RADIUS Capabilities

A short presentation
(with math)

Alan DeKok
Infoblox, Inc.

Goals

- Establish a common set of requirements for capabilities.
- Establish a common set of terminology for capabilities.
- Focus on requirements, independent of representation and implementation.

- End up with requirements that can be manipulated symbolically.

Requirements for RADIUS

- Capabilities are advertised in packets.
- No existing clients or servers send capabilities in a packet.
- Capability aware systems must be inter-operable with existing systems.
- Capabilities may traverse capability-unaware intermediaries.
- Multi-round capability negotiation is itself a capability that can be negotiated.

Base Assumptions

- Client and server each have a *set* of individual capabilities: $C = \{ c_i \}$
- Goal is to agree on the *intersection* of capabilities: $C_{\text{Interoperable}} = C_{\text{Client}} \cap C_{\text{Server}}$
- Capabilities are further divided into mandatory and supported sets *M* and *S*:
  - $M_I = M_C \cap M_S$
  - $S_I = S_C \cap S_S$

Compatibility Requirements

- Both client and server have $C \supseteq \{ c_{RADIUS} \}$
  - i.e. capabilities include *at least* normal RADIUS.
- If no capabilities are in a packet, capability-aware systems must use
  - $M = S = \{ c_{RADIUS} \}$
- This lets newer systems use the same capability algorithms for all conversations.

Proposal for Negotiation

- Negotiation is one round of advertising.
  - Client sends M_c and S_c to server.
  - Server has it's own M_s and S_s.
  - Server decides on M_l and S_l.
  - If $M_l \neq M_s$, the server rejects the request.
  - Otherwise, it sends M_l and S_l to client.
- Further exchanges (if any) are based on mutually agreed upon capabilities.

Additional Requirements

- Mandatory is subset of supported
  - $M \subseteq S$
  - This makes later analysis easier.
- Supported is subset of full capabilities
  - $S \subseteq C$
  - i.e. not all capabilities have to be advertised
- If $M = S = \{ c_{RADIUS} \}$, that information does not have to be advertised in a packet.

Summary

- The requirements presented here try to satisfy all parties.
- Mathematical approach helps to minimize communication issues.
- Mathematical approach helps to simplify analysis, using standard tools (sets, intersection, etc).
- Mathematical approach may help to ensure correctness of design and implementation.

Recommendations

- Establish WG opinion on assumptions and approach presented here.
- Work out differences with Emile's presentation.
- Continue with mathematical approach.
- Derive additional relationships.

Additional notes

- Capabilities must be tied to a client-server relationship
  - Client -> Proxy -> Server
  - Server says:
    - Who sent the capability? Client or Proxy?
  - Client says:
    - Who ACK'd the capability? Proxy or server?
- Client must advertise more than $\{c_{RADIUS}\}$, otherwise it is indistinguishable from existing implementations.