THE TOLLY GROUP

No. 6253 March 1996

ISDN Technology Trial

Cisco Systems ISDN Solutions

Cisco 7000, 4000, 2500, 1000 Series

Executive Summary

In the past, Small Office/Home Office (SOHO) sites rarely had connections to corporate LANs. This was because neither of the available connectivity options could deliver both acceptable performance and reasonable cost. Leased lines offered good performance but often at too high a price. Inexpensive dial-up analog links proved too slow for handling bandwidth-hungry LAN applications. Today, the Integrated Services Digital Network (ISDN) presents a viable option. ISDN is an increasingly popular wide area network service capable of combining high bandwidth (128 Kbit/s or greater) with a cost-effective, usage-based "dial up" implementation. The worldwide availability of ISDN brings high-powered internetworking into the realm of possibility for the SOHO user.

In addition to being a viable option for a primary connection, ISDN can be employed as a secondary connection between distant LANs. When used as a secondary connection in conjunction with leased lines, ISDN provides supplemental "bandwidth on demand" or emergency backup in the event of a primary service failure. ISDN brings to the corporate LAN a completely new set of network design challenges that did not exist with traditional leased lines, such as the need for cost control, security and more complex network management.

Cisco Systems commissioned The Tolly Group to demonstrate the effectiveness of Cisco's ISDN product set, including the 1000, 2500, 4000, and 7000 series routers (all run the Cisco Internetwork Operating System (Cisco IOS™) version 11.0(2.3))

Test Highlights

Cisco ISDN Products for the Headquarters site

- Multiple BRI interfaces per router
- PRI interface capability
- Callback feature

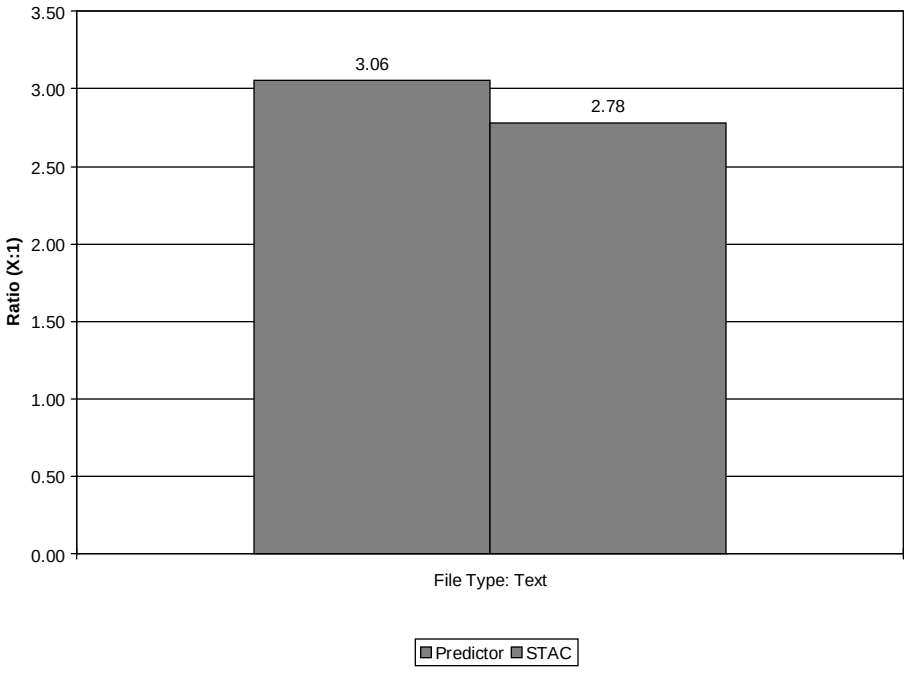
ISDN Leased Line Backup

- Non-disruptive backup of failed leased lines

Cisco ISDN Products for the Small Office/Home Office

- PPP Multilink
- Link speeds up to 128 Kbit/s
- Data compression
- Integrated Security (PPP CHAP, PPP PAP)
- SNMP Manageability

Compression Ratio
IPX File Transfer (2 B Channels)



Source: The Tolly Group, March 1996

Figure 1

running actual AppleTalk, IP, and NetWare (IPX) environments. The Tolly Group examined several aspects of ISDN that are important to SOHO and headquarters use: basic dial-on-demand connectivity for primary ISDN connections and leased line backup, bandwidth aggregation, performance (dual B-channels with compression), cost control via link/tariff management, security, and network management.

