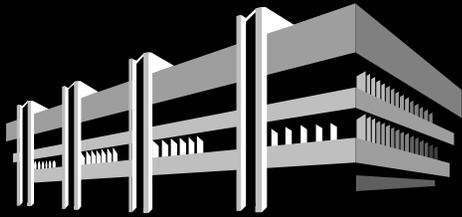


Remote Network Server Access

Michael P. Andrews
Ameritech Electronic Commerce
Senior Technology Consultant
Network Services - National Operations
Mike.Andrews@Ameritech.COM

Mike@MikeA.COM



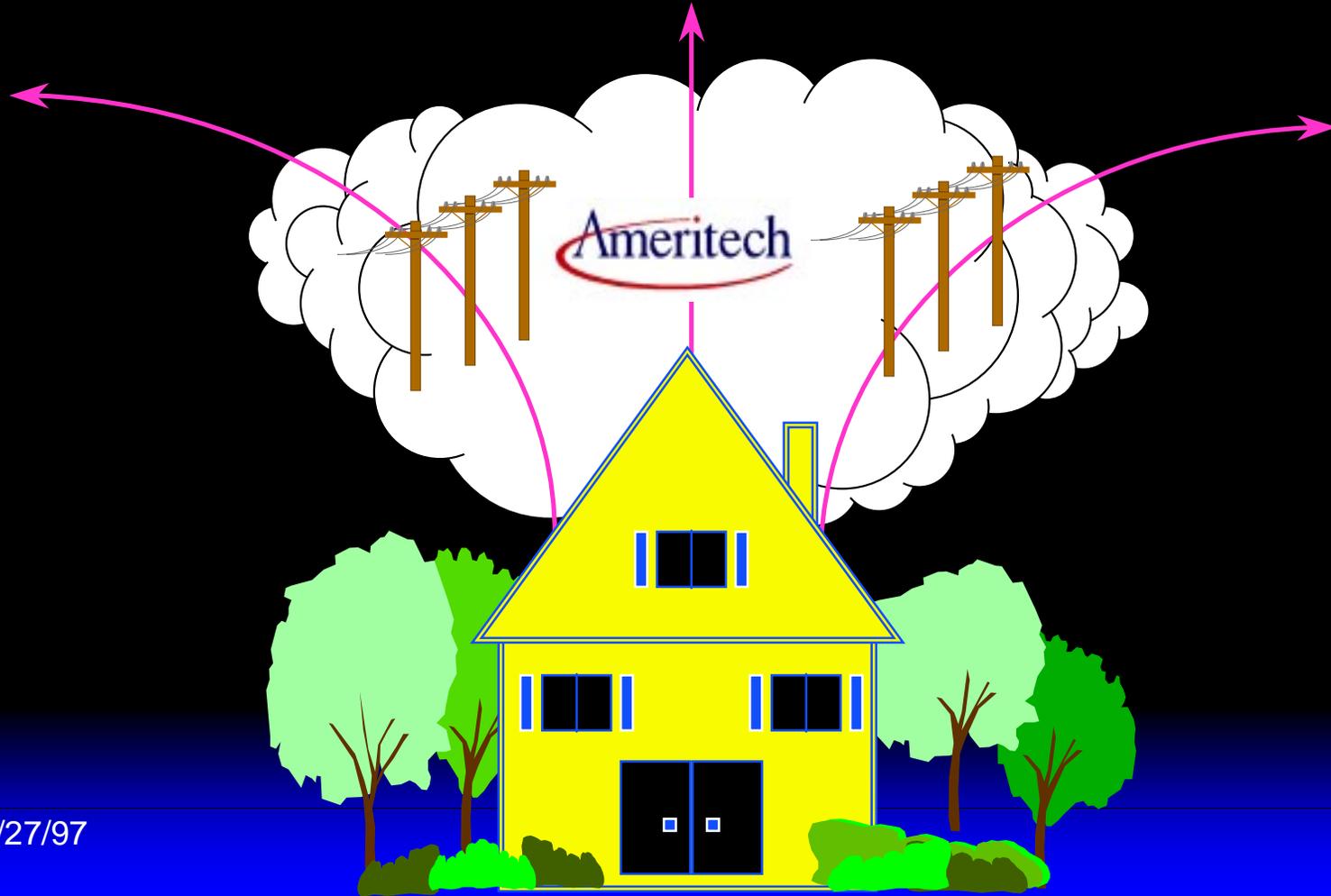
Work At Home



On-Line Access



Intranet Access



Introduction

- ◆ Need to provide services on the Corporate LAN and/or Intranet to remote users:
 - I/T support staff
 - “Road Warriors”
 - Other staff working from home
 - Contractors and vendor support staff

