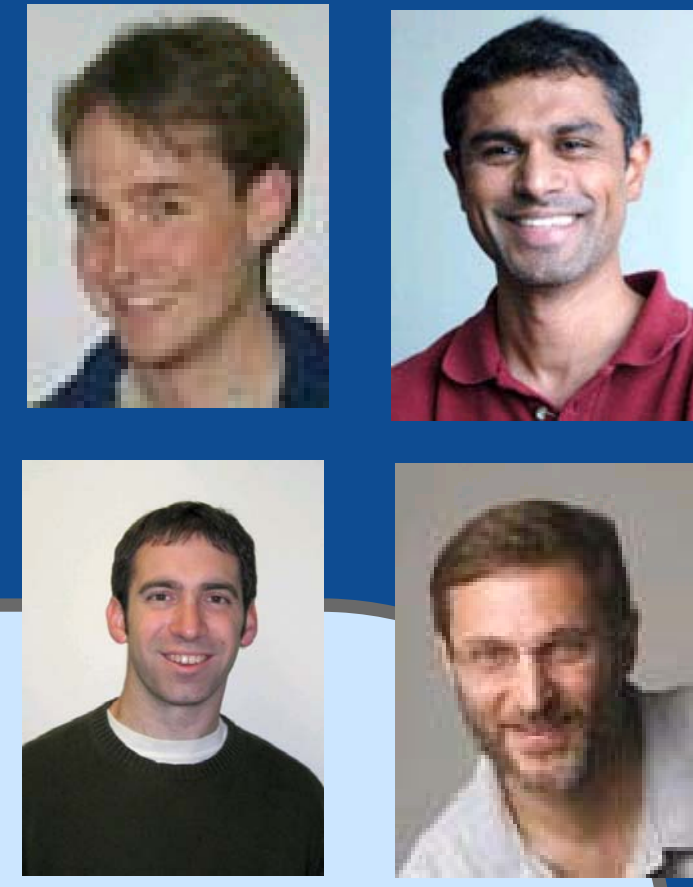


Accountable Internet Protocol

David Andersen (CMU), Hari Balakrishnan (MIT),
Nick Feamster (Georgia Tech), Scott Shenker (UC Berkeley)



