ISDN

August 2000

ISDN

Table of Contents

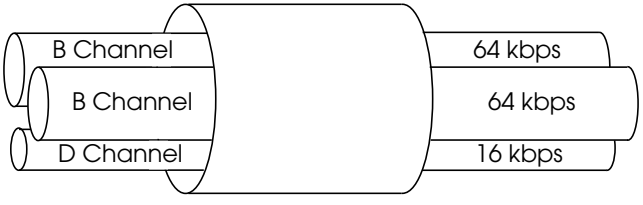
REFERENCE

1 ISDN Connections on a BinTec router

1.1 Some background on ISDN

The term ISDN (Integrated Services Digital Network) was defined by the ITU-T (formerly CCITT) and describes a telecommunications service package supported by telephone companies around the world. As an enhancement to the existing public telephone network, ISDN allows voice, data, video, etc. to be transmitted over existing telephone lines using digital transmission. This allows ISDN users to access multiple services such as telephony, telex, teletex, fax, videotex, and X.25 networking simultaneously from one access point. The ISDN access point, often called subscriber outlet, consists of a standard RJ-45 twisted pair port.

The subscriber outlet can be seen as the user end of a sort of 'digital-pipe' which transfers digital traffic to and from the local telephone company. This digital pipe allows data transfers using a number of channels, commonly known as the B and D channels.



ISDN Basic Rate Interface

1.1.1 B and D Channels

B-channel: The B-channel is used for transferring user data; text, data, voice and still images in full duplex mode. The B-channel can handle data transmission at a rate of 64 kbps.

D-channel: The D-channel's primary function is for signalling between the user equipment (telephone, facsimile, computer, etc.) and the telephone company. The D-channel can handle data transmission at a rate of 16 kbps. In Euro-ISDN the D-channel can also be used for transferring user data.

1.1.2 ISDN Interfaces

The capacity and type of service this digital pipe provides can vary and depends on the type of access you have to the ISDN. The most common types of ISDN interfaces, which are defined by the ITU-T, are the basic rate interface (BRI) and the primary rate interface (PRI). These in turn determine the number of available channels within the pipe and the transfer rates used by each channel.

Basic Rate Interface

An ISDN basic rate interface, or BRI is sometimes called an S_0 interface. It provides two B-channels (64 kbps each) and one D-channel (16 kbps) allowing for a total user data rate of the 144kbps (2 x 64 kbps + 16 kbps). Up to eight end-devices can be connected to an S_0 interface, including telephones, facsimile machines, computers etc.

The network sends control messages over the D-channel to establish connections with the end-devices corresponding to the type of service requested. Two different

end-devices can be used simultaneously and independently via a single S_0 interface.

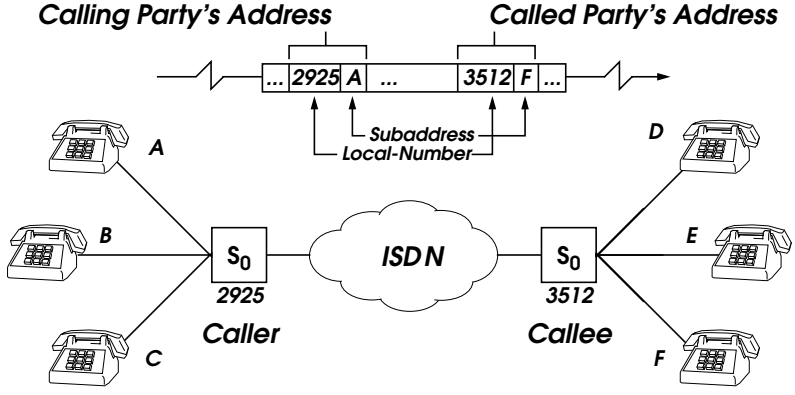
Primary Rate Interface

A primary rate interface, or PRI, is sometimes called an S_{2M} interface. It provides 30 B-channels and one D-channel. As with a BRI the D-channel is used for signalling but since 30 B channels need to be managed in a PRI, the D-channel has a data rate of 64 kbps. This allows for a total user data rate of 1.984 Mbps (31 x 64 kbps).

