

Information Centric Networking and Internet of Things

Sridhar

Agenda

Host centric networking vs Information Centric Networking

Why ICN with IoT

Design Challenges

Naming

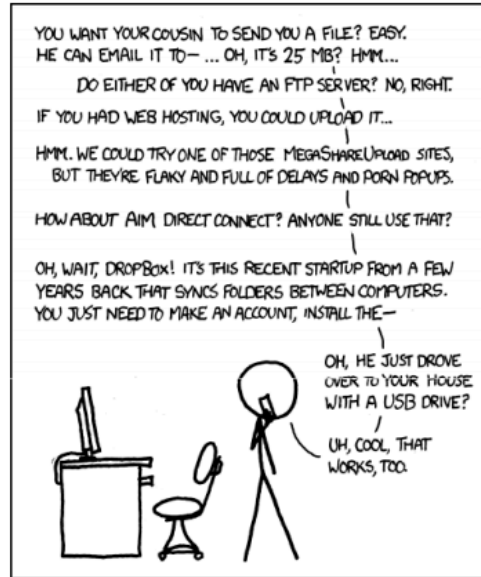
Caching

Routing

Security

....

What is the talk all about



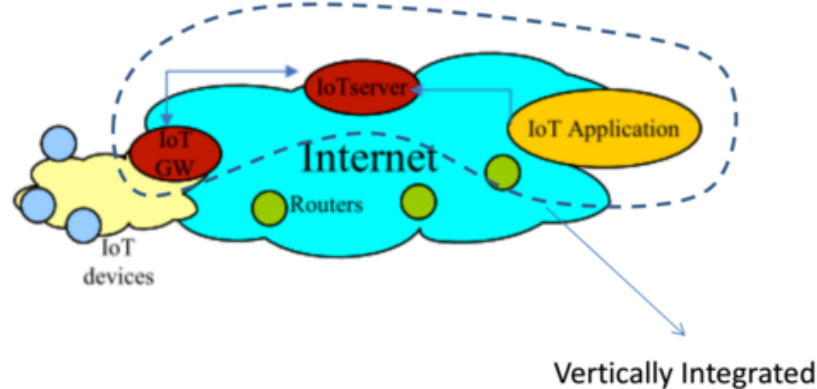
I LIKE HOW WE'VE HAD THE INTERNET FOR DECADES,
YET "SENDING FILES" IS SOMETHING EARLY
ADOPTERS ARE STILL FIGURING OUT HOW TO DO.

Evolution of IoT: Legacy IoT systems

Silo IoT Architecture: (Fragmented, Proprietary), e.g. DF-1, MelsecNet, Honeywell SDS, BACnet, etc.

A small set of pre-designated applications.

Moving towards Internet based service connectivity (ETSI One M2M Standards).

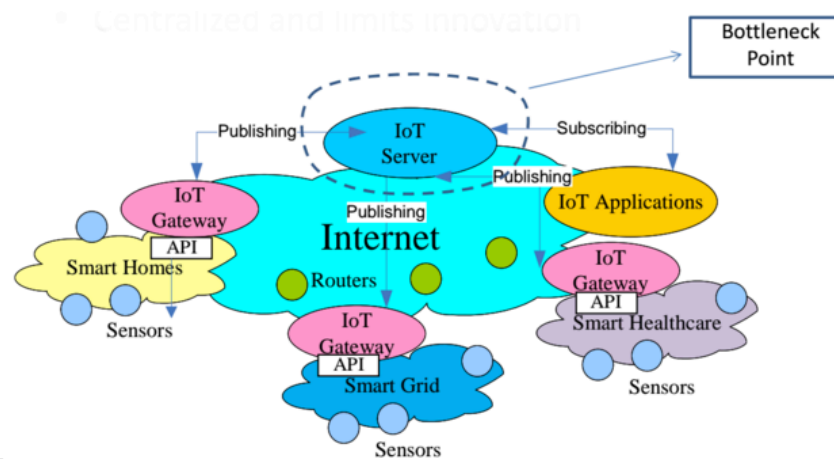


Evolution of IoT: State of the art

Internet Overlay Based Unified IoT Solutions, inter-connecting multiple publishers and consumers

Coupled control/data functions

Centralized and lin



Limitations with host-centric networks

Caching -

- possible only in a few nodes near server/client

- even that is not possible if SSL is used

Guarantees are only host based - not content based.

