Allied Data

TECHNOLOGIES

Installation Manual

CopperJet 16xx series

Based on firmware 6.10

June 2006

Document History

Date	Version	Status	Description
02 June 2006	1.0	Final	Updated to firmware 6.10

Product DISCLAIMER

This manual by ALLIED DATA TECHNOLOGIES B.V. (hereafter referred to as ALLIED DATA TECHNOLOGIES) is a reflection of the current state of the products described in it.

It has been our goal to provide a manual that is complete and clear to ensure that our products are as easy to use. However, this manual may contain technical inaccuracies and typing errors. As a result of rapid developments, we are also obliged to reserve the right to implement technical modifications and developments without prior notice. For this reason, ALLIED DATA TECHNOLOGIES does not guarantee the contents of the manual and its permanent applicability.

Neither is ALLIED DATA TECHNOLOGIES liable for possible loss of information or any improper use of information resulting from the consultation of this manual. In particular, ALLIED DATA TECHNOLOGIES is not liable for any direct or indirect damage (including loss of profits and comparable losses) resulting from the use or improper use of this manual, even if ALLIED DATA TECHNOLOGIES or a representative of ALLIED DATA TECHNOLOGIES has been informed that such damage could arise. Of course, this does not detract us from our legal liability for intentionally inflicted damage or damage on the basis of gross negligence.

In relation to the information mentioned in this manual, ALLIED DATA TECHNOLOGIES does not guarantee that there are no industrial rights of ownership (trademarks, patents, etc.). This also applies to commonly used brand names, company names and product names, but these are subject to the relevant trademark, patent and registered design laws.

The information is not to be copied, translated, reproduced or transferred or stored on any electronic medium or other machine, neither wholly nor partly, without prior permission in writing from ALLIED DATA TECHNOLOGIES.

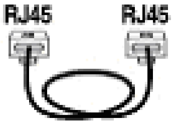
The sale and use of software is subject to the ALLIED DATA TECHNOLOGIES General Terms of Delivery and Payment as well as its License Terms.

Should any term regarding the disclaimer be or become void for legal reasons, this will not affect the other terms.

Contents

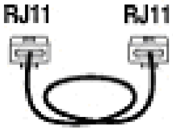
1 Packaging contents

The packaging should contain the following parts:



Ethernet RJ45
Straight or Cross
cable

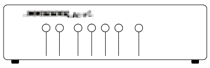
+



RJ11 cable

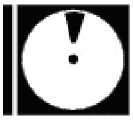
+

USB cable



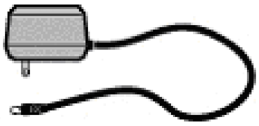
CopperJet

+



CD Rom

+



Power Adaptor

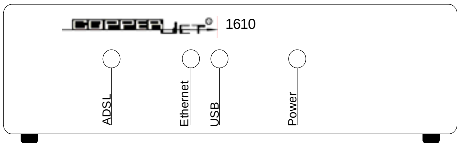
Caution!
To prevent overheating, make sure that the CopperJet has enough free space on both sides and above to permit free airflow.

2 LED Indicators and back panel

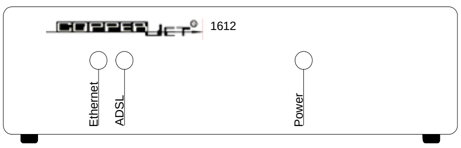
Before you begin with the installation, please take a moment to become more familiar with the LED indicators and back panel of the CopperJet.

2.1 CopperJet 16xx series LED indicators

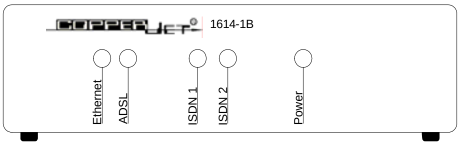
Front panel



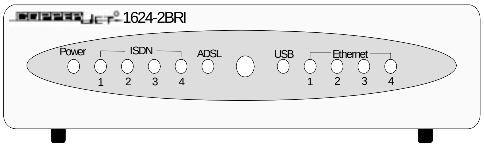
Front panel



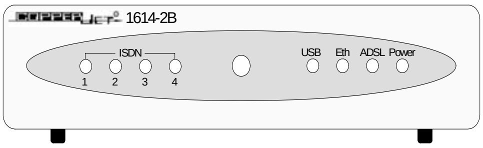
Front panel



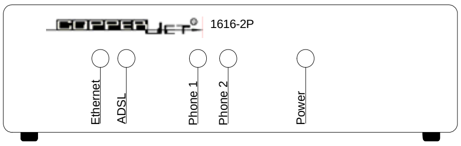
Front panel



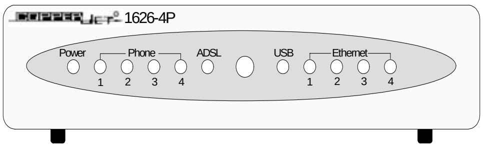
Front panel



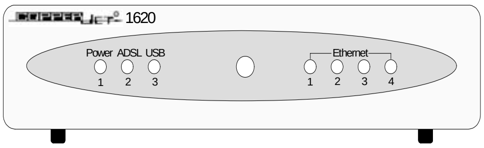
Front panel



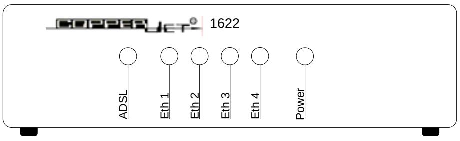
Front panel



Front panel



Front panel



Ethernet/ETH: The Ethernet led will illuminate when you connect the CopperJet to the Ethernet port on the PC or hub/switch.

USB: The USB led will illuminate when you connect the CopperJet to the USB port on the PC.

Phone: To connect the CopperJet to the analogue phone (PSTN).

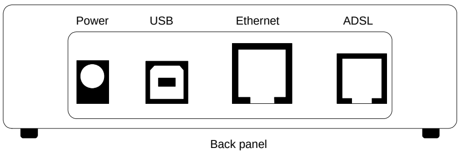
ISDN: To connect the CopperJet to the ISDN phone (BRI).

ADSL: Blinking indicates that the ADSL protocols starts handshaking. Illuminates when the ADSL network is correctly configured and connected.

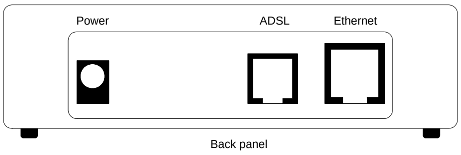
Power: When the CopperJet is connected to a power source, the Power LED will illuminate.

2.2 CopperJet 16xx series back panel

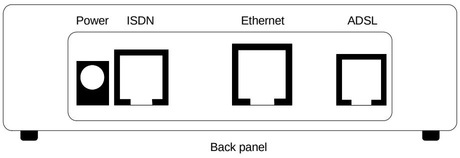
CopperJet 1610



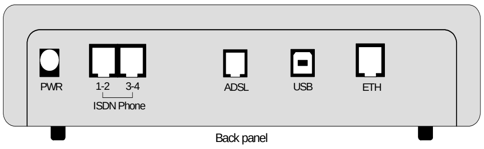
CopperJet 1612



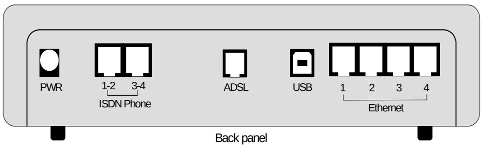
CopperJet 1614-1BRI



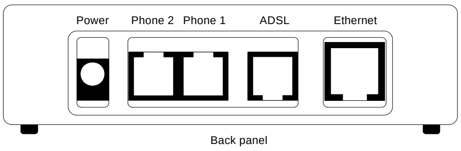
CopperJet 1614-2BRI



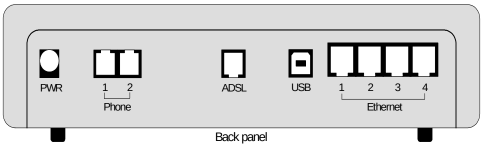
CopperJet 1624-2BRI



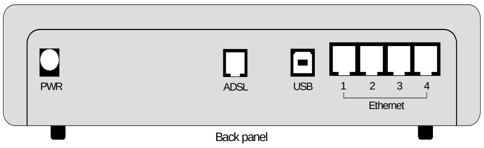
CopperJet 1616



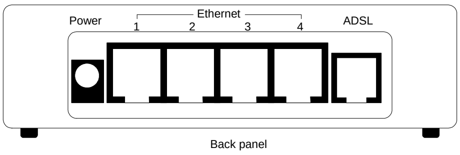
CopperJet 1626



CopperJet 1620



CopperJet 1622



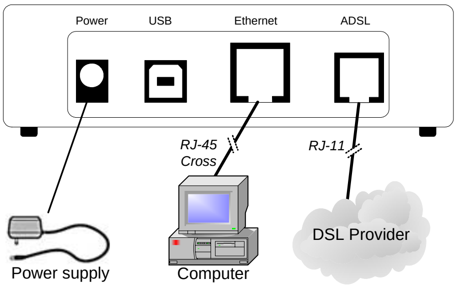
Power:	Only the power adapter that comes with the package can be connected to the power jack.
ADSL:	To connect the CopperJet to the ADSL line of your provider.
Phone:	To connect the CopperJet to the analogue phone (PSTN).
ISDN:	To connect the CopperJet to the ISDN phone (BRI).
USB:	To connect the CopperJet to the USB port of the PC.
Ethernet:	To connect the CopperJet to the Ethernet port of the PC, hub or switch.

3 Connecting the CopperJet

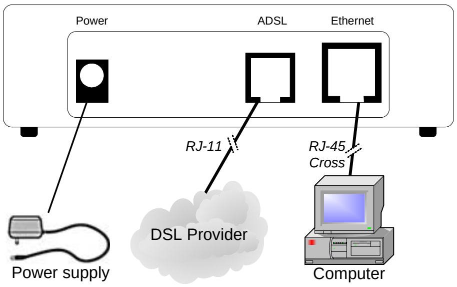
To connect the CopperJet to the computer, you must have installed an Ethernet 10/100Base-T card in your computer. You need to have a static IP address on your network card that is in the same subnet as the web interface IP address of the CopperJet. The default web interface IP address for Ethernet is **172.19.3.1** (USB IP address is **172.20.3.1**). When using the default IP addresses, your network card can have the following IP address 172.19.3.2 with subnetmask 255.255.0.0.

3.1 Connecting the CopperJet 16xx series

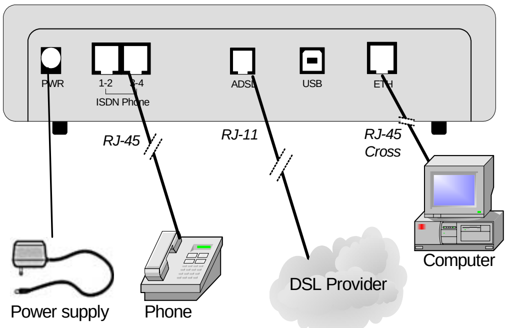
CopperJet 1610



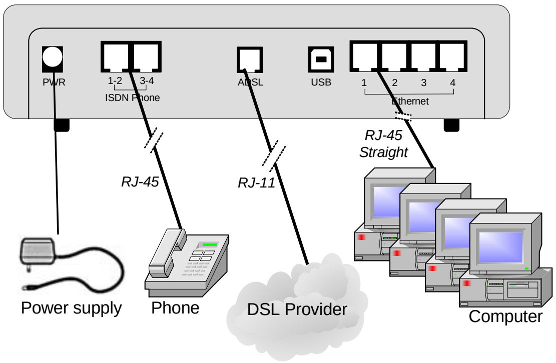
CopperJet 1612



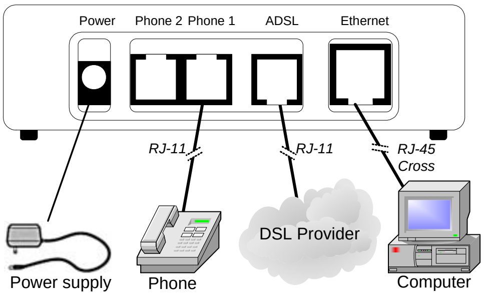
CopperJet 1614



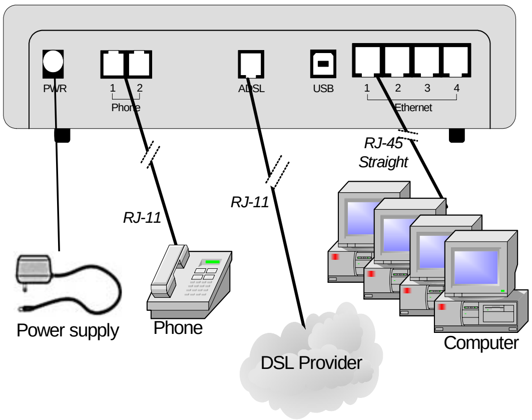
CopperJet 1624



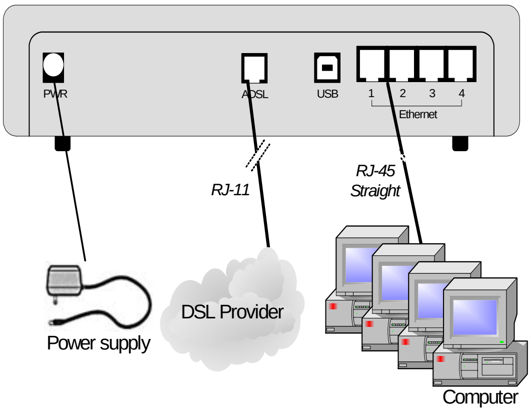
CopperJet 1616



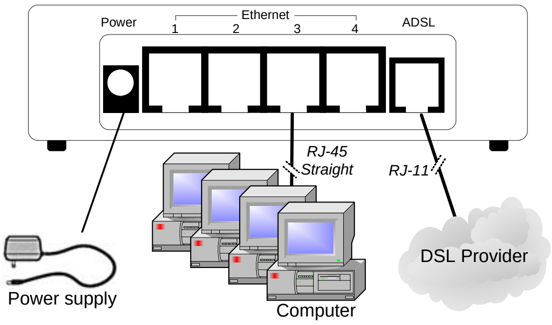
CopperJet 1626



CopperJet 1620



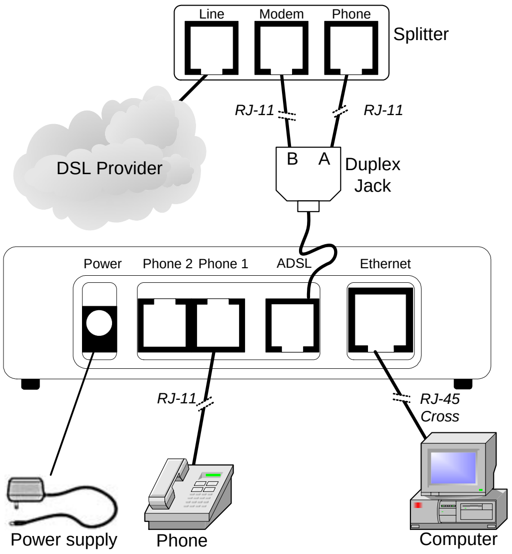
CopperJet 1622



3.2 Connecting the CopperJet 1616/1626 with Active inbound Call Switching (ACS)

Active Inbound Call Switching (ACS) enables the user to have both his traditional Voice line and the VoDSL/VoIP line connected to a single telephone.

See picture below how to connect the CopperJet 1616/1626 for Active Inbound Call Switching.



Note: Active Inbound Call Switching is only possible on Annex A DSL lines with analogue phone ports (POTS FXS). Not for Annex B and ISDN phone ports (BRI).

4 Before you start

The following information may be required for configuring the CopperJet. If you do not know if all the information is needed, please contact your DSL service provider before proceding with the configuration.

4.1 IP Address Settings

The CopperJet allows the ISP to dynamically assign IP Address settings. If your ISP requires static setting of specific IP address information, you need to receive the following information:

- IP Address
- Subnet Mask
- Default Gateway

4.2 Name Server Information

The CopperJet allows the ISP to dynamically assign Name Server Address settings. If your ISP requires static setting of specific DNS address information, you need to receive the following information:

- Primary DNS Address
- Secondary DNS Address

4.3 ATM Settings

The following ATM settings should be available during configuration

- ATM Virtual Path ID (VPI); *Required if not using default value*
- ATM Virtual Circuit ID (VCI); R*equired if not using default value*
- Encapsulation type; *Required if not using default value*
- Modulation type; *Required if not using default value*

4.4 PPP Settings

The following PPP settings should be available during configuration of a PPP connection.

- Username (for PPP applications only)
- Password (for PPP applications only).

4.5 VoATM settings

The following VoATM settings should be available during configuration.

- ATM Virtual Path ID (VPI);
- ATM Virtual Circuit ID (VCI);
- VoDSL Signalling.

4.6 VoIP settings

The following VoIP settings should be available during configuration.

- Signal protocol (SIP or MGCP);
- Send Transport;
- SIP Registrar/Proxy;
- SIP User Domain;
- Endpoint Username;
- Endpoint Password.

5 Configuring the CopperJet

Configuration of the CopperJet ADSL router can be done through the build-in HTTP WebServer. Users can access this WebServer using a standard browser like Netscape Navigator or Microsoft Internet Explorer.

5.1 Accessing the build-in WebServer

To access the build-in WebServer, you need to launch a HTTP Web browser. Enter the IP address of the CopperJet in the address bar.

The default Ethernet IP address of the CopperJet is: **172.19.3.1**
The default USB IP address of the CopperJet is: **172.20.3.1**

The address for accessing the CopperJet's WebServer through an Ethernet connection would be HTTP://172.19.3.1/ and for the USB connection would be HTTP://172.20.3.1/ .

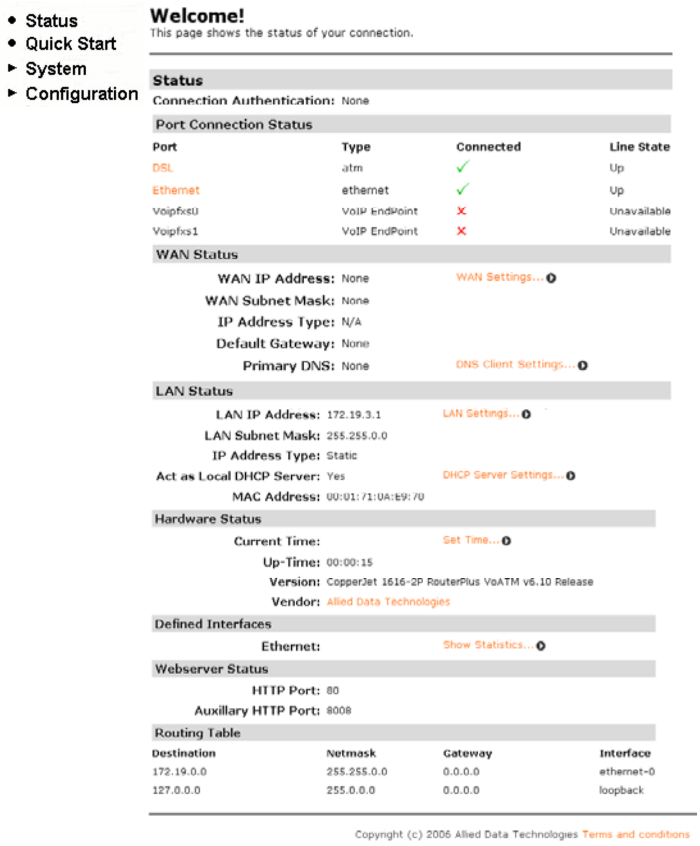
Note: To access the WebServer you need to have an IP address on your network card that is in the same subnet as the CopperJet (Example:172.19.3.2 subnet mask 255.255.0.0). By default the DHCP Server of the CopperJet is enabled, so an IP address will be provided automatically from the CopperJet on the network card.

You will be asked for a Username and Password. Enter your username and password to access the pages. The default network login is:

Username: **admin**
Password: **admin**

Click on *OK*. You can now configure your CopperJet using the WebServer.

The first time that the WebServer is launched during a session, the *Welcome!* message is displayed at the top of the Status homepage. This message is replaced by the Status heading once the page is automatically or manually refreshed.



Welcome!
This page shows the status of your connection.

Status
Connection Authentication: None

Port Connection Status

Port	Type	Connected	Line State
DSL	atm	✓	Up
Ethernet	ethernet	✓	Up
Voipfxs0	VoIP EndPoint	✗	Unavailable
Voipfxs1	VoIP EndPoint	✗	Unavailable

WAN Status
WAN IP Address: None — WAN Settings...
WAN Subnet Mask: None
IP Address Type: N/A
Default Gateway: None
Primary DNS: None — DNS Client Settings...

LAN Status
LAN IP Address: 172.19.3.1 — LAN Settings...
LAN Subnet Mask: 255.255.0.0
IP Address Type: Static
Act as Local DHCP Server: Yes — DHCP Server Settings...
MAC Address: 00:01:71:0A:E9:70

Hardware Status
Current Time: — Set Time...
Up-Time: 00:00:15
Version: CopperJet 1616-2P RouterPlus VoATM v6.10 Release
Vendor: Allied Data Technologies

Defined Interfaces
Ethernet: — Show Statistics...

Webserver Status
HTTP Port: 80
Auxillary HTTP Port: 8008

Routing Table

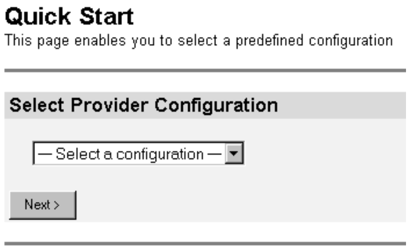
Destination	Netmask	Gateway	Interface
172.19.0.0	255.255.0.0	0.0.0.0	ethernet-0
127.0.0.0	255.0.0.0	0.0.0.0	loopback

Copyright (c) 2006 Allied Data Technologies Terms and conditions

5.2 Quickstart

With the Quickstart option you can configure your CopperJet in only a few steps. The number of steps is depending on the specific ISP network.

To use the Quickstart, click on Quickstart (on the left hand side).
The *Quickstart* page is displayed.



Quick Start

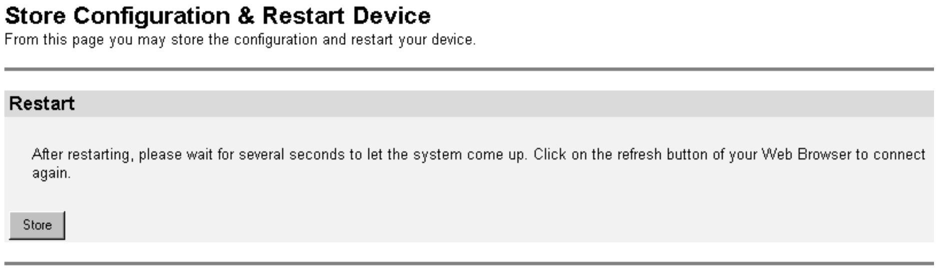
This page enables you to select a predefined configuration

Select Provider Configuration

Select your ISP network from the dropdown-list and click on *Next>*. Some settings may already been pre-configured. This is shown at the top of the page *Pre-defined Settings*.

Depending on the selected network, you may have to enter more information like fill in Username and Password.

If you are finished entering all the information, click on *Next>* and the S*tore Configuration & Restart Device* page is displayed.



Store Configuration & Restart Device

From this page you may store the configuration and restart your device.

Restart

After restarting, please wait for several seconds to let the system come up. Click on the refresh button of your Web Browser to connect again.

Click on *Store*.

The configuration will now be saved into the device and will reboot.
After reboot the CopperJet is correctly configured for your ISP network.

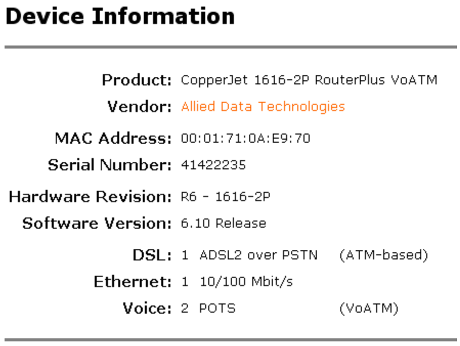
Note: Depending on the pre-defined settings, your network card settings may not be correct anymore. Make sure that your network card is correctly configured.

5.3 System

The System menu contains options which provide information about the CopperJet and enable you to manage and maintain the system by downloading new firmware images, uploading and downloading configuration profiles and viewing event logs.

5.3.1 Device Info

The *Device Info* page contains product specific information like Serial number, MAC address and more. From the *System* menu click on *Device Info*. The *Device Info* page is displayed.