Summary

Intrinsic support for network-layer accountability in the Internet

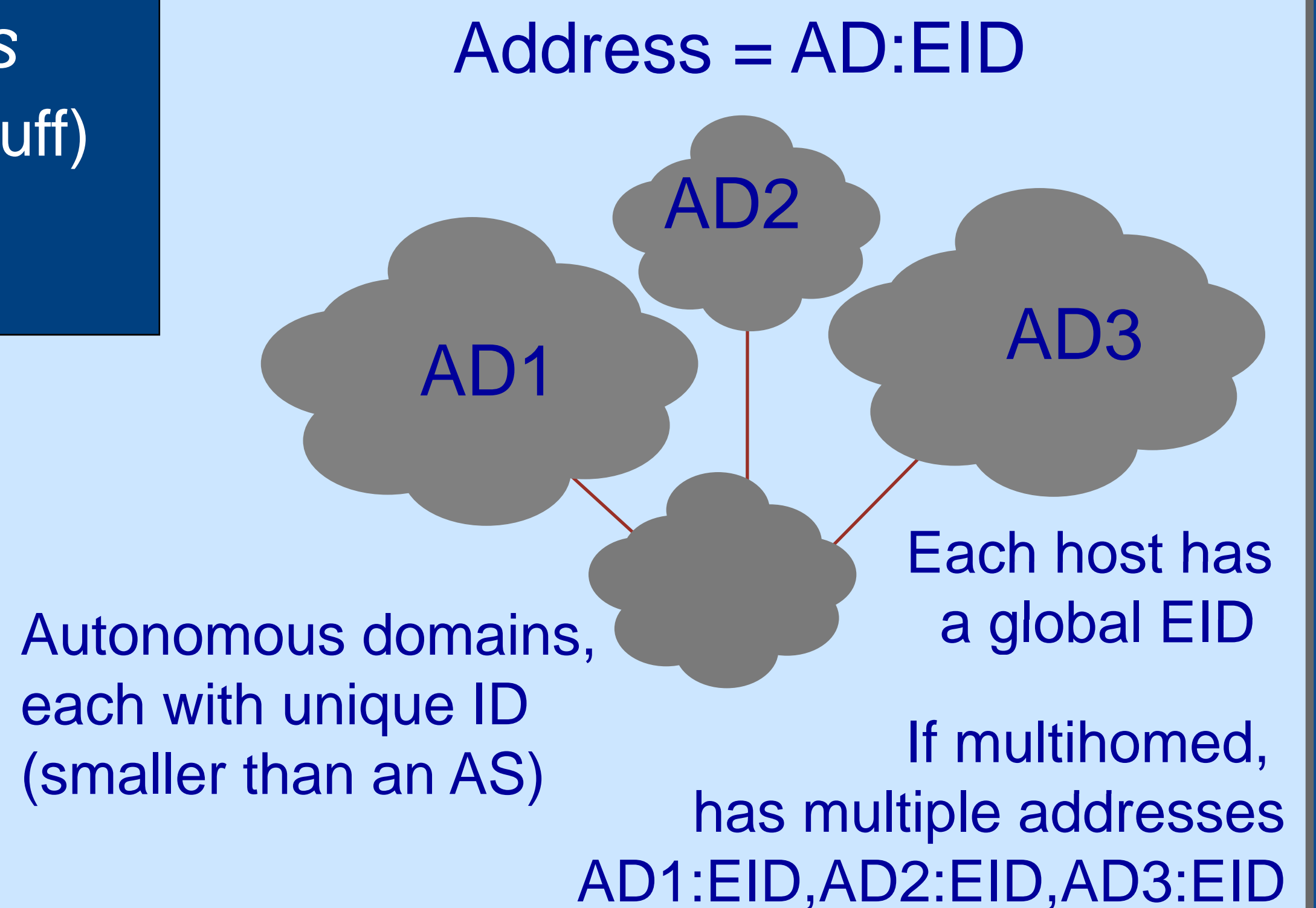
Main idea: New addressing scheme for networks and hosts

AD and EID: *self-certifying flat names*

- AD = hash(public_key_of_AD, other_stuff)
- Self-certification binds name to named entity

Two Types of Accountability

- **Control-plane accountability** improves security of the routing protocol
- **Source accountability** detects spoofing and forgery



Control-Plane Accountability

Origin authentication: Ensure routing prefix being originated by AS X actually belongs to X

