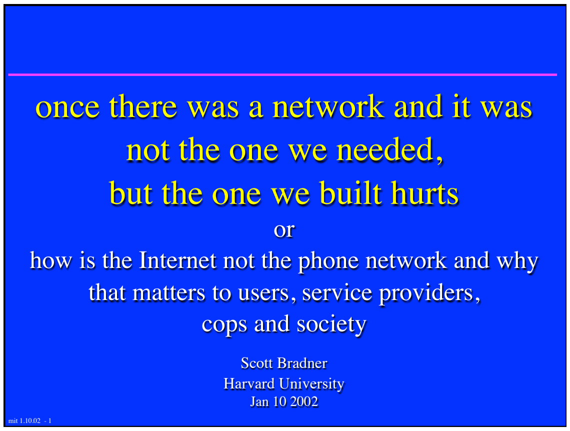
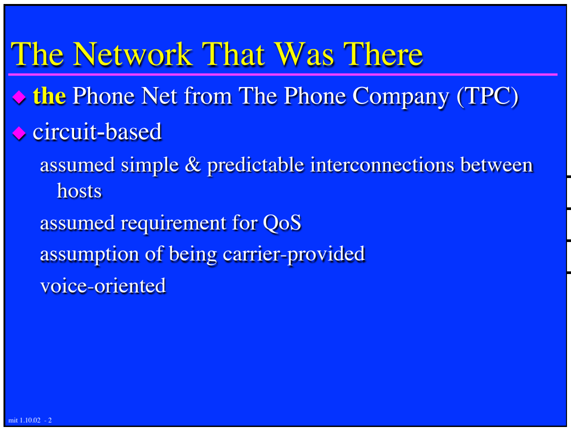


# once there was a network and it was not the one we needed, but the one we built hurts

or

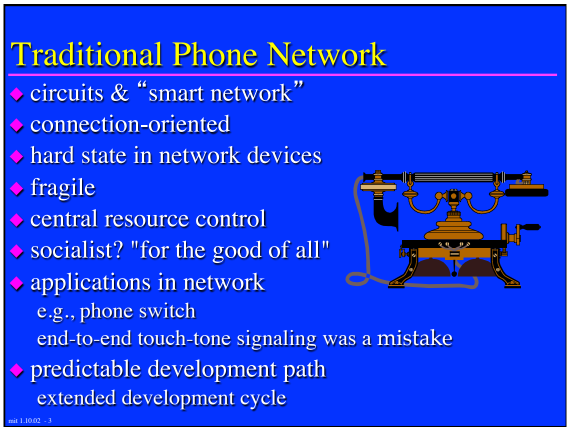
how is the Internet not the phone network and why that matters to users, service providers, cops and society

Scott Bradner
Harvard University
Jan 10 2002



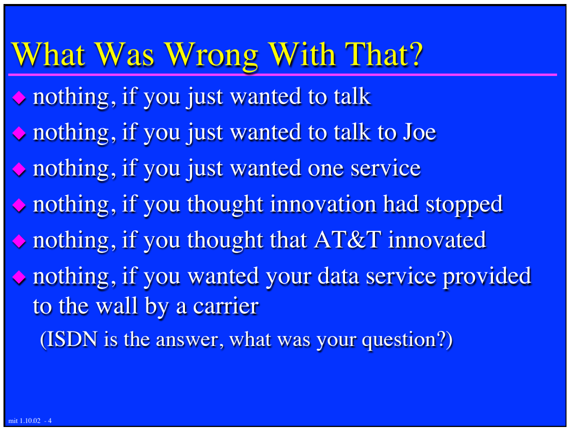
## The Network That Was There

- **the** Phone Net from The Phone Company (TPC)
- circuit-based
  - assumed simple & predictable interconnections between hosts
  - assumed requirement for QoS
  - assumption of being carrier-provided
  - voice-oriented



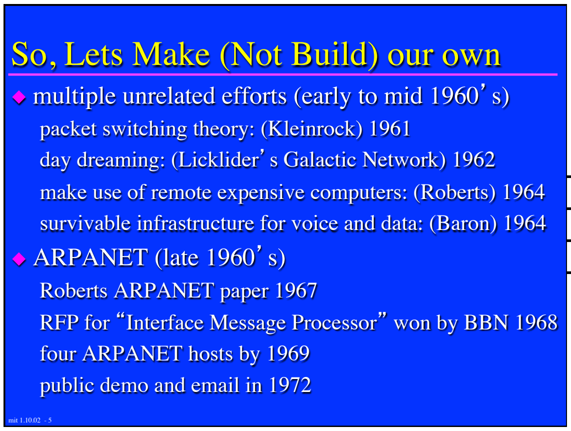
## Traditional Phone Network

- circuits & “smart network”
- connection-oriented
- hard state in network devices
- fragile
- central resource control
- socialist? "for the good of all"
- applications in network
  - e.g., phone switch
  - end-to-end touch-tone signaling was a mistake
- predictable development path
  - extended development cycle



