Named Data Networking

IEEE CCW
Oct 10, 2011

www.named-data.net

Agenda

A. NDN Overview

B. NDN Security

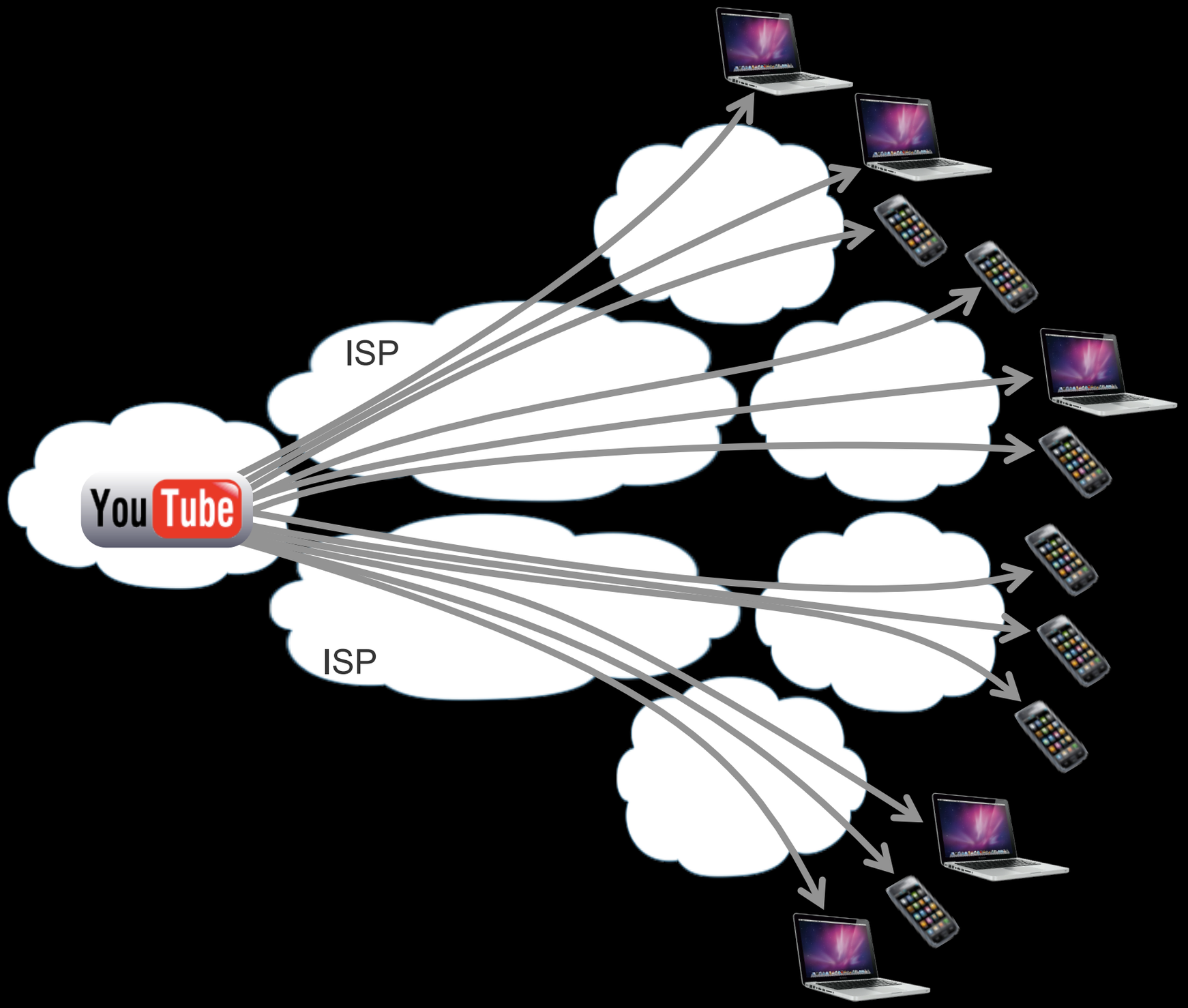
   1) Architecture Basics

   2) Privacy

   3) Routing and Application Security

