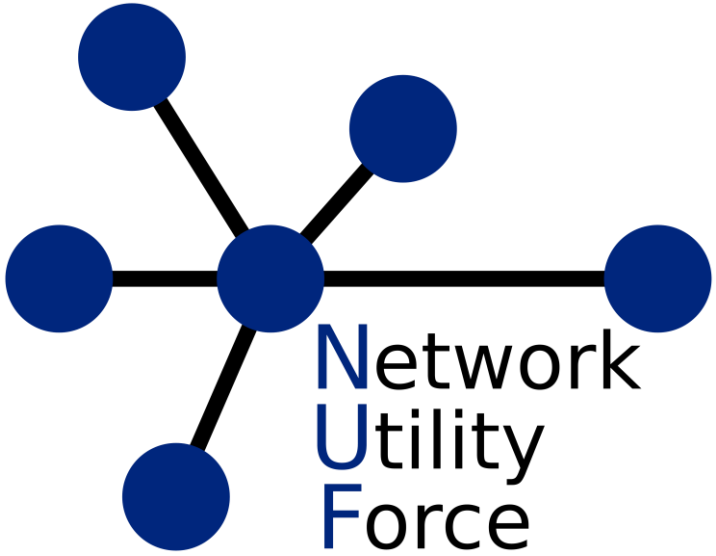



# NAT64
# Demonstration Deployment

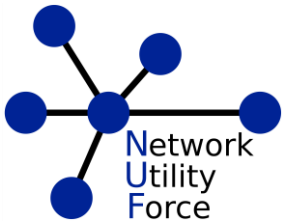
RMv6TF 2013

Demo network was available during the live presentation

Notes have been added to slides 30-32 to clarify FTP issues.

# Agenda

- Introduction
- Problem Statement
- NAT64 Concepts
- Demo Setup
- NAT64 Experience
- Conclusion



# Core Values and Beliefs

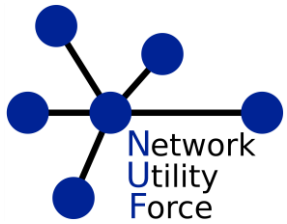
Network Utility Force believes that, above and beyond our experience, it's our values that drive our success in both business and life. As such, NUF has adopted a system of Core Values & Beliefs that we live by:

- We respect the individual, and believe that individuals who are treated with respect and given responsibility respond by giving their best.
- We require complete honesty and integrity in everything we do.
- We make commitments with care, and then live up to them. In all things, we do what we say we are going to do.
- Work is an important part of life, and it should be fun. Being a good business person does not mean being stuffy and boring.
- We are frugal. We guard and conserve the company's resources with at least the same vigilance that we would use to guard and conserve our own personal resources.
- We insist on giving our best effort in everything we undertake.
- Furthermore, we see a huge difference between "good mistakes" (best effort, bad result) and "bad mistakes" (sloppiness or lack of effort).
- Clarity in understanding our mission, our goals, and what we expect from each other is critical to our success.
- We are believers in the Golden Rule. In all our dealings we will strive to be friendly and courteous, as well as fair and compassionate.
- We feel a sense of urgency on any matters related to our customers. We own problems and we are always responsive. We are customer driven.

Permission to use these values granted by their creator, Charles Brewer of MindSpring.

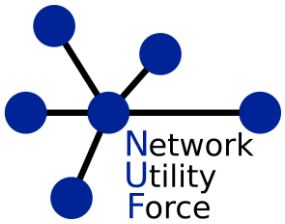
Network
Utility
Force

# INTRODUCTION



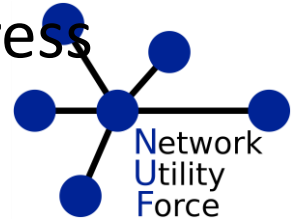
# NUF Tenets

- Our reputation is EVERYTHING, without it, we are worthless
  - We will ALWAYS advise our clients on what we believe is the right answer for them without exception
- Vendor neutral – The right tool for the right job
  - Cisco, Juniper, Brocade, HP, Huawei, A10, Dell (Force10), Extreme, Vyatta, ADVA, Arista, Alcatel, etc., etc
- No hardware sales, 100% professional services
- No geographical boundaries, we go where we are needed



# Who is NUF?

- Founded in December of 2011
- 6 principal consultants/owners
- Numerous specialist contractors
- Example experience
  - Recently highlighted by local news for deployment of community wifi network sponsored by Google
  - Consulting for Ethiopia TLD
  - Netrail, MindSpring, Comcast, Internap, numerous small service providers
  - ARIN, NANOG, IETF participation
- IPv6 training, architecture, deployment and address management



