Table of Contents

TABLE OF CONTENTS **1**

INTRODUCTION **3**

FEATURES 3

CONNECTING TO OVIDA **4**

INSTALLATION WIZARD **5**

ADSL WIZARD **6**

ISDN WIZARD 7

PC SETTINGS **8**

USING THE INTERNET **8**

LOCAL AREA NETWORK **8**

WIDE AREA NETWORK **9**

ADSL 9
ISDN 9
DIAL BACKUP 9

INDICATORS **9**

RESET BUTTON **9**

PROFILES **10**

ADSL PROFILE 10
ISDN PROFILE 13

MLPPP **15**

TIMEBANDS **16**

ADSL TIMEBANDS 16
ISDN TIMEBANDS 17

DHCP SERVER **18**

STATISTICS **20**

LAN STATISTICS 21
Statistic *21*
Description *21*
ICMP STATISTICS 22
Statistic *22*
Description *22*

FIREWALL **23**

FILTER STACKS 24
FILTERS 24
ADSL INCOMING FILTER STACK 26
ADSL OUTGOING FILTER STACK 27
ISDN INCOMING FILTER STACK 28
ISDN OUTGOING FILTER STACK 29

DIAGNOSTICS **30**

SPECIFICATIONS **32**

LAN 32
ADSL 32
ISDN 32
PROTOCOLS 32
AUTHENTICATION 32
DHCP 32
ROUTING 32
FIREWALL 32
CALL MANAGEMENT 32
MANAGEMENT 32

Introduction

The Internet Module is a Commander Connect system module that provides multi-user high-speed Internet access using ADSL and ISDN. It also provides a Local Area Network that allows users to network PCs and share printers and other resources within the office. It is easy to install and manage using the installation wizard and management system. It can be installed at the initial installation phase or added later.

Features

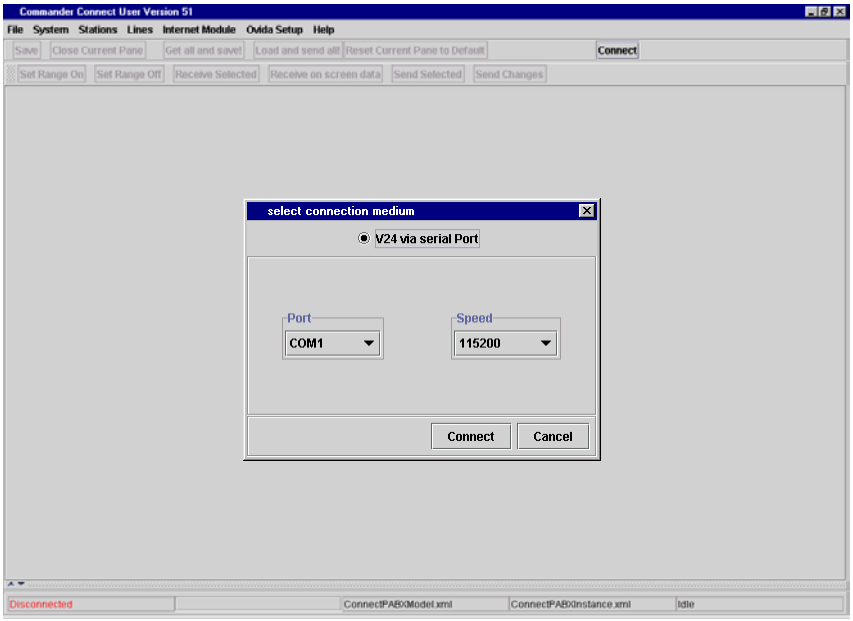
The Internet module has the following features:

- Installation Wizard for easy setup
- Multi-user Internet access
- Local Area Networking
- ADSL
- ISDN
- Firewall
- ISDN dial backup
- Cost control for dial-up calls
- PC based management
- External indicators

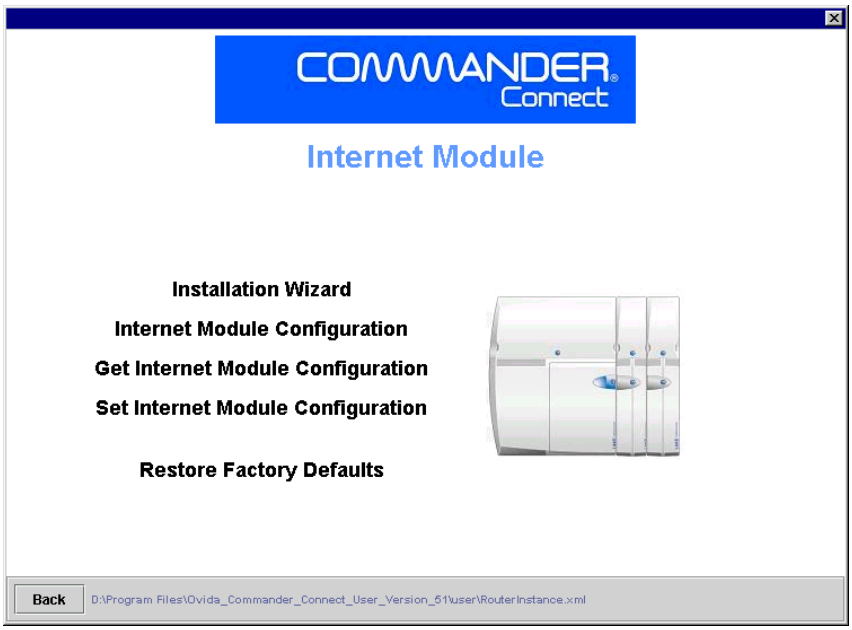
Connecting to Ovida

The Internet Module is programmed using Ovida.

- Establish a connection to the system.



- Select the **Internet Module** tab on the main menu.
- The following screen is displayed.



- **Installation Wizard** takes you to the Installation Wizard settings
- **Internet Module Configuration** takes you to the LAN, Internet Module and WAN settings
- **Get Internet Module Configuration** receives all settings and updates the corresponding fields in the management system.
- **Set Internet Module Configuration** sends all management system settings to the Internet Module.
- **Restore Factory Settings** restores all settings to the original default settings.
- **Back** takes you back to the previous screen.

For some configuration changes to take effect, a warm reset must be performed on the Internet Module. A prompt will appear on the Ovida screen requesting a reset.

Installation Wizard

The installation wizard allows you to quickly and easily set up an Internet connection.

Before you use the wizard, you must have the following information to hand.

- Will ADSL or ISDN be used to access the ISP?
- If ADSL is to be used, get the following information. This will be provided by your ISP.

  - Username
  - Password
  - Which of the following protocols are used by the ADSL modem

    - PPPoE
    - Dynamic IP address assignment
    - Static IP address assignment.
      If static IP addressing is used, the user should skip the ADSL Wizard and proceed to the ADSL Profile in WAN settings.

