Caution!

As an ISDN multiprotocol router, your product establishes ISDN connections in accordance with the system´s configuration. Incorrect or incomplete configuration of your product may cause unwanted charges. The conditions that lead to establishing connections are largely dependent on the respective network configuration.

- To avoid unintentional charges, it is essential that you carefully monitor the product. Observe the LEDs of your product, use the monitoring function in the Setup Tool, or the Activity Monitor (with Software Release 5.1.1).
- Use filters to deny certain data packets, as described in your User's Guide. You should be aware that especially in a Windows network broadcasts may establish connections.
- Use the Credits Based Accounting System, as described in your User's Guide, to define a maximum number of ISDN connections resp. the accounted charges allowed in a certain period of time and thus limit unwanted charges in advance.
- Use the checklist ISDN Connections to prevent the most common causes of unintentional charges.

ISDN Connections

Here you will find possible causes for unintentional ISDN charges.

The telephone bill is unusually high.

Use the credits based accounting system. You can thus set a limit for connections with your product to prevent unnecessary charges from accumulating as a result of mistakes made during configuration.

In case of ISDN connections that remain open or unwanted ISDN connections being established:

- Using `debug all` or `trace`, check if a PC in the LAN is using a different netmask from the one entered on your router.
- Using `debug all` or `trace`, check if a PC in the LAN is configured for Remote CAPI or Remote TAPI with an incorrect IP address (destination port 2662).
- Check in ***System*** ➧ ***External System Logging*** if your router is configured to send syslog messages to a host outside the LAN (destination port 514).
- Check in the MIB table **biboAdmTrapHostTable** if your router is configured to send SNMP traps to a host outside the LAN (destination ports 161, 162).
- Check if, due to different loads of traffic, frequent opening and closing of a B-channel is occurring for connections with dynamic channel bundling.
- Using `debug all` or `trace`, check if a PC in the LAN is configured with an incorrect IP address for the WINS server (destination ports 137-139). If necessary, configure the PC properly or enter the corresponding filters.
- Using `debug all` or `trace`, check if a PC in the LAN is configured for the resolution of NetBIOS names with the help of DNS (it is accessed from a client port to destination port). Do not try to resolve NetBIOS names with DNS!

- Using `debug all` or `trace`, check if an application on a PC in the LAN is trying to resolve names that the name server at the Internet provider does not know (it is accessed from a client port to destination port 53). Install a local HOSTS file in the Windows directory that can facilitate name resolution.
- Using `debug all` or `trace`, check if NetBIOS over IP is configured on a PC in the LAN (it is accessed from source port 137 to destination port 53). The attempt is thus made to resolve NetBIOS names over DNS. Disable NetBIOS over IP or insert filters (configuration of the corresponding filters can be found in your User's Guide or use the simple NetBIOS filter of the Configuration Wizard).
- Check if you have configured Callback and in doing so entered an incorrect dial number (*Number* under ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***WAN NUMBERS*** ➧ ***EDIT***).
- If you have configured Callback, check if your partner denies your initial call using `debug all` or `trace` (D channel). For example, if your dial number is not being transmitted over the ISDN during the initial call, your partner firstly takes the call to identify the caller before a callback is being established.
- Check if you left running a trace program over an ISDN-PPP connection. That would cause the constant sending of packets over ISDN, the connection would remain permanently open.
- In the DIME Tools check under **Configuration** ➧ **Options** if **DNS Name Resolution** is activated for the **Syslog deamon**. That would cause an ISDN connection if the DNS server is outside your LAN. For example, if you configured Internet acces with your router, usually the DNS server of your Internet Service Provider is used for name resolution.
- For X.25 connections check in ***X.25*** ➧ ***LINK CONFIGURATION*** ➧ ***EDIT*** if you set the *Layer 2 Behaviour* to *always active*. (Corresponds with a value of -1 for the variable **L2IdleTimer** in the **X25LinkPresetTable**). The connection could remain permanently open.
- With Release 5.1.1: Check if you set a shorthold of -1 for one of your WAN partners (**PPPShortHold** variable in the **biboPPPTable**). That would cause a constant reestablishment of the connection.

- With Release 5.1.1: Check in ***SYSTEM*** ➧ ***EXTERNAL ACTIVITY MONITOR*** if your router is configured to send packets for the Activity Monitor to a host outside the LAN.