



Fermi National Accelerator Laboratory

FERMILAB-TM-1863

Proposal for Fermilab Remote Access via ISDN

William P. Lidinsky and David E. Martin

*National HEPnet Management, Fermi National Accelerator Laboratory
P.O. Box 500, Batavia, Illinois 60510*

July 1993

Disclaimer

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.



DCD Design Note 69.0

Proposal for Fermilab Remote Access via ISDN (Ver. 1.0)

William P. Lidinsky and David E. Martin
National HEPnet Management

July 2, 1993

TABLE OF CONTENTS

1. INTRODUCTION	2
2. ISDN	3
3. ACCESS SCHEMES	4
3.1 Differences from Current Modem Access	5
3.2 Combinet Bridge Features	6
4. ARCHITECTURE	7
4.1 Specific Protocol Considerations	7
4.2 Security	9
5. EQUIPMENT AND SERVICES REQUIRED	9
5.1 ISDN Service at Remote Sites	10
5.2 Equipment at Remote Site	11
5.3 ISDN Service at the Hub Site	13
5.4 Equipment at the Hub Site	13
6. PILOT PROJECT	14
6.1 Establishing and Breaking Remote Connections	16
6.2 Security	16
6.3 Hub Bridge Control System	17
6.4 Remote Bridge Configuration	17
6.5 Questions to be Answered by Pilot Project	18
6.6 Pilot Project Candidates	19
6.7 Pilot Project Cost	19
7. SUMMARY	20
APPENDIX 1. ISDN BRIDGE PROVIDERS	21
APPENDIX 2. COMBINET BRIDGE COMMANDS	27



Proposal for Fermilab Remote Access via ISDN (Ver. 1.0)

William P. Lidinsky and David E. Martin

National HEPnet Management

1. INTRODUCTION

Currently, most users at remote sites connect to the Fermilab network via dial-up over analog modems using a dumb terminal or a personal computer emulating a dumb terminal. This level of connectivity is suitable for accessing a single, character-based application, but does not support applications with modern graphical user interfaces (GUIs) or remote file sharing or printing. A few users have been using serial-line IP (SLIP) which provides a full range of IP services, or Xremote, which allows the remote computer to act as an X-window terminal. Although a V.32bis link at 14.4 Kbps (or a V.fast link at 28 Kbps) provides excellent response for character-based and some X-window applications, is not fast enough to support a full suite of LAN-based services or even to run X-window applications that use intensive graphics. Thus the power of personal computers that are becoming ubiquitous is under-utilized.

National HEPnet Management (NHM) has been monitoring and experimenting with remote access via the integrated services digital network (ISDN) for over two years. Members of NHM felt that basic rate ISDN had the potential for providing excellent remote access capability. Initially ISDN was not able to achieve this, but recently the situation has improved. The authors feel that ISDN can now provide, at a remote site such as a user's home, a computing environment very similar to that which is available at Fermilab. Such an environment can include direct LAN access, windowing systems, graphics, networked file systems, and demanding software applications.

This paper proposes using ethernet bridging over ISDN for remote connectivity. With ISDN remote bridging, a remote Macintosh, PC, X-terminal, workstation, or other computer will be transparently connected to the Fermilab LAN. Except for a slight speed difference, the remote machine should function just as if it were on the LAN at Fermilab, with all network services—file sharing, printer sharing, X-windows, etc.—fully available.

There are two additional reasons for exploring technologies such as ISDN. First, by mid-decade environmental legislation such as the Federal Clean Air Act of 1990 and Illinois Senate Bill 2177 will likely force increased remote-worker arrangements. Second, recent pilot programs and studies have shown that for many types of work there may be a substantial cost benefits to supporting work away from the site.

2. ISDN

Until recently, ISDN, the integrated services digital network, has not been widely usable for a number of reasons. First, ISDN was not ubiquitous. When first surveyed by NHM in 1991, only a few of the 50 Fermilab personnel in a semi-random survey “loop qualified” for home ISDN service from Ameritech; qualification required that, among other things, the subscriber be within 18,000 wire feet of a central office that supported ISDN. Second, all ISDN implementations were not the same; the same equipment could not communicate with both AT&T and Northern Telecom ISDN-equipped central office (CO) switches. Third, usage rates were prohibitively expensive compared to analog voice calls. Fourth, ISDN equipment, such as remote bridges, was expensive and fairly primitive. Lastly, even though basic rate ISDN had the potential for providing bit rates of up to 128Kbps, this was still not enough to achieve “crisp-response” remote computing environment similar to that available over the local area network at Fermilab.

In the past two years a number of things have changed. ISDN is now being widely deployed. The authors have worked with the Telecommunications Group at Fermilab and have applied pressure to Ameritech. This along with the pressure from other potential users of ISDN has had its effect. Not only has Ameritech accelerated its ISDN deployment plans, but they have promised to supply ISDN service to anyone who lives within 30,000 wire feet of any CO, even if it means running expensive dedicated lines from another CO. Also, ISDN as implemented by vendors such as AT&T and NTI are rapidly becoming standardized. Much of this has been accelerated by the efforts of Bell Communications Research (Bellcore) in the promulgation of a US ISDN interoperability standard—National ISDN One (NI-1).

In the area of usage costs, Ameritech has successfully petitioned the Illinois public utility commission to lower ISDN tariffs for circuit-switched data calls to the same as analog business voice calls. As a result, ISDN local loops for data now have a cost structure very similar to that for plain old telephone service. While the cost of ISDN bridges has dropped only slightly, there are now more vendors offering ISDN bridge products and the number of features available has increased dramatically. The market is poised for substantial equipment price reductions in the near future. Also, ISDN bridges can no longer be considered primitive. Moreover their capabilities have begun to address the issues needed for remote access to an enterprise network such as Fermilab’s LAN complex. Finally, data compression has been integrated into some ISDN bridges, thus achieving effective usable bit rates up to of 300Kbps. Experiences of NHM indicate that response is fast enough to provide a remote computing environment nearly identical to that available when at Fermilab.

It may be helpful to define ISDN in more detail. ISDN is a set of international standards for delivering, directly to the end user, digital access to the world-wide public switched telephone network. Currently, almost all phone calls in the US are carried digitally and translated to analog on each end. ISDN makes it possible to avoid the analog-digital-analog conversion and thus establish an end-to-end digital connection over which voice, facsimile and other data can be sent. ISDN service is delivered either via standard twisted-pair residential wiring, called a basic rate interface (BRI), or via a T1-style interface, called a primary rate interface (PRI). A ISDN line is comprised of multiple 64-Kbps B (bearer) channels and a single D (call setup and control) channel. A BRI

line has 2B+D, a PRI line, 23B+D. Each B channel can be individually accessed and controlled. In this paper we will concentrate on BRI ISDN. BRI lines are delivered in two forms, T (4-wire) or U (2-wire). Unless the installation is within 2000 wire feet of the central office, a U delivery form is used. Since almost all ISDN customer-premises equipment (CPE) is made to use a T interface, an NT1 must be used to provide the 2-wire to 4-wire conversion, isolation, and loop-back. The NT1 is necessary because the ISDN U interface can be as long as 18,000 wire feet (30,000 with a repeater) and the NT1 terminates and provides a standard interface for ISDN. Actually the NT1 has the capacity for some network administration, loopback testing, maintenance, and performance monitoring. From the customer's point of view, the common-carrier network boundary is the user side of the NT-1, the T reference point.

