# Networking


- Adam Schechter
- Precision Consulting / Precision Audio Visual
- adam@pav.us.com

# ENGINEERING FACT

**There are two kinds of people:**

**Those who can extrapolate from incomplete data.**

# “As my wife says”

- “Hi My name is Adam
  - your network sucks “

| Concept | Action | Goal | Tool |
|---|---|---|---|
| Monitoring | Analysis | Uptime | Watchman Monitoring / R-U-On |
| Monitoring | Tracking/Support | Uptime/Trend | Intermapper / Solarwinds |
| Monitoring | Point in Time/Net | Issue Resolution | Wireshark |
| Monitoring | Point in Time/One | Issue Resolution | Debookee |
| Analysis | Network Scan/Mac | Who is there | iNet / LanScan/ ARD |
| Analysis | Network Scan/iOS | Who is there | SubnetInsight |
| Long Term Analysis | Forensic Analysis | Sample ALL or Some Traffic | NetFlow / sFlow |

# Network Cabling

- Category Cable
  - Cat 5, 5e, 6, 6e, 6a ( Augmented )
    - Summary: Therefore, install Cat6,  OM3/4
- Best Practices
  - Optimize for Maintainability

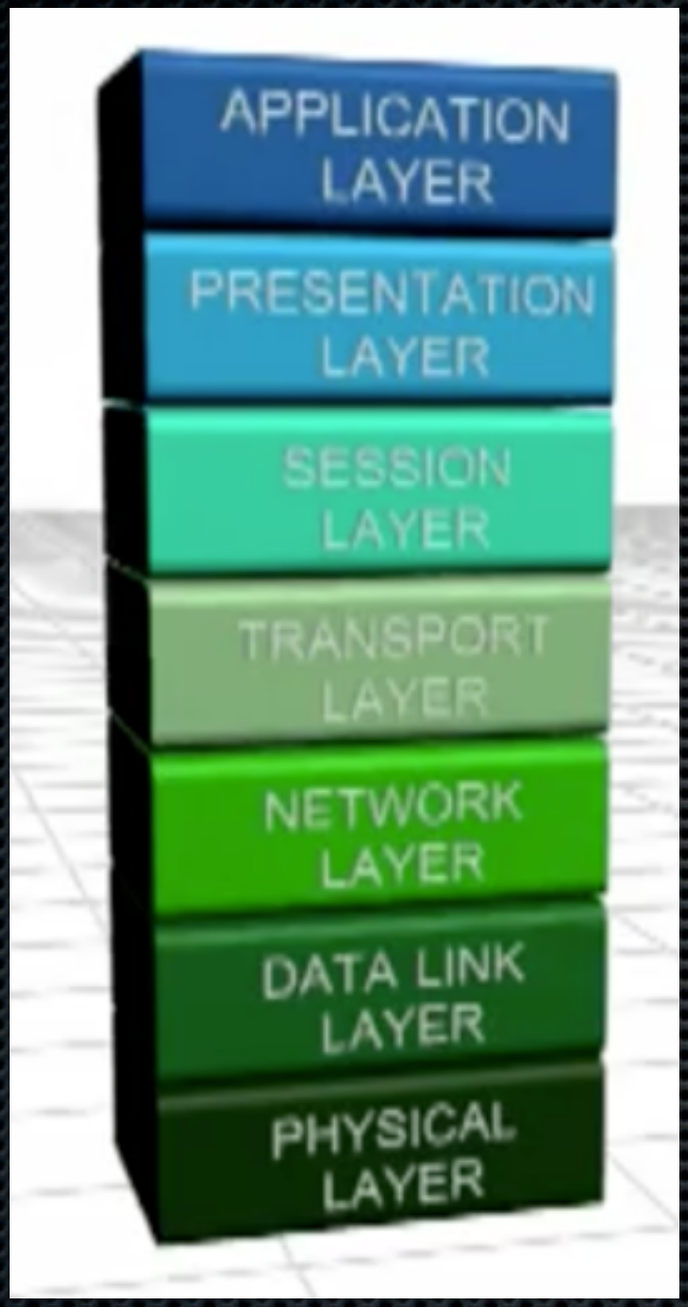
# Network Dressing

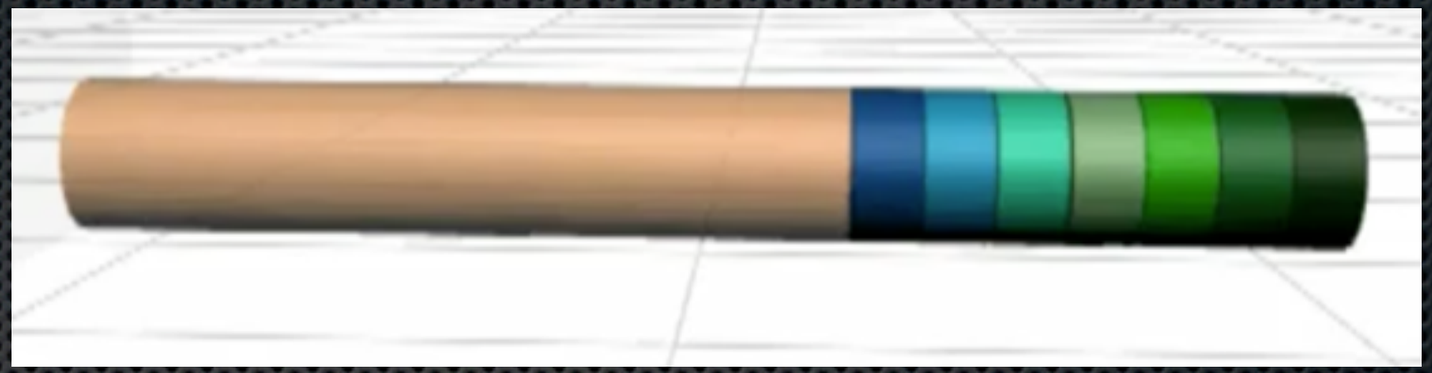
# OSI Model
## (Open Systems Interconnection)

