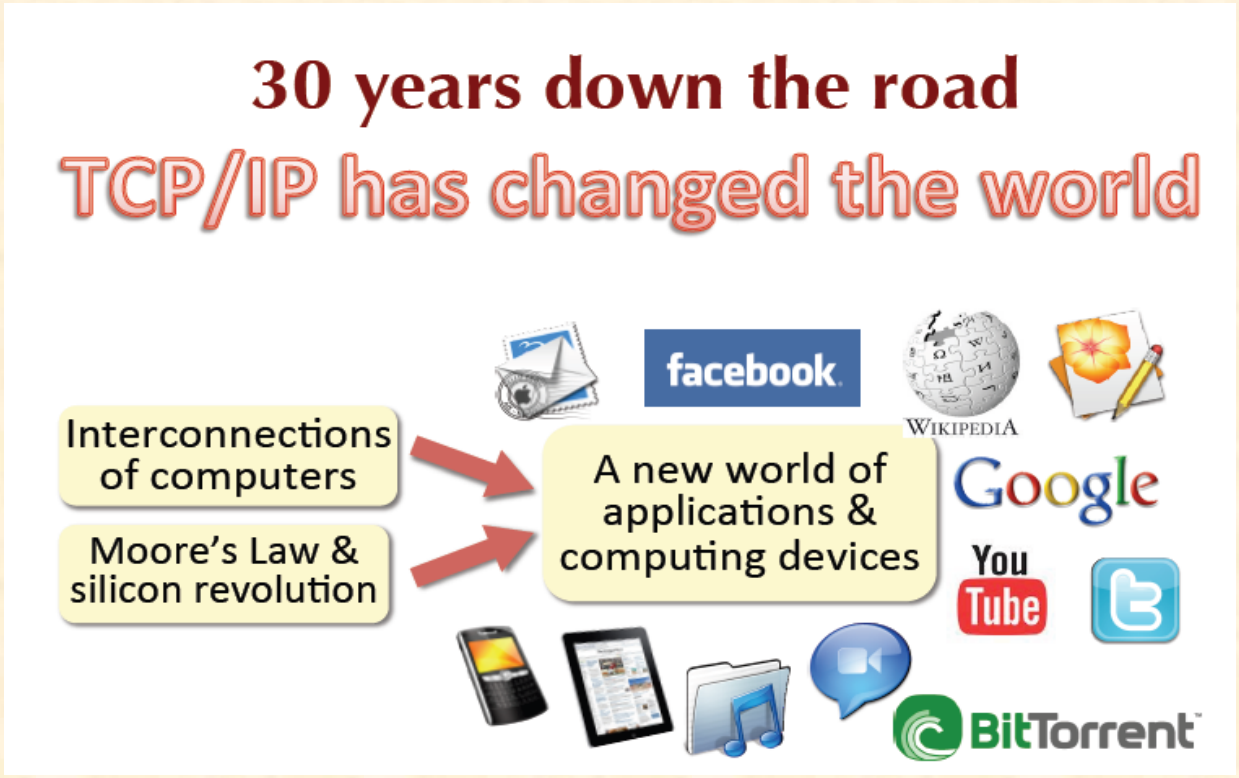
NAMED DATA NETWORKING (NDN)

BRIEF HISTORY

- When the Networking was developed in the 60s and 70s
  - Networking was mainly used for resource sharing.
  - IP was the effective communication protocol in place.
- TCP/IP was built to solve the issues that arose with telephony.
- TCP/IP was created to allow two machines have a pt to pt conversation
- It was created for a few systems, multiple users per machine, immobile and wired networks

TODAY



Many machines per user, mobile, wireless networks, vast amount of data to be sent

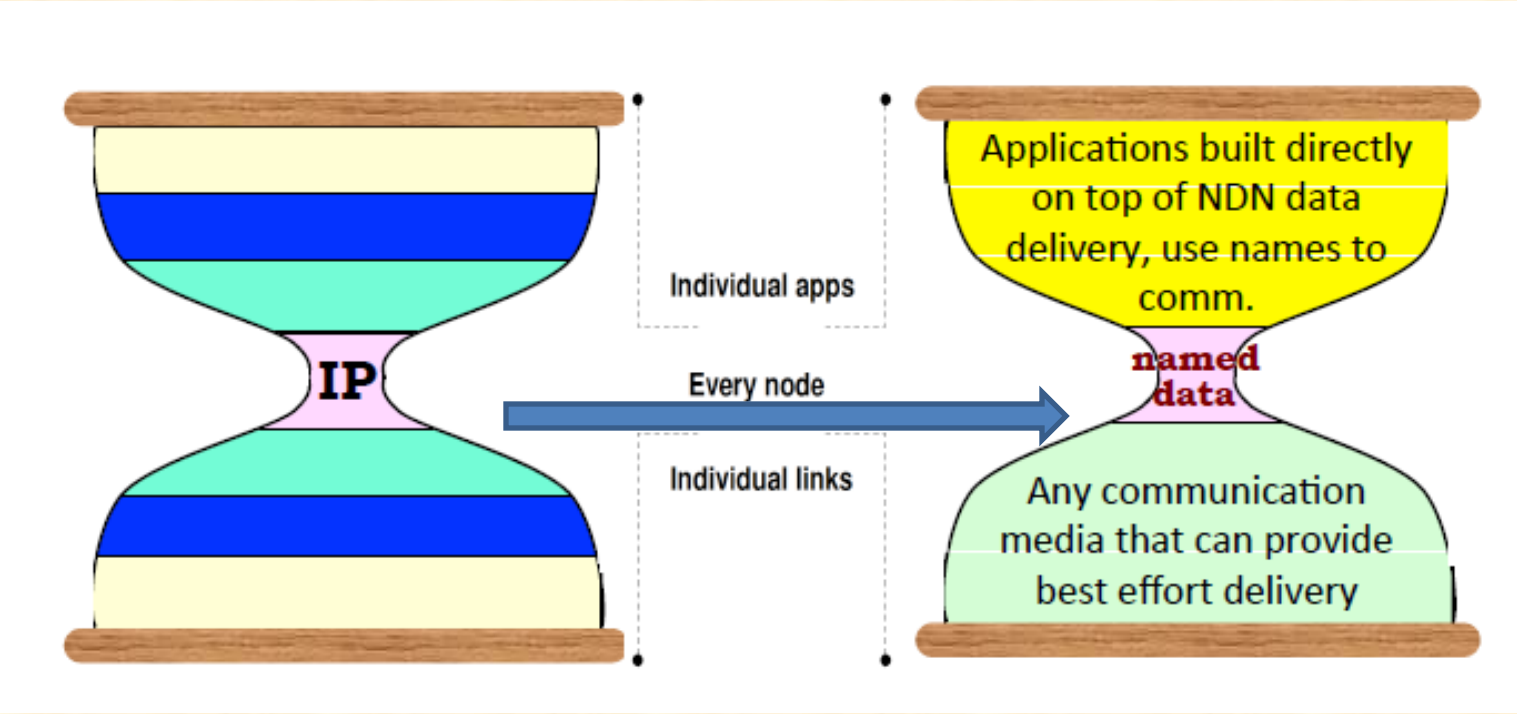
Issues of Today's IP Networks

- IP was not created for content distribution
  - Inefficient networking
- Massive scale of data dissemination
- Computing devices becoming increasingly mobile
- Internet of Things
- Robust data delivery
- Network security is an afterthought
  - IP identifies interfaces, networks
  - Current solution: Securing the channel, the box and using firewall

What is NDN?

