Eicon Diva 2440
Direct IP^{TM}
ADSL router for unlimited VPN

- Executive Summary
- Diva 2440 ADSL Router in general
- Introduction public / private IP
- When to use Direct IP^{TM}
- Direct IP^{TM} technical background
- How to use Eicon Direct IP^{TM} on a Diva 2440

Executive Summary

Most IPSec VPN/Firewall implementations need 100% transparent Internet connections using a public IP address. In order to achieve such a connection legacy routers require special Internet services that include a range of routable IP addresses (public subnet). For several reasons end-users would like to be able to use a combination of a service and router which only requires a single IP address per connection while maintaining application compatibility. Eicon Networks recognized this demand as a challenge and developed a new product that introduces the intelligent Direct IP^{TM} feature that saves IP addresses and overcomes NAT problems at the same time. From now on any Firewall or VPN router can be used on ADSL services that provide just a single IP address using an Eicon Diva 2440 Direct IP^{TM} router.

Diva 2440 ADSL router in general

The Diva 2440 ADSL router is the ideal Connect & Surf^{TM} Internet Access device to share a connection with a number of PC's or servers. Simplicity is assured and support requirements reduced. Connect & Surf^{TM} technology automatically detects ADSL service parameters. Built-in PPPoE and PPPoA Internet connectivity guarantees a full automatic always on connection and eliminates the need to run software on a server-like PC. Offering support for IP over ATM and Ethernet over ATM as well makes it a product that can really be used on almost any implementation of any ISP (preferably providing fixed IP addresses).

The Diva 2440 ADSL router can operate in two modes depending on the application used. In the normal mode a standard ADSL service can be shared by up to 254 concurrent users. The Diva 2440 built-in Firewall meets the requirements of SOHO environments to protect a network from the outside world while maintaining the flexibility to run specific applications. The built-in DHCP server automatically assigns IP addresses to all PC's. In the normal mode, NAT allows multiple PC's to share a single routable public IP address while keeping them invisible to hackers on the Internet. Connect the Diva 2440 to an Ethernet hub or switch and it becomes a spectacular Internet sharing machine. The built-in VMDZ support makes it possible to obtain a range of Public IP addresses from the ISP automatically (when the ISP provides this service) which then can be distributed on the LAN together with Private IP addresses.

NAT-less Direct IP^{TM} mode guarantees compatibility with every network capable application including IPsec VPN's and Firewalls. Using a Diva 2440 in combination with any well known Firewall makes it the ideal transparent Internet sharing VPN and Firewall bridge.

Introduction public / private IP

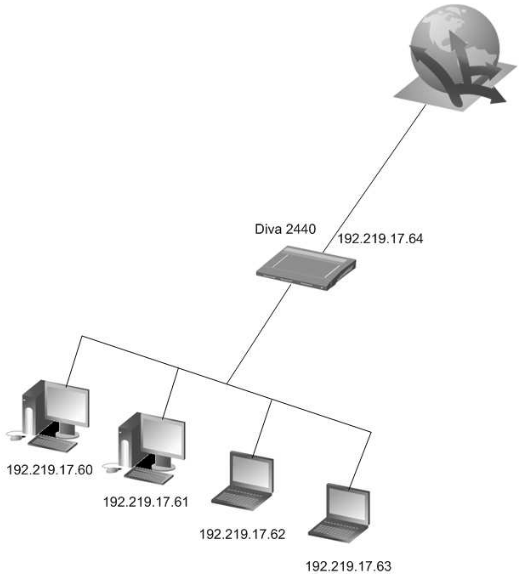
Simply put, "public" IP addresses can be routed across the Internet, and "private" IP addresses cannot be routed across the Internet. The IP address that the ISP provides is a public address. They are unique throughout the Internet, and are accessible from any other user on the Internet.

The Internet community has reserved certain IP address blocks for use in private networks, and the entire 192.168.0.0 network is one of those reserved blocks. If you are using Network Address Translation (NAT), e.g. the 192.168.1.x addresses that a normal DSL router assigns to your client PCs are private addresses, and these addresses cannot be routed across the Internet. In order to give devices with private IP addresses access to the Internet, the private IP address will be translated by the router into the correct public router network address. This means that the devices behind NAT won't be visible using their own IP address but they

will only be visible and reachable via the router network address. But most Firewalls and VPN routers simply require a public IP address without NAT in order to make themselves accessible to the Internet.

When to use Direct IP™

Effectively we know two types of connection services to the Internet from an IP point of view. We know services with a range of public IP address (subnet range) and services with a single public IP address.

