# Internet v2.0?

## Rethinking the Internet - exemplified by Cjdns

Lasse Grinderslev Andersen

20th of July, 2015 @ The Camp

# Contents of this talk

- Introduction
- The Internet
  - History of the Internet
  - Basic mechanics
  - Challenges
- Cjdns
  - Technical outline
  - Present status
  - Future

# Contents of this talk

- Introduction
- The Internet
  - History of the Internet
  - Basic mechanics
  - Challenges
- Cjdns
  - Technical outline
  - Present status
  - Future

# Contents of this talk

- Introduction
- The Internet
  - History of the Internet
  - Basic mechanics
  - Challenges
- Cjdns
  - Technical outline
  - Present status
  - Future

## Why this talk?

- Internet is a fundamental/generative/general technology
- The Internet was made under *completely* different circumstances than today
- Cjdns is a daring (and experimental!) attempt at rethinking this basic technology.

## Why this talk?

- Internet is a fundamental/generative/general technology
- The Internet was made under *completely* different circumstances than today
- Cjdns is a daring (and experimental!) attempt at rethinking this basic technology.

## Why this talk?

- Internet is a fundamental/generative/general technology
- The Internet was made under *completely* different circumstances than today
- Cjdns is a daring (and experimental!) attempt at rethinking this basic technology.

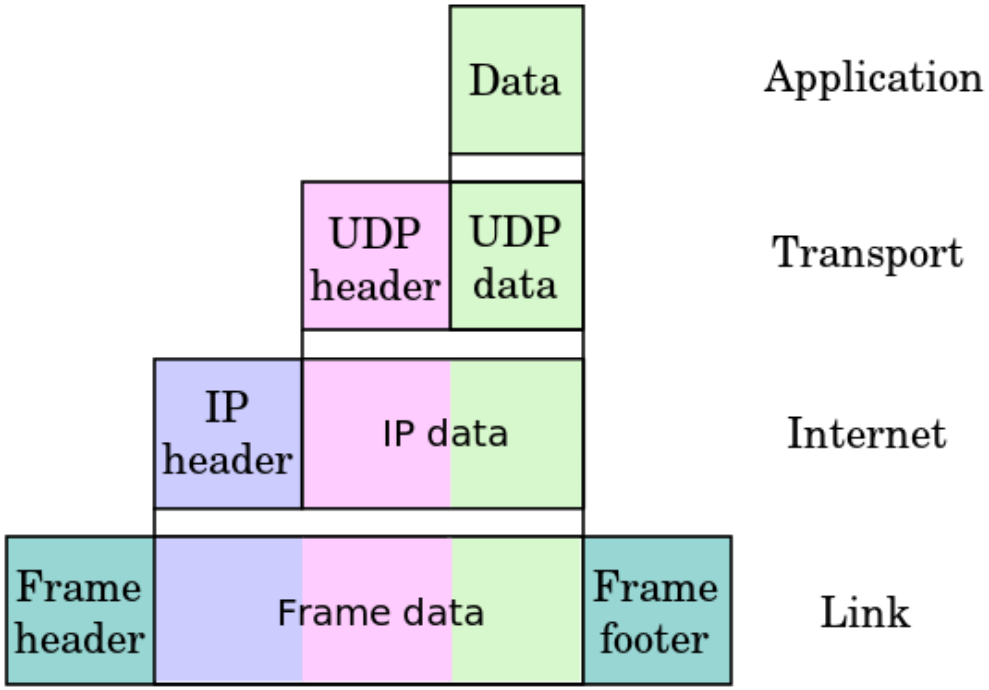
# *Rough* outline of Internet development