| Layer | Name | Example |
|---|---|---|
| 1 | Physical | 1000Base-T |
| 2 | Data Link | 802.3 Ethernet |
| 3 | Network | IP |
| 4 | Transport | TCP |
| 5 | Session | Sockets |
| 6 | Presentation | SSL |
| 7 | Application | HTTP |


On reflection, allowing Buddy to watch the end of Old Yeller may not have been the best idea.

# What's in a packet ?

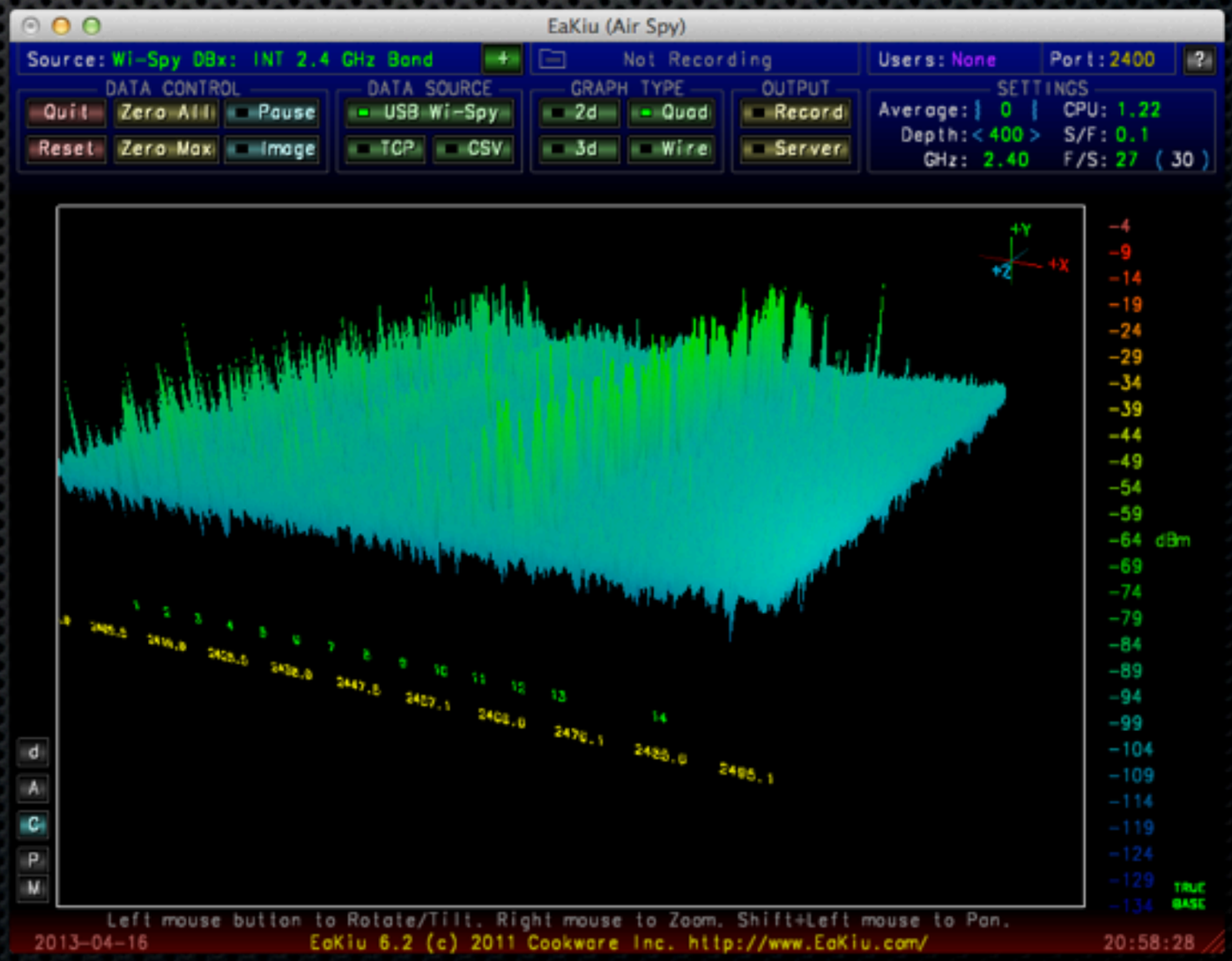


- Payload
- Header

# WiFi 2.4 & 5.8Ghz

- WiFi is shared medium, channels overlap
- WiSpy and similar can let you peek into the RF spectrum



# Layer 2 or Layer 3

- Switching
  - Unmanaged
  - Managed
- Routers
- Bridges

# IPv4 and IPv6

- Different layer 3 implementations, but same at layer 4 and above
- "Dual Stack" is common today, and will be for years to come
- IPv6 tunneling services, if you need to access v6 with only a v4 connection

