Port Control Protocol, Base Specification

draft-ietf-pcp-base-24

Dan Wing, Stuart Cheshire, Mohamed Boucadair, Reinaldo Penno, Paul Selkirk

Dan Wing
dwing@cisco.com

IETF83 -- March 2012
Progress with pcp-base

• At IETF82, I summarized changes through -17
• We had WGLC against -19 (December 19)
• document shepherd reviewed -21 (January 13)
• AD review and some other WG comments resulted in -23

• IETF last call against -24
• 5 DISCUSSes remain open
DISCUSS: Add Transaction ID (Russ Housley)

• “add Transaction ID to help security”
• True, adding a transaction ID provides some protection against spoofing the PCP server
• However, adding a transaction ID provides no protection against spoofing a PCP client
  – Shorten PCP client mappings (lifetime=0)
  – Create lots of mappings (denial of service)
• We contend that PCP server spoofing is as likely as PCP client spoofing
  – And both need to be prevented for PCP (just as for UDP and TCP, which suffer the same problem)
DISCUSS: Add Transaction ID (Russ Housley, Robert Sparks)

• “add Transaction ID to simplify protocol”
• Stuart added “Protocol Design Note”
  – draft-ietf-pcp-base-24, Section 6

• Russ and Robert have not updated their DISCUSSes on this point since -24 was published
DISCUSS: Section 6
(Pete Resnick)

• Unhappy with Section 6, but has not updated his DISCUSS to clarify
DISCUSS: port numbers (Ralph Droms)

• Text on port 5350/5351 is conflicting
• Authors currently working to clarify

• Design question: should unicast unsolicited ANNOUNCE be sent to:
  – Port 5351
  – The source port(s) from currently-active mappings
DISCUSS: remove THIRD_PARTY (Stephen Farrell)

- Wants THIRD_PARTY removed
  - Separate document, discussing mandatory-to-implement security mechanism
- Implementations are using THIRD_PARTY for web portals
DISCUSS: ANNOUNCE causes server flood (several)

• In -24, clients delay random 0-5 seconds
• This DISCUSS will likely be closed by everyone
Thank you