**<1973 Packet switching but numerous networks:**
ARPANET, CYCLADES, etc. - unable to talk!

# *Rough* outline of Internet development

**1973-83 Robert E. Kahn & Vinton Cerf (et.al) standardized communication across different networks: TCP/IP.**

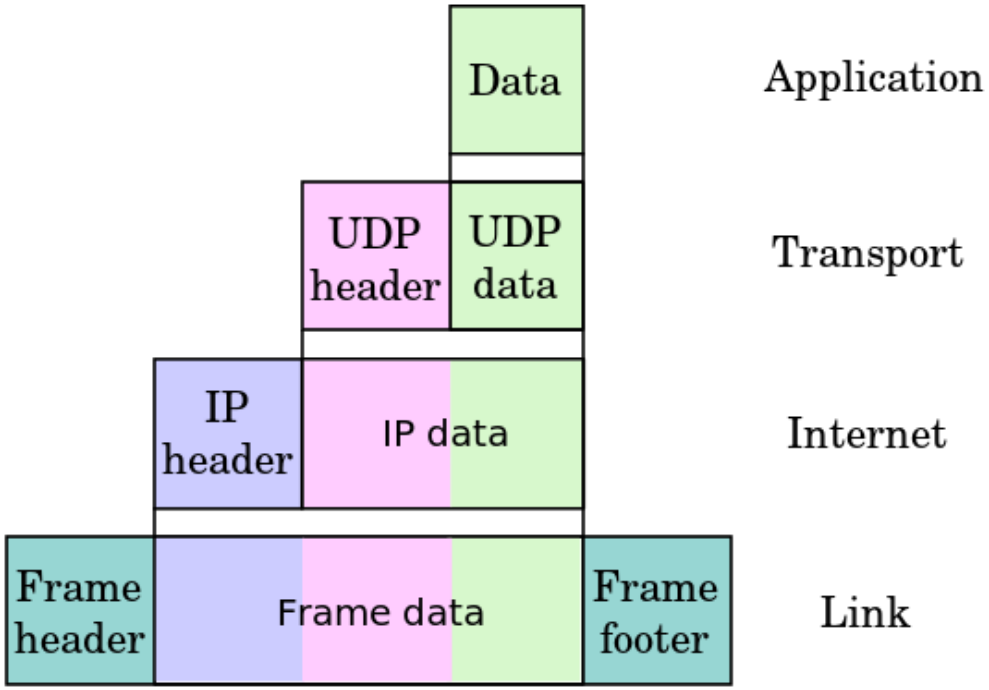
- Unique address-format across networks
- Networks connected by gateways
- Simplicity in design ⇒ End-to-end principle
- By academics for academics



# *Rough* outline of Internet development

**1973-83 Robert E. Kahn & Vinton Cerf (et.al) standardized communication across different networks: TCP/IP.**

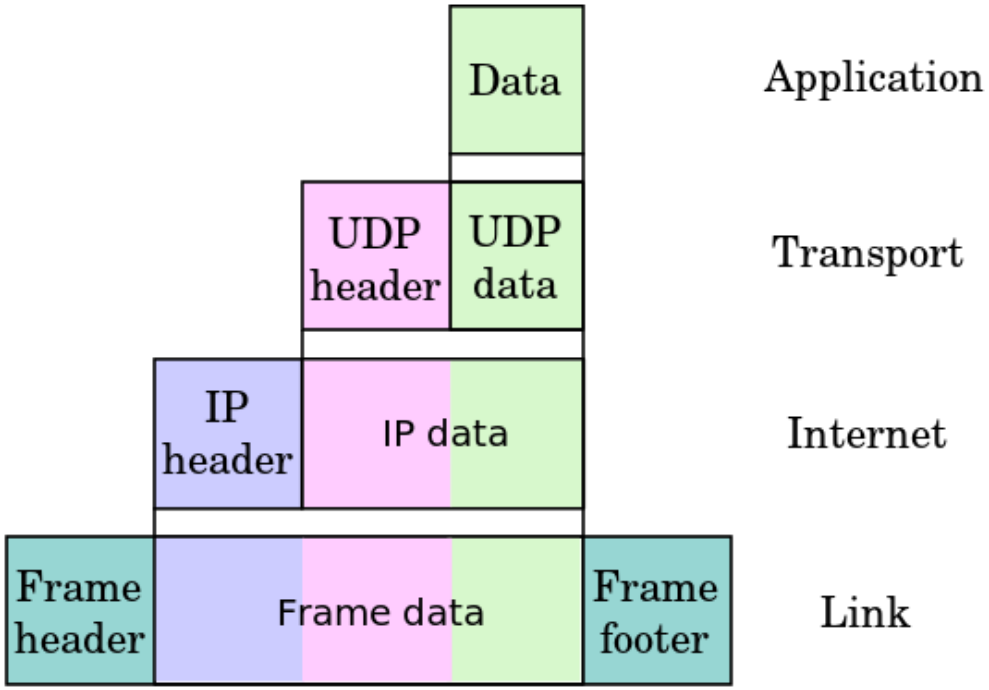
- Unique address-format across networks
- Networks connected by gateways
- Simplicity in design ⇒ End-to-end principle
- By academics for academics



