

Op deze pagina kunnen de instellingen voor de draadloze radio worden gewijzigd, zoals de landkeuze, het kanaal en de bandbreedte.

Zigo modemrouter **ubee**

Basic Gateway Firewall Parental Control **Wireless** VPN Logout

Radio
Primary Network
Advanced
Access Control
WMM
Bridging

Wireless

802.11 Radio

This page allows configuration of the Wireless Radio including current country and channel number.

Wireless Interfaces: DeNieuweZigoModemrouter (90:00:4E:0F:79:F4)

Wireless: **Enabled**

Country: **NETHERLANDS**

Output Power: **100%**

802.11 Band: **24Ghz**

802.11 n-mode: **Auto**

Bandwidth: **Auto (M)**

Sideband for Control Channel (40 MHz only): **Lower**

Control Channel: **Auto** Current: 6

Regulatory Mode: **Off**

Pre-Network Radar Check: **60**

In-Network Radar Check: **60**

TPC Mitigation (db): **0 (Off)**

OBSS Coexistence: **1 (Enabled)**

Apply **Restore Wireless Defaults**

©2010 Ubee Interactive. All rights reserved.

Wireless Interfaces

Uitlezing van de naam van het draadloze netwerk (Service Set Identifier (SSID)) en de naam van het MAC adres.

Wireless

Instelling van de huidige status van het draadloze netwerk.

**Tip**

*Wanneer er andere routers in het netwerk voor draadloos internet worden gebruikt, kunt u **Wireless** uitschakelen voor betere prestaties.*

Country

Instelling van het land waarin de radio wordt gebruikt. Het Wi-Fi modem staat standaard op **Nederland**.

Output Power

Instelling van de signaalsterkte.

**Tip**

*De signaalsterkte kan in stappen van 25% worden ingesteld. Wanneer er meer dan 1 draadloze router wordt gebruikt, kunt u de **Output Power** laag instellen. Hierdoor wordt de interferentie tussen de draadloze routers minder, zodat de prestaties beter worden.*

802.11 Band

Instelling van de frequentieband.

**Tip**

De frequentieband kan op 2.5GHz of 5GHz worden ingesteld. Het bereik van de 5GHz frequentieband is kleiner dan de 2.4GHz frequentieband en wordt door minder netwerkapparaten ondersteund.

802.11n Mode

Instelling van de datasnelheid.

**Tip**

*Wanneer de **802.11n Mode** op **Auto** wordt ingesteld, zal de radio deze mode gebruiken (indien mogelijk). Om de maximale snelheid te bereiken is een kanaalbreedte van 40MHz nodig.*

Bandwith

Instelling van de bandbreedte van het draadloze transmissiekanaal.

**Let op**

Past u de 40MHz kanaalbreedte alleen toe indien er geen overlap is met andere draadloze netwerken in de buurt. In dit geval zal de 40MHz een betere prestatie leveren dan de 20MHz.

**Tip**

*Wanneer u hier voor 20MHz kiest kan **Sideband** niet worden gekozen. Om de maximale draadloze snelheid van het Wi-Fi modem te halen kiest u hier voor 40MHz.*

**Sideband for
Control
Channel (40
MHz only)**

Instelling van de Sideband wanneer u bij **Bandwith** voor 40MHz gekozen heeft.

**Tip**

*De twee 20MHz (**Control Channel** en **Extension Channel**) kanalen worden samengevoegd. Het **Extension Channel** nummer wordt bepaald door de **Control Channel** +4 (lager) of -4 (hoger).*

**Control
Channel**

Instelling of de kanalselectie automatisch plaatsvindt.

**Tip**

*U kunt in Nederland het **Control Channel** nummer kiezen tussen 1 en 13.*

**Regulatory
Mode**

Instelling van de speciale modus.

**Tip**

Inschakelen heeft negatieve gevolgen voor de prestaties. In Nederland is deze modus niet van toepassing.

**Pre-Network
Radar Check**

Veld voor het instellen van de tijdsduur (seconden) dat naar radarsignalen gezocht wordt, voordat het gewenste kanaal geactiveerd wordt.

**Let op**

*Deze functie is alleen van toepassing indien **802.11h** is geselecteerd bij de functie **Regulatory Mode**.*

Standaard staat deze functie op 60 seconden (maximaal 99 seconden). Wanneer u 0 instelt, wordt er niet naar radarsignalen gezocht.

**In-Network
Radar Check**

Veld voor het instellen van de tijdsduur (seconden) om radarsignalen te detecteren, nadat een kanaal gekozen is.

**Let op**

*Deze functie is alleen van toepassing indien **802.11h** is geselecteerd bij de functie **Regulatory Mode**.*

Standaard staat deze functie op 60 seconden (minimaal 10 seconden en maximaal 99 seconden).

