

CSC4200 – NEXT-GENERATION NETWORKING

INFORMATION CENTRIC NETWORKING

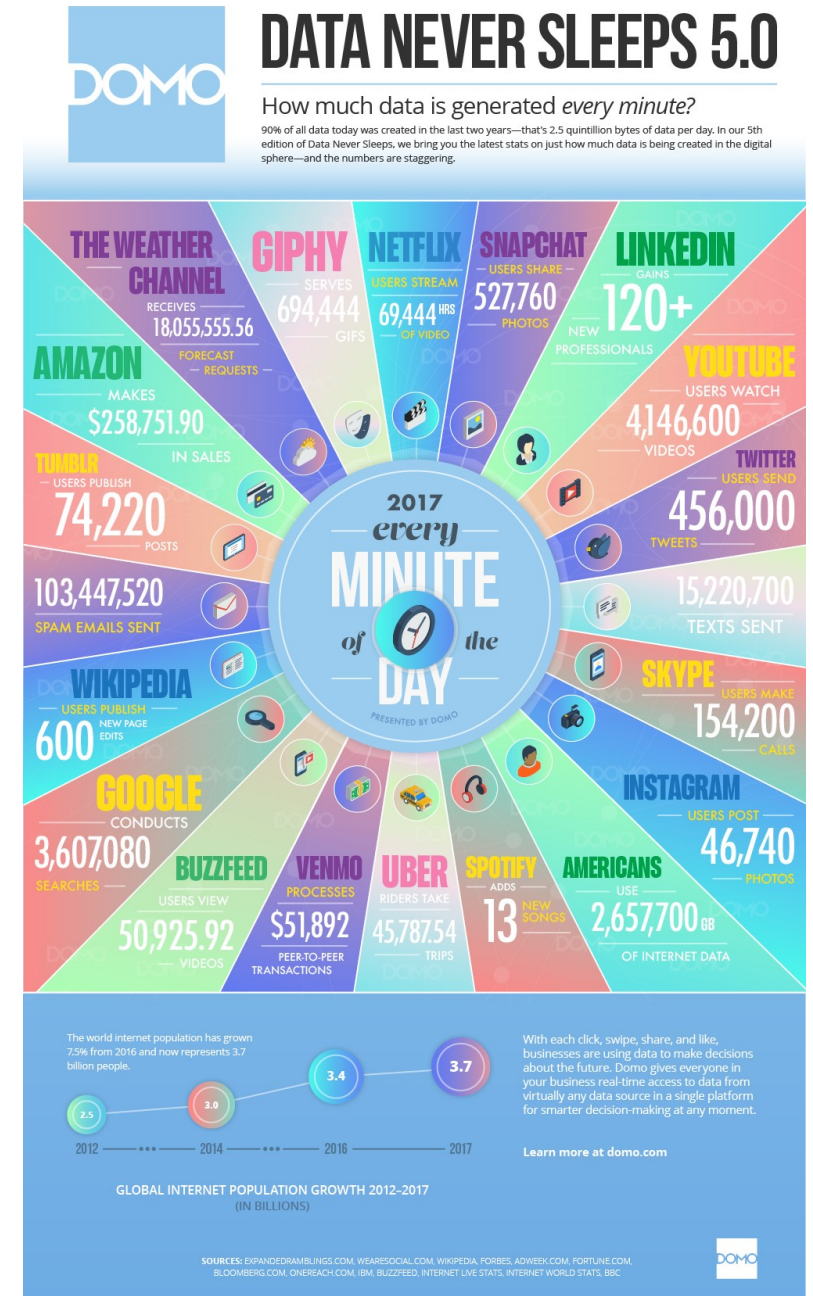
Instructor: Susmit Shannigrahi
sshannigrahi@tntech.edu

TCP/IP Design Rationale

- The Internet was designed for communication between a source and a destination
 - Networks were slow and computers super expensive
 - Sharing computing resources across long distances was desirable
 - Security was not even considered
 - First use-case: file transfer from/to a server
- Do these assumption hold today?

Today...

- Internet users are streaming data..
 - Many different streaming services (Amazon, Hulu, Netflix..)
- Internet users generate huge amounts of data
 - 2.5 quintillion (10^{18}) bytes per day
 - So many devices (IoT, mobile phones) generating data
- So many heterogeneous network environments
 - Vehicular, core Internet, building sensors, mobile, data center, etc...



