Jargon Busting -

An Introduction to the

Technology of Data Networks

Tutorial III

ACM SIGUCCS
User Service Conference XX
November 8, 1992
Cleveland, Ohio

Scott Bradner
Harvard Office of Information Technology

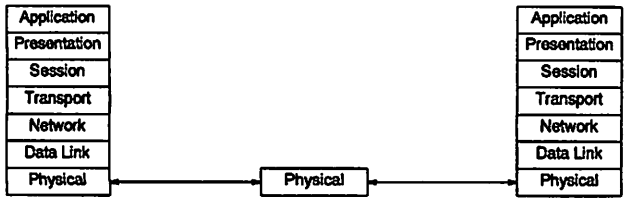
Definitions

What are we talking about anyway?

ISO's view of the world:

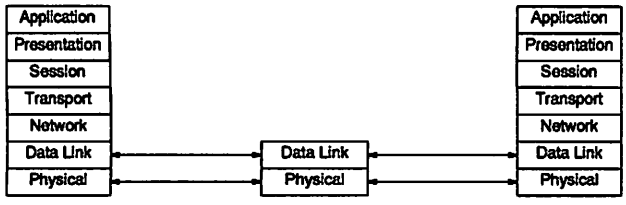
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Repeater



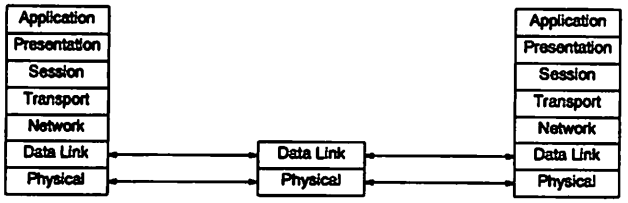
Repeater:
- operates at the ISO physical layer
- networks operate as if they are a single network
- copies (and sometimes gains or loses) bits
- unconditionally forwards bits
- not frame store-and-forward
- does not regenerate checksums
- protocol independent
- end node transparent
- swappable

Transparent bridge



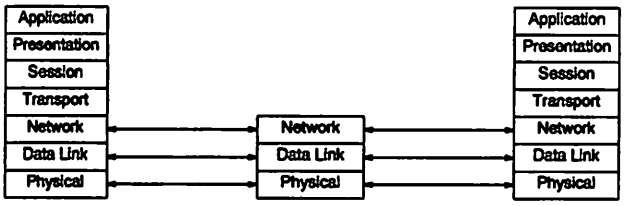
Transparent bridge:
- operates at the ISO data link layer
- networks operate as if they are a single network
- frame store-and-forward device
- verifies checksums
- does not regenerate checksums
- conditionally forwards frames
- protocol independent
- end node transparent
- usually swappable

Source Route Bridge



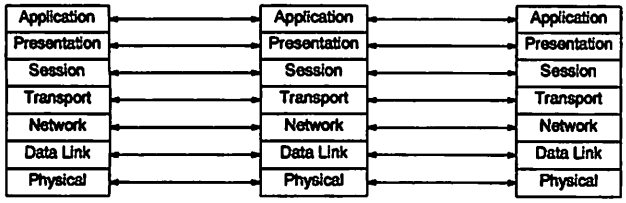
Source route bridge:
- operates at the ISO data link layer
- path in packet header
- at data link level, networks operate as if they are separate networks
- at protocol level, networks operate as if they are one network
- frame store-and-forward device
- verifies checksums
- regenerates checksums
- conditionally forwards frames
- protocol independent
- not end node transparent
- must be configured

Router



Router:
- operates at the ISO network layer
- networks operate as separate networks
- frame store-and-forward device
- verifies & may regenerate checksums
- conditionally modifies frames
- conditionally forwards frames
- not end node transparent
- protocol specific
- "runs" routing protocol software
- must be configured

Gateway



Gateway:
- operates above the ISO network layer
- networks operate as separate networks
- frame store-and-forward device
- translates applications
- protocol specific
- not end node transparent
- must be configured

Hybrid animal

router + bridge in the same box

Brouter:
- operates at the ISO data link layer
- operates at the ISO network layer

- acts as a bridge for selected protocols
- acts as a router for selected protocols

- frame store-and-forward device

Transparent bridge operation, learning

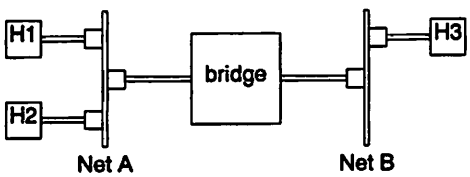
Ethernet packet format:

preamble	dest addr	src addr	length	data	FCS

- runs in promiscuous mode
- looks at source address in MAC frame
  - if address is broadcast address, ignore
  - if address is multicast address, ignore
  - if address is not in database, add new entry
  - if address is on "new" port, entry changed
  - if address is on "old" port, timestamp updated
- database entry:

MAC address	port	timestamp

Transparent bridge operation, forwarding



- runs in promiscuous mode
- looks at destination address in each MAC frame
  - if address is broadcast address
    - forward to all other ports if mode enabled
  - if address is specific multicast address
    - forward to all other ports if mode enabled
- check for address in database
  - if address is not in database
    - frame is sent to all other ports (flood)
  - if address is in database & is received on listed port
    - frame is not forwarded
  - if address is in database & is received on another port
    - frame is forwarded to listed port

Transparent bridge operation, overhead

- all database entries are checked for timeout
  expired entries are flushed
- spanning tree:
  timeouts checked
  if "root" bridge, send out hello packets
  if not, forward hello packets

Router operation; frame selection

- router:
  receives frames addressed to router
  receives broadcast frames
  can receive multicast frames
- end node must:
  know address of router
  know to send data frame to router
- routing information frames often via broadcast
- when frame is received
  checksum is verified
  MAC header removed

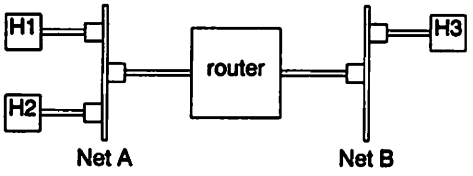
Router operation, path determination

- if frame contains routing information
  frame passed to routing process

- aim of routing process is to create next-hop table
  list of reachable networks and next-hop in path
  next-hop could be:
    destination
    next router or gateway along path

- routing protocol specific mechanism
  many different best-choice procedures
  usually results in single table per transport protocol

Router operation, forwarding



- destination node could be on attached network
- router could know route to network
- destination could be on unknown network

- if on attached network
  frame sent directly on network

- if route to network known
  frame sent to next router in route

- if network unknown and router has default route
  frame sent to default router
- if network unknown and no default route
  frame discarded
  message may be returned to source

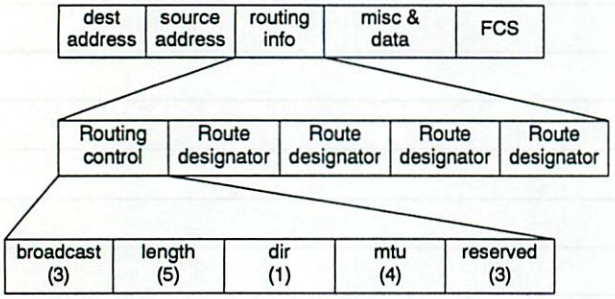
Router operation contd.

- *MTU mismatch*
  - if maximum frame size on output network
    - smaller than input frame
  - frame must be split up for transmission
    - called "fragmentation" or "segmentation"

- datagram lifetime
  - Time to Live (TTL) in IP
    - used to catch loops
  - TTL field decremented by router
  - if turns to 0
    - frame discarded
    - message may be returned to source

Source route bridge operation

- token ring frame format



- look at routing data in MAC header
- look for own address in route designators
  - if own address missing, packet discarded
- forwards packet based on next route designator

- route designator contains:
  - 12 bit LAN segment number
  - 4 bit Bridge number

- special procedure for end station to get path

Source route addressing modes

- null
  - destination on same LAN segment
- nonbroadcast
  - destination on different LAN segment
  - path inserted into header
  - bridges use path to direct packet
- all-routes broadcast
  - bridge address added to path in header
  - bridges will forward packet to all ports
    - unless network # already in path
  - will get multiple copies on each LAN segment
    - one copy for each path to LAN segment
- single-route broadcast
  - uses Spanning Tree to configure network
  - one copy of packet gets to each LAN segment

Source route path discovery

- on new connection source sends out "discovery" packet
  (aka "explorer" packet)
  - sent using all-routes broadcast mode
  - packet will travel along all paths to whole network
  - each bridge adds its own address to header path
- destination will receive one packet for each path
  - destination returns all received packets using routes
  - source chooses which route to use

Combination bridges

- mixed media bridges
  - token ring to Ethernet
  - Ethernet to FDDI
- description:
  - integrates discovery packet concept
    - with broadcast nature of Ethernet
  - looks like SR bridge to TR side
  - looks like transparent bridge to Ethernet
- operation
  - maintains two databases
    - Ethernet addresses
    - TR addresses & SR path information
  - monitors Ethernet for packet source addresses
  - TR database updated when packet set to Ethernet
  - timeouts on database entries

Combination bridges, features

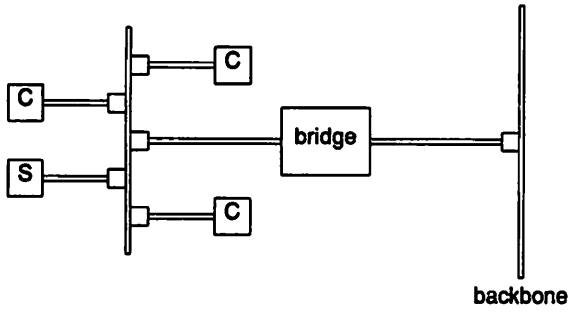
- protocol specific
  - must re-encapsulate some protocols
  - different MAC packet formats
  - different MAC address formats
- MTU problem
  - Ethernet - 1518 octet max
  - 4MB TR - 4K octet max
  - 16 MB TR - 17.8K octet max
- must be configured

Bridge Applications

Where Bridges are best
(Transparent Bridges)

Simple cases:

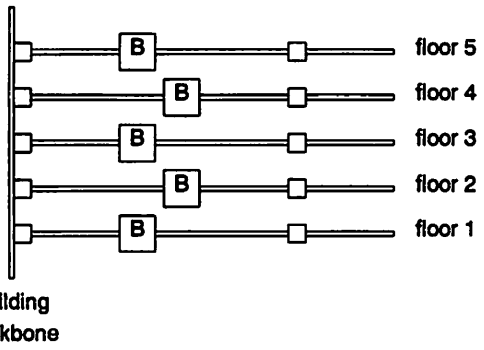
- functions as traffic isolating repeater



- isolate data concentrations
  - workstation clusters
  - VAXclusters
  - disk sharing groups
  - RPC clusters
  - Novell servers and clients

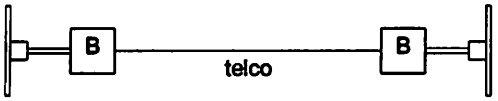
Simple cases, contd.

- isolate floors in a building



- some minimal security
  - isolate sensitive data
  - add simple filters

Simple cases, contd.



- connect two sites
  - small remote net via slow line
  - encrypt public data stream
- many protocols on small net
- small net with limited management support
- unroutable protocols required
  - LAT
  - MOP
  - 802.1 management protocols

Judgement calls:

- many protocols on large net
- minimize management required
- timing dependencies in protocols
  - IPX
  - LAT
- connect buildings together

Bridge advantages

- simple to install and set up
- swappable in most applications
- good performance/cost ratio
- protocol independent
- network seen as a single LAN
- filter at hardware level
- transparent redundant connections
- much less management required
  under normal conditions
- much less expertise required
  to set up and run

Bridge disadvantages

- no or proprietary management
  SNMP on the way
- most have unauthenticated management
- multiport devices rare
- protocol independent
- network seen as a single LAN
- cannot (must not) isolate broadcast/multicast
- most filter only at hardware level
- much more management required
  under abnormal conditions

Router Applications

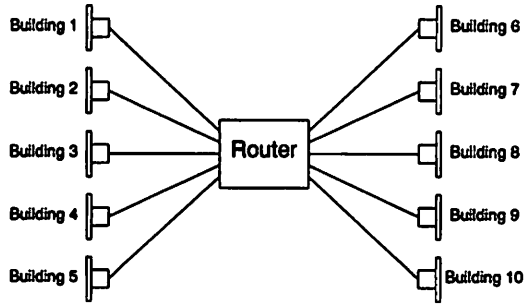
Where Routers are best

Simple cases:

- more than maximum nodes on protocol
  - > 253 in IP net
  - > 1023 in DECNET
  - > ~64 in LocalTalk net
- complex filtering requirements
- medium security
- connection to regional or national tcp/ip networks
- only routers available for network technology
  AppleTalk to Ethernet
- distributed authority

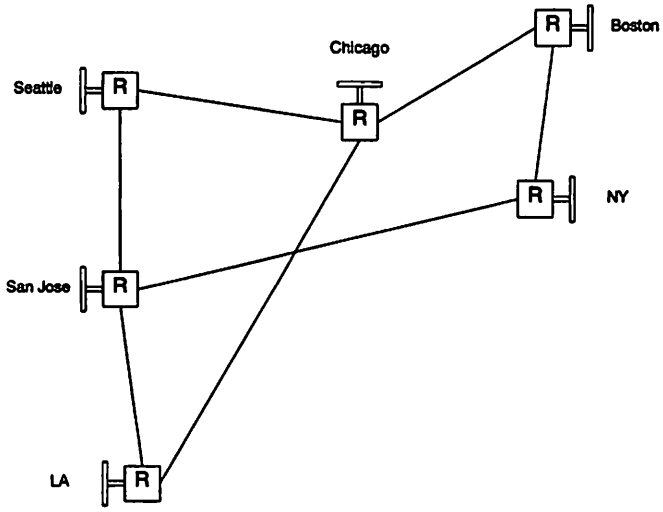
Judgement calls:

- connecting building nets together



Judgement calls, contd.

- regional or national multi-protocol nets
  if single enterprise



Router advantages

- OK performance/cost ratio
- protocol dependent
- network not seen as a single LAN
- filter at protocol level
- good, standard management (SNMP)
- multi-port devices common
- isolates broadcast/multicast
- isolates adminstrative zones
- same difficulty of management in normal and abnormal conditions

Router disadvantages

- protocol dependent
- requires expertise to set up
- requires expertise to manage
- not swappable
- initial installation disruptive

The rest

is

religion

(or product line)

Network Design Factors

can networks be designed?
or do they just grow?

Factors in data network design

- statutory and technological limitations
- usage patterns
- physical coverage required
- security required
- reliability required
- performance required
- applications present
- current environment
- transport protocols required
- resources available

- determine:
  - media selection
  - network layout
  - interconnect device selection
  - future flexibility
  - service guarantees

Statutory and technological limitations

legal, electrical, and protocol limitations

- national electrical code
  - must ground cables within each building
  - Ethernet coax can only be grounded in one place
  - therefore, Ethernet coax cannot be extended
    - between buildings
- network specific limits
  - max length for media characteristics
    - Ethernet or FDDI max distance
  - max latency for physical layer timing
    - max number of repeaters
  - max number of nodes on network segment
    - Ethernet, AppleTalk
- protocol specific limits
  - max latency for protocol function
    - LAT
  - consistent delay required by "lock-step" protocols
    - IPX (soon to be fixed)

Usage patterns

who is doing what, where

- workstation clusters
  - need to isolate load if heavy usage
- distribution of clients for disk server
  - can't isolate if server & clients are spread
- heavy traffic between two sites
  - big pipe needed
- wide spread heavy traffic
  - big backbone needed

Physical coverage required

where is here, where is there, and how
do you get between them?

- physical layout
  - everything in one place
  - spread out
  - all along one road
- interconnection pathways
  - daisychain
  - star(s)
  - ring(s)
  - mesh
- interconnection distances
  - <500 m
    - do it yourself
  - >500 mi
    - call a telco

Security required

- email to someone else's "so"
  - embarrassing but not terminal
- student records
  - legal requirements
  - fun loving students
- DOD weapons research
  - come with DOD regulations
- patent records
  - legal requirements
- student records
  - legal requirements
- sources for Nintendo
  - !!!

Reliability required

how important is it to have the net working?
    lessons to learn from AT&T!
        dead cows & training operators

- clinical patient care
    redundancy, redundancy (& a very good lawyer)

- accounting systems that produce your paycheck
    high profile

- all you ever do is read net.singles
    no problem with a single path

Performance required

so - how fast do you want to do it

- EMail to Albuquerque
    periodic dial-up

- keeping up with net news (~50MBytes/day)
    Ethernetish

- real time rotation of CAT scan information
    FDDIish

- Connection machine frame buffer
    UltraNetish

Applications present

- delay-insensitive, loss-sensitive
  email & file transfer
- delay-sensitive, loss-insensitive
  digital voice and video
- delay-sensitive, loss-sensitive
  interactive graphics, interactive computing
- regular load
  terminal traffic
- bursty load
  distributed computing

Current environment

where in the networking process are you

- blank slate - nothing there now
  you must be living right
- isolated islands built up
  melding cultures will be biggest problem
    e.g. what email package to use
- some/a lot of interconnection
  was interconnection done by you?
    great!
  was it done by 1 other group/person?
    not so bad
  was it done by different groups as the need arose?
    "may you live in interesting times"

Transport protocols required

never met a protocol you didn't like?

- TCP/IP only, DECnet only
- un routables (LAT)
- lock-step (IPX)
- little bit of this, little bit of that
- don't know

Resources available

are gurus a dime a dozen?

