IPv6 Services for Residential Networks

<draft-bnss-v6ops-upnp-01>

Mark Baugher

Erwan Nedellec

Mika Saaranen

Barbara Stark

Overview

- Background
- Problem Space
- Requirements
- Solution Space
- Security Considerations

The UPnP™ Forum is considering revisions to IPv6 usage. This talk presents some proposed revisions to the UPnP Device Architecture.

Background

- UPnP and the UPnP Forum
  - Hundreds of millions of UPnP devices are in the marketplace
  - Most commercial home gateway/routers run UPnP
  - Multicast service discovery and unicast service description
  - SOAP-based control protocol and eventing protocol
- UPnP Security
  - Well-publicized attacks against UPnP gateway devices
  - Basic problem: Lack of authorization, authentication
- Goals of the Draft
  - Seek comments on use of scoped addressing, address selection
  - Seek support for best practices for home-network firewall

Requirements

- Private network addressability
  - Routed residential networks
    - May become common, 64-bit MACs, sensor networks
    - Site-local operation needed in addition to link-local scope
- Outside-in access
  - Remote access into the residential network
- Firewall control
  - To enable outside-in addressability
- Site-to-site services
  - Two or more residential networks are statically connected

Problem Space

- Routed Private Networks
  - Link-local scope is likely inadequate for UPnP services
  - Site-local scope needs to be supported, ULA is needed
  - Address selection over multiple UDA versions is complex
- Remote Access
  - Current solutions use DDNS and UPnP NAT Traversal
  - Addressing and FW traversal are needed for IPv6
- Site-to-Site Access
  - Addressing model for permanent IPv6 inter-site connections
- Firewall Traversal
  - IPv4 NAT traversal is insecure, IPV6 needs to be better

Solution Space

- Addressing for Routed Private Networks
  - ULA needs to be supported in commercial home gateways
  - Update to RFC 3484 needed for home networks
    - Prioritize address selection: link-local plus site-local, ULA, GUA
- Addressing for Remote Access
  - Tunneled IPv6 uses GUA and DDNS
- Site-to-Site Addressing Uses ULA
  - Static site-to-site tunneling connecting ULA addresses
- Firewall Traversal
  - Industry would benefit from IPv6 firewall best practices
  - Authenticated, authorized FW traversal as a best practice?

Security Considerations

- Home network assets, risks and threats
  - Assets: gateways, PCs, NAS, firewall, etc.
  - Risks: reconfiguration of network devices, theft of secrets
  - Threats: Malware and war drivers
- Big problem: unauthenticated, programmatic control
  - Such as management of gateway DNS server names
- Authentication and authorization best practice

Summary

- Update to address selection for home networks
- Support for ULA needed in home network gateways
- Need to have practices for home network firewalls
  - Must consider authorized, authenticated FW traversal

Are these appropriate topics for the IETF?

Thank You