In North America, a PRI consists of 23 B-channels and one D-channel. The differences between the number of channels are historically based and relates to voice technologies that existed when ISDN was developed.

1.1.3 Called & Calling Party's Numbers

The signalling used in setting up ISDN calls includes information that identifies both the **caller** and **callee** and is referred to as the *Calling Party's Number* and *Called Party's Number* respectively. Both addresses consist of a **Local Number** and an optional **Subaddress.** The calling party and called party numbers are sometimes called *directory numbers* in the ISDN world.



Local Number

Most ISDN basic rate interfaces today come with three separate telephone numbers. These numbers are commonly used to identify specific telecommunications equipment at a subscriber's site. For example, the caller in the diagram above might have the ISDN numbers 2925, 2926, and 2927. Euro-ISDN and National-ISDN in Germany use different names and procedures for identifying separate local numbers.

- **Euro-ISDN**
  In Euro-ISDN, the DSS1 signalling protocol is used. Depending on the type of service arrangement with the local telephone company, the subscriber

NOTE: Subaddressing in ISDN should not be confused with the different local numbers available in Euro ISDN and 1TR6 (National ISDN in Germany). Subaddressing is not available in the 1TR6 protocol. In other ISDN protocols subaddresses are optional and usually have to be purchased separately from the ISDN provider.

receives three or more Local Numbers. These numbers are called MSNs (multiple subscriber number). Additional MSNs can normally be purchased from the ISDN service provider.

- **1TR6** (National ISDN in Germany)
  In Germany, the 1TR6 signalling protocol is used. The ISDN number assigned by the telephone company, e.g. 0911 / 99002, can be extended by appending an additional digit (known as the EAZ, or Endgeräteauswahlziffer) to this number. Up to nine different EAZ numbers (1...9) can be used. EAZ 0 is used as a global, to allow all equipment to receive incoming calls in parallel. This signalling protocol is not supported by PABX-BinTec routers and, in any case, will no longer be supported in the new millenium, as it is being replaced by the DSS1.

1.1.4 ISDN Screening Indicator

The ISDN screening indicator is a service provided by ISDN that can be used to test the trustworthiness of the calling party's number. The calling party's number (CPN) reported by an incoming call may have been assigned by the user placing the call or by the telephone switching station.

If the CPN was assigned by the user the switching station may optionally verify this address is correct in order to detect malicious calls. The party (user or network) that assigned the CPN and whether or not the CPN has been verified is reported in ISDN in the Screening Indicator field of

the call packet. The values shown below are used and indicate the respective circumstances.

Screening Indicator	CPN assigned by	Status of Calling Party's Number
network	network	The CPN was set by the network. (verification not required)
user-verified	user	The CPN was set by the user and was verified by the network.
user	user	The CPN was set by the user but no verification was attempted.
user-failed	user	The CPN was set by the user and verification of the number failed.

1.2 Attached ISDN hardware

1.2.1 ISDN Auto Configuration

The ISDN auto configure procedure attempts to verify:

1. The presence of each ISDN interface.
2. Which type of D channel protocol is used.
3. Which TEI procedure is used.

Normally, the BinTec router attempts to configure its ISDN interface(s) automatically at boot time (see Turning Off Auto Configuration). If your ISDN module is installed, the auto configuration process is started once the module is connected to your subscriber outlet. The configuration process can also be started manually while the system is running (see Restarting Auto Configuration).

Once the auto configure process is complete (see Verifying Auto Configuration) the BinTec router initializes a protocol stack for each D channel. The results of the auto configure process are then written to the ***isdnStkTable*** which lists the attributes of each ISDN stack. Access to the ISDN is possible once the following objects are defined:

isdnStkTable **Field**	**Must be:**
ProtocolProfile	dss1 **or** dtr6
Configuration	point_to_point **or** point_to_multipoint
Status	loaded

Verifying Auto Configuration

You can verify whether the auto configuration procedure was successful. First, display the status of the auto config-

ure process by displaying the ***isdnIfTable***. If the ***AutoconfigState*** field is set to **done**, then the auto configure procedure is complete.