In the US, many of the trunks between telephone central offices are still configured to use in-band signalling these situations one bit out of eight is "robbed" from the bearer data stream and used for call control. With ISDN, however, all signalling is done out-of-band so the full 64 Kbps of the channel can be used for bearer data. Since not all facilities have been upgraded to support ISDN, many times an ISDN call will be sent across a trunk using in-band signalling. The call will not fail, but the sender must not use the eighth bit since it will be overwritten by the central office. All equipment sold in the US can meet this requirement through a scheme known as rate adaption which reduces the available bandwidth to 56 Kbps per B channel.

ISDN terminal equipment is often referred to as a "modem" although since the transmission is all-digital, there is no modulation/demodulation being performed. A more accurate term is ISDN terminal adapter. A terminal adapter typically has a basic rate ISDN interface and a serial port such as V.35 or RS-232. The terminal adapter places calls, handles necessary rate adaption and makes the B-channel bandwidth available on the serial port. The serial port may either be asynchronous (usually at speeds up to 19.2 Kbps) or synchronous (usually at speeds up to 128 Kbps).

3. ACCESS SCHEMES

There are many ways of using ISDN to provide remote access. One is to use an ISDN line and a terminal adapter as a direct replacement for an analog line and modem. This would increase the link bitrate to 128 Kbps, but few personal computers drive their serial port at 128 Kbps and most terminal software is not capable of taking advantage of the increased speed. Finally, few terminal adapters run at an asynchronous speed of more than 38.4 Kbps. A variation on this scheme is to use a terminal adapter and a asynchronous line protocol like ARAP, PPP, or asynchronous DECnet with the protocol stack running on the remote machine. However, this variation suffers from the same problem, lack of support on personal computers or terminal adapters for very high asynchronous speeds, as well as loading down the remote computer with packet serialization.

Another scheme is to place a multi-protocol router at each remote site and use a terminal adapter to connect the router's V.35 port to an ISDN line. The problem with the router scheme is that routers are expensive and would need to support a wide variety of protocols if the same type of router was used at every remote location. In addition, both a router and a terminal adapter would have to be purchased and managed for every location.

The scheme recommended in this paper is remote bridging using a stand-alone ethernet half-bridge with an integrated terminal adapter. With remote bridging (sometimes called half-bridging) two pieces of equipment act together to provide a transparent communications path for ethernet packets. In the case of ISDN remote bridging, the two bridges are connected via a dial-up ISDN circuit. Arriving packets at one bridge are checked to see if they should be forwarded. If so, they are wrapped in an HDLC frame and passed over an ISDN circuit to the other bridge which then unwraps the HDLC envelope and puts the packet on its ethernet. Compression may be used, in which case the packet is compressed before being encapsulated in an HDLC frame and uncompressed after being removed from the frame. Bridging has an advantage over routing since it is independent of higher-layer protocols such as IP or DECnet; it will transparently bridge any protocol that can be sent over ethernet. The disadvantage of bridging is that it may send more packets over a remote link. However, this problem can be mitigated by using a learning bridge and packet filtering.

Appendix 1 lists a number of manufacturers of ISDN remote bridges and the details their offerings. Currently, all vendors use proprietary or vendor-specific protocols for communication between bridges, thus no vendor will fully interoperate with another. National HEPnet Management has been using bridges from Combinet for the past two years and has built up a great deal of expertise with their product. In addition, Combinet is a market leader and the only vendor providing compression. Therefore, this proposal is centered around using the Combinet CB-400 bridge. However, evaluations of other products will continue and the approach is such that another vendors products could be substituted if it becomes appropriate. Since new products and features are being introduced at a dizzying rate, a full-scale evaluation would quickly be outdated even before it could be completed. It is the authors' opinion that further evaluation prior to the pilot project would be wasted.

3.1 Differences from Current Modem Access

ISDN remote bridging differs in several significant ways from the current terminal server access via a modem pool. Instead of communications via an asynchronous serial port (usually limited to around 50 Kbps), communications is via an ethernet interface (with a capability of 10 Mbps). This has several advantages. Since an ethernet interface uses direct memory access (DMA) instead of interrupting the processor every few bytes, the load on the remote machine is reduced and the ethernet interface can take advantage of the 300 Kbps possible with ISDN and compression.

Also, instead of using a terminal emulator, a protocol stack runs on the remote machine on top of which a full suite of applications can communicate concurrently. Thus a user may have several remote files open, be printing to a remote printer, and be reading mail simultaneously. Finally, the method of connection is different. Whereas a modem user must issue commands to the modem to dial manually or through a computer-based script, the ISDN bridge senses ethernet traffic at the remote site, dials the pre-assigned number, requests a call back, and starts transmitting packets when the link is established, all in a few seconds, and all without user intervention.

ISDN service also differs from traditional analog service. With ISDN, a single pair of wire can provide two channels and, although this paper suggests using them both for data, a user could have a data connection on one channel and a voice call on the other. ISDN service is also more expensive than a residential analog line. Since Ameritech has not filed for a residential ISDN tariff a remote user must install a business line at approximately four times the monthly cost of second residential line. The charge per call is the same for an analog residential line and an ISDN business line with one important difference, all calls are timed with the ISDN line. With residential service, calls within a few miles are not timed and only incur a flat \$0.50 charge.

3.2 Combinet Bridge Features

The Combinet CB-400 is a combined 2-channel terminal adapter and ethernet half-bridge with learning, often referred to as a remote bridge. In this paper we will refer to it simply as a bridge. It has the ability to dynamically establish B channel calls depending on traffic levels; it can be configured to establish the first B channel on a user-settable threshold (traffic over a Kbps for b seconds) and the second B channel on a different threshold (traffic over c Kbps for d seconds). The bridge can also be set to drop each B channel independently, again by setting separate thresholds for each channel. Adding and subtracting channels does not affect the bridging in any way. A queue of incoming packets is maintained in the bridge and the oldest packet is sent out on the next available channel. Incoming packets can be filtered based on their ethertype and either thrown away, ignored in traffic calculations but sent, or counted and sent. The bridges have the ability to compress each packet before it is sent and de-compress it when it arrives at the other bridge without increasing delay.

A bridge can either call another bridge directly and begin passing packets, or request a call back. If a call back is requested, both the calling and called bridge hang up, and the called bridge calls back the caller on either one or both B channels, then packets begin to flow. The call back bridge can be programmed with a set of known phone numbers and set not to call any number not in the list. Packets can be checked against a table of ethernet addresses and only passed if recognized. Also, before a connection is established, the caller-ID and the offered password of the calling bridge can be checked and the call rejected if either is not recognized.

The Combinet bridge can be configured either through an asynchronous RS-232 serial port or by an IP connection from another bridge. Through either mechanism, the user is presented with a command-line interface. Serial port control requires a terminal or machine running a terminal emulator to connect at 9.6 Kbps. Bridge-to-bridge control requires a serial port connection to one bridge, which can then provide a connection to the command-line interface of any other bridge. The bridge-to-bridge protocol uses IP (thus every bridge must have an IP address) but is non-standard. Appendix 2 gives the bridge command set.

In addition to the RS-232 connection, the bridge has both a 10BASE-2 (thin net) and 10BASE-T (twisted pair) for ethernet connections, an RJ-45 connector for connections to an ISDN BRI line at the S/T reference point, and a power cord connector. The front panel has indicator LEDs for monitoring LAN traffic, traffic being bridged onto B1 and B2, power, and ISDN line status.

