IP Router-Alert Considerations and usage

draft-rahman-rtg-router-alert-considerations-03

Reshad Rahman
David Ward
Francois Le Faucheur
Ashok Narayanan
Cisco

Adrian Farrel
Old Dog Consulting

Tony Li
Redback

Francois Le Faucheur
flefauch@cisco.com

What is this all about?

- Problem Statement:
  - RAO security concerns & solutions not documented well
  - Some feel careful router implementation & careful deployment address the RAO security concerns
  - Most feel concerns are far from addressed
  - Practical questions remain unanswered:
    - Should IETF discourage use of RAO-based protocols in The Internet?
    - Should IETF discourage use of RAO-based protocol in all environments?
    - Should an operator block e2e RAO packets to protect itself?

RAO = IPv4 and IPv6 Router Alert Option

What is this all about?

- **Objective**: produce a BCP documenting:
  - The concerns
  - Recommendations on environments were RAO should not be used
  - Recommendations on environments were RAO may be used
  - Recommendations on Protection approaches for Service Providers
  - Guidelines for RAO implementation on routers

RAO = IPv4 and IPv6 Router Alert Option

What is this NOT about?

- This I-D does not discuss potential changes to the definition, or re-definition, of RAO
  - This is investigated in draft-narayanan-rtg-router-alert-extensions
- This I-D discusses situation based on current RAO definition and implementations

Changes 02→03

- Generalized the earlier recommendation that “new” protocols don’t use RAO end-to-end into a recommendation that applies both to “old” and “new” protocol

REPLACED:

- “it is RECOMMENDED that new end to end applications or protocols be developed without using IP Router Alert”

BY:

- “<u>it is RECOMMENDED that applications and protocols not be deployed with a dependency on processing of the Router Alert option (as currently specified) across independent administrative domains in the Internet</u>.”

Based on list discussion with Jukka

Use of Router Alert End-to-End in the Internet (Peer Model)

```
 --------         --------          --------          --------
/   A    \       /   B    \        /   C    \        /   D    \
| (*)    |       | (*)    |        | (*)    |        | (*)    |
| | |<============>| |<===============>| |<===============>| |    |
|  -     |       |  -     |        |  -     |        |  -     |
\        /       \        /        \        /        \        /
 --------         --------          --------          --------

(*)  closer examination of Router Alert option datagrams

<==>   flow of Router Alert option datagrams

Figure 1:  Use of Router Alert End-to-End in the Open Internet
          (Router Alert in Peer Model)
```

Changes 02→03

- Detailed several Models of Controlled Environments where “an application relying on exchange and handling of RAO packets MAY be safely deployed”:
  - Within an Administrative Domain
  - In Water-tight Overlay
  - In Water-tight Overlay at Two Levels
  - In Leak-Controlled Overlay Model

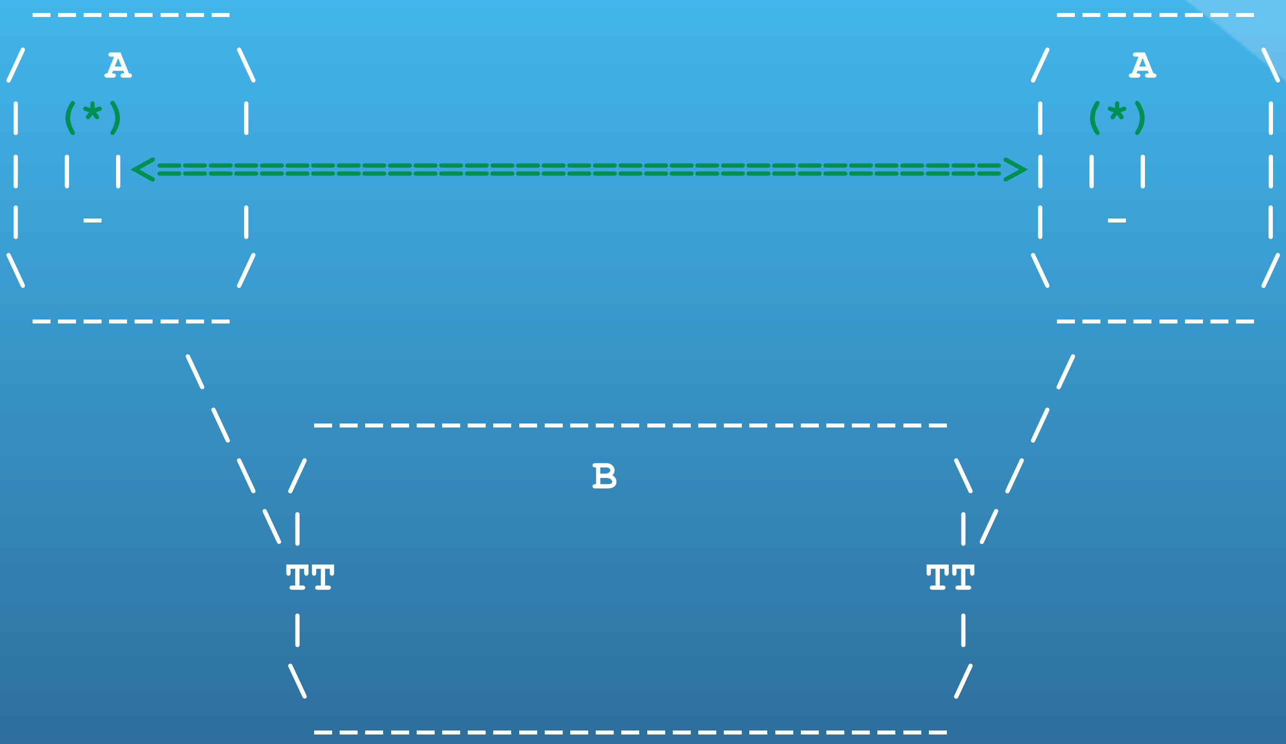
Use of Router Alert Within an Administrative Domain

```
   --------         --------------------------          --------
  /   A    \       /             B            \        /   C    \
  |        |       |  (*)             (*)   |        |        |
  |        |-------TT | |<=============>| |  TT------- |        |
  |        |       |   -                 -    |        |        |
  \        /       \                          /        \        /
   --------         --------------------------          --------


(*) closer examination of Router Alert option datagrams
<==>  flow of Router Alert option datagrams
TT   Tunneling of Router Alert option datagrams

    Figure 3: Use of Router Alert Within an Administrative Domain
```

