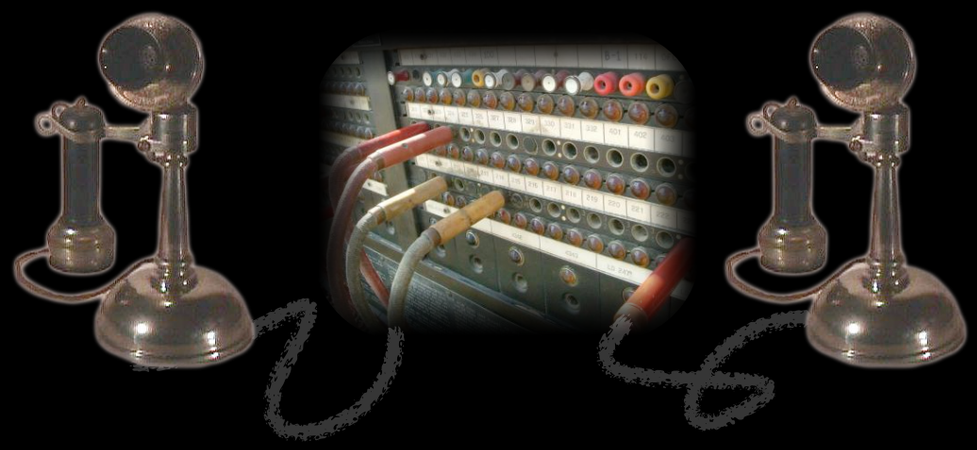
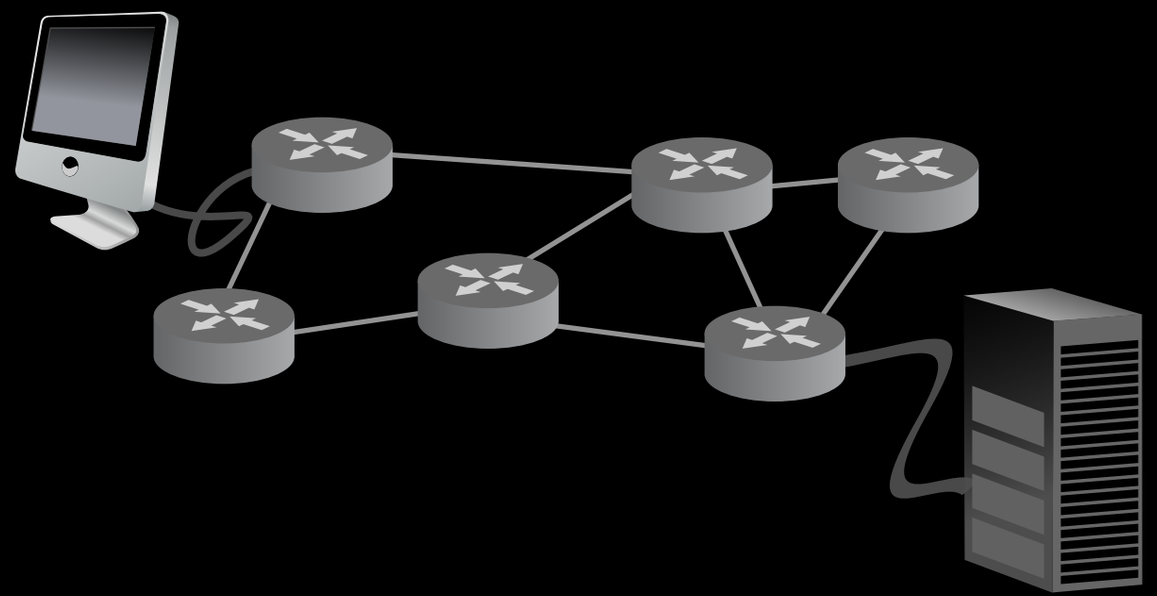
CCN / NDN

Van Jacobson
Palo Alto Research Center (PARC)

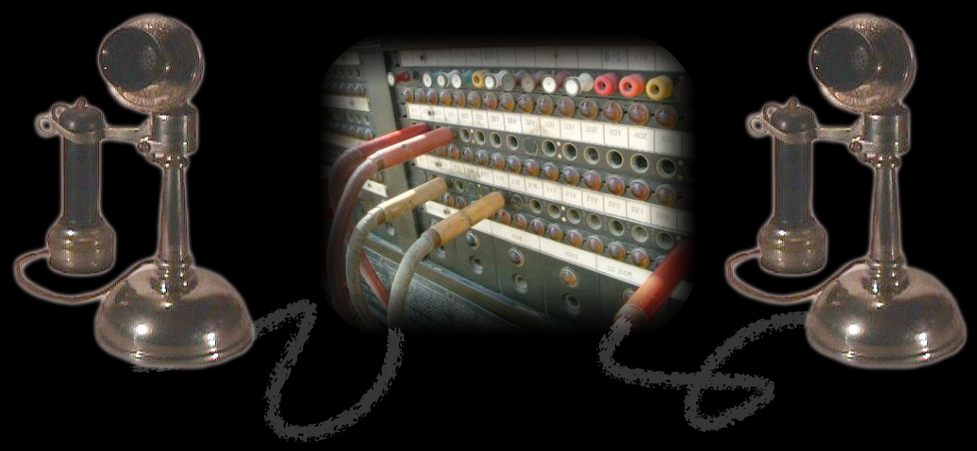
Global Future Internet Summit
Seoul, Korea
30 November 2011

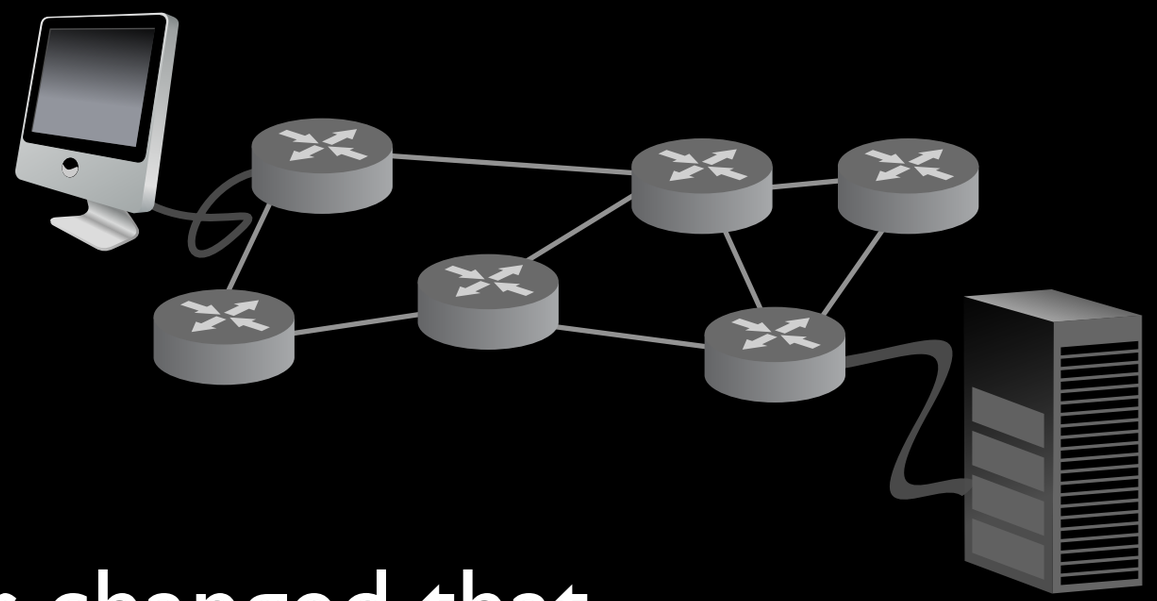
For 150 years ‘communication’ has meant
a conversation over a wire connecting two devices:





For 150 years ‘communication’ has meant
a conversation over a wire connecting two devices:





For consumers, the Web forever changed that.
The information matters, not how or where you get it.


RESERVE BANK OF INDIA
$1
NEGARA BRUNEI DARUSSALAM
SATU RINGGIT
Bank of England
FIVE
Pounds
0424661184
ORANJESTAD
ARUBA
FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
E40450785E
1000
MIL
PESETAS
NARODOWY BANK POLSKI
BANCA NATIONALĂ A REPUBLICII SOCIALISTE ROMANIA
ZWANZIG
SCHILLING
10
6094310
NARODNA BANKA
JUGOSLAVIJE
Bank Centrali ta' Malta
ŻEWĠ
LIRI
NORGES BANK
4200546460
50
FEMTI


RESERVE BANK OF INDIA
NEGARA BRUNEI DARUSSALAM
SATU RINGGIT
Bank of England
FIVE
Pounds
ORANJESTAD
ARUBA
FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
NARODOWY BANK POLSKI
MIL
PESETAS
BANCA NATIONALĂ A REPUBLICII SOCIALISTE ROMANIA
ZWANZIG
SCHILLING
NORGES BANK
50
FEMTI
Bank Centrali ta' Malta
ŻEWĠ
LIRI


RESERVE BANK OF INDIA
NEGARA BRUNEI DARUSSALAM
SATU RINGGIT
Bank of England
FIVE
Pounds
ORANJESTAD
ARUBA
THE UNITED STATES OF AMERICA
NARODOWY BANK POLSKI
BANCA NATIONALĂ A REPUBLICII SOCIALISTE ROMANIA
ZWANZIG
SCHILLING
Bank Centrali ta' Malta
ŻEWĠ
LIRI
NORGES BANK
FEMTI


NEWS

A home information inventory – 2007

- 30,000 songs 300 GB
- 1,000 movies 300 GB
- 40,000 pictures 200 GB

71,000 items 800 GB

A home information inventory – 2007

- 30,000 songs 300 GB
- 1,000 movies 300 GB
- 40,000 pictures 200 GB

71,000 items **800 GB**

Way beyond human capacity

Where information lives

Where information lives

We're drowning in bits and our machines don't help

- Our interaction with content must evolve to a higher level than moving individual items.
- People should specify policy, machines should implement it:
  - I tell our media server to store my pictures.
  - I tell my cameras that they're mine.
  - ➡ New pictures move to the media servers as soon as a camera's in proximity.

To implement our policies machines need *context*

- *Ontology* (how is this information related to other information)
- *Provenance* (what is my relationship to the source of this information)
- *Locality* (what is my proximity to this information)

Reducing friction

- Moving up-level is an amplifier.
  - We shouldn't amplify mistakes.
    (E.g., if you accidentally delete a file anywhere, FolderShare makes sure it's deleted everywhere.)
  - We shouldn't amplify attacks.
    (Machines need a very high level of confidence in context & data integrity).

- CCN gets rid of a useless abstraction (the host and file that contain the bits) and captures:
  - *Ontology* via hierarchical names and links.
  - *Provenance* via signing the binding between the bits and their name (“Z asserts that X is his name for Y”)
  - *Locality* via a “guided diffusion” dissemination model.
- CCN reduces friction by moving from a ‘container’ to a ‘collection’ model.

Making content move itself

Making content move itself

- Devices express 'interest' in data collections.
- Devices with data in collection respond.

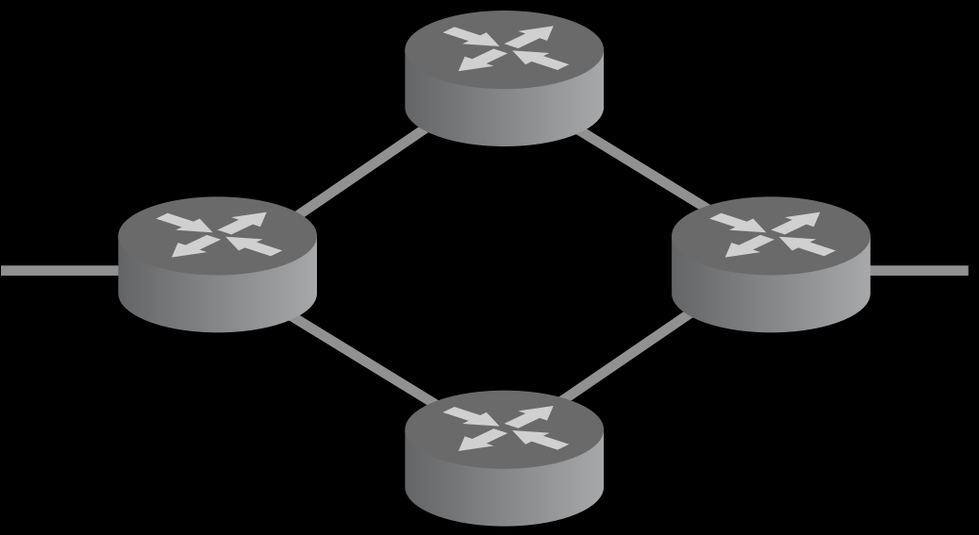
Making content move itself

van's calendar?

pointless mtg 08:30

- Devices express 'interest' in data collections.
- Devices with data in collection respond.

- Users specify the objective, not how to accomplish it.
- Data appears wherever it needs to be.
- Model loves wireless and broadcast (802.11, RFID, Bluetooth, NFC, ...).
- Data security and integrity are the architectural foundation, not an add-on.
- There's no distinction between bits in a memory and bits in a wire.



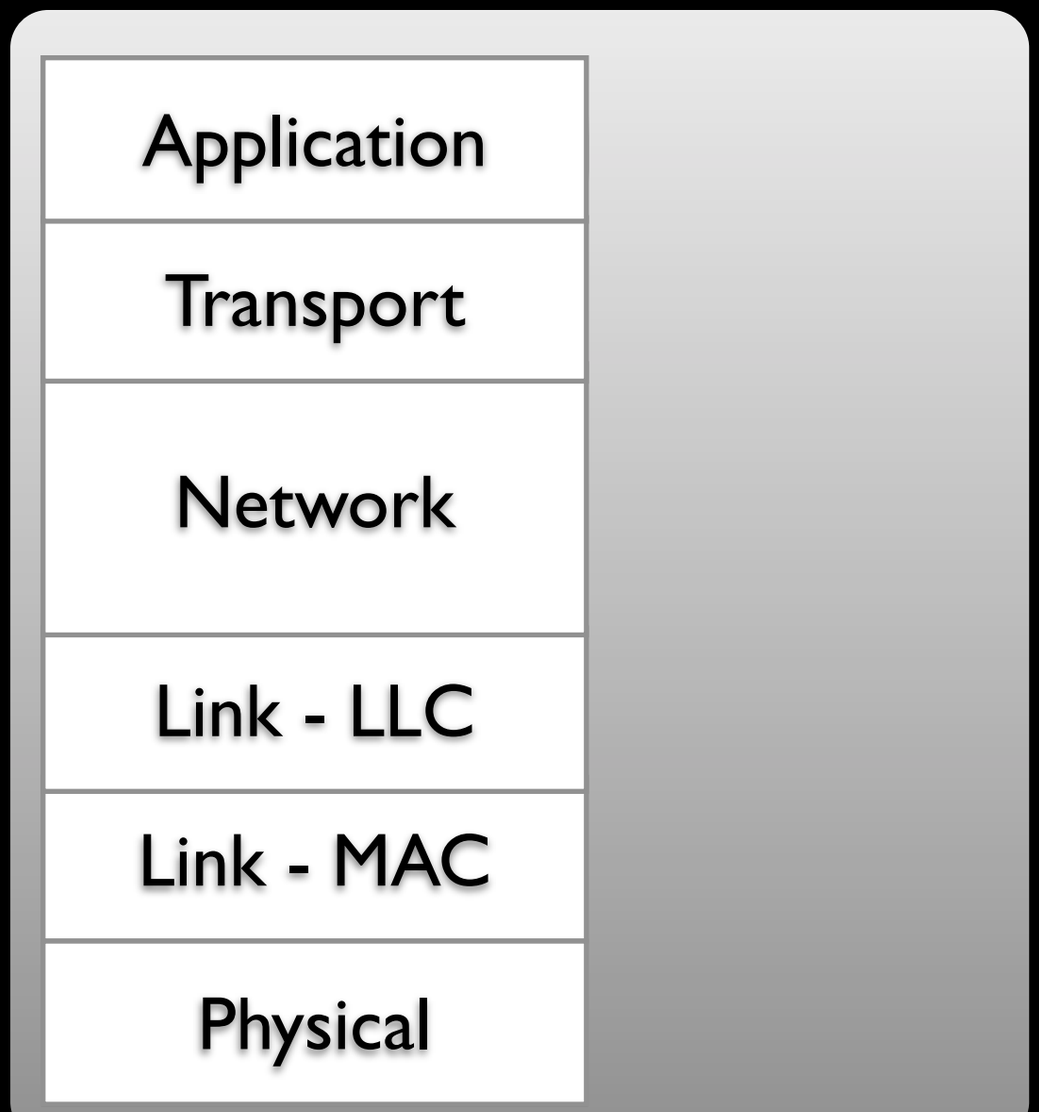
Today's network architecture
embraces wires & interconnects

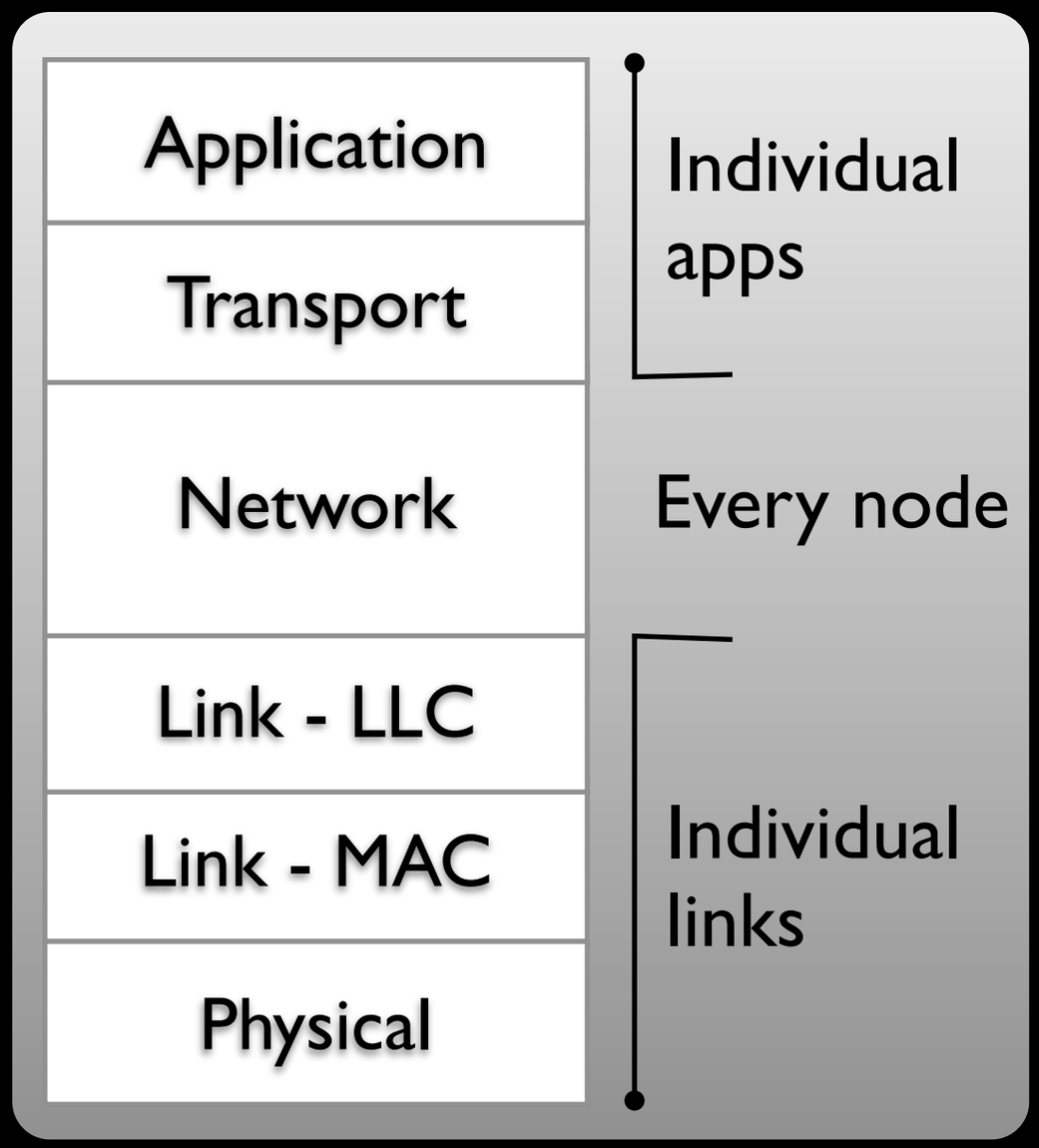
but not cycles or storage.

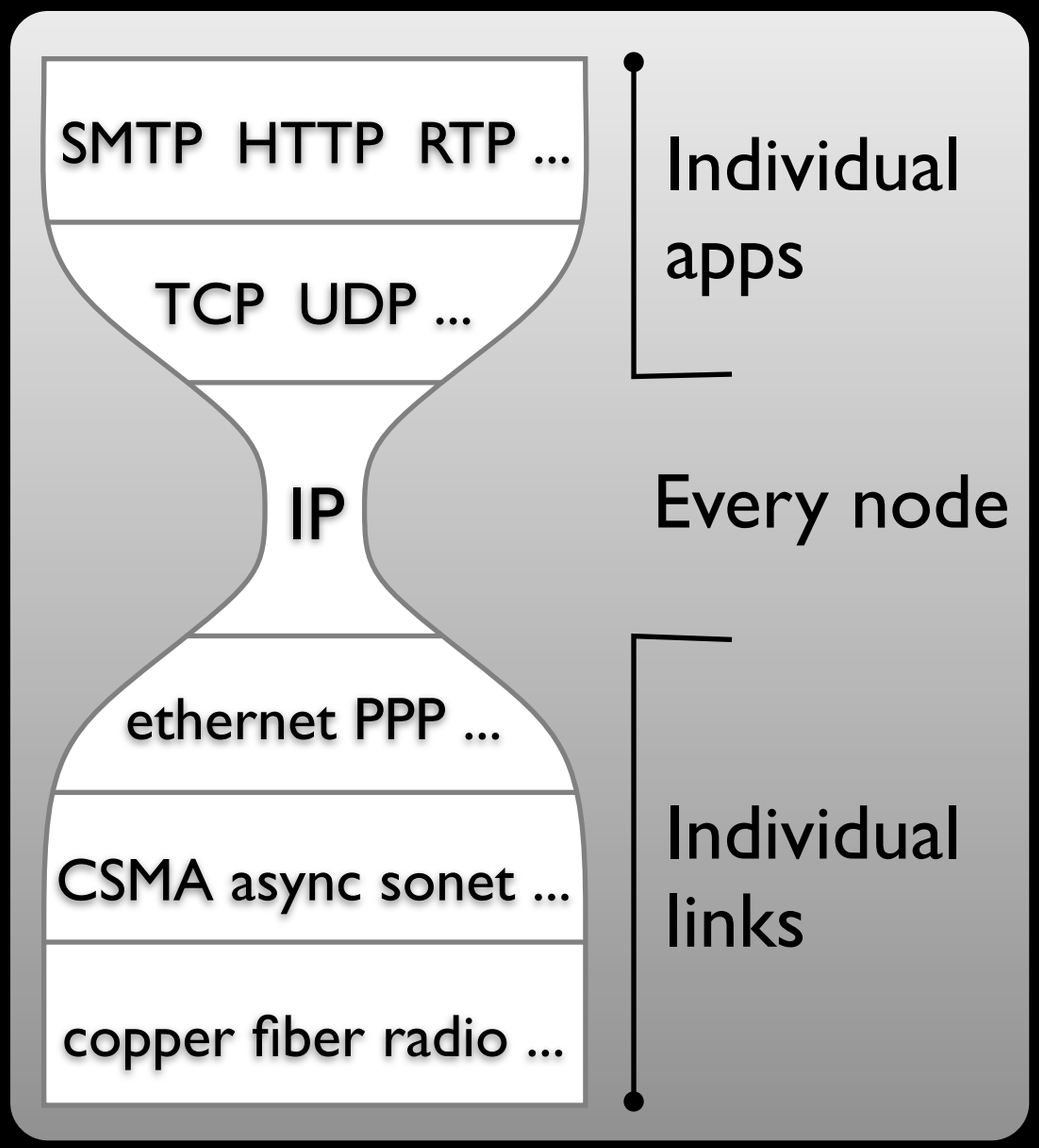
They are different only because we conceptualize in terms of *process* rather than *outcome*.