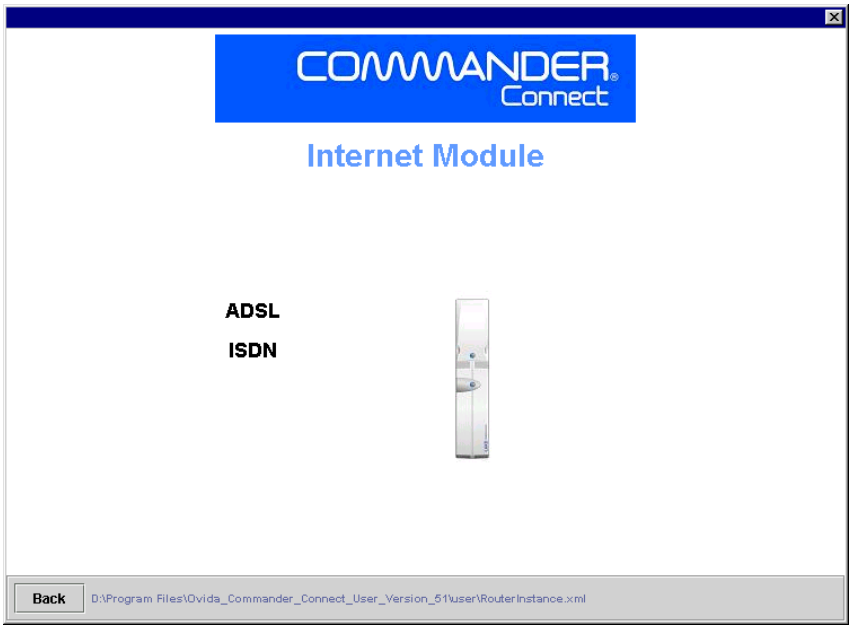
- If ISDN is to be used, get the following information. This will be provided by your ISP.

  - Username
  - Password
  - Telephone number

The following procedure is now used to set up Internet access.

- Select Installation Wizard from the main menu

- The following screen is displayed



ADSL Wizard

ADSL provides a high-speed "always on" service whereby the Internet module is permanently connected to the Internet using a standard telephone line.

Please refer to the installation manual for instructions for connecting the ADSL modem and LAN PCs.

- Select **ADSL** on the Installation Wizard screen
- The following screen is displayed

- Enter the **Username**. This will be provided by the ISP.
- Enter the **Password.** This will be provided by the ISP.
- Select a Protocol either **PPPoE** or **IP**.

  Note: If static IP addressing is used, the user should skip the ADSL Wizard and proceed to the ADSL Profile.
- **Set Profile Enabled - Yes.**
- Click on the **Send** button.

The Internet module is now set up to access the Internet using ADSL.

ISDN Wizard

If ADSL is not provided, the Internet module can use any ISDN line connected to the PABX to establish a dial-up connection to the Internet.

Note : if ADSL is installed and ISDN dial backup is required, the user should proceed to the ADSL Profile and ISDN Profile in WAN settings.

The following procedure is used to set up an ISDN connection.
- Select **ISDN** from the Wizard screen
- The following screen is displayed

- Enter the **Username**. This will be provided by the ISP.
- Enter the **Password**. This will be provided by the ISP.
- Enter the **Tel No** (telephone number) that the Internet module dials to access the Internet. This will be provided by your ISP. Ensure that the telephone number is preceded by the PABX access code for an outside line. The default access code is 0.
- **Profile active** must be set to Yes.
- Click on the **Send** button.

The ADSL Profile MUST be disabled (where an ADSL service is not connected).

- Click on **Cancel.** This takes you back to the previous screen.
- Select **ADSL**.
- The ADSL wizard screen is displayed
- Set **Profile Enabled** - **No**. This disables the ADSL profile.
- Click on the **Send** button.

The Internet module is now set up to access the Internet using ISDN.

PC Settings

Each PC used to browse the Internet must be configured to obtain an IP address automatically.

- Right click **Network Neighbourhood**
- Left click **Properties**
- Select **Protocols** tab
- Scroll through protocols listed and highlight **TCP/IP Protocol** and click properties tab
- Click radio button **Obtain an IP address from a DHCP server**
- Click **OK.**

The PC is now set up to automatically obtain an IP address from the DHCP server in the Internet Module.

Internet Explorer must also be configured as follows.

- Select **Tools** on **menu bar**
- **Select Internet** Options on drop down menu
- Click **Connections** tab
- Click **LAN Settings**
- Proxy Server. Ensure that Use a proxy Server box is not ticked.

Using the Internet

Launching Internet Explorer on any PC connected to the LAN will automatically connect the user to the Internet.

Local Area Network

The Internet module has a LAN (Local Area Network) which allows multiple PCs to connect to the Internet. It also allows users to network PCs and share printers and other resources.

The Internet module has four 10/100 switched Ethernet ports for connecting PCs or other devices. If more than four LAN devices are to be connected, an external Ethernet hub or hubs can be connected to any or all of the ports to expand the LAN. The Internet module can accommodate up to a total of 100 LAN devices.

The RJ-45 connectors for these ports are located on the MDF and are used to connect PCs or other LAN devices to the Internet module. Each port is set for autoconfiguration and autosensing to automatically adapt to network card settings in the PC or other device that is connected to it. Also, each port can automatically adapt itself to a standard or crossover cable.

Wide Area Network

The Internet module can use ADSL and/or ISDN to access the Internet.

ADSL

ADSL provides "always on" service, i.e. with ADSL services the Internet module is permanently connected to the Internet using a standard telephone line. The telephone line is terminated at the user end by a splitter that provides a normal telephone line as well as a high-speed data connection.

The Internet module is factory fitted with a 10 Base-T port for connecting to an external ADSL modem. A RJ-45 connector is provided on the Internet module backplane. The service provider installs the line, the splitter and the ADSL modem.

ISDN

Where the user has no ADSL service, ISDN can be used for Internet access. Any ISDN line connected to the PABX can be used to establish a dial-up data connection to the Internet. If ADSL is not installed, it is recommended that ADSL be disabled using either on the ADSL Wizard or ADSL Profile. The ISDN line may disconnect where no line activity is detected for a period set by an idle timer. However, the connection will be automatically re-established when browsing activity is next detected. The settings for the idle timer can be adjusted in the ISDN Profile settings.

Dial backup

In a system equipped with ADSL and ISDN, the ISDN profile can be configured to provide dial backup in the event of ADSL line failure. If the ADSL line fails, an ISDN call is established after approximately 1 minute. When the ADSL line is restored, the Internet Module automatically switches back to ADSL and the ISDN call is disconnected.

Where the Internet Module is connected to an external ADSL modem, it is necessary to disconnect the cable between the Internet Module and the ADSL modem to invoke ISDN dial backup. When the ADSL service has been restored, the cable should again be reconnected and the Internet module will automatically reconnect to ADSL and disconnect the ISDN call.

Indicators

The Internet module has six LEDs on the front of the Internet module which indicate the following:

- Active Flashing indicates normal operation
- WAN ADSL line connected
- LAN 1 indicates activity on LAN port 1.
- LAN 2 indicates activity on LAN port 2.
- LAN 3 indicates activity on LAN port 3.
- LAN 4 indicates activity on LAN port 4.

Reset Button

The Internet Module must be reset for some configuration changes to take effect. It can be reset via Ovida or by using the RESET button on the MDF.

Profiles

While the Installation Wizard provides a simple method of setting up the Internet module using the minimum number of settings, the Profile settings provide the user with the ability to also change the default values of other settings for ADSL and ISDN.

