Table of Contents

1. SUMMARY 1

2. EUROPEAN ISDN SWITCH SUPPORT 2

3. NOVELL IPX ROUTING 2

3.1 CONFIGURING IPX ROUTING ON THE AUTOBAHN 2
3.1.1 LAN-Based IPX Routing 2
3.1.1.1 Enable IPX Routing 3
3.1.1.2 IPX Frame Type 3
3.1.1.3 IPX Network Number 3
3.1.1.4 IPX RIP 4
3.1.1.5 IPX SAP 4
3.1.1.6 Forward IPX Packet Type 20 5
3.1.2 WAN-Based IPX Routing 5
3.1.2.1 Configuring IPX in a Connection Profile 6
3.1.2.1.1 Routing Protocol 6
3.1.2.1.2 IPX Options 6
3.1.2.1.2.1 IPX Peer Type 6
3.1.2.1.2.2 Remote IPX Network Number 6
3.1.2.1.2.3 Dial On Filer Server Query 7
3.1.2.1.2.4 IPX RIP 8
3.1.2.1.2.5 IPX SAP 8
3.1.2.1.2.6 Forward IPX Packet Type 20 8
3.1.2.2 Matching Connection Profiles on Incoming IPX Calls 9
3.1.2.3 Configuring IPX in the Default Answer Profile 9
3.1.2.3.1 Routing Protocol 9
3.1.2.3.2 IPX RIP 9
3.1.2.3.3 IPX SAP 10
3.1.2.3.4 Forward IPX Packet Type 20 10
3.1.2.4 Routing Table and SAP Table Maintenance 10
3.2 CONFIGURING IPX FILTERS ON THE AUTOBAHN 11
3.2.1 IPX Packet Filters 11
3.2.1.1 Configuring IPX Packet Filters 11
3.2.1.2 Applying IPX Packet Filters to Autobahn Network Interfaces 12
3.2.2 IPX SAP Filters 13
3.2.2.1 Configuring IPX SAP Filters 13
3.2.2.2 Applying IPX SAP Filters to Autobahn Network Interfaces 14
3.3 IPX UTILITIES 15
3.3.1 IPX Routing Table Display 15
3.3.2 IPX SAP Table Display 17
3.4 IPX ROUTING APPLICATIONS 18
3.4.1 NetWare Servers on Both Sides of the Connection 18
3.4.1.1 Connection Establishment 21
3.4.2 NetWare Servers on One Side of the Connection 22
3.4.3 Connecting to a Remote ISDN-Attached Client 23

4. NETWORK ADDRESS TRANSLATION (NAT) 25

4.1 CONFIGURING NAT ON THE AUTOBAHN 25
4.1.1 IP Options 25
4.1.1.1 NAT Enable 25
4.1.1.2 NAT Local WAN IP Address 25
4.1.2 Exported Services 26
4.2 SAMPLE CONFIGURATION 26

5. SUPPORT FOR GRAPHICAL USER INTERFACE UTILITY 29

1. Summary

ALR Autobahn Firmware release 2.0.0 is a ***Major*** release incorporating many feature enhancements and problem resolutions. Major new features in this release include:

- **Support for EuroISDN switches**
- **Novell IPX Routing support**
- **Network Address Translation (NAT) support for IP Routing**
- **Support for Graphical User Interface Utility**

The following minor feature enhancements are also included in this release:

1. The Autobahn configuration information is automatically saved and restored when performing a firmware upgrade. ***Note:*** The Autobahn will be reset to defaults when upgrading to firmware version 2.0.0. This feature applies to future releases.

2. Added support for call bumping for National ISDN switches configured with Additional Call Offering (ACO). This feature allows incoming voice calls to a POTS port to bump a B-Channel from an existing DYNAMIC 2-Channel connection and ring the appropriate POTS port.

3. Added ***ping***, ***traceroute***, ***ldp*** (last dial packet) and ***uptime*** commands to the Autobahn command line interface. The ***ldp*** command displays the last packet that caused the Autobahn to dial out. The display includes the packet type (IP/IPX), source/destination addresses and ports (when applicable). The ***uptime*** command simply displays the current Autobahn up time value.

4. The ISDN/WAN Event Log is now presented in chronological order. Also, new events have been added to log a dynamic IP address assignment when NAT is enabled and when an IP address conflict is detected.

5. IP Packet filters are now configurable for the LAN interface as well as the WAN interface.

6. The default Router IP address has been changed to 192.168.0.1 with a subnet mask of 255.255.255.0.

7. Added ISDN D-Channel and LAN statistics display functions to command line interface.

8. The Autobahn will do a fast (2 second) restart when either the router IP address or netmask is changed.

The following problem resolutions are also included in this release:

1. An incoming call that matches a connection profile *with authentication* (i.e., PAP, CHAP, or CLID) will use the Link Header and Link Data Compression settings from the matching profile as opposed to those from the Answer Profile. This allows different settings to be used on simultaneous connections to different remote peers. ***Note***: if authentication is *not* used, the Autobahn still uses the Link Header and Link Data Compression settings from the default Answer Profile.

2. Several problems were fixed within DNS. Problems mainly manifested as time-outs when host names were used with TFTP or PING.

3. Data over voice calls now use a 3.1KHz AUDIO bearer capability rather than SPEECH bearer capability. The change was made because calls using SPEECH bearer capability are subject to signal processing by the public telephone network which can alter or corrupt WAN data.

4. An outgoing POTS call would steal a B-Channel when the channel was allocated to a 2-Channel incoming call matching a 2 B-Channel connection profile if the Answer Profile indicated DYNAMIC for ISDN B-Channel Usage. This has been resolved, so that the channel cannot be stolen when the incoming call matches a connection profile with ISDN B-Channel Usage = 2 B-Channels, regardless of the setting in the Answer Profile.

5. When the Autobahn connects to a Livingston PortMaster with two B-Channels it may occasionally stop routing or become very sluggish. The problem usually occurred under heavy traffic conditions and could be corrected by manually terminating and re-establishing the call.

The sections that follow provide detailed descriptions and illustrations for the ***Major*** feature enhancements (see bullet items above) that have been added in this release of the Autobahn firmware.

2. European ISDN Switch Support

The ALR Autobahn now supports EuroISDN switches that meet European Telecommunications Standards Institute (ETSI) specifications. The EuroISDN switch type can be selected via the ***Basic Setup => Switch Type*** or ***Advanced Setup => WAN Configuration => ISDN Configuration => Switch Type*** menus. The EuroISDN switch should be provisioned for VOICE and DATA on both B-Channels, two subscriber numbers and in-band call progress tones.

Note: When the EuroISDN switch type is selected, the D Channel Light Emitting Diode (LED) on the front/top of the Autobahn will only illuminate when the ISDN line is activated and many EuroISDN switches only activate the ISDN line when a call is in progress.

3. Novell IPX Routing

Heretofore, the ALR Autobahn was a single-protocol router with support for IP only. With this release of firmware, the ALR Autobahn now supports IPX routing as well. The addition of IPX routing support has resulted in fairly extensive updates to the user interface and configuration mechanisms on the Autobahn. These updates are documented in detail in these release notes. All new configuration parameters and utilities that have been added for IPX are presented with detailed explanations of their purpose and use. Finally, a section on IPX routing applications is included, with associated discussions on relevant configuration and setup requirements for the ALR Autobahn.

3.1 Configuring IPX Routing on the Autobahn

With the addition of IPX, the ALR Autobahn is now a full-fledged multi-protocol router. Flexible management has been incorporated to allow IP-only, IPX-only, or both IP and IPX to be routed on a *per-interface* basis. The following sections provide discussions on the configuration parameters that have either been modified or newly added to support IPX routing on the Autobahn:

3.1.1 LAN-Based IPX Routing

IP is *always enabled* on the Autobahn's LAN interface, as long as a valid IP address and network mask have been configured via the ***Basic Setup*** or ***Advanced Setup => LAN Configuration => IP Configuration*** menus. This allows LAN-based network management and other IP-based applications (e.g., TELNET, PING, TFTP) to be used with the Autobahn at all times. However, in order to route IPX traffic to/from the Autobahn's LAN interface, the following parameters must be correctly configured:

3.1.1.1 Enable IPX Routing

IPX Routing is enabled/disabled for the LAN interface by making the following menu selections:

Advanced Setup => LAN Configuration => IPX Configuration => Enable IPX Routing

Select **YES** to enable IPX routing for the Autobahn's LAN interface and select **NO** to disable IPX routing for the Autobahn's LAN interface.