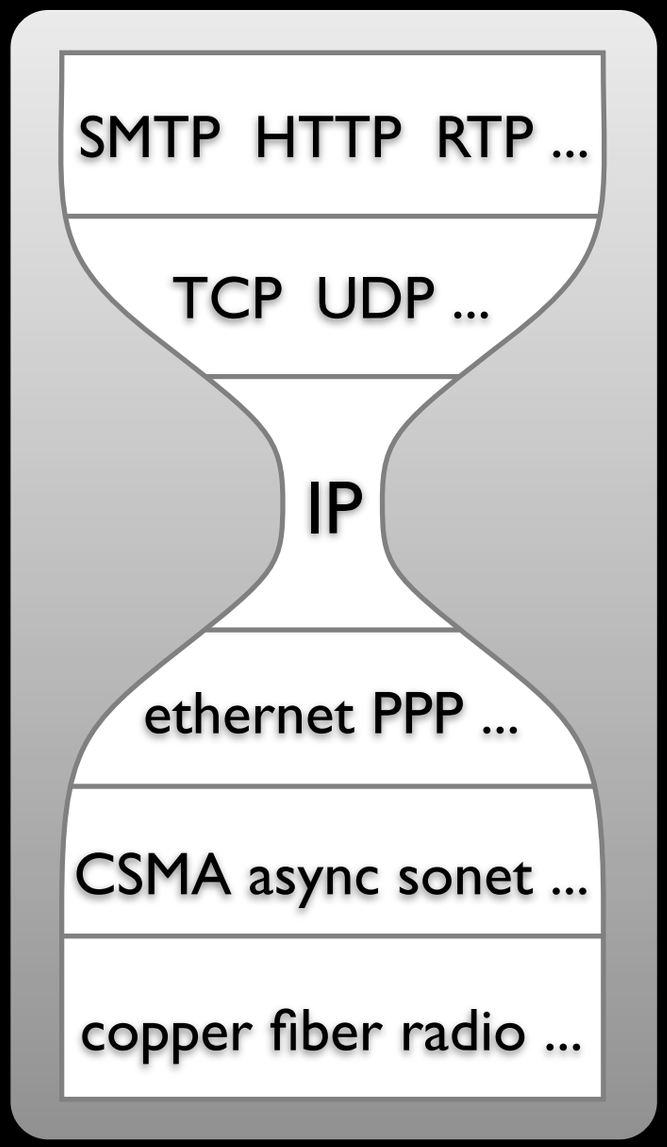
If we view networking as *information delivery*
all three can work together seamlessly.

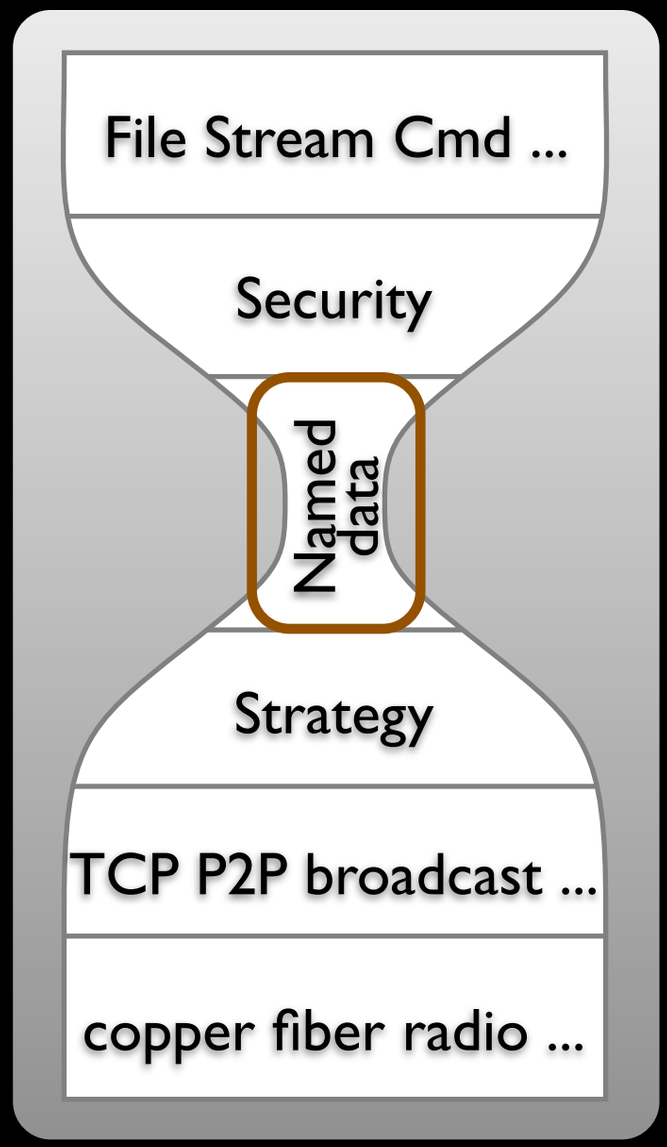
Architecture

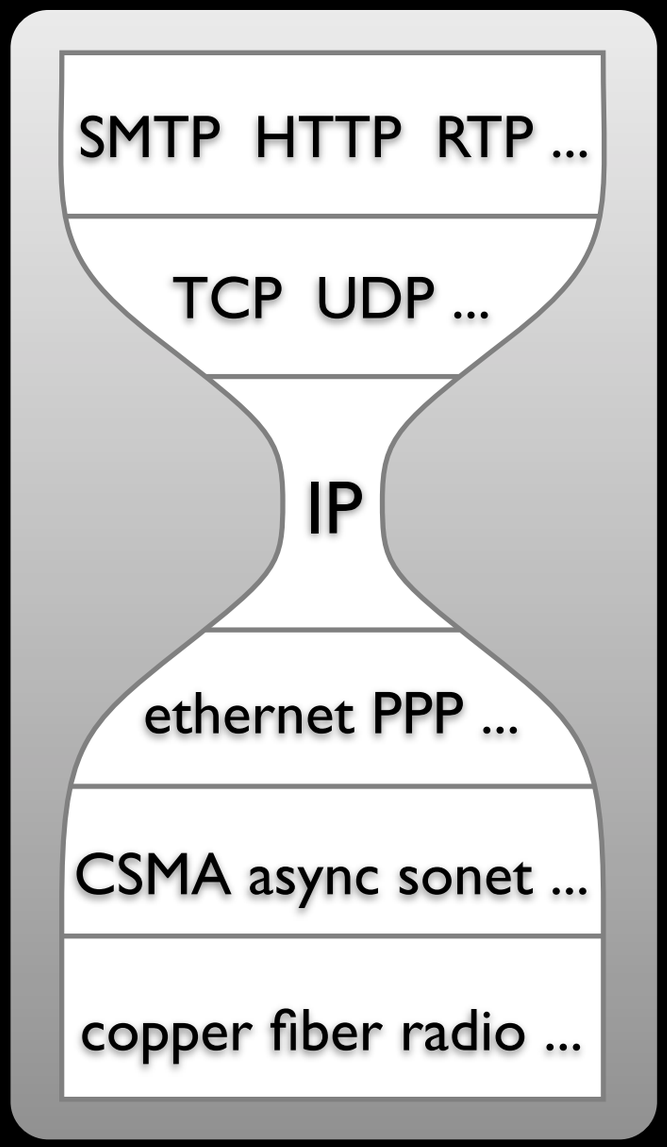

Application
Transport
Network
Link - LLC
Link - MAC
Physical

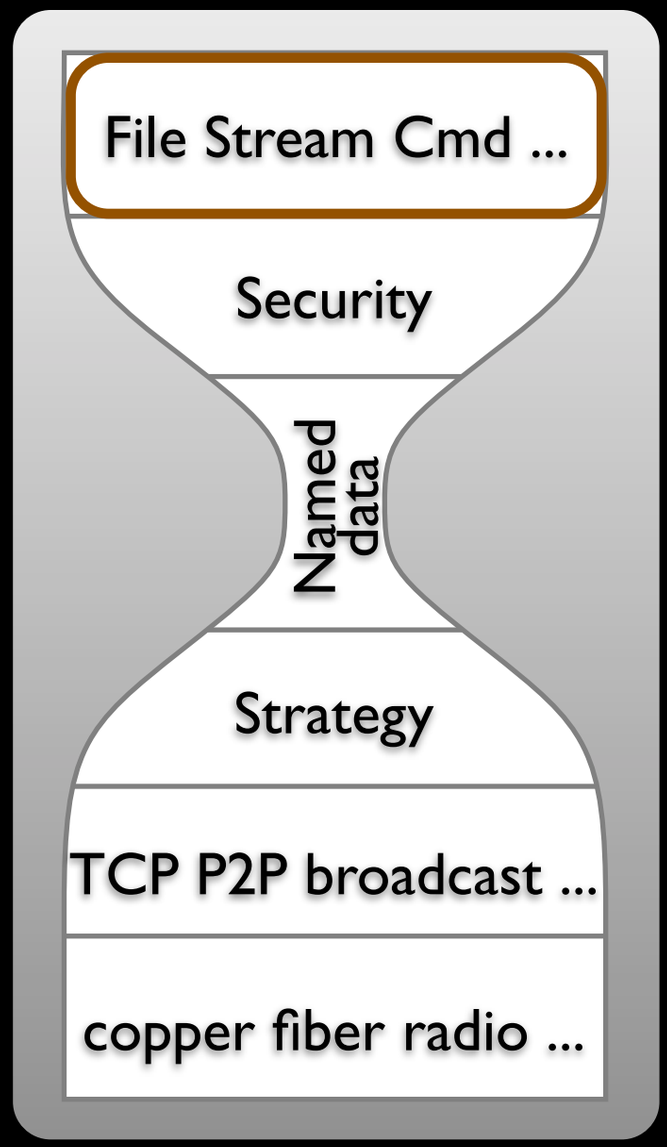

Application
Transport
Network
Link - LLC
Link - MAC
Physical
Individual apps
Every node
Individual links

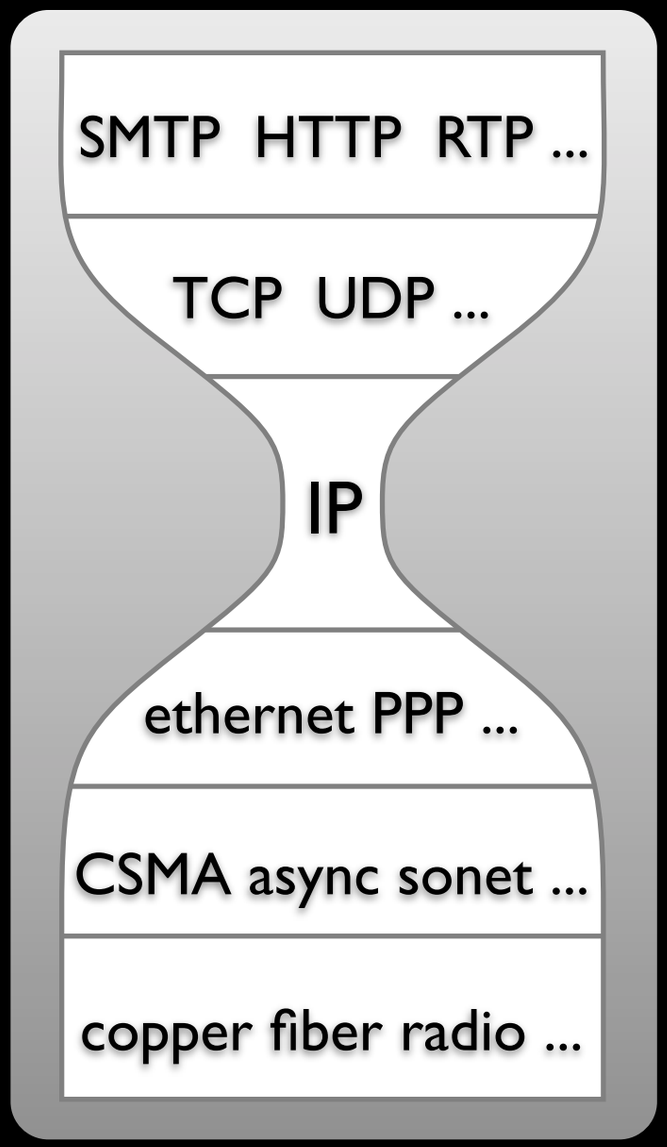

SMTP HTTP RTP ...
TCP UDP ...
IP
ethernet PPP ...
CSMA async sonet ...
copper fiber radio ...
Individual apps
Every node
Individual links

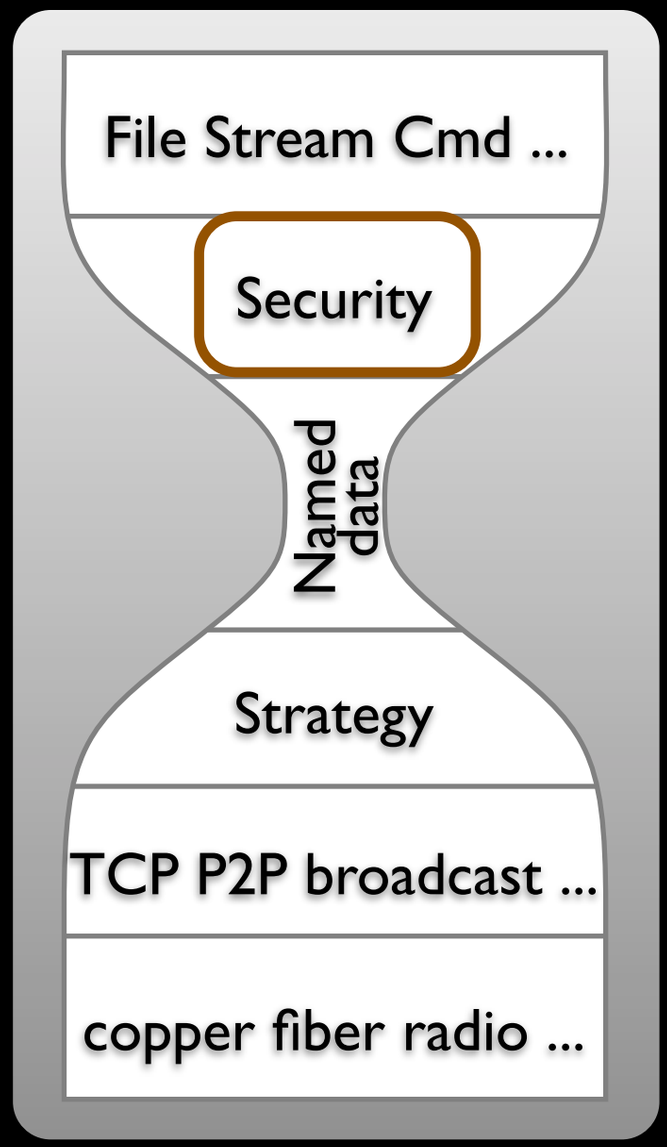

SMTP HTTP RTP ...
TCP UDP ...
IP
ethernet PPP ...
CSMA async sonet ...
copper fiber radio ...

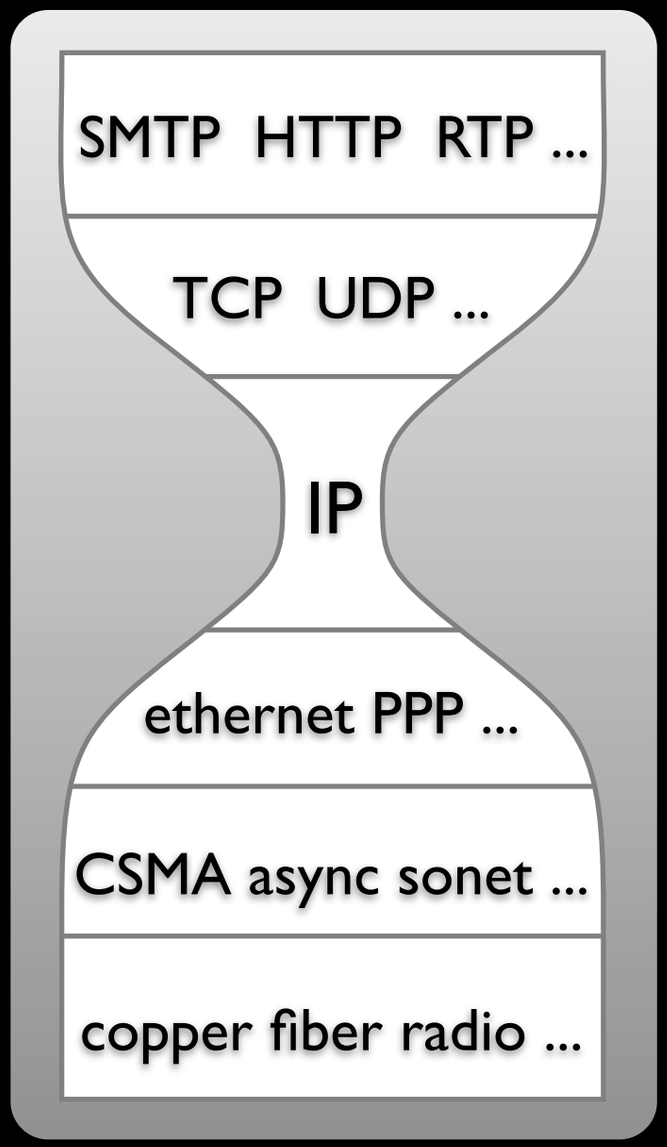

File Stream Cmd ...
Security
Named data
Strategy
TCP P2P broadcast ...
copper fiber radio ...

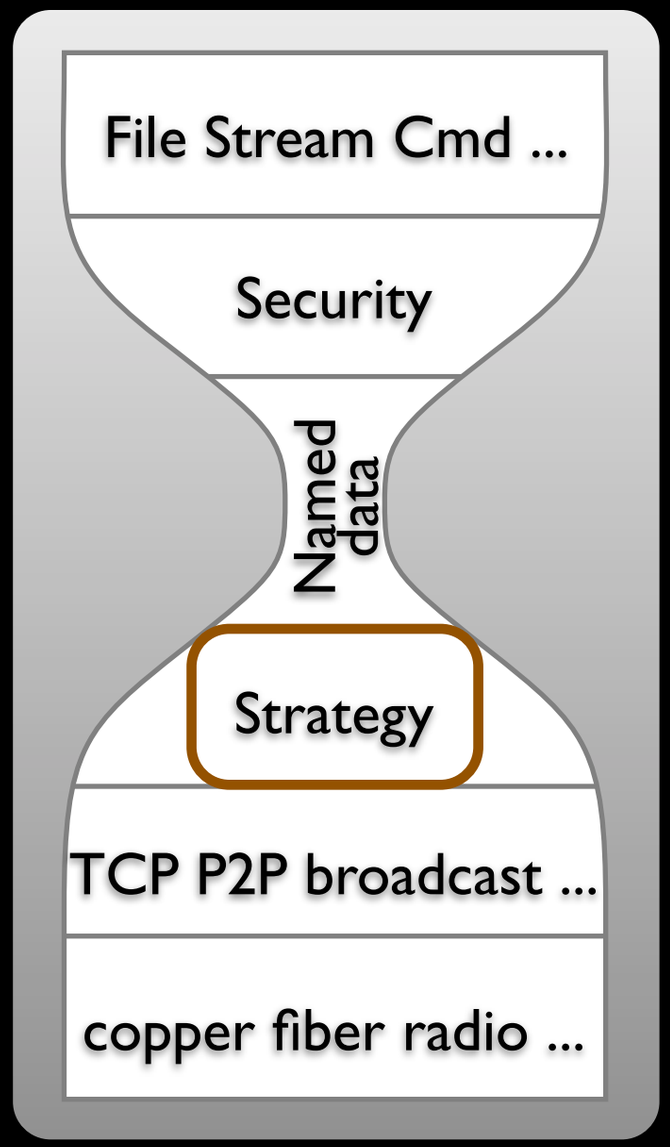

SMTP HTTP RTP ...
TCP UDP ...
IP
ethernet PPP ...
CSMA async sonet ...
copper fiber radio ...