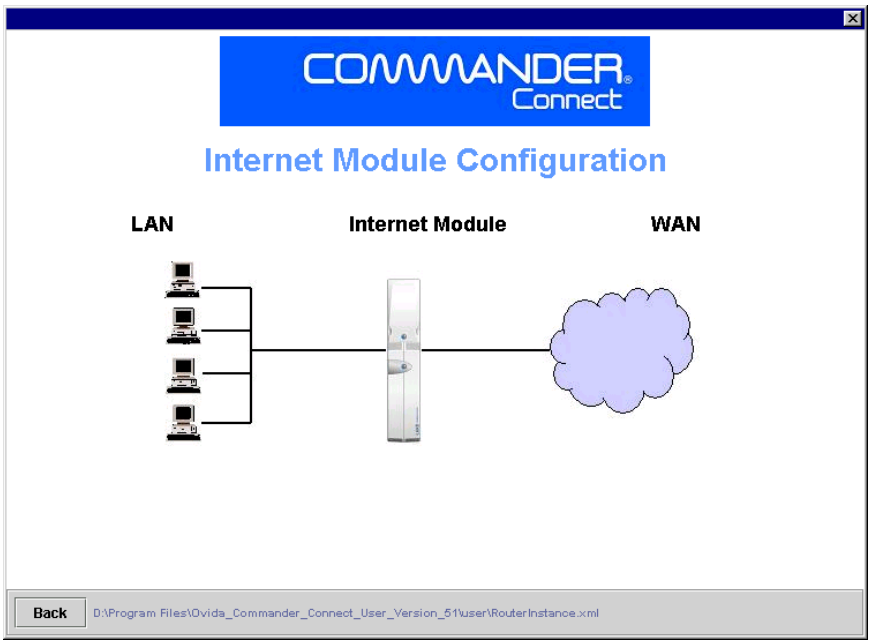
Two profiles can be defined, one for ADSL and one for ISDN.

ADSL profile

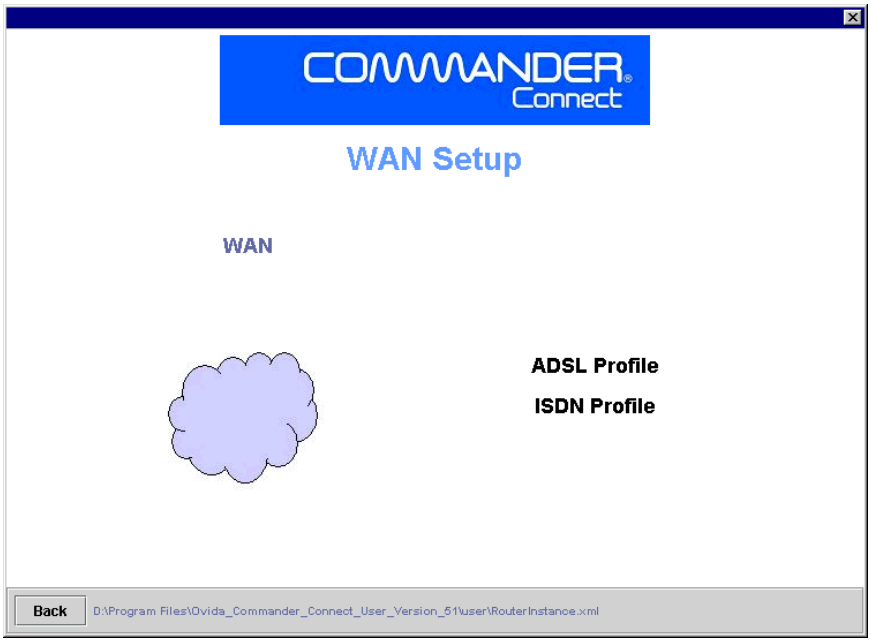
If the Internet module is connected to an ADSL line or modem, the ADSL profile is always used for Internet access. There is also an option to use ISDN for automatic dial backup in the event of ADSL line failure.

The following procedure is used to set up the ADSL profile.

- Select **Internet Module Configuration** on the main screen
- The following screen is displayed.



- Select **WAN**
- The following screen is displayed



- Select **ADSL Profile**
- The following screen is displayed

- Enter the **Username** assigned by the ISP to allow access to the Internet. The username can be up to 30 alphanumeric characters long.
- Enter the **Password** assigned by the ISP to allow access to the Internet. The password can be up to 20 alphanumeric characters long.

- Select **Dial Backup - On** if ISDN dial backup is to be used in the event of ADSL line failure. The default setting is **Dial Backup - Off.**
- **NAT enabled - Yes** is the default setting. This allows all PCs connected to the local LAN to concurrently access the Internet.
- Selecting **PPPoE** or **IP** depends on how the ADSL service is delivered to the end user by the ISP.
    - PPPoE - select PPPoE and proceed to the next step (Profile Enabled)
    - IP (dynamic) - if IP addresses are dynamically assigned by the ISP, select IP and proceed to the next step (Profile Enabled)
    - IP (static) - if IP addresses are statically defined, select IP and enter the relevant IP addresses in the following fields

      Default gateway
      WAN IP address
      WAN Netmask
      Primary DNS
      Secondary DNS
- Set **Profile Enabled - Yes**
- Click on the **Save** button
- Click on the **Send** button
- **Timebands** takes you into the Timebands menu, which allows you to restrict Internet access to certain times of the day. The default setting is that no restrictions are applied. See section on Timebands.

The Internet module is now set up for Internet access using an ADSL line.

ISDN profile

Where the Internet module has no ADSL service, any ISDN line connected to the PABX can be used for Internet access.

The following procedure is used to set up the ISDN profile.

- Select **Internet Module Configuration** on Internet Module screen
- Select **WAN** on Internet Module Configuration screen
- Select **ISDN Profile** on WAN Settings screen
- The following screen is displayed

- Enter the **Username** assigned by the ISP to allow access to the Internet. The username can be up to 30 alphanumeric characters long.
- Enter the **Password** assigned by the ISP to allow access to the Internet. The password can be up to 20 alphanumeric characters long.
- Enter the **Tel No** (telephone number) that the Internet module dials for Internet access.
- Enter the **Backup No** (telephone number). This allows the Internet module to dial an alternative telephone number for Internet access in the event that the first number is unreachable. If no number is entered here then only the first number is used.
- Enter the **Number of Retries**. If the first attempt to dial the ISP is unsuccessful, the number is redialed a number of times which can be set within the range 1 - 10. The default setting is 4 retries. The number of retries applies first to the main telephone number and then to the backup telephone number, if it is used. If a connection cannot be established on the backup number after the last retry, no further attempt is made to establish a connection and the profile is disabled. The profile must be manually reset using the **RESET** button on the MDF.
- Enter the **Retry Interval**. This defines the time interval between retry attempts and can be set within the range 5 - 60 seconds. The default setting is 10 seconds.
- **Cost Control**
  These settings are designed to minimise the cost of ISDN data calls.

During an ISDN call a timer is set to disconnect the call if no data is sent or received for a period of time. Three timers are used:

The **Initial Period** defines the period from the start of the call to the end of the initial billing period. This is designed to be set by the user to the initial billing period of the service provider. The range is between 0 and 60 minutes. The default setting is 3 min.

The **Recurring period** defines the recurring billing period. The range is between 0 and 60 minutes. This is designed to be set by the user to the recurring billing period of the service provider. The range is 0 to 60 minutes. The default setting is 3 min.

The **Idle timer** monitors the call for a period before the expiry of the Initial billing period and subsequent recurring periods. If no data is present during the idle timer period, the call is disconnected at the end of that billing period.

If the Initial Timer and the Recurring Timer are set to zero, no cost control is applied and the call will always remain connected regardless of whether data is present or not until manually disconnected.

If the Initial Timer is set to Zero, and the Recurring Timer is set to a non-zero value, then the call is only monitored for idle periods during the Recurring Period.

If the Initial Timer is set to a non-zero value, and the Recurring Timer is set to zero value, then the call is only monitored for idle periods during the Initial Period. If the call is still connected after the Initial Period, it will remain connected until manually disconnected.