# Overview

**Leader in Application Networking**

**Profitable with consistent growth**

**Flagship Product**

***AX Series Platform***

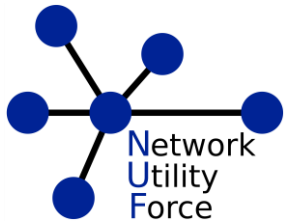
**Founded Q4/2004**

*Lee Chen, Founder of Foundry & Centillion Networks*

**500+ employees**
**Customers in over 35 countries**

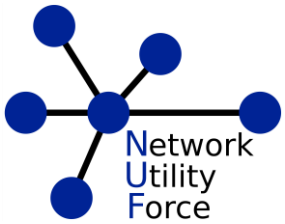
Network Utility Force

# PROBLEM STATEMENT



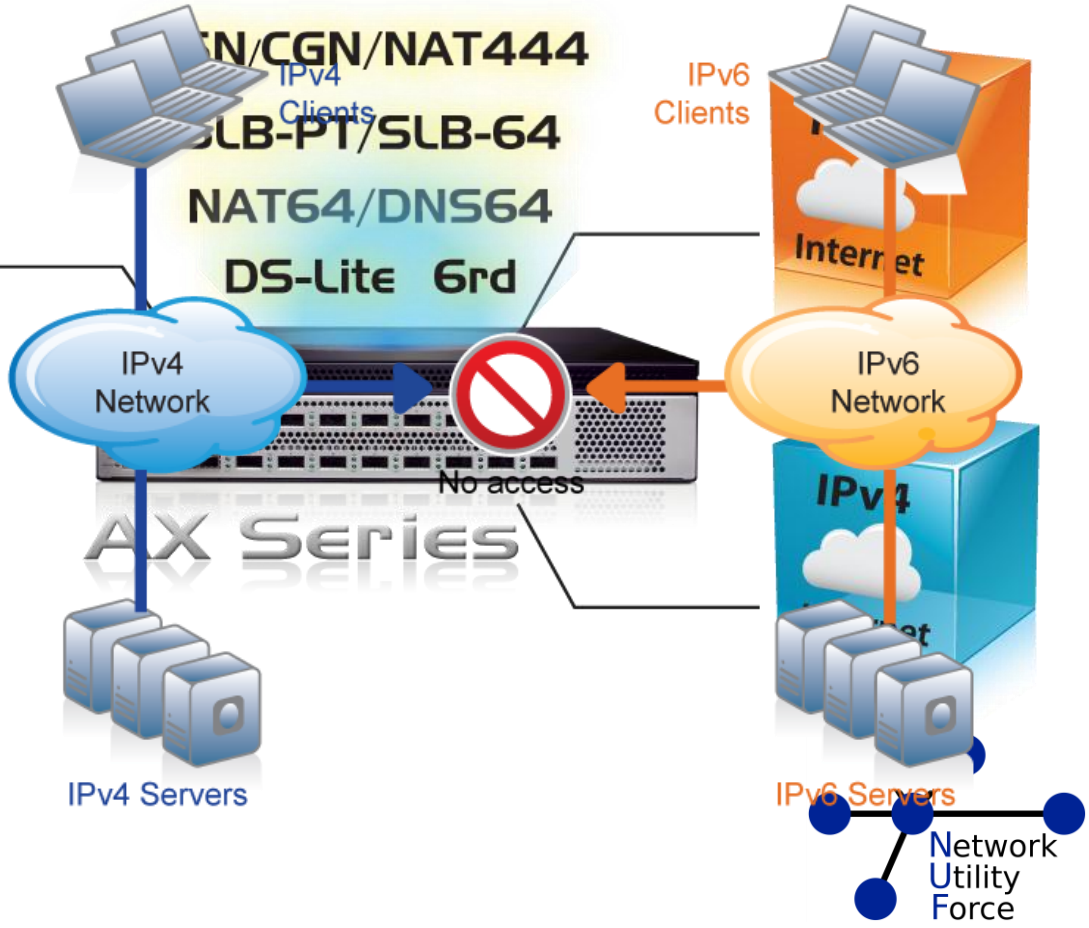
# Problem Statement

I have run out of IPv4 addresses and need to find a way to provide Internet access to my clients. My core network supports IPv6, but there are many IPv4-only resources my clients need to reach. I want to go with IPv6 because I want to future-proof my internal network, however I understand I need connectivity to IPv4 resources for quite some time.



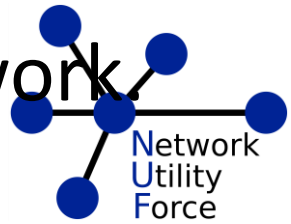
# IPv4 Exhaustion and IPv6 Migration Solutions

- No standard compatibility
- Different requirements
  - Home
  - Enterprise
  - Service Provider
- "IPv4 Legacy Networks"

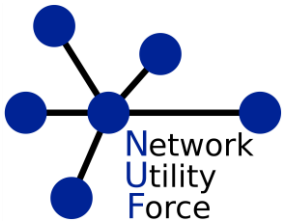
# Transition Mechanisms

- Dual Stack – All network links and hosts have both IPv4 and IPv6 addressing, all traffic is native to its protocol
- Dual Stack – Lite (DS-Lite) – Allow distribution network (including CPE) to have ONLY IPv6 addressing.
- NAT64 – Translate IPv6 into IPv4 and vice versa.
- 6rd – Carry IPv6 across an IPv4-only network.

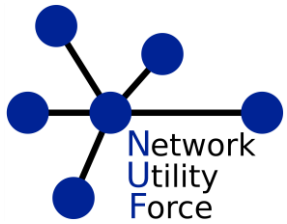


# Protocol Translations

- May prefer to use IPv6-IPv4 protocol translation for:
  - new kinds of Internet devices (e.g., cell phones, cars, appliances)
  - benefits of shedding IPv4 stack (e.g., serverless autoconfig)
- Simple extension to NAT techniques, to translate header format as well as addresses
  - IPv6 nodes behind a translator get full IPv6 functionality when talking to other IPv6 nodes located anywhere
  - Get the normal (i.e., degraded) NAT functionality when talking to IPv4 devices
  - Drawback : minimal gain over IPv4/IPv4 NAT approach
  - Drawback : no support for legacy IPv4-only devices

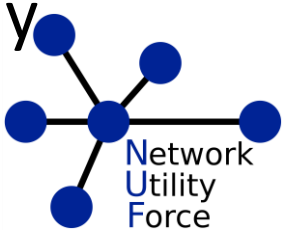


# NAT64 CONCEPTS



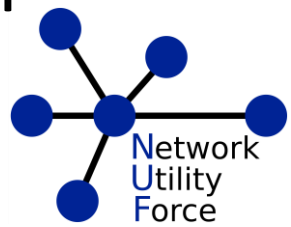
# NAT64 and DNS64

- Provides stateful translation between IPv6 and IPv4 traffic when that traffic is initiated by an IPv6-only node
  - NAT64 translates IPv6 and IPv4 traffic
  - DNS64 maps IPv6-only address record (AAAA) DNS queries to IPv4 address record (A) queries
- Makes it possible for IPv6-only nodes to initiate communications with IPv4-only nodes with no changes to the IPv6-only node and the IPv4-only node



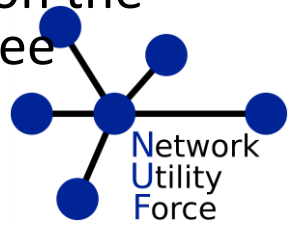
# NAT64

- No host or CPE support necessary
- No IPv4 address at all required on the CPE or host to access IPv4 resources (compare with DS-Lite which requires RFC1918 addresses)
- Host gets only an IPv6 address
- NAT44 issues for IPv4 traffic still apply including session start from behind the NAT to establish state and ALGs are necessary for many protocols



