



RELEASE NOTE

BIANCA/BRICK-XS

07.08.1996

New System Software Release 4.1.7

The new BIANCA/BRICK-XS system software release 4.1 revision 7 contains a couple of new features and fixes a number of bugs from the previous revision 6.

New Features

Improved Setup Tool

The BIANCA/BRICK now comes with a new, enhanced Setup Tool for easy first-time configuration. Manuals for the Setup Tool are supplied in both English (*BIANCA/BRICK-XS - Getting Started*) and German (*BIANCA/BRICK-XS - Los Geht's*).

XON/XOFF protocol now supported

The serial console interface now supports the XON/XOFF protocol, to allow slow terminals to reduce the output speed of the BRICK.

Domain Nameservers

If the primary domain nameserver (DNS) can not be reached via IP-Routing, and an ICMP unreachable message is received, the secondary nameserver is now used immediately (i.e. without further attempts to reach the primary nameserver).

New Encapsulations

Two new encapsulations are available:

mpr-lapb can be used, when error correction or data compression (V.42bis) is desired.

Data compression can be enabled on LAPB links only, because V.42bis requires an error free connection (either *ip-lapb* or *mpr-lapb* will work).

mpr-hdlc allows for compatibility with Cisco's HDLC encapsulation.

On IP-only links it is also possible to use the ISO LAPB protocol (*ip-lapb*, also known as X.75), or raw HDLC framing (*ip-hdlc*).

Improved IPX RIP behaviour

In earlier releases, if RIP was disabled (*ripCircState:x=off*) for one of the routers on a WAN connection, then *dynamic* was chosen as routing type (*ipxCircType*).

This had the effect, that no RIP or SAP packets were transmitted on this circuit, making it difficult to configure *unnumberedRIP* or *wanRIP* on both of the routers.

The new states *auto_off* and *auto_on* for the fields *ripCircState* and *sapCircState* were introduced to circumvent the problem described above.

The *ripCircState* and *sapCircState* fields can now assume the following values:

auto_off (Default)

No RIP or SAP packets are transmitted. If the remote side in a WAN connection wants to establish RIP or SAP the state changes to *auto_on*.

auto_on As long as the connection is active, RIP or SAP packets are transmitted, and the fields *Update* and *AgeMultiplier* indicate, when these packets are transmitted (see RIP/SAP update/ spoofing). Once the connection is terminated the state returns to *auto_off*.

off No RIP or SAP packets are transmitted or accepted.

on RIP or SAP packets are transmitted, the fields *Update* and *AgeMultiplier* indicate, when these packets are transmitted (see RIP/SAP update/ spoofing).

To activate RIP or SAP you have to set *ripCircState* or *sapCircState* of the appropriate interface to *on*, as before.

The new states *auto_off* and *auto_on* never have to be configured manually.

Bug Fixes

CAPI

- CAPI 1.1 and CAPI 2.0 now correctly recognize DTMF tones.
- When using the National ISDN 1 profile (USA) the CIP values are now correctly set to use the μ law coding for voice connections.
- When successfully closing a fax connection the *CAP1_DISCONNECTB3_IND* message now correctly indicates *reason_b3=0*.

- If a fax connection cannot be established (e.g. if the fax number is called from a telephone) the disconnect cause is now indicated in the *CAP1_DISCONNECTB3_IND* as a CAPI error message.

IPX

- When resetting the *ipxCircNetNumber* of an interface to *0:0:0* the corresponding route is now deleted correctly and the change is made known to the network.
- Three small problems concerning IPX and IPX WAN 2 were fixed.
 - Under certain conditions the BRICK rebooted when a connection was dismantled immediately after its set-up.
 - When disconnecting and then reconnecting the ISDN cable on a leased line during a call sometimes sending and receiving IPX packets became impossible.
 - In earlier releases, when an IPX license was installed, the BRICK arbitrarily locked up when an interface changed from the *UP* state to another state.

PPP

- Deleting entries for active PPP interfaces from the *pppTable* is now possible.
- At boot time the *State* field of the *biboPPPipAssignTable* is now initialized correctly.
- PPP IDs and passwords for use with the PAP and CHAP authentication protocols can be up to 32 characters long. If longer strings are used, the authentication fails.

- There can now be several entries in the *biboPPPTable* which use *dynamic* IP address assignment and have identical entries for *AuthIdent* (PPP ID) and *AuthSecret* (PPP password).
- A problem concerning connections which were authenticated inband (e.g. *x.25_ppp* connections) was resolved. Now an arbitrary number of these calls can be handled.
- If *MaxConn* is set to 1 (use only one B channel) the MRRU option (Multilink PPP) is not used for this connection. This is to ensure compatibility with older routers from other vendors.
- If the variable *biboPPPMaxRetries* is set to 0 now only one dialling attempt is made.'

Miscellaneous

- The output of the tool *isdnlogin* is now formatted correctly on all terminal types.
- Sometimes, after an ISDN connection was setup the first packet was received improperly resulting in a delayed B channel setup.
- The configuration of an ISDN leased channel from *leased_dce* to *leased_dte* was not possible while the system was running. A reboot was necessary to allow this configuration to work. The configuration from *leased_dte* to *leased_dce* worked without problems.
- Some arbitrary interface state changes (interface moved from up→down and back from down→up) when changes to IP routing tables were made have been removed.
- *RIP* packets are now transmitted with *ttl=1* (time-to-live) and are discarded after the next hop.

- When using the *1TR6 Point-to-Point* protocol, the telephone number is now correctly displayed in the *isdnCallTable*.
- *TFTP* transfer of configuration files is now handled correctly, even when the BRICK's system load is very high.
- Dynamic IP address allocation and subsequent IPCP negotiations are now handled correctly.
- The IP driver now reliably handles more messages and in rapid succession (especially insecure UDP messages).