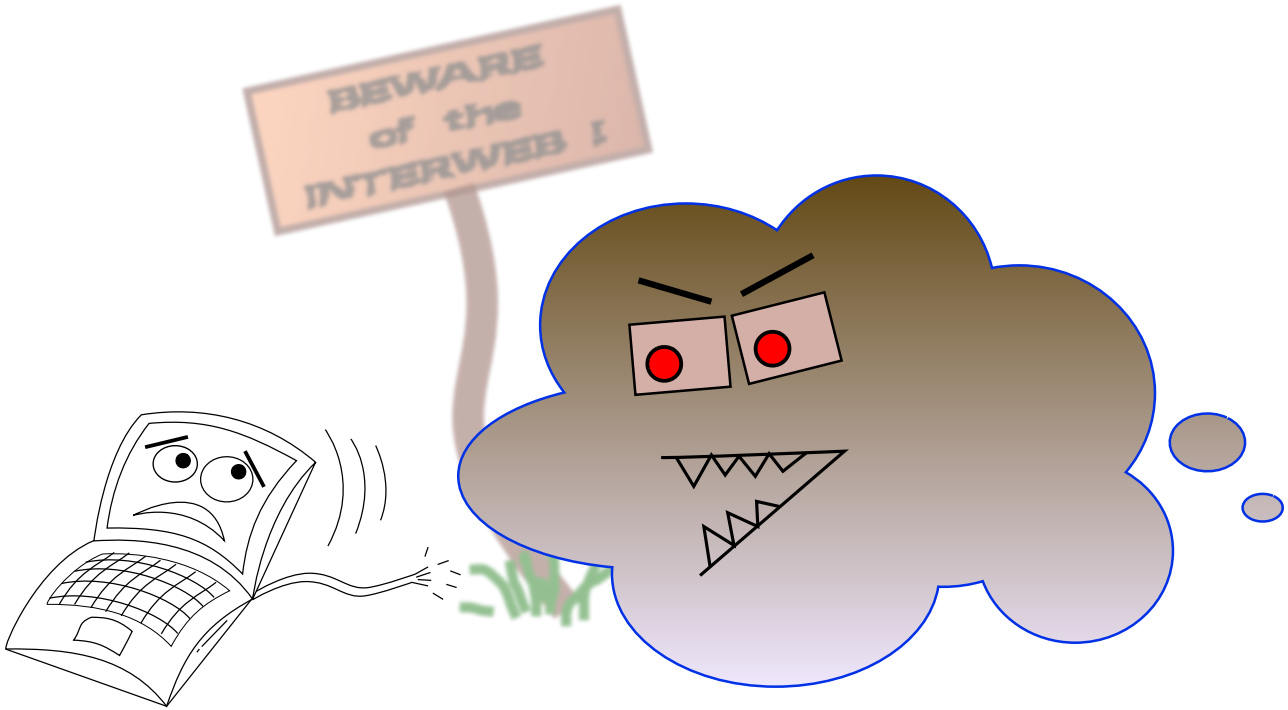
An introduction to tinc

Hamburg, July 28, 2014



Guus Sliepen

guus@tinc-vpn.org

Introduction

Communicating over the Internet

The problem of NAT

The problem of MTU

Other problems

Future plans for tinc

Authentiation and authorization

The end

Before September 1997:

- Bad support for network virtualization
- No IPsec
- PPP module:
  - You have to speak the PPP protocol
  - Or run pppd through something else (like SSH)
  - Very poor performance
- CIPE module
  - out-of-tree
  - Does everything inside the kernel
  - Very inflexible, hard to maintain

Introduction

Communicating over the Internet

The problem of NAT

The problem of MTU

Other problems

Future plans for tinc

Authentiation and authorization

The end

September 1997, Linux 2.1.53 is release.

- Introduces the Ethertap module
- ```
  modprobe ethertap
  ifconfig tap0 ...
  fd = open("/dev/tap0", O_RDWR);
  ```
- Several userspace projects start here.

