netopia

MAKING BROADBAND WORK™

Netopia Firmware Version 4.11 Release Note

July 15, 2002

This release note includes information that supplements the *User's Reference Guide* and the *4.10 Firmware Addendum* with information for the Netopia R-Series Routers. Please read it carefully. It lists changes incorporated in this firmware release.

The 4.11 firmware release incorporates a number of bug fixes as well as the following changes in functionality:

These notes cover the following topics:

ICMP Ping from Multiple LAN Hosts

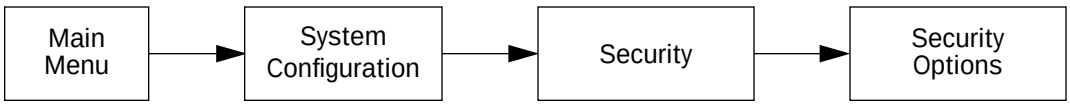
Firmware version 4.10.1 introduced enhanced ICMP ALG support for multiple Pings. This allows you simultaneously to Ping a single external public host address from multiple PCs on your LAN behind a PAT (Port Address Translation) connection. For more information on the Ping utility, see your *User's Reference Guide* section on "Utilities & Diagnostics."

Console Tiered Access – Two Password Levels

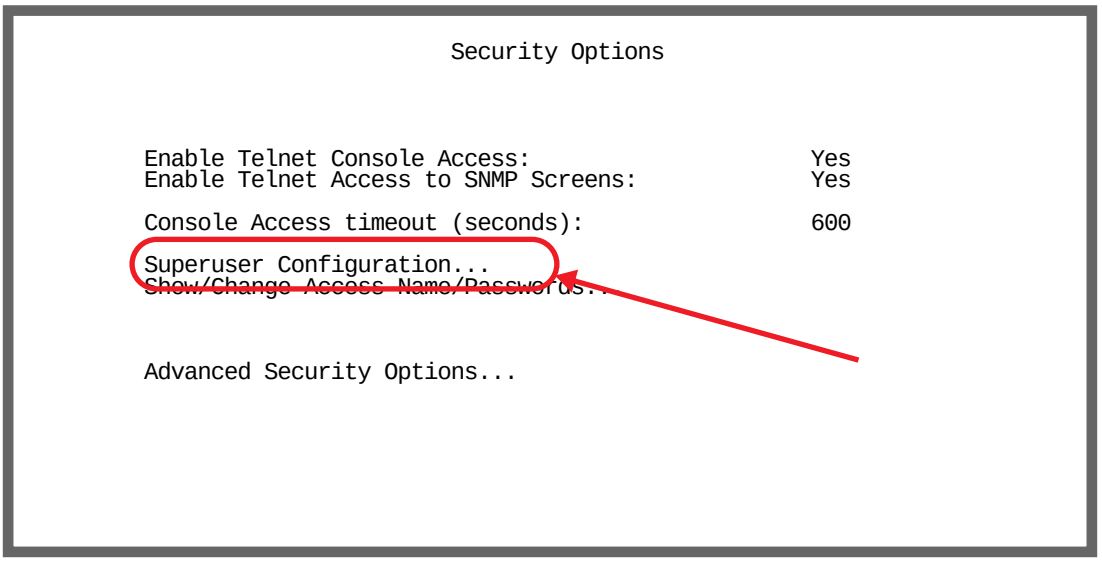
Firmware Version 4.11 offers tiered access control for greater security and protection against accidental or malicious misconfiguration. Service providers and network administrators can now limit the access of other users to the various configuration screens to prevent misconfigurations.

The access privileges of various users that may be assigned are governed by a *Superuser* administrative account. The Superuser can assign different privileges to *Limited* users who will be accessing the router functions in some way.

Configuration access names and passwords are specified in the **Security Options** screen. From the Main Menu, select **System Configuration**, then **Security**.



The **Security Options** screen appears.

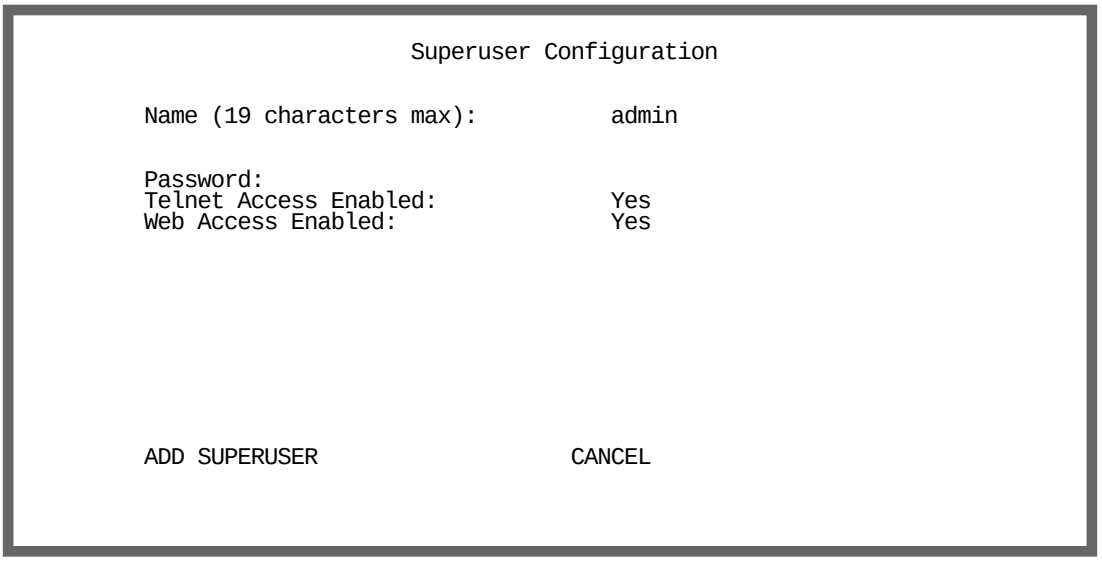


Superuser configuration

The access privileges of the Superuser account are not modifiable. It is possible, however, to control who can log in as Superuser. You can limit this to serial console only.

Select **Superuser Configuration** and press **Return**.

The Superuser Configuration screen appears.