C. Summary

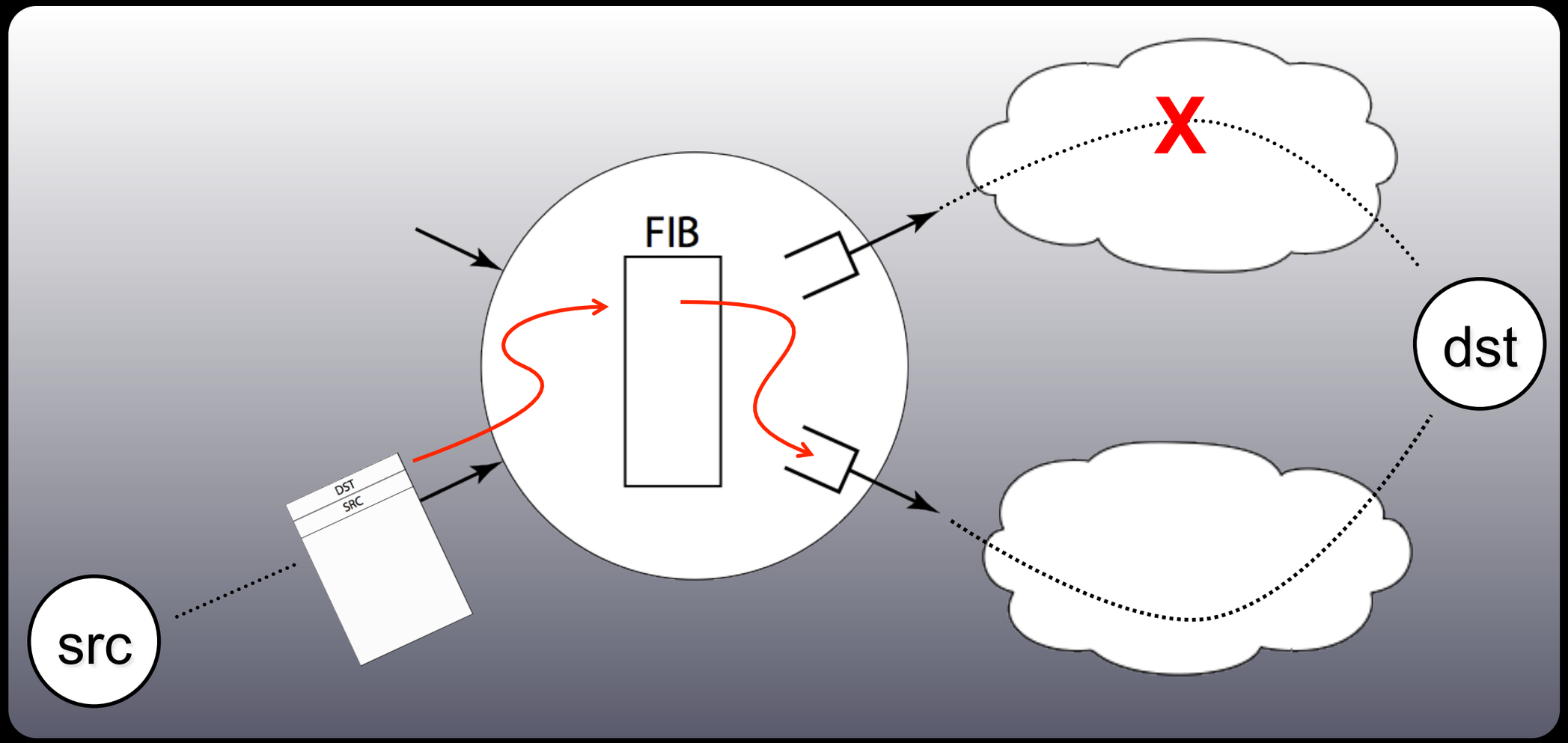
The problem



Communication v. Distribution

	Communication	Distribution
Naming	Endpoints	Content
Security	Secure Process	Secure Content

