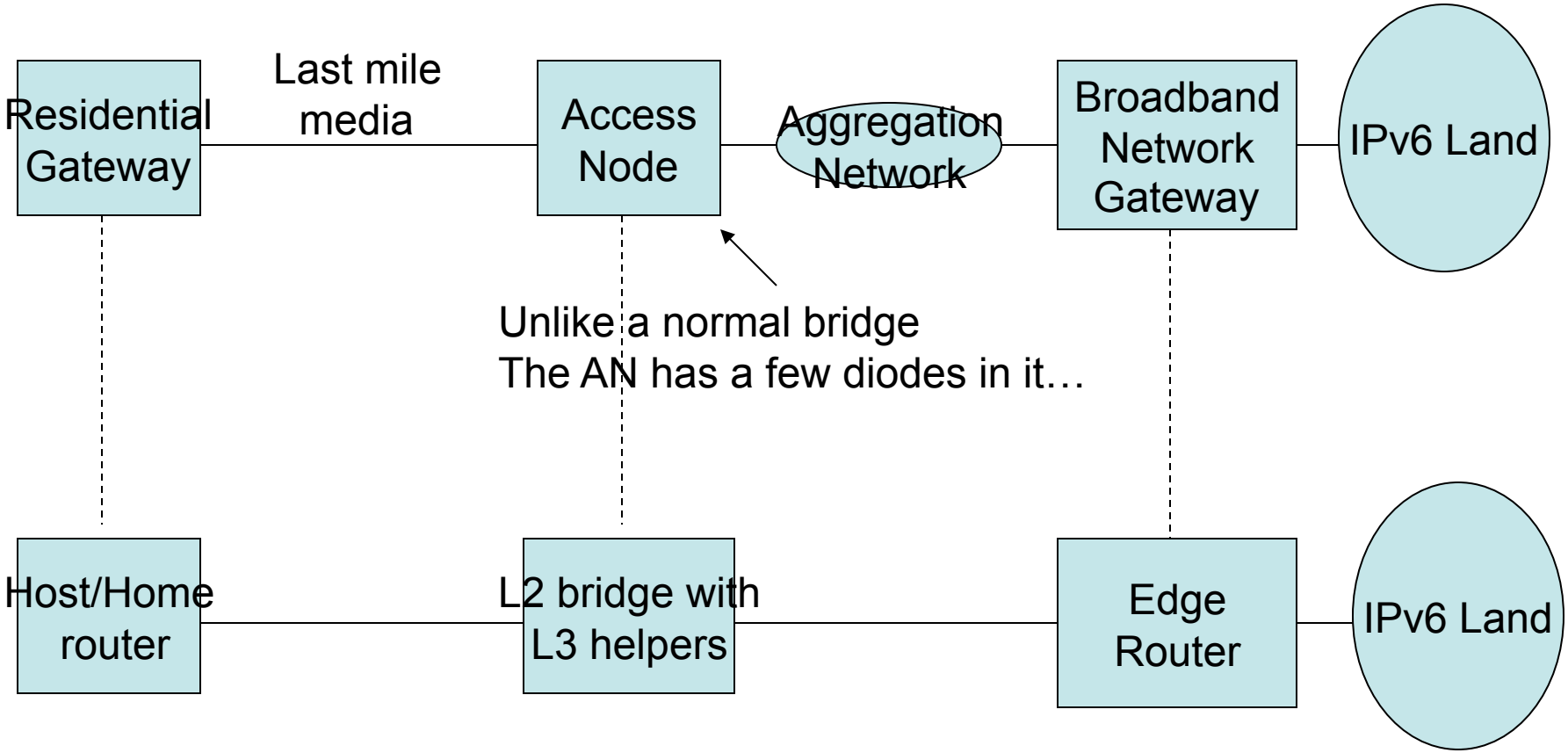
Mapping Terminology



Background
(From BBF 2009.877.01)

- In order to enable IPv6 connectivity, every host must first of all create a link-local address (of the range FE80::/64) in order to allow communication on a single link.

- The procedure for creating link-local addresses is defined in RFC 4862 [1]. When an IPv6 interface becomes active it will first concatenate it's Interface ID with the link-local prefix FF08::/64.

- The Interface ID for an Ethernet interface is derived from the EUI-64 identifier as spedified in RFC 2464 [2]. This 64-bit identifier in turn is derived from the 48-bit interface MAC address.
  - For example: an interface MAC address 00-1B-E9-58-B0-6D would be mapped to a 64-bit Interface ID 02-1B-E9-FF-FE-58-B0-6D. As a result, the link-local address would be FE80::21B:E9FF:FE58:B06D.

- Under such conditions, if the interface MAC address is unique, then the derived link-local address will also be unique.
  - Direct inheritance

Current state of the art in Uniqueness
(From BBF 2009.877.01)

- To protect against cases where the Interface ID would not be unique, IPv6 nodes test their address on the IPv6 link using Duplicate Address Detection (DAD). This test is performed to ensure uniqueness of the link-local address on the link. In case the Interface ID is derived from the MAC address, then link-local addresses should always be unique.

- The above procedures work well in a trusted environment. Contrary to a trusted network deployment, a broadband access network is generally an untrusted network:
  - a malicious user may try to spoof a link-local address (e.g. by connecting a PC to a bridged modem and configuring a specific link-local address on the PC)
  - a malicious user may try to flood the network with a large number of different link-local addresses, leading to a Denial of Service attack on the BNG
  - If two devices happen to have the same Ethernet MAC address as a consequence of incompetent manufacture, the link-local address derived for that interface will also be non-unique, provided it is derived from the EUI-64 identifier. This has been identified as an inconveniently frequent scenario (impacting ~4% of access nodes at any given time)

Complication
(From BBF 2009.877.01)

- Even if the customer equipment was benign and altruistic w.r.t. network behaviour, direct layer 2 user-to-user communication is controlled in a broadband access network by means of split-horizon forwarding, per TR-101.
- As a result, link-local connectivity only exists between the host and the BNG/edge router. There is no way for the individual hosts to know whether they are using duplicate link-local addresses as direct observation of neighbours traffic is precluded.
  - Editorial comment: This is not unique to BBF TR101, numerous link layers exhibit this behaviour (e.g. HFC or PON), and this can be virtualized at the networking level (e.g. MEF ETREE service definition, 802.1ad (2005) Asymmetric VID, 802.1ah/.1aq also support this model)

Consequences
(From BBF 2009.877.01)

- When deploying a plain IPv6 router that is not subscriber-aware, different hosts / RGs using the same link-local address would force the router to overwrite the corresponding entry in the Neighbor Cache. This can lead to a Theft of Service attack.

What is Needed
(From BBF 2009.877.01)

- When numerous hosts share an Ethernet broadcast domain, the BNG/edge router needs to support a mechanism that ensures duplicate link-local addresses can be handled correctly without necessarily depending on cooperative action by the hosts
  - it is explicitly required to do something to make this happen