# *Rough* outline of Internet development

**1973-83 Robert E. Kahn & Vinton Cerf (et.al) standardized communication across different networks: TCP/IP.**

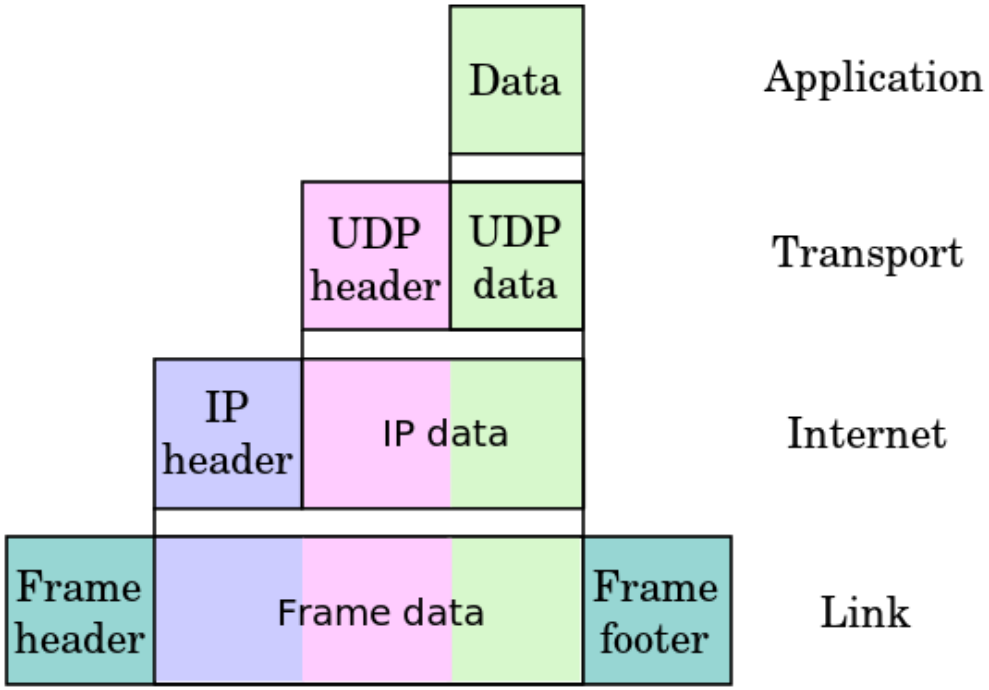
- Unique address-format across networks
- Networks connected by gateways
- Simplicity in design ⇒ End-to-end principle
- By academics for academics



# *Rough* outline of Internet development

**1973-83 Robert E. Kahn & Vinton Cerf (et.al) standardized communication across different networks: TCP/IP.**

- Unique address-format across networks
- Networks connected by gateways
- Simplicity in design ⇒ End-to-end principle
- By academics for academics



# *Rough* outline of Internet development

**1983-90 Gradual commercialisation**:

- Military part of ARPANET broke off in 1983.
- Several US government bodies working on TCP/IP networks, NASA, NSF, Dept. of Energy etc.

# *Rough* outline of Internet development

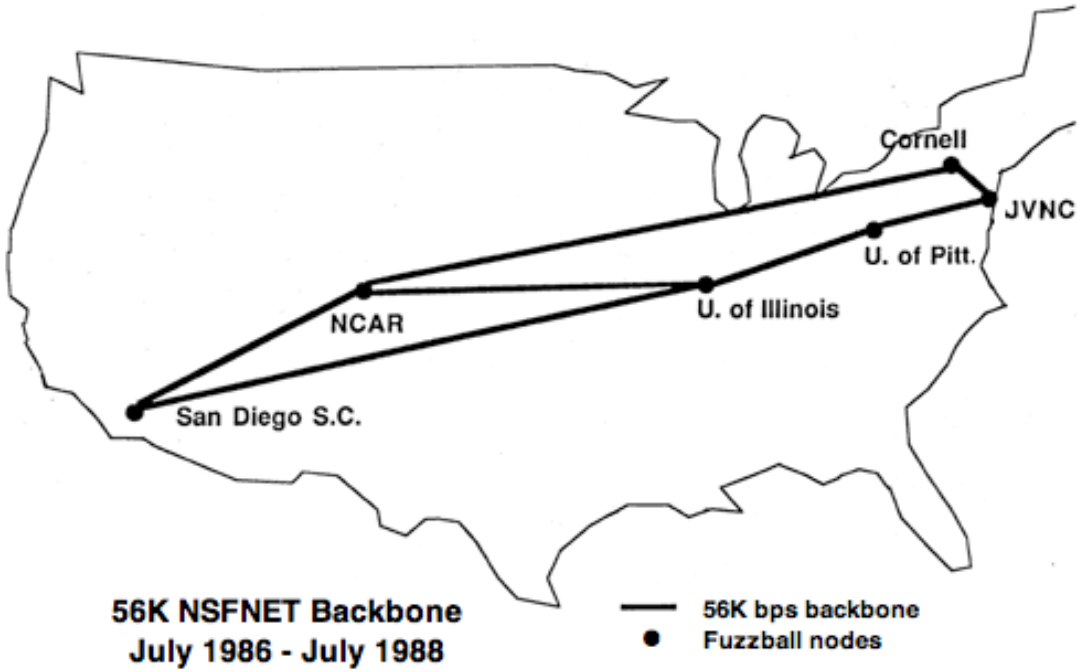
**1983-90 Gradual commercialisation**:

- Military part of ARPANET broke off in 1983.
- Several US government bodies working on TCP/IP networks, NASA, NSF, Dept. of Energy etc.