4. ARCHITECTURE

Figure 1 shows the architecture of the ISDN remote access network. In some ways it resembles Fermilab's present modem pool arrangement, with ISDN bridges replacing the modems and the absence of a terminal server. However, this architecture has other differences. The most significant is that instead of terminal access, a Fermilab local area network segment is extended via the ISDN bridges to the remote location. Thus a computer at a remote location is attached to the LAN just as a computer physically located at Fermilab would be. The remote computer will have an ethernet card or adapter and thus an ethernet address, as well as an Appletalk, IP, or DECnet address depending on the protocol stack the remote computer is running.

A pool of ISDN bridges (or more precisely, ISDN half-bridges) are attached to one or more ethernet segments dedicated to ISDN remote access. If more than one remote access segment is needed, a number of segments will be bridged together to form one logical segment. As is the case with the Fermilab modem pool, a single number hunt group is provided by the Fermilab centrex that will choose a non-busy bridge to answer an incoming call. A connection manager is attached to these ethernet segments. It works with the bridges to control access and to monitor operations. It communicates primarily over the ethernet using IP packets, but in the event of a failure of the IP communications path, it can communicate through a serial connection to one or more of the hub bridges. Although Figure 1 shows serial connections going to bridges in one segment, connections to at least one bridge in each segment may be added for added redundancy.

At the remote site, the user's computer is connected to a small ethernet segment with at least two attached devices, the computer and an ISDN bridge. The bridge is, in turn, connected to a NT-1 device which provides a connection to the ISDN network. A link is established by the remote bridge calling the hub number and requesting a call-back from the bridge that answers. When the call-back is complete, packets begin to flow.

4.1 Specific Protocol Considerations

There has been some concern that bridging, rather than routing, will be used to connect remote users. If pure bridging were used, all traffic from one remote user would be bridged to all remote users. Fortunately, the Combinet bridges use learning. It learns what side of the bridge devices are on, and does not forward packets to a remote ethernet when it knows that the device is local. Learning is performed by examining all ethernet packets on the segment and remembering the source addresses of each.

A level 3 router isolates the remote access segment from the rest of the Fermilab network. The router can be used to quickly shut off remote access if needed, and also keeps traffic on the remote access segments to a minimum by filtering out all non-local broadcasts. This router will filter traffic and only allow DECnet Phase IV, Appletalk, and TCP/IP traffic to pass, if it is routed to the remote access segment.

The segment will have a unique IP subnet address. All remote devices with an IP address will be statically listed in the router's address resolution protocol (ARP) tables so that there will be no ARP

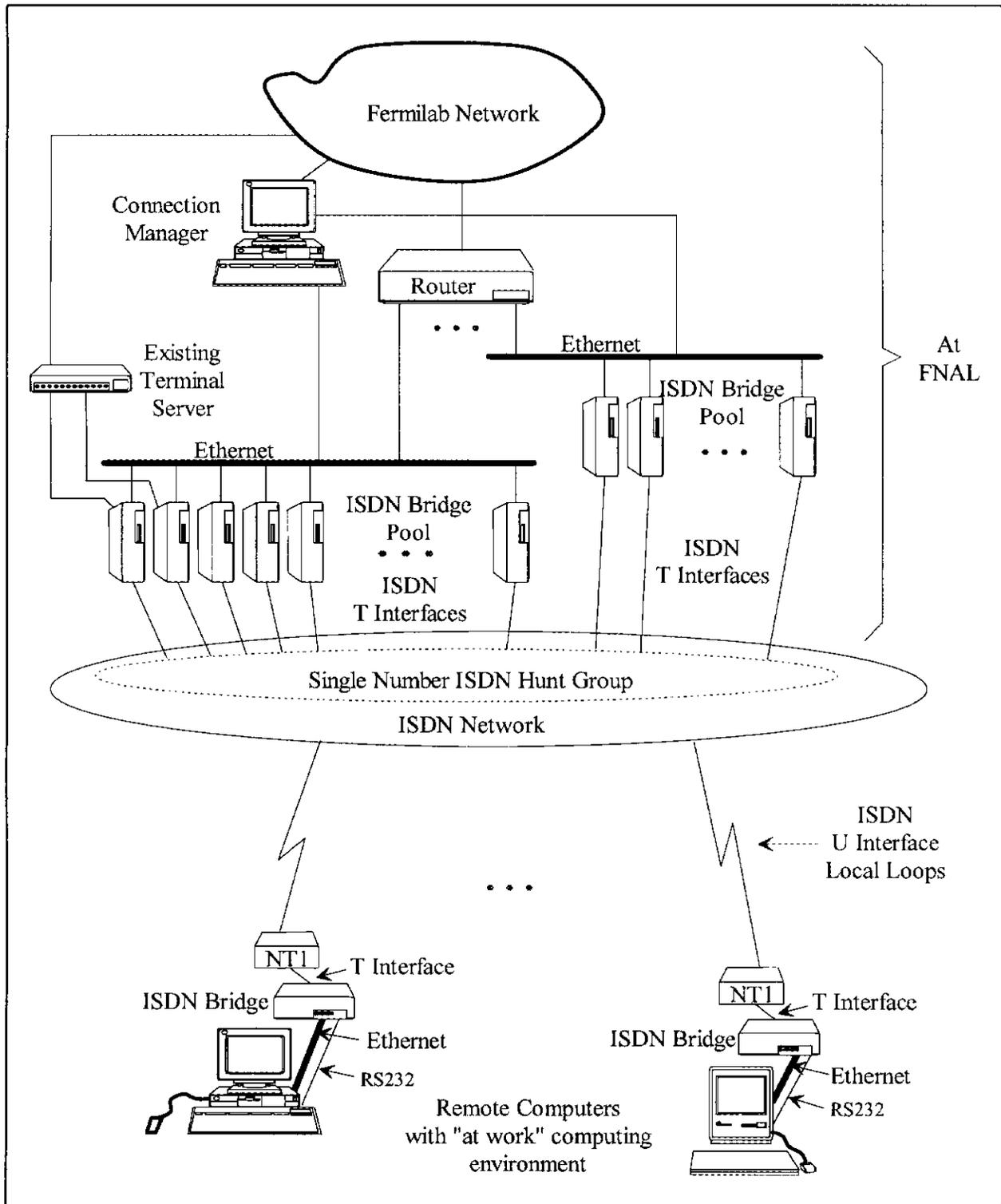


Figure 1. Remote Access Architecture

broadcast traffic from the router. The router will be set as the default router for all remote IP devices and an 8-bit subnet mask will be used. All remote devices will be assigned a permanent IP address and IP hostname in the fnal.gov domain. The fnal.gov Internet nameservers, fnserv1 and fnserv2 will have all hostnames registered and provide name resolution service to remote devices. Remote users may want to populate the ARP table of their machine with the router's ethernet address to avoid unnecessary ARP broadcasts.

The remote access segment will also have a unique Appletalk zone assigned. Since the router will perform Appletalk routing, it should help keep broadcasts to a minimum. The only significant amount of Appletalk broadcast traffic will be when a new Appletalk node connects and negotiates its address.

