Authentication Extensions for the Dynamic Host Configuration Protocol

draft-pruss-dhcp-auth-dsl-00.txt
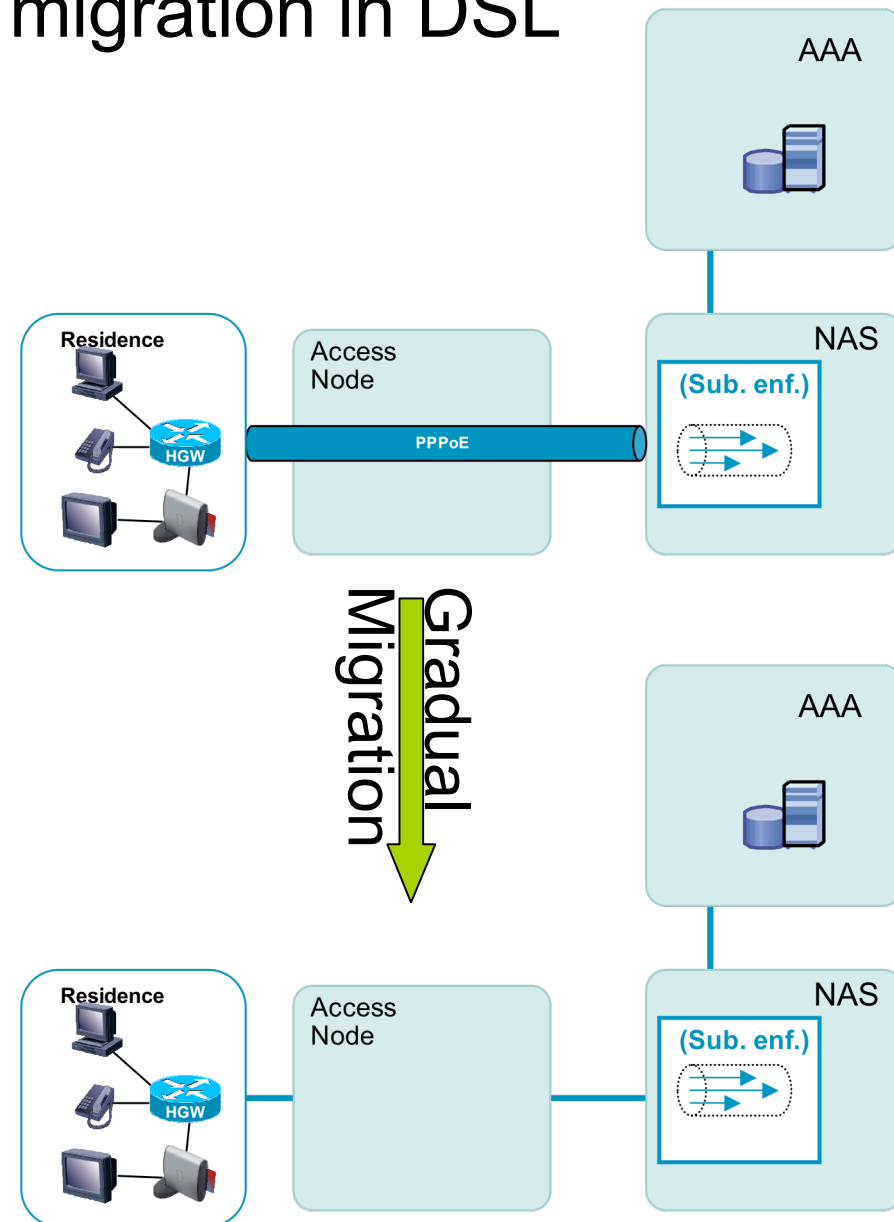
Ric Pruss (ric@cisco.com)

Problem space
Incremental PPP to IP migration in DSL

Gradual migration from ATM to Ethernet, and from PPPoE and PPPoA to "IP Sessions".