Introduction
Communicating over the Internet
The problem of NAT
The problem of MTU
Other problems
Future plans for tinc
Authentiation and authorization
The end
  ```

The very beginning of tinc: "tapencaps"

- Read packets from tap device, send them to TCP socket.
- Read packets from TCP socket, send them to tap device.
- Rest is left to the user.

That's nice but what can you do with that?

- Set up a private network to a friend!

This was started by me.

Introduction

Communicating over the Internet

The problem of NAT

The problem of MTU

Other problems

Future plans for tinc

Authentiation and authorization

The end

The next stage: "vpnd"

- Turn tapencaps into a proper UNIX daemon.
- And make releases.
- And put source code into CVS.
- Slap the GPL license on it.

In short...

- Become an Open Source project.

This work was mostly done by Ivo Timmermans.

Introduction

Communicating over the Internet

The problem of NAT

The problem of MTU

Other problems

Future plans for tinc

Authentiation and authorization

The end

We used it for our own friend network.

- Everyone wants to be able to connect to each other.
- Try a hub-and-spoke setup.
- One vpnd per spoke.
- Hub gets a lot of traffic.
- Falls apart everytime the hub goes down.
- Soon we reach the limit of 16 Ethertap devices.

That's not good. What to do?

Introduction

Communicating over the Internet

The problem of NAT

The problem of MTU

Other problems

Future plans for tinc

Authentiation and authorization

The end

December 1998, project renamed "tinc".

January 1999, support for multiple connections:

- One daemon can connect to multiple other daemons
- One daemon still uses only one Ethertap device
- Tinc reads the IP header, routes packets.

This set tinc apart from other VPN projects.

Introduction
Communicating over the Internet
The problem of NAT
The problem of MTU
Other problems
Future plans for tinc
Authentiation and authorization
The end

Fast-forward - Current features:

- Connects multiple sites together
- Can act as router (layer 3) or switch (layer 2)
- Full support for IPv6
- No central server
- You configure some endpoints, tinc will do the rest

Modus operandi:

- Metadata exchanges via TCP
- VPN packets directly via UDP
- Fall back to TCP if UDP is not possible

Introduction

Communicating over the Internet

The problem of NAT

The problem of MTU

Other problems

Future plans for tinc

Authentiation and authorization

The end

The competition:

- CIPE†
- VTun†
- IPsec
- OpenVPN
- Hamachi

But also:

- GVPE
- CloudVPN
- SocialVPN
