Advances in Routing
RST-4310
Alvaro Retana (aretana@cisco.com)
IP Routing Deployment and Architecture

Objective

• Introduction of New Technology recently implemented or in development in Routing Protocols.
• Focus on Routing Mobility
  Network Mobility (NEMO)
  Mobile Ad-Hoc Networks (MANET)
Advances in Routing - Agenda

- Definition of the Problem Space
- Network Mobility (NEMO)
- Mobile Ad Hoc Networks (MANET)

Defining the Problem Space
Defining the Problem Space

- There are (at least) two different problem spaces
- Device/Network Mobility
  A host or network (including attached hosts) moves as a unit
  The host or network can always reach back to a “home” without worrying about bandwidth utilization, etc.
  Each host or network connects only to its upstream—no lateral connections

Defining the Problem Space

- Ad Hoc Mobility
  Hosts move independently
  If a network is going to move as a unit, hosts attached to it would be numbered in the same IP address space
  No “reach back” to any specific network is guaranteed
  Lateral connections between devices are common
Defining the Problem Space

• Device/Network Mobility
  
  *Mobile IP/Mobile Router/NEMO (NEMO) fit these requirements*
  
  Reach back can be problematic in a red/black world
  Reach back consumes limited bandwidth across networks
  Placing the “home agent” is a difficult puzzle to solve
  Lack of lateral connections between “trees”

• Ad Hoc
  
  *Mobile Ad Hoc Networks (MANET) fits these requirements*
  
  Ad hoc networks may have a major impact on upstream “clouds”
  Will take time to develop and deploy
  Scaling is a possible concern

Defining the Problem Space

• NEMO
  
  Large, relatively stable networks
  Guaranteed reachback
  Only one path out, or multiple “equally good” paths (optimum routing is not a requirement)

• MANETs can attach behind the NEMO
  
  Routing information has to float up the NEMO and be injected into routing at the edge
  The MANET only receives a default route (no optimal routing through the NEMO)
  Back doors cannot be used to route to NEMO devices
Defining the Problem Space

- **MANET**
  - Higher mobility (not the same thing as faster mobility)
  - No “home,” or no guaranteed reachback
  - Multihoming with optimal routing important
- **NEMOs can attached behind a MANET**
  - Reachback is through the MANET
  - The NEMO devices don’t see the MANET as anything out of the ordinary

**Defining the Problem Space**

- **Classify each device as MANET or NEMO**
  - Examine the environment and assumptions for each device or network
  - Compare these to the limitations and capabilities of each technology
- **Resolve the Technical Issues**
  - Make certain NEMOs have the ability to leak routing information upstream through the cloud
  - Discover the NEMO/MANET/infrastructure edge and respond correctly
IP Mobility: problem definition

Vertical Market Applications

Public Services
- Emergency services
- Police
- Fire Fighters

Armed Services
- Military: Army, Navy, Marines, NATO, UK DoD, etc.

Commercial Markets
- Package delivery fleets
- Trucking
- Rental fleets

Consumer Automotive
- Telematics
- Infotainment
- Railroads
Network Mobility (NEMO)

NEMO - Agenda

- Mobile IP Review
- What is NEMO?
- MIPv6/NEMO Operation
Mobile IPv4

Mobile IP is a Dynamic Routing Protocol where Mobile Devices Signal Their Own Routing Updates and Dynamic Tunnels are Used to Eliminate the Need for Host Route Propagation.

Mobile IPv4: Triangle Routing

- Inbound Traffic is sent to the home subnet
- The Home Agent intercepts the traffic while the mobile node is registered as away
- Traffic is tunneled to the COA and forwarded to MN
- Traffic from the mobile node is forwarded directly to the correspondent host via the FA
Mobile IPv6 Basic Operation

1) CareOf Address
   The Mobile Node obtains an address in the visited network by autoconfiguration and neighbor discovery

2) Bind Update
   The Mobile Node finds a Home Agent and negotiates a binding between CoA and Home Address

3) Tunnel and RO
   Packets are exchanged with the Correspondent Node via a reverse tunnel or directly using Route Optimization

What is NEMO?

