Outline

- Drawbacks of Existing Hierarchical Tunnel Solutions
- Elements of a Flat Wireless Internet Service Provider
- Mobility Management
- Secure Binding of Assigned Address
- Conclusions
Existing Practice: Hierarchical Tunnels

Many UEs will be stationary; Most will be clients not servers and don’t need a fixed address
Typical Wireline Internet Service Provider

Network appears as one or more Autonomous Systems (AS) to the peers in the Internet; runs BGP

Multiple redundant points of connectivity to the Internet

Redundant aggregation routers act as IBGP route reflectors for the access layer

Technology-specific Network Access Servers facing customer lines

Shortcut link used in IGP (e.g., OSPF, EIGRP, IS-IS) but NOT an IBGP peering

IBGP Peering Relationships
Possible Future Wireless ISP

- Flat network of Base Stations
- Redundant upstream ISPs
- Redundant mesh of IP connectivity
- Not a strict hierarchy
- No single point of failure
- Blue routers are COTS
  - (vanilla wireline routers)
Mobility Management in a Flat Network

- Each BS owns a pool of addresses
- Mobile nodes attach/authenticate, get an address
- Upon attachment/authentication to new BS, send iBGP routing update with NLRI set to the already-assigned address
  - All iBGP routers will set the new BS as the next hop
    - Punches a hole in the routing tables
    - Update is limited in scope if movement is within the same route reflector cluster
IBGP Routing Update

1. UPDATE sent to parent aggregation routers
2. UPDATE reflected down to all access routers in the same cluster
3. UPDATE sent to core routers
4. Core routers make BGP policy decision and route traffic on direct path to new base station
5. Traffic from old base station may follow direct routing path if available
IBGP from an HA

MN that moved out of local AS

Home DNS Server(s)

Local Caching Resolver(s) and in-addr.arpa Server(s)

Aggregation

Core

Home Agent

BS

Access

BS

BS

BS

Access

BS

Access

BS

Access

BS

Access
Alternative Solution: Dynamic HA in the AR

- Assign original BS as a dynamic HA
- Send a Registration Request or Binding Update from the new point of attachment
- Inefficient if backhaul is expensive and scarce
- Requires MN to send IP packets at new BS

Original Point of Attachment (IP assigned from this local pool)

Traffic Traverses Backhaul 3 Times

Current Point of Attachment
Issues

- How does new BS learn about the already-assigned address?
- How does new BS guarantee the assignment is authentic?
- Answer: DNS
DNS storage of assigned address(es)

UE

my-ue.example.com

BS

BS learns MN’s DNS name & agrees on MSK

L-DNS

DHCP Address Assignment

H-DNS

Dynamic DNS Update

Mapping:
my-ue.example.com → 192.0.2.3
A Target eNB checks this to discover IP address

Mapping:
3.2.0.192.in-addr.arpa → my-ue.example.com
A Target eNB checks this to verify IP address
DNS retrieval of assigned address(es) during handoff

- UE
- eNB/L-GW
- L-DNS
- H-DNS

my-ue.example.com

Authentication

BS learns MN’s DNS name & agrees on MSK

DNS Lookup of my-ue.example.com

Mapping: my-ue.example.com → 192.0.2.3

DNS Lookup of 3.2.0.192.in-addr.arpa

Mapping: 3.2.0.192.in-addr.arpa → my-ue.example.com

iBGP Routing Update
Authentication without RADIUS/Diameter

- Round-trips to the home network add to latency of handover
- Leverage DANE work putting public keys into DNS
  - Public keys can be cached
- Re-run public key based authentication on every new attachment
Dynamic Re-Binding

- During quiet periods, MN should re-run DHCP to get a new address that is local to the current BS
- MN must keep track of which connections are using which addresses
  - Keep renewing the lease of used addresses (unicast DHCPREQUEST)
    - Remotely from current BS: the BS must add the Agent Remote ID
  - Garbage collect unused addresses & remove from Home DNS entry
Data Point: BGP Pass-through Time

- How fast does a BGP Update propagate through the network?
- See “Measuring BGP Pass-Through Times” by Feldman, Kong, Maennel, and Tudor
- Time for a BGP Update to be processed and resulting Updates to be propagated (MRAI disabled):
  - Best case: 2.4 ms
  - Worst case: 400 ms
  - Variation due to 200ms polling interval in a particular BGP implementation
Conclusions

- Existing tunnel hierarchies are inefficient and unnecessary
- BGP is used in typical wireline ISP environments
- BGP Updates can be used to handle mobility events
  - Must limit the time and scope of mobility for scalability
  - MNs can re-bind to new IP addresses during periods of inactivity
  - Performance studies needed
- DNS names can be used as node identifiers
  - Leverage DNS as a mapping database to find current IP addresses
  - Leverage DANE for storage of public key material
  - Enhance authentication to remove AAA round-trips and eliminate transport of symmetric secret key material