Named-Data Transport: An End-to-End Approach for an Information-Centric IP Internet

Abdulazaz Albalawi J.J. Garcia-Luna-Aceves

Computer Communication Research Group (CCRG)
UC Santa Cruz

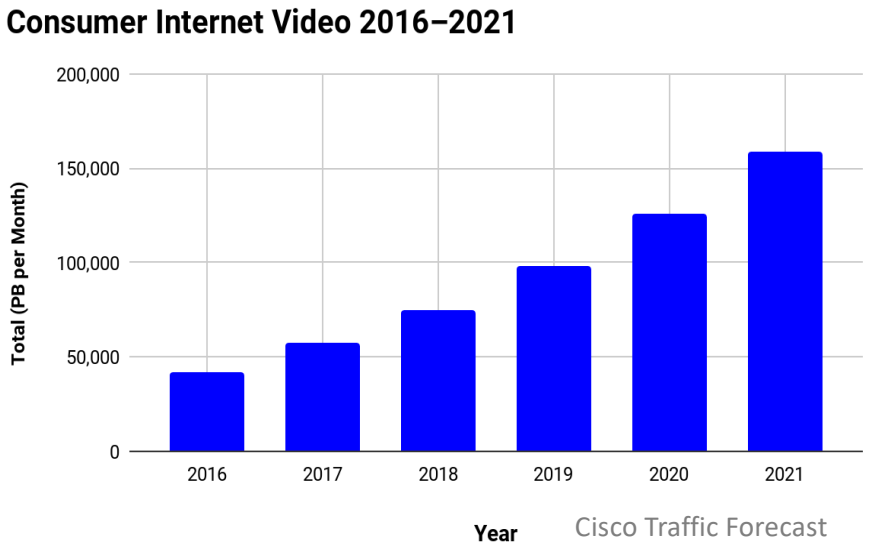
Outline

- Problem
- Existing Solutions
- Named Data Transport
- Named Data Transport Protocol
- My-DNS
- Named Data Proxies
- Performance
- Conclusion