- funding sequencing
  - cash up front
  - cash when connecting group
- what kind of support center can you afford?
  - little or none
  - big & brash
- is there a real central authority?
- "every tub on it's own bottom"

Ideal network

- sob's ideal network

  (not what he has, though)

Ideal network, topology

- fiber backbone connecting a few secure "backbone" node locations
- single mode fiber for future
- redundant power and UPS for nodes
- redundant fiber pathways between nodes
- separate management net connecting nodes
- fiber from nodes to buildings
- extend building net to backbone nodes
- separate monitoring network, able to be switched to any building net

- unity in buildings
- cascaded concentrators in buildings
- every node on own port of concentrator

- all external net connections directly to backbone

- redundant connections between NOC and backbone nodes

Ideal network, management

- no "transparent" devices
- common management protocol for all devices
- authenticated management via separate pathway
- management agents in all remotely accessed hosts
- management agents in all hosts offering network services

- all external net connections under control of NOC

- all authority resides in NOC
- NOC accounts on all remotely accessed hosts

- few protocols
- forgiving protocols

Ideal network, security & privacy

- user authentication at all entry points to network
- hosts reject all non-authenticatied access requests
- user authentication for all services
- services reject all non-authenticatied access requests
- service authentication for all services

- segmented traffic, only packets for host sent to host

- NOC managed person_name to email_address mapping
- NOC managed post office servers
- all interactive and email traffic encrypted

The network, the user's view

There is no network from the user's point of view. There are only services.

The goal of all network design and management is to preserve this misunderstanding.

Connecting Your Corporation Using the Internet

I don't even know what an internet is, now you want to talk about the Internet!

Scott Bradner
Harvard University(HRV)
sob@harvard.edu

What are we talking about anyway?

- *an* internet
  local (to one company) network of networks

- *the* Internet
  the big picture

What's out there

- a good chunk of the cooperative technical world
- > 700,000 computers directly connected
- > 500,000 more reachable
- > 5,000,000 users
- > 100 GBytes PD software & information
- > 3,000 mailing lists and newsgroups
- gateways to commercial email systems

How do I find it?

1) not easily
2) ask a friend
3) look at lists
4) watch mailing lists
5) use archie
6) get tool

newsgroups
- harvard has > 2300 (81KB file)
- list on **`hsdndev.harvard.edu`** (128.103.202.40)
  filename: **`pub/stuff/active`**

mailing lists
- Dartmouth has list of > 2300 (.5MB file)
- list on **`dartcms1.dartmouth.edu`** (129.170.16.19)
  filename: **`siglists/listserv.lists`**

Anonymous FTP

- File Transfer Protocol (FTP)
  TCP/IP file transfer program

- normally requires account on target host

```
ftp hsdndev.harvard.edu
 Connected to hsdndev.
 220 hsdndev FTP server (Version 5.4 Sat Aug 31
  17:59:14 EDT 1991) ready.
 Name : fred
 331 Password required for fred.
 Password: *****
 230 User fred logged in.
```

- gets interactive access to host, restricted command set
  same system view as normal user login
    dir - get listing of current directory
    cd xx - change directory to xx
    get xx - retrieve file xx
    put xx - put file xx onto remote system
    help - print list of implemented commands

- can setup special account called *anonymous*
    ftp using this name and user's own name as password
      (sometimes requires "guest" or an email address)
    login with same command set but restricted view

Archie

files database
- resource discovery tool
- tracks ~900 anonymous FTP sites
- currently lists 1,600,000 files
- represent > 90 GB data
  > 90,000,000,000 bytes
- docs
- software
- databases

whatis database
- descriptions of software packages and information
- currently ~3,500 descriptions

Archie use

how to use archie

- telnet to **archie.mcgill.ca** (132.206.2.3)
  - login as *archie* - no password
  - type *help* for help
- email to **archie@archie.mcgill.ca**
  - single word *help* as subject or body
    - to get operational instructions
- get archie client
  - from **archie.mcgill.ca** in archie/clients
    - via anonymous ftp
  - sends query to server, much easier on server
  - clients for:
    - C (berkeley sockets), ms-dos, VMS
    - also X-window version

Archie example

example user interface to UNIX client

- archie *string* - find string in files database
  - exact match
- archie -s *string* - find string in files database
  - substring match - case insensitive

UNIX client on my home machine

```
hsdndev> archie hsdn.rfi

Host hsdndev.harvard.edu

 Location: /pub
  DIRECTORY dr-xrwxr-x  512  Oct 31 08:09 hsdn.rfi

Host minnehaha.rhrk.uni-kl.de

 Location: /pub/harvard
  DIRECTORY drwxrwxrwx  512  Dec 18  1990 hsdn.rfi

hsdndev>
```

WAIS

Wide Area Information Server (WAIS)
- context search of on-line information
- > 150 public servers
  - specialized data
    - Supreme Court decisions
    - cookbook
    - Bible, Koran
    - weather

to use WAIS
- telnet to **quake.think.com**, login as *wais*
  - no password
- get client - can save results locally
- clients from **think.com** (131.2390.2.1)
  - in **public/wais** for anonymous ftp
  - clients for:
    - UNIX (shell, emacs & X-windows)
    - Mac, NeXT, ms-dos, Motif, RS/6000, SunView, VMS

- Mac client quite nice
  - cut & paste including graphics

Internet Resource Guide

- list of resources with short descriptions
- NSF funded
- retrieve from **nnsc.nsf.net** (128.89.1.178)
  - in directory **resource-guide**

- resource-guide-help

```
Request: resource-guide
Topic: resource-guide-help                    2/3/92
Date: 3 Feb 92
Subject: FTP Help for the Resource Guide

             FTP Help for the Resource-Guide
FTP users:
Please see file with the pathname
   '/resource-guide/index-resource-guide'.
From the top-level directory,
        cd resource-guide
        get index-resource-guide
For over-all help with the NNSC Info-Server, see the
file with the pathname 'help' (in the top-level
directory and also in the second-level directories
```

Internet Library List

- list of Internet accessable library catalogs
- with instructions for use

- > 100 library catalogs
  world-wide
  some for free, some for fee
- > 20 campus-wide information systems

- retrieve from **`hsdndev.harvard.edu`** (128.103.202.40)
  in directory **`pub/stuff`**

Tools

e.g. InterNavigator
- menu driven system to access Internet resources

The Architecture of the Internet

General Concepts

The Internet is the collection of interconnected networks that run the TCP/IP protocol suite.

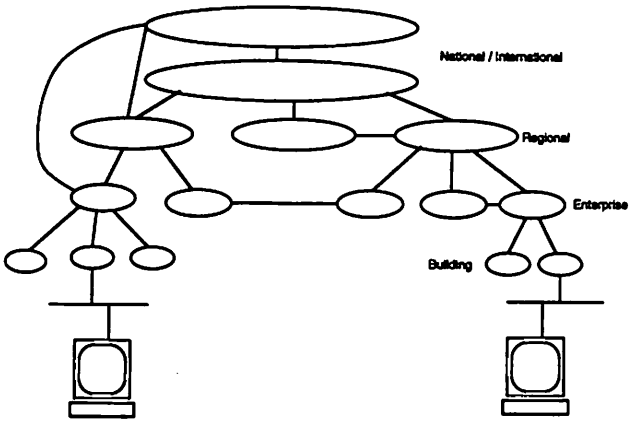
(soon to include other protocols)

The Internet:

starts at desktop
then to building LAN
then to university/enterprise network
then to regional net
then to national/international backbone
then to regional net
then to university/enterprise network
then to building LAN
then to another desktop

- has multiple national backbones
  run by different authorities

Internet



Backbones

Federal

- NSF - NSFNET
- DARPA - DRI (Defense Research Internet)
- NASA - NSI (NASA Science Internet)
- DOE - ESnet (Energy Science Network)
- DARPA - MILnet

Private

- AlterNet (uunet)
- PSInet
- ANS

Future

- NREN - National Research and Education Network

NSFNET

RFP won by IBM, MCI & Merit
- IBM - hardware and software
- MCI - communications links
- Merit - Management

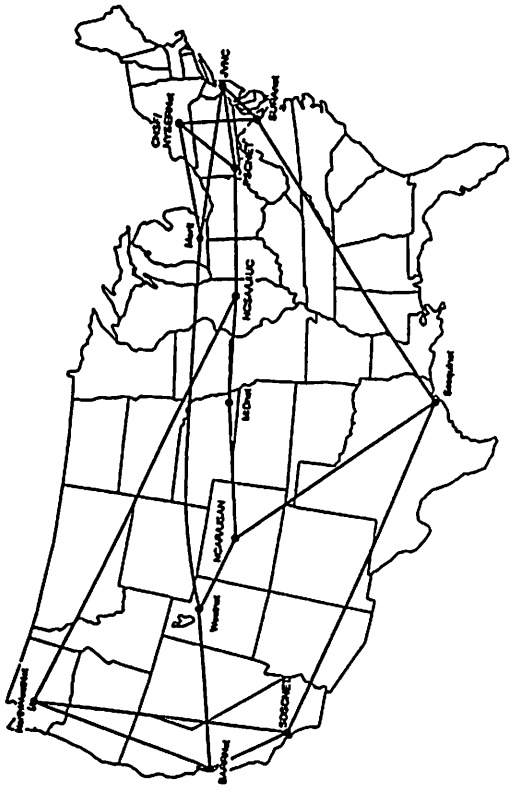
old design
- T1 (1.544Mb/sec) links connecting switching nodes (NSS)
- all nodes other than MIDnet have 3 links

new design
- T3 (45 Mb/sec) links connecting swiching nodes in MCI pops (CNSS)
- T3 link to customer site (ENSS)

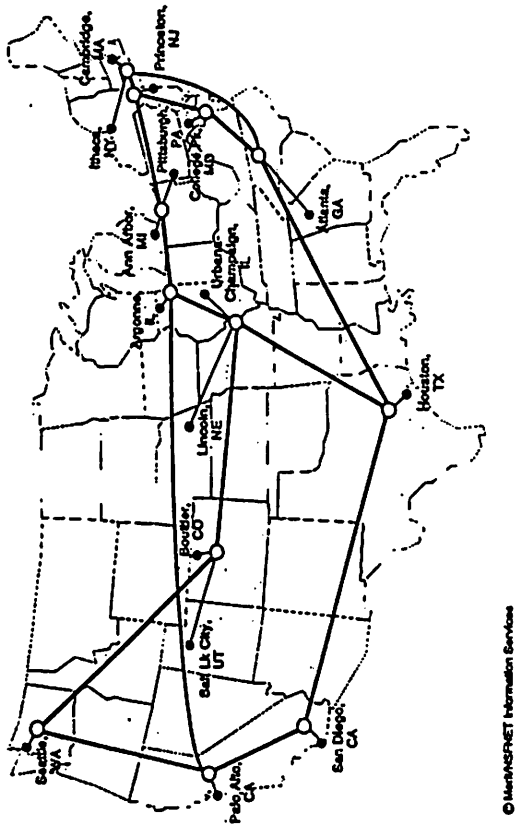
Management
- NOC at U of Michigan
- "7 x 24" coverage
- SNMP monitoring

New organization
- management contracted to ANS
- ANS now contracts MERIT for people

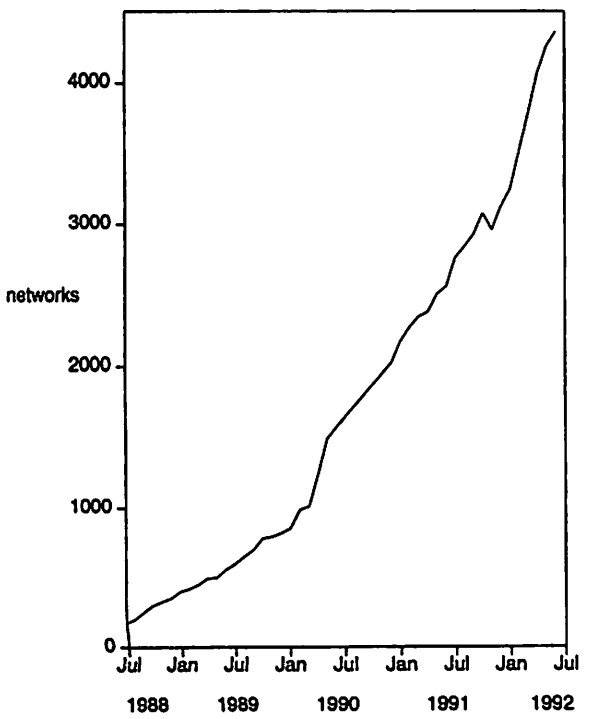
NSFNET: T1 network



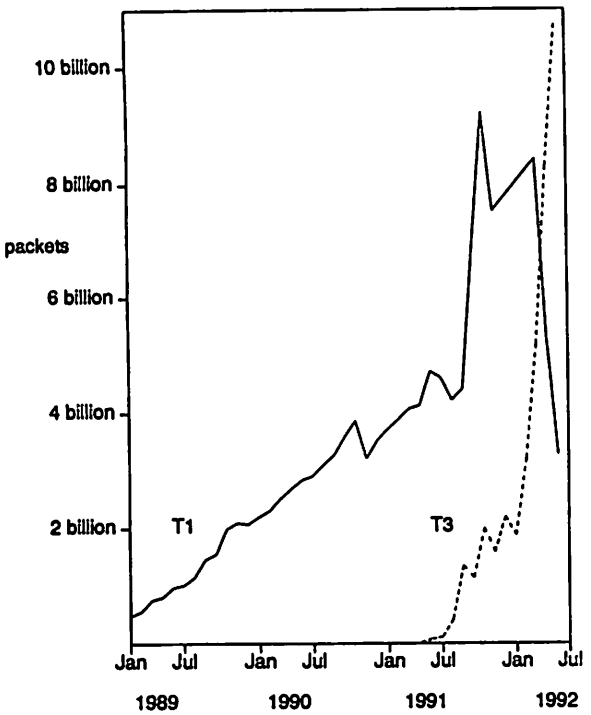
NSFNET: T3 network



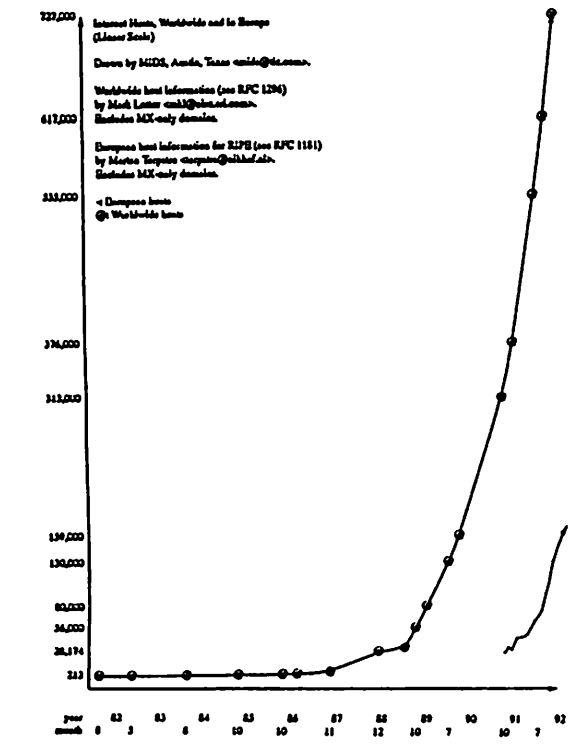
NSFNET: connected networks



NSFNET: traffic



NSFNET: hosts



NSFNET: NSS design

- old NSS

  located at customer site

  constructed of IBM PC/RTs

  n Packet Switching Processors (PSPs)
  1 for each of the T1 circuits
  1 Packet Switching Processor - Gateway (PSP-G)
  used as a gateway to the regional network
  Ethernet interface
  1 Routing Control Processor (RCP)
  runs SNMP agent
  runs EGP and HELLO
  1 NNSTAT processor

NSFNET: NSS design contd.

- new NSS design

  two parts
  CNSS
  located at MCI POP
  MCI personnel help out

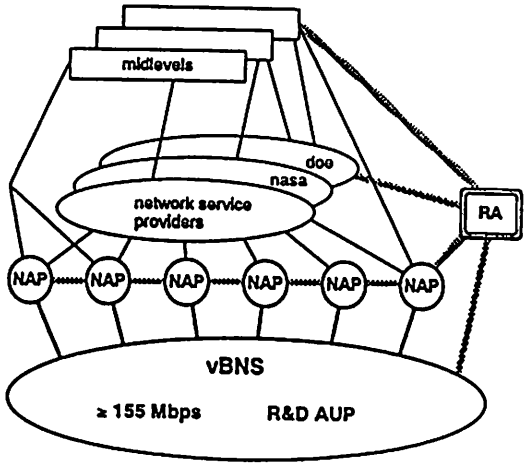
  ENSS
  located at customer site
  Ethernet or FDDI interface

  connected together by 1 or 2 T3 lines

NREN

proposed NREN design

NAPs - no AUP



NSF regional networks

- NSFNET does not provide connectivity to end user or even to campus networks
- NSFNET mission is to provide connectivity between regional networks
- most regionals were started with NSF funds and are associated with supercomputer centers
- the regionals are independently operated
- service plans range from 9 to 5 weekdays up to "7 x 24"

NSF regional networks contd.

- BARRNet
  Northern California
- JVNC
  Connecticut, Rhode Island, New Jersey
- Merit
  Michigan area
- MIDnet
  Nebraska area
- NEARnet
  North East US
- NYSERNet
  New York
- NorthWestNet
  North West US
- PSCNET
  Pennsylvania

NSF regional networks contd.

- SDSCNET
  Southern California
- Sesquinet
  South Central US
- SURAnet
  South East US
- Westnet
  Utah area
- UIUC
  Illinois area
- USAN
  Colorado area

Case Studies

What can one learn from the
trials of others?

Case Study method

- big at Harvard
- by studying what others have done, one can learn and apply lessons.