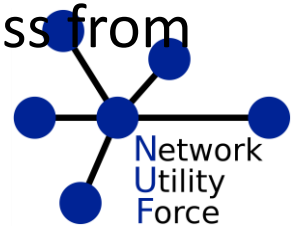
# NAT64 cont'd

- Workstation (which has only IPv6) requests communication with a IPv4-only site (www.example.com)
  - It asks for a AAAA record since it is IPv6 only
- DNS server (DNS64) first tries a AAAA query. If one exists, it is passed to the client and the client communicates with the site via IPv6. If no AAAA record exists, the DNS64 functionality will translate an A record into a AAAA.
  - To translate, the DNS64 server must know the prefix in use in the network for NAT64
    - Can be assigned by administrator
    - Can use well-known prefix 64:ff9b::/96
  - When using a /96, simply concatenate the IPv4 address on the end (more complex rules available for shorter prefixes, see RFC6052)

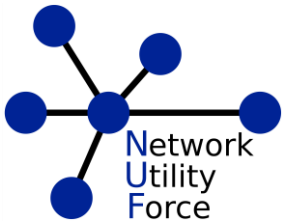


# NAT64 cont'd

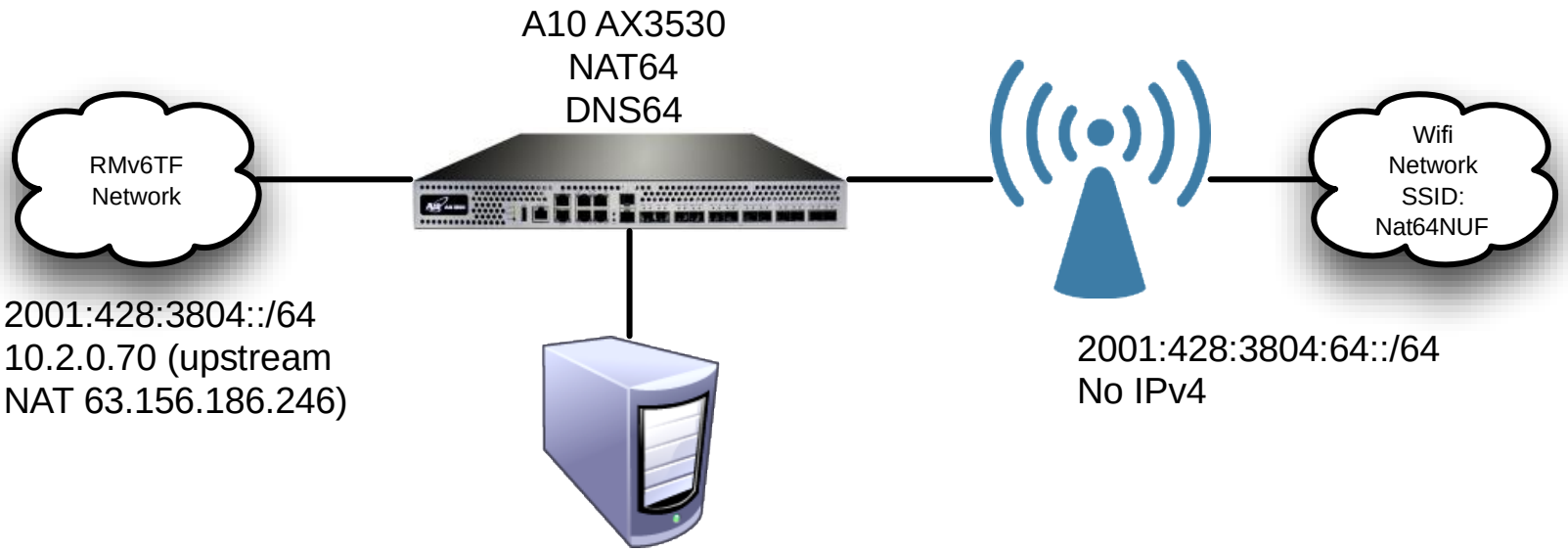
- The workstation, having received a AAAA for www.example.com initiates a TCP session with that IPv6 address
- The NAT64 device has the IPv6 prefix just discussed routed to it (could be OSPF, BGP, etc.)
- The NAT64 device recognizes that this address is an encapsulated IPv4 address
  - Adds NAT state if necessary
  - Strips the prefix to find the IPv4 destination address
  - Translates other parts of the header
  - Sends packet to IPv4 host using a source IPv4 address from a local pool



# DEMO SETUP



# Demo Topology



# A10 Config Bits

## Inside config

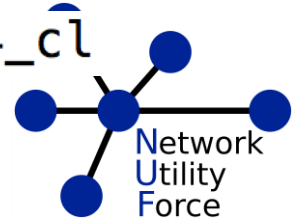
```
interface ve 64
 ipv6 address 2001:428:3804:64::1/64
 ipv6 nat inside
 ipv6 ndisc router-advertisement other-configuration-flag enable
 ipv6 ndisc router-advertisement prefix 2001:428:3804:64::/64
 ipv6 ndisc router-advertisement enable
```

## Configure NAT pools

```
ip nat pool dns64pool 10.2.0.71 10.2.0.71 netmask /24  gateway 10.2.0.152
ip nat pool nat64pool2 10.2.0.72 10.2.0.72 netmask /24  lsn
```