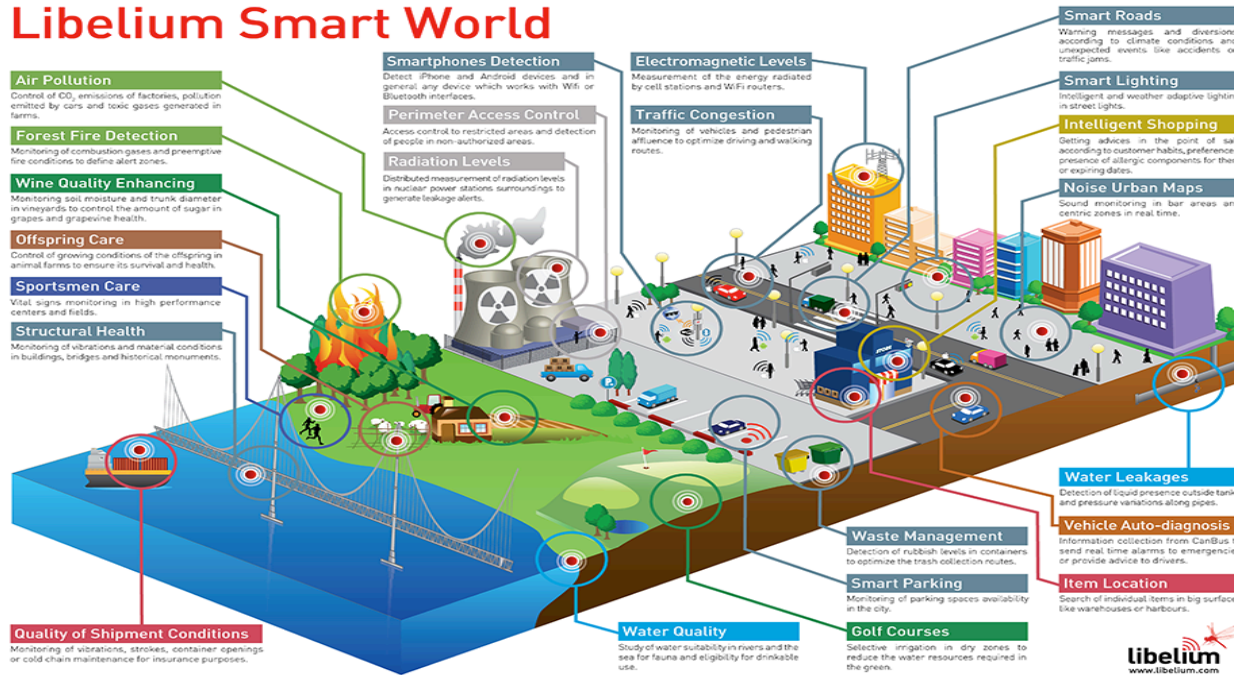
Easier for applications to discover and use data.

No inherent support for mobility

Resources are always coupled with IP addresses

Data matters, not the supplier

Libelium Smart World



To get sensor information:

Send a request to
a.b.c.d/8 (holder of
information)

vs

Get location/
sensor_data

Information Centric Networking

What if networking takes place based on content instead of hosts?

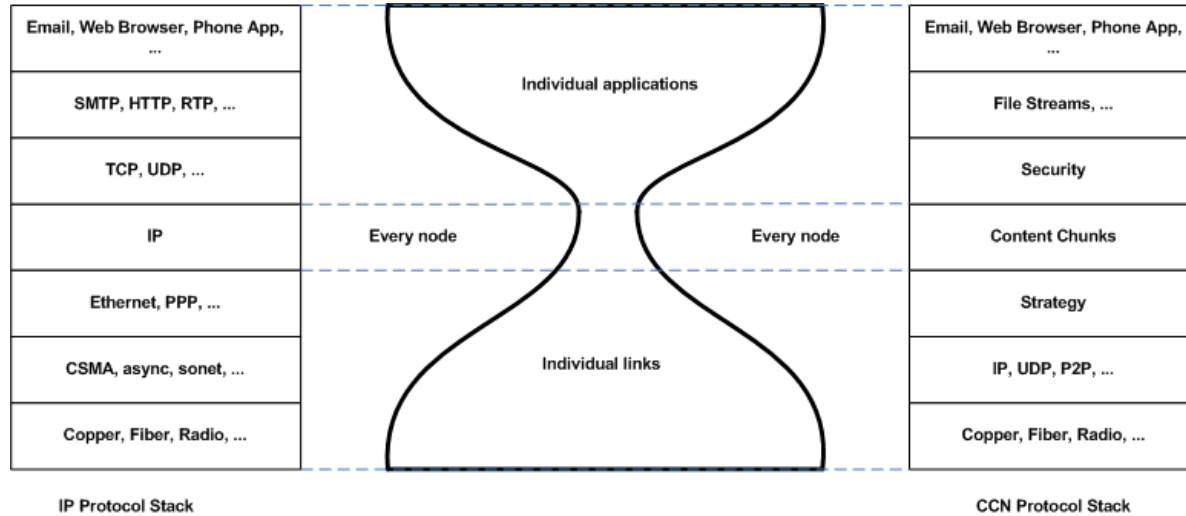
Content can be collected from the network, processed in the network, and stored in the network

