Principles of Internet Host Configuration

Wednesday, March 21, 2007

draft-aboba-ip-config-00.txt
Bernard Aboba
Dave Thaler
IETF 68
Prague

Architectural Principles

- Minimize Configuration
- Less is more
- Diversity is not a benefit
- Lower layer independence
- Configuration is not access control

- Other Considerations
  - Reuse of general purpose configuration mechanisms

Minimize Configuration

- Anything that can be configured can be misconfigured.
- [RFC1958] Section 3.8:
  - “Avoid options and parameters whenever possible. Any options and parameters should be configured or negotiated dynamically rather than manually.”
- Wherever possible, parameters should be automatically determined or have reasonable defaults.

Less is More

- The availability of standardized, simple mechanisms for general purpose Internet host configuration is highly desirable.
  - Since the resources available for host configuration may be very small, it is desirable for a host to configure itself in as simple a manner as possible.
- [RFC1958]:
  - Performance and cost must be considered as well as functionality.
  - Keep it simple. When in doubt during design, choose the simplest solution.
- In order to reduce complexity, it is desirable for Internet layer configuration mechanisms to avoid dependencies on higher layers.

Diversity is Not a Benefit

- The number of Internet layer configuration mechanisms should be minimized.
- Diversity is not a benefit, creating issues with:
  - Interoperability: A host may not support the configuration mechanisms required on a given network.
  - Footprint: hosts need to implement multiple configuration mechanisms.
  - Redundancy: Operators need to support multiple configuration services.
  - Latency: Hosts may spend increasing effort to determine which mechanism(s) are supported.
  - Conflicts: Hosts may need to merge conflicting configurations.
  - Additional traffic: Traffic may increase.

Lower Layer Independence

- [RFC1958]:
  - Modularity is good. If you can keep things separate, do so.
- It is desirable for hosts to be able to configure themselves on multiple networks without adding configuration code specific to a new link layer.
- In order to provide media independence, Internet host configuration mechanisms should be link-layer protocol independent.
- Extensions to link layer protocols for the purposes of Internet, Transport or Application layer configuration should be avoided.

Configuration is not Access Control (1/2)

- Network access authentication is a distinct problem from Internet host configuration.
  - Attempting to control access simply by requiring authentication to obtain configuration parameters has little value if the user can manually configure the host.
- Access control means actually controlling *access* (regardless of the configuration mechanism)
- Controlling access to the *link* is different from controlling access to the *network beyond the link*
  - Different enforcement points in general

Configuration is not Access Control (2/2)

- Client must be able to authenticate configuration information learned
- Server must be able to authenticate client before providing configuration information IF server has to consume a scarce resource
  - Not for controlling access to the link
  - (No statement is made about controlling access to the network beyond the link)

Reuse of General Purpose Mechanisms

- Protocols should either be self-configuring, or use general-purpose configuration mechanisms.
  - There is no apparent need for development of additional general-purpose configuration mechanisms.
- Where configuration is necessary, designers should consider:
  - The authoritative source of information.
  - Who will administer the information.
  - Whether the parameter is per-interface or per-host.

Feedback?