**TPC Mitigation
(db)**

Instelling van de signaalreductiefactor als andere netwerken binnen bereik zijn.

**Let op**

*Deze functie is alleen van toepassing indien **802.11h** is geselecteerd bij de functie **Regulatory Mode**.*

**OBSS
Coexistence**

Instelling om ondersteuning voor overlappende netwerkanalen in te schakelen. Bijvoorbeeld als 20MHz apparaten zijn verbonden met het Wi-Fi modem en de radio in 40MHz mode staat ingesteld.

**Let op**

*Past u de **OBSS Coexistence** 1 (On) alleen toe indien er overlap is met andere draadloze netwerken in de buurt.*

**Tip**

Deze functie heeft een positief effect op interferentie met 20MHz netwerkverkeer. Om de maximale draadloze snelheid van het Wi-Fi modem te halen kiest u hier voor 0 (Off).

Apply

Knop om de ingestelde waarden door te voeren.

**Restore
Wireless
Defaults**

Knop om de standaard instellingen te herstellen.

7.2 Primary Network

Op deze pagina kunnen verschillende draadloze beveiligingsinstellingen worden gemaakt.

Zigo modemrouter **ubee**

Basic | Gateway | Firewall | Parental Control | **Wireless** | VPN | Logout

Radio
Primary Network
 Advanced
 Access Control
 WMM
 Bridge/UP

Wireless

802.11 Primary Network

This page shows configuration of the Primary Wireless Network and its security settings.

DeLuxeZigoModemrouter (80.00.42.05/19/14)

Basic Network

Primary Network: ☒ Enabled

Network Name (SSID): DeLuxeZigoModemrouter

Channel: Disabled

AP Isolate: Disabled

WPA: Disabled

WPA-PSK: Disabled

WPA2: Disabled

WPA2-PSK: Disabled

WPA/WPA2 Encryption: TKIP+AES

WPA Pre-Shared Key: *****

RADIUS Server: 192.168.1.1

RADIUS Port: 1812

RADIUS Key:

Group Key Rotation Interval: 0

WPA/WPA2 Re-auth Interval: 300

WEP Encryption: Disabled

Shared Key Authentication: Disabled

802.1x Authentication: Disabled

Network Key 1:

Network Key 2:

Network Key 3:

Network Key 4:

Current Network Key:

PassPhrase:

Automatic Security Configuration

WPS: ☒ Enabled

WPS Config Mode: Configure

The physical button on the AP will provision wireless clients using WPA Protected Setup (WPS).

Device Name: UbeeAP

WPS Setup AP

PIN: 8821452

WPS Add Client

Add a client: Pin/Name PIN

PIN:

©2010 Ubee Interactive. All rights reserved.

Primary Network Instelling om het eerste draadloze netwerk in of uit te schakelen.

Network Name Veld voor het instellen van de naam van het draadloze netwerk (SSID).
Standaard is de naam **Ziggo12345** waarbij 12345 willekeurig gekozen cijfers zijn. De SSID staat op de sticker onderop het Wi-Fi modem.

Closed Network Instelling of SSID zichtbaar is voor andere netwerkapparaten.



Let op

*Wanneer u deze functie op **Disabled** zet is het bij het verbinding maken met het Wi-Fi modem noodzakelijk de SSID handmatig in te stellen.*

AP Isolate Instelling om onderling dataverkeer tussen draadloze netwerkapparaten en het Wi-Fi modem te forceren.

WPA Instelling om Wi-Fi Protected Access (WPA) voor het beveiligen van het draadloze netwerk in te schakelen. Deze functie heeft een externe RADIUS Server nodig voor gebruikersauthenticatie.

WPA-PSK Instelling om Wi-Fi Protected Access Pre-Shared Key (WPA-PSK) voor het beveiligen van het draadloze netwerk in te schakelen.

WPA2 Instelling om WPA2 voor het beveiligen van het draadloze netwerk in te schakelen. Deze functie heeft een externe RADIUS Server nodig voor gebruikersauthenticatie.

WPA2-PSK Instelling om WPA2-PSK voor het beveiligen van het draadloze netwerk in te schakelen.

**WPA-WPA2
Encryption**

Instelling van de WPA en WPA 2 encryptie. Hierbij kunt u kiezen tussen uit Advanced Encryption Standard (**AES**) en Advanced Encryption Standard + Temporal Key Integrity Protocol (**AES+TKIP**) (standaard).

**Tip**

TKIP biedt compatibiliteit met oudere apparatuur. **AES** is daarentegen veiliger. **AES+TKIP** gebruikt waar mogelijk **AES** en gebruikt voor apparatuur die geen **AES** ondersteunen **TKIP**.