- **Max calls/day** sets a threshold on the maximum number of ISDN calls allowed per day. When this threshold is exceeded, the profile is disabled and must be manually reset using the RESET button on the MDF. The range is 0 -1000. The default setting is 200. If Max calls/day is set to zero, then there is no restriction on the number of calls that can be made in any day.
- **Max call duration** sets the threshold on the maximum duration in hours during any day that calls can be made. The range is 0 - 24 hours.
- **WAN Gateway** is normally left at the default setting, which is 0.0.0.0, which allows the address to be assigned by the ISP at connection setup. If static IP addressing is used, a static IP address is entered here.
- **WAN IP address** is normally left at the default setting, which is 0.0.0.0, which allows the address to be assigned by the ISP at connection setup. If static IP addressing is used, a static IP address that is entered here.
- **WAN NetMask** is normally left at the default setting, which is 0.0.0.0, which allows the Netmask to be assigned by the ISP at connection setup. If static IP addressing is used, the appropriate Netmask is entered here.
- **NAT enabled - yes** is the default setting. This allows all PCs connected to the local LAN to concurrently access the Internet.
- Set **Profile Enabled - Yes.** The profile must be enabled to allow users to use the ISDN for Internet access.
- Click on the **Save** button
- Click on the **Send** button

Additional ISDN Settings

- **Timebands** takes you into the Timebands menu, which allows you to restrict Internet access to certain times of the day. The default setting is that no restrictions are applied. See Timebands for programming options.
- **MLPPP** takes you to the MLPPP menu, which is used to control the ISDN bandwidth available for the connection.

MLPPP

This menu provides the options for adding a second B-channel to the ISDN connection.

- Select **MLPPP** in the ISDN Profile
- The following screen is displayed

Three options are available in the MLPPP menu

- Selecting **Never use** always limits the call to 64 kb/s. A second B-channel will never be invoked.
- Selecting **Always use** always provides 128 kb/s (two ISDN B-channels) for the call. Note that if Always Use is selected and a call is made to an ISP, which does not support MLPPP, both B-channels will be used for the duration of the Initial billing period. The second B-channel will then be dropped and the call will remain connected on a single B-channel.
- Selecting **Dynamic** allows dynamic invocation of the second B-channel on an as-required basis which is controlled by the following parameters

  - **Add threshold** defines the bandwidth threshold for adding the second B-channel. The second B-channel is added if the bandwidth threshold is exceeded in either the transmit or receive direction for the period defined by a delay timer. Bandwidth threshold is specified as a percentage of bandwidth within the range 0 – 100%. The default setting is 80%.

  - **Add timer** sets the delay timer within the range 1 – 60 seconds. The default setting is 10 seconds.

  - **Remove threshold** defines the bandwidth threshold for removing the second B-channel. The second B-channel is removed if the data in both transmit and receive directions on the first B-channel falls below the bandwidth threshold for the period defined by the delay timer. Bandwidth threshold is specified as a percentage of bandwidth within the range 0 – 100%. The default setting is 40%.

  - **Remove timer** is set within the range 1 – 60 seconds. The default setting is 10 seconds.

- Click on the **Save** button
- Click on the **Send** button

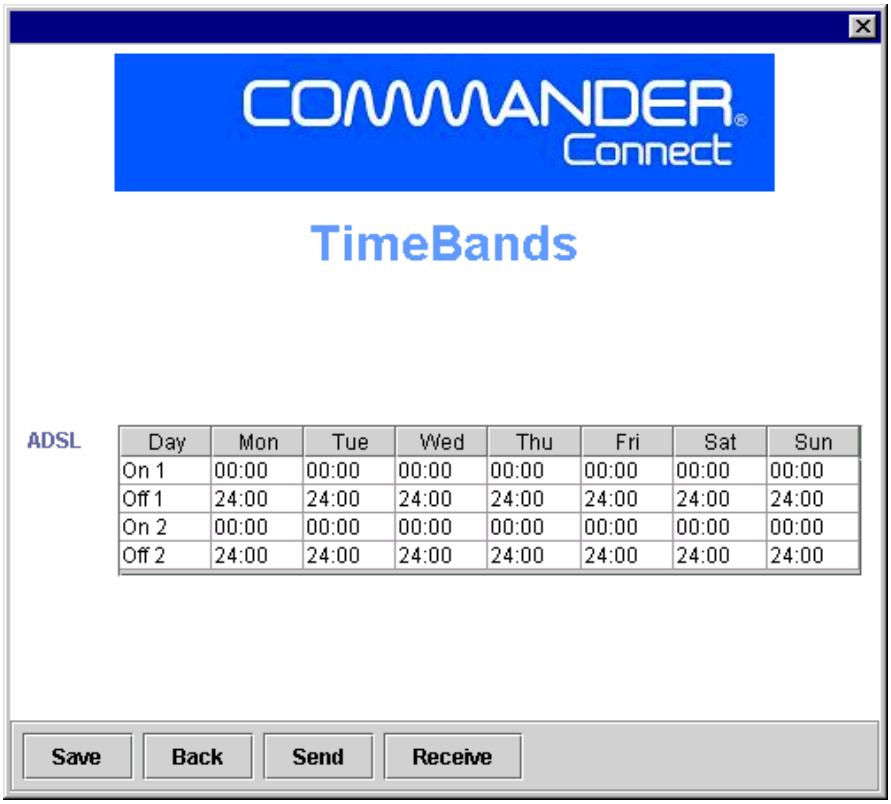
Timebands

Two timebands can be specified for each day of the week to define periods when Internet access is allowed. The default setting is that Internet access is always allowed.

ADSL Timebands

The following procedure is used to program timebands for the ADSL profile.

- Select **Timebands** in the ADSL Profile
- The following screen is displayed



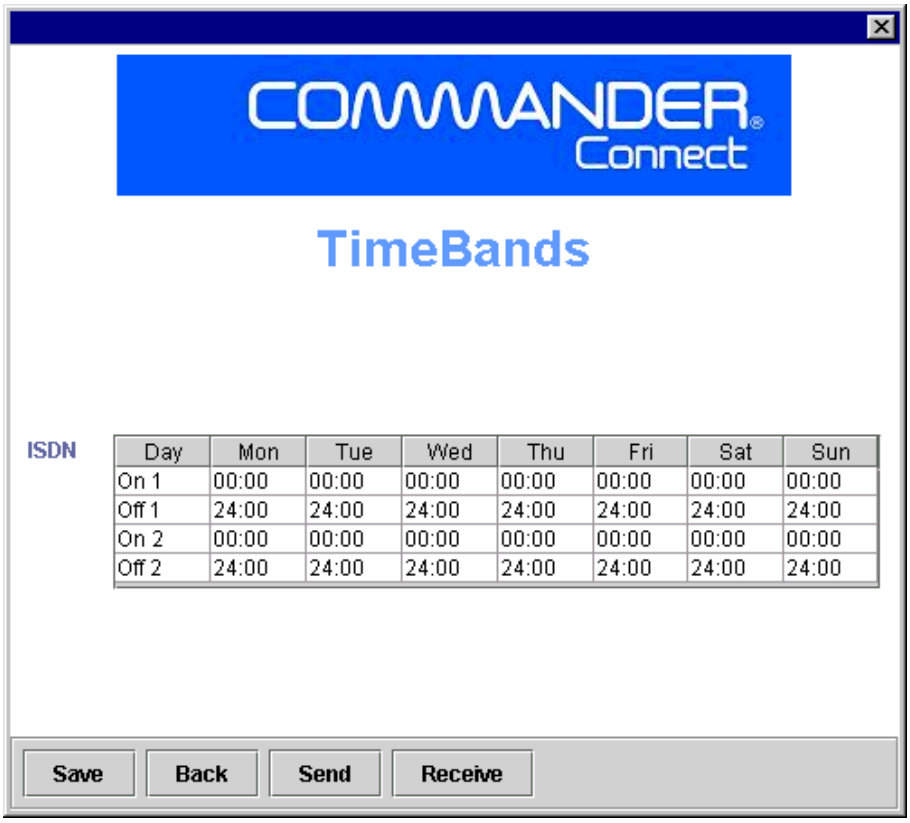
- Set on-time 1(hh:mm) for day of week
- Set off-time 1 (hh:mm) for day of week
- Set on-time 2 (hh:mm) for day of week
- Set off-time 2 (hh:mm) for day of week
- Set on-time 1 for next day, etc.
- Click on the **Save** button
- Click on the **Send** button

ISDN Timebands

Two timebands can be specified for each day of the week to define periods when Internet access is restricted. The default setting is that Internet access is always allowed.