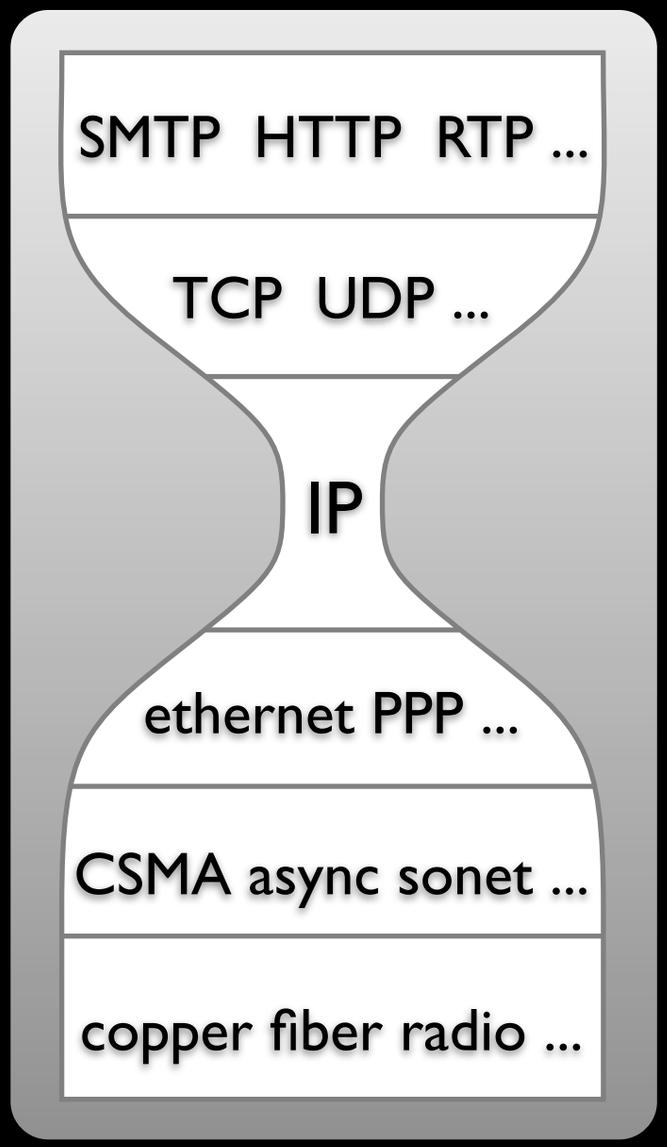

File Stream Cmd ...
Security
Named data
Strategy
TCP P2P broadcast ...
copper fiber radio ...

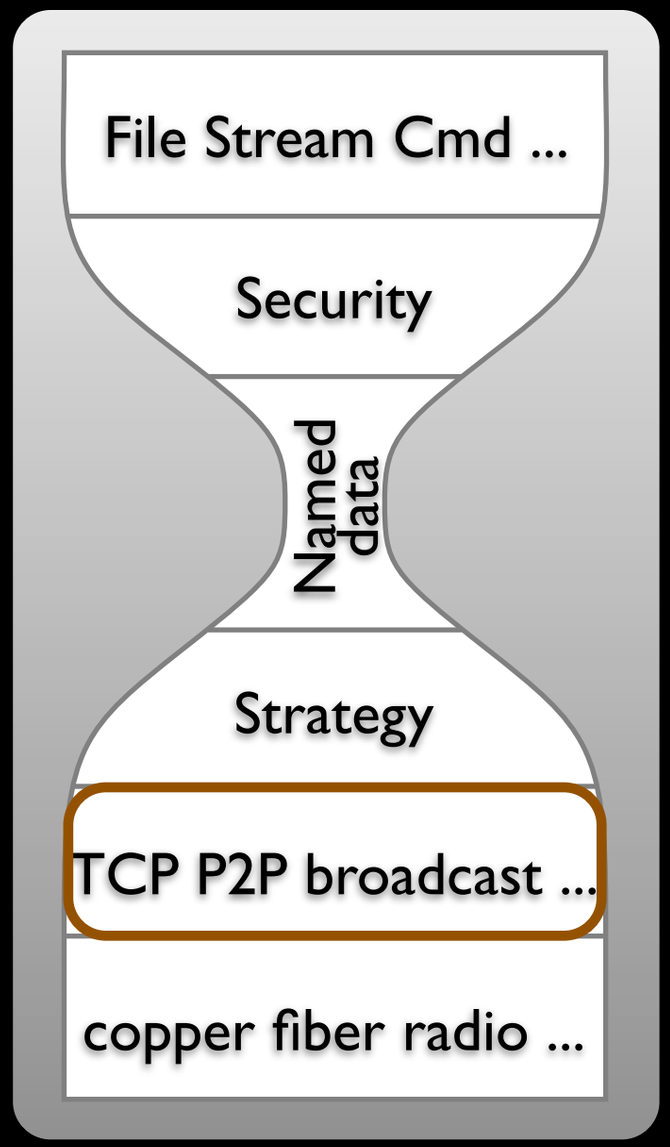

SMTP HTTP RTP ...
TCP UDP ...
IP
ethernet PPP ...
CSMA async sonet ...
copper fiber radio ...

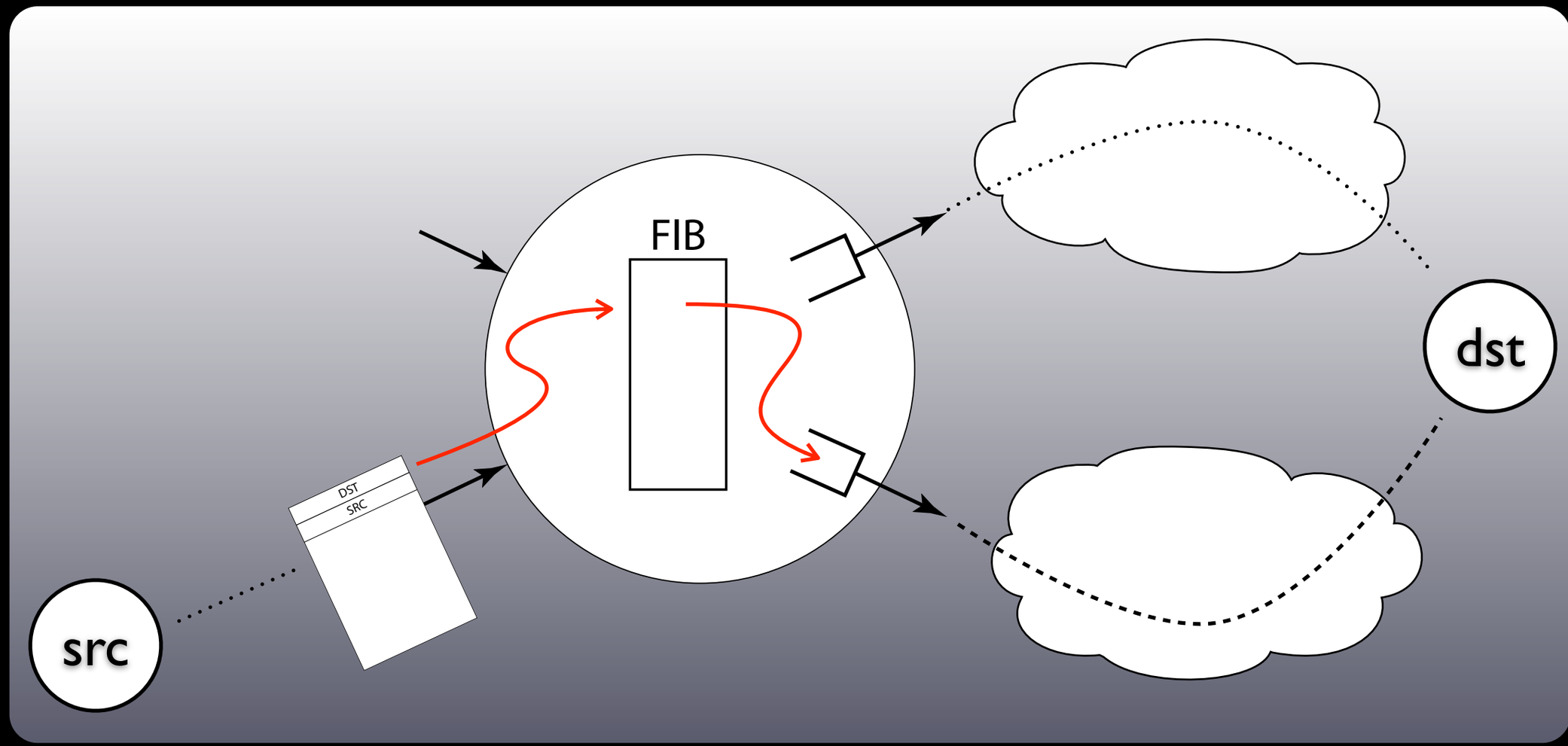

File Stream Cmd ...
Security
Named data
Strategy
TCP P2P broadcast ...
copper fiber radio ...

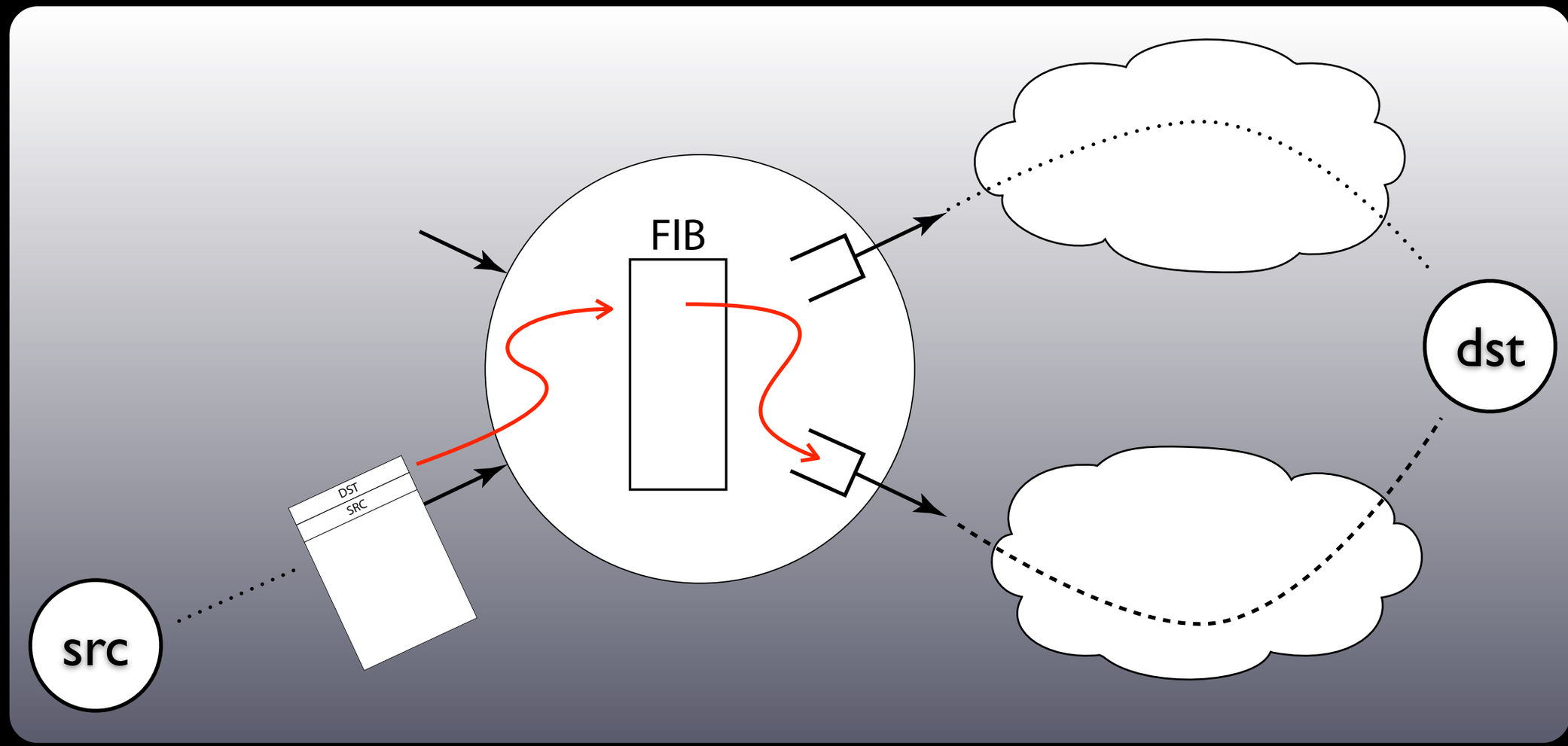

SMTP HTTP RTP ...
TCP UDP ...
IP
ethernet PPP ...
CSMA async sonet ...
copper fiber radio ...


File Stream Cmd ...
Security
Named data
Strategy
TCP P2P broadcast ...
copper fiber radio ...

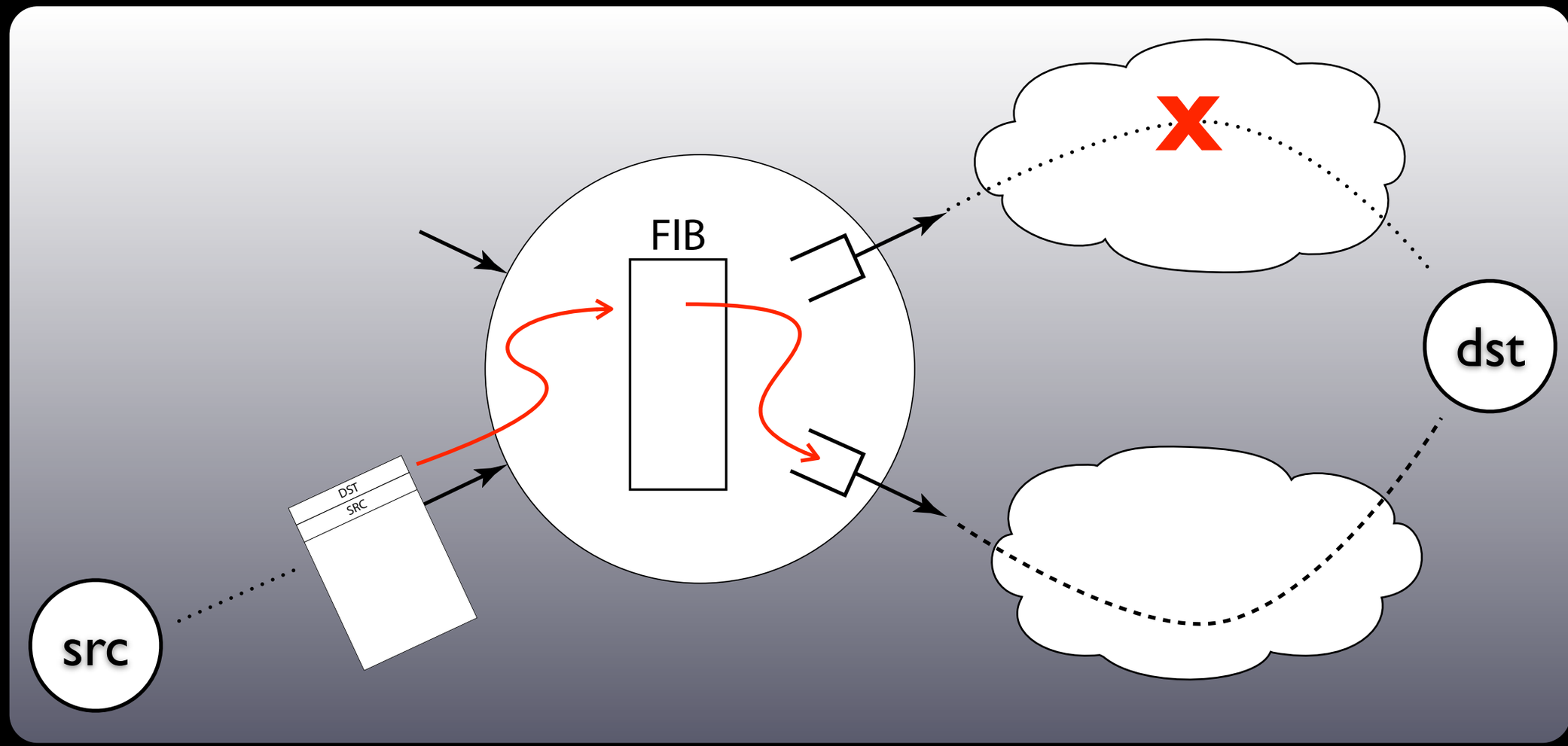

SMTP HTTP RTP ...
TCP UDP ...
IP
ethernet PPP ...
CSMA async sonet ...
copper fiber radio ...


File Stream Cmd ...
Security
Named data
Strategy
TCP P2P broadcast ...
copper fiber radio ...


FIB
DST
SRC
src
dst

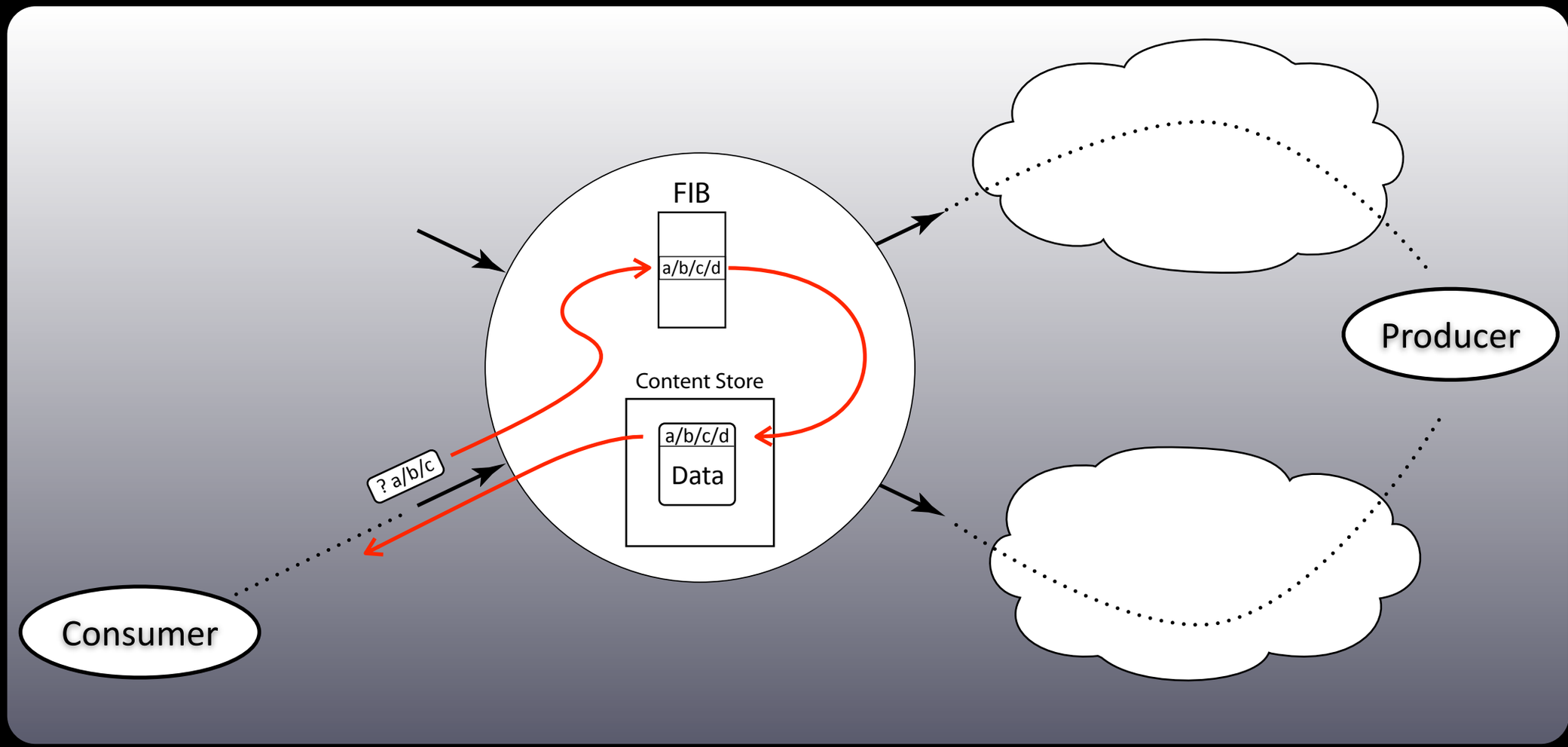


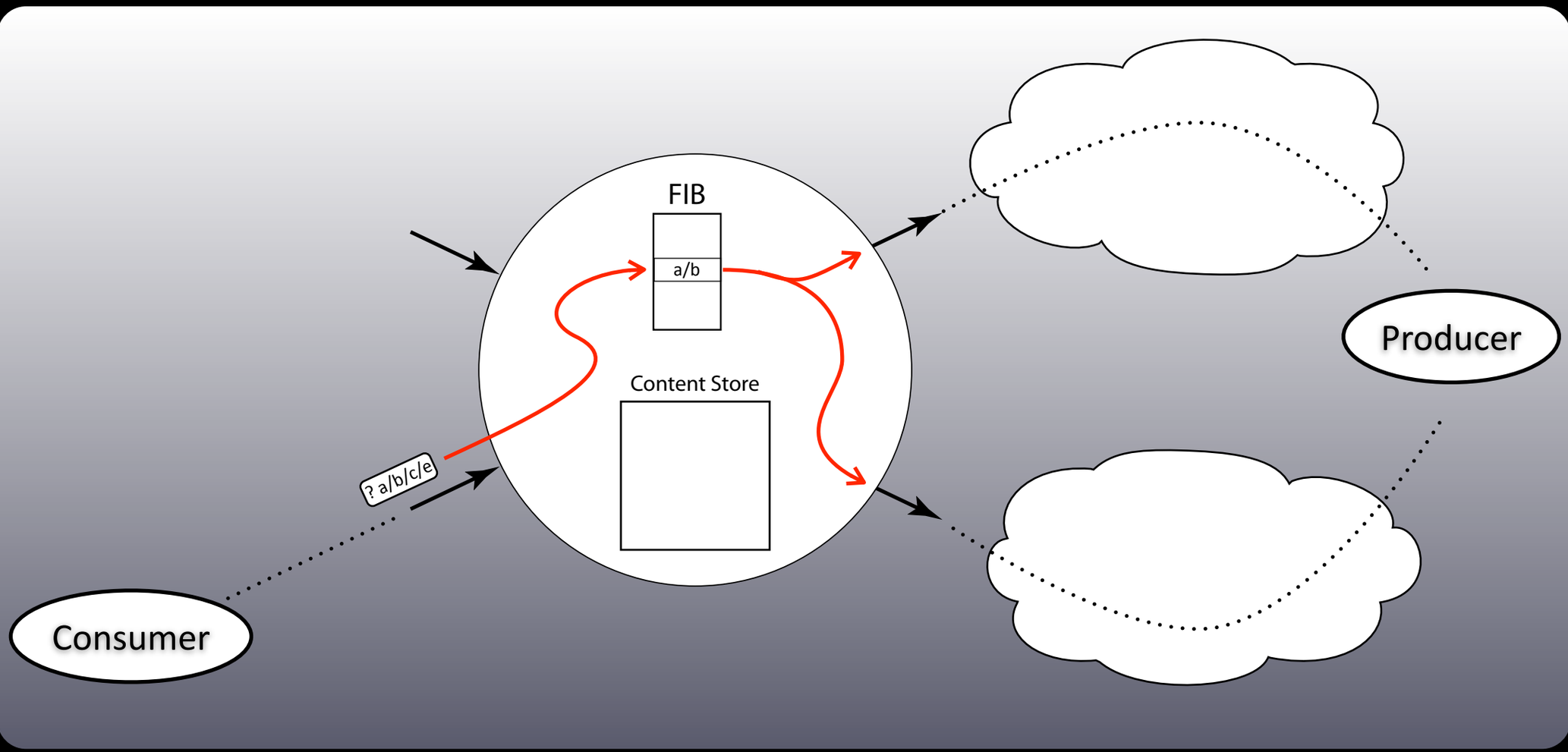
- Intermediate nodes are invisible
- Intermediate nodes can’t choose.
- Intermediate nodes can’t measure success