**WPA Pre-
Shared Key**

Veld voor het instellen van de netwerksleutel voor de WPA en WPA2 encryptie. De netwerksleutel bestaat uit een reeks van 8 tot 63 ASCII tekens of een 64 digit hexadecimaal getal. Bij elk Wi-Fi modem is de standaard netwerksleutel anders. De netwerksleutel staat op de sticker onderop het Wi-Fi modem.

RADIUS Server

Veld voor het instellen van het IP adres van de RADIUS Server. Alleen voor Enterprise WPA, WPA2 en 802.1x.

RADIUS Port

Veld voor het instellen van het poortnummer van de RADIUS Server. Alleen voor Enterprise WPA, WPA2 en 802.1x.

RADIUS Key

Veld voor het instellen van de sleutel van de RADIUS Server. Alleen voor Enterprise WPA, WPA2 en 802.1x.

**Group Key
Rotation
Interval**

Veld voor het instellen van de tijdsduur (seconden) van de interval dat aangeeft wanneer een groepsnetwerksleutel wordt vervangen. Een interval van 0 seconde schakelt de netwerksleutelvervanging uit.

**WPA/WPA2
Reauth Interval**

Veld voor het instellen van de tijdsduur (seconden) waarmee de verbonden apparaten zich moet her-authenticeren bij de RADIUS Server. Alleen bij Enterprise WPA, WPA2.

**WEP
Encryption**

Instelling van de Wired Equivalent Privacy (WEP) encryptie (64 of 128 bit).

**Let op**

*Om de functie **Shared Key Authentication** te gebruiken moet u deze functie inschakelen. WEP kan niet tegelijk met WPA of WPA2 worden ingeschakeld. WEP is minder veilig dan WPA en WPA2.*

**Shared Key
Authentication**

Instelling om authenticatie voor het draadloze netwerk volgens de IEEE802.11 standaard uit te voeren. De authenticatie bestaat uit een geheime netwerksleutel die bij de verbonden apparaten bekend is.

**802.1x
Authentication**

Instellingen om het 802.1x authenticatie mechanisme te gebruiken. Alleen zinvol voor bedrijfsnetwerken.

Network Key 1-4

Veld voor het instellen van de netwerksleutel voor de WEP encryptie. Een 64-bit sleutel bestaat uit 5 ASCII tekens of 10 hexadecimale teksten. Een 128-bit sleutel bestaat uit 13 ASCII teksten of 26 hexadecimale tekens.

**Current
Network Key
PassPhrase**

Instelling van de huidige netwerksleutel (1-4).

Veld voor het instellen om een WEP netwerksleutel door het Wi-Fi modem te laten genereren. De hier ingevulde tekst (maximaal 26 tekens) moet als wachtwoord worden ingevoerd op de te verbinden apparaten.

**Generate WEP
Keys**

Knop om 4 WEP netwerksleutels te genereren.

Apply

Knop om de ingestelde waarden door te voeren.

Automatic Security Configuration

Automatic Security Configuration	Instelling om Wi-Fi Protected Setup (WPS) te configureren.
Device Name	Veld voor het instellen van de naam voor het Wi-Fi modem als draadloos access point met WPS.

WPS Setup AP

PIN	Veld voor het instellen van de PIN code van het Wi-Fi modem. Bij elk Wi-Fi modem is de standaard PIN code anders en is vooraf ingevuld. De PIN code mag worden gewijzigd. Houdt hierbij rekening met het EAN-8 formaat (7 cijfers + 1 check digit).
Configure	Knop om verbinding te maken met een externe registrar via WPS.

WPS Add Client

Add a client	Instelling op welke manier verbinding met een netwerkkapparaat gemaakt wordt (via WPS).
Add	Knop om apparaten toe te voegen.
PIN	Veld voor het instellen van de PIN code om met een netwerkkapparaat verbinding te maken.

7.3 Advanced

Op deze pagina kunnen geavanceerde instellingen voor het draadloze netwerk worden gewijzigd.



54g™ Network Mode

Instelling om een keuze te maken tussen oudere draadloze protocollen:

- **54g Auto** biedt compatibiliteit met oudere 54g™, 802.11g en 802.11b netwerkkaparen.
- **54g Performance** staat alleen verbindingen met 54g netwerkkaparen toe.
- **54g LRS** biedt compatibiliteit met oude 54g™ apparaten.
- **802.11b** staat alleen verbindingen met 802.11b netwerkkaparen toe.



Let op

Deze functie kunt u alleen wijzigen als **802.11n Mode** uitgeschakeld is op de pagina **Radio**.

