THE BINTEC ROUTER FEATURES

August 2000

THE BINTEC ROUTER FEATURES

REFERENCE

1 The BinTec router Features

As a multiprotocol ISDN router, the BinTec router supports too many networking protocols and ISDN features to cover in detail in a single chapter. The configuration of many of these features are tucked away in the BinTec router's systems tables and can only be explained in light of their usage. This chapter gives you an overview of the major features found on the BinTec router and references other locations within this document where they are explained in more detail.

1.1 ISDN Features

1.1.1 ISDN Protocol Support

The BinTec router supports the following ISDN protocols:

- Euro ISDN (Europe)
- 1TR6 National ISDN in Germany
- National ISDN 1 (USA)
- National ISDN 2 (USA)
- Northern Telecom DMS-100 (USA)
- AT&T 5ESS Custom ISDN (USA)
- NTT INS64 ISDN (Japan)

1.1.2 V.110 Support

V.110 is a ITU-T standard that defines the communications procedures to use when a communications device can't match the data rates offered by an ISDN and is aptly called bit rate adaption. Basically the transmitter and receiver have to agree to add additional bits during transmission to adjust the data rate to a mutually compatible rate. Asynchronous bit rate adaptation is often used in communication with terminal adapters and for connecting to GSM networks from the ISDN.

The BinTec router supports bit rate adaption according to the V.110 standard for both incoming and outgoing calls. The type of bit rate adaption can be configured separately for each dialup PPP partner in the ***biboPPPTable***. This is explained in ISDN.

1.1.3 ISDN Callback Support

The BinTec router supports ISDN Callback in both directions. Also an important security feature, callback can be configured on a per-partner basis to:

enabled — Here, the BinTec router accepts an initial call from a specified partner. Upon succesful identification, the BinTec router immediately closes the connection and returns the call.

expected — When callback is expected, the BinTec router is the initiating party. The BinTec router calls the specified partner, closes the connection, and waits (expects) the partner to return the call.

Configuring callback is covered in IP.

1.2 IP Features

1.2.1 Bandwidth On Demand

There is a range of possibilities available to optimize the efficiency of your line utilization. The BinTec router can bundle leased lines with dialup lines; it can bundle pure dialup lines; backup operation is also available for leased line connections; or Bandwidth On Demand can be configured for backup connections.

For a detailed description and configuration, see IP.

1.2.2 DHCP Server

The BinTec router can be used as a DHCP (Dynamic Host Configuration Protocol) Server to manage networking resources for a number of local or remote DHCP clients. This is an efficient way of administering limited IP address resources. The BinTec router supports DNS and WINS Relay.

Clients such as Windows 95 and Windows NT hosts can be configured to request networking resources from a DHCP server and to adjust their configurations appropriately. Configuring the BinTec router as a DHCP server is covered in IP.

1.2.3 DNS and WINS (NBNS) Negotiation over PPP

The BinTec router supports DNS and WINS Negotiation over PPP as specified in RFC 1877. This means that the BinTec router is able to negotiate and configure its primary and secondary domain name servers and its primary and secondary NetBios name servers at connection time with compliant hosts.

DNS/WINS Negotiation over PPP can be configured separately for each PPP partner in the ***biboPPPTable***; this is covered in IP.

1.2.4 Dynamic IP Address Assignment

Dynamic IP address assignment in both client and server modes.

Client Mode — In client mode the BinTec router is configured to accept it's own IP address after establishing an IP connection.
This is useful for sites using low to mid-range BinTec routers to connect to Internet Service Providers.

Server Mode — In server mode the BinTec router assigns an available IP addresses from a preconfigured IP address pool.
This is useful for any site using a BinTec router product as a remote access point to a central LAN.

Dynamic IP address assignment can be configured for each partner separately in the ***biboPPPtable***. This is covered in IP.

1.2.5 Extended IP Routing

Most routers base IP routing decisions solely on an IP packet's destination address. With Extended IP Routing on the BinTec router, routing decisions can be made based on additional information contained in the data packet. This gives you a much finer control over routing decisions and allows you to make routing decisions based on the contents of the IP packet:

- Type of Service (TOS field in ethernet frame)
- Source IP Address
- TCP Source Port
- TCP Destination Port

Routing decisions can also be based on BinTec router interfaces:

- Source Interface
- State of the Destination Interface

The main advantage of extended IP routing is that traffic can be selectively routed over different transport mediums based on your site's needs. Some users require greater bandwidth for bulk data transmissions while others need shorter bursts for interactive sessions. Extended IP routing allows you to take advantage of different technologies (ISDN dialup, leased lines, X.25, and/or X.31 links) based on your site's specific needs.

Configuring Extended IP Routing is covered in Chapter Configuring the BRICK as an IP Router.

1.2.6 IP Session Accounting

As an advanced IP feature, IP Session Accounting lets you generate BinTec router accounting records for each TCP, UDP, or ICMP session routed over the BinTec router. Accounting records contain information such as protocol usage, source and destination addresses, transfer activity, and the date, time, and duration of the IP session. By default, accounting records are written to the BinTec router's system logging table but can also be forwarded to remote log hosts on the LAN for later processing. (See in Chapter 5).