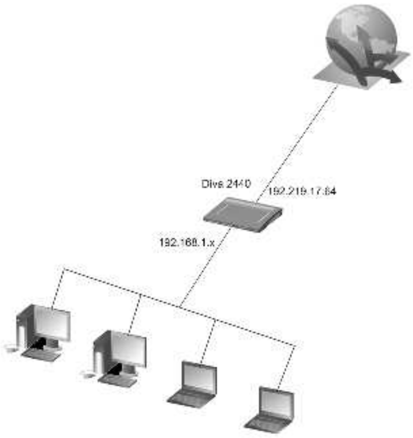


Services that provide a range of public IP addresses in principal work fine with a normal router like a Diva 2440. Each device will have it's own public IP address from within the public range like displayed in above drawing. However the scenario above makes inefficient use of valuable public IP addresses. Even small public IP subnets will lose 3 IP addresses because of overhead (router, broadcast and subnet identifier). ISP's most often provide 8 IP addresses by default although branch offices effectively only use one IP address, this of course results in an inefficient usage of IP addresses.

Direct IP™ overcomes this inefficiency and optimizes the usage of IP addresses to the max. This is important since the availability of IP addresses is limited, ISP's really need to defend their own usage and provisioning of IP addresses towards RIPE (RIPE is the European registry that is responsible for the fair allocation of IP address space). So it's also in the ISP's interest to use as few addresses as possible and that's why any ISP prefers to provide services with just a single IP address whenever possible. End-users who require a bigger range of IP addresses need to justify this need. Details about Network designs have to be provided and a lot of administration and bureaucracy is involved. The ideal solution for anybody would just be to overcome the need of a full subnet.

NOTE: Direct IP™ could be called "IP Unnumbered" or such a 2440 Direct IP™ device could be called a "netless device". There has been seen a similar feature called "PPP bridging", but we are not sure whether the "PPP bridging" feature is as powerful as Direct IP™.

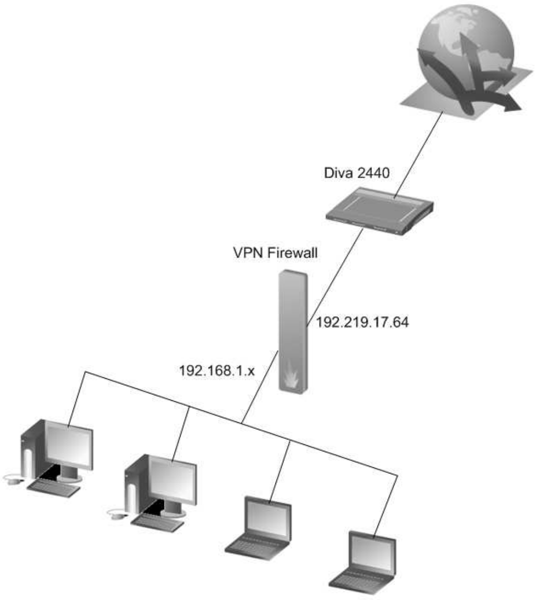
A Firewall or VPN server could be considered as an Internet appliance. Simply put each real Internet appliance requires a public IP address. In order to save the number of used IP addresses, NAT is often used since all connected devices will share the same service with the same IP address. This means per definition that any device behind NAT will have a private IP address because the NAT router will alter the IP packets in a way that all PC's will share the same routable public IP address. That's why the scenario below is causing problems for NAT unfriendly applications.



The altering described on the previous page changes the IP addressing of the IP packet in a way which makes it incompatible with many applications including most Firewall and VPN solutions. That's why most IPsec and Firewall solutions simply demand a dedicated public routable IP address. For this reason NAT is unacceptable between the Internet and the IPsec Firewall. More about this subject can be read on: http://www.networkcomputing.com/1123/1123ws2.html

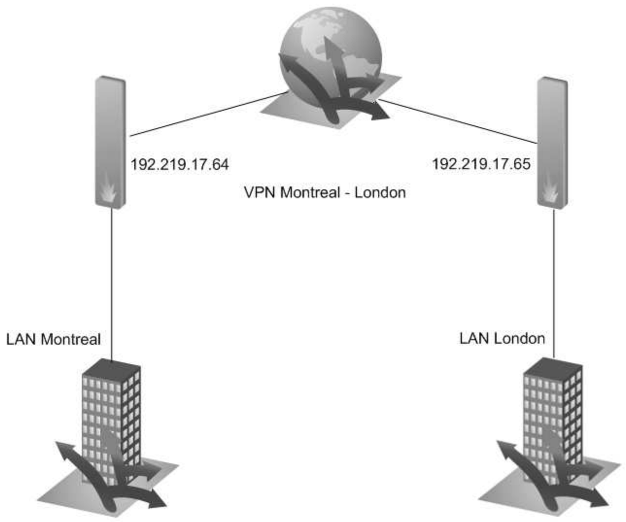
Direct IP™ technical background

You'll find a drawing of Eicon's Direct IP™ solution below that - when desired - eliminates NAT. The VPN Firewall will be connected to the Internet using a Diva 2440 ADSL router. The router will obtain a single IP address from the Internet. Normal NAT routers will use this IP address themselves but Eicon's Direct IP™ mode will now ensure that this single public IP address can be made available to e.g. the IPsec server itself (without NAT!). Effectively the Diva 2440 is behaving like a unique bridging router like shown in the below drawing. Please note that the VPN Firewall uses the public IP address and the Diva 2440 doesn't consume any public IP address.