## Configure NAT using the well-known prefix

```
nat64 prefix well-known inside source class-list nat64_cl
```

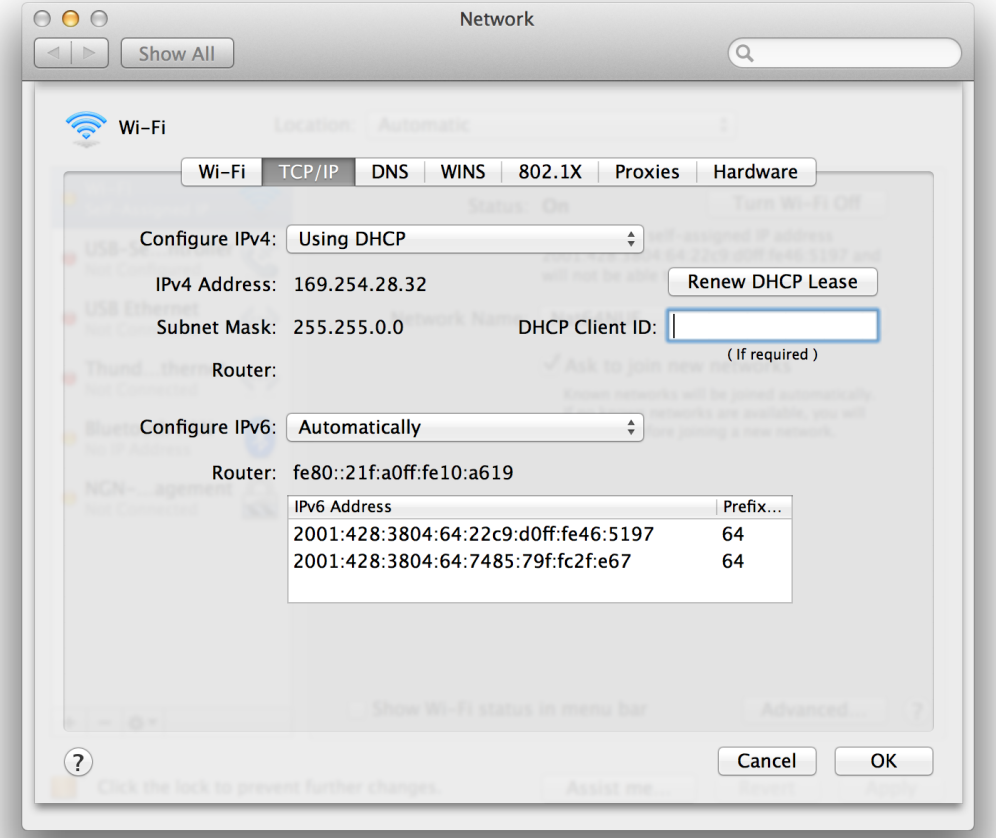


# A10 Config Bits

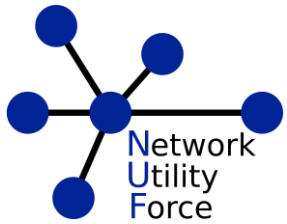
```
lb server localdns-rs 8.8.8.8
  port 53  udp
lb server localdns-rs1 10.2.0.10
      weight 100
  port 53  udp

lb service-group dns53 udp
   member localdns-rs1:53 priority 10
   member localdns-rs:53


lb template dns dns64-temp
   dns64

lb virtual-server dns_vs 2001:428:3804:64::64
  port 53  dns-udp
     source-nat pool dns64pool
     service-group dns53
     template dns dns64-temp
```

# Demo Setup

Join the network using SSID:  Nat64NUF

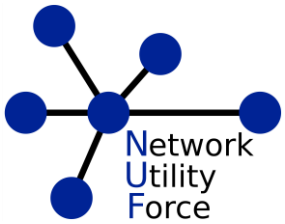


# NAT64 EXPERIENCE



# What works?

- Nearly everything
  - A10's implementation was solid, no signs of bugs or performance problems
  - Operating systems: Windows, MacOS, Linux
  - Nearly all classic IP protocols:  POP, IMAP, SSH, Telnet, Standard web stuff, SMTP
  - Many chat protocols:  Google talk, FaceBook chat
  - Entertainment:  Pandora web client, Netflix, YouTube, Hulu



