

# Controls and Centralised Wireless

Neal Wise, CISSP CISA  
Oliver Greiter, CISSP RHCE



assurance

# Agenda

Threats to 802.11-type wireless

Autonomous vs. Controller-based wireless solutions

Examples of controller operations

Turning the tables

Architecture, Strategies and “Gotchas”



# #include <disclaimer.h>

We're not RF engineer-types obviously

We just like to break stuff

No guarantees, warranties, etc... if something breaks  
you get to keep both parts



# About Assurance / Us

Assurance = compliance { penetration testing/ethical “hacking”, review, audit }, wireless & mobility, UNIX/network and security consulting/support

Neal = UNIX guy, mac zealot, packet monkey, hacker^H^H^H^H^H^Hsecurity professional

Oliver = wrecker of havoc upon networks and applications (with a signed engagement letter) ;)



# Assurance Wireless

## Wireless stuff we do

- Secure wireless solution design & implementation - .11/3G
- Independent review services - .11/3G
- Talk about wireless a lot to anyone who'll listen (hi)
- Research



# AusCERT '08 "WarBus"

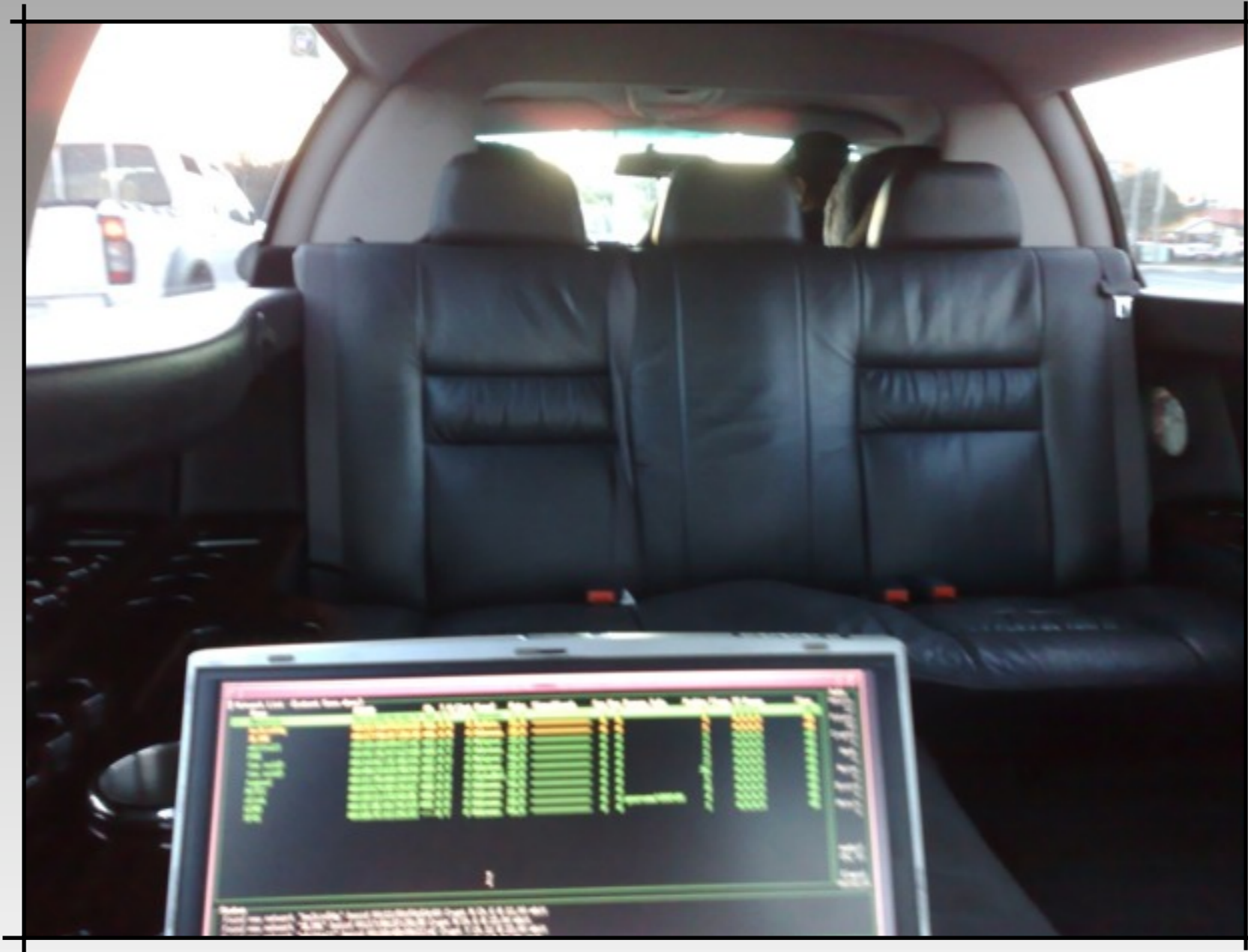
~15 people  
Surfer's  
Paradise, QLD  
- May 2008

45 minutes -  
1300+  
networks, 57  
discoverable  
bluetooth  
devices  
Thanks  
AusCERT!