The Results

Test results indicate the Cisco products tested offer extensive provisions for effective ISDN use including a complete set of features for dial-on-demand, tariff/link management, performance, security, management and ISDN backup for leased lines. Additionally, Cisco has successfully integrated a number of ISDN features, such as PPP Multilink and Tariff Management, into the Cisco IOS software for the 1000, 2500, 4000, and 7000 series routers. Cisco rounds out its ISDN product line with the Cisco 200 series (from the acquisition of Newport Systems, Inc.) and the 750 series (from the acquisition of Combinet Corp.). Cisco IOS software has been incorporated into the entire Cisco product line. Neither the PC-based 200 series nor the standalone 750 series were tested in this evaluation.

Dial-on-demand

When ISDN is used as the primary connection for LAN to LAN access, dial-on-demand provides fast connectivity to network resources. (Note: the actual ISDN call is completed in approximately 250 ms. The additional time is needed for LAN protocol handshaking.) The remote router is simply configured with a destination network, be it an IP subnetwork or IPX network and the matching ISDN number. A connection will automatically be established when a client station at the remote site attempts to access the headquarters-based network resource. Dial-on-demand also provides both cost effective bandwidth to congested leased lines and fast, high-bandwidth backup in the event of leased line failure.

The Tolly Group utilized dial-on-demand routing for AppleTalk, IP and IPX throughout the evaluation. Configurations include a remote Basic Rate Interface (BRI) to an HQ BRI, two remote BRIs to a single router with multiple BRI interfaces and two remote BRIs to an HQ Primary Rate Interface (PRI). The total 144 Kbit/s data bandwidth of a BRI is comprised of two 64 Kbit/s data "B" channels and one 16 Kbit/s signaling "D" channel (2B+D). A PRI contains 23 B channels and one D (23B+D) combined for T1 data rate. To provide PRI E1 speeds, Cisco supplies 30B+D, which was not tested.

The Tolly Group found that, in all cases, connections were established for each protocol tested. Cisco's ISDN software implements a sophisticated set of filters and buffers to ensure that packets reach their proper destination. Additionally, access filters permitted only the packets destined for the configured networks to activate the link. The router's buffers successfully preserved outgoing packets while the ISDN link underwent activation.

Leased line backup

The Tolly Group set up a T1 link with a Basic Rate Interface (BRI) backup and verified that the BRI preserved a NetWare client/server file transfer when the T1 line was deliberately disconnected to simulate a network outage. The Tolly Group also verified timers in the router software that affect the delay between the leased line deactivation and the ISDN call. The timers eliminate unnecessary ISDN calls from momentary leased line failures. When the T1 link was reactivated, the BRI connection was automatically disabled and traffic was restored to the T1.

Performance

Efficient link utilization is a key factor in minimizing ISDN usage charges. The faster a file transfer is completed, the sooner the link can be brought down. Compression methods can effectively reduce file transfer times by as much as 50% and are an important part of any high performance strategy. Additionally, an ISDN BRI has two 64 Kbit/s Bearer "B" channels that carry data and a D channel for the signaling of the data channels. Aggregation of both B channels for the same session can give users more bandwidth for batch data transfer. (Depending on local tariff schemes, however, use of two B channels can double line charges.)

