

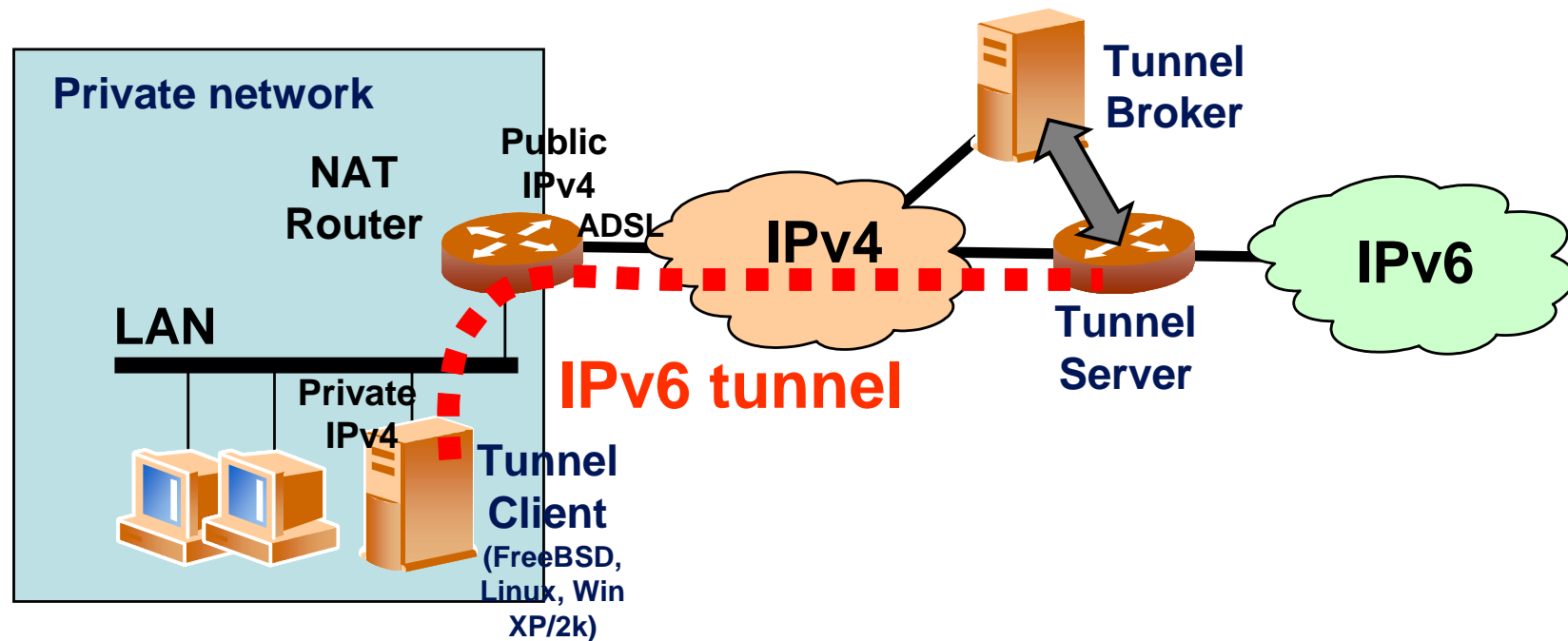
Forwarding Protocol 41 in NAT Boxes <draft-palet-v6ops-proto41-nat-00.txt>

Jordi Palet

jordi.palet@consulintel.es

Overview

- Some NAT boxes allow IPv6 tunnels from systems in the private LAN



What's new?

- This behavior isn't documented
 - Some people use it, others don't know
 - Most manufacturers don't document it
- Provides one more opportunity to deploy a huge number of IPv6 nodes and networks (if the tunnel end point is configured as a router)
- No need for a new transition mechanism

How it works?

- Address translations performed by NAT are session based, for incoming and outgoing packets of that session
- IPv6 over IPv4 tunnels are identified as protocol 41
- Our “session”:
 - Source Address + Target Address + proto 41

Different NAT boxes

- Some don't allow proto-41 based entries
- Basic NAT and NAT

 - Unidirectional, usually with a timeout
 - Require the session to be initiated from inside

- Bidirectional and configurable NAT

 - Session initiated also from outside

Applicability

- Limited for Basic NAT and NATPT
 - Only for outgoing (and then immediate incoming) traffic
 - Unless we can play with the timeout or some “keep alive”
- Good for the other kind of NATs
 - Could require a minimum configuration
 - Can be like a “default” configuration

NAT design considerations

- Most of the NAT boxes support this feature if properly configured
- New firmware versions should ensure the support for proto-41 forwarding
 - Isn't a big deal
- It will be nice a “simple” HTTP interface
 - Do you want to enable IPv6 tunnel support ?
 - For what private IP ?

Tunnel Broker design considerations

- New releases should detect or at least manually allow to use this function
 - NAT box address, instead of private one
- Create the correct script to configure the tunnel end point

Security Considerations

- NAT “false security” no longer applies
- Recommend the usage of personal firewalls
- Possible DoS Attack by another node in the private LAN
 - Depend on NAT design
 - Not an issue in SOHO/Home networks

Next steps

- Become a WG item ?
- Continue the survey
- Ideas from the WG