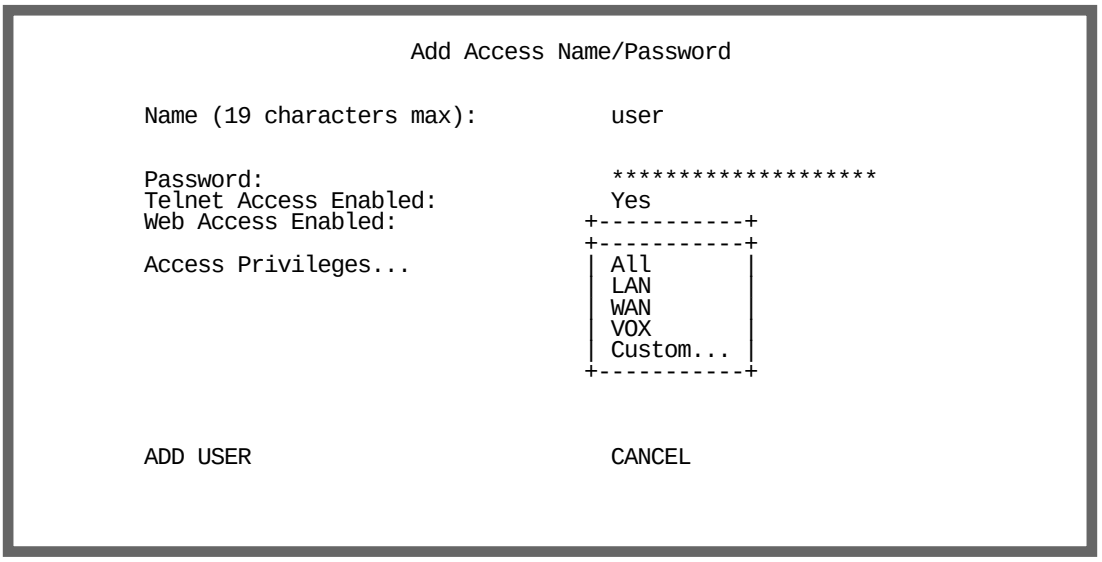


- Assign a Superuser **Name**. It can be up to 19 characters long. It is good practice *not* to use any easily-guessed combination such as your birthday.
- Assign a **Password**. Keep this password secure. If you lose or forget it, you will not be able to access the router without factory defaulting it, thereby losing all of your configuration information.
- You can disable Telnet or Web Access. This may be useful for extra security in preventing remote attempts to access the router.
- Select **ADD SUPERUSER** and press **Return**. The Superuser account is now configured.

  You will be challenged for this name and password every time you attempt to log into the router.

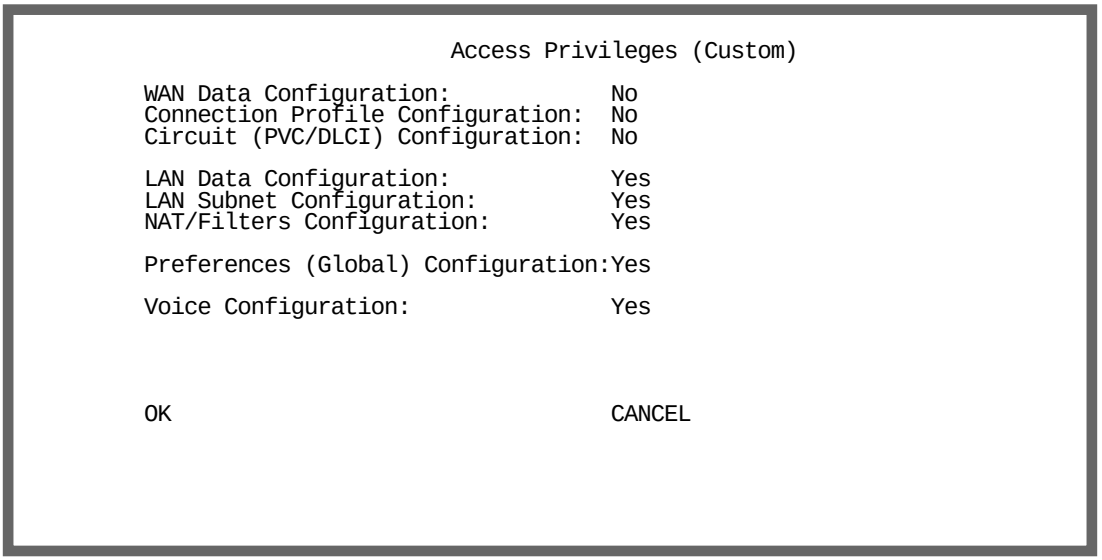
Limited user configuration

The Add Access Name/Password and Show/Change Access Name/Passwords screens allow you to select which configuration features a limited (non-Superuser) user can access. From the Security Options screen, select **Add Access Name/Password**. The Add Access Name/Password screen appears.



- Assign a User Name and Password, and enable or disable Telnet and Web access as in the Superuser Configuration screen.
- Select **Access Privileges**, and from the pull-down menu, choose which access privilege you want this user to have: **All**, **LAN**, **WAN**, or for IADs only, **VOX**.

  If you assign any of these privileges, limited users will have full access to privileges associated with these interfaces. You can customize these privileges further, in order to limit access to only certain portions of those interfaces' configuration, by selecting **Custom**. If you select Custom, the **Access Privileges (Custom)** screen appears.



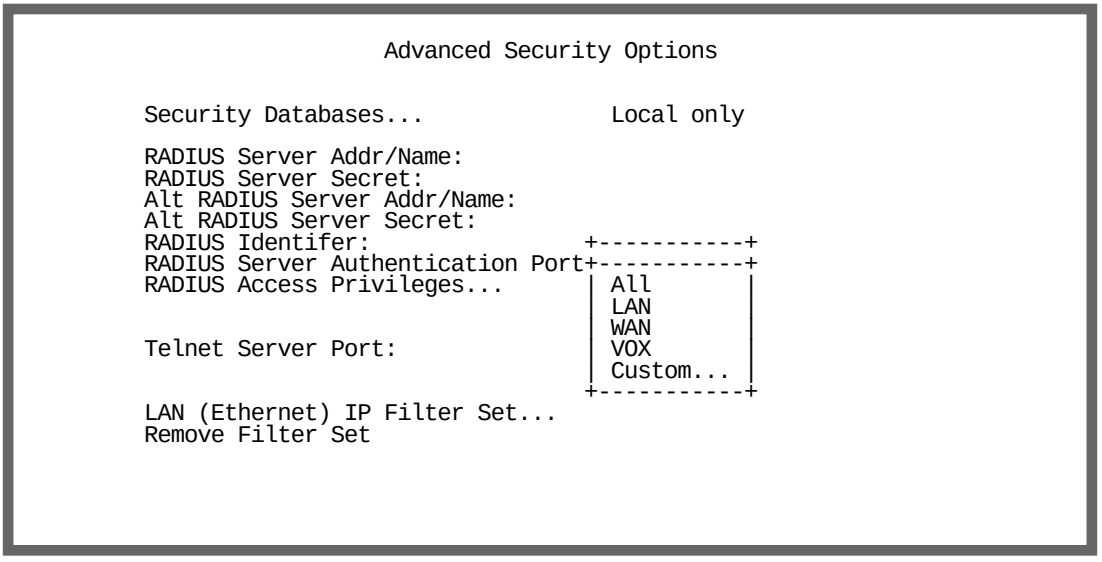
You can toggle the default user privileges for each user. The defaults are set to minimize the possibility of an individual user inadvertently damaging the WAN connection. Exercise caution in assigning privileges other than these defaults to limited users.