- cases:
  three Universities

  large corporate, limited protocols
  large corporate, many protocols

  two regional data networks

Harvard University

- university stats:
  - faculty - 1,166 non-medical area
    - 4,626 medical area
  - students - 18,179
    - undergraduate - 6,592
  - staff - 3,894
  - university budget - $1.2B

  (Nobel prize winners - 33
  Pulitzer prize winners - 30
  Endowment - $4.7B
  Graduates that became U.S. Presidents - 6)

- network name:
  - HSDN (High Speed Data Network)

- overall plan:
  - connect building LANs together

- funding:
  - central bank for capital expenses
  - charge departments or buildings

Old Harvard

what we learned from at Harvard

- before the fiber:
  - collection of separate islands
  - local ethernets
  - some connected using serial IP
  - broadband cable used as port selector and
    - PC LAN

- using advent of supercomputer at JvNCC as excuse:
  - 12 buildings connected together with 10MB
    - fiberoptic Ethernet
  - using passive stars (3)
  - Ethernets in most buildings
  - Ethernets connected to f/o with f/o repeaters
  - some connections to DELNIs or single cpus

- "progress"
  - "upgraded" repeaters to bridges
  - added a router to isolate one building
  - used a SUN as a gateway to isolate another

New Harvard

- using new phone system as excuse:
- produced RFI
  (available from hsdndev.harvard.edu)

- design:
  - 7 "backbone nodes"
  - redundant pathways too expensive
  - fibers between backbone node locations
    - 24 mm, 22 sm
  - designed with FDDI in mind
    - can arrange fiber into "ring"
  - routers at backbone nodes
    - each building on seperate router port
  - fibers from node locations to surrounding buildings
    - 10 mm, 8 sm
  - transceiver cable extender or Ethernet
    - extender between node and building LAN(s)

- 1st pass, Ethernet backbone and pair links

New Harvard, contd.

- management:
  - central NOC at Network Services
  - SNMP monitoring
  - provision for separate management network

- protocols:
  - TCP/IP (RIP routing)
  - DECnet, AppleTalk & IPX
  - LAT, NetBIOS
  - OSI sometime
  - other protocols on LANs

- funding:
  - central organization putting in backbone
    - backbone bankrolled by University
    - buildings added upon funds commitment
  - almost all LANs under individual management
    - most installed by building people
  - NOC funding from building access charges

New Harvard, contd.

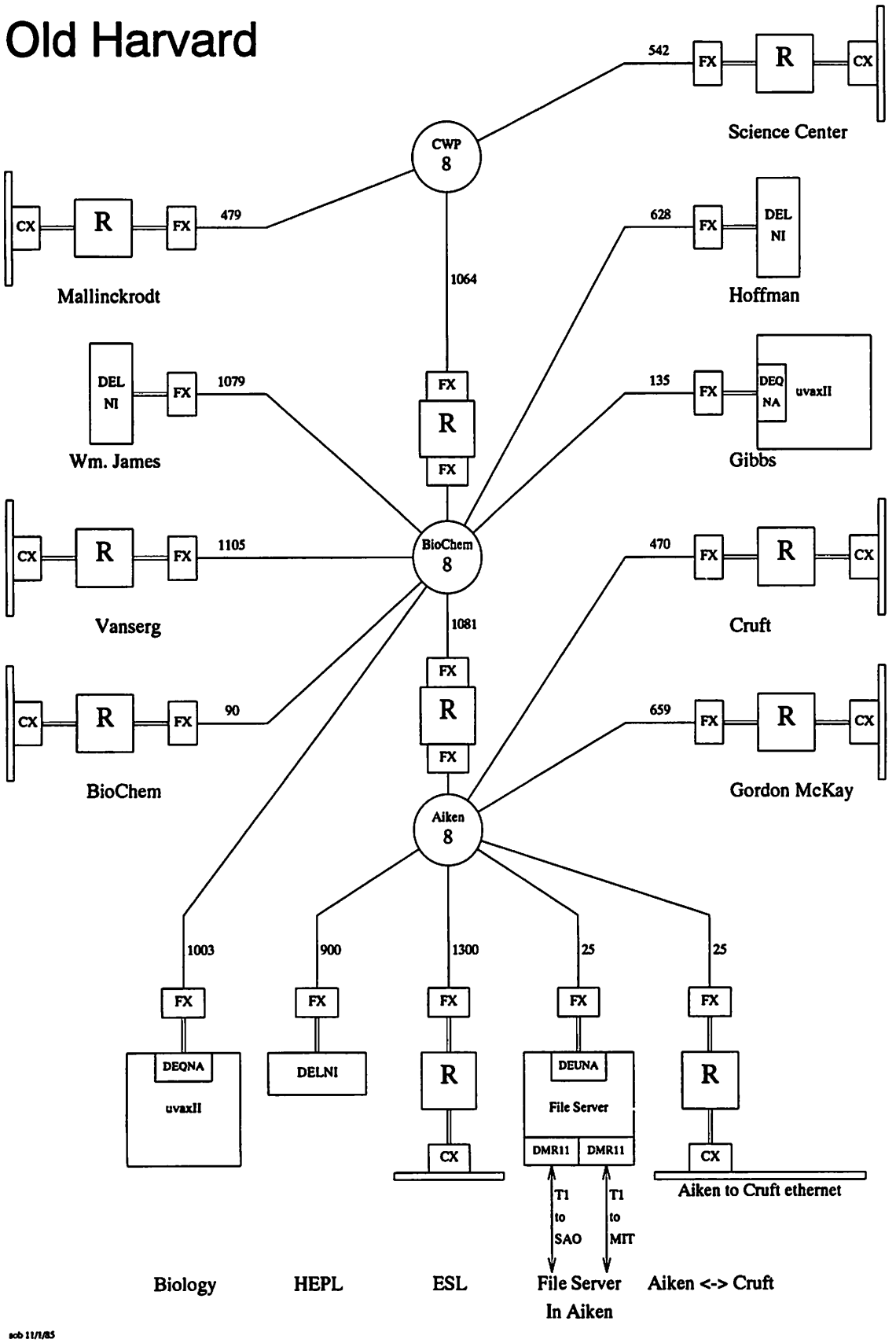
- new phone installation
  using AT&T 5ESS ISDN switch

  almost all new wiring, >400 buildings
  "every pillow" in dorms

  2 4-pair cables to each jack
    "Phone" set and "Data" set of wires
    separate termination at IDF locations
  fiber from MDF to IDFs

- gateways between ISDN and HSDN
  ISDN assync to telnet and rlogin
  LAN to HSDN using 64Kb packet switched X.25
  PC on X.25 "LAN"

Old Harvard



scb 11/1/85

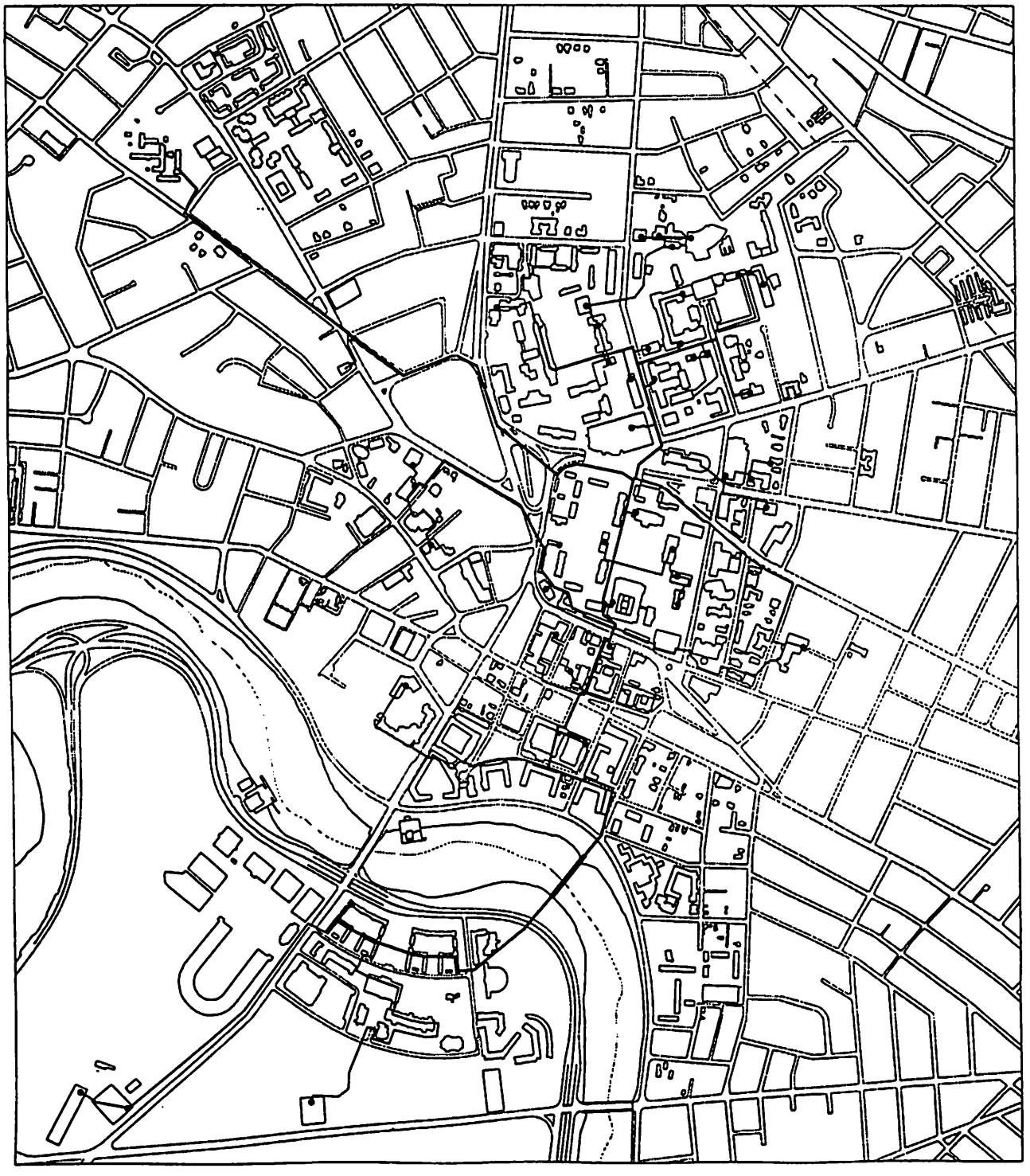
Old Harvard, features

- many existing nets
- put in by many people
- no standards
- much LAT & PCSA
- much AppleTalk
- large PCNET network
- no central NOC

- mainframe computer center "net"
  - ~400 terminals on direct lines & muxes
  - 1/2 for library
  - direct to mainframe via 7171
  - migration to PCs on data network
- batch to mainframe via rscs
- many sync lines for BITNET (rscs)