Use of Router Alert In Water-Tight Overlay Model



(*) closer examination of Router Alert option datagrams
<==> flow of Router Alert option datagrams
TT Tunneling of Router Alert option datagrams

Figure 4: Use of Router Alert In Water-tight Overlay

Use of Router Alert In Water-Tight Overlay At Two Levels

```
 --------                                --------
/   A    \                              /   A    \
| (*)    |                              | (*)    |
| | |<=================================>| | |    |
|  -     |                              |  -     |
\        /                              \        /
 --------                                --------
       \                                 /
        \   -------------------------   /
         \ /           B             \ /
          \|  (*)              (*)   |/
           TT | |<============>| | TT
           |   -                -    |
           \                         /
            -------------------------
```

```
(*) closer examination of Router Alert option datagrams
<==>  flow of Router Alert option datagrams
TT   Tunneling of Router Alert option datagrams
```

Figure 5: Use of Router Alert In Water-tight Overlay at Two Levels

Changes 02→03

- Split the “Introduction” section into:
  - “Introduction” section
  - “Security Concerns of Router Alert” section
- Added a paragraph on IPv6 hop-by-hop options: *(*)*
  - Similar concerns apply
  - Outside the scope of this document
  - Reference to [I-D.krishnan-ipv6-hopbyhop]
- Added a paragraph on IPv4 options: *(*)*
  - Similar concerns apply
  - Outside the scope of this document
- Expanded discussion on use of Value field based on nsis-ntlp

(*) Based on discussion with Suresh & Jukka

Next Steps

- Proposal to turn this document in WG document ? (*)

(*) *Assuming IntArea WG is formed*

Back Up slides

The Fundamental RAO Concern

- Basic RAO semantic → alert router to more closely examine the contents of IP packet

- No convenient universal mechanism to accurately and reliably distinguish between “RAO packets of interest” and “unwanted RAO packets”.

→Potential RAO-based DOS attack

History

- Work started in Routing Area
- Recently moved to Internet-Area

IP Router Alert Documents

draft-rahman-rtg-router-alert-considerations-03

- Based on current RAO definition
- BCP Track
- Concerns & Recommendations

draft-narayanan-rtg-router-alert-extensions-00

- Explores enhanced RAO definition

Changes 01→02

- Adjusted structure for clarity and to provide clearer answers to the key RAO related questions:
  - we recommend new protos don't use RAO
  - it is OK for existing protos to use RAO in an umber of controlled environments
  - there are better ways for an SP to protect themselves than dropping RAO packets
  - router implementations should think about protection against RAO DOS
- In accordance with RTG WG feedback, remove the details on the various mechanisms that could be implemented by a router for RAO protection (those are implementation specific) and replace with generic recommendation (section 4)

Use of Router Alert Within an Administrative Domain

```
 -------------------------          --------          --------
/           A            \         /   B    \        /   C    \
| (*)                (*)  |   --   |         |       |         |
| |  |<=============>|  | |--|FW|--|         |-------|         |
|  -                 -    |   --   |         |       |         |
\                         /        \         /       \         /
 -------------------------          --------          --------
```

```
(*)  closer examination of Router Alert option datagrams

<==>   flow of Router Alert option datagrams

FW Firewall


    Figure 2: Use of Router Alert Within an Administrative Domain
```

Use of Router Alert In Leak-Controlled Overlay

```
   --------                                --------
  /   A    \                              /   A    \
  |        |                              |        |
  |        |   ------------------------   |        |
  | (*)    |  /(*)              (*)    \  | (*)    |
  | | |<======>| |<============>| |<=====>| | |    |
  |  -     |  | -                -     |  |  -     |
  \        /  |  \    -     -   /      |  \        /
   --------   |   TT-| |   | |-TT      |   --------
              |       -     -          |
              \                        /
               ------------------------


(*) closer examination of Router Alert option datagrams
<==>  flow of Router Alert option datagrams
TT   Tunneling of Router Alert option datagrams
```

Figure 6: Use of Router Alert In Leak-Controlled Overlay

Router Alert Protection Approaches for Service Providers

- →it is RECOMMENDED that a SP implements strong protection against RAO attack
- →it is RECOMMENDED that an SP uses mechanisms that avoid dropping of e2e RAO
- → SP may:
  - → Turn-off RAO punting (if does not depend on RAO)
  - → Use selective filtering and rate-limiting (e.g. to protect RSVP-TE)
  - → "Tunnel RAO" via mechanisms such as discussed in [I-D.dasmith-mpls-ip-options]
  - → As the very last resort, drop RAO packet

Guidelines for Router Implementation

- →It is RECOMMENDED that RAO implementations include protection mechanisms against RAO-based DOS attacks appropriate for their targeted environments
  - → e.g ability on an edge router to "tunnel" RAO as discussed in [I-D.dasmith-mpls-ip-options]
  - → e.g. new implementations may include selective (possibly dynamic) filtering and rate-limiting of RAO packets

- → A router implementation SHOULD forward within the "fast path" a packet carrying RAO containing a payload that is not of interest