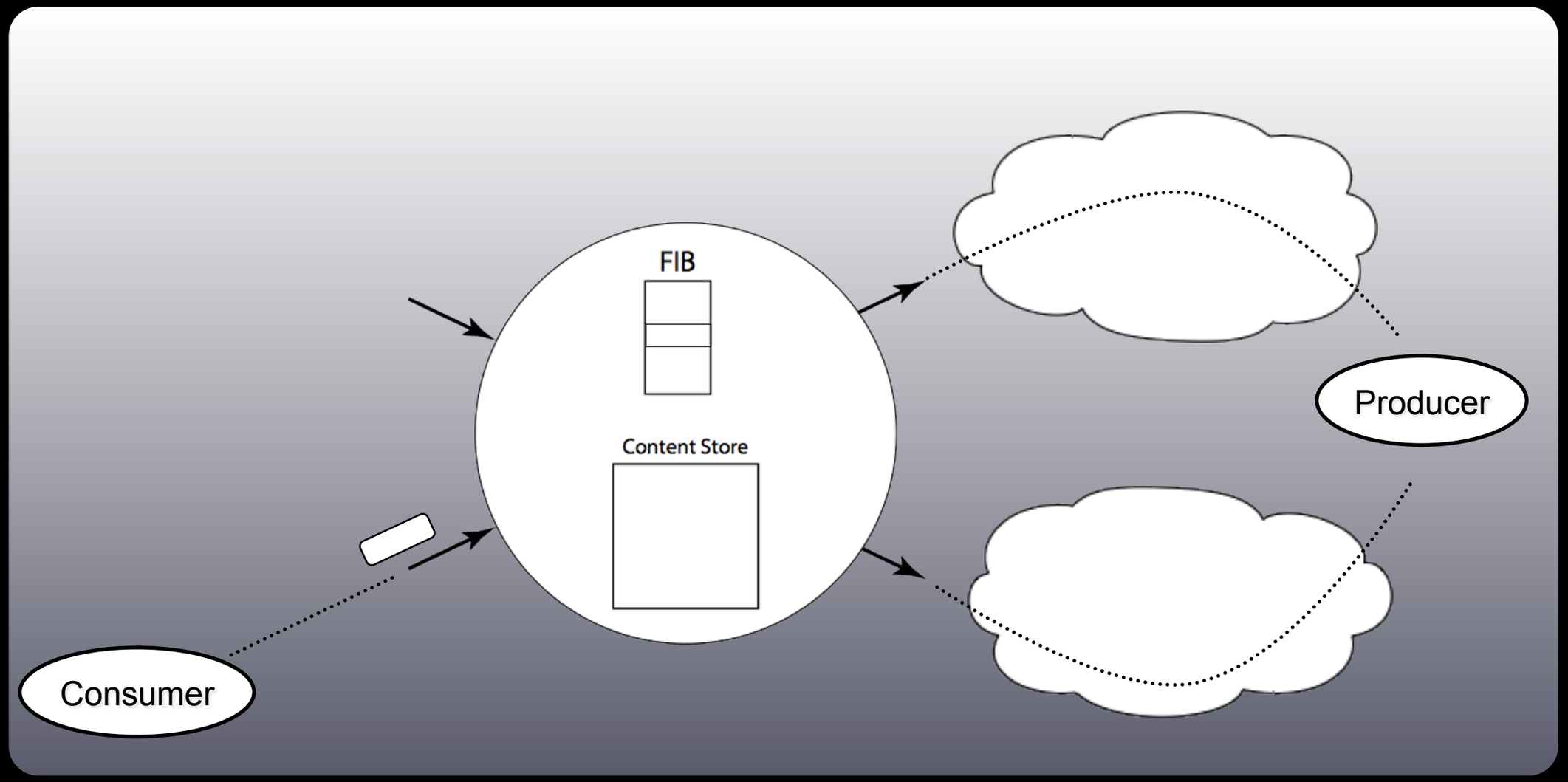
Today



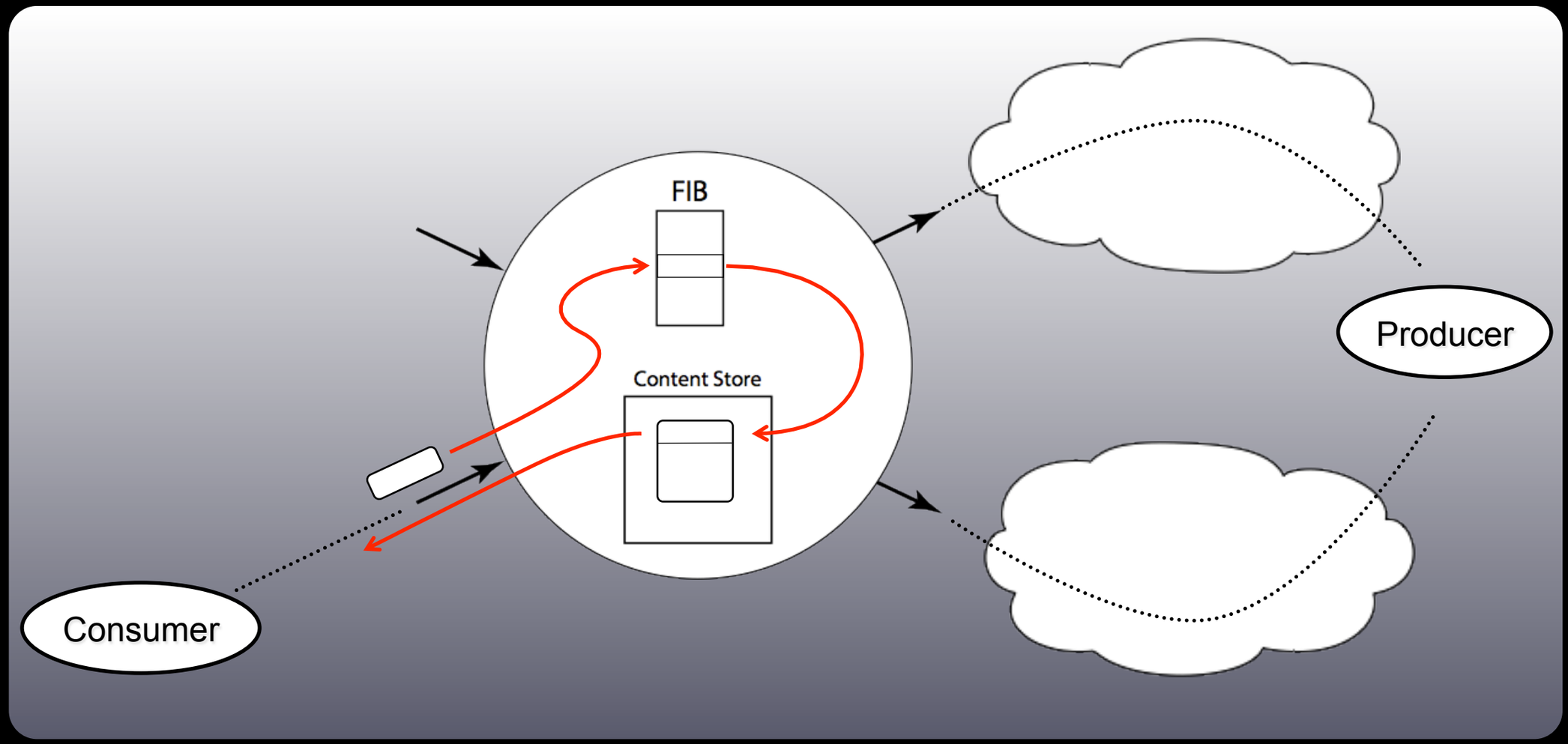
Path determined by global routing, not local choice