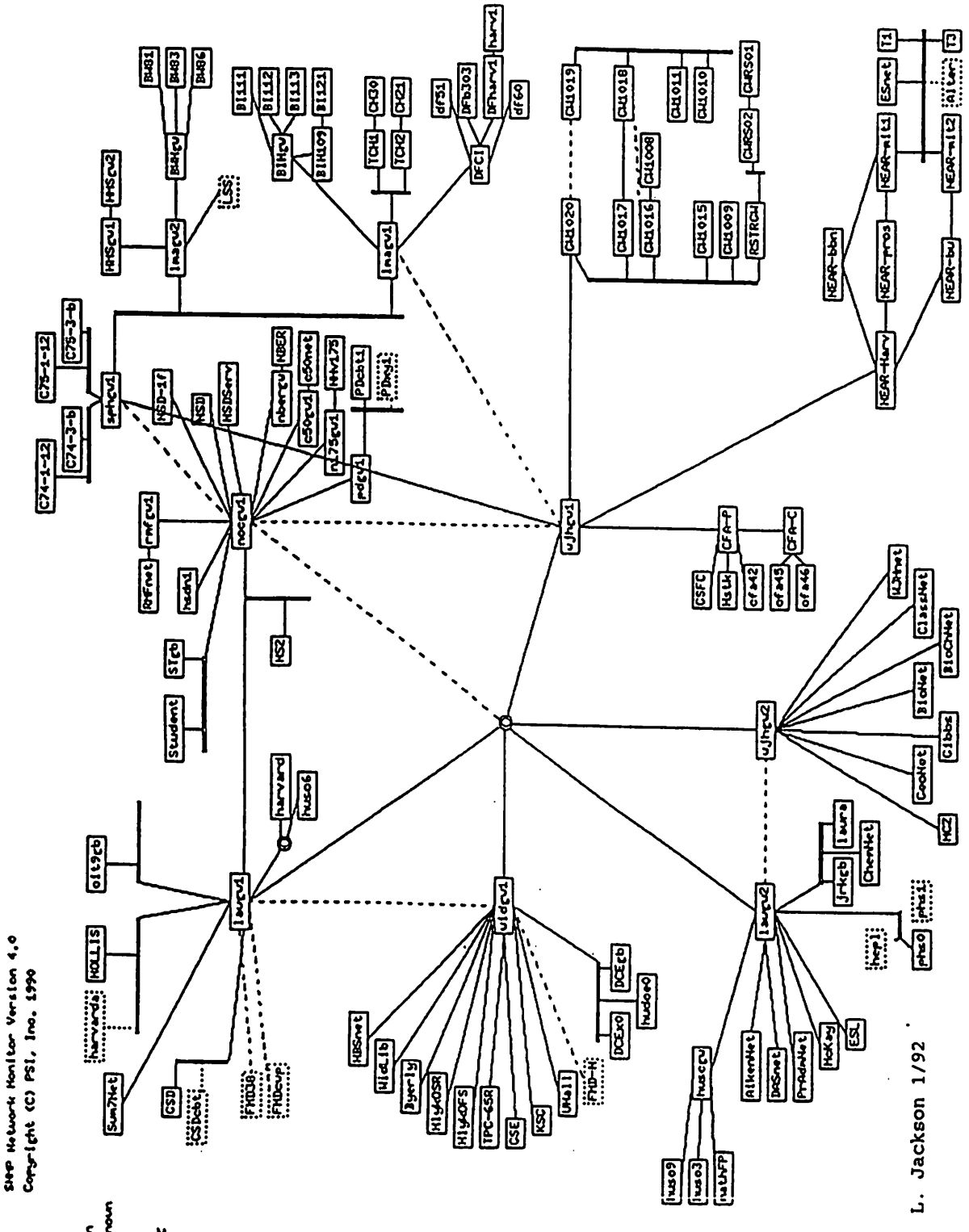
New Harvard

physical



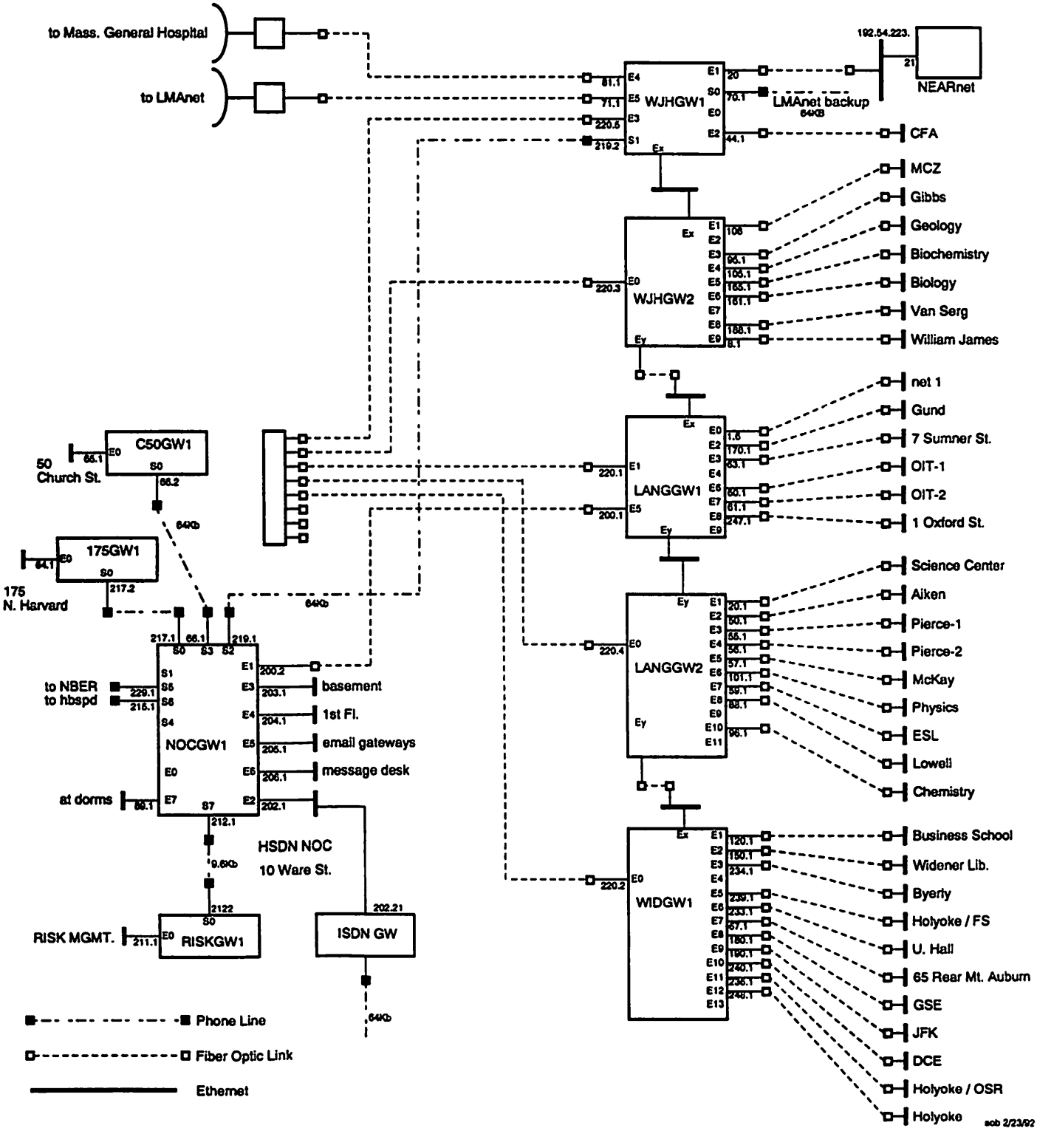
New Harvard

logical



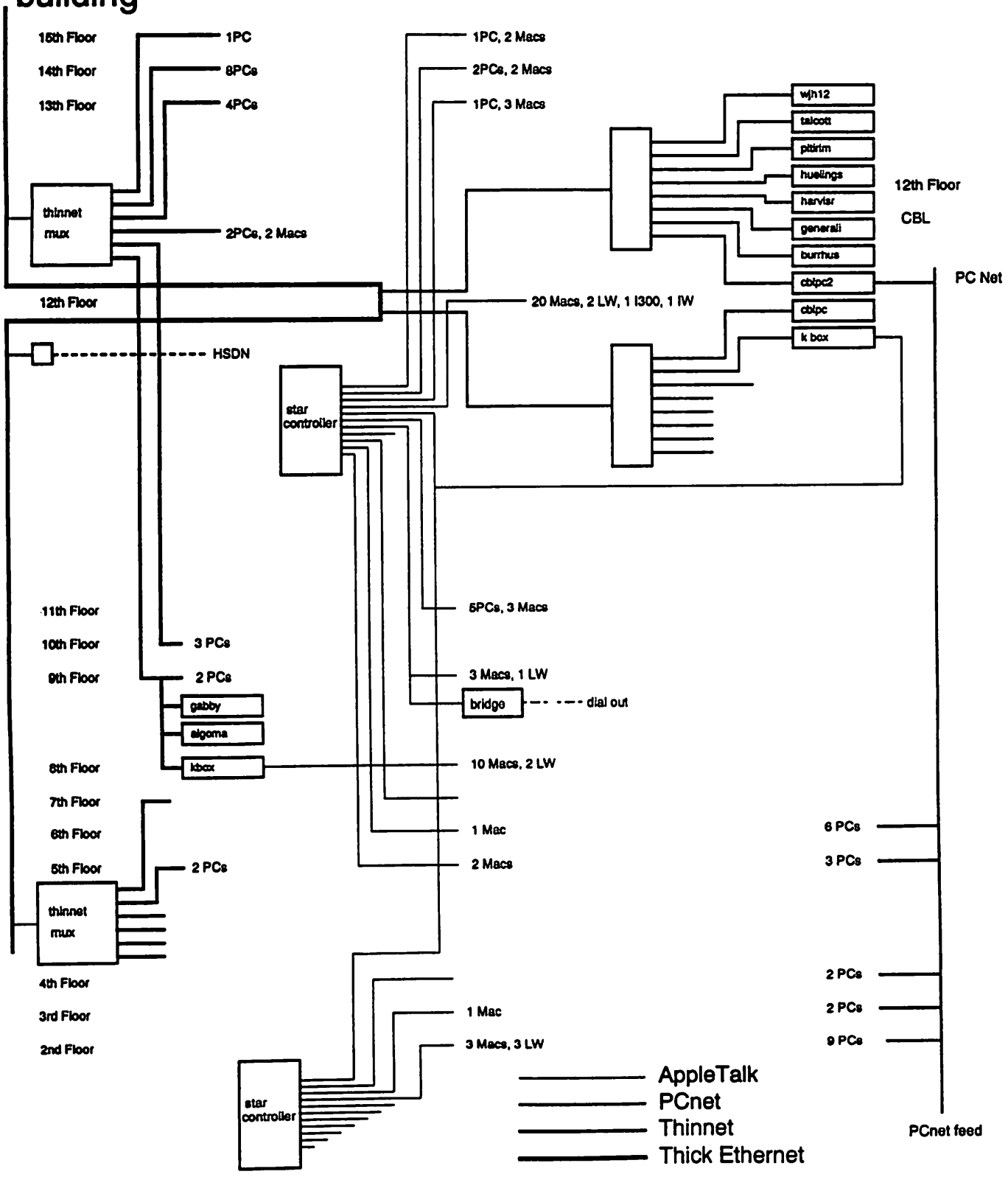
New Harvard

detail



New Harvard

building



Case Western Reserve University

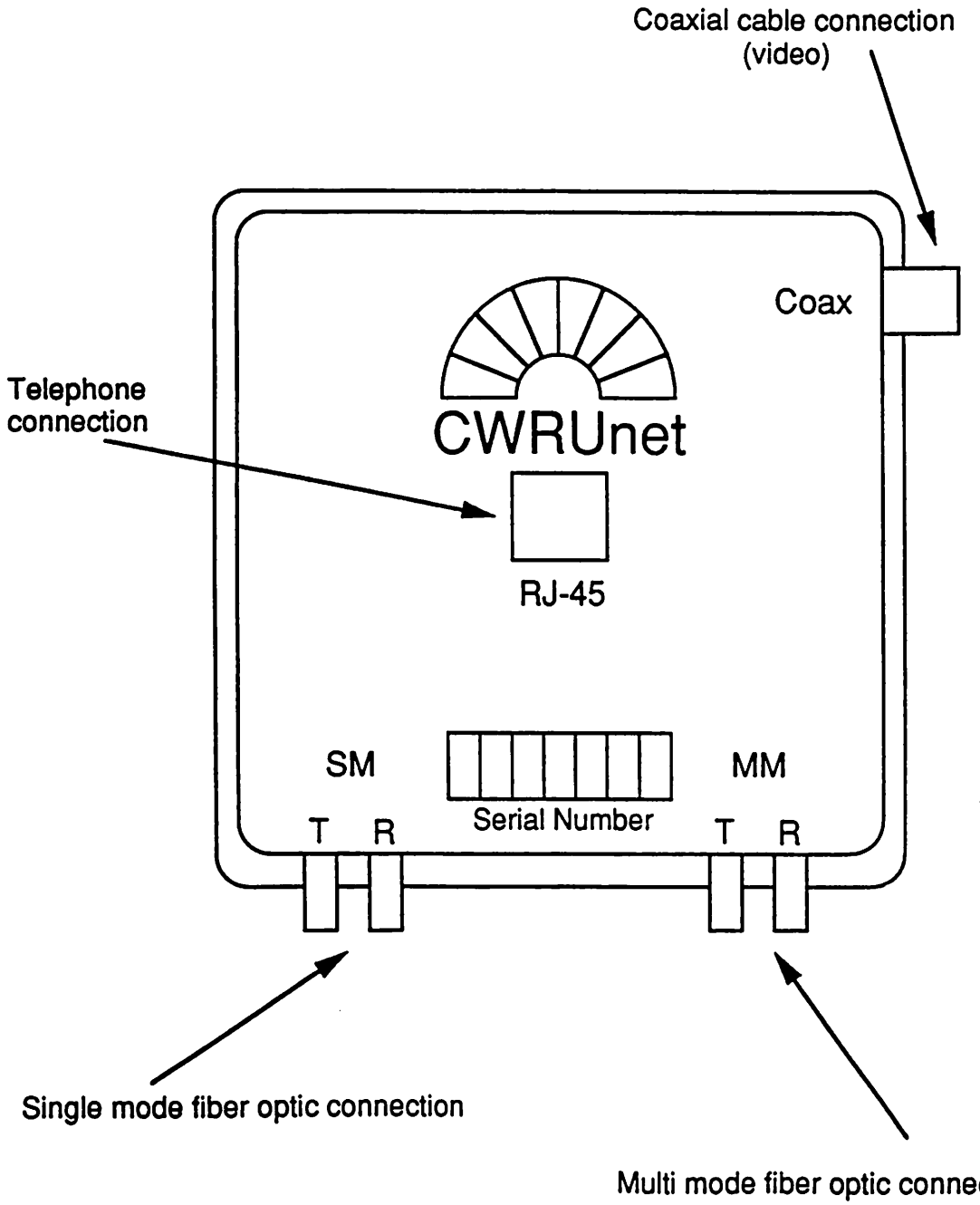
- university stats:
  - faculty - 1,611
  - students - 16,256
    - undergraduate - 5,890
    - other - 10,366
  - staff - 2,219
  - university budget - $266M
- network name:
  - CWRUnet
  - ("crew-net")
- overall plan:
  - network service to every desk & pillow
  - fiber to every jack
  - includes phone and video
  - system also supports environmental controls and building access/security
- funding:
  - central funding
  - networking and computer access provided for "free"

Case Western Reserve University

- physical
  - hub and star system
    - hubs connected with 24mm & 24sm
    - buildings connected with 18mm & 6sm
    - connection to room composite cable + coax
      - 2sm, 4mm, 4 twisted pair
  - initial - 5 hubs, 26 buildings
  - final - 7 hubs, 85 buildings
  - much fiber in steam tunnels (in conduit)
  - new in-ground conduit protected with red concrete
- logical
  - all bridged network
  - only supported protocol - tcp/ip
  - pc and Mac interface cards accessible with SNMP
  - can monitor each port from NOC

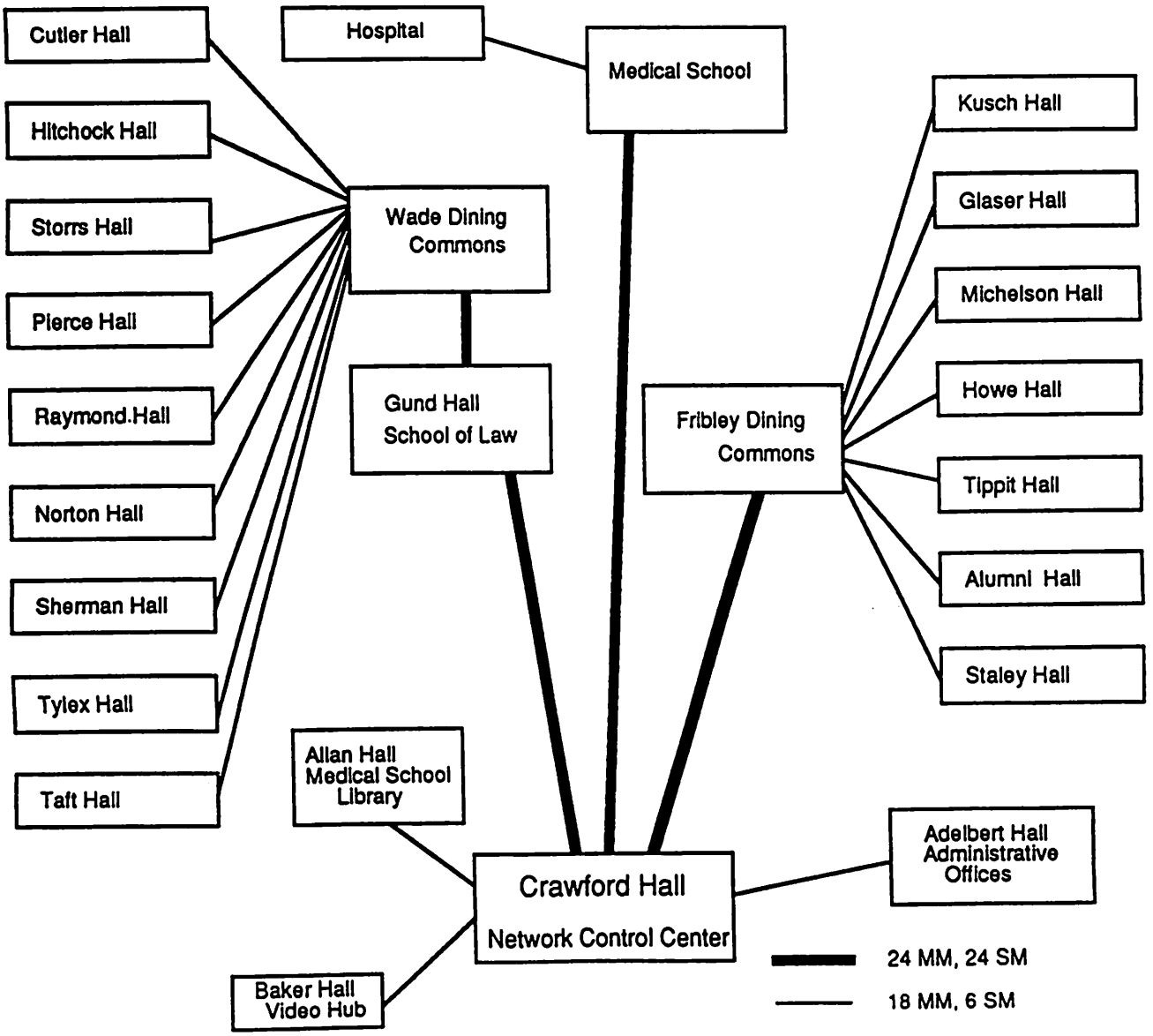
Case Western Reserve University

- faceplate



Case Western Reserve University

topology



Boston University

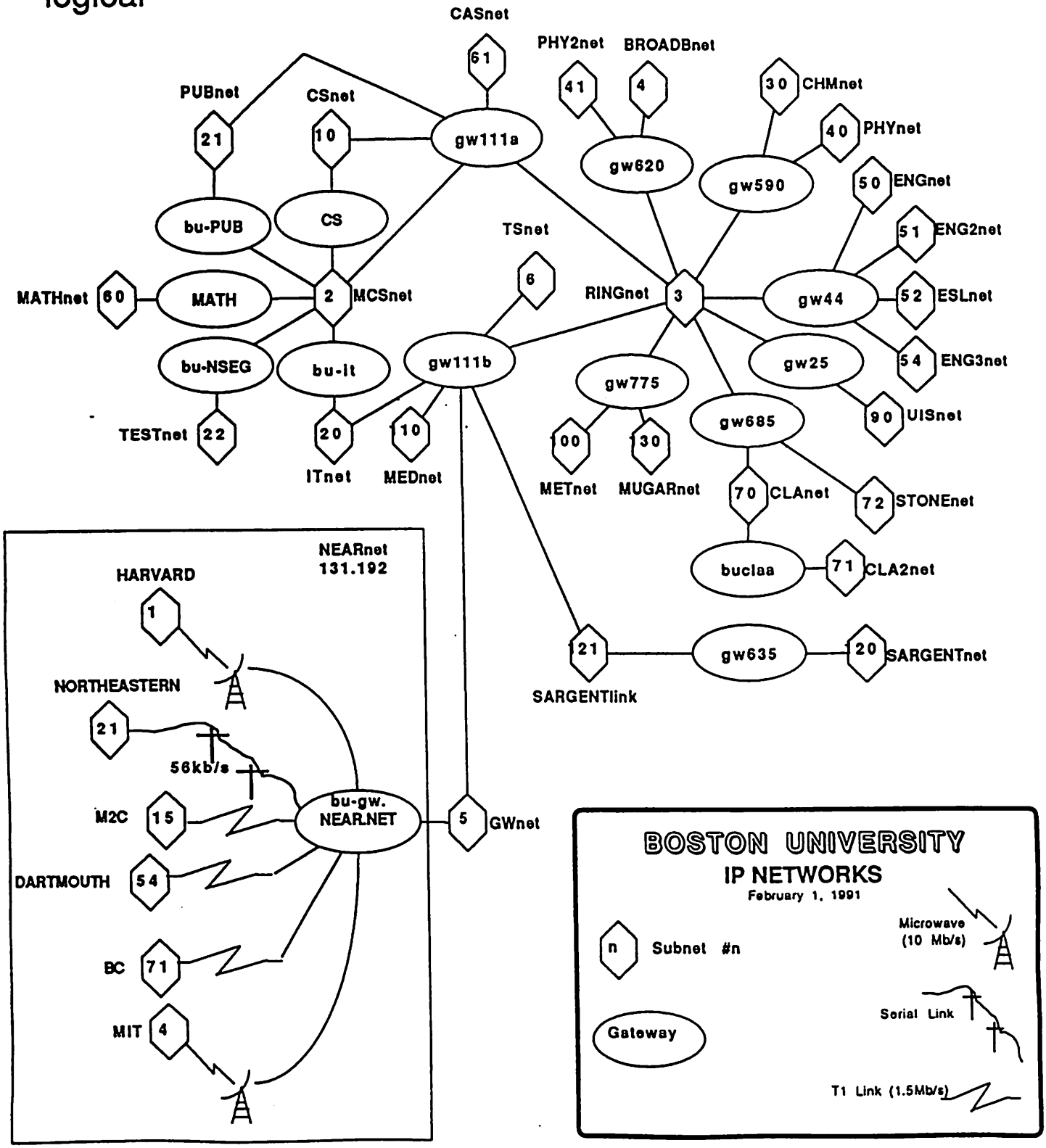
- university stats:
  - faculty + staff - 6,000
  - students - 28,000
  - university budget - $560M
- network name:
  - The Campus Network
- overall plan:
  - provide network connectivity
- funding:
  - central funds augmented by department funds

Boston University, contd.

