# The Network Discovery and Selection Problem

Draft-ietf-eap-netsel-problem-06.txt
Paul Congdon & Bernard Aboba
IEEE 802.1af
March 14, 2007

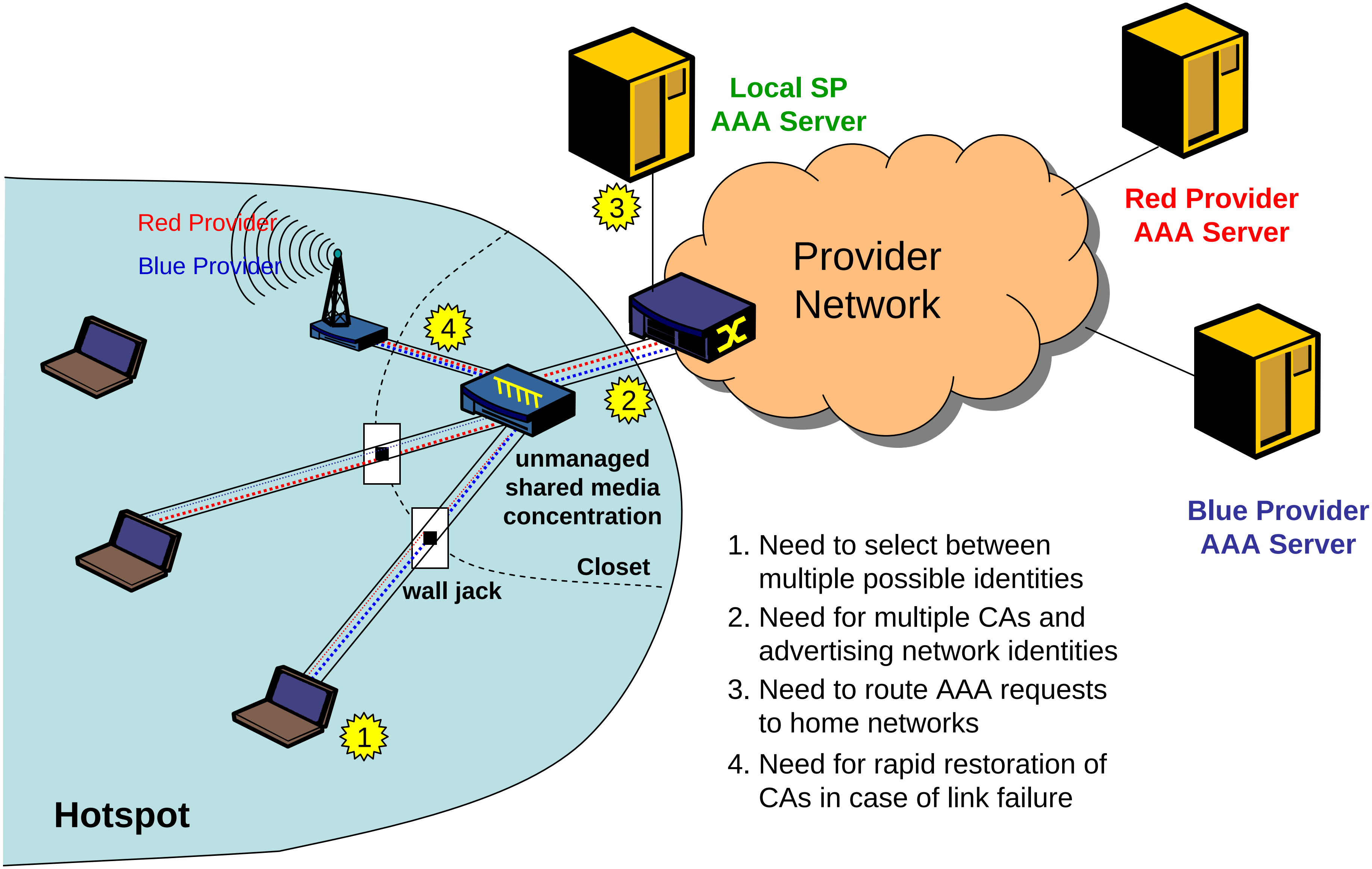
# Terminology

- Network Access Identifier (NAI)
  - The user identity submitted by the peer during network access authentication. The NAI consists of a userid (which may be missing or ‘anonymous’) and a realm, which identifies the home backend authentication server. Defined in RFC 4282.
- Network Discovery
  - Discovery of the access networks to which a host may connect, along with the capabilities of those networks.
- Realm Selection
  - Discovery of the backend authentication servers to which a host may authenticate from a given access network

# Issues in Network Discovery and Selection

- Access network selection
  - Which access network should be selected, if more than one is available?
- Identity selection
  - Which identity should be used for authentication?
- EAP method selection
  - Which EAP method should be used to authenticate with a given network?
- AAA route selection
  - What path should be used to reach the home backend authentication server?
  - Long term not the client's problem. Likely to be solved by AAA, not RFC 4284 Source Routing.

