

Empowering Peer-to-peer Services

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

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.

In The Beginning There Was P2P...

- P2P has been a truly killer and disruptive application that changed the Internet.
- Since the introduction of Napster (05/1999) P2P applications have grown and moved from a niche (file sharing) to a broader use (VoIP, remote control, Seti@Home).
- Currently we have the 3rd P2P generation.

P2P Features [1/2]

- P2P has overcome all the limitation of the “closed” internet (firewalls, dynamic IP and NAT).
- P2P can be seen as a “new/modern” IP routing protocol.
- P2P allows decentralized application design and works even with non-permanent connections contrary to IP (always on).

P2P Features [2/2]

- P2P is limited to a service (TCP/UDP port) and has no notion of IP: you target at a file or user contrary to the internet where the target is an IP (e.g. <http://www.google.com>).
- P2P allows two or more peers to communicate regardless of their network configuration (addressing, firewall etc.).

Looking Ahead [1/4]

- As of today, the type of Internet access can vary in terms of connection type (cable, wifi, phone) and location (IP addressing).
- People don't care of IP configuration, they do care of (permanent) service availability.
- Users with common interests (e.g. belonging to the same company) need to aggregate and exchange data.

Looking Ahead [2/4]

- Closed Internet (firewall and NAT) prevent aggregation, and even IPv6 (give an address to everyone) is not the solution: we need privacy.
- Internet it's not just a transport but it's a place where networks administrators (addressing, routing, traffic policies) decide whereas users cannot.
- Mobility and remote access don't fit with centralized connectivity (VPNs).

Looking Ahead [3/4]

- Network administrators use (centralized) VPNs in order to aggregate remote homogeneous users.
- Limitations: centralized design as heterogeneous users (company A and B) cannot belong to the same community although share the same interests (e.g. they work on the same research project).

Looking Ahead [4/4]

- Question: can we have decentralized network administration, privacy, and permanent service access regardless of the place and network access type?
- Indeed: do move P2P from L4 to L3 in order to create a human-friendly network!

N2N Features [1/2]

- Ability for end-users to create “dynamic/ad hoc” networks where people can join like on a “conventional” network without administrator intervention and with limited centralized dependencies.
- Dynamic AS/network infrastructure with interior routing (among participants) and (optional) exterior routing (Internet).

N2N Features [2/2]

- A PC can belong to several ad-hoc networks at the same time: each network represents a community.
- Each host has a virtual network interface for each network it joined.
- Meshed, semi-centralized architecture (like P2P) with super-nodes that can be build the basic network infrastructure.

Don't Reinvent The Wheel [1/2]

- In 2007 the basic technologies are already available, just add what's missing.
- Existing routing protocols (e.g. OSPF/BGP) can be enhanced in order to take into account dynamic networks.
- Naming (e.g. luca.mycommunity) is important (DNS Service Discovery, <http://www.dns-sd.org/>) for identifying hosts.

Don't Reinvent The Wheel [2/2]

- L2/L3 encrypted tunnels are used by peers to communicate.
- P2P protocols will be used for finding and registering hosts, as well as announcing new networks (communities).
- Tun/tap interfaces combined with P2P protocols to run the software across OSs.

An Opportunity For Everyone [1/3]

- NRENs can provide the basic network infrastructure for building communities.
- Researchers can simultaneously share remote resources (e.g. a telescope) while belonging to different communities.
- N2N is a network virtualization technique.

An Opportunity For Everyone [2/3]

Many technologies are available, but there's a lot of network research to be carried on:

- How to route packets across dynamic networks.
- Allow connections from closed network with limited internet access (NAT and closed port).
- How to prevent edge hosts to do (unwanted) intra-community routing.

An Opportunity For Everyone [3/3]

- Re-route packets directed to disconnected hosts.
- How to find the best path in interior routing.
- How to prevent naming/addressing overlapping.
- Direct vs. P2P multihop (in case of restricted firewalls) communications.

N2N isn't just a P2P-VPN

- 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 administrator can change the policy (routing, security etc) of their networks.

Going Beyond

- Rethink IP services (e.g. email) in terms of community/service: first join the community then use your service.
- Design virtual community routers.
- P2P is a (interim) solution for today's networks, might not be necessary in the future.

Related Work

- <http://vtun.sourceforge.net/> Virtual tunnels
- <http://www.hamachi.cc/> P2P VPN
- <http://openvpn.org> L2/L3 VPNs
- <http://jxta.org> Open P2P
- <http://tor.eff.org> Onion Router
- <http://www.seclarity.com/> Sinic Cards

Credits

- Alex Tudor <alexander.tudor@mac.com>
- Yuri Francalacci <yuri@ntop.org>