Wireless in (somewhat) hostile environments

ARUBA™

The Mobile Edge Company

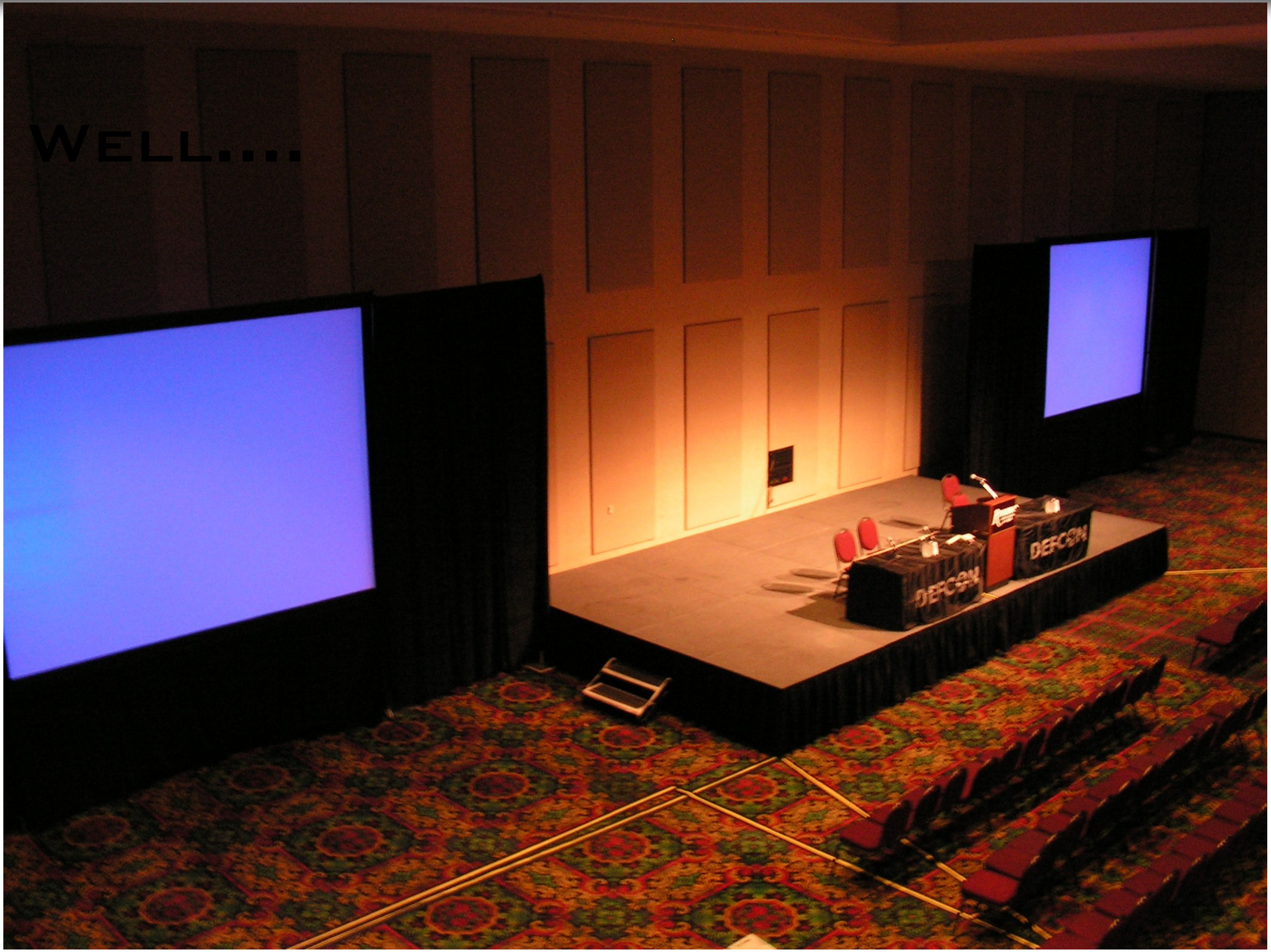
Luiz Eduardo
CISSP, CWNE, GCIH, CEH
Systems & Security Engineer, CALA

Agenda

- History
- Why the network?
- The NOC Team
- Network infrastructure
- Statistics
- Challenges
- Other conferences
- conlusion

History

- Well….