# *Rough* outline of Internet development

**1983-90 Gradual commercialisation**:

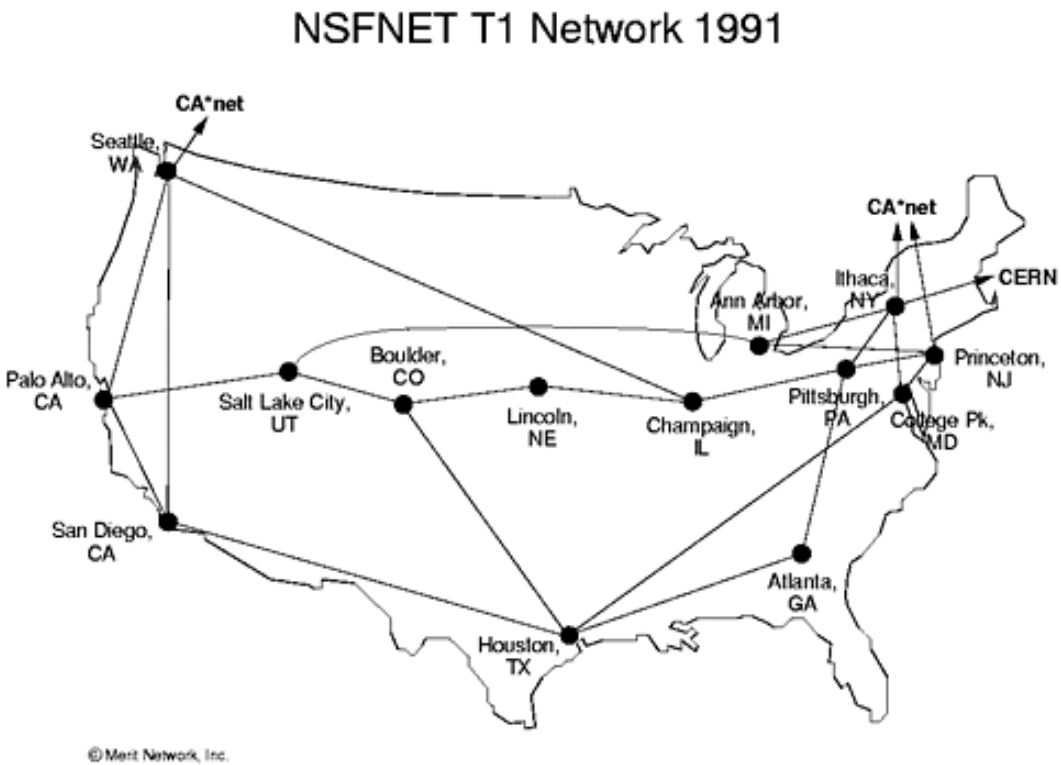
- 1986 NSFNET started up: Six 56kbit/s backbones connecting universities and their super computers. "primarily for research and education in the sciences and engineering."



# *Rough* outline of Internet development

**1983-90 Gradual commercialisation**:

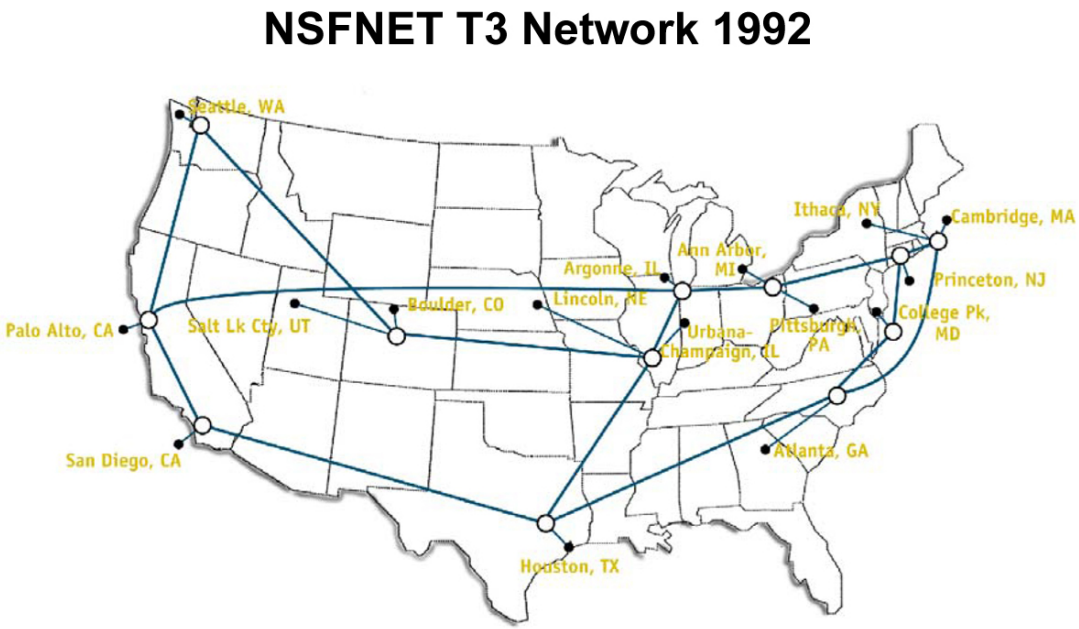
- 1988 T1 upgrade: Thirteen 1.5mbit/s backbones. Many networks joined in, e.g., NASA (NSN), US Military (MILNET) etc. ARPANET decomissioned 1990.



# *Rough* outline of Internet development

**1983-90 Gradual commercialisation**:

- 1991 T3 upgrade: Sixteen 45mbit/s backbones.
- 1995 Goverment backbones replaced by commerical ISPs.



