PPP Working Group

Fred Baker, Chair

Agenda

- Steve Coya: ECP/CCP Patent Status Report
- Gerry Meyer: Encryption Control Protocol
  returned to WG by IESG
- Keith Sklower: Multilink Procedures
- Larry Blunk: Authentication Procedures
  ftp://merit.edu/pub/ppp/eap-draft.txt
- Badari Narayana: Public Key Authentication Proposal
  ftp://ftp.cisco.com/fred/draft-ietf-pppext-public-key-00.txt
- Glenn McGregor+ Gurdeep Singh Pall
  IP Control Protocol
  draft-ietf-pppext-ipcp-00.txt

PPP Encryption Control Protocol

- Encryption algorithm negotiated using PPP.
- Similar concept to Compression negotiation.
- Standard encryption algorithms.
- Manufacturer specific encryption algorithms (IEEE 802 OUI).
- Algorithm may be different in each direction.
- Negotiate above or below multilink (different protocol).
- Reset-Request and Reset-Ack.
- If negotiation fails - call is aborted.

ECP Issues Raised by the IESG

- draft-ietf-pppext-encryption-03.txt:
- Clarification of some text.
- OUI - Ethernet address prefixes a restriction.
- Role of IANA needing clarified.
- Specific (non-proprietary) encryption mechanisms

PPP Multilink: Doomed Chains

- M jumps to middle of a good packet chain.

```
Link1: -----[4x-5-----------[7------9---------------
Link2: ------------6]---10------11--------12]--[13--
Link3: [3]-----------------------------8------------
```

Time increases ---------->

[: has begin bit

]: has end bit

x: gets dropped

PPP Multilink: Doomed Chains

- M jumps exposing two doomed chains.

```
Link1: -----[4x-5-----------[7------10--------------
Link2: ------------6]---8x------11--------12]--[13--
Link3: [3]-----------------------------9------------
```

Time increases ---------->

[: has begin bit

]: has end bit

x: gets dropped

Public Key Authentication Proposal (PKAP)

- Badari Narayana - Novell
- Based on CHAP
- Implementation uses RSA Public Key Technology
- Playback Attack Avoidance
  - Incrementally changing identifier
  - Variable encrypt key value

PKAP Authentication Procedure Overview

- Authenticator:
  - Generates public key
  - Generates private key
  - Sends public key to Peer
    - Authentication Key Message
- Peer:
  - Encrypts public key using its private key
  - Sends encrypted public key to Authenticator
    - Authentication Request
- Authenticator:
  - Encrypts public key using its private key
  - Compares encrypted public keys
  - Send Authentication-Ack or Authentication- Reject

IP Control Protocol

- Glenn McGregor and Gurdeep Singh Pall
- Update to RFC 1332

IPCP Options Unchanged

- Type 1 IP Address option
  - removed
- IP-Compression-Protocol (Type 2)
  - no change
- Van Jacobson header compression
  - no change

IP-Address Option (type 3)

- Announcement of address:
  - Ack: “OK, you are that address”
  - Nak with address: “No, use this one”
  - Nak with 0.0.0.0: “I consider this an unnumbered link”
  - Reject: “huh?”
- Announce 0.0.0.0 = address request
  - Ack with 0.0.0.0: “I consider this an unnumbered link”
  - Nak with address: “use this one”
  - Reject: “huh?”

IP-Broadcast-Forwarding Option

- Supports Legacy Applications not converted to IP Multicast
- Augments Router/Serve Configuration
  - if router configured to forward, can disable forwarding
  - if router configured to not forward- what?
- Bit Mask= broadcast types requested
  - 00 No Broadcast forwarding (default)
  - 01 IP Broadcast forwarding
  - 02 IP Network Broadcast forwarding
  - 04 IP Sub-Network Broadcast forwarding