# Routers / Firewalls

- Routing as a service
- Processing of Data  ( services )

Untangle – firewall.mactech-boston.com

https 10.20.80.1/webui/startPage.do

Address Book | Bonjour | 37signals Launchpad | Projection C... Screen Size | Dazian | Pin It | Reference Material | Advanced LED Technology | Savant University | Homes with ...Real Estate | 10 Most Am...Geek About

Unlock 1Password to save this Login — Master Password — Unlock

Untangle – firewall.mactech-boston.com | WLANs – admin@10.20.80.2 – ZoneDirector

untangle

Apps | Config

- Virus Blocker — Install
- Virus Blocker Lite — Install
- Spyware Blocker — Install
- Spam Blocker — Install
- Phish Blocker — Install
- Bandwidth Control — Install
- Application Control — Install
- Application Control Lite — Install
- Ad Blocker — Install
- WAN Failover — Install
- WAN Balancer — Install
- IPsec VPN — Install

Help | My Account | Logout

Default Rack

Tx: 87.02KB/s
Rx: 297.14KB/s
Network | Sessions: 493 | CPU Load: low | Memory: 2935.61 MB / 667.04 MB

**Number of Processors / Type / Speed:**
2, Intel(R) Pentium(R) CPU G640 @ 2.80GHz, 2793.699
**Load average (1 min , 5 min , 15 min):**
0.66, 0.2, 0.11
**Tasks (Processes)**
106
**Uptime:**
2 Hours, 50 Minutes

**Web Filter** — Settings | Help
Pages scanned
Pages blocked
Pages passed
Passed by policy

**Web Cache** — Settings | Help
Cache hits
Cache misses
User Bypass
System Bypass

**Firewall** — Settings | Help
Sessions passed
Sessions logged
Sessions blocked
Current Sessions

**Intrusion Prevention** — Settings | Help
Sessions scanned
Sessions logged
Sessions blocked
Current Sessions

Services

**Reports** — Settings | Help

**Policy Manager** — Settings | Help

**Directory Connector** — Settings | Help

**Captive Portal** — Settings | Help
Sessions blocked
Clients authorized

**OpenVPN** — Settings | Help
Sessions passed
Clients Connected

**Attack Blocker** — Settings | Help
Sessions accepted
Sessions limited
Sessions dropped
Sessions rejected

# Traffic Shaping , Management

- QOS
- VLANS
- Client isolation
- Rogue AP Detection
- Client Bandwidth Management (from the AP)

# Time Sensitive

FedEx®
Express

# Time Sensitive : Media

- Airplay Audio
- Airplay Video
- Streaming Content
- Uncompressed Video
- Secure Content with Verification

# oops.....8.8.8.8

- Apple TV issue
- https://discussions.apple.com/thread/3884143?start=30&tstart=0

# Traffic Shaping , Management

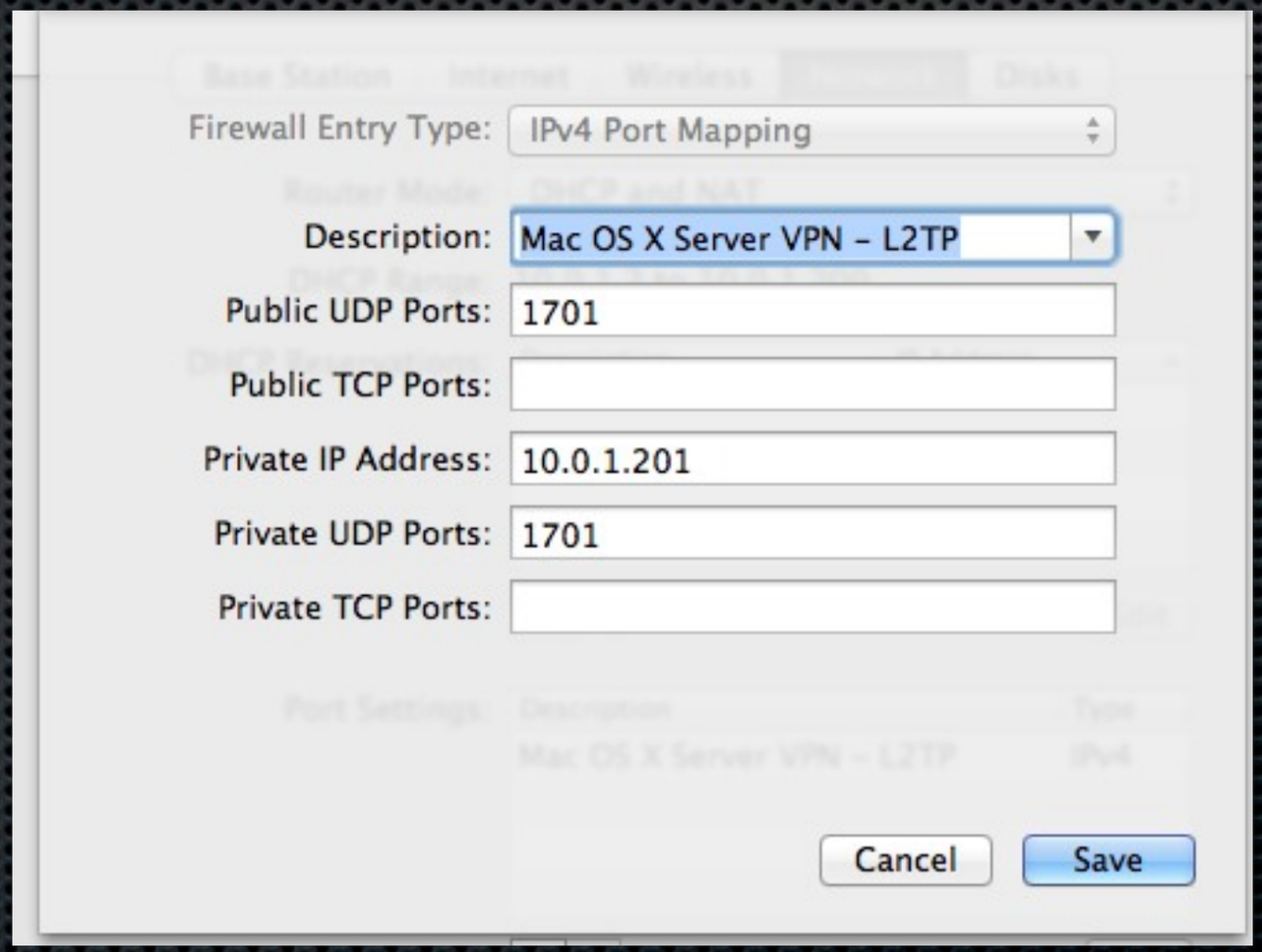
- QOS
- VLANS
- Client isolation
- Rogue AP Detection
- Client Bandwidth Management (from the AP)