- n2n
- VDE

Introduction

Communicating over the Internet

The problem of NAT

The problem of MTU

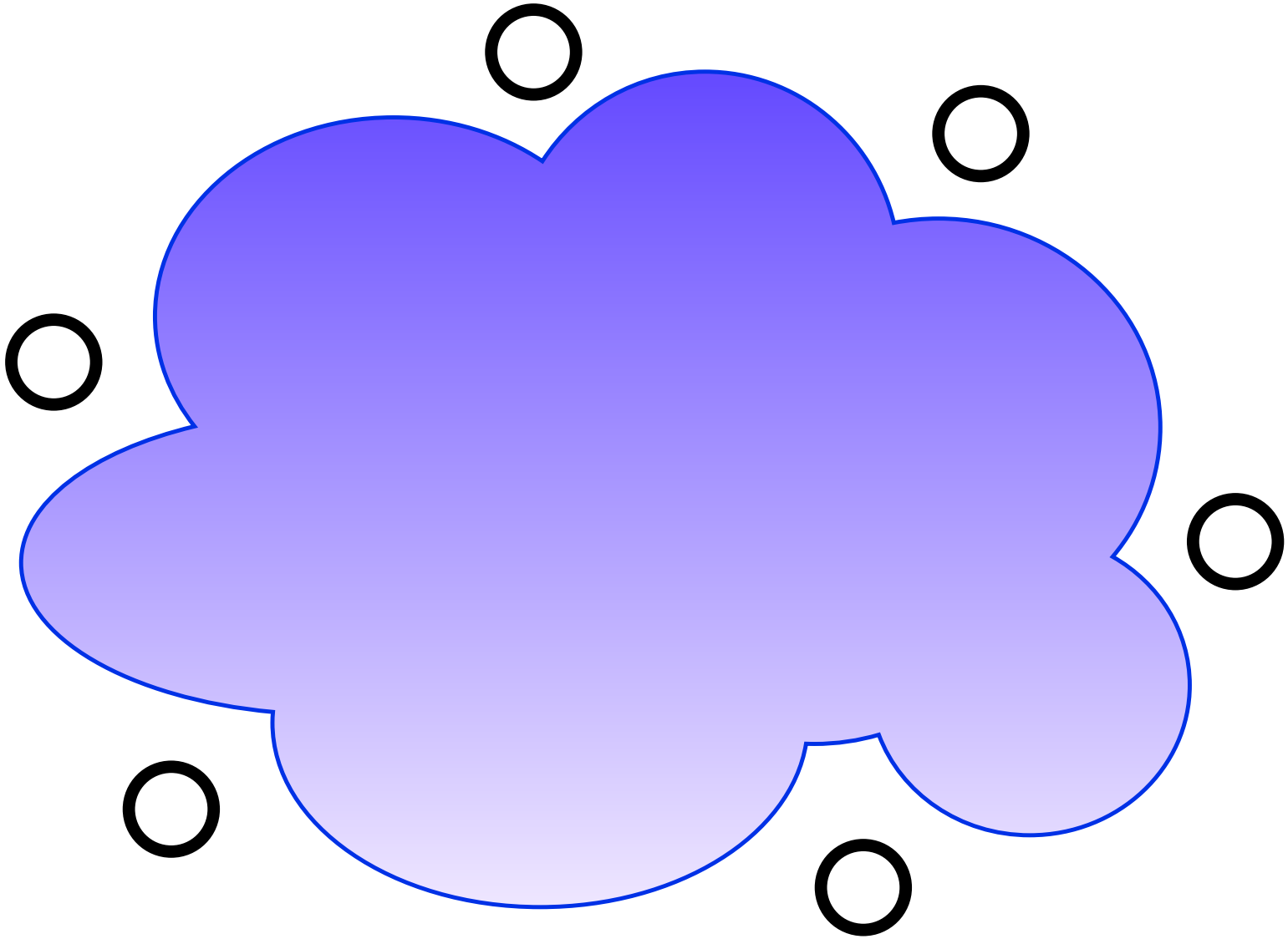
Other problems

Future plans for tinc

Authentiation and authorization

The end

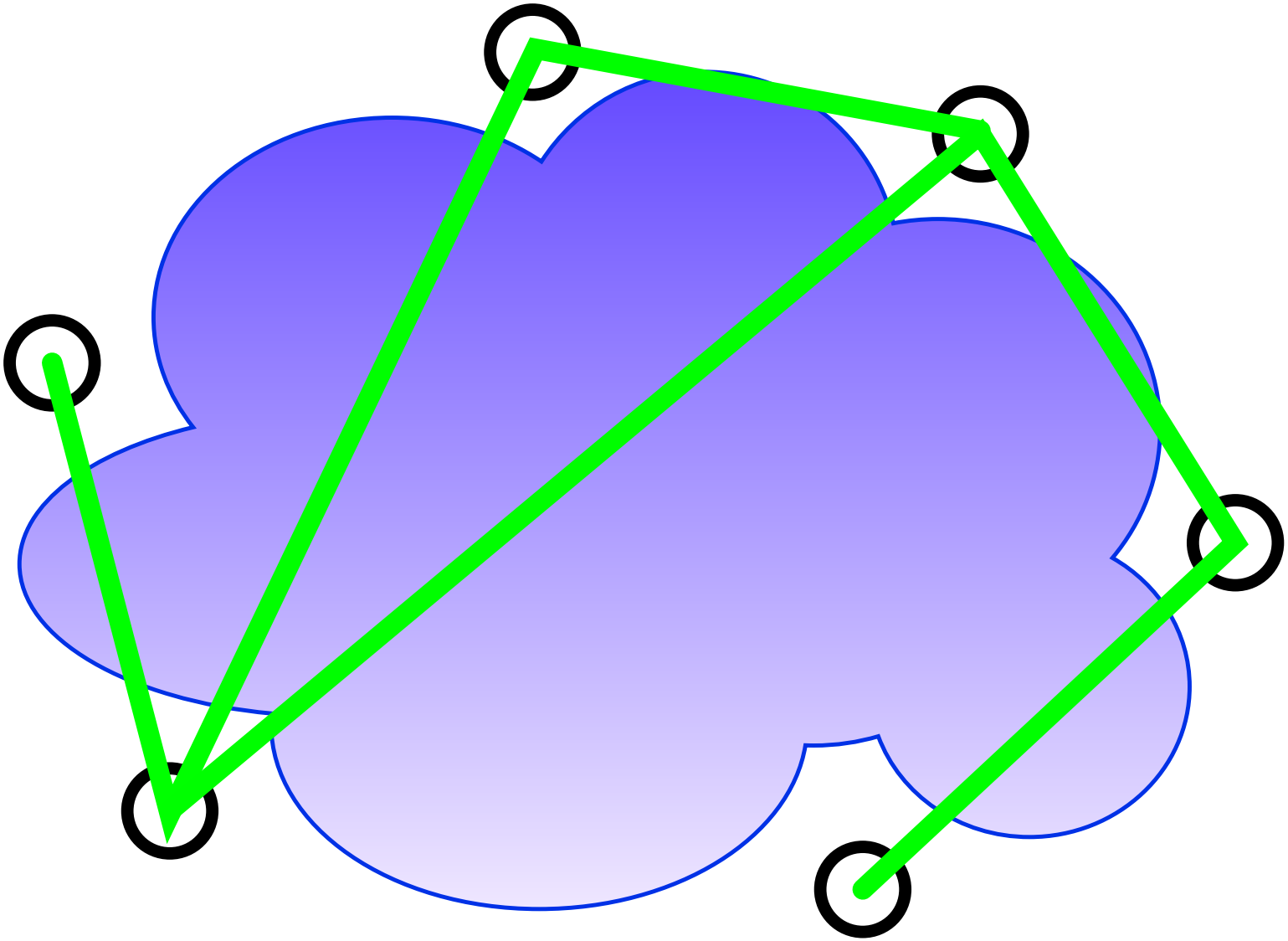
Network before VPN is configured:



Blue cloud: the Internet
Black circles: VPN nodes

Introduction
Communicating over the Internet
The problem of NAT
The problem of MTU
Other problems
Future plans for tinc
Authentiation and authorization
The end

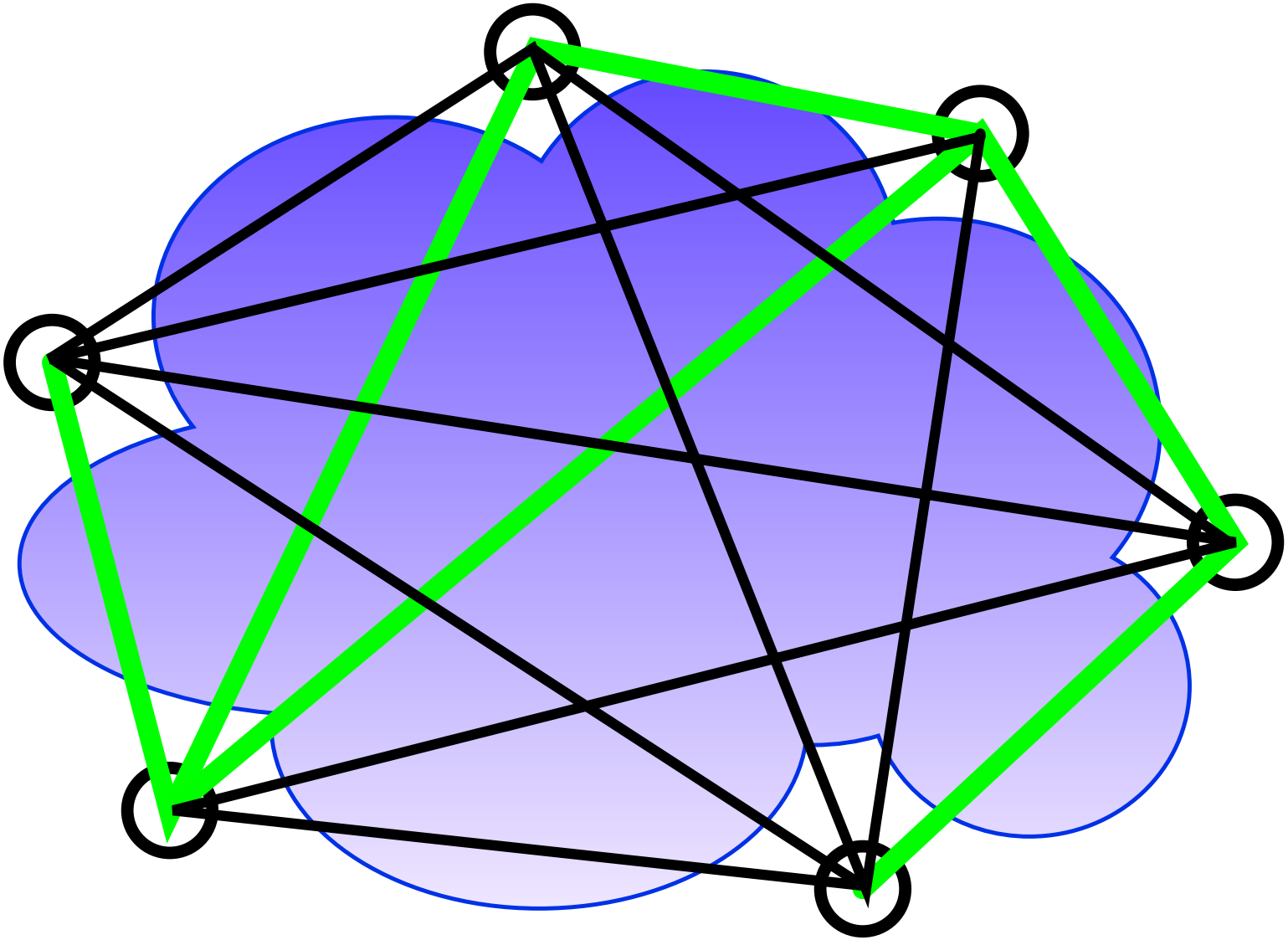
Initial connections configured by user:



Green lines: initial connections

Introduction
Communicating over the Internet
The problem of NAT
The problem of MTU
Other problems
Future plans for tinc
Authentiation and authorization
The end

Full mesh created by tinc:



Black lines: UDP tunnels

An introduction to tinc

Guus Sliepen

Introduction

Communicating over the Internet

The problem of NAT

The problem of MTU

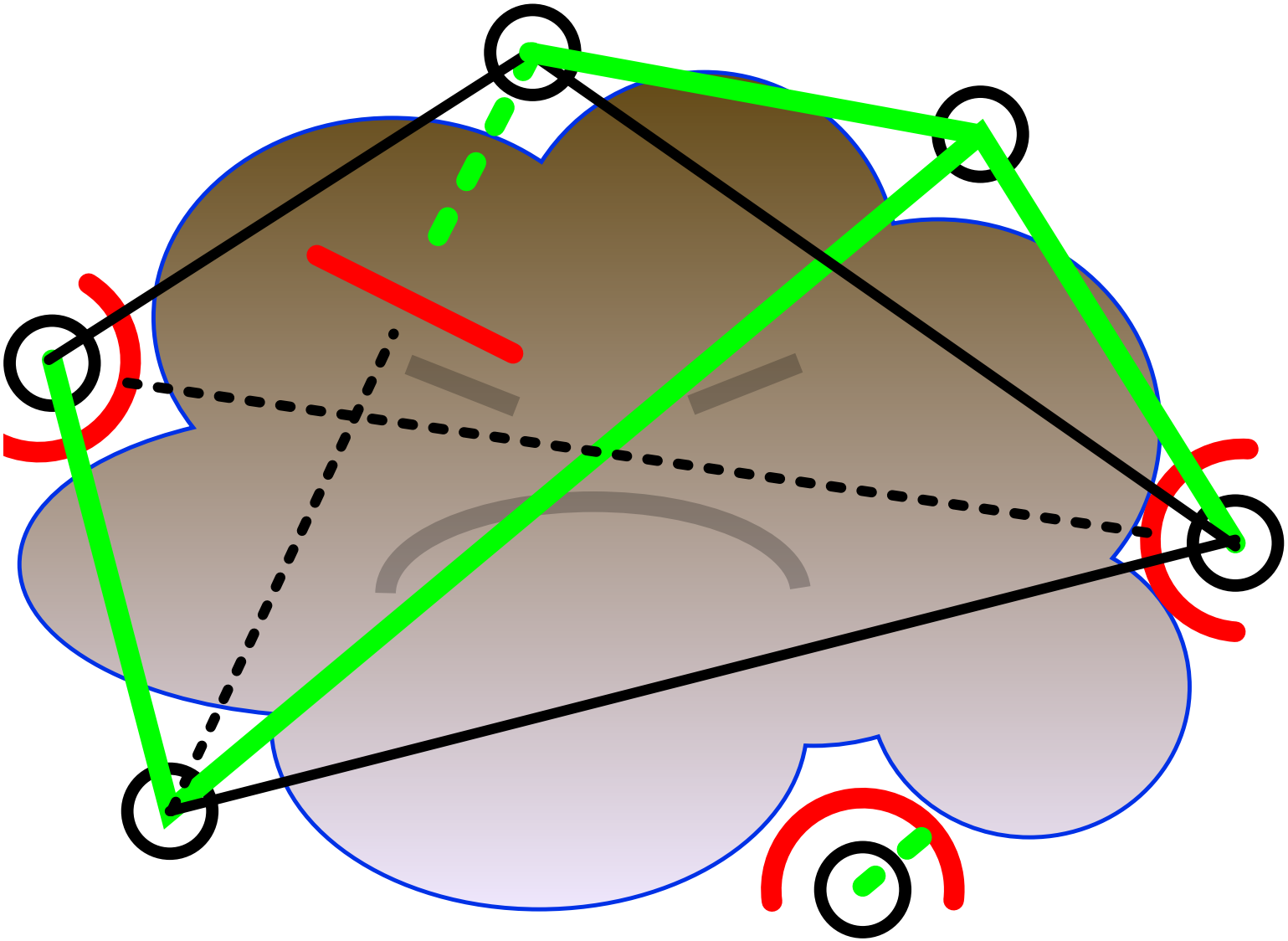
Other problems

Future plans for tinc

Authentiation and authorization

The end

Reality is not so nice:



Red arcs: NAT
Red line: ISP blocking traffic
Dotted lines: failed connections

An introduction to tinc
Guus Sliepen
Introduction
Communicating over the Internet