The following procedure is used to program timebands for the ISDN profile.

- Select **Timebands** in the ISDN Profile
- The following screen is displayed



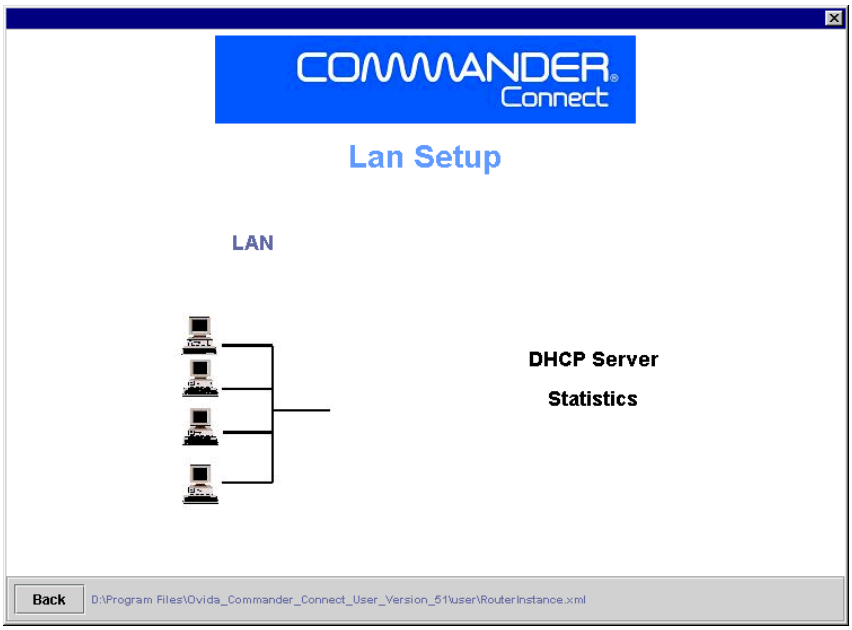
- Set on-time 1(hh:mm) for day of week
- Set off-time 1 (hh:mm) for day of week
- Set on-time 2 (hh:mm) for day of week
- Set off-time 2 (hh:mm) for day of week
- Set on-time 1 for next day, etc.
- Click on the **Save** button
- Click on the **Send** button

DHCP Server

The DHCP server automatically assigns IP addresses to each host on the LAN. It also provides them with a default gateway address, Primary and secondary DNS server address, Primary and Secondary WINS server address, starting IP address, lease duration and number of IP addresses.

The following procedures are used to change the DHCP settings.

- Select **LAN** on the Internet Module Configuration menu
- The following screen is displayed



- Select **DHCP Server**
- The following screen is displayed

- The **LAN gateway address** defines the address of the Internet Module and is set by default to 192.168.1.1. All traffic destined for the Internet is sent to this address and the Internet Module then forwards the traffic. This address can be changed if static addressing is used or if all IP traffic is to be sent to a different gateway on the LAN.

- The **LAN gateway Netmask** defines the subnet mask to be applied to the Default gateway address. This can be changed if the Gateway address is changed from the default setting.

- The **Primary DNS Server** is the address to which all requests to resolve domain names are sent. With the default setting 192.168.1.1, all requests are sent to DNS relay, which in turn forwards the requests to a DNS server at the ISP. If a different Primary DNS server is to be used, the address can be entered here. This applies to ISDN only. For ADSL see DNS Relay below.

- The **Secondary DNS Server** is set by default to 0.0.0.0. to forward requests to the secondary DNS server at the ISP. If a different secondary DNS is to be used, the address is entered here. If a different Secondary DNS server is to be used, the address can be entered here. This applies to ISDN only. For ADSL see DNS Relay below.

- The **Primary WINS server** is the address of the primary WINS server on the local LAN.

- The **Secondary WINS server** is the address of the secondary WINS server on the local LAN.

- The **Starting IP address** is the first IP address to be automatically assigned to a LAN host. The default setting is 192.168.1.2. Subsequent addresses assigned follow in ascending order. A different starting IP address can be assigned if required and subsequent numbers in the range follow in ascending order.

- The **Number of Addresses** defines how many IP addresses the DHCP server can assign. Up to 100 addresses can be allocated and the default setting is 100.

- **Duration Units** defines the units of time used for the IP address lease. Days, Hours or Minutes can be defined. The default setting is days.

- The **Lease duration** is the period for which the IP address is assigned to a host. The default setting is 3 days.

- **DHCP server enabled** - **Yes** option turns the DHCP server on. The default setting is On. Off should only be selected if another DHCP server is connected to the LAN or static addressing is required.

- **DNS Relay Enabled** - **On** turns DNS Relay on. The default setting is DNS Relay On.

  ISDN only **-** DNS Relay should only be turned Off if a server other than that negotiated with the ISP is to be used. The static IP addresses should be inserted in the Primary and Secondary DNS Server fields.

  ADSL only - static addresses should be inserted in the Primary and Secondary DNS server fields in the ADSL Profile and DNS Relay should be On.

- Click on the **Save** button

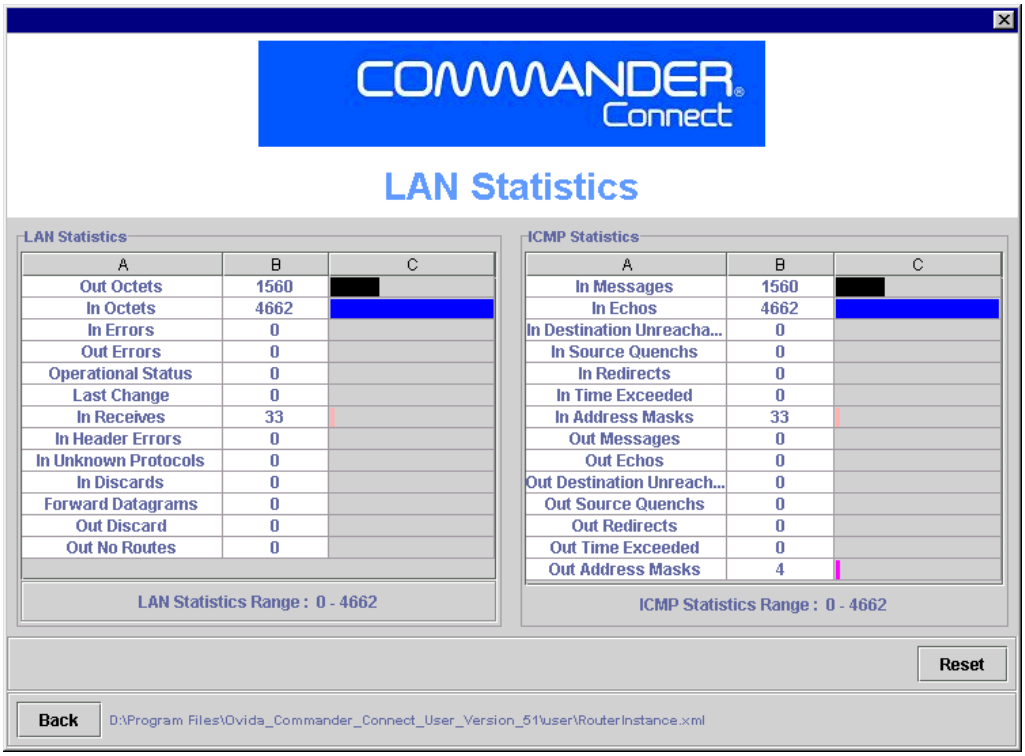
- Click on the **Send** button

- Press the **RESET** button when prompted by Ovida or press the reset button on the MDF for the changes to take effect.

