MobilityFirst architectural components

- Name resolution
- Routing
- Transport
- Context-awareness
- Management plane
- Computing layer

Standard components of a network stack, but better refactoring in MobilityFirst
Global name resolution service (GNRS)

- Functions
  - Name certification
  - Location resolution
  - Content retrieval
Global name resolution service (GNRS)

- Design metrics
  - Fast
  - Scalable
  - Fault-tolerant
  - Secure
  - Privacy-aware
Location Service: **Scale to billions of mobiles**

- **Function**: Resolve GUID $\rightarrow$ [NA$_1$, NA$_2$, ...]
- **Target scale**: 10B devices moving across 100 networks/day $\Leftrightarrow$ 10M updates/sec
Routing: **Scale to millions of networks (1)**

- **Function:** Route to GUID@NA
- **Scale:** Millions of NA’s ↔ huge forwarding tables

```
send(GUID@NA, data)
```

<table>
<thead>
<tr>
<th>Network</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>NA1</td>
<td>2</td>
</tr>
<tr>
<td>NA2</td>
<td>6</td>
</tr>
<tr>
<td>NA3</td>
<td>1</td>
</tr>
<tr>
<td>NA4</td>
<td>2</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>NA1000000</td>
<td></td>
</tr>
</tbody>
</table>
Routing: **Scale to millions of networks (2)**

- **Function:** Route to GUID@NA scalably
- **Approach:** Leverage natural hierarchy in networks
Location Service: **Mechanisms and tradeoffs**

1. Consistent hashing
   - Load balance, fault-tolerance
   - Proximity
2. Active replication
   - Proximity
   - Update bandwidth
3. Passive Caching
   - Proximity
   - Staleness
Location Service for content retrieval

**Function:** Resolve $\text{GUID} \rightarrow [\text{NA}_1, \text{NA}_2, \ldots]$, where $\text{NA}_i$'s are locations where GUID is cached or can be authoritatively tracked

**API design challenges:**

1. Proximate content retrieval
2. Storage-aware routing and traffic engineering
3. Customizing and tracking consumed content
Routing
Routing mechanisms (1)

- Robust to connectivity and technology diversity
  - Uncertainty-driven metrics + self-adaptive replication
Routing mechanisms (2)

- **Storage-aware routing**
  - Deferred delivery
  - Opportunistic retrieval
Routing mechanisms (3)

- Multihomed multipath
- Multicast
- Anycast

ISP1 → ISP2

File → File → File

Server1 → Server2 → Server3
Segmented transport design

- Storage at segment (contiguous sequence of links) boundaries
- Unit of transmission a large block (instead of small packets in E2E TCP)
Security and Privacy
Verifiable identifiers (unlike IP)

- Name certification service
  - human_readable_name → public_key
  - contextual_keywords → public_key
  - network_name → public_key

Verifiable identifiers are robust to hijacking or spoofing unlike location-encoding IP addresses

- Network operations
  - send(GUID, <data>) or send(NA:GUID, <data>)
  - get(GUID) or get(NA:GUID)
Decentralizing trust in naming

- **Goal**: No single root of trust in name certification

- **Approach**:
  - Multiple name certification service (NCS) providers
  - Many-to-many mapping from namespaces to NCSs
  - Quorum-based certification
Proportional robustness

Goal: A small number of malicious nodes must not be able to disproportionately impact network performance/availability

- Byzantine fault-tolerant name service
- Routing
  - Multihomed multipath
  - Disruption-tolerant
  - Storage-aware
  - Logically centralized intradomain decisions

Today, a single faulty router can render most of Internet unavailable.
Intentional data receipt

An end-host must be contactable only if the transmission is consistent with its receipt policy.
**Intentional data receipt for security + privacy**

**Goal:** Controlling access to network location

**Approaches:**
- Blacklist known bad senders
- Whitelist known good senders
- Switch GUID pseudonyms

Pseudonym switching can help both security and privacy.
Other threats and mitigations