Basic Rate Set	<p>Instelling om de Basic Rate Set te selecteren die netwerkapparaten ondersteunt bij het verbinden maken met het Wi-Fi modem.</p> <ul style="list-style-type: none"> • Default is de Rate Set die bij de gekozen 54g Mode hoort. • All is de Rare Set die bij alle Mode hoort.
54g™ Protection	<p>Instelling om de RTS/CTS Flow Control te gebruiken om datadoorvoer te optimaliseren in 802.11b en 9 Mixed Mode.</p> <p>De Uit mode kan gebruikt worden in de meeste 802.11g verbindingen.</p>
XPress™ Technology	<p>Instelling om de 802.11g Wi-Fi doorvoersnelheid te verbeteren. Deze optie staat standaard uitgeschakeld.</p>
Rate	<p>Instelling om de Data Rate te kiezen. Alleen voor 802.11g apparaten.</p>
Beacon Interval	<p>Veld voor het instellen van de tijdsduur (milliseconden) van de Beacon interval (minimaal 100 en maximaal 65535 milliseconden).</p>
DTIM Interval	<p>Veld voor het instellen van de tijdsduur (milliseconden) waarmee het Beacon een Delivery Traffic Indication Message (DTIM) bevat.</p>
Fragmentation Threshold	<p>Veld voor het instellen van de data pakketgrootte (van 256 tot 2346 bytes) waarboven het pakket zal worden gefragmenteerd.</p>
RTS Threshold	<p>Veld voor het instellen van de Request To Send (RTS) drempelwaarde van 0 tot 2347 bytes.</p>
NPHY Rate	<p>Instelling van de maximale doorvoersnelheid van de fysieke laag (Physical Layer (PHY)) in 802.11n Mode. Deze instelling kan alleen gedaan worden als de 802.11n Mode op Automatic staat.</p>

**802.11n
Protection**

Instelling van de maximale doorvoersnelheid te verbeteren.

**Tip**

*Wanneer deze functie op **Auto** staat ingesteld, wordt flow control (RTS/CTS) gebruikt om de doorvoersnelheid te verbeteren in gemengde netwerken. Indien deze functie is uitgeschakeld wordt de alleen 802.11n doorvoersnelheid geoptimaliseerd, andere protocollen (bijvoorbeeld 802.11b) krijgen een lagere prioriteit.*

Multicast Rate

Instelling van de doorvoersnelheid van multicast pakketten in het draadloze netwerk.

Apply

Knop om de ingestelde waarden door te voeren.

7.4 Access Control

Op deze pagina kunnen instellingen gewijzigd worden om bepaalde MAC adressen toegankelijk te maken (White List) of te blokkeren (Black List).

Wireless

802.11 Access Control

This page allows configuration of the Access Control to the AP as well as status on the connected clients.

Wireless Interface: DeNieuweZigoModemrouter! 60:00:4E:0F:79F4

MAC Restrict Mode: Disabled

MAC Addresses

MAC Address	SSID	IP Address
00:24:06:0A:C8:74	0	-71
00:1B:77:21:AD:37	81420	-81
40:FC:89:F6:92:9C	77576	-79

Apply

Connected Clients

MAC Address	SSID	IP Address	Host Name	Mode	Speed (Mbps)
00:24:06:0A:C8:74	0	192.168.178.12	L302216	g	24000
00:1B:77:21:AD:37	81420	ERROR	ERROR	g	10000
40:FC:89:F6:92:9C	77576	ERROR	ERROR	n	20000

© 2010 Ubee Interactive. All rights reserved.

Wireless Interface

Instelling van de draadloze netwerkomgeving. In het Wi-Fi modem is er slechts één draadloos netwerk beschikbaar.

MAC Restrict Mode

Instelling om het toegangsbeleid te bepalen.

- **Off** betekent dat er geen beperkingen zijn
- **Allow** betekent dat uitsluitend apparaten waarvan het MAC adres in de lijst voorkomt toegang krijgen
- **Deny** betekent dat de apparaten waarvan het MAC adres in de lijst voorkomt de toegang wordt geweigerd

MAC Addresses Veld voor het instellen van de MAC adressen die geweigerd of toegestaan worden in het draadloze netwerk (afhankelijk van de MAC Restrict Mode).

Apply Knop om de ingestelde waarden door te voeren.

Connected Clients

In de tabel staan de apparaten die in het draadloze netwerk opgenomen zijn. De volgende gegevens worden weergegeven:

MAC Address	Uitlezing van het MAC adres.
Age(s)	Uitlezing van de tijdsduur dat het apparaat deel uitmaakt van het netwerk.
RSSI(dBm)	Uitlezing van de signaalsterkte.
IP Addr	Uitlezing van het IP adres.
Host Name	Uitlezing van de hostname.
Mode	Uitlezing van de gebruikte draadloze standaard.
Speed (kbps)	Uitlezing van de communicatiesnelheid.

7.5 Wi-Fi Multimedia (WMM)

Op deze pagina kunnen de Quality of Service (QoS) parameters worden ingesteld. Wi-Fi multimedia bepaalt de transmissieprioriteit van de draadloze netwerkpakketten afhankelijk van de op deze pagina ingestelde condities.