Goal is to provide a network infrastructure capable of providing services better suited to today's application requirements:

- content distribution & mobility

- more resilience to disruption and failures

ICN Stack



Change of network abstraction from “named host” to “named content”

Security built-in: secures content and not the hosts

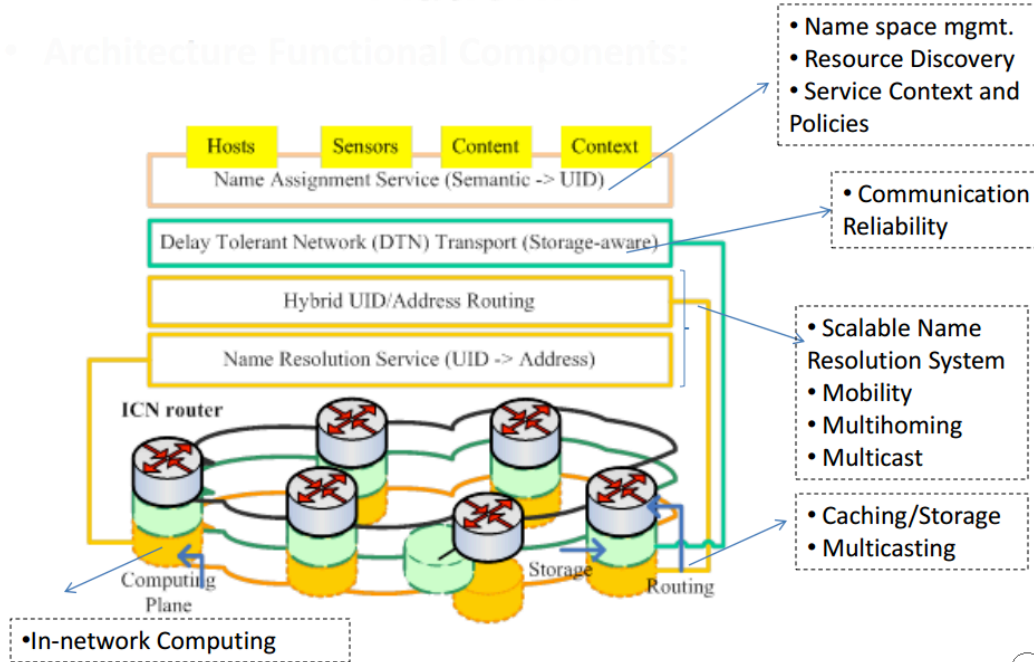
Mobility is present by design

Can handle static as well as dynamic content

ICN Platform for IoT

Platform

Architecture Functional Components:



Dissemination networking

Data is requested by name.

Anything which has valid information can respond.