“The NEMO Working Group is concerned with managing the mobility of an entire network, which changes, as a unit, its point of attachment to the Internet and thus its reachability in the topology. The mobile network includes one or more mobile routers (MRs) which connect it to the global Internet.

A mobile network is assumed to be a leaf network, i.e. it will not carry transit traffic. However, it could be multihomed, either with a single MR that has multiple attachments to the internet, or by using multiple MRs that attach the mobile network to the Internet.”

Network Mobility (nemo) IETF Working Group Charter
http://www.ietf.org/html.charters/nemo-charter.html
**Mobile Router: Roaming Scheme**

- **IPV6/V4 Mobile network**
- **IPV6 Mobile router**
- **IPV6 Roaming**
- **IPV6/V4 Home Network**
- **IPV6 Home Agent**

**Ideal topology**

**Reverse Routing Header**

- **New Routing Header: type 4**
- **Outer IPv6 header**
- **RRH Routing Header type 4**
- **Encapsulated IPv6 packet**

- Works with plain V6 hosts on both ends
- HOME Equivalent Privacy option via HA
- First MR or MN builds a tunnel with RRH
- Next MRs add the source to the RRH and overwrite source with their COA
- A combination of IP Routing in Infrastructure and On Demand Source Route in the mobile cloud to adapt faster to topology changes
Dynamic Home Agent Address Discovery

• Step 1: Each Home Agent receives Router Advertisement from all the other HAs on the Home Network using standard Neighbor Discovery protocol.

• Step 2: Each Home Agent maintains an ordered list of the Current Home Agents with their lifetime and preference.

• Step 3: The Mobile Router sends an ICMP Home Agent Discovery Request message to the Mobile IPv6 Home-Agents Anycast address.

• Step 4: The first HA to receive the message reply with an ICMP Home Agent Discovery Reply with the list of all the Global IP addresses of the Home Agents in the order of preference.
Dynamic Home Agent Address Discovery

- Step 5: The Mobile Router having acquired a Care Of Address by auto-configuration sends a Binding Update message to the first Home Agent in the list.
- Step 6: The Home Agent answers back with a Binding Acknowledgment message. It updates its Binding Cache table with the CoA of the Mobile Router.
- Step 7: A bidirectional tunnel is established between the Mobile Router and the Home Agent.

Mobile Network Sample Configuration

- Home Agent configuration:
  ```
  interface Ethernet1
  ipv6 address CABA:4::BB4/64
  ipv6 enable
  ipv6 mobile home-agent run
  ipv6 route D093::/64 CABA:4::10
  ```

- Mobile Router Configuration:
  ```
  ipv6 unicast-routing
  ipv6 mobile router
  home-network CABA:4::BB4/64
  home-address home-network ::9
  interface FastEthernet0/0
  ipv6 address autoconfig
  ipv6 enable
  ipv6 nd suppress-ra
  ipv6 mobile router-service roam
  interface FastEthernet1/0
  ipv6 address D093::1/64
  ipv6 enable
  ```
Mobile Tunnel Support (IPv4/IPv6 in IPv6)

- Configuration of IPv6 tunnel between the Mobile Router and its Home Agent.
- Both IPv4 and IPv6 traffics can go thru this mobile tunnel.
- The mobility being handled at the IPv6 level.

Tree Discovery

- Each Mobile router has only one COA (MIPV6)
- Each Mobile Router attaches to another one following rules that force Tree topology
  - Based on autonomous decision of each Mobile router
  - Based on Loop avoidance mechanism
Tree Discovery

- Addition of a Tree Information Option to Router Advertisement

```
0 1 2 3 4 5 6 7
8 9 0 1 2 3 4 5
6 7 8 9 0 1 2 3
4 5 6 7 8 9 0 1
+--------------------------------------------------+
<table>
<thead>
<tr>
<th>Type</th>
<th>Length - 5</th>
<th>Tree_IdCode</th>
<th>TreeDepth</th>
</tr>
</thead>
</table>
+--------------------------------------------------+
| FIN | Reserved | Bandwidth | DistTime |
| Def | TreeLength | RootToRootCap | PathCost |
+--------------------------------------------------+
```