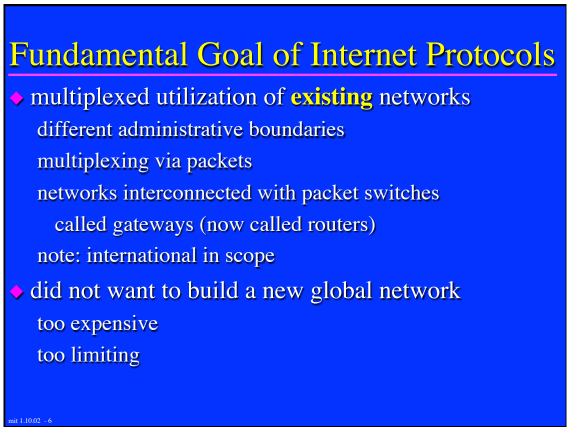
## What Was Wrong With That?

- nothing, if you just wanted to talk
- nothing, if you just wanted to talk to Joe
- nothing, if you just wanted one service
- nothing, if you thought innovation had stopped
- nothing, if you thought that AT&T innovated
- nothing, if you wanted your data service provided to the wall by a carrier
  - (ISDN is the answer, what was your question?)



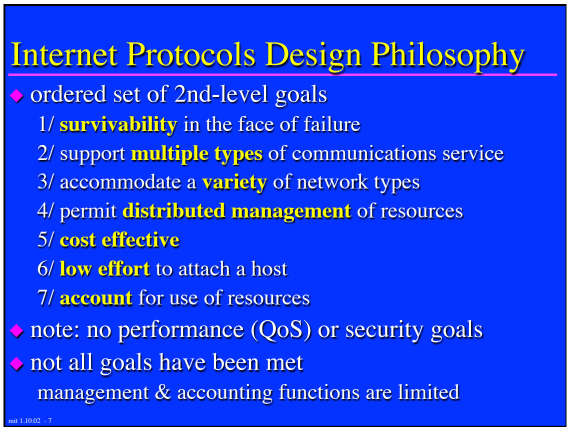
## So, Lets Make (Not Build) our own

- multiple unrelated efforts (early to mid 1960's)
  - packet switching theory: (Kleinrock) 1961
  - day dreaming: (Licklider's Galactic Network) 1962
  - make use of remote expensive computers: (Roberts) 1964
  - survivable infrastructure for voice and data: (Baron) 1964
- ARPANET (late 1960's)
  - Roberts ARPANET paper 1967
  - RFP for "Interface Message Processor" won by BBN 1968
  - four ARPANET hosts by 1969
  - public demo and email in 1972



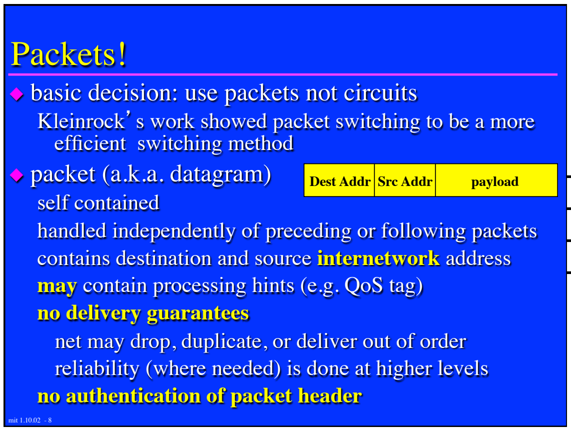
## Fundamental Goal of Internet Protocols

- multiplexed utilization of **existing** networks
  - different administrative boundaries
  - multiplexing via packets
  - networks interconnected with packet switches
    - called gateways (now called routers)
  - note: international in scope
- did not want to build a new global network
  - too expensive
  - too limiting



## Internet Protocols Design Philosophy

- ordered set of 2nd-level goals
  - 1/ **survivability** in the face of failure
  - 2/ support **multiple types** of communications service
  - 3/ accommodate a **variety** of network types
  - 4/ permit **distributed management** of resources
  - 5/ **cost effective**
  - 6/ **low effort** to attach a host
  - 7/ **account** for use of resources
- note: no performance (QoS) or security goals
- not all goals have been met
  - management & accounting functions are limited

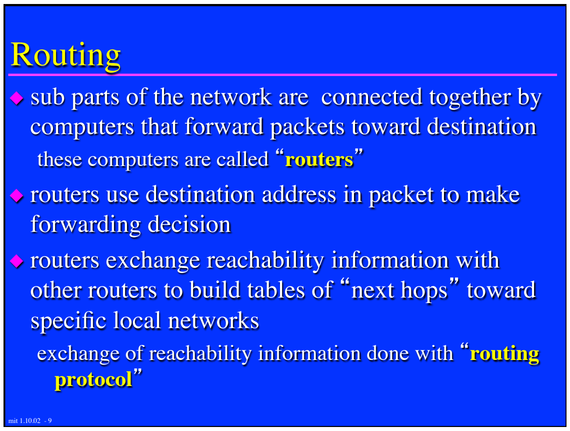


## Packets!

- basic decision: use packets not circuits
  - Kleinrock' s work showed packet switching to be a more efficient switching method
- packet (a.k.a. datagram)

| Dest Addr | Src Addr | payload |
|---|---|---|

  - self contained
  - handled independently of preceding or following packets
  - contains destination and source **internetwork** address
  - **may** contain processing hints (e.g. QoS tag)
  - **no delivery guarantees**
    - net may drop, duplicate, or deliver out of order
    - reliability (where needed) is done at higher levels
  - **no authentication of packet header**