3.1.1.2 IPX Frame Type

In order to successfully route IPX traffic to/from its LAN interface, the Autobahn must be configured to use the same IPX frame encapsulation method as other IPX nodes (i.e., routers, servers, clients) that are attached to its LAN segment. The IPX frame encapsulation method for the LAN is configured by making the following menu selections:

Advanced Setup => LAN Configuration => IPX Configuration => IPX Frame Type

or

Basic Setup => IPX Frame Type

The frame type selected here must match the frame type being used for IPX encapsulation on the LAN segment to which the Autobahn is attached. This information should be obtained from local MIS staff.

3.1.1.3 IPX Network Number

In order to communicate with other IPX nodes attached to its LAN segment, the Autobahn must be configured to use the same IPX network number as those other nodes. This value is used as the source network number in all IPX packets that the Autobahn *originates* (e.g., for RIP / SAP processing), and as the destination network number in all *non-broadcast* IPX packets that the Autobahn originates. In the absence of other routers or servers on the local LAN, IPX client workstations will *learn* the local network address from the Autobahn when it transmits packets (e.g., RIP / SAP information) containing the configured network number for the source / destination address fields.

The Autobahn automatically broadcasts a route to this network on any active WAN interface, unless filter or RIP settings prevent such broadcasts. A value of zero is illegal for this parameter.

The IPX network number for the LAN interface is configured by making the following menu selections:

Advanced Setup => LAN Configuration => IPX Configuration => IPX Network Number

or

Basic Setup => IPX Network Number

The network number is an 8 hex digit value that should be obtained from local MIS staff.

3.1.1.4 IPX RIP

Like IP, IPX routers exchange routing information via RIP. Although the information exchange format of IPX RIP differs slightly from that of IP RIP, the information that is exchanged between routers is essentially the same. The Autobahn uses information that it receives from other routers on the LAN (in the form of RIP responses) to maintain its internal IPX routing table. Additionally, the Autobahn generates RIP responses onto the LAN, both in response to RIP requests and at regular intervals, to keep other routers appraised of which remote networks are reachable via its LAN interface.

IPX RIP is configured on the Autobahn's LAN interface by making the following menu selections:

Advanced Setup => LAN Configuration => IPX Configuration => IPX RIP

The available choices for IPX RIP configuration are:

Transmit and Receive: The Autobahn will generate RIP requests on the LAN to obtain information from other routers about networks that are reachable via the LAN. The Autobahn will update its internal IPX routing table with RIP information received from other routers on the LAN. The Autobahn will generate RIP responses onto the LAN, both in response to RIP requests and at regular intervals, to keep other routers appraised of which remote networks are reachable via its LAN interface.

Transmit: The Autobahn will generate RIP responses onto the LAN, both in response to RIP requests and at regular intervals, to keep other routers appraised of which remote networks are reachable via its LAN interface.

Receive: The Autobahn will generate RIP requests on the LAN to obtain information from other routers about networks that are reachable via the LAN. The Autobahn will update its internal IPX routing table with RIP information received from other routers on the LAN.

Off: The Autobahn will neither generate nor process received IPX RIP traffic on the LAN interface.

Note: The safest setting for this parameter is **Transmit and Receive**. This ensures that routing information is correctly disseminated among all routers on the attached LAN.

3.1.1.5 IPX SAP

In addition to advertising routing information, IPX routers are responsible for advertising and maintaining Novell server information for their network interfaces. IPX routers exchange server routing information among themselves and with Novell client workstations using the Service Advertising Protocol, or SAP. This information is used by routers to maintain a coherent, up-to-date view of available network services, and by client workstations to locate file servers, print servers, etc. on the network.

In addition to an internal routing table, the Autobahn maintains an internal SAP table which contains routes to all services (or servers) that are reachable via any of its network interfaces. The Autobahn uses information that it receives from other routers on the LAN (in the form of SAP responses) to maintain its internal IPX SAP table. Additionally, the Autobahn generates SAP responses onto the LAN, both in response to SAP requests and at regular intervals, to keep other routers appraised of which servers are reachable via its LAN interface.

IPX SAP is configured on the Autobahn's LAN interface by making the following menu selections:

Advanced Setup => LAN Configuration => IPX Configuration => IPX SAP

The available choices for IPX SAP configuration are:

Transmit and Receive: The Autobahn will generate SAP requests on the LAN to obtain information from other routers about servers that are reachable via the LAN. The Autobahn will update its internal IPX SAP table with SAP information received from other routers on the LAN. The Autobahn will generate SAP responses onto the LAN, both in response to SAP requests and at regular intervals, to keep other routers appraised of which servers are reachable via its LAN interface.

Transmit: The Autobahn will generate SAP responses onto the LAN, both in response to SAP requests and at regular intervals, to keep other routers appraised of which servers are reachable via its LAN interface.

Receive: The Autobahn will generate SAP requests on the LAN to obtain information from other routers about servers that are reachable via the LAN. The Autobahn will update its internal IPX SAP table with SAP information received from other routers on the LAN.

Off: The Autobahn will neither generate nor process received IPX SAP traffic on the LAN interface.

Note: The safest setting for this parameter is **Transmit and Receive**. This ensures that SAP information is correctly disseminated among all routers on the attached LAN.

3.1.1.6 Forward IPX Packet Type 20

In order for certain protocol implementations, like NetBIOS, to function in the NetWare environment, IPX routers must allow a broadcast packet to be propagated throughout an internet. The IPX packet type 20 is used specifically for this purpose. Enabling this option for the LAN interface will cause the Autobahn to forward type 20-encapsulated packets that are received from the LAN port on all active WAN ports, updating the associated connection idle timers as required. However, the Autobahn will NOT dial inactive connections to forward type 20-encapsulated IPX frames received from the LAN.

IPX packet type 20 forwarding is configured for the LAN by making the following menu selections:

Advanced Setup => LAN Configuration => IPX Configuration => Forward IPX Packet Type 20

IPX packet type 20 forwarding for the LAN is enabled by selecting YES for this option, and disabled by selecting NO for this option.

3.1.2 WAN-Based IPX Routing

Autobahn WAN interface attributes are defined within *connection profiles*. Additionally, for incoming calls that fail to negotiate link attributes matching any of the eight pre-defined connection profiles, a default *answer profile* is used to supply link attributes. A considerable number of changes have been made to the Autobahn's profile configuration menus to support IPX routing for the WAN interface. The following sections discuss the modifications and additions that have been made to these menus in detail:

3.1.2.1 Configuring IPX in a Connection Profile

In order for the Autobahn to negotiate and route IPX over a WAN link, the proper parameters must be configured within an associated connection profile. The following sections describe each required parameter and its use in detail:

3.1.2.1.1 Routing Protocol

Autobahn connection profiles can now be configured to route only IP, only IPX, or both IP and IPX. This parameter can be configured on a per-connection profile basis by making the following menu selections:

Advanced Setup => WAN Configuration => Connection Profiles => <Select Desired Profile> =>
Routing Protocol

This parameter can also be configured for the *FIRST* connection profile by making the following menu selections:

Basic Setup => Routing Protocol

Select **IP** for IP-only routing, **IPX** for IPX-only routing, and **IP+IPX** for both IP and IPX routing.

3.1.2.1.2 IPX Options

The IPX Options submenu within each individual connection profile allows for the configuration of IPX routing protocol parameters for WAN links that are established using that profile. The following sections describe these parameters and their use in detail:

3.1.2.1.2.1 IPX Peer Type

From an IPX standpoint, there are two different types of remote peer to which a connection can be established: 1.) another *router* or 2.) a remote *client*. This parameter can be configured on a per-connection profile basis by making the following menu selections:

Advanced Setup => WAN Configuration => Connection Profiles => <Select Desired Profile> =>
IPX Options => IPX Peer Type

Select **Router** for this parameter if the remote peer is another router (e.g., another Autobahn, an Ascend Pipeline or Ascend MAX, etc.). Select **Client** for this parameter if the profile will be used to accept and negotiate an *incoming* connection from an ISDN-attached client workstation (i.e., an IPX client running on top of an ISDN terminal adapter or ISDN modem).

