The X-Bone & its Virtual Internet Architecture
10 Years Later

Lars Eggert
Dagstuhl Seminar on Network Virtualization for the Future Internet
Schloss Dagstuhl, Germany
September 18-19, 2008
Talk Outline

history
Virtual Internets
  why
  what
  architecture highlights
related projects at ISI (time permitting...)
  X-Bone, DynaBone, TetherNet
History

**X-Bone** was a series of research projects at USC/ISI

- X-Bone, DynaBone, TetherNet, X-Tend, NetFS, GeoNet, ...

1997-2005+

Initial funding from DARPA, follow-on funding from the NSF

[http://www.isi.edu/xbone/](http://www.isi.edu/xbone/)

Key results

- **an architecture** (the “Virtual Internet” architecture)
- **a deployment/management system** (the “X-Bone”)

Follow-on work using virtual nets:

- **DynaBone** spread-spectrum virtual networks
- **TetherNet** rent real Internet behind firewall + NAT
- **GeoNet** geographically-routed virtual networks
Prior & Related Work

new services & protocols
Cronus, M/6/Q/A-Bone

multi/other layers
Cronus, Supranet, MorphNet, VANs

partial solutions
VPN, VNS, RON, Detour, PPVPN, SOS

virtualization, revisitation, recursion
X-Bone, Spawning, Netlab/Emulab

OS virtualization
VMware, jails, vserver, XEN, PlanetLab
Virtual Internet – Why

“network equivalent of virtual memory”

protection
  separate topology, optionally secured
  test + deploy new protocol/service

sharing
  increase utility of infrastructure

abstraction
  adapt topology to application
Virtual Internet – What

network = hosts + routers + links

virtual network =
  virtual host → packet src/sink
  + virtual router → packet gateway
  + virtual link → tunnel X over Y

virtual Internet – “network of networks”
use Internet as physical media
create virtual link & network layers
strong L2 vs. weak L3 host model

a virtual Internet should look exactly like the real thing
“if an app can know it runs in a VI, we did it wrong

September 18, 2008

Lars Eggert | Nokia © 2008
VI Architecture Feature – Recursion

virtual Internets on top of virtual Internets

our litmus test:
   system should be able to do recursive VI-in-VI without hacks

recursion has real uses cases
   e.g., allows transparent reconfiguration
       change outer VI w/o affecting inner fault tolerance, basis for DynaBone

also allows VI “embedding”
   “router is a network inside”
VI Architecture Feature – Concurrency

one node participates in multiple virtual Internets at the same time
basis for isolation & abstraction

bind different apps/VMs to different VIs on the same physical node
one node participates in the same virtual Internet but multiple times
allows creation of VIs larger than physical resources
fully decouples virtual from physical topologies
Hop-by-Hop Security in the Virtual Internet architecture is a virtual link property decoupled from topology. It transparently coexists with end-to-end security inside the VI and also transparently coexists with security underneath a VI.

**IPsec tunnel mode**

- Base IP
- IPsec
- VPN IP
- Data

**IPIP tunnel + IPsec transport mode**

- Base IP
- IPsec
- VPN IP
- Data

IPIP tunnels + IPsec transport mode is modular tunnel mode equivalent. There was a huge IETF debate around 2000 (draft-touch-ipsec-vpn-05.txt).
The X-Bone System

deployment + management system for virtual Internets programs → standardized API
humans → web interface

high-level virtual network description language
express virtual topology + services
XML

collaborating, distributed management daemons
multicast expanding-ring discovery
distributed resource reservation
instanitate + manage virtual network

non-goals: topology optimization, non-IP VIs, ...
X-Bone Screenshots

X-Bone Overlay Operation
You are logged in with these credentials: (taken from your X-SOA certificate).

User: Yu-Chun Wang <yu.chun.wang@nokia.com>
Location: Hannover, Germany
Organization: Nokia Research Center, Div. 7

This page allows you to view a new overlay. You may select all remaining node names.

**Node**
- Name: The name of the overlay.
- Type: The type of the overlay.
- Status: The status of the overlay.

**Topology**
- Use Dynamic Routing: Enables dynamic routing within the overlay.
- Use Fixed Application: Enables fixed application deployment.

**Host Properties**
- Number of Hosts: The number of hosts in the overlay.
- Host Operating System: The operating system of the hosts.

**Router Properties**
- Number of Routers: The number of routers in the overlay.
- Router Operating System: The operating system of the routers.

**Link Properties**
- Authentication: The authentication method used to authenticate all overlay traffic.
- Encryption: The encryption algorithm used to encrypt all overlay traffic.

**Overlay Parameters**
- Node: The node number.
- Role: The role of the node.
- Source: The source node.
- Destination: The destination node.
- Port: The port number.
- Protocol: The protocol used.

**Overlay Status**
You are logged in with these credentials: (taken from your X-SOA certificate).
X-Bone Status

current release: 3.2

mature: 10 years of open source availability

platforms: FreeBSD, Linux

unofficial: NetBSD, Cisco

widely used (by 2003):

UCL, UPenn, Aerospace, DOD Canada, Sinica Taiwan + more
Related Work at USC/ISI
DynaBone

parallel inner virtual networks = algorithmic & protocol diversity
spread-spectrum multiplexer, wrapped inside outer virtual network
TetherNet

issue: firewalls, NATs, clueless ISPs
broken end-to-end connectivity

solution: relocate real Internet subnet
real = routable IP + DNS + no fw + ...
tunnel subnet from anchor router to tether router at remote site

September 18, 2008
Lars Eggert | Nokia © 2008
TetherNet Features

true Internet behind NATs and firewalls
- IPv4 + IPv6
- multicast
- fwd/rev DNS
- traffic shaping
- 802.11b AP
- secure: IPsec for traffic, X.509 for user auth
- web interface configuration

U.S. patent filed, talks with licensees
TetherNet Screenshots

TetherNet Rental

Required rental parameters:
- **Rental Site**: Marina del Rey, USA
- **Subnet Size**: 192.22.14.91
- **Access Code**: [enter access code]

Optional rental features:
- **TCP**
- **UDP**
- **IPv4**
- **IPv6**

Optional advanced networking features:
- **IPv6**
- **Multicast**
- **DHCP Server**
  - **Enable**: [check box]
  - **Range**: [enter range]

Start TetherNet Service

Rental Server Response

Rental information:
- **Rental Server**: anchor.postel.org<@lars@isi.edu>
- **Organization**: USC/ISI, TetherNet
- **Location**: Marina del Rey, CA, US
- **Local Time**: Tue Sep 17 13:13:00 2002

Rented network block:
- **IP Block**: 206.117.27.16
- **Size**: 10

TetherNet properties:
- **Rental Site**: 198.22.10.91
- **LAN Size**: 206.117.27.16/28, 9 hosts, IP addresses 206.117.27.22 - 206.117.27.30
- **DNS Suffix**: tethernet.net
- **Tunnel Type**: UDP (local port 35770, remote port 34213)
- **DHCP Service**: on, handing out the range from 206.117.27.22 to 206.117.27.22
- **IPv6**
- **Multicast**: on

Check status:
- **Check Status**: It may take several seconds to bring up the rental.
Other Projects

X-Tend
maintain + extend X-Bone as tool for research + education

GeoNet
geographically-addressed overlays

NetFS
access control for the network stack via a pseudo file system
THANK YOU!