

Introduction to Information Centric Networking

... with a Dash of Security

Claudio Marxer <claudio.marxer@unibas.ch>

Computer Networks Group · University of Basel · Switzerland

Open Source IoT & Blockchain Hackathon, Berlin · January 18, 2018

– www.iothon.io –

Historic Perspective

- Past: “Circuit-Centric”

Path Names: 0041 61 207 05 55

You say how to contact...

- Present: Host-Centric

Host/Location Names: 131.152.228.33

You say who to contact...

- Future: Information-Centric (?)

Information/Content Names: /the/content/name

You say what you want to receive...

Outline

ICN & Friends

- Jungle of Abrevs (ICN, CCN, CICN, CCNx, NDN, ...)
- Content Centric Networking
 - Naming Scheme
 - Packet Types
 - Node Model

Data Security in a Location-Agnostic World

- Mindset: Content-Based Security
- Some Mechanisms
 - Access Control / Confidentiality
 - Authenticity & Integrity

Through the Jungle of Abrevs

Research Field & Architecture Paradigm:

Information Centric Networking

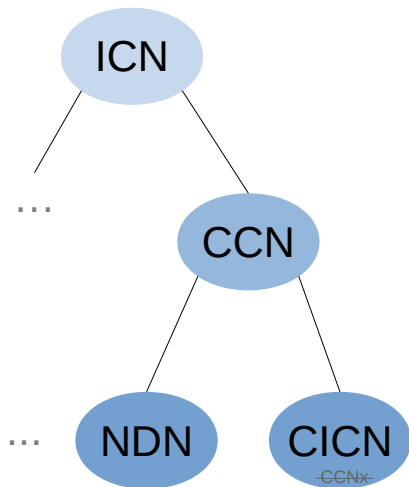
Network Service: `lookup(<content-ID>)`

Recent ICN Flavour: *Content Centric Networking*

Naming Scheme, Packet Types, Node Model, ...

CCN Derivates:

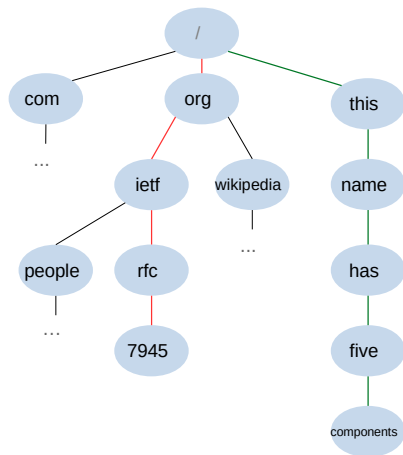
Wire Formats, Running Code, ...



CCN Naming Scheme

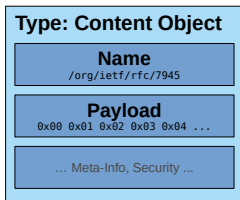
`/this/name/has/five/components`

- Hierarchical Namespace
- Human-Readable
- Publisher “owns” a Domain (i.e. Prefix)
 - `/org/ietf`
 - `/org/ietf/rfc`



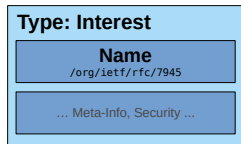
CCN Packet Types

Content Object



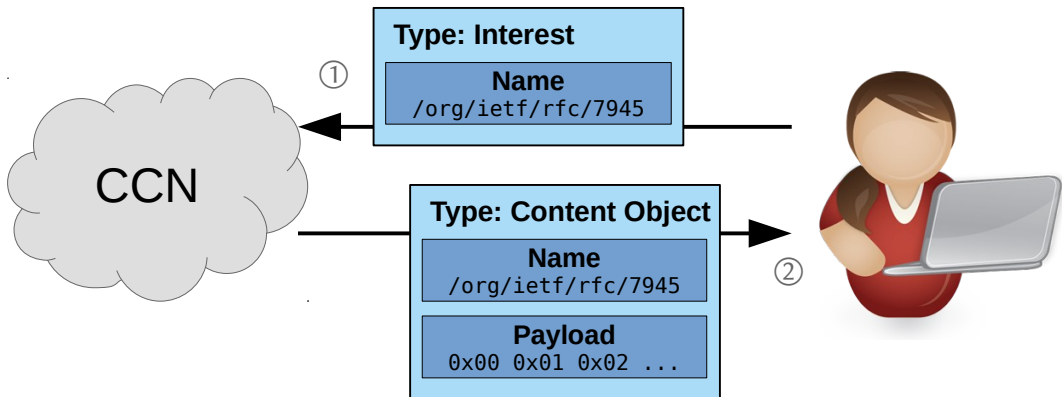
- Unique and unchangeable binding of a name and content
- Container for a chunk of content
- Location-independent and self-containing

Interest

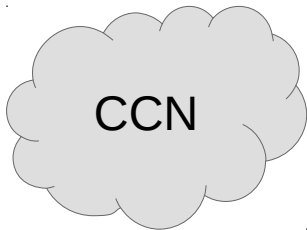


- Semantics: Sender expresses interest in receiving the named content object
- Interface to the network: `lookup(/some/content)`

CCN Packet Types (2)



Communication pattern: pull-based, consumer-driven, flow-balanced.



