

N2N: Layer Two Peer-to-Peer VPN

Luca Deri <deri@{unipi.it,ntop.org}>

The Internet Isn't Really Open

- Was originally been designed as a flat data network delivering a multitude of protocols and services between peers.
- Is actually a constrained network severely enforcing client-server communication.
- Addressing plans, packet routing, security policies and users' reachability issues are entirely managed and limited by access providers.

User's View of the Internet

- NAT devices mask the user's IP identity and limit peers accessibility.
- No control over the connection configuration, totally managed by ISPs.
- Firewall greatly reduce the possibility of a user being contacted by a direct session opened elsewhere over the Internet.

In a Nutshell...

The Internet is a large “department store” where users can go shopping for communication services, but it can’t be easily used as a geographically distributed LAN except at the price of setting up static VPNs relying upon “premium fee” access services.

Vision

- The internet should be a “transparent” IP-based transport for users, not a geographical/ISP constrain.
- Users should control/create their community networks (today network administrators do).
- Security is a community to community policy (today it has to do with IP addresses, ports, NAT..).
- The focus is on the service/content (email, song etc.) rather than on the host that provides it.

What is n2n ?

- A layer-two peer-to-peer virtual private network (VPN) which allows users to exploit features typical of p2p applications at network instead of application level.
- In a nutshell, as OpenVPN moved SSL from application (e.g. used to implement the https protocol) to network protocol, n2n moves p2p from application to network level.

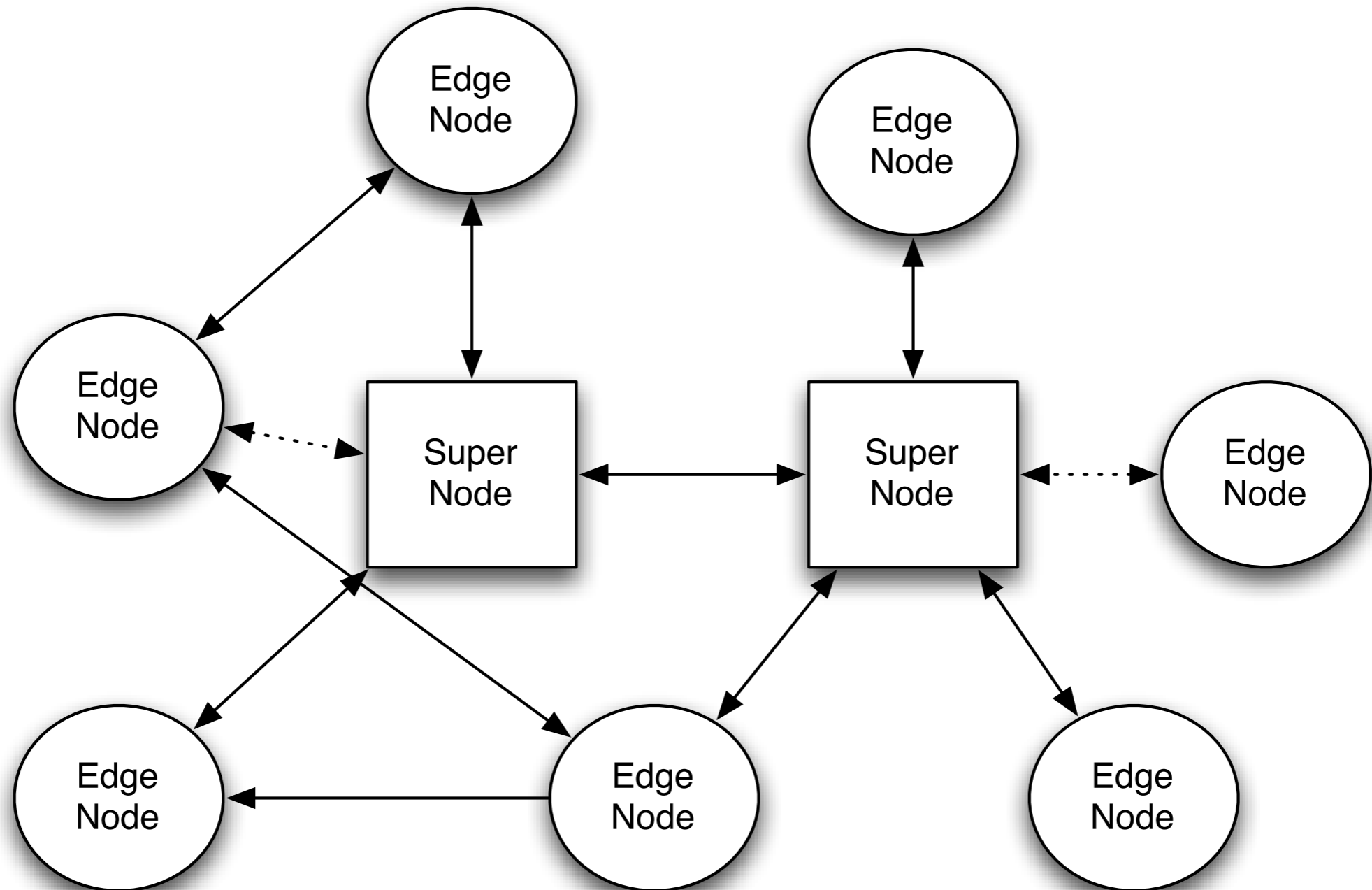
N2N Features [1/2]