Tip

*Er zijn weinig apparaten die WMM kunnen toepassen, daarom staat WMM standaard op **Off**.*



WMM Support Instelling om WMM Support in of uit te schakelen.

No Acknowledgement Instelling om Frame Acknowledgement in of uit te schakelen. Voor tijdkritische data kan Acknowledgement worden uitgeschakeld om hertransmissie te voorkomen.

Power Save Support Instelling om de energiebesparing in of uit te schakelen. WMM Power Save verhoogt de efficiëntie en flexibiliteit van de datatransmissie. Afhankelijk van de QoS parameters kan de transmissie van meerdere pakketten dusdanig worden samengesteld dat een optimaal energieverbruik wordt bereikt.

Apply Knop om de ingestelde waarden door te voeren.

EDCA-AP Parameters

Access Point parameters voor Enhanced Distributed Channel Access.

AC-BE	Veld voor het instellen van de Access Point - Best Effort (AC-BE).
AC-BK	Veld voor het instellen van de Access Point - Background (AC-BK).
AC-VI	Veld voor het instellen van minimale delay, voor bijvoorbeeld video streams (AC-VI).
AC-VO	Veld voor het instellen van tijdkritische (jitter gevoelige) data, zoals Voice (AC-VO).
CW min	Veld voor het instellen van de minimum tijd die verstrijkt voordat een herstransmissie gestart wordt (CW min).
CW max	Veld voor het instellen van de maximum tijd die die gewacht wordt voordat een herstransmissie gestart wordt (CW max).
AIFSN	Veld voor het instellen van de Arbitration Inter Frame Spacing Number (AIFSN).
TXOP (b) Limit (usec)	Veld voor het instellen van de Transmit Opportunity Window Per Access Categorie (TXOP). Het window is gespecificeerd in micro seconde en kan voor b en a/g mode worden onderscheiden. Tijdens de duur van het window kan het access point frames uitzenden. Frames die niet in het window passen worden gesplitst. De waarde 0 betekent dat slechts één frame uitgezonden kan worden.
TXOP (a/g) Limit (usec)	Veld voor het instellen van de Transmit Opportunity Window Per Access Categorie (TXOP). Het window is gespecificeerd in micro seconde en kan voor b en a/g mode worden onderscheiden. Tijdens de duur van het window kan het access point frames uitzenden. Frames die niet in het window passen worden gesplitst. De waarde 0 betekent dat slechts één frame uitgezonden kan worden.

- Discard Oldest First** Instelling om de nieuwste dataframes de hoogste prioriteit te geven.
- Apply** Knop om de ingestelde waarden door te voeren.

7.6 Bridging

Op deze pagina kunnen externe access points als bridge aan het Wi-Fi modem gekoppeld worden. Er kunnen vier externe draadloze bridges worden gekoppeld.



Let op

Voorkom bridge loops.



Wireless Bridging Instelling om de draadloze bridge in of uit te schakelen.

Remote Bridges Veld voor het instellen van de MAC adressen van de andere draadloze access points waartussen de bridge wordt opgezet. Deze access points moeten ook als bridge te worden geconfigureerd.

Apply Knop om de ingestelde waarden door te voeren.



VPN

Basic	Gateway	Firewall	Parental Control	Wireless	VPN	Logout
-------	---------	----------	------------------	----------	------------	--------

In dit hoofdstuk worden de VPN instellingen beschreven. De instellingen kunt u onder het menu **VPN** wijzigen.

Informatie over VPN

Internet protocol Security (IPSec) is een gestandaardiseerde manier om VPN's op te zetten. Met IPSec is het mogelijk om op een flexibele manier veilig te communiceren via het publieke internet. IPSec gebruikt een aantal gestandaardiseerde encryptietechnieken die de vertrouwelijkheid en integriteit van gegevens waarborgen en tevens zorgen voor authenticatie op IP niveau. Een VPN tunnel wordt gewoonlijk in twee stappen gerealiseerd. In elke stap wordt een Security Association (SA) contract opgezet. Een SA is een overeenkomst tussen de apparatuur aan weerszijden van de verbinding waarin de beveiligingsinstellingen worden vastgelegd.

Stap 1 in het opzetten van een VPN tunnel betreft het uitwisselen van een sleutel.

Stap 2 is het opzetten van een beveiligde verbinding die de sleutel gebruikt voor encryptie van alle data.

8.1 Basic

Op deze pagina kunnen VPN tunnels worden aangezet.



IPsec Endpoint Instelling van het eindpunt (IP adres) van de IPsec tunnel.

Name Uitlezing van de naam van de tunnel.

Status Uitlezing van de status van de tunnel.

Control Knop om de tunnel aan of uit te zetten.

Configure Knop om de tunnel in te stellen.

Add New Tunnel Knop om een nieuwe VPN tunnel toe te voegen.