{Information, Data, Name,...} – Centric World

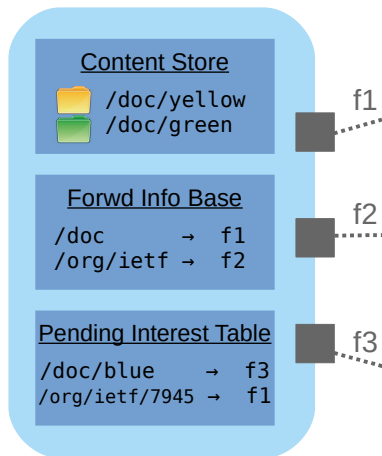
First-Class Citizens: Name-Payload-Signature Bundles

Following: Internal Rules of this World

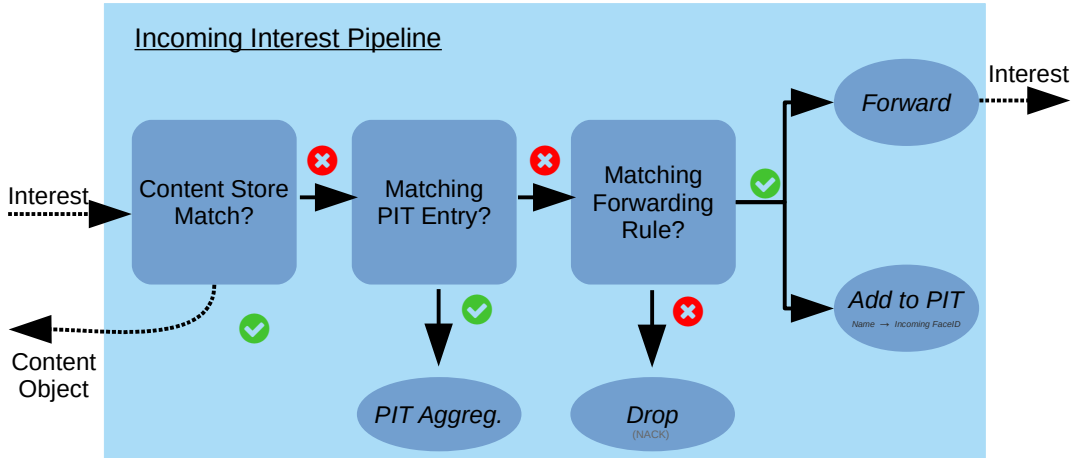
CCN Node Model (1) (or how the network satisfies an interest)

A CCN relay maintains ...

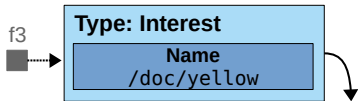
- *Faces*: Links to adjacent nodes (e.g. via UDP, wifi, ethernet, bluetooth)
- *Content Store (CS)*
Content object cache
- *Forwarding Information Base (FIB)*
Name-prefix-based forwarding rules
- *Pending Interest Table (PIT)*
Tracking interests from adjacent nodes



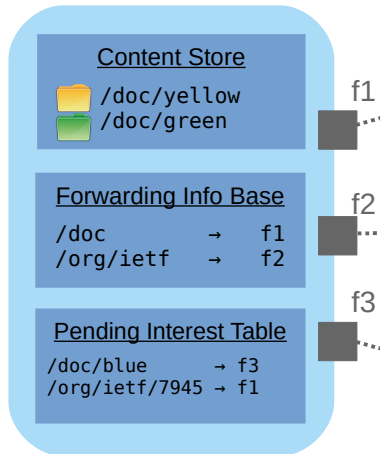
CCN Node Model (2) (or how the network satisfies an interest)



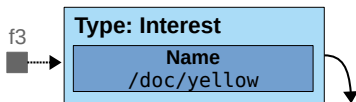
Example 1: Content Store Hit



Internal State



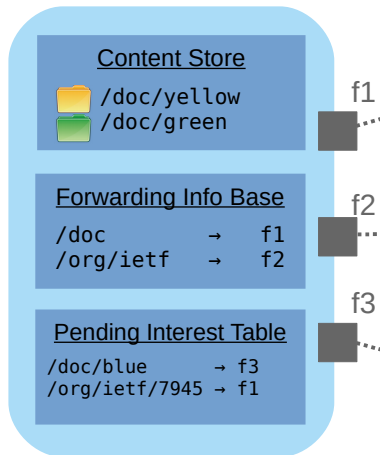
Example 1: Content Store Hit



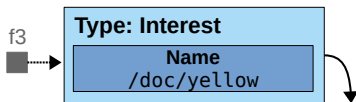
Incomming Interest Pipeline

Content Store Match?

Internal State



Example 1: Content Store Hit

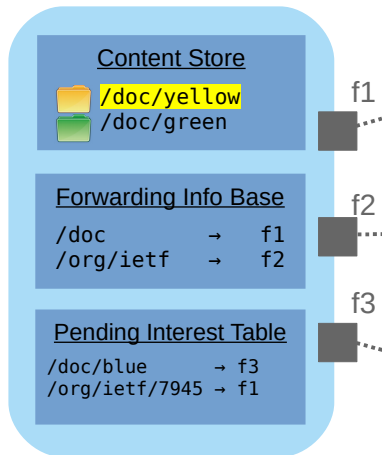


Incomming Interest Pipeline

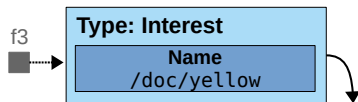
Content Store Match? 

– Satisfy interest from CS

Internal State



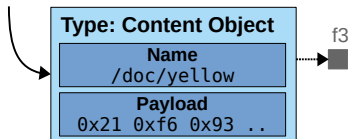
Example 1: Content Store Hit



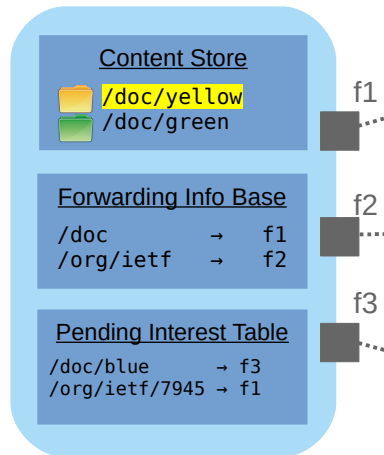
Incomming Interest Pipeline

Content Store Match? 