Statistics

To view Internet Module statistics

- Select **Statistics** on the LAN Setup screen
- The following screen is displayed



- **RESET** sets all counters to zero.

LAN Statistics

Statistic	***Description***
InHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options. Some vendors, including Cisco, increment this object when TTL is exceeded, so traceroutes can affect it.
InUnknownProtocols	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported layer 4 protocol. Note that these are packets destined for this device and not simply forwarded to it at layer 2 or 3.
InDiscards	The number of IP packets received successfully by this device and then dropped during input processing, even though they did not contain errors. This is often the result of either resource limitations (e.g lack of buffer space) or traffic shaping, but can also be caused by filters.
ForwDatagrams	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets which were Source-Routed via this entity, and the Source- Route option processing was successful
OutDiscards	The number of IP packets successfully received by this device and then dropped during output processing, even though they did not contain errors. This is often the result of either resource limitations or traffic shaping, but can also be caused by filters. Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
OutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this `no-route' criterion. Note that this includes any datagarms which a host cannot route because all of its default gateways are down.

ICMP Statistics

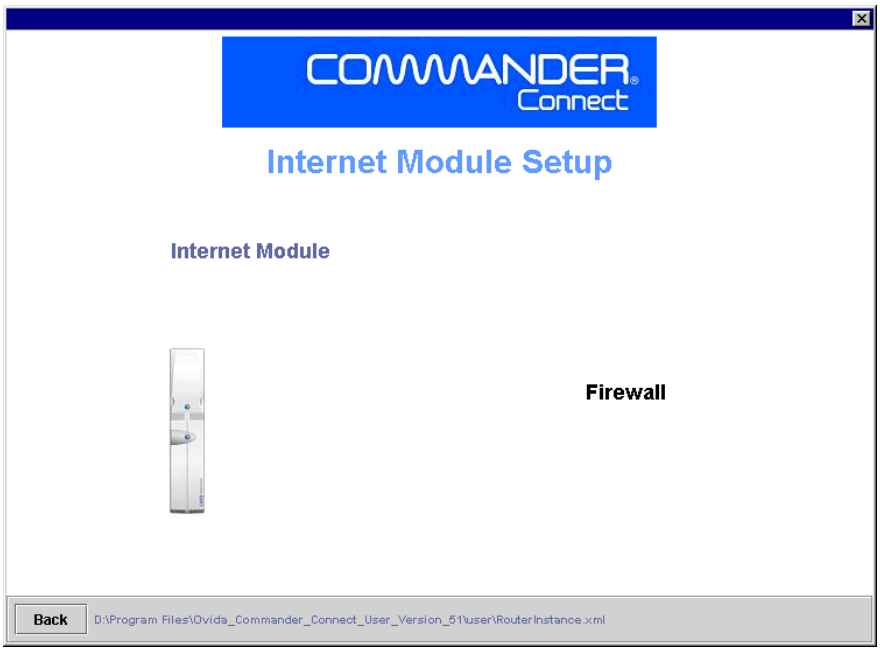
Statistic	*Description*
OutOctets	The total number of octets transmitted out of the interface, including framing characters.
InOctets	The total number of octets received on the interface, including framing characters.
InErrors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol
OutErrors	The number of outbound packets that could not be transmitted because of errors
OperStatus	Indicates the state of each interface.
LastChange	Indicates last Internet Module reset
InEchos	The number of ICMP Echo (request) messages received
InDestUnreachable	The number of ICMP Destination Unreachable messages received
InSrcQuenches	The number of ICMP Source Quench messages received
InRedirects	The number of ICMP Redirect messages received
InTimeExcds	The number of ICMP TTL Exceeded messages received. In small volumes this is often the result of Traceroutes. Larger volumes may indicate routing instability or loops.
InAddrMasks	The number of ICMP Address Mask Request messages received
Outmsgs	The total number of ICMP messages which this device attempted to send.
OutEchos	The number of ICMP Echo (request) messages sent
OutDestUnreachs	The number of ICMP Destination Unreachable messages sent
OutSrcQuenchs	The number of ICMP Source Quench messages sent
OutRedirects	The number of ICMP Redirect messages sent
OutTimeExcds	The number of ICMP TTL Exceeded messages sent. In small volumes this is often the result of Traceroutes. Larger volumes may indicate routing instability or loops.
OutAddrmasks	The number of ICMP Address Mask Request messages sent.

Firewall

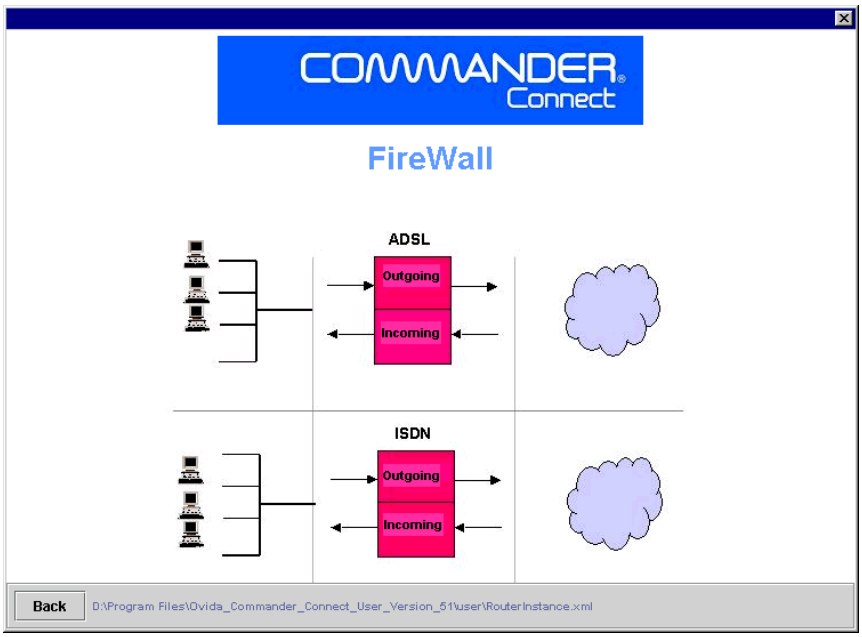
A firewall is used to restrict access between the internal LAN and the Internet. The firewall consists of packet filters, which are used to control the flow of traffic between the internal LAN and the Internet. All traffic passing through the Internet module is examined and compared to a set of packet filtering rules. Traffic can be allowed to pass through, or it can be blocked depending on the rules defined by the user.

The following procedure is used to program the firewall.

