Port set Type:
Contiguous vs. Non-Contiguous


Qi Sun
2013.3 Orlando
Motivation for port sharing

• IPv4 exhaustion
  – Several nodes share one IPv4 address by assigning non-overlapped port sets to each node
  – Providing IPv4 service without IPv4 routing on the provider IPv6 network

• Port set: Is contiguous port-set sufficient or do we need non-contiguous port-sets?
Back in Beijing Interim Meeting

From Ole’s slides

Mainly focus on statelessly mapping IPv4 address and port into IPv6 prefix
Comparison Points

- Security
- Preservation of Well-Known Ports
- Complexity
- Backwards Compatibility with uPnP IGD:1
Contiguous / Non-Contiguous Port Sets

- **Contiguous:** A single port range per-client
- **Non-Contiguous:** Multiple port ranges distributed evenly across port space per-client

**Bit Presentation**
- **Contiguous:**
  - Bit Presenta.on
  - Port Mask

- **Non-Contiguous:**
  - Bit Presenta.on
  - Port Mask

**Option format**

<table>
<thead>
<tr>
<th>Port Mask</th>
<th>GMA</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5</td>
<td>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5</td>
</tr>
<tr>
<td>+-----------------+-----------------+</td>
<td>+-----------------+-----------------+</td>
</tr>
<tr>
<td>OPTION_PORT_SET</td>
<td>option-length</td>
</tr>
<tr>
<td>Port Set Index</td>
<td></td>
</tr>
<tr>
<td>Port Set Mask</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Security

• Limited port range reduces port entropy -> it could be simpler for an attacker to guess ports
  – Source port randomization

• Ratio of address sharing increases -> the next port easier to predict
  – irrespective of whether it is contiguous or not

• Contiguous
  – Single port range: Predictable if allocation policy is known

• Non-Contiguous
  – Algorithmic port-set allocation: Predictable if allocation policy is known
Preserving Well-Known Ports

• Contiguous
  – Don’t assign PSIDs falling within the WKP range
  – WKPs only available for the first few PSIDs

• Non-Contiguous
  – a-bits (A > 0)
  – PSID can be arbitrary, so that ISPs won’t be required to exclude some of prefixes (as PSID is part of MAP IPv6 prefix)
  – WKPs only available for the first few PSIDs
Complexity

• Contiguous
  – Simple for CPE, Tunnel Concentrator, provisioning system, logging system, etc.
  – ‘Human readable’ format makes it easier to troubleshoot without tools

• Non-Contiguous
  – Brings complexity to all devices – CPE, server and clients (DHCP based)
  – Necessitates the use of tools to calculate allocated port ranges, complicating troubleshooting, logging, etc.
  – Could be hard to debug
Backward Compatibility to uPnP

• Mainly about IGD:1
  – No external port negotiation
  – Fail if external port unavailable

• Testing shows neither have good compatibility

• Probability for IGD:1 to work normally is the same for both port-set algorithms
## Summary

<table>
<thead>
<tr>
<th></th>
<th>Contiguous Port-set</th>
<th>Non-Contiguous Port-set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Predictable</td>
<td>Predictable</td>
</tr>
<tr>
<td></td>
<td>Sharing ratio increases -&gt; Easier to predict (RFC[6056])</td>
<td></td>
</tr>
<tr>
<td>Cost to Preserve WKP</td>
<td>Not allocate first few PSIDs</td>
<td>a-bit in port number (A &gt; 0) (PSID can be arbitrary)</td>
</tr>
<tr>
<td>Complexity</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Compatibility with IGD:1</td>
<td>Not Good</td>
<td>Not Good</td>
</tr>
</tbody>
</table>

- Non-contiguous port-sets offer little security with greater complexity.
- Conclusion: a simple contiguous port range, plus port randomization on the client side is preferable
For the WG

- Is contiguous port-set enough?
- Conclusion?