draft-ietf-dna-link-information-05 Changes

- Removed text in normative language directed towards other SDOs
- Rewrite text about PDP contexts in GPRS
- Clarified that creation of secondary PDP context MUST NOT result in a link up event
- BSSID and SSID no longer a MUST in the auxiliary information for link up

draft-ietf-dna-link-information-05 Changes

- Added text regarding RSTP
- Rewrite text regarding effects of bridging
- New Security Considerations section
- Editorial changes

New Text (Secondary PDP context)

Successful establishment of a PDP Context on a GPRS link signifies the availability of IP service to the MT. Therefore, this link-layer event MUST generate a link up event notification sent to IP-layer. An MT has the possibility to establish a secondary PDP Context while re-using the IP configuration acquired from a previously established and active PDP Context. Such a secondary PDP Context does not provide additional information to IP-layer and only allows another QoS profile to be used. The activiation of a such secondary PDP Context MUST NOT generate another link up event notification. However, other additional PDP Context activiations are to be treated as indicated earlier.

New Text (Influence of Bridging)

Where it is not known that forwarding operations are available, a host SHOULD assume that RSTP or STP is being performed. Hosts MAY listen to STP/RSTP and 802.1AB messages to gain further information about the timing of full connectivity on the link, for example, to override an existing indication.

Notably, though, it is not easy for a host to distinguish between Disabled bridge ports and non-bridge ports with no active transmitters on them, as Disabled ports will have no traffic on them, and incur 100% sender loss.

If no bridge configuration messages are received within the Bridge_Max_Age interval (default 20s), then it is likely that there is no visible bridge whose port is enabled for bridging (S8.4.5 of [IEEE-802.1D]), since at least two BPDU hello messages would have been lost. Upon this timeout, a link up notification MUST be generated, if one has not been already.

New Text (BSSID/SSID to MAY)

BSSID and SSID MAY be provided as auxiliary information along with the link up notification. Unfortunately this information does not provide a deterministic indication of whether the IP-layer configuration MUST be changed upon movement. There is no standards-mandated one-to-one relation between the BSSID/SSID pairs and IP subnets.

New Text(Security Considerations)

Attackers may spoof various indications at the link-layer, or manipulate the physical medium directly in an effort to confuse the host about the state of the link-layer. For instance, attackers may spoof error messages or disturb the wireless medium to cause the host to move its connection elsewhere or to even disconnect. Attackers may also spoof information to make the host believe it has a connection when, in reality, it does not.

These attacks may cause use of non-preferred networks or even denial-of-service.

This specification does not provide any protection of its own for the the indications from the lower layers. But the vulnerabilities can be mitigated through the use of techniques in other parts of the protocol stack. In particular, it is RECOMMENDED that authentication, replay and integrity protection of link-layer management messages is enabled when available.

New Text(Security Considerations)

Additionally, the protocol stack may also use some network layer mechanisms to achieve partial protection. For instance, SEND [RFC 3971] could be used to confirm secure reachability with a router. However, network layer mechanisms are unable to deal with all problems, such as with insecure lower layer notifications that lead to the link not functioning properly