Next, verify the operational status of the interface by viewing the ***isdnStkTable***. If the ***Status*** field is set to **loaded** then auto configuration was also successful. The interface is ready to accept connections.

Turning Off Auto Configuration

As long as ***isdnIfAutoconfig*** is set to **on** (the default), auto configuration will be performed. If set to **off** then information for the respective interface will not be configured, but will be loaded from the ***isdnStkTable*** instead.

Restarting Auto Configuration

If auto configuration was not successful you can restart the procedure by assigning **start** to the ***isdnIfAutoconfigState*** field of the isdnIfTable .

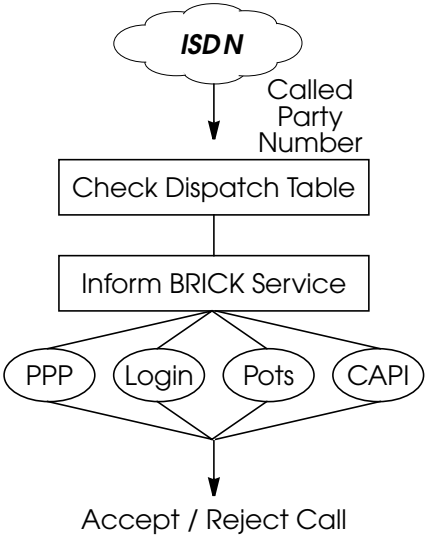
```
isdnIfAutoconfigState:0=start
```

1.3 ISDN Call Dispatching

1.3.1 Overview

The BinTec router uses an internal Dispatching Algorithm to dispatch incoming ISDN calls to various services based on the Called Party Number, or CPN, signalled by the ISDN. Currently, BinTec router services include:

- Routing Service — The PPP service is the BinTec router's main routing service. This service is used for incoming data calls for dialup network connections from ISDN WAN partners.
- Login Service — The login service provides access to the SNMP shell.
- Pots Service — The pots service is only available on the V!CAS and is for calls that need to be routed to attached analog devices (V!CAS POTS ports A and B).
- CAPI Service — The CAPI service is used for incoming calls from remote CAPI applications (version 1.1 or 2.0) that need to connect to CAPI application running on a workstation on the BinTec router's LAN.