Problem

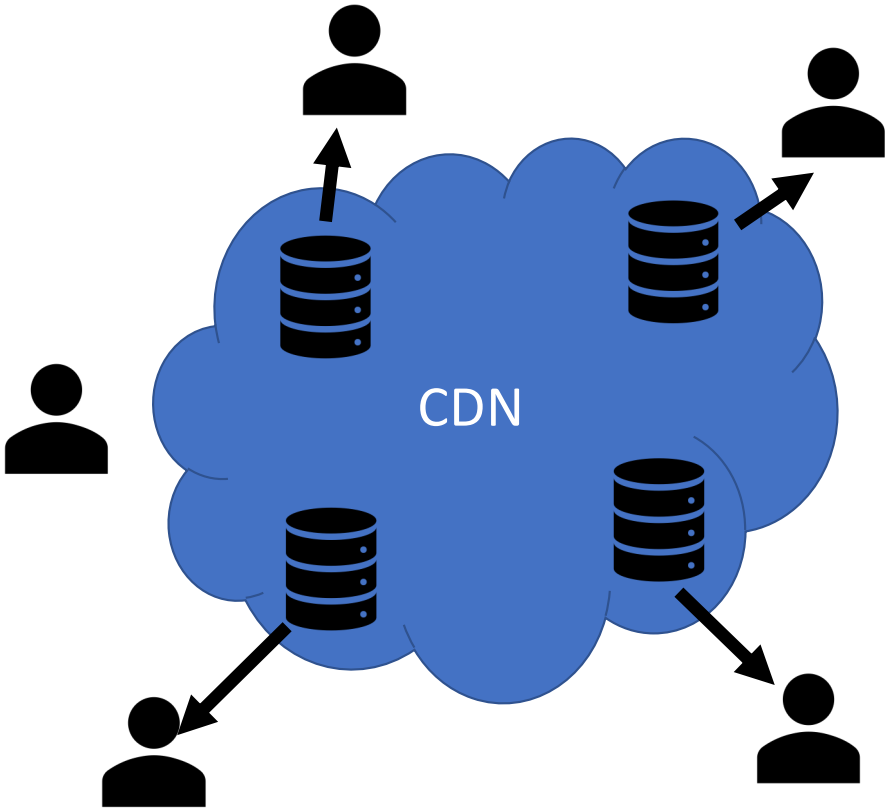
Today's Internet Architecture

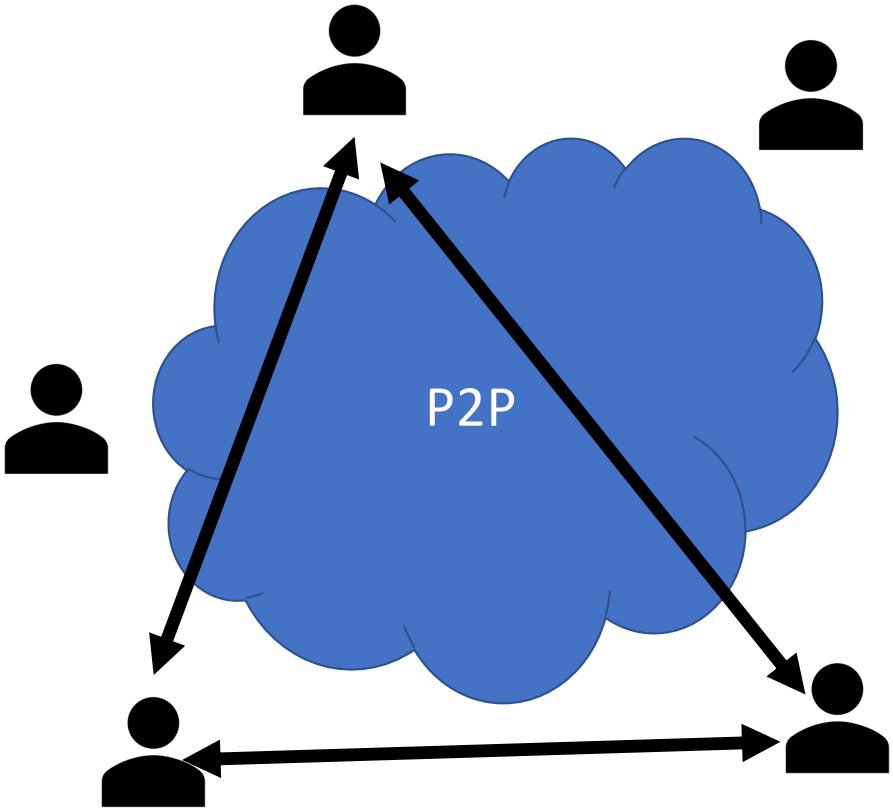
- Limited support for reliable and efficient access to contents and services.
- Security is left to end hosts
- Limited mobility support



Solutions

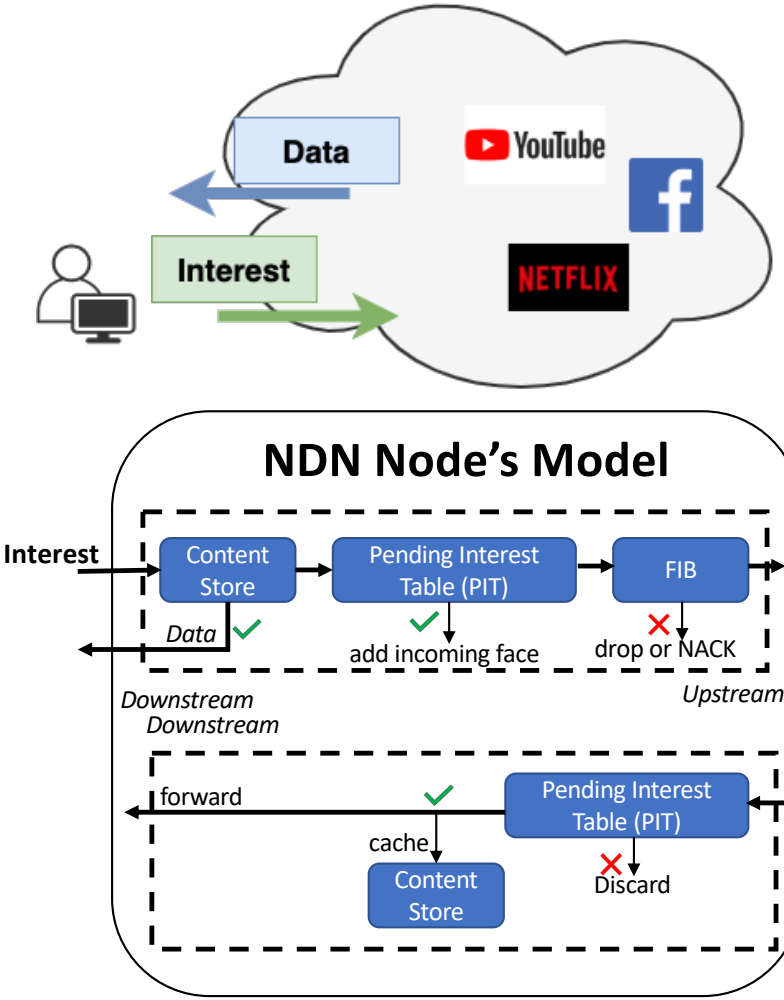
CDN and P2P Approaches





Prior ICN Architectures

- Information-Centric Network (ICN) architectures:
  - Request content from the network not the host
  - Caching is universal in the network.
  - Security is bound to the content not a host
- Redesign the network layer
- Redesign existing applications



DNS-based Approaches

- Aims to provide ICN benefits in the Internet by leveraging the DNS system

iDNS

- Resolve content names to metadata
- Metadata contains address of servers and local caches
- No protocol was specified to retrieve contents

idICN

- Also, resolve content names to nearby caches or severs
- Uses HTTP as the baseline for the transfer protocol
- Doesn’t provide transparent caching for non-HTTP applications