Internet is a success because of applications

- Applications today are “data-centric”
 - They request the data they need
 - They do not care where the data comes from
 - All they need is to verify data authenticity
- “Data-centric” applications combined with a “host-centric” Internet and tech companies?
 - Internet consolidation! [1]

[1] <https://tools.ietf.org/html/draft-arkko-iab-internet-consolidation-02>

What is Internet Consolidation?

- Internet was meant to enable communication among humans
 - Tech companies want any sort of communication to pass through them
 - Why?
- Result: The Internet has become extremely centralized
 - Communication typically passes through a cloud server
 - If users cannot reach the cloud, they cannot communicate
 - Example: messaging app with participants next to each other
- From the IAB draft: *“If the world changes, the Internet and its technology/architecture may have to match those changes”*

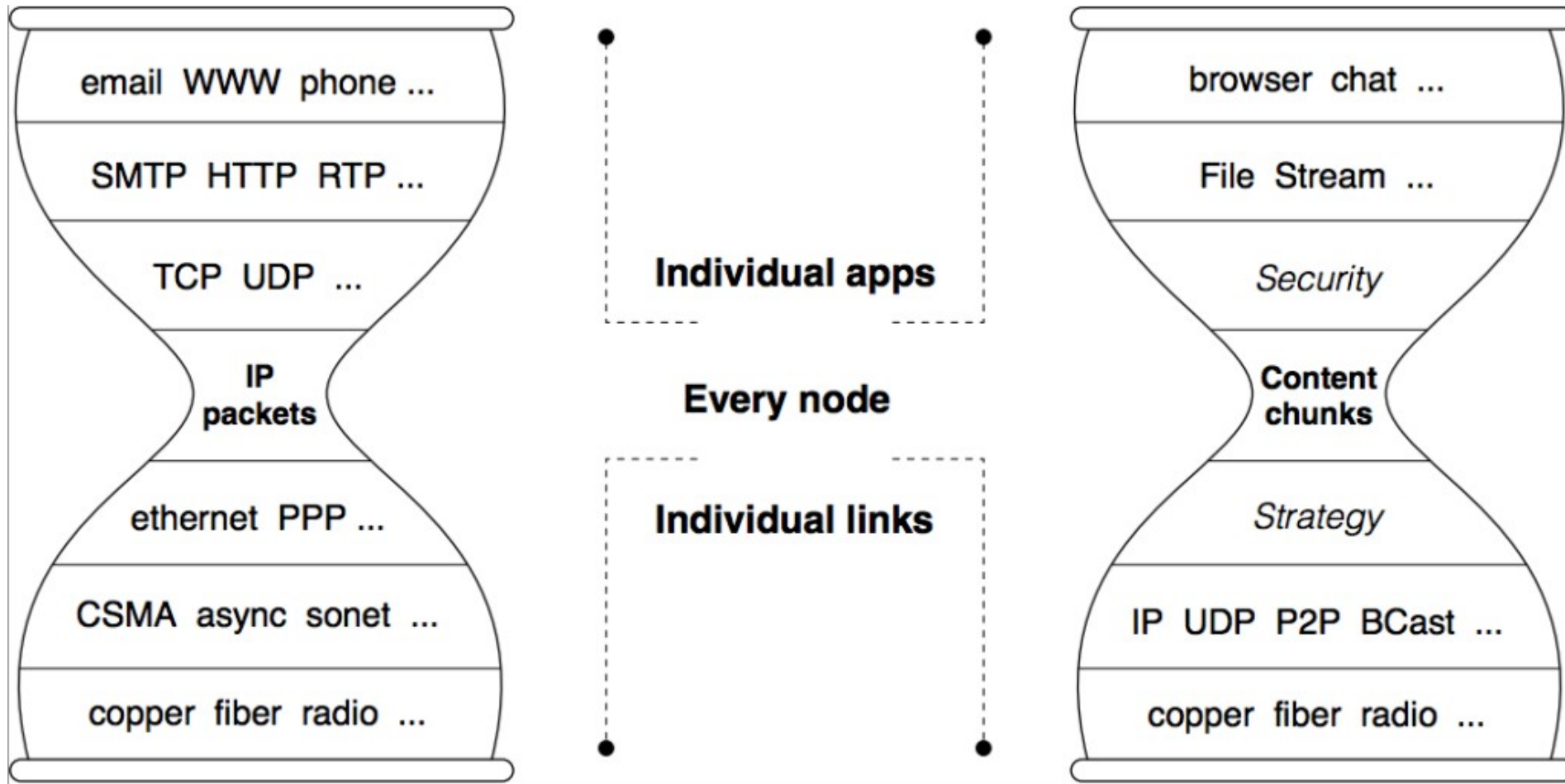
The world is changing..