Structural asymmetry precludes market mechanisms and encourages monopoly formation

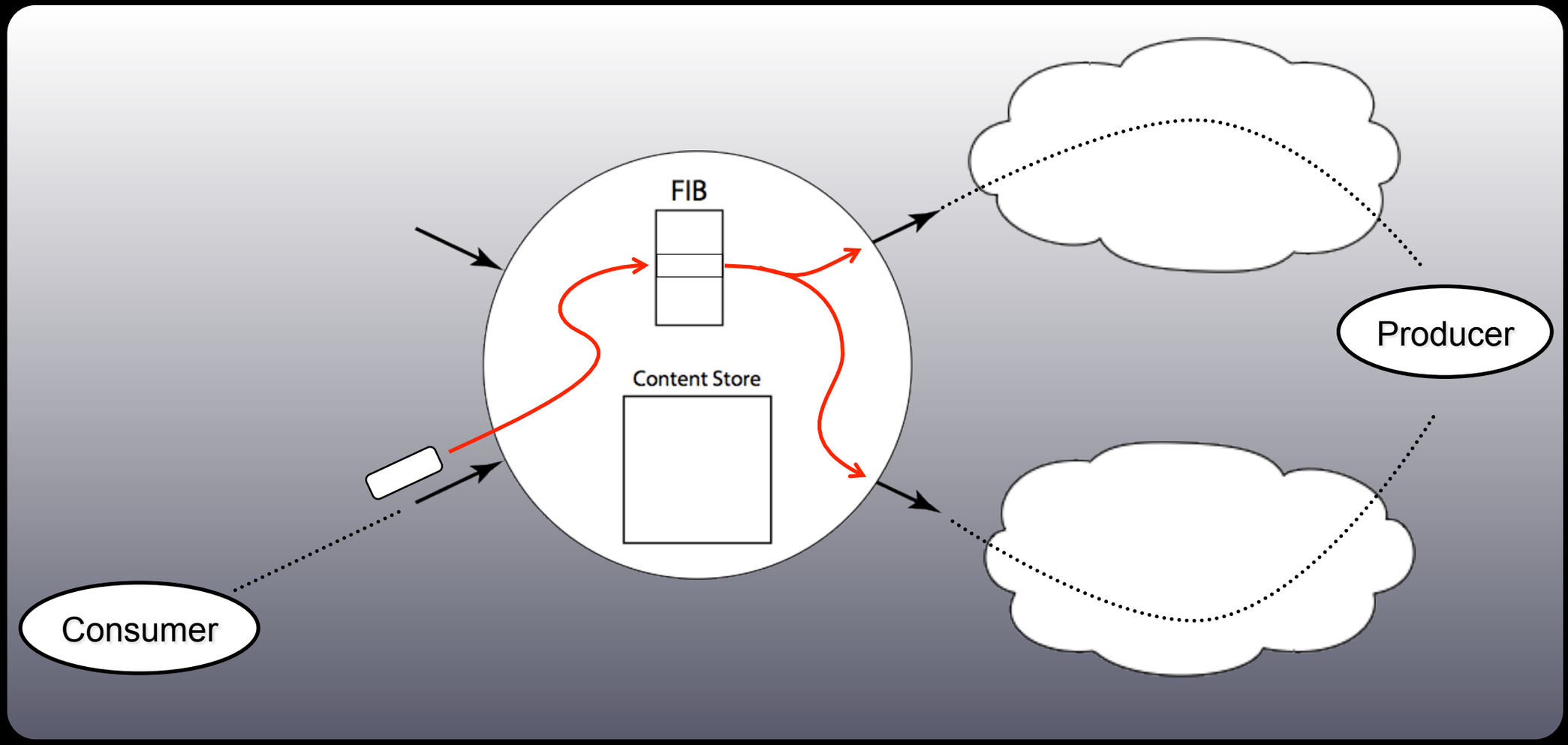
NDN approach



NDN approach

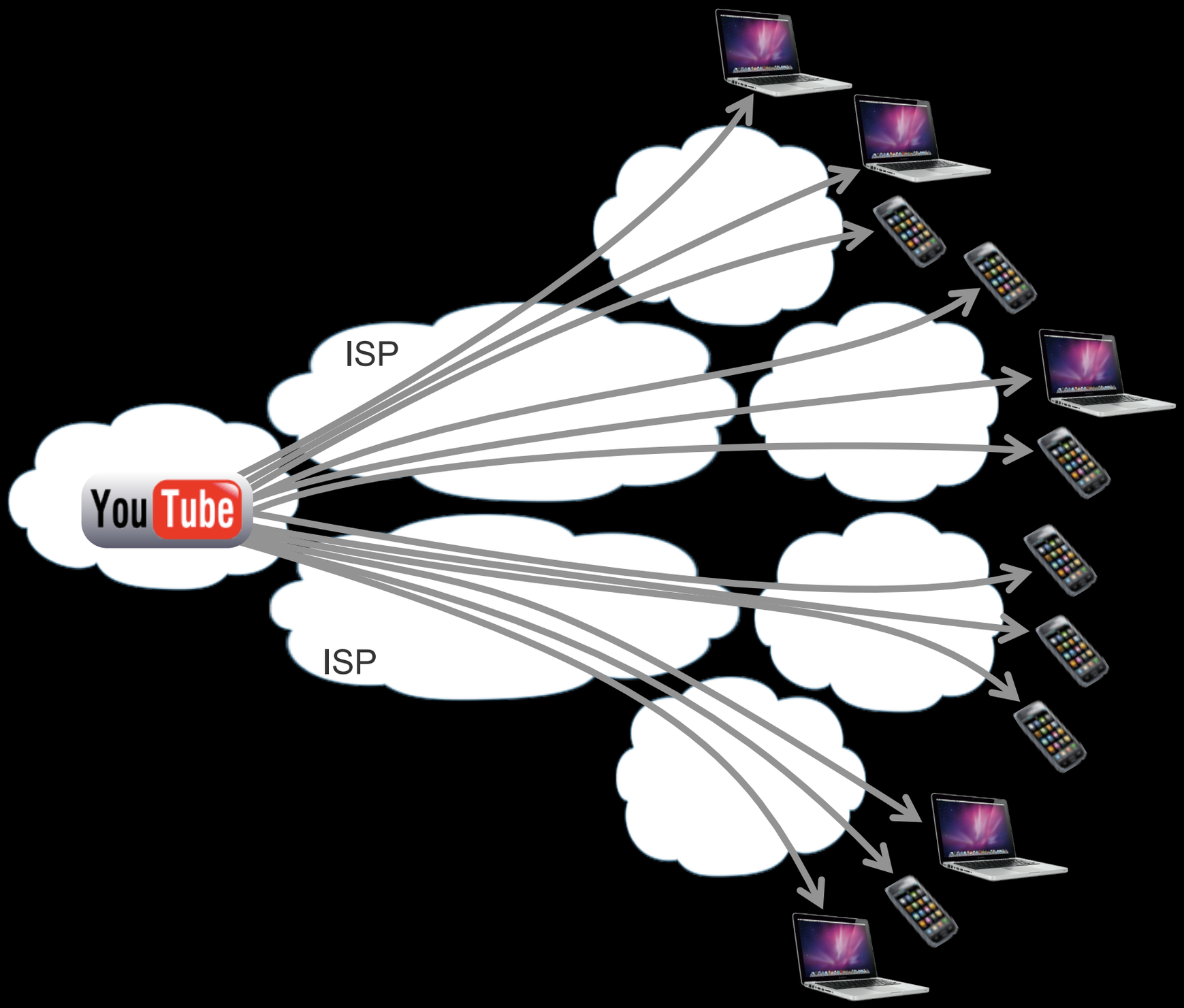


NDN approach