3.1.2.1.2.2 Remote IPX Network Number

This parameter is only necessary if the route to a remote network is required before a connection can be established, or if the IPX Peer Type is **Client** and the Autobahn is expected to supply the IPX network number for the WAN link (which is usually the case for dial-in clients). This parameter is almost never needed if the remote peer is another router. This parameter can be configured on a per-connection profile basis by making the following menu selections:

Advanced Setup => WAN Configuration => Connection Profiles => <Select Desired Profile> =>
IPX Options => Remote IPX Network Number

The Remote IPX Network Number is an 8 hex digit value that should be obtained from local MIS staff.

3.1.2.1.2.3 Dial On Filer Server Query

When the Autobahn is first powered up and integrated into the local IPX environment, its IPX routing and IPX SAP tables are both empty. Therefore, initial file server queries that are generated by locally attached client workstations (i.e., IPX workstations attached to the Autobahn's LAN segment) will go unanswered and the clients will be inoperable. In order to allow locally attached client workstations to transparently connect to and communicate with remote Novell file servers, the Dial On File Server Query option should be set to YES in at least one IPX-enabled connection profile. In the event that the Autobahn's SAP table contains no routing information for Novell file servers on receipt of a file server query packet, the Autobahn will automatically bring up all (up to 2) IPX-enabled connections with Dial On File Server Query set to YES. This will result in an immediate exchange of RIP and SAP information between the Autobahn and its remote peer, causing the Autobahn to populate its internal RIP and SAP tables, and enabling it to reply to further file server queries generated by locally attached client workstations (i.e., retries). This parameter can be configured on a per-connection profile basis by making the following menu selections:

Advanced Setup => WAN Configuration => Connection Profiles => <Select Desired Profile> =>
IPX Options => Dial On File Server Query

3.1.2.1.2.4 IPX RIP

The IPX RIP parameter setting in a connection profile results in the same protocol exchanges over a WAN link established through that profile as those described in section 3.1.1.4 for the LAN segment. Additionally, the following properties hold:

- IPX RIP exchanges over a WAN link do *not* cause connection idle timers to be reset.
- IPX RIP packets will *not* cause a connection to be established via dial-on-demand.

This parameter can be configured on a per-connection profile basis by making the following menu selections:

Advanced Setup => WAN Configuration => Connection Profiles => <Select Desired Profile> =>
IPX Options => IPX RIP

3.1.2.1.2.5 IPX SAP

The IPX SAP parameter setting in a connection profile results in the same protocol exchanges over a WAN link established through that profile as those described in section 3.1.1.5 for the LAN segment. Additionally, the following properties hold:

- IPX SAP exchanges over a WAN link do *not* cause connection idle timers to be reset.
- IPX SAP packets will *not* cause a connection to be established via dial-on-demand.

This parameter can be configured on a per-connection profile basis by making the following menu selections:

Advanced Setup => WAN Configuration => Connection Profiles => <Select Desired Profile> =>
IPX Options => IPX SAP

3.1.2.1.2.6 Forward IPX Packet Type 20

This parameter enables/disables packet type 20 forwarding on a WAN port in the same fashion that the analogous parameter described in section 3.1.1.6 does for the LAN port. Enabling this option in a connection profile will cause the Autobahn to forward type 20-encapsulated packets that are received from a WAN link that is established via that profile, updating the associated connection idle timers as required. However, the Autobahn will NOT dial inactive connections to forward type 20-encapsulated IPX frames received from a WAN port.

IPX packet type 20 forwarding is configured in a connection profile by making the following menu selections:

Advanced Setup => WAN Configuration => Connection Profiles => <Select Desired Profile> =>
IPX Options => Forward IPX Packet Type 20

IPX packet type 20 forwarding for the connection is enabled by selecting YES for this option, and disabled by selecting NO for this option.

3.1.2.2 Matching Connection Profiles on Incoming IPX Calls

Unlike an Autobahn IP connection, which is defined by the IP address that is configured in the corresponding connection profile, an Autobahn IPX connection has no defining *network layer* parameter(s) by which it may be identified. Therefore, in order to match a connection profile on an incoming *IPX-Only* connection, the profile must be matched with a lower layer authentication protocol (i.e., CLID or PAP / CHAP authentication).

If no form of authentication is performed for an incoming call, the routing protocols that are negotiated for the call are taken from the ***Routing Protocol*** parameter setting in the default answer profile. If this parameter is configured for IPX only, the only possible profile match for the call is the default answer profile. In this case, the IPX control settings for the call are taken from the default answer profile. If this parameter is configured to include the IP protocol, there is still a possibility that a connection profile will be matched once the remote IP address is negotiated. If a profile is matched on the remote peer's negotiated IP address and if IPX is also negotiated (i.e., the ***Routing Protocol*** setting in the answer profile = IP+IPX), the IPX control settings for the call are taken from the matched profile[1].

If a lower layer authentication protocol (i.e., CLID or PAP / CHAP) is used by the remote calling party and authentication succeeds, the routing protocols that are negotiated for the call are taken from the ***Routing Protocol*** parameter setting in the matched connection profile. If IPX is specified and successfully negotiated with the calling peer, the IPX control settings for the call are taken from the matched connection profile.

Note: In order to successfully connect to a remote ISDN-attached Novell client (i.e., **IPX Peer Type** = *Client* in the matching connection profile), the remote peer (calling party) MUST be successfully authenticated by the Autobahn using either CLID or PAP / CHAP. Otherwise, the Autobahn does not know how to negotiate IPX with the remote peer, and it will default to the negotiation method for a remote router.

3.1.2.3 Configuring IPX in the Default Answer Profile

As stated in section 3.1.2.2, when an incoming call does not match a connection profile, the IPX control settings for the connection are taken from the Autobahn's default answer profile. The following sections briefly describe the IPX-specific parameter settings in the Autobahn's default answer profile:

3.1.2.3.1 Routing Protocol

If neither CLID nor PPP receive authentication is required for incoming connections, the Autobahn will use the Routing Protocol setting from the default answer profile to determine which network protocol(s) to negotiate for the link. If the routing protocol selected in the default answer profile is IPX or IP+IPX, the Autobahn will attempt to establish the IPX network layer with the remote (calling) peer. This parameter can be configured in the answer profile by making the following menu selections:

Advanced Setup => WAN Configuration => Answer Profile => Routing Protocol

3.1.2.3.2 IPX RIP

[1] The **IPX Peer Type** setting from the matched profile cannot be used in this case; the remote peer is assumed to be of type *Router*.

For connections that match the default answer profile, the IPX RIP setting in the default answer profile functions identically to the IPX RIP setting specified in section 3.1.1.4 for connections that match a connection profile. This parameter is configured in the answer profile by making the following menu selections:

Advanced Setup => WAN Configuration => Answer Profile => IPX RIP

3.1.2.3.3 IPX SAP

For connections that match the default answer profile, the IPX SAP setting in the default answer profile functions identically to the IPX SAP setting specified in section 3.1.1.5 for connections that match a connection profile. This parameter is configured in the answer profile by making the following menu selections:

Advanced Setup => WAN Configuration => Answer Profile => IPX SAP

3.1.2.3.4 Forward IPX Packet Type 20

For connections that match the default answer profile, the Forward IPX Packet Type 20 setting in the default answer profile functions identically to the Forward IPX Packet Type 20 setting specified in section 3.1.1.6 for connections that match a connection profile. This parameter is configured in the answer profile by making the following menu selections:

Advanced Setup => WAN Configuration => Answer Profile => Forward IPX Packet Type 20

3.1.2.4 Routing Table and SAP Table Maintenance

When the Autobahn is first powered up, its IPX routing and SAP tables are both empty. If and when IPX is enabled on an *active* interface (i.e., on the LAN interface or on a newly established WAN interface with Routing Protocol = IPX or IP+IPX), the Autobahn will initiate the exchange of RIP and SAP information between itself and other network agents (i.e., routers and servers). As a result, the Autobahn's IPX Routing and IPX SAP tables are dynamically constructed from information that is received from these agents.

Like most routing protocols, IPX RIP and SAP maintain aging timers for each entry in their respective tables[2]. Each aging timer is incremented once per second, and whenever the Autobahn receives a RIP or SAP update for a particular entry, the entry's associated aging timer is reset to zero. If an entry's aging timer is allowed to advance for a period of 180 seconds (i.e., an update for the entry is not received within that timeframe), the entry is "aged out" of the associated table. In this case, adjacent RIP/SAP agents are informed through a mechanism known as "poisoning" that the associated network entity (server or network) is no longer accessible through the Autobahn.