Tree TLM Identification

Tree Group

Tree Discovery

```
0 1 2 3 4 5 6 7
8 9 0 1 2 3 4 5
6 7 8 9 0 1 2 3
4 5 6 7 8 9 0 1
+--------------------------------------------------+
<table>
<thead>
<tr>
<th>Type</th>
<th>Length - 5</th>
<th>Tree_IdCode</th>
<th>TreeDepth</th>
</tr>
</thead>
</table>
+--------------------------------------------------+
| FIN | Reserved | Bandwidth | DistTime |
| Def | TreeLength | RootToRootCap | PathCost |
+--------------------------------------------------+
```

Tree TLM Identification

Tree Group
Summary

• Support for IETF NEMO specifications
• Mobile Rrouter Trees allow for cascaded configurations
• Dynamic HA allow for Geographically dispersed Home Agents

References

• IETF NEMO Working Group
  [http://www.ietf.org/html.charters/nemo-charter.html]
• IETF Mobility for IPv6 Working Group
  [http://www.ietf.org/html.charters/mip6-charter.html]
• Selected NEMO Drafts:
  [http://www.ietf.org/internet-drafts/draft-ietf-nemo-basic-support-03.txt]
Mobile Ad Hoc Networks (MANET)

MANET - Agenda

- What is a MANET?
- Mobile OSPF
- Mobile BGP
“Ad Hoc Network”—A collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration.

What is a MANET?

• Characteristics
  - Host movement frequent
  - Topology change frequent
  - No infrastructure; multi-hop wireless links.
  - Data must be routed via intermediate nodes

• Applications
  - Personal area networking
  - Military environments
  - Civilian environments
  - Emergency operations
Routing and Mobility

• Issues
  Frequent route changes – arbitrary movement, changing topology
  Low bandwidth links
  Route Changes may be related to node movement (adjacency changes / hidden and exposed nodes)
  Low power/CPU nodes

• Requirements
  Decrease control overhead
  Find Short Routes
  Find “stable” routes (despite mobility)

Characteristics of MANETs (RFC2501)

• Dynamic topologies
  Nodes are free to move arbitrarily. Network topology may change randomly and rapidly at unpredictable times.

• Bandwidth-constrained, variable capacity links
  Wireless links have significantly lower capacity than their hardwired counterparts. After accounting for the effects of multiple access, fading, noise, and interference conditions, etc.; the actual throughput is often much less than a radio’s maximum transmission rate.

• Energy-constrained operation
  Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. Network & routing optimization must be cognizant of energy conservation.

• Limited physical security
  Mobile wireless networks are more prone to physical security threats (i.e. eavesdropping, spoofing, and DOS attacks) than hardwired networks.
Dynamic Topology

- Random interconnection
  - Minimal or no engineering
  - Low bandwidth links
- Constant or frequent change (motion)
  - Neighbor changes;
    - New neighbor may be less reliable connection
    - More reliable connection may be at lower bandwidth
  - Resulting information propagation (flooding)

Radio Characteristics

- Directional Antennae
  - Some radios send in a stated direction; have to send when peer is listening in that direction
- Varying signal strength, link quality
  - Route cost *should* take link quality into consideration
- Overlapping connectivity
  - No unifying concept like Designated Router
  - Haphazard connections
Radio regions overlap haphazardly

Energy-constrained Operation

- Some nodes (e.g. hand-held, or laptop devices) are powered by batteries
- Others (e.g. vehicle-based) may be able to rely on a “constant” power source
- Battery drain will influence a node’s ability to participate as a routing next-hop
  - You could suspend a node if it hasn’t participated in a MANET for some period of time, but then how do you wake it up when appropriate?
  - Route cost should take energy constraints into consideration
- Inefficient data link, MAC, or network layer design can result in additional packets being transmitted, hence, more battery power being consumed.
Limited Physical Security

- Radio transmission is inherently less secure than wired transmission
  - Easier to snoop or eavesdrop
- More susceptible to DoS attacks
- Detection avoidance for military applications