- A n2n network is an encrypted layer two private network based on a p2p protocol.
- Unlike Skype/Hamachi, encryption is performed on edge nodes using open protocols with user-defined encryption keys.
- Each n2n user can simultaneously belong to multiple networks.
- n2n has one or more supernodes and several edge nodes, one per n2n endpoint

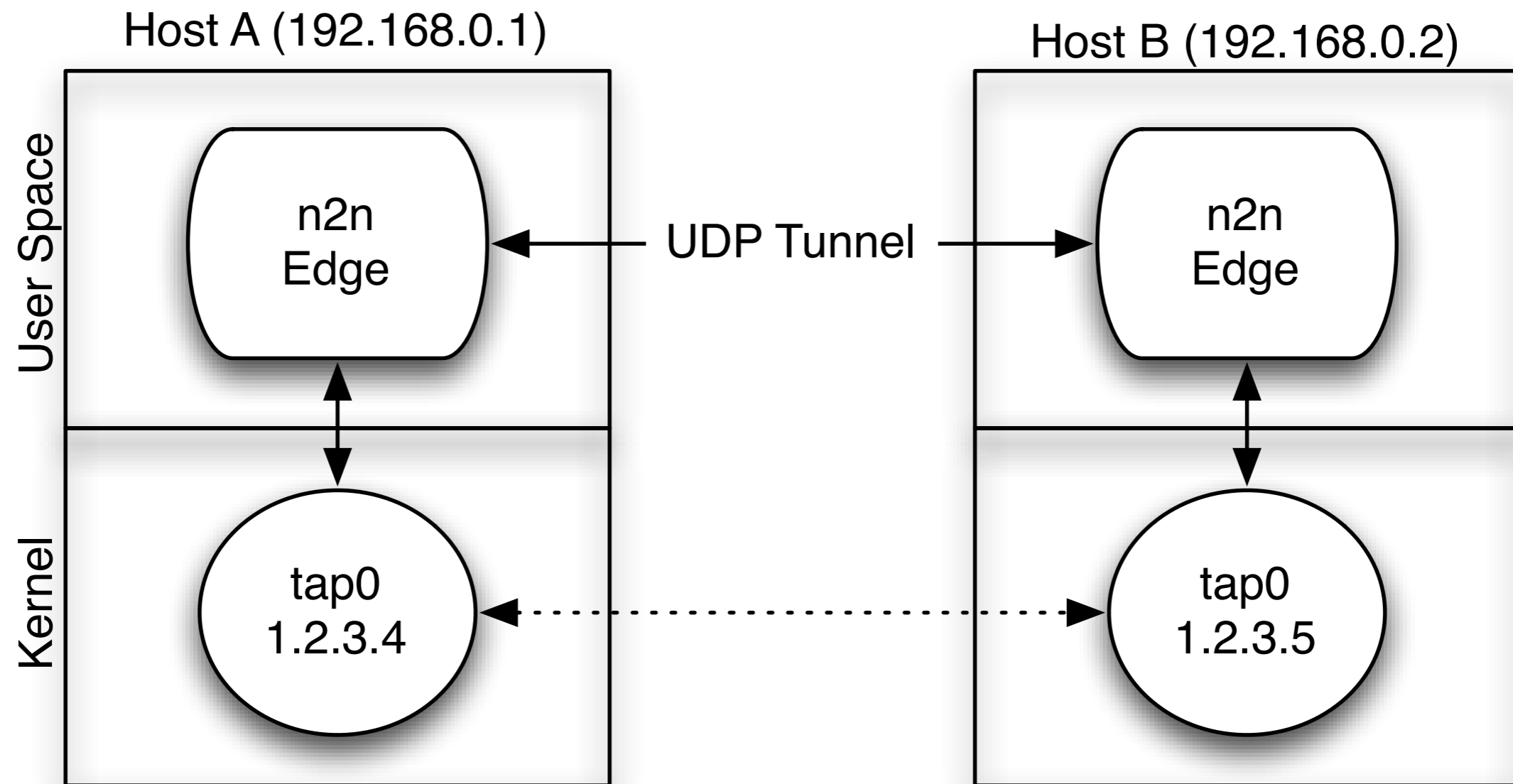
N2N Features [2/2]