Cisco offers two user-selectable compression algorithms: STAC (Stac Electronics) and Predictor (public domain). The Tolly Group tested both using two B channels. Predictor achieved ratios of up to 3.06:1 and STAC achieved 2.78:1 when transferring a text file. As expected, further compression of already compressed ZIP and MPEG video files resulted in no additional compression gains.

Bandwidth on demand for a BRI interface allows the activation of the second B channel based on utilization on the first. This is also known as bandwidth aggregation. Once a link utilization threshold is maintained for a user-determined amount of time the second B channel is activated and logically combined with the first to provide a 128 Kbit/s "pipe" for data transfer. Once the utilization on the first B channel drops below the threshold for a predetermined interval, the second B channel is dynamically deactivated.

The industry standard for aggregating multiple B channels to achieve greater bandwidth is Multilink Point-to-Point protocol (PPP) (IETF RFC-1717). Multilink PPP also provides a basis for interoperable bandwidth aggregation among implementations. The Tolly Group configured bandwidth on demand and Multilink PPP and verified that the second channel was activated and utilized during a NetWare file transfer (IPX) and an FTP (TCP/IP) download.

TARIFF/LINK MANAGEMENT

Since most Regional Bell Operating Companies (RBOCs) charge for link usage in increments of one minute, ensuring that the link is active only when necessary to transmit data can keep a reign on potentially high WAN cost. The Tolly Group tested several features of Cisco IOS that control the activation and deactivation of the link: a routing configuration update mechanism, spoofing for IPX and SPX, filters for AppleTalk Name Binding Protocol (NBP) packets, and a link idle timer.

Dynamic routing protocols necessary to maintain topologies in large-scale networks can undermine the cost advantages of ISDN by forcing the link to remain active even when not needed for data transfer. IP and IPX routers update network topologies by broadcast Routing Information Protocol (RIP) packets on 30 to 60 second intervals (an IP RIP is a different packet than an IPX RIP but they serve similar purposes), that will activate an ISDN link if no provisions are made for filtering them. AppleTalk has a similar packet called a Routing Table Maintenance Protocol (RTMP) packet (sent once every 10 seconds). NetWare networks use an additional management packet called the Service Advertisement Protocol (SAP). Packets are transmitted from NetWare file and print servers (the default setting is one packet per minute).

An alternative to using RIP, SAP or RTMP protocols, (or any other dynamic network configuration protocol), is using static routes that forward packets based on fixed, user configured routing tables. Setup and maintenance of the static routing tables requires human resources and may not be an option for remote branch offices and/or complex enterprise networks.

Cisco offers a mechanism called "snapshot routing" that controls RIP, SAP and RTMP (and various other routing protocols which were not verified in this evaluation) packets while maintaining updates. Snapshot Routing is a critical component in building large, scalable, internetworks with ISDN. Snapshot routing activates the link for a specified amount of time over a cycle (for example 5 minutes out of 1 day) to allow update packets to be exchanged by the ISDN routers, (if the link is already up to forward data, RIP and RTMP packets will also be exchanged at this time). Snapshot routing functioned according to vendor specifications in the tests. Cisco also supports the configuration of static routing tables.

A NetWare server checks to see if its clients are active about once every minute when there is no data flow. IPX "watchdog" packets, as well as similar Sequenced Packet Exchange (SPX) keep-alives that are transmitted at an even higher frequency, can cause an ISDN link to remain active during the entire business day. IPX and SPX spoofing is a method that keeps watchdogs and keep-alives from activating the link. While spoofing, an ISDN router will reply to the NetWare server as if it were a client, thereby eliminating the need to bring up the link. The Tolly Group tested this feature in a live NetWare 4.x and 3.12 client/server environment and found that it successfully spoofed both IPX and SPX watchdog and keep-alive packets.