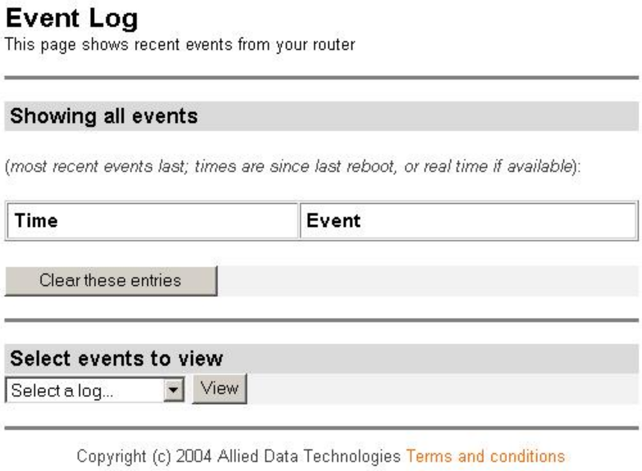


Device Information

Product:	CopperJet 1616-2P RouterPlus VoATM		
Vendor:	Allied Data Technologies		
MAC Address:	00:01:71:0A:E9:70		
Serial Number:	41422235		
Hardware Revision:	R6 - 1616-2P		
Software Version:	6.10 Release		
DSL:	1	ADSL2 over PSTN	(ATM-based)
Ethernet:	1	10/100 Mbit/s	
Voice:	2	POTS	(VoATM)

5.3.2 Event Log

The *Event Log* page shows recent events which have been generated from the CopperJet. From the left-hand menu, click on *System* then *Event Log*.
The *Event Log* page is displayed.



Event Log

This page shows recent events from your router

Showing all events

(most recent events last; times are since last reboot, or real time if available):

Time	Event

Select events to view

Copyright (c) 2004 Allied Data Technologies Terms and conditions

By default, this page displays a table containing all types of events which have been generated by the CopperJet during a current session. The following types of events are displayed:

- *Configuration errors*: These errors are highlighted in red in the Event table.
- *Syslog messages*: These messages shown in black in the Event table

For each event displayed in the table, the following information is provided:

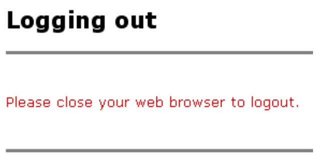
- when the event occurred (in seconds since your system was restarted)

  Note: If you are using the SNTP module, this column will display the current time as given by the SNTP server.
- which process the event occurred in
- brief descriptions of the Event

To clear the event log, click on *Clear these entries*.

5.3.3 Log out

Log out enables you to close your web browser properly.
Press on Log out and the *Log out* page is displayed.



Logging out

Please close your web browser to logout.

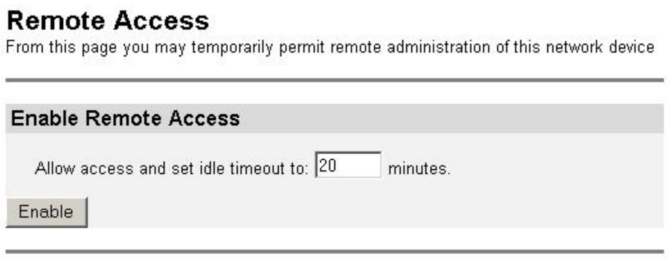
Close the web browser.

5.3.4 Remote Access

The Remote Access section allows you to enable temporary remote access to your CopperJet directly, bypassing NAT and the Firewall. More specifically, it allows IP packets from a Management Station addressed to the external interface using the specified transport and port to bypass NAT and the Firewall. Management Stations can only be directly manipulated via the CLI. It is expected that the Management Stations, that an end user will be using, will be saved in the default configuration of the device.

Note: In order to configure remote access, you first need to enable the Firewall.

Once you have configured Security, from the *System* menu, click on *Remote Access*. The *Remote Access* page is displayed.



Remote Access

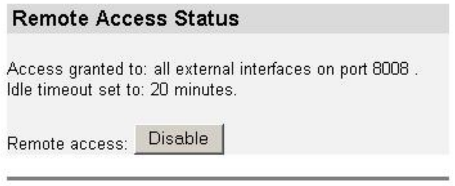
From this page you may temporarily permit remote administration of this network device

Enable Remote Access

Allow access and set idle timeout to: 20 minutes.

Enable

Type in the length of time that you want to allow remote access for. Click on *Enable*. The *Remote Access Status* page is displayed, confirming the number of seconds remaining for remote access.



Remote Access Status

Access granted to: all external interfaces on port 8008 .
Idle timeout set to: 20 minutes.

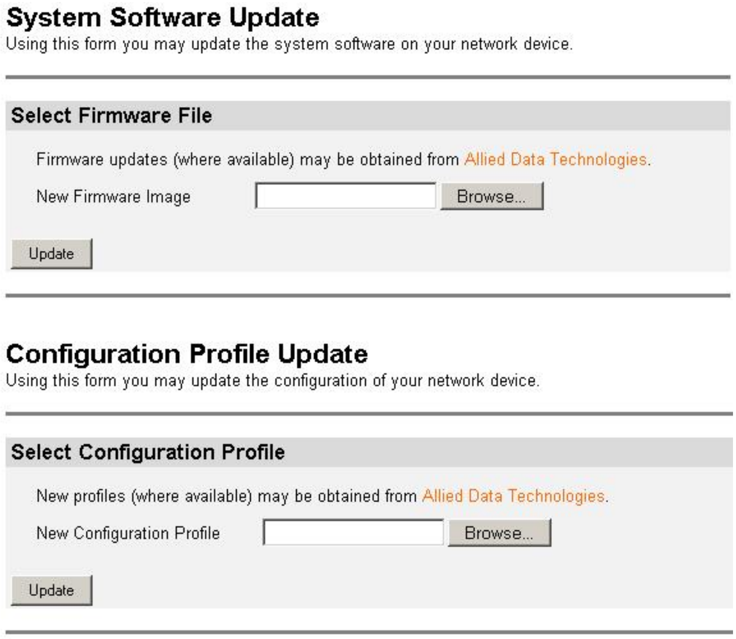
Remote access: Disable

There is also a *Disable* button that allows you to stop remote access before the specified time ends. For example, suppose that an idle timeout of 10 minutes is used when enabling Remote Access. This causes all defined management stations to be enabled with an idle timeout of 10 minutes. If no sessions are created by the Management Station within 10 minutes, the Management Station will be disabled. However, if any session is created, then it will also have an idle timeout of 10 minutes, whether the session is TCP, UDP or fake (i.e., anything else). Until that session expires, the Management Station will not be disabled.

Note: That a TCP session may be terminated before the end of the idle timeout, since TCP is a connection-oriented protocol and the end of the TCP session will be detected by the Security software.

5.3.5 Update Firmware and Restore Configuration Profile

The *Update* page enables you to upload new firmware release and/or restore saved configuration profiles. From the *System* menu click on *Update*. The *System Software Update/Configuration Profile Update* page is displayed.



System Software Update

Using this form you may update the system software on your network device.

Select Firmware File

Firmware updates (where available) may be obtained from Allied Data Technologies.

New Firmware Image

Configuration Profile Update

Using this form you may update the configuration of your network device.

Select Configuration Profile

New profiles (where available) may be obtained from Allied Data Technologies.

New Configuration Profile

To upload new firmware, enter the firmware filename at the *New Firmware Image* text box and type the name of the firmware file that you wish to upload (***.tbi**). If you do not know the filename details, click on the *Browse* button and locate the file using the *Choose file* box. Click on the *Update* button. The page is refreshed with a Firmware upload message and details of the number of bytes uploaded.

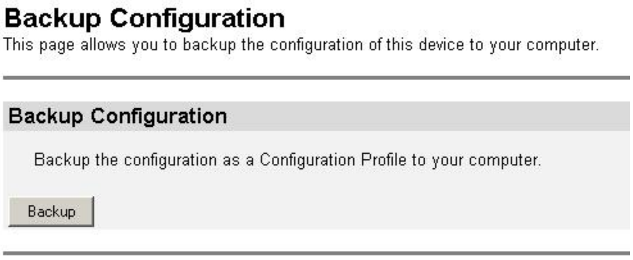
Note: After a firmware update you need to reset the CopperJet to it's Vendor default settings (see section 5.3.7 how to do this), otherwise some parameters of the new firmware don't take effect. The current configuration will be lost. Before updating the firmware, make a backup of the configuration. How to make a backup go to section 5.3.6.

Note: Depending on the current and new firmware version, you may be required to enter a Configuration Profile also.

To restore a saved configuration profile, enter the profile filename at the *New Configuration Profile* text box and type the name of the configuration profile that you wish to restore (***.tpr**). If you do not know the filename details, click on the *Browse* button and locate the file using the *Choose file* box. Click on the *Update* button. The page is refreshed with a Configuration upload message and details of the number of bytes restored.

5.3.6 Backup Configuration Profile

The *Backup* page allows you to backup your configuration profile to your computer. From the *System* menu click on *Backup*. The *Backup Configuration* page is displayed.



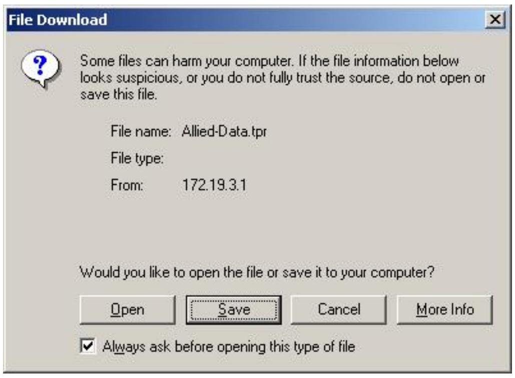
Backup Configuration

This page allows you to backup the configuration of this device to your computer.

Backup Configuration

Backup the configuration as a Configuration Profile to your computer.

From the *Backup Configuration* section, click on the *Backup* button. The *File Download* window is displayed.



File Download

Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: Allied-Data.tpr

File type:

From: 172.19.3.1

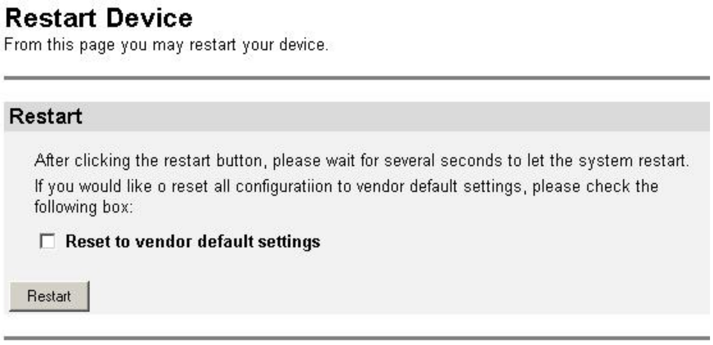
Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

Click *Save* to Save this file to disk. From the *Save As* window, select a file in which to save your configuration profile. Click on *Save*. The configuration profile is being saved.

5.3.7 Restart Device

The *Restart Device* page allows you to restart your CopperJet. From the *System* menu click on *Restart Device*. The *Restart Device* page is displayed.



Restart Device

From this page you may restart your device.

Restart

After clicking the restart button, please wait for several seconds to let the system restart. If you would like o reset all configuratiion to vendor default settings, please check the following box:

□ **Reset to vendor default settings**

Click on the *Restart* button to restart the CopperJet.
When you mark the box *Reset to vendor default settings* and click on the *Restart* button, the Copperjet will be set to it's vendor default settings.

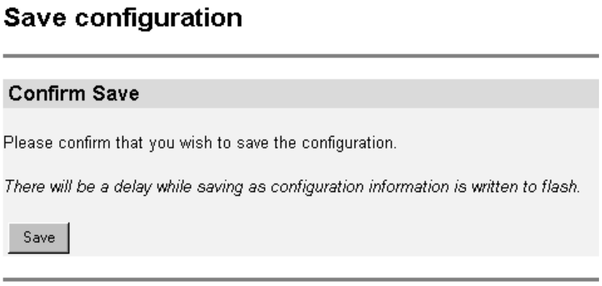
5.4 Configuration

The Configuration menu enables you to configure the basic and advanced network settings of the CopperJet.

5.4.1 Save Config

This menu option enables you to save your current configuration to Flash Memory.

From the *Configuration* menu, click *Save config*. The following page is displayed:



Save configuration

Confirm Save

Please confirm that you wish to save the configuration.

There will be a delay while saving as configuration information is written to flash.

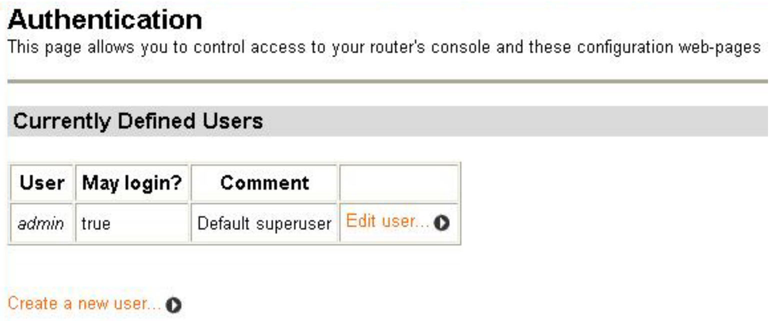
Click *Save* to save your current configuration in the *im.conf* file from ISFS and in to FlashFS.

After a short time the configuration is saved and the following confirmation message is displayed:

Saved information model to file //flashfs/im.conf

5.4.2 Changing the login settings

To change the default username and/or password, go to the *Configuration* menu and click on *Authentication*. The *Authentication* page is displayed.



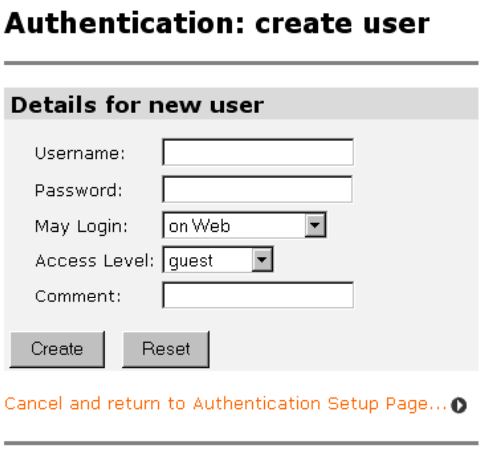
Authentication

This page allows you to control access to your router's console and these configuration web-pages

Currently Defined Users

User	May login?	Comment	
admin	true	Default superuser	Edit user...

This page displays the users that are currently defined. To add a new user click on the *Create a new user…*hyperlink. The *Authentication: create user* page is displayed.



Authentication: create user

Details for new user

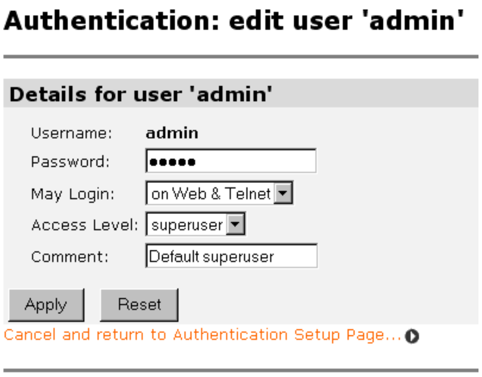
Username:	
Password:	
May Login:	on Web
Access Level:	guest
Comment:	

Fill in the required fields.

Username:	Username of the new user.
Password:	Password of the new user
May Login:	Login access via web or telnet or both.
Access Level:	The access level the user has when logged in (Default, Guest, Engineer, Super user).
Comment:	A comment you want to place for a user. (Optional)

After the fields are filled in, press on the *Create* button.

To change the username and/or password click on the *Edit user…*hyperlink of the user you want to edit. The *Details for user* page is displayed.



Authentication: edit user 'admin'

Details for user 'admin'

Username:	admin
Password:	●●●●●
May Login:	on Web & Telnet
Access Level:	superuser
Comment:	Default superuser

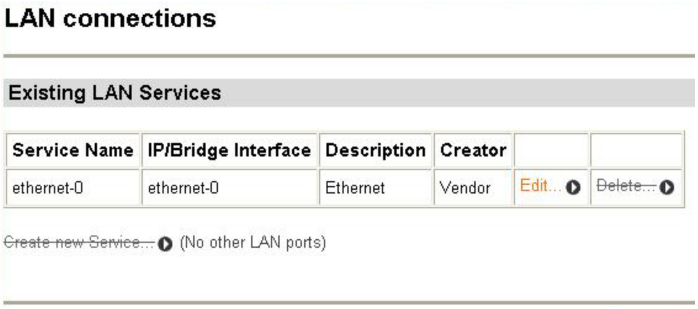
On this page you can change the password or access rights and level of the specific user. When the changes have been made, click on *Apply*.

When finished configuring the users, go to the *Configuration* menu and click on *Save config* to save the new settings into the CopperJet.

5.5 LAN Connections

LAN Connections allows you to configure the Ethernet connection. The Ethernet connection CANNOT be removed only edited.

Go to the *Configuration* menu and click on *LAN connections*. The *LAN Connections* page is displayed.



LAN connections

Existing LAN Services

Service Name	IP/Bridge Interface	Description	Creator		
ethernet-0	ethernet-0	Ethernet	Vendor	Edit...	~~Delete...~~

~~Create new Service...~~ (No other LAN ports)

This page displays a table that lists all existing LAN connections. This table contains the following information:

Service Name: Name of the LAN port

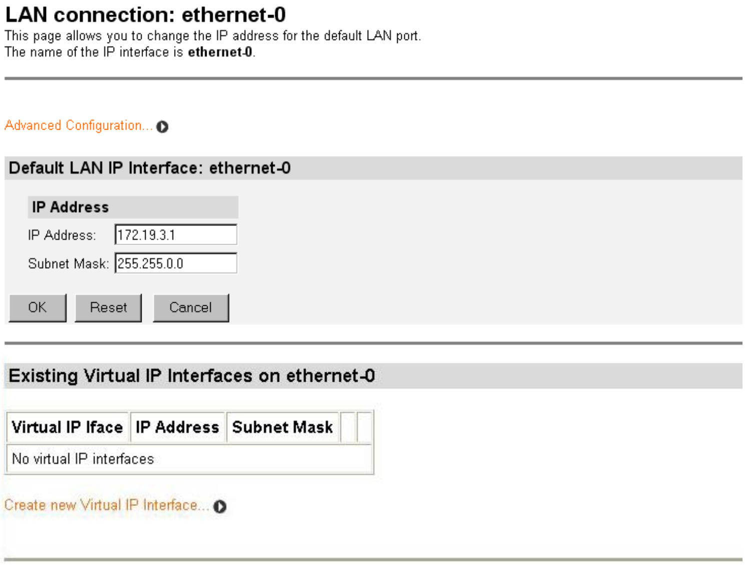
IP/Bridge Interface: Internal name of the LAN port.

Description: Description of the connection.

Creator: Which management entity the service was created in; *CLI, Firmware, WebAdmin or Vendor (Factory Defaults).*

5.5.1 Edit a LAN connection

To update or edit your LAN IP address, click on the *Edit* hyperlink of the LAN connection you want to update or edit. The *Default LAN Port* page is displayed.



LAN connection: ethernet-0

This page allows you to change the IP address for the default LAN port.
The name of the IP interface is **ethernet-0**.

Advanced Configuration...

Default LAN IP Interface: ethernet-0

IP Address

IP Address: 172.19.3.1

Subnet Mask: 255.255.0.0

Existing Virtual IP Interfaces on ethernet-0

Virtual IP Iface	IP Address	Subnet Mask	
No virtual IP interfaces			

Create new Virtual IP Interface...

This page contains the *Default LAN Port* table that allows you to configure the following:

IP Address:	Configure the Primary (default) IP address and subnet mask for the IP interface.
Virtual IP interface:	Create or edit a Virtual IP interface.

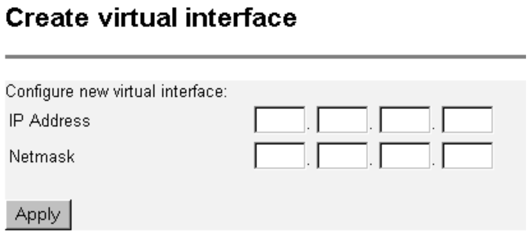
For more advanced options of the IP interface, click on the *Advanced Configuration…* hyperlink.

Once you have configured your IP addresses, click on the *OK* button. A message is displayed confirming that your address information is being updated. You may need to enter the new IP address in your web browser address box.

5.5.1.1 Virtual Interface

A virtual Interface can be used to assign a multiple IP address to the CopperJet (Multi homing). The IP address of the Virtual Interface MUST be in a different subnet than the Default LAN IP address.

To add a Virtual IP interface click on the *Create new Virtual IP Interface…* hyperlink.
The *Create virtual interface* page is displayed.



Fill in IP address and Netmask. This should be in a different subnet as the Default Ethernet IP interface address. Once you have configured your Virtual IP address and Netmask, click on *Apply*. You will return to the LAN connections page. The virtual interfaces section contains a table listing the names of the virtual interface(s). Each virtual interface is called item# by default.

Each virtual interface name has an *Edit* and a *Delete* link associated with it.
To edit a service:

a Click *Edit*.

b Change the options for the existing virtual interface, then click *Apply*.

The page is reset and the new values are displayed.
To delete a service:

a Click *Delete*.

b Click on *Delete this connection*.

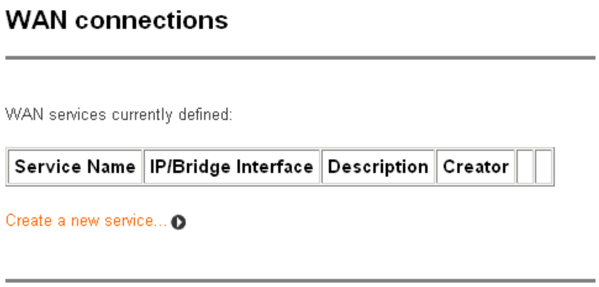
When finished configuring, go to the *Configuration* menu and click on *Save config* to save the new settings into the CopperJet.

Note: Make sure, after you have changed the LAN IP addresses, that your network card is in the same subnet as your new CopperJet LAN IP address.

5.6 WAN Connections

To create a DSL Connection, you need to add a WAN connection. Depending on the network of your ISP, you need to configure either a BRIDGED or ROUTED WAN connection. Bridged connections are often RFC1483 BRIDGED (attached to the Bridge). Routed connections are often RFC1483 ROUTED, PPPoE, PPPoA or IPoA (attached to the Router). The most commonly used WAN connections are described in section *6 WAN Configuration Examples.*

To create and configure WAN connections for your CopperJet, go to the *Configuration* menu and click on *WAN connections.* The *WAN connections* page is displayed.



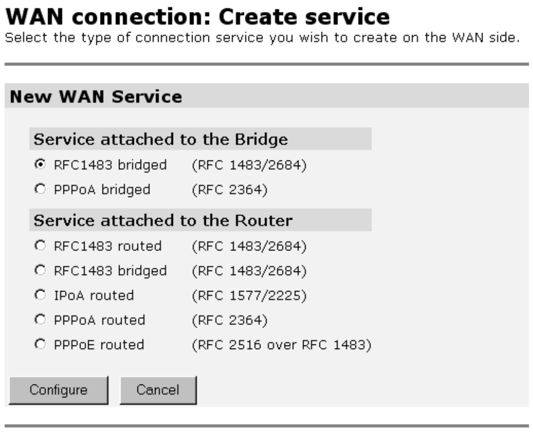
WAN connections

WAN services currently defined:

Service Name	IP/Bridge Interface	Description	Creator		

Create a new service...

This page contains a table that displays the current WAN connections or services that have been created. To create a new WAN connection, click on *Create a new service*. The *New WAN Service* page is displayed.



WAN connection: Create service

Select the type of connection service you wish to create on the WAN side.

New WAN Service

Service attached to the Bridge

● RFC1483 bridged (RFC 1483/2684)
○ PPPoA bridged (RFC 2364)

Service attached to the Router

○ RFC1483 routed (RFC 1483/2684)
○ RFC1483 bridged (RFC 1483/2684)
○ IPoA routed (RFC 1577/2225)
○ PPPoA routed (RFC 2364)
○ PPPoE routed (RFC 2516 over RFC 1483)

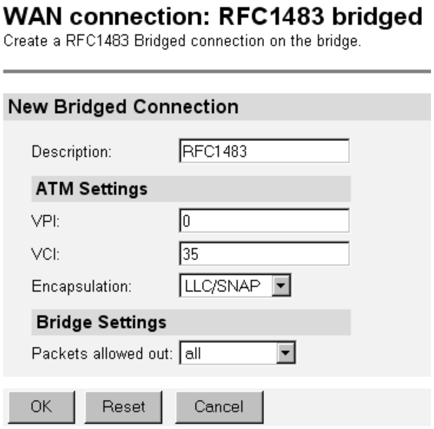
This page contains a list of all the WAN connections that are available. Select the type of service you wish to create and click on *Configure*.