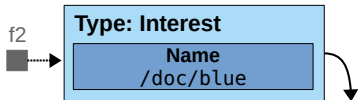
– Satisfy interest from CS



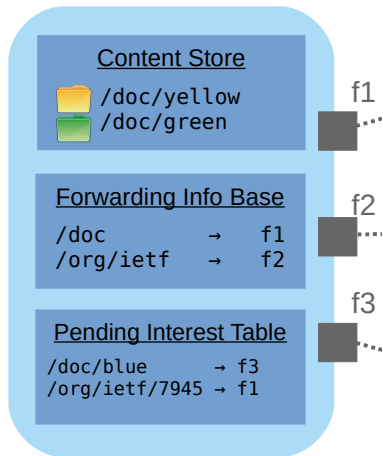
Internal State



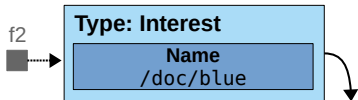
Example 2: PIT Aggregation



Internal State



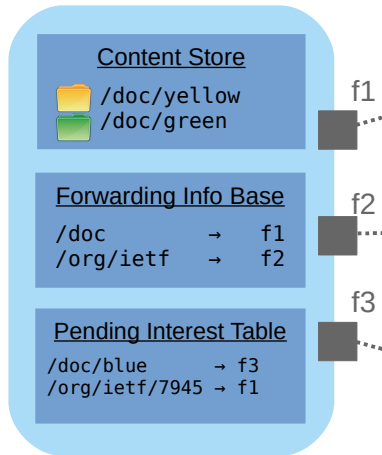
Example 2: PIT Aggregation



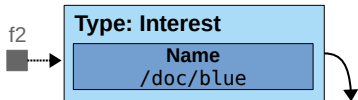
Incomming Interest Pipeline

Content Store Match? 

Internal State



Example 2: PIT Aggregation



Incomming Interest Pipeline

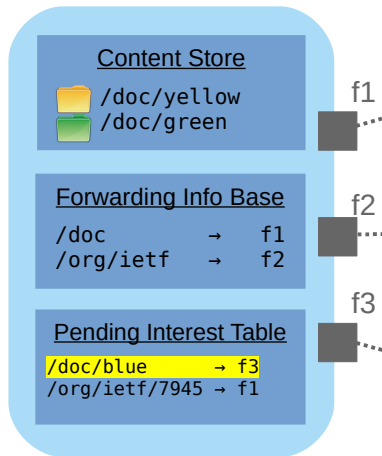
Content Store Match?



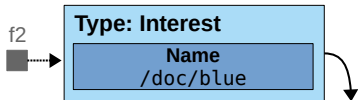
Matching PIT Entry?



Internal State



Example 2: PIT Aggregation



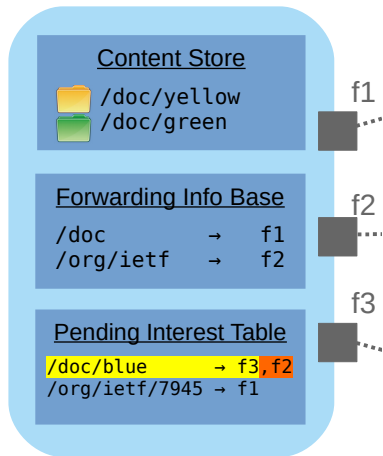
Incomming Interest Pipeline

Content Store Match? 

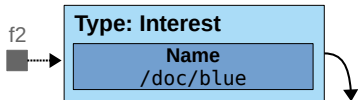
Matching PIT Entry? 

– PIT Aggregation

Internal State



Example 2: PIT Aggregation



Incomming Interest Pipeline

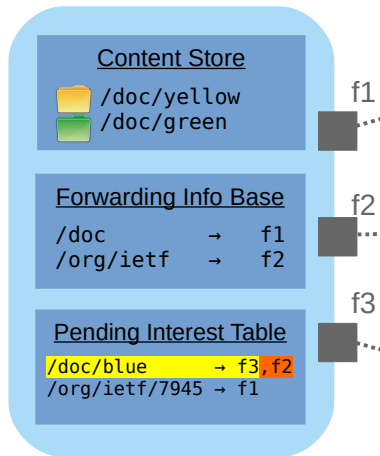
Content Store Match? 

Matching PIT Entry? 

– PIT Aggregation



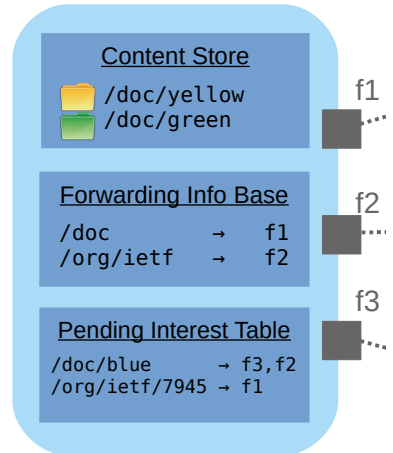
Internal State



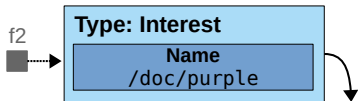
Example 3: Interest Forwarding



Internal State



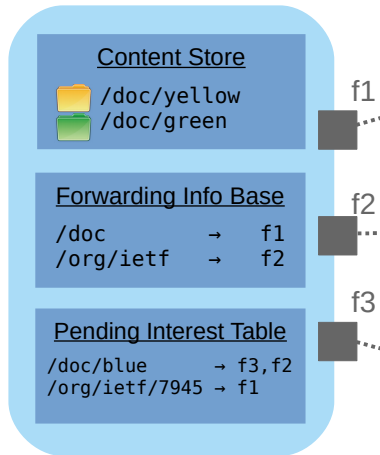
Example 3: Interest Forwarding



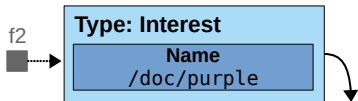
Incomming Interest Pipeline

Content Store Match? 

Internal State



Example 3: Interest Forwarding

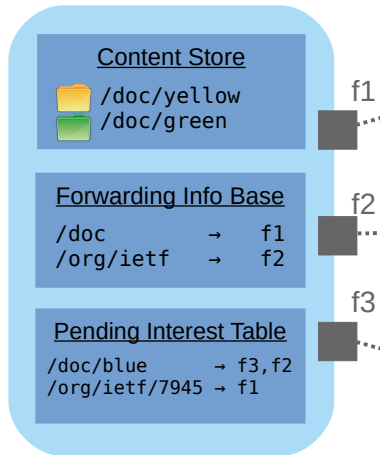


Incomming Interest Pipeline

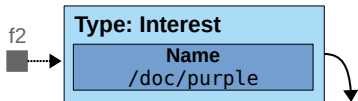
Content Store Match? 