Cisco Systems
ISDN Solutions
Cisco 7000, 4000, 2500, 1000 Series

ISDN Performance

Cisco Systems
ISDN Solutions
Cisco 7000, 4000, 2500, 1000 Series
Product Specifications*

Cisco 1003
LAN: Ethernet
WAN: ISDN
WAN Rate: ISDN BRI

Cisco 2516
LAN: Ethernet (integrated 14-port concentrator)
WAN: Serial (T1/E1), ISDN
WAN Rate: ISDN BRI

Cisco 4500
LAN: Token Ring, Ethernet, FDDI
WAN: Serial, ATM, ISDN, Frame Relay, X.25, HDLC
WAN Rate: ISDN BRI/PRI, ATM OC-3, ATM DXI and UNI, Serial 8 Mbit/s, Frame Relay E1

Cisco 7010
LAN: Token Ring, Ethernet, Fast Ethernet, FDDI
WAN: Serial, ATM, ISDN, Frame Relay, X.25, HDLC
WAN Rate: ISDN PRI, ATM OC-3, ATM DXI and UNI, Serial 8 Mbit/s, Frame Relay E1

BRI = Basic Rate Interface (128 Kbit/s)
PRI = Primary Rate Interface (T1/E1)

Cisco IOS Software code level: 11.0 (2.3)
Routed protocols supported: TCP/IP, IPX, AppleTalk, VINES, XNS, DECnet, OSI, APPN
Bridged protocols supported: SRB, Transparent, SRT, DLSw, SDLLC

**Vendor-supplied information not verified by The Tolly Group*

Another link activating packet is the AppleTalk Name Binding Protocol (NBP) packet. The Tolly Group verified that the Cisco routers tested were able to filter NBP packets. Cisco, does however, recommend that the NBP filter be used with caution as one of the NBP's functions is to link an application to network resources. If the NBPs are filtered then certain resources may be unavailable to applications. Cisco recommends that the application vendors be consulted on how best to eliminate NBP traffic.

Finally, the link idle timer deactivates the link once a predetermined period of idle time (when no useful traffic is present on the link) expires. The Tolly Group verified that the idle timer functioned properly.

Security

As with any remote dial-in configuration, security is an important concern. There are several means of ensuring that the call is initiated from a legitimate source: PPP challenge-handshake authentication protocol (CHAP), password authentication protocol (PAP), calling line identification screening (callerID), and called party number verification (CPNV).

PPP CHAP and PAP will allow establishment of an ISDN link between two routers only if user specified device names and passwords are exchanged. CHAP is more robust than PAP. CHAP performs a multistage encrypted password negotiation whereas PAP passwords travel unencrypted over the ISDN link and can be easily intercepted. The Tolly Group verified that link establishment was denied when invalid device name/password combinations were presented. This test was run with both CHAP and PAP.

With callerID, the router compares the caller identification field (if supported by the service provider) of an incoming call with a user-configured list of acceptable numbers. If the ID of the incoming call does not match one of the numbers in the list, the call is rejected by the receiving router. This is useful for small office-to-headquarters security. The number of each of the branch offices is configured in to the central router and only calls from those offices are accepted.

The Tolly Group attempted to create connections with numbers not on the receiving router's callerID list and verified that the link was not established. The Tolly Group also verified that a call with a number on the callerID list was accepted.

Called party number verification (CPNV) allows the receiving router to verify that its configured number or subaddress matches the destination number and subaddress of the incoming call. ISDN contains an additional field in the calling and called number called a subaddress. A single BRI connection can be connected to multiple ISDN devices, each with the same ISDN number but a unique subaddress. CPNV allows a single Basic Rate Interface (BRI) to accommodate multiple devices while having only the device with the ISDN number and subaddress that is specified by the call originator answer the call and establish the link. The Tolly Group verified that the receiving router established a link only when the correct number and subaddress were dialed by the router initiating the call.

Management

The added complexity of ISDN's dial-up nature makes effective management even more important. Keeping track of called numbers, link-active times, individual B channel usage and other link statistics makes bill verification a less formidable task. Error messages also make troubleshooting switch/router configuration mismatches possible. Cisco offers many features to assist with call tracking and troubleshooting: a set of ISDN MIB variables, callback, statistics, and debug capabilities.