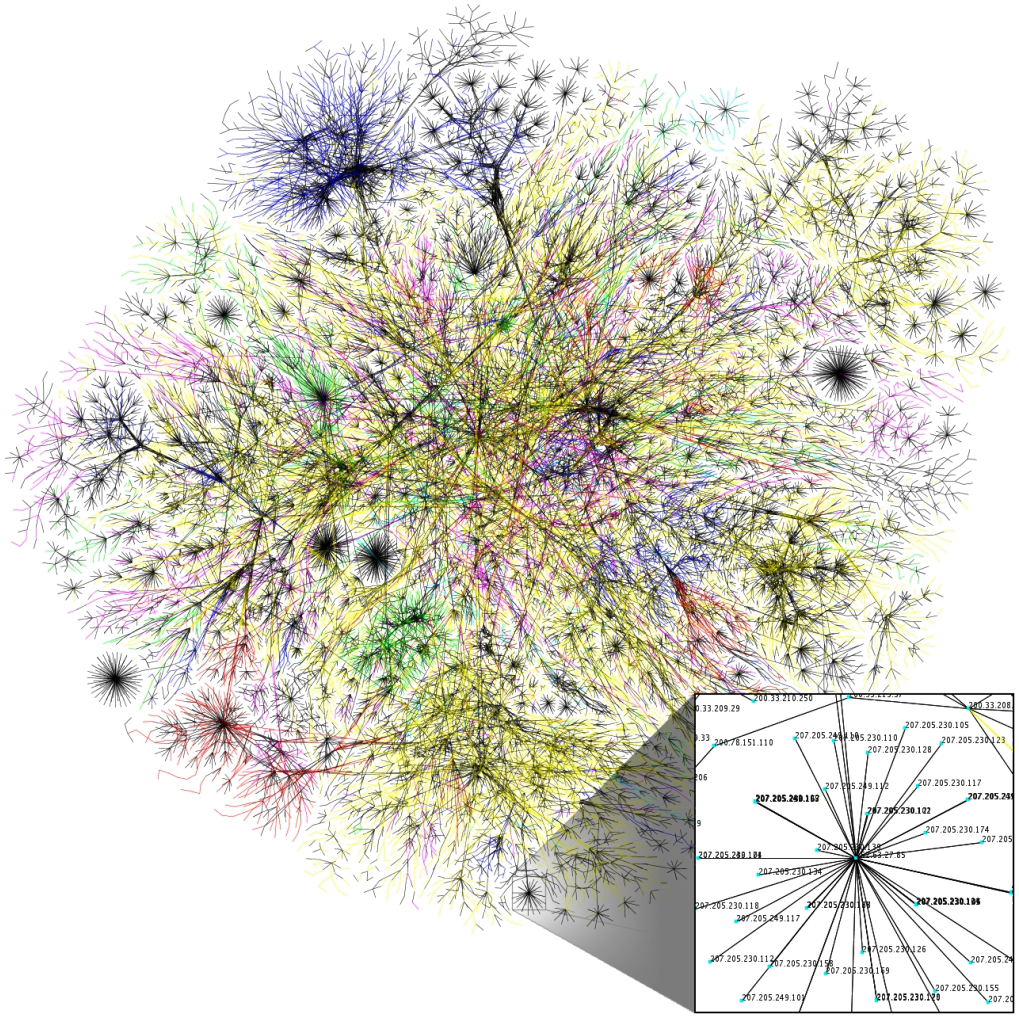
# The Internet now

**Basic functioning of the Internet:**

- AS numbers and IP blocks are delegated by IANA
- AS holders routes prefixes to each other using BGP