The Networks

- Wired
  - Speakers
  - Press
  - Goons
  - Public Servers
- Wireless
  - Public Access

The NOC Team

DC14 Network

- 6 Mb internet uplink
- trusty OpenBSD firewalls
- Lots of cable & gaffers tape
- Trusty Aruba Networks gear
- awesome hotel AV/IT staff!

WLAN gear

- Aruba Controller
- ~20 APs and ~10 AMs
- Carefully designed configuration
- Wireless IDS/IPS
- ... And the cool RF stuff

Statistics

DC14 WLAN Stats

- Average number of users on WiFi: 220 users
- Max number of users at the same time: 515 users
- WLAN Traffic:
  - ~ 70 Gig In
  - ~ 35 Gig Out

More Stats...

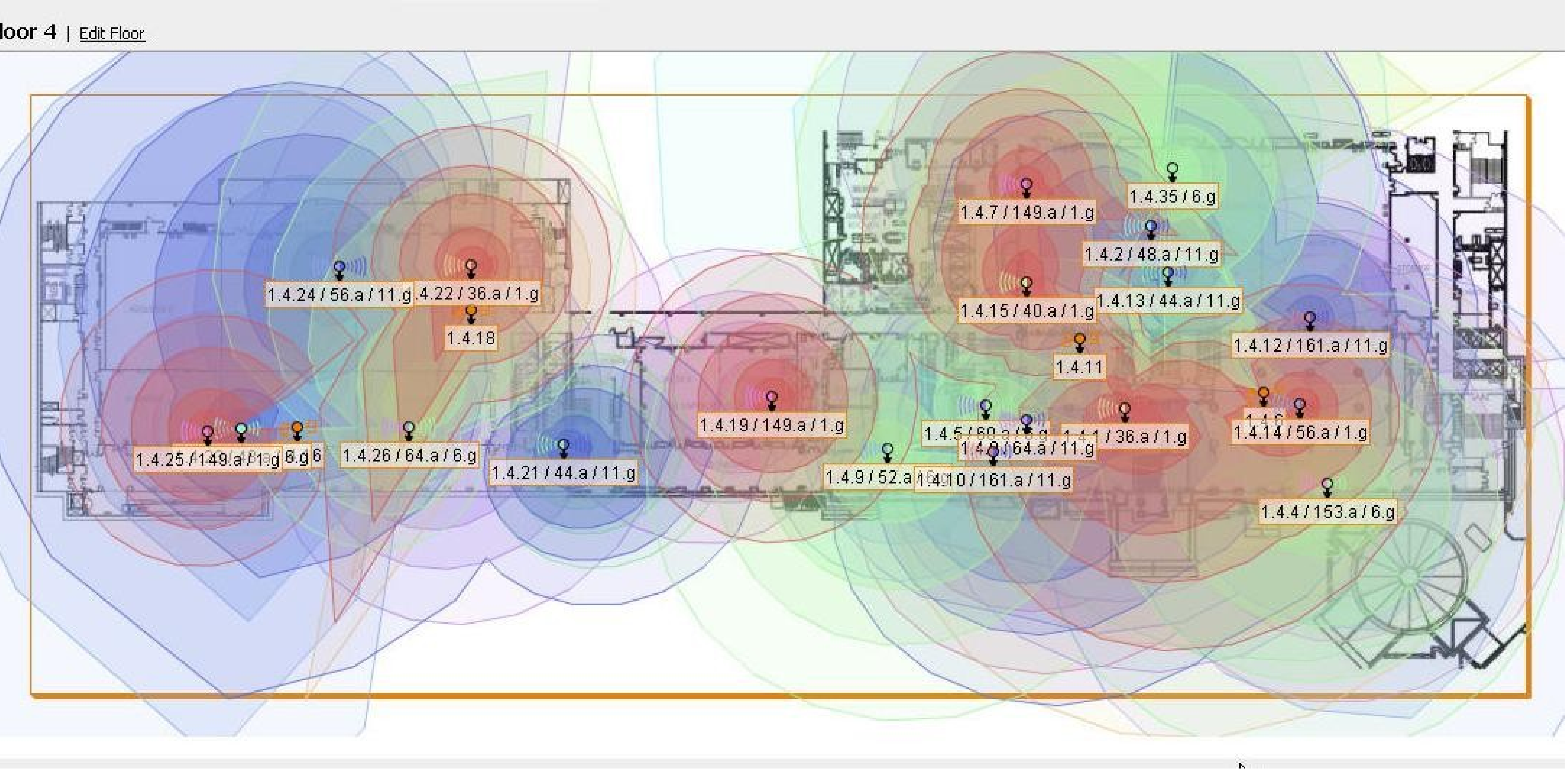
Events	
Adhoc Network Detected Events	6120
AP Impersonation Events	142
ARM Events	2040
Channel Rate Auth Anomaly Events	270
Channel Rate Associate Anomaly Events	11
Channel Rate Deauth Anomaly Events	21
Channel Rate Disassociate Anomaly Events	2
Channel Rate Probe Request Anomaly Events	3
Channel Rate Probe Response Anomaly Events	52
Deauth Broadcast Signature Match Events	60
Frame Receive Error Rate Events (above 50%)	1019
Frame Retry Rate Events (above 50%)	62,922
NetStumbler Generic Signature Match Events	80
NetStumbler Ver 3.3.x Signature Match Events	180
Null Probe Response Signature Match Events	241
Interfering AP Events	19,582
Man In the Middle Events	9,144
Node Rate Auth Anomaly Events	1,472
Node Rate Associate Anomaly Events	210
Node Rate Deauth Anomaly Events	215
Node Rate Disassociate Anomaly Events	32
Node Rate Probe Request Anomaly Events	1,802
Node Rate Probe Response Anomaly Events	3866
Rogue AP Events	10
Sequence Number Anomaly Events	12,826
Wireless Bridge Events	1,990