Introduction

- ◆ Today's Applications require live, "real time" access:
 - Email
 - Web
 - Database

Summary

- ◆ How to provide transparent remote access to all services on multiprotocol LAN servers
- ◆ How to maximize performance
- ◆ How to maintain security
- ◆ Configure Windows 95 / NT 4.0 client
- ◆ Configure Access Server / Router

Summary (cont.)

◆ Protocols

– TCP/IP

- ❖ Internet / Intranet
- ❖ Microsoft NT

– IPX

- ❖ Novell NetWare / IntraNetWare
- ❖ Microsoft NT

– NETBEUI (NETBIOS)

- ❖ Windows for Workgroups
- ❖ Windows 95
- ❖ Microsoft NT

What remote access are you using now?

- ◆ What types of servers do you have?
 - Are you using or planning on using NT?
- ◆ What kind of remote users?
 - How easy for users to dial in?
 - How usable is the access speed?
- ◆ What kind of security is in place?
 - Firewall
 - Token authentication
 - VPN

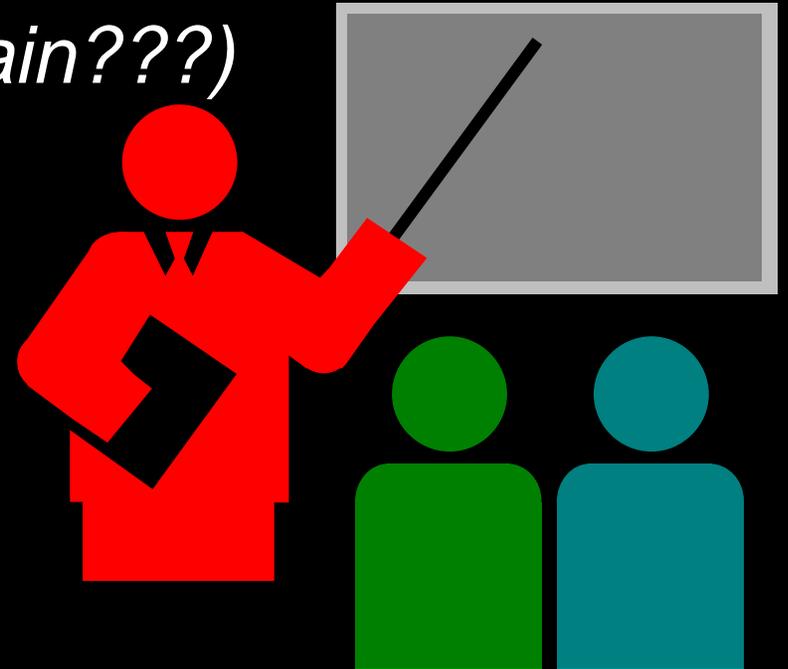
Agenda

- ◆ *a little* Theory on Communications technology
- ◆ Security methods
- ◆ Network planning
- ◆ Windows 95 configuration
- ◆ (General) Access server configuration

Up and Down the stack

- ◆ The Network Layers (*again???*)

- Application
- Presentation/Session
- Transport
- Network
- Data Link
- Physical



TCP/IP on LAN

- ◆ The Network Layers
 - Netscape (Application)
 - HTTP (Presentation/Session)
 - TCP (Transport)
 - IP (Network)
 - Ethernet (Data Link)
 - Twisted Pair (Physical)

TCP/IP on Dial-up

- ◆ The Network Layers
 - Netscape (Application)
 - HTTP (Presentation/Session)
 - TCP (Transport)
 - IP (Network)
 - PPP (Data Link)
 - Serial Modem (Physical)