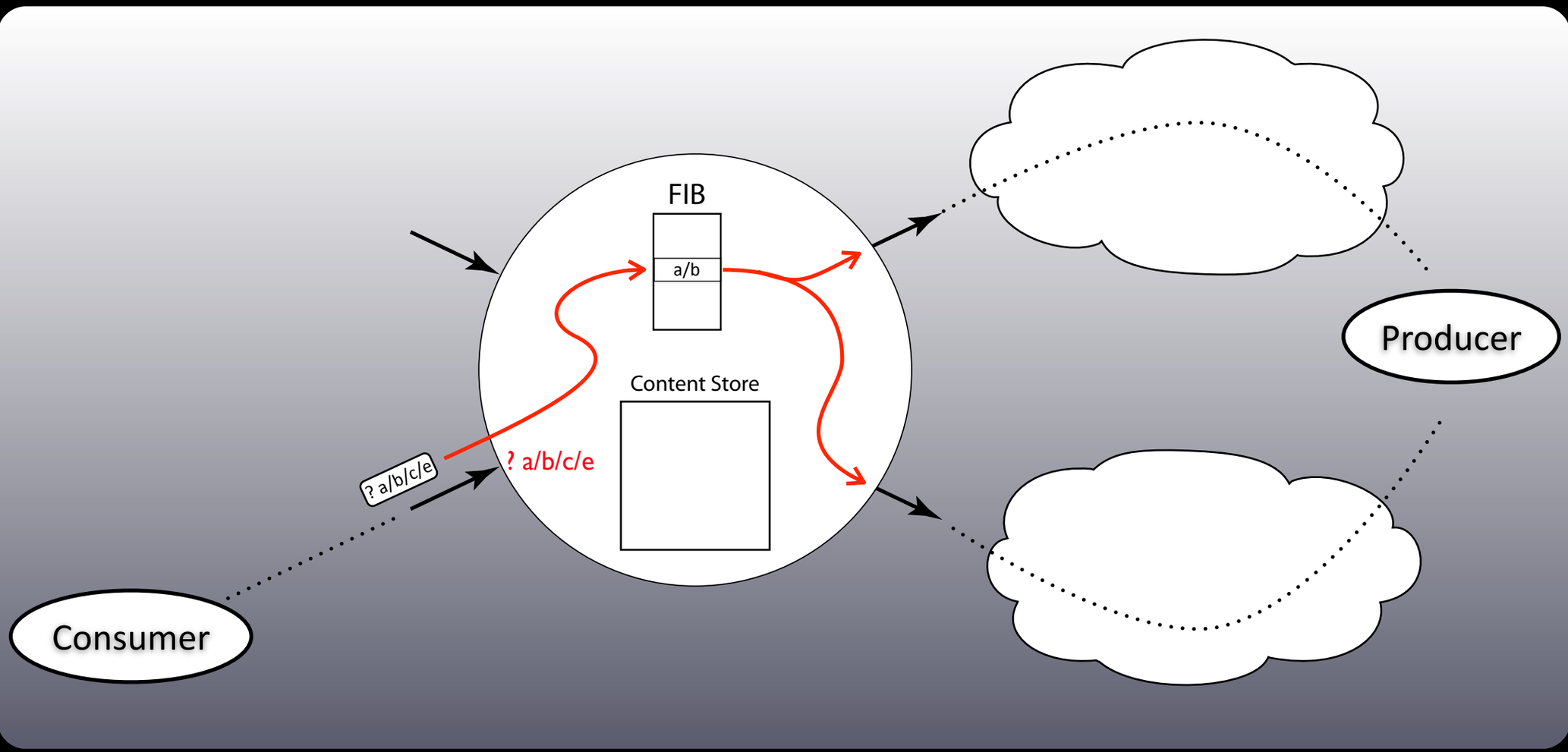


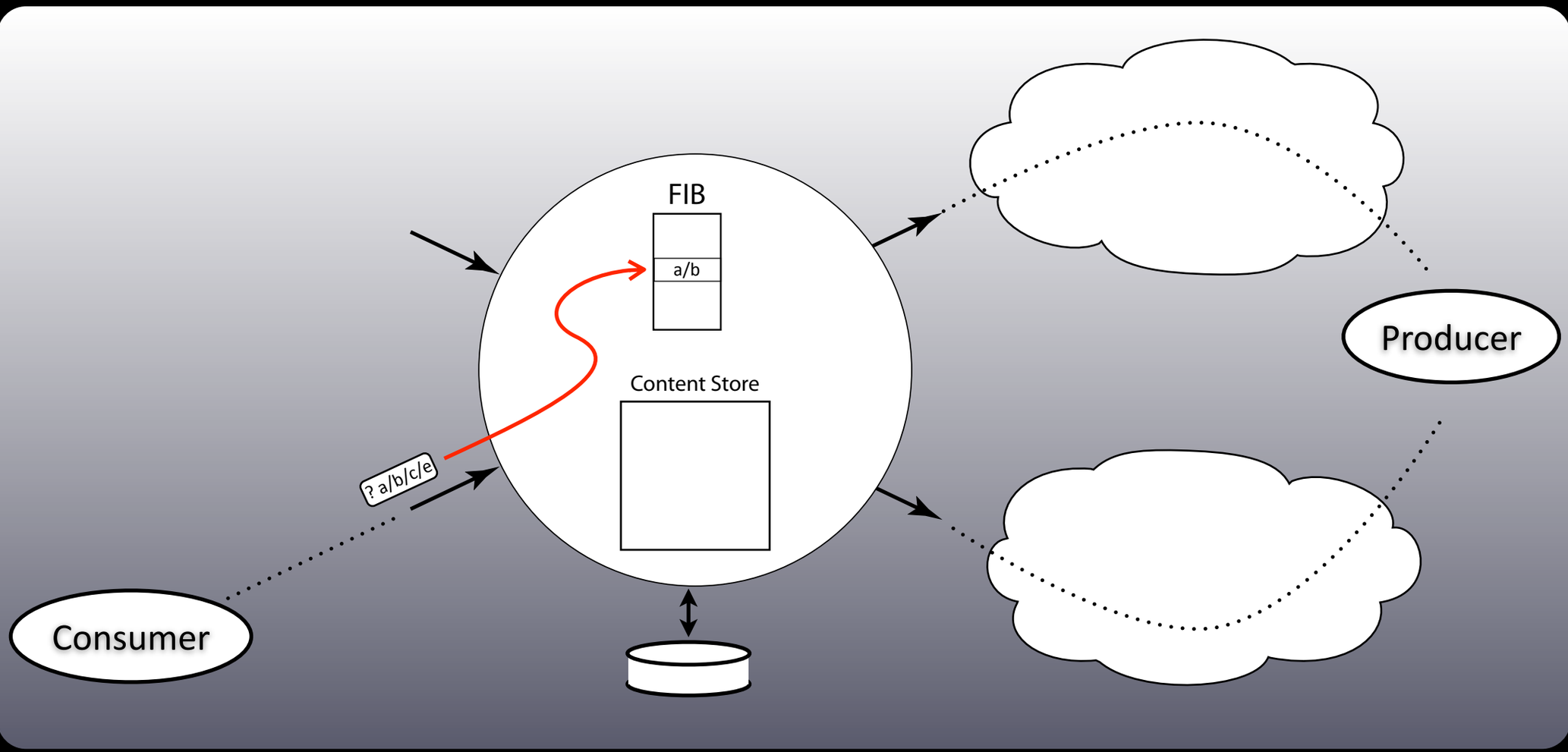
Path determined by global routing, not local choice.

Structural asymmetry precludes market mechanisms and encourages monopoly formation.


FIB
a/b/c/d
Content Store
a/b/c/d
Data
? a/b/c
Consumer
Producer


FIB
a/b
Content Store
? a/b/c/e
Consumer
Producer

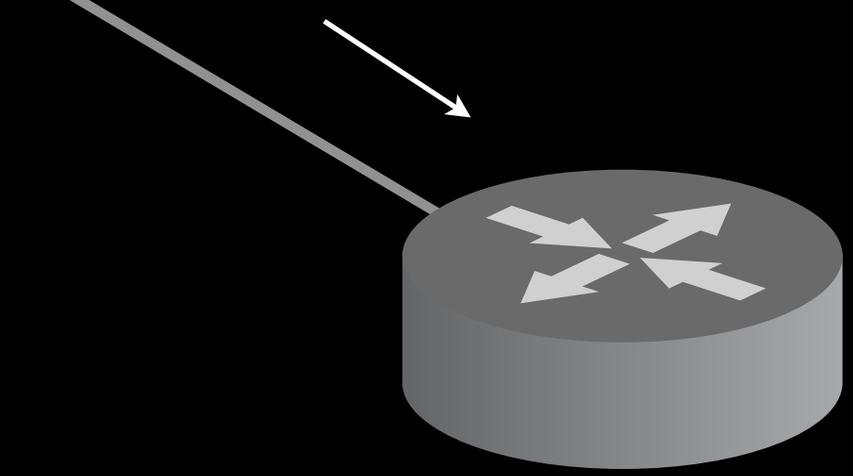

FIB
a/b
Content Store
? a/b/c/e
? a/b/c/e
Consumer
Producer



- Packets say ‘what’ not ‘who’ (no src or dst)
- communication is to local peer(s)
- upstream performance is measurable
- memory makes loops impossible

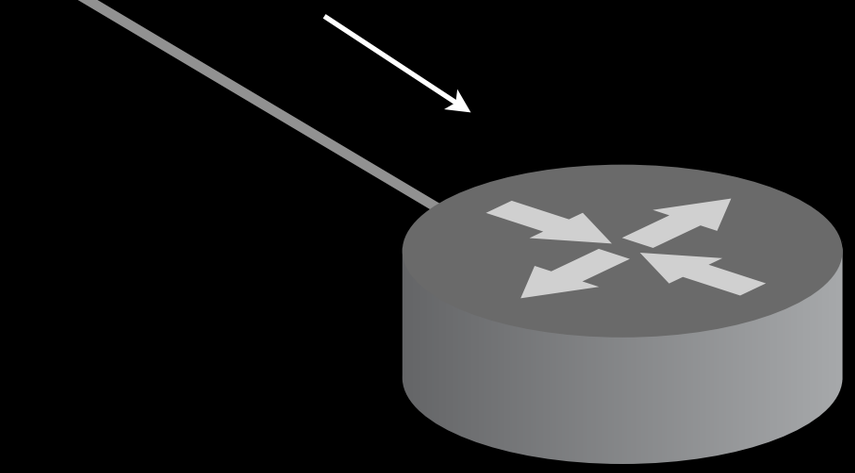
At startup:

register: /netflix
strategy: first



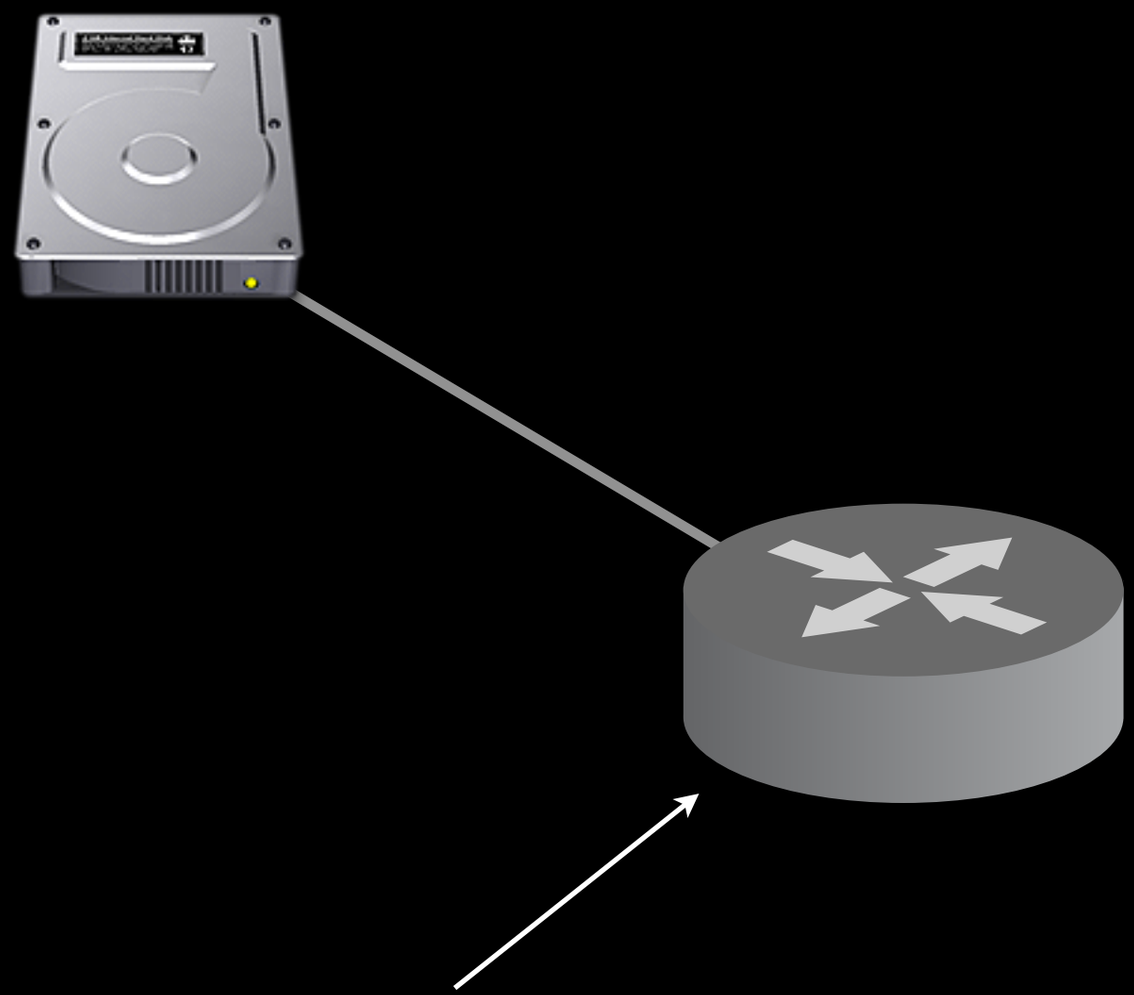
At startup:

register: /netflix
strategy: first



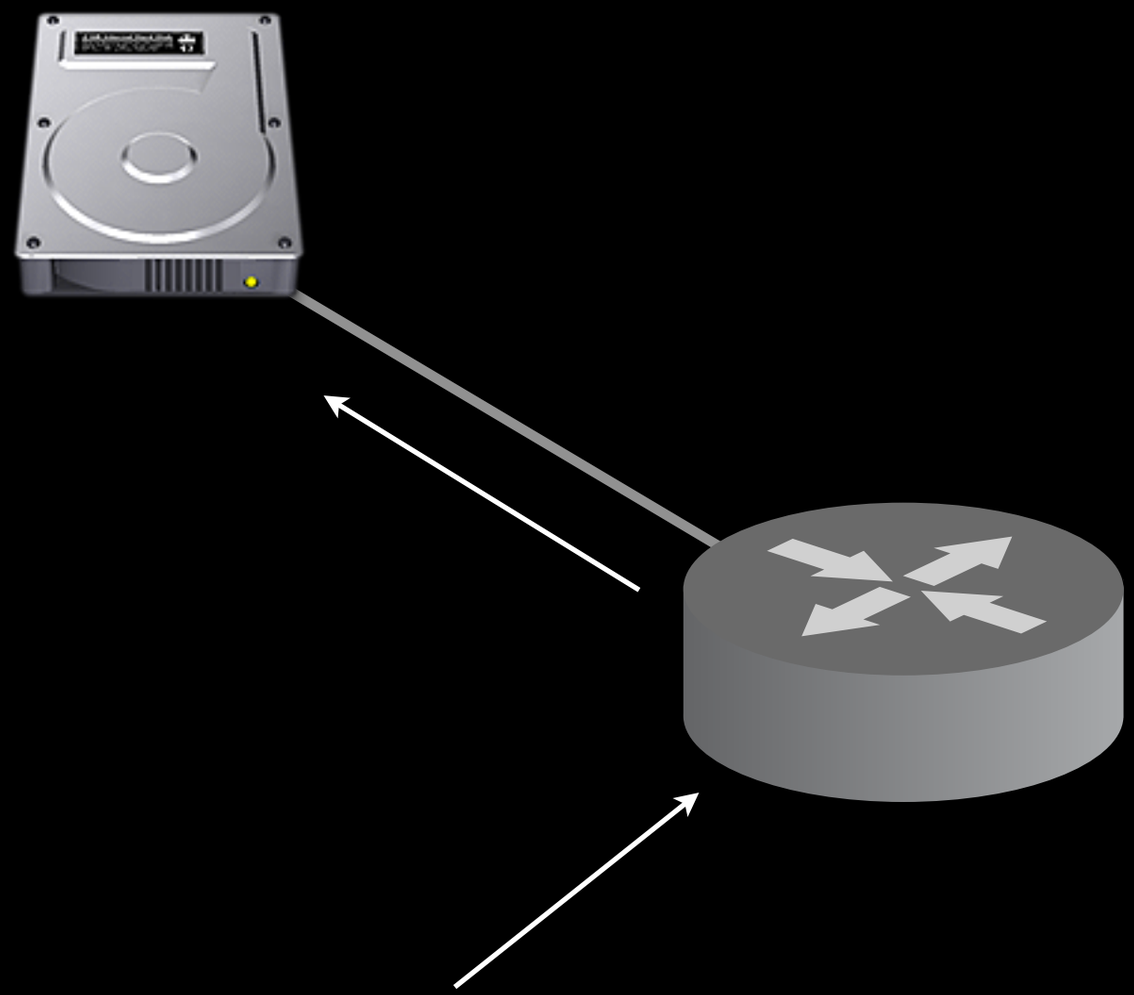
FIB:
...
/netflix ask{F_{disk}}
bestOf{F2,F4}
...