Challenges

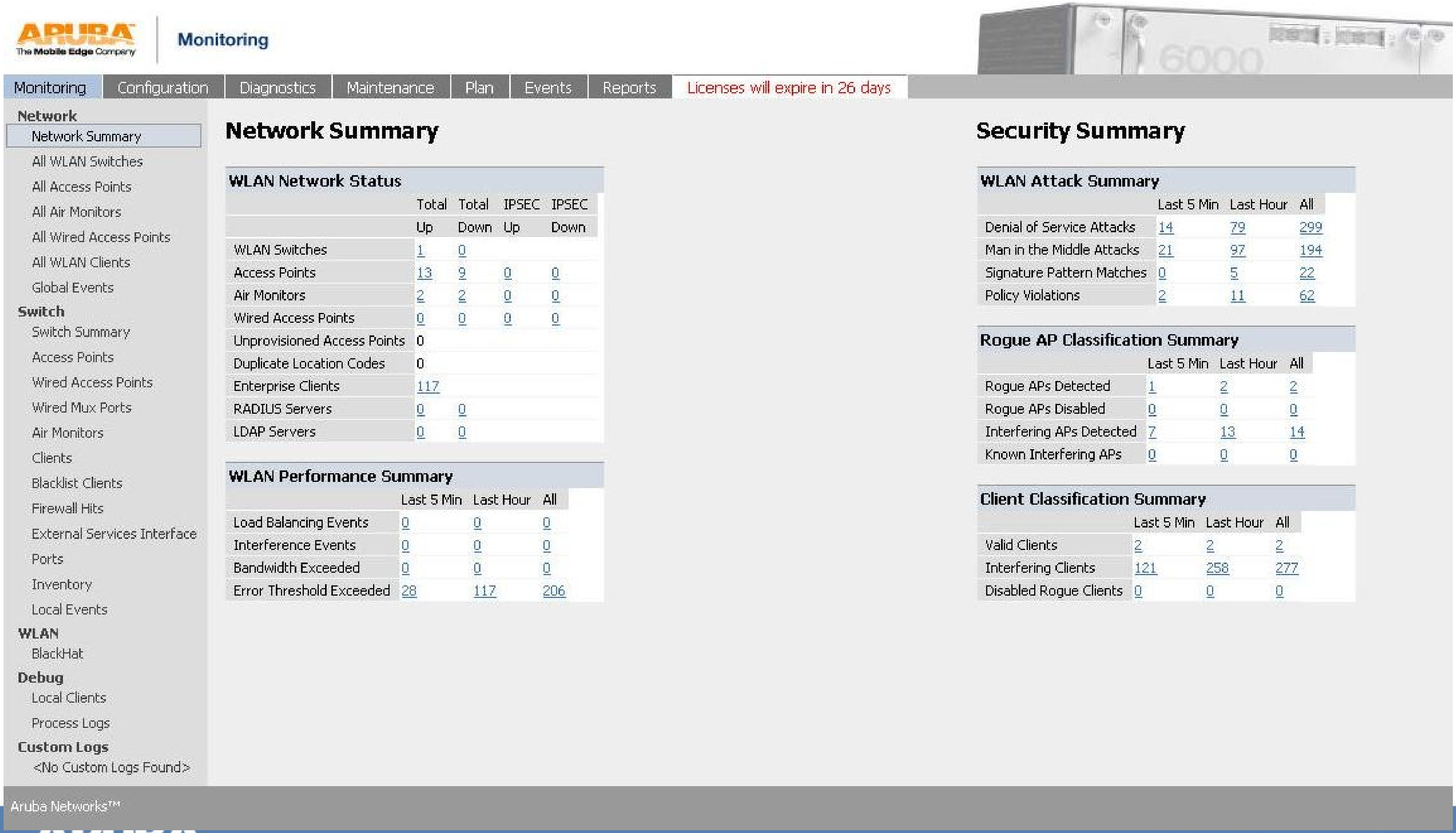
- Installation (kinda)
- Small problems, incidents here and there
- A few special requests
- (some) of the usual problems in totally opened wireless networks

… (ONCE AGAIN) IT WORKED

Blackhat WLAN



Blackhat USA 06 - WLAN Stats



Licenses will expire in 26 days

Network Summary

WLAN Network Status

	Total Up	Total Down	IPSEC Up	IPSEC Down
WLAN Switches	1	0		
Access Points	13	9	0	0
Air Monitors	2	2	0	0
Wired Access Points	0	0	0	0
Unprovisioned Access Points	0			
Duplicate Location Codes	0			
Enterprise Clients	117			
RADIUS Servers	0	0		
LDAP Servers	0	0		

WLAN Performance Summary

	Last 5 Min	Last Hour	All
Load Balancing Events	0	0	0
Interference Events	0	0	0
Bandwidth Exceeded	0	0	0
Error Threshold Exceeded	28	117	206

Security Summary

WLAN Attack Summary

	Last 5 Min	Last Hour	All
Denial of Service Attacks	14	79	299
Man in the Middle Attacks	21	97	194
Signature Pattern Matches	0	5	22
Policy Violations	2	11	62

Rogue AP Classification Summary

	Last 5 Min	Last Hour	All
Rogue APs Detected	1	2	2
Rogue APs Disabled	0	0	0
Interfering APs Detected	7	13	14
Known Interfering APs	0	0	0