# A Complex Yet Demonstrative Scenario



1. Need to select between multiple possible identities
2. Need for multiple CAs and advertising network identities
3. Need to route AAA requests to home networks
4. Need for rapid restoration of CAs in case of link failure

# Access Network Selection

- Scenarios encountered in wireless networks:
  - Selecting between overlapping networks of different providers (e.g. RedProvider vs. BlueProvider)
  - Selecting between services offered to different user classes (e.g. GUEST vs. CORPNET)
  - Selecting between access mechanisms providing different security or QoS levels (e.g. WEP vs. WPA vs. WPA2 or WMM vs. IEEE 802.11e)
- Equivalent scenarios encountered in wired networks
  - PPPoE [RFC2516] Active Discovery messages enable discovery of a Service-Name along with capabilities.

# Identity Selection

- Users may have multiple identities (e.g. corporate, home, RedProvider, BlueProvider)
  - Identity may depend on the access network
  - Identity may depend on the EAP method
    - EAP-SIM Identity is different from EAP-TLS Identity.
- Wireless networks
  - Default EAP method (and associated Identity) typically configured for each network
- Wired networks
  - Where a network name is not available, a single global Identity (and EAP method) is typically configured.

# EAP Method Selection

- An EAP peer needs to determine which EAP method to use with an authenticator.
  - From [RFC3748] Section 7.8:
    - “Within or associated with each authenticator, it is not anticipated that a particular named peer will support a choice of methods.”
    - Where the authenticator operates in ‘pass-through’ mode, substitute ‘home backend authentication server’ for ‘authenticator’ in the above quotation.
  - If the appropriate method cannot be determined, the peer will NAK the authenticator proposal, and authentication may fail.

# How Peers Select EAP Methods

- From the network name
  - Assumption: A single EAP method can be used with a given network name.
  - Assumption valid when: the peer only has a single identity usable with a given network name (e.g. corporate network access)
  - Assumption invalid when:
    - Peer has several identities usable with a given network name, each of which corresponds to different EAP methods (inter-provider roaming)
- From the realm advertisement (RFC 4284)
  - Assumption: A single EAP method can be used with a given realm.
  - Assumption valid when: realm routing table is static and known by the authenticator, announced to the peer
  - Assumption not valid when: realm routing table is dynamic or too large, so that it is not available to the authenticator

# RFC 4284 Identity Selection

- Available realms encoded within EAP-Request/Identity after a NUL character
  - Example: \0NAIRealms=example.com;marketing.example.com
- Concerns
  - Completeness of the realm list
    - Realms typically not configured on the authenticator, only on core proxies
    - Complete realm routing table may not fit in a single EAP packet due to verbose encoding, EAP min MTU (1020)
    - Operator may not provide the complete realm routing table to a supplicant without “need to know”
  - Performance
    - Without authenticator participation, multiple attempts required to recover from Identity selection problems
      - Unreachable realm required to receive realm hints

# Current Wired 802.1X Deployment Issues

- Delays
  - Wired 802.1x supplicants encounter delays accessing non-802.1x networks due to forced timeouts to detect their non-802.1x capability.
- Portability
  - Wired 802.1X supplicants typically support only a single global profile because network name is not advertised (e.g. no SSID).
- Guest access
  - Once 802.1X authentication fails (EAP Failure received), supplicant controlled port prevents access, even if authenticator receives an Access-Accept from the backend authentication server (e.g. access granted to guest VLAN).
  - Supplicant support for “failback” (no supplicant-controlled port) opens potential security holes.

# Suggested .1af Network Selection Requirements

- Ability to advertise a network name and associated capabilities needed for authentication
- Ability to advertise authenticator identity associated with most recent CAK
- Support for selection of .1AE PSKs as well as EAP identity, based on network name
- Network name long enough to enable uniqueness (e.g. FQDNs, not 32-octet names)
- Ability to support multiple feature sets (e.g. 802.1af with encryption, 802.1X with no encryption).
- Support for guest access
- Ability to quickly determine if 802.1X is supported or not
- Support for localization of network names unlike SSID
- Ability for clients to probe network name and capabilities on demand

# Considerations for 802.1

- RFC 4284
- LLDP Enhancements
- EAPOL/MKA Enhancements
- Others (e.g. new 802.1X frame type)?