Session accounting can be configured on a per-interface basis in the ***ipSessionTable***. This is covered in IP Session Accounting.

1.2.7 Network Address Translation

With Network Address Translation, or NAT, the BinTec router is able to hide a complete LAN behind a single IP address. This means that no matter how many users are connected to the LAN, only one official IP address is required to connect the complete LAN to the Internet. This address can also be a static address or dynamically assigned by an ISP at connection time.

NAT is accomplished by manipulating all incoming/ outgoing IP packets to reflect different source and destination addresses. The translation process remains invisible to the connected networks. Hosts on the LAN continue to use standard IP addresses, however they are no longer accessible from hosts external to the LAN.

NAT is most useful where:

- Security is an issue. (controlling access to a limited number of hosts)
- The number of available IP addresses is limited.
- Monitoring of outgoing connections is desired.

NAT is an advanced IP feature, Configuring NAT see Chapter Network Address Translation.

1.2.8 Proxy ARP

Proxy ARP is supported on the BinTec router for dial-in hosts that aren’t connected directly to the LAN. With Proxy ARP the BinTec router answers ARP requests for such hosts. To the local hosts the dial-in host appears to be on the LAN segment. Note that ARP (Address Resolution Protocol) is a standard method used to map IP addresses to physical MAC address.

Proxy ARP on the BinTec router is straightforward; the respective interface is enabled in the ***ipExtIfTable***, the BinTec router adjusts its routing tables automatically. See Chapter Proxy ARP for more information on configuring Proxy ARP.

1.2.9 RIP Support

The Routing Information Protocol is commonly used in IP networks to propagate routing information among routers. The BinTec router supports version 1 and version 2 of RIP. Selected BinTec router interfaces can be configured to independently send (and/or receive) version 1, version 2, both, or no RIP packets.

See the Advanced IP Features section for information on configuring RIP Options.

1.2.10 OSPF

The BinTec router supports OSPF (Open Shortest Path First) and has been implemented according to the Internet standsards defined in RFCs 1583 (OSPF Version 2), 1793 (OSPF over Demand Circuits), and 1850 (OSPF Version 2 Management Information Base).

Special OSPF features such as MD5 authentification, importing of routing information via external protocols, and propagation of system-wide default routes is also supported.

For background info on the OSPF protocol refer to **OSPF**. Configuring OSPF on the BinTec router is explained in detail in the section Routing with OSPF.

1.3 Security Features

1.3.1 Web based Monitoring

A HTTP server is included on the BinTec router and provides SNMP community password protected access to all system tables and variables via a TCP connection (port 80 by default). This means that the BinTec router can be monitored via any WWW browser[1].

A built-in status page provides a quick overview of current operating state and hypertext links to all system information. A CGI program is also included and allows you to monitor selected system variables. Simply point a compatible web browser at the BinTec router's status page as follows.

`http://`<BinTec router*'s System Name*><**`:`***HTTP Port Number*>

More information on web based access to the BinTec router is covered in Chapter System Administration.

1.3.2 RADIUS support

RADIUS (Remote Authentication Dial In User Service), is an emerging client - server security system (initially developed by Livingston Enterprises, Inc.) to control access to network resources. The RADIUS server manages a database of user authentication data.

The BinTec router can be configured to operate as a RADIUS client that consults the RADIUS server at connection time for specified dial-in partners. Partner specific connection parameters can be centrally managed in this way. This allows sites already using the RADIUS systems to centrally manage network resources, to easily integrate the BinTec router into their existing network management system.

RADIUS support is configured using the ***biboAdmRadiusServer*** variable and the ***biboPPPTable***. This is covered in Chapter IP.

[1] Browsers must support the HTML 2.0 standard and HTML tables (RFC 1942).

1.3.3 IP Access Lists

IP Access Lists provide you with the ability to fine tune access restrictions to and from connected IP networks. Access lists define the types of IP traffic that the BinTec router should accept or deny (i.e., packets are either routed or are discarded). Access decisions are based on information contained in the IP packet such as:

- Source and/or Destination IP Address
- Source IP port (port ranges are supported)
- Destination IP port (port ranges are supported)

Sites using the BinTec router to connect a LAN to the Internet for example might want to deny all incoming FTP requests, or outgoing telnet sessions from selected LAN hosts. Access Lists provide a powerful tool in controlling access to network resources. Refer to your User's Guide for more information.

1.3.4 Bridge Filtering

Bridge Filtering, sometimes called packet filtering, can be used to control the type and amount of traffic that is bridged over local interfaces. This is an important feature most useful when bridging over WAN links such as ISDN.

Bridge filtering is relevant for sites requiring bridging where:

- Minimizing ISDN costs is a concern.
- Greater control of bridging traffic is desired.

See the section Bridge Filtering in Chapter Bridging for detailed information.

1.3.5 ISDN Call Screening

The BinTec router supports the call screening service provided by the ISDN and uses this service as an additional security measure to check the authenticity of incoming ISDN connections.

Call screening is mainly used in screening incoming PPP connections but can also be used to ensure access to the BinTec router's isdnlogin service is secure. Refer to Chapter ISDN, for information on using the ISDN screening mechanism.