## Basic functioning of the Internet:

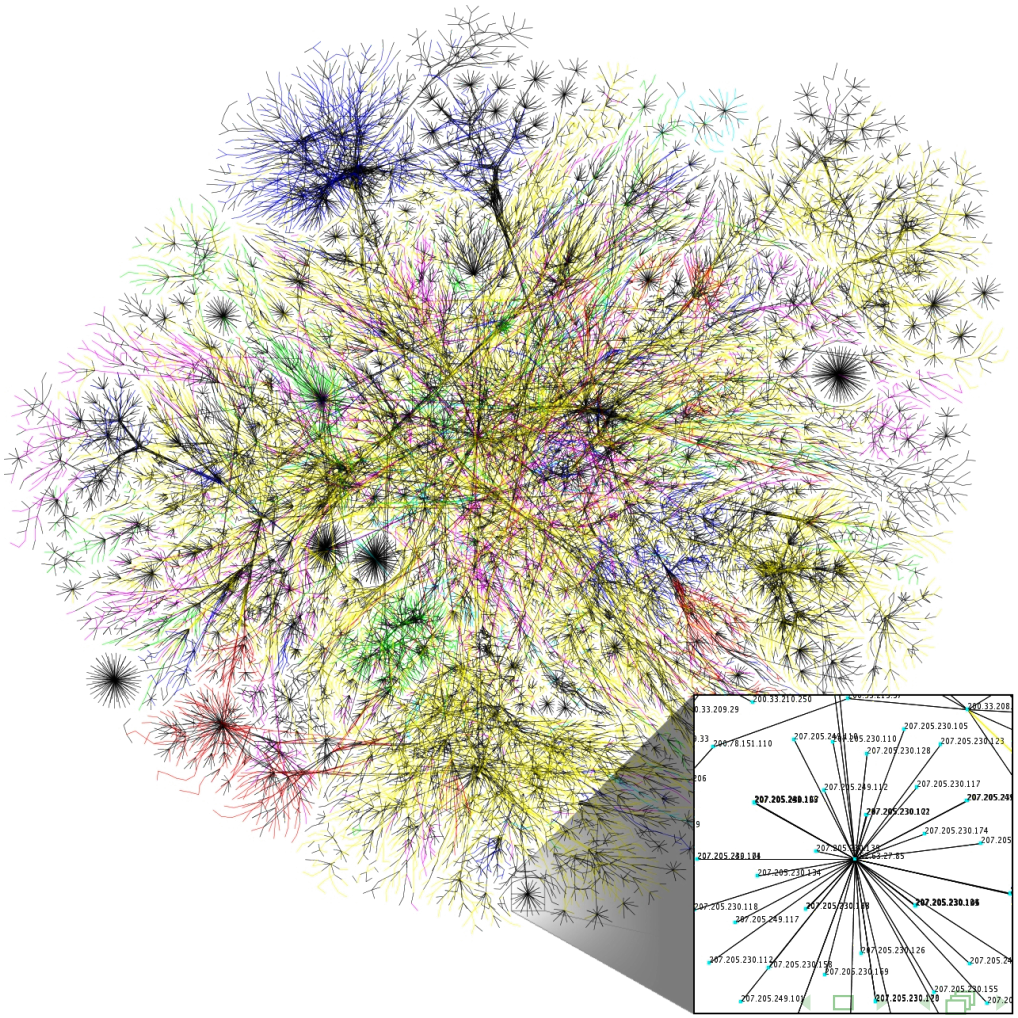
### Huge network but security was not built into core protocols



# The Internet now - challenges

**Issues & solutions**

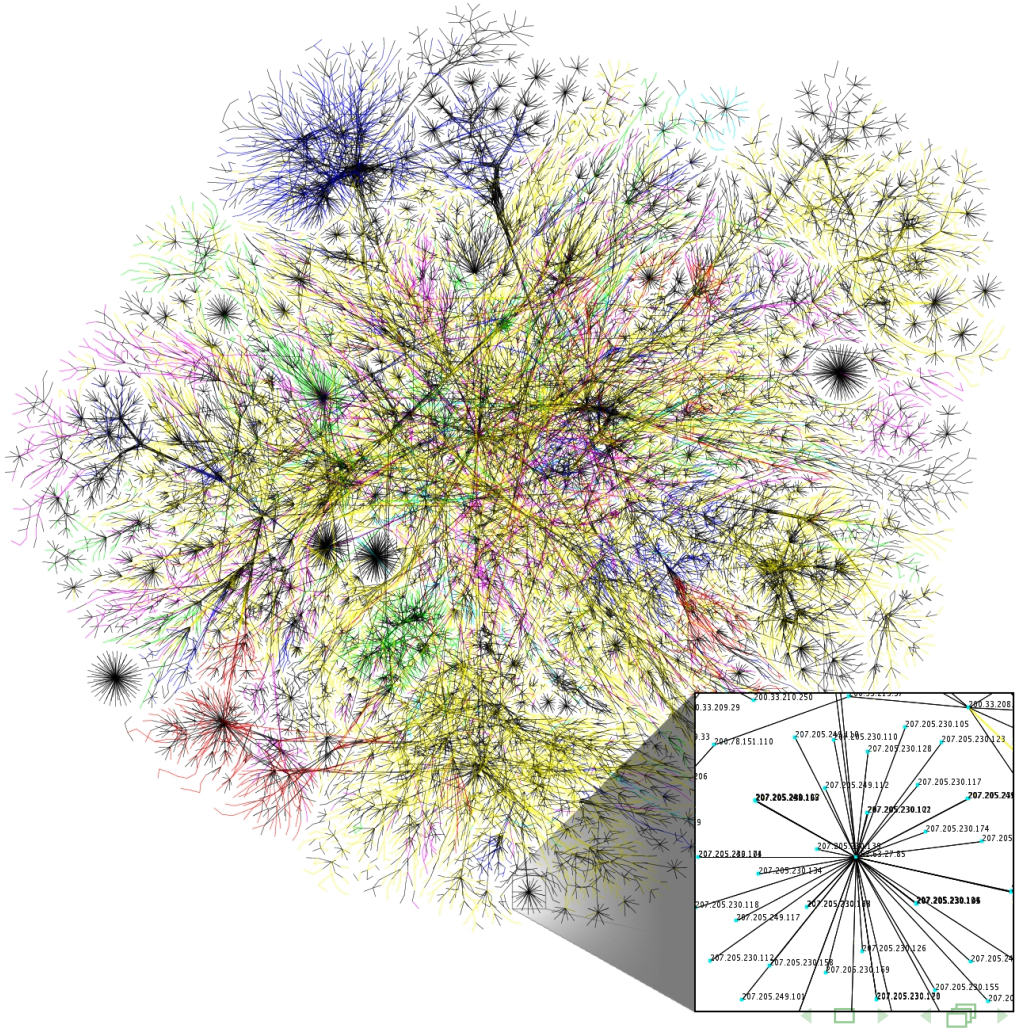
- **Data encryption** ⇒ TLS/SSL, VPN, IPSEC
- **Authenticity** ⇒ CA, CRL, OCSP (stapling), DNSSEC, PGP