Client Classification Summary

	Last 5 Min	Last Hour	All
Valid Clients	2	2	2
Interfering Clients	121	258	277
Disabled Rogue Clients	0	0	0

Stats

Events	
Adhoc Network Detected Events	4,096
AP Impersonation Events	92
ARM Events	1,400
Channel Rate Auth Anomaly Events	220
Channel Rate Associate Anomaly Events	6
Channel Rate Deauth Anomaly Events	16
Channel Rate Disassociate Anomaly Events	0
Channel Rate Probe Request Anomaly Events	0
Channel Rate Probe Response Anomaly Events	38
Deauth Broadcast Signature Match Events	46
Frame Receive Error Rate Events (above 50%)	862
Frame Retry Rate Events (above 50%)	43,922
NetStumbler Generic Signature Match Events	60
NetStumbler Ver 3.3.x Signature Match Events	140
Null Probe Response Signature Match Events	168
Interfering AP Events	13,582
Man In the Middle Events	6,144
Node Rate Auth Anomaly Events	1,472
Node Rate Associate Anomaly Events	132
Node Rate Deauth Anomaly Events	174
Node Rate Disassociate Anomaly Events	24
Node Rate Probe Request Anomaly Events	1,348
Node Rate Probe Response Anomaly Events	2,866
Rogue AP Events	20
Sequence Number Anomaly Events	9,826
Wireless Bridge Events	1,990

22c3 – Berlin

22c3 Network Infra

1.2.7 / 6.g
1.2.10 / 1.g
1.2.8 / 52.a
1.2.1 / 6.g
1.2.9
1.2.3 / 6.g
1.2.12 / 6.g
1.2.1
1.3.6
1.3.1 / 1.g
1.3.5
1.3.2 / 6.g
1.3.10 / 60.a
1.3.11 / 64.a
1.3.9 / 36.a
1.3.8 / 1.g
1.3.12 / 1.g
1.1.4 / 1.g
1.1.6 / 6.g
1.1.7 / 44.a
1.1.5
1.1.8 / 1.g
1.1.3
1.1.1 / 1.g
1.1.2 / 6.g

- 10 Gig “in-house” backbone
- 2000+ wired GigE ports available
- 10Gig + uplink to the Internet
- Aruba controller w/ 26 APs and 9 AMs

22c3 Internet Stats (4 days)