Because the Autobahn's WAN interface is a switched interface, the link is typically in a DOWN state during periods of network inactivity. Because RIP/SAP updates are not received from remote peers when the WAN link is DOWN, the Autobahn suspends aging of RIP/SAP table entries associated with a particular connection when that connection is brought down. This mechanism prevents RIP and SAP

[2] The IPX routing table is also referred to as the IPX RIP table.

information from being prematurely aged when the associated nodes are still reachable via the Autobahn, and it also enables the Autobahn to maintain an IPX network number-to-connection profile mapping for future dial-on-demand IPX packet routing.

Once a connection is re-established, the aging process begins again for associated RIP/SAP table entries. If a particular entry is not updated before the associated connection goes inactive again, the Autobahn will continue to age the entry while the link is down. Therefore, the Autobahn may age out and poison RIP/SAP table entries that are associated with a connection profile, regardless of whether or not the profile is currently active. Using this mechanism, the Autobahn keeps abreast of changes that occur in the network topology even when WAN links are inactive.

The Autobahn will store a maximum of 300 SAP and 300 RIP entries. If your network contains more than this number, use SAP filters and packet filters respectively to isolate the information that is required for dial-up connectivity. This also has the added advantage of improved security.

3.2 Configuring IPX Filters on the Autobahn

There are two types of filters associated with IPX routing on the ALR Autobahn: *packet filters* and *SAP filters*. The Autobahn's packet filter configuration interface has been modified to allow specification of a *filter type* (i.e., IP or IPX) for each input and/or output filter in a filter set. Therefore, a packet filter set can now contain a mixture of both IP and IPX packet filters for use on Autobahn network interfaces which are routing both protocols. Additionally, the capability to construct IPX SAP filter sets has been added to the filter set configuration interface. The following sections describe the new IPX packet and IPX SAP filter set configuration interfaces in detail.

3.2.1 IPX Packet Filters

IPX packet filters can be configured to allow for the filtering of IPX traffic received from and/or transmitted onto any Autobahn network interface. There are still four configurable packet filter *sets* on the Autobahn, with each set containing up to twelve *input* packet filters and twelve *output* packet filters. Input packet filters are applied to traffic that is received from a network interface, and output packet filters are applied to traffic that is to be transmitted onto a network interface. An input or output IPX packet filter may be defined within any Autobahn packet filter set by making the following menu selections:

Advanced Setup => Filter Set => Packet Filter Set Config => <Select Filter Set #> =>
<Select Input Filter or Output Filter> => <Select Filter #>

3.2.1.1 Configuring IPX Packet Filters

Once a filter has been selected for configuration using the menu selections listed in 3.2.1, the filter *Type* must be configured as **IPX Filter**. The interface will then provide configuration fields for the following packet filter elements:

Status: Select *Enable* or *Disable* to activate or deactivate the specific filter for application during packet routing.

Forward: Specifies whether packets that match this filter are to be forwarded or discarded.

Source Network #: 8 hex digit IPX network number that is compared to the source network number in all IPX packets to which the filter is applied. A value of zero will match any network.

Source Node #: 12 hex digit IPX node number that is compared to the source node number in all IPX packets to which the filter is applied. A value of zero will match any node.

Source Socket #: 4 hex digit IPX socket number that is compared to the source socket number in all IPX packets to which the filter is applied. A value of zero will match any socket.

Destination Network #: 8 hex digit IPX network number that is compared to the destination network number in all IPX packets to which the filter is applied. A value of zero will match any network.

Destination Node #: 12 hex digit IPX node number that is compared to the destination node number in all IPX packets to which the filter is applied. A value of zero will match any node.

Destination Socket #: 4 hex digit IPX socket number that is compared to the destination socket number in all IPX packets to which the filter is applied. A value of zero will match any socket.

3.2.1.2 Applying IPX Packet Filters to Autobahn Network Interfaces

A packet filter set for the Autobahn's LAN interface may be configured by making the following menu selections:

Advanced Setup => LAN Configuration => Packet Filter Set # => <Select Filter Set #>

Selecting a filter set # other than *None* (i.e., 1 - 4) will cause the IP and IPX packet filters defined in that set to be applied to traffic that is routed to/from the Autobahn's LAN port.

A packet filter set for an Autobahn WAN link which is established via a connection profile may be configured by making the following menu selections:

Advanced Setup => WAN Configuration => Connection Profiles => <Select Connection Profile> =>
Other Options => Packet Filter Set # => <Select Filter Set #>

A packet filter set for an Autobahn WAN link which is established via the default answer profile may be configured by making the following menu selections:

Advanced Setup => WAN Configuration => Answer Profile => Packet Filter Set # =>
<Select Filter Set #>

Selecting a filter set # other than *None* (i.e., 1 - 4) will cause the IP and IPX packet filters defined in that set to be applied to traffic that is routed to/from the associated WAN port(s).

Filters are applied to packets by looking for a filter specification (one of 12) within the specified filter set (one of 4) which matches the packet. If a match is found, the packet is either accepted (if the filter's Forward parameter = *Yes*) or discarded (if the filter's Forward parameter = *No*). Once a match is found, no other filters are applied to the packet. When looking for a match, the filters in a set are applied in ascending order (filter #1 first, filter #12 last). Only filters which have their *Status* parameters set to *Enable* will be compared to the packet when searching for a match.

If every filter (1-12) in a filter set (Input or Output) fails to match a particular packet, the packet is handled as follows:

1. Discarded if all the filters are configured to pass (all Forward parameters = *Yes*).

2. Passed if all the filters are configured to discard (all Forward parameters = *No*).

3. Discarded if the filter set contains a combination of filters with Forward = *Yes* (pass) and Forward = *No* (discard).

Finally, dial-on-demand is not initiated and WAN port idle timers are not updated for IPX packets that are filtered by input or output filters.

3.2.2 IPX SAP Filters

IPX SAP filters control the flow of information into and out of the Autobahn's IPX SAP table. Through the use of SAP filters, specific SAP information received by the Autobahn can be excluded from the SAP table, and specific SAP table entries can be excluded from SAP updates generated by the Autobahn.

Like IPX packet filters, IPX SAP filters can be configured to allow for the filtering of SAP traffic received from and/or transmitted onto any Autobahn network interface. There are four configurable SAP filter *sets* on the Autobahn, with each set containing up to four *input* SAP filters and four *output* SAP filters. Input SAP filters are applied to SAP traffic that is received from a network interface before the corresponding entries are updated in the SAP table. Output SAP filters are applied to SAP table entries before they are included in SAP updates that are transmitted by the Autobahn onto a network interface. An input or output IPX SAP filter may be defined within any Autobahn SAP filter set by making the following menu selections:

Advanced Setup => Filter Set => IPX SAP Filter Set Config => <Select Filter Set #> =>
<Select Input Filter or Output Filter> => <Select Filter #>

3.2.2.1 Configuring IPX SAP Filters

Once a SAP filter has been selected for configuration using the menu selections listed in 3.2.2, the interface will provide configuration fields for the following SAP filter elements:

Status: Select *Enable* or *Disable* to activate or deactivate the specific filter for filtering SAP traffic that is received / generated by the Autobahn.

Filter Type: Specifies whether or not SAP entries that match this filter are to be included in SAP table updates (input filter) or in SAP responses generated by the Autobahn (output filter).

Server Name: ASCII string (up to 47 characters) that is compared to the server name field in all IPX SAP entries to which this filter is applied. A blank server name will match any server name.

Server Type: 4 hex digit server type (e.g. file server = 0004) that is compared to the server type field in all IPX SAP entries to which this filter is applied. A value of zero will match any server type.

Server Socket: 4 hex digit server socket number that is compared to the server socket portion of the IPX address in all IPX SAP entries to which this filter is applied. A value of zero will match any server socket.

IPX Network Number: 8 hex digit IPX network number that is compared to the IPX network number portion of the IPX address in all IPX SAP entries to which this filter is applied. A value of zero will match any network number.

IPX Node Number: 12 hex digit IPX node number that is compared to the IPX node number portion of the IPX address in all IPX SAP entries to which this filter is applied. A value of zero will match any node number.