Interest handling: hit



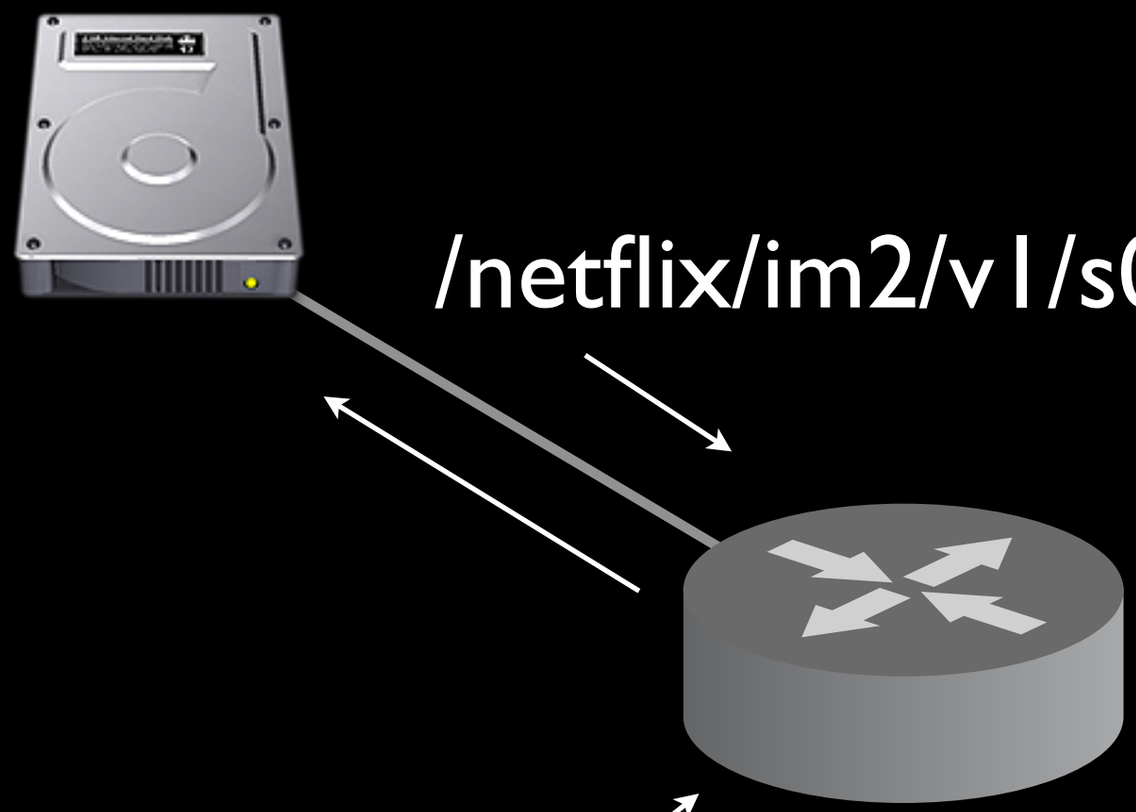
? /netflix/im2

Interest handling: hit

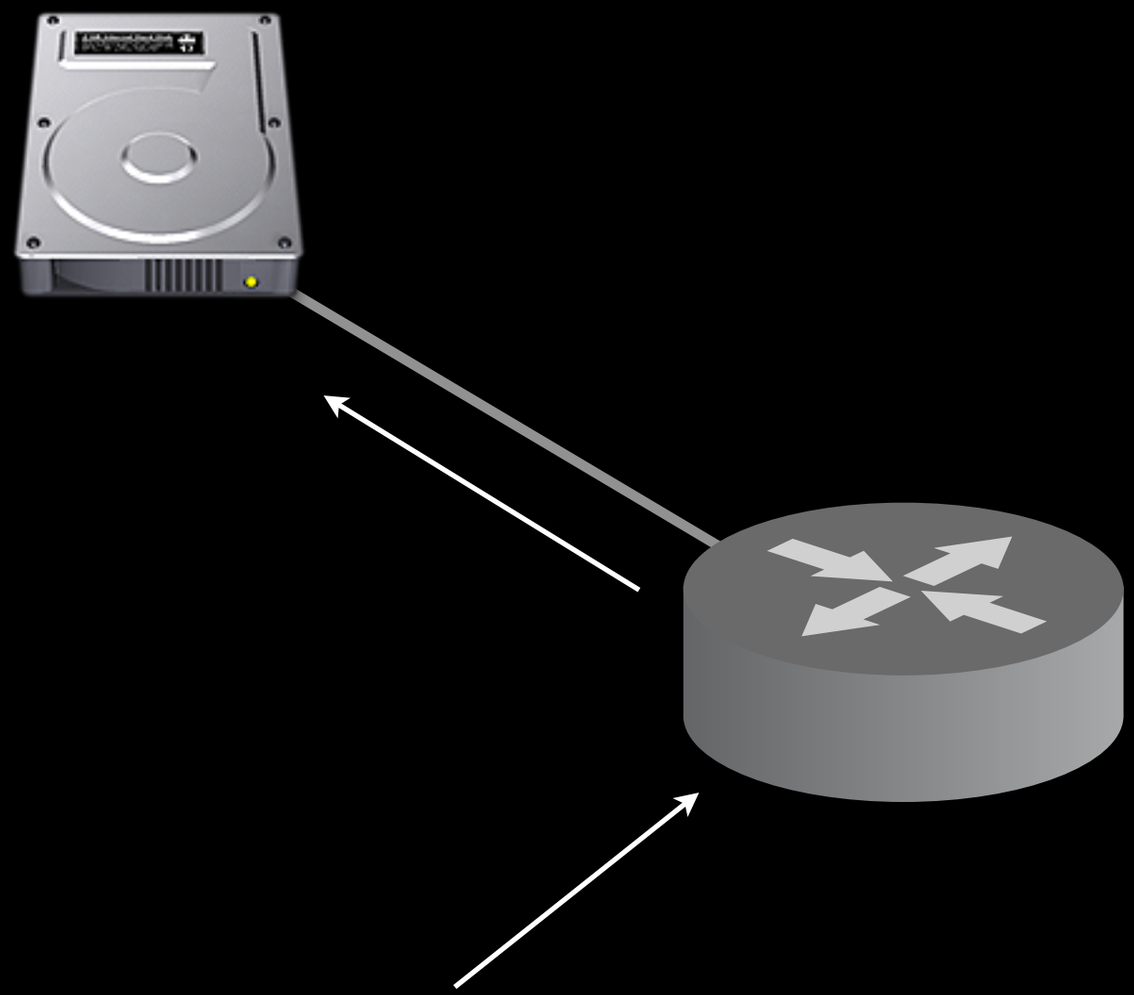


? /netflix/im2

Interest handling: hit

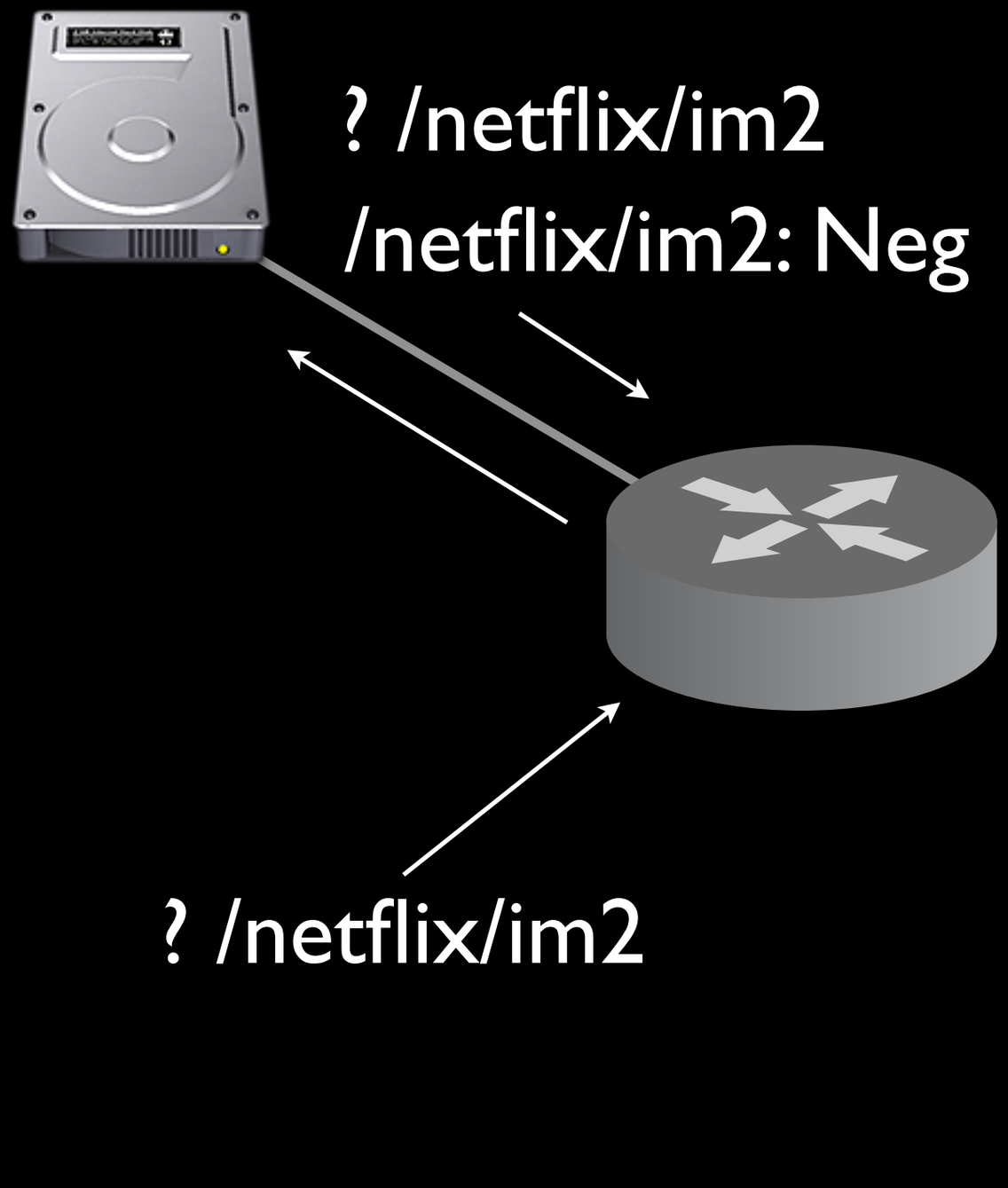


Interest handling: miss



? /netflix/im2

Interest handling: miss



The cache expresses it's own interest in the data so it will get a copy when it arrives.

It works automatically and autonomously with minimal configuration, just like a line card.

Customer-edge PoP

- Rigid qualification for all equipment
- Hostile, lights-out environment
- Remote subscriber configuration
- No other configuration
  (IP line cards hook themselves up)

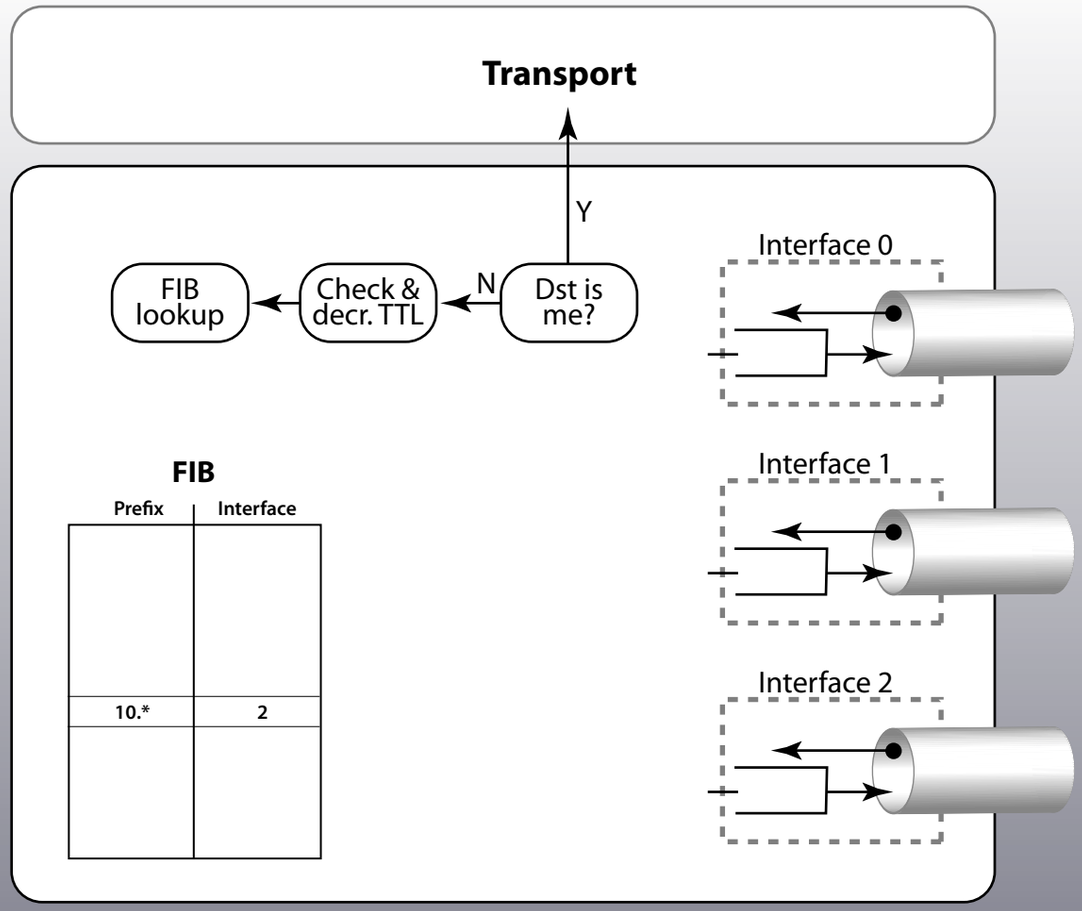
4x 10Gb Ethernet line card

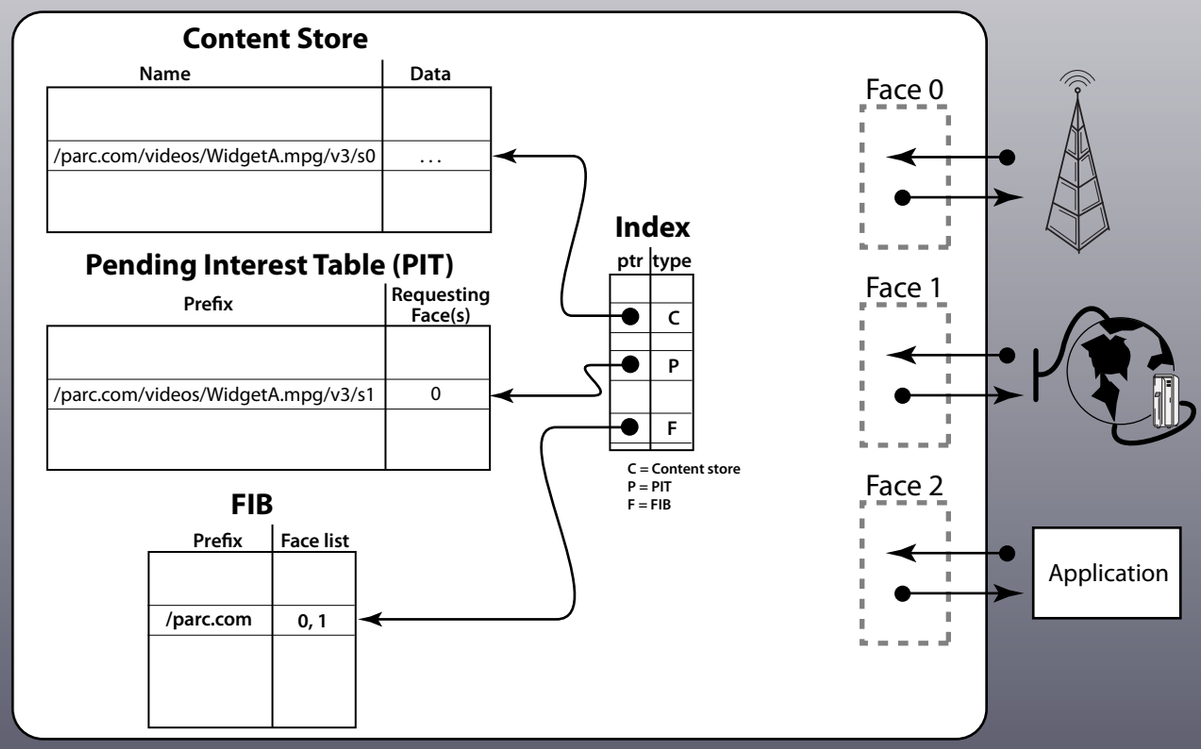
40 Gbps
20”x14”x2”
500W
$65K

1 TB SATA-3 SSD

48 Gbps
4”x0.75”
5mW
$2K / TB

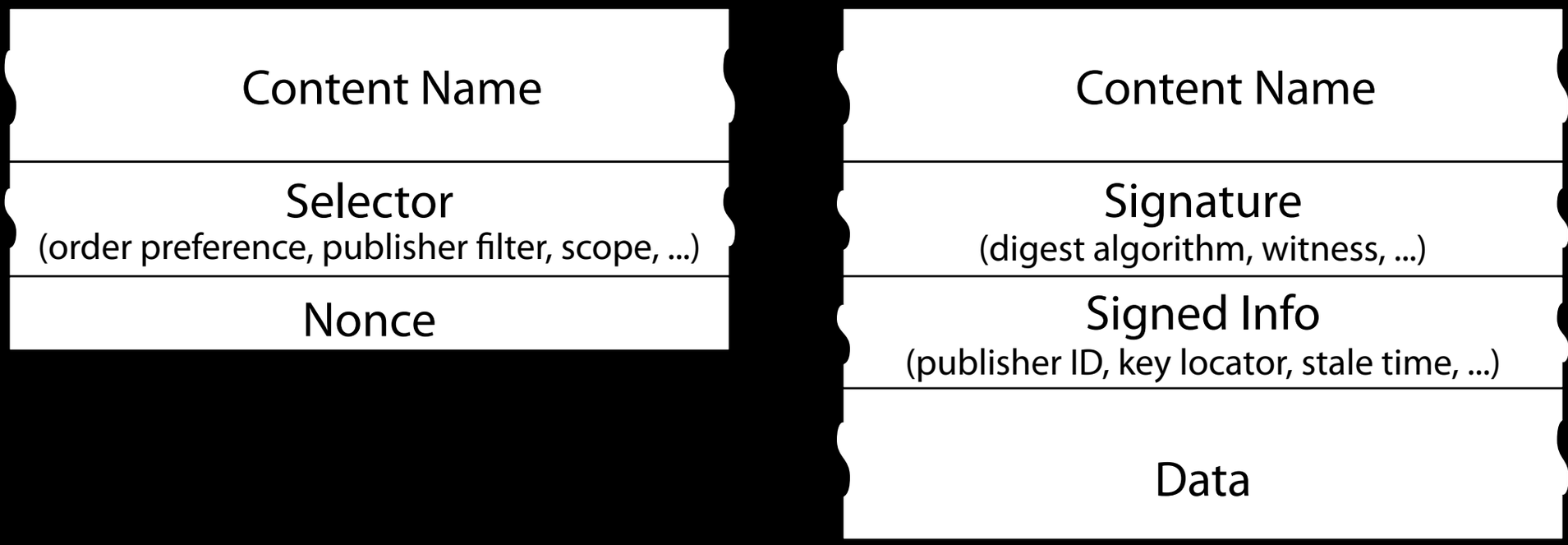
How different are IP & CCN?





They're similar: it's easy to add CCN to an IP router

CCN packets

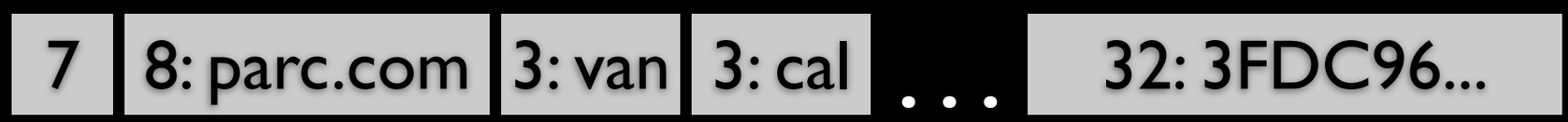


There are two packet types: *Interest* (a question) and *Data* (an answer). Both are encoded in an efficient binary XML.

CCN names are opaque, structured byte strings

`/parc.com/van/cal/417.vcf/v3/s0/0x3fdc96a4...`

is represented as a component count
then, for each component, a byte count
followed by that many bytes:



The *only* assumption CCN makes about names is hierarchical structure.
E.g., names or components can be encrypted or contain arbitrary binary data.

Basic CCN forwarding

- Consumer 'broadcasts' an interest over any available communications media:

```
want '/parc.com/van/slides.pdf'
```

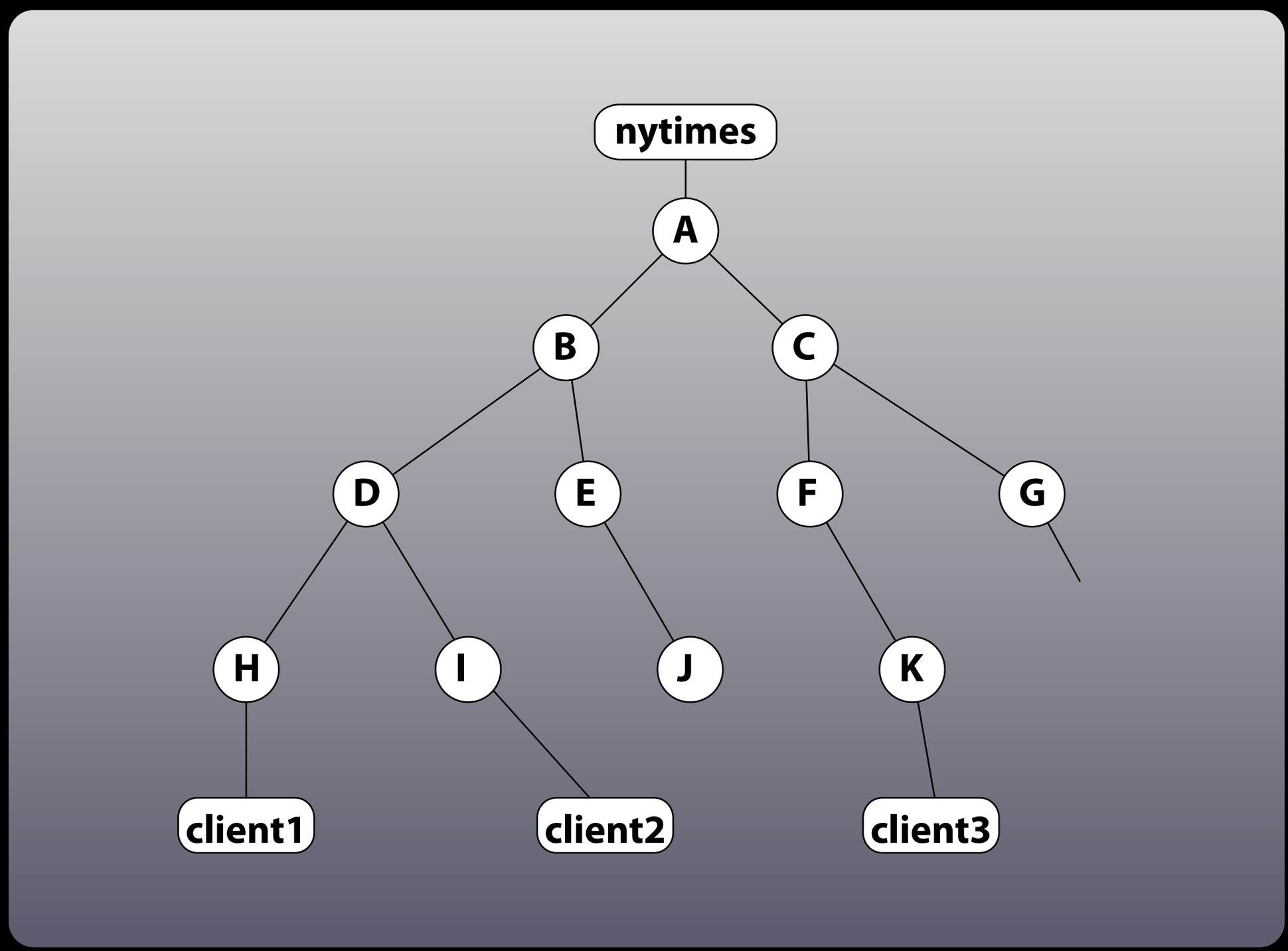
- Interest identifies a *collection* of data - all data items whose name has the interest as a prefix.