5.6.1 Configuring RFC1483 Bridged service attached to the Bridge

One of the most commonly used connections is RFC 1483 Bridged, attached to the Bridge. This WAN connection performs a transparent bridge between the ADSL connection and the LAN connection. The CopperJet does not route any packets. All packets received on one interface (i.e. ADSL) are transparently bridged to the other interface (i.e. Ethernet).

***Important: DHCP Server need to be disabled when using RFC1483 bridged, attached to the bridge*.**

If RFC 1483 Bridged is attached to the Router, the CopperJet routes the packets from and to the different interfaces. Usually, you would configure NAT to allow multiple IP addresses on the LAN interface of the CopperJet.



WAN connection: RFC1483 bridged

Create a RFC1483 Bridged connection on the bridge.

New Bridged Connection

Description: RFC1483

ATM Settings

VPI: 0

VCI: 35

Encapsulation: LLC/SNAP

Bridge Settings

Packets allowed out: all

You need to add detailed configuration information about the WAN service that you are creating. Your service provider must provide this information.

Description: *RFC1483*, this is the default WAN connection name.

VPI: Virtual Path Identifier. A field in the ATM header. The VPI is used to identify the virtual path that a circuit belongs to. The VPI can be any value between 0 and 4095.

VCI: Virtual Channel Identifier. Part of the ATM header. The VCI is a tag that identifies which channel a cell will travel over. The VCI can be a value between 1 and 65535.

Encapsulation: *LLC/SNAP*. Ethernet over LLC/Snap. This is a bridge connection method and is the default setting of RFC1483.

Bridge Settings: Packet allowed out: By default *all*.

When finished configuring the WAN connection, click on *OK.* Go to the *Configuration* menu and click on *Save config* to save the new settings into the CopperJet.

After configuring the CopperJet in RFC1483 Bridge mode, you may need to configure your DHCP settings on your local network card. DHCP, which stands for Dynamic Host Configuration Protocol, automatically allocates an IP address on your local networkcard.

5.6.1.1 Configuring DHCP on your network card

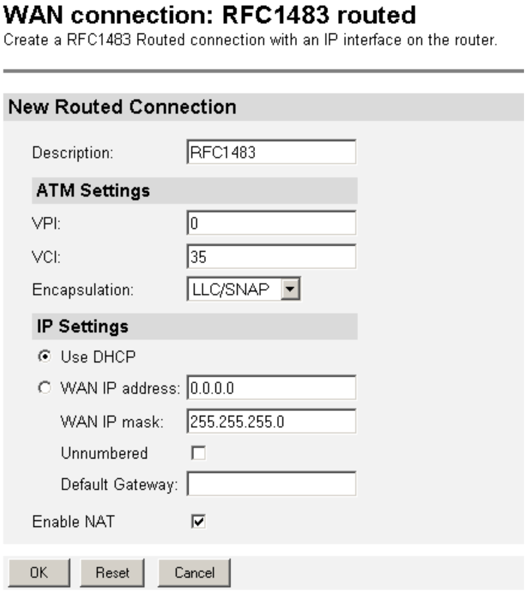
To configure DHCP on a network card for a Windows PC, follow the steps below:

1. Click the *Start menu*.
2. Click *Settings* -> *Control panel*.
3. Double-click the *Network* icon in the Control Panel window.
4. In the C*onfiguration* tab of the Network window, select the *TCP/IP* component of your Network Interface Card (NIC) from the list.
5. Click on *Properties*. The TCP/IP Properties window appears.

Make sure that the *Obtain IP address automatically* button is selected. This will ensure that your PC will get it's IP address from your ISP via DHCP.

5.6.2 Configuring RFC1483 Routed service attached to the Router

A RFC 1483 Routed connection is used when your Service Provider delivers a routed connection between the CopperJet and the Service Provider Network.



WAN connection: RFC1483 routed

Create a RFC1483 Routed connection with an IP interface on the router.

New Routed Connection

Description: RFC1483

ATM Settings

VPI: 0

VCI: 35

Encapsulation: LLC/SNAP

IP Settings

● Use DHCP

○ WAN IP address: 0.0.0.0

WAN IP mask: 255.255.255.0

Unnumbered □

Default Gateway:

Enable NAT ☑

You need to add detailed configuration information about the WAN service that you are creating. This information must be provided by your service provider.

Description: RFC1483, this is the default WAN connection name.

VPI: Virtual Path Identifier. A field in the ATM header. The VPI is used to identify the virtual path that a circuit belongs to. The VPI can be any value between 0 and 4095.

VCI: Virtual Channel Identifier. Part of the ATM header. The VCI is a tag that identifies which channel a cell will travel over. The VCI can be a value between 1 and 65535.

Encapsulation: LLC/SNAP. Ethernet over LLC/Snap. This is the default setting of RFC1483.

Use DHCP: When your ISP automatically allocates an IP address, use this option.

WAN IP address: Select this option when you have a fixed WAN IP address. This IP address is provided by your ISP.

Unnumbered: Disabled by default.

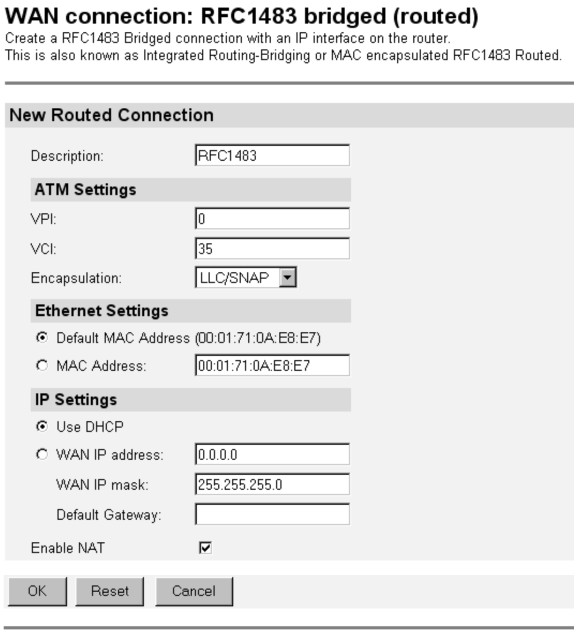
Default Gateway: When you use the option WAN IP address, you must fill in the default gateway.

Enable NAT: NAT is by default enabled.

When finished configuring the WAN connection, click on *OK.* Go to the *Configuration* menu and click on *Save config* to save the new settings into the CopperJet.

5.6.3 Configuring RFC1483 Bridged service attached to the Router

RFC1483 Bridged service attached to the Router is mostly used when you have a bridged line, but you want to have more then 1 pc on the internet (sharing).



WAN connection: RFC1483 bridged (routed)

Create a RFC1483 Bridged connection with an IP interface on the router.
This is also known as Integrated Routing-Bridging or MAC encapsulated RFC1483 Routed.

New Routed Connection

Description: RFC1483

ATM Settings

VPI: 0

VCI: 35

Encapsulation: LLC/SNAP

Ethernet Settings

● Default MAC Address (00:01:71:0A:E8:E7)

○ MAC Address: 00:01:71:0A:E8:E7

IP Settings

● Use DHCP

○ WAN IP address: 0.0.0.0

WAN IP mask: 255.255.255.0

Default Gateway:

Enable NAT ☑

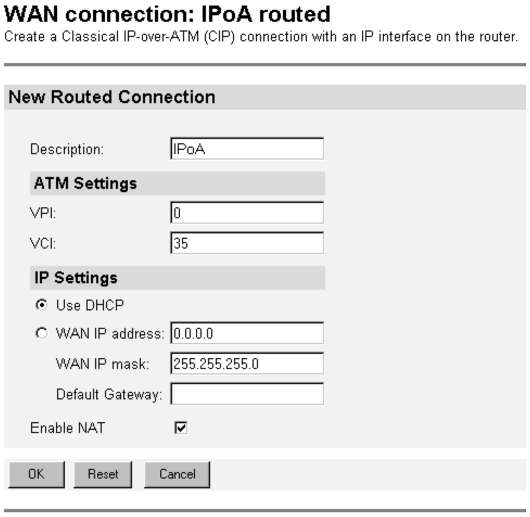
You need to add detailed configuration information about the WAN service that you are creating. This information must be provided by your service provider.

Description:	RFC1483, this is the default WAN connection name.
VPI:	Virtual Path Identifier. A field in the ATM header. The VPI is used to identify the virtual path that a circuit belongs to. The VPI can be any value between 0 and 4095.
VCI:	Virtual Channel Identifier. Part of the ATM header. The VCI is a tag that identifies which channel a cell will travel over. The VCI can be a value between 1 and 65535.
Encapsulation:	LLC/SNAP. Ethernet over LLC/Snap. This is a bridge connection method and is the default setting of RFC1483.
Default MAC Address:	Use the MAC address of the CopperJet on the WAN side.
MAC address:	Fill in the MAC address that you want to use on the WAN side.
Use DHCP:	When your ISP automatically allocates an IP address, use this option.
WAN IP address:	Select this option when you have a fixed WAN IP address. This IP address is provided by your ISP.
Default Gateway:	When you use the option WAN IP address, you must fill in the default gateway.
Enable NAT:	NAT is by default enabled.

When finished configuring the WAN connection, click on *OK.* Go to the *Configuration* menu and click on *Save config* to save the new settings into the CopperJet.

5.6.4 Configuring IPoA routed service attached to the Router

An IPoA routed connection is used when your Service Provider delivers a routed connection between the CopperJet and the Service Provider Network.



WAN connection: IPoA routed

Create a Classical IP-over-ATM (CIP) connection with an IP interface on the router.

New Routed Connection

Description: IPoA

ATM Settings

VPI: 0

VCI: 35

IP Settings

● Use DHCP

○ WAN IP address: 0.0.0.0

WAN IP mask: 255.255.255.0

Default Gateway:

Enable NAT ☑

You need to add detailed configuration information about the WAN service that you are creating. This information must be provided by your service provider.

Description: IPoA, this is the default WAN connection name.

VPI: Virtual Path Identifier. A field in the ATM header. The VPI is used to identify the virtual path that a circuit belongs to. The VPI can be any value between 0 and 4095.

VCI: Virtual Channel Identifier. Part of the ATM header. The VCI is a tag that identifies which channel a cell will travel over. The VCI can be a value between 1 and 65535.

Use DHCP: When your ISP automatically allocates an IP address, use this option.

WAN IP address: Select this option when you have a fixed WAN IP address. This IP address is provided by your ISP.

WAN IP mask: Fill in the WAN IP mask.

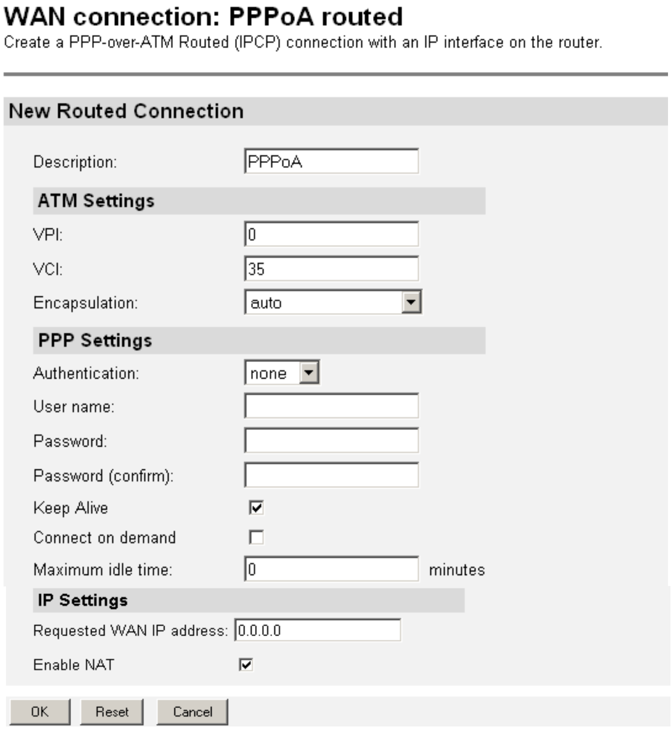
Default Gateway: When you use the option WAN IP address, you must fill in the default gateway.

Enable NAT: NAT is by default enabled.

When finished configuring the WAN connection, click on *OK.* Go to the *Configuration* menu and click on *Save config* to save the new settings into the CopperJet.

5.6.5 Configuring PPPoA routed service attached to the Router

PPPoA routed is mostly used when your Service Provider has an ATM network which requires authentication (username and password).



WAN connection: PPPoA routed

Create a PPP-over-ATM Routed (IPCP) connection with an IP interface on the router.

New Routed Connection

Description: PPPoA

ATM Settings

VPI: 0

VCI: 35

Encapsulation: auto

PPP Settings

Authentication: none

User name:

Password:

Password (confirm):

Keep Alive ☑

Connect on demand □

Maximum idle time: 0 minutes

IP Settings

Requested WAN IP address: 0.0.0.0

Enable NAT ☑

You need to add detailed configuration information about the WAN service that you are creating. This information must be provided by your service provider.

Description: PPPoA, this is the default WAN connection name.

VPI: Virtual Path Identifier. A field in the ATM header. The VPI is used to identify the virtual path that a circuit belongs to. The VPI can be any value between 0 and 4095.

VCI: Virtual Channel Identifier. Part of the ATM header. The VCI is a tag that identifies which channel a cell will travel over. The VCI can be a value between 1 and 65535.

Encapsulation: Auto by default.

Authentication: Choose the authentication method provided by your service provider.

None: You don’t need to set any authentication.

PAP: Password Authentication Protocol. The server sends an authentication request to the remote user that is dialling in. PAP passes the unencrypted username and password and identifies the remote end.

CHAP: Challenge Handshake Authentication Protocol The server sends an authentication request to the remote user that is dialling in. CHAP passes the encrypted username and password and identifies the remote end.

Username: Fill in the username provided by your service provider.

Password: Fill in the password provided by your service provider.

Password (confirm): Fill in the password provided by your service provider.

Keep Alive: On by default. Some ISP’s time-out if the connection has not been used. To avoid it, you can enable keep-alive that keeps the connection by accessing an Internet site at regular intervals.

Connect on demand: Off by default. When enabled, the PPP link will be established when traffic is sent to the Service Provider and disconnected when traffic has stopped for a certain amount of time. See also the Maximum Idle Time.

Maximum idle time: 0 by default. When *Connect On demand* is enabled, this time represents the idle time when the PPP link will be disconnected.

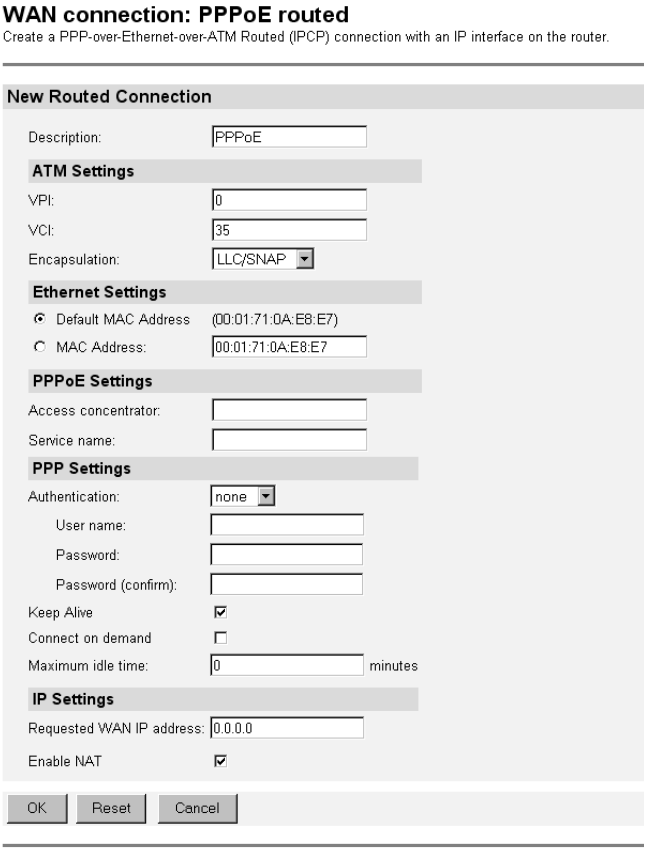
Requested WAN IP address: Fill in 0.0.0.0 when you get an IP address after authentication, or fill in a fixed IP address provided by your service provider.

Enable NAT: NAT is by default enabled.

When you are finished with configuring the WAN connection, click on *OK.* Go to the *Configuration* menu and click on *Save config* to save the new settings into the CopperJet.

5.6.6 Configuring PPPoE routed service attached to the Router

PPPoE routed is mostly used when your Service Provider has an Ethernet network which requires authentication (username and password).



WAN connection: PPPoE routed

Create a PPP-over-Ethernet-over-ATM Routed (IPCP) connection with an IP interface on the router.

New Routed Connection

Description: PPPoE

ATM Settings

VPI: 0

VCI: 35

Encapsulation: LLC/SNAP

Ethernet Settings

● Default MAC Address (00:01:71:0A:E8:E7)

○ MAC Address: 00:01:71:0A:E8:E7

PPPoE Settings

Access concentrator:

Service name:

PPP Settings

Authentication: none

User name:

Password:

Password (confirm):

Keep Alive ☑

Connect on demand □

Maximum idle time: 0 minutes

IP Settings

Requested WAN IP address: 0.0.0.0

Enable NAT ☑

You need to add detailed configuration information about the WAN service that you are creating. Your service provider must provide this information.

Description: PPPoE, this is the default WAN connection name.

VPI: Virtual Path Identifier. A field in the ATM header. The VPI is used to identify the virtual path that a circuit belongs to. The VPI can be any value between 0 and 4095.

VCI: Virtual Channel Identifier. Part of the ATM header. The VCI is a tag that identifies which channel a cell will travel over. The VCI can be a value between 1 and 65535.

Encapsulation: LLC/SNAP by default.

Default MAC Address: Use the MAC address of the CopperJet on the WAN side.

MAC address: Fill in the MAC address that you want to use on the WAN side.

Access concentrator: Some service provider requires this entry. If the service provider does not provide this, leave it blank.

Service name: Some service provider requires this entry. If the service provider does not provide this, leave it blank.

Authentication: Choose the authentication method provided by your service provider.

None: You don't need to set any authentication.

PAP: Password Authentication Protocol, the server sends an authentication request to the remote user that is dialling in. PAP passes the unencrypted username and password and identifies the remote end.

CHAP: Challenge Handshake Authentication Protocol, the server sends an authentication request to the remote user that is dialling in. CHAP passes the encrypted username and password and identifies the remote end.

Username: Fill in the username provided by your service provider.

Password: Fill in the password provided by your service provider.

Password (confirm): Fill in the password provided by your service provider.

Keep Alive: On by default. Some ISP's time-out if the connection has not been used. To avoid it, you can enable keep-alive that keeps the connection by accessing an Internet site at regular intervals.

Connect on demand: Off by default. When enabled, the PPP link will be established when traffic is sent to the Service Provider and disconnected when traffic has stopped for a certain amount of time. See also the Maximum Idle Time.

Maximum idle time: 0 by default. When *Connect On demand* is enabled, this time represents the idle time when the PPP link will be disconnected.

Requested WAN IP address: Fill in 0.0.0.0 when you get an IP address after authentication, or fill in a fixed IP address provided by your service provider.

Enable NAT: NAT is by default enabled.

When finished configuring the WAN connection, click on *OK.* Go to the *Configuration* menu and click on *Save config* to save the new settings into the CopperJet.

5.7 Security

The CopperJet has extensive Security functionality like a Stateful Inspection Firewall, Network Address Translation (NAT) and Filters. One of the most used functionality is NAT.

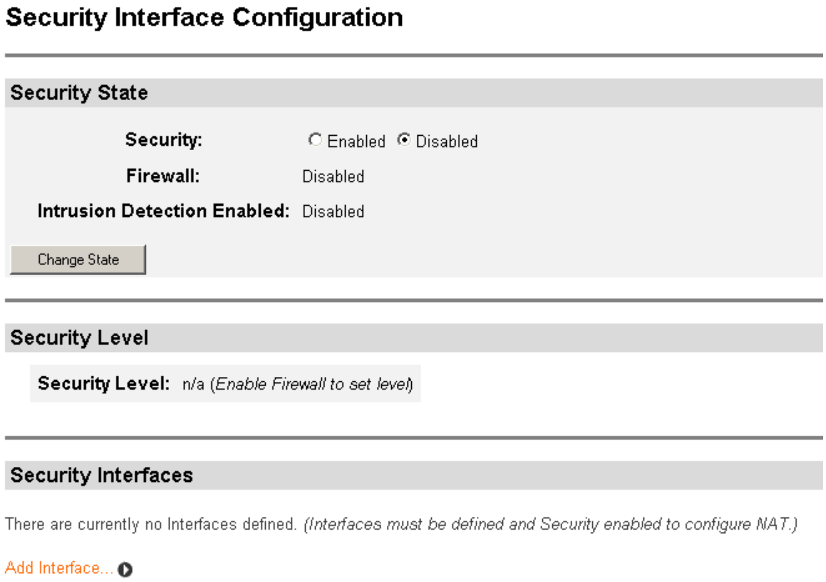
Security allows you to:

- Enable Security
- Enable Firewall
- Enable Intrusion Detection
- Configure Security level
- Configure Security interfaces
- Configure Firewall Policy
- Configure Firewall Trigger
- Configure Intrusion Detection

NAT allows you to:

- Enable NAT between interfaces
- Configure global addresses
- Configure reserved mapping

Go to the *Configuration* menu and select *Securit*y. The *Security Interface Configuration* page is displayed.



Security Interface Configuration

Security State

Security: ○ Enabled ● Disabled

Firewall: Disabled

Intrusion Detection Enabled: Disabled

Security Level

Security Level: n/a (*Enable Firewall to set level*)

Security Interfaces

There are currently no Interfaces defined. *(Interfaces must be defined and Security enabled to configure NAT.)*

This page contains the default Security settings. Before the security options can be configured, interfaces need to be defined to which the security can be assigned to.

5.7.1 Enabling Security

You must enable *Security* before you can add security functionality like Firewall, NAT or filters.

In the *Security State* section:
Click on the *Security Enabled* radio button and select *Change State* to update the *Security State* section. The overall Security is now enabled.

5.7.2 Configuring Security Interfaces

Before Security options can be configured, there must be at least 2 Security interfaces defined and configured. Security interfaces represent the logical connections to and from the CopperJet. These interfaces are used to enable the security on these connections.

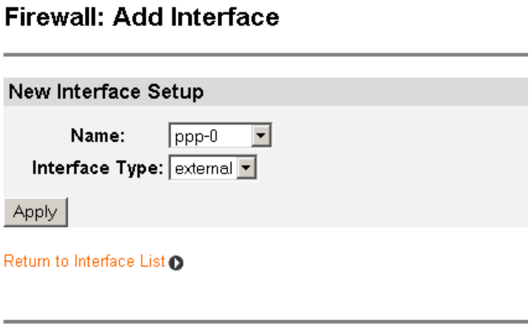
There are three different types of security interfaces available

- Internal: usually the LAN connection
- External: usually the WAN connection
- DMZ: usually a second LAN connection or IP subnet

Note: The security interfaces are directly linked to the LAN and WAN connections. Be sure that the necessary LAN and WAN connections are configured correctly. The security interfaces can be assigned to these connections.

Important: When a WAN connection is already configured with NAT enabled, both the internal and external Security Interfaces are automatically added and configured. These Security Interfaces can be used to enable the other security options.

To add a Security Interface, go to the *Configuration* menu and select *Security*. The *Security Interface Configuration* page is displayed. Select *Add Interface* at the *Security Interface* section. The *Firewall: Add interface* page is displayed.



Firewall: Add Interface

New Interface Setup

Name: ppp-0

Interface Type: external

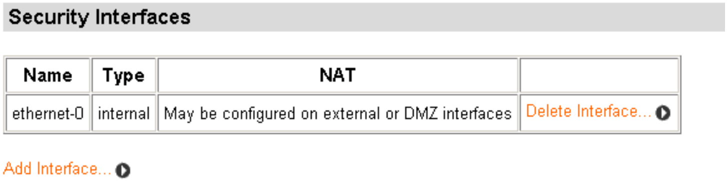
Select the proper WAN or LAN connection from the *Name* section.

- The Ethernet LAN connection is represented as *ethernet-0*.
- The USB LAN connection is represented as *ethernet-1*.
- WAN connections are represented as *ppp-0*, *rfc1483-0*, or *ipoa-0*.

Select the proper *Interface type*. Usually the LAN connections *ethernet-0* or *ethernet-1* are *internal*. The WAN connections are usually *external.*

Click on *Apply* to add the security interface.