## Routing

- sub parts of the network are connected together by computers that forward packets toward destination
  - these computers are called "**routers**"
- routers use destination address in packet to make forwarding decision
- routers exchange reachability information with other routers to build tables of "next hops" toward specific local networks
  - exchange of reachability information done with "**routing protocol**"

## A Quote

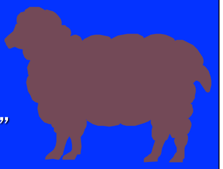
*"the lesson of the Internet is that **efficiency is not the primary consideration**. Ability to grow and adapt to changing requirements is the primary consideration. This makes simplicity and uniformity very precious indeed."*

Bob Braden

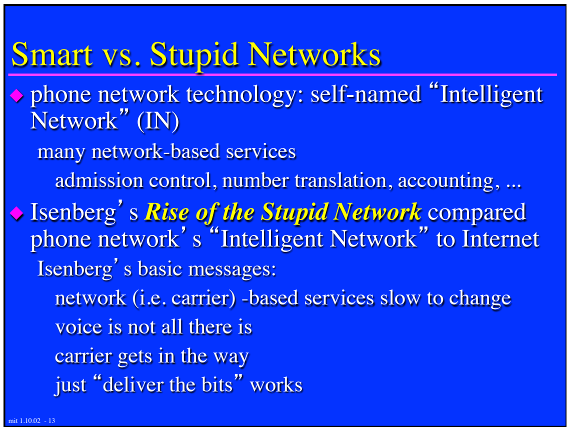
## *End-to-End Argument*

- 1981 paper by Saltzer, Reed & Clark
- "smart networks" do not help
  - adding functions into network can be redundant since actual function is **end-to-end**
    - e.g. encryption, data reliability
  - also harder to change to support new technology
    - also see Lampson ***Hints for Computer System Design***
- e2e argument projected to mean
  - no per-session knowledge or state in the network
    - but some "soft-state" (auto refreshed) may be OK
  - network should be transparent to end-to-end applications

## Internet

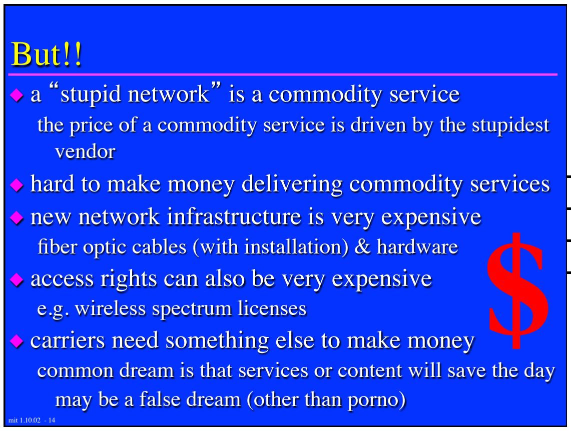


- packets & e2e
- soft state in network devices
- resilient
- competitive resource control
- capitalist? "individual initiative"
  - but too much selfishness hurts all
  - must play by the same rules - but no enforcement
    - **the tragedy of the commons**
- applications in hosts at edges (end-to-end)
  - and in 3rd party servers anywhere on the net
- hard to predict developments
  - chaos at the rate of "Internet time"



## Smart vs. Stupid Networks

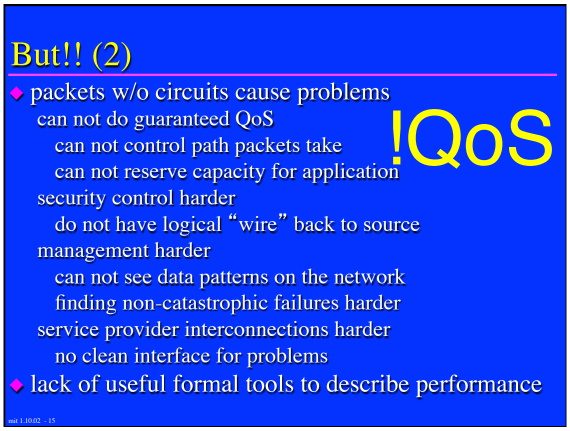
- phone network technology: self-named “Intelligent Network” (IN)
  - many network-based services
    - admission control, number translation, accounting, ...
- Isenberg’s ***Rise of the Stupid Network*** compared phone network’s “Intelligent Network” to Internet
  - Isenberg’s basic messages:
    - network (i.e. carrier) -based services slow to change
    - voice is not all there is
    - carrier gets in the way
    - just “deliver the bits” works