Routing Protocol Characteristics

- Proactive protocols (Description)
  - Traditional distributed shortest-path protocols
  - Maintain routes between every host pair at all times
  - Based on periodic/triggered updates; High routing overhead
- Proactive protocols (Trade Offs)
  - Always maintain routes
  - Little or no delay for route determination
  - Consume bandwidth to keep routes up-to-date
  - Maintain routes which may never be used
Routing Protocol Characteristics

- Reactive protocols (Description)
  Determine route if and when needed
  Source initiates route discovery

- Reactive protocols (Trade Offs)
  Lower overhead since routes are determined on demand
  Significant delay in route determination
  Employ flooding (global search)
  Control traffic may be bursty

MANET WG

- IETF WG chartered to bring into Experimental status a set of core routing protocols designed specifically for MANET
  Ad hoc On-Demand Distance Vector (AODV)
  Optimized Link State Routing Protocol (OLSR)
  Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)
  Dynamic Source Routing Protocol (DSR)
AODV

- Based on Destination-Sequenced Distance-Vector (DSDV) routing algorithm
- Routes are discovered as-needed by broadcasting a route-request (RREQ) through the network, and waiting on a unicast route-reply (RREP)
- Routes are maintained “as long as needed”
- Route errors are signaled by a Route Error (RERR) message to all effected destinations

Ad Hoc Distance Vector (AODV)

- A route between two nodes is found by sending an Route Request to a locality
  - Initial locality small, grows with failure
  - After that, a little larger than the locality target last found in
- Route Response sent
  - By target if necessary
  - By neighboring routing node if possible to “join” existing route
- Network stores the route
AODV Continued

- Each route is to a router
- Each route advertisement has a sequence number
  Originator bumps sequence number on new information
  Others bump only when withdrawing failed route
- Effect: we always know relative order of information
  No count to infinity
  No looping routes

AODV Analysis

- Opportunities
  Perhaps good in application in which devices interact with
  relatively small number of others
  Possibility of adding traffic engineering parameters
  Device knowledge minimized
- Issues
  Delay during route installation/change
  Heavy multicasting during network change
  Route authentication/authorization
## Optimized Link State Routing (OLSR)

- **Systems trade**
  - Some form routing backbone
  - Some act as “hosts”

- **As devices move**
  - Topological relationships change
  - Routes change
  - Backbone shape and composition changes

## OLSR Analysis

- **Opportunities**
  - Proactive: knows network up front
  - Parameters can be added for engineering
  - Minimizes distribution traffic for SPF protocol

- **Issues**
  - Every network change requires every router to do something
  - No hierarchical routing concept comparable to OSPF areas
How about the other protocols available?

LUNAR
MOSAIC
FISHEYE
ABR
TORA
LAR
SSA
STAR
LANMAR
ZRP
MobileMan
Ant

Why OSPF?

• Why not a MANET WG protocol?
  - No ‘optimal’ protocol
  - Performance depends on network scenario and application (traffic patterns)
  - Testing studies – not validated in real-world deployments
  - Experimental RFCs (Not standard!!)

• Advantages
  - Proactive protocol
  - Integration with existing networks – Devices can more easily migrate between a MANET and infrastructure network
  - Stability of code that comes from years of deployment and testing
  - Industry knowledge
  - Time to market
  - Standard protocol
Why OSPF?

• Baseline Requirements
  Protocol needs to be well known and widely deployed
  Protocol will integrate well with wireline networks
  Protocol will be able to provide input into a wireline routing protocols, and take new optimizations and capabilities as they are proposed and deployed
  Time to market is a consideration, a known working code base is a plus
  Field experience and familiarity are important

• We are working with OSPFv3 as our initial protocol
  All the modifications we are contemplating for OSPFv3 are possible in IS-IS
  EIGRP is also under consideration for future work

Why OSPF?