8.2 IPsec

Op deze pagina kunnen VPN tunnels worden ingesteld.

VPN

IPsec

This page shows configured IPsec tunnels.

Tunnel: 1

Name:

Enabled: ☒ Disabled

Local endpoint settings

Address group type: IP subnet

Subnet: 192.168.178.0

Mask: 255.255.255.0

Identity type: Automatically use WAN IP address

Identity: 255.255.255

Remote endpoint settings

Address group type: IP subnet

Subnet: 0.0.0.0

Mask: 255.255.255.0

Identity type: Automatically use remote endpoint IP address

Identity: 0.0.0.0

Network address type: IP address

Remote Address: 0.0.0.0

IPsec settings

Pre-shared key: EnterAKKey

Phase 1 CH group: Group 1 (768 bits)

Phase 1 encryption: DES

Phase 1 authentication: MD5

Phase 1 SA lifetime: 28800 seconds

Phase 2 encryption: DES

Phase 2 authentication: MD5

Phase 2 SA lifetime: 3600 seconds

Show Advanced Settings

Apply

Tunnel

Instelling om een VPN tunnel te configureren.

Name

Veld voor het instellen van de naam van de VPN tunnel.

Enable / Disable

Instelling om de VPN tunnel te in of uit te schakelen.

Delete Tunnel	Knop om de geselecteerde VPN tunnel te verwijderen.
Add New Tunnel	Knop om een VPN tunnel toe te voegen.
Apply	Knop om de ingestelde waarden door te voeren.

Local endpoint setting

Address Group Type	<p>Instelling van het adresgroep type dat het bereik van de VPN bepaald binnen het externe netwerk.</p> <ul style="list-style-type: none"> • IP Subnet bepaalt dat het totale LAN subnet onder VPN valt. • ID Adres bepaalt dat een IP adres onder het VPN valt. • IP Adresreeks bepaalt dat meerdere IP adressen in een reeks onder het VPN vallen.
Subnet	Veld voor het instellen van het subnet adres.
Mask	Veld voor het instellen van het subnet masker adres.
Identity Type	<p>Instelling van het identificatietype waarmee het Wi-Fi modem wordt geïdentificeerd:</p> <ul style="list-style-type: none"> • WAN IP adres: het WAN adres van het Wi-Fi modem. • IP adres: IPadres van de LAN poort van het Wi-Fi modem. • FQDN: Fully Qualified Domain Names • E-mail adres: E-mailadres.
Identity	Veld voor het instellen van de waarde van het identity-type.

Remote endpoint setting

Address group type	<p>Instelling van het adresgroep type dat het bereik van de VPN bepaald binnen het externe netwerk.</p> <ul style="list-style-type: none"> • IP Subnet bepaalt dat het totale LAN subnet onder VPN valt. • ID Adres bepaalt dat een IP adres onder het VPN valt. • IP Adresreeks bepaalt dat meerdere IP adressen in een reeks onder het VPN vallen.
Subnet	Veld voor het instellen van het subnet adres.
Mask	Veld voor het instellen van het subnet masker adres.
Identity type	<p>Instelling van het identificatietype waarmee het Wi-Fi modem wordt geïdentificeerd.</p> <ul style="list-style-type: none"> • WAN IP adres: het WAN adres van het Wi-Fi modem. • IP adres: IPadres van de LAN poort van het Wi-Fi modem. • FQDN: Fully Qualified Domain Names • E-mail adres: E-mailadres.
Identity	Veld voor het instellen van de waarde van het identity-type.
Network Address Type	<p>Instelling van het adrestype van het externe netwerk.</p> <ul style="list-style-type: none"> • IP adres meestal statisch, publiek adres. • FQDN (Fully Qualified Domain Name), meestal voor dynamische, publieke IP adressen
Remote address	Veld voor het instellen van het FQDN adres van de externe VPN gateway, waarmee het Wi-Fi modem een IPSec VPN gaat opzetten.

IPsec settings

- Pre-shared Key** Veld voor het instellen van een sleutel voor de eerste IKE fase onderhandeling. De sleutel dient bij beide eindpunten bekend te zijn.
- Phase 1 DH Group** Instelling van de Diffie-Hellman sleutelgroep voor de encryptie.
- DH1 - 768-bit random getal
 - DH2 - 1024-bit random getal
 - DH3 - 1536-bit random getal
- Phase 1 Encryption** Instelling van de sleutellengte en encryptie algoritme voor het dataverkeer. Beide eindpunten dienen dezelfde encryptie te gebruiken. Langere sleutels vergen meer rekenkracht van het Wi-Fi modem en kunnen leiden tot tragere verbindingen.
- DES – 56-bit sleutel met DES encryptie
 - 3DES – 168-bit sleutel met DES encryptie
 - AES – 128 bit sleutel per 128 bit datablokken. AES is sneller dan 3DES. Er kan gekozen worden uit 128, 192 en 256 bit AES.
- Phase 1 Authentication** Instelling van het hash algoritme voor de authenticatie van data in IKE SA. SHA1 is sterker dan MD5 maar ook langzamer.
- MD5, message digest 5, genereert een 128-bit digest voor data authenticatie
 - SHA1, secure hash algorithm, genereert een 160-bit digest
- Phase 1 SA Lifetime** Veld voor het instellen van de gebruiksduur (tussen 120 en 86400 seconden) van een IKE SA. Indien de gebruikduur verstrijkt, wordt automatisch een nieuwe sleutel overeengekomen. Een korte gebruiksduur verhoogt de veiligheid. Het nadeel van een korte gebruiksduur is dat er vaker een nieuwe sleutel moet worden overeengekomen, waardoor de VPN verbindingen tijdelijk worden verbroken.