# The Internet now - challenges

**Issues & solutions**

- **Route hijacking** $\Rightarrow$ BGPSEC (RPKI)
- **Centralized administration of network addresses**



# Cjdns - Overview

What Cjdns **isn't**:

- Tor replacement
- Something to do with DNS (yes, silly name!)

What Cjdns **tries** to be:

- Decentralized routing
  (friend-2-friend, no central address management)
- Secure (data encryption & authenticity)
- Modular (generate address and connect to peer)

*A system is only secure if nobody has total control.*
- Caleb James DeLisle

# Cjdns - Overview

What Cjdns **isn't**:

- Tor replacement
- Something to do with DNS (yes, silly name!)

What Cjdns **tries** to be:

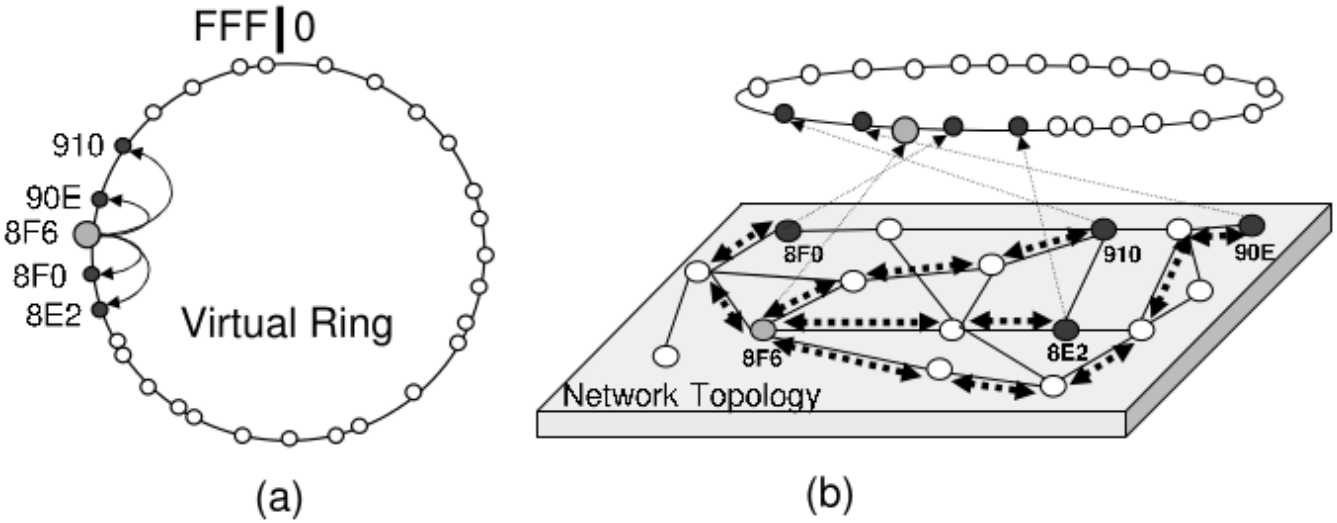
- Decentralized routing
  (friend-2-friend, no central address management)
- Secure (data encryption & authenticity)
- Modular (generate address and connect to peer)