Matching PIT Entry? 

Internal State



Example 3: Interest Forwarding



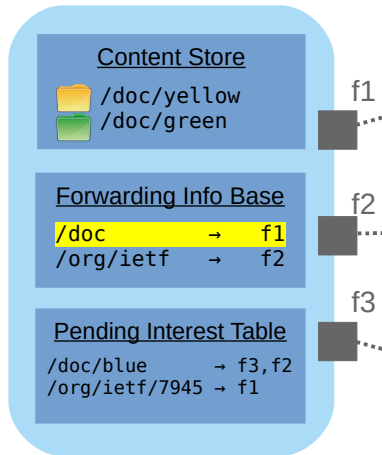
Incomming Interest Pipeline

Content Store Match? ❌

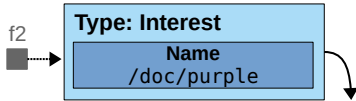
Matching PIT Entry? ❌

Matching Forwarding Rule? ✅




Internal State

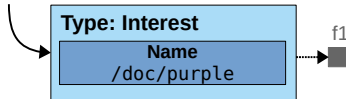


Example 3: Interest Forwarding

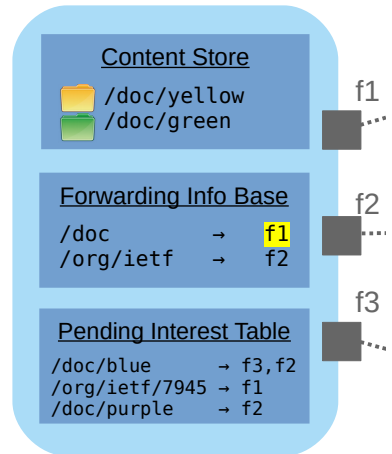


Incomming Interest Pipeline

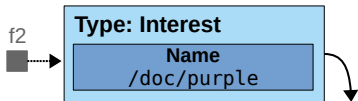
Content Store Match? 
Matching PIT Entry? 
Matching Forwarding Rule? 
– Forward



Internal State



Example 3: Interest Forwarding



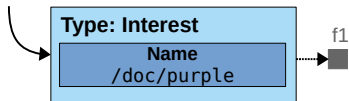
Incomming Interest Pipeline

Content Store Match? ❌

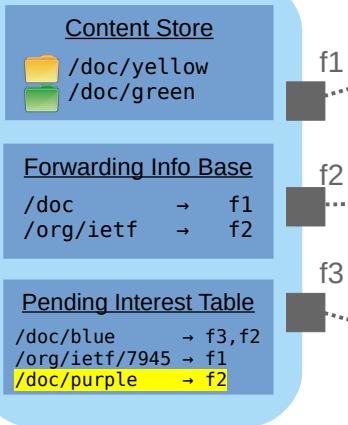
Matching PIT Entry? ❌

Matching Forwarding Rule? ✅

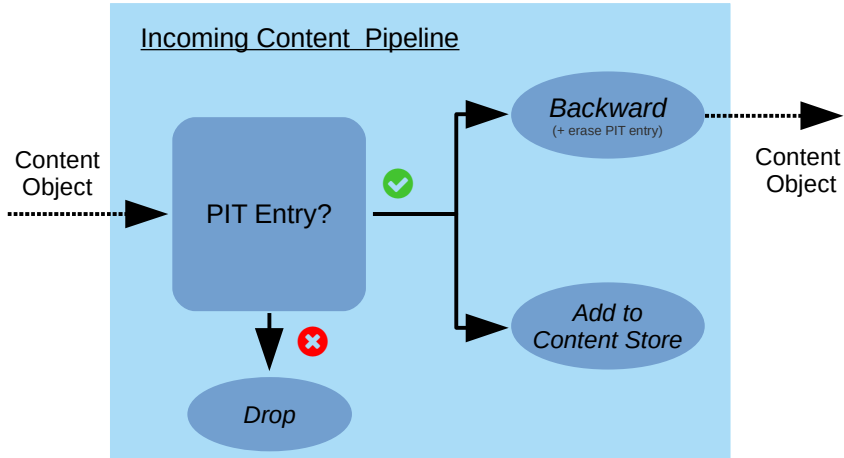
- Forward
- Add PIT Entry



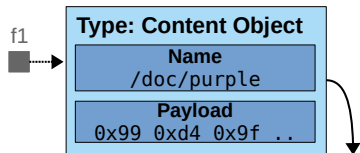
Internal State



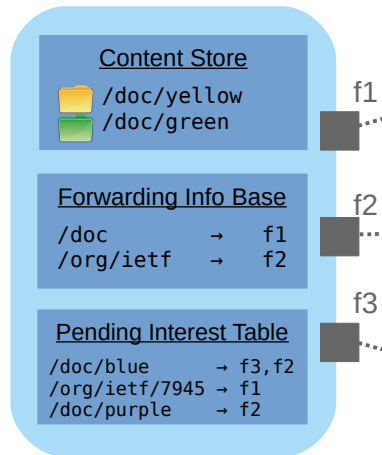
CCN Node Model (3) (or how the network satisfies an interest)



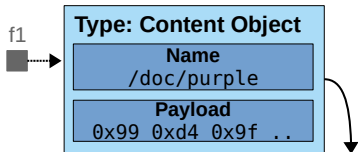
Example 4: Content Backwarding



Internal State



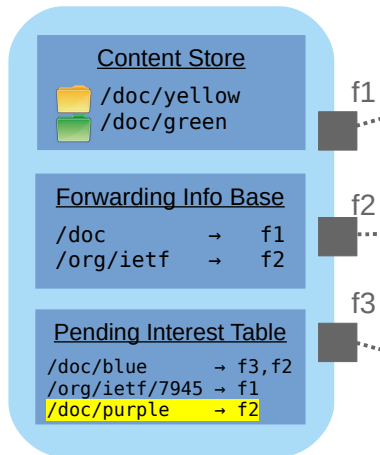
Example 4: Content Backwarding



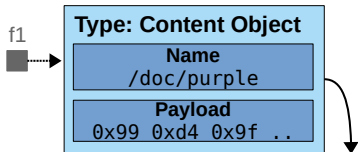
Incomming Content Pipeline

Existing PIT Entry?