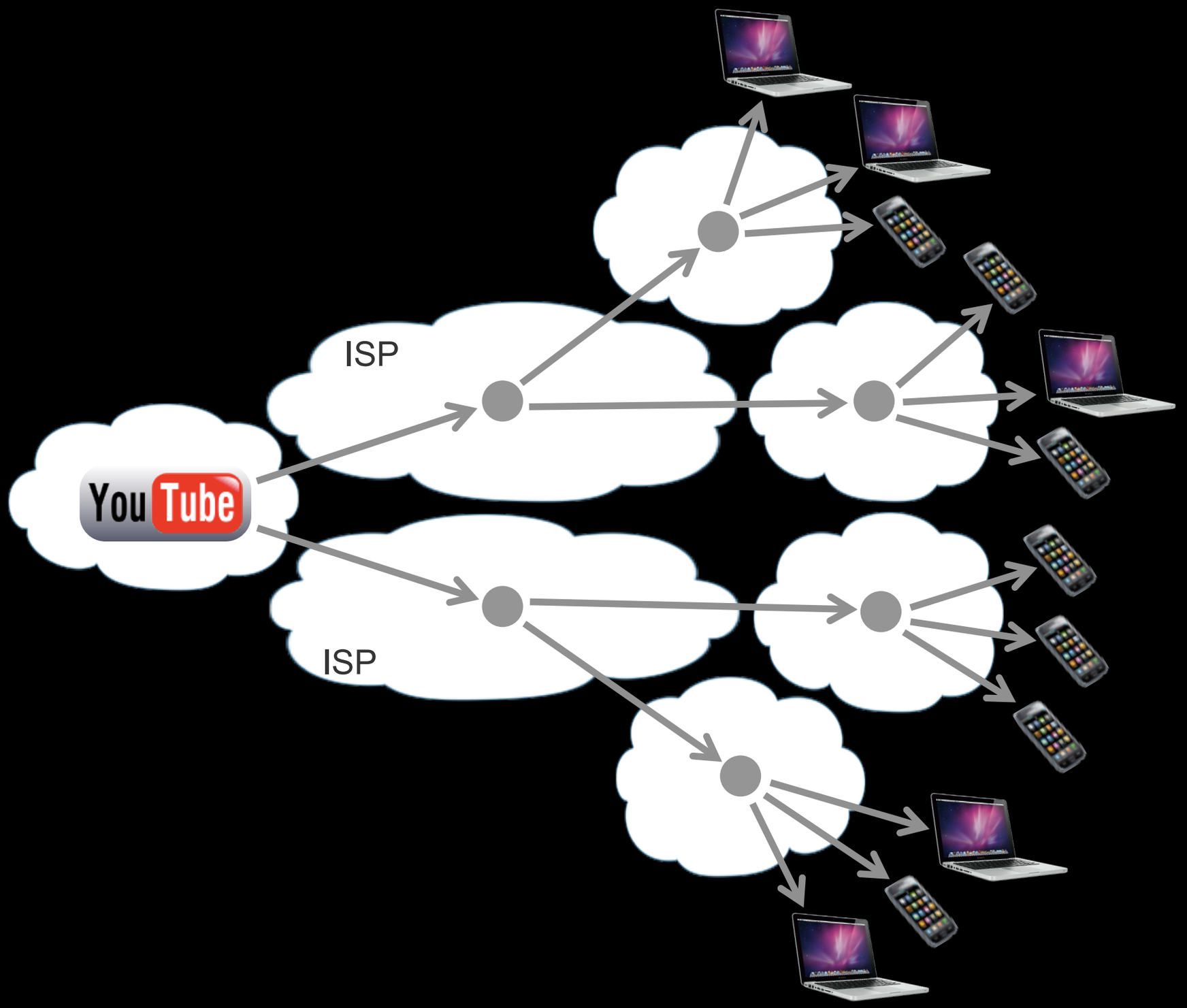


- Packets say ‘what’ not ‘where’ (no src or dst)
- Forwarding decision is local
- Upstream performance is measurable

We envision replacing this:



With THIS:



Agenda

A. NDN Overview