assurance

# War... Limo-ing?



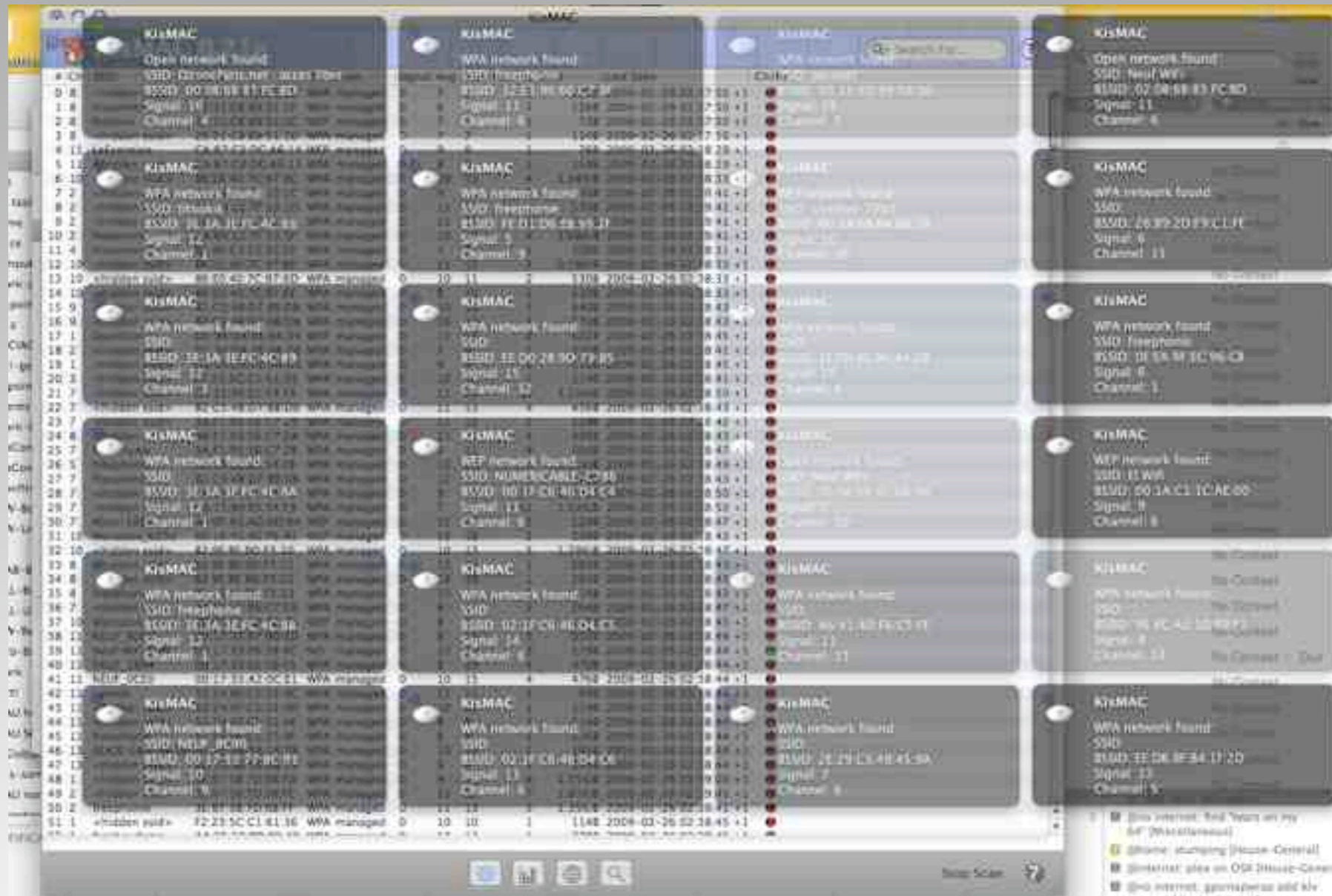
This was a new one for me...