- Ability to cross NAT and firewalls in the reverse traffic direction (i.e. from outside to inside) so that n2n nodes are reachable even if running on a private network.
- n2n networks are not meant to be self-contained, but it is possible to route traffic across n2n and non-n2n networks.

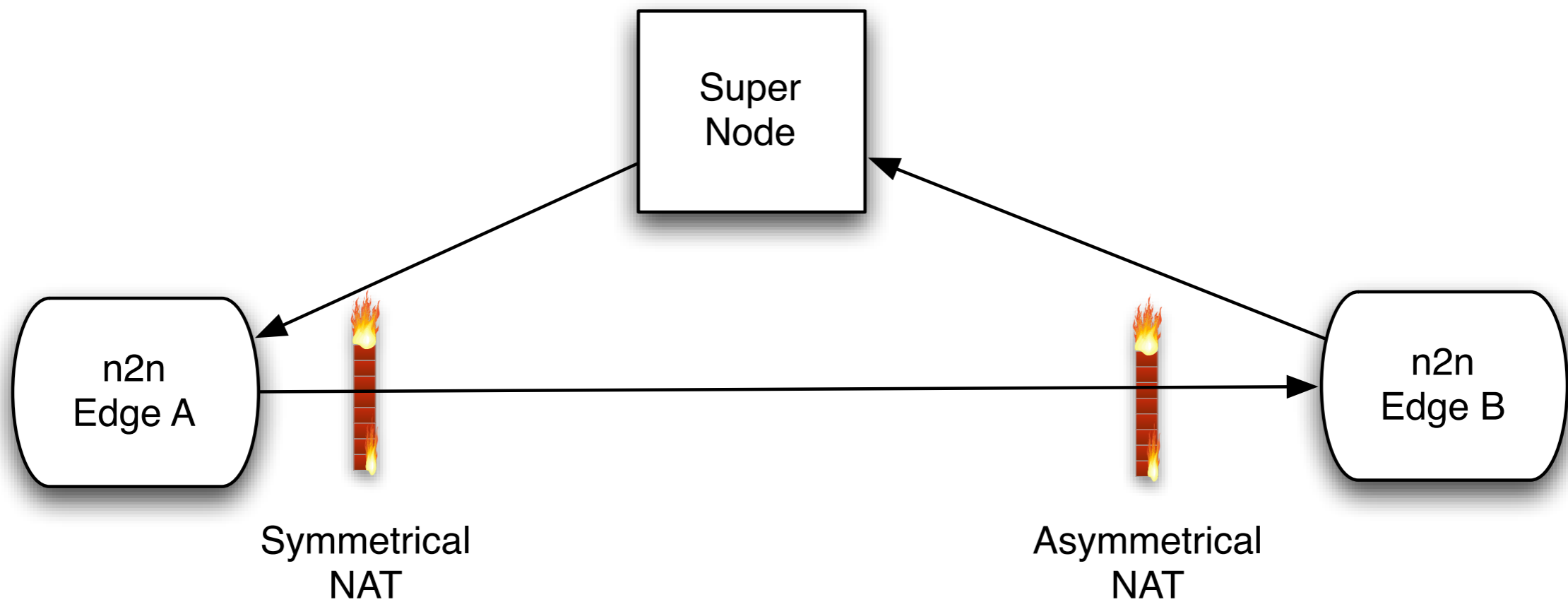
Architecture [1/2]