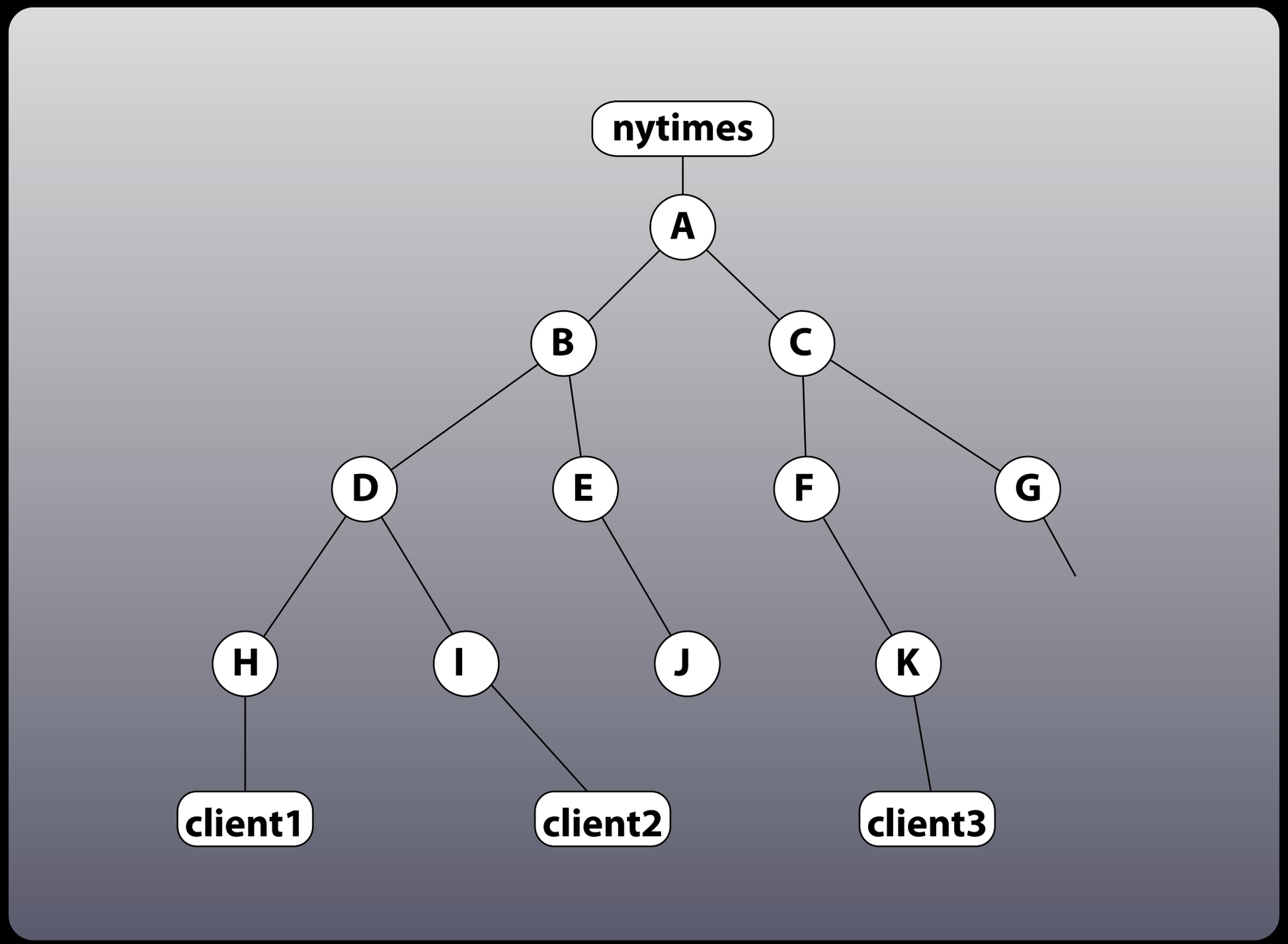
- Anything that hears the interest and has an element of the collection can respond with it:

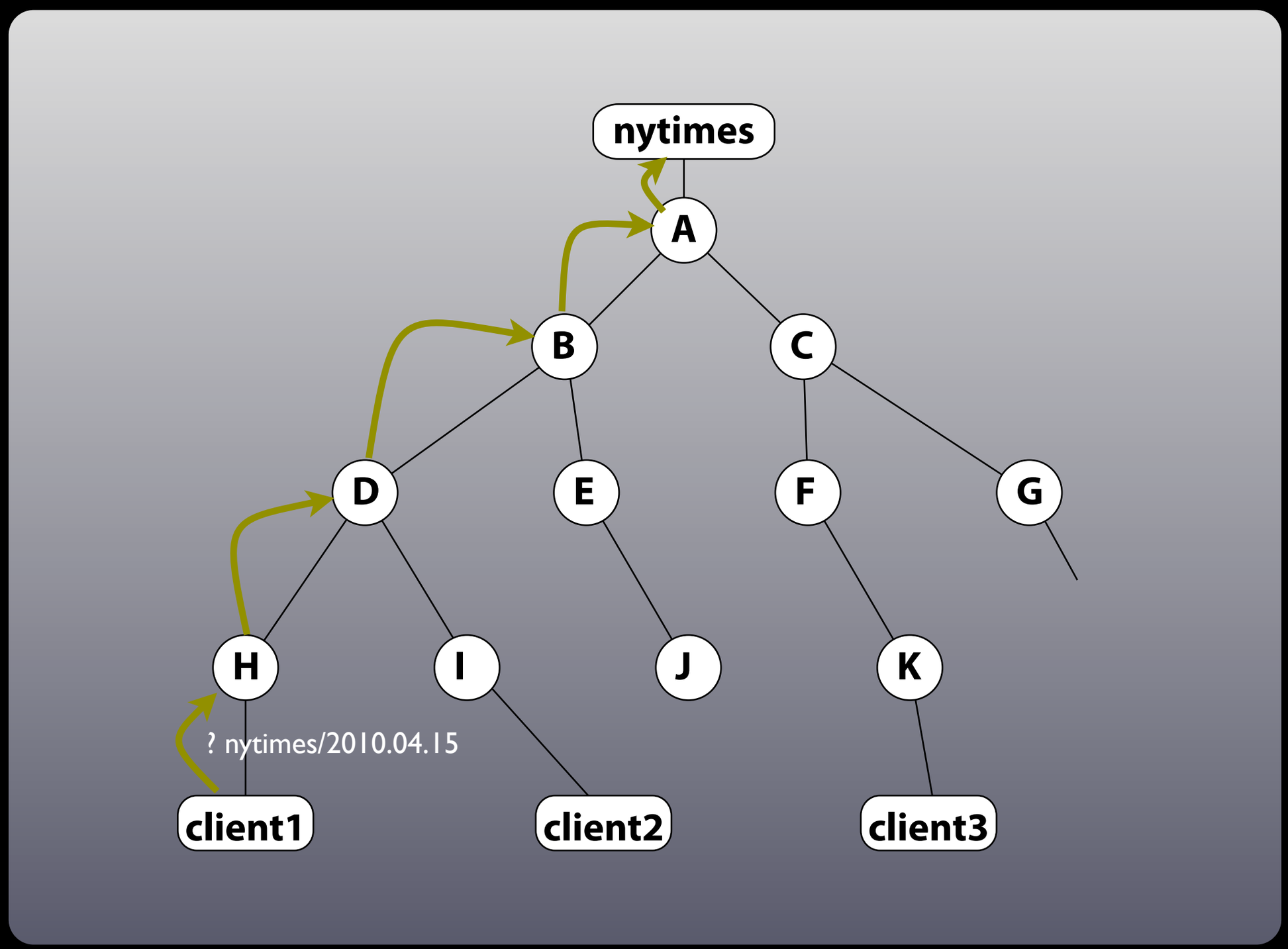
```
HereIs '/parc.com/van/slides.pdf/v6/p1' <data>
```

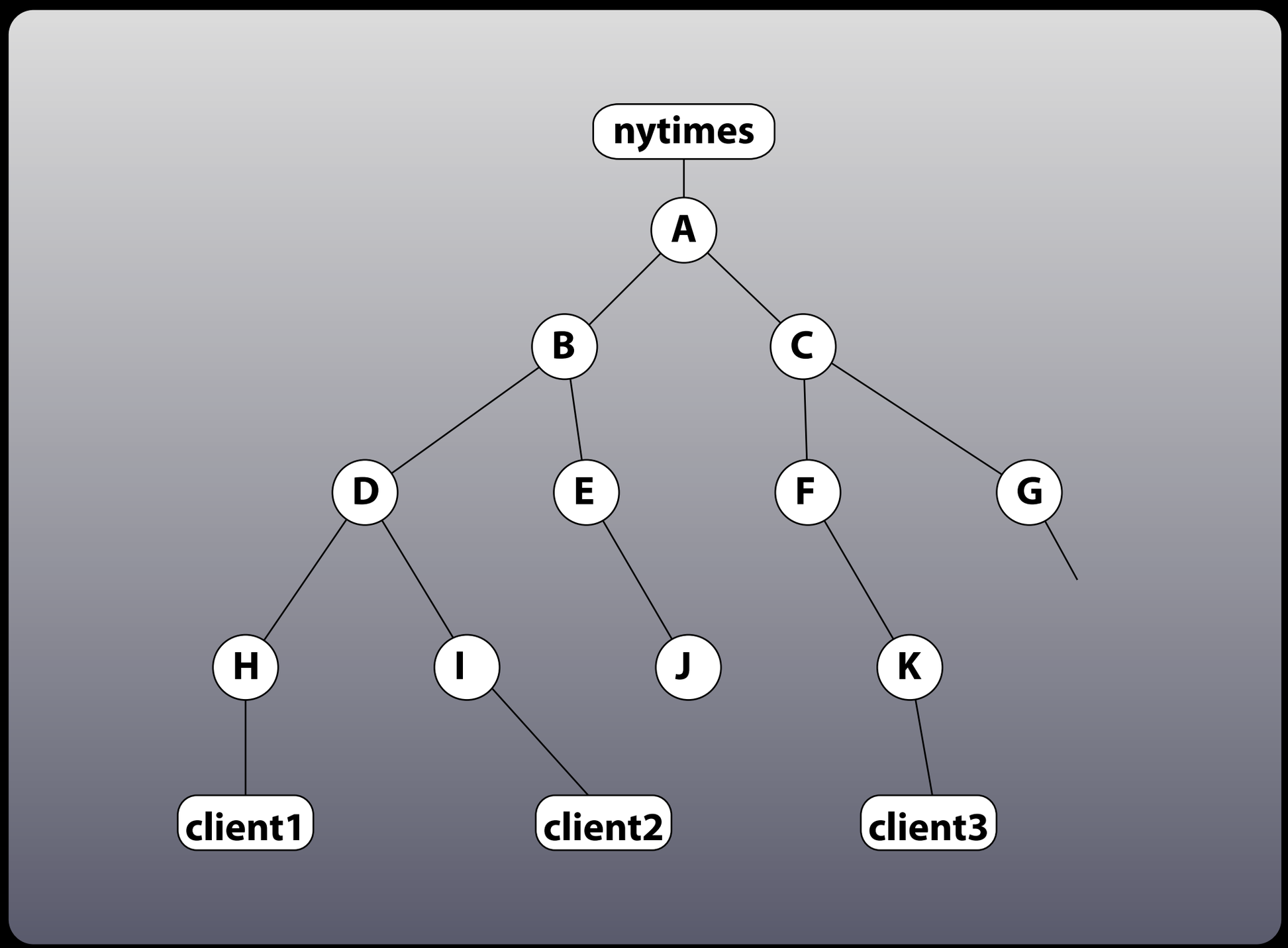
Basic CCN transport

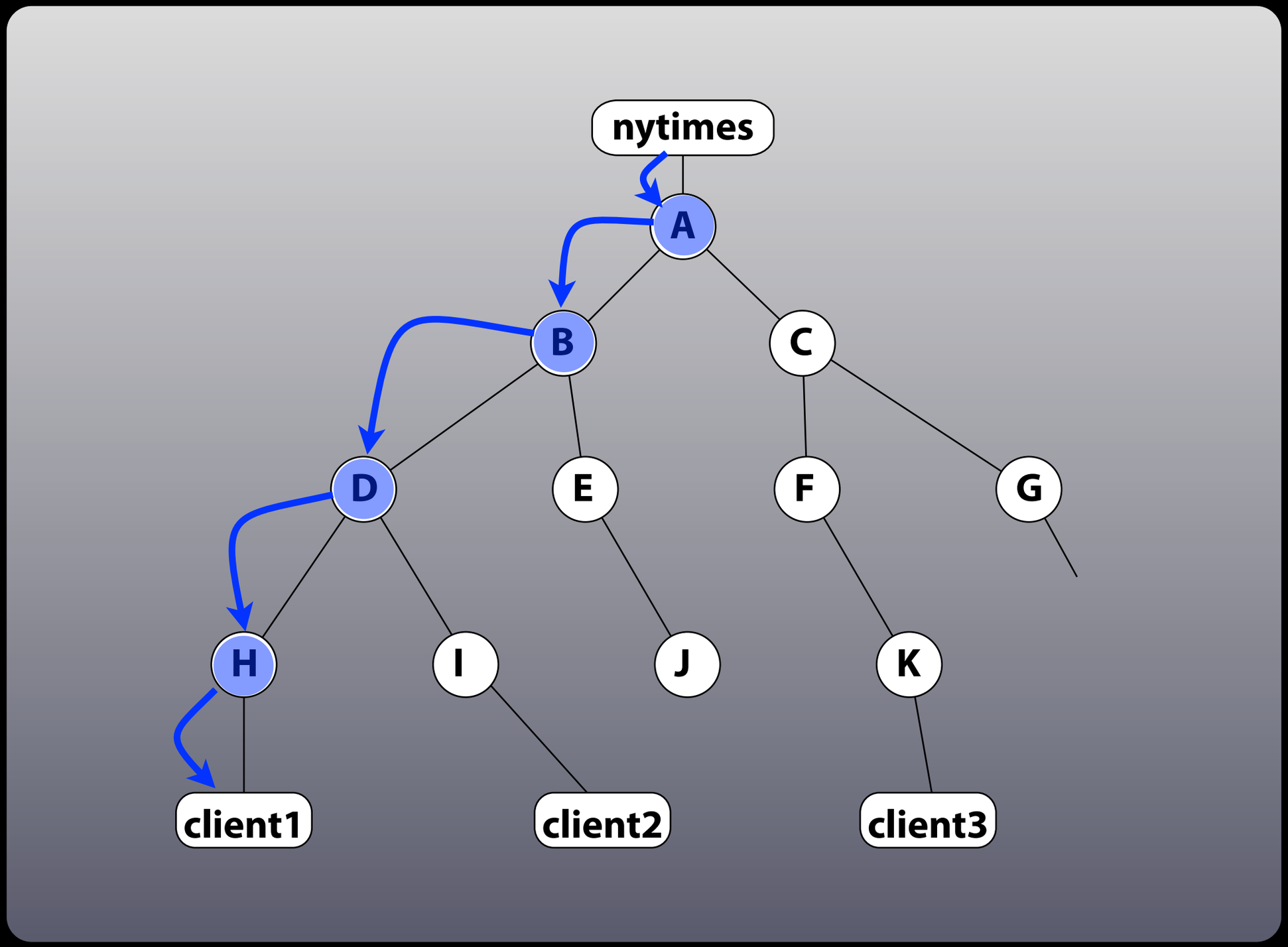
- Data that matches an interest 'consumes' it.
- Interest must be re-expressed to get new data.
  (Controlling the re-expression allows for traffic management and environmental adaptation.)
- Multiple (distinct) interests in same collection may be expessed (similar to TCP window).