## But!!

- a “stupid network” is a commodity service
  - the price of a commodity service is driven by the stupidest vendor
- hard to make money delivering commodity services
- new network infrastructure is very expensive
  - fiber optic cables (with installation) & hardware
- access rights can also be very expensive
  - e.g. wireless spectrum licenses
- carriers need something else to make money
  - common dream is that services or content will save the day
    - may be a false dream (other than porno)

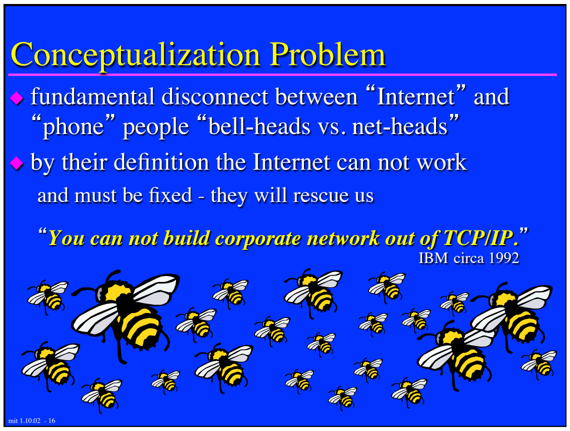
$



## But!! (2)

- packets w/o circuits cause problems
  - can not do guaranteed QoS
    - can not control path packets take
    - can not reserve capacity for application
  - security control harder
    - do not have logical “wire” back to source
  - management harder
    - can not see data patterns on the network
    - finding non-catastrophic failures harder
  - service provider interconnections harder
    - no clean interface for problems
- lack of useful formal tools to describe performance

!QoS

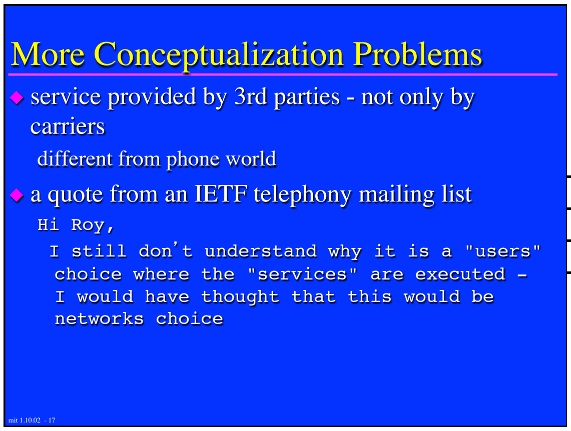


## Conceptualization Problem

- fundamental disconnect between “Internet” and “phone” people “bell-heads vs. net-heads”
- by their definition the Internet can not work

  and must be fixed - they will rescue us

  “*You can not build corporate network out of TCP/IP.*”
  IBM circa 1992

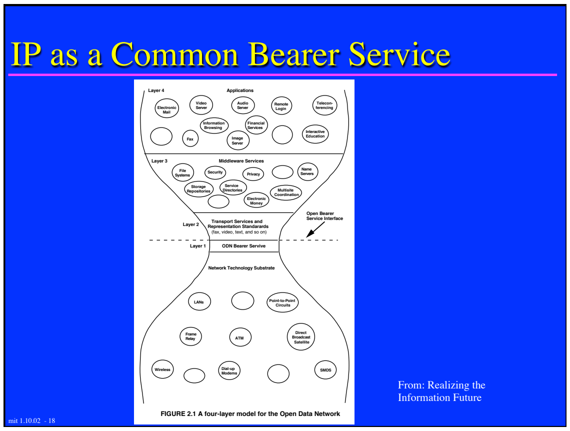


## More Conceptualization Problems

- service provided by 3rd parties - not only by carriers

  different from phone world
- a quote from an IETF telephony mailing list

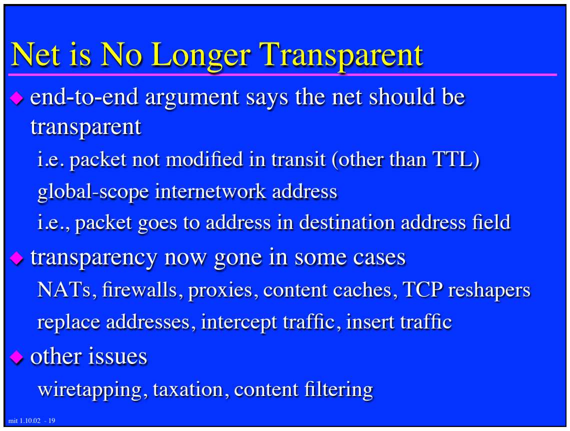
```
Hi Roy,
  I still don't understand why it is a "users"
   choice where the "services" are executed -
   I would have thought that this would be
   networks choice
```