# IOS is Weird

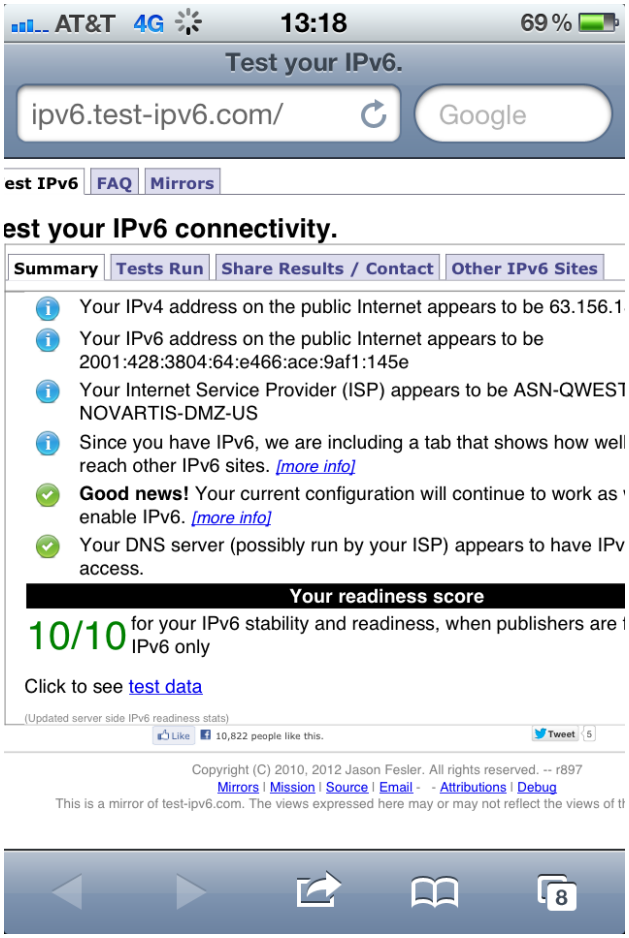

We appear to be connected

# IOS is Weird


Seems to be stuck in the process of connecting…

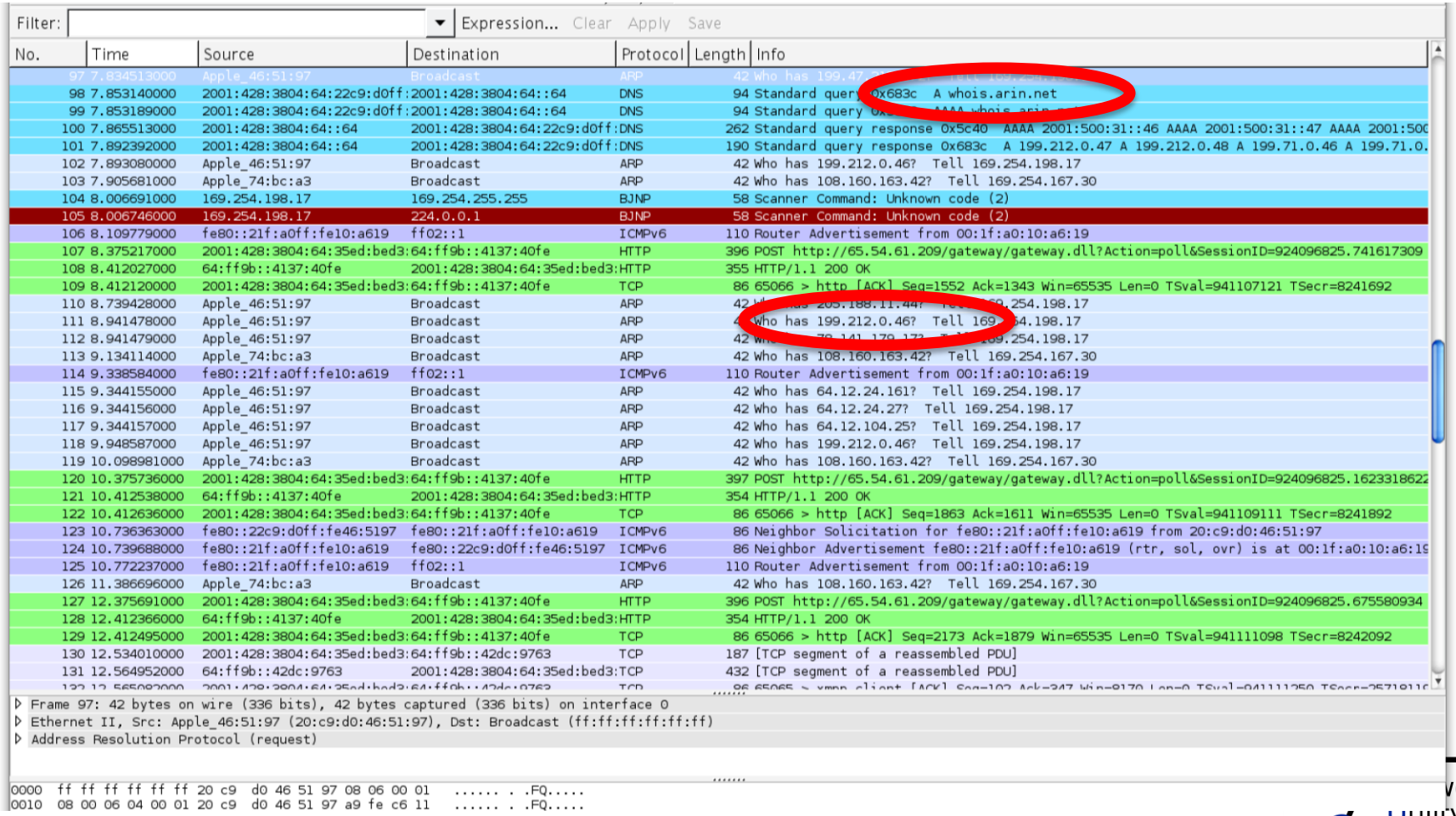
Network Utility Force

# IOS is Weird



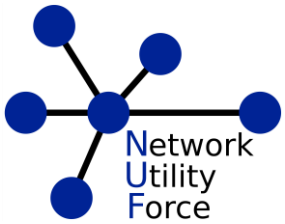

But look, it worked!