- “Data-centric” applications
 - That’s the way applications are designed
 - They request data through names (URLs..)
- Heterogeneous network environments
 - Not only file transfers from/to a server!
 - Multicast support necessary
- Security by design
 - We do not know every Internet user anymore...
 - We trust the data we download if we trust the server that we communicate with (i.e., secure connection). What if the server gets hacked?

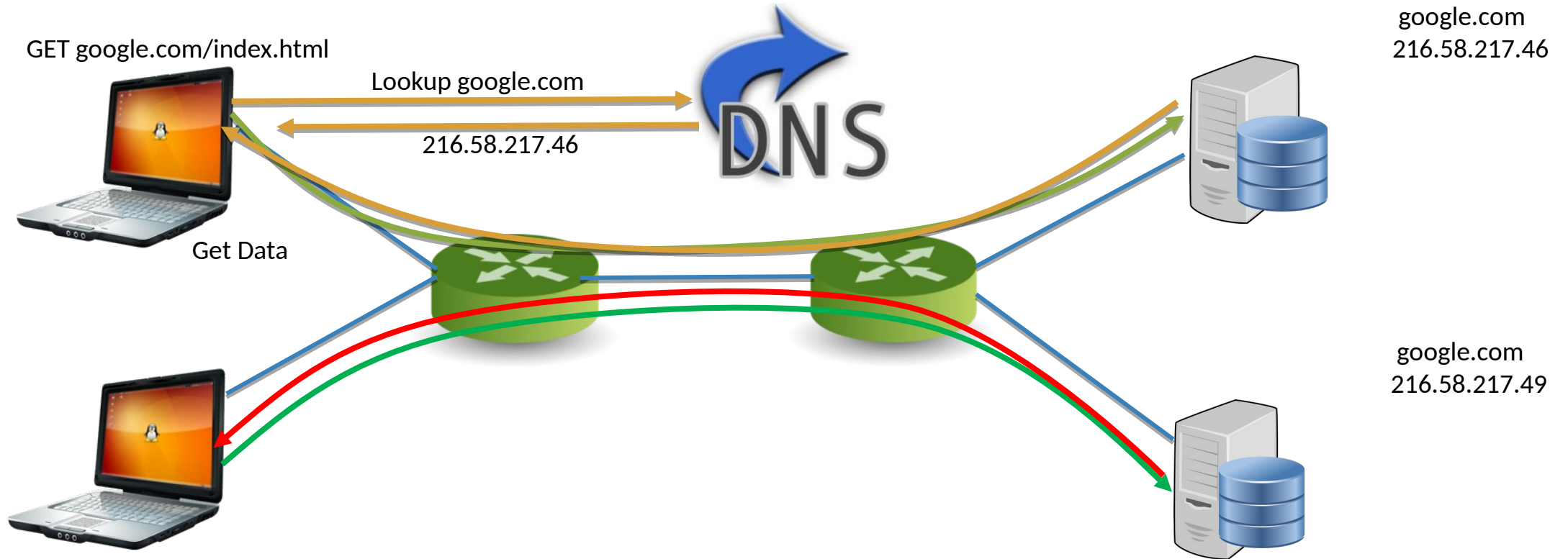
Information-Centric Networking (ICN)

- Shift from a host-centric to a data-centric communication model
 - Instead of using IP addresses, entities communicate based on "named-information"
- Named Data Networking (NDN): The most prominent realization of ICN
 - Started as an NSF-funded Future Internet Architecture (FIA) project in 2010
 - <http://named-data.net>