**Phase 1
Encryption**

Instelling van de sleutellengte en encryptie algoritme voor de datacommunicatie.

- Null, geen encryptie in IPSec SA. Niet aanbevolen
- DES, een 56-bit sleutel met DES encryptie
- 3DES, een 168-bit sleutel met DES encryptie. Modem-router en IPSec eindpunt dienen hetzelfde algoritme en sleutel te gebruiken. Hoe langer de sleutel hoe meer rekenkracht van de Wi-Fi modem wordt geleverd, hetgeen resulteert in vertraagde communicatie en verminderde doorvoer van data.
- AES, Advanced Encryption Standard is een nieuwere methode van data encryptie die ook een geheime sleutel gebruikt. AES is sneller dan 3DES. Er kan worden gekozen uit AES-128, AES-192 en AES-256 (bit sleutellengte).

**Phase 2
Authentication**

Zie Phase 1 Authentication

**Phase 2 SA
Lifetime**

Zie Phase 1 SA Lifetime

**Show Advanced
Settings**

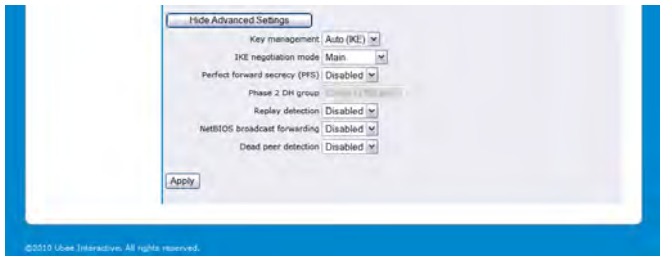
Knop om de geavanceerde instellingen te tonen. De standaard waarden zijn meestal correct.

Apply

Knop om de ingestelde waarden door te voeren.

8.2.1 IPsec Advanced Settings

Wanneer u op de knop **Show Advanced Settings** geklikt heeft, ziet u onderstaande pagina verschijnen. Op deze pagina staan de geavanceerde instellingen van IPsec.



Key Management

Instelling om een VPN verbinding op te zetten (automatisch of handmatig).

IKE Negotiation Mode

Instelling via welke methode de SA tot stand komt voor elke connectie met IKE.

- **Main Mode** hoogste beveiligingsniveau tijdens de authenticatie (fase 1)
- **Aggressive Mode** sneller dan Main mode, omdat diverse stappen worden overgeslagen tijdens de authenticatie (fase 1)

Perfect Forward Secrecy (PFS)

Instelling om PFS in te schakelen (DH1, DH2 of DH5).

Perfect Forward Secret (PFS) is standaard uitgeschakeld in fase 2 van de IPsec setup. Hierdoor wordt de setup sneller, maar minder veilig.

Phase 2 DH Group

Instelling van de DH group.

Replay Detection

Instelling om Replay Detection in of uit te schakelen.

De IPsec ontvanger kan oude of gedupliceerde pakketten detecteren en blokkeren ter bescherming tegen replay aanvallen

**NetBIOS
broadcast
forwarding**

Instelling om NetBIOS pakketdoorgave via de VPN verbinding in of uit te schakelen. NetBIOS pakketten zijn TCP of UDP pakketten waarmee een computer andere computers kan vinden. Wanneer NetBIOS pakketten worden doorgegeven via de VPN kunnen computers in het remote netwerk worden gevonden.

**Dead Peer
Detection**

Instelling om Dead Peer Detection in of uit te schakelen. Wanneer Dead Peer Detection wordt ingeschakeld wordt gedetecteerd of de IPSec gateway nog beschikbaar is.

Apply

Knop om de ingestelde waarden door te voeren.

8.3 Event Log

Op deze pagina staat een logboek van de VPN events.



Time

Uitlezing van het tijdstip van het event.

Description

Uitlezing van informatie over het event.

Refresh

Knop om de pagina te verversen, zodat de laatste events zichtbaar worden.