## IP as a Common Bearer Service

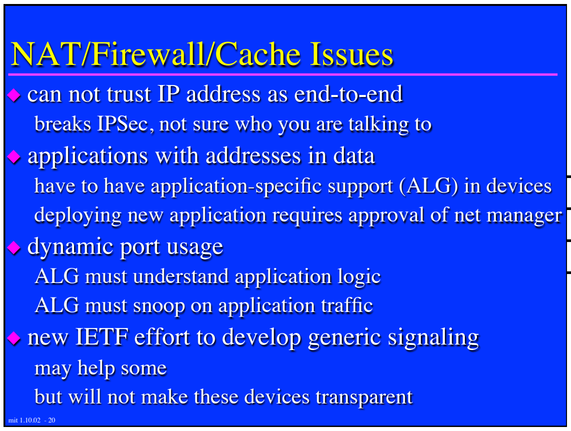
FIGURE 2.1 A four-layer model for the Open Data Network

From: Realizing the Information Future



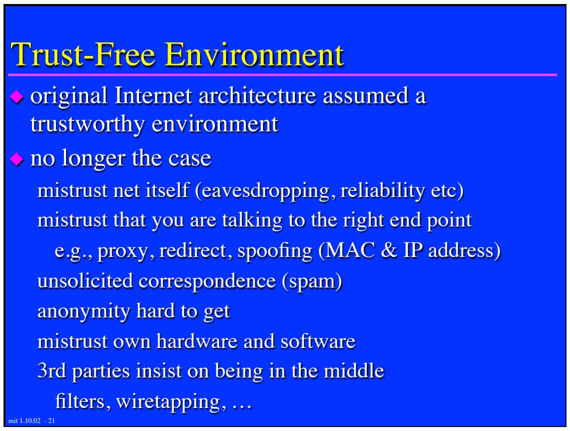
## Net is No Longer Transparent

- end-to-end argument says the net should be transparent
  - i.e. packet not modified in transit (other than TTL)
  - global-scope internetwork address
  - i.e., packet goes to address in destination address field
- transparency now gone in some cases
  - NATs, firewalls, proxies, content caches, TCP reshapers
  - replace addresses, intercept traffic, insert traffic
- other issues
  - wiretapping, taxation, content filtering



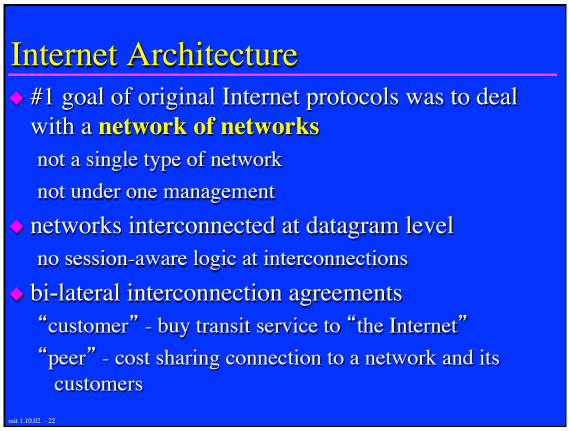
## NAT/Firewall/Cache Issues

- can not trust IP address as end-to-end
  - breaks IPSec, not sure who you are talking to
- applications with addresses in data
  - have to have application-specific support (ALG) in devices
  - deploying new application requires approval of net manager
- dynamic port usage
  - ALG must understand application logic
  - ALG must snoop on application traffic
- new IETF effort to develop generic signaling
  - may help some
  - but will not make these devices transparent



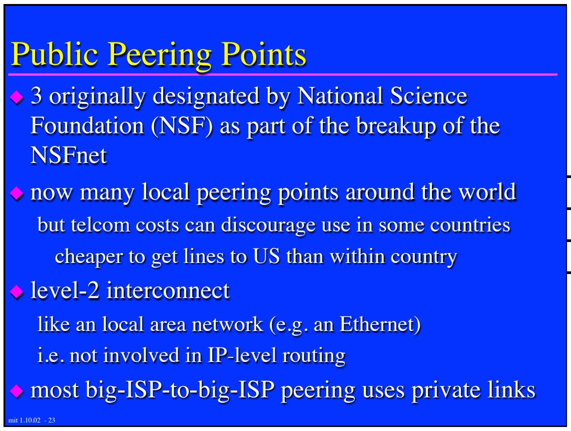
## Trust-Free Environment

- original Internet architecture assumed a trustworthy environment
- no longer the case
  - mistrust net itself (eavesdropping, reliability etc)
  - mistrust that you are talking to the right end point
    - e.g., proxy, redirect, spoofing (MAC & IP address)
  - unsolicited correspondence (spam)
  - anonymity hard to get
  - mistrust own hardware and software
  - 3rd parties insist on being in the middle
    - filters, wiretapping, …