Average

802 Mbps out

233 Mbps in

Peak

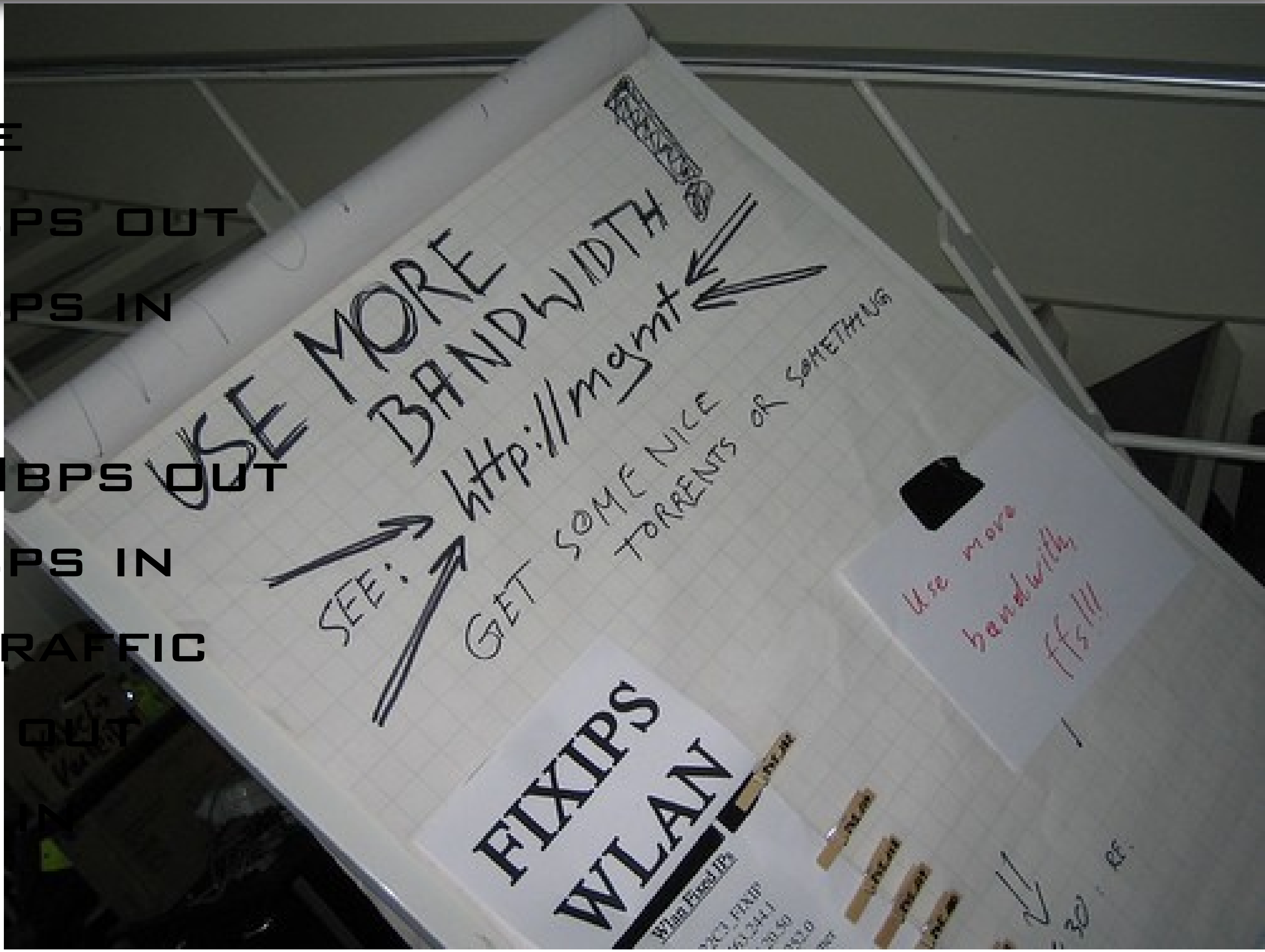
1325 Mbps out

526 Mbps in

Total Traffic

~40 Tb out

~10 Tb in