• Technical Challenges
  Consider normal link state operation:
    Discover Neighbors
    Verify Two Way Connectivity
    Exchange Link State Databases
    Flood New Information
  We need to optimize at each of these points
Mobile OSPF - Agenda

- Data Link Management System
- Incorporating L2 feedback into routing metrics
- Hybrid MANET Interface
- Incremental Hellos
- Optimized Flooding
- Temporary Link State Database
- Future Work

Project Raven – Phase I Features

- Data Link Management System
- Incorporating L2 feedback into routing metrics
- Hybrid MANET Interface
- Incremental Hellos
- Optimized Flooding
- Temporary Link State Database
- Support for IPv4 in OSPFv3

General Radio/RF Link Assumptions

- Radio detects & authenticates neighbors, reports neighbor joining/loss to router
- Data link rates range from 80 Kbps to 29 Mbps effective throughput
- Data link rates are dynamic, controlled by Radio
- RF bandwidth changes, assigned radio channel(s), etc. are controlled by radio (independent of router)

Basic Router-Radio Architecture

- Router-radio interface has what amounts to virtual circuits:
  - Each routing neighbor has a different data rate, managed by the radio
  - Therefore each neighbor must have its own windowed protocol, and it must be windowed to control rate
  - There must be separate QoS data structures per routing neighbor
  - PPPoE sessions are established between the router and the radio – a session for each neighbor
  - Radio detects and authenticates neighbors, reports neighbor joining or leaving (LOS) to router
Credit Based Flow Control

- **Design intent:**
  - Push delayed data back into router queues
  - Queues provide QoS support (priority, isolation)
- **Many similarities to TCP and LAPB**
  - Receiver offers credit to sender
  - Sender may send up to that amount
  - Credit in bytes (correlates to time)
- **Not a reliable protocol**
  - Retransmission at higher layers or application
Metrics reported by radio (L2 Feedback)

- Current Data Rate
- Maximum Data Rate of link technology/policy
- Relative Link Factor
  Intended as a radio-vendor-specific measure of link quality
- Resources
  A node specific value that represents a percentage of resources remaining that effect continued operation (e.g. battery power)
- Latency
  One-way propagation delay in milliseconds
- Metrics are used by OSPF to calculate route cost based on link quality

OSPF Link Local Signaling

- **OSPF Link-local Signaling**: backward-compatible technique to exchange arbitrary data on a link.
  A special data block is added at the end of OSPF packets (or right after the authentication data block).
  The LLS data block may be attached to OSPF Hellos and the DD packets.

### Options Field

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| L | AF | DC | R | N | MC | E | V6 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
OSPF Link Local Signaling

- The LLS data block may contain any type of arbitrary information in a TLV format.

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Checksum           |       LLS Data Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+  
|                                                           |
|                           LLS TLVs                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+  
```

Format of LLS Data Block

OSPF Link Local Signaling

Extended Options TLV

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Type = 1            |         Length = 4            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+  
|                       Extended Options                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+  
```

The E0-TLV
Hybrid MANET Interface

- Media (air) is multi-access, but may also behave as point-to-point (unidirectional antennas) with both exposed and hidden nodes.
- OSPF: Interface is modeled as point-to-multipoint.
  - Adjacencies treated as point-to-point
  - May take advantage of multi-access characteristics
  - Link metric can be set per neighbor

Incremental Hellos

- Objective: reduce the control overhead.
  - OSPF Hello Messages
    - Periodic
    - Overhead increases with rate
    - Overhead increases with the size and density of the network (neighbor list included in every Hello)
- OSPF: Incremental State Hellos (Don't include full neighbor list!)
  - Two-way connectivity check
  - Incrementally update as neighbor state changes
  - Compatible with Graceful Restart
  - Include information about capabilities (Overlapping Relays, Willingness)
The Hello Process

- OSPF discovers neighbors through multicast hello packets
- Each hello carries a list of neighbor’s we’ve heard from
  - Ensures two connectivity exists before building an adjacency
  - State increases with each additional neighbor
  - Constant state that’s not interesting to other neighbors
- We need to reduce this state, both a new neighbor discovery and normal operation

The Hello Process

- Replace the state with a state sequence
  - A small (32 bit) number
    - Indicates “current hello state”
- Each time the sender changes state
  - Include new information
  - Increment the state sequence
- Receiver can request a state update to synchronize
- Reduces the state carried in hellos to the minimum possible, while ensuring two way connectivity
Incremental Hellos - Details

• The original neighbor list should be kept for adjacency formation purposes.

The I-bit (in the Options Field) indicates only newly discovered neighbors are listed in the list of neighbors.