Data is secured, but not necessarily the communication channels

REQ <http://nytimes.com/today> -->

<-- RESP <http://nytimes.com/today>
<http://nytimes.com/20060330/index.html>

Named, DataId

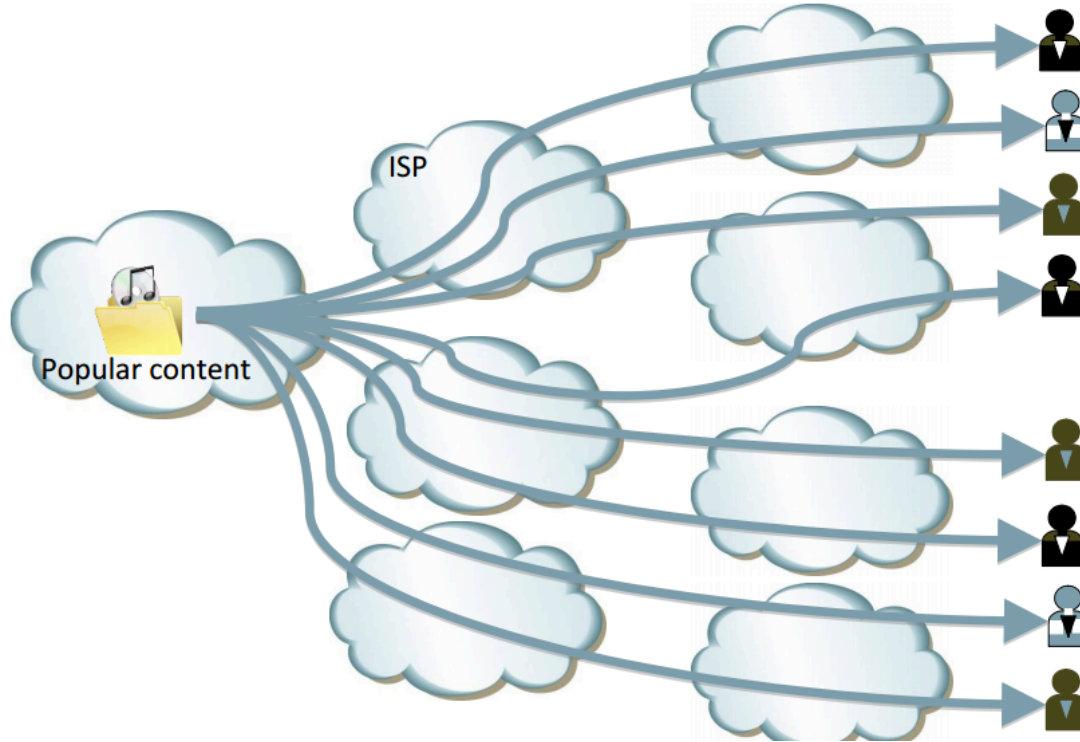
<html>...</html>

Communication

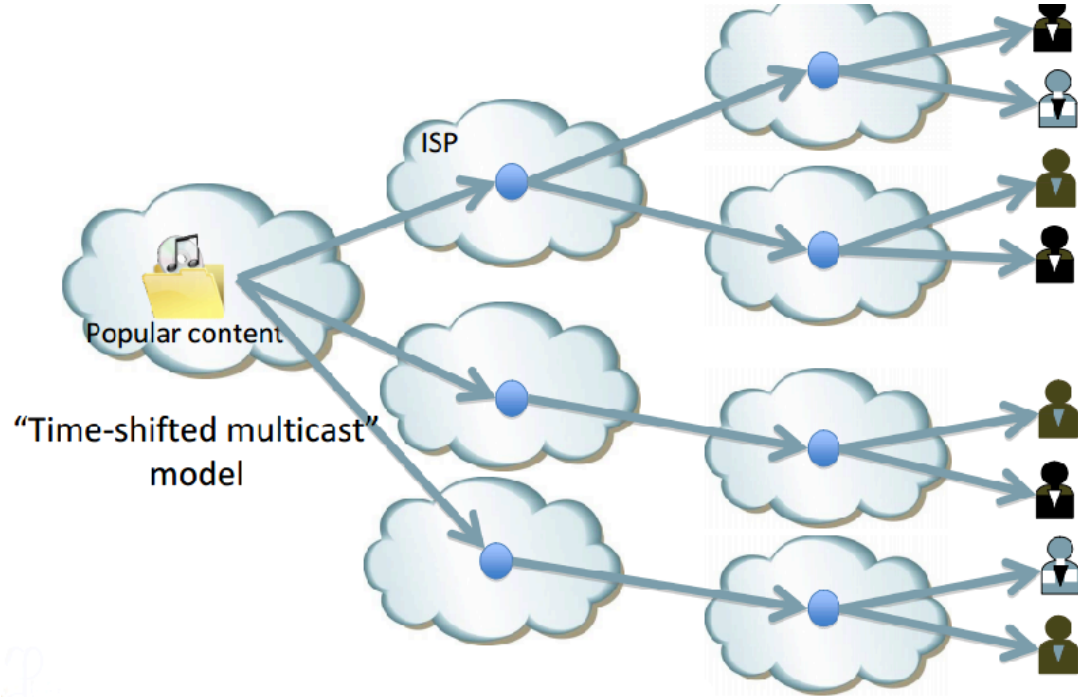
User communicates intent to the network so that the network can do more on behalf of the user