Application

“doesn’t see a difference”

◆ LAN

- Netscape
- HTTP
- TCP
- IP
- Ethernet
- Twisted Pair

◆ Dial-up

- Netscape
- HTTP
- TCP
- IP
- PPP
- Serial Modem

SLIP vs. PPP

◆ SLIP

- Serial Link IP
- IP with minimal header
- No error checking
- IP ONLY

◆ PPP

- Point to Protocol
- HDLC
- LCP - Error checking
 - ◆ LQM - FCS
- NCP - Carries Multiple Protocols:
 - ◆ IPCP (IP)
 - ◆ IPXCP (IPX)
 - ◆ ATCP (Appletalk)
 - ◆ NBCP (NetBIOS)

PPP Node Authentication

◆ PAP

- plain text password sent across line during PPP negotiation

◆ CHAP

- password is MD5 digest key to random challenge, password never crosses the link
- challenge periodically re-occurs during PPP connect



Out of Band Node Authentication

- ◆ Username/Password
 - Use script to answer prompts
 - password may be exposed
- ◆ Caller ID
 - reject call if not from home number
 - doesn't support "Road Warriors"
- ◆ Callback

More Secure Node Authentication

◆ One time Password

– S/Key

- ◆ software freely available

– Token

- ◆ SecureID

- ◆ others

Dial-up Link choices

- ◆ Analog Modem
- ◆ Cellular Modem
- ◆ Digital ISDN “Modem”
- ◆ Digital ISDN Router
- ◆ Packet Services
- ◆ ADSL

Analog Modem

- ◆ Available in Internal/External/PC card
- ◆ Uses existing POTS phone line
- ◆ *67, to disable Call Waiting
- ◆ Lifting phone extension causes errors
- ◆ Best with separate phone line
- ◆ Adapters available for use with Digital PBX lines (connects to handset)

V.34bis Modem

- ◆ up to 33.6Kbps
- ◆ Error correcting
- ◆ Adaptive link speed
 - “downshifts” for poor-quality lines
- ◆ Data Compression
 - up to 4X better throughput

56Kbps Modem

- ◆ Same features but...
- ◆ Requires Digital lines at POP (more later)
- ◆ Two incompatible “standards”
 - X2 (USR)
 - K56Flex (Rockwell, Lucent, others)
- ◆ Now limited to 52Kbps

Cellular Modem

- ◆ Call (modem carrier) gets interrupted as cells change
- ◆ MNP 10 required
 - Special interruption tolerant protocol
 - Must be on modems at both ends
- ◆ V.34bis modem will work (*sorta*)
 - Set higher “carrier loss detect” S register on both sides

What can ya expect?

- ◆ Good performance for API, data only applications
 - Web
 - File transfer
 - SMTP, POP, or API E-mail

What d'ya expect?

- ◆ Lousy performance for DOS file access intensive applications
 - Running apps from file server
 - DOS Database apps
 - Microsoft Mail 3.2
- ◆ Disable processing of Novell server logon scripts

Use remote control for those

- ◆ Remote Control Products that use TCP/IP or IPX network transport will work OK
 - Symantec PC Anywhere 32
 - Carbon Copy
 - Stac Reachout Remote

ISDN

*It Still Does Nothing**

ISDN

*It Still Does Nothing**

**if you don't try it*

How Does ISDN Work?

ISDN provides a standard “pipe” called the Basic Rate Interface.