Access Privilege	Default
WAN Data Configuration	No
Connection Profile Configuration	No
Circuit (PVC/DLCI) Configuration	No
LAN Data Configuration	Yes
LAN Subnet Configuration	Yes
NAT/Filters Configuration	Yes
Preferences (Global) Configuration	Yes
Voice Configuration (IADs only)	Yes

Advanced Security Options

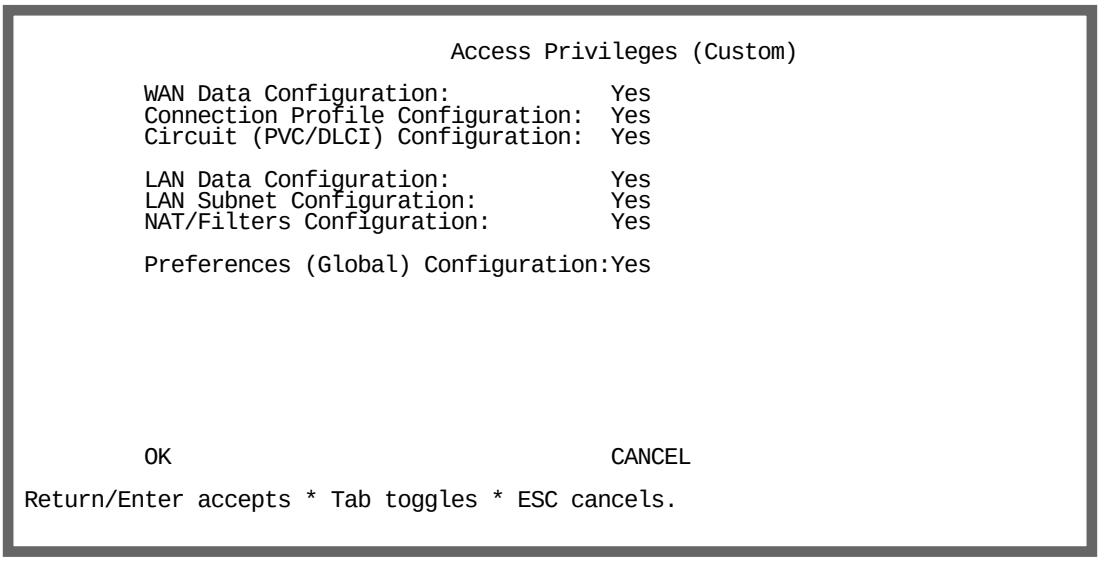
The Advanced Security Options screen allows you to configure the global access privileges of users authenticated via a RADIUS server.

From the Security Options screen, select **Advanced Security Options**. The Advanced Security Options screen appears.



- Select **RADIUS Access Privileges**, and from the pull-down menu, choose which access privilege you want this user to have: **All**, **LAN**, **WAN**, or for IADs only, **VOX**.

  If you assign any of these privileges, limited users will have full access to privileges associated with these interfaces. You can customize these privileges further, in order to limit access to only certain portions of those interfaces' configuration, by selecting **Custom**. If you select Custom, the **Access Privileges (Custom)** screen appears.



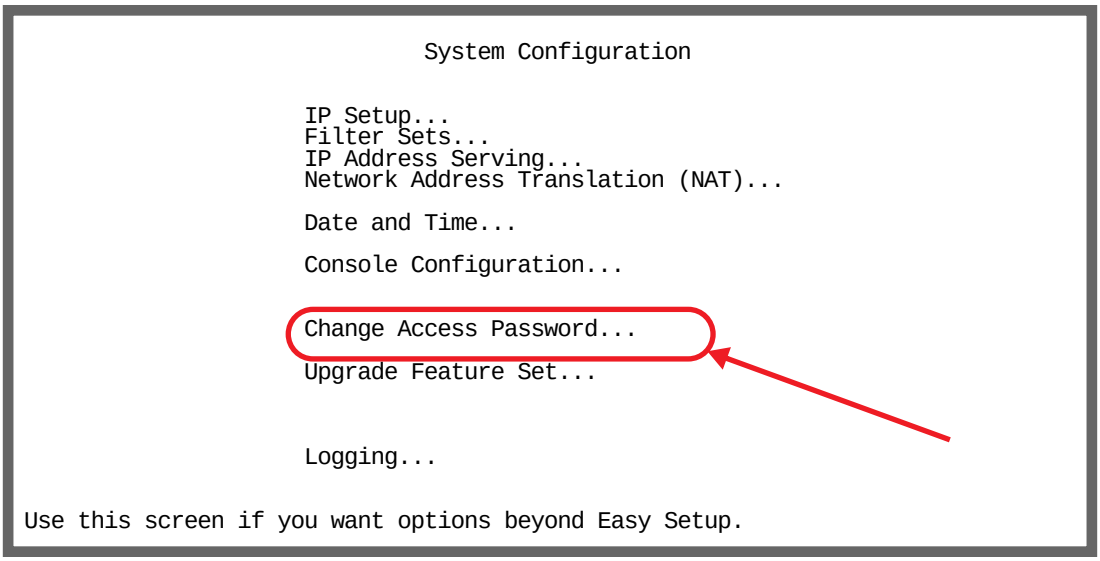
Since authentication via RADIUS server is, by definition, authentication of remote users, the WAN-related defaults are preset to Yes. Toggle any that should be changed.

User access password

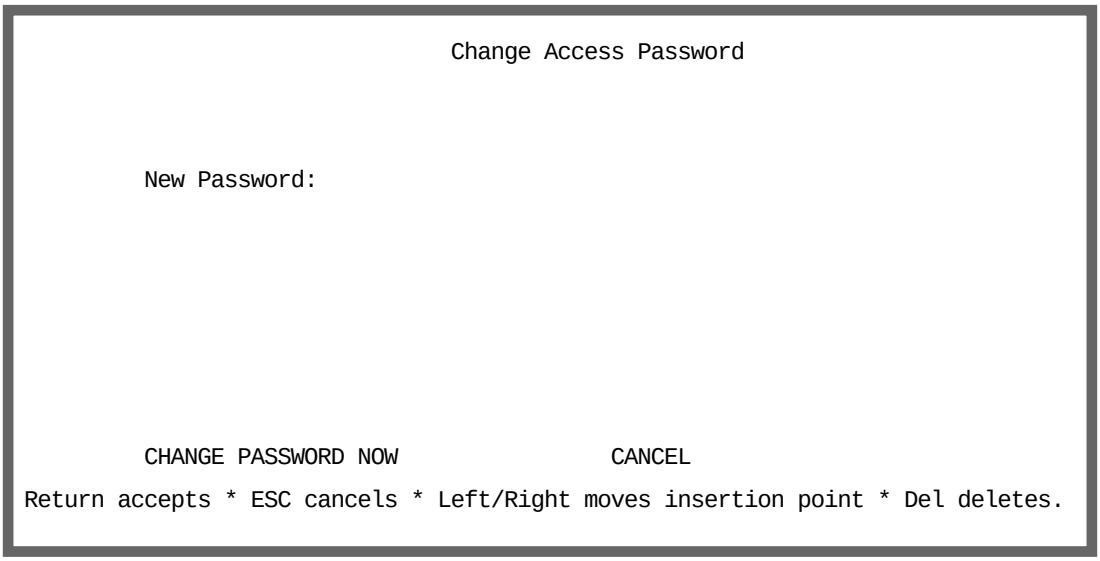
Users must be able to change their names and passwords, regardless of other security access restrictions.

If a user does not have security access, then they will only be able to modify the password for their account.

When a limited-access user logs into the router. and accesses the System Configuration menus, the only Security option displayed is **Change Access Password**.



Selecting this option displays the **Change Access Password** screen.



When changing a password, you will be challenged to enter it again to be sure you have entered it correctly.