In order to simplify migration, protocol changes are necessary only where the PPP endpoints reside (NAS and HGW)
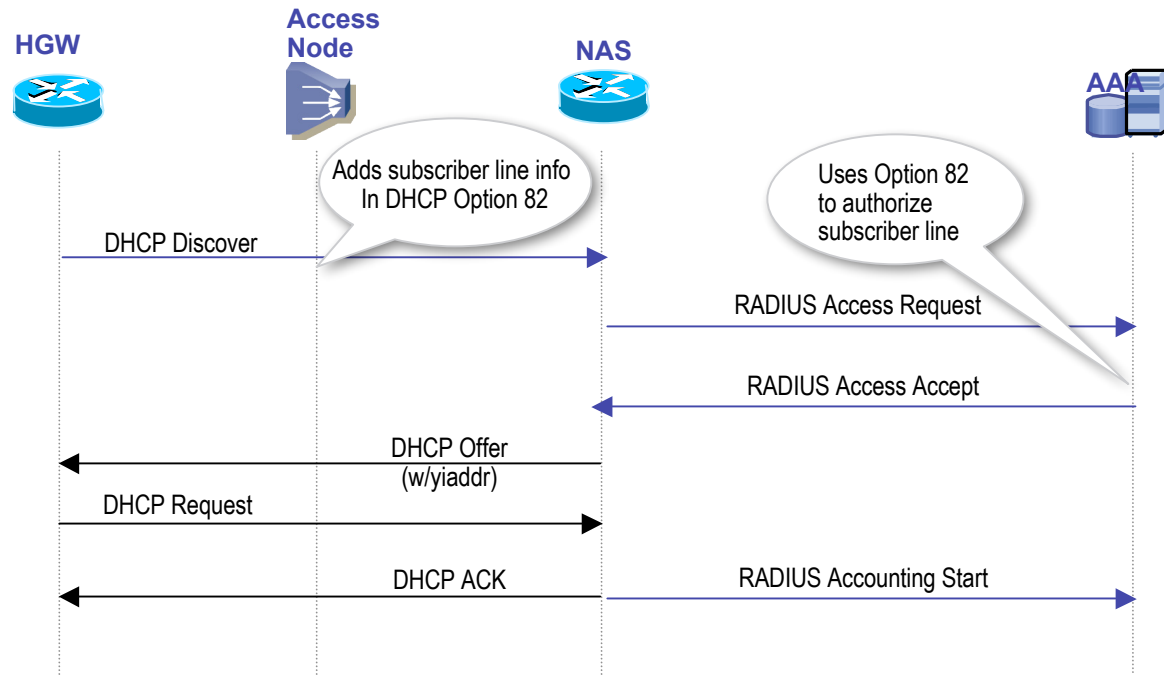
"DHCP Proxy" to AAA*

Host configuration provided by centralized AAA systems

RADIUS subscriber attributes are mapped to DHCP Options

Driven by the need to protect massive investments in custom AAA systems and back-end infrastructure