Clear

Knop om het logboek leeg te maken.



Overzicht van LED lampjes

In onderstaande tabel vindt u mogelijke weergaven van de LED lampjes op het Wi-Fi modem.

Position	LED 1	LED 2	LED 3	LED 4	LED 5	LED 6	LED 7	LED 8	LED 9	LED 10	LED 11	LED 12	LED 13
Kleuren	Groen	Groen/Blauw				Groen	Groen	Groen	Groen	Groen	Groen/Blauw	Groen/Blauw	Groen
Label	RTR	LAN4	LAN3	LAN2	LAN1	WPS	WLAN	TEL2	TEL1	RDY	US	DS	PWR
Status:													
Power ON	Aan	Aan				Uit	Aan		Aan	Aan	Aan	Aan	Aan
Zelf test	Uit	De kleuren van de lampjes staan in relatie met de snelheid; blauw = gigabit; groen = snel Ethernet.				Uit	Uit		Uit	Uit	Uit	Uit	Knip-peren
Initialiseren Ethernet switch	Uit	Aan				Uit	Uit		Uit	Knip-peren	Knip-peren	Knip-peren	Uit
Initialiseren WLAN	Uit	De kleuren van de lampjes staan in relatie met de snelheid				Uit	Aan	Uit		Knip-peren	Knip-peren	Knip-peren	Aan
Initialiseren Router	Aan, in RTR modus	De kleuren van de lampjes staan in relatie met de snelheid				Uit	Aan	Uit		Knip-peren	Knip-peren	Knip-peren	Aan
Downstream zoeken	Aan, in RTR modus	De kleuren van de lampjes staan in relatie met de snelheid				Uit	Aan	Uit		Uit	Uit	Knip-peren	Aan
Downstream vergrendeld	Aan, in RTR modus	De kleuren van de lampjes staan in relatie met de snelheid				Uit	Aan	Uit		Uit	Uit	Aan	Aan
Upstream variatie	Aan, in RTR modus	De kleuren van de lampjes staan in relatie met de snelheid				Uit	Aan	Uit		Uit	Knip-peren	Aan	Aan
Registratie	Aan, in RTR modus	De kleuren van de lampjes staan in relatie met de snelheid				Uit	Aan	Uit		Knip-peren	Aan	Aan	Aan
Registratie OK verbinding met netwerk ingeschakeld	Aan, in RTR modus	De kleuren van de lampjes staan in relatie met de snelheid				Uit	Aan	Uit		Aan	Aan (blauw)	Aan (groen)	Aan
Registratie OK verbinding met netwerk uitgeschakeld	Aan, in RTR modus	De kleuren van de lampjes staan in relatie met de snelheid				Uit	Aan	Uit		Uit	Aan (blauw)	Aan (groen)	Aan

Position	LED 1	LED 2	LED 3	LED 4	LED 5	LED 6	LED 7	LED 8	LED 9	LED 10	LED 11	LED 12	LED 13
Router provisioning	Knippen	De kleuren van de lampjes staan in relatie met de snelheid				Uit	Aan	Uit		Uit	Aan (blauw)	Aan (groen)	Aan
Koppelen apparaat via WPS	Aan, in RTR modus	De kleuren van de lampjes staan in relatie met de snelheid				Knipperend tijdens WPS interval	Aan	Uit		Aan	Aan (blauw)	Aan (groen)	Aan
VoIP registratie	Aan, in RTR modus	De kleuren van de lampjes staan in relatie met de snelheid				Uit	Aan / strobe on link activity	Knipperen		Aan	Aan (blauw)	Aan (groen)	Aan
VoIP geregistreerd	Aan, in RTR modus	De kleuren van de lampjes staan in relatie met de snelheid				Uit	Aan / strobe on link activity	Aan		Aan	Aan (blauw)	Aan (groen)	Aan
VoIP off-hook	Aan, in RTR modus	De kleuren van de lampjes staan in relatie met de snelheid				Uit	Aan / strobe on link activity	Knipperen		Aan	Aan (blauw)	Aan (groen)	Aan
Normaal in bedrijf	Aan					Uit	Aan	Uit	Aan*	Aan	Aan	Aan	Aan

*= afhankelijk van abonnement

Ondanks alle aan deze handleiding bestede zorg kan Ziggo geen aansprakelijkheid aanvaarden voor schade die het gevolg is van enige onvolkomenheid of fout in deze uitgave. De handleiding is uitdrukkelijk niet bedoeld ter nadere invulling of toelichting op de algemene voorwaarden. Derhalve kunnen er geen rechten aan ontleend worden.

© Copyright 2011, Ziggo B.V.

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, en/of openbaar gemaakt in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen, of enige andere manier, zonder voorafgaande schriftelijke toestemming van Ziggo.



AZIP.GHI.1104

Versie 1.0

april 2011