All remote DECnet nodes will be assigned a node number in a hidden area. The router will filter traffic so that only packets bound for a remote device will be put on the remote access segment for bridging to that device. All remote DECnet nodes will send periodic end-node HELLOs which the router will pick up and use to determine routing.

4.2 Security

The Combinet bridge provides several kinds of security. Currently, the following characteristics of the calling site are checked against lists internal to the bridge:

- Ethernet address of the remote node
- Caller-ID or call-back number of calling bridge
- Password.

Thus, in order to gain access to the Fermilab LAN, a remote bridge must be configured with the correct password, and the hub bridge must be configured to know the ethernet address of the remote machine, the phone number of the calling bridge, and the call-back number of the calling bridge. (The phone number and call-back number of the bridge will usually be the same). If a remote bridge meets all the requirements except for correct ethernet address, the call will stay up but no traffic will be passed. Note that this is a higher level of security that the Fermilab modem pool provides since only callback is supported and each transmitted packet is checked.

5. EQUIPMENT AND SERVICES REQUIRED

This section details the equipment and ISDN services required to extend the Fermilab LAN to a remote site. It is assumed that a suitably powerful personal computer, workstation, or X terminal is already available at the remote site and that the machine has an ethernet interface. The equipment and services are subdivided into that needed at the remote site, and that needed at the hub site.

5.1 ISDN Service at Remote Sites

A single basic rate ISDN line should be ordered for each remote site. The ISDN line should be configured as follows:

- Circuit-switched data on B1 and B2
- Default inter-exchange carrier (IXC) set to AT&T
- Terminal Type C
- National ISDN-1 (NI-1) signalling (if available, otherwise AT&T or Northern Telecom custom, whichever is available)
- 2B1Q signalling
- Caller-ID delivery via an information element (IE)
- Delivery via a U interface
- Two directory numbers (DNs)
- Two service profile identifiers (SPIDs) (one for each DN)
- Point-to-point service
- Connected via an RJ-45 jack

Ameritech is the local-exchange carrier (LEC) providing residential service to most Fermilab personnel. Ameritech has established a special office to handle question about BRI installations which may be reached at 1-800-TEAM-DATA. Ameritech has been very aggressive recently in deploying BRI lines and, in fact, almost everyone can get ISDN service if they live in the Chicago area and are served by Ameritech. Team Data can consult a database to determine if a particular site can get BRI service. In some cases they may have to do a loop qualification that involves doing a line-loss measurement on an existing line to the remote site. Table 1 specifies what should be ordered and the current costs. A typical installation will cost \$164.50 if no premises wiring is required.

Description	Price
Order Charge	\$64.00
Line Connect Charge	\$20.50
2 Wire Interface	\$50.00
B1 Data Channel Activation	\$15.00
B2 Data Channel Activation	\$15.00
Premise Visit (if necessary)	\$35.00 + \$15.00 add'l per 1/4 hour

Table 1: Installation Charges

Table 2 lists the monthly charges for BRI service. The line extender will be needed only in installations where the site is more than 18,000 wire feet from the central office. A line extender allows

the remote site to be 30,000 wire feet from the central office. Currently, Ameritech does not allow more than one repeater to be used on a line, so those over 30,000 wire feet cannot get ISDN service. For a typical suburban Chicago site, BRI service will cost \$41.33 per month.

Description	Price	Note
Base Basic Rate ISDN Service	\$14.65, \$18.49 or \$22.02	depending on location
Circuit Switched Data (CSD) Service on B1	\$8.00	
Circuit Switched Data (CSD) Service on B2	\$8.00	
Common Line Charge	\$3.31	
Line Extender	\$22.50	may not be needed

Table 2: Fixed Monthly Charges

In addition to the fixed monthly charges, usage charges will apply for all calls placed. Table 3 shows the amount Ameritech charges for the different mileage bands in the Chicago area. The charges are exactly the same as for business analog voice calls. Note that residential voice call differ in that 0-8 mile calls are not timed. Since a call-back scheme will be used, there will be only one minute of usage charged to the remote site for each session. The total usage charges at the remote site are expected to be less than \$2.00 per month. Section 5.3 discusses usage costs at the hub site.

Centel and Contel also provide local-exchange carrier service in the Chicago area. Both offer BRI, but a detailed cost review was not performed for this paper. The costs are rumored to be in the same range as Ameritech.

5.2 Equipment at Remote Site

The remote site needs the communications equipment listed in Table 4. Prices reflect the Fermilab discount for a single unit, but significantly higher discounts will apply for bulk orders. The NT1 provides a 2-wire (U interface) to 4-wire (T interface) conversion and also loopback for testing. The Combinet bridge provides an integrated terminal adapter and ethernet half-bridge.

At the remote site, each machine to be connected must have an ethernet interface and the appropriate LAN communications software. A workstation or X terminal typically already has all the necessary interface hardware and software, although in the case of a workstation, the user may want to add some network-aware applications such as POPmail or a netnews reader.

For a standard Macintosh, the user must add an ethernet card and EtherTalk software, or connect an SCSI-to-Ethertalk converter (such as the one made by Asante). In addition, the user may add one or more of the following:

- MacTCP or NCSA Telnet for TCP/IP connectivity

Miles	Duration of Call	Price Per Minute		
		Mon-Fri 9AM-11AM, 2PM-8PM	Mon-Fri 8AM-9AM, 11AM-2PM, 8PM-9PM	Mon-Fri 9PM-8AM, All Hours Sat-Sun, Holidays
0 - 8	First Minute	3.9¢	3.5¢	2.3¢
	Each Additional Minute	1.0¢	0.9¢	0.6¢
8 - 15	First Minute	8.0¢	7.2¢	4.8¢
	Each Additional Minute	2.3¢	2.1¢	1.4¢
15-40	First Minute	10.4¢	9.4¢	6.2¢
	Each Additional Minute	3.4¢	3.1¢	2.0¢
40+	First Minute	16.3¢	14.7¢	9.8¢
	Each Additional Minute	6.5¢	5.9¢	3.9¢

Table 3: Circuit-Switched Data Usage Pricing

Description	Price
Northern Telecom 2B1Q NT-1	\$136.85
Northern Telecom NT-1 Power Supply	\$44.20
Combinet CB-400 Bridge	\$1642.50
Ethernet Cable, T, and Terminating Resistors	\$10.00

Table 4: Equipment at Remote Site

- Pathworks for DECnet connectivity
- NFSshare for mounting NFS volumes
- MacX for displaying X-window applications
- A variety of network-aware applications such as QuickMail, POPmail, and Eudora

For a standard IBM PC compatible, the user must add an ethernet card or ethernet adapter and appropriate communications software such as:

- FTP Software's PC-TCP (for MS-Windows or DOS)
- Netmanage's Chameleon or ChameleonNFS (both for MS-Windows)
- NCSA Telnet (for DOS)
- DEC Pathworks (for MS-Windows or DOS)

These PC packages typically come with a suite of applications such as electronic mail, FTP clients and server, and often even NFS clients and servers. Still the user may wish to add such applications as an X server from Hummingbird or NCD.

5.3 ISDN Service at the Hub Site

The hub site will have a number of ISDN BRI lines provided through the Fermilab centrex. It may seem more reasonable to install a single PRI line instead of multiple BRI lines but there are several advantages to using multiple BRI lines. First, B channels are significantly cheaper when delivered via BRI; Ameritech charges about \$300 per month for 12 BRI lines (24 B channels, \$12.50 per channel per month), and \$1500 per month for a single PRI line (23 B channels, \$65 per channel per month). Second, almost no remote access equipment exists that uses PRI lines. Combinet offers no PRI equipment and only provides limited interoperability with Network Express' PRI equipment. Finally, a PRI line gives one single point of failure while multiple BRI lines provide redundancy.