Since there is no industry standard SNMP MIB for ISDN, Cisco has designed two proprietary MIB groups, the Cisco ISDN MIB and the Cisco Call History MIB. The ISDN MIB records variables such as number called, maximum duration of call, duration of last call, and number of calls refused. The Call History MIB tracks the time that calls take place. The Tolly Group performed a simple read of several of the MIB variables from a proprietary UNIX MIB reader supplied by Cisco. Cisco plans to update Cisco Works, Cisco's management platform, to read the variables in Q1 1996.

Cisco's callback feature, following RFC-1570, allows central billing of all ISDN calls. Since all calls originate from a single location, one tariff structure is used and the accounting and bill verification processes are simplified. Callback also allows added security when used in conjunction with PPP authentication protocols to verify the identity of the router initiating the call.

Operation of callback is as follows: the originating branch router calls its partner router (in our tests, the headquarters site router) and transmits a "request callback" packet sequence. Both the originating router and the central site exchange authentication packet sequences so the central site router can determine the location and dial number of the originating branch router. The connection is then terminated. The central site then calls the branch router and a connection is established. Proper functioning of callback was verified.

Vital statistics for each BRI interface, such as calls attempted, packets transmitted and errors, can be displayed using a set of "show" com-

mands (e.g., show dialer, show interface bri 0). Statistics are complemented by a comprehensive set of "debug" commands (e.g., debug ppp negotiation, debug dialer and Q.921 and Q.931 for ISDN signaling) capable of troubleshooting ISDN link activity. Cisco's event logging tools allowed the tracing of link activity and protocol decodes to assist with configuration. The Tolly Group used the show and debug commands throughout the trial to determine status of the links and to facilitate configuration and testing.

Test Methodology

Small Office/Home Office

The Tolly Group configured a routed AppleTalk, IP, and NetWare network that consisted of several Ethernet LANs linked by two branch routers, a Cisco 2516 and 1003, and three headquarters routers, two Cisco 4500s and a Cisco 7010 (see Test Bed, figure 2). These tests were conducted at Cisco Systems headquarters in San Jose, California. Each branch router connected to the Pacific Bell ISDN network via a single BRI link. The first 4500 connected to ISDN via two BRIs and each of the remaining headquarters routers connected via a PRI. Each branch office router linked its own Ethernet segment (the 2516 has 14 built-in Ethernet concentrator ports) and each of the headquarters routers were connected to a Cisco Catalyst Ethernet switch.

The Tolly Group used a Network Communications Corp. Network Probe 7300 ISDN analyzer and a Network General Expert Sniffer Ethernet LAN analyzer throughout the test. The ISDN analyzer was used to monitor the BRI connections for call setup, and data transfer. The LAN analyzer was used to monitor packet exchange and file transfer times throughout the test.

Dial-on-demand

AppleTalk, IP and IPX routing were configured on all of the routers. For basic dial-on-demand connectivity, The Tolly Group established links between the BRI interfaces of the branch routers to the 7010 PRI, the first 4500 via a PRI and to the second 4500 using multiple BRI interfaces. IP ping commands were sufficient to bring up the link. Snapshot routing was tested by verifying that a BRI link between a 2516 and 4500 was activated at the pre-configured time. When the link was down, the Tolly Group verified that AppleTalk RTMP, IP RIP and IPX RIP packets, that are naturally broadcast from each router in a routed network, did not activate the link. The Tolly Group also verified that a NetWare client at the branch was able to connect to a headquarters NetWare 4.1 server.

Leased Line Backup

The Tolly Group configured a T1 leased line by connecting two VeriLink Access System 2000 Connect T1 Plus CSU/DSUs that were attached to two 2516 routers (see Test Bed, figure 2). The two routers were also connected to the ISDN network via BRI connections. The Tolly Group disconnected the link between the CSU/DSUs and verified that a NetWare client/server file transfer was unaffected. The T1 link was reconnected and The Tolly Group verified that the T1 file transfer continued over the T1 and the ISDN call was dynamically terminated.