- design:
  - backbone ring + broadband
    - backbone ring 48mm & 8sm
  - buildings connected to ring with Proteon routers
    - buildings connected with 12mm
- protocols:
  - TCP/IP (RIP routing)
  - DECnet
  - some AppleTalk
- management
  - NOC at Information Services
  - SNMP monitoring

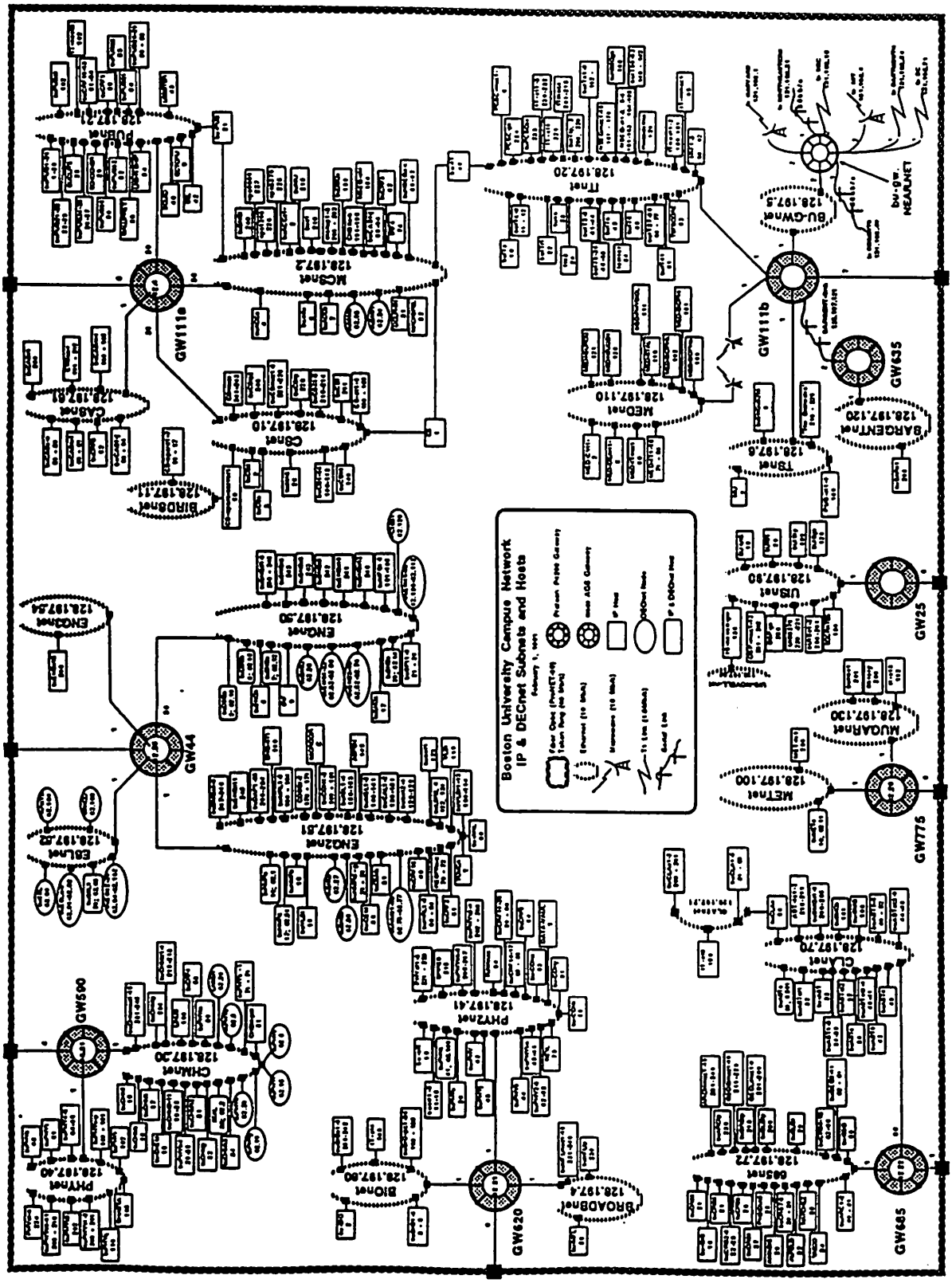
Boston University

logical



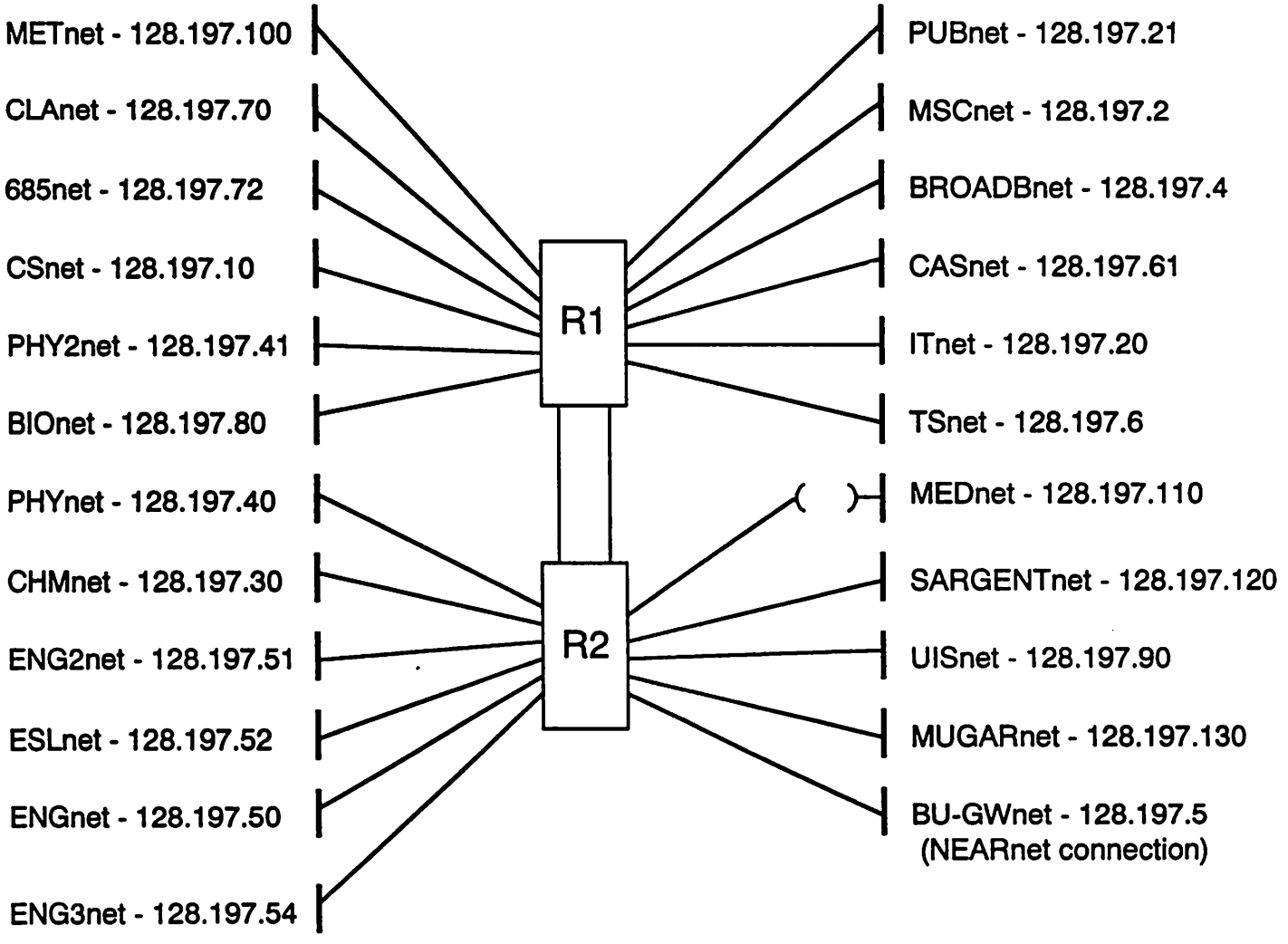
Boston University

schematic



Boston University

new logical



Large corporate, limited protocols

DEC's EASYnet

- company stats: (1990)
  - employees - 125,900
  - locations - 800
  - countries - 66
  - revenues - $12.5 B
- network name:
  - EASYnet, IP EASYnet
- overall plan:
  - provide service to all corporate nodes
- funding:
  - central funding
  - too expensive to collect usage stats
  - want users to see "network as utility"

DEC EASYnet, contd.

- very large corporate network
  - 57,000 DECnet hosts, > 15,000 IP hosts
  - 111,839 email users
  - private, > 320 mi, fiber network in NE
    - single mode fiber
  - >200 T1 links in US, redundant paths
  - hubs in Europe & England
  - mesh design
  - >200 IP subnets reachable, 600 assigned
- strong central management
  - regional & local responsibility
- protocols
  - DECnet & LAT
  - seperate TCP/IP network
  - AppleTalk tunneled in DECnet (world wide)

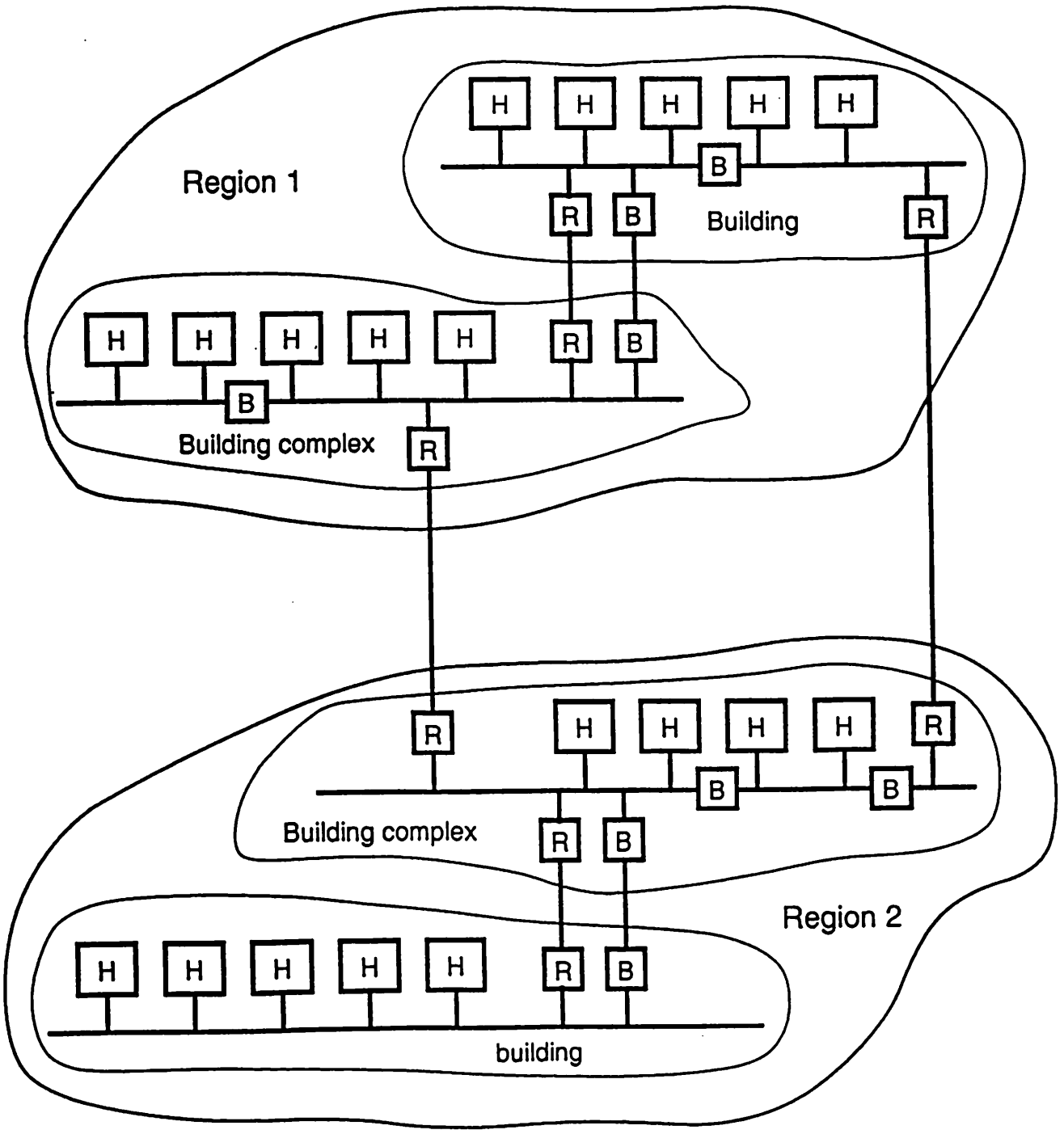
DEC EASYnet, misc.

DECnet EASYnet
- regional "Ethernets"
  Segments connected with bridges.
- LAT within regions
- some within region DECnet connections
  with DECnet routers, only LAT traffic
  on bridged links
- regional nets connected with DECnet routers

IP EASYnet
- global connectivity
- 348Kb links in U.S., 128Kb Trans-Atlantic
- global latency < 700 ms
- availability > 99%
- OSPF routing on backbone
- default route into subnets

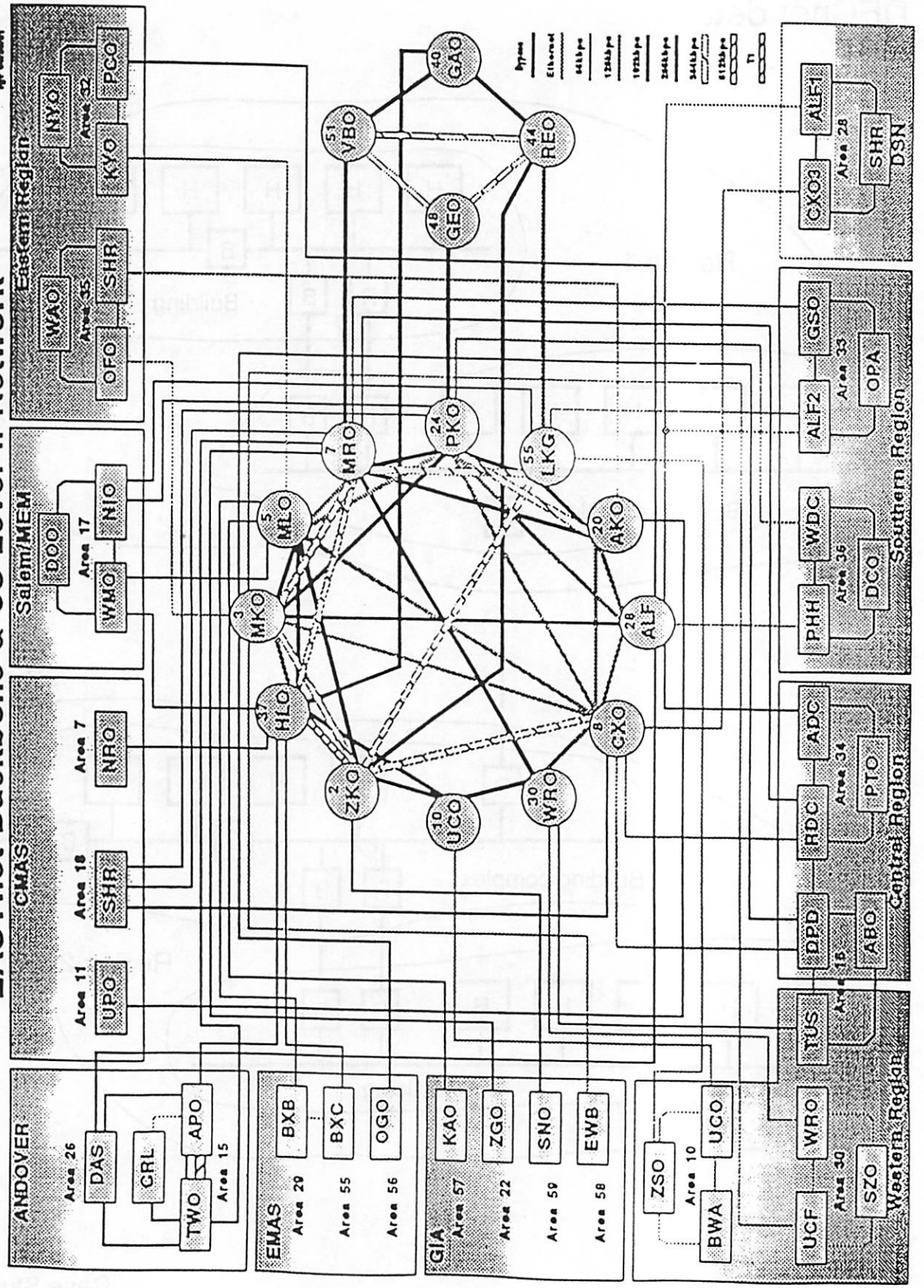
DEC EASYnet

DECnet detail



DEC EASYnet, contd.

logical

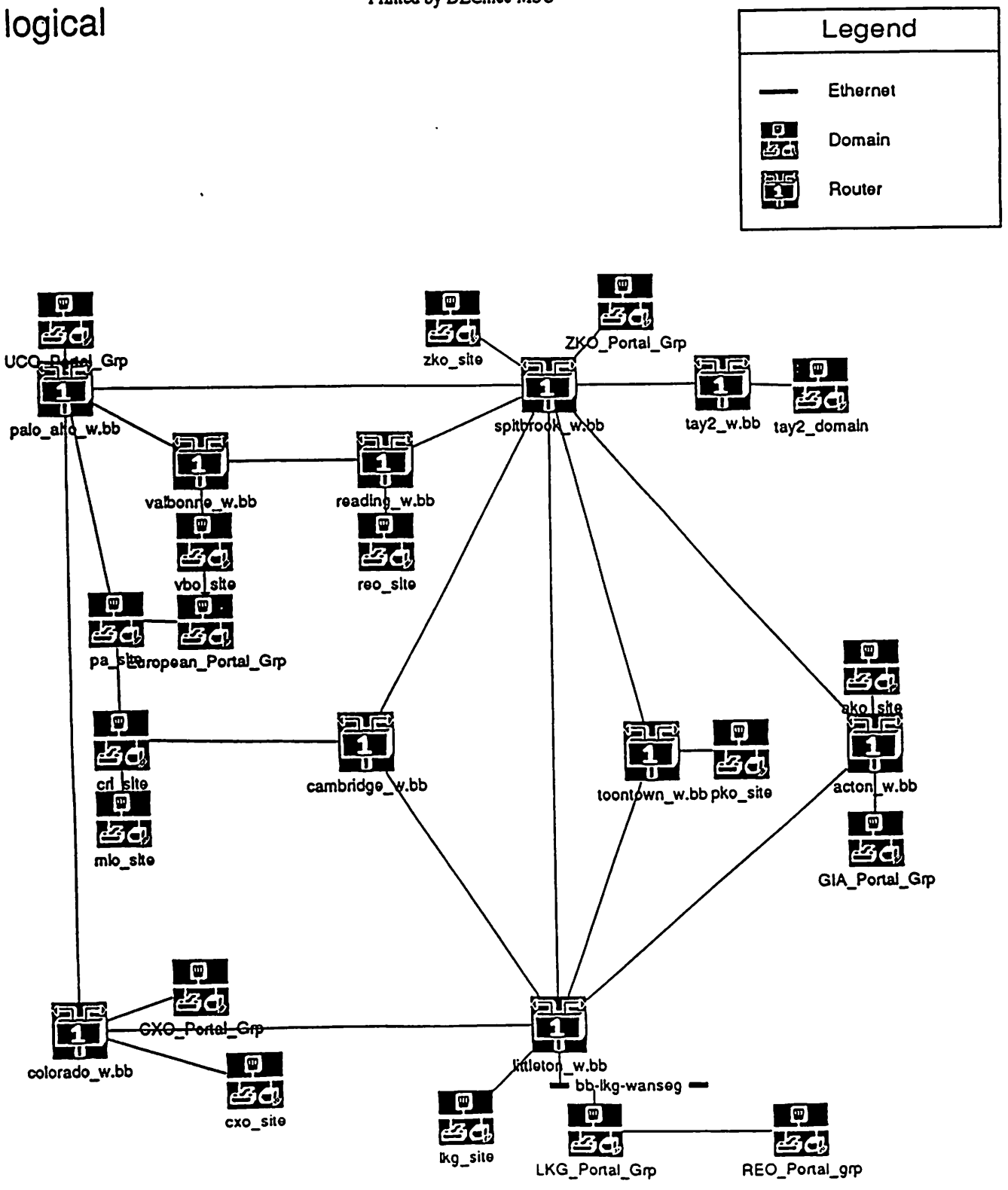


DEC IP Easynet

Map of Root

Printed by DECmcc MSU

logical



Large corporate, many protocols

- unnamed national company
- corporate stats:
  - employees - > 50,000
  - locations - ~100
  - revenues - > $1B
- network name:
  - -
- overall plan:
  - link all corporate sites
  - provide access to applications
- funding:
  - central funding

Large corporate, many protocols, contd.