- Select **Internet Module Configuration** from the main menu
- Select **Internet Module** from the Internet Module Configuration menu
- The following screen is displayed



- Select **Firewall** from the Internet Module Setup menu.
- The following screen is displayed



Filter Stacks

Up to 8 filters can be defined for each of the following:

- ADSL incoming traffic
- ADSL outgoing traffic
- ISDN incoming traffic
- ISDN outgoing traffic

Filters

Each filter has fields whose contents are compared to every IP packet passing through the firewall. If the contents of any field match the corresponding information in an IP packet, the packet is either blocked or allowed to pass through to the next filter. The next filter carries out the same operation on the IP packet using the criteria defined in it's fields and so on.

Each field is programmed as follows

- **INC**
  A ✔ in this box indicates that a filter is enabled and that the contents of the fields are compared to IP traffic. If the box is blank (not ✔) then the filter is not applied.

- **No**
  Each filter is numbered from 1 - 8. This field is not programmable.

- **Action**
  This field has a drop-down menu with two items. Selecting ✔ allows any packet through whose contents match any of the remaining fields in the filter. Selecting ✕ blocks any packet whose contents match any of remaining fields in the filter.

- **Protocol**
  This field defines a protocol and has a drop-down menu with four items.

  - ALL compares the protocol field in the IP packet to the UDP, TCP and ICMP protocols
  - UDP compares the protocol field in the IP packet to the UDP protocol only
  - ICMP compares the protocol field in the IP packet to the ICMP protocol only
  - TCP compares the protocol field in the IP packet to the TCP protocol only

- **Source Address**
  The filter compares the source address of the IP packet and with the address specified in this field

- **Source NetMask**
  This is used in combination with the source address field to specify a network address and compare it with the network address of the IP packet.

- **Destination Address**
  The filter compares the destination address of the IP packet and with the address specified in this field

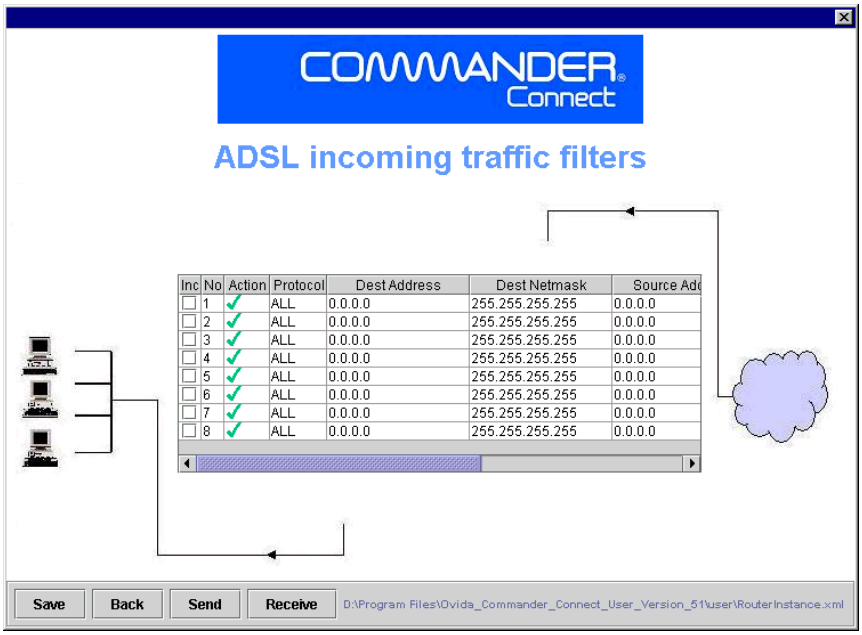
- **Destination NetMask**
  This is used in combination with the destination address field to specify a network address and compare it with the network address of the IP packet.

- **Start port**
  A range of TCP or UDP destination ports can be defined. This defines the start of the range.

- **End port**
  This defines the end of the TCP or UDP destination ports range.

ADSL incoming filter stack

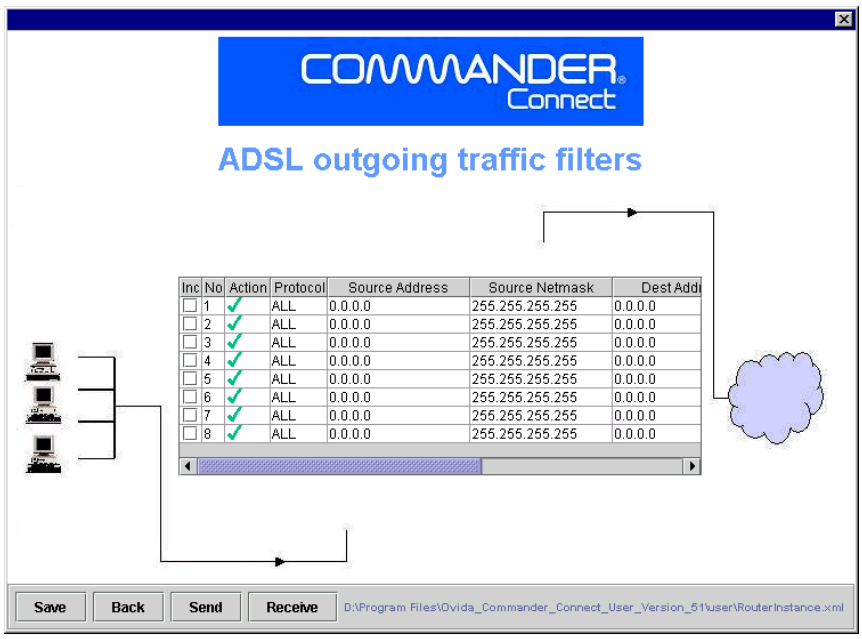
Up to eight filters can be applied to incoming ADSL traffic



- Program filter fields as defined above
- Click on the **Save** button
- Click on the **Send** button

ADSL outgoing filter stack

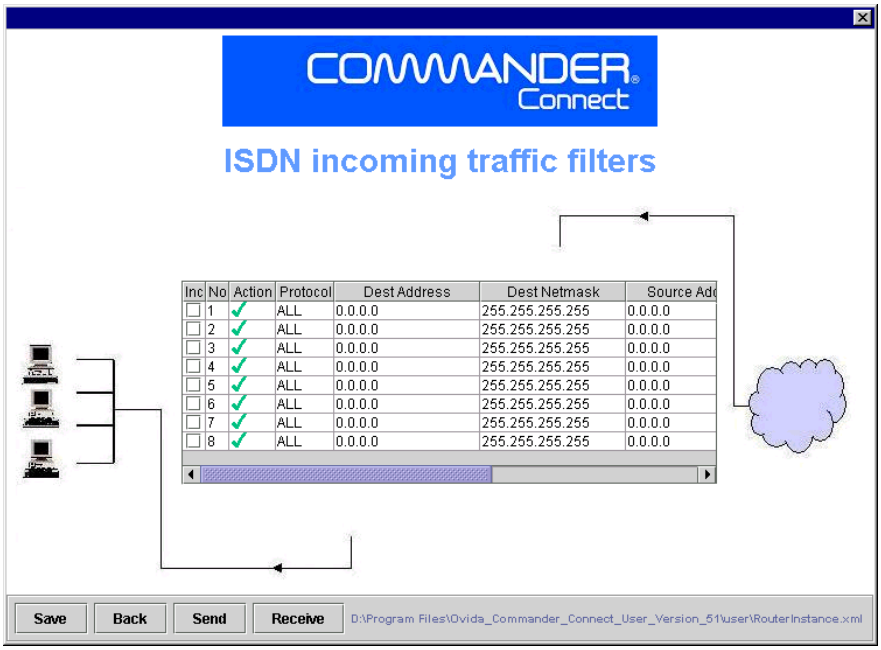
Up to eight filters can be applied to outgoing ADSL traffic