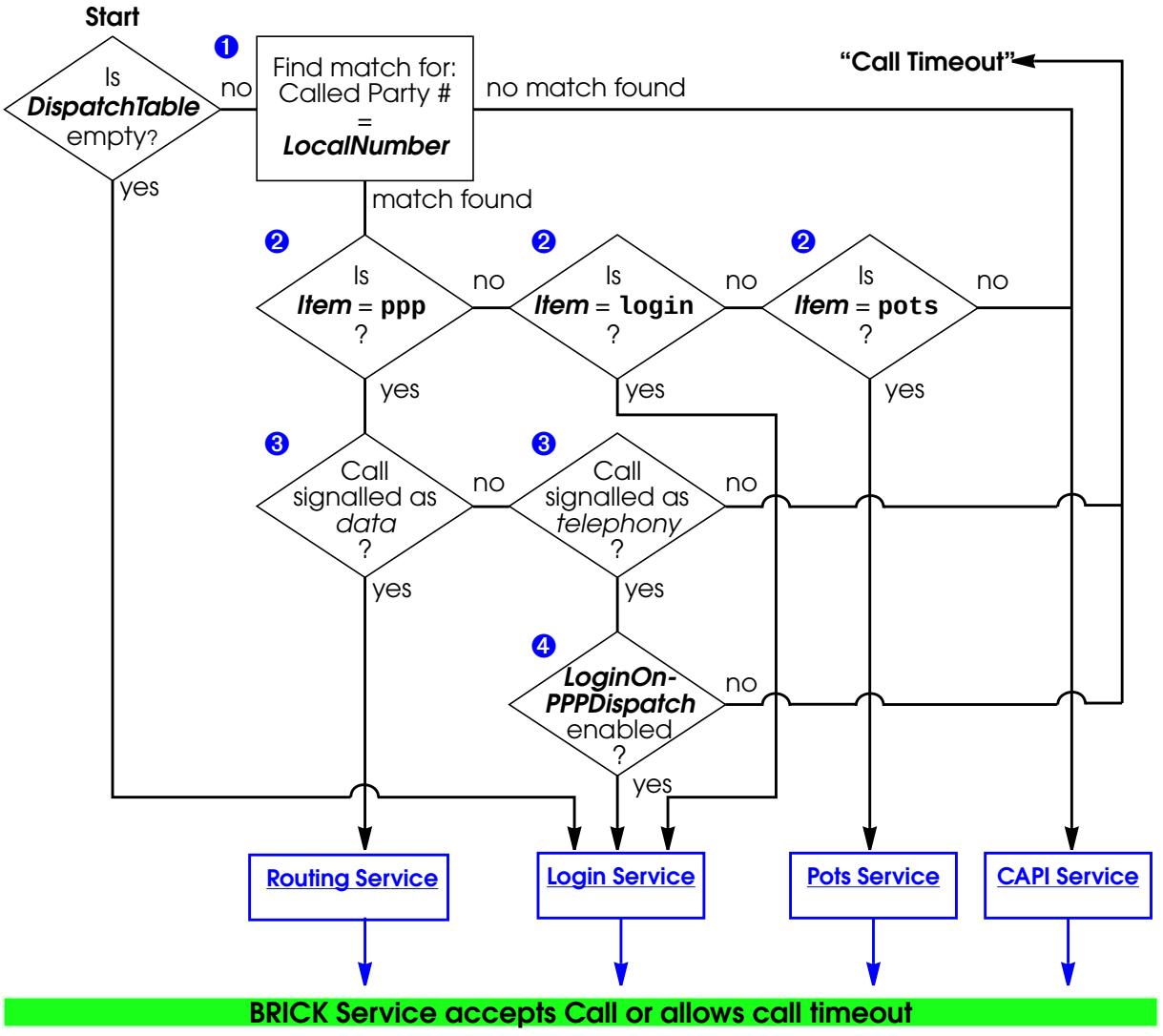
The basic procedure for dispatching incoming calls shown here simply means that when an incoming call is received, the BinTec router then searches the ***isdnDispatchTable*** for an entry that matches the CPN. If a match is found the call is given to the appropriate service which may decide to accept or reject the call based on other information relating to the call. If no match is found the call is given to the CAPI service which informs CAPI applications on the LAN of the call.

These decisions are described in further detail in the following sections. Note that the dispatching table is also used for outgoing calls too. This is covered in the section Outgoing Calls.

1.3.2 Dispatching Algorithm

This diagram shows the initial steps used to dispatch incoming calls on the BinTec router. Information relating to

each step is listed on the following page. Additional steps taken by the respective services are described separately.



❶ Here, the ***isdnDispatchTable*** is searched for a matching entry. Note that since this is an incoming call, only entries with ***Direction*** = both or incoming are valid in this context. A match is found if the Called Party's Number matches the ***LocalNumber*** field. It is important that each MSN is mapped to no more than one service.

❷ The ***Item*** field of the matched entry determines which BinTec router service is informed of the call.

❸ Note that the ISDN may signal a call (just another term for identifying the calls type) as being a data or a telephony call. This step has been implemented for sites that only have one MSN. See step 4.