Network transactions in the form of content and not conversations. So, popular content won't congest network

Flash Crowd Effect due to content popularity



Scalable Cache based content distribution



Evolution of Networking

Traditional networking

Host-centric communications addressing end-points

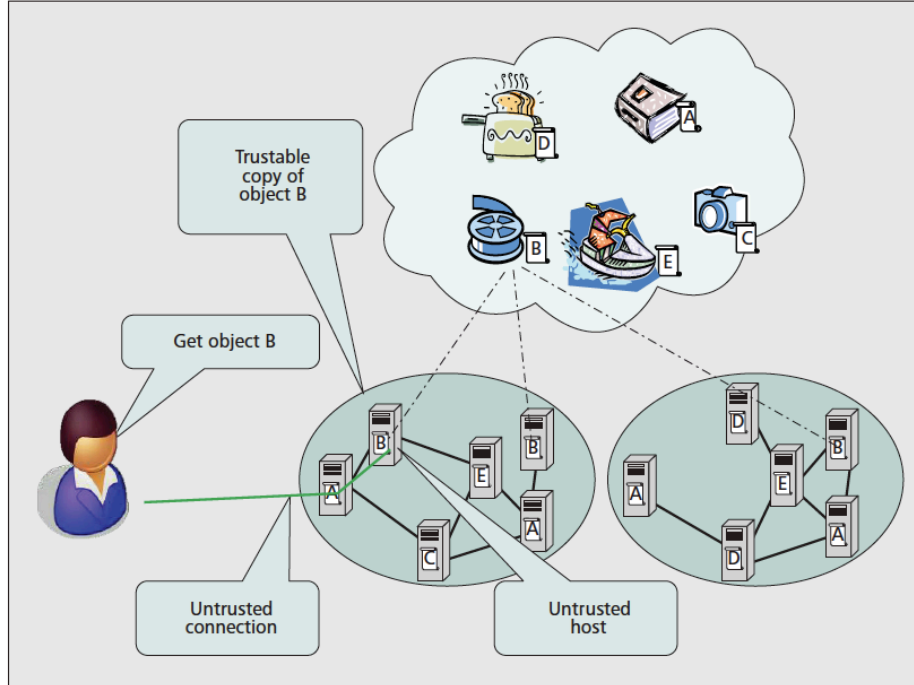
Information-centric networking

Data-centric communications addressing information (e.g., data in context).

Decoupling in space – neither sender nor receiver need to know their partner.

Decoupling in time – “answer” not necessarily directly triggered by “question”, asynchronous communication.

ICN Communication model



From a networking perspective, these objects can be viewed as named data chunks without semantics, but some ICN designs have an information abstraction model including multiple representations, i.e., unique bit patterns, for the same object.

Figure 1. ICN communication model: client side.

Why ICN in IoT?

Ability to name data independently from the location in which it is stored.