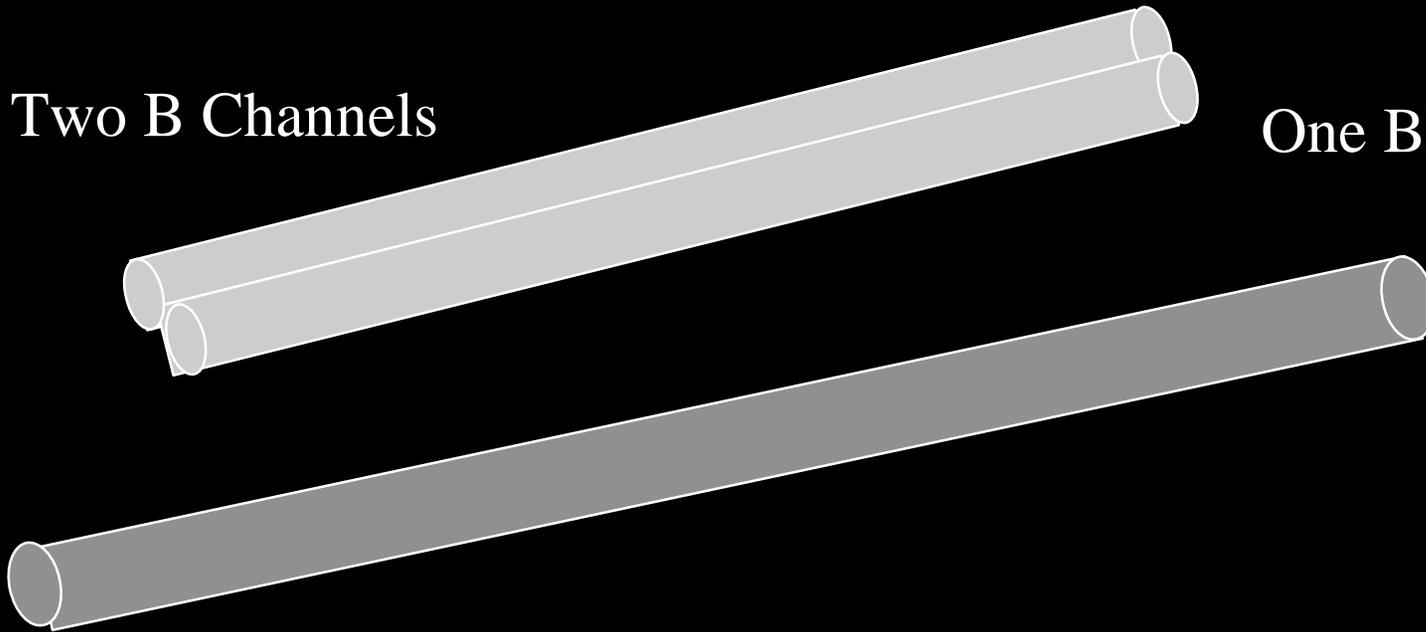
BRI is transmitted over the normal 2-wire copper cable facilities which are familiar to telephone transmission all over the world.

Unlike ordinary analog transmission which restricts this pipe to one conversation at a time, BRI combines, or multiplexes, three communications channels into that one pipe - all of which can be used simultaneously.

Basic Rate Interface (BRI)

Two B Channels

One BRI = 2B + D



16 Kbps D Channel

B Channels - User, Voice, Data, Image, Sound

D Channels - Call Signaling, Set-up, User Packet Data

A 64Kbps “line”

- ◆ Also called “DS0”
- ◆ Standard digital US phone call unit
- ◆ Supports one Voice call
- ◆ 8 bits sampled @ 8,000 times/second
 - =64,000 bits per second
 - =64Kbps
- ◆ Faster lines are time-div-multiplexed groups of DS0s

ISDN BRI features

- ◆ Special Digital Line delivered on a single pair
- ◆ BRI - Two 64Kbps B Channels
- ◆ Call sets up in seconds
- ◆ Use spare B for
 - Voice
 - FAX
 - Analog Modem (some have built-in)
- ◆ Combine B's for 128Kbps with
 - BONDING (no “demand” to it!)
 - MPPP (Multilink PPP)

ISDN “Modem”

- ◆ Not really a “Modem” - ISDN TA
- ◆ Internal / External / PC card
- ◆ External has serial port connection to PC
 - serial bottleneck causes less than optimum performance (*more later*)
- ◆ Some have Parallel port
- ◆ Data Compression
 - up to 4X better throughput (200-300Kbps)

ISDN Router

- ◆ External with 10Mbps Ethernet (10BaseT) port
- ◆ PC requires LAN card
- ◆ Some with BOOTP/DHCP to dynamically assign IP address
- ◆ Data Compression
 - up to 4X better throughput (200-300Kbps)

What does ISDN cost?