- Dynamic peering with unknown mobile network
  - Trust management service
- Ensuring fair resource allocation with multicast
- Balancing utility and privacy in context-aware services
Other threats and mitigations

- Dynamic peering with unknown mobile network
- **Ensuring fair resource allocation with multicast**
- Balancing utility and privacy in context-aware services

send(taxis in times square, DATA)
Other threats and mitigations

- Dynamic peering with unknown mobile network
- Ensuring fair resource allocation with multicast
- **Balancing utility and privacy in context-aware services**
Summary

- Mobility and security synergistic – mechanisms for one improve other, e.g.,
  - Unstructured names
  - Disruption-tolerance
  - Intentional/context-aware receipt
  - Management plane
- Design, evaluation, re-design cycle ongoing
Summary

- Designing for mobility also improves trust
- Key challenge is performance security
  - Ensuring graceful performance/availability degradation with malicious node presence
- Logically centralized decision making is easier to secure
Mobility = Trust

Mobility
- Unstructured = location-independent
- Performance
- Multihomed TE Geo-services
- Client-assisted Visibility+choice
- Mobile content Geo-services

Trust
- Unstructured = cryptographically verifiable
- Reliability
- DDoS Usability
- Security
- Usability Emergency
- Disruption tolerance
- Intentional receipt
- Management plane
- Context-awareness
MobilityFirst Design Goals

1. Host + network mobility
2. No global root of trust
3. Intentional data receipt
4. Proportional robustness
5. Content addressability
6. Evolvable network
Location Service: **Scalability to billions of mobiles**

- **Function:** Resolve GUID $\rightarrow [\text{NA}_1, \text{NA}_2,...]$  
- **Scale:** 10B devices, 100 networks/day $\leftrightarrow 10M/\text{sec}$

- **Metrics:**
  1. Query/Update delay (<50ms)
  2. Response staleness (<500ms)
  3. Load balance
  4. Fault tolerance
Location Service: Scalability to billions of mobiles

- **Function:** Resolve Host → [NA\(_1\), NA\(_2\),...]
- **Scale:** 10B devices, 100 networks/day ↔ 10M/sec

**Design issues:**
1. In-situ routing deflection (?)
2. Structured local scope IDs (?)
3. Network anycast to root servers
4. Context-based addressing
Proportional robustness (1)

**Goal:** A small number of malicious nodes must not be able to disproportionately impact network performance/availability

**Approach for naming:**
- Byzantine-fault tolerant (BFT) name certification and location service
- BFT both within and across name service providers
Proportional robustness (2)

**Goal**: A small number of malicious nodes must not be able to disproportionately impact network performance/availability

**Approach for routing:**

1. **Multipath routing and congestion control**
2. Disruption-tolerance
3. Storage-aware routing
4. Logically centralizing decisions with network-wide impact
   - **Intradomain**: Aggregate network-wide information centrally, compute routes, and disseminate to routers
   - **Interdomain**: BFT “consensus routing”
Proportional robustness (2)

**Goal:** A small number of malicious nodes must not be able to disproportionately impact network performance/availability

**Approach for routing:**

1. **Multipath**
   - Well-connected (wired networks)

2. **Disruption-tolerance**
   - A. Hop-by-hop transport
   - B. Uncertainty-driven replication routing

3. **Storage-aware routing**

4. **Logically centralizing decisions with network-wide impact**
   - A. Intradomain: Aggregate network-wide information centrally, compute routes, and disseminate to routers
   - B. Interdomain: BFT “consensus routing”

Well-connected (wired networks): WiFi, Cellular, WiMax, LTE

Sparsely-connected (Mobile DTNs): Connectivity
**Intentional receipt for DDoS**

**Goal:** Scalable fair resource allocation under DDoS

**Approach:**
- Packets carry unspoofable congestion policing feedback
- Congested routers use pair-wise keys for congestion policing feedback that receivers use as capability tokens
- Access routers police senders’ traffic to guarantee per-sender fairness without per-sender queues