The *Security Interface Configuration* page is displayed and the security interface is added to the section *Security Interface.*



Security Interfaces

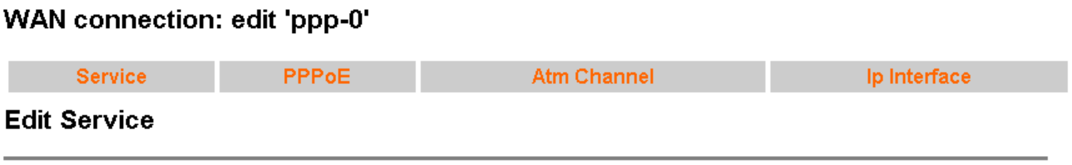
Name	Type	NAT	
ethernet-0	internal	May be configured on external or DMZ interfaces	Delete Interface...

5.7.3 Configuring Network Address Translation (NAT)

The Network Address Translator (NAT) implements Port Address Translation (PAT) and provides Network Address Port Translation (NAPT), also known as IP Masquerading. NAT allows a single real IP address on the WAN side to be shared among many devices on the LAN side, each of which have private addresses.

NAT can be enabled directly when configuring the WAN connection. See section 5.6 WAN Connections for more details.

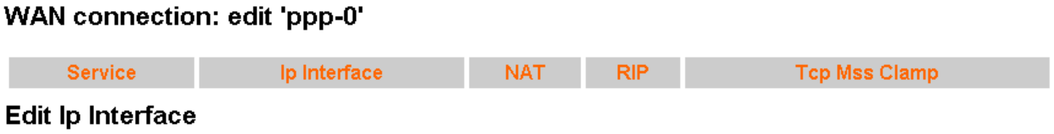
If NAT is not enabled during configuration of the WAN connection, go to the *Configuration* menu and select *WAN Connections*. The *WAN Connections* page is displayed. Edit the WAN connection by selecting the *Edit…* hyperlink. The *WAN Connection:edit '   '* page is displayed.



WAN connection: edit 'ppp-0'

Edit Service

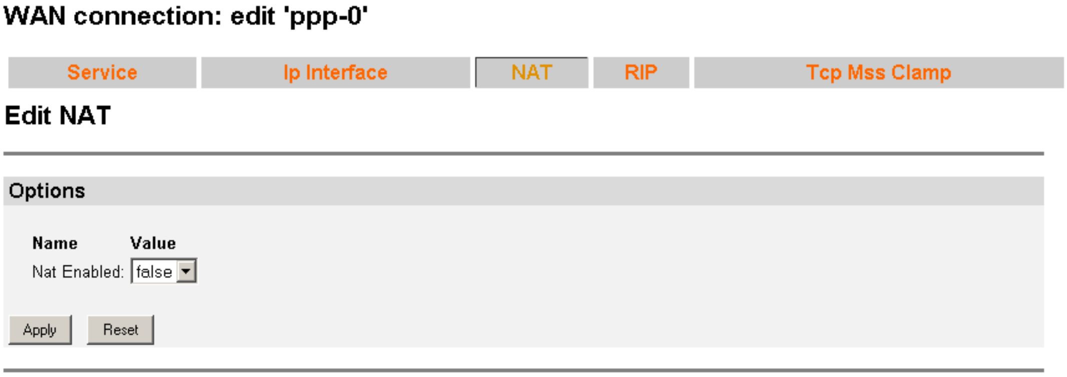
Select the *IP Interface* tab. The *Edit IP Interface* page is displayed.



WAN connection: edit 'ppp-0'

Edit Ip Interface

Select the *NAT* tab. The *Edit NAT* page is displayed.



WAN connection: edit 'ppp-0'

Edit NAT

Options

Name	Value
Nat Enabled:	false

On this page NAT can be enabled or disabled.

Nat Enabled:	*false* NAT is disabled *true* NAT is enabled

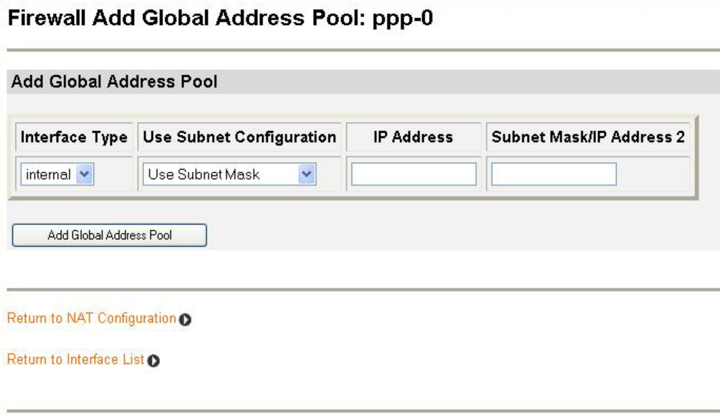
After you changed the setting, click on *Apply*. Don't forget to save the changes. Go to the *Configuration* menu and click on *Save config* to save the new settings into the CopperJet.

5.7.3.1 Configuring NAT global addresses

Global address pools allow you to create a pool of outside network addresses that is visible outside your network. Before you can configure global addresses, you need to configure NAT.
If you want to set up a global address pool on your existing NAT enabled interfaces:

From the *NAT Security Interfaces* table, click on the *Advanced NAT Configuration* hyperlink for the interface that you want to add a global pool to.
Click on *Add Global Address Pool* The *Firewall Add Global Address Pool* page is displayed:

This page allows you to create a pool of network IP addresses that are visible outside your network. Add values for the following table entries:



Firewall Add Global Address Pool: ppp-0

Add Global Address Pool

Interface Type	Use Subnet Configuration	IP Address	Subnet Mask/IP Address 2
internal	Use Subnet Mask		

- *Interface type*; the internal address type that you want to map your external global IP addresses to. Click on the drop-down list and select an interface type.

- *Use Subnet Configuration*; there are two ways to specify a range of IP addresses. You can either *Use Subnet Mask* (specify the subnet mask address of the IP address) or *Use IP Address Range* (specify the first and last IP address in the range). Click on the drop-down list and select a method.

- Type in the *IP Address* that is visible outside the network.

- *Subnet Mask/IP Address 2*; the value you specify here depends on the subnet configuration that you are using. If you chose *Use Subnet Mask*, type in the subnet mask of the IP address. If you chose *Use IP Address Range*, type in the last IP address in the range of addresses that make up the global address pool.

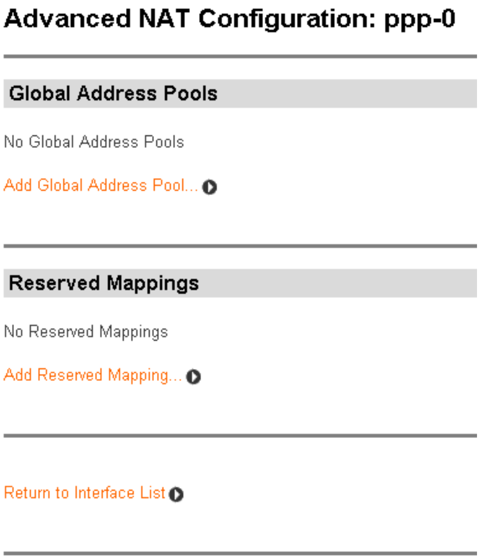
Once you have configured the table, click on *Add global address pool*. The table is refreshed and the global address pool is added to your NAT configuration.

To delete a global address pool, click on the *Delete* hyperlink, then click on the *Delete Global Address Pool* button.

5.7.3.2 Configuring NAT reserved mapping

Reserved mapping allows you to map an outside security interface or an IP address from a global pool to an individual IP address inside the network. Mapping is based on transport type and port number. Before you can configure reserved mapping, you need to configure NAT. See section 0 Configuring Network Address Translation (NAT)

To set up a reserved mapping on your existing NAT enabled interfaces, go to the *Configuration* menu and select *Security*. From the *Security Interfaces* table, click on the *Advanced NAT Configuration* hyperlink for the interface that you want to add the reserved mappings to. The *Advanced NAT Configuration:* page is displayed.



Advanced NAT Configuration: ppp-0

Global Address Pools

No Global Address Pools

Add Global Address Pool...

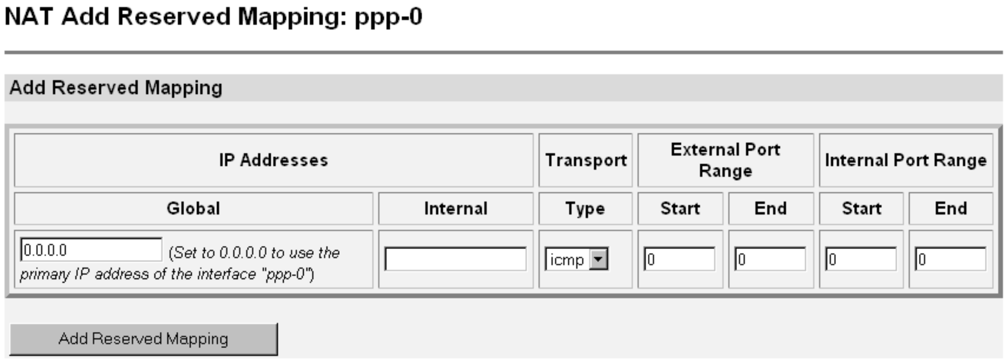
Reserved Mappings

No Reserved Mappings

Add Reserved Mapping...

Return to Interface List

Click on the *Add Reserved Mapping* hyperlink. The *Add Reserved Mapping* page is displayed.



NAT Add Reserved Mapping: ppp-0

Add Reserved Mapping

IP Addresses		Transport	External Port Range		Internal Port Range	
Global	Internal	Type	Start	End	Start	End
0.0.0.0 *(Set to 0.0.0.0 to use the primary IP address of the interface "ppp-0")*		icmp	0	0	0	0

This page allows you to configure your reserved mapping. Add specific values for the following table entries.

Global IP Address: If you are mapping from a global IP address, type the address here. If you are mapping from a security interface, type *0.0.0.0*.

Internal IP Address: The IP address of an individual host inside your network.

Transport Type: Specify the transport type that you want to map from the outside interface to the inside.

External Port Range: The external port range that your transport uses. Can also be a single port as Start and End port.

Internal Port Range: The internal port range that your transport uses. Can also be a single port as Start and End port.

Once you have configured the table, click on *Add reserved mappin*g. The table is refreshed and the reserved mapping is added to your NAT configuration.

Important: Make sure the Internal IP address is in the same subnet as your CopperJet LAN IP address.

To delete a reserved mapping, click on the *Delete* hyperlink. The *Delete Reserved Mapping Confirmation* page is displayed. Click on the *Delete Reserved Mapping* button. The reserved mapping is deleted.

Don't forget to save the changes. Go to the *Configuration* menu and click on *Save config* to save the new settings into the CopperJet.

5.7.4 Enabling Firewall

Before enabling the firewall, you must have Security enabled and you must have at least **1 internal interface or 1 external interface** configured. Be sure that the WAN and/or LAN connection and the Security Interfaces are defined and configured.

To enable the Firewall go to the *Security State* section and select *Firewall Enabled.* Click on *Change State* to update the *Security State* section. The Firewall is now enabled on the CopperJet.

Important: Enabling the Firewall will block ALL traffic going in and out of the CopperJet. Firewall Policies need to be configured for allowing traffic to pass through.

5.7.5 Enabling Intrusion Detection

Before enabling Intrusion Detection, you must have Security enabled and you must have at least **1 internal interface or 1 external interface** configured. Be sure that the WAN and/or LAN connections and the Security Interfaces are defined and configured.

To enable Intrusion Detection, go to the *Security State* section and select *Intrusion Detection Enabled.* Click on *Change State* to update the *Security State* section. The Intrusion Detection is now enabled on the CopperJet.

5.7.6 Set a Security level

When you have enabled the firewall, you can set a Security Level.
Select a *Security Level* and click on *Change State*.

The *high*, *medium*, *low and default* levels contain default policy and port filter configurations for each of your network interface connections, so you do not need to set your own individual policies and port filters. If you explicitly set the level to *none*, all traffic is blocked.
By default, no security level is set in your default configuration.

Setting a Firewall default security level automatically clears all previous Firewall settings.

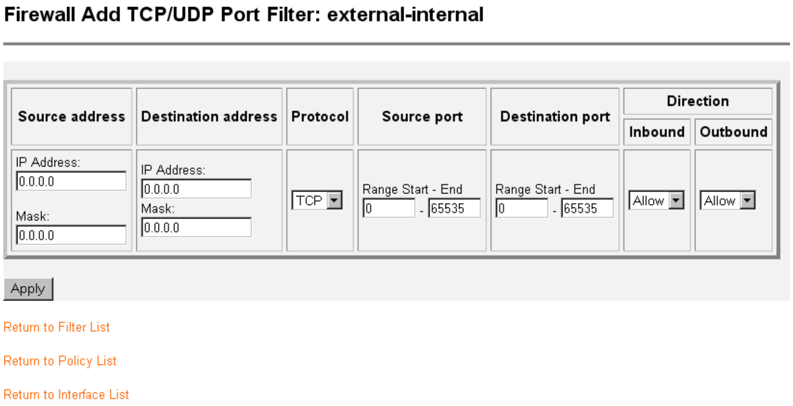
5.7.7 Configuring portfilters

A portfilter is an individual rule that determines what kind of traffic can pass between two interfaces specified in an existing policy.

To configure a portfilter:

From the *Current Firewall Policies* table, click on the *Port Filters* link for the policy that you want to configure. The page displayed contains three *Add Filter* hyperlinks that allow you to create three different kinds of portfilter:

For a TCP portfilter click on *Add TCP Filter*.
The *Firewall Add TCP Port Filter* page is displayed:

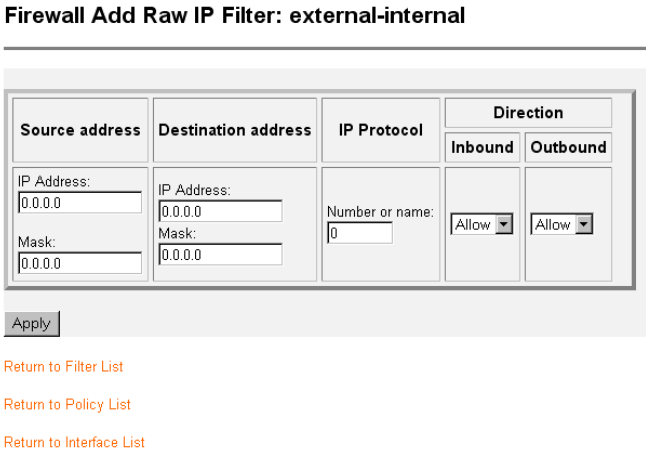


Firewall Add TCP/UDP Port Filter: external-internal

Source address	Destination address	Protocol	Source port	Destination port	Direction	
					Inbound	Outbound
IP Address: 0.0.0.0 Mask: 0.0.0.0	IP Address: 0.0.0.0 Mask: 0.0.0.0	TCP ▾	Range Start - End 0 - 65535	Range Start - End 0 - 65535	Allow ▾	Allow ▾

Complete the source/destination addresses, and the source/destination port range for the protocol (TCP or UDP selected from the protocol drop-down list) that you want to filter. Use the *Direction* drop-down lists to specify whether you want to allow/block inbound traffic, and allow/block outbound traffic. Click *Apply*. The *Firewall Port Filters* page is displayed, containing details of the TCP/UDP port filter that you have just added.

For a non-TCP/UDP portfilter (Raw IP Filter) click on *Add Raw IP Filter.* The *Firewall Add Raw IP Filter* page is displayed:



Firewall Add Raw IP Filter: external-internal

Source address	Destination address	IP Protocol	Direction	
			Inbound	Outbound
IP Address: 0.0.0.0 Mask: 0.0.0.0	IP Address: 0.0.0.0 Mask: 0.0.0.0	Number or name: 0	Allow ▾	Allow ▾

Specify the source/destination addresses and the IP protocol number in the relevant text boxes. For example, for IGMP, enter protocol number 2.
Then use the *Direction* drop-down lists to specify whether you want to allow/block inbound traffic, and allow/block outbound traffic. Click on *Apply*. The *Firewall Portfilters* page is displayed, containing details of the IP port filter that you have just added.

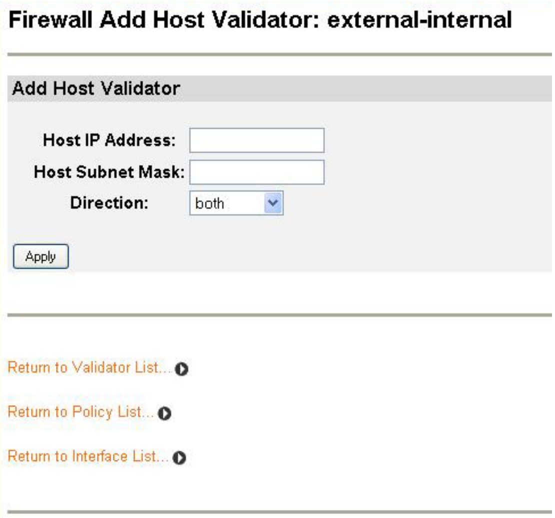
Each portfilter displayed in the *Firewall Port Filters* page has a *Delete* hyperlink assigned to it. To delete a portfilter, click on this link, then at the confirmation page, click on the *Delete* button. The portfilter is removed from the Firewall configuration.

5.7.8 Configuring validators

A validator allows/blocks traffic based on the source/destination IP address and netmask. Traffic will be allowed or blocked depending on the validator configuration specified when the policy was created.

To configure a validator:

From the *Current Firewall Policies* table, click on the *Host Validators* link for the policy that you want to configure. The *Configure Validators* page is displayed. Click on the *Add Host Validator* link. The *Firewall Add Host Validator* page is displayed:



Firewall Add Host Validator: external-internal

Add Host Validator

Host IP Address:	
Host Subnet Mask:	
Direction:	both

1 In the *Host IP Address* text box, type the IP address that you want to allow/block.

2 In the *Host Subnet Mask* text box, type the IP mask address. If you want to filter a range of addresses, you can specify the mask, for example, *255.255.255.0*. If you want to filter a single IP address, use the specific IP mask address, for example, *255.255.255.255*.

3 Click on the *Direction* drop-down list and select the direction of traffic that you want the validator to filter.

4 Click on *Apply*. The *Configure Validators* page is displayed, containing details of the host validator that you have just added.

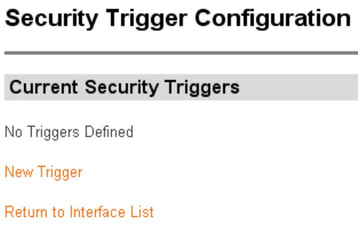
5 Each portfilter displayed in the *Configure Validators* page has a *Delete Host Validator* hyperlink assigned to it. To delete a validator, click on this link, then at the confirmation page, click on the *Delete Host Validator* button. The validator is removed from the Firewall configuration.

5.7.8.1 Configuring Triggers

A trigger allows an application to open a secondary port in order to transport packets. The most common applications that require secondary ports are Messenger and NetMeeting. Triggers are mandatory for these applications to work with NAT of other security options.

This section assumes that you have enabled Security and defined at least 1 security interface.

To configure a trigger, go to the *Policies, Triggers and Intrusion Detection* section of the *Security Interface Configuratio*n. Click on *Security Trigger Configuration.* The *Security Trigger Configuration* page is displayed.



Security Trigger Configuration

Current Security Triggers

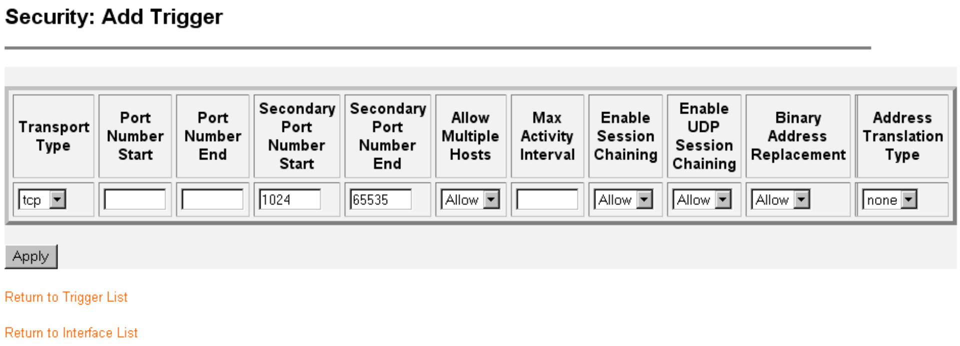
No Triggers Defined

New Trigger

Return to Interface List

5.7.8.2 Adding Triggers

To add a trigger, click on the *New Trigger* link. The *Security Add Trigger* page is displayed.



Security: Add Trigger

Transport Type	Port Number Start	Port Number End	Secondary Port Number Start	Secondary Port Number End	Allow Multiple Hosts	Max Activity Interval	Enable Session Chaining	Enable UDP Session Chaining	Binary Address Replacement	Address Translation Type
tcp			1024	65535	Allow		Allow	Allow	Allow	none

Return to Trigger List

Return to Interface List

A list of options is displayed for configuring the Trigger.

Transport Type: Select a transport type from the drop-down list, depending on whether you are adding a trigger for a TCP or a UDP application.

Port Number Start: Type the start of the trigger port range that the primary session uses.

Port Number End: Type the end of the trigger port range that the primary session uses.

Secondary Port Number Start: Type the start of the trigger port range that the secondary session uses.

Secondary Port Number End: Type the end of the trigger port range that the secondary session uses.

Allow Multiple Hosts: Select *allow* if you want a secondary session to be initiated to/from different remote hosts. Select *block* if you want a secondary session to be initiated only to/from the same remote host. Default *allow.*

Max Activity Interval: Type the maximum interval time (in milliseconds) between the use of secondary port sessions. Default *10000*.

Enable Session Chaining: Select *Allow* or *Block* depending on whether you want to allow multi-level TCP session chaining. Default *allow.*

Enable UDP Session Chaining: Select *Allow* or *Block* depending on whether you want to allow multi-level UDP and TCP session chaining. You must set *Enable Session Chaining* to *Allow* if you want this to work. Default *allow.*

Binary Address Replacement: Select *Allow* or *Block* depending on whether you want to use binary address replacement on an existing trigger. Default *allow.*

Address Translation Type: Specify what type of address replacement is set on a trigger. You must set *Binary Address Replacement* to *Allow* if you want this to work. Default *none.*

When finished configuring the Trigger, click on *Apply*. The *Firewall Trigger Configuration* page is displayed, containing details of the trigger that you have just configured.

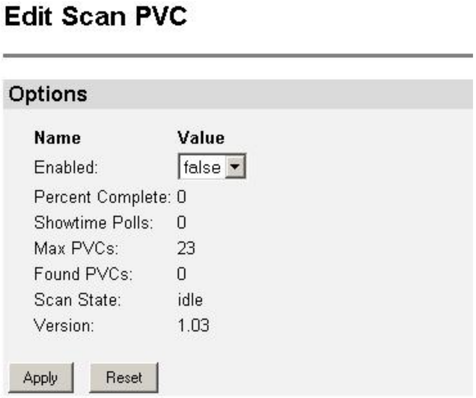
5.7.8.3 Deleting Triggers

Each trigger displayed in the *Firewall Trigger Configuration* page has a *Delete* hyperlink assigned to it. To delete a trigger, click on this link. The *confirmation* page is displayed. Click on the *Delete* button to delete the Trigger.
The *Firewall Trigger Configuration* page is displayed and details of the deleted trigger have been removed.

5.8 Search Service

The Search Service menu allows you to set auto-provisioning to scan a fixed list of PVCs for protocols such as RFC 1483, PPPoA and PPPoE. It automatically creates a suitable transport and attaches it to the IP Stack.

From the Configuration menu, click on *Search service*. The *Edit Scan PVC* page is displayed.



Edit Scan PVC

Options

Name	Value
Enabled:	false ▾
Percent Complete:	0
Showtime Polls:	0
Max PVCs:	23
Found PVCs:	0
Scan State:	idle
Version:	1.03

Click on the *Value* drop-down list and click on *true*. Click on the *Apply* button. The scan starts, and the Options on this page are updated with the status of the scan:

- *Percent Complete*: displays scan progress (as a percentage)
- *Showtime Polls*: number of times that DSL showtime is checked
- *Max PVCs*: maximum number of PVCs that the scan should look up
- *Found PVCs*: Number of PVCs found by the scan
- *Scan State*:

  idle (not scanning)
  waitingForResponse (currently scanning)
  waitingForShowtime (currently polling DSL showtime)
  Aborted (the scan was stopped before scanning was complete)
  FoundPVC (scanning is complete - at least one PVC found)
  noPVCsFound (scanning is complete - scan failed to detect any PVCs)
- *Version*: version number of the scan module

5.9 Zero Installation PPP Bridge (ZIPB)

Dynamic ZIPB, also known as *PPP Half Bridge*, allows a home user to share the public IP address assigned by their ISP with a single PC on the LAN. This avoids problems caused by certain applications having to work through NAT, and avoids the need to run a PPP software stack on a customer's PC. It is not a bridge, but rather an IP router with specialized address management.