User menu differences

Menus reflect the security access level of the user. Consequently, configuration menus will display differing options based upon the parameters a particular user is allowed to change. Some differences include:

- Limited users (non-Superusers) do not have access to Easy Setup.
- All users have access to System Configuration, Quick Menus, and Quick View, but limited users have only limited access to configuration elements in their descendant menus.
- Configuration screen elements to which configuration access is forbidden are usually hidden.
- The Quick Menus screen reflects the security access level of the user. Menus to which configuration access is forbidden are hidden.

Main Menu

The following is an example comparison of the Main Menu as seen by the Superuser and by a Limited user.

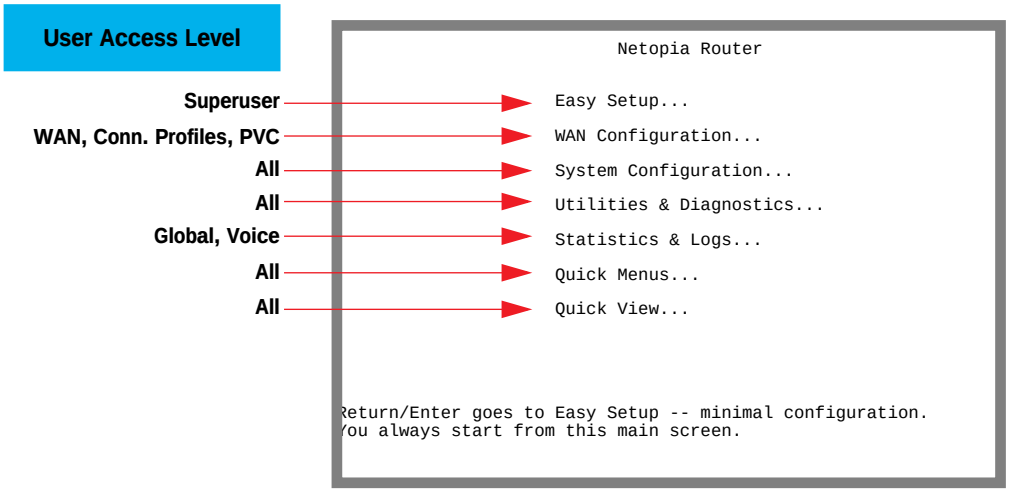
Superuser

```
Netopia Router

Easy Setup...
WAN Configuration...
System Configuration...
Utilities & Diagnostics...
Statistics & Logs...
Quick Menus...
Quick View...

Return/Enter goes to Easy Setup -- minimal configuration.
You always start from this main screen.
```

Limited user

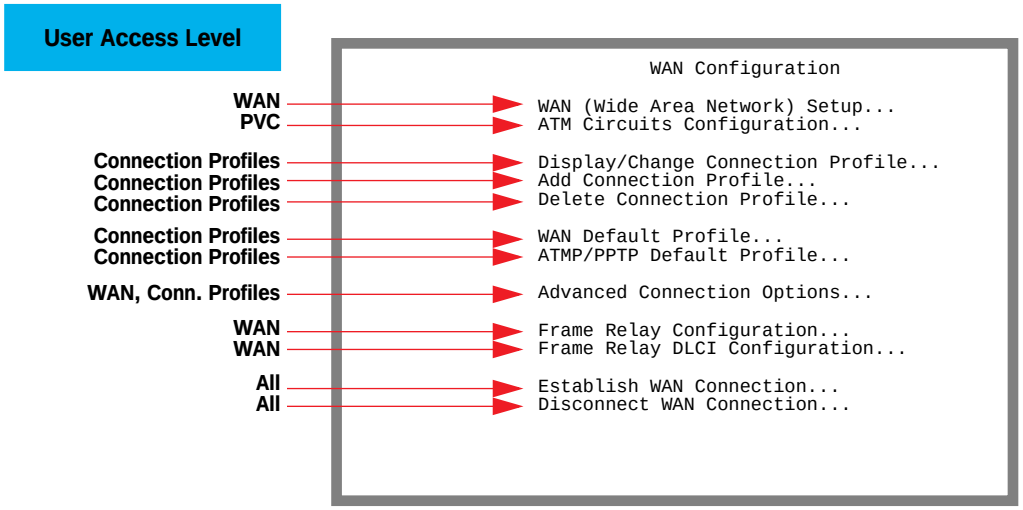
```
Netopia Router

System Configuration...
Utilities & Diagnostics...
Statistics & Logs...
Quick Menus...
Quick View...

Return/Enter goes to Easy Setup -- minimal configuration.
You always start from this main screen.
```

Based on access level, the Main Menu displays its configuration options according to the following diagram:

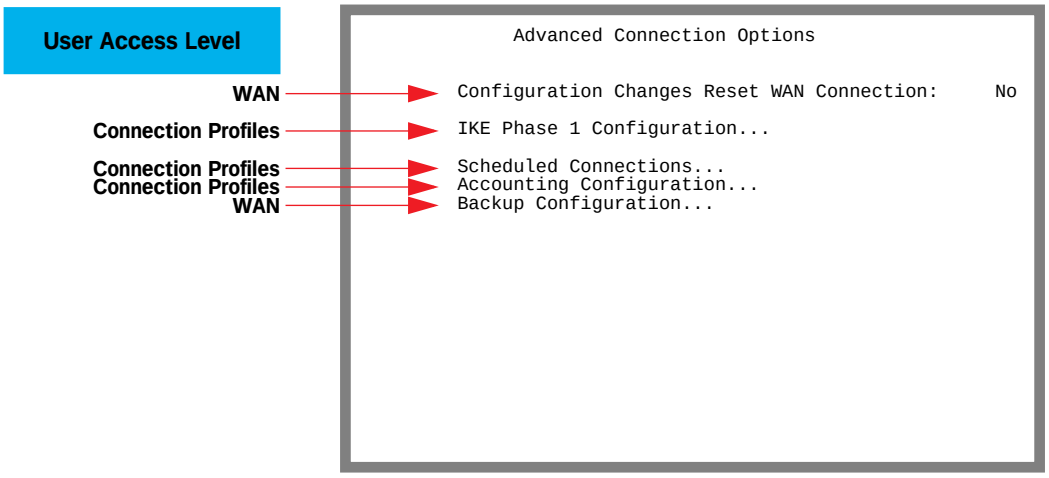


WAN Configuration screens

If a limited user is allowed WAN, Connection Profile, or PVC configuration access, the WAN Configuration option in the Main Menu is visible. If a limited user selects **WAN Configuration** in the Main Menu, the WAN Configuration screen displays its configuration options according to the following diagram:

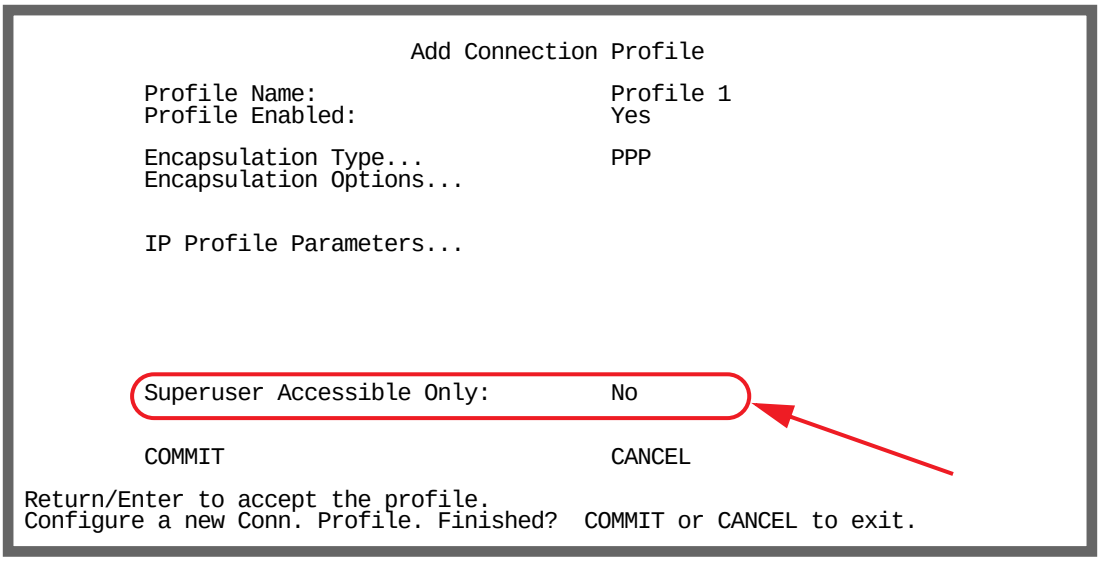


If a limited user selects **Advanced Connection Options** in the WAN Configuration menu, the Advanced Connection Options screen displays its configuration options according to the following diagram:



Connection Profiles

The Superuser can disallow limited user access to a particular Connection Profile. When adding a Connection Profile in the Add Connection Profile screen the Superuser can toggle the **Superuser Accessible Only** option to **Yes** or **No**.

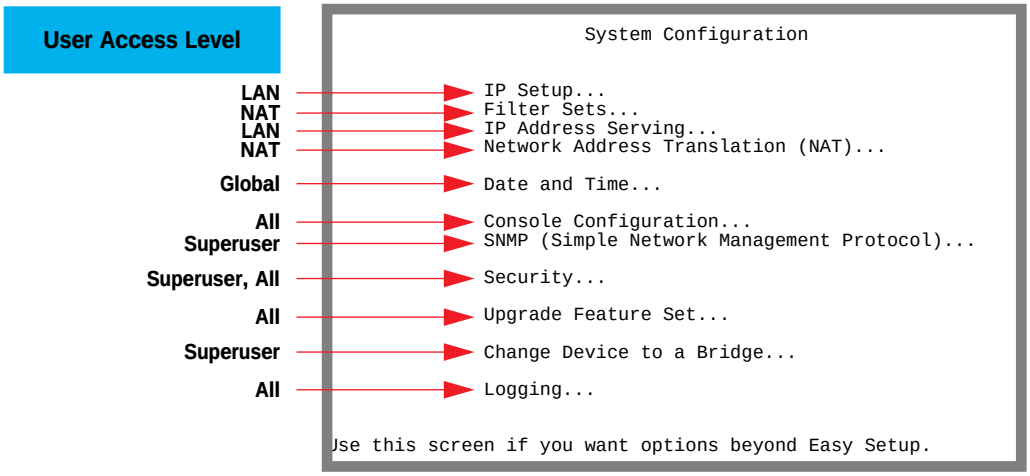


This option is visible whether or not there are authorized username/passwords other than the Superuser.

The Superuser can also change the user accessibility after creating a Connection Profile or a limited user in the **Change Connection Profile** screen.

System Configuration menu

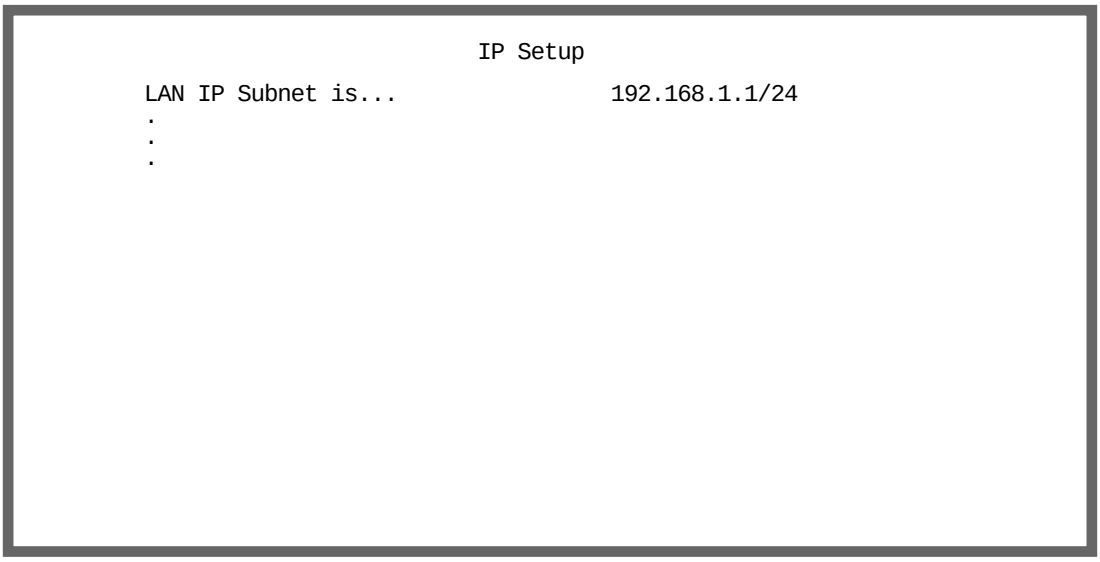
The System Configuration menu is always available to all users. Based on access level, the System Configuration menu displays its configuration options according to the following diagram:



Note: **Network Address Translation (NAT)** is displayed in this screen in order to make access control simpler. **Security** becomes **Change Access Password** for non-Superusers, and provides access to the associated menu described previously.

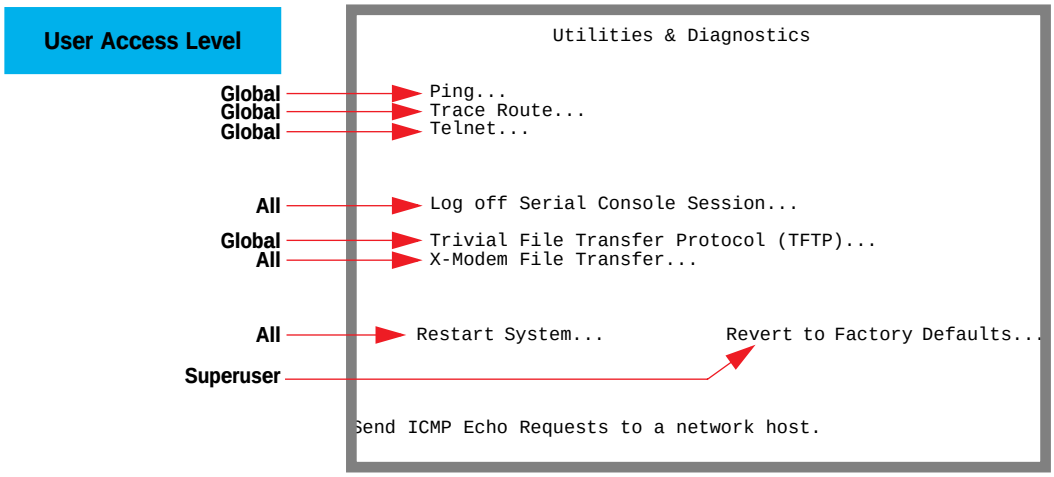
IP Setup menu

In the IP Setup menu, users that do not have LAN Subnet Configuration access will see a screen similar to the following:



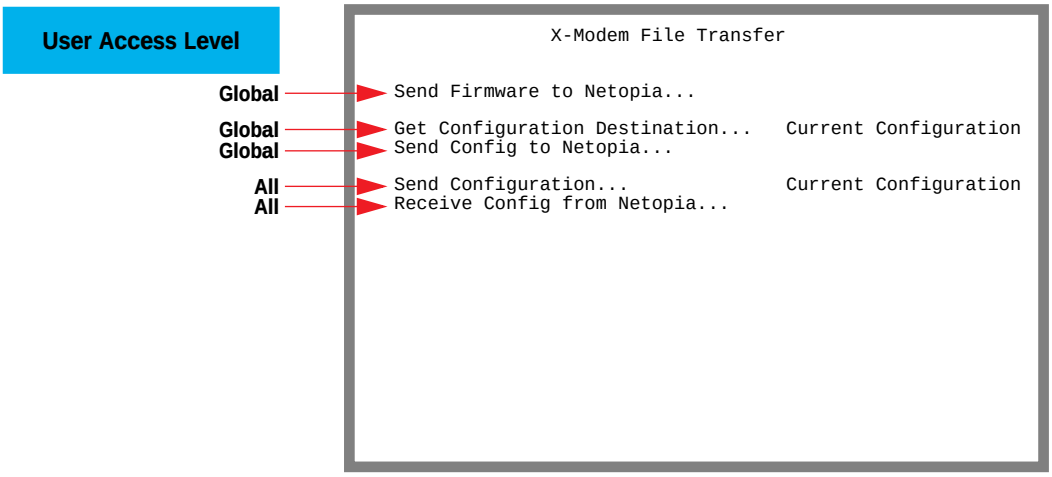
Utilities & Diagnostics menu

Based on access level, the Utilities & Diagnostics menu displays its configuration options according to the following diagram:



X-Modem File Transfer menu

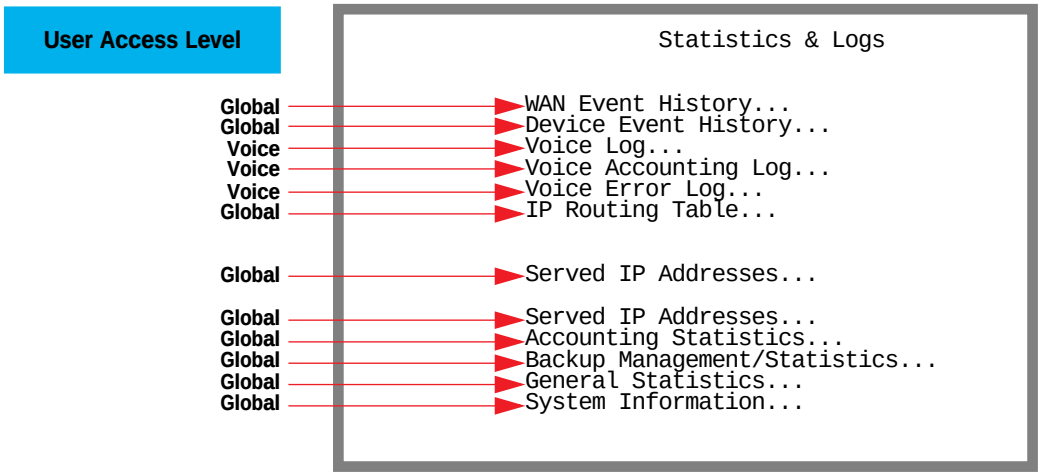
Based on access level, the X-Modem File Transfer menu displays its configuration options according to the following diagram:



Statistics & Logs menu

The Statistics & Logs menu shown below is a composite of all the possible options on all Netopia routers and IADs supported by the firmware. Substantial differences exist among screens on a given router or IAD. Here, all selection options are shown.

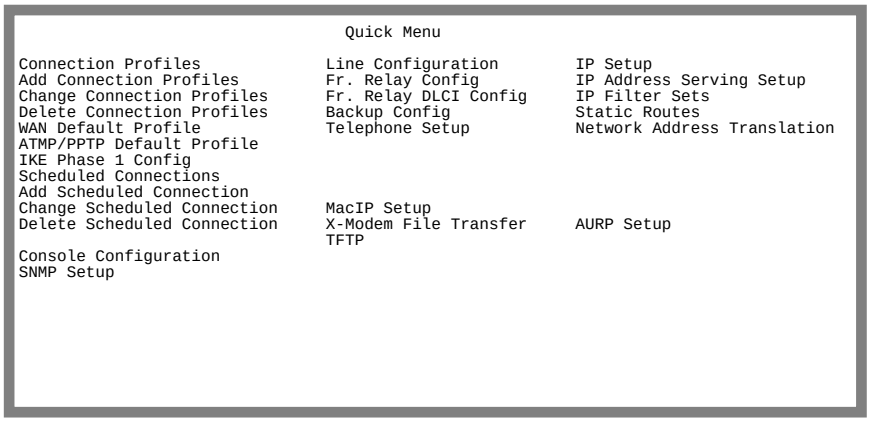
Based on access level, the Statistics & Logs menu displays its options according to the following diagram:



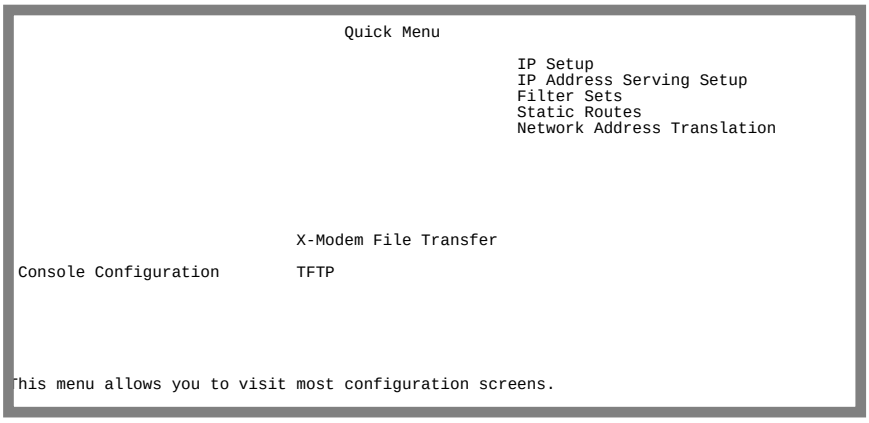
Quick Menus

Quick Menus vary considerably between models, features, and access levels. The following is an example comparison of the Quick Menu as seen by the Superuser and by a Limited user.