The problem of NAT
The problem of MTU
Other problems
Future plans for tinc
Authentiation and authorization
The end

The problem of NAT:

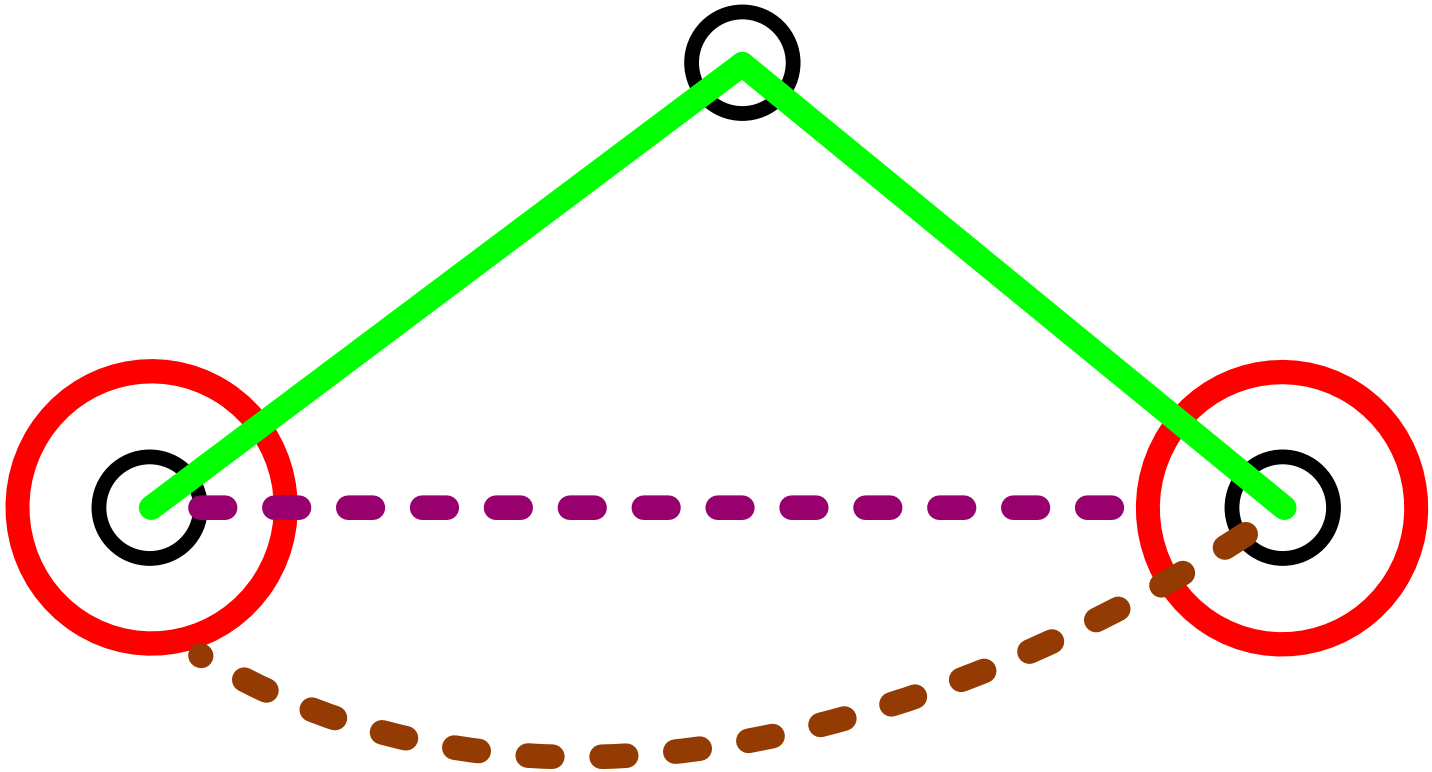
- Source address and port change
- Incoming connections blocked

Solutions:

- Routing via non-NAT node (not efficient)
- Port forwarding (not always possible, manual work)
- UPnP (needs router support, complex)
- STUN/ICE (not always possible, complex)

Introduction
Communicating over the Internet
The problem of NAT
The problem of MTU
Other problems
Future plans for tinc
Authentiation and authorization
The end

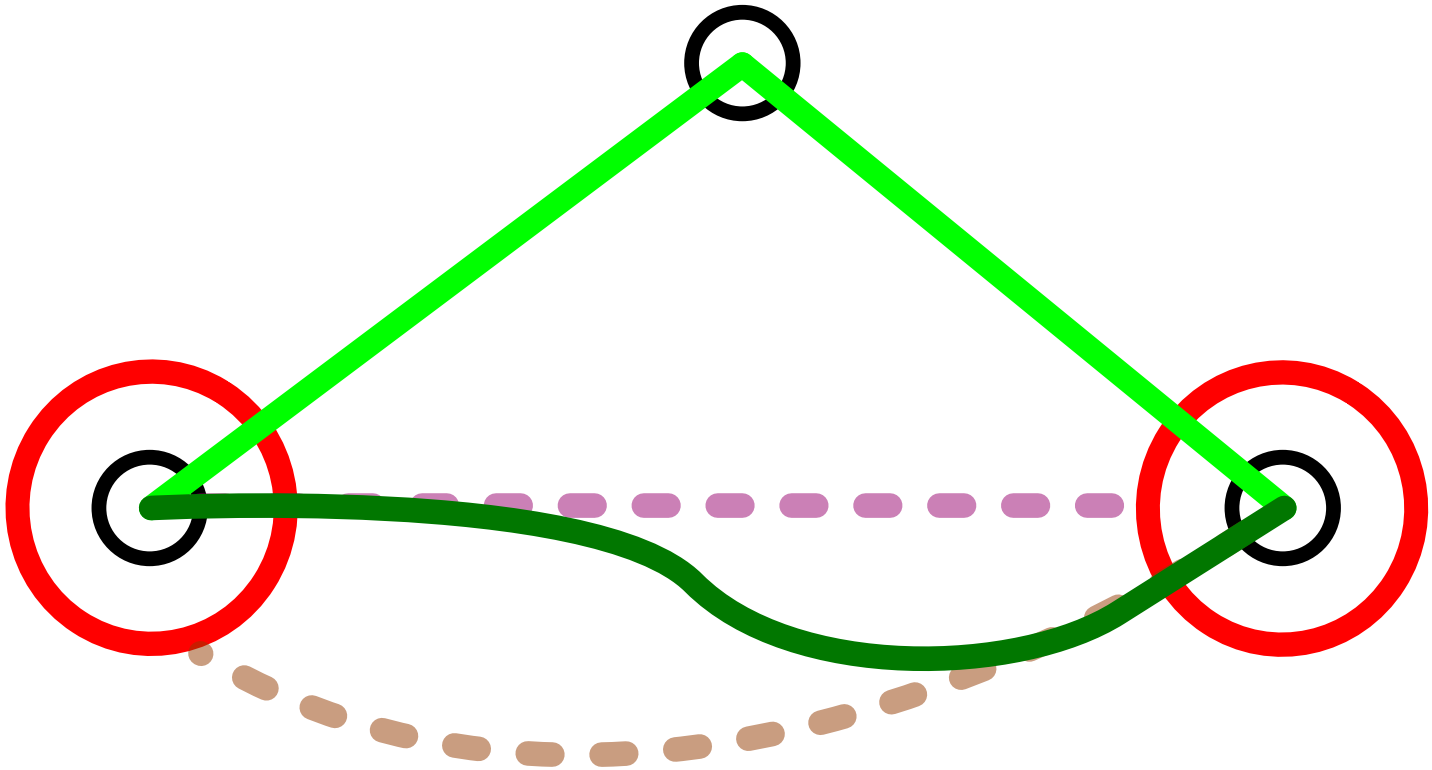
Two nodes behind NAT:



Both nodes can talk to a third node.
NAT changes ports, nodes cannot talk to each other.

Introduction
Communicating over the Internet
The problem of NAT
The problem of MTU
Other problems
Future plans for tinc
Authentiation and authorization
The end

STUN in action:

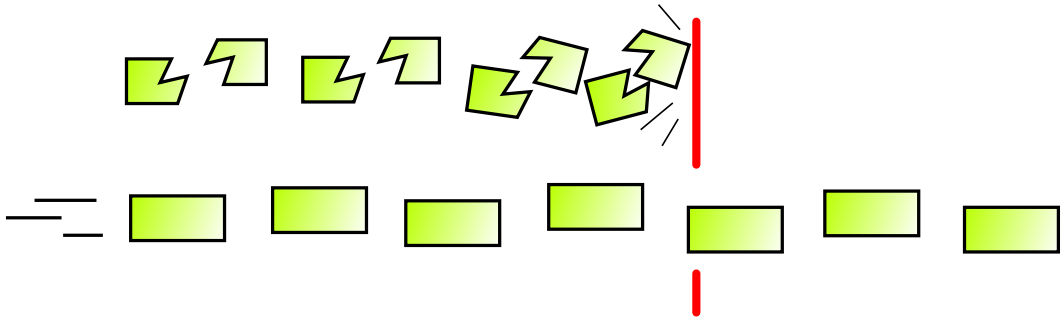


Third node tells other nodes about their addresses and ports.
Nodes connect to each other using this information.

Introduction
Communicating over the Internet
The problem of NAT
The problem of MTU
Other problems
Future plans for tinc
Authentiation and authorization
The end

The problem of packet fragmentation:

- MTU inside tunnel smaller than outside
- Outer layer fragments bad for performance
- Some firewalls/ISPs block fragments



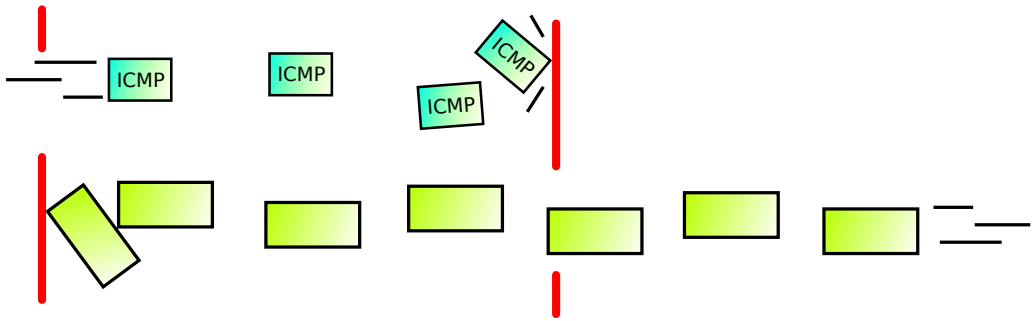
Solution:

- Determine path MTU between nodes
- Generate ICMP Fragmentation Needed packets
- Should work for all IPv4/IPv6 traffic
- Fall back to TCP for other traffic

An introduction to tinc
Guus Sliepen
Introduction
Communicating over the Internet
The problem of NAT
The problem of MTU
Other problems
Future plans for tinc
Authentiation and authorization
The end

The problem of firewalls/ISPs blocking ICMP:

- ICMP Fragmentation Needed does not work!
- Happens when network traffic leaves the VPN (for example, when having default gateway on VPN)



Solution:

- Clamp MSS field in TCP packets to path MTU
- Works only for TCP

Introduction
Communicating over the Internet
The problem of NAT
The problem of MTU
Other problems
Future plans for tinc
Authentiation and authorization
The end

Other problems:

- Frequently changing IP addresses
  - use dyndns
  - cache & forward known addresses between nodes
- Only allowing certain ports, like HTTP
  - tunnel over ICMP/DNS/HTTPS
- ISPs dropping/delaying small UDP packets
  - because they think it's VoIP!
  - severely slows down TCP streams inside tunnel