Internal State



Example 4: Content Backwarding

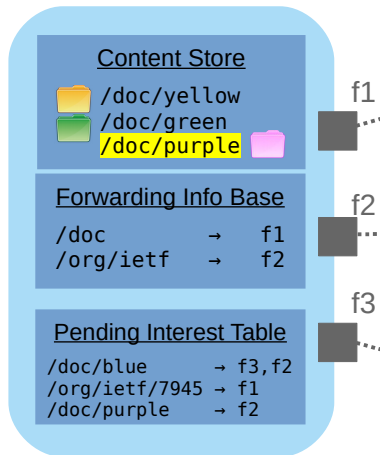


Incomming Content Pipeline

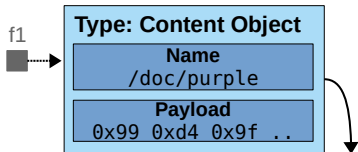
Existing PIT Entry?

– Add to Content Store

Internal State



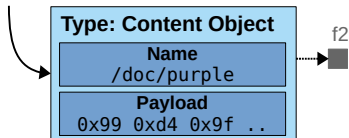
Example 4: Content Backwarding



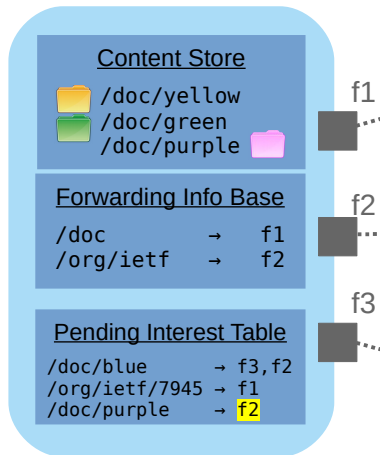
Incomming Content Pipeline

Existing PIT Entry? 

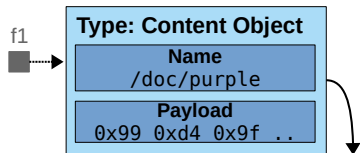
- Add to Content Store
- Backward according to PIT



Internal State



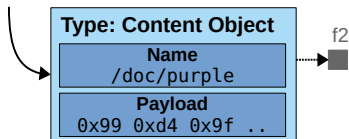
Example 4: Content Backwarding



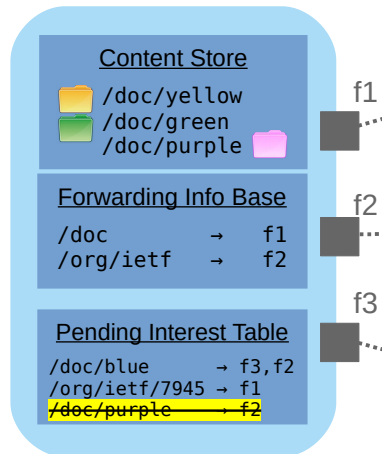
Incomming Content Pipeline

Existing PIT Entry?

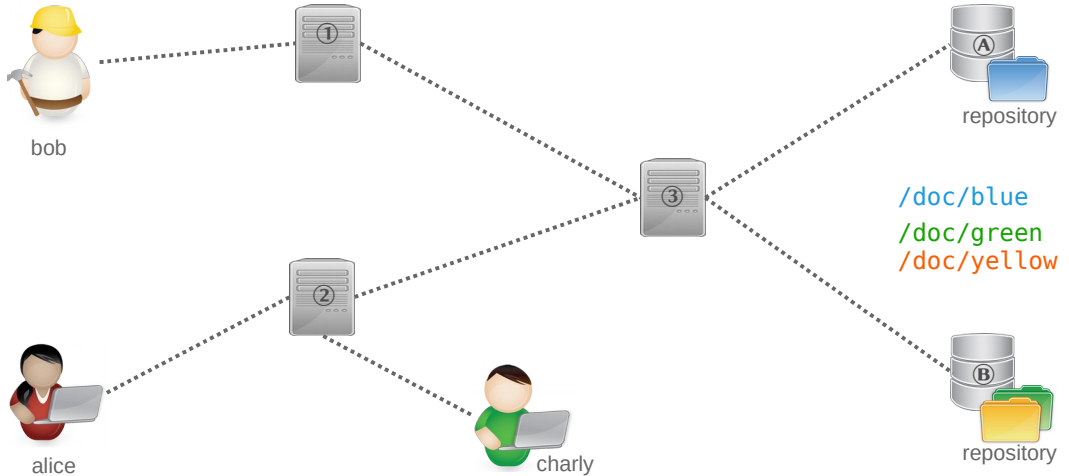
- Add to Content Store
- Backward according to PIT
- Erase PIT Entry