Superuser



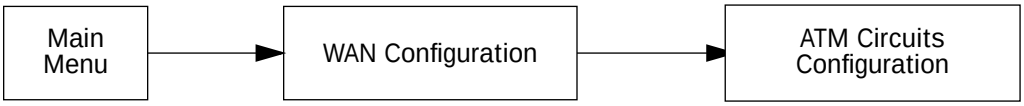
Limited user



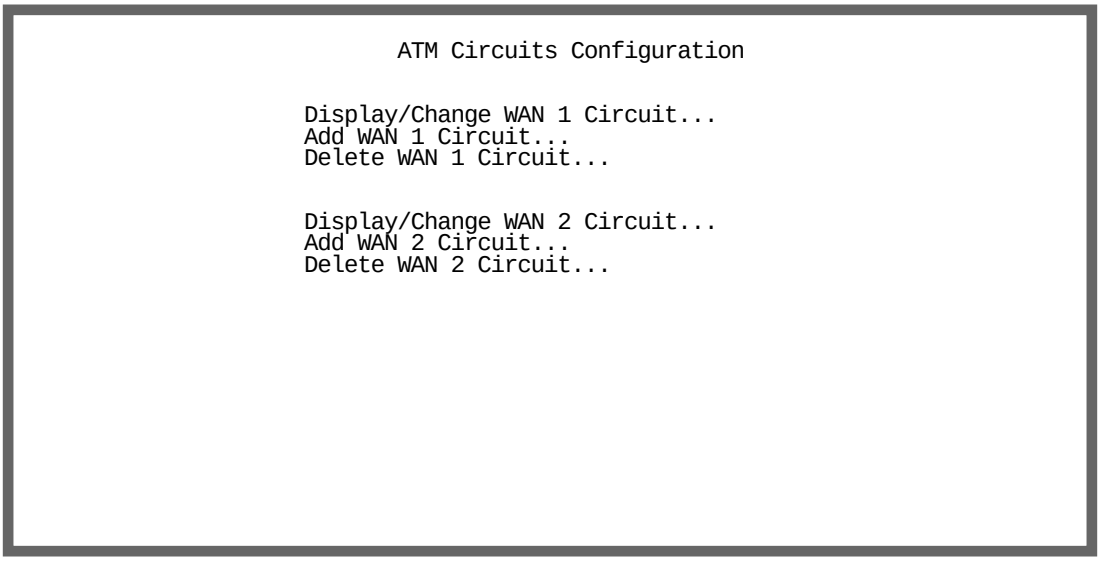
Note: Console Configuration is always visible.

ATM Circuits Configuration menu

You select **ATM Circuits Configuration** from the WAN Configuration menu.



The ATM Circuits Configuration menu screen appears as follows:



Note: Multiple ATM circuit configuration is supported on multiple ATM-capable routers. Although some of the parameters of the Circuit Configuration screens pertain to Voice and Connection Profiles, it is assumed that if the user has been granted PVC configuration access, they are permitted configuration access to all PVC parameters.

Call Filtering

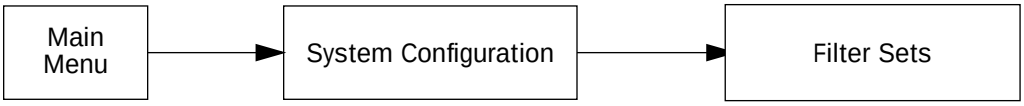
Firmware Version 4.11 introduces a call filtering mechanism that lets you control which packets cause connections to be established and which packets cause connections to be maintained (that is, to not time out due to inactivity). This feature is part of the Filter Set management component of the firmware. Call filtering makes use of the existing sets of filter rules that can be associated with a connection.

The term *connection* includes both non-VPN connection profiles for which the remote network is reached through a switched WAN interface, such as Analog or ISDN, and all VPN connection profiles, such as ATMP, PPTP, and IPsec.

Be sure to read the *User's Reference Guide* for information about setting up "Filters and Filter Sets."

The call filtering mechanism is useful if you have a time-limited type of connection. Such a connection may time out during a period of inactivity and may you want it to be re-established or maintained automatically for certain types of traffic.

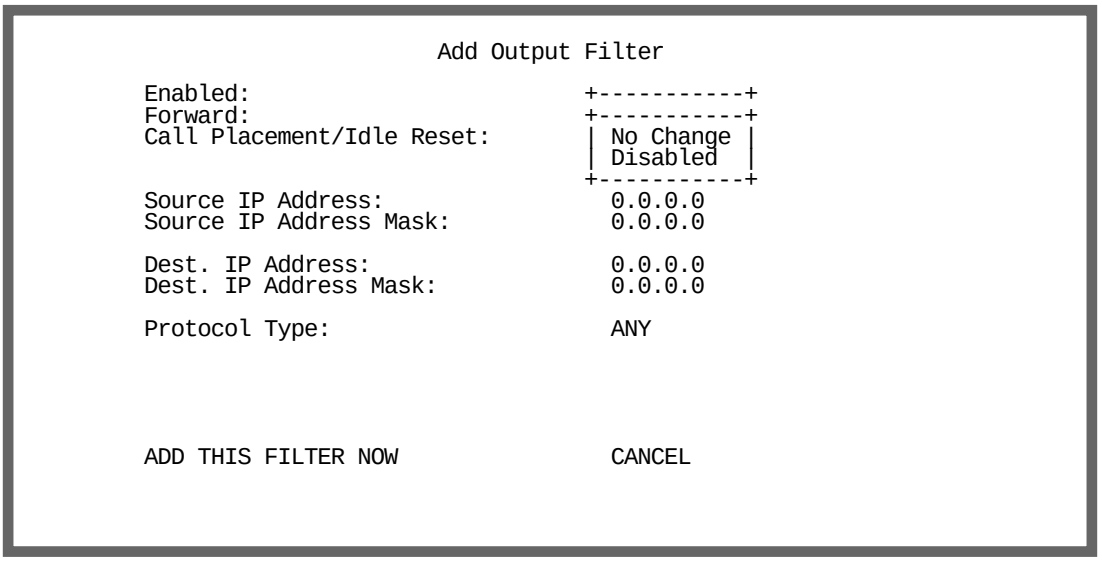
You manage Filters and Filter Sets in the Filter Sets management screen under the System Configuration menus.



The Add Output Filter menu appears as follows:

```
                          Add Output Filter

        Enabled:                          Yes
        Forward:                          Yes


        Source IP Address:                0.0.0.0
        Source IP Address Mask:           0.0.0.0

        Dest. IP Address:                 0.0.0.0
        Dest. IP Address Mask:            0.0.0.0

        Protocol Type:                    ANY




        ADD THIS FILTER NOW               CANCEL

Return/Enter accepts * Tab toggles * ESC cancels.
Enter the packet specific information for this filter.
```

When you add (or change) an output filter, and toggle **Forward** to **Yes**, a new **Call Placement / Idle Reset** pop-up menu becomes visible.



This pop-up menu allows you to configure what action will be taken for packets that the filter rule specifies should be forwarded.

- If you set **Call Placement / Idle Reset** to **No Change** (the default), no change will be made to the call filtering attribute associated with the packet. If no other filter rule with its Call Placement / Idle Reset pop-up set to Disabled previously has been or subsequently will be applied to the packet, the packet will be forwarded as usual. No special action will be taken.