Performance

Compression of the 2516 and 4500 was tested by performing three NetWare file transfers from the branch client to a headquarters server. The Tolly Group used a highly compressible text file, and two pre-compressed files: a file compressed with PKZIP (PKWare) and an MPEG file. Transfer times were clocked without compression and then again with first, STAC compression enabled and then, Predictor compression enabled. Compression ratios were calculated by dividing the transfer time of the respective file with compression enabled by the transfer of the file with compression disabled. Transfer times were clocked on the LAN with a Network General Expert Sniffer Ethernet analyzer.

Bandwidth on demand was tested by performing a file transfer between the NetWare client and server with the link utilization threshold set to 50%. The Tolly Group verified both the activation (upon initiation of the file transfer) and deactivation of the second B channel (once the file transfer was finished).

Tariff/Link Management

IPX spoofing was tested by logging in the client to the NetWare server, waiting for the router's idle timer to bring the link down, then verifying, with a Network Communications Corp. Network Probe 7300 ISDN analyzer, that the link remained down while the router replied to the server's watchdog packets. A directory of a network drive (which reactivated the link) was then executed at the client to verify that the NetWare connection was still operational. SPX spoofing was tested in a similar fashion. The Tolly Group ran RCONSOLE.EXE, an application that allows remote management of NetWare servers, from the client which utilizes the SPX protocol and then followed the previous procedure to verify the router correctly spoofed the server's SPX keep-alive packets and the session was preserved.

The Tolly Group verified that the 4500 router filtered NBP packets and kept the link down. The NBP packets were forwarded from Cisco's production

Test Bed

LANs

Topology
10 Mbit/s Ethernet (Qty 2)
Concentrators
Cisco Catalyst Ethernet switch (Qty 2)
Wiring
10 ft. unshielded twisted pair (UTP) (RJ-45 termination)

WANs

Topology
64 Kbit/s ISDN BRI (2B+D)
56 Kbit/s B channel ISDN PRI (23B+D)
Provider
Pacific Bell for BRI service and AT&T for PRI service
Switch
AT&T 5ESS for BRI, 4ESS for PRI
Signaling
National ISDN-1
NT-1
Northern Telecom

Topology
Synchronous T1 (1.536 Mbit/s)
CSU/DSU
VeriLink Access System 2000 Connect T1 Plus (Qty 2)

Network Analyzers

Analyzer 1
Vendor
Network Communications Corp.
Product Name
Network Probe 7300
Topology
ISDN
Version Number
6.00A

Analyzer 2
Vendor
Network General
Product Name
Expert Sniffer
Topology
Ethernet
Version Number
4.5

Routers

Vendor
Cisco
Product
7010 w/PRI, 4500 w/PRI, 4500 w/ Multiport BRI, 2516, 1003
Version Number
Cisco Internetwork Operating System 11.0 (2.3)

End Stations

End Station 1
Vendor/Model
Toshiba T2130CT Satellite
Processor/Speed
Intel DX-4 75 MHz
Memory
16 Mbytes
Operating System
MS-DOS 6.2, Microsoft Windows for Workgroups 3.1, NetWare Client 4.1
Network Interface Cards
Xircom Credit Card Ethernet
Function
Remote NetWare Client

End Stations 2 and 3
Vendor/Model
AST P/90 Premia GX (Qty 2)
Processor/Speed
Pentium 90 MHz
Bus
PCI/ISA
Memory
32/38 Mbytes
Operating System
MS-DOS 6.2, Novell NetWare 3.12, NetWare 4.1
Network Interface Cards
AST on-board Ethernet
Function
NetWare Server

End Station 4
Vendor/Model
Compaq ProSignia
Processor/Speed
80486 33 MHz
Bus
ISA
Memory
42 Mbytes
Operating System
Microsoft NT 3.5
Network Interface Card
3Com Etherlink III
Function
NT Server

network connected to the headquarters LAN by a Cisco AGS+ router. The link idle timer was used throughout the link management tests to deactivate the link before each test.