The router behaves like a real bridge and will therefore virtually not exist, that's why we can remove the Diva 2440 from the drawing from an IP point of view and that's why the VPN Firewall can use the public IP address. If you expand the above network with a remote location, then the diagram below would apply. As you can see the VPN Firewall's in both Montreal and London are directly connected to the Internet. Although the Diva 2440

ADSL Router is connected between the Firewall and the Internet has virtually disappeared and is not visible from an IP point of view.



The VPN network on the previous drawing can be expanded without any problems. The Diva 2440 architecture is designed in a way that it will support Direct IP^TM bridging on any ADSL network.

Direct IP^TM is compatible with almost any service provider implementation based on:

- PPP over ATM (RFC 2364)
- PPP over Ethernet (RFC 2516)
- IP over ATM (RFC 1483R)

NOTE: The support of “Ethernet over ATM” can be added at a later time if needed.

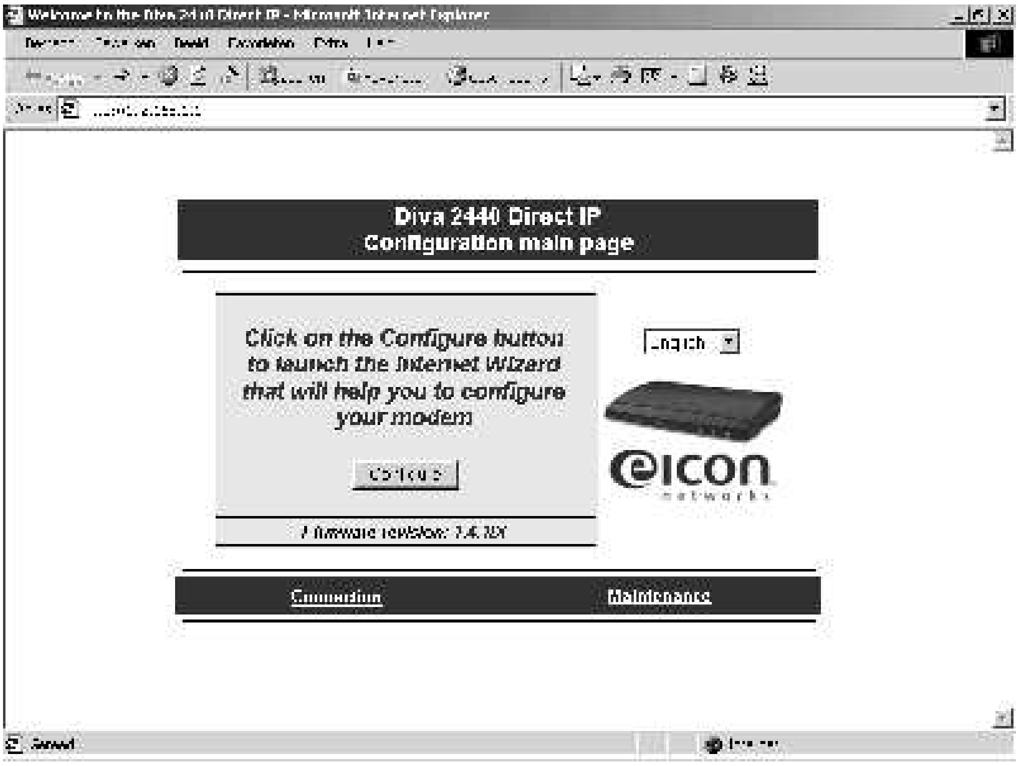
How to use Eicon Direct IP^TM on a Diva 2440

Power on the Diva 2440, connect the PC using the yellow cross cable connect the the ADSL using the grey cable. By default the 2440 will operate as DHCP server, we recommend to use DHCP. Using a static IP configuration on the PC is not recommended at this stage. Therefore please make sure your own PC will operate as DHCP client, for more information please visit:
http://www.eicon.com/support/helpweb/adsl/DHCP_client.asp

After you’ve verified that your PC will obtain it’s IP settings automatically please release and renew the IP addresses of the PC or reboot the PC. Now the PC will use the IP settings obtained from the Diva 2440. Use any WEB-browser to visit the built-in WEB server of the Diva 2440 using the Diva’s IP address:
http://192.168.1.1

After you have obtained access to the WEB-interface you should check the firmware version of the Diva 2440. The supported firmware should be labeled Diva 2440 1.4.1DI (or a newer version which supports Direct IP^TM when applicable). If you have installed any other firmware older then 1.4.1 or without the ‘DI’-label please visit our software download area of the Eicon Helpweb and update the firmware:
http://www.eicon.com/support/helpweb/software.asp

After you've verified that the correct Firmware is installed (e.g. 1.4.1DI), please select 'configure'. Then you can choose Autodetect Settings. Doing this will start a wizard which tries to find the correct network parameters of the ADSL network.