Options Field

1                      2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+--+--+--+--+--+--+--+
| | | | | | | | | | | | | | |I|L|AF|DC| R| N|MC| E|V6|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+--+--+--+--+--+--+--+

State Check Sequence TLV

Represents current state

SCS Number: A circular two octet unsigned integer indicating the current state of the transmitting device.

R: If set, this is a request for current state. (AKA Hello Request)

A: If set, this is a response to a request for current state.
Incremental Hellos - Details

- Neighbor Drop TLV
  Indicates previously adjacent neighbor(s) that have been removed from the list of known neighbors.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Type = 3          |           Length              |
|+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Dropped Neighbor(s)                     |
+---------------------------------------------------------------+
```

Optimized Flooding

- All new LSAs are flooded to all neighbors, except the one from which the advertisement was received – this behavior may result in duplication of information in some segments.
- OSPF: Overlapping Relays
  Use knowledge of two-hop neighborhood, allowing more intelligent flooding decisions and intelligent ACKing decisions to be made.
  Active Overlapping Relays (ORCA) immediately flood, while backups delay the flooding until successful transmission is confirmed.
  Algorithm used to select ORCAs is similar to OLSRs MPR Selection.
Standard OSPF Flooding

Overlapping Relays
Optimized Flooding

- New reachability and topology change information is flooded to all adjacent neighbors
  - Several copies of an LSA may reach a neighbor two hops away
  - This is wasteful of available bandwidth and processing power
- We need to optimize flooding

Optimized Flooding

- Find common “two hop” neighbors
  - Each neighbor advertises its willingness to become an active overlapping relay
  - WILL_NEVER means not to choose this neighbor
  - Heuristic based on the OLSR MPR selection algorithm
- Calculate minimum set of overlapping relays (ORCAs)
  - Pick one neighbor from each group of neighbors with the same “two hop” neighbors
  - Group neighbors based on their neighbor sets
Optimized Flooding

- Calculate minimum set of overlapping relays
  - Pick one neighbor from each group of neighbors with the same "two hop" neighbors
- Signal overlapping relays to flood LSAs
- When A floods a new LSA
  - D refloods to F
  - B refloods to E
  - C doesn’t reflood at all

- C automatically backs up B, since it’s not an ORCA
- When C receives the new LSA from A, it starts a “pushback timer”
  - When B refloods, this timer is stopped
  - If the timer expires, C assumes B is not operational, so it refloods
- This backup process prevents dynamic network conditions from causing database synchronization issues and thus, packet loss
Intelligent Acknowledgements

- Assume A floods a new LSA
  When B receives this LSA, it acknowledges its receipt
  B then refloods the LSA to C
  C sees the LSA to A
  A sees the reflood to C by B

- Why should B acknowledge A’s LSA if A is going to hear B’s reflood to C?
  If B is reflooding the LSA, A can assume B received it correctly

- A uses B’s reflood to C as an acknowledgement
  Cuts down on traffic on the wire
Overlapping Relays

Red – Active Relays for node 0

Tan – node 0 (point of calculation for Active Relays)

Yellow – other network nodes

Overlapping Relays – Details

• Active Overlapping Relay TLV

  Used by each speaker to convey its set of active overlapping relays.

  Relays Added - Number of active overlapping relays that are being added. Note that the number of active overlapping relays that are being dropped is then given by: \([(\text{Length} - 4)/4 - \text{Relays Added}]\).
Overlapping Relays – Details

- Willingness TLV

Each speaker conveys its willingness to serve as an active overlapping relay.

Willingness - 1 byte to indicate the willingness of the node to serve as an active overlapping relay for its peers.

- 0: WILL_NEVER
- 128: WILL_DEFAULT
- 255: WILL_ALWAYS

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Type = 5           |          Length = 4           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Willingness  |                  Reserved                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Overlapping Relays – Initial Results

![Graph showing initial results](image)
Temporary Link State Database

- Only LSAs from adjacent (> Exchange) neighbors are kept in local Link State Database.
