

Address Usage Recommendations

draft-gont-6man-address-usage-recommendations-02

F. Gont, G. Gont, M. Garcia Corbo , C. Huitema

IETF 98

March 30, 2017

Address Usage Problem

- Multiple Addresses: temporary and stable
- Outgoing address selection is well specified in RFC 6724
- Server address selection is not well specified
- Dominant practice: Bind(socket, [::]:<port>)

Issues with Bind(socket, [::]:<port>)

- Device presence
 - Private service bound to “stable” address,
 - Probe the service to see whether the device is on this network again
- Unexpected address discovery
 - Temporary address exposed in outgoing connections
 - Adversary probe range of service ports for that address
- Availability outside the expected scope
 - Service is meant to be local, e.g., only exposed through mDNS
 - But it is available in global scope

Alternative to Bind(socket, [::]:<port>) ?

- In theory, developers could
 - Enumerate all the addresses available on all interface
 - Pick the ones that fits the application's profile
 - Bind individual sockets to each selected address
- In practice, few developers do that
 - Requires tracking address changes
 - Requires testing address properties
 - Tends to not be portable
- And it may not even be available in “service level” API

Address Configuration issues

- Address Selection is performed by the application
- Address Configuration is performed by the system
- Several options are available
 - Configure stable addresses or not,
 - Configure temporary addresses or not,
 - Configure addresses globally for the system, versus by subsystem
 - Sandboxed browser, Container, Compartment...
- Configuration decision may depend on "profile" of the device or its operation mode:
 - trusted vs untrusted network, mobile node vs enterprise node etc.

Next steps

- Prepare revision
 - Get feedback, additional input
 - Better text
- Get working group consensus:
 - Is there interest for informational RFC documenting the issues?
 - Is there interest in BCP for “address configuration”?
 - Is there interest in proposed standard for “service address selection”?