Architectural Comparison with IP



IP Based Communication

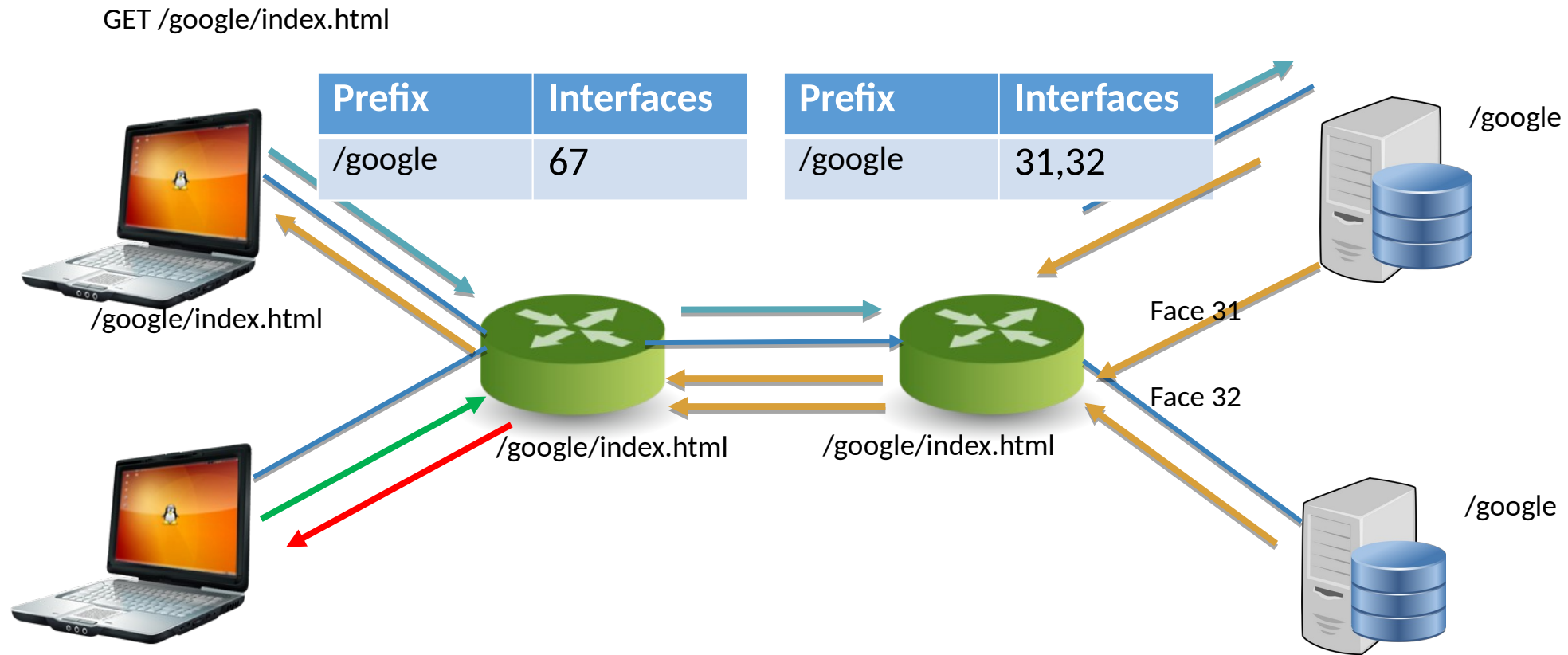


Named Data Networking