Named Data Transport: An End-to-End Approach for an Information-Centric IP Interne

NDT Goals

1. Allowing all Internet applications to request content and services by name rather than locations
2. Eliminating performance issues associated with TCP connections
3. Provide Transparent Caching
4. Providing added privacy to content consumers

NDT Architecture

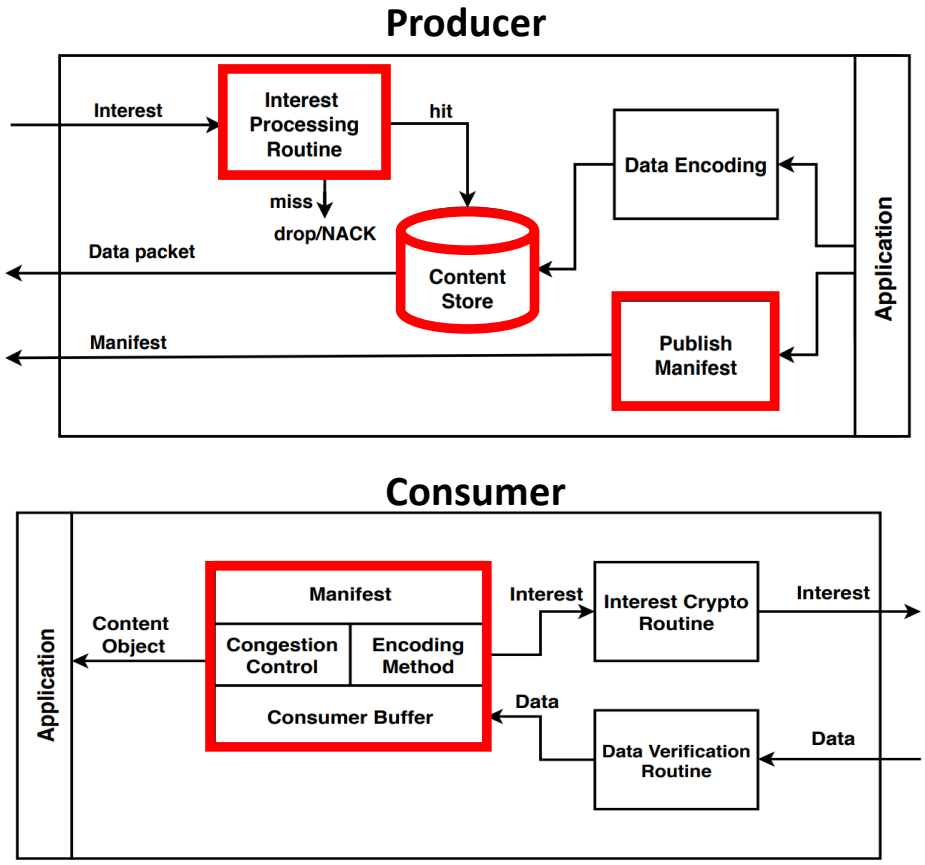
NDT consists of the integration of three end-to-end architectural components:

1. Named Data Transport Protocol (**NDTP**), a connection-free reliable transport protocol.
2. manifest-yielding DNS (**my-DNS**), an extension to the Domain Name System (DNS) to include records containing manifests describing content.
3. NDT Proxies (**NP**), transparent caches that track pending requests for content at the transport layer.

Named Data Transport Protocol

Named Data Transport Protocol

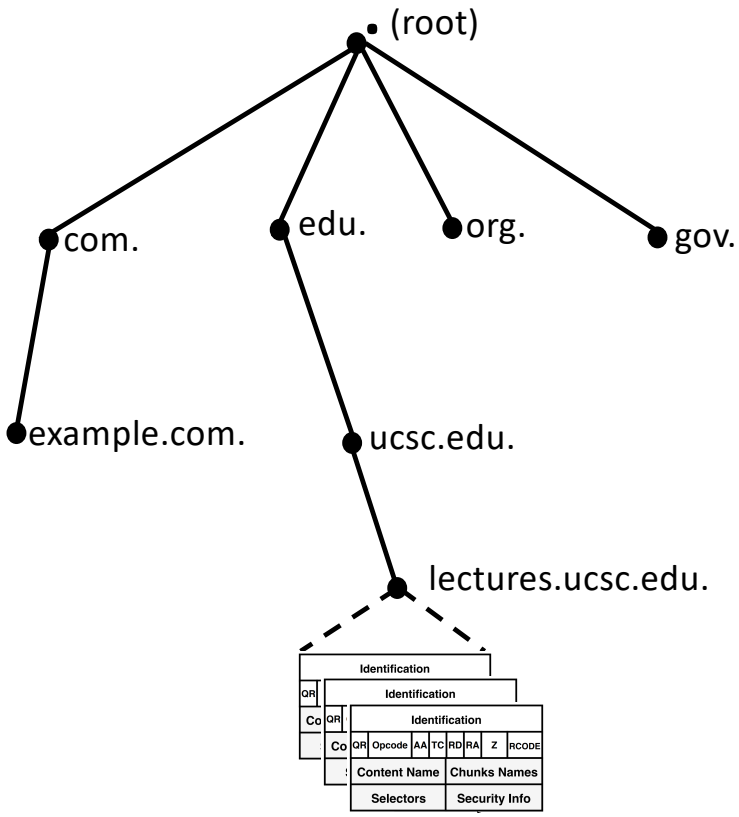
- NDTP design can be viewed as the Interest-based approach used in NDN
- There are three main packets in NDTP:
  - Manifest
  - Interest
  - Data packet
- Manifests describe how a content object is structured into smaller units called object chunks.