- sites:
  - home office
  - 9 divisional offices
  - 8-15 branch offices / division office
- protocols:
  - DECnet, LAT, AppleTalk, SNA, TCP/IP
- Current:
  - home office & the 9 divisional offices
    - bridged together
  - over part of T1
    - rest of T1 used for SNA
  - no connections to branch

Large corporate, many protocols, contd.

- plan for next version (early 1990)

- keep home/division connection unchanged
- add router at division
- add routers at branch sites

- router at branch has:
  - 1 T1 interface
  - 1 ethernet interface
  - 1 token ring interface

- router at division has:
  - 2 ethernet interfaces
  - 1 token ring interface
  - n T1 interfaces

Large corporate, many protocols, contd.

users & uses

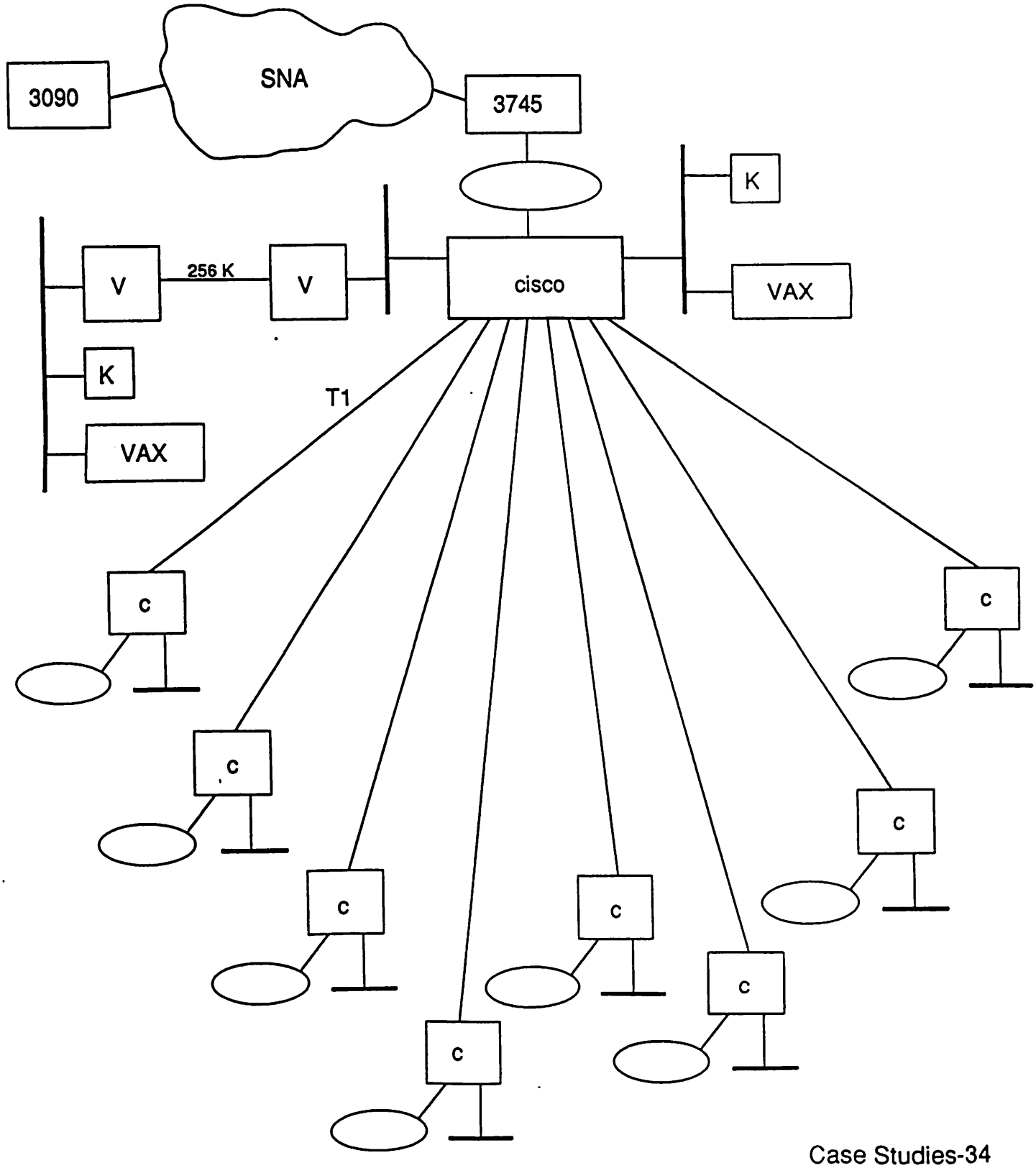
- from branch, division or home
  - MACs, AppleShare with local/remote servers
  - MACs, login to local/remote cpus
  - MACs, print to local/remote LaserWriters
  - PCs, login to local/remote cpus
  - PCs, use local/remote Novell servers
  - PCs, use local/remote printers
  - CPUs, use local/remote printers

- from home
  - backup?
  - security?

