n2n - Peer 2 Peer VPN

ntopConf'22

Hamish Coleman - hamish@zot.org

Thanks

$company

What is it?

What is it?

- Peer to Peer VPN

What is it?

- Peer to Peer VPN
- NAT Piercing

What is it?

- Peer to Peer VPN
- NAT Piercing
- "Distributed Ethernet Switch"

What is it?

- Peer to Peer VPN
- NAT Piercing
- "Distributed Ethernet Switch"
- Userspace tuntap

What is it?

- Peer to Peer VPN
- NAT Piercing
- "Distributed Ethernet Switch"
- Userspace tuntap
- Low resource requirements

Basic Concepts

Supernodes

- Public IP Address
- Central Coordination Point
- Can implement some Access Control
- Last-resort packet forwarding

Communities

- Form a virtual Ethernet Segment
- Packets are protected by a shared key

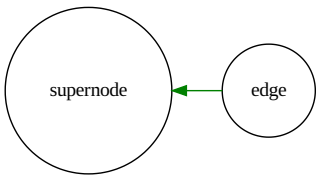
IP Addresses

- An address can be allocated by Supernode
- Static addresses are available
- Can even allocate via a DHCP server

Connection Lifecycles

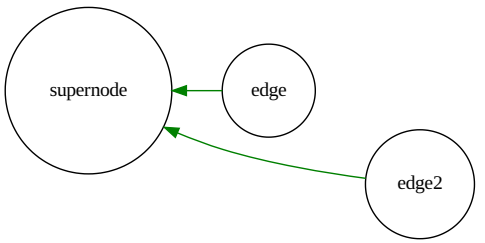
Connection Lifecycles

Each edge connects to a supernode



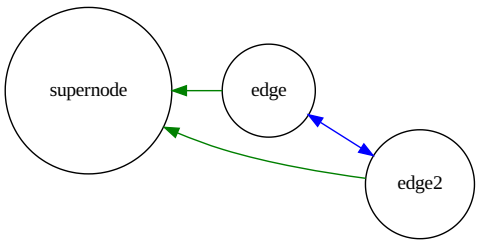
Connection Lifecycles

Extra edges join, and will try to find each other



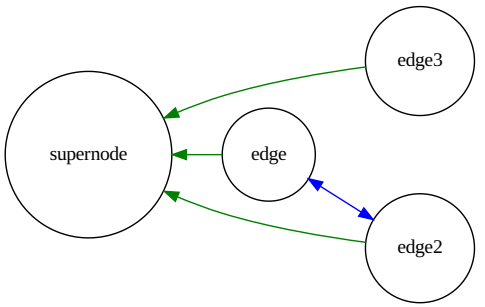
Connection Lifecycles

Extra edges join, and will try to find each other



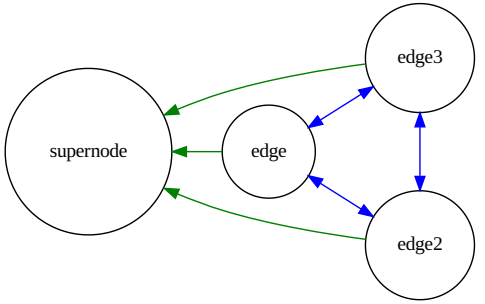
Connection Lifecycles

Extra edges join, and will try to find each other



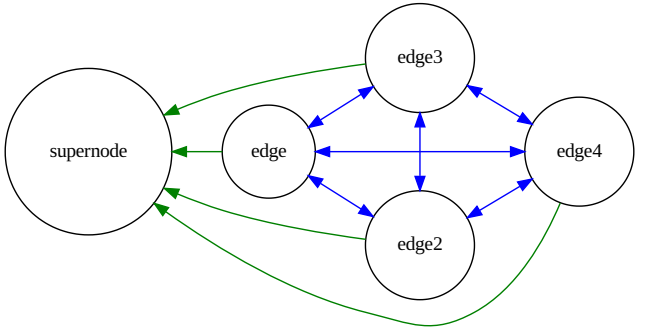
Connection Lifecycles

Extra edges join, and will try to find each other



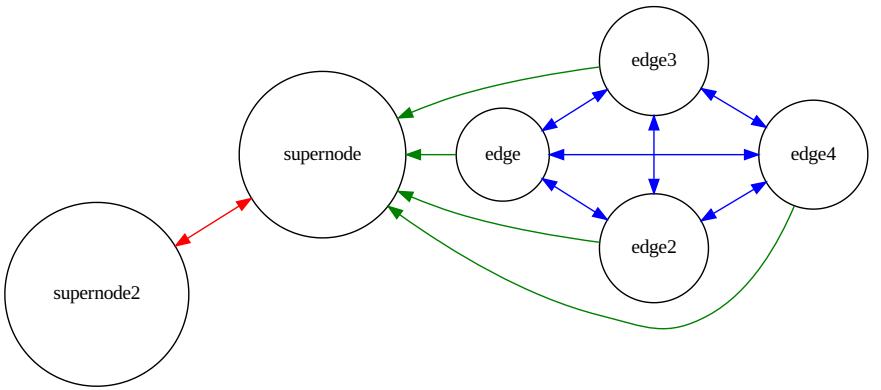
Connection Lifecycles

Ideally, all edges can form a full mesh



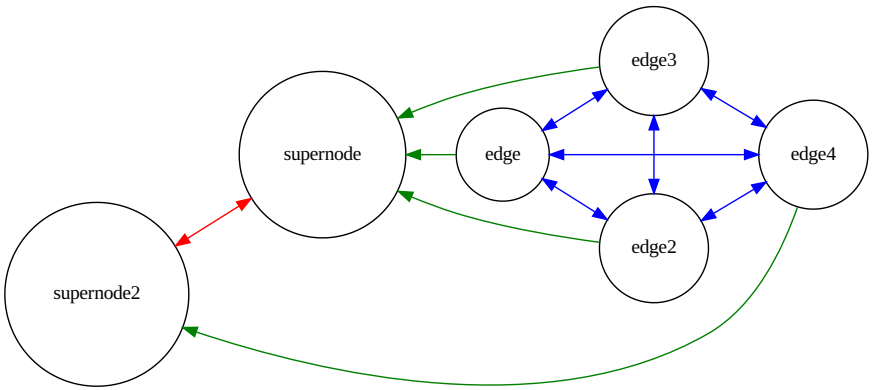