5.9.1 ZIPB in bridged configurations

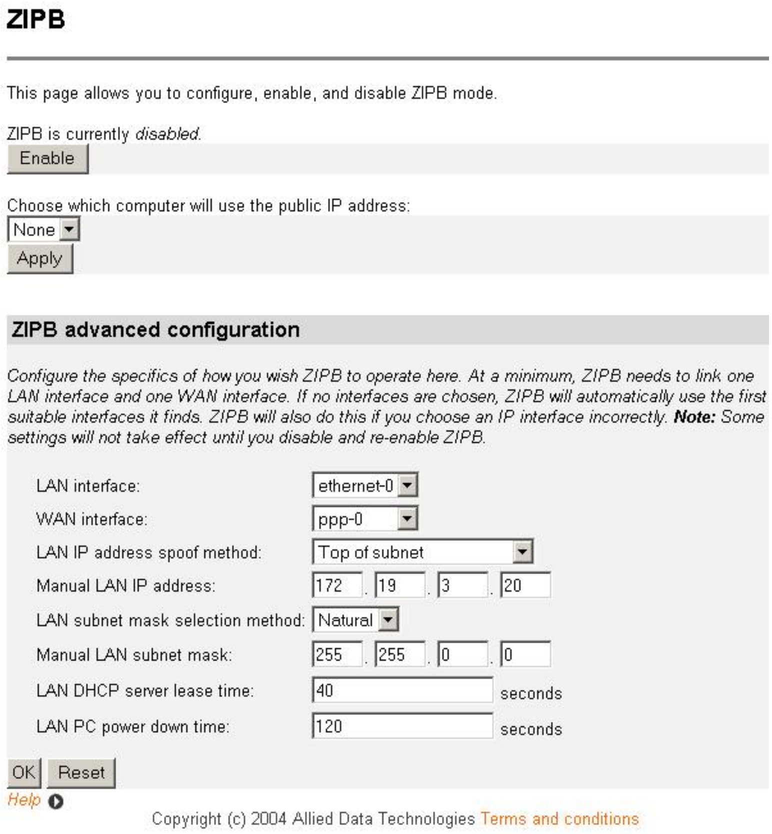
In some bridged configurations, a PPPoE/PPPoA client must be installed on each LAN side PC. No public address is assigned to the device; each LAN side PC uses its public IP address directly. Enabling ZIPB in your bridged configuration means that there is no requirement to install third party PPPoE clients on the LAN side PCs, because the CopperJet runs an embedded PPPoE/PPPoA client.

5.9.2 ZIPB in routed configurations

In NAT routed mode, the PPPoE/PPPoA client is installed on the CopperJet. The CopperJet uses the public IP address assigned by the ISP, and NAT is used to provide a private subnet on the LAN. As NAT is being used, ALGs are required for many typical applications. Certain applications encounter problems when running through NAT. By allowing one PC on the LAN to temporarily share the public IP address that has been assigned by the ISP, this PC can run applications without having to go through NAT. The other PCs on the LAN may access the external network by running through NAT.

5.9.3 Enabling/Disabling ZIPB

To enable or disable ZIPB, go to the *Configuration* menu and select *ZIPB*. The *ZIPB* page is displayed.



ZIPB

This page allows you to configure, enable, and disable ZIPB mode.

ZIPB is currently *disabled*.

Choose which computer will use the public IP address:

None

ZIPB advanced configuration

Configure the specifics of how you wish ZIPB to operate here. At a minimum, ZIPB needs to link one LAN interface and one WAN interface. If no interfaces are chosen, ZIPB will automatically use the first suitable interfaces it finds. ZIPB will also do this if you choose an IP interface incorrectly. ***Note:*** *Some settings will not take effect until you disable and re-enable ZIPB.*

LAN interface: ethernet-0

WAN interface: ppp-0

LAN IP address spoof method: Top of subnet

Manual LAN IP address: 172 . 19 . 3 . 20

LAN subnet mask selection method: Natural

Manual LAN subnet mask: 255 . 255 . 0 . 0

LAN DHCP server lease time: 40 seconds

LAN PC power down time: 120 seconds

Copyright (c) 2004 Allied Data Technologies Terms and conditions

Click on the *Enable* button to enable ZIPB. Click on the *Choose which computer will use the public IP address* drop-down list and select a LAN PC. The public WAN IP address will be shared with this PC, and the PC will no longer need to go through NAT. Click *Apply*.

Find below an example on how to get ZIPB to work.
Example:

- Make sure that you have a working routed WAN connection configured.
- Make sure that the DHCP server of the CopperJet is enabled and that your network card of your pc is on obtain IP address automatically.
- When the DHCP server is enabled and the network card of the pc is set to obtain IP address automatically, the pc name is available in the list.
- Configured ZIPB as follows:
  - Select “ethernet-0” as LAN interface
  - Select “rfc1483-0 or ppp-0” as WAN interface
  - Select “Increment” as LAN IP address spoof method
  - Click on *Apply* to apply the settings
  - Now enable ZIPB, by clicking on the *Enable* button.
  - As last select the pc from the list. And click on *Apply*.
  - Do an **ipconfig /release** and then **ipconfig /renew** (in a DOS box) on the pc that you have selected in the list. The pc will get a WAN IP assigned.

Once the device has retrieved the public IP address via IPCP, the ZIPB process creates a spoofed IP address and assigns this address to a virtual interface attached to the device’s LAN interface. The LAN side DHCP server is updated to allow the selected PC to obtain the public IP address and public DNS server addresses on the next DHCP lease renewal.

Click on the *Disable* button to disable ZIPB again.

5.9.4 ZIPB Advanced configuration

Note: You must ensure that ZIPB is in a disabled state before you carry out any configuration changes. Once you have changed the configuration and clicked on OK, you can enable ZIPB and changes will be reflected in the configuration. Any changes made to the configuration while ZIPB is enabled will be ignored.

You can configure the following advanced settings:

LAN interface: Select the LAN interface that ZIPB will run on. Usually *Ethernet-0*.

WAN interface: Select the WAN interface that ZIPB will run on. Usually *ppp-0.*

LAN IP address spoof method: Set the LAN IP address spoof method. Once a public IP address is assigned to the LAN PC, an IP address on the same subnet as the public IP address must be created and assigned to the device's LAN interface. This option configures how the LAN interface IP address is created. Click on the *LAN IP address spoof method* drop down list and select one of the following:

Top of subnet: Selects the highest available address in the subnet

Bottom of subnet: Selects the lowest available address in the subnet

Increment: Increments the assigned IP address by 1

Manual: Uses the IP address specified in the Manual LAN IP address field.

Use PPP server address: Uses the address of your PPP server.

Manual LAN IP address: Set the manual LAN IP address only if you selected Manual as your LAN IP address spoof method.

LAN subnet mask selection method: Set the LAN subnet mask selection method. You can select one of the following methods:
Natural: Uses the subnet mask of the assigned IP address
Manual: Uses the netmask specified in the Manual LAN subnet mask field

Manual LAN subnet mask: Set the manual LAN subnet mask only if you selected *Manual* as your *LAN subnet mask selection method*.

LAN DHCP server lease time: Set the LAN DHCP server lease time duration, in seconds, of DHCP leases on the LAN.

LAN PC power down time: set the LAN PC power down time duration, in seconds, of down time before ZIPB assumes that the LAN PC has been turned off and that the user no longer needs access to the Internet.

Once you have configured ZIPB, click on the *OK* button.

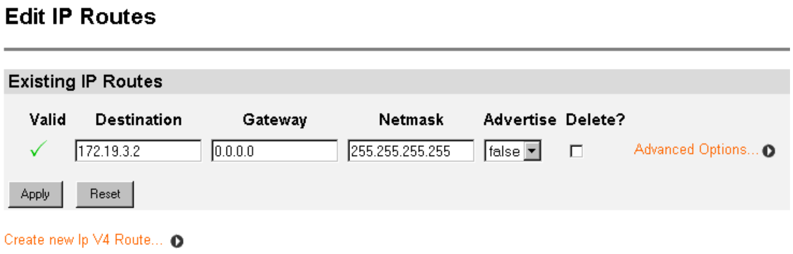
Note: that the configuration changes will not take effect until ZIPB is set to enabled. Click on the Enable button at the top of the page.

5.9.5 Limitations of ZIPB

If Dynamic ZIPB is enabled, traffic originating from your CopperJet, such as pings or one-click update requests bound for the Internet, will not receive a reply. This is because traffic will appear to come from the public IP address and will therefore always be routed back to the PC that is currently sharing the public IP address. Only responses to traffic originating from a PC on the LAN can be routed back.

5.10 IP Routes

This option allows you to create static IP routes to destination addresses via an IP interface name or a Gateway address. From the *Configuration* menu, click on *IP routes*. The *Edit Routes* page is displayed:



Edit IP Routes

Existing IP Routes

Valid	Destination	Gateway	Netmask	Advertise	Delete?	
✓	172.19.3.2	0.0.0.0	255.255.255.255	false ▾	□	Advanced Options...

This page lists the following information about existing routes:

- Whether the route is valid ✓ or invalid ✗
- Destination IP address
- Gateway address
- Netmask address

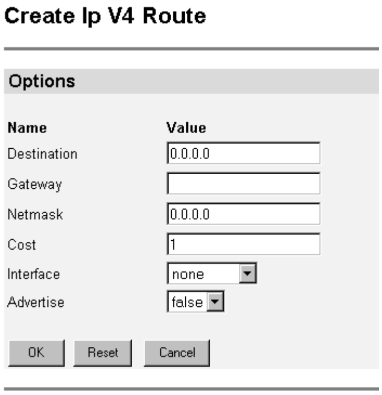
To edit the destination, gateway and netmask address of a route, click in the relevant text box, update the information then click on *Apply*.

To edit the cost and interface setting for the route, click on the *Advanced Options* hyperlink for a specific route and update the relevant information. Click on *OK*.

To delete an existing route, check the *Delete?* box for a specific route and click on *Apply*.

5.10.1 Creating an IP V4 Route

To create an IP V4 Route click on Create new IP V4 Route. The *Create new IP V4 Route* page is displayed:



Create Ip V4 Route

Options

Name	Value
Destination	0.0.0.0
Gateway	
Netmask	0.0.0.0
Cost	1
Interface	none ▾
Advertise	false ▾

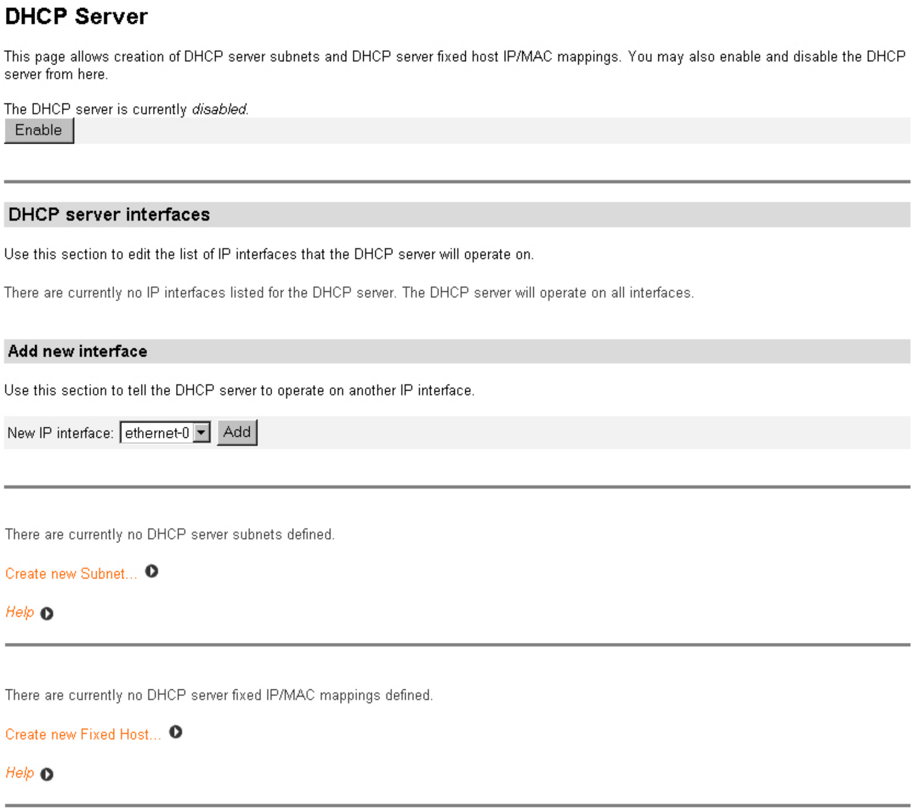
Complete the Create IP v4 Route form in order to configure the route. When you have typed the details, click on *OK*. The *Edit Routes* page is displayed. The table now contains details of the route that you have just created.

5.11 DHCP Server

DHCP allows you to dynamically assign IP address to the computers connected to the Ethernet of the CopperJet. The CopperJet allows multiple DHCP Servers for multiple IP subnets. Usually, you would only require 1 DHCP Server.

5.11.1 Configuring DHCP Server

To enable the DHCP Server, go to the *Configuration* menu and select *DHCP server*. The *DHCP Server* page is displayed.



DHCP Server

This page allows creation of DHCP server subnets and DHCP server fixed host IP/MAC mappings. You may also enable and disable the DHCP server from here.

The DHCP server is currently *disabled*.

Enable

DHCP server interfaces

Use this section to edit the list of IP interfaces that the DHCP server will operate on.

There are currently no IP interfaces listed for the DHCP server. The DHCP server will operate on all interfaces.

Add new interface

Use this section to tell the DHCP server to operate on another IP interface.

New IP interface: ethernet-0 Add

There are currently no DHCP server subnets defined.

Create new Subnet...

Help

There are currently no DHCP server fixed IP/MAC mappings defined.

Create new Fixed Host...

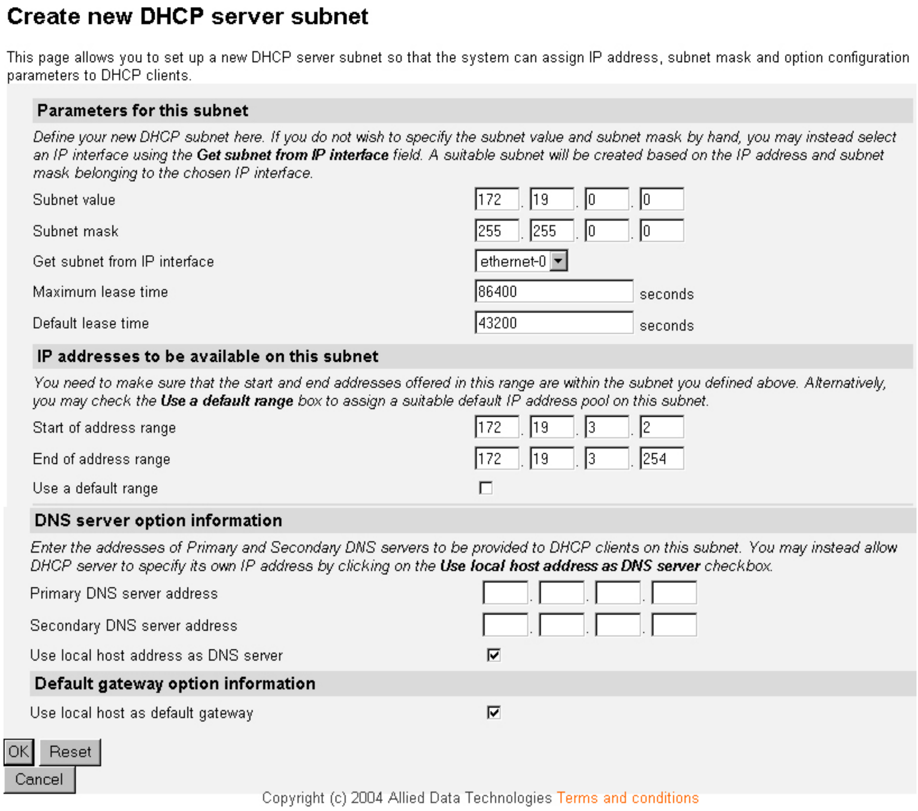
Help

Click on the *Enable* button.

By *Add new interface*, select the interface that you want to use and click on *Add*. Ethernet-0 is only available at the moment!

After you have enabled the DHCP Server (by clicking on the Enable button), you need to define a DHCP Server subnet(s).

Click on *Create new Subnet…*.
The *Create new DHCP server subnet* page is displayed.



Create new DHCP server subnet

This page allows you to set up a new DHCP server subnet so that the system can assign IP address, subnet mask and option configuration parameters to DHCP clients.

Parameters for this subnet

*Define your new DHCP subnet here. If you do not wish to specify the subnet value and subnet mask by hand, you may instead select an IP interface using the **Get subnet from IP interface** field. A suitable subnet will be created based on the IP address and subnet mask belonging to the chosen IP interface.*

Subnet value	172 . 19 . 0 . 0
Subnet mask	255 . 255 . 0 . 0
Get subnet from IP interface	ethernet-0
Maximum lease time	86400 seconds
Default lease time	43200 seconds

IP addresses to be available on this subnet

*You need to make sure that the start and end addresses offered in this range are within the subnet you defined above. Alternatively, you may check the **Use a default range** box to assign a suitable default IP address pool on this subnet.*

Start of address range	172 . 19 . 3 . 2
End of address range	172 . 19 . 3 . 254
Use a default range	□

DNS server option information

*Enter the addresses of Primary and Secondary DNS servers to be provided to DHCP clients on this subnet. You may instead allow DHCP server to specify its own IP address by clicking on the **Use local host address as DNS server** checkbox.*

Primary DNS server address	. . .
Secondary DNS server address	. . .
Use local host address as DNS server	☑

Default gateway option information

Use local host as default gateway	☑

Copyright (c) 2004 Allied Data Technologies Terms and conditions

This page allows you to:

- Set the subnet for the DHCP Server manually **OR** use the same subnet used on the IP interface by selecting *Ethernet-0*.

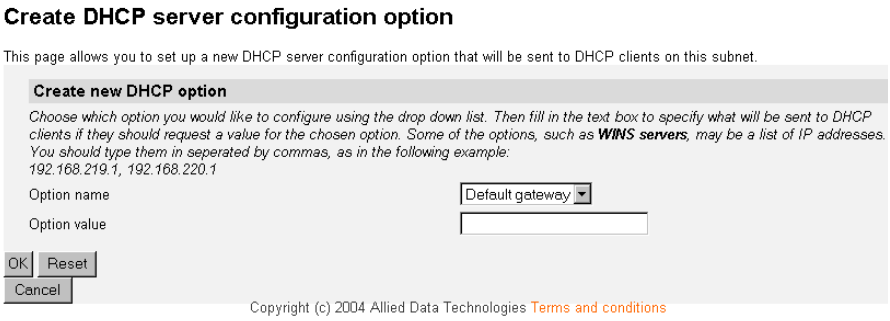
  Default lease time: If the client that requests the lease, does not ask for a specific expiry time (43200) the default time (in seconds) will be assigned to a lease.

  Max lease time: The maximum time (in seconds) that a subnet assigns to a lease if the client requesting the lease does not ask for a specific expiry time (86400).

- Set the DHCP address range manually **OR** use a default range of 253 addresses by selecting *Use Default Range*.
- Set your CopperJet to give out its own IP address as the DNS Server address **OR** manually set the primary and secondary DNS Server addresses. When *Use Router as DNS* Server is selected, DNS Relay will be enabled.
- Set your CopperJet to give out its own IP address as the default Gateway address. In most situations this is enabled.

Once you have entered new configuration details for your DHCP server, click on *OK*.
You will return to the DHCP Server page. The DHCP Server subnet is now added. To delete the DHCP Server subnet mark the box *Delete?* and click on *Apply*.

For advanced options click on the *Advanced Options…* hyperlink. This allows you to edit all of the values that were set when the subnet was created. At the bottom of the page, click on the *Create new DHCP option* link. The *Create DHCP server configuration option* page is displayed:



Create DHCP server configuration option

This page allows you to set up a new DHCP server configuration option that will be sent to DHCP clients on this subnet.

Create new DHCP option

*Choose which option you would like to configure using the drop down list. Then fill in the text box to specify what will be sent to DHCP clients if they should request a value for the chosen option. Some of the options, such as **WINS servers**, may be a list of IP addresses. You should type them in seperated by commas, as in the following example: 192.168.219.1, 192.168.220.1*

Option name: Default gateway

Option value:

Copyright (c) 2004 Allied Data Technologies Terms and conditions

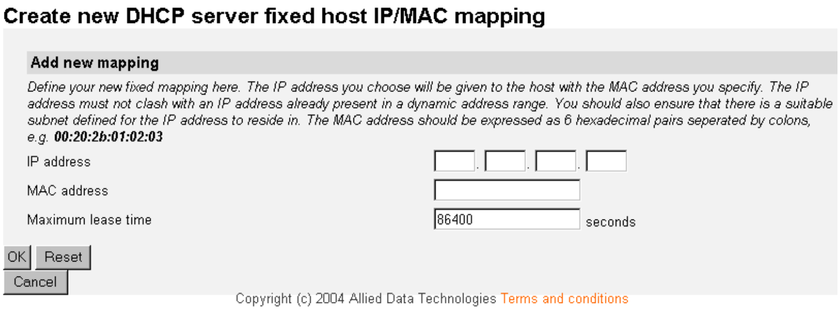
Click on the *Option name* drop-down list and select a name. Type a value that matches the selected option name in the *Option value* text box. Click on *OK*.

The *Edit DHCP server subnet* page is displayed, and details of your new option are displayed under the sub-heading *Additional option information*. To delete an existing option, check the *Delete?* box for a specific option and click *OK*.

Go to the *Configuration* menu and click on *Save config* to save the new settings into the CopperJet.

5.11.2 Creating a fixed host

To create a fixed host click on *Create new Fixed Host…*. The *Create new DHCP server fixed host IP/MAC mapping* page is displayed.



Create new DHCP server fixed host IP/MAC mapping

Add new mapping

*Define your new fixed mapping here. The IP address you choose will be given to the host with the MAC address you specify. The IP address must not clash with an IP address already present in a dynamic address range. You should also ensure that there is a suitable subnet defined for the IP address to reside in. The MAC address should be expressed as 6 hexadecimal pairs seperated by colons, e.g. **00:20:2b:01:02:03***

IP address: . . .

MAC address:

Maximum lease time: 86400 seconds

Copyright (c) 2004 Allied Data Technologies Terms and conditions

Complete the following:

1 Type in the IP address that will be given to the host with the specified MAC address.

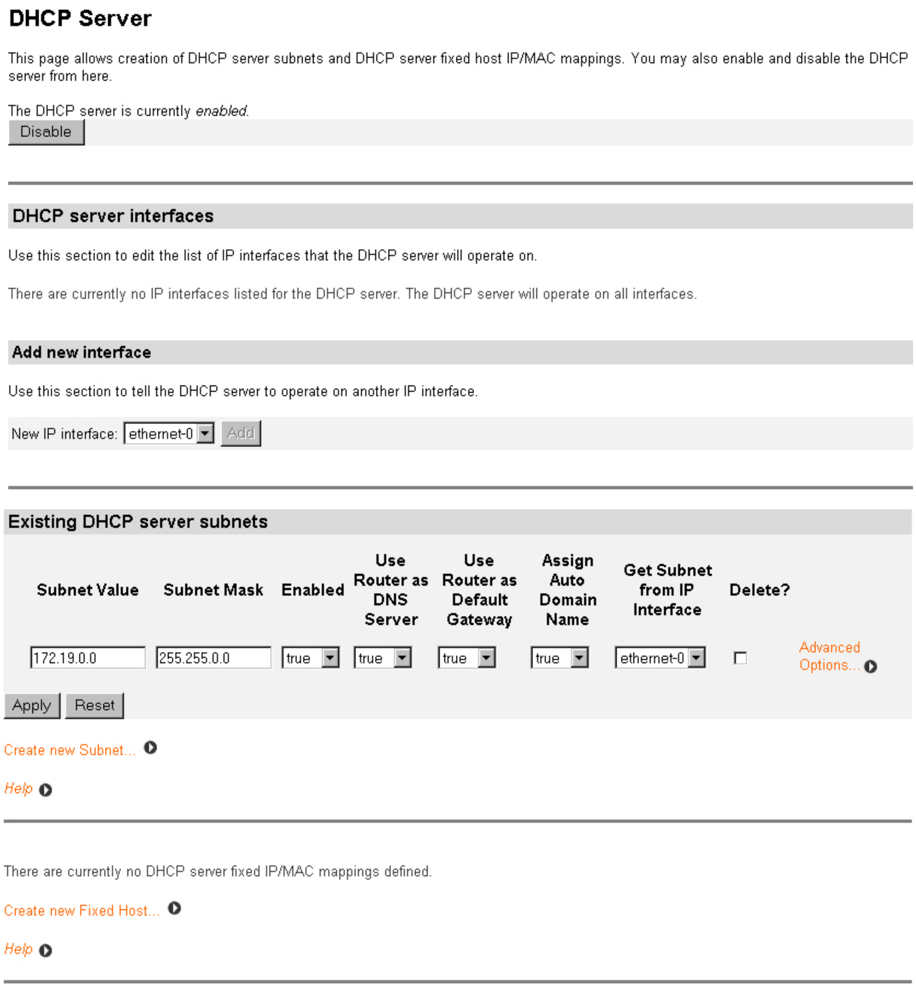
2 Type in the MAC address and the maximum lease time (default is 86400 seconds).