B. NDN Security

   1) Architecture Basics

   2) Privacy

   3) Routing and Application Security

C. Summary

Securing Content

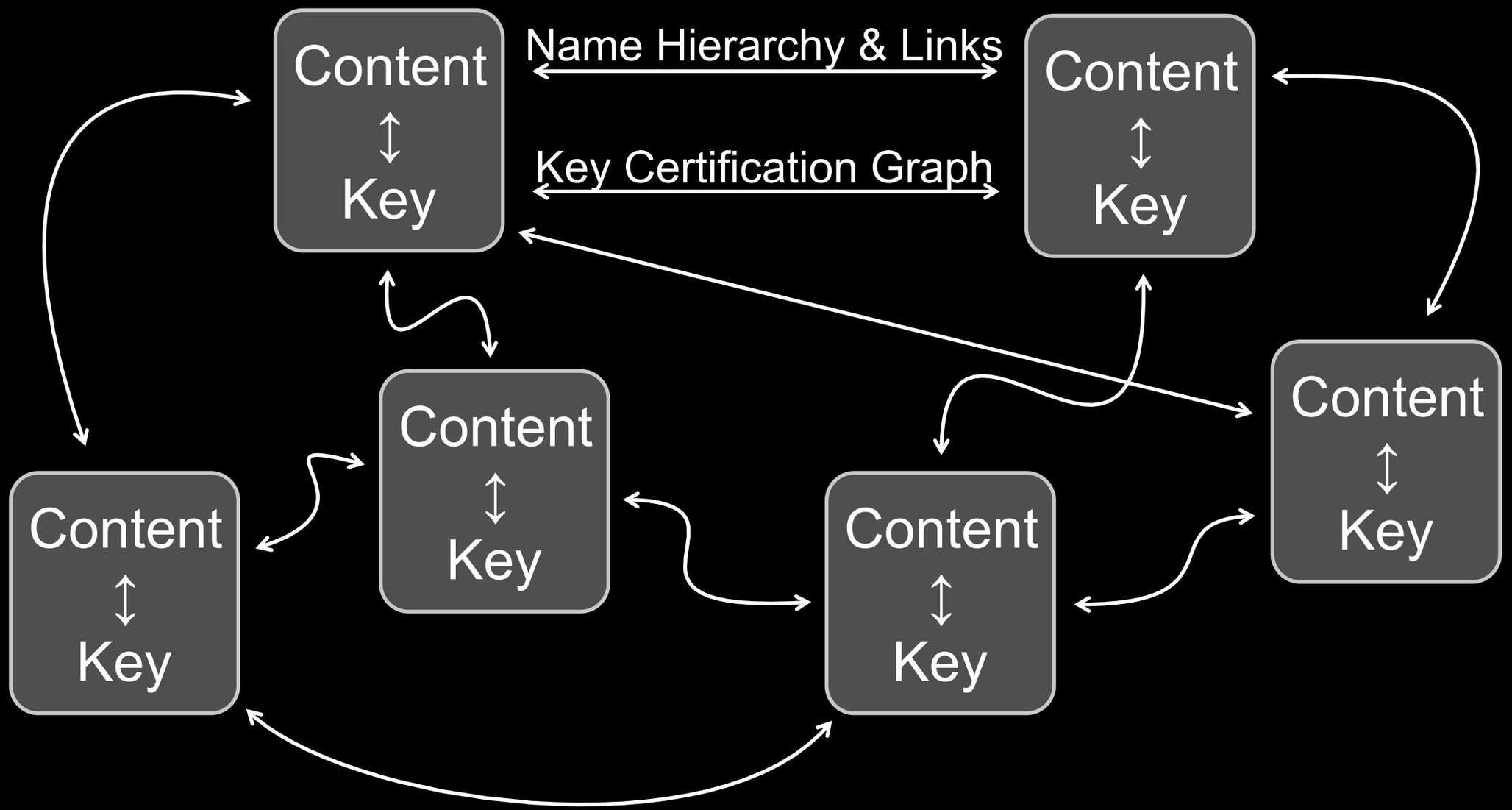
Content Packet = 〈 *name*, *data*, *signature* 〉