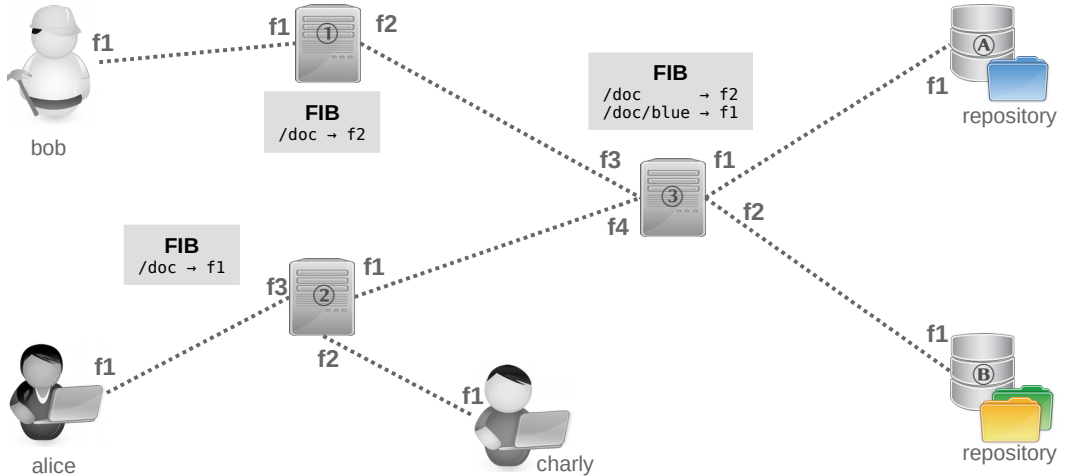
Internal State



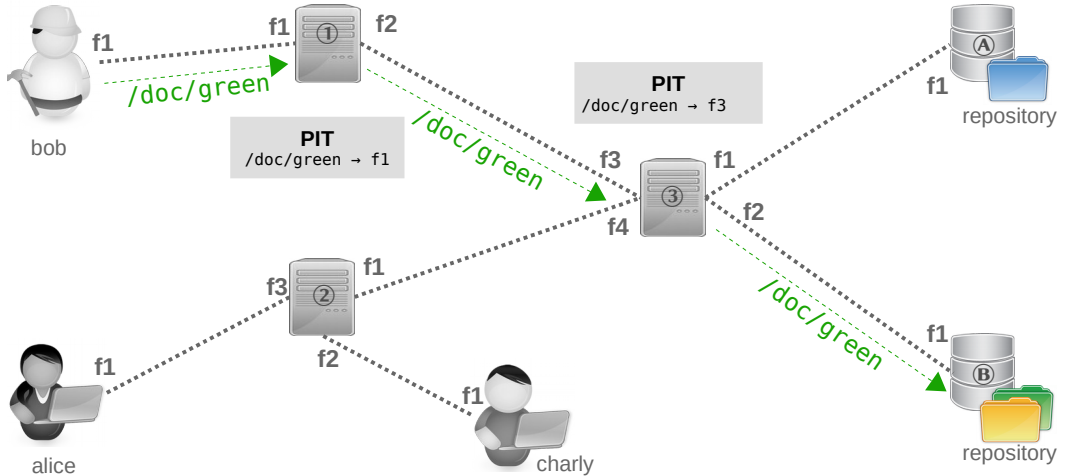
CCN in Action..



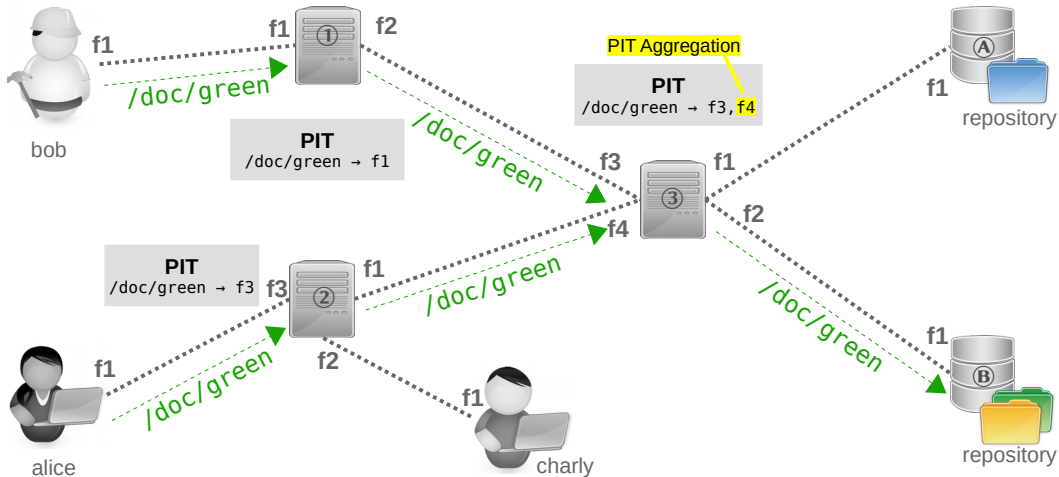
CCN in Action..



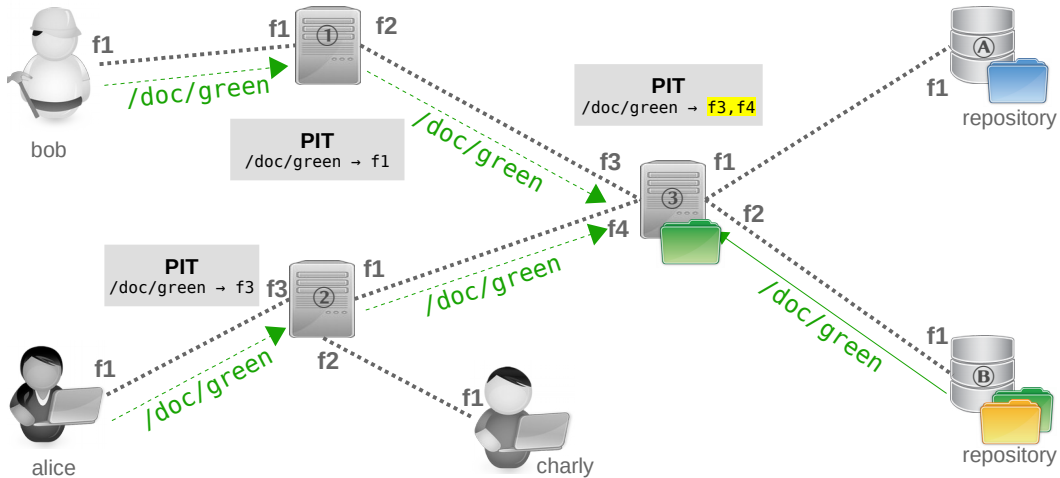
CCN in Action..