# Whois broken??

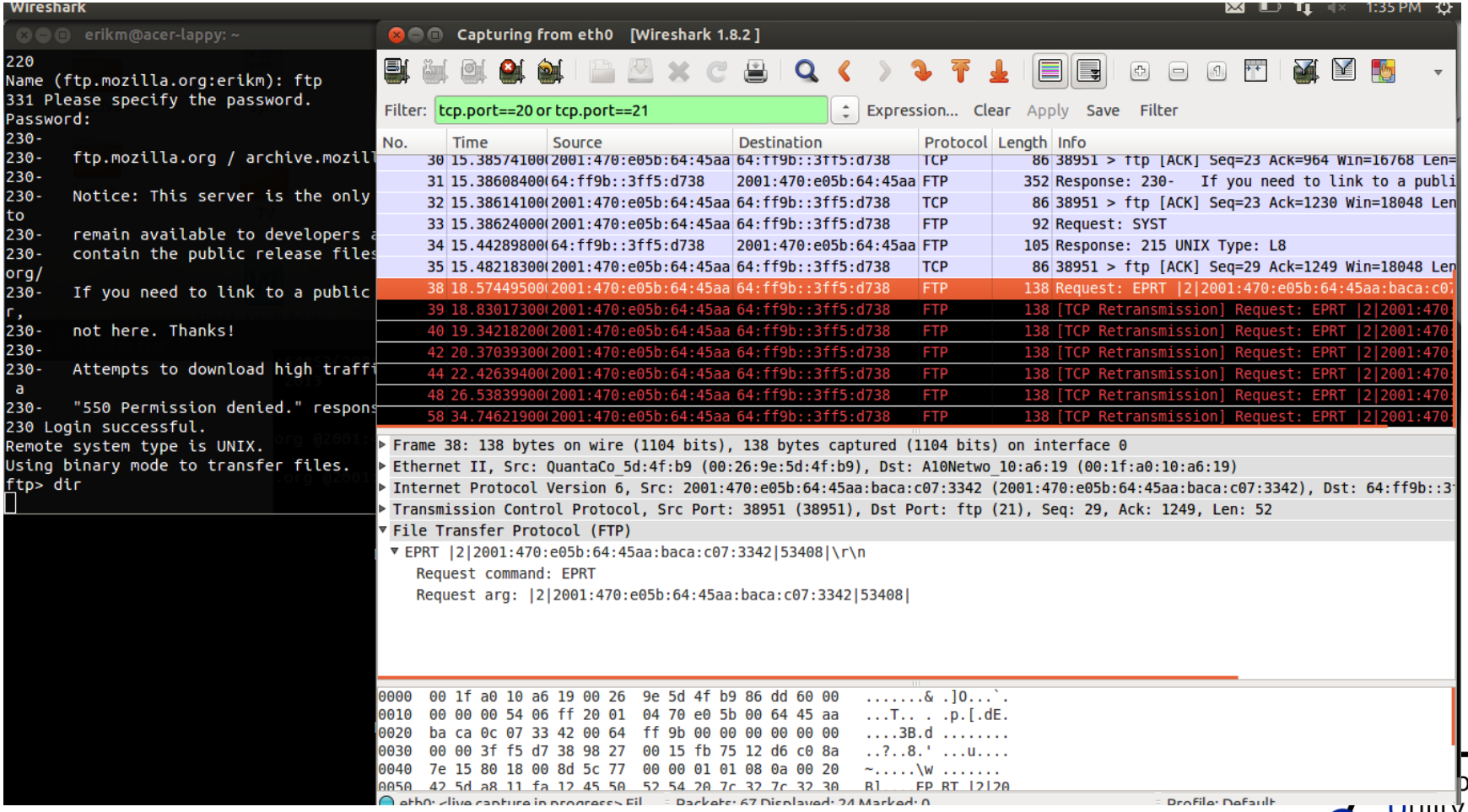


# Whois

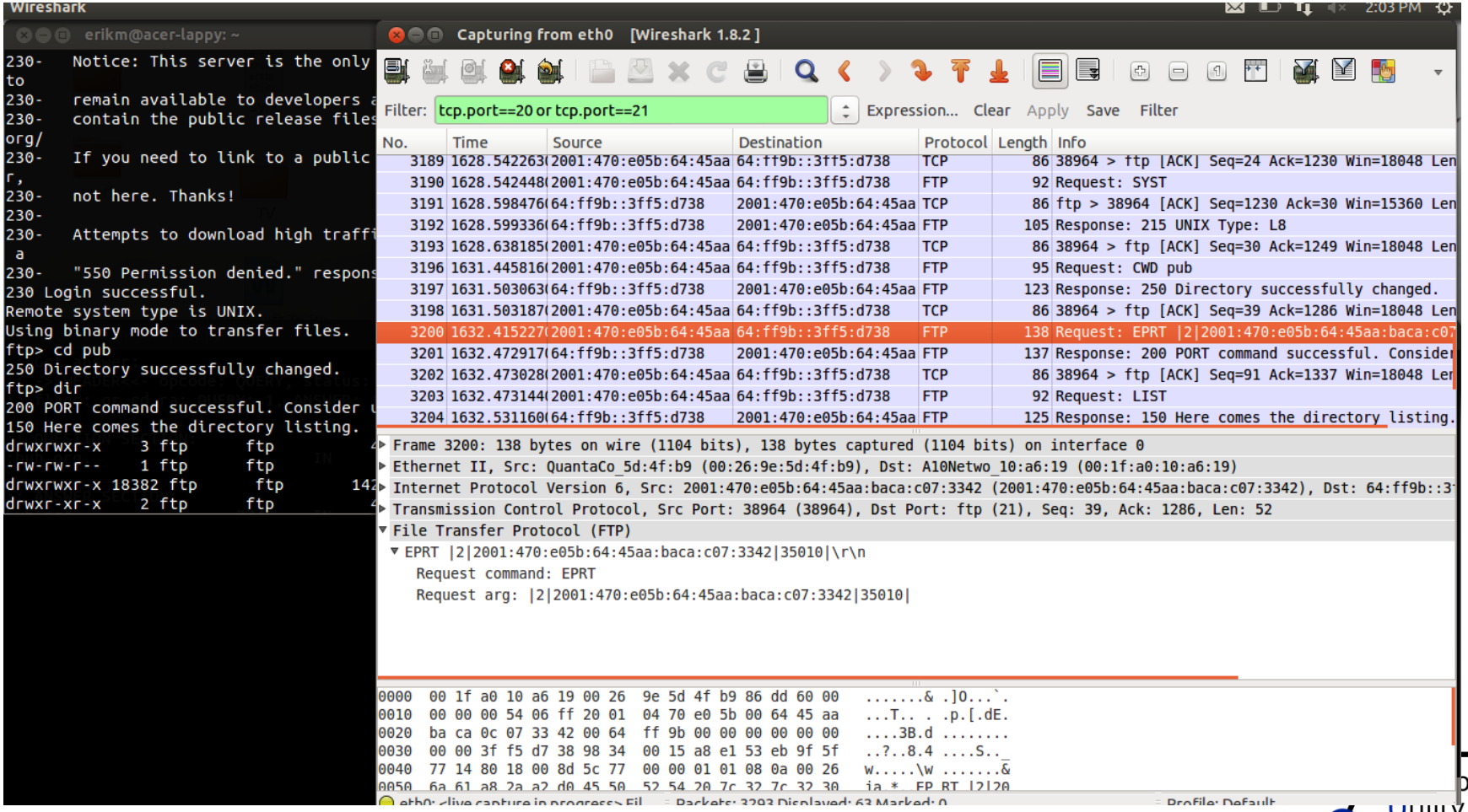
- A few whois attempts later, everything was working
- Does it depend on if the AAAA or A record comes back first?