- Named Data Networking
- Also known as Content-Centric Networking (CCN) or Information-Centric Networking (ICN)
- Next Generation Internet Architecture
- Changes the focus of data transmissions **from “where” to “what”**
- Data Delivery is done using **Data names (what)** Instead of **IP addresses (where)**
  - **Applications use names**
- Preserves the design and decisions that make TCP/IP robust and scalable

Named-Data Networking

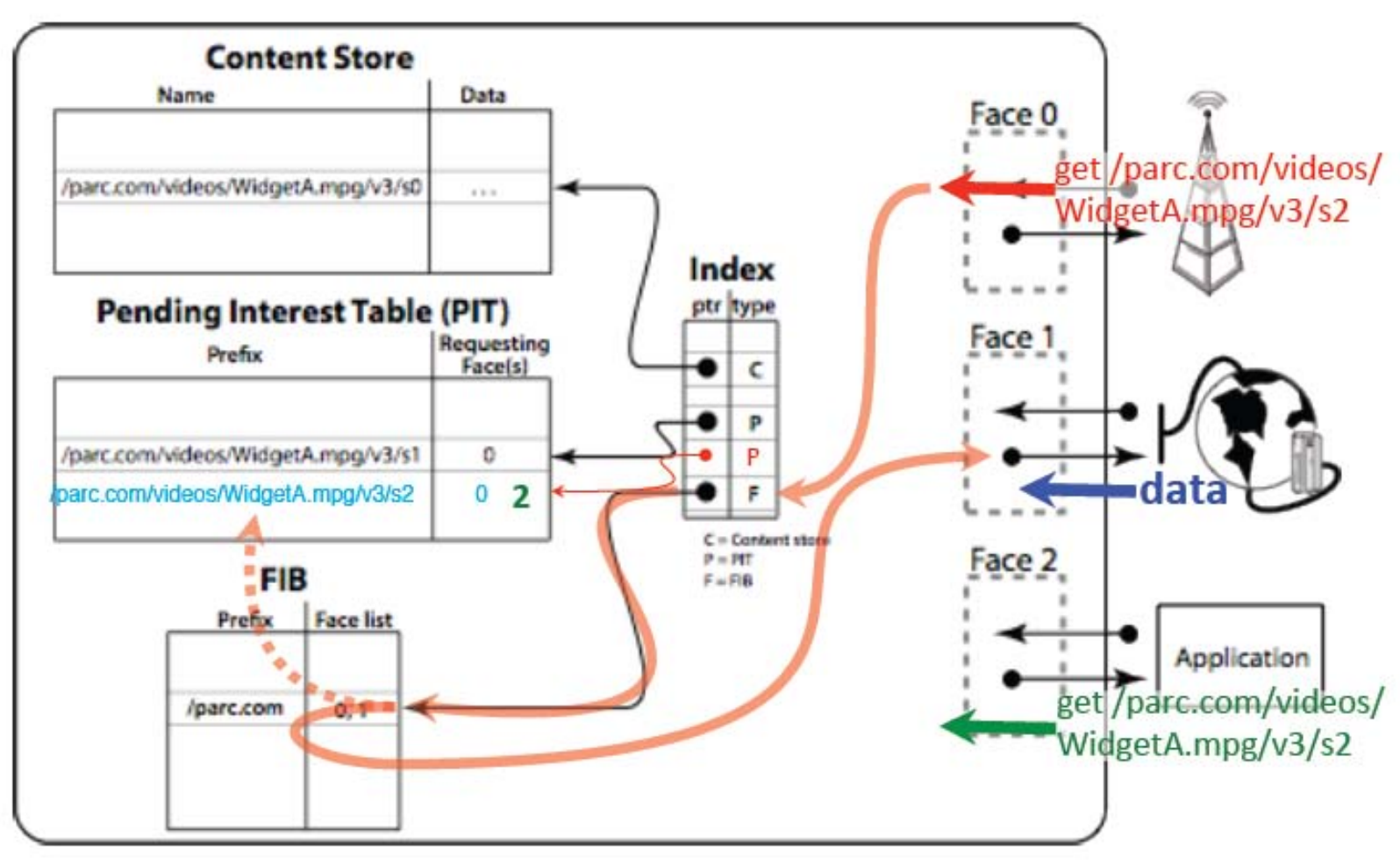


- Moving the universal component in Internet protocol stack from IP packets to named data
- Content-Centric Networking (CCN)

NDN Advantages

- Content distribution
  - Application-friendly communications and naming
- Solves today's communication issues
  - Scalable and more efficient than TCP/IP
- Built-in security
- Easier configurations
- Built-in multicast delivery
- Supports multi-path routing, load balancing, service prevention and discourages the formation of loops
- Easy mobility and broadcast