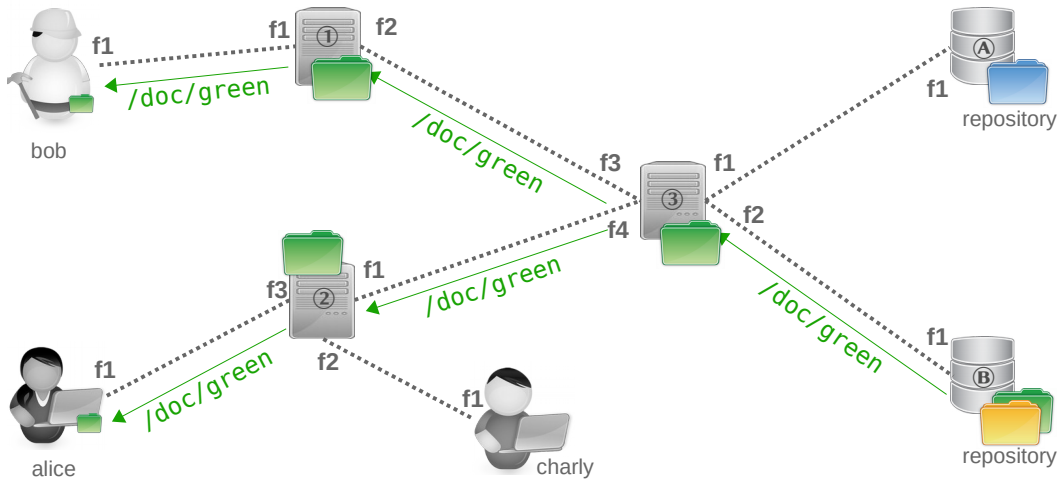
CCN in Action..



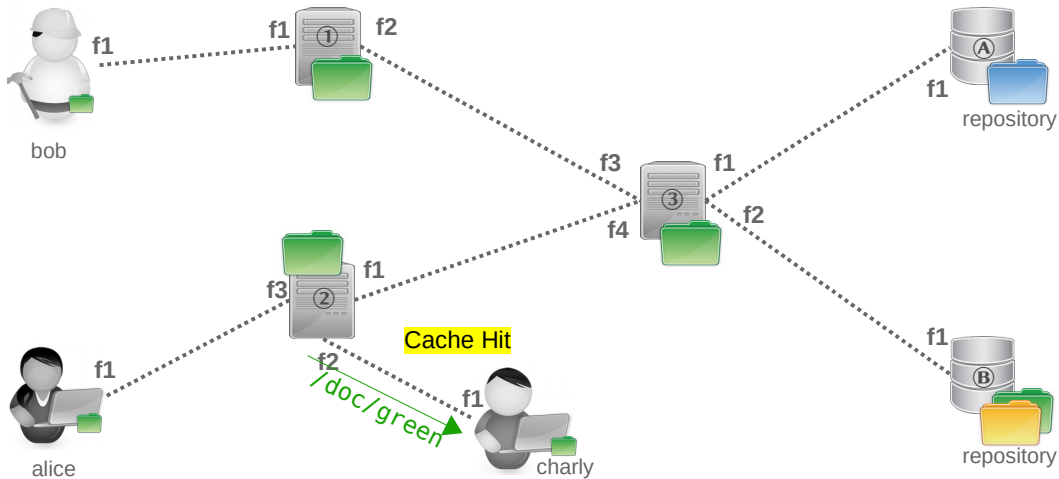
CCN in Action..



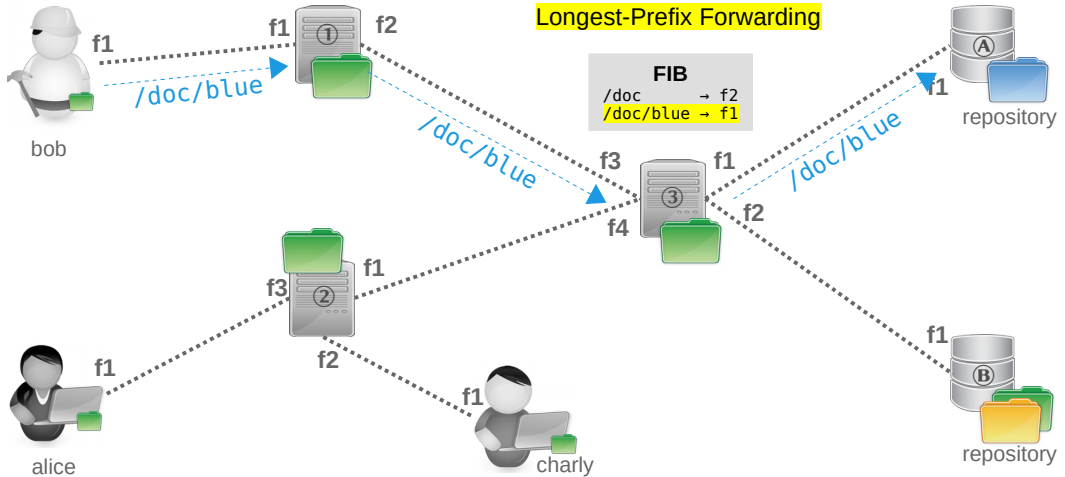
CCN in Action..



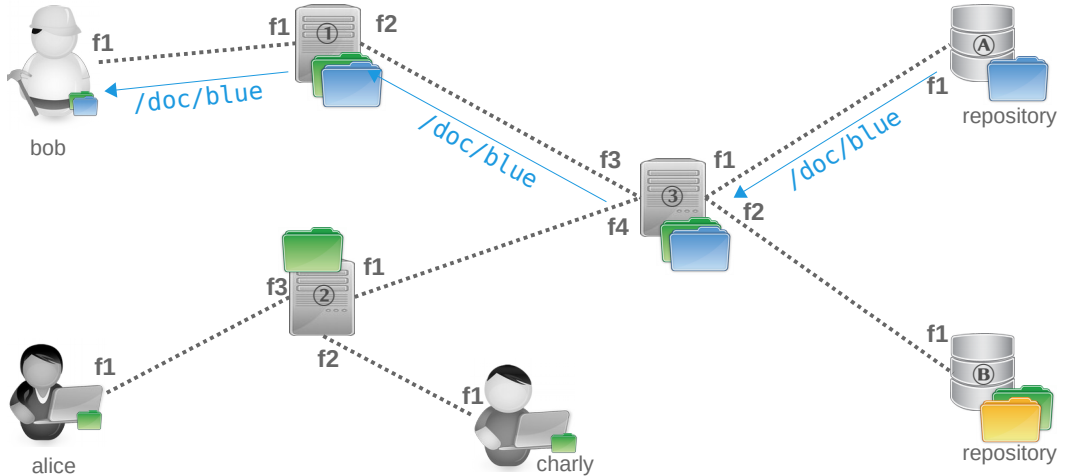
CCN in Action..