3.2.2.2 Applying IPX SAP Filters to Autobahn Network Interfaces

An IPX SAP filter set for the Autobahn's LAN interface may be configured by making the following menu selections:

Advanced Setup => LAN Configuration => IPX Configuration => IPX SA Filter Set # =>
<Select Filter Set #>

Selecting a filter set # other than *None* (i.e., 1 - 4) will cause the IPX SAP filters defined in that set to be applied to all SAP updates that are received or generated by the Autobahn on the LAN interface.

An IPX SAP filter set for an Autobahn WAN link which is established via a connection profile may be configured by making the following menu selections:

Advanced Setup => WAN Configuration => Connection Profiles => <Select Connection Profile> =>
Other Options => IPX SAP Filter Set # => <Select Filter Set #>

An IPX SAP filter set for an Autobahn WAN link which is established via the default answer profile may be configured by making the following menu selections:

Advanced Setup => WAN Configuration => Answer Profile => IPX SAP Filter Set # =>
<Select Filter Set #>

Selecting a filter set # other than *None* (i.e., 1 - 4) will cause the IPX SAP filters defined in that set to be applied to all SAP updates that are received or generated by the Autobahn on the associated WAN port(s).

IPX SAP filters are applied to SAP entries (either in SAP updates received by the Autobahn or in the Autobahn's SAP table) by looking for a filter specification (one of 4) within the specified filter set (one of 4) which matches the SAP entry. If a match is found, the entry is either accepted (if the Filter Type = *Include*) or discarded (if the Filter Type = *Exclude*). Once a match is found, no other SAP filters are applied to the entry. When looking for a match, the filters in a set are applied in ascending order (filter #1 first, filter #4 last). Only filters which have their *Status* parameters set to *Enable* will be compared to the entry when searching for a match.

If every filter (1-4) in a filter set (Input or Output) fails to match a particular SAP entry, the entry is handled as follows:

1. Discarded if all the filters are configured to accept (all Filter Type parameters = *Include*).

2. Accepted if all the filters are configured to discard (all Filter Type parameters = *Exclude*).

3. Discarded if the filter set contains a combination of filters with Filter Type = *Include* (accept) and Filter Type = *Exclude* (discard).

3.3 IPX Utilities

Two new functions have been added to the Autobahn’s utilities menu for IPX routing. They are: ***IPX Routing Table*** display and ***IPX SAP Table*** display. The following sections describe these functions and the meanings of their corresponding display fields:

3.3.1 IPX Routing Table Display

The Autobahn’s internal IPX routing table can be displayed by making the following menu selections:

Utilities => IPX Routing Table

The following is an example of a real-life Autobahn IPX Routing Table display:

```
 Network    Next Hop       Interface           Hops   Ticks   Type    Age

 98765432   ---            Ethernet               0       1   Local     0
 00000101   00c00d092718   Remote Autobahn        1      11   RIP      20
 08675309   00c00d092718   Remote Autobahn        2      12   RIP      20
 00000581   00c00d092718   Remote Autobahn        2      12   RIP      20
 00000808   00c00d092718   Remote Autobahn        2      12   RIP      20
 00008888   00c00d092718   Remote Autobahn        2      12   RIP      20
 00000b0b   00c00d092718   Remote Autobahn        2      12   RIP      20
 0000b0b2   00c00d092718   Remote Autobahn        2      12   RIP      20
 1234abcd   00e76b923908   Ascend MAX             3      18   RIP      11
 00000002   00e76b923908   Ascend MAX             3      18   RIP      11
 00000001   00e76b923908   Ascend MAX             3      18   RIP      10
 00001111   00e76b923908   Ascend MAX             3      18   RIP      12
 00000202   00e76b923908   Ascend MAX             3      18   RIP      10
 0000aaaa   00e76b923908   Ascend MAX             3      18   RIP      10
 00000909   00e76b923908   Ascend MAX             3      18   RIP       9
 00013579   00e76b923908   Ascend MAX             4      28   RIP       9
 00009091   00e76b923908   Ascend MAX             5      32   RIP       8
 00009092   00e76b923908   Ascend MAX             3      18   RIP      10

  [Update]            [Next Page]         [Previous Page]
```

In the preceding display, the IPX routing table columns have the following meanings:

Network: Gives the IPX network number of for the destination network described by the routing entry.

Next Hop: Gives the IPX node number of the next hop gateway en route to the destination network.

Interface: For networks that are reachable via the Autobahn's LAN interface, this field contains the string "Ethernet". For networks that are reachable via an Autobahn WAN interface, this field contains the name of the corresponding connection profile (or simply "Answer Profile" if there is no matching connection profile) that is associated with the link. The above example illustrates the scenario where the Autobahn is connected to two separate remote IPX networks, one through a connection profile called "Remote Autobahn" and the other through a connection profile called "Ascend MAX".

Hops: Gives the number of intervening routers on the path to the destination network.

Ticks: This field indicates how much time that it takes for a packet to reach the specified destination network using this route. A tick is roughly 1/18 of a second.

Type: Type is either "Local" or "RIP". "Local" indicates that the route entry was installed as a result of local configuration (i.e., configuration of the IPX Network Number for the LAN or configuration of the Remote IPX Network Number in a connection profile's IPX Options submenu). "Local" routing information is not aged. "RIP" indicates that the route entry was installed as a result of a RIP update received over the associated WAN interface.

Age: Gives the time in seconds since the last RIP update was received for the route entry.

The control buttons at the bottom of the IPX Routing Table display screen function as follows:

1.) Update: Obtains and displays a fresh image of the internal IPX routing table.

2.) Next Page: Scrolls forward one page in the IPX Routing Table display screen.
3.) Previous Page: Scrolls back one page in the IPX Routing Table display screen.

3.3.2 IPX SAP Table Display

The Autobahn's internal IPX SAP table can be displayed by making the following menu selections:

Utilities => IPX SAP Table

The following is an example of a real-life Autobahn IPX SAP Table display:

```
 IPX Network:Node:Socket     Type  Server Name

 00000101:000092b62702:4010  0355  00202065ROBINDRI
 00000101:0000929b165f:0555  067b  WORKGROUP
 00000101:0800096b74aa:400c  030c  0800096B74AA03CECENTRALGRPH
 00000101:000092b629ba:0555  067b  RECEIVING
 08675309:000000000001:0451  0004  HW_LAB
 08675309:000000000001:8104  0107  HW_LAB
 00000101:0800099a6438:400c  030c  0800099A643803CEPROD-LJ
 00000101:000092906ec8:4098  064e
CCWEB!!!!!!!!!!A5569B20ABE511CE9CA400004C7628
 00000101:00009290bcf9:0555  067b  PRODUCTION
 00000002:000000000001:4068  064e
INTRANET!!!!!!!A5569B20ABE511CE9CA400004C7628
 00000001:000000000001:e885  0640  INTERNETSERVER
 00000808:000092b61823:0555  067b  ADMIN
 00000808:000092b6343d:e885  0640  SMS
 00008888:000000000001:0451  0004  MIS
 00008888:000000000001:4004  0355  0004MIS
 00008888:000000000001:8104  0107  MIS
 00008888:000000000001:907b  023f  MIS
 00000101:0000929b082d:e885  0640  DUAL_6

  [Update]            [Next Page]         [Previous Page]
```

In the preceding display, the IPX SAP table columns have the following meanings:

IPX Network:Node:Socket: IPX address consisting of the **`IPX Network Number:IPX Node Number:IPX Socket Number`** triplet describing the network location of the advertised service.

Type: 4 hex digit IPX server type description (e.g., 0004 = file server).

Server Name: Gives the ASCII name of the server as advertised in received SAP updates (up to 47 characters).

The control buttons at the bottom of the IPX SAP Table display screen function as follows:

1.) Update: Obtains and displays a fresh image of the internal IPX SAP table.
2.) Next Page: Scrolls forward one page in the IPX SAP Table display screen.
3.) Previous Page: Scrolls back one page in the IPX SAP Table display screen.