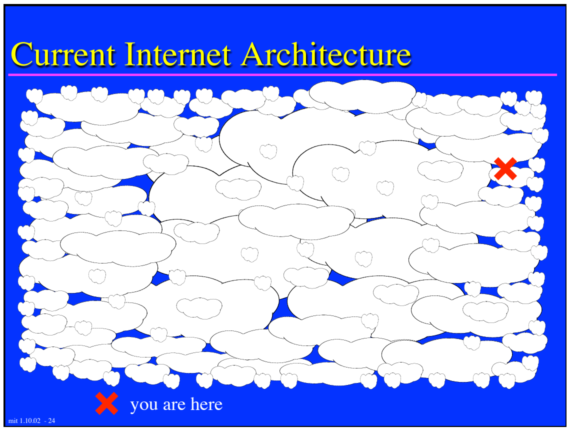
## Internet Architecture

- #1 goal of original Internet protocols was to deal with a **network of networks**
  - not a single type of network
  - not under one management
- networks interconnected at datagram level
  - no session-aware logic at interconnections
- bi-lateral interconnection agreements
  - "customer" - buy transit service to "the Internet"
  - "peer" - cost sharing connection to a network and its customers



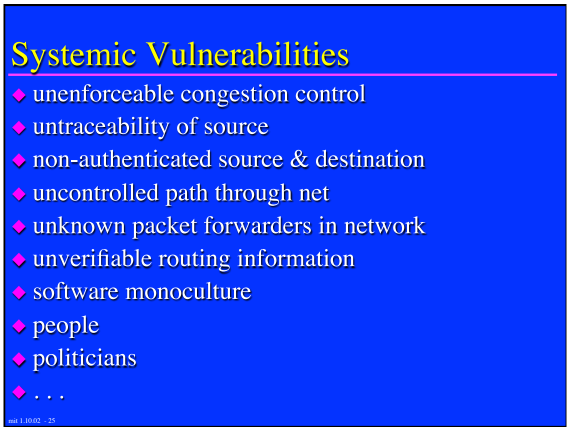
## Public Peering Points

- 3 originally designated by National Science Foundation (NSF) as part of the breakup of the NSFnet
- now many local peering points around the world
  - but telcom costs can discourage use in some countries
    - cheaper to get lines to US than within country
- level-2 interconnect
  - like an local area network (e.g. an Ethernet)
  - i.e. not involved in IP-level routing
- most big-ISP-to-big-ISP peering uses private links



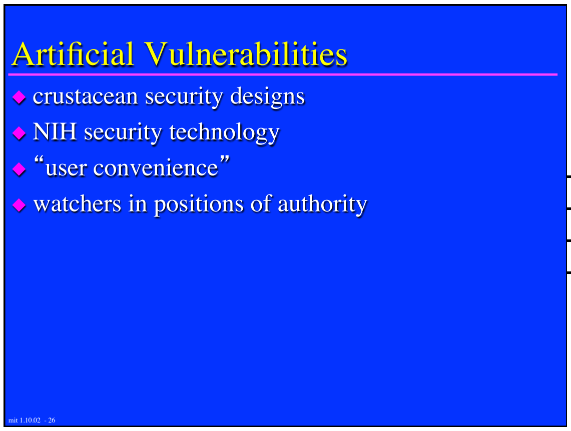
## Current Internet Architecture

✗ you are here



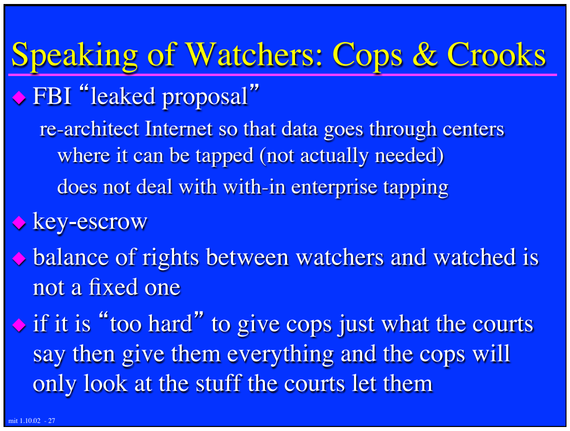
## Systemic Vulnerabilities

- unenforceable congestion control
- untraceability of source
- non-authenticated source & destination
- uncontrolled path through net
- unknown packet forwarders in network
- unverifiable routing information
- software monoculture
- people
- politicians
- . . .



