Achtung!

Als ISDN-Multiprotokollrouter baut Ihr Produkt in Abhängigkeit von der Systemkonfiguration ISDN-Verbindungen auf. Eine fehlerhafte oder unvollständige Konfiguration Ihres Routers kann erhöhte Gebühren verursachen. Die Bedingungen, die zu vermehrten Verbindungsaufbauten führen, hängen stark vom jeweiligen Netzwerk ab, in dem Ihr Router eingesetzt wird.

- Um ungewollte Gebühren zu vermeiden, sollten Sie Ihr Produkt unbedingt überwachen. Beobachten Sie die Leuchtanzeigen Ihres Produkts, benutzen Sie die Monitorfunktion des Setup Tools oder den Activity Monitor (ab Software Release 5.1.1).
- Setzten Sie Filter ein, wie in Ihrem Handbuch beschrieben, um bestimmte Datenpakete zu verwerfen. Achten Sie darauf, daß speziell in Windows-Netzwerken durch Broadcasts ISDN-Verbindungen aufgebaut werden können.
- Nutzen Sie das Taschengeldkonto (Credits Based Accounting System), wie in Ihrem Handbuch beschrieben, um eine maximale Anzahl/Dauer von ISDN-Verbindungen oder eine maximale Höhe der Gebühren innerhalb einer bestimmten Zeit festzulegen. So schränken Sie überhöhte Gebühren im voraus ein.
- Verwenden Sie die Checkliste ISDN-Verbindungen, um die meisten Gründe für überhöhte Gebühren auszuschließen.

ISDN-Verbindungen

Hier finden Sie mögliche Gründe für überhöhte ISDN-Gebühren.

Die Telefonrechnung ist ungewöhnlich hoch.

Nutzen Sie die Funktion Taschengeldkonto. Damit können Sie für Verbindungen mit Ihrem Produkt ein Limit festlegen, um Gebühren aufgrund von Fehlern bei der Konfiguration in Grenzen zu halten.

Möglicherweise gibt es auf Ihrem Gerät ISDN-Verbindungen, die ständig offen bleiben oder es werden ungewollte ISDN-Verbindungen aufgebaut.

- Überprüfen Sie mit `debug all` oder `trace`, ob ein Rechner im LAN eine andere Netzmaske verwendet als auf Ihrem Gerät eingetragen ist.
- Überprüfen Sie mit `debug all` oder `trace`, ob ein Rechner im LAN mit einer falschen IP-Adresse für Remote-CAPI or Remote-TAPI konfiguriert ist (Zielport 2662).
- Überprüfen Sie in ***System*** ➧ ***External System Logging***, ob Ihr Gerät so konfiguriert ist, daß Syslog-Messages auf einen Host außerhalb des LANs geschickt werden (Zielport 514).
- Überprüfen Sie in der MIB-Tabelle **biboAdmTrapHostTable**, ob Ihr Gerät so konfiguriert ist, daß SNMP-Traps auf einen Host außerhalb des LANs geschickt werden (Zielports 161, 162).
- Überprüfen Sie, ob bei Verbindungen mit dynamischem Channel Bundling häufiges Auf- und Abbauen des zweiten B-Kanals aufgrund von schwankendem Traffic geschieht.
- Überprüfen Sie mit `debug all` oder `trace`, ob ein Rechner im LAN mit einer falschen IP-Adresse für den WINS-Server konfiguriert ist (Zielports 137-139). Konfigurieren Sie gegebenenfalls den Rechner richtig oder setzen Sie entsprechende Filter ein.
- Überprüfen Sie mit `debug all` oder `trace`, ob ein Rechner im LAN für Namensauflösung von NetBIOS-Namen mit Hilfe von DNS konfiguriert ist

(es wird von einem Clientport aus auf Zielport 53 zugegriffen). Versuchen Sie nicht, NetBIOS-Namen mit DNS aufzulösen!

- Überprüfen Sie mit `debug all` oder `trace`, ob eine Applikation auf einem Rechner im LAN versucht, Adressen aufzulösen, die der Name-Server beim Internet Service Provider nicht kennt (es wird von einem Clientport aus auf Zielport 53 zugegriffen). Richten Sie eine lokale HOSTS-Datei im Windows-Verzeichnis ein, die die Namensauflösung durchführen kann.
- Überprüfen Sie mit `debug all` oder `trace`, ob auf einem Rechner im LAN NetBIOS over IP eingerichtet ist (es wird vom Sourceport 137 auf den Zielport 53 zugegriffen). Dabei wird versucht, NetBios-Namen über DNS aufzulösen. Schalten Sie NetBIOS over IP ab oder setzen Sie Filter ein (Konfiguration der entsprechenden Filter finden Sie in Ihrem Handbuch oder nutzen Sie den einfachen NetBIOS-Filter des Configuration Wizards.
- Überprüfen Sie, ob Sie Callback konfiguriert haben und dabei eine falsche Rufnummer eingegeben haben (*Number* unter ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***WAN NUMBERS*** ➧ ***EDIT***).
- Wenn Sie Callback konfiguriert haben, überprüfen Sie mit `debug all` oder `trace` (im D-Kanal), ob die Gegenstelle den initialen Ruf ablehnt. Wird beispielsweise Ihre ISDN-Rufnummer beim initialen Ruf der Gegenstelle nicht mitgeliefert, nimmt die Gegenstelle Ihren Ruf zunächst an bevor der eigentliche Rückruf stattfindet.
- Überprüfen Sie, ob Sie ein trace-Programm über eine ISDN-PPP-Verbindung laufen lassen. Damit werden ständig Pakete über die ISDN-Verbindung gesendet, die Verbindung bleibt permanent offen.
- Überprüfen Sie, ob in den DIME Tools unter **Configuration** ➧ **Options** die Funktion **DNS Name Resolution** für den **Syslog deamon** aktiviert ist. Ist die Funktion aktiviert, werden bei DNS-Anfragen ISDN-Verbindungen aufgebaut, wenn sich der DNS-Server außerhalb Ihres LANs befindet. Wenn Sie z. B. über Ihren Router einen Internetzugang eingerichtet haben, dann ist typischerweise der DNS-Server beim Internet Service Provider.
- Überprüfen Sie bei X.25-Verbindungen, ob Sie in ***X.25*** ➧ ***LINK CONFIGURATION*** ➧ ***EDIT*** für *Layer 2 Behaviour* den Wert *always active* eingestellt haben. (Das entspricht dem Wert -1 der Variablen **L2IdleTimer** in der MIB-Tabelle **X25LinkPresetTable**). Dies kann eine Dauerverbindung zur Folge haben.

- Ab Release 5.1.1: Überprüfen Sie, ob Sie zu einem Ihrer WAN-Partner einen Shorthold von -1 eingestellt haben (Variable **PPPShortHold** in der Tabelle **biboPPPTable**). Wenn ja, werden ständig erneut Verbindungen aufgebaut.
- Ab Release 5.1.1: Überprüfen Sie in ***System*** ➧ ***External Activity Monitor***, ob Ihr Gerät so konfiguriert ist, daß es die Pakete für den Activity Monitor auf einen Host außerhalb des LANs schickt.