The NDN architecture

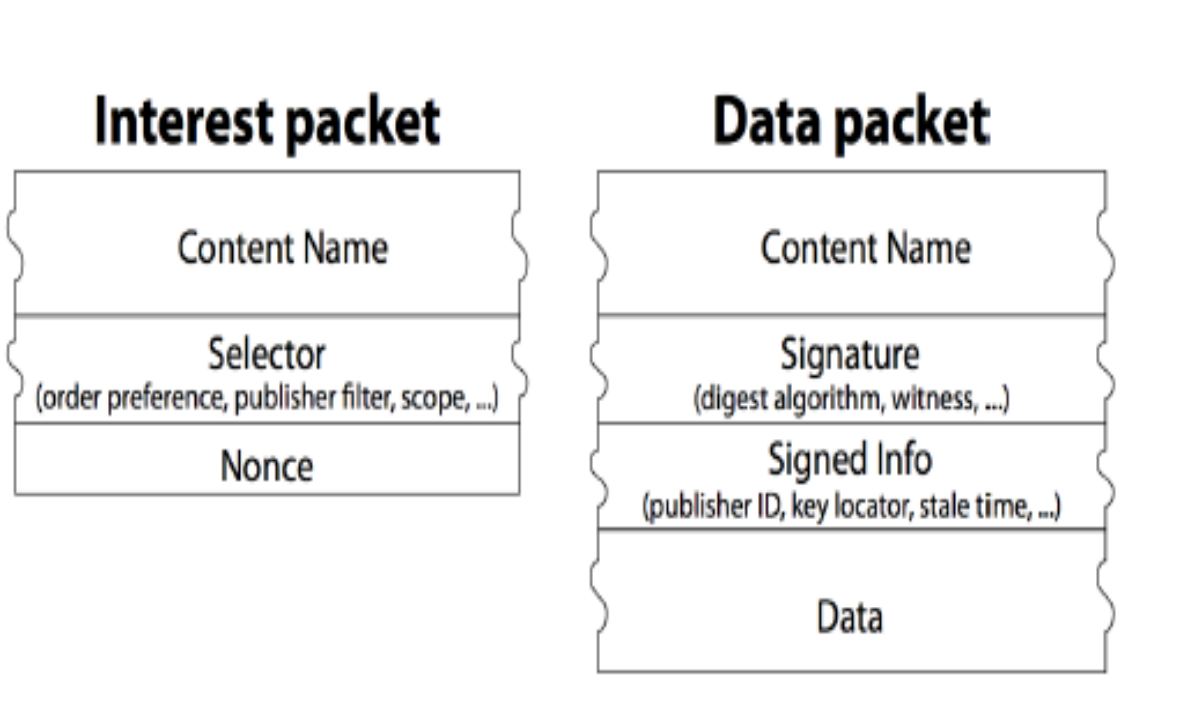


Some details

- Routers do component-wise longest prefix match of the Content Name from a packet against the FIB
  - Content is “reused” after forwarding which is contrast to IP data forwarding
- Cache management and replacement is subject to ISP policies
- The naming system is still under active research; how to define and allocate top level names remains an open challenge

Forwarding Process

- Exchange of Data is consumer controlled
- Two types of Packets



NDN Overview

- Every NDN router contains three major components:
  - Forwarding Information Base (FIB)

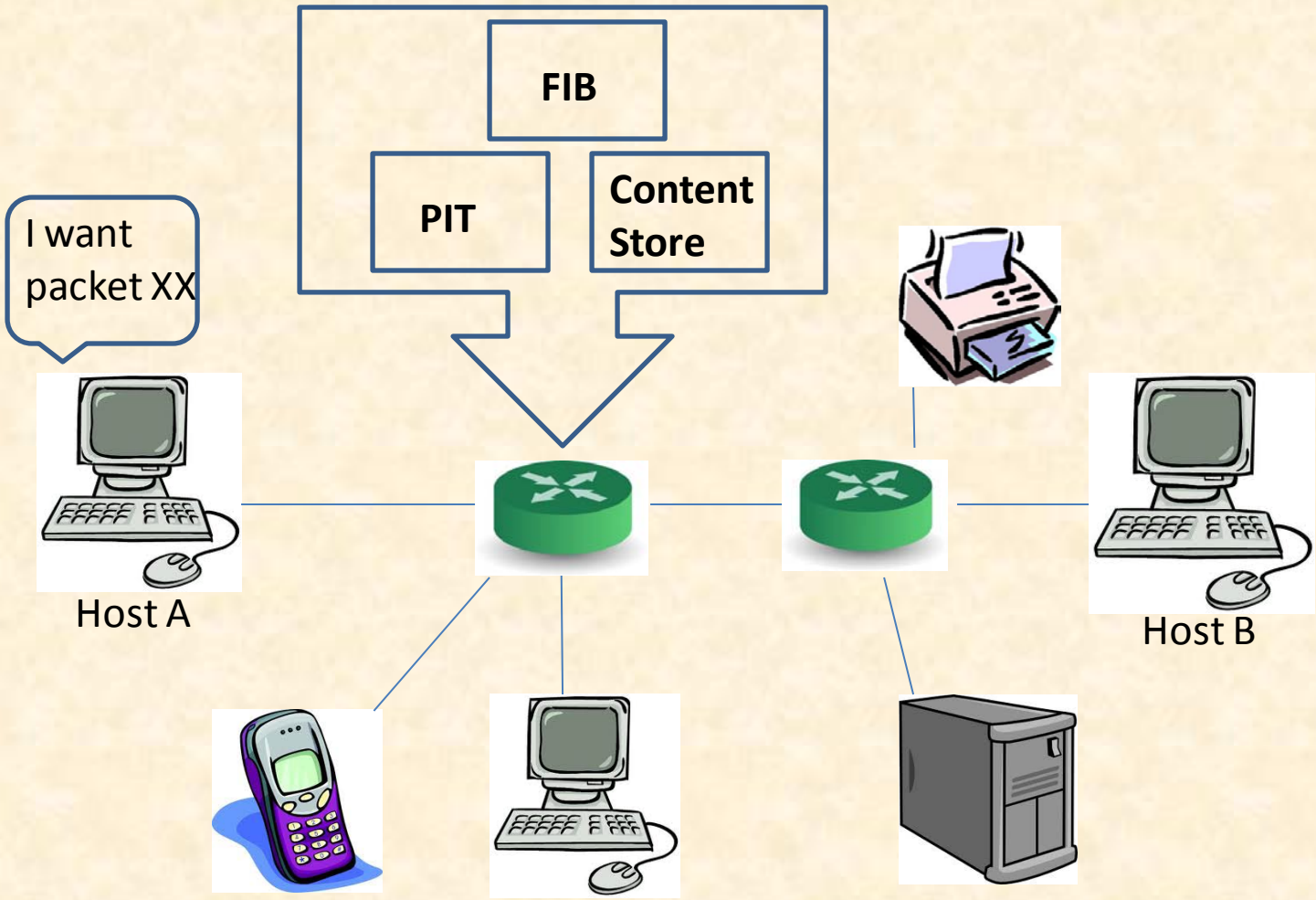
    Forwards interest towards potential sources of matching data
  - Pending Interest Table(PIT)