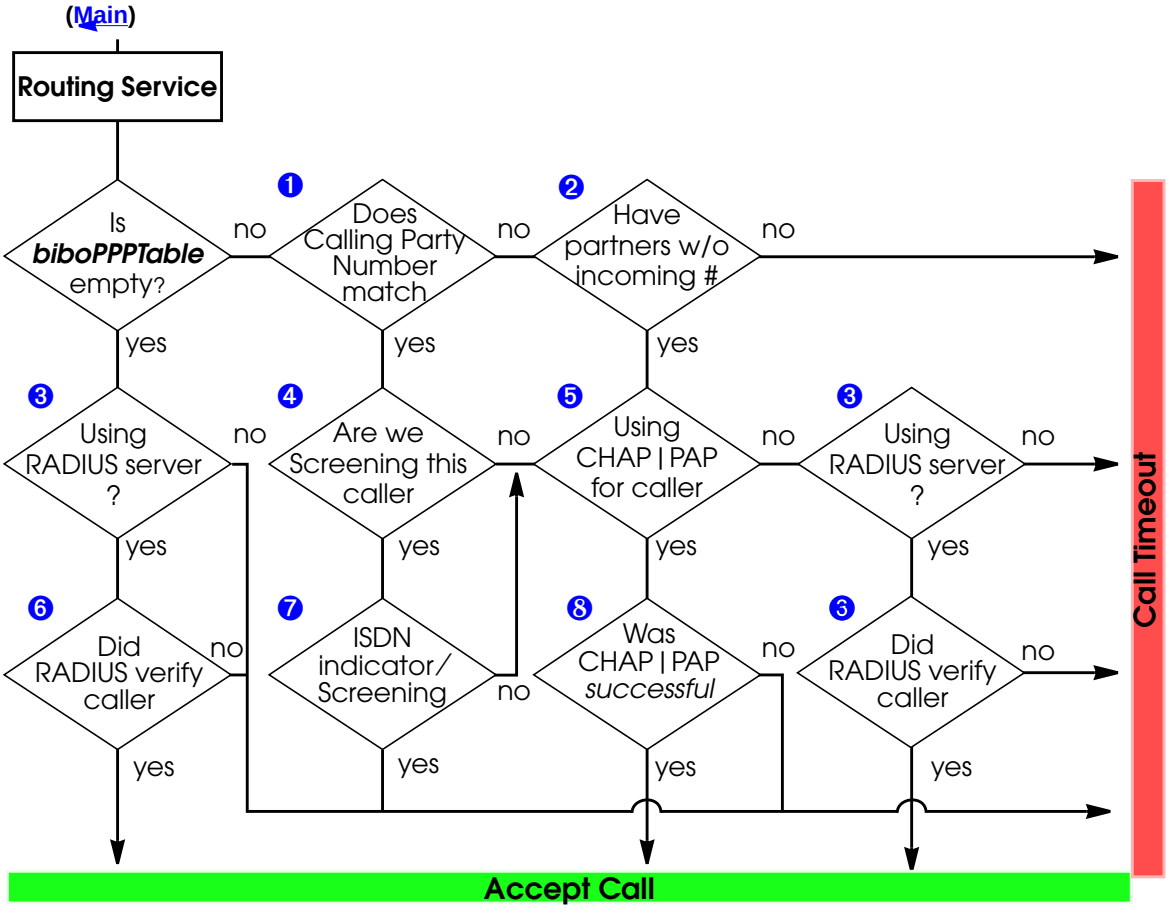
❹ This additional step has been implemented for sites that only have one
MSN. Since these sites will have to use their sole MSN for the routing service this step allows them to dispatch calls to the login service using the ***isdnLoginOnPPPDispatch*** variable.

The isdnlogin command (from the SNMP shell) can be used from a remote BinTec router to establish an ISDN call to a BinTec router with one MSN (and appropriately configured) using the servicename "telephony".

`isdnlogin` <*telephone number*> **`telephony`**

Routing Service

The Routing service decides whether to accept or reject the call based on the diagram shown below.



❶ Here, the Calling Party's Number transmitted via the ISDN is compared to each entry's ***Number*** field in the ***biboDialTable***. This is the first step of "OUTBAND" authentication, also known as Calling Line ID. Note that even if a match is

found the caller still has not incurred any charges at this point.

❷ If the Calling Party's Number couldn't be matched in the ***DialTable*** the BinTec router checks to see if any WAN partner's exist (***biboPPPTable***) that do not have an incoming number (***biboDialDirection*** = `both` or `incoming`).

❸ If a RADIUS server is configured in ***biboAdmRadiusServer*** this step resolves as yes. The call is then initially accepted (charges are incurred by the caller) if it hasn't already been, and the RADIUS server is consulted.

❹ The Screening field from the matched ***DialTable*** entry from step 1 determines whether screening should be performed for calls from this number. If ***Screening*** for this entry is set to `dont_care` the screening feature is not being used. Screening is the second step of OUTBAND authentication; meaning that ISDN charges for the caller still have not been incurred.

Background information on ISDN Screening is covered the section ISDN Screening Indicator.