ISDN lines should be configured as specified in Section 5.1. Since the Fermilab centrex supports NI-1, all lines should be configured with NI-1 signalling. In addition, lines should be configured to support circuit-switched voice on B1 so that voice CPE can be used to verify line operations.

The BRI lines will be arranged in a hunt group with hunting on the first B channel on each BRI only. This will keep two calls from arriving at the same bridge, one on each channel. The second channel will only be used for outbound calling.

All ISDN lines will be ordered through the Fermilab Telecommunications Group in the Business Services section. The cost of installing, maintaining, and usage of the ISDN lines will be absorbed into the Fermilab telecommunications overhead, just as is the case with the current dial-back modem pool. BRI lines cost approximately \$50 to install and \$25 per month. CSD calls off site are charged at the rate shown in Table 3 less a 50% discount. At some time in the future, Fermilab telecom may begin a charge-back system for telecommunications services.

5.4 Equipment at the Hub Site

The hub site must have a sufficient number of Combinet bridges to satisfy peak demand. The exact number required will be determined through the pilot project. If the location of the hub is in Wilson Hall, all of the ISDN lines can be supplied with a T interface, thus eliminating the need for NT-1s. Otherwise, each Combinet bridge will require an NT1. In addition, an ethernet segment must be dedicated to the ISDN bridges and a port on an existing router or a separate router must be supplied. A Cisco IGS/L router would be sufficient at a cost of approximately \$3,100. To provide back-up to the IP control of the ISDN bridges, an RS-232 connection (possibly through a terminal server) should be provided to one or two bridges. In addition, a workstation will be needed to act as the control system for the hub ISDN bridges. Table 5 summarizes the equipment needed.

Description	Price	Note
Combinet CB-400 Bridge	\$1642.50	each
Northern Telecom 2B1Q NT-1	\$136.85	for each bridge (may not be needed)
Northern Telecom Power Supply for NT-1	\$44.20	for each NT-1 (needed only if NT-1s are used)
Cisco IGS/L Router	\$3,100.00	may use port on existing router
Workstation	\$6,000	may use existing system
Terminal Server	\$1,000	may use existing system

Table 5: Hub Site Equipment

6. PILOT PROJECT

To gain experience, it is useful to run a pilot system for several months. A pilot project, if carefully monitored, can turn up problems that can be corrected before they would affect a larger community. The pilot project is intended to function as a miniature production system, and therefore will be reliable and stable. Any gross experimentation will be performed on the existing NHM experimental system that will continue to operate in parallel with the pilot project. Users will be carefully monitored and asked to provide detailed feedback on experiences with software and hardware used.

Figure 2 shows the architecture of the pilot project. At the hub site, eight Combinet bridges will be connected to a dedicated LAN segment. Twelve remote sites (initially) will have identical Combinet bridges, giving a concentration of 1 hub bridge for every 1.5 remote sites. This may seem conservative, but pilot project users are expected to use the service heavily. 1.5 is established as an initial concentration until experience can be gained. There is nothing in the architecture that limits the number of remote bridges; add more remote bridges and the concentration increases.

The hub bridges will each have an individual phone number, but a hunt group with one well-known number will be established so that a remote bridge will call one number and be connected to the next available bridge. This service will be provided by the Fermilab centrex. Hunting will be sequential; that is, bridges will be checked in a pre-determined order and the first non-busy line will get the call. When a bridge is taken out of service, it will be disconnected from the phone line. The switch will see that no CPE is available to answer the call and mark the line as unavailable to the hunt group. Note that the hunt group will be set up so that hunting is always on B1 of each BRI line and that the line will be seen as busy even though B2 may not be in use. Additions or deletions of lines in the hunt group will require switch maintenance requests to the Fermilab telecom department.

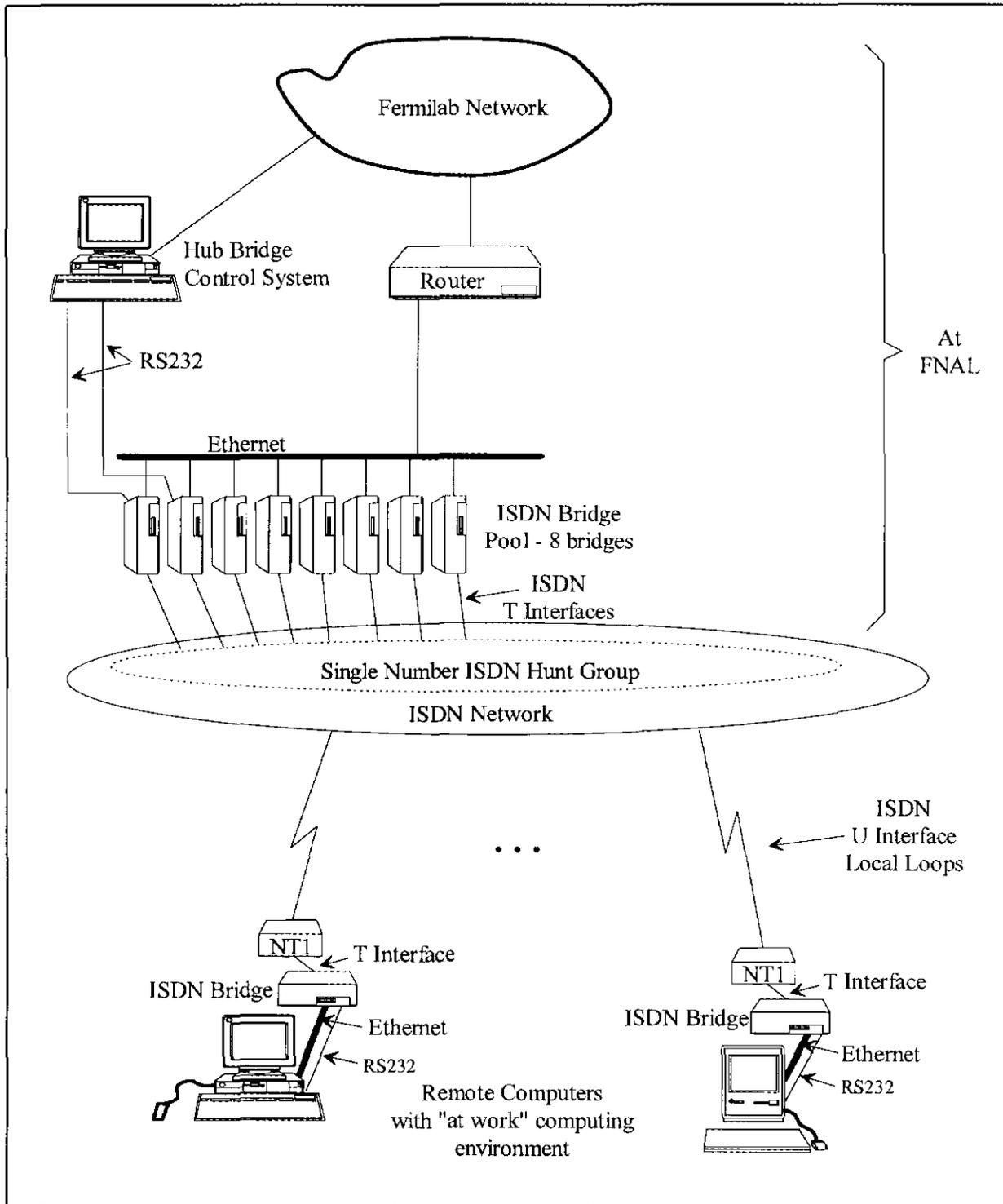


Figure 2. Pilot Project Architecture

6.1 Establishing and Breaking Remote Connections

The scenario for connecting a remote machine is as follows.