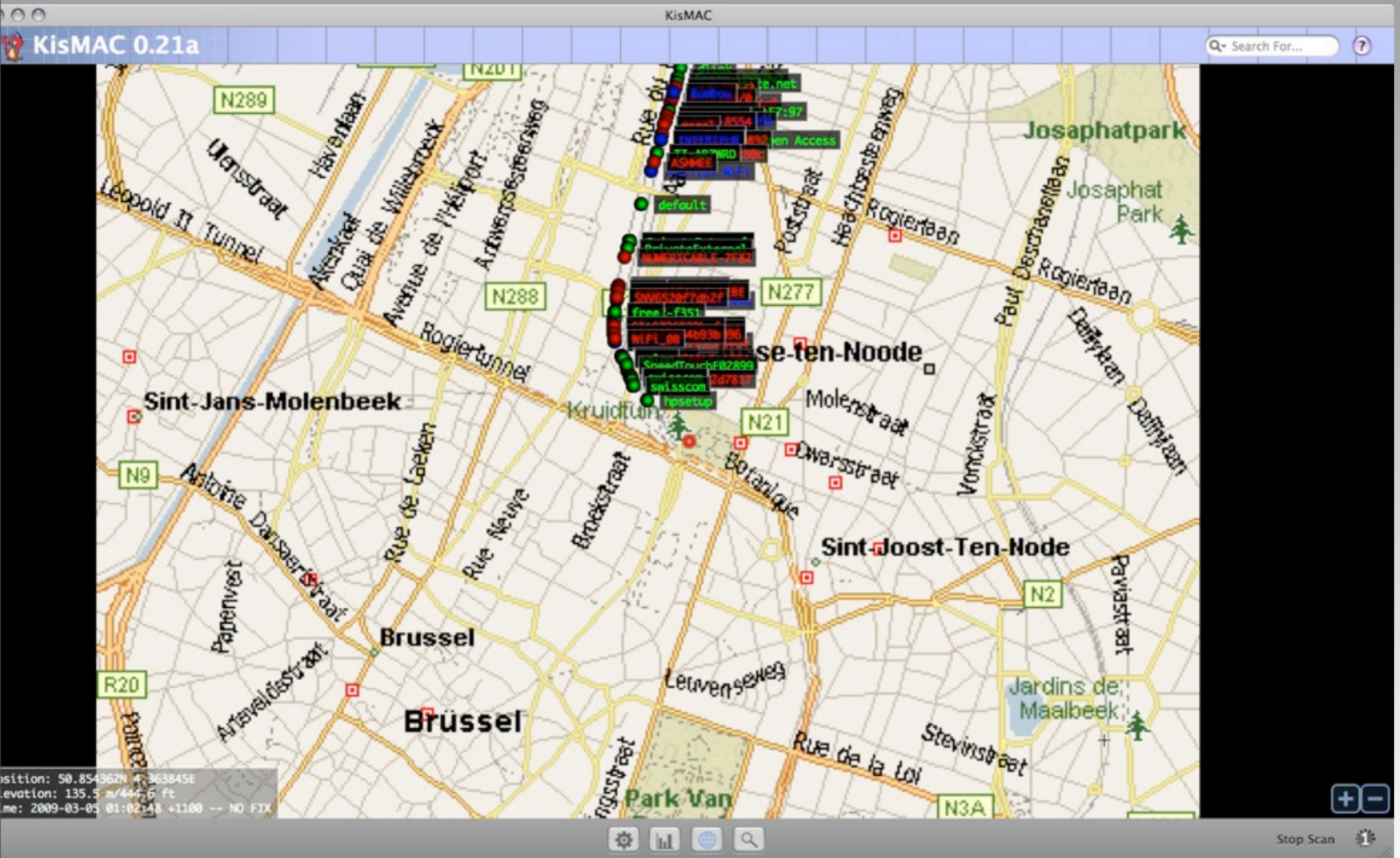
assurance

# War-train-ing on the Eurostar

10 minutes before Paris - ~800 networks



# More train stuff



assurance

AusCERT 2009

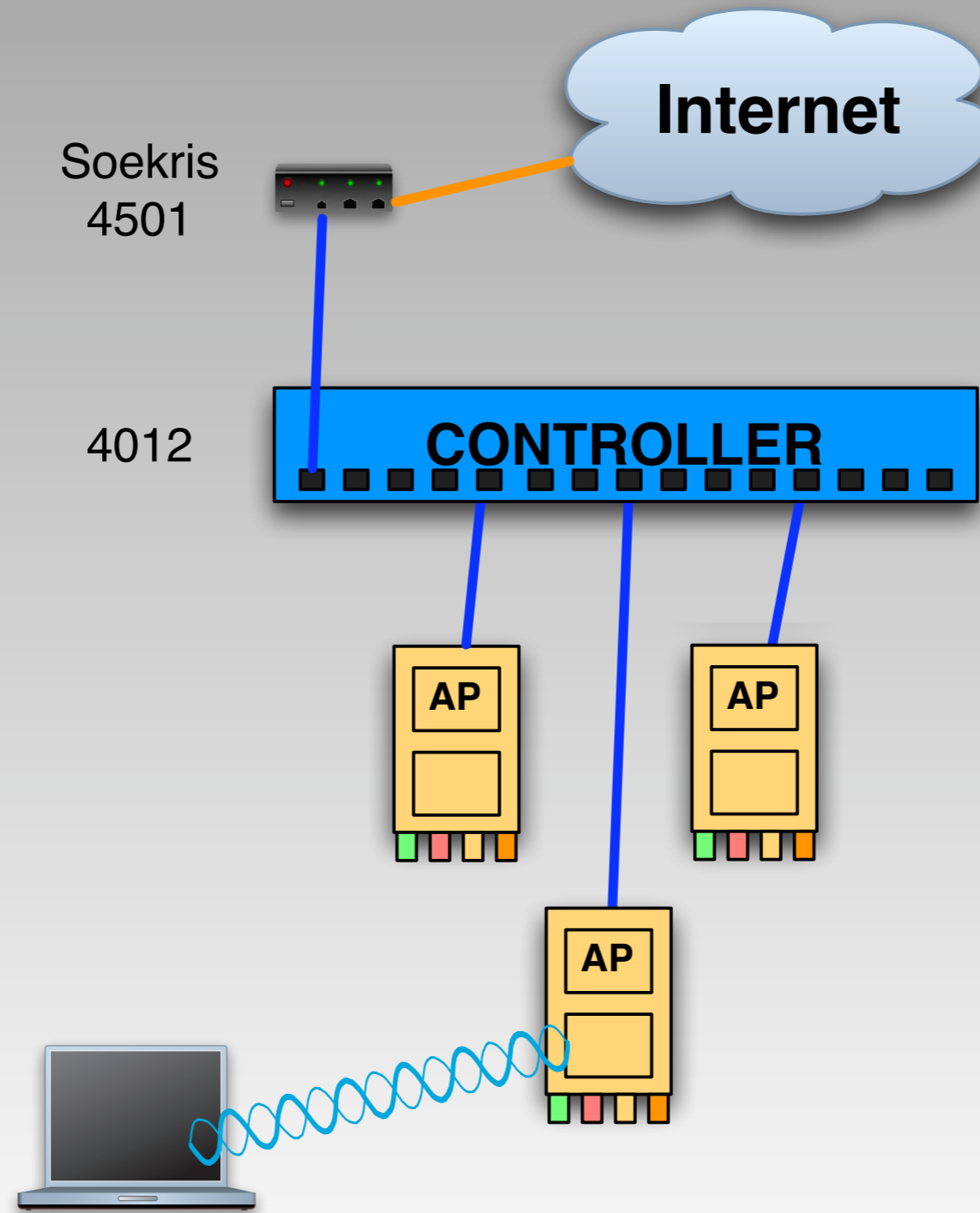
# Kit used today

## Old-ish Airespace wireless solution

- Airespace 4012 controller - last before Cisco branding
- WAPs - Cisco 1010 WAP, Nortel 2230 WAPs, Airespace 1250 WAP
- Some magic geode boards for network glue
- WLAN client stuff - cards, etc



# Arranged something like this...



# FYI - cards I use

Here's my 802.11 card "evolution" (by chipset):

- 1999-2000 - Nokia "real 802.11" - 2mbit - craptacular
- 2000-2002 Hermes / Orinoco / WaveLan - cheap + PCCard connector (boo) - 802.11b
- 2002-2003 Cisco LMC350 - MMCX connector (yay) - .11b
- 2003-2005 Prism2 / Prism54 cards - unnecessary POWER! + MMCX connectors - .11b & .11g (p54)
- ~2005-present - Atheros 5k a/b/g, rt73, rt8180/87 b/g



# FYI - software we use

Not today's focus - see "Wireless Insecurity" presentation on website

Mostly Kismet and WEXT-based use of tcpdump / wireshark - sometimes Kismac

- Oliver's the Kismac WEP-smashing posterboy - <http://ethicalhack.org/vids/kismac-vid.php>

Aircrack Suite stuff



# Lets have a look



assurance

# General 802.11 threats



- Management Interfaces / Audit facilities for wireless service
- Poor Design & Implementation
- Attack / Misuse of RF service, network and application protocols including attacking “weak controls”
- Attack / Misuse of “wired” environment beyond wireless
- Wired  $\Leftrightarrow$  wireless integration / network architecture