3 Click on *OK*. The *DHCP Server* page is displayed, and details of your new fixed host are displayed under the sub-heading *Existing DHCP fixed IP/MAC mappings*. To edit a fixed mapping, click on the IP address, MAC address or max lease time, type a new entry and click *Apply*. To delete a fixed mapping, check the *Delete?* Box for a specific mapping and click *Apply*.

Go to the *Configuration* menu and click on *Save config* to save the new settings into the CopperJet.

5.11.3 Disabling DHCP Server

To disable the DHCP Server, go to the *Configuration* menu and select *DHCP server*. The *DHCP Server* page is displayed.



DHCP Server

This page allows creation of DHCP server subnets and DHCP server fixed host IP/MAC mappings. You may also enable and disable the DHCP server from here.

The DHCP server is currently *enabled*.

DHCP server interfaces

Use this section to edit the list of IP interfaces that the DHCP server will operate on.

There are currently no IP interfaces listed for the DHCP server. The DHCP server will operate on all interfaces.

Add new interface

Use this section to tell the DHCP server to operate on another IP interface.

New IP interface: ethernet-0

Existing DHCP server subnets

Subnet Value	Subnet Mask	Enabled	Use Router as DNS Server	Use Router as Default Gateway	Assign Auto Domain Name	Get Subnet from IP Interface	Delete?	
172.19.0.0	255.255.0.0	true	true	true	true	ethernet-0	□	Advanced Options...

Create new Subnet...

Help

There are currently no DHCP server fixed IP/MAC mappings defined.

Create new Fixed Host...

Help

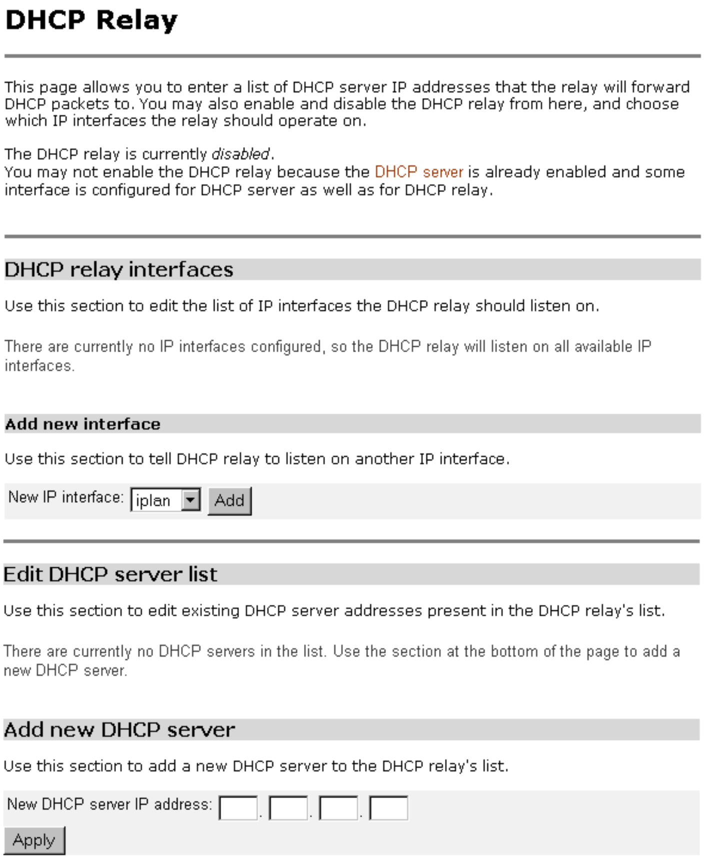
Click on the *Disable* button.
The DHCP Server is now disabled.

Go to the *Configuration* menu and click on *Save config* to save the new settings into the CopperJet.

5.12 Configuring DHCP Relay

DHCP Relay provides a means for relaying DHCP and BOOTP requests from a subnet to which no DHCP server is directly connected to one or more DHCP servers on other subnets. The DHCP Relay Agent listens for DHCP and BOOTP queries and responses. When a query is received from a client, DHCP Relay forwards it to the list of DHCP servers specified. When a reply is received from a server, it is broadcast or unicast (according to the client's request) on the network from which the original request came.

From the *Configuration* menu, click on *DHCP relay*. The *DHCP Relay* page is displayed:



DHCP Relay

This page allows you to enter a list of DHCP server IP addresses that the relay will forward DHCP packets to. You may also enable and disable the DHCP relay from here, and choose which IP interfaces the relay should operate on.

The DHCP relay is currently *disabled*.
You may not enable the DHCP relay because the DHCP server is already enabled and some interface is configured for DHCP server as well as for DHCP relay.

DHCP relay interfaces

Use this section to edit the list of IP interfaces the DHCP relay should listen on.

There are currently no IP interfaces configured, so the DHCP relay will listen on all available IP interfaces.

Add new interface

Use this section to tell DHCP relay to listen on another IP interface.

New IP interface: iplan

Edit DHCP server list

Use this section to edit existing DHCP server addresses present in the DHCP relay's list.

There are currently no DHCP servers in the list. Use the section at the bottom of the page to add a new DHCP server.

Add new DHCP server

Use this section to add a new DHCP server to the DHCP relay's list.

New DHCP server IP address: _ . _ . _ . _

5.12.1 Enabling / disabling DHCP relay

Click on the *Enable/Disable* button at the top of the page. If you click on the *Disable* button, DHCP server is disabled and the button changes to *Enable*.

Note: The Enable/Disable button is only visible when the DHCP Server of the CopperJet is disabled. DHCP Relay only works when the DHCP Server is disabled.

5.12.2 Configuring DHCP relay on specific interfaces

You can configure DHCP relay to run on one or more specific interfaces. By default, once enabled, DHCP relay operates on all available IP interfaces. You may set DHCP relay to run on one of your LAN interfaces and the WAN interface, so that it can listen for replies from a DHCP server at your ISP. This allows you to set DHCP server to run on a different interface at the same time.

To specify an interface for DHCP relay to run on:

1. Click on the *New IP interface* drop-down list and select an interface.
2. Click *Add*.

5.12.3 Adding a DHCP server to the DHCP relay list

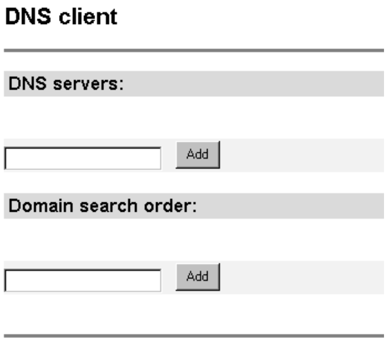
1 In the *Add new DHCP server* section, type an address in the *New DHCP server IP address* text box.
2 Click *Apply*. The address is displayed in the *Edit DHCP server list* section.

5.12.4 Editing/deleting entries in the DHCP relay list

1 To edit an entry, click on an IP address and type a new entry, then click *Apply*.
2.To delete an entry, check the *Delete?* box for a specific IP address, then click *Apply*.

5.13 Configuring DNS client

The DNS client enable the CopperJet to resolve IP addresses from external DNS Servers. To manually configure DNS client, go to the *Configuration* menu and select *DNS client*. The *DNS client* page is displayed:



5.13.1 Configuring DNS servers

1 Type the IP address of the unknown domain name in the *DNS servers:* text box.

2 Click *Add*. The IP address appears in the DNS servers table. You can add a maximum of three server IP addresses. Each IP address entry has a *Delete* button associated with it. Click on *Delete* to remove an IP address from this list.

5.13.2 Configuring DNS search domains

1 Type a search string in the *Domain search order:* text box.

2 Click *Add*. The search string is displayed in the *Domain search order* table. You can add a maximum of six search strings. Each search string entry has a *Delete* button associated with it. Click on *Delete* to remove a string from this list.

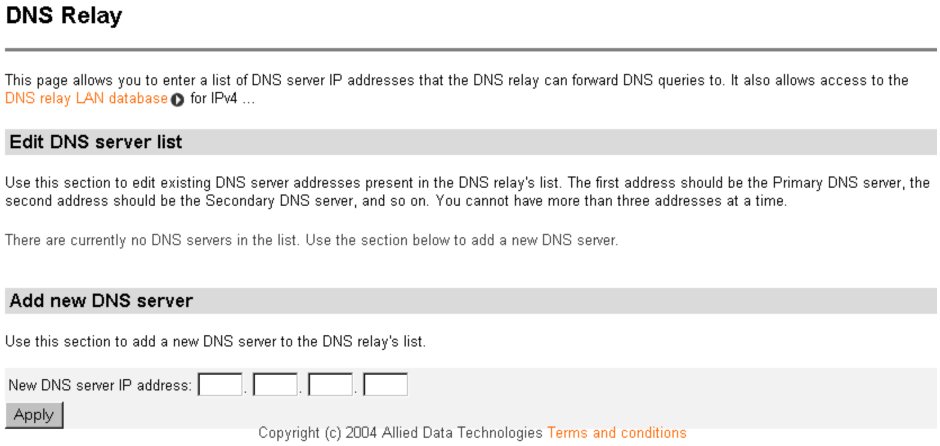
5.14 Configuring DNS Relay

DNS Relay allows you to send DNS requests to the CopperJet instead of the DNS servers at the service provider. The CopperJet relays these requests to specified DNS Servers.

The DNS servers can be discovered automatically through DHCP on the WAN interface **OR** configured manually.

5.14.1 Configuring DNS Relay manually

To manually configure DNS Relay, go to the *Configuration* menu and select *DNS relay*. The *DNS Relay* page is displayed:



DNS Relay

This page allows you to enter a list of DNS server IP addresses that the DNS relay can forward DNS queries to. It also allows access to the DNS relay LAN database for IPv4 ...

Edit DNS server list

Use this section to edit existing DNS server addresses present in the DNS relay's list. The first address should be the Primary DNS server, the second address should be the Secondary DNS server, and so on. You cannot have more than three addresses at a time.

There are currently no DNS servers in the list. Use the section below to add a new DNS server.

Add new DNS server

Use this section to add a new DNS server to the DNS relay's list.

New DNS server IP address: [ ] . [ ] . [ ] . [ ]

Apply

Copyright (c) 2004 Allied Data Technologies Terms and conditions

Fill in the required DNS address and click on *Apply*. You will now see that the DNS address is added. To delete the DNS address mark the box *Delete?* and click on *Apply*. Click *Reset* to undo your selection.

When finished configuring DNS Relay, go to the *Configuration* menu and click on *Save config* to save the new settings into the CopperJet.

Note: You need to fill in the CopperJet IP address as DNS server on your network card or configure the DHCP Server and enable the setting: Use Router as DNS Server.

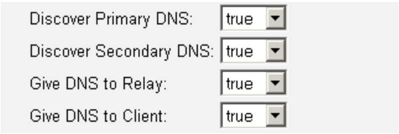
5.14.2 Automatically discover DNS Relay addresses

For configuring the automatic discovery of DNS addresses, a WAN Connection need to be configured. See section *5.6 WAN Connections* for configuring WAN connections.

For both PPPoA and PPPoE connections, the CopperJet can discover the DNS addresses automatically. The service provider will provide the DNS addresses through DHCP. In this situation, there is no need to configure DNS Relay manually. Go to the *Configuration* menu and select *WAN Connections*. The WAN connections that are defined are displayed. Edit the preferred WAN connection by selecting *Edit*. The *WAN connection* page is displayed.

For PPPoA, select the *PPP* tab. For PPPoE, select the *PPPoE* tab.

Be sure that following options are set to **true** if you want the CopperJet to automatically discover the DNS addresses.



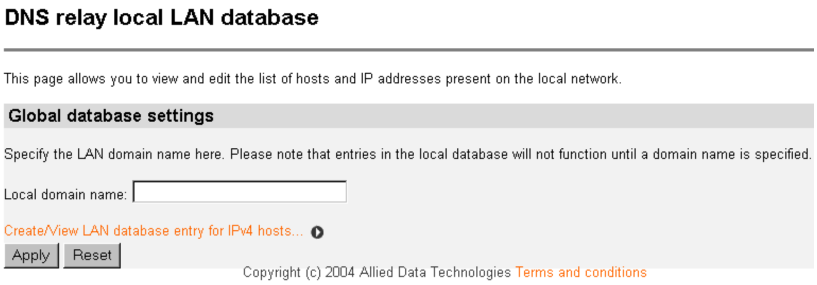
Discover Primary DNS:	true
Discover Secondary DNS:	true
Give DNS to Relay:	true
Give DNS to Client:	true

When you are finished with configuring DNS Relay for the WAN connection, click on *Apply.* Go to the *Configuration* menu and click on *Save config* to save the new settings into the CopperJet.

Note: You need to fill in the CopperJet IP address as DNS address on your network card or configure the DHCP Server and enable the setting: Use Router as DNS Server.

5.14.3 Configuring DNS relay LAN database

The LAN database lists details about local host names and IP addresses which DNS relay uses to determine if a query is for local host information. To configure the database click on *DNS relay LAN database*. The *DNS relay local LAN database* page is displayed:



DNS relay local LAN database

This page allows you to view and edit the list of hosts and IP addresses present on the local network.

Global database settings

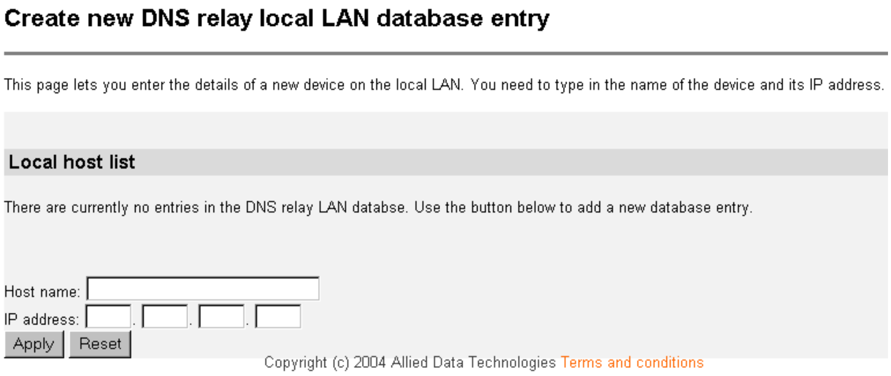
Specify the LAN domain name here. Please note that entries in the local database will not function until a domain name is specified.

Local domain name:

Copyright (c) 2004 Allied Data Technologies Terms and conditions

To set the LAN domain name, type a domain name in the *Local domain name* text box. This is used by DNS relay to determine if a host name request is for the local database.

To create a new local host entry; click on *Create/View LAN database entry for Ipv4 hosts*. The *Create new DNS relay local LAN database entry* page is displayed.



Create new DNS relay local LAN database entry

This page lets you enter the details of a new device on the local LAN. You need to type in the name of the device and its IP address.

Local host list

There are currently no entries in the DNS relay LAN databse. Use the button below to add a new database entry.

Host name:

IP address: . . .

Copyright (c) 2004 Allied Data Technologies Terms and conditions

Type the host name and IP address in the relevant text boxes and click on *Apply*. The *DNS relay local LAN database* page is displayed. To view the local host(s), click on *Create/View LAN database entry for Ipv4 hosts.*

Configure an existing local host entry; type in the relevant *Host name* and/or *IP address* box(es) and click *Apply*. Delete an existing local host entry; check the corresponding *Delete?* Box and click *Apply*.

To configure/add aliases for an existing local host, click on the corresponding *Extra host names and IP addresses list* link. The displayed page allows you to:

1) Create a new host name and/or IP address aliases. Type a new name and/or IP address in the relevant *Enter new alias* text box and click *Apply*.

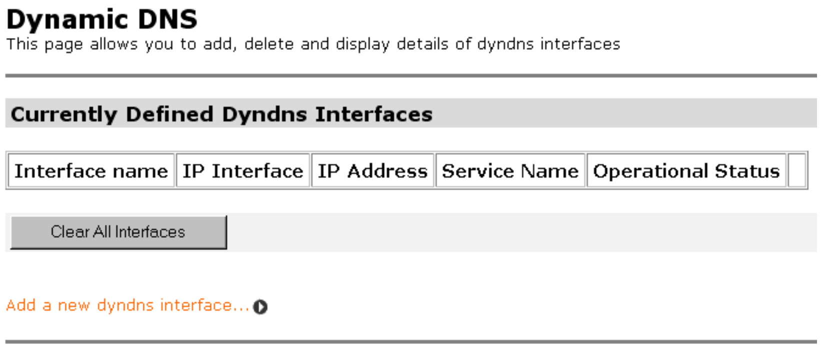
2) Configure an existing host name and/or IP address aliases. Type a new name and/or IP address in the relevant text box and click *Apply*.

3) Delete an existing host name or IP address aliases. Check the corresponding *Delete?* box and click *Apply*.

5.15 Configuring Dynamic DNS Client (DynDNS Client)

If some host has a dynamic IP address that keeps changing frequently, it is difficult to keep updating the IP record that is associated with the domain name of this host in the zone files. This will result in non-accessibility of this host on the Internet. Dynamic DNS service allows to keep mapping of a dynamic IP address of such host to a static hostname. Dynamic DNS services are provided by many websites. The host needs to register with some website and get a domain name. When the IP address of the host changes, it just needs to send a message to the website that's providing dynamic DNS service to this host. For this to work, an automated update client needs to be implemented. These update clients send update messages to the servers whenever there is some change in the IP address of that host. Then, the server updates the entries for that host and replies back with some return code.

To configure the Dynamic DNS Client settings, go to *Configuration* menu and click on *DynDNS client*. The *Dynamic DNS* page is displayed.



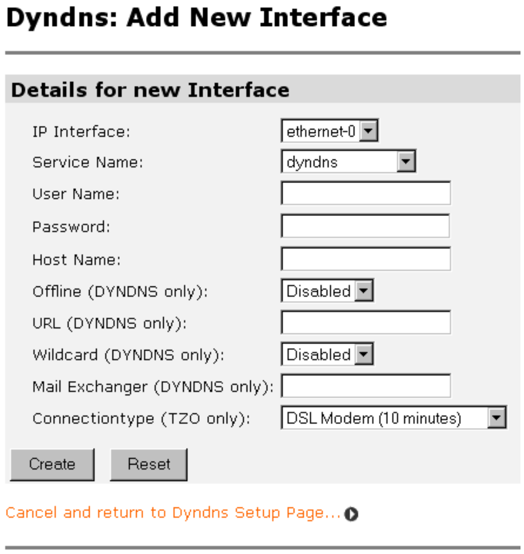
Dynamic DNS

This page allows you to add, delete and display details of dyndns interfaces

Currently Defined Dyndns Interfaces

Interface name	IP Interface	IP Address	Service Name	Operational Status	

On this page you can see the defined DynDNS interfaces.
To add a new DynDNS interface, click on the link *Add a new dyndns interface….*
The Dyndns: Add New Interface page is displayed.



Dyndns: Add New Interface

Details for new Interface

IP Interface:	ethernet-0
Service Name:	dyndns
User Name:	
Password:	
Host Name:	
Offline (DYNDNS only):	Disabled
URL (DYNDNS only):	
Wildcard (DYNDNS only):	Disabled
Mail Exchanger (DYNDNS only):	
Connectiontype (TZO only):	DSL Modem (10 minutes)

This page allows you to:

IP Interface: This parameter is the interface name of the public interface for which this entry defines the Dynamic DNS profile.

Service Name: This parameter represents the name of the Dynamic DNS service provider where you have registered and the type of service. This parameter accepts these values: dyndns, dyndnscustom, dyndns-static, and tzo.

User Name: Username registered at service provider. tzo requires mail ID as the username.

Password: Password provided by service provider.

Host Name: This is the hostname that you specified while registering with your service provider. This hostname remains fixed, while the IP address mapping to this hostname changes.

Note: Only one hostname is allowed per Dynamic DNS interface.

Offline (DYNDNS only): If enabled, the service provider redirects browsers to its own site if the registered host is currently offline.

URL (DYNDNS only): Specifies the URL of the host.

Wildcard (DYNDNS only): Specifies whether Wildcard aliases are to be resolved or not.

Mail Exchanger (DYNDNS only): Specifies a Mail Exchanger (MX) to which the records for a specific domain have to be mailed.

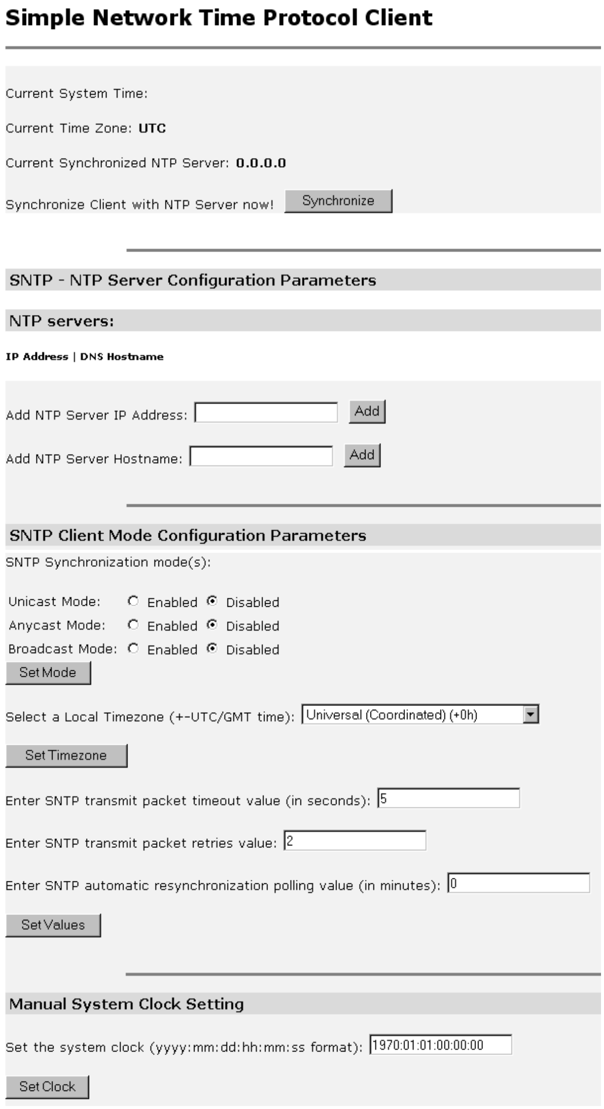
Connectiontype (TZO only): Specifies the kind of connectivity the host has, such as LAN, Cable modem, or Dial-up modem. This sets the cache time for the hostname at TZO.

Note: Before using DYNDNS, you need to be registered to a Dynamic Service Provider. At the moment 2 Dynamic DNS Service Providers are supported (www.tzo.com, www.dyndns.com).

5.16 Configuring Simple Network Time Protocol (SNTP) Client

Configuring your device as an SNTP client allows you to obtain accurate time/date information from an associated SNTP server. If you are not attached to an SNTP server, you can set the time/date on your own device instead.

To configure the SNTP Client settings, go to *Configuration* menu and click on *SNTP client.* The *SNTP client* page is displayed.



Simple Network Time Protocol Client

Current System Time:

Current Time Zone: **UTC**

Current Synchronized NTP Server: **0.0.0.0**

Synchronize Client with NTP Server now! [Synchronize]

SNTP - NTP Server Configuration Parameters

NTP servers:

IP Address | DNS Hostname

Add NTP Server IP Address: [ ] [Add]

Add NTP Server Hostname: [ ] [Add]

SNTP Client Mode Configuration Parameters

SNTP Synchronization mode(s):

Unicast Mode: ○ Enabled ● Disabled
Anycast Mode: ○ Enabled ● Disabled
Broadcast Mode: ○ Enabled ● Disabled

[Set Mode]

Select a Local Timezone (+-UTC/GMT time): Universal (Coordinated) (+0h)

[Set Timezone]

Enter SNTP transmit packet timeout value (in seconds): 5

Enter SNTP transmit packet retries value: 2

Enter SNTP automatic resynchronization polling value (in minutes): 0

[Set Values]

Manual System Clock Setting

Set the system clock (yyyy:mm:dd:hh:mm:ss format): 1970:01:01:00:00:00

[Set Clock]

This page displays the default SNTP Client settings:

- Universal Time Coordinate (UTC), with no SNTP server set or synchronized to
- Synchronization mode disabled.
- Received packet response timeout value set to 5 seconds, and retry value set to 2.

To configure SNTP:

1 At the NTP servers section, add the NTP server that you want your client to obtain information from.

2 At the SNTP Client Mode Configuration Parameters section, select the SNTP Synchronization mode(s) by clicking on the Unicast Mode Enabled, Anycast Mode Enabled or the Broadcast Mode Enabled radio button. Click Set Mode.