◆ Residential BRI

- Install ~\$150
- Monthly ~\$34.00
- Each B usage charge same as POTS phone line
 - ❖ “A Band” (8 miles) “Nickel zone” call .05 untimed
 - ❖ “B Band,” “C Band” calls timed

How to order ISDN

- ◆ Call 1-800-TEAM-DATA (Business orders from CBS, EBS, or SBS. See phone bill)
- ◆ Order National ISDN1
- ◆ Switched Voice/Data on BOTH B channels
- ◆ Phone numbers on BOTH B channels
- ◆ Indicate equipment vendor
- ◆ ISDN Provisioning center will FAX order confirmation with SPIDs

Choosing ISDN equipment

- ◆ Choose built-in NT (Network Terminator)
- ◆ Look for unit with one or two POTS jacks for analog phone and FAX
- ◆ Look for EZ setup

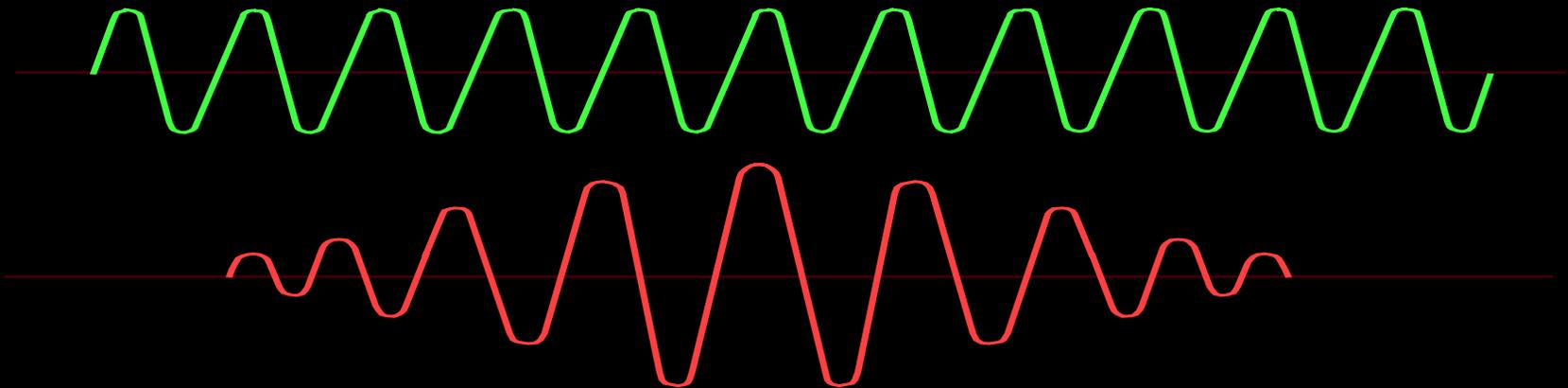
Configuring ISDN device

- ◆ Switch type: National ISDN1
- ◆ Enter SPIDs, LDN (phone numbers)
 - LDN1: 8479361212
 - SPID1: 84793612120111
 - LDN2: 8479361213
 - SPID2: 84793612130111