CCN in Action..



CCN in Action..



Wrap Your Mind: Security in a Channel-Less World

“Protection and trust [should] travel with the content itself rather than being a property of the connections over which it travels.” (Smetters & Jacobson, 2009)

Host-Centric World: Unsecured data travels through secured connections.

→ *Transport Layer Security (TLS)*

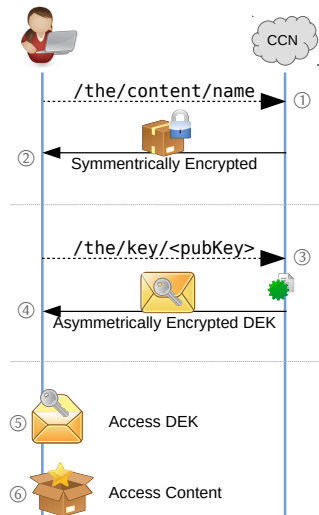
Information-Centric World: Secured data is delivered by an untrusted network.

→ *Content-Based Security*

Content-Based Access-Control / Confidentiality

Two-step approach:

- Content is symmetrically encrypted (Data Encryption Key, DEK)
- Authorized clients: DEKs are provided separately
 - Identification: Public Key



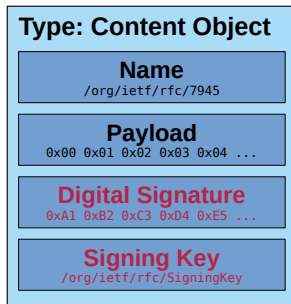
Authenticity/Integrity of Location-Independent Content

Approach: Publisher attaches a digital signature to each content object.

Signing-authority policy framework:

- Publisher can “own” domains in the namespace
- Owner exclusively holds signing authority in his domain
- Ownership of sub-domains can be granted

Challenge: Assessing authority of signing keys.



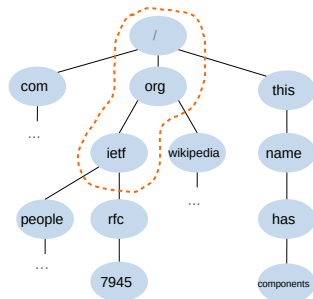
Authenticity/Integrity of Location-Independent Content

Approach: Publisher attaches a digital signature to each content object.

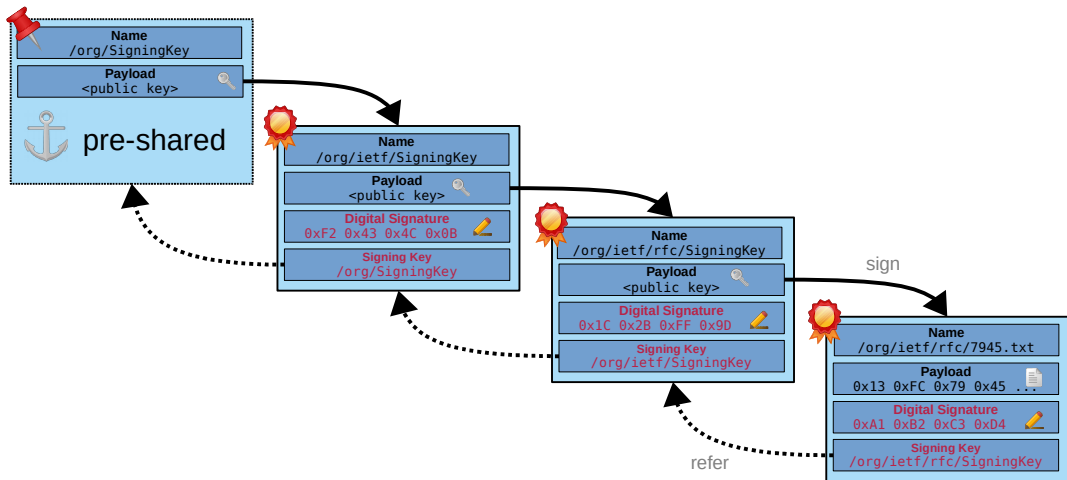
Signing-authority policy framework:

- Publisher can “own” domains in the namespace
- Owner exclusively holds signing authority in his domain
- Ownership of sub-domains can be granted

Challenge: Assessing authority of signing keys.



Authenticity/Integrity: Signing Key Chain



Wrap-Up

- Information-Centric Networking (Paradigm): Data as the pivotal entity
- Content-Centric Networking (Architecture):
 - Network Service to Consumer:
Pull-Based Content Retrieval (interest-based)
 - Network Service to Publisher:
Scalable Content Distribution: Multicasting due to PIT Aggregation & Caching
 - Network State & Mechanics:
CS (in-network caching), FIB (name-based forwarding), PIT (forwarding state);
Interest & Content Object Pipelines
- Content-Based Security: Secure Content, not Connections.

Q & A

Further Reading

Information-Centric Networking

- IRTF Research Group: <https://trac.ietf.org/trac/irtf/wiki/icnrg>
- ACM ICN Conference: <https://conferences.sigcomm.org/acm-icn/2018>

Content-Centric Networking

- V. Jacobson et al., “*Networking Named Content*” in International Conference on Emerging Networking Experiments and Technologies, 2009.
- Named Data Networking Project: <https://named-data.net>
- Community ICN (CICN) Project: <https://wiki.fd.io/view/Cicn>
- CCN-Lite (Relay): <https://github.com/cn-uofbasel/ccn-lite>
- PiCN (Toolbox): <https://github.com/cn-uofbasel/PiCN>