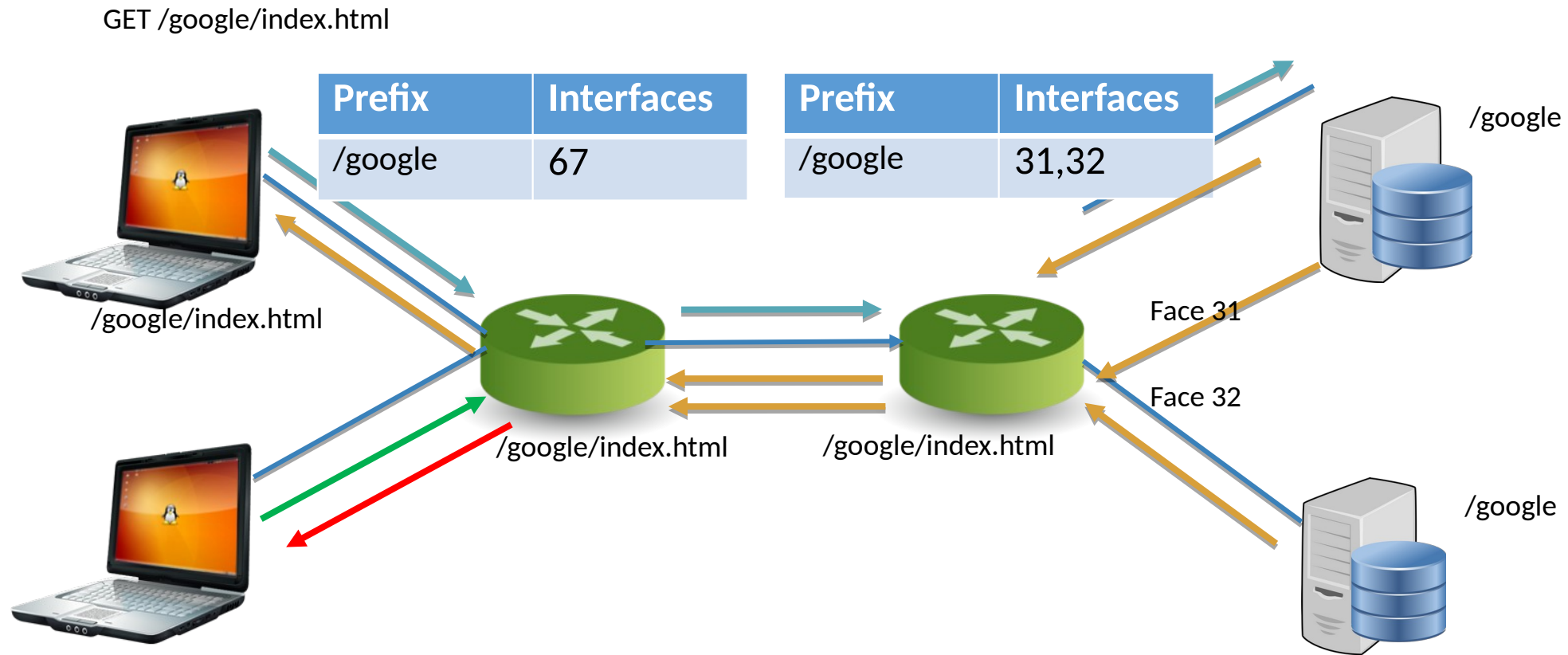
- A clean slate future Internet architecture
 - Emphasizes on **what (named content)**, not **where (hosts)**