**controller-based  
wireless vs.  
autonomous wireless**



**assurance**

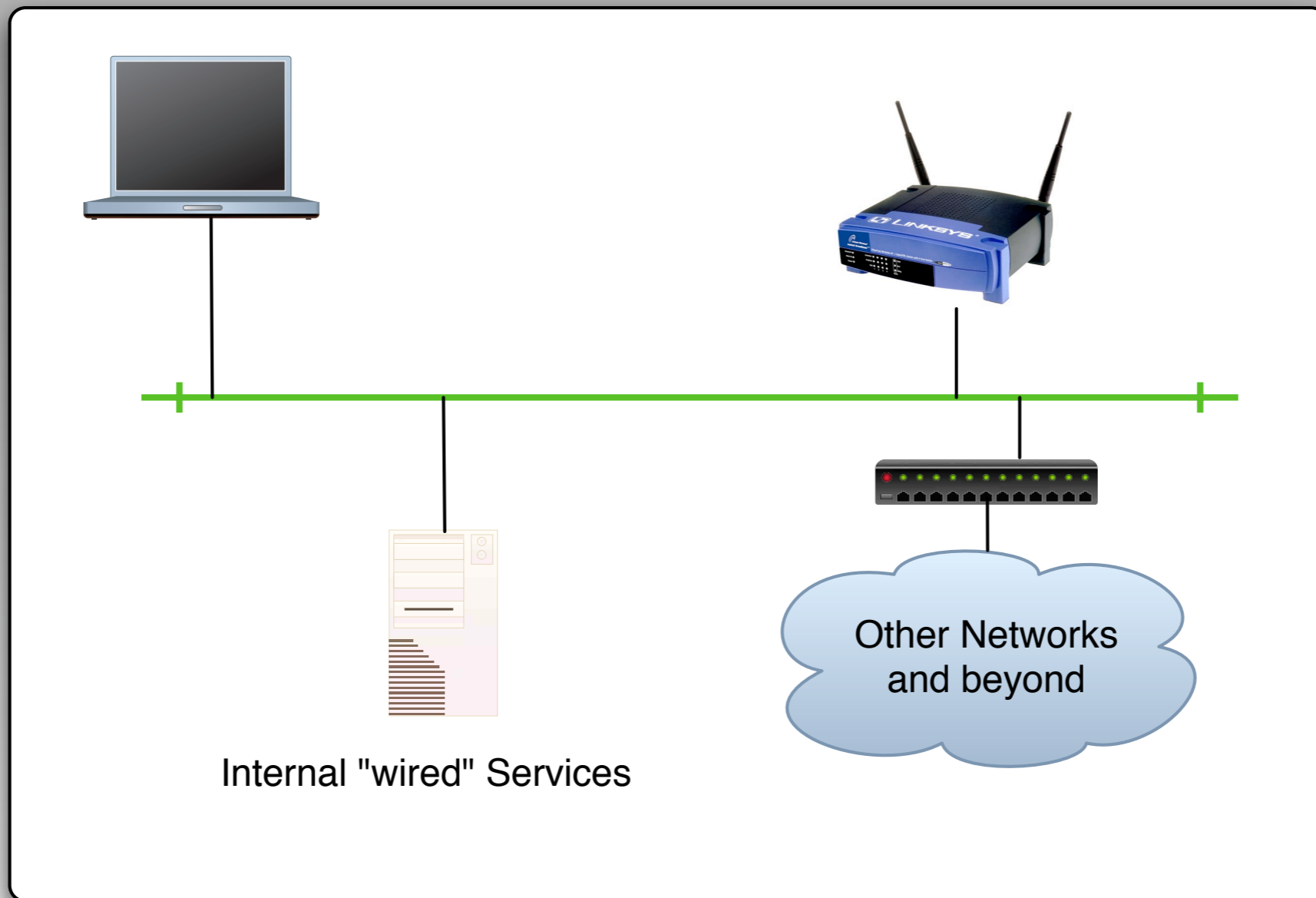
# Autonomous WAPs

## “Standalone” WAPs - most WAPs

- Your AP is likely this - bridge or (rarely) routing device
- De-centralised configuration / provisioning - all “once off” builds or sometimes using a management system
- Centralised / de-centralised authentication
- Enterprise devices support multiple network profiles
- Controls at edge and gateways - little in-between typically
- “Raw” or VLAN tagged traffic between WAPs and network

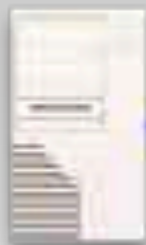


# Typical autonomous WLAN

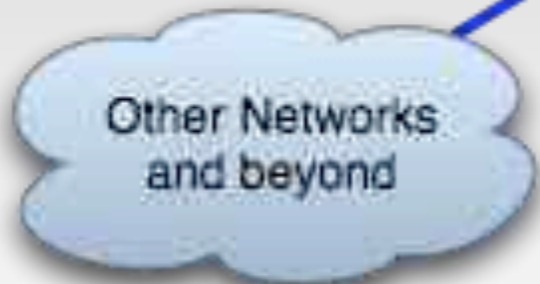


# More realistically...

WLANs with "ranked" QoS  
SSID1 VoIP-o-WIFI - WEP\*  
SSID2 Internal Data - 802.1x using PEAP, etc  
SSID3 - Guest - open?



Internal "wired" Services



Other Networks  
and beyond



**trunked VLANs - "native" VLAN =  
management**

**N-number of VLANs - 1 per SSID +  
mgmt**

**Something doing intervlan routing &  
hopefully filtering**



assurance

AusCERT 2009

# Threats to autonomous wireless

Consistency of configuration

Physical access often = access to device / net goodies

For Cisco Aironet this means console access using reset button (unless disabled by firmware)

“Type 7” or plaintext passwords, SNMP comm. strings, auth shared secrets, blah blah blah often exposed



# Moar! (threats)

Unprotected data in transit between WAP and wherever at mercy of route/switch infrastructure

Complex WiFi service = complex switch configuration for WAPs = mistakes/forgotten stuff

“Trojan” WAP introduction

Also... device is easily reused if stolen



# Wireless controllers

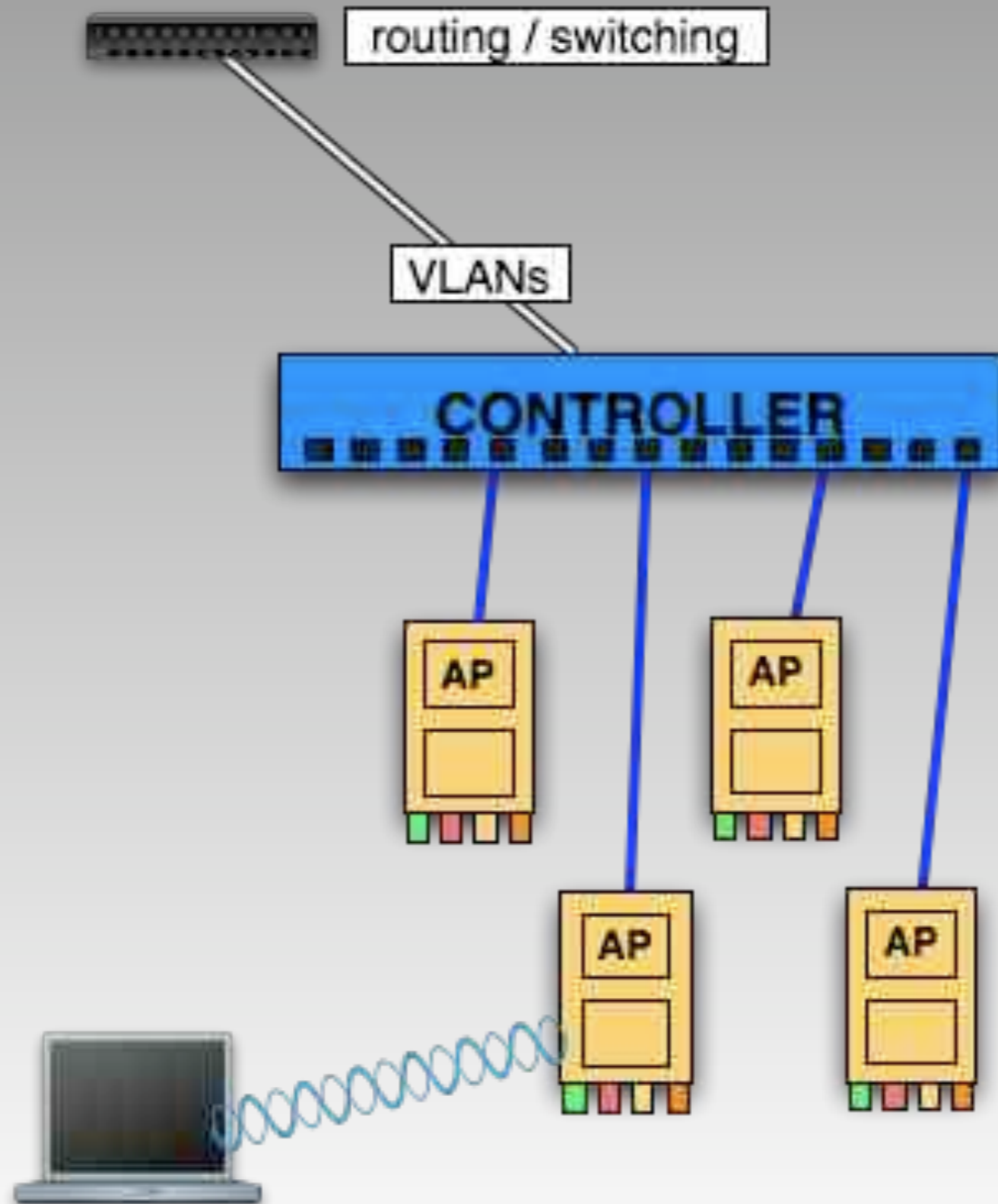
Controller-based WAPs  
Cisco, Aruba, Meru, etc



