Related Work: Reverse-DNS Prefix Naming

- A mechanism to name a CIDR prefix in the Reverse DNS. Data records associated with that prefix enable a variety of useful applications
  - authenticated geolocation for a prefix
  - devices/apps associated with a prefix
  - blacklist

- The naming convention will be discussed at DNSOP on Friday

- Routing verification is one of the applications making use of the naming convention
  - focus of the remainder of this discussion
What?

- BGP Data records published in the reverse-DNS to enable a variety of route verification applications
- 2 independent internet drafts:
  - draft-gersch-dnsop-revdns-cidr to define names for address blocks,
  - draft-gersch-grow-revdns-bgp to define record types

Why?

- A complement to RPKI
- Can deploy in a short time-frame with existing infrastructure
  - DNS already exists and is a world-wide distributed namespace with redundancy, resiliency, caching, near-real-time distribution, and cryptographic authentication
- flexible; new record types can be defined; e.g. a repository pointer, etc.
ROVER Design Model

Applications tailored to unique ISP Operations

ROVER Access Methods

DNS DNSSEC etc.
ROVER Design Model

Applications tailored to unique ISP Operations

Small set of methods:
- DNS Naming Convention
- Data Publishing Format
- Data Authentication
- “Best Effort” retrieval

ROVER Access Methods

DNS DNSSEC etc.
ROVER Design Model

Applications tailored to unique ISP Operations

ROVER Access Methods

DNS DNSSEC etc.

ISP Applications:
- verify routing DB
- build prefix filters
- interface to RTR
- real-time notification/block
- (exponential retry)

Small set of methods:
- Data Naming Convention
- Data Publishing Format
- Data Authentication
- “Best Effort” retrieval
ROVER Design Model

Applications tailored to unique ISP Operations

ROVER Access Methods

DNS DNSSEC etc.

ISP Applications:
- verify routing DB
- build prefix filters
- interface to RTR
- real-time notification/block
- (exponential retry)

Small set of methods:
- Data Naming Convention
- Data Publishing Format
- Data Authentication
- “Best Effort” retrieval

Foundations / Protocols
- pre-existing DNS infrastructure
- IN-ADDR.ARPA signed with DNSSEC
- redundancy/resiliency
- real-time updates
How is this different from RPKI?

- Uses existing technology and infrastructure to publish data
- Uses DNSSEC for authentication instead of certificates
- Different semantics and different operational model -- means it can do some things that RPKI can’t do, and RPKI can do some things that ROVER cannot do. Examples:
  - Rover can manage secure & non-participating customers delegations (see the next slide)
  - Different approach to legacy addresses
  - ISP’s can opt-in or out in near-real time
Example capability: management of customer participation

- Secure Customer X: 10.1/16
- Protected Customer Y: 10.2/16
- Non-Player Customer Z: 10.2/16
Some Comments we’ve heard

- The DNS idea has been tried several times before....*but much has changed or is new:*
  - DNSSEC is real now, IN-ADDR.ARPA is signed
  - the proposed CIDR naming convention gives a great deal of flexibility

- There is a cyclic dependency; besides, a low-level protocol shouldn’t depend on a higher level protocol
  - ROVER mechanism is “best-effort” only. A failure to retrieve data results in BGP working exactly as it does today
  - If necessary, applications can perform query-retries with exponential back-off
## Publicly Available Testbed
**ROVER.SECURE64.COM**

### BGP ROVER: Route Origin Verification

#### Organization Data found for 'frii.net'

- **Name**: FRII (Front Range Internet Inc.)
- **Address**: 3350 Eastbrook Drive, Fort Collins, CO 80525, UNITED STATES
- **Parent Network**: (click to re-display this page using parent info) - ARIN (American Registry for Internet Numbers)

#### AS Numbers associated with FRII

- AS22729 (FRII)
- AS6582 (FRII)

#### Networks registered to FRII

<table>
<thead>
<tr>
<th>CIDR address block</th>
<th>Zone creator (blank if not provisioned yet)</th>
</tr>
</thead>
<tbody>
<tr>
<td>216.17.128.0/17 (NET-FRII-1)</td>
<td>Expand</td>
</tr>
<tr>
<td>65.183.64.0/19 (NET-FRII-1)</td>
<td>Expand</td>
</tr>
<tr>
<td>2607:FA88::32 (NET-FRII-1)</td>
<td>Expand</td>
</tr>
</tbody>
</table>

#### BGPMON Advisory: Unregistered Networks announced from AS6582 (FRRI - Front Range Internet Inc.)

<table>
<thead>
<tr>
<th>CIDR address block</th>
<th>Zone creator (blank if not provisioned yet)</th>
</tr>
</thead>
<tbody>
<tr>
<td>69.2.128.0/19 assigned to WCSDS (Weld County School District Six)</td>
<td>Expand</td>
</tr>
</tbody>
</table>

---

Step 2: Click on a CIDR address block to create a zone and authorize routes within that block.

The "Expand" button displays a new table containing the next lower octet or IPv6 nibble.
ROVER testbed - creates zone files

Once submitted, it will be placed in the queue for live publication in the public shadow zone.
Real live signed data on the net

dig 1.m.17.216.in-addr.arpa.secure64.com +dnssec TYPE65401

;; flags: qr rd ra ad; QUERY: 1, ANSWER: 4, AUTHORITY: 3, ADDITIONAL: 5

;; ANSWER SECTION:
1.m.17.216.in-addr.arpa.secure64.com. 3600 IN TYPE65401  # 8 000019B6000007DB8
1.m.17.216.in-addr.arpa.secure64.com. 3600 IN TYPE65401  # 8 000019B6000000AE
1.m.17.216.in-addr.arpa.secure64.com. 3600 IN TYPE65401  # 8 000019B600000D1C
1.m.17.216.in-addr.arpa.secure64.com. 3600 IN RRSIG TYPE65401 7 8 3600 20120403090055 20120327080055 32438 1.m.17.216.in-addr.arpa.secure64.com. XUcmYfoZJ5KcvB/Igy7GXaSOg +HCWydyr9CgSomeKcUrVrhVg7wli+D5 kyORRTYuwUbcZRmdYgEERJNNVvPQHQkHncJ1lejfae23XQIlqA6zLi+v 9sNa+jdhwgihz3RsFn+i3eNjV +tjwdfjWcVmeODqJqdPgLnQOfi5ZsmU q0Y=

;; WHEN: Tue Mar 27 09:31:17 2012
;; MSG SIZE  rcvd: 929

(try it yourself!)
IETF considerations

- This is not a request for a new protocol
- Call to Action:
  - Determine the appropriate working group
  - Get IANA numbers for new record types
  - Obtain Expert Review to strengthen and improve the idea
  - Encourage ISPs to publish data in testbed and in the real IN-ADDR.ARPA
  - Encourage the development of applications tuned to ISP operations
Questions; Feedback?

- we will log these

- BAR-BOF:
  - Wednesday night at 8PM lobby bar
  - demos, get deeper into the technology explanation