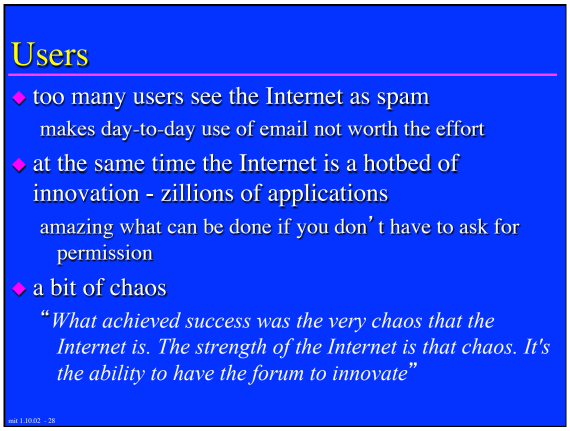
## Artificial Vulnerabilities

- crustacean security designs
- NIH security technology
- “user convenience”
- watchers in positions of authority



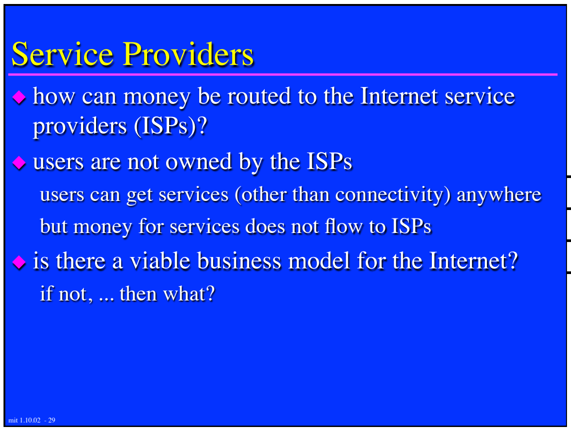
## Speaking of Watchers: Cops & Crooks

- FBI “leaked proposal”
  - re-architect Internet so that data goes through centers where it can be tapped (not actually needed)
  - does not deal with with-in enterprise tapping
- key-escrow
- balance of rights between watchers and watched is not a fixed one
- if it is “too hard” to give cops just what the courts say then give them everything and the cops will only look at the stuff the courts let them



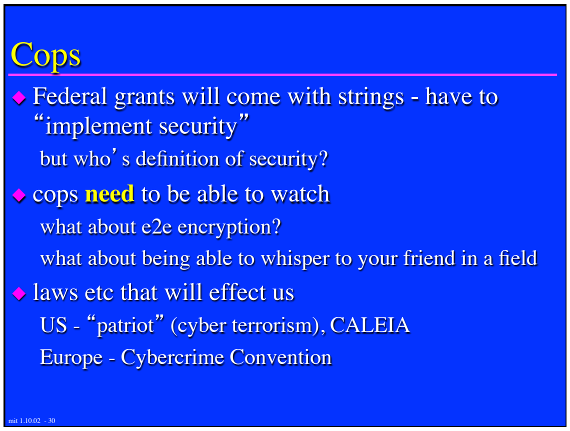
## Users

- too many users see the Internet as spam
  - makes day-to-day use of email not worth the effort
- at the same time the Internet is a hotbed of innovation - zillions of applications
  - amazing what can be done if you don’t have to ask for permission
- a bit of chaos
  - “*What achieved success was the very chaos that the Internet is. The strength of the Internet is that chaos. It's the ability to have the forum to innovate*”



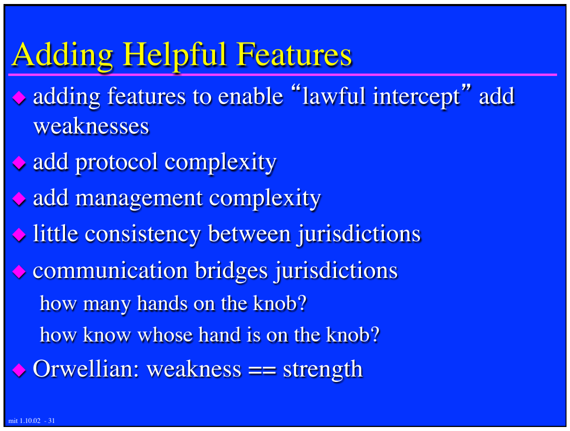
## Service Providers

- how can money be routed to the Internet service providers (ISPs)?
- users are not owned by the ISPs
  - users can get services (other than connectivity) anywhere
  - but money for services does not flow to ISPs
- is there a viable business model for the Internet?
  - if not, ... then what?



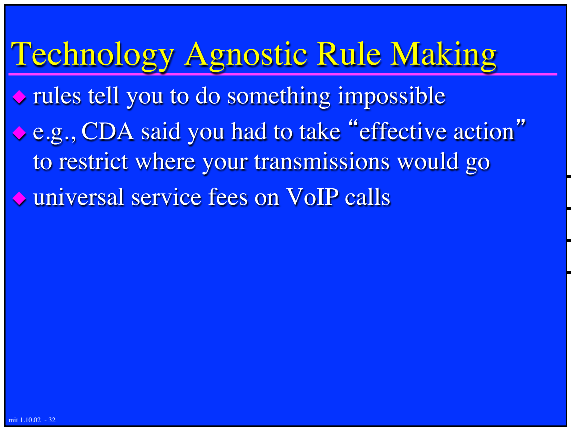
## Cops

- Federal grants will come with strings - have to “implement security”
  - but who’s definition of security?
- cops **need** to be able to watch
  - what about e2e encryption?
  - what about being able to whisper to your friend in a field
- laws etc that will effect us
  - US - “patriot” (cyber terrorism), CALEIA
  - Europe - Cybercrime Convention