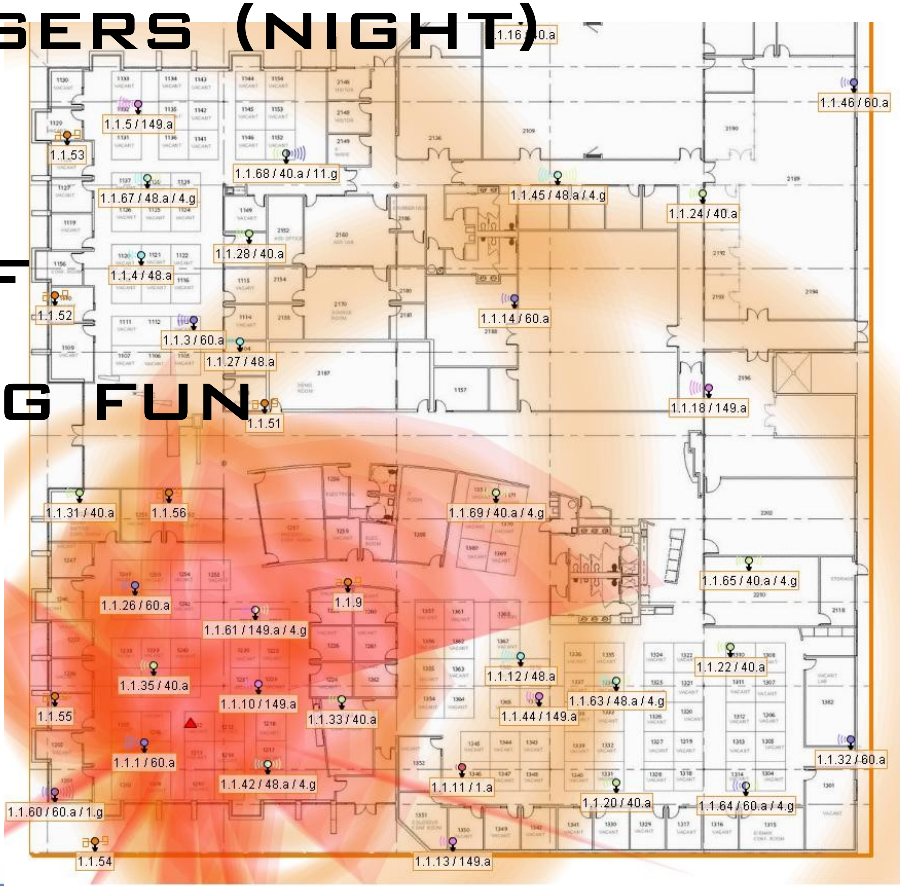
22c3 WLAN stats

- Average = 350 users (day)

  130 users (night)

Peak = 509 users

- WIDS/ WIPS stuff
- Location tracking fun