3 If you enabled unicast mode in the previous step, you can set the dedicated unicast server by either IP address or hostname. At the SNTP Server Configuration Parameters section of the page, enter the IP Address or Hostname and click on the corresponding button.

4 At the SNTP Client General Configuration Parameters section:

- Click on the relevant entry from the Select a New Local Timezone drop-down list. Click Set New Timezone.
- Edit the transmit packet timeout value, retry value and/or a new resynchronization polling value by typing a new value in the corresponding text box(es). Click Set New Values.

5 To set the clock to a specific time and date without having to synchronize with a local system clock, enter the required time and date and click Set Clock.

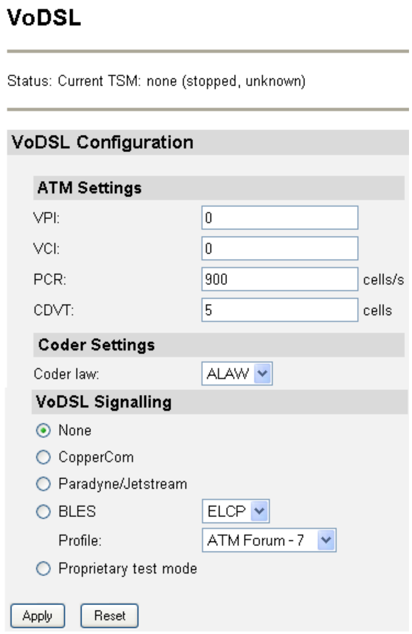
6 To synchronize the local time with the SNTP server using the mode previously selected, go to the top of the page and click Synchronize.

5.17 Configuring Voice over DSL

Basic configuration of the Voice over DSL (VoDSL) settings in the CopperJet Integrated Access Device (IAD) can be done through the WebServer Interface. Advanced configuration can only be done through TELNET.

5.17.1 Basic VoDSL Settings

To configure the basic Voice over DSL settings, go to *Configuration menu* and click on *VoDSL*. The *VoDSL* page is displayed.



VoDSL

Status: Current TSM: none (stopped, unknown)

VoDSL Configuration

ATM Settings

VPI: 0

VCI: 0

PCR: 900 cells/s

CDVT: 5 cells

Coder Settings

Coder law: ALAW

VoDSL Signalling

● None

○ CopperCom

○ Paradyne/Jetstream

○ BLES ELCP

Profile: ATM Forum - 7

○ Proprietary test mode

You need to add configuration information for VoDSL. This information must be provided by your Voice over DSL service provider.

VPI: Virtual Path Identifier. A field in the ATM header. The VPI is used to identify the virtual path that a circuit belongs to. The VPI can be any value between 0 and 4095.

VCI: Virtual Channel Identifier. Part of the ATM header. The VCI is a tag that identifies which channel a cell will travel over. The VCI can be a value between 1 and 65535.

Coder Law: ALAW is in general meant for Europe.
ULAW is in general meant for the US.

None: There is no VoDSL signaling configured.

CopperCom: CopperCom proprietary VoDSL signaling.

Paradyne/Jetstream: Paradyne/Jetstream proprietary VoDSL signaling.

BLES: BLES VoDSL signaling.

ELCP: *ELCP* is a standard protocol that specifies the mechanism where V5.2-based signaling messages are exchanged between the VoDSL Gateway and IAD to support both POTS (plain old telephone system) and ISDN voice over ATM.

CAS: *Channel Associated Signaling (CAS)* is used in bit-based schemes where dedicated signaling bandwidth is required for every connection.

Profile: Select ITU-T (voice over AAL2) or ATM-Forum (AF–voice traffic over ATM (VTOA)). Profile Source and Identifier are only used for BLES signalling (both CAS and ELCP). For voice gateways with an ADPCM only mode (for all UUI values 0..15) the special atmforum profile number 13 is used.

Proprietary test mode: This mode enables the internal PBX functionality for testing the Voice ports.
Voice port 1: number 101
Voice port 2: number 102
Voice port 3: number 103
Voice port 4: number 104

When finished configuring VoDSL, click on *Apply.* Go to the *Configuration* menu and click on *Save config* to save the new settings into the CopperJet.

5.17.2 Advanced Voice over DSL Configuration

Configuration of advanced Voice over DSL settings in the CopperJet IAD’s is done through TELNET. To access the TELNET configuration mode, start a TELNET session from your computer (i.e. `TELNET <ip-address>`) and enter your username and password (default username and password are **admin, admin**). To access the advanced settings enter the following commands:

```
console enable [enter]
iad [enter]
```

The prompt has changed into `<ip-address> iad>`.

5.17.2.1 Flash on hook timing

Because the requirements of flash on hook timing differ a lot per country, the minimum and maximum hook flash time can be configured.

Syntax:`flashmin <value>`

Minimum flash-on-hook time in milliseconds after a hook-flash is detected. Below this value no flash nor hook state change is detected.

Syntax:`flashmax <value>`

Maximum flash-on-hook time in milliseconds before a hook flash is detected. Above this value a hook state change is detected.

Note: that if flashmax < flashmin, hook flash detection is disabled. Flashmin can be used to set the minimum time a hook state change is detected.

Example: to set the minimum flash-on-hook timing to 60 milliseconds enter the following command:

```
flashmin 60 [enter]
```

Example: to set the maximum flash-on-hook timing to 200 milliseconds enter the following command:

```
flashmax 200 [enter]
```

5.17.2.2 Initial ring timing for CLIP

Because the requirements of the initial ring timing differ a lot per country, the initial ring time can be configured.

Syntax:initring <value>

Time in ms the phone will ring. After the ring is finished the End-of-pulse information element will be send within a SIGNAL message to the CO.

Example: to set the initring value to 250 milliseconds enter the following command:

```
initring 250 [enter]
```

5.17.2.3 Network Time Reference Clock

Syntax:pcmclk <value>

<value> can be one of the following:

network	Use network as time reference.
networkcor	Use network as time reference with automatic correction
local	Use local/onboard oscillator as time reference.

Example: to set the internal clock reference to NTR enter the following command:

```
pcmclk network [enter]
```

5.17.2.4 Ring cadence configuration support

Because the requirements for ring cadences differ per country, a list of ring cadences can be configured.

Syntax:
cadence <id>,<make1>,<break1>,<make2>,<break2>,<make3>,<break3>

<id> The index number of the ringing pattern. This must equal the cadence number send by V5 in case of ELCP. See also *5.17.2.5 Define Cadences*. Each ringing pattern must have a unique id.

<makeX> Time in milli seconds the phone is ringing.
<breakX> Time in milli seconds the phone is silent.

```
-make 1-|         |-make 2-|           |-make 3-|          |- make 1|
        |         |        |           |        |          |        |
        |-break 1-|        |-break 2- |         |-break 3- |        |-
```

If the second or third period is not used, specify 0 as the make/break values for the first unused period.

Note: that it is not possible to specify 0 for make2/break2 and a non zero value for make3/break3.

A ringing pattern with make2/break2 and make3/break3 equal 0 would look like this:

```
-make 1-|         |-make 1-|           |-make 1-|          |- make 1|
        |         |        |           |        |          |        |
        |-break 1-|        |-break 1- |         |-break 1- |        |-
```

Example: to set the ring cadences enter the following commands:

```
cadence 0,2000,4000,0,0,0,0 [enter]
cadence 1,800,400,800,4000,0,0 [enter]
cadence 2,400,200,400,200,800,4000 [enter]
cadence 3,300,200,1000,200,300,4000 [enter]
cadence 4,500,5500,0,0,0,0 [enter]
```

5.17.2.5 Define Cadences

Syntax: `defcadence <id>`

Specify the id that is used as default ring cadence from the cadence table.
In case of CAS signalling: The default cadence id is used at all times. In case of ELCP signalling: If the id, sent by the V5 network, is not found in the cadence table, the default id is used.

Note: that if the default cadence id does not exist in the table, id 0 is used.

5.17.2.6 Echo Cancellation

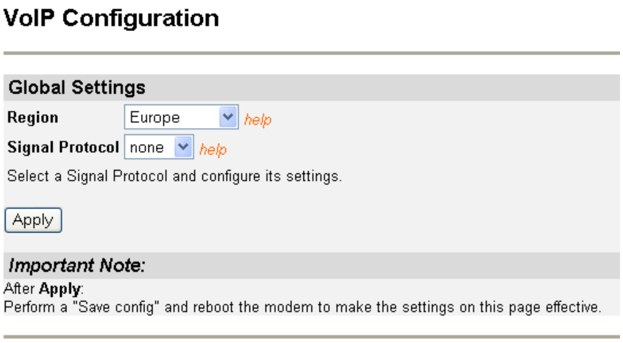
The IAD complies with G.168:
The echo cancellers covered by this Recommendation should be equipped with a tone detector that conforms to this sub clause. This tone detector should disable the echo canceller only upon detection of a signal which consists of a 2100 Hz tone with periodic phase reversals inserted in that tone, and not disable with any other in-band signal, e.g., speech, or a 2100 Hz tone without phase reversals. The tone disabler should detect and respond to a disabling signal which may be present in either the send or the receive path.

The IAD is detecting the tone in both directions. The Phone LED indicates the status of the echo canceller:
Stays ON continuously, echo canceller is ON in both directions.
600ms ON 100ms OFF the echo canceller is OFF in one direction.
1600ms ON 100ms OFF the echo canceller is OFF in both directions.

5.18 Configuring VoIP

VoIP enables telephone calls to be made over an IP network. This enables DSL Service providers to sell telephone services over DSL to customers without the expense of providing any extra physical connections to the consumer, or network infrastructure in addition to their existing IP network.

From the *Configuration* menu, go to *VoIP*. The *VoIP Configuration* page is displayed.



VoIP Configuration

Global Settings

Region Europe help

Signal Protocol none help

Select a Signal Protocol and configure its settings.

Important Note:

After **Apply**:
Perform a "Save config" and reboot the modem to make the settings on this page effective.

Select the Caller ID Region that applies to your country.

Available regions are:

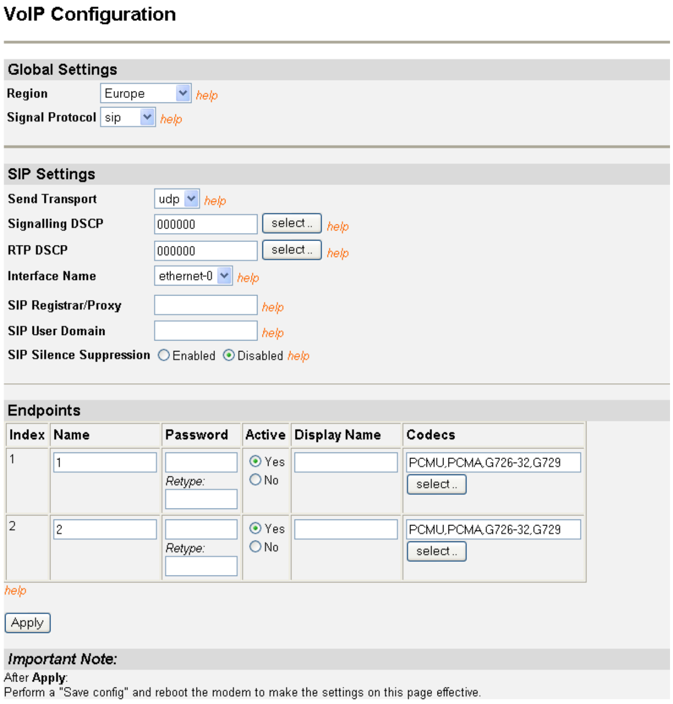
- US
- JAPAN
- UK
- China
- Europe
- Netherlands

When you select a Signal Protocol (SIP or MGCP) and click on the *Apply* button, the necessary fields for that protocol comes available.
You can select SIP or MGCP. For configuring SIP, go to section *5.18.1 Configuring VoIP using SIP.* For configuring MGCP, go to section *5.18.2 Configuring VoIP using MGCP*.

5.18.1 Configuring VoIP using SIP

SIP stands for Session Initiation Protocol (SIP), an application-layer control (signalling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions can include Internet telephone calls, multimedia distribution, and multimedia conferences.

When you select *SIP*, as Signal Protocol, the *SIP Configuration* page is displayed.



VoIP Configuration

Global Settings

Region: Europe help
Signal Protocol: sip help

SIP Settings

Send Transport: udp help
Signalling DSCP: 000000 select.. help
RTP DSCP: 000000 select.. help
Interface Name: ethernet-0 help
SIP Registrar/Proxy: help
SIP User Domain: help
SIP Silence Suppression: ○ Enabled ● Disabled help

Endpoints

Index	Name	Password	Active	Display Name	Codecs
1	1	Retype:	● Yes ○ No		PCMU,PCMA,G726-32,G729 select..
2	2	Retype:	● Yes ○ No		PCMU,PCMA,G726-32,G729 select..

help

Apply

Important Note:
After **Apply**:
Perform a "Save config" and reboot the modem to make the settings on this page effective.

You need to add detailed configuration information about the SIP service that you are creating. This information must be provided by your service provider.

Send Transport: Udp is selected by default. This option is used to configure the default transport used for outgoing SIP INVITE requests. It is not directly related to *tcpPort* and *udpPort* settings used by SIP and MGCP.

Signalling DSCP: This option is used to set QoS characteristics for signalling packets. See section *5.18.1.1 Configuring Signalling DSCP and RTP DSCP.* how to configure.

RTP DSCP: This option is used to set QoS characteristics for RTP data packets. See section *5.18.1.1 Configuring Signalling DSCP and RTP DSCP* how to configure.

Interface Name: Interface name of CopperJet which finds the SIP Proxy Server.

SIP Registrar/Proxy: This option is used to identify the IP domain for the SIP Proxy server. The domain can be:

- IP address – Of the SIP Registrar/Proxy.
- IP Domain name - The domain name should be a FQDM (Fully Qualified Domain name).

SIP User Domain: This option is used to set the SIP user domain. The domain can be:

- IP address - for example, 192.168.1.1

- IP Domain name - The domain name should be a FQDM (Fully Qualified Domain name).

SIP Silence Suppression: This command enables or disables Silence Suppression. Silence suppression controls the silence suppression insertion in the voice data samples.

Endpoints:

Index: An index value that identifies the endpoint.

Name: A name for the endpoint.

Password: This command sets a password to be associated with an endpoint.

Active: By default Yes. *Yes* endpoint is Active. *No* and endpoint is not Active.

Display Name: The display name for the endpoint. The name must only be composed of alphanumeric characters.

Codecs: This command specifies the codec types which can be used to compress the Voice packets from the endpoint specified.
The codecs are listed in order of preference to be used for a phone call. The endpoint will negotiate with the other end to choose a codec which they can both use.

Voice codec support:

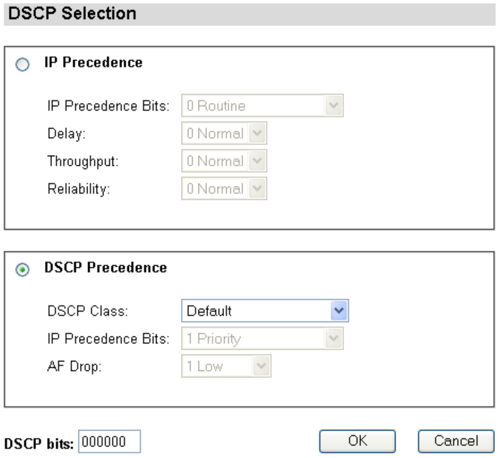
- G.711 (A-Law and μ−Law),
- G.726 (32kb) and
- G.729 a/b

After the correct settings are filled in, click on *Apply*. Go to the *Configuration* menu and click on *Save config* to save the new settings into the CopperJet. SIP is only active after a restart of the CopperJet. To Restart the CopperJet, go to *System -> Restart* and click on the *Restart* button.

5.18.1.1 Configuring Signalling DSCP and RTP DSCP

This option is used to set QoS characteristics for signalling packets. It sets the DSCP (Differentiated Services Code Point) in the IP header. This is a 6-bit value that is used to select the per-hop behavior (PHB) to be applied to a signalling packet when it is forwarded. The six most significant bits of the DiffServ field is called as the DSCP (Differentiated Services Code Point).

To configure the Signalling DSCP, click on the *Select…* button. The *DSCP Selection* page is displayed.



DSCP Selection

○ IP Precedence

IP Precedence Bits: 0 Routine
Delay: 0 Normal
Throughput: 0 Normal
Reliability: 0 Normal

● DSCP Precedence

DSCP Class: Default
IP Precedence Bits: 1 Priority
AF Drop: 1 Low

DSCP bits: 000000

IP Precedence:

IP Precedence Bits: Default "0-Routine". An independent measure of the importance of this datagram. You can select:

- 0-Routine
- 1-Priority
- 2-Immediate
- 3-Flash
- 4-Flash Override
- 5-CRITIC/ECP
- 6-Internetwork Control
- 7-Network Control

Delay: Default "0-Normal". Prompt delivery is important for datagrams with this indication. You can select:

- 0-Normal
- 1-Low

Throughput: Default "0-Normal". High data rate is important for datagrams with this indication. You can select:

- 0-Normal
- 1-High

Reliability: Default "0-Normal". A higher level of effort to ensure delivery is important for datagrams with this indication. You can select:

- 0-Normal
- 1-High

DSCP Precedence:

DSCP Class: Default value is 'Default". Set the DSCP field in packet header to the value represented by the DiffServ class value. This class may be EF, BE or any of the CSxx or AFxx classes. You can select:

- Match IP Precedence
- Assured Forwarding 1
- Assured Forwarding 2
- Assured Forwarding 3
- Assured Forwarding 4
- Expedited Forwarding
- Default

IP Precedence Bits: Default "0-Routine". An independent measure of the importance of this datagram. You can select:

- 0-Routine
- 1-Priority
- 2-Immediate
- 3-Flash
- 4-Flash Override
- 5-CRITIC/ECP
- 6-Internetwork Control
- 7-Network Control

AF Drop: Default "1-Low". The drop priority can take three values: 0, 1 or 2. The values are described below:

- 1-Low
- 2-Medium
- 3-High

In the DSCP bits field, you will see the binary value of what you have selected.
Click on *OK*.

5.18.1.2 Advanced SIP Configuration

Configuration of advanced Voice over IP settings in the CopperJet IAD's is done through TELNET. To access the TELNET configuration mode, start a TELNET session from your computer (i.e. `TELNET <ip-address>`) and enter your username and password (default username and password are **admin, admin**). To see the VoIP settings type the following command:

```
-->voip show    <Enter>
```

With this command you see the SIP and MGCP settings.

To see the options available for SIP, type the following:

```
-->voip set sip ?    <Enter>
```

5.18.1.3 Configuring Silence Suppression

This command enables or disables Silence Suppression.

Silence suppression controls the silence suppression insertion in the voice data samples. When silence suppression is enabled, silence is 'transmitted' as a special type of compact voice sample. This is a much more efficient use of bandwidth, instead of just sending normal voice samples which contain nothing but silence.

With the following command you can enable or disable Silence Suppression:

```
--> voip set sip silenceSuppression {enabled|disabled}    <Enter>
```

Example:

```
--> voip set sip silenceSuppression disabled    <Enter>
```

5.18.1.4 Configuring Digitmap

A digit map is a regular expression string which defines a pattern of digits which will be recognised by the system as a valid phone number.
The digit map can be used to specify not only the number of digits required to make a valid phone number but also the range of digits and special characters which can be entered and timeout values after the digits have been dialed.

With the following command you can set the digitmap:

```
-->voip set sip digitmap <digitmap>    <Enter>
```

Example:

```
-->voip set sip digitmap(x.T|##S|*[268]xS|*74x.#S|x#S)    <Enter>
```

The above digitmap sets the following characteristics for the SIP phones:

- **x.T** - any number of digits followed by a timeout to dial the digits. This is not a special call code.
- **##S** - Last number redial.
- ***[268]xS** - is a compound entry which matches the following codes:
- ***20** - Set DND (Do-Not-Disturb) ON
- ***80** - Set DND (Do-Not-Disturb) OFF
- ***69** - Return the last missed call

All other numbers which are also matched by this entry will return an error if entered.
For example, entering ***82** will generate an error.

- ***74x.#S** - Speed dial 8 setting.
- **x#S** - Speed dial call.

5.18.1.5 Configuring Echo Cancellation

Echo canceling suppresses the 'echo' which can be received by sound transmitted from the Local end of a call being re-transmitted back to the Local end from the Far end.
Echo canceling prevents this echo effect from occurring.

To enable or disable Echo Cancel, use the following command:

```
-->voip set sip echocancel {enabled|disabled}    <Enter>
```

Enabled = Enable Echo Cancellation. Suppress echo of noise from being re-transmitted back to the Local end.
Disabled = Disable Echo Cancellation.

Example:

```
-->voip set sip echocancel enabled    <Enter>
```

5.18.1.6 Configuring Packetperiod

The length of the Voice sample (in ms) which is put in a packet. Typically, this value is set to 20 but can be set to other values between 5 and 50 depending on the Codec being used. The lower the value, the more Voice packets that will be generated.

This command sets the length of the Voice sample (in ms) which is put in a packet.

```
-->voip set sip packetperiod <period>    <Enter>
```

Example:

```
-->voip set sip packetperiod 20    <Enter>
```

5.18.1.7 Configuring Proxyroute

This command sets the type of SIP routing proxy to use for SIP calls. Currently, there are two versions of this proxy. The SIP Proxy Server you are using may not support both sets of proxies so you may need to alter this setting to be compatible with the SIP Proxy Server you are using.

```
-->voip set sip proxyroute {loose|strict}    <Enter>
```

Example:

```
-->voip set sip proxyroute strict    <Enter>
```

5.18.1.8 Configuring Registration Expires

This command specifies the time interval after which registration with the SIP Proxy Server is refreshed. The Voice-IAD systems will automatically attempt to refresh their registrations before they expire. If they expire without being refreshed then the SIP Registrar deletes the corresponding entries and the phones connected to that Voice-IAD system will no longer be able to receive incoming calls as it will be unknown to the Registration Server.

```
        -->voip set sip regexpires <seconds>    <Enter>
```

Example:

```
        -->voip set sip regexpires 3600    <Enter>
```

5.18.1.9 Configuring Registration port

This command is used to identify the port used by SIP agents to communicate with the SIP Proxy server.

```
        -->voip set sip regport <port>    <Enter>
```

Example:

```
        -->voip set sip regport udp    <Enter>
```

5.18.1.10 Configuring Outboundserver

This command sets the outbound server address.

```
        -->voip set sip outboundserver <address>    <Enter>
```

Example:

```
        -->voip set sip outboundserver sip.example.com    <Enter>
```

5.18.1.11 Configuring Outboundserverport

This command sets the outbound server port.

```
        -->voip set sip outboundserverport <portno>    <Enter>
```

Example:

```
        -->voip set sip outboundserverport 5060    <Enter>
```

5.18.1.12 Configuring Outboundservertransport

This command sets the outbound server transport.

```
        -->voip set sip outboundservertransport {tcp|udp}    <Enter>
```

Example:

-->voip set sip outboundservertransport udp <Enter>

5.18.1.13 Enable SIP tracing in the CopperJet

To enable SIP tracing in the CopperJet, please follow these steps:

- Open a telnet session to the CopperJet

  Note: To open a telnet session, go to ***Start -> Run*** *and type* ***cmd*** *and click on* ***OK****. A DOS box will open. Now type* ***telnet 172.19.3.1*** *and press* ***Enter****. Default username and password is* ***admin****.*

- Type the following commands:

  -->system log enable voip pots <Enter>

  Note: VoIP must be registered for using this command.

  -->console enable

  Quantum>log level 1 <Enter>

  The trace is now started.

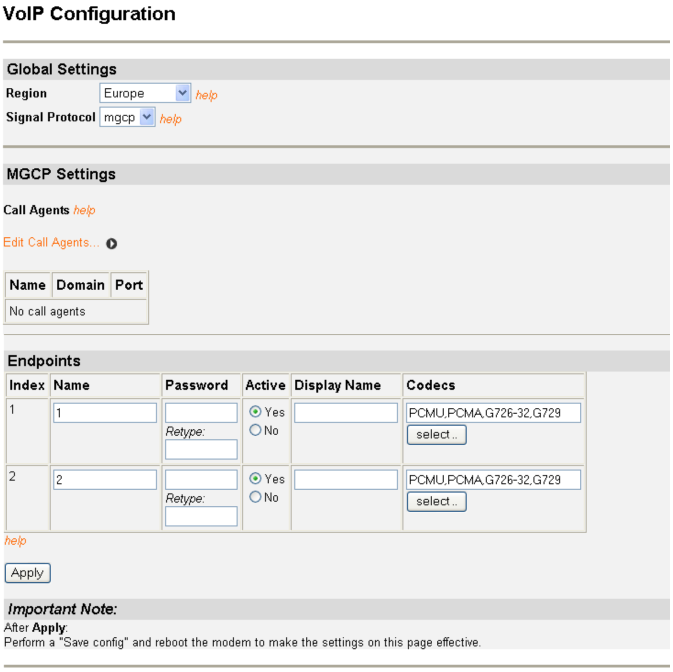
  To stop the logging, type:

  Quantum>log level 0 <Enter>

5.18.2 Configuring VoIP using MGCP

MGCP stands for Media Gateway Control Protocol. It consists of a Call Agent, which contains the call control ‘intelligence’, and a media gateway which contains the media functions required.