❺ WAN partners configured to use CHAP and/or PAP authentication are identified in the ***biboPPPTable*** by the ***Authentication*** field which will be set to either; `pap`, `chap`, or `both`.

Once the dispatching algorithm reaches this step, the ISDN call is initially accepted to perform INBAND authentication.

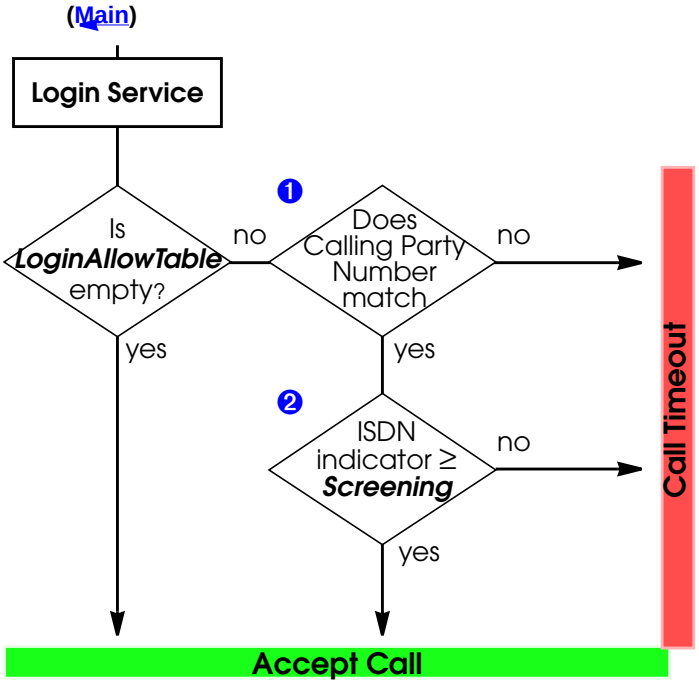
❻ If the RADIUS server was able to verify the caller, the BinTec router accepts the call and establishes the network connection according to the parameters provided by the RADIUS server. Otherwise, the call is disconnected.

❼ When screening incoming calls, the ***biboDialScreening*** variable is compared to the screening indicator provided by the ISDN. The value provided by the ISDN must be greater than or equal to ***biboDialScreening***.

❽ The last step for WAN partners that must authenticate via CHAP or PAP.

Login Service

The Login Service may accept or reject an incoming call based on the diagram shown below.



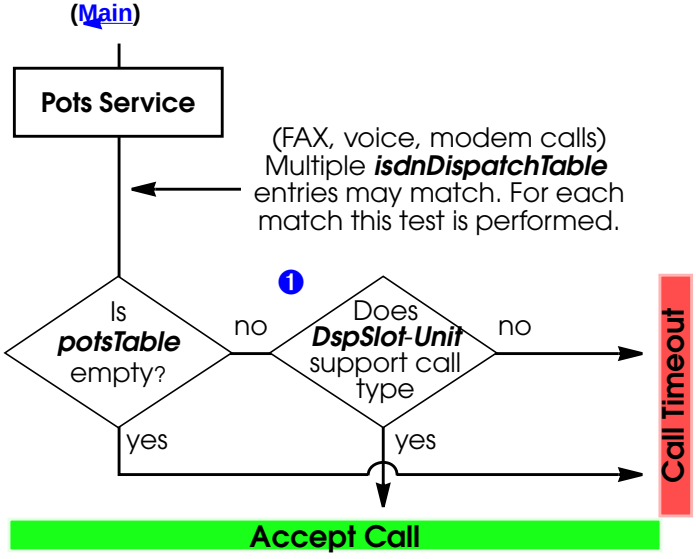
❶ Here, the ***isdnLoginAllowTable*** is searched for a matching entry. A match is found by comparing the Calling Party's Number with the ***Number*** fields of each entry. Note that the number field supports wildcard characters and multiple entries may match an incoming call. A match without wildcards is always used before a match with wildcards.

❷ Once a match is found the value of the ***isdnLoginAllowScreening*** field is compared with the screening indicator provided by the call setup packet. The call is accepted if

the indicator (from the setup packet) is greater than or equal to the ***Screening*** field.