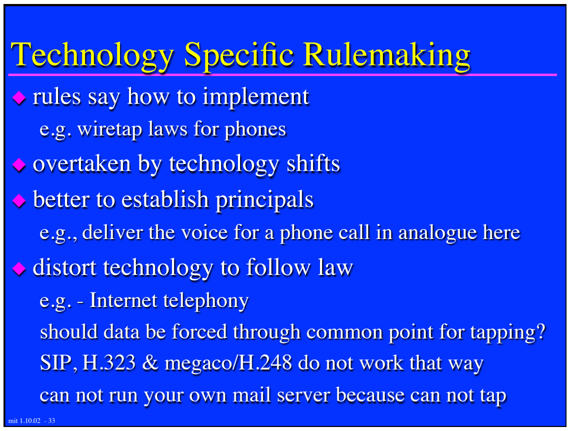
## Adding Helpful Features

- adding features to enable “lawful intercept” add weaknesses
- add protocol complexity
- add management complexity
- little consistency between jurisdictions
- communication bridges jurisdictions
  - how many hands on the knob?
  - how know whose hand is on the knob?
- Orwellian: weakness == strength



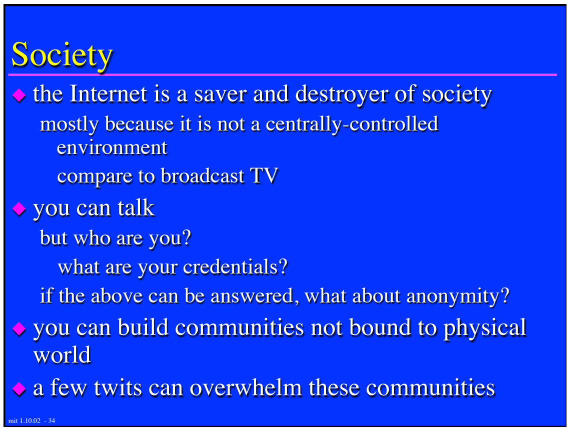
## Technology Agnostic Rule Making

- rules tell you to do something impossible
- e.g., CDA said you had to take “effective action” to restrict where your transmissions would go
- universal service fees on VoIP calls



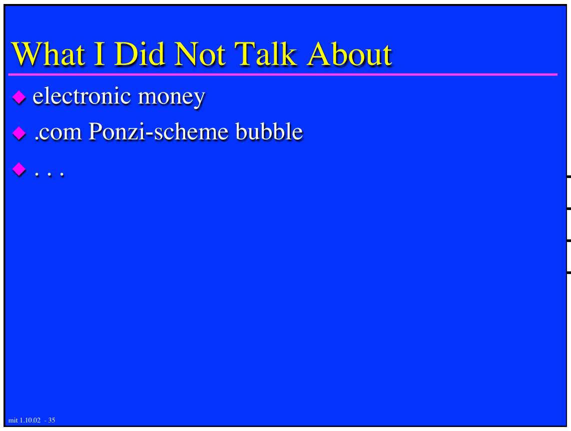
## Technology Specific Rulemaking

- rules say how to implement
  - e.g. wiretap laws for phones
- overtaken by technology shifts
- better to establish principals
  - e.g., deliver the voice for a phone call in analogue here
- distort technology to follow law
  - e.g. - Internet telephony
  - should data be forced through common point for tapping?
  - SIP, H.323 & megaco/H.248 do not work that way
  - can not run your own mail server because can not tap



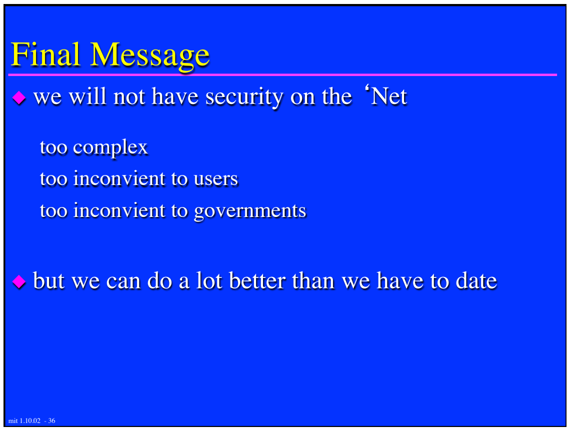
## Society

- the Internet is a saver and destroyer of society
  - mostly because it is not a centrally-controlled environment
    - compare to broadcast TV
- you can talk
  - but who are you?
    - what are your credentials?
  - if the above can be answered, what about anonymity?
- you can build communities not bound to physical world
- a few twits can overwhelm these communities



## What I Did Not Talk About

- electronic money
- .com Ponzi-scheme bubble
- . . .



## Final Message

- we will not have security on the ‘Net
  - too complex
  - too inconvient to users
  - too inconvient to governments
- but we can do a lot better than we have to date