Overview of Privacy Implications of IP Addresses

Fernando Gont

SI6 NETWORKS

PEARG Interim Meeting
January 19th, 2021

IPv6 Address Configuration
Background

Background

- 128-bit long addresses: /64 subnets, 64-bit Interface-IDs
- Address configuration mechanisms:
  - Manual configuration
  - SLAAC (mandatory)
  - DHCPv6 (optional)
- Mechanism to be used specified in Router Advertisements (RAs):
  - PIOs with A (“autonomous addr conf”) bit set → SLAAC
  - M (“Managed addr conf”) bit set → DHCPv6
  - PIO(A=1) + M=1 → unspecified, but typically **both** SLAAC + DHCPv6

Interface-ID Generation

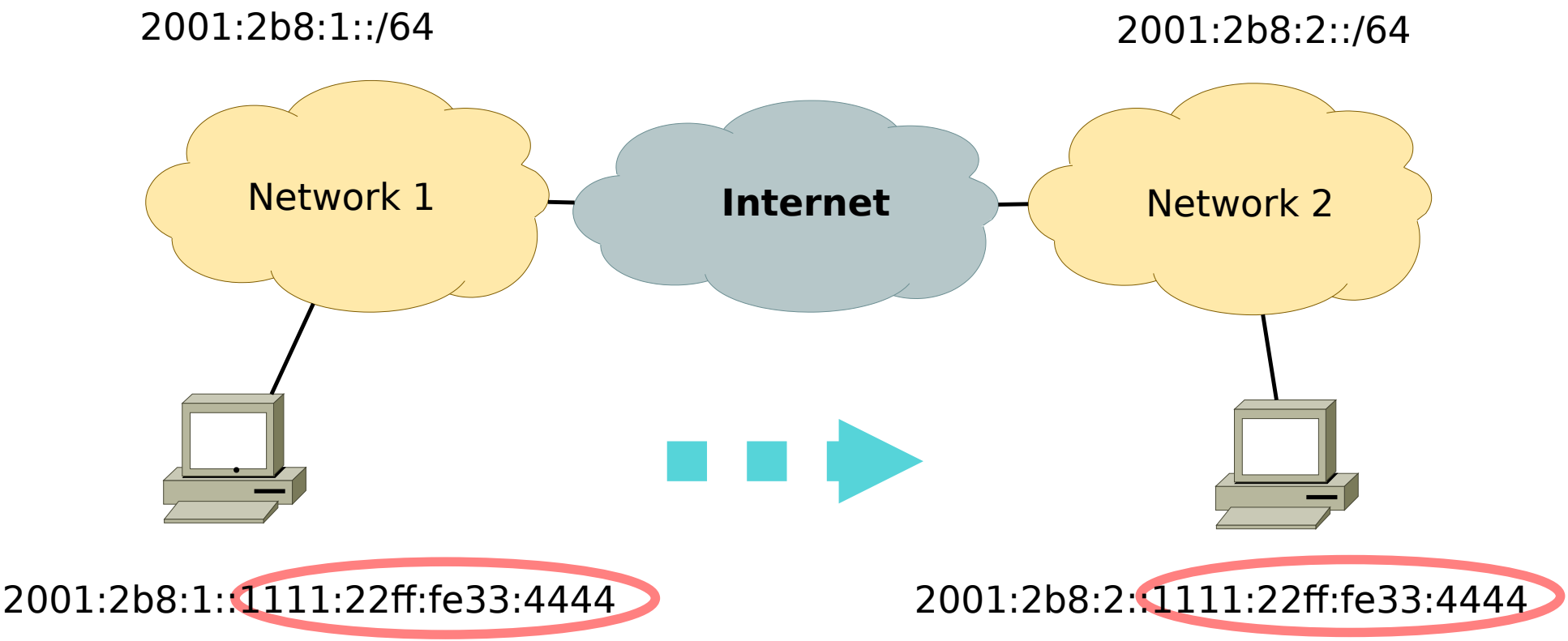
- SLAAC:
  - Legacy [RFC4291]: MAC address embedded in Interface-ID
  - Stable-privacy [RFC7217]: F(Prefix, secret)
  - Temporary [RFC4941]: randomized & regenerated over time
- DHCPv6:
  - Mostly unspecified, and hence implementation-specific
  - Typically: Linear sequence from small address pool