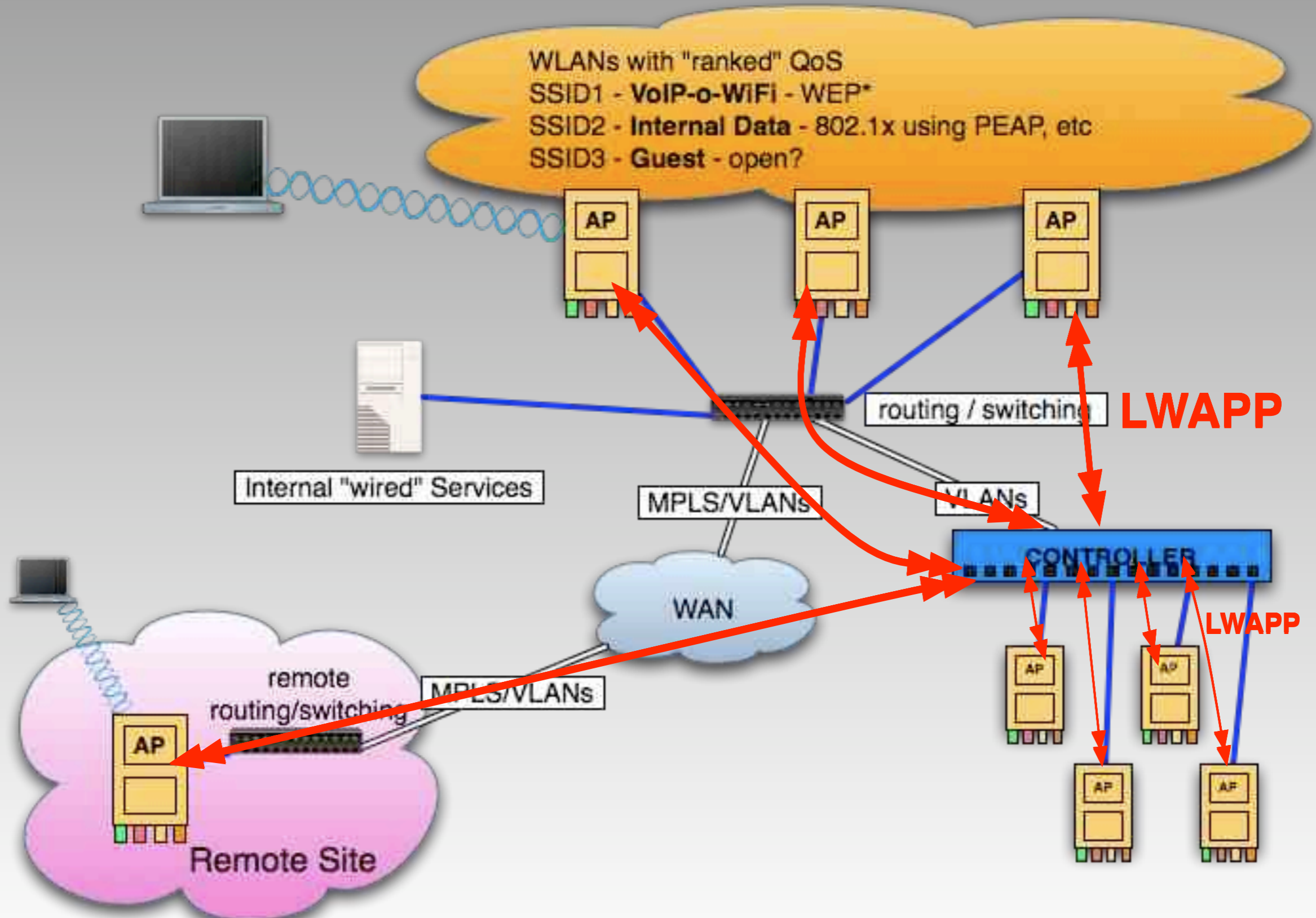
- Centralised configuration, provisioning and event management (if enabled!)
- Some WIDS functionality\* and ACLs\*
- Centralised authentication including advanced services - “Catch and release” portals, etc.
- Like autonomous multiple wireless services often achieved by VLANs but kinda differently



# which looks like



# Or...



assurance

AusCERT 2009

# Airespace Controllers

Controller is Linux based. But has a NetBSD stage2 boot loader. Weird.