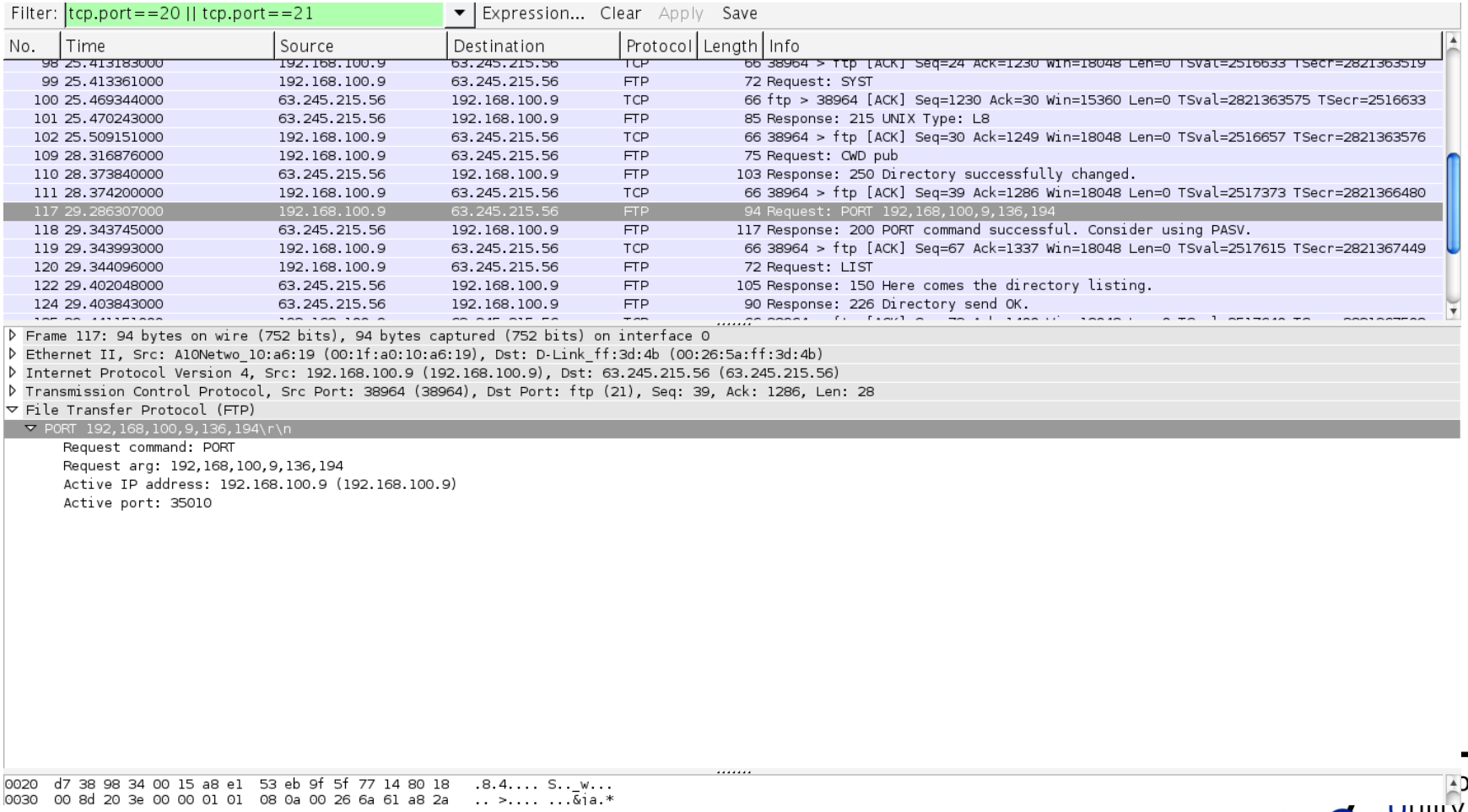
# FTP before ALG



# FTP with ALG, Outside

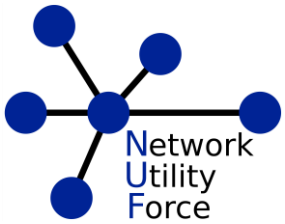


# FTP with ALG, Inside



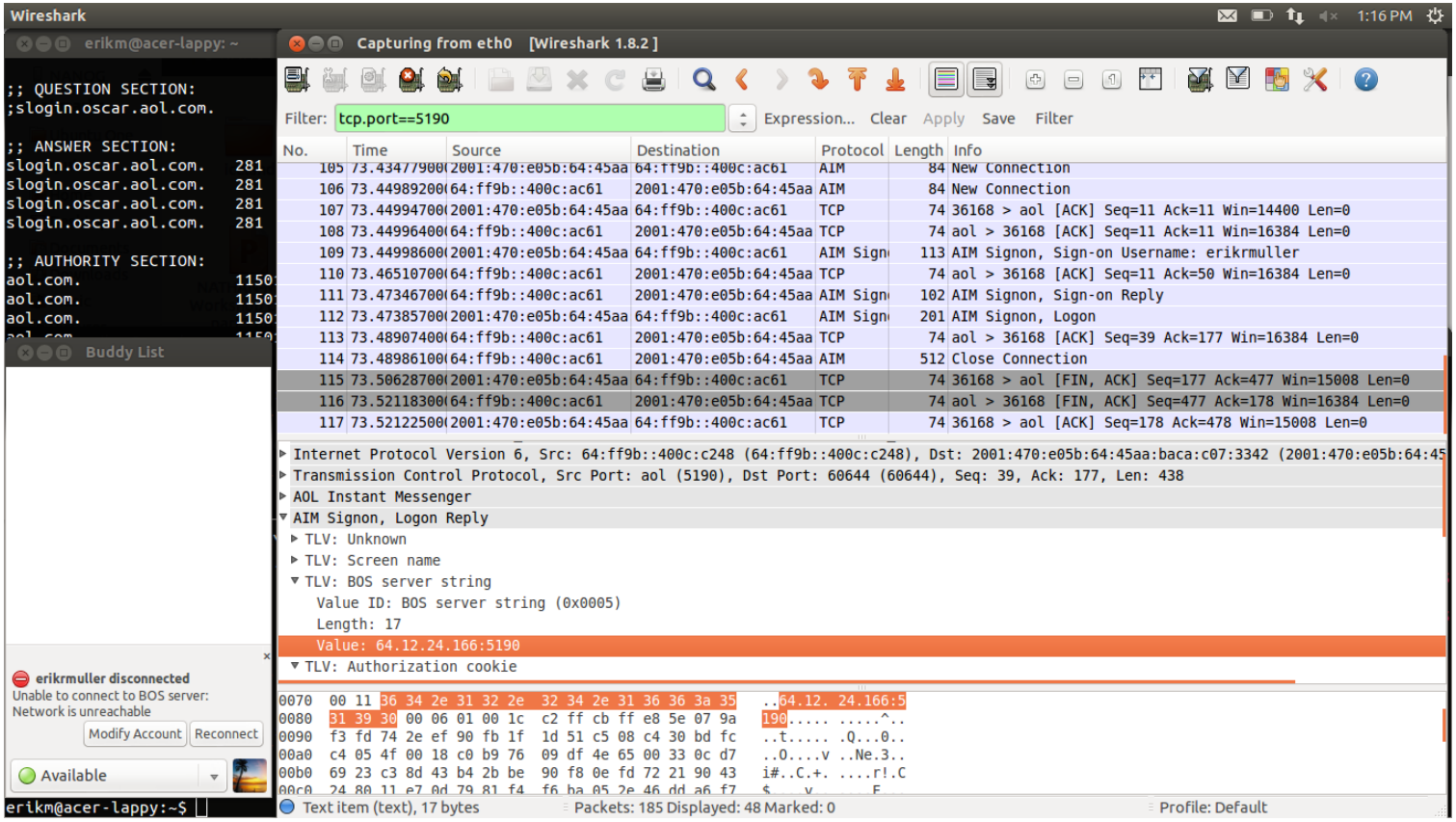
# What doesn’t work?