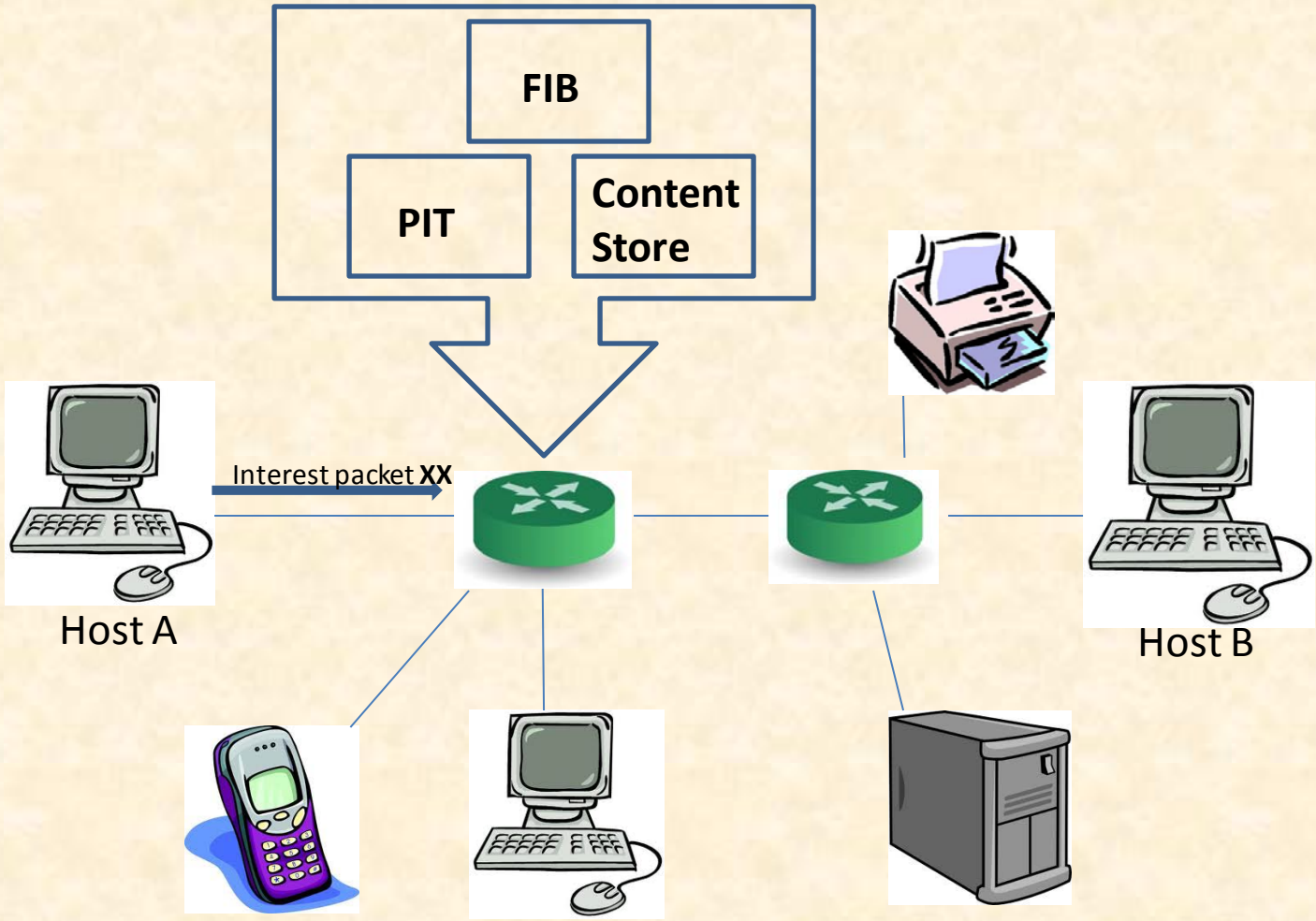
    Keeps tracks off interests sent upstream
  - Content Store

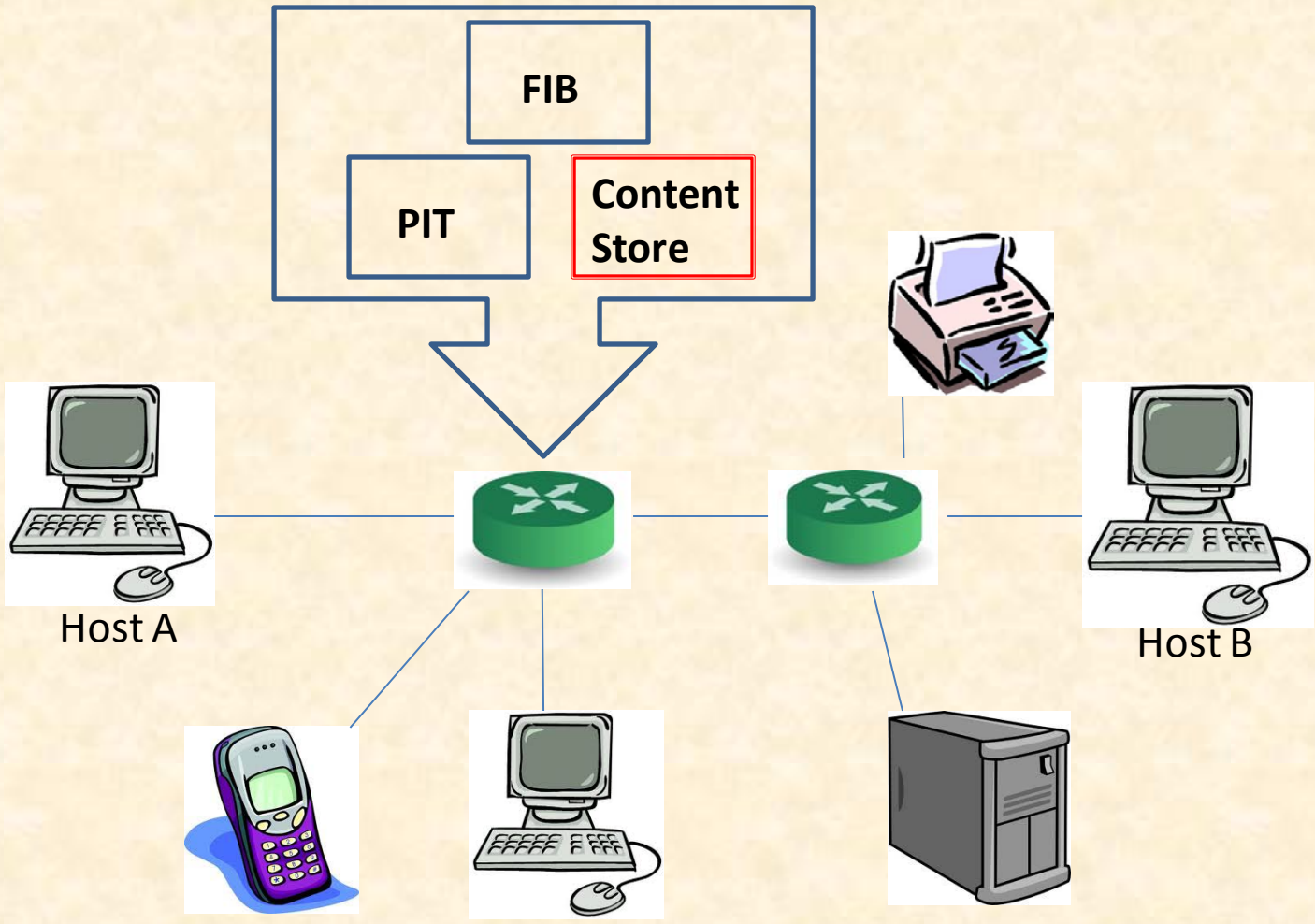
    Acts just like an IP buffer memory but with a longer keep period.