Distributed Caching

Decoupling sender and receiver - Disconnected modes of operation

Reduce bandwidth consumption

Mobility

Authentication and verification of content

Design Challenges of IoT over ICN

Naming and Name resolution

Caching/Storage

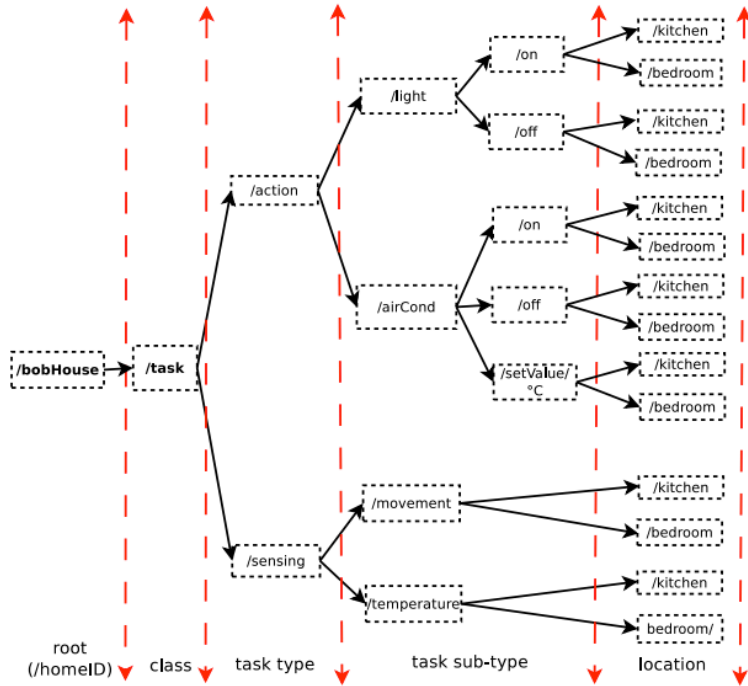
Routing and Forwarding

Contextual Communication

In-network computing

Security and Privacy

Naming and Name resolution



Naming in a smart home

Naming and Name resolution

Request for objects contain name of the object

Name can be resolved to some kind of locator where object is found
(2-step)

The request can be forwarded by name

Hierarchical names

Structured Flat names

Unstructured Flat names

Naming and Name resolution

Naming of devices - Why is it needed?

Size of the data/name - Is the size of the name larger than data?

Should the names be human readable or can it include cryptographic parts?

How to solve scalability issues?

Establishing trust

Flexibility - Dynamic publishing

Latency

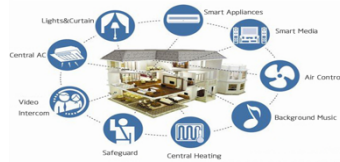
Control and Scoping

Naming requirements in common IoT applications

Smart Homes -

Local and wide area interactions

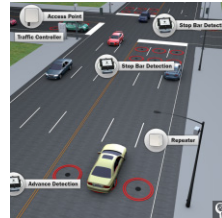
Security and privacy



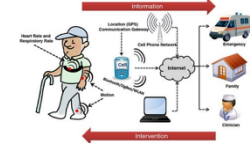
Smart Grid -

Real-time Control

Security



Telemedicine



Smart Transportation

Extreme mobility



Distributed Caching

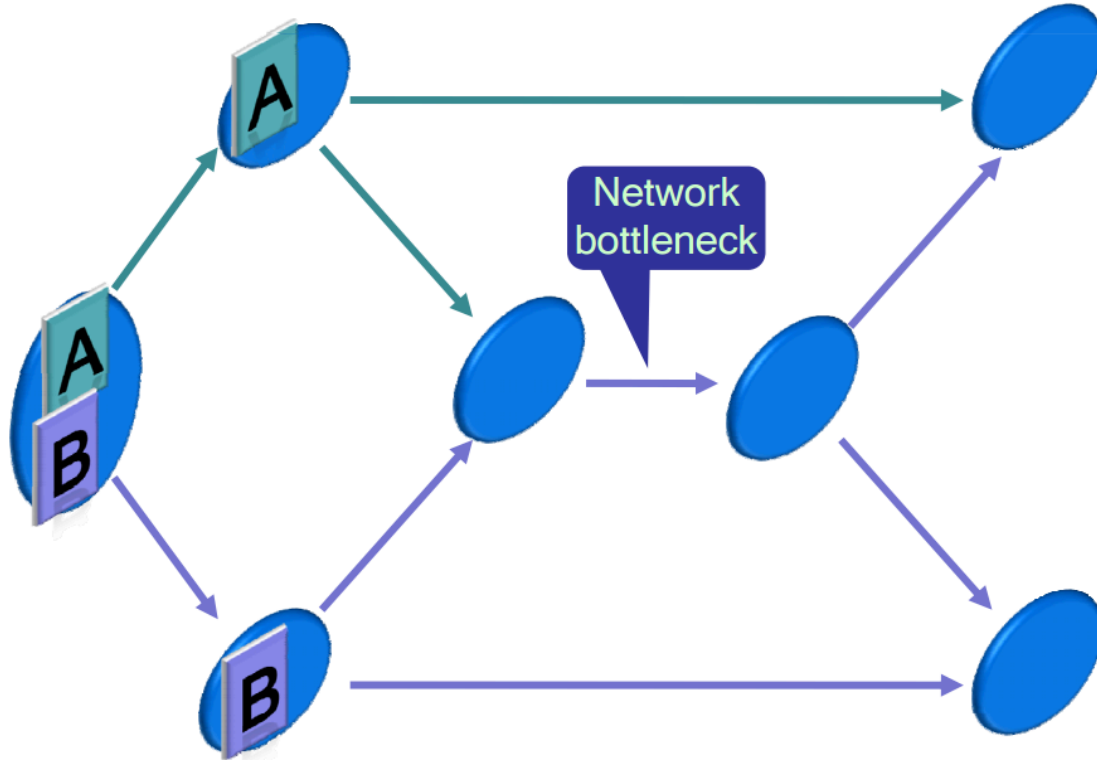
When is caching useful?