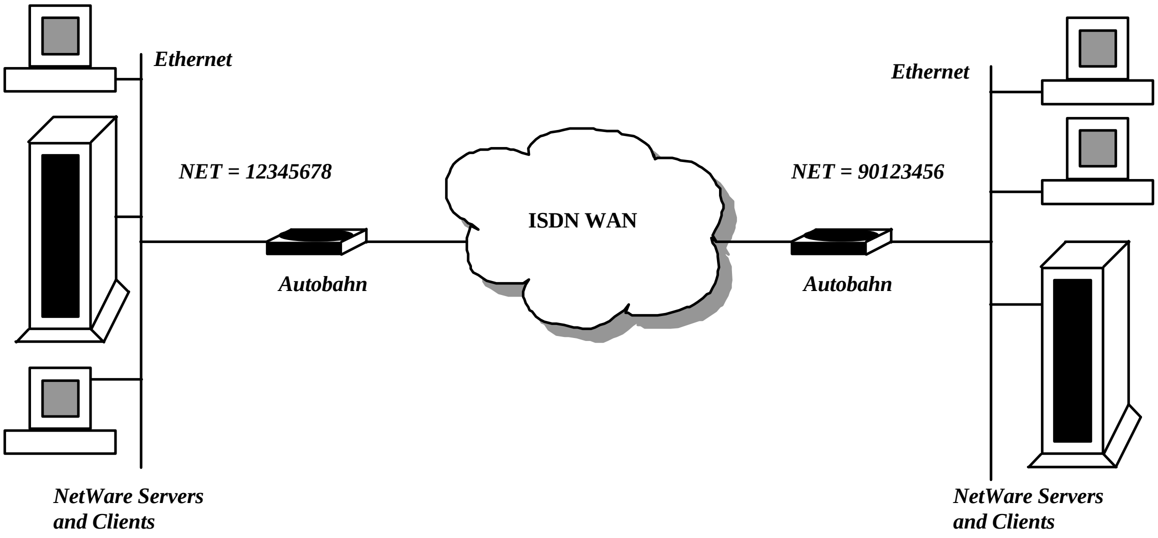
3.4 IPX Routing Applications

In general, there are three basic types of IPX network application into which the Autobahn is likely to be configured. Two of the applications involve router-to-router connectivity, while the third is characterized by remote clients dialing in directly to the Autobahn over the ISDN WAN link(s). The following sections illustrate each of these scenarios, and present the configuration steps required on both local and remote Autobahns to achieve the desired topologies[3].

3.4.1 NetWare Servers on Both Sides of the Connection

In the case where Autobahns are being used to connect geographically remote NetWare LANs, both NetWare servers and NetWare client workstations will typically exist on both LANs. In this scenario, each LAN will likely contain at least one Novell file server. Other Novell services may or may not exist on both sides of the connection. Hence, it is likely that each LAN is autonomous in the sense that attached workstations can communicate among each other, store and print files, etc., without ever needing to access nodes on the respective remote NetWare LANs. Figure 1 illustrates such a scenario.

In the case where a client explicitly requests the services of a remote NetWare node, an IPX routing connection must be established between the two associated routing peers. In order to achieve this interconnection in the most seamless fashion possible, the following parameter settings should be used at the respective Autobahns. Assume that the Autobahn labeled **(a)** is the calling party and the Autobahn labeled **(b)** is the called party.



[3] The router-to-router scenarios present Autobahn-to-Autobahn connection paradigms solely for the purpose of illustrating the configuration requirements on both a *calling* and an *answering* Autobahn. In all cases, an Autobahn may be connecting to a *non-Autobahn* remote peer, on either side of the connection.

(a) **(b)**

Figure 1. NetWare Servers on Both Sides of the Link

Parameter Settings at Autobahn (a):

Advanced Setup => LAN Configuration => IPX Configuration => Enable IPX Routing = YES

Advanced Setup => LAN Configuration => IPX Configuration => IPX Frame Type = Select Accordingly

See local MIS staff to obtain correct setting for this parameter.

Advanced Setup => LAN Configuration => IPX Configuration => IPX Network Number = 12345678

Indicated value adheres to the example in figure 1. See local MIS staff to obtain correct setting for this parameter.

Advanced Setup => LAN Configuration => IPX Configuration => IPX RIP = Transmit and Receive
Advanced Setup => LAN Configuration => IPX Configuration => IPX SAP = Transmit and Receive
Advanced Setup => LAN Configuration => IPX Configuration => Forward IPX packet Type 20 = YES

Advanced Setup => WAN Configuration => Connection Profiles => <Select Connection Profile> => Routing Protocol = IPX or IP+IPX

Advanced Setup => WAN Configuration => Connection Profiles => <Select Connection Profile> => IPX Options => IPX Peer Type = Router

Advanced Setup => WAN Configuration => Connection Profiles => <Select Connection Profile> => IPX Options => IPX RIP = Transmit and Receive

Advanced Setup => WAN Configuration => Connection Profiles => <Select Connection Profile> => IPX Options => IPX SAP = Transmit and Receive

Advanced Setup => WAN Configuration => Connection Profiles => <Select Connection Profile> => IPX Options => Forward IPX Packet Type 20 = YES

Advanced Setup => WAN Configuration => Connection Profiles => <Select Connection Profile> => ML-PPP Options => Send Authentication Method = PAP or CHAP

Advanced Setup => WAN Configuration => Connection Profiles => <Select Connection Profile> => ML-PPP Options => Send User Name = Enter Send User Name string

Advanced Setup => WAN Configuration => Connection Profiles => <Select Connection Profile> => ML-PPP Options => Send Password = Enter Send Password string

Note that PPP send authentication (i.e., PAP / CHAP) is not required if the receiving end (router (b)) is using CLID authentication.

Parameter Settings at Autobahn (b):

Advanced Setup => LAN Configuration => IPX Configuration => Enable IPX Routing = YES

Advanced Setup => LAN Configuration => IPX Configuration => IPX Frame Type = Select Accordingly

See local MIS staff to obtain correct setting for this parameter.

Advanced Setup => LAN Configuration => IPX Configuration => IPX Network Number = 90123456

Indicated value adheres to the example in figure 1. See local MIS staff to obtain correct setting for this parameter.

Advanced Setup => LAN Configuration => IPX Configuration => IPX RIP = Transmit and Receive
Advanced Setup => LAN Configuration => IPX Configuration => IPX SAP = Transmit and Receive
Advanced Setup => LAN Configuration => IPX Configuration => Forward IPX packet Type 20 = YES

***Advanced Setup => WAN Configuration => Answer Profile => Receive Authentication* =** PAP or CHAP

Note that PPP receive authentication (i.e., PAP / CHAP) need not be used if the calling party (i.e., router (a)) is authenticated with CLID (Caller ID Authentication).

***Advanced Setup => WAN Configuration => Connection Profiles => <Select Connection Profile> => Routing Protocol* =** IPX or IP+IPX

***Advanced Setup => WAN Configuration => Connection Profiles => <Select Connection Profile> => IPX Options => IPX Peer Type* =** Router

***Advanced Setup => WAN Configuration => Connection Profiles => <Select Connection Profile> => IPX Options => IPX RIP* =** Transmit and Receive

***Advanced Setup => WAN Configuration => Connection Profiles => <Select Connection Profile> => IPX Options => IPX SAP* =** Transmit and Receive

***Advanced Setup => WAN Configuration => Connection Profiles => <Select Connection Profile> => IPX Options => Forward IPX Packet Type 20* =** YES

***Advanced Setup => WAN Configuration => Connection Profiles => <Select Connection Profile> => ML-PPP Options => Receive User Name* =** Enter match for router (a) Send User Name

***Advanced Setup => WAN Configuration => Connection Profiles => <Select Connection Profile> => ML-PPP Options => Receive Password* =** Enter match for router (a) Send Password

3.4.1.1 Connection Establishment

Again, with servers on both sides of the WAN, it is likely that each remote LAN is autonomous. In such a case, it is likely that NetWare client-generated **"Get Nearest File Server"** requests have already been satisfied by local servers, and are no longer being generated. Therefore, setting the **"Dial On File Server Query"** parameter to YES in the calling party's connection profile (at router (a)) is not likely to cause dynamic connection establishment with the remote peer (router (b)).

In this case, the remote network can either be manually dialed (via the "Establish Connection" utility in the calling party's connection profile), or a route to the remote network can be manually configured by entering the correct remote network number in the calling party's connection profile, as follows:

Advanced Setup => WAN Configuration => Connection Profiles => <Select Connection Profile> => IPX Options => Remote IPX Network Number = 90123456

The first method is the most foolproof, since it is unlikely that any of the nodes on router (a)'s network will generate traffic for network 90123456 (router (b)'s network) before knowing that it exists.