- All Android based devices we tried did not function
  - We suspect that Android performs an IPv4 connectivity specific test and reject networks that doesn’t have IPv4
  - We also suspect that Android will not consider DNS over IPv6 transport



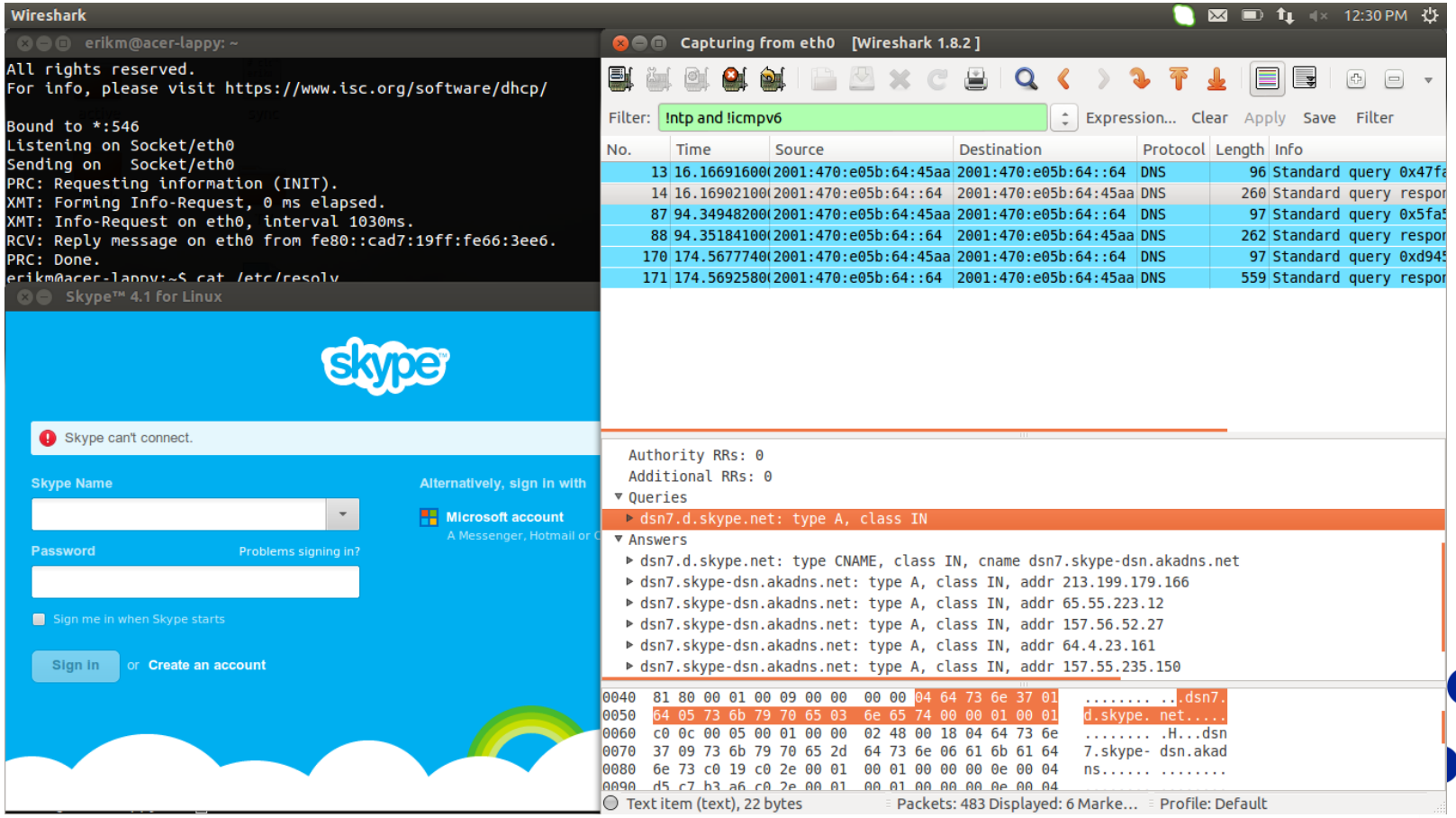
# AOL Instant Messenger

Won’t connect to the server, why?



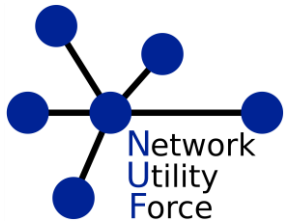
# Skype

## Also won’t connect to the Skype network



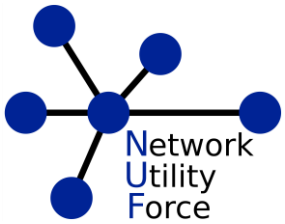

Network Utility Force

# CONCLUSION

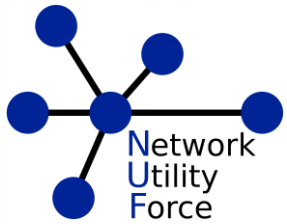


# NAT64 is good

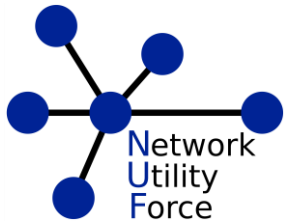
- Works for most apps
- Most of the non-working apps seem reasonably fixable
- Very good vendor support from A10



# Thanks!!

# Q and A



# Download the presentation here:

Network Utility Force

Brandon Ross – Chief Network Architect – Network Utility Force – bross@netuf.net
Erik Muller – Network Architect – Network Utility Force – em@netuf.net
René Paap - Technical Marketing Engineer – A10 network – rpaap@a10networks.com

Network Utility Force