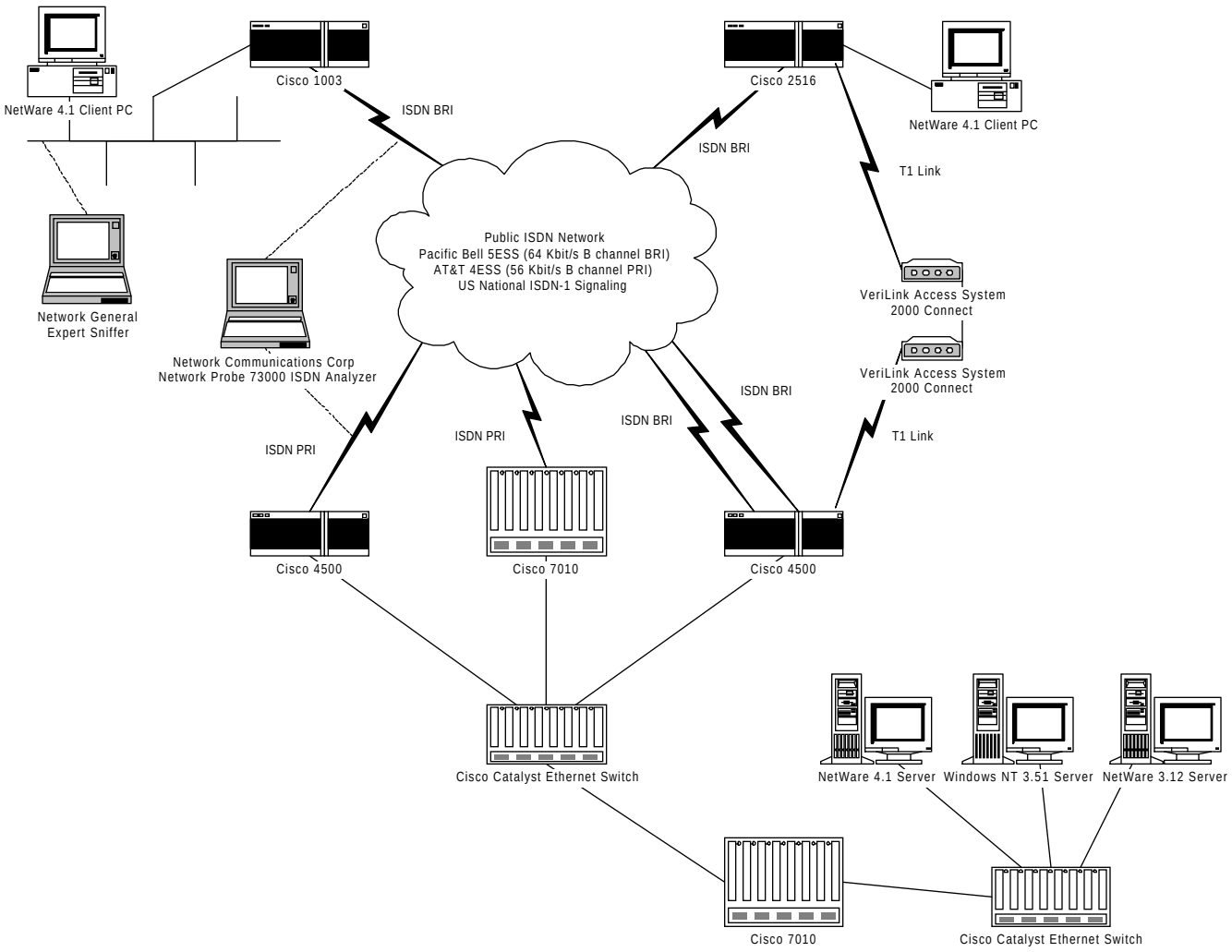
Security

CHAP and PAP were tested by verifying that the NetWare client was able to attach to the server when correct device names and passwords were used on the branch routers and that the client was unable to connect when incorrect names and passwords were configured on the branch router.