- OSPF: Create a Temporary Link State Database to store LSAs received from non-adjacent neighbors.
  
  Listen in promiscuous mode
  
  Leverage these LSAs to reduce link state requests

Database Exchange

- Routers exchange their link state database (LSDB) to become fully adjacent
  
  Verify two way connectivity
  
  Exchange database descriptors
  
  Request LSAs as needed
- MANET connections may not last long
  
  Reduce adjacency build time
  
  Route across connection faster
- Reduce bandwidth required
  
  Hold information speculatively
  
  Synchronize over a longer period of time
Database Exchange

- Listen to new information while building adjacency
  - Hold until synchronized
  - Reduces data exchanged in database exchange
- Send a summary of the reachability information
  - Instant reachability through new neighbor
  - Schedule a full synchronization later
  - Neighbor state brought to FULL
- Synchronize databases
  - Out of band synchronization used for OSPF graceful restart

Mobile OSPF Future Work - Agenda

- Scalability Enhancements
- Reactive Route Discovery
- Contiguous Mobility
- Auto-Configuration
- Interaction with Infrastructure Networks
- Covert Mode
Scalability

- **Requirements**
  - reduce the amount of information to be stored
  - reduce the amount of information on the media

- **Solutions**
  - *Edge Detection*: dynamically limit the size of the SPT
  - *Fisheye Routing*: dynamically reduce the rate at which information is propagated as the distance to the source increases
  - *Database Synchronization Enhancements*: reduce the overhead when synchronizing with nodes that may have redundant information

Flooding Boundaries

- **Future Work**
  - In link state protocols, routers flood information about the state of their links to all other routers, carrying topology information to all the routers in the network
  - All the routers receiving the flooded link state information are said to be in the same flooding domain
  - We summarize topology information into reachability information at a flooding domain border
Flooding Boundaries

• Future Work
  • C advertises reachability to 10.1.1.0/24
    Information about connections between C, D, E, F, & G is hidden in the OSPF type 3
  • OSPF has manually configured flooding boundaries
    Area Border Routers
  • Flooding boundaries are critical to OSPF scaling in the real world
    Flooded topology information has more impact on convergence times than the number of reachable destinations (prefixes)

Flooding Boundaries

• Future Work
  • In MANET networks, flooding boundaries aren’t so well defined
    Based on the distance from the originator of the routing information?
    Based on edges detected in the network?
  • Edge detection and bounding flooding are two areas still under investigation
Reactive Route Discovery

- In some communication models (where local communications are highly dominant), it may be desirable to learn about remote destinations on a need to know basis only.

- Solution

  *Reactive OSPF*: Uses a Query LSA to search for destinations; creates an extra hierarchy level (zones) inside an OSPF area.

  draft-retana-reactive-ospf-00.txt

Contiguous Mobility

- While moving in the network, a node may find itself in a different domain.

- Solutions

  *Enhanced Neighbor Discovery*: ability to establish adjacencies with nodes in other domains

  *Auto Flooding Domain Detection and Join*: ability to change local characteristics and seamlessly join new domains (no IP address changes)
Auto-configuration

• Through noncontiguous mobility, a node may need to reconfigure (or receive initial configuration parameters) itself

• Solutions

   Discovery and Selection of DHCP Server: selection of “closest” server (to provide locally significant configuration)
   Dynamic DNS
   Auto-Configuration
   Application Continuity: ability of the applications to survive IP address changes

Interaction with Infrastructure Networks

• The MANET should integrate seamlessly with the infrastructure protocols.

• Solutions

   IPv4/IPv4 OSPFv3/OSPFv2 Border: maintain route characteristics between the two protocols (super backbone like behavior)
   Explore Mobility in other protocols (BGP, EIGRP, etc.)
Covert Mode

- Nodes may need to be silent (i.e. no transmissions), but still be able to receive traffic (and possibly transit it locally).

- Solution

  Covert Mode: reachability to a node ("node" may also define a group of network elements in a common transport) is maintained even though adjacency is not maintained.

Mobile BGP - Agenda

- Why Mobile BGP?
- Technical Challenges
- Promiscuous eBGP
- iBGP
- Routing Through the AS