1. The remote user powers on the Combinet bridge.
2. The remote user powers on his computer and brings up the operating environment.
3. The computer makes a network query.
4. The remote bridge senses packets to be bridged and makes a call on the first B channel to the hub number.
5. The Fermilab centrex chooses the next non-busy line from the hunt group and passes the call to that line.
6. The hub bridge on the chosen line answers the call.
7. The remote bridge sends the hub password and its call-back number.
8. The remote bridge and hub bridge both drop the call.
9. The hub bridge checks the password and call-back number against its tables and ignores the request if either are invalid, otherwise;
10. The hub bridge calls back the remote bridge on either one or both B channel (see below).
11. The hub sends the remote password.
12. The remote bridge checks the password and caller-ID (if available) against its tables and drops the call if either is invalid, otherwise;
13. Packets begin to flow. All packets are checked for an acceptable ethernet address before they are put on the Fermilab LAN.

Disconnect of B1 can happen in three ways. The hub bridge will be set so that after certain time with no non-broadcast traffic being bridged, the call will be dropped. The timeout will be set to the same value as the Fermilab modem pool uses. However, most of the time the user will disconnect by either powering off the remote bridge or by sending a disconnect command via the remote bridge's serial interface.

The connection on B2 will be used as traffic demands. The hub bridge be set up to call back the remote bridge on either one B channel or both. When a traffic level over a high-water mark (specified as traffic over x Kbps for y seconds) is detected by the hub bridge and the second channel is not in use, it calls the remote bridge on the second B channel. When traffic drops below a low-water mark (specified as traffic under a Kbps for b seconds) the second B channel is dropped. The dynamic bandwidth allocation should be transparent to the user except for bitrate differences. B1 will never be dropped until disconnected by the remote user, except for the inactivity timeout described above.

6.2 Security

Security on the hub bridges will be maintained through three different mechanisms. First, remote bridges that call in must supply the correct hub password (common to all hub bridges) before a

callback can occur. Second, each hub bridge will have an list of valid remote bridge phone numbers and will only call back a number that is in the callback list. (For the trial, only numbers in the same area as supported by the Fermilab dial-back modem pool will be called.) Third, all hub bridges will have a list of ethernet addresses for all devices at all remote sites and packets from unrecognized ethernet devices will be dropped.

Security on the remote bridge will use one or two security methods. First, when a hub bridge calls back a remote bridge, the hub bridge must supply the correct remote password (common to all remote bridges). Second, where Caller-ID is available, the remote bridge will have a list of hub bridge ISDN numbers and not accept calls from any other number. This level of security is less than that of the central site since few remote machines will offer any network services that would be of interest to a malicious user.

In addition, both the hub bridges and remote bridges will benefit from "security by obscurity," since neither the hub bridge numbers, the remote bridge numbers, nor any passwords will be made publicly available. Also, there are probably few hackers with Combinet bridges and ISDN lines.

6.3 Hub Bridge Control System

A workstation will be used as the control system. It will talk to the bridges through an applications-level protocol unique to Combinet running over UDP/IP. As a backup connection, the workstation will connect to the serial ports of two of the bridges through a terminal server. Either of these bridges may be used to talk to the others.

The control system will keep complete call information: who called, when, and the duration of each call. This information will be made available in real-time and stored for analysis. In addition, the control system will allow bridge characteristics to be set on a per-user basis. That is, when a user calls in, the control system will download to the hub bridge the appropriate profile. The profile will contain the following information:

- Ethernet addresses of all remote devices
- Remote telephone number
- Number of channels allowed (1 or 2)
- Bitrate supported (56 or 64 Kbps)
- High-water mark for each channel
- Low-water mark for B2
- What ethernet types should be bridged or, alternatively, what types should be blocked

6.4 Remote Bridge Configuration

A remote bridge may be configured by establishing an ISDN connection to it and then sending commands over UDP/IP. However, it is expected that the remote users will power off the remote

bridge when it is not in use. Therefore, remote configuration via ISDN will be used only for small changes during discussions with the user. Instead, the remote bridges will be configured via its serial port. The remote user will be given a text file that will configure the bridge appropriately. This file will be downloaded to the bridge through a serial connection from the remote computer. X terminals are a special case and the bridge that connects them must be brought into the central site for downloading. An alternate approach is for users to bring the bridge back to the central site for configuration changes. A hybrid of the two approaches will be used.

The following parameters will need to be set for each remote bridge. (See Appendix 1 for details.)

- Set Service Profile ID (SPID) for each B channel
- Set number for each B channel (should be the same)
- Set number for hub bridge to dial to reach this remote bridge
- Set number to call to reach hub hunt group
- Enable demand dialing on B1
- Disable demand dialing on B2
- Set high-water mark on B1 for 1 Kbps (dial as soon as first packet arrives)
- Disable automatic tear-down
- Set host password (hub bridge must give this password before connection is allowed)
- Set remote password (remote bridge must give this password before connection is allowed)

Since some parameter changes could result in a remote user being unable to establish or maintain a connection, significant changes will be made concurrently on the hub bridges and remote bridges. Such changes will be widely publicized and care will be taken to ensure that every user has the proper configuration before any changes are made.

6.5 Questions to be Answered by Pilot Project

It is hoped the following questions will be answered by the pilot project.

- What percentage of the time do users need two B channels?
- What specific configuration parameters must be set on the remote machine's TCP/IP configurations?
- What is the appropriate ratio of hub bridges to a remote sites?
- How do typical applications perform over the ISDN bridges?
- Does dynamic allocation of the second B channel provide for fast enough response?
- What overall compression ratio is achieved?
- Does remote configuration of remote bridges work better than having the user download a configuration over the serial port?
- Should the initial callback be done with one or two B channels?
- What communications packages on each platform are best?

- Do users feel the cost of the system is justified?
- Does the security system satisfy all DOE requirements?
- What level of performance is required for the remote computer?

6.6 Pilot Project Candidates

The pilot project is intended as a miniature production system. The representation of users from different areas and with different skill levels is encouraged, although all should have high bandwidth requirements. The only caveat is that the candidates be “friendly” users, tolerant of occasional failures and lack of detailed documentation. It is hoped that a wide variety of computing platforms, protocols, and communications programs will be represented in the pilot project. Some systems of special interest are:

- Macintosh running System 7, MacTCP, and MacX (included in Pathworks package)
- Macintosh running System 7 and DECnet Pathworks
- Macintosh running System7 and Appletalk
- Macintosh running System 7 and Ethertalk
- IBM PC-compatible running MS-DOS, MS-Windows, ChameleonNFS and PC-Xview
- IBM PC-compatible running MS-DOS, DECnet Pathworks and X-windows
- IBM PC-compatible running MS-DOS and PC-TCP
- IBM PC-compatible running MS-Windows NT
- VAXstation running VMS and DECwindows
- SparcStation running Solaris and OpenLook
- X terminal running X windows

Each machine at a remote site must be configured and “tuned” for optimum network performance. IP, DECnet, and Appletalk should each be represented by at least one machine in the pilot project. In addition, the pilot project users will be encourage to try a variety of network protocols and applications packages and report their experiences.