# NAT and Port Forwading

- NAT = Network Address Translation
  - RFC1918 block behind a single Public IP
  - Translates the IP header, keeps track of state
- Port forwarding
  - Allows ports inside network to be exposed to outside

# Port Forwarding Example 1

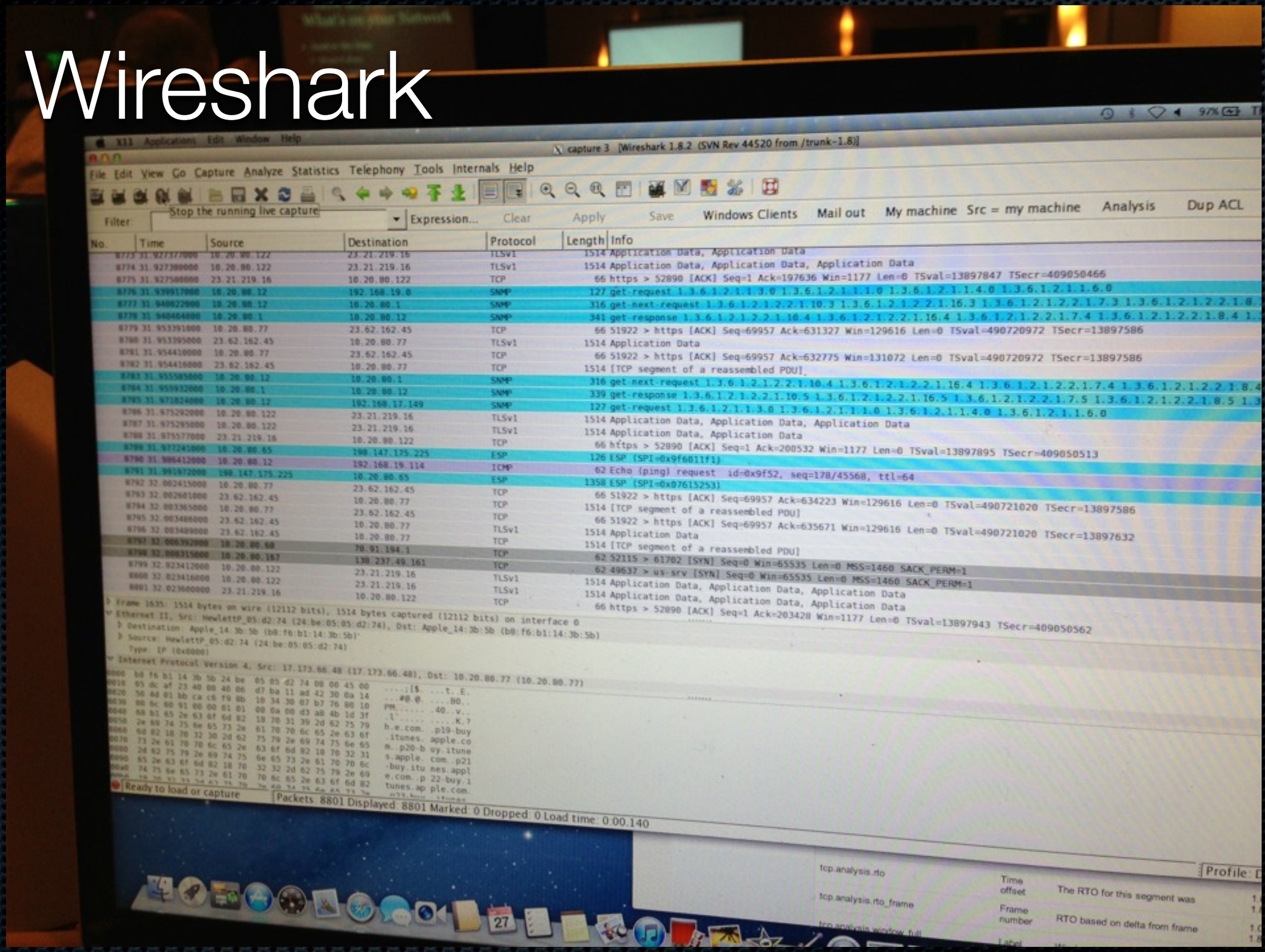
- Airport Base Station



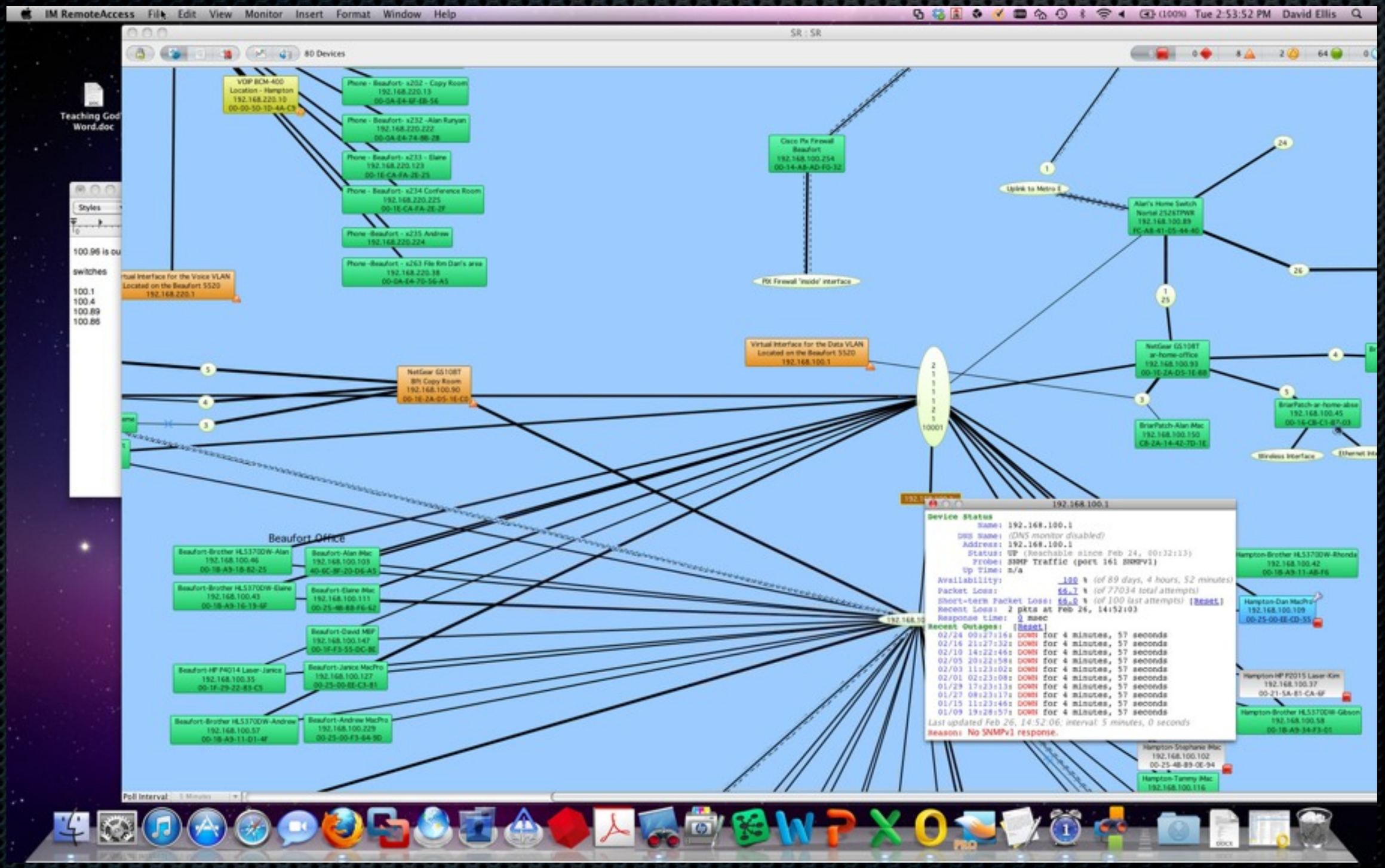
# Why can’t I find the problem ?

What you aren’t seeing ....