Has an integrated switch which is integrated into embedded board

Provides 802.3af power to 12 ports - We've used this one for VoIP phones as well



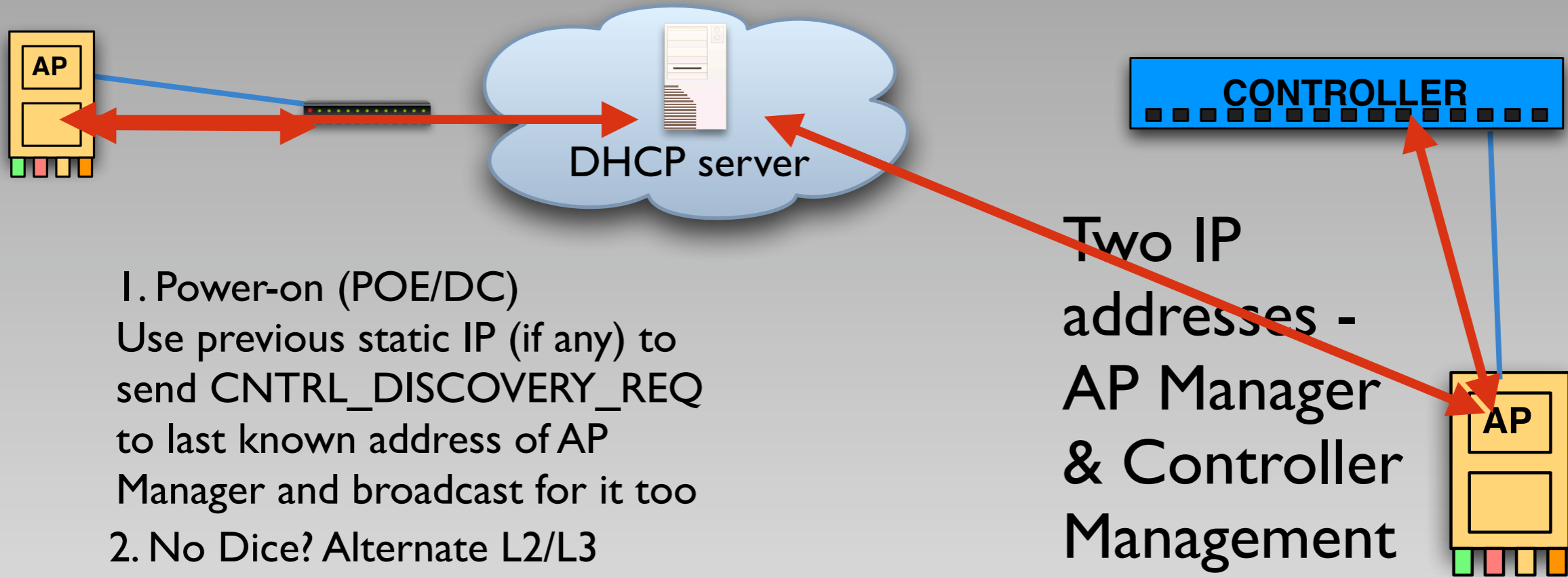
# Airespace magic sauce = LWAPP

## Lightweight Access Point Protocol

- Handles all controller to WAP traffic - carries various data traffic - all VLANs for all SSID + WAP mgmt
- Uses x509 certs in WAPs - hardware “factory installed” for “real” Airespace APs for mutual authentication
- Self-generated (and signed) certs for converted Cisco Aironet 1130, 1230 and 1242 WAPs for same - kinda scary
- SSL over UDP for most part - kinda neat but what does this mean



# LWAPP L3



1. Power-on (POE/DC)  
Use previous static IP (if any) to send CNTRL\_DISCOVERY\_REQ to last known address of AP Manager and broadcast for it too
2. No Dice? Alternate L2/L3 mode and ask the network.  
Get L3 DHCP address

3. DHCP Option 43? Connect to that for Controller IP.  
Otherwise broadcast looking for it and ask DNS for **CISCO-LWAPP-CONTROLLER** - A record

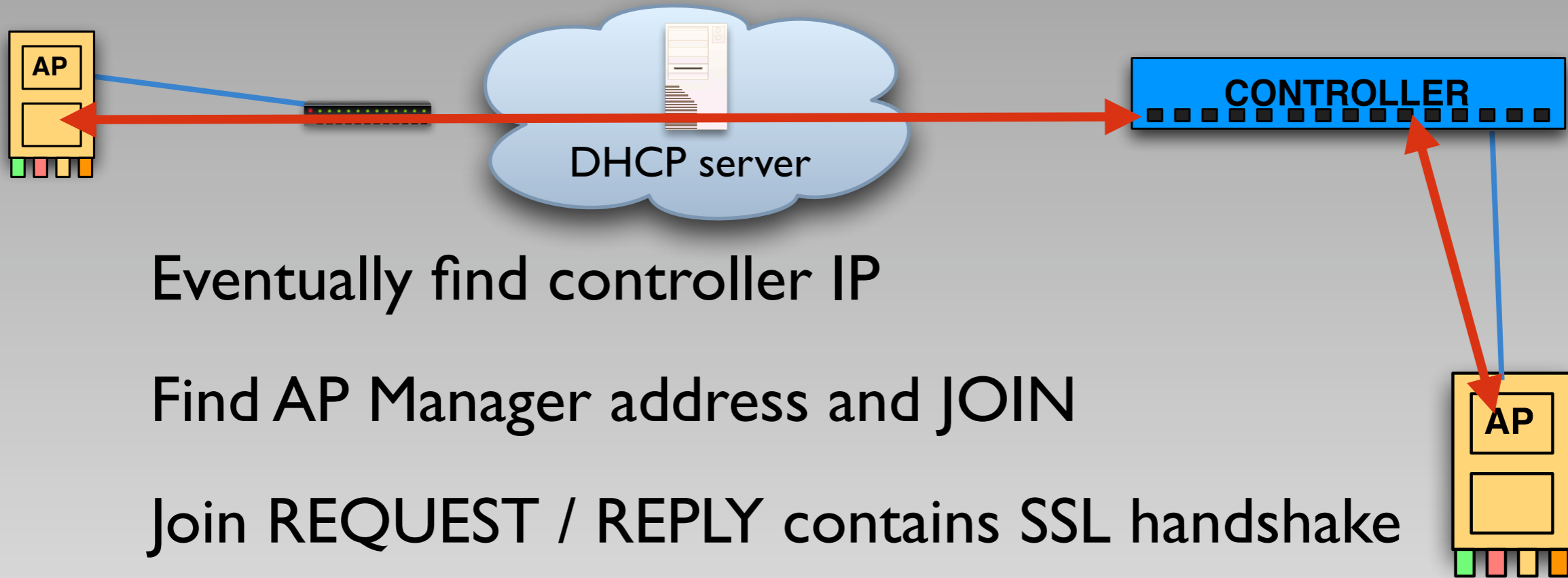
Two IP addresses -  
AP Manager  
& Controller Management

**Being Annoying:**  
Rogue DHCP server - race condition to direct WAP device to you



assurance

# LWAPP L3



Eventually find controller IP

Find AP Manager address and JOIN

Join REQUEST / REPLY contains SSL handshake

Off you go - all on UDP 12222 / 12223

**Being Annoying:**  
IP conflicts / MAC  
conflicts blah blah blah



# Lets have a look



assurance

# OSI-style threats to LWAPP controllers

## L0/1 for L2/L3 wireless mode

- physical tampering - theft, substitution, etc - x509 helps

## L2/L3 for L2/L3 wireless mode

- Creating conflicts, APs, GWs, etc; attacking path from AP to controller; DHCP option 43 and DNS misdirection for CISCO-LWAPP-CONTROLLER.\${DHCP domain name} - hello Kaminsky?

## L4-7 for mgmt interfaces



# LWAPP console 2-stage

Base ethernet MAC Address: **00:1b:0c:fb:b6:c2**

Initializing ethernet port 0...

Reset ethernet port 0...

Reset done!

link auto-negotiating....

auto-negotiation takes 10000 milli-seconds to complete

ERROR: timeout waiting for auto-negotiation to complete

ERROR: fail to bring ethernet link up

The system has been encountered an error initializing ethernet port. You may need to check hardware

The system is ignoring the error and continuing boot.