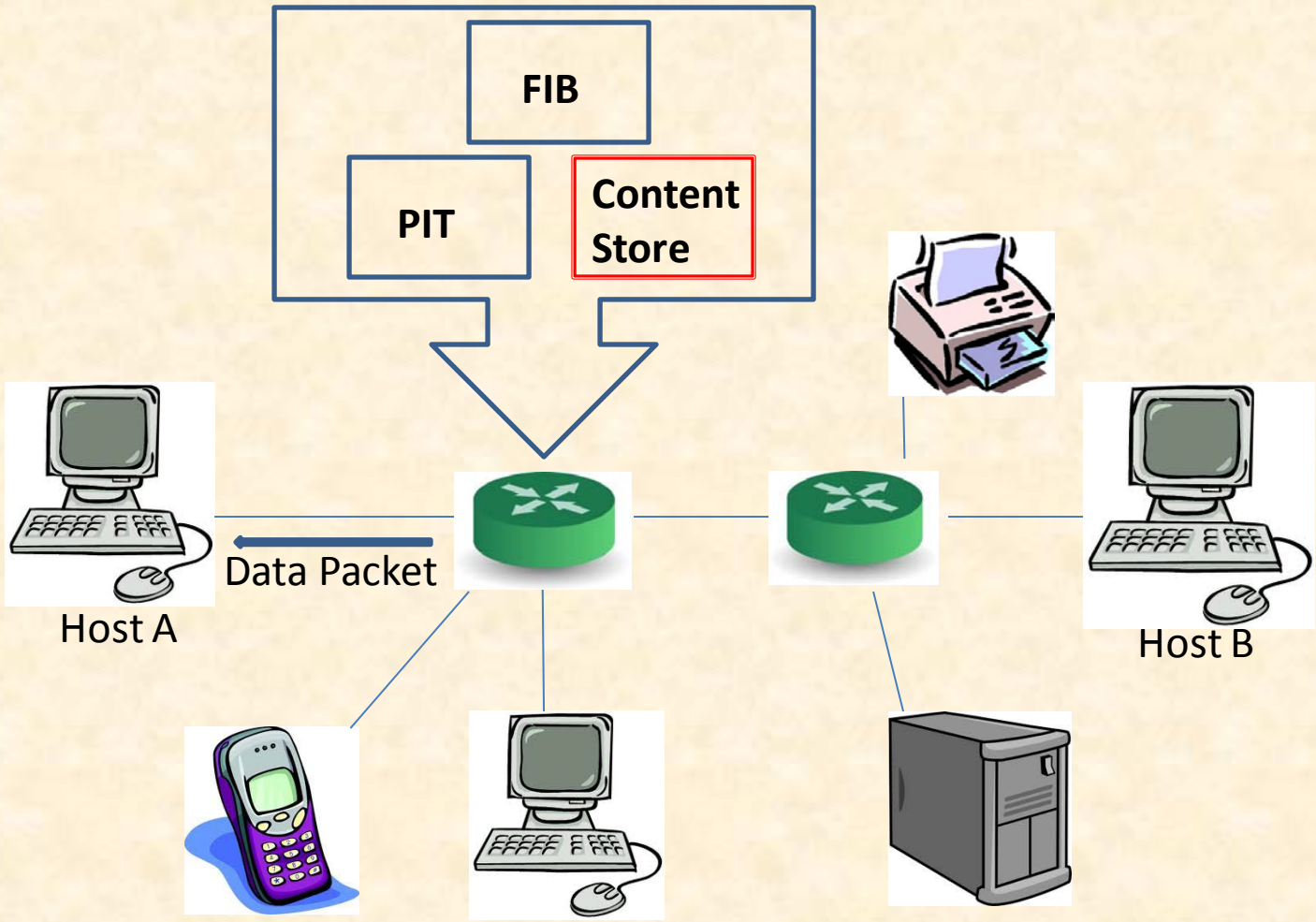
MODEL

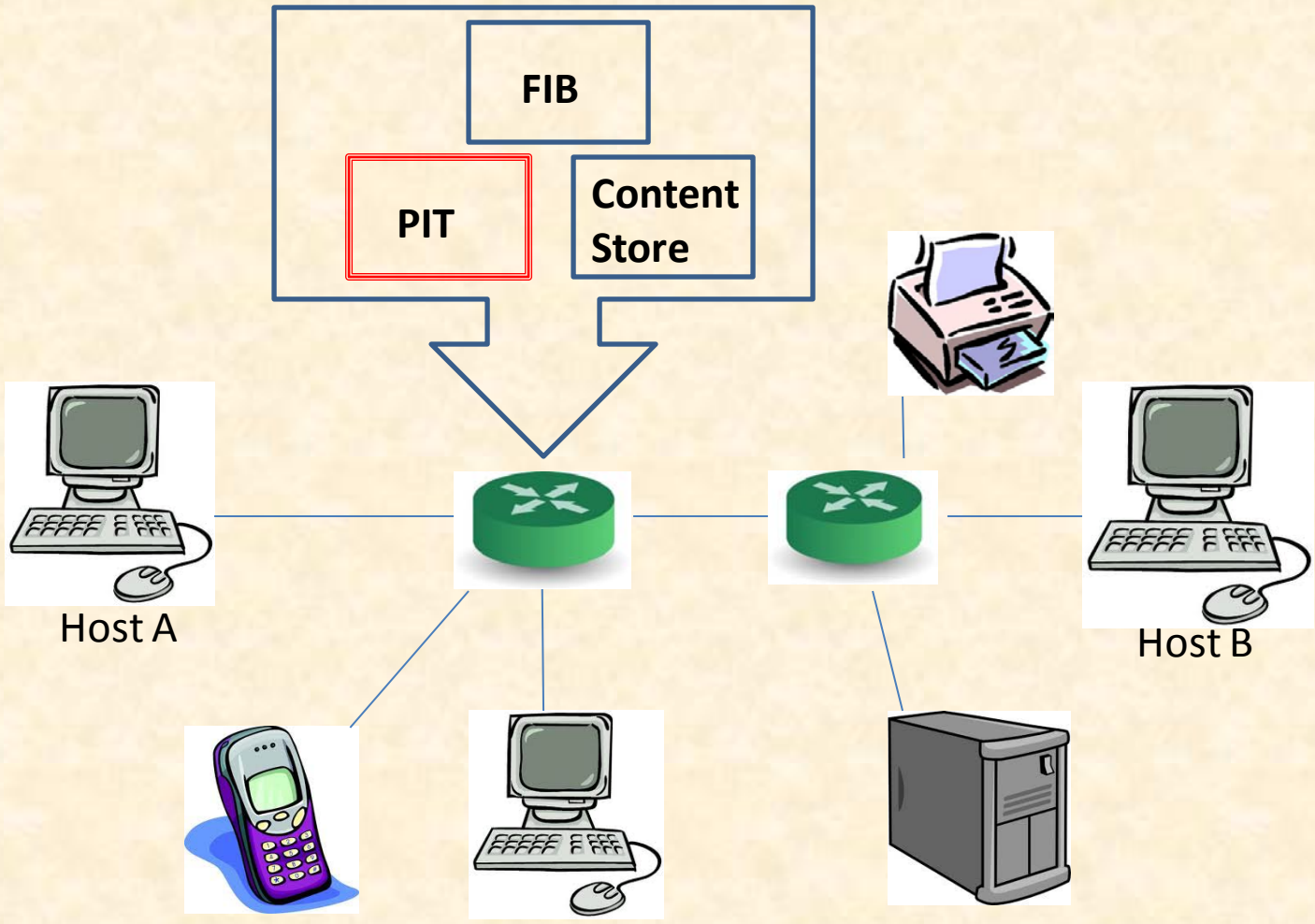
- Consumer sends out an Interest packet
- Any Node that has the Requested data sends a Data packet back
- Data Packets traces the reverse path of the Interest Packet
- All packets are routed using names and not IP addresses
- Lookup is ordered so that a Content Store match is preferred over a PIT match which in turn is preferred over a FIB match.