6.7 Pilot Project Cost

The pilot project’s costs can be broken into two areas, remote site costs and hub sites costs. Each remote site will require a fairly powerful computer or X terminal with an ethernet interface and communications software, an NT-1, an basic rate ISDN line, a Combinet bridge, and ethernet thin-wire cabling. Adding these costs as detailed in Section 5.1 and Section 5.2 produces a cost of \$2000 initially and then \$45 monthly. This assumes:

- A suburban Chicago location
- No inside wiring by Ameritech needed
- No line extender required
- A computer or terminal with an ethernet interface and communications software is available

For the hub site, it is expected that an existing workstation, Cisco router port, and terminal server can be used in the pilot project. Since the ISDN lines and usage charges will be absorbed as part of the Fermilab telecommunications overhead, the only actual outlay of funds will be for the Combinet bridges at \$1642.50 each, assuming that NT-1s are not needed.

For a pilot project consisting of 12 remote sites and a concentration of 1.5 remote sites for each hub bridge, the cost will be:

- \$13,140 for hub bridges
- \$23,330 for remote bridges and NT-1s
- \$1,975 for remote ISDN line installation
- \$540 per month for remote ISDN service

Thus, the total cost of the pilot project will be approximately \$38,500 plus \$540 monthly. However, this cost may be substantially reduced by negotiating volume discounts with vendors.

7. SUMMARY

Because of (1) advances in technology that now allow s remote computing environment similar to that at Fermilab, (2) wide deployment of basic rate ISDN, (3) state and federal environmental legislation, (4) the experiences of NHM with ISDN, and (5) the cost benefit of supporting high-bandwidth remote access, the authors recommend that Fermilab launch a this pilot project.

APPENDIX I. ISDN BRIDGE PROVIDERS

This section is intended to provide a comparison of the various ISDN bridges available in the market. All of the following manufacturers make an ethernet half bridge with an integrated ISDN terminal adapter.

Combinet
Sunnyvale, CA
(408) 522-9020
FAX: (408) 732-5479

Develcon Electronics
Atlanta, GA
(800) 667-9333
FAX: (306) 931-1370

DigiBoard
Eden Prairie, MN
(612) 943-9020
FAX: (612) 943-5398

Network Express
Ann Arbor, MI
(313) 761-5005
FAX: (313) 995-1114

Teleos Communications makes an IBM-compatible PC card that bridges IP only and a hub systems that the cards may dial into. It is included here although it is not a general-purpose bridge. The question marks in the table represent the lack of response from the Teleos, despite repeated requests for details. Gandalf Premier makes a stand-alone bridge that is designed to be hooked to an external terminal adapter. The Gandalf product is included in this comparison as well.

Teleos Communications
Eatontown, NJ
(908) 389-5700
FAX: (908) 544-9890

Gandalf Premier
Schaumburg, IL
(708) 517-6300
FAX: (708) 517-3627

Table A1 shows a comparison of the following features.

Configuration. Is the bridge a stand-alone device, an AT-bus card, or an integrated PC unit?

Integrated Power Supply. Does the bridge have an internal electrical adapter?

Call-Back. Can the bridge be set up to call back a bridge that calls it?

Number of B Channels Supported. What is the maximum number of B channels the bridge can utilize?

Rate Adaption to 56 Kbps. Can the bridge use rate adaption to allow communications across trunks with in-band signalling (“bit robbing”).

Independent Use of B Channels. Can the bridge be connected to a different site with each B channel?

ISDN Forms Supported. Does the bridge support AT&T Custom (AT&T), Northern Telecom Custom (NT), Nippon Telephone and Telegraph (NTT), and/or US National ISDN 1 (NI-1)?

Compression. Does the bridge provide compression of frames before they are sent across the ISDN line?

Password Protection. Can the bridge be configured to require a password before allowing a connection?

Caller-ID Check. Can the bridge be configured to check the inbound caller-ID against a list before allowing a connection, and refuse the connection if the number is not recognized?

Connection Manager Available. Is there a manager that treats a number of bridges as a pool to allocate?

Number of Profiles. How many distinct configurations of number of channels, phone number, filtering, etc. can be set? Profiles may be retrieved based on destination address of packet to be bridged.

Management Scheme. How is the bridge managed? Via the simple network management protocol (SNMP), a RS-232 serial connection, through an integrated management console, through a front-panel control, through a proprietary protocol on top of IP?

Protocols Routed/Bridged. What protocols are routed? What protocols are bridged?

Demand Dialing. Can the bridge be configured to dial a remote site when a packet needs to be bridged?

Dynamic B Channel Usage. Can the bridge be configured to dynamically add and subtract B channels as traffic warrants?

Ethernet Type Supported. What type of ethernet interface; 10BaseT (twisted pair), 10Base2 (Thin-wire), 10Base5 (Thickwire); are supplied?

Filtering. Can packets be blocked from bridging based on their ethertype or other criterion?

Dial on Power Up. Can the bridge be configured to dial a preset number on power up?

List Price. What is the list price for one unit? Note that Fermilab usually gets a 20-30% discount off of list.

Feature	Combinet			Develcon
	CL-200	CB-200	CB-400	Model 150
Configuration	Stand-Alone	Stand-Alone	Stand-Alone	Stand-Alone
Integrated Power Supply	N	N	Y	N
Call-Back	Y	Y	Y	N
Number of B channels supported	2	2	2	2
Rate Adaption to 56 Kbps	Y	Y	Y	Y
Independent Use of B Channels	N	N	N	N
ISDN Forms Supported	AT&T, NT, NTT, NI-1	AT&T, NT, NTT, NI-1	AT&T, NT, NTT, NI-1	AT&T, NT
Compression	N	Y	Y	N
Password Protection	Y	Y	Y	N
Caller-ID Check	Y	Y	Y	N
Connection Manager Available	N	N	N	N
Number of Profiles	1	1	1	2
Management Scheme	Serial, Prop. IP	Serial, Prop. IP	Serial, Prop. IP	Front Panel, Serial, SNMP
Protocols Routed/Bridged	None/All	None/All	None/All	None/All
Demand Dialing	Y	Y	Y	Y
Dynamic B channel Usage	Y	Y	Y	Y
Time-of-Day Connect	N	N	N	Y
Ethernet Type Supported	Thinnet	10BaseT, Thinnet	10BaseT, Thinnet	Thinnet
Filtering	Y	Y	Y	Y
Spanning Tree	Y	Y	Y	Y
Dial on Power Up	N	N	N	Y
List Price (US \$)	\$1,690	2,190	2,190	2,695