Path authentication: Ensure accuracy of AS path

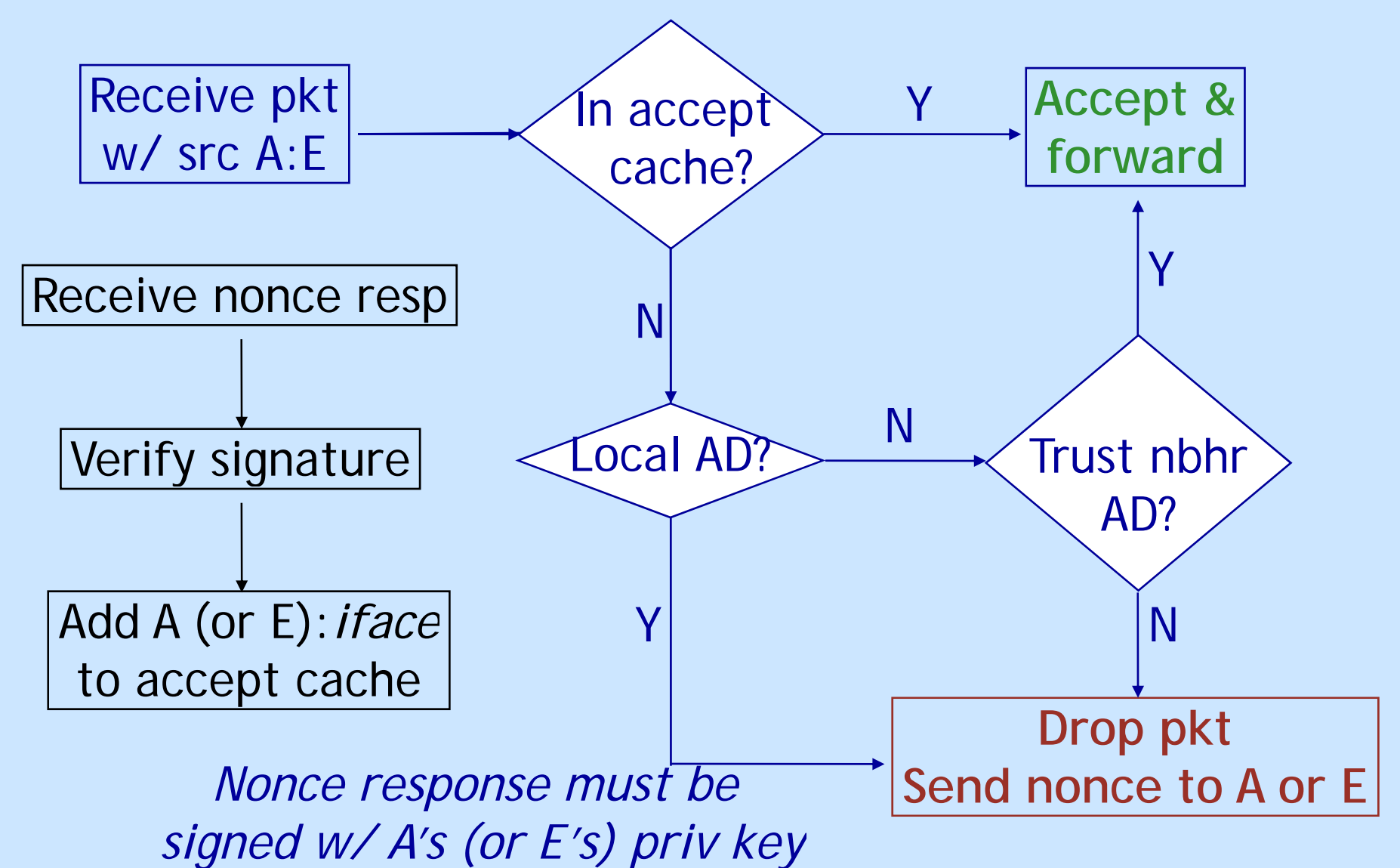
- **S-BGP (and soBGP) require external infrastructures**

Routing registry recording prefix ownership PKI (database) mapping AS to its public key. In practice, registries notoriously inaccurate

- **AIP: ADs exchange pub keys via BGP messages**

Path auth identical to S-BGP (but no PKI).
Origin authentication achieved without registry

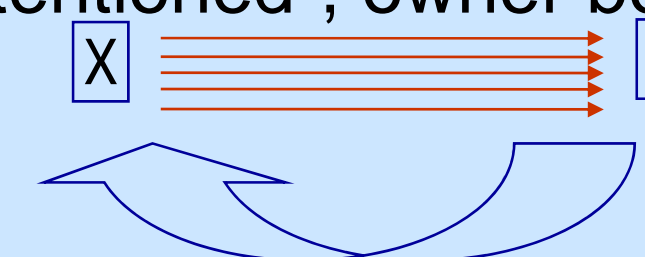
Data-Plane Accountability



Application: Shut-Off

Problem: Compromised host X sending unwanted traffic to D

(X is "well-intentioned", owner benign [Shaw])



Shut-off packet signed by D to X:
{time, D's pub key, hash of recent pkt recd from X by D, TTL}

- Can send shut-offs to hosts or to ADs
- Shut-off scheme implemented in NIC firmware
- Immutable by host software (updates require physical access via USB/serial port)

Challenges

- Minting of EIDs and ADs
- Key management and compromise
- Routing scalability
- Traffic engineering