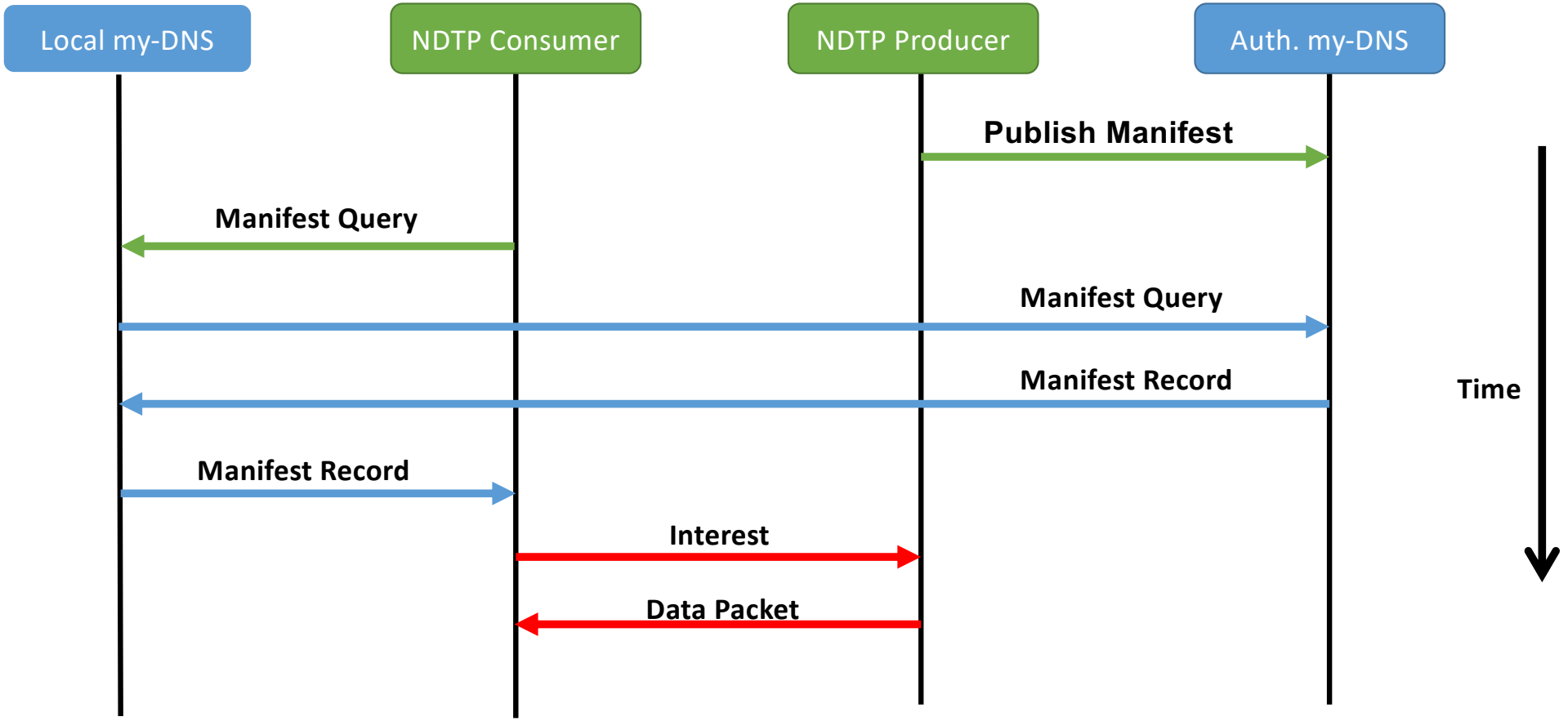
manifest-yielding DNS

manifest-yielding DNS

- Content names in NDT are based on DNS domain names
- Each content name on the Internet is mapped to an individual manifest record
- Manifest record maps the **manifest** of a content to a list of IP addresses hosting a replica of the content
- my-DNS sort the list based on consumers location