Table A1: ISDN Bridge Feature Comparison

Features	Digiboard			
	IMAC	Dual IMAC	PC IMAC	PC IMAC 4
Configuration	Stand-Alone	Stand-Alone	PC Card	PC Card
Integrated Power Supply	N	N	PC Bus	PC Bus
Call-Back	N	N	N	N
Number of B channels supported	2	4	2	8
Rate Adaption to 56 Kbps	Y	Y	Y	Y
Independent Use of B Channels	Y	Y	Y	Y
ISDN Forms Supported	AT&T, NT, NI-1	AT&T, NT, NI-1	AT&T, NT, NI-1	AT&T, NT, NI-1
Compression	Y	Y	Y	Y
Password Protection	Y	Y	Y	Y
Caller-ID Check	Y	Y	Y	Y
Connection Manager Available	N	N	Y	Y
Number of Profiles	15	15	unlimited	unlimited
Management Scheme	Serial Port, SNMP	Serial Port, SNMP	PC Bus, SNMP	PC Bus, SNMP
Protocols Routed/Bridged	None/All	None/All	Software Dependent/ All Other	Software Dependent/ All Other
Demand Dialing	Y	Y	Y	Y
Dynamic B Channel Usage	N	N	N	N
Time-of-Day Connection	N	N	N	N
Ethernet Interface	Thinnet	Thinnet	PC Bus	PC Bus
Filtering	Y	Y	Y	Y
Spanning Tree	N	N	N	N
Dial on Power Up	Y	Y	Y	Y
List Price (US \$)	2,195	2,795	995	3,995

Table A1: ISDN Bridge Feature Comparison (Continued)

Features	Gandalf	Network Express	Teleos	
	5220	InterHub	Commuter Card	Commuter Hub
Configuration	Stand-Alone	PC	PC Card	PC
Integrated Power Supply	Y	Y	PC Bus	Y
Call-Back	N	N	N	N
Number of B channels supported		4 to 32	2	23
Rate Adaption to 56 Kbps	N/A	Y	Y	Y
Independent Use of B Channels	Y	Y	N	Y
ISDN Forms Supported	N/A	AT&T, NT, NTT	?	?
Compression	Y	N	N	N
Password Protection	Y	N	?	?
Caller-ID Check	N	N	?	?
Connection Manager Available	N	N	N	Y
Number of Profiles	15	none	1	none
Management Scheme	Serial Port, Telnet	Serial, SNMP	PC Bus	Internal, Serial
Protocols Routed/Bridged	IP/All Else	IP/All Other	IP/none	IP/none
Demand Dialing	Y	N	Y	Y
Dynamic B Channel Usage	N	Y	N	N
Time-of-Day Connection	Y	N	N	N
Ethernet Interface	User-Supplied MAU	User-Supplied MAU	PC Bus	N/A
Filtering	Y	Y	N	Y
Spanning Tree	Y	Y	N	N
Dial on Power Up	Y	N	Y	N
List Price (US \$)	2,995 plus TA	8,000+	?	?

Table A1: ISDN Bridge Feature Comparison (Continued)

APPENDIX 2. COMBINET BRIDGE COMMANDS

The following is the Combinet CB-200/400 command set. Only the uppercase letters need to be typed at the command prompt.

- `DEmand <port> [THreshold = <Kbps>] [DUration = <seconds> [SOURCE = ISDN | LAN | BOTH]`
Make a call on <port> when the traffic from the local LAN, the remote LAN, or both exceeds <Kbps> for <seconds>.
- `LOG None | CALLs | COUNT`
Log nothing, all calls, or all calls and a running packet count.
- `SEt Address = <address> ACcept | BLock`
Enter <address> in the address table as either ACCEPT or BLOCK.
- `SEt AGE = OFF | <seconds>`
Either never automatically remove ethernet addresses from the address table, or remove them after they have not been seen for <seconds>.
- `SEt [<port>] AUTO = ON | OFF`
Enable or disable automatic calling on <port> when conditions set by DEMAND statement are met.
- `SEt CALLBACK = ON | OFF | BOTH`
Allow connections where this bridge calls the other back, where this bridge is called, or both.
- `SEt INTerval = OFF | <seconds>`
Send test packet every <seconds> to test integrity of link. If test packet fails, drop link and re-establish.
- `SEt IPaddress XXX.XXX.XXX.XXX`
Set the IP address of the bridge to XXX.XXX.XXX.XXX
- `SEt SUBnetmask XXX.XXX.XXX.XXX`
Set the IP subnet mask the bridge to XXX.XXX.XXX.XXX.
- `SEt GAteway XXX.XXX.XXX.XXX`
Sets the gateway the bridge will use to communicate with devices not on the same IP subnet to XXX.XXX.XXX.XXX.
- `SEt <port> DELay = <seconds>`
Wait <seconds> before retrying failed call on <port>.
- `SEt DEFaults`
Return to factory set defaults.
- `SEt ECho = ON | OFF`
Controls whether characters sent to the interface will be echoed.
- `SEt LEarn = ON | OFF`
When ON, the bridge will learn ethernet addresses that it sees on the ethernet or from incoming (from the ISDN line) bridged traffic. When OFF, the bridge will learn only from incoming bridged traffic.

- SET MODe = SIngle | ONly | ANy
When MODe=ANy all packets entered in the address table as BLOCKED will be forwarded. When MODe=ONly, only addresses marked as ACCEPT in the address table (in addition to broadcast packets) will be forwarded. When MODe=SIngle, only a single address will be marked as ACCEPT in the table.
- SET [<port>] NUmber = NUmber
Number or remote bridge to call to connect <port>.
- SET PRoTocol = HDLc | ORdered | COmpressed
Forward packets using HDLC, HDLC while maintaining packet order, or HDLC with Stacker compression.
- SET PASSword [HOst]
When HOst is specified, the interface prompts for the host password--the password that is sent when connecting to a remote bridge. When HOst is not specified, the interface prompts for an acceptable password from remote bridges. There can be multiple remote passwords.
- SET [<port>] DIrectoryNumber = [<number>]
Specify number of <port> (7 digits in US).
- SET [<port>] REceive [= <number>]
Allow calls from <number> to connect on <port>. May be used repeatedly. If no number in receive list, accept calls from any number.
- SET [<port>] RIngback [= <number>]
Specified the <number> that the <port> should be called back at.
- SET REMote ENable | DIsable
Enable or disable remote bridge-to-bridge control.
- SET SPEed = 56k | 64k | AUto
Set bridge rate adaption to 56 Kbps, use 64 Kbps clear channel, or try 64 and then, if the call fails, try 56.
- SET [<spid#>] SPId [= <number>]
Set the service profile identification (SPID) for each <number>. Typically, each bridge will only have one number and will not need a SPID.
- SET [<port>] TImeout = OFF | <seconds>
Disable time-outs, or disconnect <port> after <seconds> if there is no forwarded ethernet traffic.
- SET TYpe = <type> ACcept | BLock | DEMand | IGNore
This command filters packets based on the ether type. ACcept means forward entries <type>, BLock means do not forward any packets of <type>. There can be multiple BLock entries or multiple ACcept entries in the type table, but not both. DEMand means bring up the link (if AUto ON is set) if a packet of this type arrives. IGNore means forward the type, but do not count it in time-out calculations or demand dialing.

- `TIMEout <port> [THreshold = <Kbps>] [DURATION = <seconds>]`
`[SOURCE = ISDN | LAN | BOTH]`
Disconnect <port> after traffic is below <Kbps> for <seconds>. Count traffic from ISDN link, the LAN, or both.
- `UNlearn`
Removes all learned addresses from address table. Does not remove addresses entered manually.
- `VERSION`
Displays version of Combinet software running on bridge.