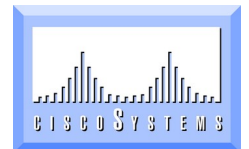




Updates to IPsec Base Specs

Randall Atkinson <rja@cisco.com>

Montreal IETF, June 1996





IETF has 3 levels of standard:

Proposed Standard

Draft Standard

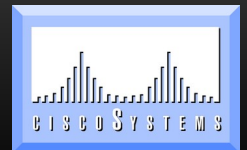
requires demonstrated interoperability of multiple independent implementations

opportunity for editorial/technical corrections

Full Standard

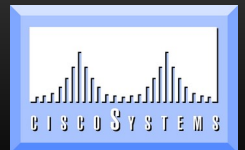
final editorial clarifications

no substantive technical changes



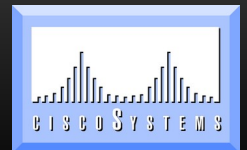
What is happening now?

- Normal IETF process reissues specs as Internet-Drafts before advancing on the Standards Track.
- Normally, editorial changes and are made before advancing.
- If needed, technical clarifications or corrections are made before advancing.



What Is Changing ?

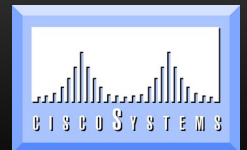
- ❑ **Clarification on which specific IPv4 and IPv6 header fields zeroed for AH purposes.**
- ❑ **Technical corrections to address security issues identified over the past months specifically including those in Bellovin's paper**
- ❑ **Editorial clarifications**





When can the drafts advance ?

- ❑ The base documents cannot be considered for advancement before the end of 1996 because of IETF process rules.
- ❑ Drafts out now to give ample time for review and comment.
- ❑ Drafts must have consensus of the IPsec WG before they can move to Draft Standard.





How can one suggest changes ?

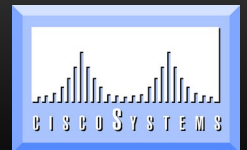
■ **The BEST way is to send the document editor an email message:**

■ indicating specific requested changes

■ providing specific new text for the drafts

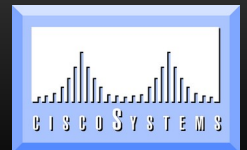
■ providing rationale for the proposed change

■ **Alternately, can propose changes directly to the IPsec WG mailing list.**



Long-term Plan for Base Specs

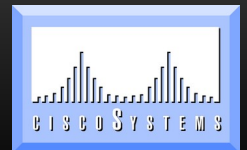
- Move revisions of RFC-1825 thru RFC-1827 to Draft Standard in 6 to 9 months.
- Move them to Full Standard a year later.
- Delays can happen due to:
 - WG not having consensus to advance drafts
 - IETF not having consensus to advance drafts
 - IESG not having consensus to advance drafts







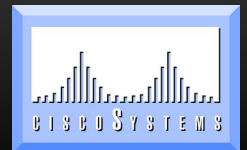
What about the Transforms ?

- ❑ **RFC-1828 will move to Historic status if the IETF and IESG approve the new AH HMAC transforms to Proposed Standard.**
- ❑ **RFC-1829 will move to Historic status if this WG, the IETF, and IESG approve a replacement ESP transform (e.g. Combined ESP Transform edited by Jim Hughes) to Proposed Standard.**



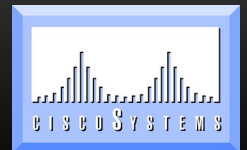
Long-Term Plan for Transforms

-  **6 months or so after Proposed Standard RFC, consider moving them to Draft Standard.**
-  **One year after making Draft Standard, consider moving them to Full Standard.**



What about other transforms ?

- **Other transforms can be created as**
 - Informational RFCs
 - Experimental RFCs
 - Standards-track RFCs
- **If transform is has intellectual property (e.g. trade secret, patent) issues, it isn't a candidate for standards-track since unencumbered alternatives exist.**





Other Standard Transforms

- ❑ Can be created if WG so desires.
- ❑ Should be significantly different from existing standards-track transforms.
- ❑ Generally should be optional-to-implement.
- ❑ Must not have intellectual-property issues.