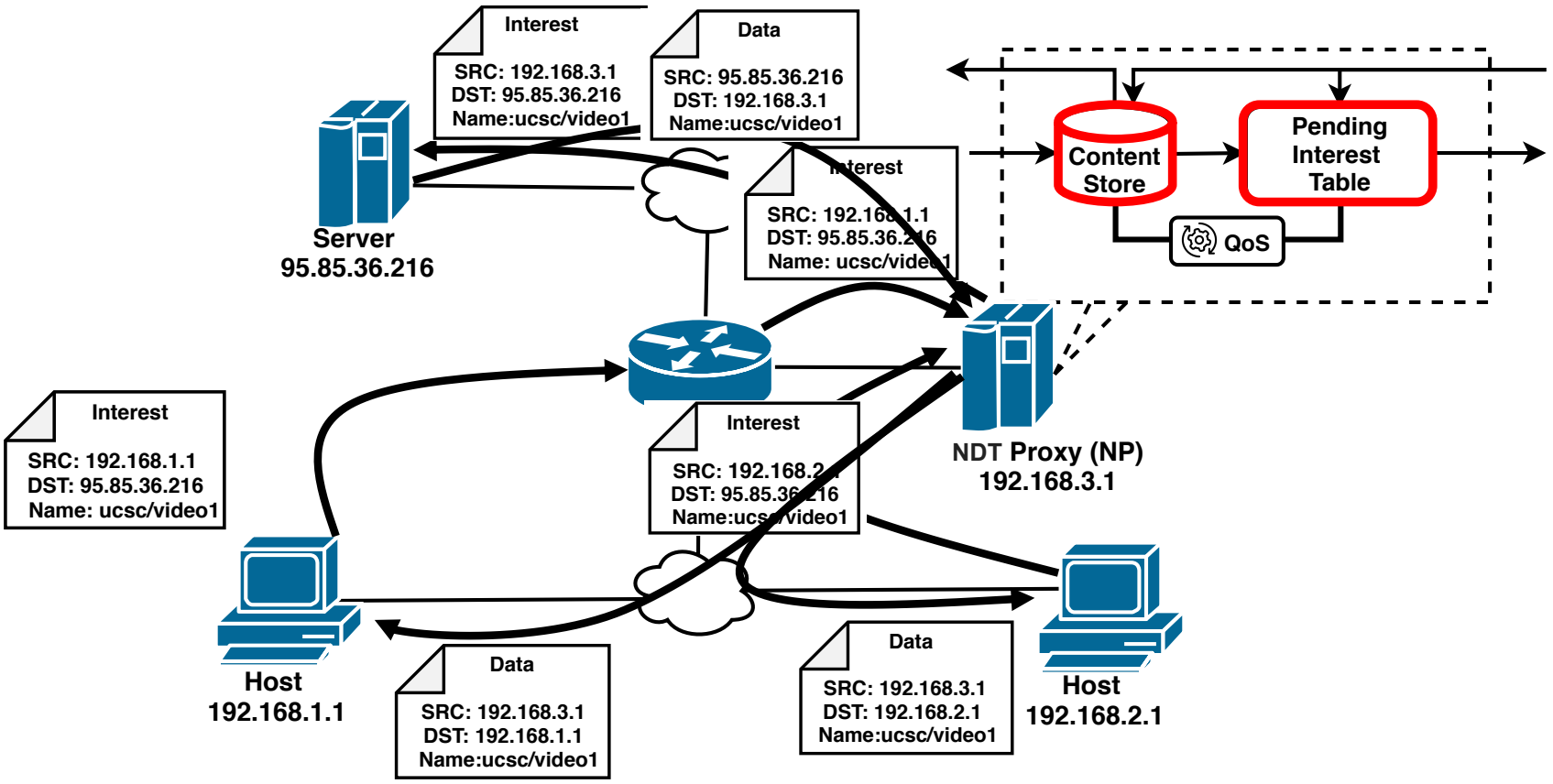


Mapping Content Names To Manifest Records



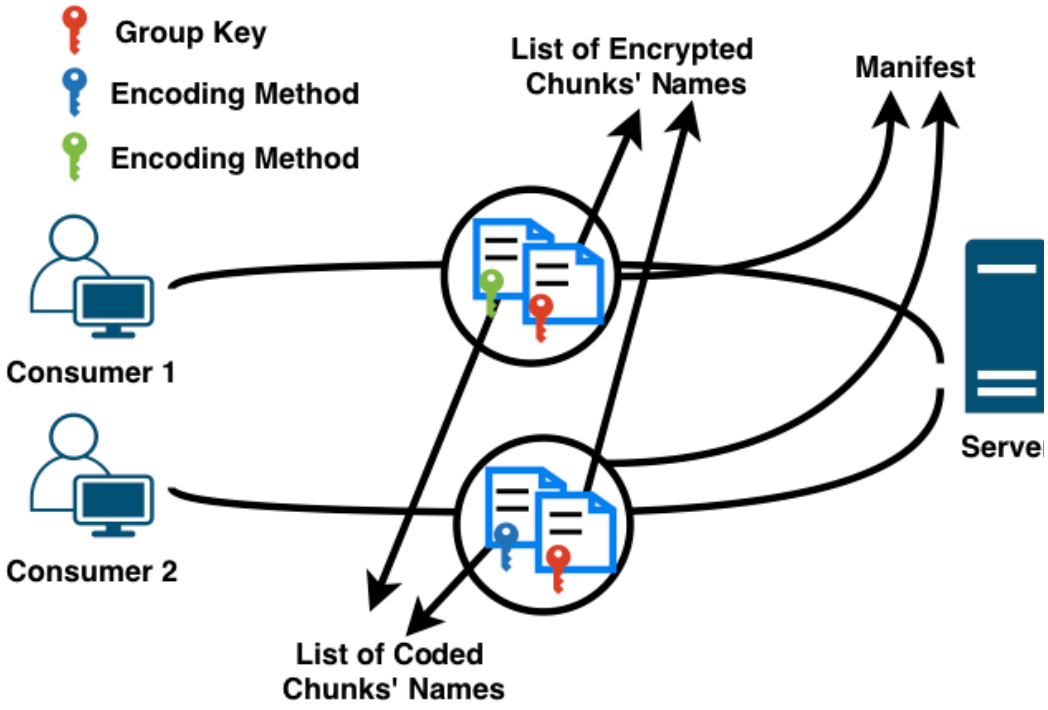
Named Data Proxies

Named Data Proxies



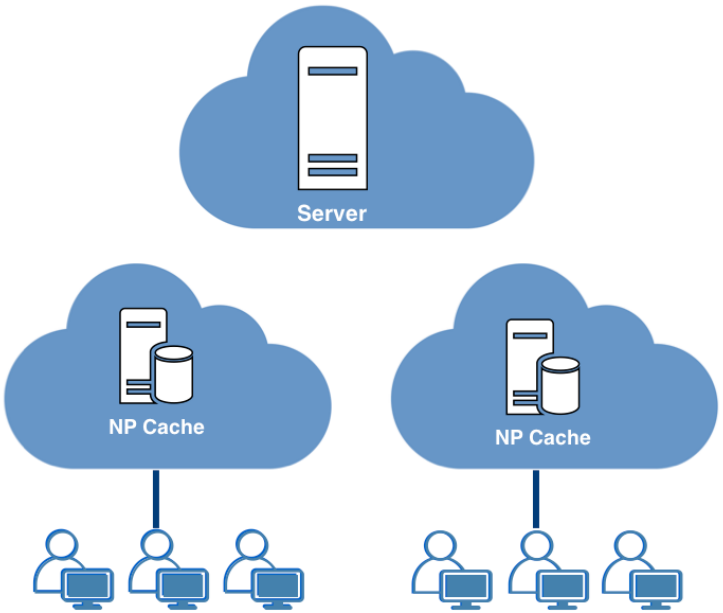
Securing Cached Content in NDT

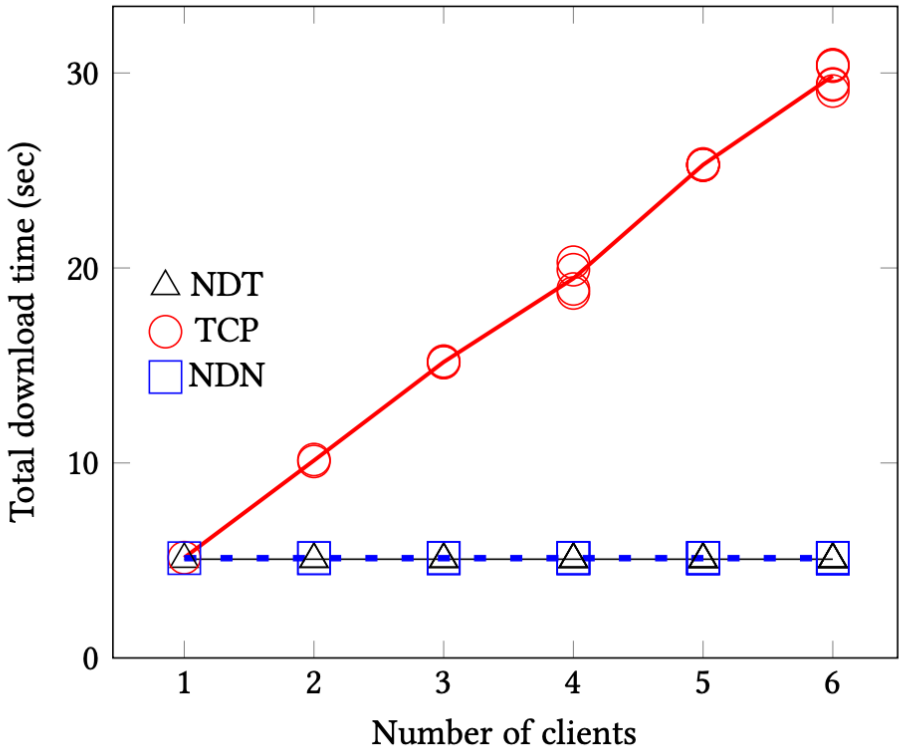
- **TLS**
  - Session based
  - Preclude caching in middle-boxes
- **Group Keys**
  - One Key per CO
  - Only authorized consumers will have access to this key as part of manifest
- **Data Encoding**
  - Obfuscation CO with useless data
  - Only authorized consumers will have access to the encoding method
- **Partial Caching/Encryption**
  - Use group key per content
  - Encoding method per consumer