Welcome to the Diva 2440 Direct IP - Microsoft Internet Explorer

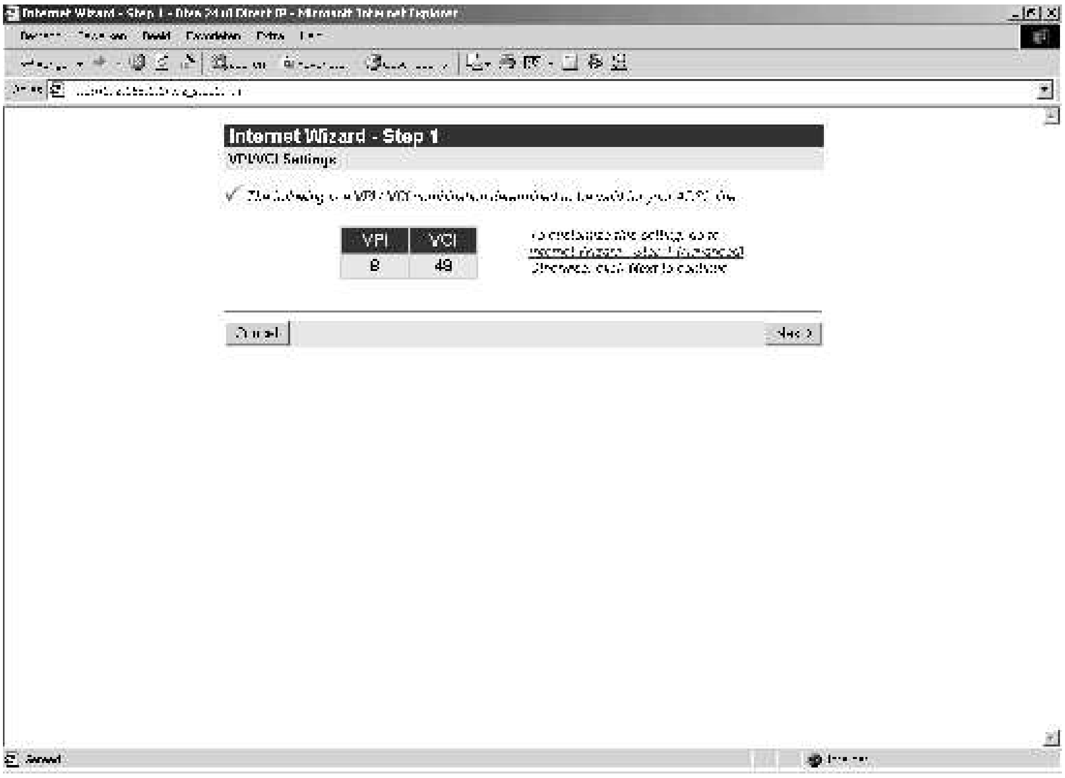
Diva 2440 Direct IP
Configuration main page

Click on the Configure button to launch the Internet Wizard that will help you to configure your modem

Configure
English
eicon networks

Firmware revision: 1.4.1DI

Accept the settings suggested by the Diva 2440 like similar displayed below.