Serial is a Killer

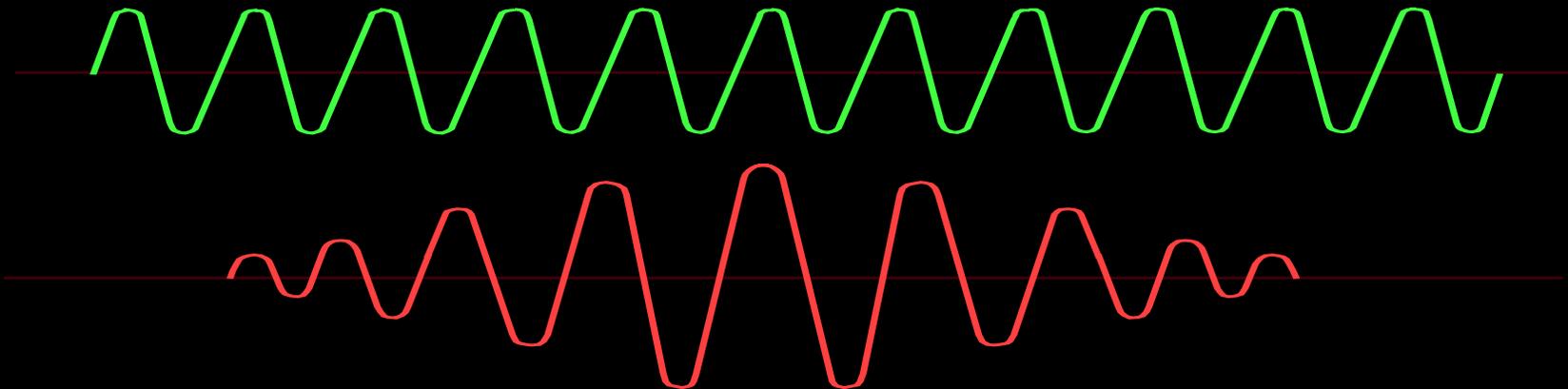
- ◆ ASYNCH port ships 10 bits for 8-bit byte of data, a 20% overhead
- ◆ 38,400bps, 57,600bps, 115,200bps (not as fast as raw 128Kbps 2B ISDN!)
- ◆ Requires 16550 or 16650 UART with FIFO buffer
- ◆ PC / Windows cannot service serial port interrupts fast enough, losing data
- ◆ Lowering the port speed may improve throughput performance! (check PPP stats)

Network Protocols



Network Protocols

- ◆ TCP/IP
- ◆ IPX/SPX
- ◆ NetBEUI (NetBIOS)



TCP/IP

- ◆ Universal DOD protocol of the Internet
- ◆ Requires unique network address (or NAT)
- ◆ Routable - choice of routing protocols, typically RIP
- ◆ Scalable packet size
- ◆ Commonly used to carry (tunnel) other protocols like IPX, NetBEUI, SNA

Remote TCP/IP Network Planning

Either

- ◆ Hard code Client IP address
 - For node identification, DNS rev, Security

or

- ◆ Assign IP addresses during PPP negotiation
 - Server has IP address pool

Remote TCP/IP Network Planning

Either

- ◆ Treat remote nodes as separate advertised subnet

or

- ◆ Use existing subnet with proxy ARP
- ◆ Same DNS, WWW, Email, etc. server addresses

Remote TCP/IP Network Planning

- ◆ Same DNS, WWW, Email, etc. server IP addresses

VPN - Secure TCP/IP

- ◆ The Network Layers
 - Netscape (Application)
 - HTTP (Presentation/Session)
 - TCP (Transport)
 - IP (Network)
 - **ENCRYPTION**
 - PPP (Data Link)
 - Serial Modem (Physical)

VPN - Secure TCP/IP

- ◆ Secure link from node to firewall, even across unsecure networks, i.e.. the Internet
- ◆ IPSec
 - part of IETF IPv6 (but v6 not required)
 - Triple DES encryption
 - even IP address encrypted

IPX / SPX

- ◆ Novell Netware / IntraNetWare
- ◆ Typical 128Kbyte (small) packet size
- ◆ Primarily File or Print services
- ◆ Broadcast to locate servers
- ◆ SAP service broadcasts
- ◆ RIP routing updates

Remote IPX Network Planning

- ◆ New arbitrary IPX network
- ◆ IPX network-node address during PPP negotiation
 - Server has IPX network address for remote nodes
 - Remote client generates node address
- ◆ Use outbound SAP filters (unless server is remote)

NetBEUI

Net BOO! Hiss!

- ◆ Extension of NetBIOS
 - Developed by IBM as basic LAN protocol
 - Emulates BIOS file access
 - Later by Microsoft LAN Manager
- ◆ Everything is a broadcast
- ◆ Not routable
- ◆ Used by WFW, Win95, NT Network chooser

NetBEUI Network Planning

- ◆ Need it to make access friendly
- ◆ Best to tunnel it!
- ◆ NetBEUI <---> WINS <---> TCP/IP <---> WINS <---> NetBEUI
- ◆ NetBEUI <---> IPX <---> NetBEUI
- ◆ Or use NBCEP in PPP link (like RAS server)
- ◆ Or... use local LMHOSTS file



On the client side

Windows 3.1, 3.11 (Windows for Workgroups)

- ◆ Recommend Stampede Remote Office Gold
 - www.stampede.com

Windows 95/NT

- ◆ “Dial-up” networking
 - In Control Panel or Accessories
 - Install from CD as “Communications”
- ◆ Primary logon --> Windows logon
- ◆ Enter node “username”, password. Click on “Save password”

Resist the urge to tinker!