# RFC 4284

- Pros
  - Well specified mechanism for obtaining realm hints
- Cons
  - Does not provide *network* information: network name or capabilities
  - Realms typically not configured on the authenticator, only on proxies
  - Realm routing table may not fit in a single EAP packet (minimum MTU: 1020 octets), fragmentation not allowed.
  - Verbose encoding limits extensibility for realm capability advertisement.
  - Performance concerns
    - EAP conversation required (not usable with PSK)
    - Multiple exchanges typically required to recover from Identity selection problems
    - Unreachable realm required to receive realm hints
  - Not needed for device to device authentication

# Enhancing LLDP

- Approach
  - Define new TLVs for Network Name and capabilities needed to establish secure access
- Pros
  - Advertising and management framework exists.  Easily extensible for this purpose
  - Current ABRev fast-start work supports rapid exchange
  - Useful for both hosts and network devices
  - Better backward compatibility with 802.1X-2004
- Cons
  - Single PDU limitations
  - Currently specified to only run over controlled port
  - Authenticator configuration required
  - Not directly linked to authentication exchange (MKA or EAPOL)

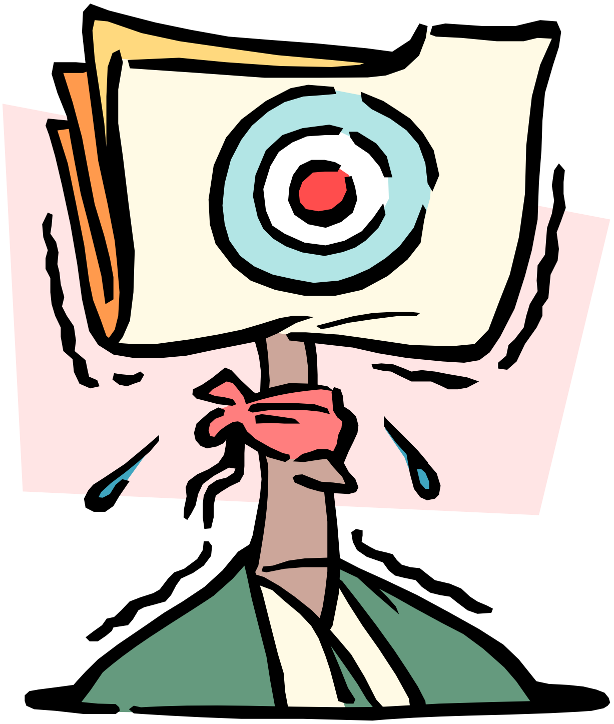
# Enhancing EAPOL/MKA

- Approach
  - Define a new EAPOL/MKA frame that carries Network Name and capabilities needed to establish secure communications
- Pros
  - Lightweight, early in the process, part of 802.1X
- Cons
  - Single PDU limitations
  - Authenticator configuration required
  - Not backward compatible with 802.1X-2004

# New 802.1X Type

- Approach
  - Define a new 802.1X frame type that carries Network Name and capabilities needed to establish secure communications
- Pros
  - Lightweight, early in the process, part of 802.1X
  - Backward compatible with 802.1X-2004 (legacy implementations will ignore the new Type)
- Cons
  - Single PDU limitations
  - Authenticator configuration required

# Feedback?



# Backup and more Detail

# Fundamental Issues with Realm Advertisement

- Problems with realm advertisement are not specific to RFC 4284
  - Issues will occur with mechanisms operating at any layer
  - Limitations difficult to address even with dynamic realm routing in AAA.
- AAA realm routing is similar to Internet routing
  - Authenticators have a default realm route (and often little else).
  - Core proxies do not have a default realm route (“default free zone”), carry a complete realm routing table.
- Implications
  - Authenticators typically do not have access to a complete realm routing table, and therefore cannot send ‘realm hints’
  - Access-Request containing a User-Name attribute with an unreachable realm will be forwarded until it reaches a core proxy.
  - Realm hints returned by a core proxy may not be complete due to packet size or security limitations.

# AAA Route Selection

- AAA route selection
  - Where more than one path to a home backend authentication server is available, a proxy may not be able to determine the path preferred by the user.
    - Source route can be provided via the ‘decorated’ NAI: example.com!joe@example.net means “route the request to the example.com home server, by way of the example.net proxy”
  - Typically not an issue in wired networks.