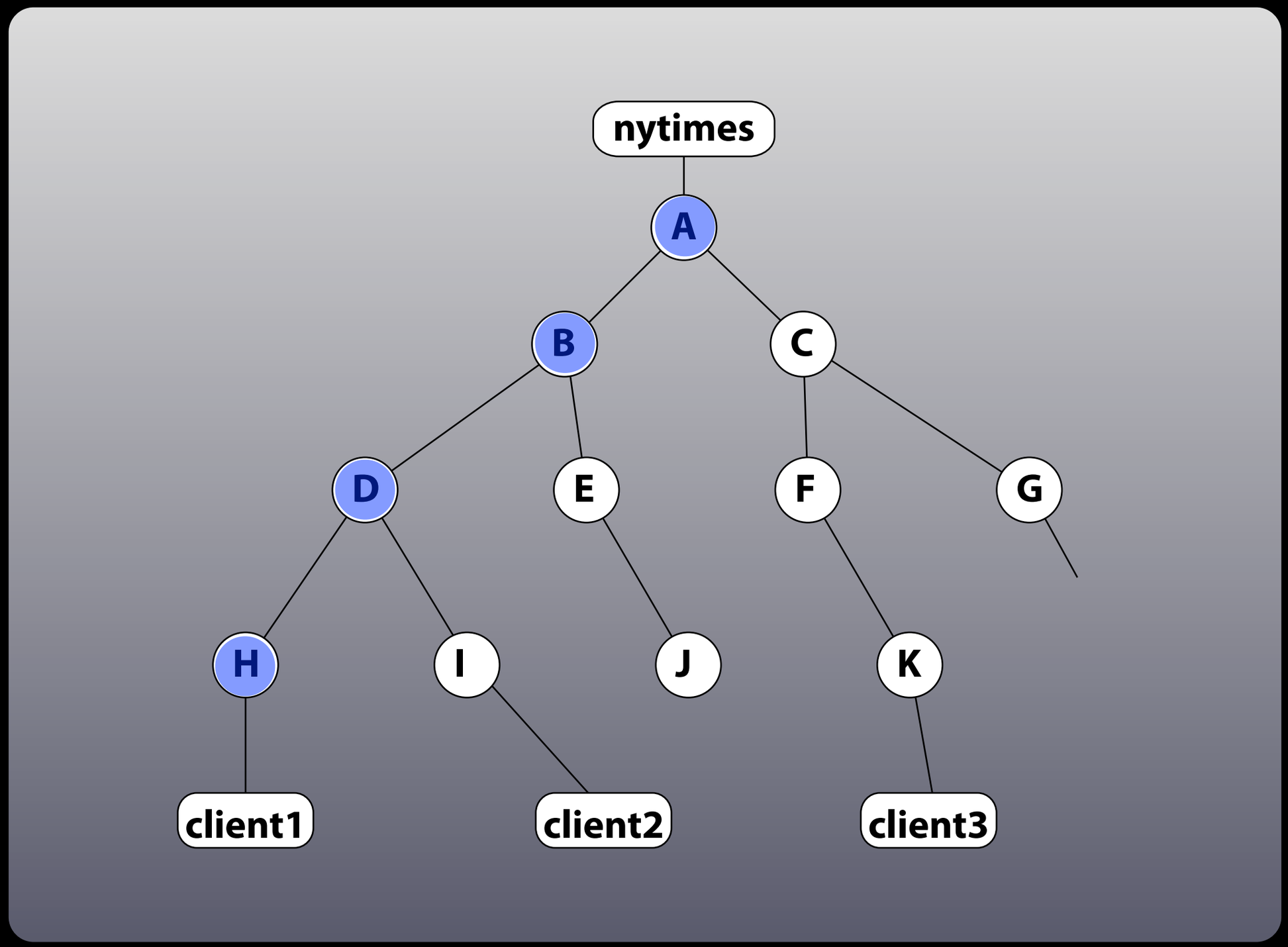

nytimes
A
B
C
D
E
F
G
H
I
J
K
client1
client2
client3

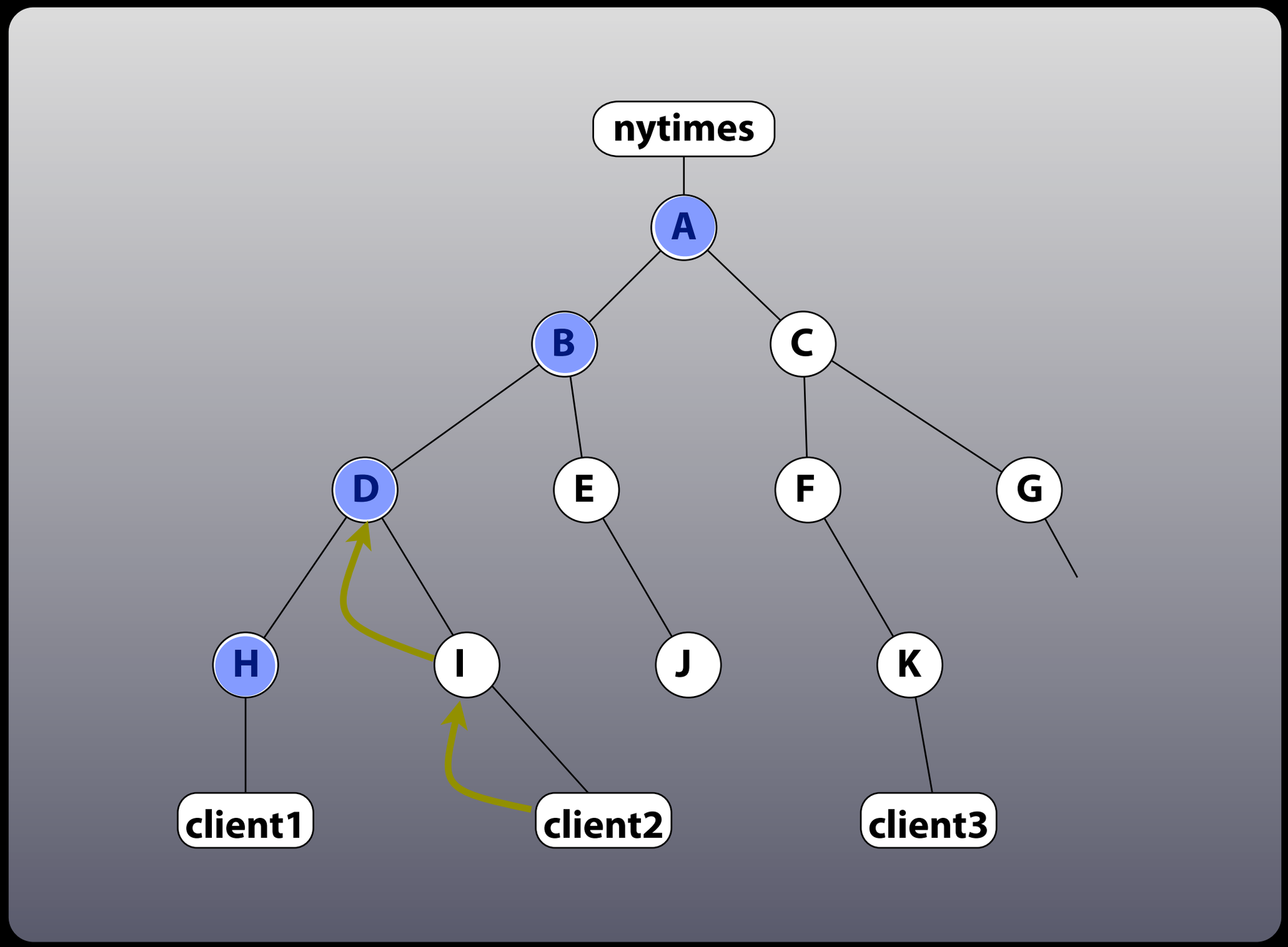

nytimes
A
B
C
D
E
F
G
H
I
J
K
client1
client2
client3

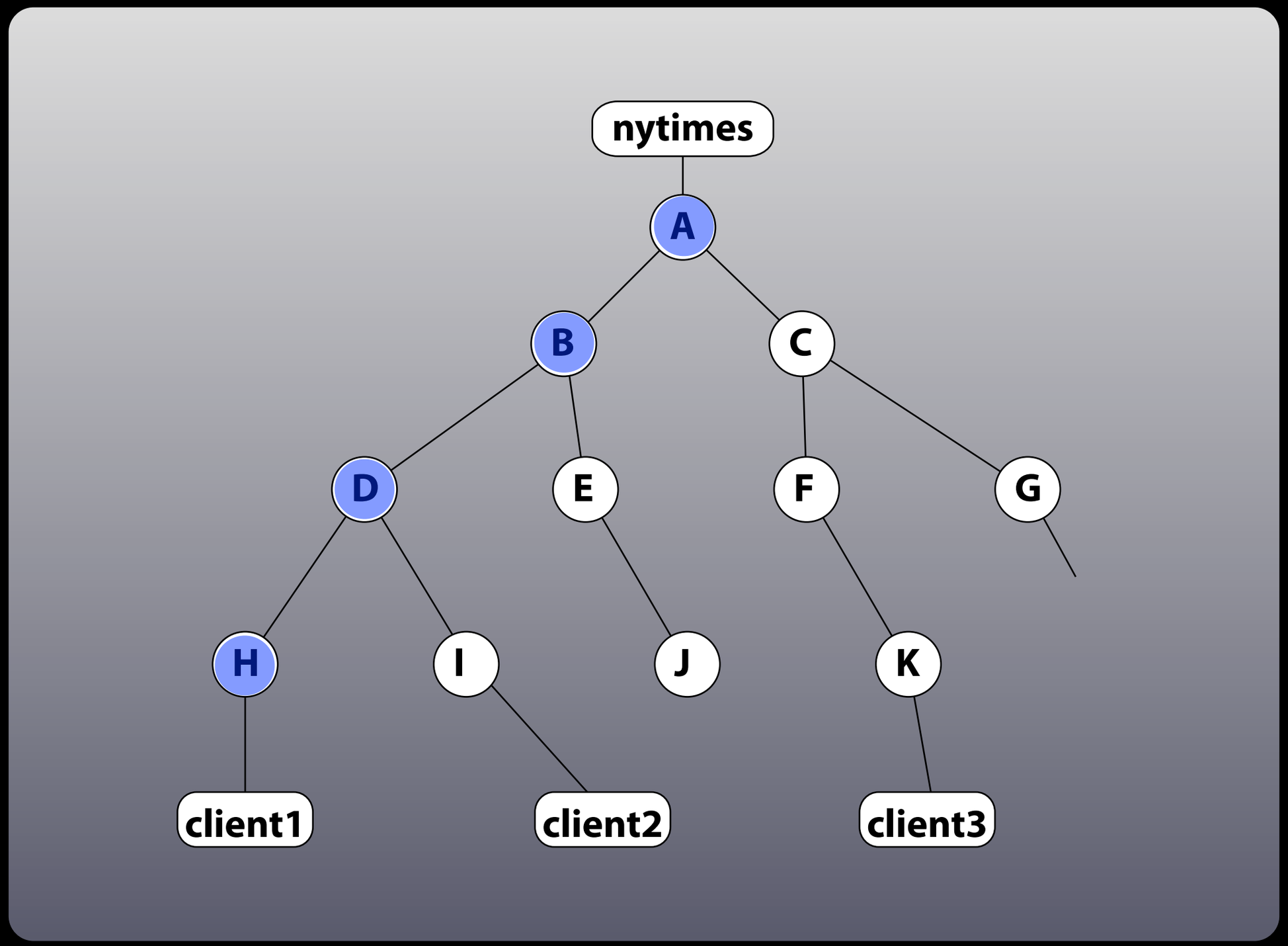

nytimes
A
B
C
D
E
F
G
H
I
J
K
? nytimes/2010.04.15
client1
client2
client3

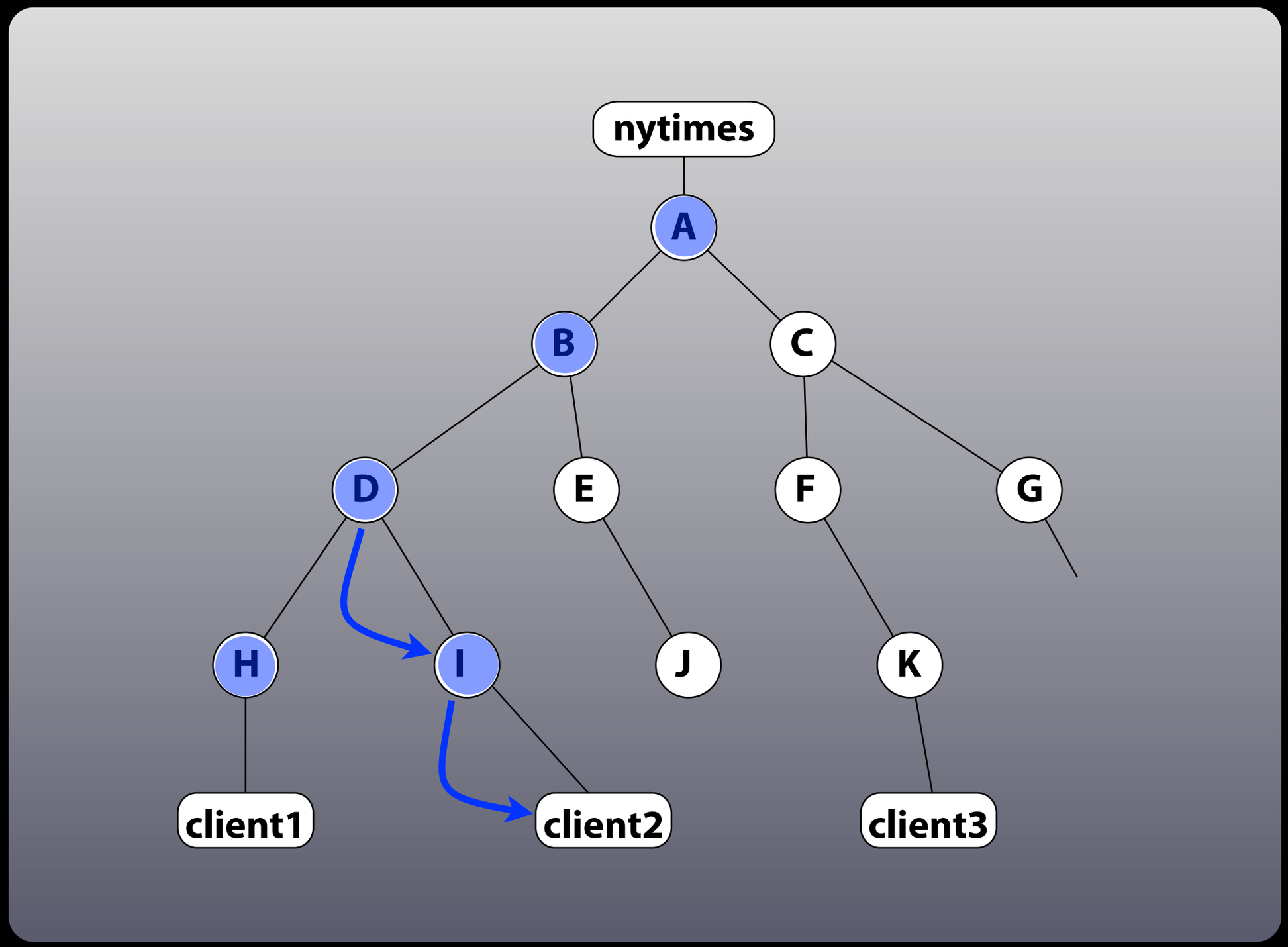

nytimes
A
B
C
D
E
F
G
H
I
J
K
client1
client2
client3

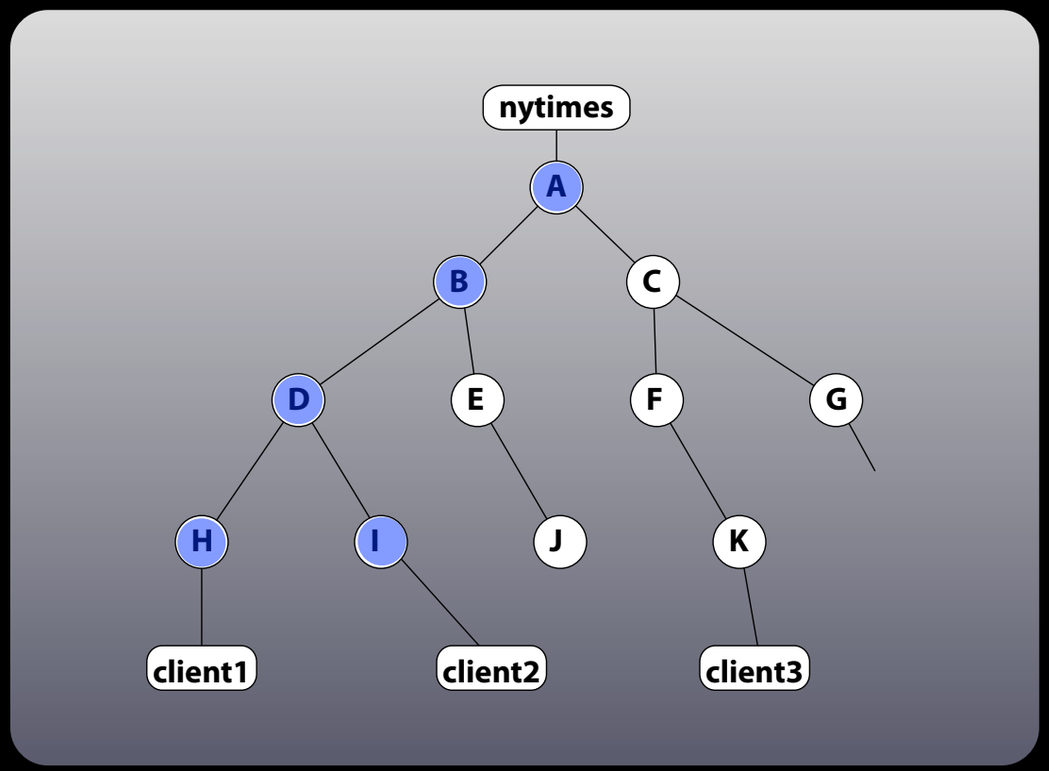

nytimes
A
B
C
D
E
F
G
H
I
J
K
client1
client2
client3


nytimes
A
B
C
D
E
F
G
H
I
J
K
client1
client2
client3


nytimes
A
B
C
D
E
F
G
H
I
J
K
client1
client2
client3

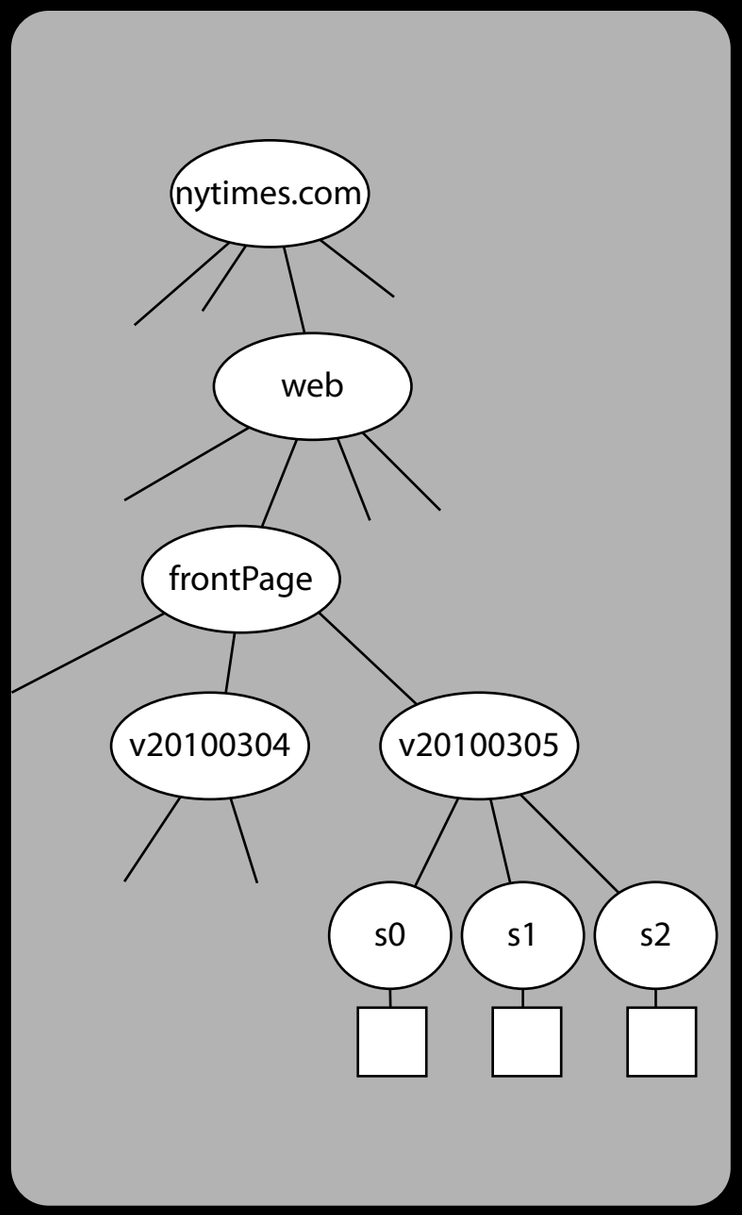

nytimes
A
B
C
D
E
F
G
H
I
J
K
client1
client2
client3


nytimes
A
B
C
D
E
F
G
H
I
J
K
client1
client2
client3



- Content goes only where there's interest.
- It follows the shortest path.
- It crosses any link at most once.
- Average latency is minimized.
- Total bandwidth is minimized.
- There's no new routing or control traffic.

‘Discovery’ problem & Name tree ordering



Newest nytimes:

nytimes.com/web/frontPage
<rightmost child>

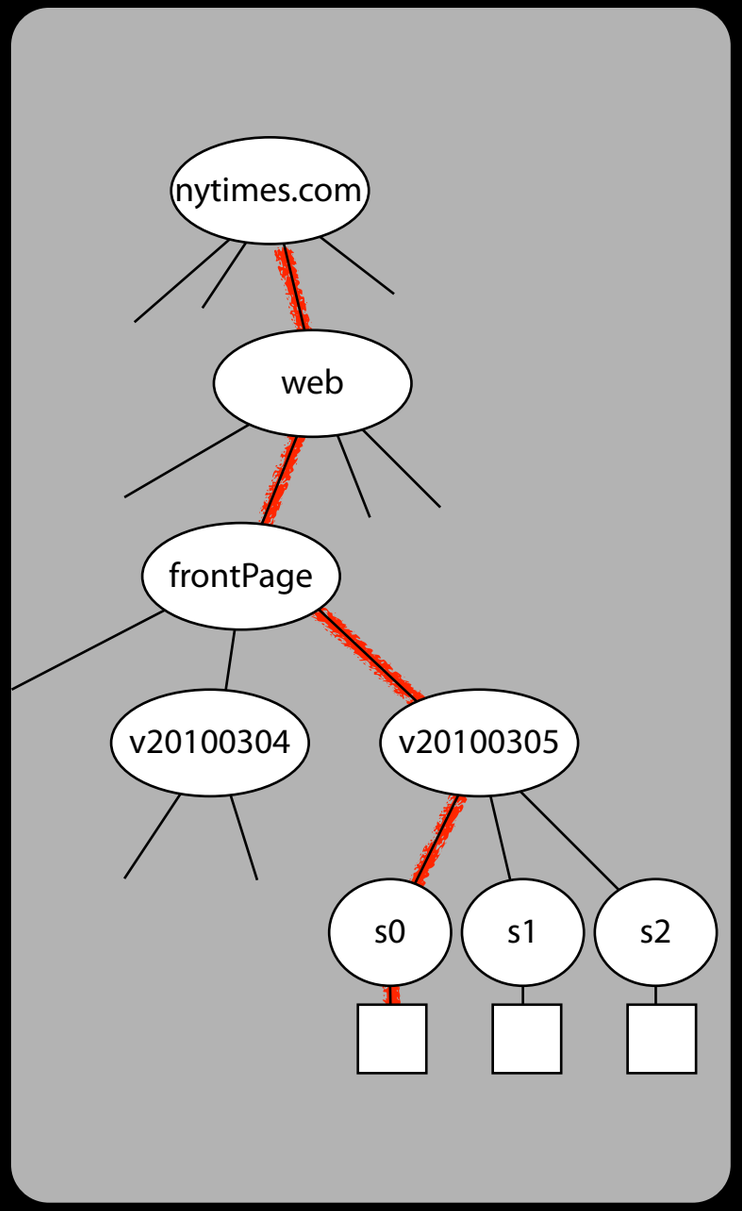
Newest that’s more recent than mine:

nytimes.com/web/frontPage/v20100301
<rightmost sibling>

Conventions:

- name tree child nodes are lexically ordered
- <leftmost child> assumed if relationship unspecified

‘Discovery’ problem & Name tree ordering



Newest nytimes:

nytimes.com/web/frontPage
<rightmost child>

Newest that’s more recent than mine:

nytimes.com/web/frontPage/v20100301
<rightmost sibling>

Conventions:

- name tree child nodes are lexically ordered
- <leftmost child> assumed if relationship unspecified

Examples: sharing pictures

Examples: sharing pictures

/thisFamily/media ?

/thisFamily/media/pictures/vjphone/img1234.jpg

Your settop box

Examples: sharing pictures

/local/media/pictures/today ?

/local/media/pictures/today/vjphone/img1234.jpg

Friend's TV

Everybody knows that ...

- Content-based networking is great for content dissemination ...
- ... but can’t handle conversational or real-time traffic.

This is half right.

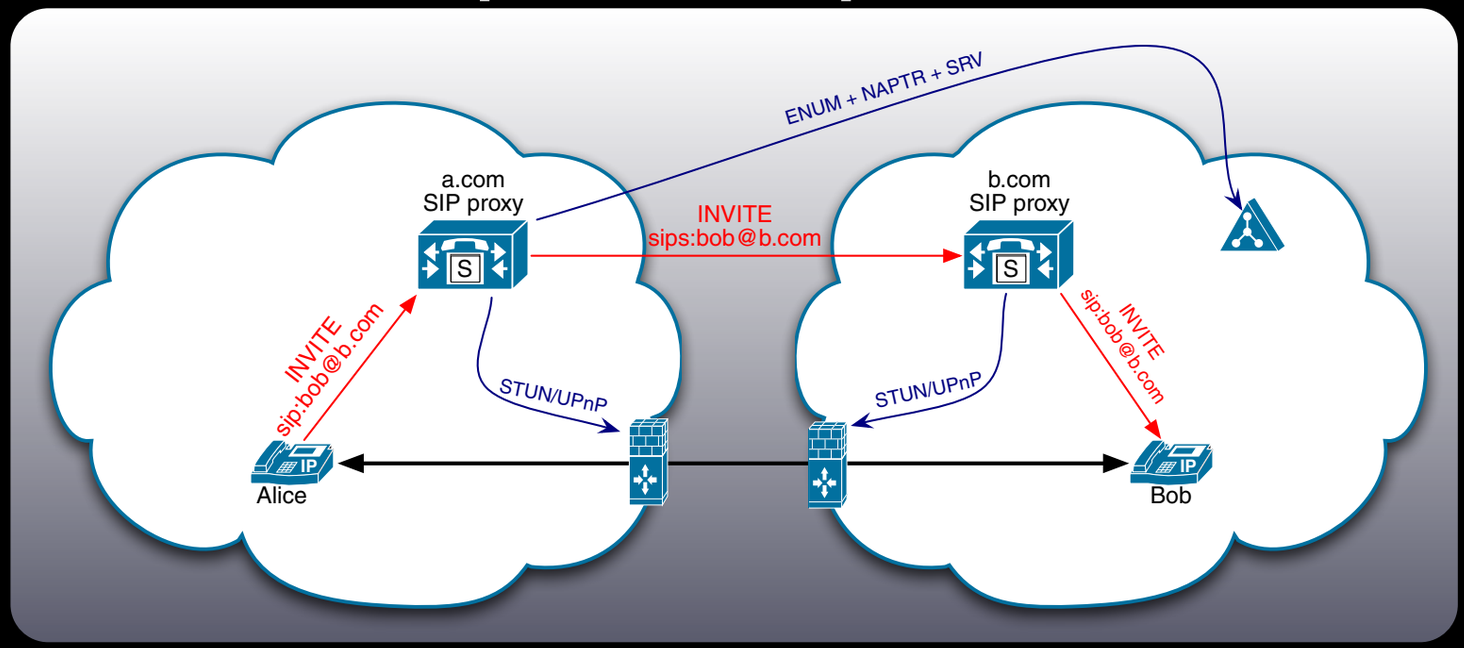
Content networking is more general than IP

It does anything that IP can.

To demonstrate this we implemented VoCCN, a VoIP-functional-equivalent based on CCN.

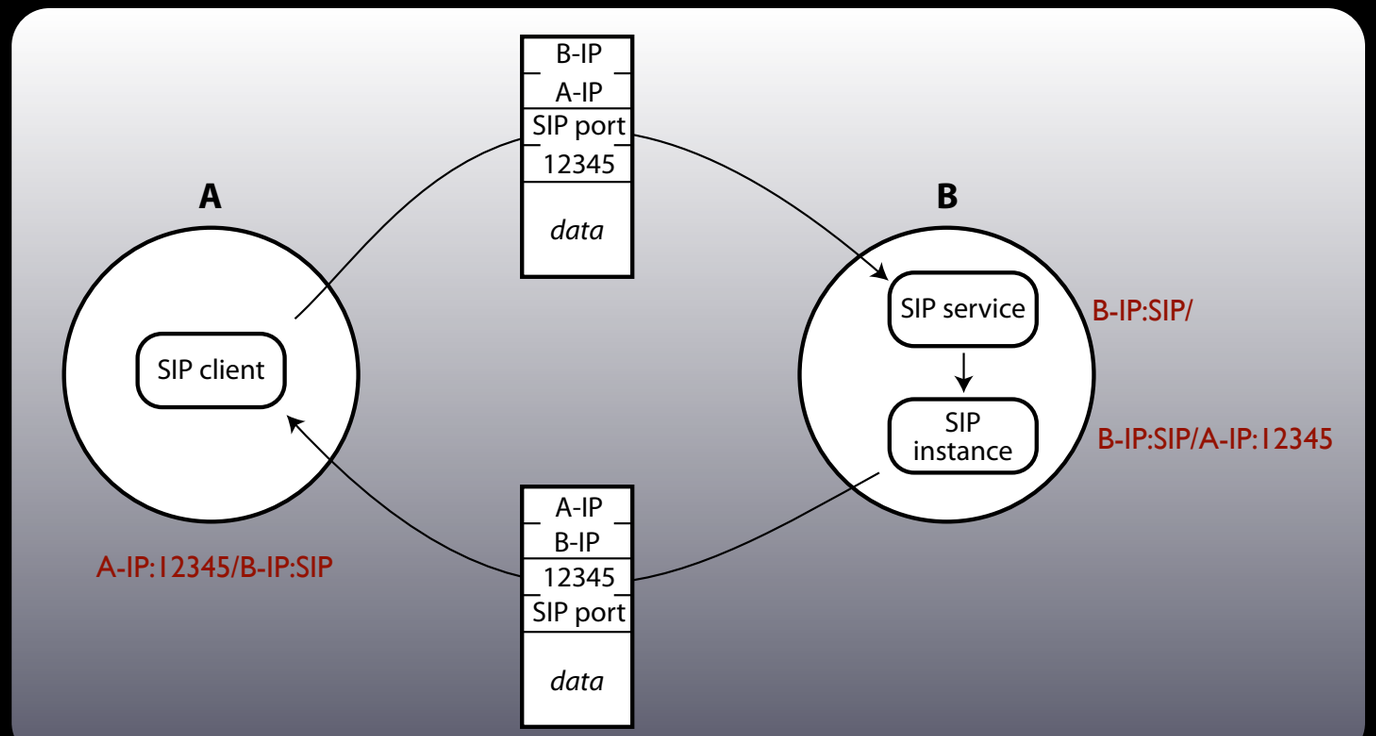
VoCCN – why bother?

- VoIP works badly for multi-point, multi-interface and mobility.
- VoIP security is poor.
- VoIP setup is complex.