Microsoft talks funny. Some options have strange behavior. The defaults are usually correct!



On the server side

Primary Rate Interface (PRI)

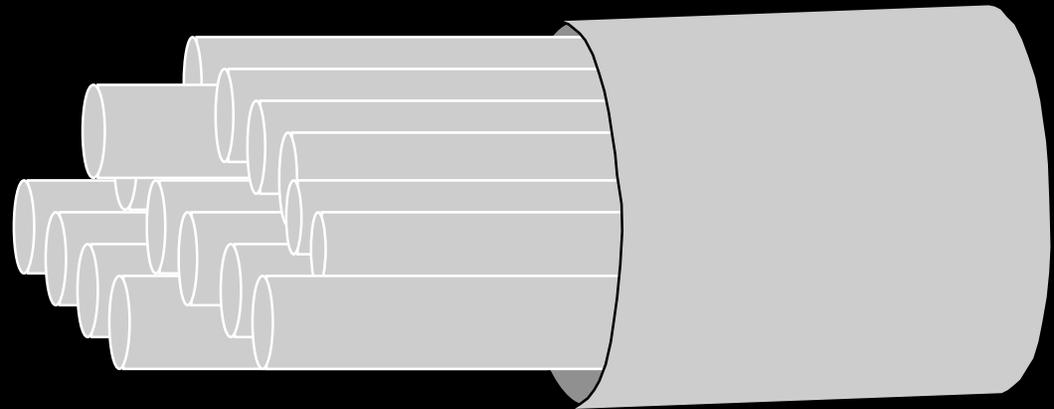
One PRI =

United States: 23 B+D

Europe/Asia: 30/31 B+D

B Channels -

User Voice, Data
Image, Sound



23 B Channels

D Channels -

Call Signaling,
Set-up, User
Packet Data



64 Kbps D Channel

PRI, the Hot Setup

- ◆ 23 channels (lines) serve both analog modem and digital ISDN users
- ◆ Digital “further in” gives clearer line
- ◆ D channel indicates voice call ---> software modem “emulator”
- ◆ D channel indicates digital call ---> digital “all the way”

PRI, the Hot Setup

- ◆ Supports “Caller ID” for logging, security
- ◆ 23 lines on one port for high density
- ◆ Up to 268 lines in one 19” rack device (Bay Networks)
- ◆ Setup used by large ISPs (i.e.. AOL)



Resist the urge to tinker!

The defaults are usually correct!

Where to get more information

- ◆ Dan Kegel's ISDN page -
<http://alumni.caltech.edu:80/~dank/isdn>
- ◆ Vendors
 - www.ascend.com
 - www.adtran.com
 - www.baynetworks.com
 - www.cisco.com
 - www.microsoft.com
 - www.shiva.com

User database

- ◆ Local
 - may be limited
- ◆ TFTP, DNS server
 - data may be exposed
- ◆ Authentication database server
 - TACACS, TACAS+
 - ◆ Cisco
 - Radius
 - ◆ others

Activity logging

- ◆ SYSLOG
- ◆ SNMP Traps
- ◆ Authentication database server
 - TACACS
 - Radius
- ◆ Parse logs with Perl to do reports, billing

Where to get more information

- ◆ Usenet Newsgroups (or...
use <http://www.dejanews.com>)
 - comp.protocols.tcp-ip
 - comp.protocols.ppp
 - comp.dcom.isdn
 - comp.dcom.modems
 - comp.dcom.servers
 - comp.dcom.modems

Where to get more information

- ◆ Network Computing Magazine

<http://techweb.cmp.com/nc/docs>

- ◆ The ISDN Literacy Book

Gerald L. Hopkins, Addison-Wesley Pub. Co.

ISBN#0201629798