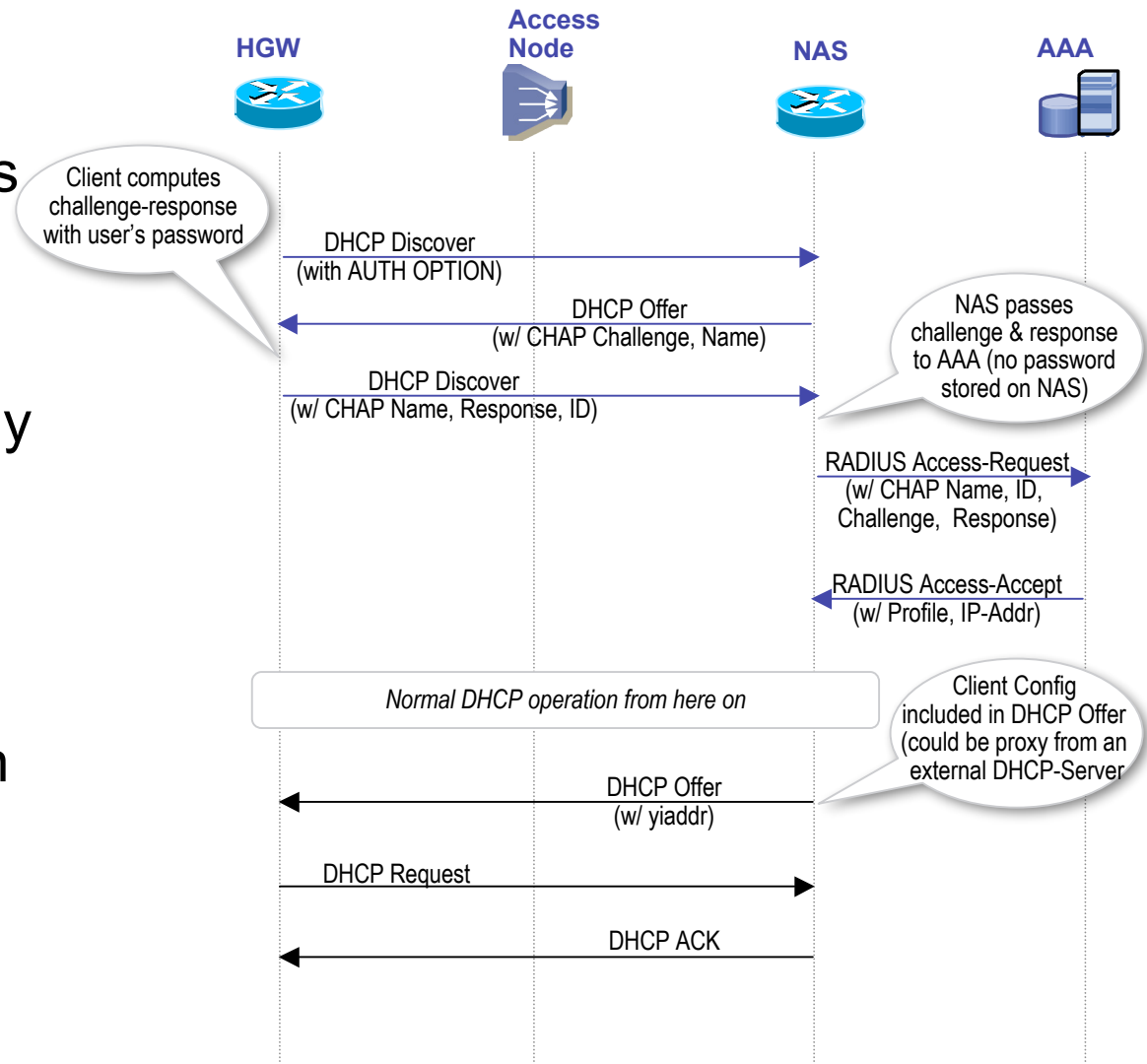* This function is available from a number of NAS vendors today

Relying on option 82 marking may not be sufficient in some cases:

- Migration existing Username/Password systems
- End user controlled retail ISP selection (@domain)
- Subscriber nomadicity
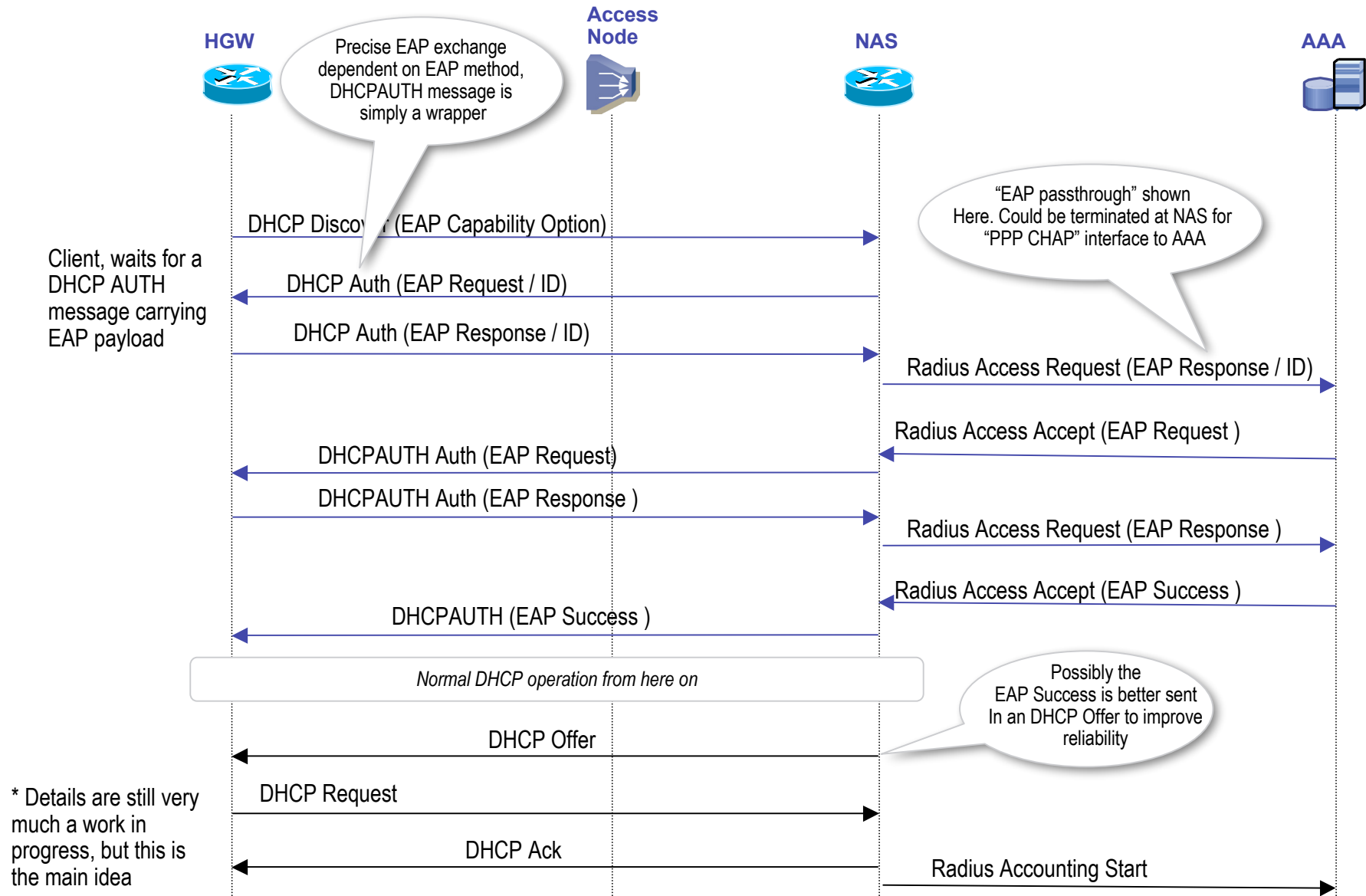- Line information at the Access Node may not always be reliable

Authentication Extensions for DHCP
(Option 1 - No new DHCP Messages)

- Same architecture as "DHCP Proxy to AAA" but with credentials from the HGW rather than only the Access Node
- Uses existing DHCP message set
- Defined only for CHAP authentication (for greatest compatibility with PPP-based AAA)

HGW   **Access Node**   **NAS**   **AAA**

Client computes challenge-response with user's password

DHCP Discover (with AUTH OPTION)

DHCP Offer (w/ CHAP Challenge, Name)

DHCP Discover (w/ CHAP Name, Response, ID)

NAS passes challenge & response to AAA (no password stored on NAS)

RADIUS Access-Request (w/ CHAP Name, ID, Challenge, Response)

RADIUS Access-Accept (w/ Profile, IP-Addr)

Normal DHCP operation from here on

Client Config included in DHCP Offer (could be proxy from an external DHCP-Server

DHCP Offer (w/ yiaddr)

DHCP Request

DHCP ACK

Authentication Extensions for DHCP
(Option 2* - EAP in new DHCPAUTH Message)

Questions