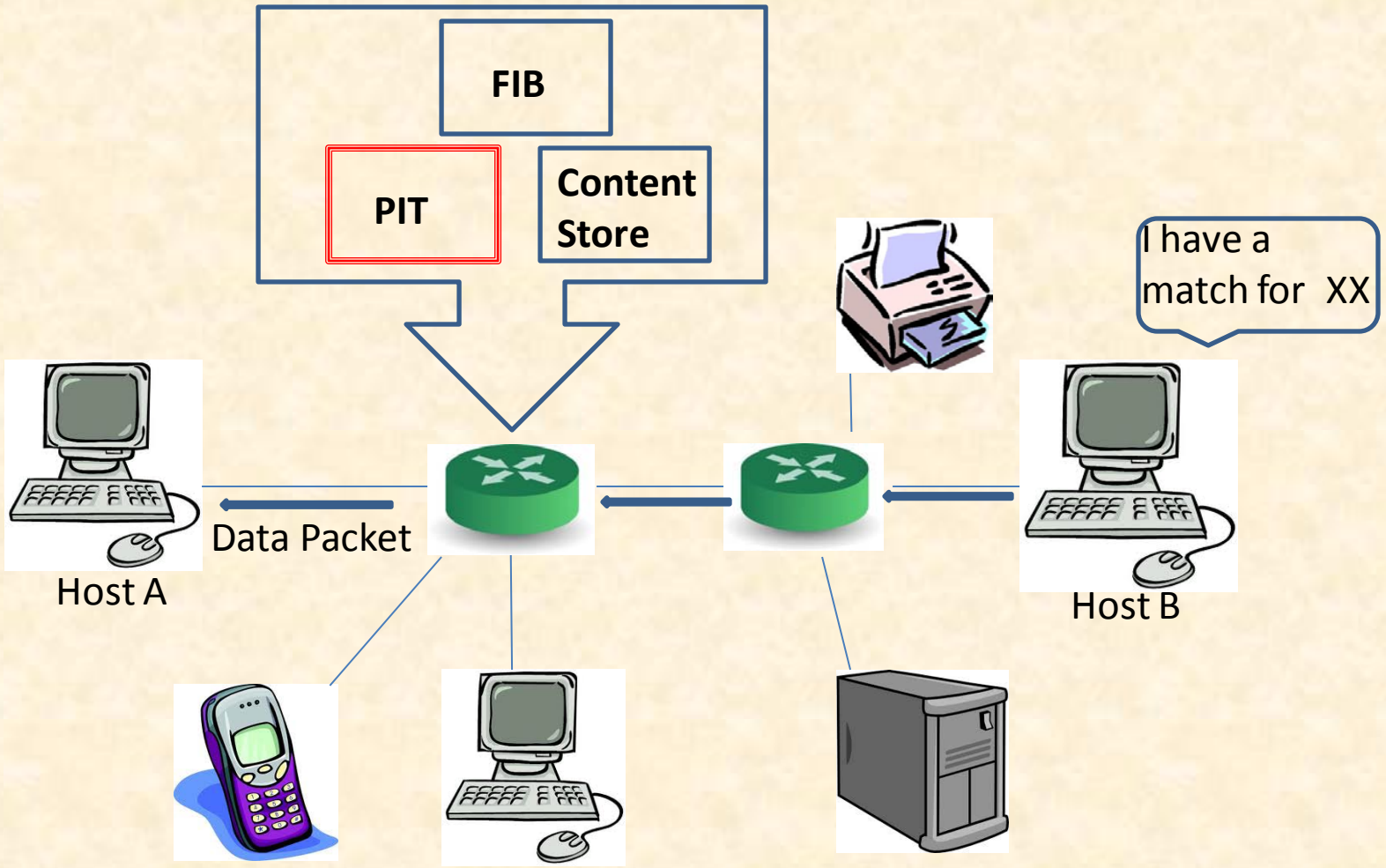

FIB
PIT
Content Store
I want packet XX
Host A
Host B

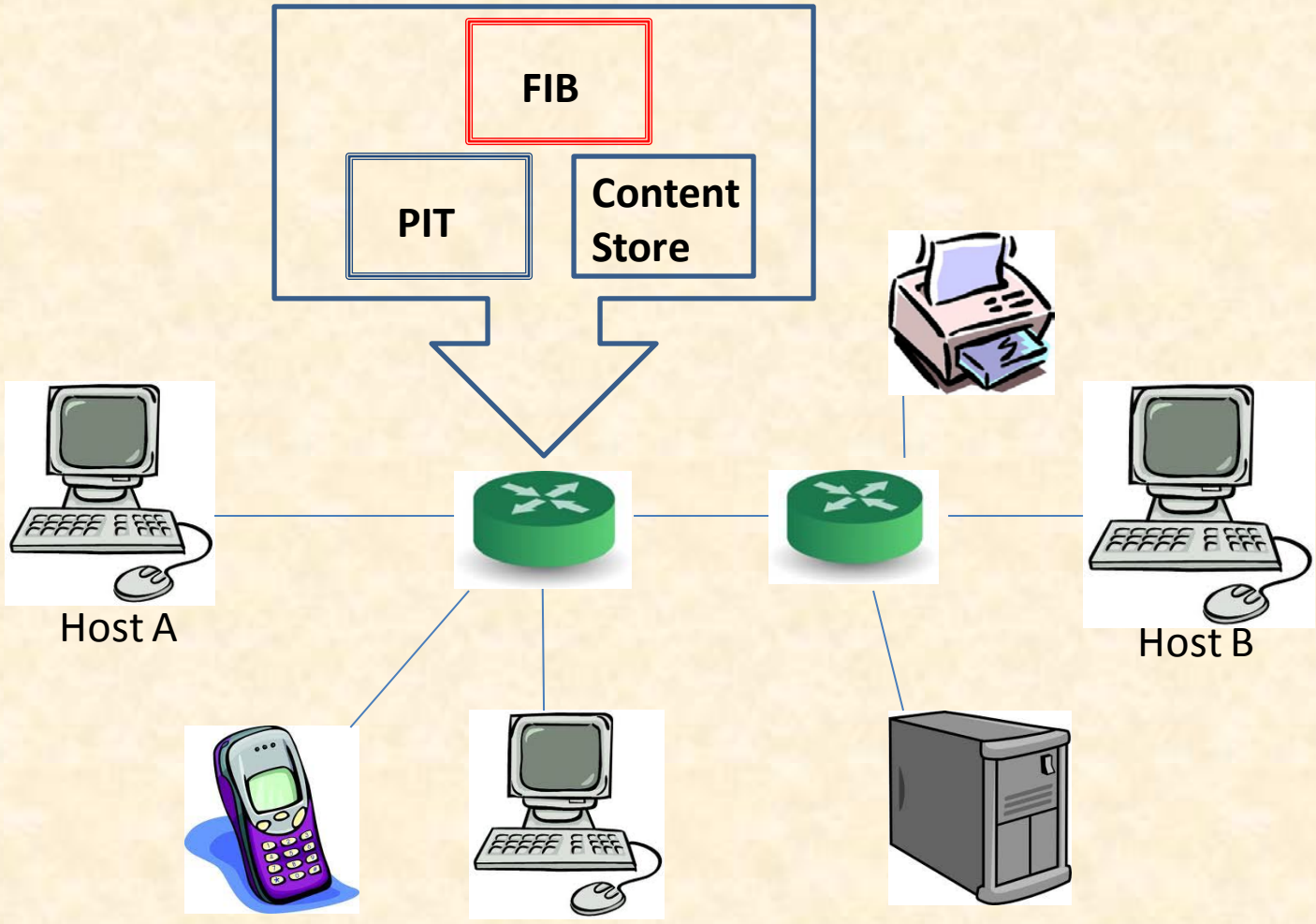

FIB
PIT
Content Store
Interest packet XX
Host A
Host B

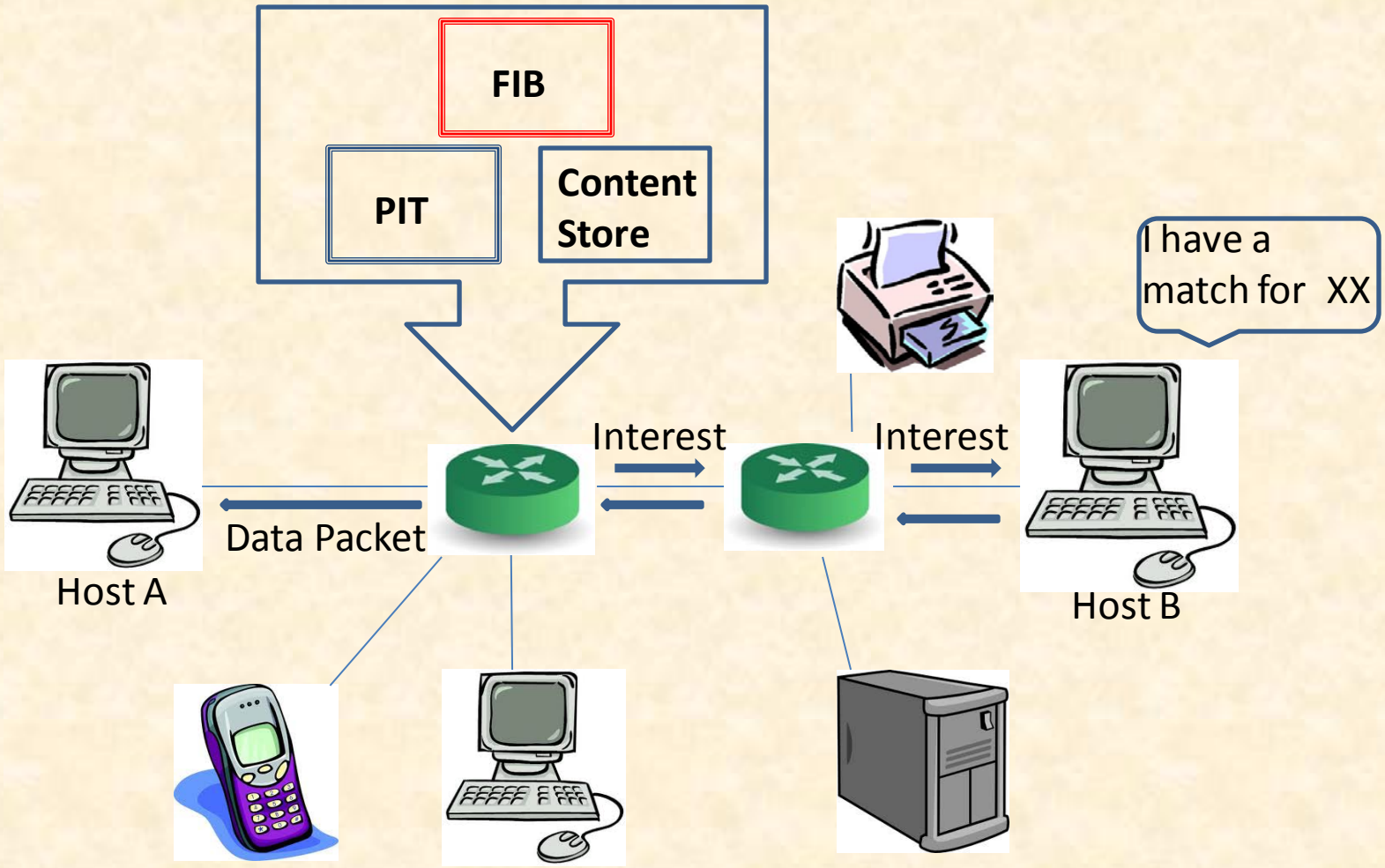

FIB
PIT
Content Store
Host A
Host B


FIB
PIT
Content Store
Data Packet
Host A
Host B


FIB
PIT
Content Store
Host A
Host B

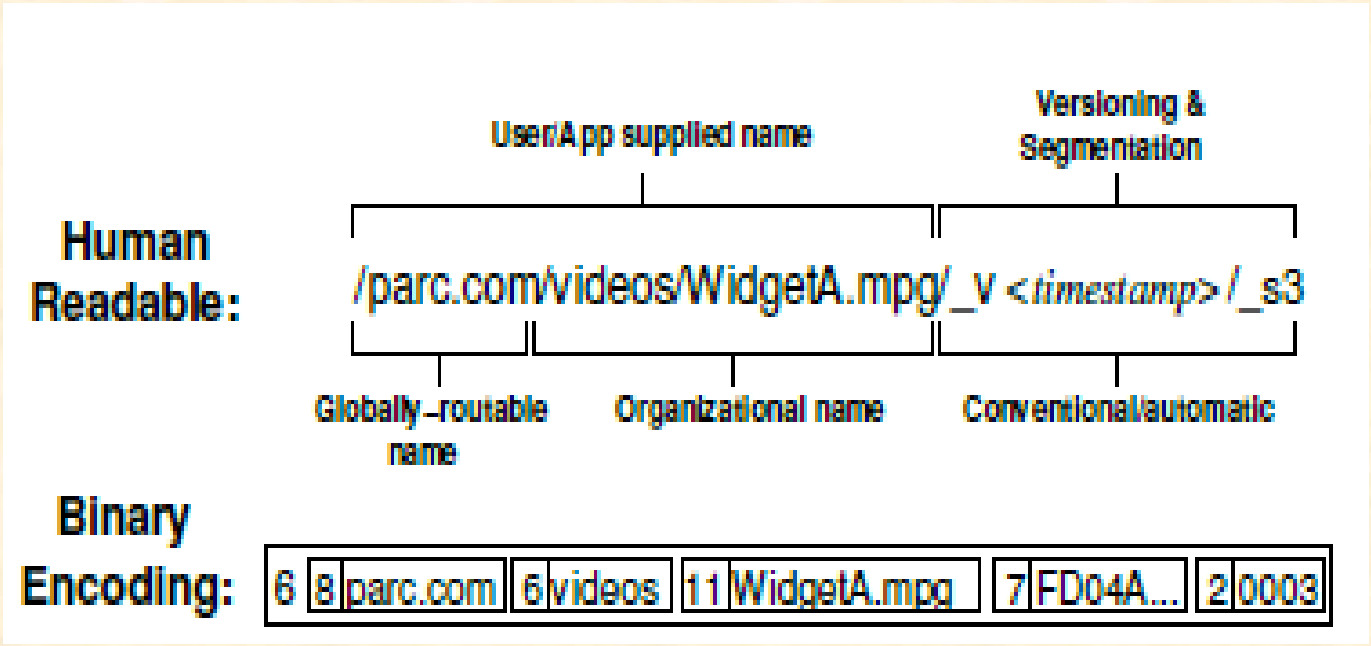

FIB
PIT
Content Store
I have a match for XX
Data Packet
Host A
Host B


FIB
PIT
Content Store
Host A
Host B


FIB
PIT
Content Store
I have a match for XX
Interest
Interest
Data Packet
Host A
Host B

Naming

- Most Important Piece in the Architecture and it is still under active research
- Hierarchically Structured Names
- Names do not need to be globally unique
- Data matches an interest if the content name in the interest packet is a prefix of the content name in the data packet
- The structure used is useful for applications to represent relationships between pieces of data



- Variable Length; usually longer than IP
- More efficient in using hashing techniques for name lookups
- Names are specific to applications and opaque to a network
- NDN supports both statically cached content and dynamically generated content like in today's web

Security

- Data gotten at the user can be validated instead of relying on the shaky trust of the data producer and the channel with which the data was forwarded as is done with IP today