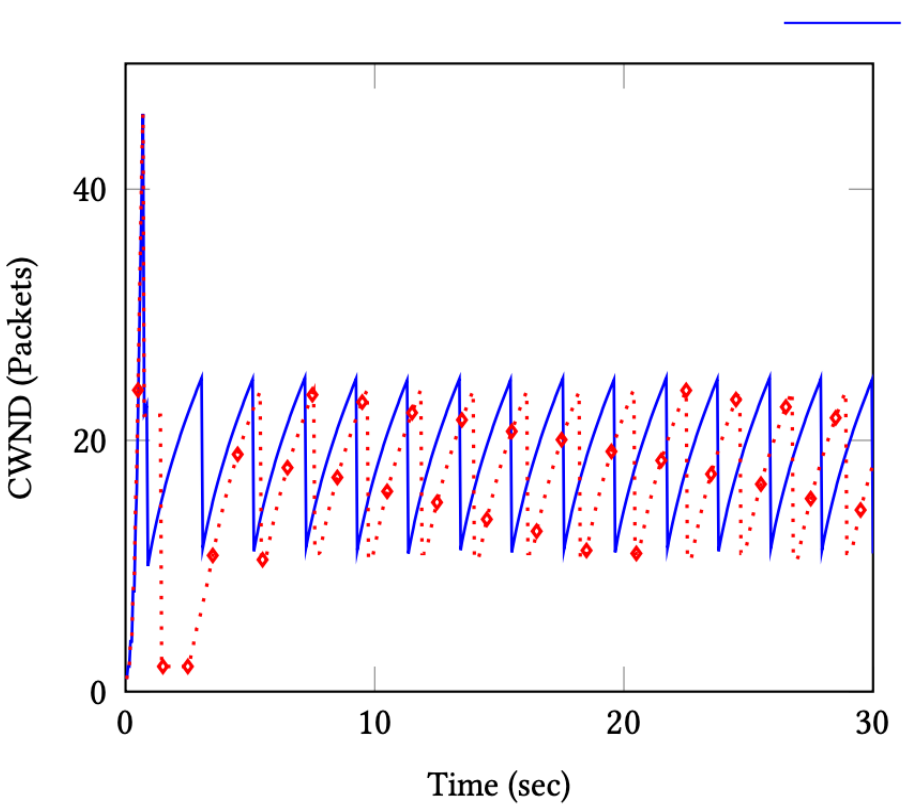
Performance

NDT vs TCP vs NDN

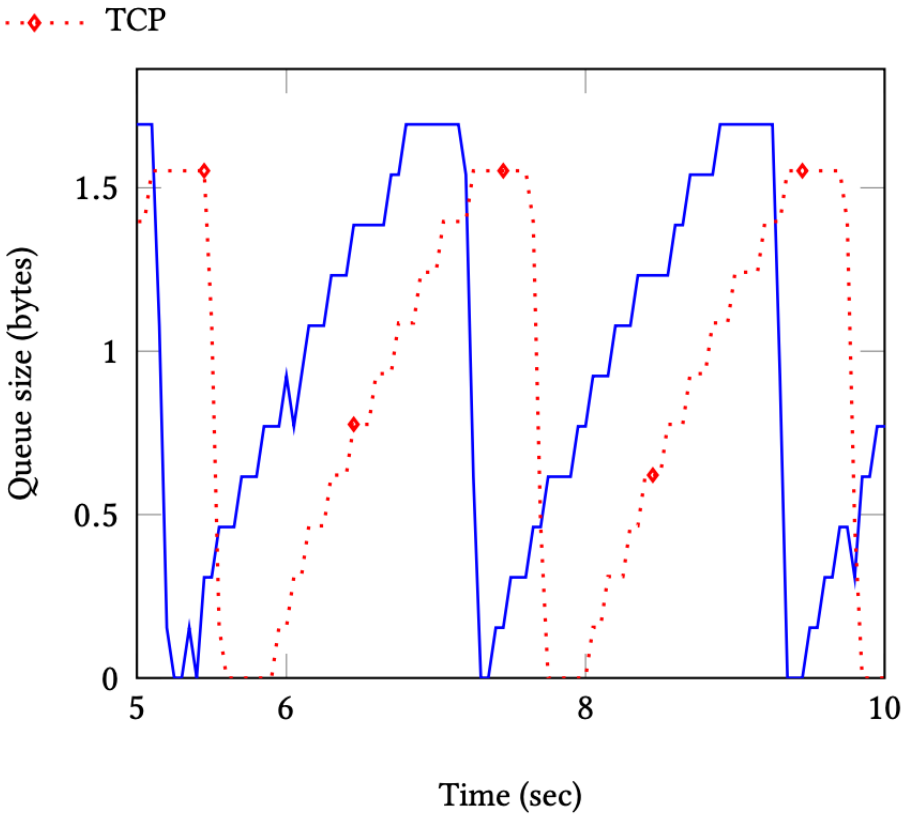




NDTP vs TCP

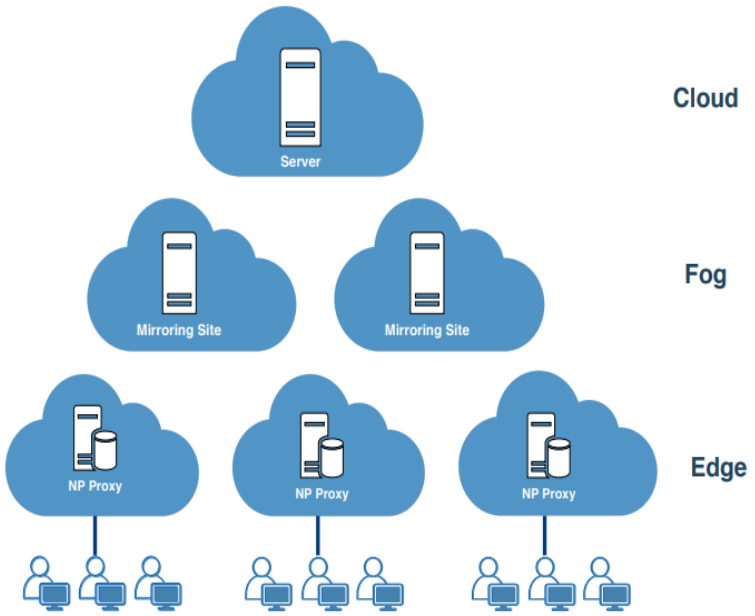


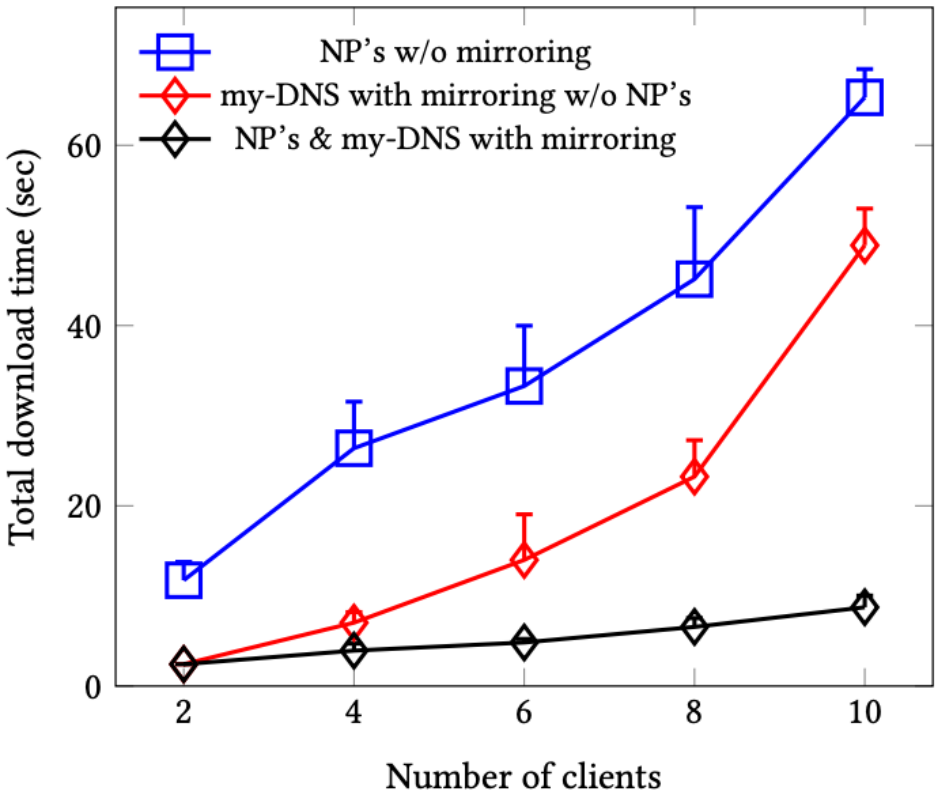
CWND Size



Router's Buffer Occupancy

Impact of Manifest Records and Mirroring





Conclusion

Summary

- NDT attains efficient content dissemination without end-to end connections or modifications to the IP routing infrastructure
- The simulation experiments show that:
  1. NDT is inherently more efficient than TCP.
  2. The performance of NDT and NDN is very similar.
  3. NDT outperforms HTTP over TCP while being able to provide privacy
- Future Work:
  - Congestion control algorithms
  - Security
  - Native Multicast

Thank You