Internet Wizard - Step 1 - Diva 2440 Direct IP - Microsoft Internet Explorer

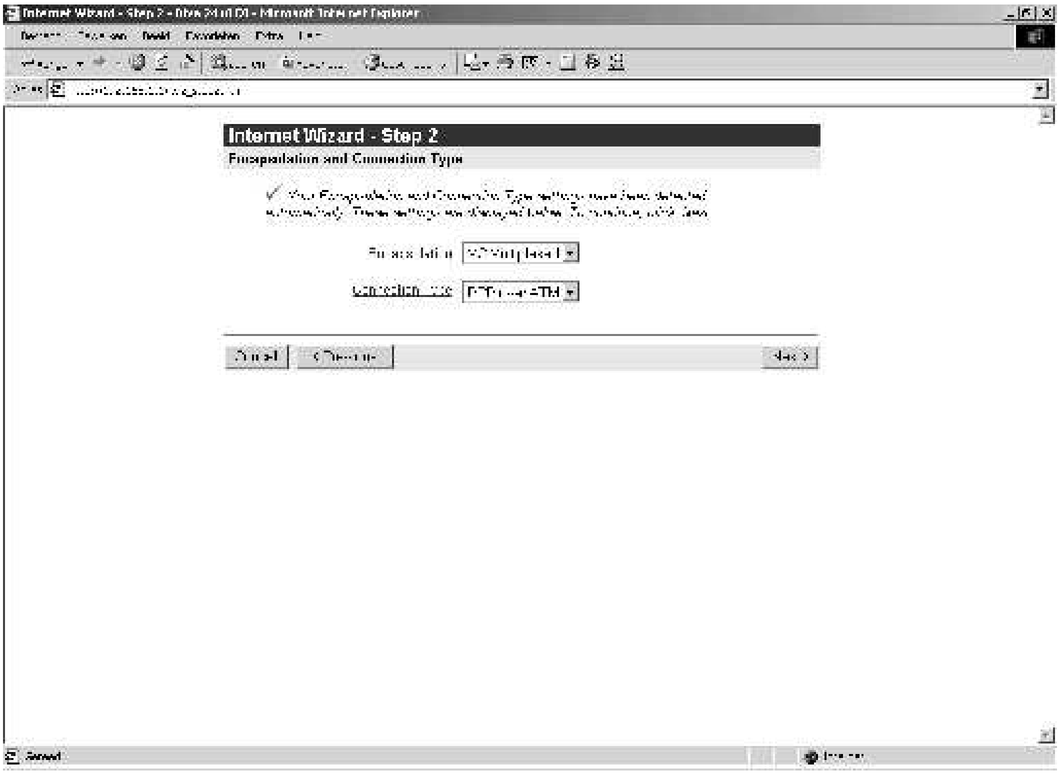
Internet Wizard - Step 1

VPI/VCI Settings

✓ The following VPI / VCI combination was determined to be valid for your ADSL line.

VPI	VCI
8	48

To customize the settings go to Internet Wizard - select [Advanced]
Otherwise, click Next to continue



Internet Wizard - Step 2

Encapsulation and Connection Type

✓ [illegible]

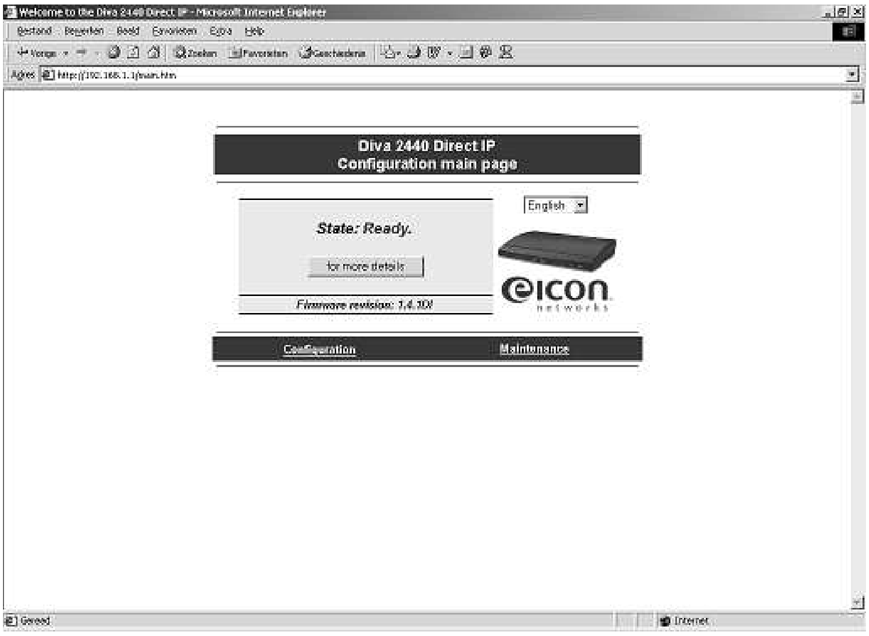
Encapsulation: VC Multiplexed

Connection type: PPP over ATM

Depending on the network used, some parameters might not be detected automatically. If this happens in your case, then please choose between the given options (if any) or go back and choose ‘Select a Service Provider’ manually. If your service provider is not listed, please configure the correct parameters manually. In the Netherlands you should select ‘KPN’ for KPN ADSL (MXSTREAM) or in Belgium ‘Turboline 2’ for ADSL Office.

Depending on the network used the required parameters might differ. Using KPN in the Netherlands you need to configure the user-name and password for the service, where in Belgium the required custom specific IP settings have to be entered. What kind of ADSL service is available in your your own region can be found via: http://www.eicon.com/support/helpweb/adsl/adsl_settings.asp

After you’ve completed the wizard click ‘Finish’ and the router will set-up a connection. As soon as the connection is established the WEB-interface should state ‘Ready’.