Which nodes should cache data?

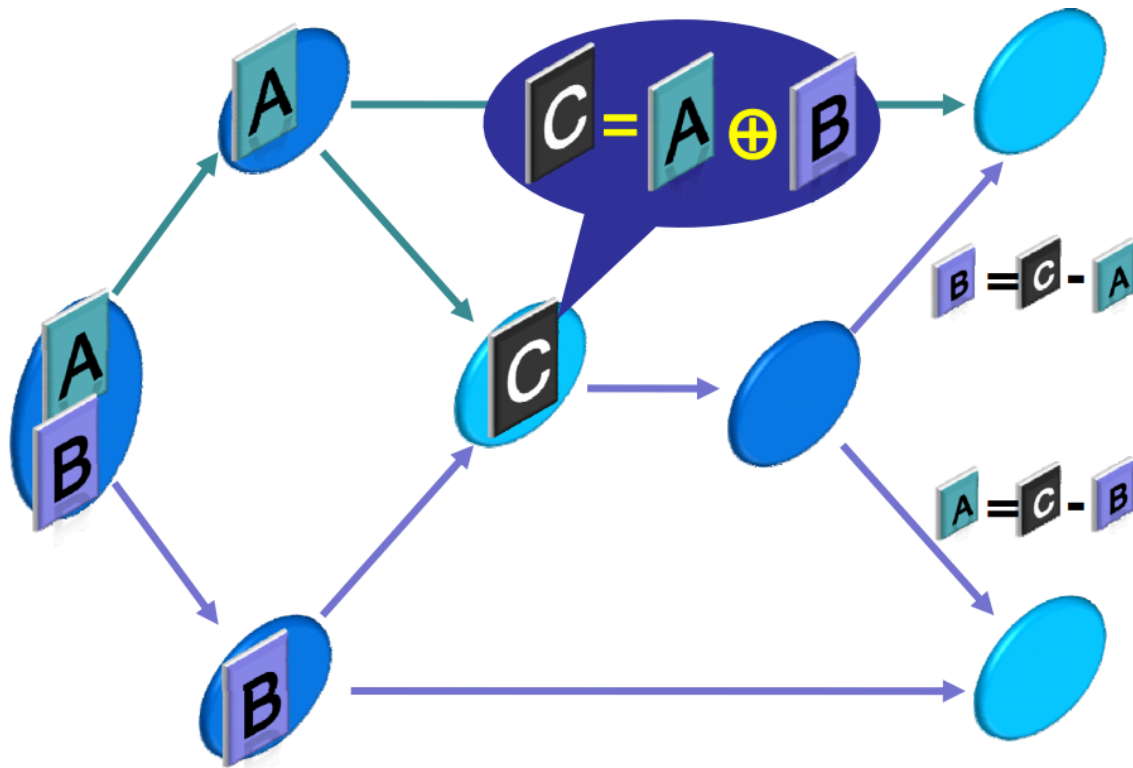
What to cache?

Context sensitivity

Network Coding



Network Coding



Routing and Forwarding

Direct Name based routing - Packets forwarded by name of the data

Indirect routing - Packets forwarded based on locator of destination node
obtained by name resolution

DHT Style

DNS Style

Cost of mobility - Static vs Dynamic binding

Other Issues

Security Considerations - Object Security

What about man in the middle attacks?

Receiving trusted content from multiple caches

Enabling application layer processing in untrusted intermediaries

Energy efficiency of cryptographic mechanisms