PANA in DSL networks

draft-morand-pana-panaoverdsl-02.txt

**Lionel Morand** France Telecom
Alper Yegin Samsung
Yoshihiro Ohba Toshiba
John Kaippallimalil Huawei

IETF-72, Dublin, Ireland
Summary

- Provides guidelines for PANA deployment over DSL access networks
- Focus on DSL networks migrating from:
  - a traditional PPP access model
    - Where PPP is used to carry authentication parameters (PAP/CHAP or EAP methods)
  - to a pure IP-based access environment
    - No built-in explicit access authentication
      - Today: Use of DHCP option 82 for line-based authentication
    - Need for a subscriber access authentication mechanism
      - Proposal about DHCP evolution for supporting EAP
      - PANA should also be considered a possible solution
Draft History

- **IETF 66:**
  - PANA use case for DSL removed from PANA Framework
- **IETF 67:**
  - First presentation of the "PANA over DSL" draft (v00)
- **From IETF 67 to IETF 71:**
  - Draft frozen during finalization of PANA protocol
  - DSL Liaison on access authentication requirements
- **IETF 71:**
  - Updated version of the "PANA over DSL" draft (v01)
    - Based on final version of the PANA base protocol and comments received and outputs of DSLF liaison discussions
- **IETF 72:**
  - Updated version (v02)
    - description of specific use of "unspecified IPv4 address"
From v01 to v02

- Addition of the possible use of unspecified IP address as PRPA
  - Besides link-local address, private address, etc.
- Addition of a new specific example
  - Describing the use of unspecified IP address in IPv4 context
- Simplification of the PAA discovery
  - Along with the use of unspecified address as PRPA
  - Using broadcasted of PCI (instead of DHCP-based discovery mechanism)
Use of (0.0.0.0) as PRPA

• Use of IPv4 addresses before access authentication still seen as an issue in the IP Session model for DSL Forum

• Proposed alternative:
  – Use of Unspecified IPv4 address as PRPA
    • Described in draft-xia-pana-simplified-00.txt
    • PAC uses (0.0.0.0) as source address of PANA messages
  – After PANA authentication, an IP address is allocated using DHCP
PANA and Unspecified IP address

• Not really a new thing for PANA!
• The use of unspecified IP address in PANA was allowed at an early stage of the PANA spec
  – As for DHCPv4 and MIPv4
• But no clear use/advantage was found and this was removed from the spec at this stage
  – See: proceedings of IETF58
    • http://www.ietf.org/proceedings/03nov/index.html
    • http://www.ietf.org/proceedings/03nov/slides/pana-5/index.html
Broadcasted PCI

• Usually, the PaC needs to discover the PAA IP address to unicast messages to PAA
  – A PAA discovery mechanism is needed e.g. use of DHCP option.

• Proposal for simplification in DSL context:
  – Send the PCI to (255.255.255.255).
  – PAA responds with a PAR message with:
    • source IPv4 address set to the PAA's IP address,
    • destination IPv4 address set either:
      – to (255.255.255.255) if the PRPA is an unspecified address
      – to the source IP address of the received PCI otherwise
  – PaC discovers the PAA's IPv4 address from the source IP address of the received PAR message and additional PANA messages will be unicast to the PAA.
Additional Scenario

- Deployment scenario in which:
  - DSL Network configuration with:
    - PaC in the DSL modem/RG
      - Main use case considered by DSL Forum
    - BRAS hosting PAA, DHCP Server/Relay, and AAA client
    - DSLAM acting as EP
  - Unspecified IPv4 address as PRPA
  - PAA discovery based on broadcasted PCI
  - EAP-MD5 Authentication method
  - POPA configured using DHCPv4
  - EP is triggered by DHCPACK whose 'yiaddr' field is filled
Specific Message flows

1. PANA client initiation
2. PANA Auth Request (EAP-MD5 Challenge)
3. PANA Auth Answer (EAP-MD5 resp)
4. RADIUS Access Req (EAP)
5. RADIUS Access Accept (EAP)
6. PANA Auth Request (EAP Success)
7. PANA Auth Answer (Ack)
8. DHCP Discover
9. DHCP Offer
10. DHCP Request (with IP address in 'yiaddr')
11. DHCP Ack
12. IP Session/data traffic

IP Address Allocation

EP Filter update based on DHCP snooping

Authentication

IP Address Allocation

EP Filter allowing only DHCP and PANA

IETF-72, Dublin, Ireland
Next Step

• Provide more details on:
  – The use of link-local IP@:
    • Mechanism to avoid/resolve possible address conflict/collision
  – PANA impacts on DSL network:
    • Host, DSL Modem, DSLAM, BRAS, DHCP server
  – DSLAM acting as EP:
    • And the use of DHCP as EP triggering mechanism
  – IP@/Identity binding management:
    • Tight/loose coupling between DHCP/PANA/AAA

• Investigate/clarify the case of hosts behind a NAT/Router in IPv4
  – Does PANA support NAT traversal?
Thank You