Calling line identification (callerID) was verified by configuring the headquarters router to accept only the number of the branch router. Since Pacific Bell does not support the callerID feature, the identification field of the Call Setup packet contained all zeros and as a result, Cisco's caller ID should not accept any calls. The Tolly Group verified first, that the 4500 accepted a call from the branch router with caller ID was deactivated, and secondly that the 4500 did not accept any calls once caller ID was activated.

Called Party Number Verification (CPNV) was tested by configuring

Test Bed



Source: The Tolly Group, March 1996

Figure 2

the CPNV command of the 4500 router with two numbers. First, The Tolly Group configured the same number on the 4500 that the branch router dialed and verified that the 4500 answered the call and established a link. Second, The Tolly Group configured the 4500 with a number that was different from the number that the branch router dialed and verified that the 4500 did not answer the call.

Network Management

The Tolly Group verified the presence of Cisco's ISDN MIB by reading MIB variables from the 2516 router, via a proprietary UNIX MIB reader provided by Cisco, and observing that values were present for several of the MIB variables. The Tolly Group did not attempt to verify the accuracy of each of the MIB variables.

For the callback feature, The Tolly Group configured the 4500 to call back the branch router. Using the Network Probe 7300 ISDN analyzer, The Tolly Group verified that once the branch router placed the call, the 4500 disconnected the call and initiated the call to the branch router.

The "show" and "debug" commands were used throughout configuration and testing.

About The Tolly Group
ISDN technology Trial

Few end-user organizations have the resources to test the wide range of ISDN products on the market today or to prototype the technology in real environments. Until now, they have been forced to rely on buyer's guides which do little more than summarize vendor data sheets. Alternatively, customers spend countless man hours researching trade publication articles assembling the information required to make an informed buying decision. Even vendors have difficulty gathering the level of performance data that comes from engineering-caliber testing.

End users have frequently asked The Tolly Group to evaluate several diverse ISDN products in an effort to provide them with the kind of information they require before deploying this new technology. As it has done in the past with Token Ring Switches, FDDI, Networked Multimedia, Data Link Switching and Local Token Ring Bridges, The Tolly Group is pleased to present the ISDN Technology Trial to help end users evaluate the various ISDN solutions currently offered.

About The Tolly Group

The Tolly Group provides strategic consulting, independent testing, and industry analysis. It offers a full range of services designed to furnish both vendor and end-user communities with authoritative, unbiased information. *Fortune* 1,000 companies look to The Tolly Group for vendor-independent assessments of critical corporate technologies. Leading manufacturers of computer and communications products engage The Tolly Group to test both pre-production and production equipment.

The Tolly Group is recognized worldwide for its expertise in assessing leading-edge technologies including networking, multimedia, and messaging. By combining engineering-caliber test methodologies with informed interpretation, The Tolly Group consistently delivers meaningful analyses of technology solutions. The Tolly Group has published more than 100 product evaluations, network design features and columns in the industry's most prestigious publications.

Kevin Tolly is President and CEO of The Tolly Group. He is a leading industry analyst and is responsible for guiding the technology decisions of major vendor and end-user organizations. In his consulting work, Tolly has designed enterprise-wide networks for government agencies, banks, retailers, and manufacturers.

For more information on The Tolly Group's services, visit our World Wide Web site at ***http://www.tolly.com,*** email to info@tolly.com, call 800-933-1699 or 908-528-3300, or fax 908-528-1888.

Tolly Group doc. 6253 rev. 4Mar96