Welcome to the Diva 2440 Direct IP - Microsoft Internet Explorer

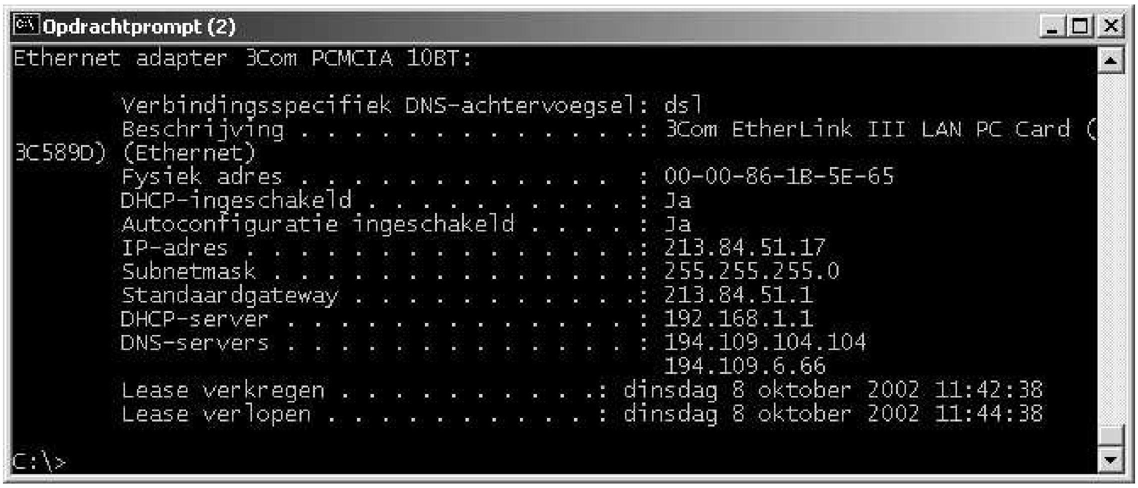
Adres: http://192.168.1.1/main.htm

Diva 2440 Direct IP
Configuration main page

State: Ready.

Firmware revision: 1.4.10!

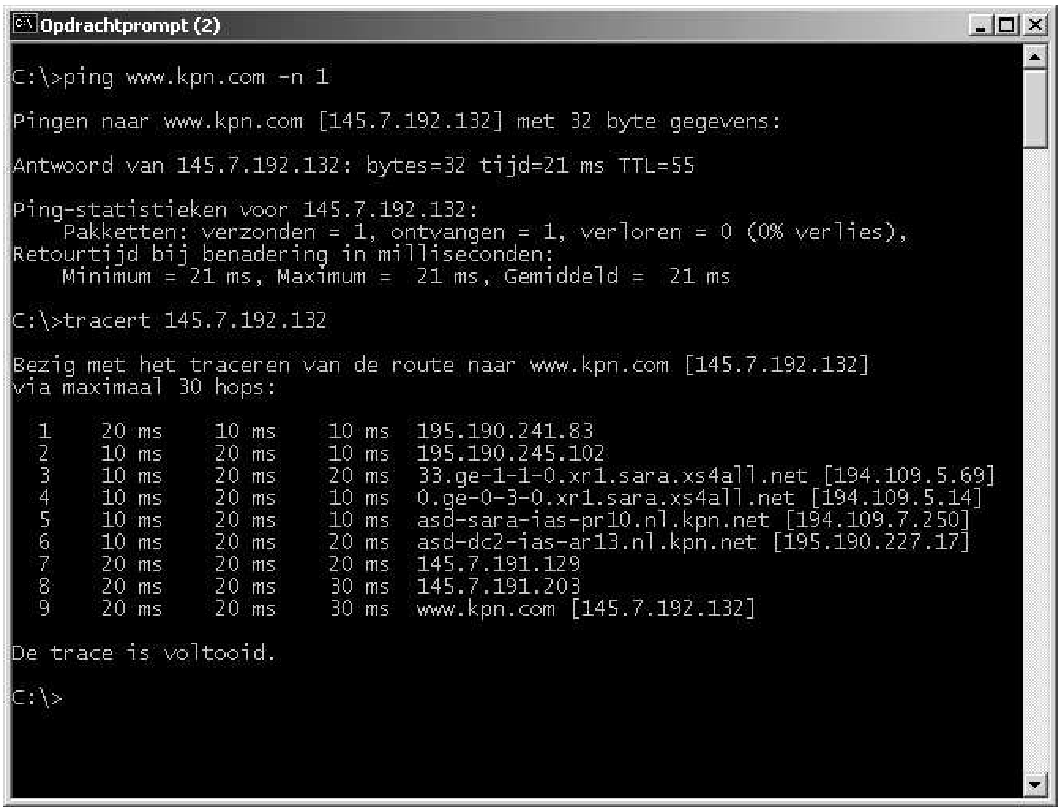
Now reboot your PC again or release and renew the IP settings of the PC. Your PC will obtain the new (public) IP settings from the Diva 2440. In our example the IP addresses are shown below.



```
Ethernet adapter 3Com PCMCIA 10BT:

        Verbindingsspecifiek DNS-achtervoegsel: dsl
        Beschrijving . . . . . . . . . . . . . .: 3Com EtherLink III LAN PC Card (
3C589D) (Ethernet)
        Fysiek adres . . . . . . . . . . . . . : 00-00-86-1B-5E-65
        DHCP-ingeschakeld . . . . . . . . . . . : Ja
        Autoconfiguratie ingeschakeld . . . . : Ja
        IP-adres . . . . . . . . . . . . . . .: 213.84.51.17
        Subnetmask . . . . . . . . . . . . . .: 255.255.255.0
        Standaardgateway . . . . . . . . . . .: 213.84.51.1
        DHCP-server . . . . . . . . . . . . . : 192.168.1.1
        DNS-servers . . . . . . . . . . . . . : 194.109.104.104
                                                194.109.6.66
        Lease verkregen . . . . . . . . . . .: dinsdag 8 oktober 2002 11:42:38
        Lease verlopen . . . . . . . . . . . : dinsdag 8 oktober 2002 11:44:38

C:\>
```