- everyone
  - email

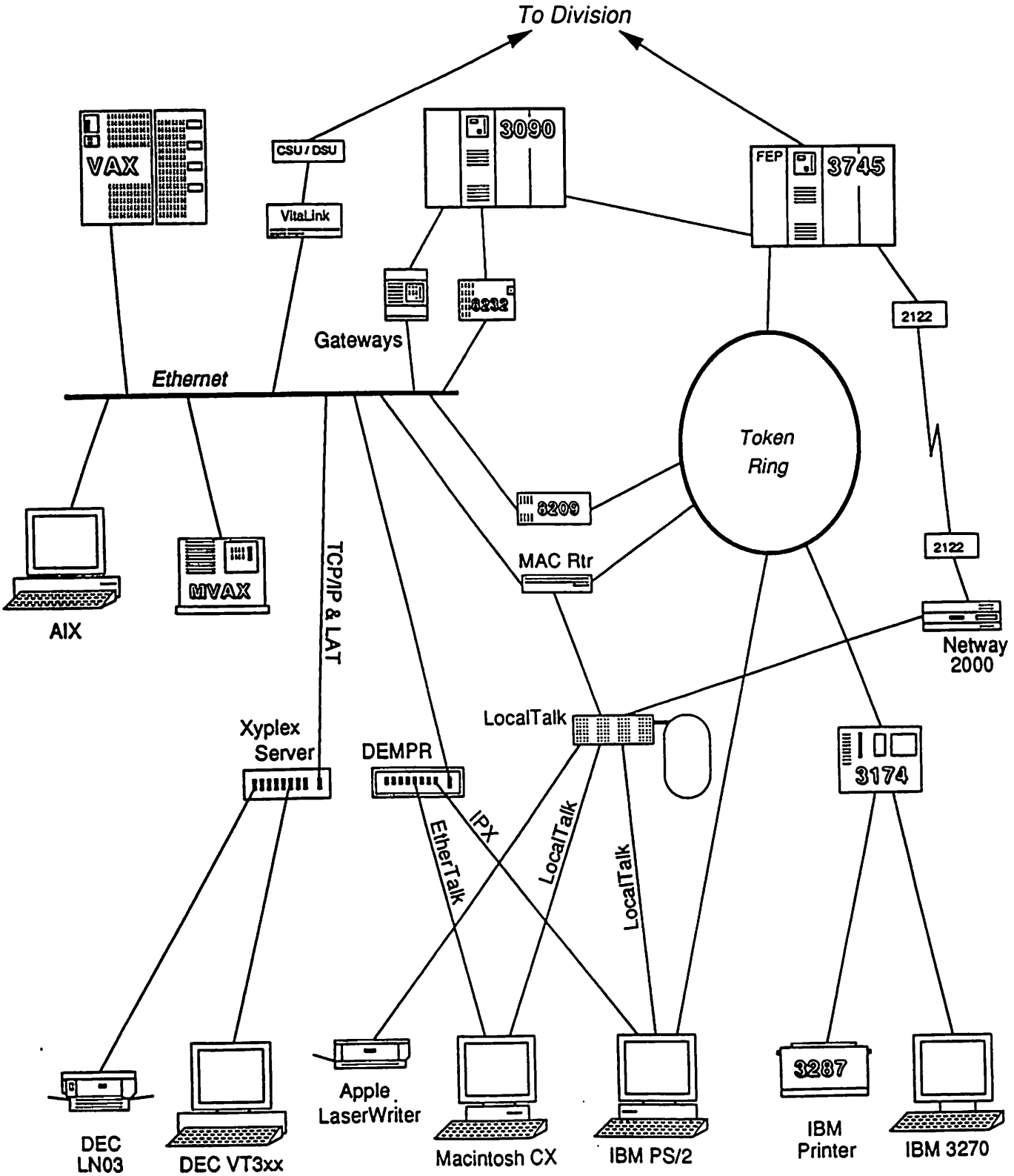
Large corporate, many protocols

logical

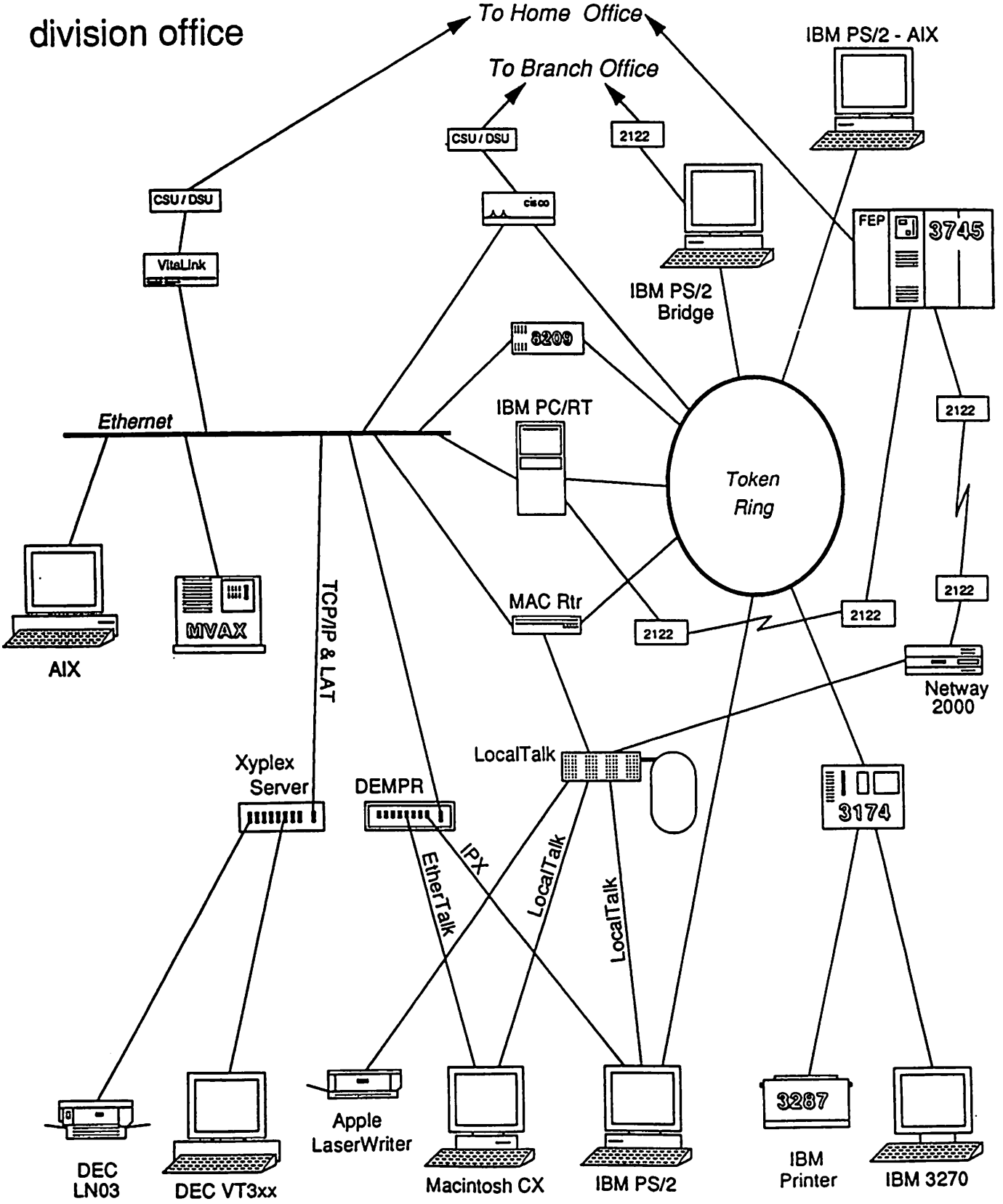


Large corporate, many protocols

home office

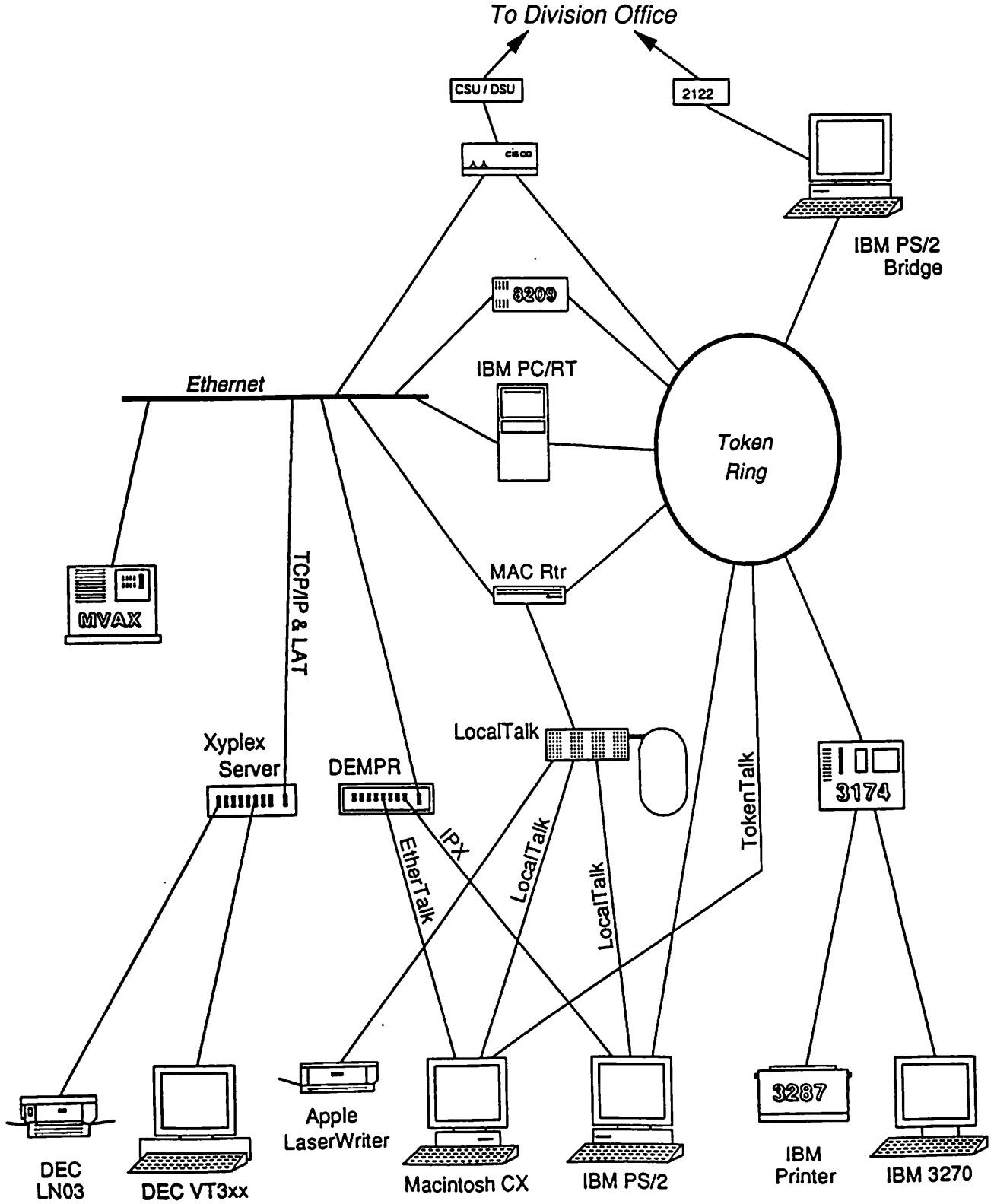


Large corporate, many protocols



Large corporate, many protocols

branch office



NEARnet

NSF regional in NE

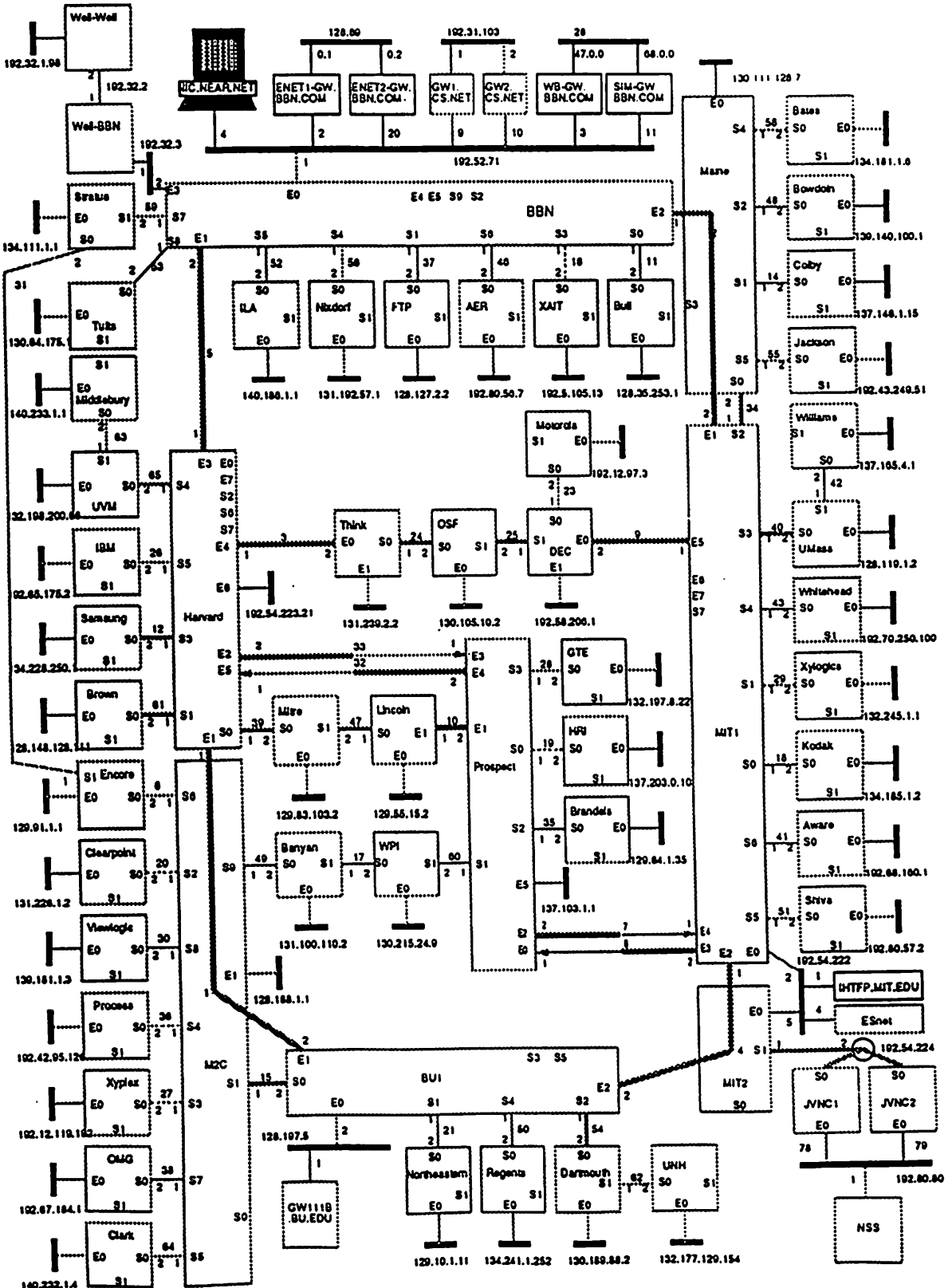
- size:
  - >149 members
- connection speeds:
  - 9.6KB to 10MB
- network design:
  - mesh topology
  - multiple paths for all high speed members
  - Cisco routers at each end of all links
- protocols:
  - TCP/IP (IGRP routing)
  - DECnet
  - OSI
- funding
  - self supporting
    - fees from members
  - no ongoing Fed $$

NEARnet, features

- management:
  - run by steering committee
    - reps from MIT, BU & Harvard
    - reps from BBN (management vendor)
  - technical committee
    - reps from MIT, BU & Harvard
  - planning committee
    - reps from NE area
- NSF connection:
  - T3 ENSS & T1 NSS
- future:
  - looking at fiber for core soon
  - expect to use FDDI to connect to ENSS soon

NEARnet

schematic



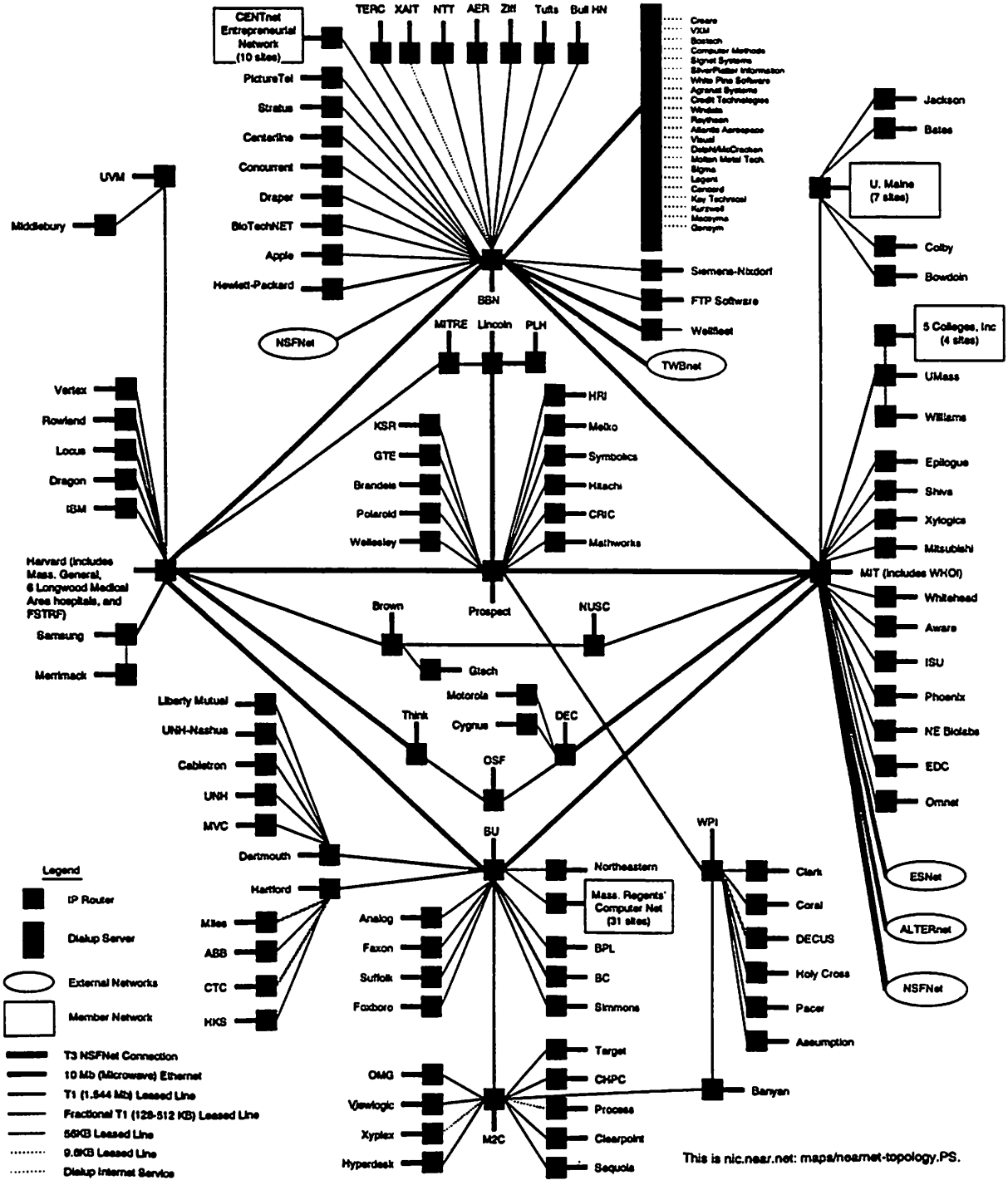
NEARnet

logical

NEARnet NETWORK TOPOLOGY

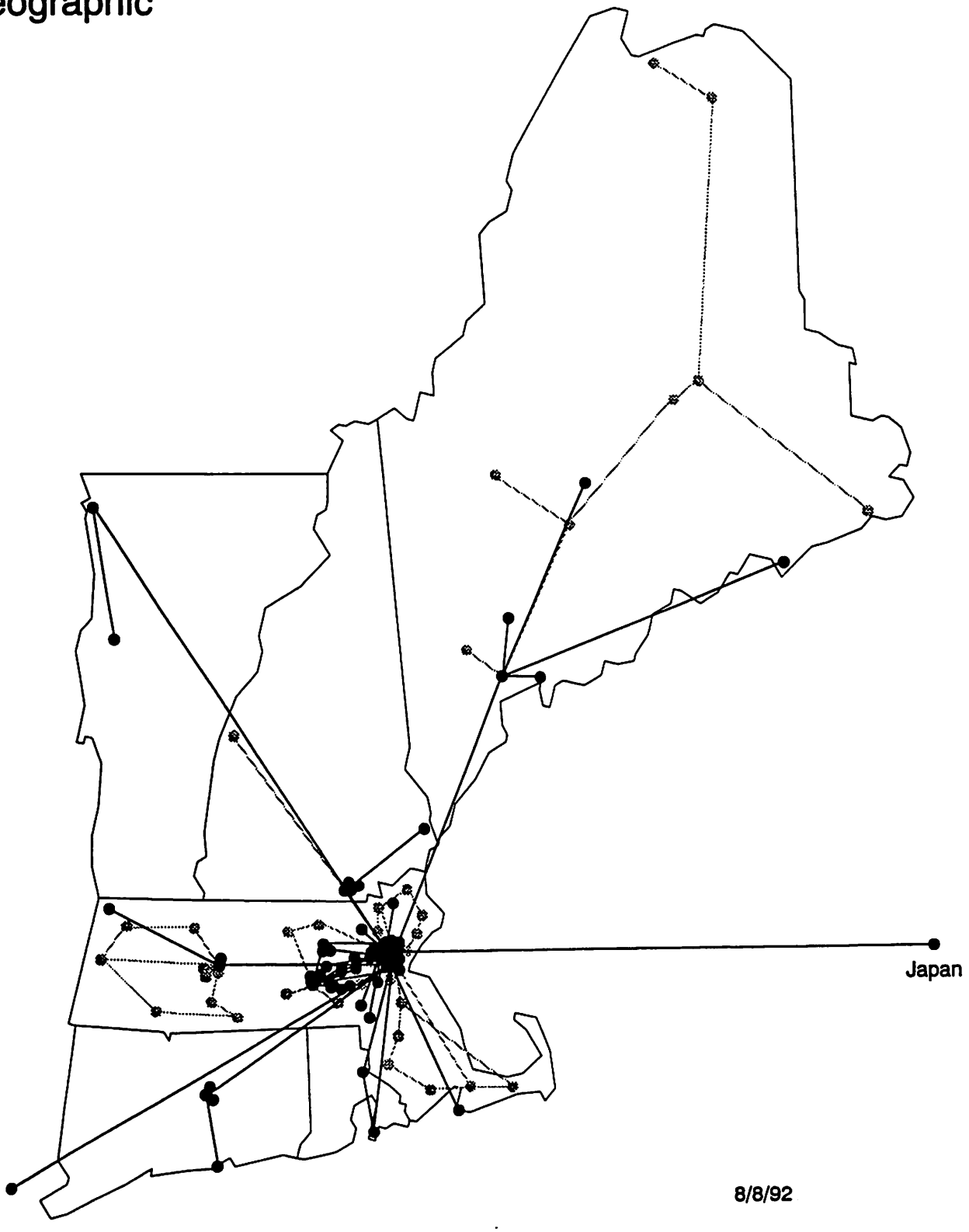
as of

June 25, 1992



NEARnet

geographic



8/8/92

Network Security

Is "Network Security" an oxymoron?

Security

"Security is recognizing

how you are exposed."

Steve McCallon

Security

- high-profile concern
- security is protecting assets
- $3 billion cost per year
- local people the major problem
- an "incident" could seriously affect the future of inter-organizational data networking

Computer & network security and the law

- little case law
  - many embezzlement cases
  - some extortion
  - Internet worm
- privacy
  - Privacy Act of 1974
    - must maintain accuracy, timeliness and security of stored information
    - subject of information must be able to check it
    - information may only be used for the purpose that the subject authorized
  - Right to Financial Privacy Act of 1978
    - government cannot get financial records without court action
  - Electronic Communications Privacy Act of 1986
    - prohibits interception or disclosure of data
    - sender must take care to protect data
  - Buckley Amendment

Computer & network security and the law

- security
  - Computer Fraud and Abuse act of 1986 (18 U.S.C. 1030) relates to "federal interest" computers
    - unauthorized access if access affects government's operation of the computer
    - access with intent to defraud
    - unauthorized damage or destruction of data
    - unauthorized prevention of use

    and causing damage > $1000 in a year
    or affects or potentially affects medical information or treatment
  - Computer Security Act of 1987
    - establishes government security programs

- many laws in the works
  - some state laws

Liability

- liability
  - if laws violated
  - if due care not exercised
    - e.g. poor contingency planning

  - if vendor doesn't fix flaws?
    - e.g. PBX hackers
    - Mitsubishi vs. AT&T
    - 30K calls, $430K bill
    - charge breach of contract & fraud
    - defective product
    - ask for > $10M

Privacy

- two issues
  - information database proliferation
  - conflict between users' privacy and security
- first outside of scope of this document
- privacy vs security
  - legal actions pending about email access
  - governmental actions against private BB operators
  - advocacy groups starting to appear (e.g. EFF)
  - particular problem in University
  - can a system or network manager:
    - examine user's data
    - deny a user access
    - intercept communications

Types of security problems

- denial of service
  - physical interruption
  - power outage
  - cut cables
  - disrupt net or computer with high traffic
  - improper control of routing information
- breakins from afar
  - hackers attacking from the Internet
- information interception
  - people peering at net
    - PCs can see anything on LAN
    - capture passwords
  - traffic analysis
- masquerade
  - illegal access to accounts/data
    - (NFS spoofing, .rhosts)
- data modification
  - change a "no" to a "yes"
- destruction of data by viruses etc
  - on PCs now ...

Basic factors in security

- networks are designed to facilitate access to resources
- user = knowledge of logname and password
  (knowledge based access control no longer sufficient
  for DOD systems)
- host security (or lack of same)
  Coopers & Lybrand survey:
  95% of data centers could not resist attack
  from a determined "hacker"
- official over-reaction
  e.g. security officer demanding super-user privilege
  on all corporate computer systems
  e.g. government "back-door" decryption requirement

"It is the sense of Congress that providers of electronic communications service equipment shall ensure that communications systems permit the government to obtain the plain text contents of voice, data and other communications when appropriately authorized by law."

Security problem areas

- local people
  legitimate computer or network users
  access to physical media
  up to 90% of problems
- no security problem on isolated networks—
  (if you trust the people)
  DoD networks
  bank networks
- network only as secure as media access
  pressurized conduits, secure manholes
  otherwise encrypt data
- ANY external access a problem
  modem lines etc
- external access networks exacerbate problem
  but do not create a new problem

Passwords

- dumb passwords are dumb
- *crack* password checker
- passwords in cleartext on network
- password change programs that restrict flexibility
  not in dictionary, not name, not phone #
- programs that create almost-English words
  tacacc
- random passwords a problem
- force password change can be a problem
- one-time passwords look good

Physical security

- access control
  locks, guards & cards
  intrusion detection
- power supply assurance
  emergency power feeds
  UPS
- connectivity assurance
  redundant cable pathways
  learn from Hinsdale & Harvard

Operational security

- good network monitoring
- access to key locations
- good people on-call
  - beepers
- disaster recovery procedures defined

Threats, personnel

- tourists
  - active attackers
  - "outsiders" of site
  - may be legitimate elsewhere
  - have little knowledge of your organization
    - don't know what is important
    - or where important data resides
- non-tourists
  - almost all important cases so far
  - disgruntled employees
  - "others with a mission"
    - after information or resources

Threats, technical

- passive
  - monitor net (wiretapping)
    - look for "interesting" information
    - do traffic analysis
  - must have physical access to "useful" part of net
    - or break security on computers with network monitoring ability
  - cannot detect most attempts
  - can prevent most damage by encrypting data
- active
  - overt action
    - login attempts
    - false data
    - interrupt service
    - message modification
    - message replay
  - cannot prevent the attempt
    - good procedures can limit exposure
    - can detect most attempts

Local security procedures

IETF SPWG recommendations

- clear written security statement always available
- adequate security controls must be implemented
  at least require the use of passwords
- have capability to monitor security incidents
- establish chain of communication and control
  for security matters
- sites must fix security flaws quickly

Security, implementations

Guard the doors

- implement filtering in devices
  connecting network to outside world
- filters can use hardware or protocol addresses
- filters can use other attributes

- different devices have different features

- bridges are limited
  most only deal with hardware addresses

- routers can have extensive capabilities

- pay some functional price

Guard router examples

Security, filter options

Filter options in NSC routers

- Filter parameters
  - Any
    - All packets will match
  - Hardware source addr ok
    - Checks physical ethernet address against IP address
  - IP datagram length
    - Checks length of IP datagram
  - IP destination address
    - Checks the destination address of the IP packet
  - IP source address
    - Checks the source address of the IP packet
  - IP protocol
    - Checks the "protocol" field in the IP header
    - e.g. ICMP, GGP, TCP, EGP, UDP, ISO-TP4
  - IP type of service
    - Checks the "type of service" field of the IP packet
    - e.g. normal, priority, immediate, flash, etc
  - TCP source port
    - Checks the source port of the TCP packet
    - e.g. echo, ftp, telnet, smtp, finger. etc
  - TCP destination port
    - Checks the destination port of the TCP packet
  - UDP source port
    - Checks the source port of the UDP packet
    - e.g. echo, time, nameserver, bootp, tftp, snmp, etc
  - UDP destination port
    - Checks the destination port of the UDP packet
  - Gateway address
    - Checks the address of the next gateway to which the packet would go
  - Gateway address two
    - Check based on whether router knows route between two IP addresses

Security, routing options

What can NSC router do when pattern matched?