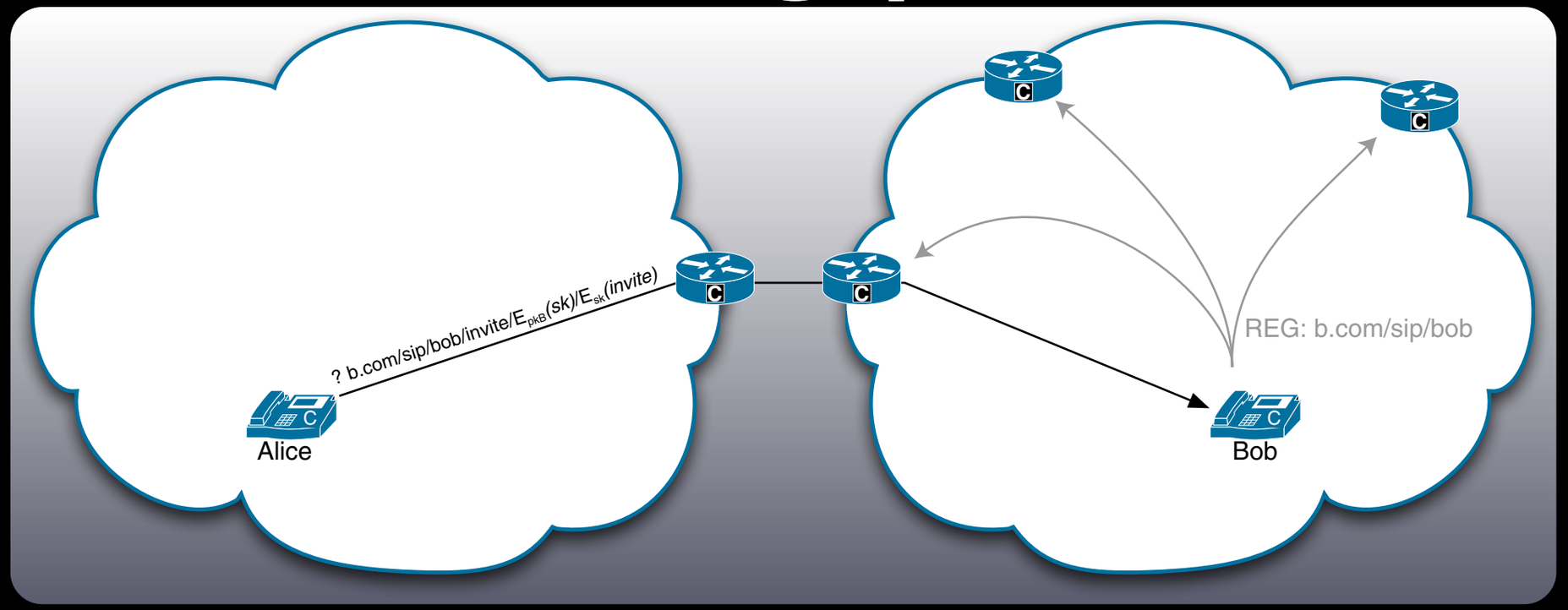
IP builds conversations using two patterns:

- Service to instance
- Uni- to bi-directional



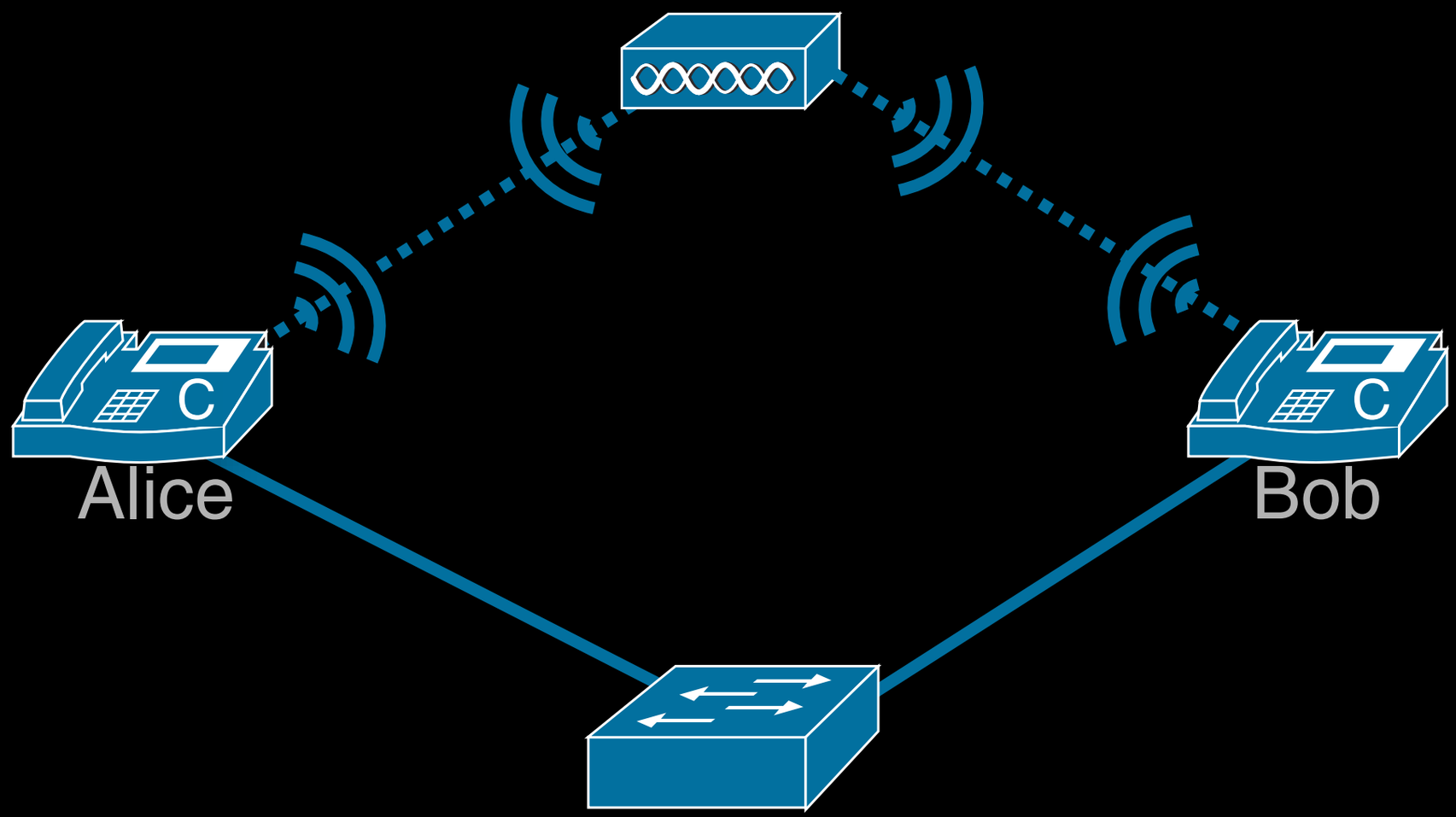
These are just ‘name’ manipulations that should map to any (topic-based) pub-sub system with hierarchical or algorithmic names.

VoCCN has only a few moving parts

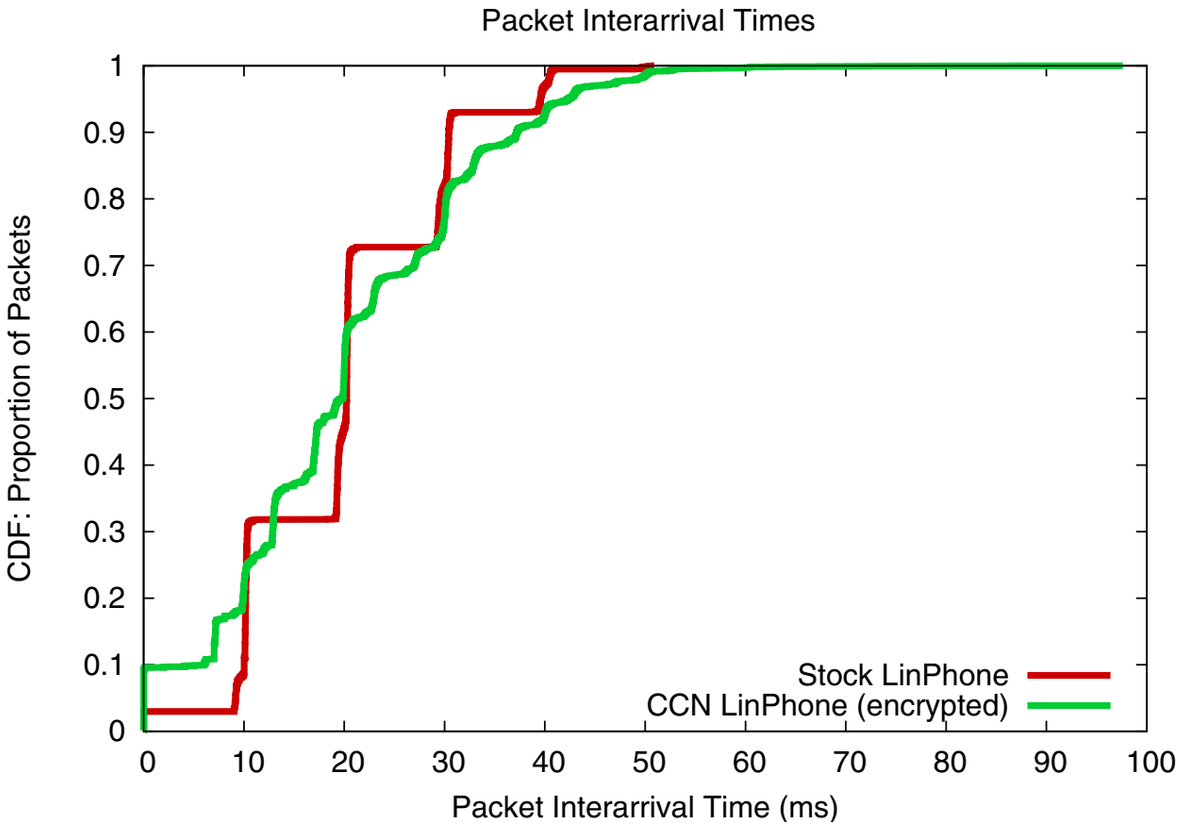


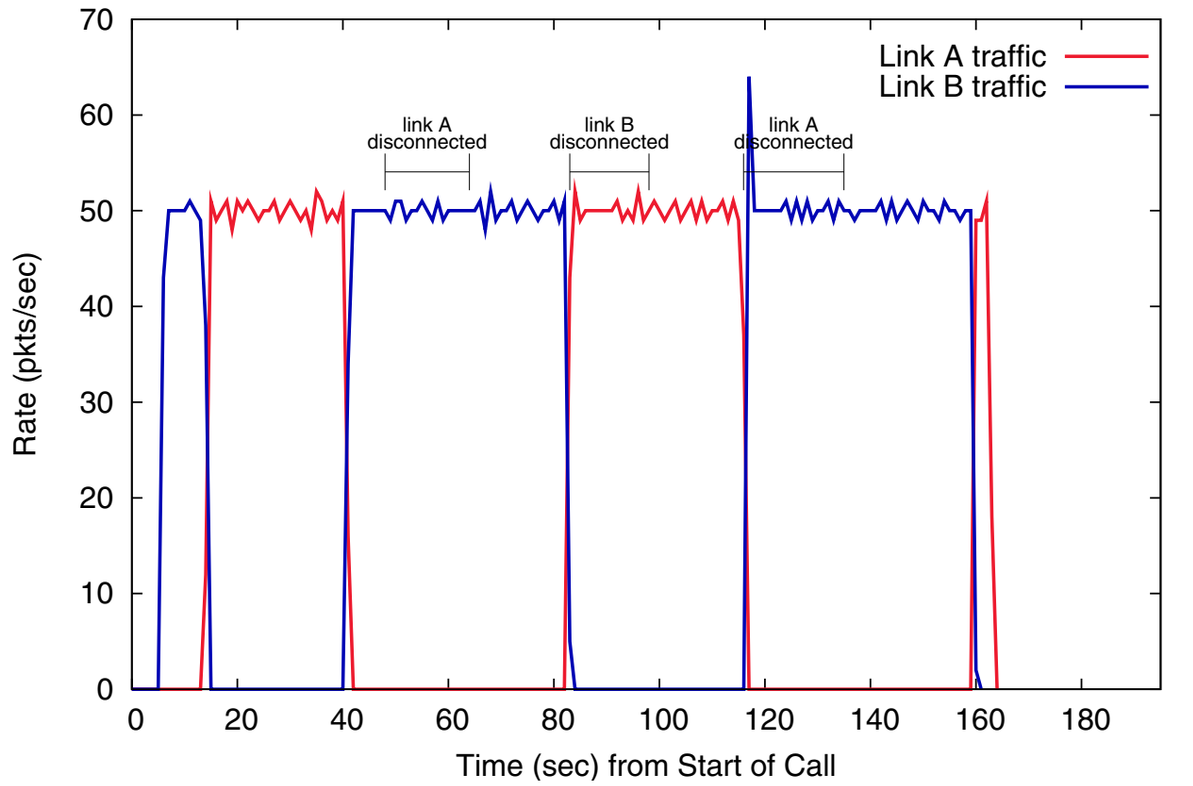
- Resulting system is simple, secure and scalable.
- Robust support for mobility and multi-point.
- Supports secure, stateless, VoIP inter-operation.

Test setup



Performance





Security

Attacker's job is a lot harder with CCN

- Can't target hosts because communication isn't to hosts.
- Can't target topology since multi-source makes topology a hint, not a requirement.
- Can't DDoS with Data packets because Data must match an Interest.

Attacker's job is a lot harder with CCN

- Can't DDoS with real Interests because local caching will negate attack.
- Can't DDoS with fake Interests since every intermediate node has a limit on pending Interests and services unsatisfied Interests at lowest priority.

Files, hosts and network connections are *containers* for information

- A *secured perimeter* is the *only* way to secure containers.

- For today's network use, any realistic perimeter encloses the planet.

Forget containers – secure the content

Do it as the final production step to minimize attack surface.

Ron Rivest's SDSI has shown this can be done if any consumer can assess *solely from the data:*

- Integrity (is data intact and complete?)
- Relevance (what question does this answer?)
- Provenance (who asserts this is an answer?)

CCN data

/nytimes.com/web/frontPage/v20100305/s0 0x3fdc96a4...

signature

0x1b048347

key

nytimes.com/web/george/desktop public key

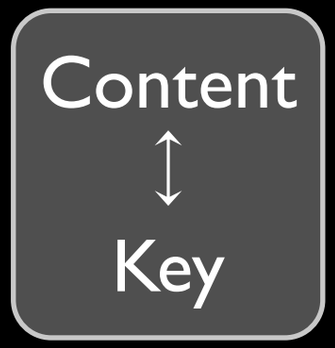
Signed by nytimes.com/web/george

Signed by nytimes.com/web

Note: Content networking has no key distribution problem since keys are just content.

Evidentiary Trust

A rich web of trustworthy information
arises from named, signed data:

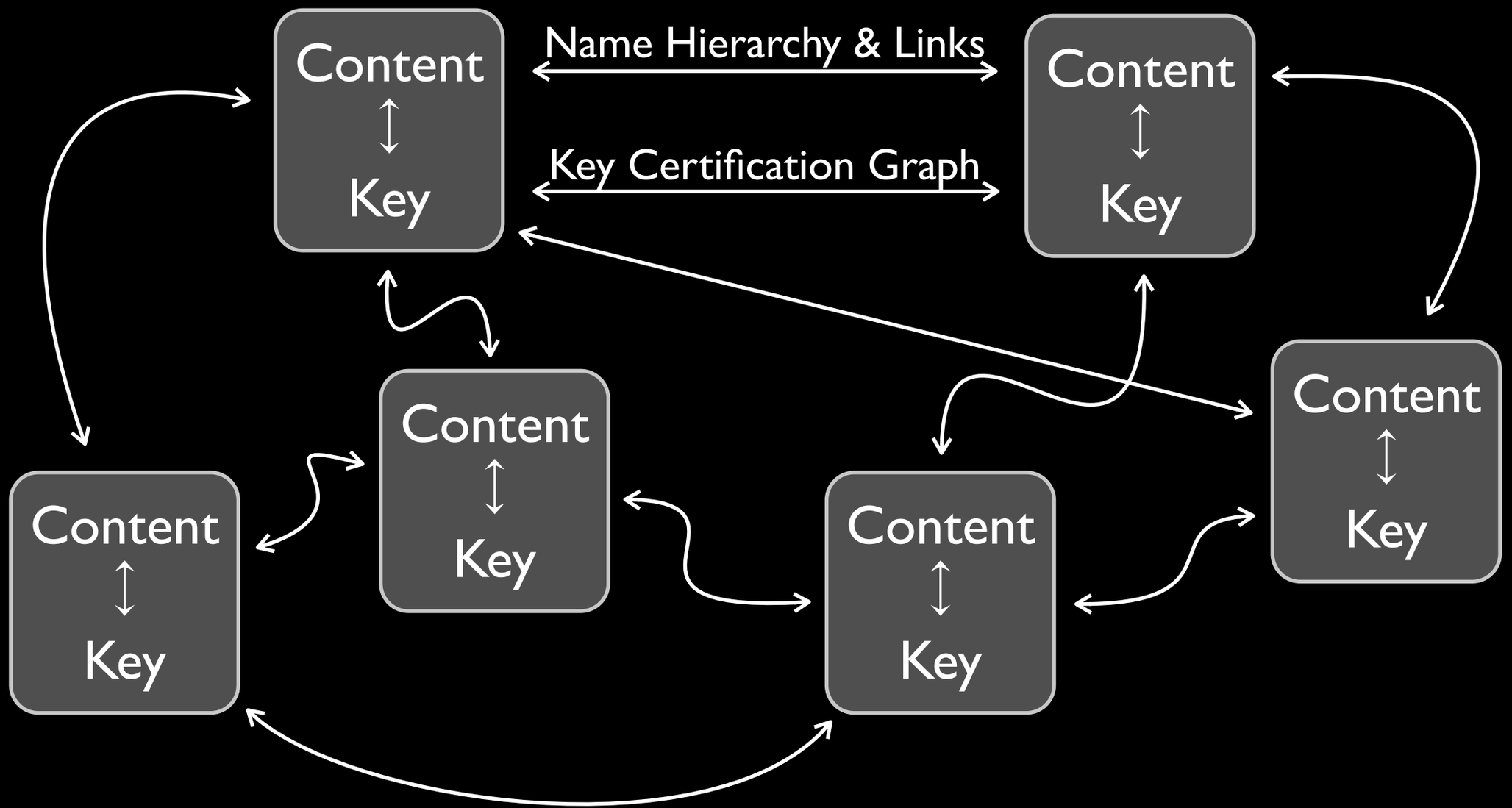


Evidentiary Trust

A rich web of trustworthy information arises from named, signed data:

Evidentiary Trust

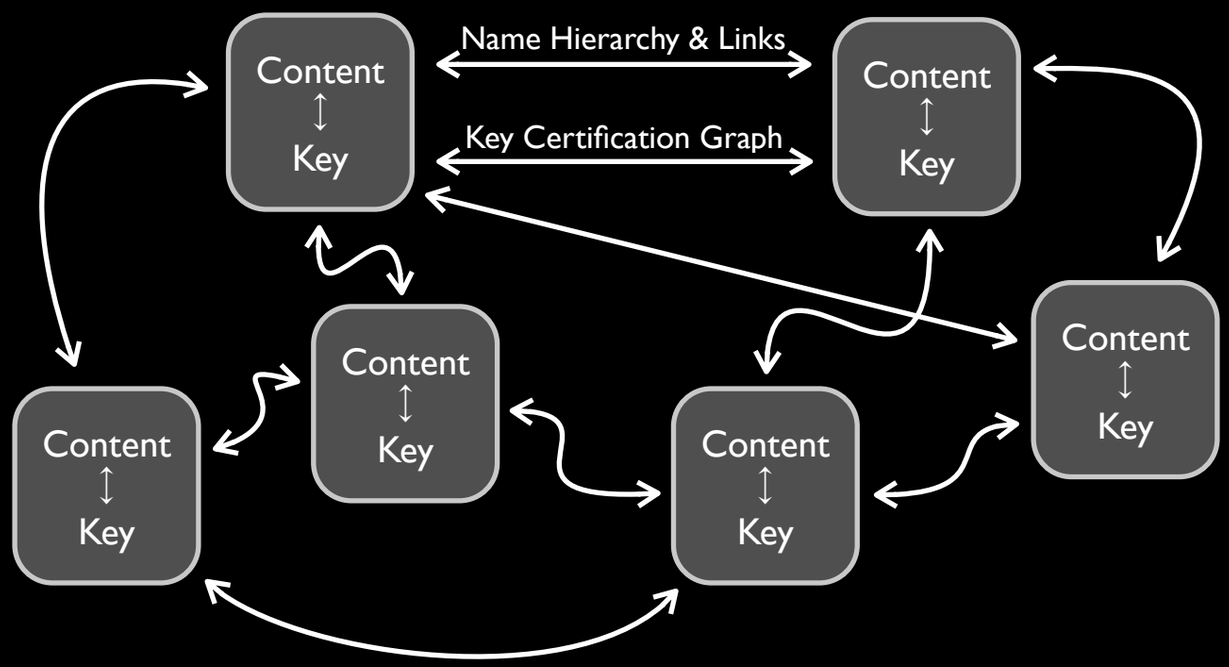
A rich web of trustworthy information arises from named, signed data:



Evidentiary Trust

- Attacker's job gets exponentially harder as you accumulate information.

➡ Security is emergent property of the system.



the PARC CCN Team

- Jim Thornton
- Diana Smetters
- Russ Atkinson
- Simon Barber
- Rebecca Braynard
- Nick Briggs
- Tim Diebert
- Priya Mahadevan
- Mark Mosko
- Michael Plass
- Paul Rasmussen
- Elaine Shi
- Ignacio Solis
- Ersin Uzun

Named Data Networking (NDN)
NSF FIA 3 year project

UCLA

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

UCIrvine
University of California, Irvine

THE UNIVERSITY OF MEMPHIS

UCSD

parc
Palo Alto Research Center

ARIZONA

Yale UNIVERSITY

Colorado State University

Washington University in St. Louis

Lixia Zhang (lead)

Jim Thornton (manager)

Deborah Estrin (advisor)

Van Jacobson (architect)

Dmitri Krioukov

Dan Massey

Christos Papadopoulos

Gene Tsudik

Tarek Abdelzaher

Jeff Burke

K Claffy

Patrick Crowley

Ersin Uzun

Lan Wang

Edmund Yeh

Beichuan Zhang

Information on CCN is available at

`www.ccnx.org`

including a GPL'd open-source release of our current research prototype.

Information on NDN is available at

`named-data.net`