The IP settings obtained by the PC have to be used on the device (VPN server or Firewall) which you prefer to connect to the Internet. This can either be done via static or dynamic configuration. Depending on the obtained IP address, the Diva 2440 will investigate what (Virtual) Default Gateway IP address should be used on the LAN side. If you prefer to connect a device via static IP addresses it is important to note the above IP settings. In any case it makes sense to verify the IP settings obtained by the PC and please note for future reference.

Obtained IP address	
Subnet Mask	
Virtual Default Gateway	
DNS1	
DNS2	
User name ADSL service (PPPoA and PPPoE only)	
Password ADSL service (PPPoA and PPPoE only)	

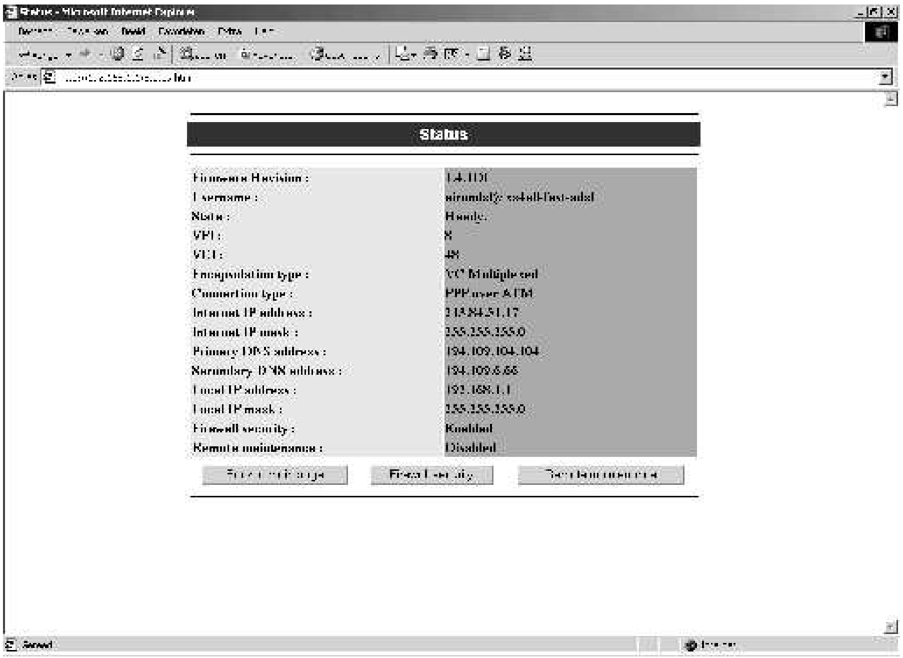


```
C:\>ping www.kpn.com -n 1

Pingen naar www.kpn.com [145.7.192.132] met 32 byte gegevens:

Antwoord van 145.7.192.132: bytes=32 tijd=21 ms TTL=55

Ping-statistieken voor 145.7.192.132:
    Pakketten: verzonden = 1, ontvangen = 1, verloren = 0 (0% verlies),
Retourtijd bij benadering in milliseconden:
    Minimum = 21 ms, Maximum =  21 ms, Gemiddeld =  21 ms

C:\>tracert 145.7.192.132

Bezig met het traceren van de route naar www.kpn.com [145.7.192.132]
via maximaal 30 hops:

  1    20 ms    10 ms    10 ms  195.190.241.83
  2    10 ms    20 ms    10 ms  195.190.245.102
  3    10 ms    20 ms    20 ms  33.ge-1-1-0.xr1.sara.xs4all.net [194.109.5.69]
  4    10 ms    20 ms    10 ms  0.ge-0-3-0.xr1.sara.xs4all.net [194.109.5.14]
  5    10 ms    20 ms    10 ms  asd-sara-ias-pr10.nl.kpn.net [194.109.7.250]
  6    10 ms    20 ms    20 ms  asd-dc2-ias-ar13.nl.kpn.net [195.190.227.17]
  7    20 ms    20 ms    20 ms  145.7.191.129
  8    20 ms    20 ms    30 ms  145.7.191.203
  9    20 ms    20 ms    30 ms  www.kpn.com [145.7.192.132]

De trace is voltooid.

C:\>
```