Name Based Communication in NDN

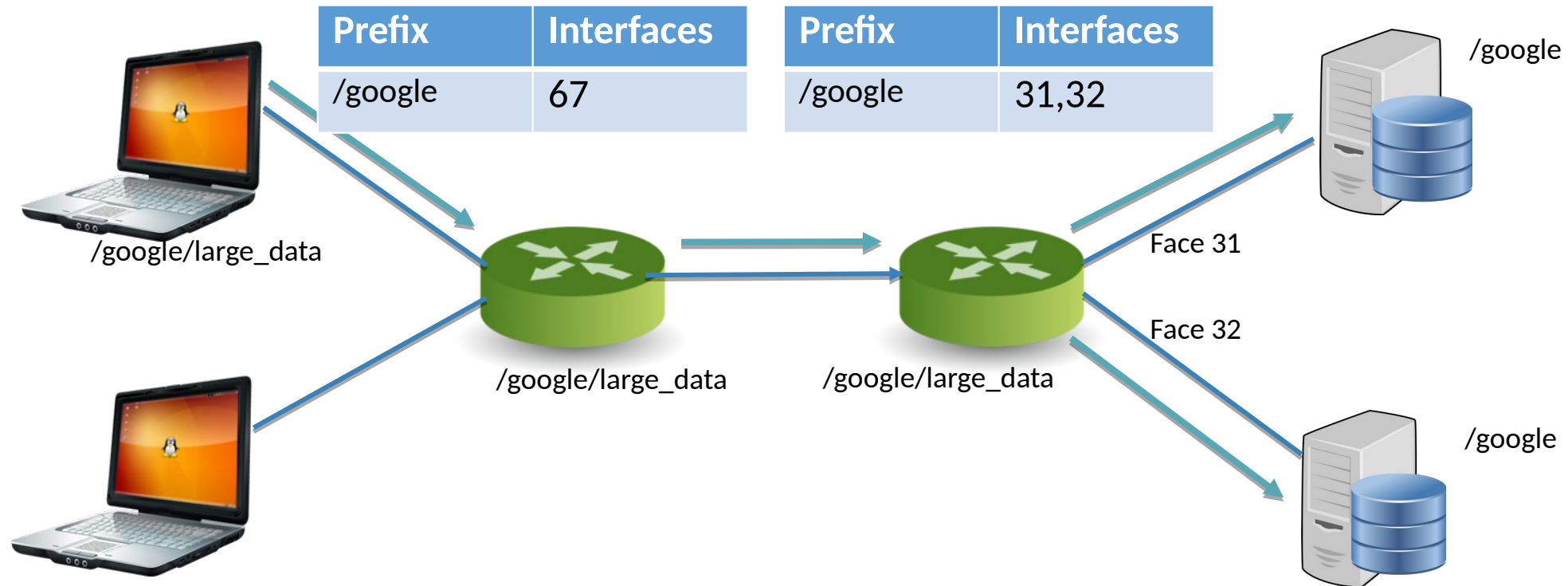


Interest aggregation and caching

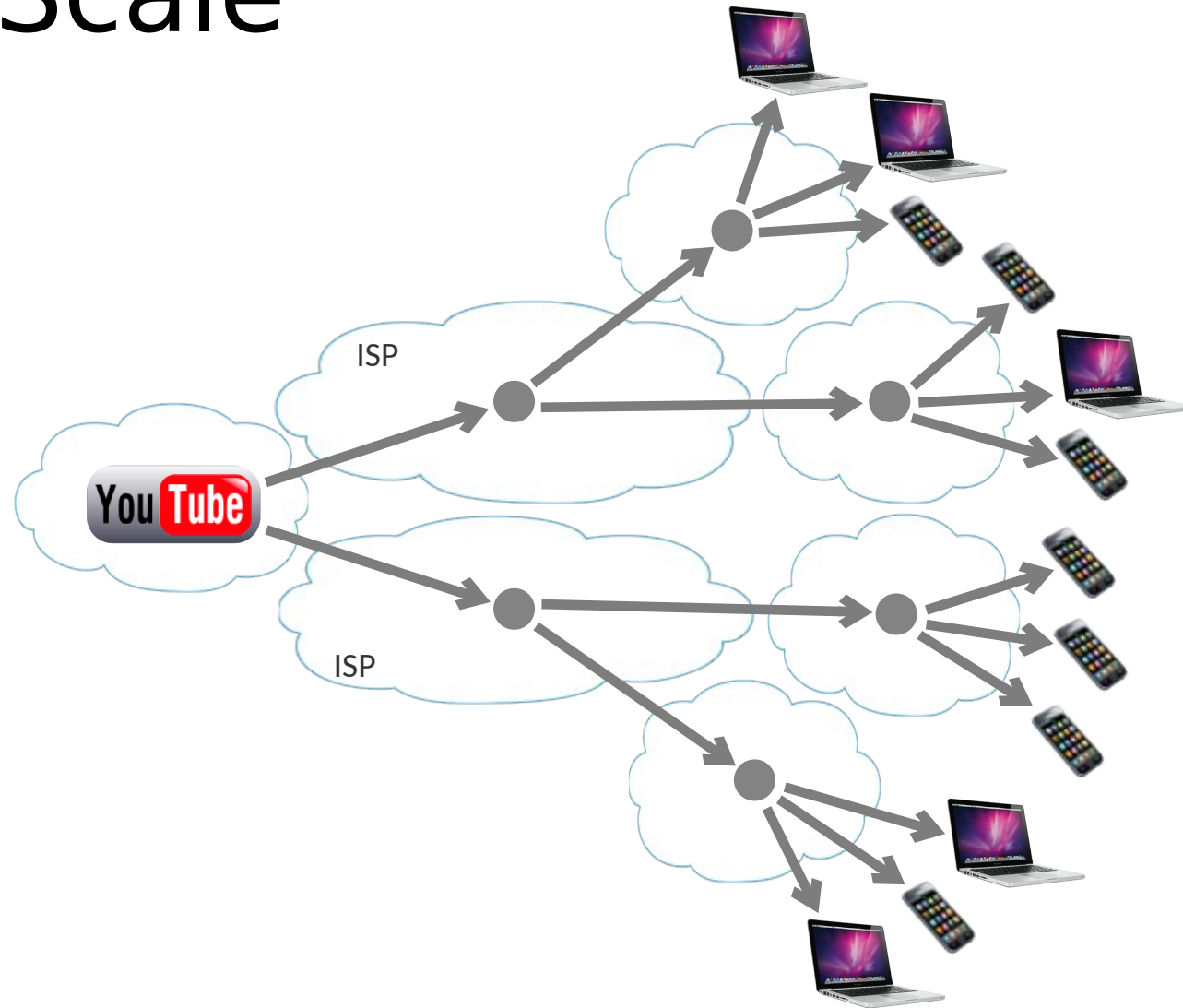


Intelligent Forwarding Strategy

GET /google/large_data



NDN at Scale



NDN Packet Format

NDN Forwarding Daemon Workflow

Why Stateful Forwarding?

- “End-to-end principle”
 - Only significantly beneficial functions must be implemented by lower layers of the architecture
 - IP is state-less
 - Why shifting so much? Can state be so beneficial?
- Scale multicast data delivery!
 - Load balancing, congestion control, data retrieval through multiple paths
- Heterogeneous and dynamic network environments
 - Adapt to network failures
 - Multi-homing and intermittent-connectivity

Security in NDN

- Every data packet has a publicly verifiable signature
 - binds content name to actual payload
 - data packets have key locators that points to the signing key
 - enables content from anywhere
- Signature verification is either done by applications or at the network
 - applications choose what to trust

Privacy Point of View

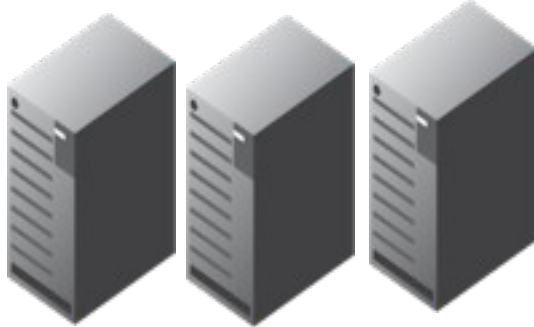
- Interests do not contain the consumer identification
 - What is the consumer identification in IP?
 - Enhances consumer privacy
- Name of requested data may be in plain-text
 - It may give away what we are looking for
- Privacy vs forwarding capability