- Reducing BGP’s Weight
Why Mobile BGP?

- **Administrative Separation**
  - In wired networks, BGP is used to separate administrative domains.
  - Any topological area under one administrative control is considered an autonomous system.
  - Autonomous systems are interconnected using BGP.
  - *In MANET networks, we anticipate the same need.*

- **Scaling Properties**
  - In wired networks, BGP is used to scale the routing domain.
  - Routes are carried through autonomous systems using BGP, rather than into the AS.
  - *In MANET networks, we anticipate the same need.*

Technical Challenges

- **BGP splits internetworking autonomous systems into two separate problems**

  - **eBGP**
    - Handles connections to other autonomous systems.
    - Heavy on policy.
    - Uses the AS Path to prevent routing loops (path vector routing protocol).

  - **iBGP**
    - Carries routes through the autonomous system.
    - Not designed to prevent routing loops.

- **We need to solve both cases**
Technical Challenges

• Neighbor Discovery
  BGP requires manually configured neighbors

• Routing Through the AS
  iBGP sessions are multihop
  If a router along the path doesn’t know how to reach the
  destination, routing fails

• Heavy Packet Formats
  BGP packets carry a lot of policy and other information

Promiscuous eBGP

• BGP requires that neighbors be manually configured
  This isn’t conducive to MANET environments
  We don’t know which neighbors will be in reach at any given
  time

• We can discover possible peers through various mechanisms
  IPv6 neighbor discovery
  Periodic polling on a well known multicast address
  ....

router bgp 65000
neighbor 10.1.1.1 remote-as 65001
Promiscuous eBGP

- Once a new peer is discovered, we can use promiscuous eBGP to build the peering relationship
  - Accept peering relationships without configuration
  - Effectively the same as automatically building a neighbor configuration on the fly from discovered information
  - Normal BGP state machine

- Security is critical in this process
  - We have to rely on outside security mechanisms, since BGP doesn’t have configured peers

iBGP

- iBGP is more difficult
  - Peer relationships are normally multihop
  - We need to detect possible iBGP peers
  - We need to detect autonomous system edges
  - We need to transmit BGP routing information optimally through the AS without route reflectors or other aids
Routing through the AS

- **Routing Flow**
  - A advertises 10.1.1.0/24 to B
  - B advertises 10.1.1.0/24 to D
  - D advertises 10.1.1.0/24 to E

- **Traffic Flow**
  - E sends a packet to 10.1.1.1 via D
  - D sends it to C, its next hop towards B
  - C has no information about 10.1.1.0/24, so it drops the packet

Routing Through the AS

- **The Wired Resolution**
  - Make C a route reflector, so it has full routing information
  - Synchronize the iBGP and IGP routing tables through redistribution
  - Make the AS a single hop deep

- **Possible MANET Solutions**
  - Tunnel the packet from D to B
  - Conditionally inject information about 10.1.1.0/24 into the IGP
  - Both of these solutions may be useful in different situations, so both may be considered
Reducing BGP’s Weight

• BGP carries a large number of attributes
  - Local Preference
  - MED
  - Origination Code
  - AS Path
  - Communities
• BGP requires a lot of processing to run the bestpath algorithm
  - 14 step process
• We would like to reduce BGP’s weight in both of these areas

Reducing BGP’s Weight

• Cost Community
  - At the inbound edge, convert to a single community containing all metrics
    - MED, Local Preference, AS Path length compiled into a single number carried in a community
  - Drop attributes through the iBGP cloud
    - Drop MED, Local Preference, and Origin
    - Keep AS Path and communities
  - Run bestpath as a single number compare among cost communities
  - At the outbound edge, convert back to BGP attributes
Summary

- MANET is an ongoing area of research.
- Continuous development to meet increasing and changing mobility demands.
- Objective is to provide a “wired-compatible” solution.
- Other protocols may also be extended.

References

- AODV - [http://www.ietf.org/rfc/rfc3561.txt](http://www.ietf.org/rfc/rfc3561.txt)
References


Q AND A
Complete Your Online Session Evaluation!

**WHAT:** Complete an online session evaluation and your name will be entered into a daily drawing

**WHY:** Win fabulous prizes! Give us your feedback!

**WHERE:** Go to the Internet stations located throughout the Convention Center

**HOW:** Winners will be posted on the onsite Networkers Website; four winners per day