

Hi :-)

- Wrote a tool – want to share

KadNode

- Yet another P2P-DNS like system
- Task
 - Find IP addresses by some identifier
 - ... but decentralized
 - Low footprint (Disk, CPU, RAM, Traffic)
- Petname system
 - ... not really/traditional DNS!
- Links look like `aa52fb210465bddd679d6853b491ccce.p2p`

Use Case

- Usable DynDNS replacement
- vpn1.freifunk.net, vpn2.freifunk.net, ...
 - Maybe make Freifunk a bit more decentralized
- Low footprint environments (~100KB size)

How it works part 1

- intercepts *.p2p domains on host system
 - /etc/nsswitch.conf (“Name Service Switch”)
 - Debian, FreeBSD
 - Buildin local DNS server (handles A, AAAA, SRV)
 - OpenWrt, Windows
- DHT (Distributed Hash Table)
 - DHT code from Transmission BitTorrent client
 - 20 Bytes => IP addresses

How it works part 2

- The node with private key announces the hash every 10 min in the DHT network
- <public-key>.p2p resolved by the DHT
- We get multiple IP-Addresses... huh?
 - By chance? Spoofing?
- Send a random string to sign to every address
 - Only those nodes with the private key can sign it!

Challenges

- Speed
 - Up to 8 seconds (not cached)
 - ~1 sec. possible, needs a modified DHT...

Future

- mbedTLS inclusion
 - Reduce effective installation size on OpenWRT
 - Used for default http server on OpenWrt
 - We can use the TLS for authentication
 - Can use own Certificate Authority
 - Anyone can say e.g. google.com is this or that IP address - others kandode instances can verify via TLS handshake on https port! :D

Features

- IPv4/IPv6
- Written in C / Open Source
- Small: 75-120KB
- Local Peer Discovery
- Packages:
 - OpenWrt, Debian, ArchLinux, OSX, Windows, FreeBSD

Thanks

- <https://github.com/mwarning/KadNode>
- Have fun!