If you interrupt the system boot process, the following commands will reinitialize ethernet, tftp, and finish loading the operating system software:

**ether\_init**

**tftp\_init**

**boot**

assurance



# LWAPP Physical Console

%DHCP-6-ADDRESS\_ASSIGN: Interface FastEthernet0 assigned DHCP address 172.16.6.204, mask 255.255.255.0, hostname AP001b.0cfb.b6c2

Translating "**CISCO-LWAPP-CONTROLLER.subdom.thevictimblahblah.com**"...domain server (**192.168.97.101**) [OK]

%LWAPP-3-CLIENTEVENTLOG: Did not get vendor specific options from DHCP.

%LWAPP-3-CLIENTEVENTLOG: Did not get log server settings from DHCP.

%SYS-6-LOGGINGHOST\_STARTSTOP: **Logging to host 255.255.255.255 started** - CLI initiated

%LWAPP-3-CLIENTEVENTLOG: Performing DNS resolution for CISCO-LWAPP-CONTROLLER.subdom.thevictimblahblah.com

%LWAPP-3-CLIENTEVENTLOG: Controller address **192.168.97.101** obtained through DNS

%LWAPP-5-CHANGED: LWAPP changed state to JOIN



assurance

# Quick look at stuff



assurance

# Turning the tables - controller as attack platform



assurance

# Rogue AP - ctrlr-style



assurance

# Evil Fun

Deploying APs into  
other people's  
networks

\* i can haz remote  
net info?

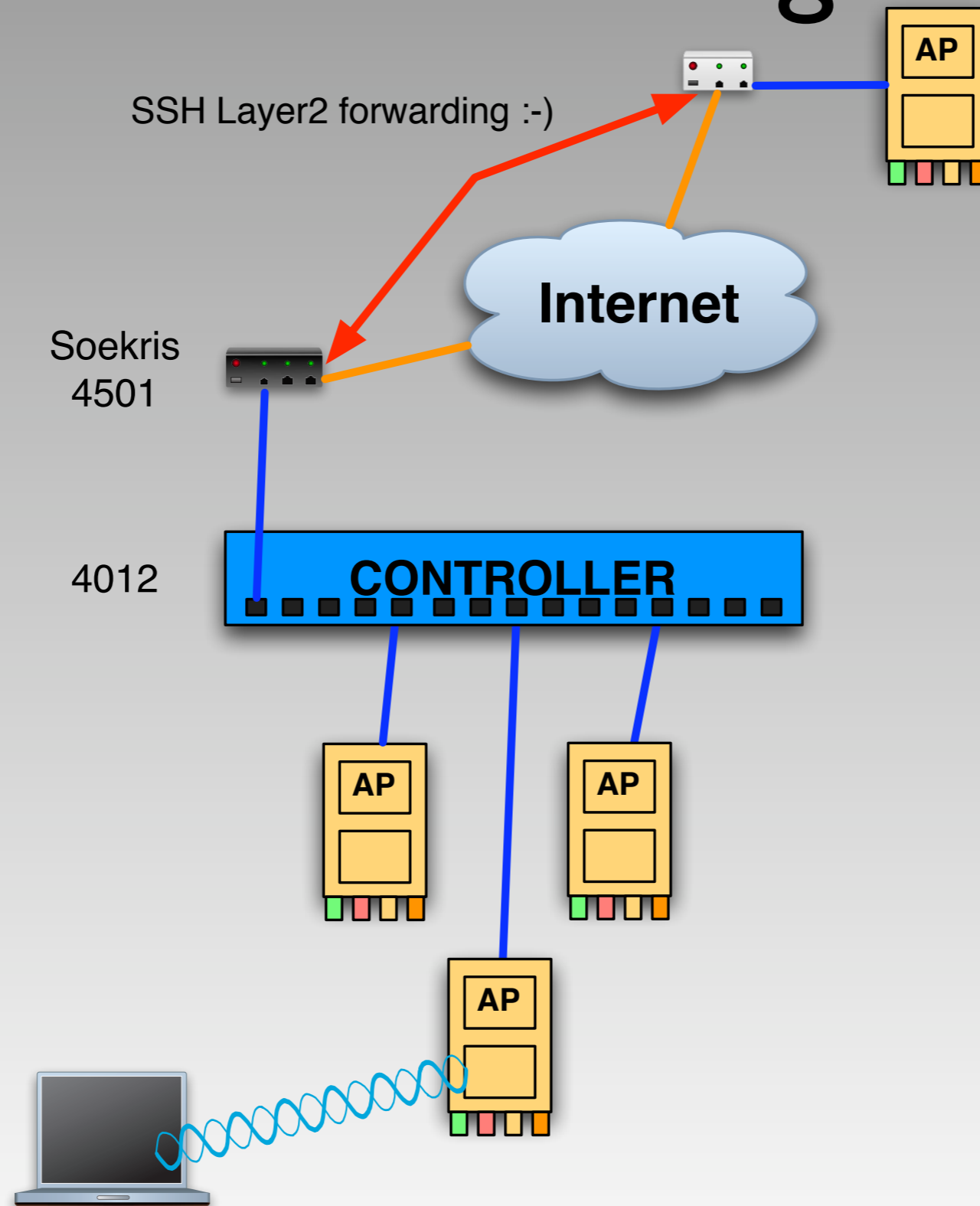
\* sniffing feature of  
airespace-style  
wireless



Coco - Libra - likes naps,  
chewing cardboard/cat5 and mayhem



# Remote WAP sniffing



# Sniffing etc

Cleaning staff are probably afraid of my room

Modified  
code from  
Andreas  
Liebe which  
did airespace  
airopeek style  
sniff to pcap