# Wireshark


capture 3 [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Stop the running live capture
Filter:
Expression... Clear Apply Save
Windows Clients
Mail out
My machine
Src = my machine
Analysis
Dup ACL
No. Time Source Destination Protocol Length Info
8774 31.927380000 10.20.80.122 23.21.219.16 TLSv1 1514 Application Data, Application Data, Application Data
8775 31.927500000 23.21.219.16 10.20.80.122 TCP 66 https > 52890 [ACK] Seq=1 Ack=197636 Win=1177 Len=0 TSval=13897847 TSecr=409050466
8776 31.939917000 10.20.80.12 192.168.19.0 SNMP 127 get-request 1.3.6.1.2.1.1.3.0 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.4.0 1.3.6.1.2.1.1.6.0
8777 31.940022000 10.20.80.12 10.20.80.1 SNMP 316 get-next-request 1.3.6.1.2.1.2.2.1.10.3 1.3.6.1.2.1.2.2.1.16.3 1.3.6.1.2.1.2.2.1.7.3 1.3.6.1.2.1.2.2.1.8.
8778 31.940484000 10.20.80.1 10.20.80.12 SNMP 341 get-response 1.3.6.1.2.1.2.2.1.10.4 1.3.6.1.2.1.2.2.1.16.4 1.3.6.1.2.1.2.2.1.7.4 1.3.6.1.2.1.2.2.1.8.4 1.
8779 31.953391000 10.20.80.77 23.62.162.45 TCP 66 51922 > https [ACK] Seq=69957 Ack=631327 Win=129616 Len=0 TSval=490720972 TSecr=13897586
8780 31.953395000 23.62.162.45 10.20.80.77 TLSv1 1514 Application Data
8781 31.954410000 10.20.80.77 23.62.162.45 TCP 66 51922 > https [ACK] Seq=69957 Ack=632775 Win=131072 Len=0 TSval=490720972 TSecr=13897586
8782 31.954416000 23.62.162.45 10.20.80.77 TCP 1514 [TCP segment of a reassembled PDU]
8783 31.955585000 10.20.80.12 10.20.80.1 SNMP 316 get-next-request 1.3.6.1.2.1.2.2.1.10.4 1.3.6.1.2.1.2.2.1.16.4 1.3.6.1.2.1.2.2.1.7.4 1.3.6.1.2.1.2.2.1.8.4
8784 31.955932000 10.20.80.1 10.20.80.12 SNMP 339 get-response 1.3.6.1.2.1.2.2.1.10.5 1.3.6.1.2.1.2.2.1.16.5 1.3.6.1.2.1.2.2.1.7.5 1.3.6.1.2.1.2.2.1.8.5 1.3
8785 31.971824000 10.20.80.12 192.168.17.149 SNMP 127 get-request 1.3.6.1.2.1.1.3.0 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.4.0 1.3.6.1.2.1.1.6.0
8786 31.975292000 10.20.80.122 23.21.219.16 TLSv1 1514 Application Data, Application Data, Application Data
8787 31.975295000 10.20.80.122 23.21.219.16 TLSv1 1514 Application Data, Application Data
8788 31.975577000 23.21.219.16 10.20.80.122 TCP 66 https > 52890 [ACK] Seq=1 Ack=200532 Win=1177 Len=0 TSval=13897895 TSecr=409050513
8789 31.977241000 10.20.80.65 198.147.175.225 ESP 126 ESP (SPI=0x9f6011f1)
8790 31.986412000 10.20.80.12 192.168.19.114 ICMP 62 Echo (ping) request id=0x9f52, seq=178/45568, ttl=64
8791 31.991072000 198.147.175.225 10.20.80.65 ESP 1358 ESP (SPI=0x07615253)
8792 32.002415000 10.20.80.77 23.62.162.45 TCP 66 51922 > https [ACK] Seq=69957 Ack=634223 Win=129616 Len=0 TSval=490721020 TSecr=13897586
8793 32.002601000 23.62.162.45 10.20.80.77 TCP 1514 [TCP segment of a reassembled PDU]
8794 32.003365000 10.20.80.77 23.62.162.45 TCP 66 51922 > https [ACK] Seq=69957 Ack=635671 Win=129616 Len=0 TSval=490721020 TSecr=13897632
8795 32.003486000 23.62.162.45 10.20.80.77 TLSv1 1514 Application Data
8796 32.003489000 23.62.162.45 10.20.80.77 TCP 1514 [TCP segment of a reassembled PDU]
8797 32.006392000 10.20.80.60 70.91.194.1 TCP 62 52115 > 61702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
8798 32.008315000 10.20.80.167 138.237.49.161 TCP 62 49637 > us-srv [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
8799 32.023412000 10.20.80.122 23.21.219.16 TLSv1 1514 Application Data, Application Data, Application Data
8800 32.023416000 10.20.80.122 23.21.219.16 TLSv1 1514 Application Data, Application Data, Application Data
8801 32.023600000 23.21.219.16 10.20.80.122 TCP 66 https > 52890 [ACK] Seq=1 Ack=203428 Win=1177 Len=0 TSval=13897943 TSecr=409050562
Frame 1635: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
Ethernet II, Src: HewlettP_05:d2:74 (24:be:05:05:d2:74), Dst: Apple_14:3b:5b (b8:f6:b1:14:3b:5b)
Destination: Apple_14:3b:5b (b8:f6:b1:14:3b:5b)
Source: HewlettP_05:d2:74 (24:be:05:05:d2:74)
Type: IP (0x0800)
Internet Protocol Version 4, Src: 17.173.66.48 (17.173.66.48), Dst: 10.20.80.77 (10.20.80.77)
Ready to load or capture
Packets: 8801 Displayed: 8801 Marked: 0 Dropped: 0 Load time: 0:00.140
tcp.analysis.rto
Time offset
The RTO for this segment was
tcp.analysis.rto_frame
Frame number
RTO based on delta from frame
Profile:

# Intermapper



# Watchman Monitoring

## Watchman Monitoring Server

Clients | Settings | Logout | Download Your Client Installer

| | |
|---|---|
| **Client Group:** | Company's nickname |
| **Asset ID:** | Asset Tag 58790 |
| **Machine Name:** | Receptionist |
| **Last User:** | veronica |
| **Serial Number:** | W86081WYVJ3 |
| **Specified Teamviewer ID:** | 123455678 |
| **Control with LogMeIn:** | Launch LMI Shortcut |
| **Model Details:** | MacBookPro1,1 |
| **OS Version:** | Mac OS X 10.5.8 (9L30) |
| **Installed RAM:** | 2 GB |
| **SMC Version:** | 1.2f10 |
| **Current Uptime:** | 10 days, 9 hours, 43 mins |
| **ClientID:** | 20110130-KE31-OVNY26 |
| **Client Version:** | 4.2 |
| **Internal Notes:** | Customer is ready for a new computer. |
| **Reported Notes:** | Call first before remotely controlling |
| **Client last checked-in:** | 06/27/2011 9:31PM |
| **Last warning received:** | |
| **Email notices muted until:** | |
| **Selected plugins muted until:** | |

Edit Notes and Muting | Delete Client Record

**Latest Plugin Status**

| | |
|---|---|
| **Check Laptop Battery**<br>Cycle count: 303 Condition: Good | View → |
| **Check Root Capacity**<br>51% (15Gb of 30Gb) used on root volume. | View → |
| **Check SoftRAID Volumes**<br>No problems found with any SoftRAID disks or volumes. | View → |
| **Report CCC Errors**<br>No new CCC logs. | View → |
| **Report Client Status**<br>The Update check found no problems. | View → |
| **Report Disk I/O Errors**<br>No Disk I/O Errors found | View → |
| **Report Kernel Panic Count**<br>Amount of Panic Logs: 8 | View → |
| **Report POST Errors**<br>Post Passed | View → |
| **Report RAM Errors**<br>BANK 0/DIMM0: Size: 1 GB<br>BANK 1/DIMM1: Size: 1 GB | View → |
| **Report SMART Errors**<br>No Disk S.M.A.R.T. Errors found | View → |
| **Time Machine Reporter**<br>This service check is all clear. Last Time Machine backup was Today at 2011-06-27 08:06:02 | View → |

 Server Version 3.0

# The External World

- Static vs Dynamic Addressing
- Multiple IP Addresses
- Bonding IP addresses
- NAT

# IPv6

- 128-bit address space, enough addresses for foreseeable future
  - You'll likely get a /64, so 18,446,744,073,709,551,616 addresses
- ISP's probably aren't ready
  - Chicken and the Egg
  - Much more important for mobile carriers, Asia, etc.
- Security Considerations

# ICMP Tools

| IPv4 | IPv6 |
| --- | --- |
| arp | ndp |
| ping | ping6 |
| traceroute | traceroute6 |

## IPv6 address notations:

2001:0db8:0000:0000:0000:0000:1428:57ab standard notation
2001:db8:0:0:0:0:1428:57ab suppressing leading zeros
2001:db8::1428:57ab zero compressed notation
fe80::5efe:192.168.20.100 mixed notation, compressed

## IPv6 address types: Unicast prefixes

2001: Globally assigned unicasts
2002: Reserved for 6to4 encapsulation
fe80: Link-Local (not routed at all)
fc00: Centrally Assigned Unique Local Address (ULA-central)
fd00: Unique Local Address (ULA, not routed in the Internet)

## IPv6 address types: Multicast prefixes and Scopes

ff01: Interface (does not leave local host)
ff02: Link-local (does not leave local subnet)
ff05: Site-local (does not leave local site)
ff0e: Global (does leave to the Internet)

## IPv6 address types: Multicast hosts

| | | | |
|---|---|---|---|
| ::1 | All nodes | ::b | All mobile agents |
| ::2 | All routers | ::c | SSDP |
| ::3 | unassigned | ::d | All PIM router |
| ::4 | DVMPR router | ::e | RSVP-encapsulation |
| ::5 | OSPF IGP | ::16 | LLMNR |
| ::6 | OSPF IGP DR | ::101 | NTP server |
| ::7 | ST router | ::1:1 | Link name |
| ::8 | ST hosts | ::1:2 | All DHCP relay agents |
| ::9 | All RIP routers | ::1:3 | DNS & LLMNR |
| ::a | All EIGRP routers | ::1:ffxx:xxxx | Solicited node multicast |

## IPv6 address types: Anycast

2001:620:20:1:: Anycast for Subnet-Router address
2001:7fd::1 Anycast for Root-Nameserver of RIPE NCC

## IPv6 address examples:

fe80::230:64ff:fe6b:8532 Link-Local unicast address
2001:620::230:64ff:fe6b:8532 Global unicast address
ff02::2 Multicast to all routers on local subnet
ff05::1:3 Multicast to all DHCP servers within the site
ff05::101 Multicast to all NTP servers within the site
ff0E::101 Multicast to all NTP servers in the Internet

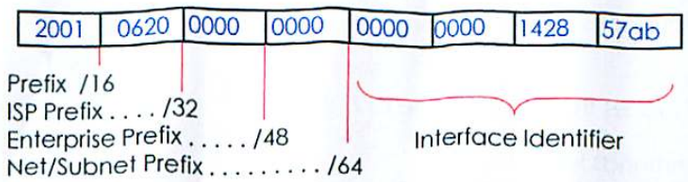
## IPv6 special addresses:

::/128 unspecified address with all zero bits, used as source address only
::1/128 local host (loopback address)