- Accumulate statistics
  - Increments per source-destination pair counters
- Counter 1
  - Increment auxiliary counter #1 for pair
- Counter 2
  - Increment auxiliary counter #2 for pair
- Alarm
  - Generate console alarm message
- ICMP unreachable
  - Send an ICMP unreachable message back to sender
- No ICMP unreachable
  - Cancel the sending of ICMP unreachable messages
- Route to
  - Re route the packet to an alternate host or gateway
- No route to
  - Cancel the route to function
- Copy to
  - Send a copy of the packet to a selected address
- No Action
  - Don't do anything

Security, routing options

- onus on sender to protect data

- source routing
  - can select exact path for packet
  - can use only trusted routers & networks
  - used by token ring
  - can be used in TCP/IP

- mostly futures (for now)
  - TCP/IP source route support mandated by host requirements RFC

- have routers only advertise public nets

Security, know thy user

Kerberos: User and service authentication

- user interacts with trusted server to get "ticket"
- ticket encrypted in service provider's key
- ticket used to access network services
- server authenticator can be requested

- service "knows" user
- user "knows" service

- ticket used instead of password
- password never goes across network
- tickets have timestamp
- can be used to distribute crypt keys

- transparent to user

- available from MIT
- in OSF DCE

Security, I can see it, but...

Encryption

- datapath encryption
  - hardware device between host and network or between network and router
  - e.g. Digital Ethernet Secure Network Controller (*DESNC*)
    - configured for specific node pairs
    - encrypts network frames
    - data integrity verified
    - verify frame source addresses
    - works with software key distribution system
    - deals with small number of nodes (~20)
- encrypting modems
  - AT&T STU-III *Secure Data Device*
- encrypting bridges

- data encryption
  - encrypt data part of packets
  - Kerberos can be used to distribute keys

Data encryption systems, DES

- Data Encryption Standard
- federal standard

- symmetric system
  - same key used to encrypt and decrypt

- "private key" or "shared secret" system

- 56 bit key

- data encrypted in chunks of 64 bits
- generally used in chaining or feedback mode
  - results of encrypting one chunk used in encrypting next chunk
  - special operation on 1st chunk
  - mask data repetitions

DES, contd.

- breakability
  - 56 bit key too short?
    - some history to length choice
  - not approved for national security information
  - NSA in 1987 announced disapproval of DES
    - for some uses then reversed decision
  - chosen-plaintext attack

- export
  - known algorithm
  - illegal to export other than for bank use
  - ftp'able verson from Finland

- anyone who can decrypt message can forge message

Data encryption systems, RSA

- Rivest-Shamir-Adleman

- adopted by a number of vendors
  - Lotus, DEC, Novell, SUN, Microsoft, Apple, Motorola, Nothern Telecom, the IAB
  - 1/2 million copies in use now
  - will be part of standard Mac OS

- asymmetric (public key) system
  - separate keys for encryption and decryption
  - can let one key be "public"
  - data encrypted by one key can only be decrypted by the other

- product of two large (~100 digit) prime numbers used as base
- mathematical manipulation of this product produces the keys

- keys up to 1024 bits long
  - must also store product of primes and other information for use in decoding

- fee for key set to RSADSI (if in U.S.)

RSA, contd.

- breakability
  - depends on difficulty in factoring large numbers
    - can lengthen numbers used in future
  - can be mathematically shown to not have trap door
- export
  - known algorithm
  - illegal to export
  - patented in U.S.
  - used by British, French and Swiss banking, CCITT, ISO
- decrypter of message cannot forge message
- NSA objects to the use of RSA
  - "all parallel non-governmental cryptographic activities" should be halted because of the threat they pose to the NSA's mission of information collection.
    - Admiral Bobby Inman, former NSA director

Other encryption systems

- when DES selected as standard
  - some algorithms classified by feds
    - even algorithm names classified
- DOD systems do not use DES
  - use "Type 1" for example
  - "available to U.S. government agencies, military organizations and defense contractors"
  - fast hardware
    - 40 Mbits/sec encryption
- non-U.S. equipment
  - *Trade Secrets* from Mobius Systems in Canada
  - card for PC
  - uses a public key system
  - 1 M byte/min encryption (593 bit key length)
  - encrypt communications line

X.509

- uses public key encryption

- sequence
  1/ *A* gets the public key for *B*
  2/ *A* encrypts message in key
  3/ *A* sends encrypted message to *B*
  4/ *B* decrypts message using private key

- the message can only be decrypted with *B*'s private key

X.509: Digital Signature

- need method to be sure that message came from *A*

- use "Digital Signature"
- appended to message before sending

- uses a "hash function"
  mathematical function for mapping a large amount of data into a small amount
  a "good" hash function will evenly distribute the results over the small range

- uses a "one-way function"
  a mathematical function which is easy to compute but hard to calculate the input data

X.509: Digital Signature contd.

- procedure for using a digital signature

  A computes a one-way hash function of the contents of the message

  A encrypts hash code with its private key the result is appended to the message

  when it gets the message *B* computes the same hash function on the body of the message

  then decrypts the received hash code using *A*'s public key

  if the hash codes match, the message came from *A* and the contents were not altered in transmission

X.509 getting public keys

- a user must get public keys in a way that is secure from tampering

- user gets a certificate that includes the public key and has the digital signature of a Certification Authority
- to verify a Certification Authority one gets a certificate with a digital signature of a Certification Authority with higher authority
- at some point one must have gotten the public key of the "master" Authority by some other means

X.509: getting rid of bad certificates

- since certificates have long lifetimes (months or years) there must be a procedure to revoke them in case of a security leak
- the Certification Authority publishes a Certificate Revocation List (CRL) from time to time

  like list of bad credit cards
- CRL can grow very large

X.509 problems

- procedures for creating certificates
- storing private key
  must store 1792 bits for PEM

NIST Digital Signature Standard

- NIST proposed a Digital Signature Standard (DSS)
  - on 30 Aug 1991
  - in response to the Computer Security Act of 1987
- to be used for authentication
  - (not for privacy)
- proposed FIPS does not include hash algorithm
  - or certificate formats
- developed in conjunction with NSA

- much public criticism
  - some from vendors of competitive systems
  - inflexible design - fixed length keys
    - too short - 512 bits
  - too easy to break
  - public key algorithm (ElGamal)
    - not well studied
    - cannot yet be "proven" to not have a trap door
  - subject to "catastropic failure"
    - all users on system compromised

Privacy Enhanced Mail (PEM)

- RFCs 1113, 1114, and 1115

- provides for
  - disclosure protection
  - sender authenticity
  - message integrity
  - non-repudiation of origin

- two types of keys
  - Interchange Keys (IK)
    - used to transfer DEKs
    - RSA used
  - Data Encryption Keys (DEK)
    - new key for each message
    - DES-CBC used

- features
  - designed for SMTP
  - encrypted messages can be sent over normal SMTP pathways (all printing characters)
  - "certificate" included in message

PEM example

```
From: "CONTEL GOVERNMENT NETWORKS GROUP"@RHETCEA.AUTODIN
Date:          Sat, 01 Jun 91  17:35:00 GMT
Subject:       DEFENSE MESSAGE TRANSFER SYSTEM (DMTS) DEMONSTRAT
To: (Action) CDR@BRUNNHILDE.CTC.CONTEL.COM
Security:      Unclassified
Status: R

-----BEGIN PRIVACY-ENHANCED MESSAGE-----
Proc-Type: 3,MIC-CLEAR
Sender-ID: (DMTS) <SYSADMIN@fricka.ctc.contel.com>:
 MIGGMQswCQYDVQQGEwJVUzEUMBIGA1UEChMLQ29udGVsIEluYy4xITAfBgNVBAs
 TGEhvbnRlbCBUZWNobm9sb2d5IEN1bnRlcjEoMCYGA1UECxMfTmV0d29yaXMgYW5
 kIFNlY3VyZSBTeXN0ZW1zIEzhYjEcMBoGA1UECxMTVGVsdCBQdXJwb3NlcyBPbmx
 5IQ==:
 8
Certificate:
 MIICkjCCAiocAQgwCgYGKw4HAgMBBQAwgY4xCzAJBgNVBAYTAlVTMRQwEgYDVQQK
 EwtDb250ZWwgSW5jLjEhMB8GA1UECxMYQ29udGVsIFRlY2hub2xvZ3kgQ2VudGVy
 MSgwJgYDVQQLEx9OZXR3b3JrcyBhbmQgU2VjdXJlIFN5c3RlbXMgTGFiKRswGgYD
 VQQLExNUZXN0IFBlcnBvc2VsIE9ubHkhMB4XDTkxMDIwNTEyNTIwWhcNOTkyMDIw
 NTEyNTIwWjCwgcUxCzAJBgNVBAYTAlVTMRQwEgYDVQQKEwtDb250ZWwgSW5jLjEh
 MB8GA1UECxMYQ29udGVsIFRlY2hub2xvZ3kgQ2VudGVyMSQwIgYDVQQLExtOZXR3
 b3JrcyBhbmQgU2VjdXJlIFN5c3RlbXMxJzAlBgNVBAsTHlN5c3RlbSBUZXN0IC0g
 RElUUyBWZXJzaW9uIDEuMDEuMCwGA1UEAxMlRGVmENW5zZSBNZXNzYWdlIFN5c3Rl
 bSAoRE1UUykgR2FOZXIdheTCBnDANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAsQnqpsxj
 g2/jn+QIDY0IgrWZO/auc5ICYiHXXXX6zZZSKSKr/NjukllWwTUsT2LWTZxeKfdF
 CjXTHMIIdrnVEWTBlXslDXElWtlEbX4QHlWjCZhEApuYDksyoOzeOLgDSahhcWP5
 H6+cXnDeDFViEnqr9eeOK2XdGpCbPVl9LPsCAwEAATANBgYrDgcCAwEFAAMEAAWw
 wlb/285kApTvcOEpgMOOX4pKqW7nmE6eYIqs+tdtYYdOdfQfXjEhDp1DmOHLFUC3
 GYRGLzd4eTMspk/whYtW77cA/xDoL1UUPw+g6/FRxLbAB2VwFhs=
Issuer-Certificate:
 MIICLjCCAS0CAQQwCgYGKw4HAgMEBQAwaTELMAkGA1UEBhMCVVMxIDAeBgNVBAoT
 F1JTQSBEYXRhIFNlY3VyaXR5LCBJbmMuMSkwJwYDVQQLEyBJbnRlcm5ldCBDZXJO
 aWZpY2F0aW9uIEF1dGhvcml0eTEMMAsGA1UECxMEQmVOTTAePwO5MDEyMTUyMDAw
 MDBaFw05MTEyMTUxOTU5NTlaMIGGMQswCQYDVQQGEwJVUzEUMBIGA1UEChMLQ29u
 dGVsIEluYy4xITAfBgNVBAsTGEhvbnRlbCBUZWNobm9sb2d5IEN1bnRlcjEoMCYG
 A1UECxMfTmV0d29yaXMgYW5kIFNlY3VyZSBTeXN0ZW1zIEzhYjEcMBoGA1UECxMT
 VGVsdCBQdXJwb3NlcyBPbmx5ITDwMAoGBFUIAQECAgK8A2IAMF8CMA7eKHttwXj1
 /wGOpYGVI7gyASLJpQ8TV/AzerdGH+7tdOGb6XnKM5JwWIm5RvW7QR2rbImRBrMe
 WVJFdPt/4JIlxQotsRe2TsTOcla4XqSx6RBiT2VWE7ECAwEAATANBgYrDgcCAwEF
 AAM/AAElWjo4AXLTHoPf+3Avw+6YyvBgI4S7QD86WsfPTKSLwPjEjiPDv64FJX95
 W+F23wSQVjzx5oPF/F1CzaeoGLHaFefdzmbA02EzmPDvIA217Zjot0tjcMmjDaDK
 7d5UGOwLOyx/KQEuo3wFbNOcV5/4h152Yn+m82cc5UnjIw==

                                                    Network Security-37
```

PEM example, contd.

```
MIC-Info: RSA-MD2,RSA,
 Cji6RmYy6FnosIsoLT4FKhsDTFQat8Xmlzukc9eC4O7PEzD2XmPPkacf2olIJlgE
 MEyC2h9Wc3Ks2FgPgn7LoLvPPmcWzWUd2kvuLH8SE8T8gtYV90CHcnIOOOoXGY8O
 F/axmFsQYWPApWvwPlI7IRDiBo/Gw+75On6rGGuQmRQ=

-----BEGIN PRIVACY-ENHANCED MESSAGE PREAMBLE-----
Received:    From RHETCEA by brunnhilde.ctc.contel.com via AUTODIN with
               id <RAAUEYUW RHETCEA0002 1550932-UUUU--RHETCEA>;
               Tue, 04 Jun 91  20:50:56 GMT
Date:          Sat, 01 SEP 2173870038991@MCI.ctc.contel.com>
Message-Id:    <c:arch}
Sender:        (DMTS) <SYSADMIN@fricka.ctc.contel.com>
Comment:       DMS Organizational Message, received from AUTODIN.
Reply-to:      (ACKNOWLEDGE RECEIPT!)  <RECEIPT@fricka.ctc.contel.com>
From:          "CONTEL GOVERNMENT NETWORKS GROUP"@RHETCEA.AUTODIN
Subject:       DEFENSE MESSAGE TRANSFER SYSTEM (DMTS) DEMONSTRATION
To:            (Action) CDR@BRUNNHILDE.CTC.CONTEL.COM,
Priority:      Routine
Security:      Unclassified
SIGNED:    04 JUN 1991 20:51:29 UT
-----END PRIVACY-ENHANCED MESSAGE PREAMBLE-----

DATELINE: WASHINGTON, D.C., 4 JUNE 1991
-
GTE CONTEL FEDERAL SYSTEMS IS PLEASED TO ANNOUNCE THE FIRST LIVE
PUBLIC DEMONSTRATION OF AN UNCLASSIFIED AUTODIN-TO-DDN INTERFACE
(ADI) CAPABILITY, A PART OF THE PROTOTYPE DEFENSE MESSAGE
TRANSFER SYSTEM (DMTS) BEING EXHIBITED AT THE 45TH ANNUAL AFCEA
INTERNATIONAL CONFERENCE AND EXHIBITION AT THE D.C. CONVENTION
CENTER.
-
IN ORDER TO PROTECT AGAINST SPURIOUS MESSAGES, THE DMTS MAKES USE OF
THE PRIVACY ENHANCED MAIL CAPABILITY BEING DEVELOPED FOR USE ON THE
INTERNET BY GTE CONTEL AND OTHER VENDORS.  THIS FEATURE IS USED TO
PROVIDE A STRONG CRYPTOGRAPHIC VERIFICATION OF THE AUTHENTICITY OF A
DMS MESSAGE BY MEANS OF AN RSA DIGITAL SIGNATURE TECHNIQUE.  WITHOUT
THIS AUTHENTICATION, A MESSAGE WILL NOT BE ACCEPTED AT EITHER THE
DMTS GATEWAY OR THE DMTS WORKSTATIONS.  FOR ADDITIONAL PROTECTION,
THE DATA ENCRYPTION STANDARD (DES) ALGORITHM CAN BE USED TO
PROVIDE END-TO-END, WRITER-TO-READER PRIVACY AND NEED-TO-KNOW
PROTECTION ON A MESSAGE BY MESSAGE BASIS, OVER AND ABOVE THE
MILITARY ENCRYPTION EQUIPMENT USED TO PROTECT ALL CLASSIFIED DOD
COMMUNICATIONS.
-
-----END PRIVACY-ENHANCED MESSAGE-----
```

Refining the "user"

- require more than just knowledge

- possession
  - electronic keys
  - smart cards
  - code generators

- characteristics (biometrics)
  - geometry of body parts
    - e.g. 3D hand scan
  - finger prints
  - retinal patterns
  - voice
  - handwriting
  - typing rhythms

  worry about reject ratio

Help

places to contact if you have a security "event"

- regional network noc

- NSFnet management (MERIT)
  1-800-66-MERIT (1-800-666-3748)

- Computer Emergency Response Team (CERT)
  412-268-7090

Keep in mind

- need to do risk analysis

  don't buy a $10,000 Halon fire protection system for a $1,000 PC if risk analysis indicates that there could be a fire once in 10 years

References

Cheswick, B., *The Design of a Secure Internet Gateway*, AT&T Bell Laboratories

Cooper, J. A., *Computer & Communications Security: Strategies for the 1990's*, McGraw-Hill, 1989, ISBN 0-07-012926-6

Denning, P. Ed., *Computers Under Attack: Intruders, Worms, and Viruses*, Addison-Wesley, 1990, ISBN 0-201-53067-8

DOD, *"Rainbow" books*, INFOSEC Awareness Office, DOD/NSA, ATTN: S332, 9800 Savadge Road, Ft. Mead, MD 20755-6000, (301) 766-8729

Holbrook, P. and J. Reynolds, Eds. *Site Security Handbook*, RFC-1244, July 1991

ISPNews: INFOSecurity Product News, MIS Training Institute Press, Inc., 498 Concord St., Framingham, MA 01701, (508)879-9792

Murray, W., *Taking a Stand on Public Key Cryptography*, ISPNews, September/October, 1991

NIST, *Executive Guide to the Protection of Information Resources*, National Institute of Standards and Technology, Gathersberg, MD

References, contd.

NIST, *Management Guide to the Protection of Information Resources*, National Institute of Standards and Technology, Gathersberg, MD

NIST, *A Proposed Digital Signature Standard (DSS)*, National Institute of Standards and Technology, Gathersberg, MD

NIST, *Data Encryption Standard*, FIPS PUB 46-1, Aug 30, 1991, National Institute of Standards and Technology, Gathersberg, MD

RSA Data Security, Inc. *RSA Encryption Standard, Version 1.4*, June 1991

RSA Data Security, Inc., *Comments on the NIST DSS proposal*, Sept 20, 1991