Once a connection is established between the two peers, RIP and SAP information will flow across all links (WAN and LAN), populating the associated RIP and SAP tables on both routers. Once the RIP and SAP tables on both sides of the connection are populated, topology information about the complete routed network can be disseminated and clients and servers from both sides of the connection can communicate with one another.

3.4.2 NetWare Servers on One Side of the Connection

The second type of router-to-router topology involves NetWare servers on one side of the connection, and only NetWare clients on the other side. This topology is typical for small branch office to home office applications, where remote clients share a LAN for peer-to-peer communications, but must communicate over a WAN to access files and data at a central location. This topology is illustrated in figure 2. The configuration requirements for such a topology are virtually identical to those outlined in section 3.4.1, except that the **"Dial On File Server Query"** parameter in the connection profile of the calling party (router (a)) must be set to YES. Doing so will cause the Autobahn to automatically dial the remote peer when it receives a NetWare "Get Nearest File Server" or "Get General File Server Info" query from any of the clients on its local LAN. See section 3.1.2.1.2.3 for details on configuring this parameter.

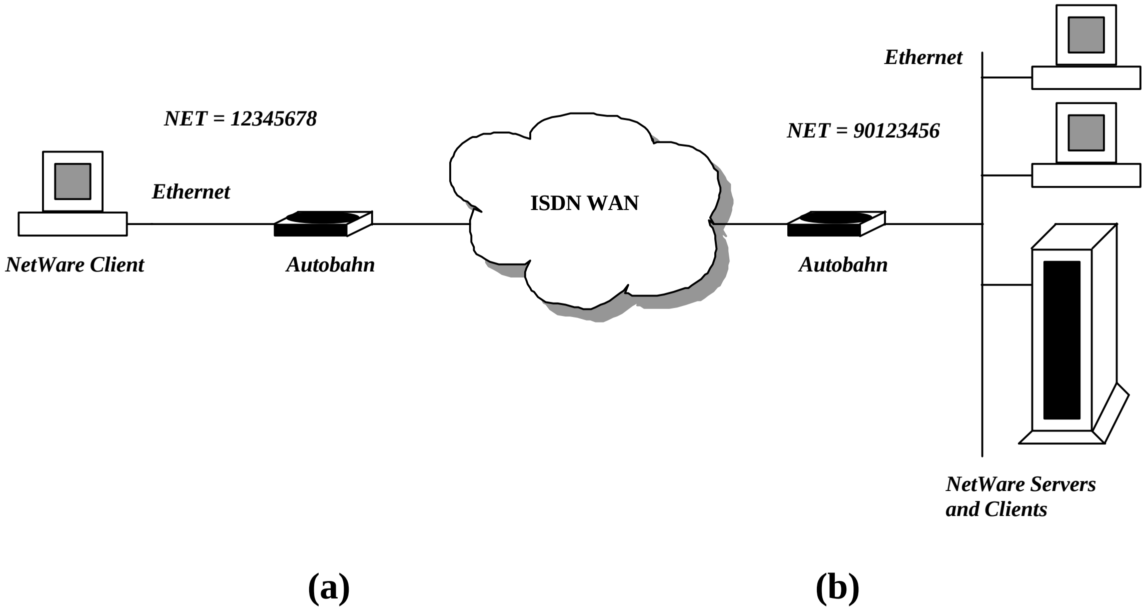


Figure 2. Local NetWare Servers Only

Again, once a connection is established between the two peers, RIP and SAP information will flow across all links, populating the associated RIP and SAP tables on both routers and allowing topology information about the complete routed network to be disseminated to all attached nodes.

3.4.3 Connecting to a Remote ISDN-Attached Client

The third type of topology, illustrated in figure 3, involves the use of the Autobahn as a server for directly attached IPX clients. These are typically PCs equipped with ISDN terminal adapter cards, or PCs that are attached to ISDN modems via their serial ports. The Autobahn supports this type of remote peer through the **“IPX Peer Type”** and **“Remote IPX Network Number”** parameters in the matching connection profile. Again, the configuration requirements for the Autobahn in this scenario are virtually identical to those listed in section 3.4.1, except that the **“IPX Peer Type”** parameter in the matching connection profile on the called party Autobahn must be set to *Client*. Additionally, the **“Remote IPX Network Number”** must be configured in the matching connection profile on the called party Autobahn in order to cause an IPX network number to be assigned to the WAN link. In the router-to-router configuration, this is not required since each peer has a local network number associated with it. However, in order to route packets to/from a remote ISDN-attached client, the Autobahn must be able to install a route to that client. This is only possible if there is a remote network with which the Autobahn can associate the remote client; this network is specified in the **“Remote IPX Network Number”** parameter in the matching connection profile on the called party Autobahn.

Note: If, on the called party Autobahn, the **IPX Peer Type** parameter in the matching connection profile is set to *Client* and the **Remote IPX Network Number** is set to 00000000, the calling party (i.e., the ISDN-attached client) must be configured to supply a non-zero IPX network number during link negotiation.

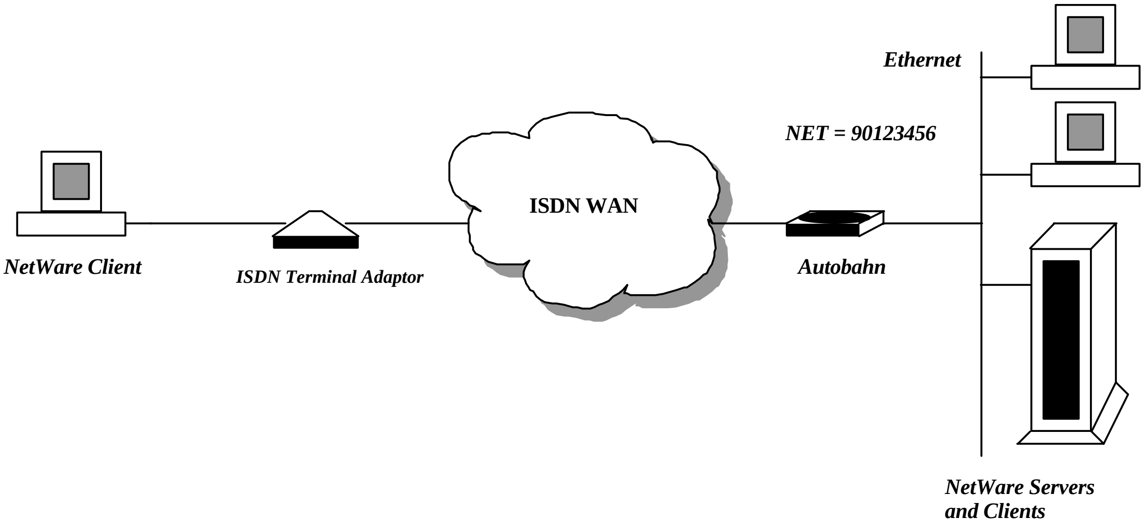


Figure 3. Direct Dial-In NetWare Client

4. Network Address Translation (NAT)

The ALR Autobahn now includes a feature called Network Address Translation (NAT). NAT allows an entire Local Area Network to be hidden from the "outside world" and represented as a single public IP address. The single public IP address can either be statically or dynamically assigned to the router. The advantages of NAT include improved security and the ability to use an low-cost single user dial-up account rather than a more costly LAN account. NAT is configurable on a per connection profile basis so the Autobahn may be configured to simultaneously do NAT and standard IP routing using multiple connection profiles.

4.1 Configuring NAT on the Autobahn

The following sections provide descriptions of the configuration parameters that have either been modified or newly added to support NAT on the Autobahn.

4.1.1 IP Options

The IP Options submenu within each individual connection profile allows for the configuration of IP parameters for WAN links that are established using that profile. The following sections describe parameters that were added for NAT:

4.1.1.1 NAT Enable

NAT can be enabled on a per-connection profile basis by making the following menu selections:

Advanced Setup => WAN Configuration => Connection Profiles => <Select Connection Profile> =>
IP Options => NAT

Select **Enable** for this parameter if the profile requires Network Address Translation. Select **Disable** for this parameter if the profile does not require Network Address Translation.