Any consumer can ascertain:

- Integrity: is data intact and complete?
- Origin: who asserts this data is an answer?
- Correctness: is this an answer to my question?

Evidentiary Trust

A web of trust gradually & organically arises from named and signed content:



DoS Resistance

Many current DoS + DDoS attacks/threats become irrelevant because of NDN architecture

- A few notable features:
  - Content caching mitigates targeted DoS
  - Content not forwarded w/out prior state set up by interests
  - Multiple interests for same content are collapsed
  - One copy of content per “interested” interface is returned
  - Stateful routing helps to fight/push back attacks

Some (new) attack opportunities (e.g., signatures) may be possible, but it is much more resistant to DoS attacks than what we have today.

Data plane resilience

- IP data delivery strictly follows FIB direction:
  - One-way data flow -- cannot detect failures
  - Has no effect on routing decisions
- NDN content delivery is a 2-step process:
  - Interest forwarding to set up state
  - Content traversal of interest path in reverse
- Interest forwarding state eliminates looping, allows exploitation of topological redundancies and multipath forwarding
- Content packets measure quality of selected (interest) paths ➔ lets forwarding plane incorporate congestion and fault mitigation into path decisions

Agenda

A. NDN Overview

B. NDN Security

   1) Architecture Basics

   2) Privacy

   3) Routing and Application Security

C. Summary

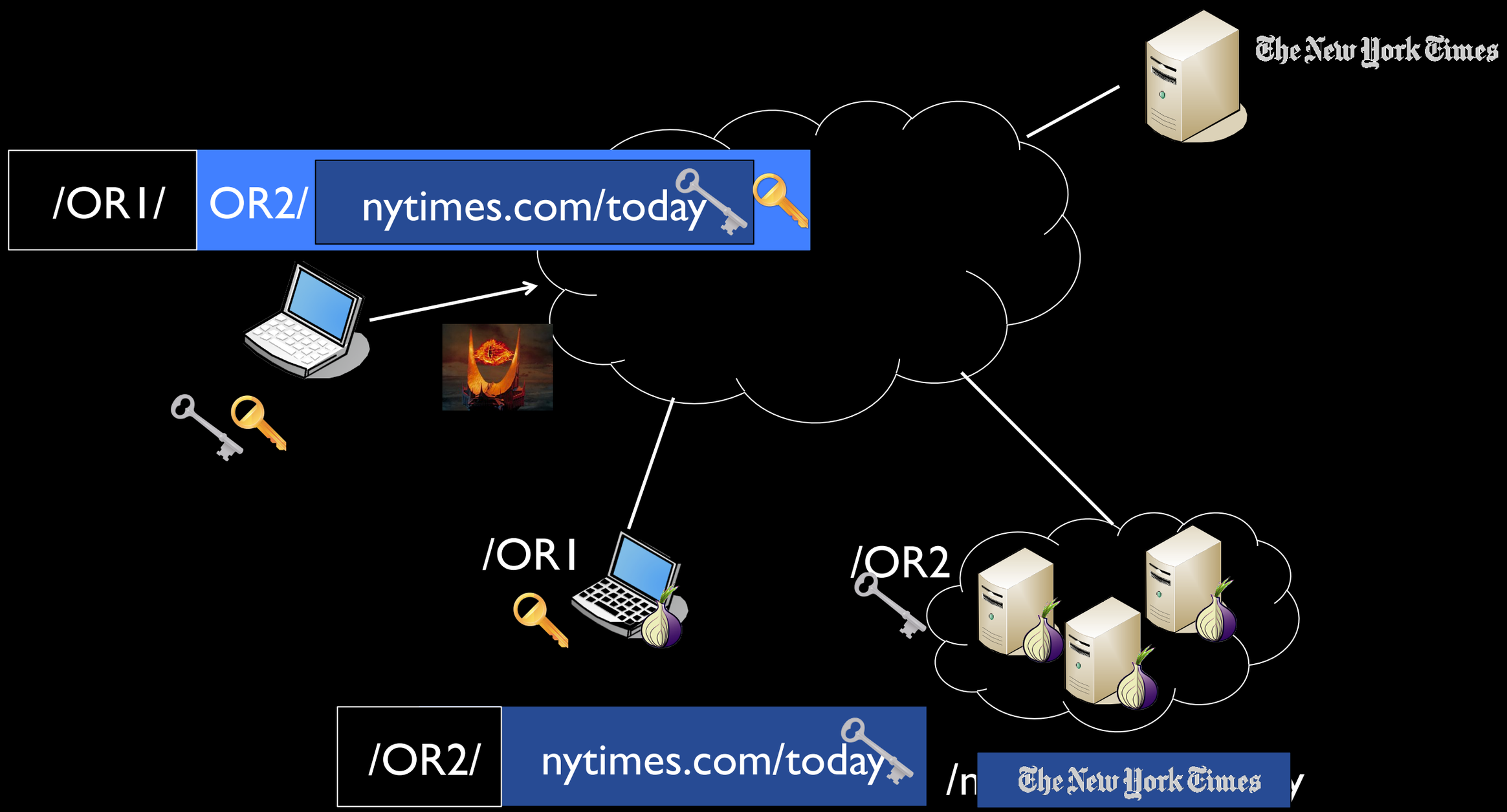
Privacy Challenges in NDN

- Lack of source addresses in NDN packets provide much better privacy than IP. However, there are still challenges if the attacker is can monitor the traffic close to the user (e.g., in the same LAN):
- *Name Privacy:* semantically related names
  - Interested in "/healthonline/STDs/.."
- *Content Privacy:* unencrypted public content.
  - Retrieved content is an ".mp3" file
- *Signature Privacy:* leaked signer(publisher) identity
  - Retrieved content is signed by "match.com"
- *Cache privacy:* detectable cache hits/misses
  - Interests from this user usually misses caches -- it is for Russian content.

Named Data Onion Routing

- Consists of client and anonymizing router (AR) software
- Layers of encrypted Interests reside inside the name component of interests
  - E.g.,: */anonymizer/Enc(Timestamp* || *key* || *Interest)*
- Content is encrypted with the client-provided key on its way back
  - Encapsulation is published under the requested name and signed by ARs.

Example


The New York Times
/OR1/
OR2/
nytimes.com/today
/OR1
/OR2
/OR2/
nytimes.com/today
The New York Times

Agenda

A. NDN Overview

B. NDN Security

   1) Architecture Basics

   2) Privacy

   3) Routing and Application Security

C. Summary

Using NDN Features to Secure Routing

- Need to protect routing updates (where content prefix is reachable)
- Router names follow network management hierarchy
- Names associated with signing keys (not only 1:1)
- Keys are authenticat-able:
  - Network operator configures trust anchor for each router, e.g., public key for /ndn/ucla.edu/
  - Router key (e.g., /ndn/ucla.edu/bb1) certified by anchor key
  - Each interface has a name, (e.g., /ndn/ucla.edu/bb1/f1); router key certifies each interface key
- Updates from each interface signed by that interface key

NDN Lighting Control Application

Testbed: UCLA Film & TV Studio #1

- Special case of actuators in an instrumented environment
- Rich set of use cases (e.g., entertainment)

IP in Lighting Systems?

- Security currently achieved by:
  - Physical network segregation, or
  - VLANs + firewalls
- Devices increasingly receive over-the-air upgrades & updates
  - Not clear how to accommodate with above in scalable manner
- IP-based addressing irrelevant to applications
  - Easier to address fixtures in application-specific terms without having to know through/to which gateway they connect
- IP configuration particularly brittle for dynamic systems
  - Lighting devices (fixtures) can come & go frequently
  - Certain building systems incorporate mobile devices

Bootstrapping

- No preconfigured information in fixture, other than manufacturer-supplied:
  - Public/Private key-pair and initial authenticator

- Standard mechanisms used for lighting interface to connect to NDN on one side and discover fixtures on another

- Fixture starts with pre-configured name:

  /ndn//lighting/<manufacturer>/<Pubkey-hash>

- To discover fixtures, configuration manager sends interests for:

  /ndn/lighting/

  - Once located new fixture, retrieves (via interest) its public key data:

    /ndn/lighting/<manufacturer>/<Pubkey-hash>/key

  - Out of band, configuration manager obtains initial authenticator & fingerprint of public key per fixture

- Configuration manager issues “signed interest” authorizing its public key to configure fixture
  - Contains KeyLocator for configuration manager public key
  - Includes initial authenticator of fixture, encrypted with latter’s public key

Subsequent Control

- After bootstrapping, configuration manager grants permissions to applications by publishing their keys under names representing (authorized) capabilities
- Fixture checks if application signing key is in:
  (1) its cache of authorized keys, or (2) built-in trust anchor list created at bootstrap time, or (3) it is published (signed) by a key that satisfies (1) or (2)
- To minimize delay, signed commands are expressed as part of name within interest

Other applications in the works

- Audio conferencing
- Participatory sensing
- Personal data cloud
- Media distribution/streaming
- VPN server/client
- Network monitor/management tools

Agenda

A. NDN Overview

B. NDN Security

   1) Architecture Basics

   2) Privacy

   3) Routing and Application Security

C. Summary

SUMMARY

- Lots of work underway
- Much of what was presented not “cast in stone”
- Didn’t cover:
  - Signature schemes (e.g., batch operations, streaming content)
  - Trust establishment / Trust frameworks
  - Usability of S&P
  - Security in other apps, e.g., sensing, conferencing

Thanks!