When you select *MGCP*, as Signal Protocol, the *MGCP Configuration* page is displayed.



VoIP Configuration

Global Settings

Region: Europe
Signal Protocol: mgcp

MGCP Settings

Call Agents

Name	Domain	Port
No call agents		

Endpoints

Index	Name	Password	Active	Display Name	Codecs
1	1	Retype:	● Yes ○ No		PCMU,PCMA,G726-32,G729 select ..
2	2	Retype:	● Yes ○ No		PCMU,PCMA,G726-32,G729 select ..

Important Note:

After **Apply**:
Perform a "Save config" and reboot the modem to make the settings on this page effective.

You need to add detailed configuration information about the MGCP service that you are creating. This information must be provided by your service provider.

Call Agents: This option adds an MGCP call agent to an MGCP Voice network. An MGCP Call Agent is used to establish and control VoIP calls between Voice-IAD systems on the network. See section *5.18.2.1 Configuring Call agents* how to configure Call Agents.

Endpoints:

Index: An index value that identifies the endpoint.

Name: A name for the endpoint.

Password: This command sets a password to be associated with an endpoint.

Active: By default Yes. *Yes* endpoint is Active. *No* and endpoint is not Active

Display Name: The display name for the endpoint. The name must only be composed of alphanumeric characters.

Codecs: This command specifies the codec types which can be used to compress the Voice packets from the endpoint specified.
The codecs are listed in order of preference to be used for a phone call. The endpoint will negotiate with the other end to choose a codec which they can both use.

Voice codec support:

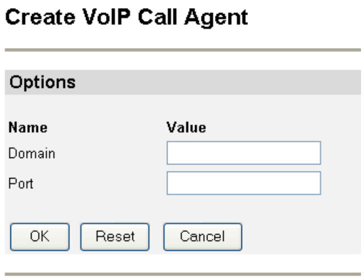
- G.711 (A-Law and μ−Law),

- G.726 (32kb) and
- G.729 a/b

After the correct settings are filled in, click on *Apply*. Go to the *Configuration* menu and click on *Save config* to save the new settings into the CopperJet. MGCP is only active after a restart of the CopperJet. To Restart the CopperJet, go to *System -> Restart* and click on the *Restart* button.

5.18.2.1 Configuring Call agents

To configure *Call agents*, click on the *Edit Call Agents* link. Then click on the *Create new VoIP Call Agent* link. The *Create VoIP Call Agent* page is displayed.



Create VoIP Call Agent

Options

Name	Value
Domain	
Port	

You need to add detailed configuration information about the MGCP service that you are creating. This information must be provided by your service provider.

Domain: A domain name (eg. callagent.test.net) or an IPv4 address (eg. 192.168.1.1).

Port: The MGCP port. Default the port number is 2727.

After configuring the fields, click on *OK*. Go to the *Configuration* menu and click on *Save config* to save the new settings into the CopperJet. MGCP is only active after a restart of the CopperJet. To Restart the CopperJet, go to *System -> Restart* and click on the *Restart* button.

5.18.2.2 Advanced MGCP Configuration

Configuration of advanced Voice over IP settings in the CopperJet IAD's is done through TELNET. To access the TELNET configuration mode, start a TELNET session from your computer (i.e. `TELNET <ip-address>`) and enter your username and password (default username and password are **admin, admin**). To see the VoIP settings type the following command:

```
-->voip show    <Enter>
```

With this command you see the SIP and MGCP settings.

To see the options available for MGCP, type the following:

```
-->voip set mgcp ?    <Enter>
```

5.18.2.3 Configuring MGCP Domain

```
-->voip set mgcp domain <domain>    <Enter>
```

This command is used to identify the MGCP domain in which the Voice-IAD system is situated. For example, by default the MGCP call agent configuration file entry for a phone connected to a Voice-IAD system with IP address 192.168.88.25 would be:

```
aaln/1@[192.168.88.25]
```

The domain name in this example is '[192.168.88.25]'.
If you wish to override this setting, you can use this command to change the domain name, for example *test*. The command:

```
-->voip set mgcp domain test    <Enter>
```

This will result in endpoints such as '**aaln/1@test**'

5.18.2.4 Configuring MGCP eptypename

```
-->voip set mgcp eptypename <eptypename>    <Enter>
```

This command is used to configure the MGCP Endpoint type name or *eptypename*.
For example, the MGCP call agent configuration file entry for a phone connected to a Voice-IAD system with IP address 192.168.88.25 would be:

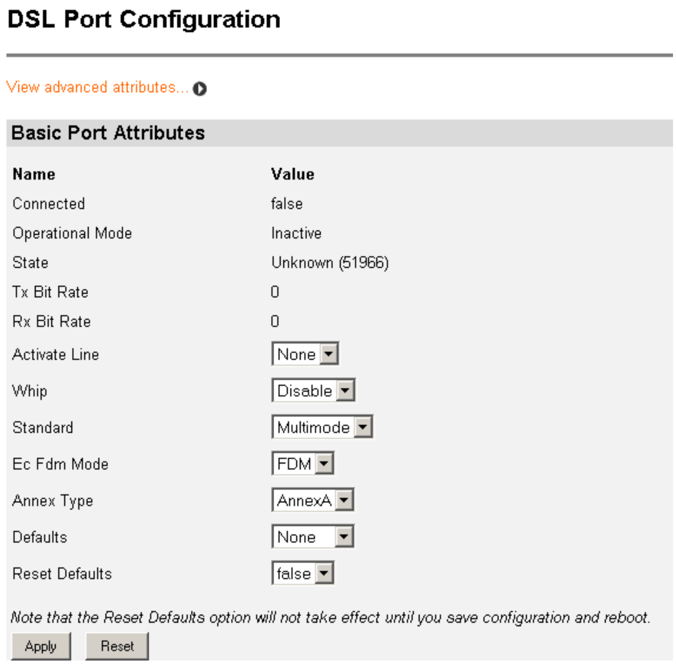
```
aaln/1@[192.168.88.25]
```

In this example, the *eptypename* is 'aaln'. This is also the default setting.

5.19 DSL Line

The DSL Port menu allows you to configure specific DSL settings. Usually, the default settings are sufficient to make a good DSL connection. Only for fine-tuning or advanced administration, the DSL port menu brings useful information.

From the *Configuration* menu, go to *Ports* and click on *DSL*. The *DSL Port Configuration* page is displayed.



DSL Port Configuration

Basic Port Attributes

Name	Value
Connected	false
Operational Mode	Inactive
State	Unknown (51966)
Tx Bit Rate	0
Rx Bit Rate	0
Activate Line	None
Whip	Disable
Standard	Multimode
Ec Fdm Mode	FDM
Annex Type	AnnexA
Defaults	None
Reset Defaults	false

Note that the Reset Defaults option will not take effect until you save configuration and reboot.

This page provides the following information.

Connected: Shows if your DSL line is up (true) or not (false).

Operational Mode: The modulation type used to make the connection. Advice: set the ADSLMode (line modulation) on Multimode.

State: Shows the status of the line: *Handshake*, *Training* or *Showtime.*

Tx Bit Rate: The maximum Transmit Bit Rate of your DSL line.

Rx Bit Rate: The maximum Receive Bit Rate of your DSL line.

Activate Line: None: DSL link will not be activate.
Abort: Deactivate the DSL link.
Start: Activate the DSL link

Whip: Propriarity protocol, disabled by default.

Standard: Multimode at default.

Ec Fdm Mode: FDM at default.

Annex Type: Shows which Annex Type you have.

Default: None at default.

Reset Defaults: False at default.

After you changed the configuration, click on *Apply*. Don’t forget to save the changes. Go to the *Configuration* menu and click on *Save config* to save the new settings into the CopperJet.

Click on *Reset* if you want the previous settings.

6 WAN Configuration Examples

In this chapter is described how to configure a basic/standard WAN connection to get you up and running.

6.1 Configuring a Bridged connection

In this section is described how to configure a transparent bridged connection (RFC1483 bridged).

Follow the steps below to configure the CopperJet as a transparent bridge.

1- Go to *Configuration -> WAN connections*.
2- Delete any existing WAN connection by clicking on the *Delete…* link.
3- Click on *Create new Service*.
4- Select as WAN Service *RFC1483 Bridged Service attached to the Bridge*.
5- Fill in the correct VPI and VCI values that is provided by your ISP.
6- Click on *OK*.
7- Make sure that the DHCP Server (Configuration -> DHCP Server) is disabled.
8- Save the configuration (Configuration -> Save config and click on Save).
9- Now configure your network card that it obtains an IP address automatically (see section 5.6.1.1 Configuring DHCP on your network card how to configure).

For more advanced settings, go to section *5.6.1 Configuring RFC1483 Bridged service attached to the Bridge*.

6.2 Configuring a Routed connection on a bridged line with NAT

When you have a bridged line and you want more then 1 pc making use of the internet (sharing), you need to configure the CopperJet as a router.

Follow the steps below to configure the CopperJet as a router on a bridged line.

1- Go to *Configuration -> WAN connections*.
2- Delete any existing WAN connection by clicking on the *Delete…* link.
3- Click on *Create new Service*.
4- Select as WAN Service *RFC1483 Bridged Service attached to the Router*.
5- Fill in the correct VPI and VCI values that is provided by your ISP.
6- Click on *OK*.
7- Preferred is to have the DHCP Server of the CopperJet enabled.
8- Save the configuration (Configuration -> Save config and click on Save).
9- Make sure that your network card is configured correctly.

For more advanced settings, go to section *5.6.3 Configuring RFC1483 Bridged service attached to the Router*.

6.3 Configuring a PPPoA connection with NAT

In this section is described how to configure a PPPoA connection (RFC2364 routed).

Follow the steps below to configure the CopperJet for PPPoA.

1- Go to *Configuration -> WAN connections*.
2- Delete any existing WAN connection by clicking on the *Delete…* link.
3- Click on *Create new Service*.
4- Select as WAN Service *RFC2364 Routed Service attached to the Router*.
5- Fill in the correct VPI and VCI values and Username and Password that is provided by your ISP.
6- Click on *OK*.
7- Preferred is to have the DHCP Server of the CopperJet enabled.
8- Save the configuration (Configuration -> Save config and click on Save).
9- Make sure that your network card is configured correctly.

For more advanced settings, go to section *5.6.5 Configuring PPPoA routed service attached to the Router*.

6.4 Configuring a PPPoE connection with NAT

In this section is described how to configure a PPPoE connection (RFC2516 routed).

Follow the steps below to configure the CopperJet for PPPoE.

1- Go to *Configuration -> WAN connections*.
2- Delete any existing WAN connection by clicking on the *Delete…* link.
3- Click on *Create new Service*.
4- Select as WAN Service *RFC2516 Routed Service attached to the Router*.
5- Fill in the correct VPI and VCI values and Username and Password that is provided by your ISP.
6- Click on OK.
7- Preferred is to have the DHCP Server of the CopperJet enabled.
8- Save the configuration (Configuration -> Save config and click on Save).
9- Make sure that your network card is configured correctly.

For more advanced settings, go to section *5.6.6 Configuring PPPoE routed service attached to the Router*.

7 Glossary

10BASE-T A designation for the type of wiring used by Ethernet networks with a data rate of 10 Mbps. Also known as Category 3 (CAT 3) wiring. See *data rate*, *Ethernet*.

100BASE-T A designation for the type of wiring used by Ethernet networks with a data rate of 100 Mbps. Also known as Category 5 (CAT 5) wiring. See *data rate*, *Ethernet*.

ADSL Asymmetric Digital Subscriber Line
The most commonly deployed "flavor" of DSL for home users is asymmetrical DSL. The term asymmetrical refers to its unequal data rates for downloading and uploading (the download rate is higher than the upload rate). The asymmetrical rates benefit home users because they typically download much more data from the Internet than they upload.

Analog An analog signal is a signal that has had its frequency modified in some way, such as by amplifying its strength or varying its frequency, in order to add information to the signal. The voice component in DSL is an analog signal. See *digital*.

ATM Asynchronous Transfer Mode
A standard for high-speed transmission of data, text, voice, and video, widely used within the Internet. ATM data rates range from 45 Mbps to 2.5 Gbps. See *data rate*.

authenticate To verify a user’s identity, such as by prompting for a password.

binary The "base two" system of numbers, that uses only two digits, 0 and 1, to represent all numbers. In binary, the number 1 is written as 1, 2 as 10, 3 as 11, 4 as 100, etc. Although expressed as decimal numbers for convenience, IP addresses in actual use are binary numbers; e.g., the IP address 209.191.4.240 is 11010001.10111111.00000100.11110000 in binary. See *bit*, *IP address*, *network mask*.

bit Short for "binary digit," a bit is a number that can have two values, 0 or 1. See *binary*.

bps bits per second

bridging Passing data from your network to your ISP and vice versa using the hardware addresses of the devices at each location. Bridging contrasts with routing, which can add more intelligence to data transfers by using network addresses instead. The CopperJet can perform both routing and bridging. Typically, when both functions are enabled, the device routes IP data and bridges all other types of data. See *routing*.

broadband A telecommunications technology that can send different types of data over the same medium. DSL is a broadband technology.

broadcast To send data to all computers on a network.

channel The channel number determines which channel frequency is used by the device to pass wireless traffic to wireless PCs. The channels available depend on which country the wireless network is operating in. Your ISP provides details of the channel(s) you should use.

DHCP Dynamic Host Configuration Protocol
DHCP automates address assignment and management. When a computer connects to the LAN, DHCP assigns it an IP address from a shared pool of IP addresses; after a specified time limit, DHCP returns the address to the pool.

DHCP relay Dynamic Host Configuration Protocol relay
A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the Copper Jet’s interfaces can be configured as a DHCP relay. See *DHCP*.

DHCP server Dynamic Host Configuration Protocol server
A DHCP server is a computer that is responsible for assigning IP addresses to the computers on a LAN. See *DHCP*.
digital Of data, having a form based on discrete values expressed as binary numbers (0's and 1's). The data component in DSL is a digital signal. See *analog*.

DNS Domain Name System
The DNS maps domain names into IP addresses. DNS information is distributed hierarchically throughout the Internet among computers called DNS servers. For example, *www.yahoo.com* is the domain name associated with IP address 216.115.108.243. When you start to access a web site, a DNS server looks up the requested domain name to find its corresponding IP address. If the DNS server cannot find the IP address, it communicates with higher-level DNS servers to determine the IP address. See *domain name.*

domain name A domain name is a user-friendly name used in place of its associated IP address. Domain names must be unique; their assignment is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN). Domain names are a key element of URLs, which identify a specific file at a web site. See *DNS.*

download To transfer data in the downstream direction, i.e., from the Internet to the user.

DSL Digital Subscriber Line
A technology that allows both digital data and analog voice signals to travel over existing copper telephone lines.

Ethernet The most commonly installed computer network technology, usually using twisted pair wiring. Ethernet data rates are 10 Mbps and 100 Mbps. *See also 10BASE-T, 100BASE-T, twisted pair*.

FTP File Transfer Protocol
A program used to transfer files between computers connected to the Internet. Common uses include uploading new or updated files to a web server, and downloading files from a web server.

Gbps Abbreviation of Gigabits per second, or one billion bits per second. Internet data rates are often expressed in Gbps.

host A device (usually a computer) connected to a network.

HTTP Hyper-Text Transfer Protocol
HTTP is the main protocol used to transfer data from web sites so that it can be displayed by web browsers. See *web browser, web site*.

Hub A hub is a place of convergence where data arrives from one or more directions and is forwarded out in one or more directions. It connects an Ethernet bridge/router to a group of PCs on a LAN and allows communication to pass between the networked devices.

ICMP Internet Control Message Protocol
An Internet protocol used to report errors and other network-related information. The ping command makes use of ICMP.

IEEE The Institute of Electrical and Electronics Engineers is a technical professional society that fosters the development of standards that often become national and international standards.

Internet The global collection of interconnected networks used for both private and business communications.

intranet A private, company-internal network that looks like part of the Internet (users access information using web browsers), but is accessible only by employees.

IP *See TCP/IP*.

IP address Internet Protocol address
The address of a host (computer) on the Internet, consisting of four numbers, each from 0 to 255, separated by periods, e.g., 209.191.4.240. An IP address consists of a *network ID* that identifies the particular network the host belongs to, and a *host ID* uniquely identifying the host itself on that network. A network mask is used to define the network ID and the host ID. Because IP addresses are difficult to remember, they usually have an associated domain name that can be specified instead. See *domain name*, *network mask*.

ISP Internet Service Provider
A company that provides Internet access to its customers, usually for a fee.

LAN Local Area Network
A network limited to a small geographic area, such as a home or small office.

LED Light Emitting Diode
An electronic light-emitting device. The indicator lights on the front of the CopperJet are LEDs.

MAC address Media Access Control address
The permanent hardware address of a device, assigned by its manufacturer. MAC addresses are expressed as six pairs of hex characters, with each pair separated by colons. For example; *NN:NN:NN:NN:NN:NN*.

mask *See network mask*.

Mbps Abbreviation for Megabits per second, or one million bits per second. Network data rates are often expressed in Mbps.

NAT Network Address Translation
A service performed by many routers that translates your network's publicly known IP address into a *private* IP address for each computer on your LAN. Only your router and your LAN know these addresses; the outside world sees only the public IP address when talking to a computer on your LAN.

network A group of computers that are connected together, allowing them to communicate with each other and share resources, such as software, files, etc. A network can be small, such as a *LAN*, or very large, such as the *Internet*.

network mask A network mask is a sequence of bits applied to an IP address to select the network ID while ignoring the host ID. Bits set to 1 mean "select this bit" while bits set to 0 mean "ignore this bit." For example, if the network mask 255.255.255.0 is applied to the IP address 100.10.50.1, the network ID is 100.10.50, and the host ID is 1. See *binary*, *IP address*, *subnet*.

NIC Network Interface Card
An adapter card that plugs into your computer and provides the physical interface to your network cabling. For Ethernet NICs this is typically an RJ-45 connector. See *Ethernet*, *RJ-45*.

packet Data transmitted on a network consists of units called packets. Each packet contains a payload (the data), plus overhead information such as where it came from (source address) and where it should go (destination address).

pass phrase A secret password used in *WPA* wireless data encryption. Encryption is based on a WPA master key that is derived from the pass phrase and the network name (SSID) of the device. The pass phrase should be at least 20 characters long in order to deter a hacker attempting to crack the pass phrase by recording a series of frames then trying commonly used passwords offline until one works (known as offline PSK dictionary attacks).

ping Packet Internet (or Inter-Network) Groper
A program used to verify whether the host associated with an IP address is online. It can also be used to reveal the IP address for a given domain name.

port A physical access point to a device such as a computer or router, through which data flows into and out of the device.

PPP Point-to-Point Protocol
A protocol for serial data transmission that is used to carry IP (and other protocol) data between your ISP and your computer. The WAN interface on the CopperJet uses two forms of PPP called PPPoA and PPPoE. See *PPPoA*, *PPPoE*.

PPPoA Point-to-Point Protocol over ATM
One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoE. You can define only one PPPoA interface per VC.

PPPoE Point-to-Point Protocol over Ethernet
One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoA. You can define one or more PPPoE interfaces per VC.

protocol A set of rules governing the transmission of data. In order for a data transmission to work, both ends of the connection have to follow the rules of the protocol.

remote In a physically separate location. For example, an employee away on travel who logs in to the company's intranet is a remote user.

RIP Routing Information Protocol
The original TCP/IP routing protocol. There are two versions of RIP: version I and version II.

RJ-11 Registered Jack Standard-11
The standard plug used to connect telephones, fax machines, modems, etc. to a telephone port. It is a 6-pin connector usually containing four wires.

RJ-45 Registered Jack Standard-45
The 8-pin plug used in transmitting data over phone lines. Ethernet cabling usually uses this type of connector.

routing Forwarding data between your network and the Internet on the most efficient route, based on the data’s destination IP address and current network conditions. A device that performs routing is called a router.

SDNS Secondary Domain Name System (server)
A DNS server that can be used if the primary DSN server is not available. *See DNS*.

SSID Service Set Identifier (also known as the Extended Service Set Identifier (ESSID)) is a unique identifier that differentiates one wireless device from another. Wireless PCs configured with the same SSID can access that device.

subnet A subnet is a portion of a network. The subnet is distinguished from the larger network by a *subnet mask* that selects some of the computers of the network and excludes all others. The subnet's computers remain physically connected to the rest of the parent network, but they are treated as though they were on a separate network. See *network mask*.

subnet mask A mask that defines a subnet. See *network mask*.

TCP See *TCP/IP*.

TCP/IP Transmission Control Protocol/Internet Protocol
The basic protocols used on the Internet. TCP is responsible for dividing data up into packets for delivery and reassembling them at the destination, while IP is responsible for delivering the packets from source to destination. When TCP and IP are bundled with higher-level applications such as HTTP, FTP, Telnet, etc., TCP/IP refers to this whole suite of protocols.

Telnet An interactive, character-based program used to access a remote computer. While HTTP (the web protocol) and FTP only allow you to download files from a remote computer, Telnet allows you to log into and use a computer from a remote location.

TFTP Trivial File Transfer Protocol
A protocol for file transfers, TFTP is easier to use than File Transfer Protocol (FTP) but not as capable or secure.

triggers Triggers are used to deal with application protocols that create separate sessions. Some applications, such as NetMeeting, open secondary connections during normal operations, for example, a connection to a server is established using one port, but data transfers are performed on a separate connection. A trigger tells the device to expect these secondary sessions and how to handle them.
Once you set a trigger, the embedded IP address of each incoming packet is replaced by the correct host address so that NAT can translate packets to the correct destination. You can specify whether you want to carry out address replacement, and if so, whether to replace addresses on TCP packets only, UDP packets only, or both.

twisted pair The ordinary copper telephone wiring used by telephone companies. It contains one or more wire pairs twisted together to reduce inductance and noise. Each telephone line uses one pair. In homes, it is most often installed with two pairs. For Ethernet LANs, a higher grade called Category 3 (CAT 3) is used for 10BASE-T networks, and an even higher grade called Category 5 (CAT 5) is used for 100BASE-T networks. See *10BASE-T, 100BASE-T, Ethernet*.

unnumbered interfaces
An unnumbered interface is an IP interface that does not have a local subnet associated with it. Instead, it uses a *router-id* that serves as the source and destination address of packets sent to and from the router. Unlike the IP address of a normal interface, the router-id of an unnumbered interface is allowed to be the same as the IP address of another interface. For example, the WAN unnumbered interface of your device uses the same IP address of the LAN interface (192.168.1.1).
The unnumbered interface is temporary – PPP or DHCP will assign a 'real' IP address automatically.

upstream The direction of data transmission from the user to the Internet.

USB Universal Serial Bus
A serial interface that lets you connect devices such as printers, scanners, etc. to your computer by simply plugging them in. The CopperJet can be equipped with a USB interface for connecting to a stand-alone PC.

VC Virtual Circuit
A connection from your DSL router to your ISP.

VCI Virtual Circuit Identifier
Together with the Virtual Path Identifier (VPI), the VCI uniquely identifies a VC. Your ISP will tell you the VCI for each VC they provide. See *VC*.

VPI Virtual Path Identifier
Together with the Virtual Circuit Identifier (VCI), the VPI uniquely identifies a VC. Your ISP will tell you the VPI for each VC they provide. See *VC*.

WAN Wide Area Network
Any network spread over a large geographical area, such as a country or continent. With respect to the CopperJet, WAN refers to the Internet.

Web browser A software program that uses Hyper-Text Transfer Protocol (HTTP) to download information from (and upload to) web sites, and displays the information, which may consist of text, graphic images, audio, or video, to the user. Web browsers use Hyper-Text Transfer Protocol (HTTP). Popular web browsers include Netscape Navigator and Microsoft Internet Explorer. See *HTTP, web site, WWW*.

Web page A web site file typically containing text, graphics and hyperlinks (cross-references) to the other pages on that web site, as well as to pages on other web sites. When a user accesses a web site, the first page that is displayed is called the *home page*. See *hyperlink, web site*.

Web site A computer on the Internet that distributes information to (and gets information from) remote users through web browsers. A web site typically consists of web pages that contain text, graphics, and hyperlinks. See *hyperlink, web page*.

WWW World Wide Web. Also called *(the) Web.* Collective term for all web sites anywhere in the world that can be accessed via the Internet.