The CDN model

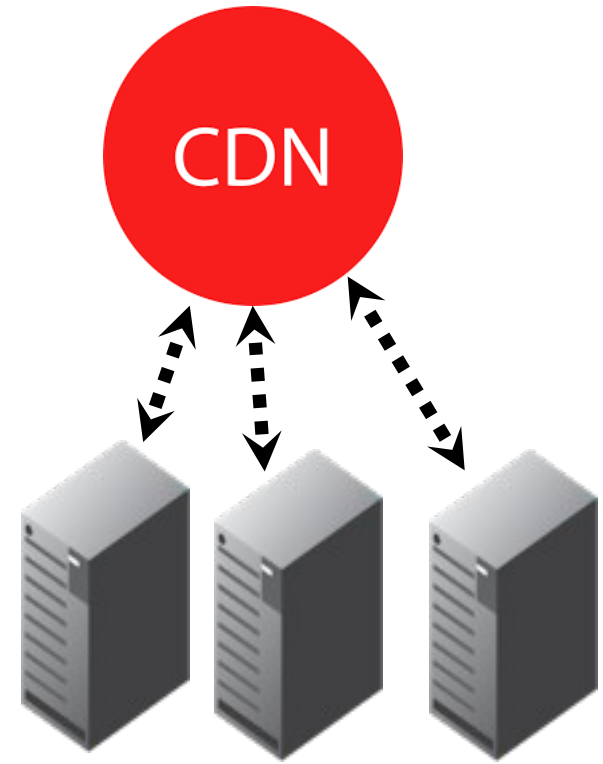
Single server model



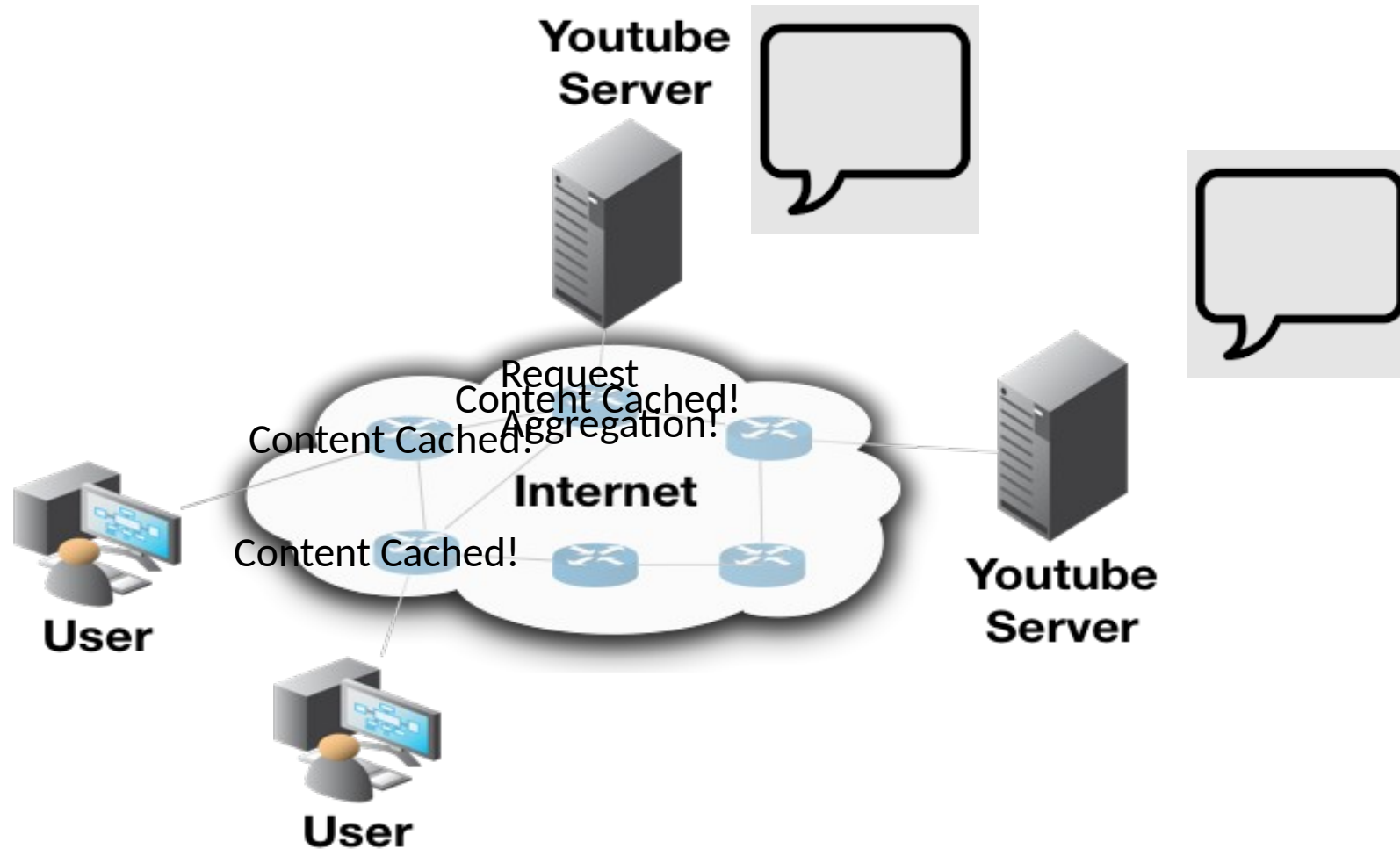
Multi-server model
(replicated content)



CDN model



NDN Communication Model Example



IP vs NDN

IP	NDN
Identifies end-hosts (IP addresses)	Identifies data by name
Stateless forwarding	Stateful forwarding
Packet delivery to destination	Request/Response data model
Secure connection	Data-centric security

Conclusion

- NDN is based on content
 - Name it
 - Secure it
 - Forward it
- Better or worse?