Pots Service

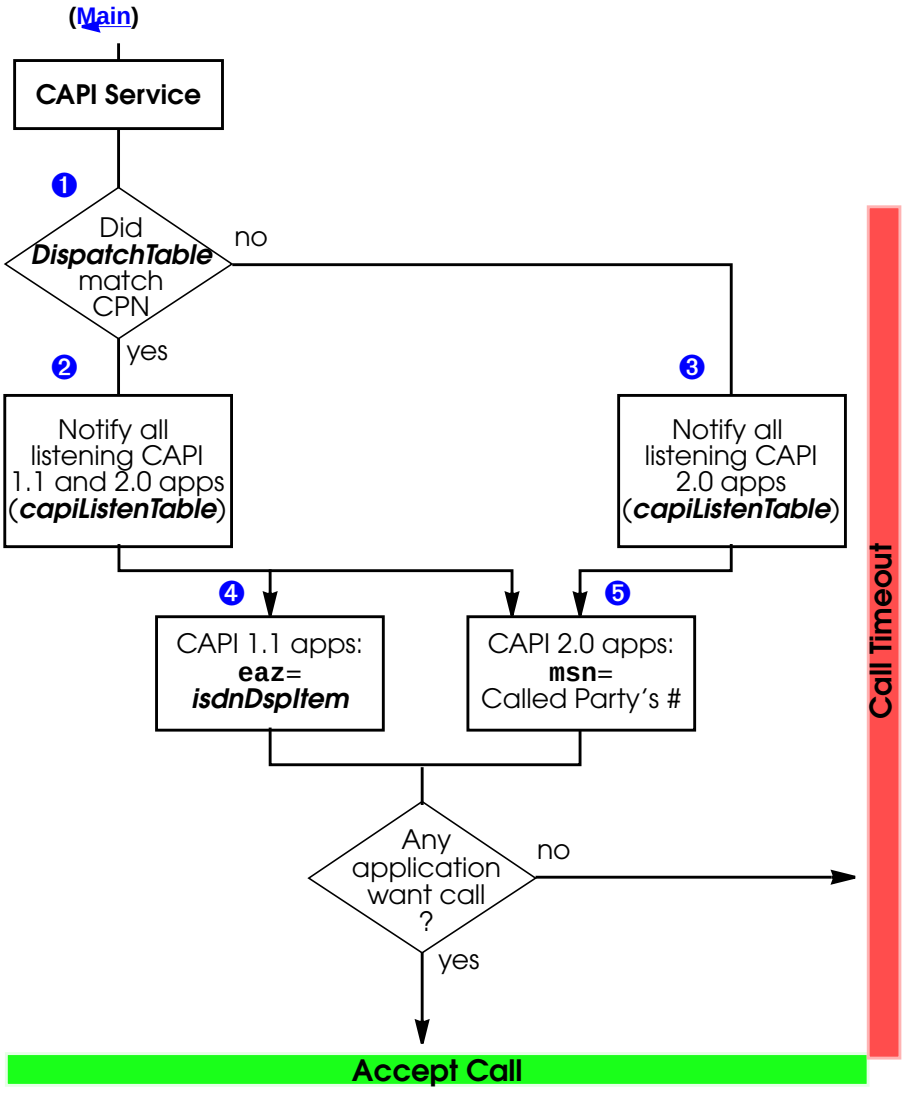
The Pots Service on the V!CAS may accept or reject an incoming call based on the diagram shown below. The Pots service is currently only available on the V!CAS.



❶ The Slot and Unit fields of the matched isdnDispatchTable entry determine the destination device for the call. The corresponding device entry is located in the ***potsIfTable***. The Type field there, determines which types of calls the device supports. See the section on POTS Interfaces for more information on the pots devices.

CAPI Service

The CAPI service on the BinTec router must inform registered CAPI clients of incoming calls. Depending on the Dispatch Table, the type of call, and the registered applications, the CAPI service accepts or rejects calls as follows.