- Data retrieved from a producer is said to be secure when the consumer is able to reliably assess three properties of each piece of information received which are:
  - Validity: is it a complete, uncorrupted copy of what the publisher sent
  - Provenance: is the publisher one the consumer is willing to trust to supply this data
  - Relevance: is this data an answer to the interest that was expressed.
- Authentication is done not on the content or the producer but the mapping between names and content

- Publisher digitally signs a mapping from his chosen name for a data to the data itself,
- Example: a producer P will say “N” is my name for content “C”
- That content will be made available to users in the network as a mapping triple: $M_{(N;P;C)} = (N;C;Sign_P(N;C))$.
- A user can then usefully send an interest for an arbitrary name N, and authenticate both the resulting content and its relationship with N, without having to know the source of the data

The user must be able to retrieve not just C but also the authenticator $Sign_P(N;C)$ and sufficient information regarding what public key to use in validating $Sign_P(N;C)$ and where to find a copy of the key if it isn't already in their possession

-The producer either included the key in the data

- Or a pointer to where the key can be found

Routing security is greatly improved

Multipath routing mitigates prefix hijacking

Since NDN messages focuses on data and cannot be addressed to hosts it makes to difficult to send malicious packets to a particular target.

Applying NDN

- NDN can be mapped over most existing internet applications while preserving security, interoperability and performance e.g. VoIP
- Application-specific middleware is not needed in NDN
- NDN model is designed to be compatible with today's internet; It is a universal overlay.
- The core IP routing protocols, BGP, ISIS and OSPF can be used as-is to deploy NDN

CONCLUSION

- Palo Alto Research Center (PARC) heads the research on NDN
- NDN generalizes the Internet architecture by replacing the focus on *where* –endpoint addresses of hosts – with ***what*** – identifiers of the ***content*** that users and applications care about
- NDN focuses on data directly to build the communication infrastructure
- Built-in data security
- Built-in multicast delivery
- Built-in data dissemination
- Built-in components to facilitate mobility, ad hoc
- Like IP, NDN is a “universal overlay”

References

- Van Jacobson, James D. Thornton, Lixia Zhang, et all. "Named Data Networking (NDN) Project" *NDN-0001 October 31, 2010*
- V. Jacobson, D. K. Smetters, J. D. Thornton, M. F.Plass, N. H. Briggs, and R. L. Braynard. "Networking Named Content". *In Proceedings of the 5th ACM International Conference on Emerging Networking Experiments and Technologies, 2009*.
- http://www.ccnx.org
- http://named-data.org

THANKS FOR LISTENING

QUESTIONS?