Architecture [2/2]



NAT Crossing



(Interior) Core Routing

- Supernodes keep track of <network name>:<MAC Address>:<Public NATed IP:port>:<private unNATed IP:port>.
- N2N header is unencrypted, N2N packets are encrypted by edge nodes: supernodes can route packets only based on n2n header.

```
struct n2n_packet_header {
    u_int8_t version, msg_type, ttl, sent_by_supernode;
    char network_name[16], src_mac[6], dst_mac[6];
    struct sockaddr_in public_ip, private_ip;
    enum packet_type pkt_type;
    u_int32_t sequence_id;
    u_int32_t crc;
};
```

(Exterior) Edge Routing

- Edge nodes can be used to route traffic among n^2n and non- n^2n networks. This as n^2n interfaces are standard OS interfaces and not application hooks.
- The edge node can prevent routing by analyzing the pair $\langle \text{IP} \rangle \langle \text{MAC Address} \rangle$ and discarding non- n^2n packets.

Addresses and Naming

- n2n nodes can have either dynamic (e.g. via DHCP) or static addresses.
- An n2n address is not dependent on the network address, i.e. a n2n node can have a permanent address independently of the network address currently used (useful for contacting roaming users).
- (Multicast) DNS can be used for resolving node names.

n2n Topology Learning

```
deri@1.2.3.6 > ping 1.2.3.4
PING 1.2.3.4 (1.2.3.4): 56 data bytes
64 bytes from 1.2.3.4: icmp_seq=0 ttl=64 time=352.721 ms
64 bytes from 1.2.3.4: icmp_seq=1 ttl=64 time=150.737 ms
64 bytes from 1.2.3.4: icmp_seq=2 ttl=64 time=157.588 ms
64 bytes from 1.2.3.4: icmp_seq=3 ttl=64 time=151.144 ms
64 bytes from 1.2.3.4: icmp_seq=4 ttl=64 time=148.873 ms
64 bytes from 1.2.3.4: icmp_seq=5 ttl=64 time=161.792 ms
64 bytes from 1.2.3.4: icmp_seq=6 ttl=64 time=156.178 ms
^C
--- 1.2.3.4 ping statistics ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max/stddev = 148.873/182.719/352.721/69.529 ms
```

n2n Evaluation [1/2]

- Ability for end-users to create networks where people can join without administrator intervention and with limited centralized dependencies.
- n2n administrator can change the policy (routing, security etc) of their networks.

n2n Evaluation [2/2]

- n2n are not “private” but they can route packets across communities, and identify users with shared DNS-like registers.
- Users can belong to multiple communities: no point-to-point and “single VPN” concept typical of VPNs.
- n2n is an interim solution for today’s networks, might not be necessary in the future.

n2n Future Developments

- Porting to embedded/mobile devices (e.g. iPhone, Android): reachability with a permanent IP address regardless of the network.
- HTTP/DNS tunneling for operating n2n on close networks.

Availability

- <http://www.ntop.org/n2n/>
- Available for Linux, OSX, Windows.
- Licensed under GPLv3.