(Main)
CAPI Service
1
Did DispatchTable match CPN
no
yes
2
Notify all listening CAPI 1.1 and 2.0 apps (capiListenTable)
3
Notify all listening CAPI 2.0 apps (capiListenTable)
4
CAPI 1.1 apps: eaz= isdnDspItem
5
CAPI 2.0 apps: msn= Called Party's #
Any application want call ?
no
yes
Accept Call
Call Timeout

❶ The ***isdnDispatchTable*** (***LocalNumber*** field) is searched for an entry that matches the called party's number contained in the ISDN call setup packet.

❷ If a match was found from the previous step, the ***Item*** field must be set to one of the values `eaz0` through `eaz9`. (see the initial dispatching diagram). In this step the BinTec router checks the contents of the ***capiListenTable*** to see which CAPI applications are listening for incoming calls. Listening version 1.1 and version 2.0 applications will be notified of the incoming call.

A brief overview of how the listening process is covered in the section The Remote CAPI.

❸ If the ***isdnDispatchTable*** contains entries but no matches were found (see the initial dispatching diagram) the call defaults to the CAPI service. In this step the BinTec router checks the contents of the ***capiListenTable*** for listening applications. Since no EAZ→MSN mapping is involved here, only CAPI 2.0 are notified of the incoming call. CAPI 2.0 applications use MSNs.

A brief overview of how the listening process is covered in the section The Remote CAPI.

❹ CAPI 1.1 applications use EAZs. When notifying CAPI 1.1 applications of a call, the EAZ value is taken from the ***isdnDspItem*** field.

❺ CAPI 2.0 applications use MSNs. When notifying CAPI 2.0 applications, the Called Party's Number from the call setup packet (which will be the same as the ***LocalNumber*** field if an ***isdnDispatchTable*** entry was matched) is sent as the MSN.

1.3.3 Outgoing Calls

For outgoing calls from CAPI 1.1 applications, the BinTec router compares the EAZ transmitted by the CAPI 1.1 application with the contents of the ***isdnDspItem*** object. Once a match is found, the BinTec router uses the respective ***isdnDspLocalNumber*** (and ***isdnLocalSubaddress*** if set) object as the "Calling Party's Address".

1.4 ISDN Line Management

1.4.1 ShortHold

To help minimize ISDN charges the ShortHold mechanism is available. ShortHold closes down unneeded dialup connections when there is no traffic to be transmitted for a specific time period. Short hold is enabled by default for all dialup partner interfaces. Two types of Short Hold mechanisms are available on the BIRCK; Static Short Hold and Dynamic Short Hold.

With ShortHold you can control the amount of time to wait before closing all remaining B-channel(s). This means that when no packets are being sent or received, the system will keep a minimum number of channels open until the ShortHold timer expires.

1.4.2 Multiple Link Support

... ISDN partners to be run over multiple channels. By dynamically allocating bandwidth (opening or closing of additional channels) higher throughput rates can be achieved. For dial-up ISDN connections this, of course, can lead to increased connection costs. To configure MLS sup-

port for a specific connection the following fields of the ***biboPPPTable*** are used:

- ***biboPPPInitConn***
  InitConn defines the number of channels to open each time an ISDN connection is requested.
- ***biboPPPMaxConn***
  MaxConn defines the maximum number of channels MLS may have open at any one time.
- ***biboPPPMinConn***
  MinConn defines the minimum number of channels to keep open at all times. If throughput drops, the number of open channels drops back to the value specified. There is one exception to this, see Shorthold.
- ***biboPPPShortHold***
  ShortHold specifies a fixed time value (in seconds) to wait before closing all channels, once the line becomes silent (i.e., no data is being transferred). For more information see: Static Short Hold.

- ***biboPPPDynShortHold***
  DynShortHold specifies the percentage of the current ChargeInterval to wait before closing all channels, once the line becomes silent. For more information see: Dynamic Short Hold

Note:

Transmitting the following packets does not result in a resetting or lengthening of the active ShortHold timer.

- IP RIP packets originating from the BinTec router
- Bridge PDU packets
- PPP Control packets (i.e., Keep Alive packets, LCP echo requests)
- IP Broadcast packets (if a transfer network exists)
- LAPB RR (or RNR) REJ-Frames (X.75).