Privacy Implications of IPv6 Addresses

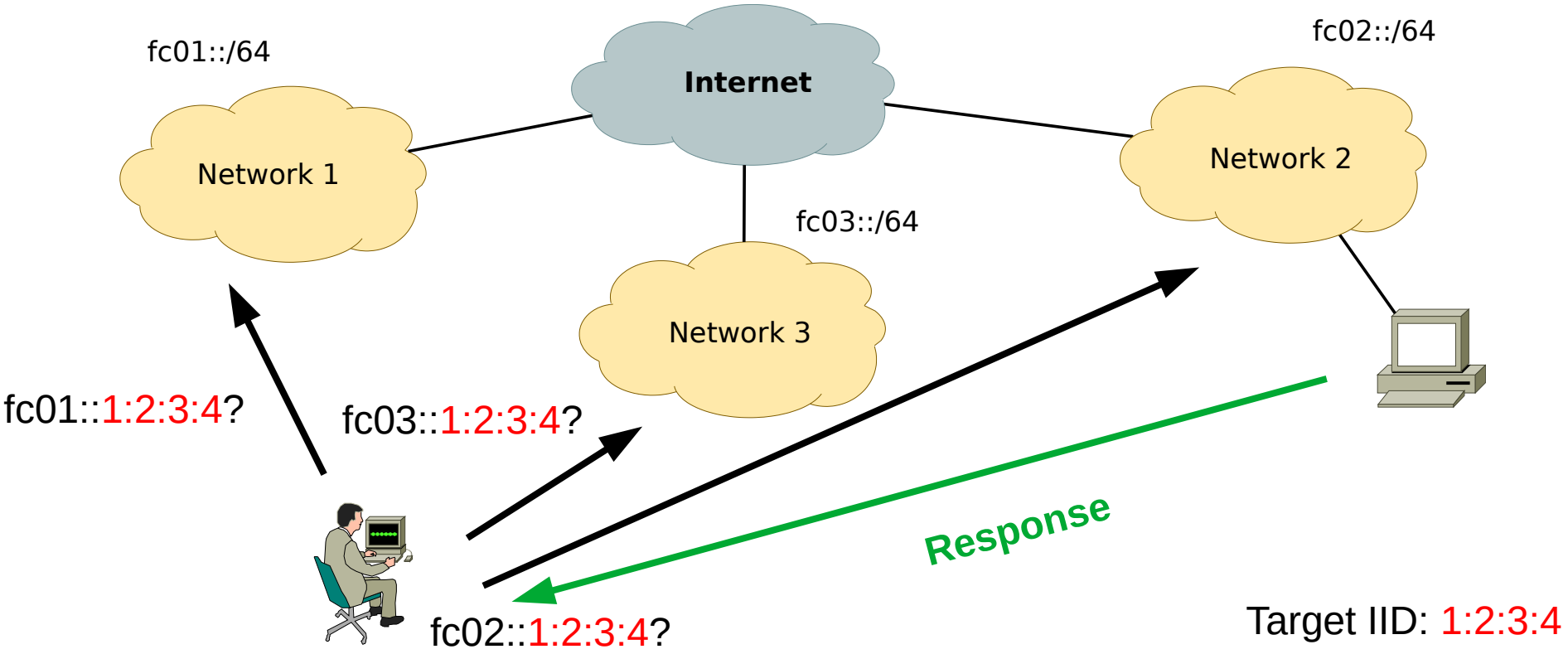
Privacy Implications of IPv6 Addresses

- Stability → network activity correlation
  - Network activity correlation possible for **as long as the same IID is used**
- IID patterns → Address scans
  - Address-based scanning attacks become feasible
- Overloaded semantics → unintended information disclosure
  - e.g. vendor information if a MAC address is embedded in the IID

Network Activity Correlation: Passive Attack



Network Activity Correlation: Active Attack



Address Scans

- IPv6 address scans originally considered unfeasible
  - search space considered huge (2^{64} addresses per subnet)
- Patterns in IIDs help reduce the search space
- Examples:
  - DHCPv6 server leases addresses from, say, PREFIX/112
  - Site manually sets IPv6 IIDs to the IPv4 address of the same network interface
- Tools exist to leverage IPv6 address patterns for address scans
  - See https://www.si6networks.com/tools/ipv6toolkit

Device-specific Attacks

- Legacy IIDs (RFC4291) disclose the underlying MAC address
- This could be leveraged to launch device-specific attacks

Privacy Implications of IPv6 Addresses

	Host-tracking	Correlation within subnet	Address-scans	Device-specific attacks
RFC4291	Yes	Yes	Yes	Yes
RFC7217	No	Yes	No	No
RFC4941	No	Moderate	No	No
MS Windows	Yes	Yes	No	No
DHCPv6 (*)	No	Yes	Yes	No

(*) Typical implementations

Caveats

- Must consider all address configuration mechanisms
  - e.g., both SLAAC and DHCPv6
- Must consider the implications of all addresses in use!
  - i.e., both stable and temporary
- Must consider stable prefixes in low host-density subnets
- Must consider MAC-address randomization

Privacy Implications of IPv4 Addresses

Properties of IPv4 Addresses

- NATed scenario:
  - IIDs not globally unique
  - Stable address shared among multiple nodes
- Non-NATed scenario:
  - IIDs not globally unique
  - Stable addresses

Privacy Implications of IPv4 Addresses

	Host-tracking	Correlation within subnet	Address-scans	Device-specific attacks
NATed	**No**	**Subnet-granularity**	**Tricky**	**No**
Non-NATed	**No**	**Yes**	**Yes**	**No**

Questions?

References

- “Security and Privacy Considerations for IPv6 Address Generation Mechanisms”. RFC7721.
- “Network Reconnaissance in IPv6 Networks”. RFC7707.