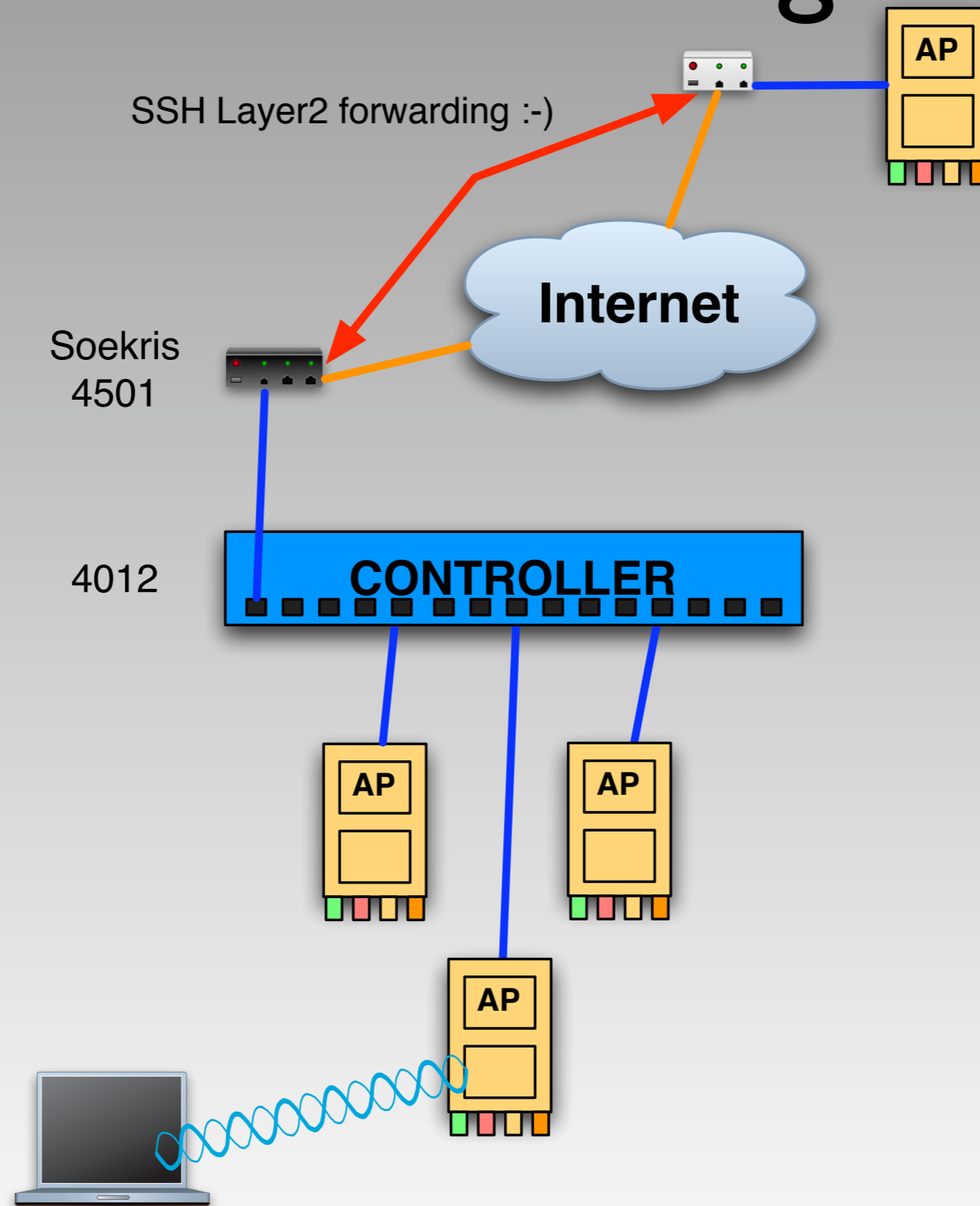
Made a quick  
hack to drive  
it to  
wireshark



assurance

AusCERT 2009

# Remote WAP sniffing

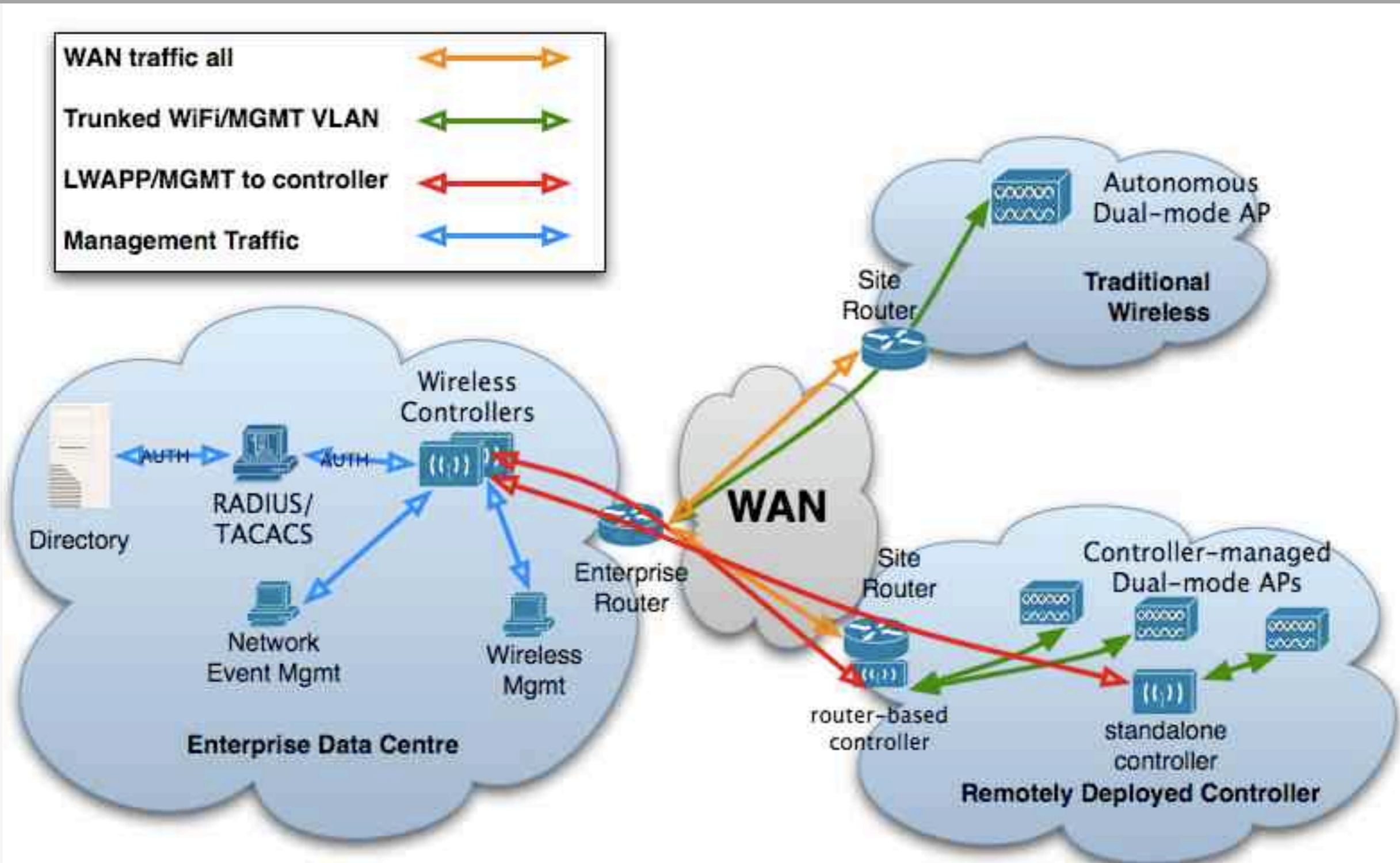


# Demo



assurance

# Architecture



# Key areas to consider

Events should be captured and reviewed

Traffic leaving the WLANs should pass over a L2 IDS to prevent network-based stuff like DNS tunneling

Management interfaces should be secured

ACLs should be applied to avoid exposing the WLAN management interfaces (I.I.I.I, real addresses, etc)

Guest WLANs should be avoided - shared infra with real WLANs



# FIN

Thanks for listening and thanks to...

AusCERT, Pat Gray, A.P., Metlstorm, antic0de, Kiwicon  
and Ruxcon folks



assurance

AusCERT 2009