Introduction
Communicating over the Internet
The problem of NAT
The problem of MTU
Other problems
Future plans for tinc
Authentiation and authorization
The end

Version 1.1:

- Control a running tinc daemon (CLI, GUI)
- Greatly simplify setting up tinc
- Improve security (SPTPS)

Version 2.0:

- Get rid of the legacy protocol
- Decentralized authorization framework (next slides)

Introduction
Communicating over the Internet
The problem of NAT
The problem of MTU
Other problems
Future plans for tinc
Authentiation and authorization
The end

Authentication and authorization

- Authentication = proving who you are
- Authorization = proving you are allowed to do something

Two well known (mostly authentication) methods:

- X.509 certificates
  - centralized approach
  - focused on identities (LDAP like), and URLs
- OpenPGP keys
  - decentralized approach
  - focused on email addresses

Introduction
Communicating over the Internet
The problem of NAT
The problem of MTU
Other problems
Future plans for tinc
Authentiation and authorization
The end

We need OpenPGP-like features:

- Completely decentralized
- Web of trust

We need more than OpenPGP can offer:

- Authorise anything, not just email
- Everyone can add/remove authorizations
- Negative authorization: forbid things
- Group decisions

Introduction
Communicating over the Internet
The problem of NAT
The problem of MTU
Other problems
Future plans for tinc
Authentiation and authorization
The end

libfides: lightweight p2p authorization framework

- Create and maintain repository of many certificates
  "X said at time T that Y is allowed to do Z"
- Newer certificates overrule older ones
  "X said at time T+1 that Y is not allowed to do Z"
- Make it simple to query the repository
  "Is Y allowed to do Z?"

- Fast & easy synchronization of repositories
- Application does not need to know about crypto
- Libfides itself uses only ECDSA primitive

- Still in alpha stage.

Introduction
Communicating over the Internet
The problem of NAT
The problem of MTU
Other problems
Future plans for tinc
Authentiation and authorization
The end

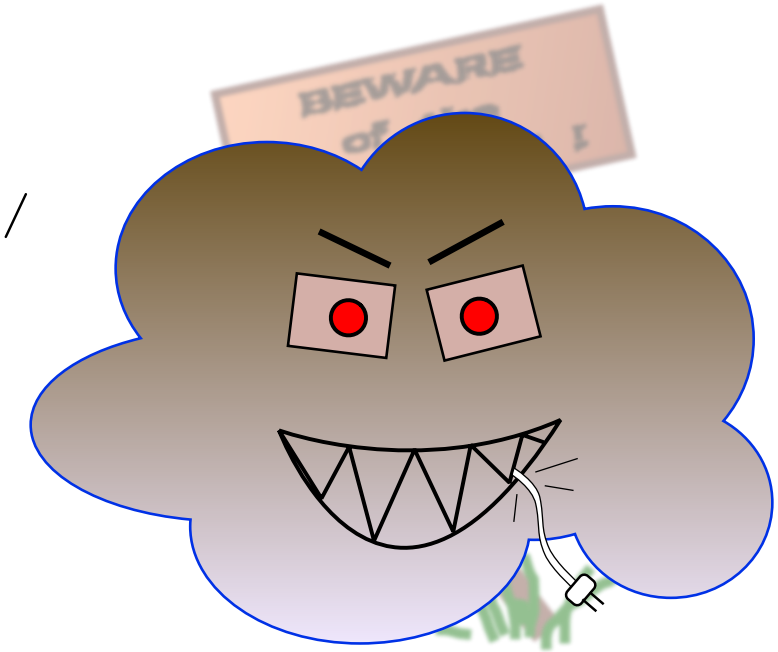
Conclusions:

- Tinc has come a long way since 1997.
- The Internet eats your packets.
- Lots of techniques necessary to work around it.
- Distributed authorization is a challenge.

That's it.

- Questions?

Visit the website:
`http://tinc-vpn.org/`



Introduction
Communicating over the Internet
The problem of NAT
The problem of MTU
Other problems
Future plans for tinc
Authentiation and authorization
The end