Connection Lifecycles

Extra supernodes can form a "Federation"



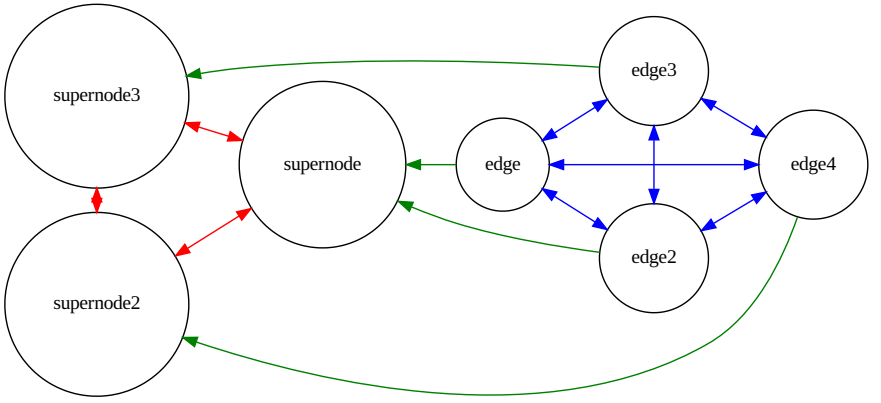
Connection Lifecycles

Edges will rebalance



Connection Lifecycles

Supernodes forward edge details



New in 3.0

Federation

- Allows extra Supernodes to be added
- Balance the Edge nodes
  - by Load
  - by Round Trip Time

JSON API

- an RPC interface to the running daemon
- Allows future extensions
- Monitoring / Statistics
- Debugging your setup

Automation / Releases

Github Action based CI

- Basic unit tests
- Linting
- Binaries and Packages

Multicast

- Send Multicast discovery packets
- Neighbour Edge nodes reply
- Send VPN data packets directly

(Supernode still needed for control plane)

Usernames, Communities and Authentication

- Supernodes default to allow all communities
- They can be restricted to a community list
- Restictions enables full header encryption
- user/password based auth also available

TCP and Filtering

- Default is to use UDP for all connections
- TCP-only as option for edge-supernode traffic
- The TAP interface default accepts all traffic
- TAP-traffic may have filter rules applied

Future plans

Near future plans

- Remove old human only management
- More JSON APIs and scripts/tools
- Move non-core functionality to helpers
- UPNP/PMP

On the Horizon

- Merge the Edge and Supernode
- Better NAT punching
- layered nat 'zone' discovery
- self-arranging tree of supernodes
- Better packaging
- More packages
- More automated test tools

Tell us your use case!

Questions?

- github project:
  - https://github.com/ntop/n2n

Hamish Coleman - hamish@zot.org