Conclusion

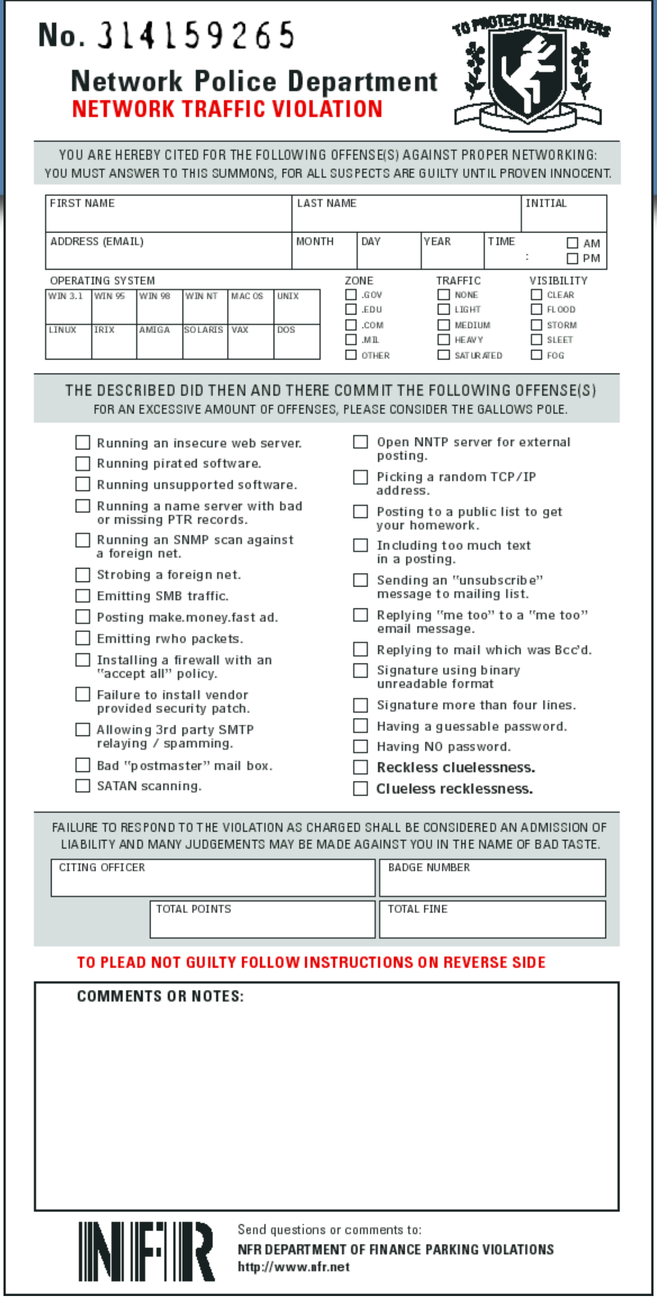
- Plan Plan Plan
- protect the users
- Protect the infrastructure
- Smart RF helps
- Provide decent service since …