4.1.1.2 NAT Local WAN IP Address

The single IP address that NAT hides the network behind can either be assigned to the Autobahn during WAN link negotiation (dynamic) or be pre-assigned (static) and simply verified during WAN link negotiation. The following parameter controls the IP address used by the Autobahn and can be configured on a per-connection profile basis by making the following menu selections:

Advanced Setup => WAN Configuration => Connection Profiles => <Select Connection Profile> =>
IP Options => NAT Local WAN IP Address

When this parameter is set to 0.0.0.0, the Autobahn will request that the remote device assign an IP address to the Autobahn during WAN link negotiation. A value of 0.0.0.0 should be used for single user accounts that use a dynamically assigned IP address. If the Autobahn has been assigned a static IP address or the remote device requires the Autobahn to present its' IP address during WAN link negotiation, then the assigned IP address should be entered in this parameter. If this parameter is not 0.0.0.0, then the Autobahn will refuse any attempts by the remote device to change the Autobahn IP address and terminate the WAN link. This parameter is not used if NAT is disabled on the selected connection profile. When NAT is enabled and this parameter is 0.0.0.0, then the IP address assigned to the Autobahn by the remote device will be logged in the ISDN/WAN Event Log.

4.1.2 Exported Services

NATs ability to hide a local network makes it impossible for computers on the public Internet to communicate with a computer on the private local network unless the connection is first established by a computer on the local network. The Exported Services submenu eliminates this restriction by mapping a specific IP port number to a specific IP address (server) on the local network. Just as an IP address specifies a particular computer on a network an IP port number specifies a particular service within that computer. The Autobahn can export up to twenty different services to the public Internet by making the following menu selections:

Advanced Setup => LAN Configuration => IP Configuration => NAT Exported Services => <Select Export>

Status: Select *Enable* or *Disable* to activate or deactivate the specific service export.

Service Name: ASCII string (up to 10 characters) that describes the type of service being exported.

Service Port Number: Decimal TCP or UDP port number (0-65,535) whose services are to be exported.

Local Server IP Address: Specifies the IP address of the computer on the “private” local network which is to provide service for the specified port number.

Note: The following rules apply to exported services: Service exports are processed in ascending order starting with export #1. A given service port can only be exported to a single server IP address. If a service port is duplicated in more than one export then all but the first occurrence will be ignored. Any service port which is not mapped to a server IP address will automatically default to the Autobahn. For example, if the Telnet service (port 23) is not exported then any attempt to Telnet to the Autobahns’ public IP address will result in the Autobahn configuration screen being displayed on the Telnet client.

Some applications will not operate properly when NAT is enabled. Cu-SeeMe is one of these applications because current implementations require fixed client and server side port numbers. However, the Autobahn allows one client on the local LAN to use this Cu-SeeMe if port 7648 is exported to the IP address of that client. If an export is not defined then Cu-SeeMe will not work.

4.2 Sample Configuration

Figure 4 depicts a sample network configuration that uses an Autobahn with NAT to provide two clients with Internet access as well as a public WWW and FTP server. Because NAT is enabled, the IP addresses used on the local LAN are hidden from the “outside” world and can therefore be any IP network as long as it doesn’t conflict with a public network. To ensure that a conflict doesn’t occur, it is best to use one of the “private” networks reserved for this purpose as described in the document *Address Allocation for Private Internets (RFC-1597).* You can FTP this document from *ds.internic.net.* The following describes how to configure the Autobahn NAT specific parameters to operate in this configuration.

Configure the Autobahn LAN IP address and subnet mask as follows:

Advanced Setup => LAN Configuration => IP Configuration => Router IP Address = 192.168.0.1
Advanced Setup => LAN Configuration => IP Configuration => Router IP Subnet Mask=255.255.255.0

Configure connection profile #1 to dial the ISP in the usual way and enable NAT as follows:

Advanced Setup => WAN Configuration => Connection Profiles => Profile #1 =>IP Options => NAT = Enabled
Advanced Setup => WAN Configuration => Connection Profiles => Profile #1 =>IP Options => NAT Local WAN IP Address = 0.0.0.0

At this point the configuration is complete enough to give all of the clients access to the Internet. However, since the sample network includes a WWW and FTP server, the public IP address that the Autobahn will represent the entire LAN with must be known so that clients on the Internet can contact the servers. If the ISP assigns a static IP address of 199.107.11.1, configure the Autobahn as follows:

Advanced Setup => WAN Configuration => Connection Profiles => Profile #1 =>IP Options => NAT Local WAN IP Address = 199.107.11.1

The final configuration step is to export the services that the WWW and FTP servers as follows:

Advanced Setup => LAN Configuration => IP Configuration => NAT Exported Services => Export #1 =>Status = Enabled
Advanced Setup => LAN Configuration => IP Configuration => NAT Exported Services => Export #1 =>Service Name = ftp
Advanced Setup => LAN Configuration => IP Configuration => NAT Exported Services => Export #1 =>Service Port Number = 21
Advanced Setup => LAN Configuration => IP Configuration => NAT Exported Services => Export #1 =>Local Server IP Address = 192.168.0.4

Advanced Setup => LAN Configuration => IP Configuration => NAT Exported Services => Export #2 =>Status = Enabled
Advanced Setup => LAN Configuration => IP Configuration => NAT Exported Services => Export #2 =>Service Name = http
Advanced Setup => LAN Configuration => IP Configuration => NAT Exported Services => Export #2 =>Service Port Number = 80
Advanced Setup => LAN Configuration => IP Configuration => NAT Exported Services => Export #2 =>Local Server IP Address = 192.168.0.5

Note: The Autobahn default configuration includes predefined exports for all of the most common services including WWW and FTP. However, this example did not use the predefined exports in an attempt to be more clear and complete.

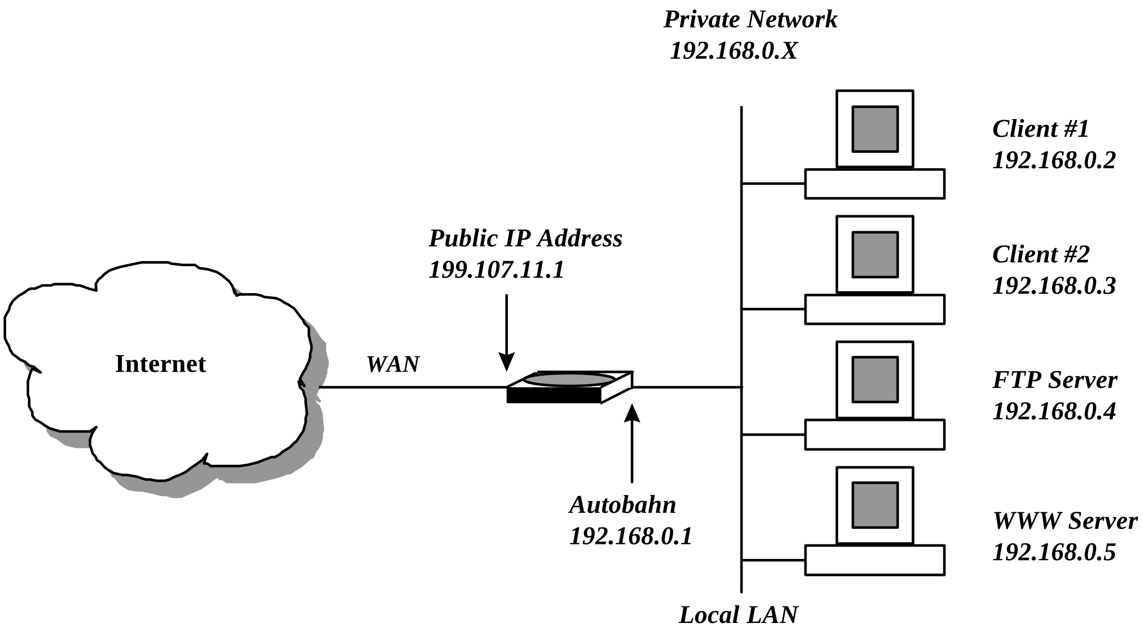


Figure 4. Sample NAT Configuration

5. Support for Graphical User Interface Utility

This release of the Autobahn firmware contains the support required to use a JAVA-based graphical user interface utility. The utility allows an Autobahn to be remotely configured even if it doesn’t have an IP address assigned to it yet. The utility is in the final testing stages and will be available soon on our WWW and FTP servers.