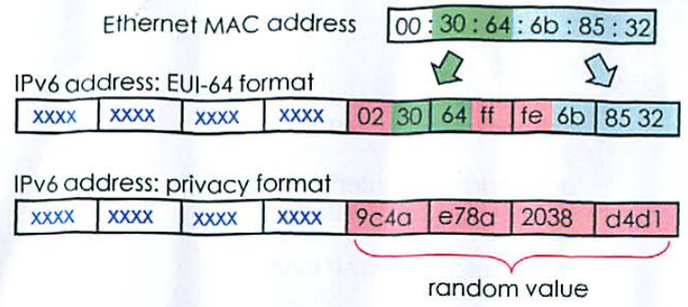
## IPv6 deprecated address prefixes:

::w.x.y.z/96 zero prefix was used for IPv4-compatible addresses
fec0::/10 site-local prefix valid only inside local organization
3ffe::/16 reserved for 6Bone (Internet test nets)

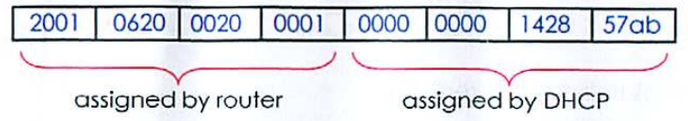
## IPv6 address formats: (best practices)




## IPv6 Stateless Address Autoconfiguration (SLAAC)

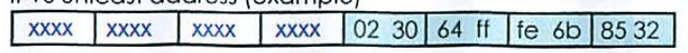



## IPv6 Stateful Address Configuration (via DHCP)

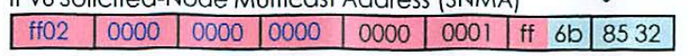



## Solicited-Node Multicast Address (SNMA)

IPv6 unicast address (example)




IPv6 Solicited-Node Multicast Address (SNMA)




SNMA derived from unicast address: ff02::1:ff6b:8532

## Wireshark display filters:

| | |
|---|---|
| eth.addr[0:2]==3333 | filters MAC multicasts 33:33:xx |
| eth.addr[0:3]==33:33:ff | filters neighbor solicitations |
| ipv6.addr [0:2]==fd00 | filters from/to prefix fd00/16 |
| ipv6.host contains "fd00::3" | filters on exact string 'fd00::3' |
| ipv6.addr [0:8]==fd00:0000:0000:0003 | filters from/to prefix fd00::3/64 |
| icmpv6.type == 133 | filters on 'Router Solicitation' |
| icmpv6.type == 134 | filters on 'Router Advertisement' |
| icmpv6.type == 135 | filters on 'Neighbor Solicitation' |
| icmpv6.type == 136 | filters on 'Neighbor Advertisement' |
| icmpv6.type == 137 | filters on 'Redirect Message' |

## IPv6 Neighbor Discovery (ND)

| | |
|---|---|
| Neighbor Solicitation | Neighbor address resolution, sent to Solicited-Node Multicast Address (SNMA) |
| Neighbor Advertisement | Response to 'Neighbor Solicitat.' sent back to requester |
| Router Solicitation | Router address resolution, sent to ff02::2 |
| Router Advertisement | Response to 'Router Solicitation' sent to ff02::1 |
| Duplicate Address-Detection (DAD) | Sent to own Solicited-Node Multicast Address (SNMA) |

## Multicast Listener Discovery (MLD)

| | |
|---|---|
| Multicast Listener Query | Sent by a multicast router to poll a network segment for group members |
| Multicast Listener Report | Sent by a host when it joins a multicast group, or in response to an MLD Multicast Listener Query sent by a router. |
| Multicast Listener Done | Sent by a host when it leaves a host group. |

## Other ICMPv6 messages

| | |
|---|---|
| Destination Unreachable | Error message |
| Packet Too Big | Error message |
| Time Exceeded | Error message |
| Parameter Problem | Error message |
| Redirect Message | Router informs node about better next-hop address |
| Echo Request/Reply | Connectivity test |

## Tunneling/encapsulation methods:

| | |
|---|---|
| 6in4 (static) | IPv6-over-IPv4 Tunneling (RFC4213) |
| 6in4 (heartbeat) | Automatic 6in4 tunnel using AICCU clients |
| 6rd | IPv6 Rapid Deployment for ISPs (RFC 5569) |
| 6to4 | IPv6 in IPv4 encapsulation, no NAT support |
| AYIYA | Anything In Anything UDP Tunneling |
| ISATAP | Intra-site Automatic Tunnel Addr. Protocol |
| (::5efe:w.x.y.z) | Address example: fe80::5efe.192.168.1.100 |
| L2TP | Layer Two Tunneling Protocol (RFC2661) |
| Teredo tunnel | IPv6 tunneled over UDP port 3544 (RFC4380) |
| TSP | Tunnel Setup Protocol for IPv6 Tunnel Broker |
| GRE tunnel | IPv6 inside Generic Routing Encapsulation |
| MPLS tunnel | IPv6 over Multiprotocol Label Switching |

## IPv6/IPv4 translation methods:

| | |
|---|---|
| NAT-PT | Network Address Translation - Protocol Translation |
| NAPT-PT | Network Address Port Translation - Protocol Transl. |
| SIIT | Stateless IP/ICMP Translation |

www.wireshark.ch



- Adam Schechter
- adam@pav.us.com


# Thank You !!