- Program filter fields as defined above
- Click on the **Save** button
- Click on the **Send** button

ISDN incoming filter stack

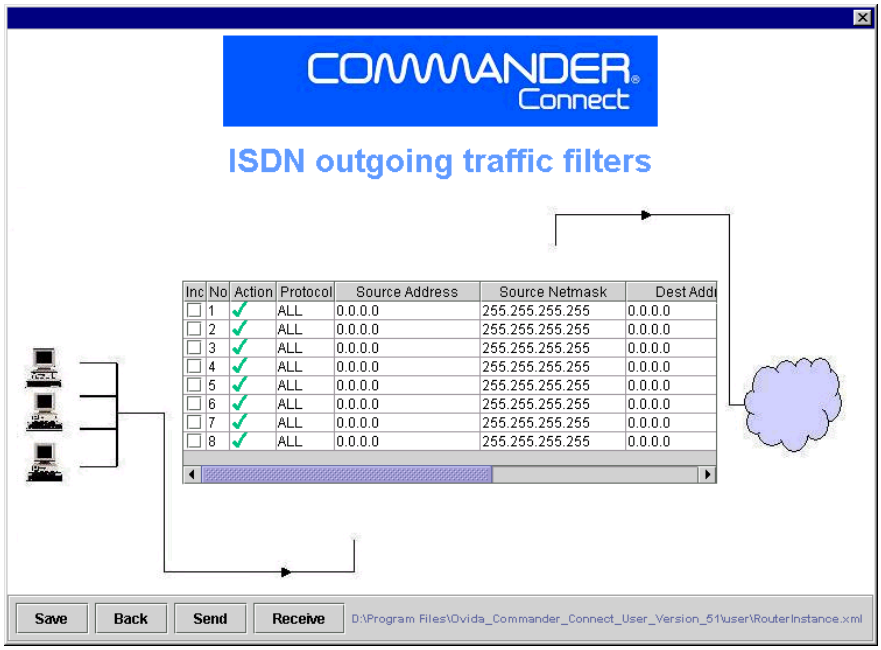
Up to eight filters can be applied to incoming ISDN traffic.



- Program filter fields as defined above
- Click on the **Save** button
- Click on the **Send** button

ISDN Outgoing filter stack

Up to eight filters can be applied to outgoing ISDN traffic.

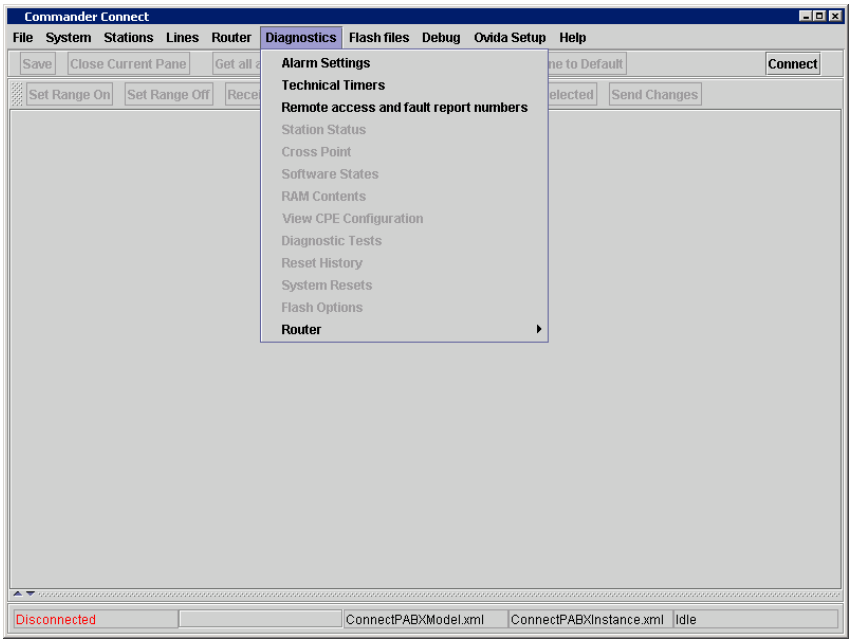


- Program filter fields as defined above
- Click on the **Save** button
- Click on the **Send** button

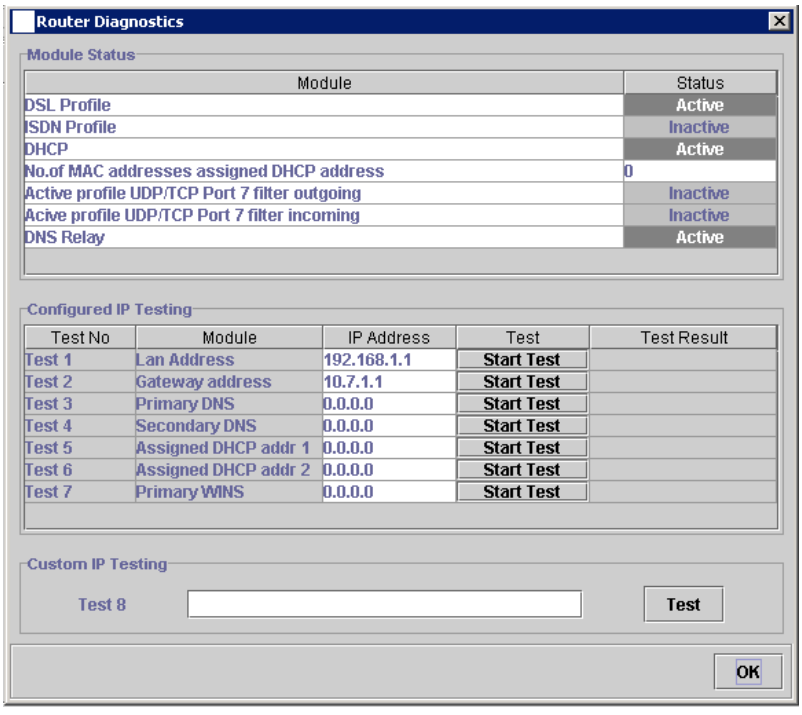
Diagnostics

Diagnostic tests for the Internet Module are accessed via the main system screen.

- Select **Diagnostics**
- The following screen is displayed



- Select **Internet Module**
- The following screen is displayed



- Module status shows the current status of:

  - DSL Profile (Active/Inactive)
  - ISDN Profile (Active/Inactive)
  - DHCP Server (Active/Inactive)
  - Number of IP addresses assigned to LAN hosts
  - Active profile UDP/TCP port 7 filter outgoing (Active/Inactive). When active, all characters sent are echoed back (Loopback test)
  - Active profile UDP/TCP port 7 filter outgoing (Active/Inactive). When active, all characters received are echoed back (Loopback test)
  - DNS Relay (Active/Inactive)

- Configured IP testing pings the associated IP address displayed in the IP address field for Test 1 - 7 and displays the test result.

- Custom IP testing (Test 8) pings the IP address entered in the field and displays the test result. Any IP address can be entered here.

Specifications

LAN	4 x 10/100 Base-T ports, autosensing
ADSL	10 Base-T port for external ADSL modem PPPoE, Dynamic IP, Static IP supported
ISDN	Access to B-chans on PABX PPP, MLPPP, BACP
Protocols	IP V4
Authentication	Automatic PAP/CHAP negotiation
DHCP	DHCP server supports up to 100 IP addresses
Routing	Static routing
Firewall	NAT, Packet filtering
Call management	Idle timers Time of day restrictions
Management	Local management Remote management