parc
A Xerox Company

Link negotiation

Marc Mosko (marc.mosko@parc.com)

ICNRG Iterim (Prague, CZ) July 19, 2015

Link negotiation (and maintenance)

- Examples from other protocols
- Assumptions
- Requirements for ICN
- Straw man protocol outline
- Moving forward

Other protocols

- FTP / HTTP
  - Exchange ASCII and “2xx, 3xx, 4xx, 5xx” codes
- TCP
  - Data offset (in 4-byte words) followed by 1-byte or TLV encoded options.
  - Options 1-way saying “this is what I will use or accept”
  - Some options only in setup others anytime
- NDNLPv2
  - 1-way mandatory and optional fields.
  - Sequence, NextHopFaceId, HopLimit, CachePolicy, NdnLpArq, NdnLpNack, NdnlpHmacSignature
- PPP Link Control Protocol (LCP)
  - Request / Ack / Nack / Reject protocol
  - Request a set of options, Ack lists those accepted, Nack lists those rejected, and Reject lists those not understood.
  - Also has close process and echo-response process for maintenance.
- Dynamic Link Exchange Protocol (DLEP)
  - https://tools.ietf.org/html/draft-ietf-manet-dlep-14
  - Init sends options, ACK lists accepted options.

Assumptions

- Protocol operation
  - Operates over CCN/NDN messages (including new link control messages)
- Priority and ordering
  - The network may re-order packets based on priority.
  - The network may re-order tunneled packets, even of same priority.
- Some environments might already do some of this
  - E.g. Dynamic Ad-hoc Wireless Networks or Mobile Adhoc Networks or Cellular
  - DLEP (https://tools.ietf.org/html/draft-ietf-manet-dlep-14)

Requirements (1)

- Security
  - Authentication and encryption need to be baked-in.
- L2 and L3 operation
  - Should operate over links or tunnels (e.g. UDP, GRE, VPN, etc.).
- Multiple-access links
  - Needs to scale to large multiple access networks, such as corporate or education networks with 100s of systems on a link.
  - How to bind the cryptographic identity to network endpoint.
- Link establishment and maintenance
  - Not only bring up a peer, but maintain the link.
  - Possibilities: loss rate, bandwidth estimation, delay estimation

Requirements (2)

- Multiple protocols and options
  - There may be multiple protocols that want to negotiate parameters
    - E.g. fragmentation, compression, key exchange, etc.
- Many types of options
  - Options defined by parent protocol, not link protocol
  - Mandatory vs optional vs unknown
  - Some options may be 1-way, some may require confirmation.

Straw man outline

- Pre-authentication
  - Setup mandatory encryption (e.g. DTLS or MACSEC).
  - Necessary early negotiation (e.g. MTU, fragmentation).
- Authentication
  - Securely exchange identities (may already be done via mandatory encryption step, or may be done in addition to it).
  - Setup optional on-going auth/encryption (e.g. hmac or GCM-AES)
- Post-authentication
  - Negotiate link protocol options.
- Data & Maintenance
  - Keepalive, teardown, periodic re-authentication or re-keying.

Moving forward

- Who's interested in working on this?
- Work outline for ICN Link Control Protocol (ICLCP)
  - Requirements document.
  - Specify a common ICN protocol.
    - Common protocol operation and messages.
    - Define the control plane and data plane.
    - Would wire format be the same?
  - Specify the nature of options (1-way vs confimed)
  - Specify in detail the low hanging fruit
    - Authentication, MTU, fragmentation, link quality, link termination over the ICLCP