*A system is only secure if nobody has total control.*
- Caleb James DeLisle

# Cjdns - Overview

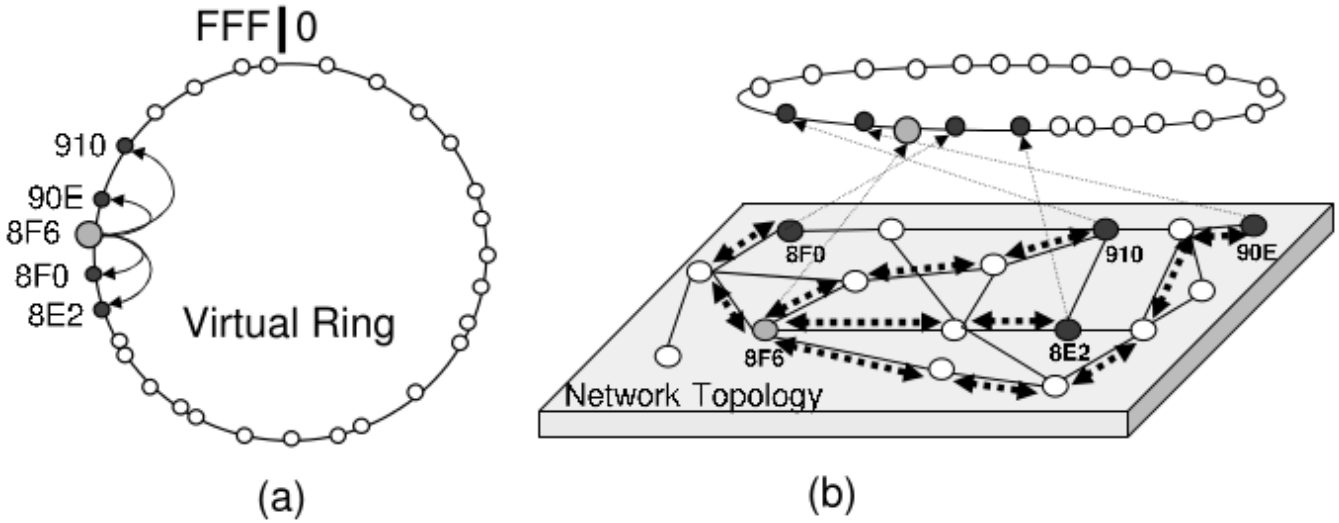
Overall architecture

- Decentralized routing layer (DHT) using pub-keys as virtual addresses
- Simple packet switching/forwarding layer
- Crypto-layer creating encrypted tunnels for sending down packets



# Cjdns - Routing

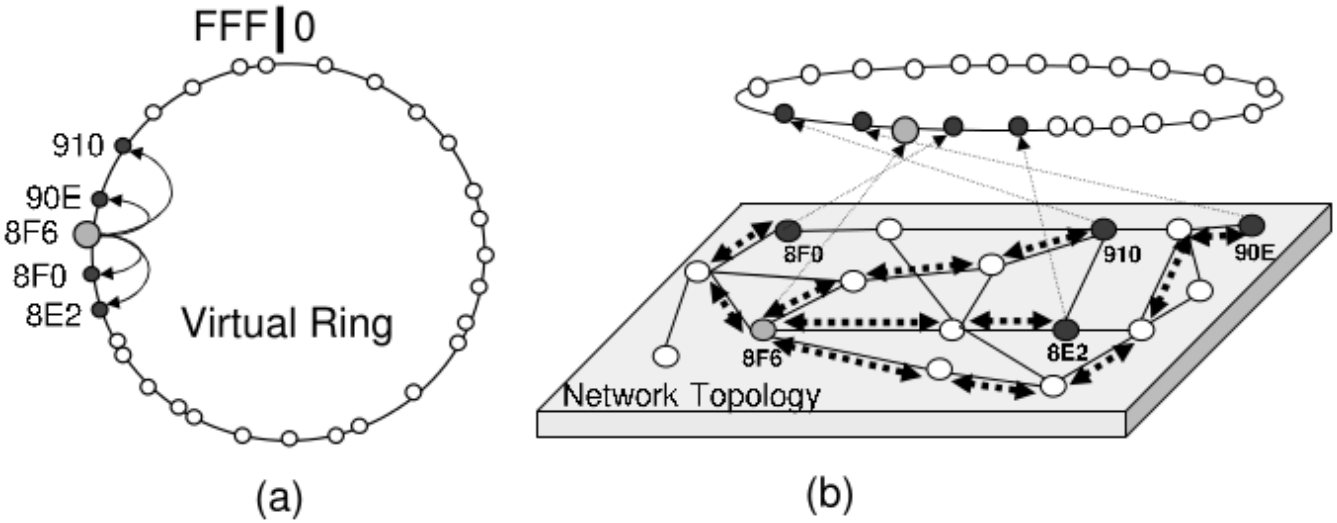
- Separation between physical links and address space
- Virtual address space used to locate nodes by routers
- Pub-keys as addresses $\Rightarrow$ identity-integrity at *transport layer*.
- Hash of pubkey used as ipv6 address (fc00:/9)



# Cjdns - Switching

Sending packets does not require the router:

- Routing label: Network path expressed as series of switch-directors
- Switching labels are not unique and vary in size
- When a packet travels through the network the label is changed s.t. the return label is obtained by reversing the route label.



# Cjdns - Crypto & Security

Tunnels of encrypted traffic are created between node

- Verified by address/pubkey but using symmetric encryption (afaik)
- $\Rightarrow$ infeasible to eavesdrop
- $\Rightarrow$ man-in-the-middle attack infeasible

No need to use encryption in applications
and relying on CA/DNS for identity!

...although malicious nodes can advertise false routes

# Cjdns - Status/challenges

Uses of cjdns atm.

- hyperboria: Global (testing) network based on 'friend-2-friend' peering (few public nodes)
- Use in meshnets, e.g, in Seattle, Vancouve, London etc. Some of these also provide internet tunneling.
- Russia?

Highly experimental, not well-documented etc.

# Cjdns - future

Future uses:

- Global network for privacy/hackers/computer entusiasts?
- Privacy enhancement?

Developments:

- Anycast?
- CIDR-style blocks?

# Cjdns - future

**Inspect/test routing/network discovery algorithms and design details.**

Tak for jeres opmærksomhed! :-)