  If the connection is up, the connection's idle timer will be refreshed and the packet forwarded as usual. If the connection is down, the packet is queued until a connection is established.

- If you set the **Call Placement / Idle Reset** to **Disabled**, the call filtering attribute associated with the packet will be set such that the packet will be dropped if the connection is down, and forwarded without resetting the idle timer if the connection is up.

D3100 Enhanced Interoperability

Firmware Version 4.11 adds enhanced central office equipment compatibility. D3100 leased ISDN CSU/DSU models will now interoperate with Nokia DSLAMs. No additional configuration is required.

RIPv2 Packets Sourced From Numbered WAN

Firmware Version 4.11 refines the behavior of RIPv2-advertised WAN IP addresses.

In previous firmware versions, if a numbered interface broadcast RIPv2, IP packets appeared to be sourced from the LAN interface instead of the WAN interface. For example, if your WAN IP address was 172.16.0.1 /24 and your LAN IP address was 192.168.1.1 /24, packets advertising the WAN interface would appear to be from 192.168.1.1/24. This meant that the network on the WAN interface of the Netopia router would not be advertised via RIP. This can be a problem for anyone more than one hop away on either interface.

Firmware Version 4.11 advertises the correct WAN IP address.

IPsec Dead Peer Detection Refinements for VPNs

Firmware Version 4.11 adds a refinement to the dead peer detection mechanism in IKE/IPsec.

When Dead Peer Detection is enabled, a counter begins in the router when any traffic is sent through the tunnel. When the router receives a reply to a transmitted packet the counter is reset to zero (0); if not, counting continues.

In previous firmware versions it was not possible to detect if a remote peer had dropped (died) in the event that an IPsec/IKE tunnel would lose its connection to the remote partner. The Netopia router could not detect that the remote peer had disappeared until the next re-key. The Netopia router would continue to send data on SAs that no longer existed on the remote router.

Firmware Version 4.11 refines the detection mechanism such that eight unanswered packets will trigger the Phase2 re-key. If the attempt is unsuccessful for two minutes, a "Dead Peer" message is logged, followed by continuous attempts to re-key Phase1 until successful.

For more information about IKE and IPsec VPN tunnels, see the *Firmware Addendum*.

Netopia SNMP MIB Enhancements

Firmware Version 4.11 includes a Simple Network Management Protocol (SNMP) agent, allowing monitoring and configuration by a standard SNMP manager.

The Netopia management information base document (Netopia MIB) has been updated to include the following support:

- SNMP support to set or show WAN parameters
- SNMP trap for changed PPPoE IP address
- SNMP support to create connection profiles
- SNMP support for setting DLE protocol
- SNMP support to set or display DHCP parameters
- SNMP support to set NAT mappings
- SNMP support to set or display T1 parameters

This MIB is available by anonymous ftp from the Netopia ftp server.

FTP to: ***ftp.netopia.com/pub/router/snmpinfo***.

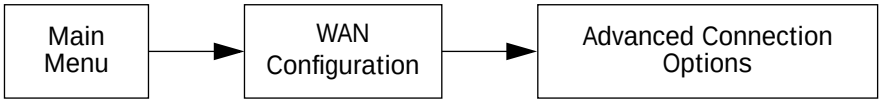
MIBs are available in a variety of formats. Load this MIB into your SNMP management software. Follow the instructions included with your SNMP manager on how to load MIBs.

Priority Queuing (TOS bit) for R-Series WAN Interfaces

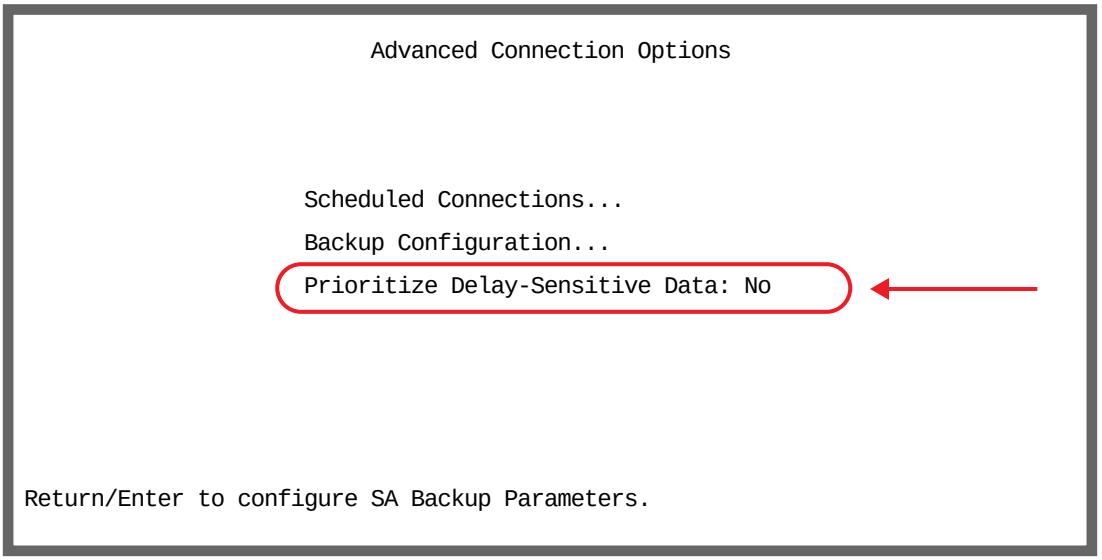
Firmware Version 4.11 offers the ability to prioritize delay-sensitive data over the WAN link for most R-Series models.

Certain types of IP packets, such as voice or multimedia packets, are sensitive to latency introduced by the network. This means that if such packets are not received rapidly, the quality of service degrades. If you expect to route significant amounts of such traffic you can configure your router to prioritize this type of traffic using the priority queuing feature.

To configure your router to prioritize delay-sensitive data, navigate to the Advanced Connection Options screen in the console menu.



The Advanced Connection Options screen appears.



The Router will recognize a delay-sensitive packet as having the low-latency bit set in the TOS field of the IP header.

If you toggle **Prioritize Delay-Sensitive Data** to **Yes** the router will place these packets at the front of the transmission queue to the WAN link, overtaking non-delay-sensitive traffic. Accepting the default **No** will allow the normal sequential queue of data packets.

Command Line Interface Additions

New CLI commands have been added to set or show the layer 2 backup failure delay timer; to display Ethernet MAC address; to display the entire current configuration of the router; to configure the SNMP System Name, Contact, and Location, and more. See the *Command Line Interface Commands Reference V 4.11 - 5.3.1* for details.

AppleTalk and IPX Support Removed

Beginning with firmware version 4.11, routing via the AppleTalk and IPX protocols is no longer supported. Users who require routing via these protocols should not apply firmware version 4.11. The latest firmware version that supports Appletalk and IPX protocols is version 4.8.4.

Embedded Web Server Removed

Firmware version 4.10.1 removed the embedded Web server used to monitor router functions through a Web browser. This is done in order to minimize Nimbda worm attack vulnerability. All of the same monitoring functions are still available in the console menu interface via Telnet or serial connection.

Note: Users who rely on the Web browser-based monitoring features, and are at minimal risk of Nimbda worm attack, should **not** install this update.