While tracing the route to a public IP address you can verify yourself that the PC is connected directly to the Internet. In our example you'll see in the above diagram that the first hop is a public IP address and this proofs that there is no Network Address Translation (using a standard KPN ADSL service based on PPPoA).

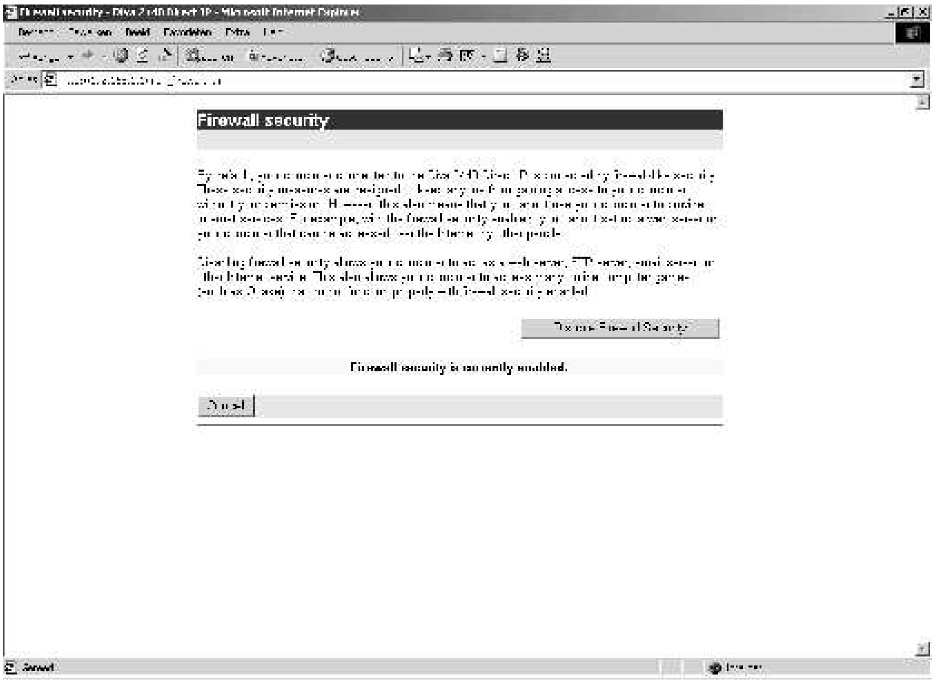
Please note: Although your PC uses a public IP address, you can still access the Diva 2440 via a private IP address 192.168.1.1 (accessible from the LAN only).

For security reasons the Diva 2440 will apply a Firewall Security mechanism by default. Most 'server' applications however require a full transparent connection. If you prefer to rely on the security capabilities of an external Firewall or prefer to have a fully transparent connection the security mechanism should be disabled. In order to do so you select from the main screen of the 2440 'Fore more information'.



Status

Firmware Revision :	1.4.1D1
Username :	[illegible]@xs4all-fast-adsl
State :	Ready
VPI :	8
VCI :	48
Encapsulation type :	VC Multiplexed
Connection type :	PPP over ATM
Internet IP address :	213.84.51.17
Internet IP mask :	255.255.255.0
Primary DNS address :	194.109.104.104
Secondary DNS address :	194.109.6.66
Local IP address :	192.168.1.1
Local IP mask :	255.255.255.0
Firewall security :	Enabled
Remote maintenance :	Disabled



Firewall security - Diva 2440 Direct IP - Microsoft Internet Explorer

Firewall security

[illegible]

[illegible]

Firewall security is currently enabled.

Select ‘Firewall Security’ and then click on ‘Disable Firewall Security’. The 2440 build-in Firewall will be disabled immediately. The configuration of the 2440 is automatically saved. In case a power-outage occurs, the Diva 2440 will re-establish the connection immediately using the saved configuration. Now you can connect any IPsec VPN Router or Firewall using the IP settings that you’ve just written down.