Application Listener Discovery (ALD) for IPv6


james woodyatt <jhw@apple.com>
A Brief History of the End-to-end Principle in IPv6 Transition Planning
Firewalls vs. Transparency

- Access across boundaries denied by policy.
- Policy applied when flows actively initiated.
- Endpoint addresses imply policy.
- Transient interior listeners are invisible.
IPv4/NAT Firewall Transparency

- Stateful filtering of transport protocols: TCP, UDP, GRE, IPsec ESP, SCTP, DCCP, etc.
- Application layer gateways: IKE, PPTP, RTSP, FTP, SIP, etc.
- Manual port redirection.
- Dynamic hole-punching services: UPnP IGD, NAT-PMP, MIDCOM, NSIS, etc.
IPv6 Firewall
Transparency

- Stateful filtering of transport protocols: TCP, UDP, GRE, IPsec ESP, SCTP, DCCP, etc.
- Application transparency helpers: IKE, PPTP, RTSP, FTP, SIP, etc.
- Manual static configuration of policy.
- What about dynamic policy for transient interior listeners?
Um...
Salvage Operations

...retaining end-to-end transparency with IPv6 firewalls.

- Firewalls need to learn about transient interior listeners.
- Listeners need to learn about firewalls requiring notification.
- Nodes need to learn how to discover relevant firewalls.
Application Listener Discovery (ALD)

- Extension to ICMP.
- New router advertisement option.
- Existing sockets API sufficient for most applications.
- Some new system, interface and socket options for advanced requirements.
Router Advertisement

- Tells nodes where to send Firewall Solicitation messages
- Destination is either unicast or multicast.
- Hop-limit contributes to scope boundary.
Firewall Discovery

- Ask firewalls to send a unicast advertisement.
- Or... wait for multicast advertisements.
Firewall Advertisement

- Declare the interior prefix.
- Elapsed time since reset informs listeners that notifications may need to be resent.
Listener Notification

- Tells firewall about transport-specific address.
- Tells firewall how long application expects to listen.
- Retransmits until acknowledged.
Listener Acknowledge

- Tells listener to stop sending notifications.
- Duration constrained by firewall.
- Elapsed time since reset is same as in firewall advertisement.

**Listener Acknowledgment**

<table>
<thead>
<tr>
<th>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</th>
</tr>
</thead>
<tbody>
<tr>
<td>+-----------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>+-----------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>+-----------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>+-----------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
| +-----------------------------------------------------------------|...
Security Considerations

• ICMP6 source address implies listener source address.
• ALD does not specify firewall policy.
• IPsec w/IKE would be a useful extension.
Q & A

- Unmanaged networks behind firewalls.
- Application programming interfaces.
- Considerations for DHCPv6.
- Policy decision at firewalls.
- Policy decision at multiuser listening nodes.