… People just can’t live without the internet

Thanks!!!!

Comments/ questions/ flames?

luiz (at) arubanetworks.com



No. 314159265

TO PROTECT OUR SERVERS

Network Police Department

NETWORK TRAFFIC VIOLATION

YOU ARE HEREBY CITED FOR THE FOLLOWING OFFENSE(S) AGAINST PROPER NETWORKING:
YOU MUST ANSWER TO THIS SUMMONS, FOR ALL SUSPECTS ARE GUILTY UNTIL PROVEN INNOCENT.

FIRST NAME		LAST NAME		INITIAL
ADDRESS (EMAIL)	MONTH	DAY	YEAR	TIME : □ AM □ PM

OPERATING SYSTEM

WIN 3.1	WIN 95	WIN 98	WIN NT	MAC OS	UNIX
LINUX	IRIX	AMIGA	SOLARIS	VAX	DOS

ZONE	TRAFFIC	VISIBILITY
□ .GOV	□ NONE	□ CLEAR
□ .EDU	□ LIGHT	□ FLOOD
□ .COM	□ MEDIUM	□ STORM
□ .MIL	□ HEAVY	□ SLEET
□ OTHER	□ SATURATED	□ FOG

THE DESCRIBED DID THEN AND THERE COMMIT THE FOLLOWING OFFENSE(S)
FOR AN EXCESSIVE AMOUNT OF OFFENSES, PLEASE CONSIDER THE GALLOWS POLE.

- □ Running an insecure web server.
- □ Running pirated software.
- □ Running unsupported software.
- □ Running a name server with bad or missing PTR records.
- □ Running an SNMP scan against a foreign net.
- □ Strobing a foreign net.
- □ Emitting SMB traffic.
- □ Posting make.money.fast ad.
- □ Emitting rwho packets.
- □ Installing a firewall with an "accept all" policy.
- □ Failure to install vendor provided security patch.
- □ Allowing 3rd party SMTP relaying / spamming.
- □ Bad "postmaster" mail box.
- □ SATAN scanning.
- □ Open NNTP server for external posting.
- □ Picking a random TCP/IP address.
- □ Posting to a public list to get your homework.
- □ Including too much text in a posting.
- □ Sending an "unsubscribe" message to mailing list.
- □ Replying "me too" to a "me too" email message.
- □ Replying to mail which was Bcc'd.
- □ Signature using binary unreadable format
- □ Signature more than four lines.
- □ Having a guessable password.
- □ Having NO password.
- □ **Reckless cluelessness.**
- □ **Clueless recklessness.**

FAILURE TO RESPOND TO THE VIOLATION AS CHARGED SHALL BE CONSIDERED AN ADMISSION OF LIABILITY AND MANY JUDGEMENTS MAY BE MADE AGAINST YOU IN THE NAME OF BAD TASTE.

CITING OFFICER	BADGE NUMBER
TOTAL POINTS	TOTAL FINE

TO PLEAD NOT GUILTY FOLLOW INSTRUCTIONS ON REVERSE SIDE

COMMENTS OR NOTES:

NFR

Send questions or comments to:
NFR DEPARTMENT OF FINANCE PARKING VIOLATIONS
http://www.nfr.net

http://lists.dc55.org/mailman/listinfo/vegas