



Unmanaged networks transition

R. Austein, S. Satapati,
C. Huitema, R. van der Pol.

`draft-ietf-v6ops-unmaneval-00.txt`

Solutions for unmanaged Networks

- ◆ Four cases (A, B, C, D)
- ◆ For each case
 - Study available solutions for connectivity, naming, security
 - If possible, recommend best practices
 - If needed, recommend IETF action, e.g. “develop a standard way to do FOO over BAR”

Case A

◆ Connectivity

- Teredo, or ISP provided tunnel (UDP, maybe TCP)

◆ Security

- Precaution principle, make sure that IPv6 only used by applications specifically designed for IPv6 Internet use

◆ Recommendation

- Proceed with publication of Teredo
- Develop “configured UDP tunnel” option

Case B, Connectivity

◆ Connectivity

- Prefix delegation through RA proxy or DHCPv6
- Use dual-stack, not NAT-PT

◆ Recommendation, connectivity

- Specify interaction between ND & RA proxy
- Provide security framework for DHCPv6

Case B, naming

◆ Naming

- Provisioning of DNS parameters, discovery of local DNS resolver
- Publication of IPv6 addresses
- Resolution of local names

◆ Recommendation

- Standardize subset of DHCPv6 (without overhead of managing addresses)
- Promote use of DDNS for publication
- Use LLNMR for local name resolution

Case B, security

- ◆ The case B solutions provide global IPv6 connectivity to the local hosts. Removing the limit to connectivity imposed by NAT is both a feature and a risk. Implementations should carefully limit global IPv6 connectivity to only those applications that are specifically designed to operate on the global Internet. Local applications, for example, could be restricted to only use link-local addresses, or addresses whose most significant bits match the prefix of the local subnet.

Case C

◆ Connectivity

- Considered 6to4, tunnel broker, ISATAP
- Recommend use of 6to4 or ISP provided tunnel

◆ Recommendation

- Develop AAA solution for tunnels
- Deploy more 6to4 relays!

◆ Naming, security

- Mostly same as case B
- Special issue of tunneling security (6to4 and also tunnels with no per-packet authentication)

Case C: Fred Templin's comments

- ◆ As per our earlier discussion, thank you for providing the analysis of ISATAP in section 4.1.3 of this document update. Unfortunately, I must point out that the analysis is incomplete in the case of ISATAP being used to provide IPv6 connectivity to the gateway.

In this case, the ISATAP-enabled gateway can receive explicit prefix delegation(s) from the provider (as described in section 3.1.2 of the document) and advertise the prefix(es) to an arbitrarily large number of native IPv6 hosts on the unmanaged network. So, it is indeed not true that: "ISATAP can thus only be used in the degenerate case when the unmanaged network consists of a single host" as stated in the current analysis.

Case D

◆ Connectivity

- Recommend to develop “IPv4 over IPv6” solution, including provision of “tunnel point”

◆ Naming

- Need to provision DNS parameters to gateway over IPv6
- Recommendation: same solution as IPv6 host in case B

◆ Security

- Similar to case B, plus potential issues created by IPv4 over IPv6

Summary of recommendations

- ◆ Develop and standardize Teredo or similar technology.
- ◆ Agree on standardized IPv6 prefix delegation mechanism
- ◆ For "informal prefix sharing", develop a standard way to perform "RA proxy", possibly as part of a "multi-link subnet" specification
- ◆ Standardize a way to provision a DNS resolver address in IPv6 only hosts
- ◆ Proceed with the standardization of LLMNR.
- ◆ Continue standardization of 6to4.
- ◆ Standardize an IPv4 over IPv6 tunneling mechanism, as well as the associated configuration services.

Next steps

- ◆ WG last call for evaluation document
- ◆ Act on recommendations