



DC BSD Con 2009

Ken Caruso

ken@shmoo.com

ShmooCon Labs

An exercise in chaos

WARNING!

- If you are looking at these slides after BSD Con please do so with accompanied video and audio. I purposely do not make slide decks that repeat what I am speaking to the audience because I feel that defeats the purpose of them. Thanks! -Ken

What is it?

- Conference network build out
- Open to the public
- Security/Network vendors invited
- Day and ½ to get everything running
- Inspired by Network World Interop Lab
 - The result?



A NETWORK CABLE IS UNPLUGGED

You're fucked.

Technologies Used

- IPS/IDS
- Switching/Vlans/Vlan routing/Trunk
- Virtualization
- Vulnerability Assessment
- Controller Based Wifi
- Configuration Management
- Network Monitoring

Commercial Products

- Cisco – ASA/Switches
- Qualys – Vuln Assessment
- Tenable – Vuln Assessment (Nessus)
- Nitro – IPS/IDS
- Aruba – Wireless Controller

Open Source

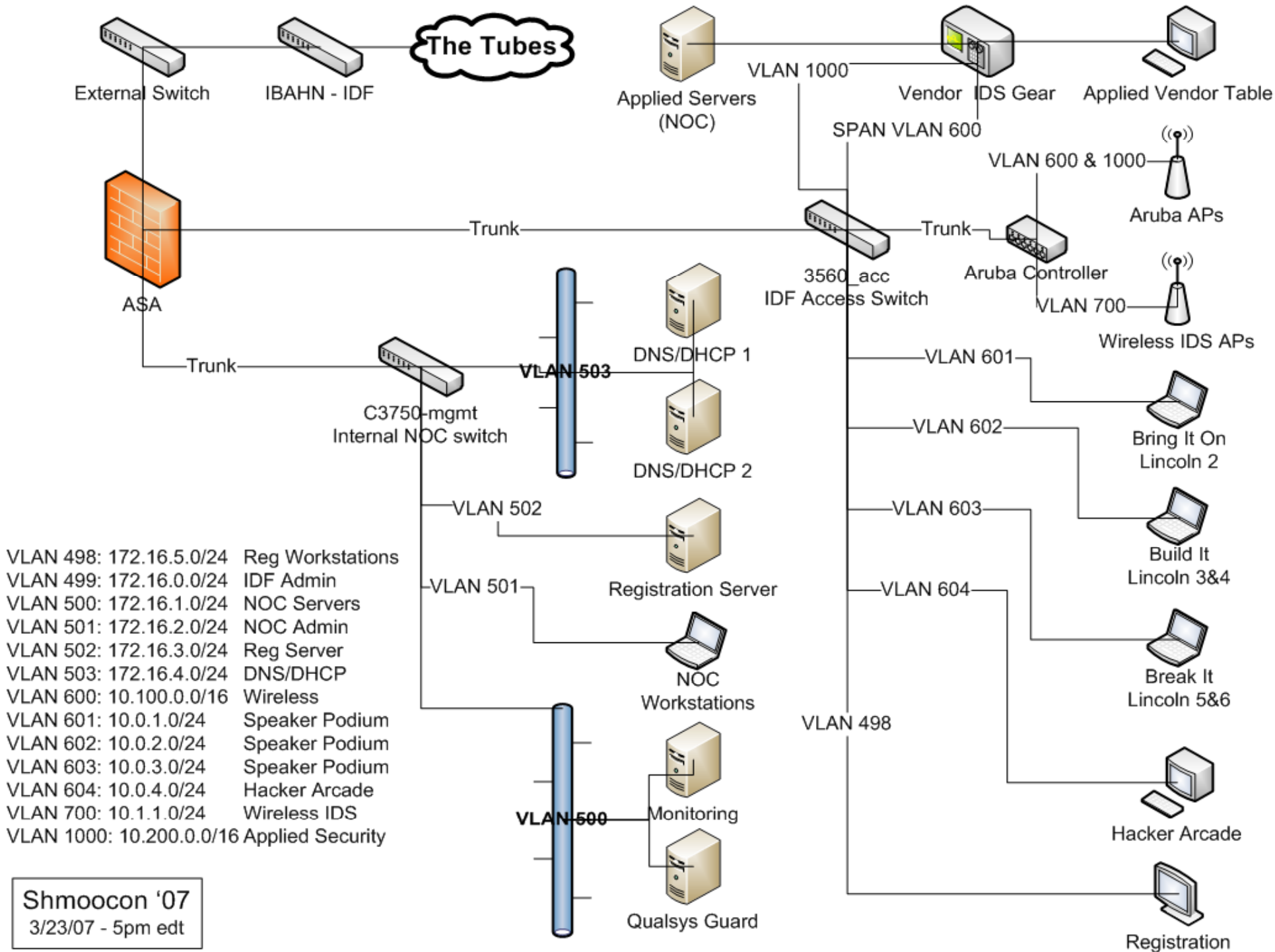
- *BSD
 - Pfsense in the past (FreeBSD /w pf)
 - Originally used FreeBSD/Soekris Aps before controller based systems
 - FreeBSD:
 - Host for Nagios, dhcpd, snort, munin, cacti etc...
 - Linux:
 - Packet Capture, KVM host, maradns,

Philosophy

- Availability > Security
 - We have no “data” to secure
 - We need to be able to troubleshoot and manage
 - Slightly different than some hacker cons
- Modular
 - Segregate network segments as much as possible
 - Aids in trouble shooting

Wireless

- WPA2 network w/certs & radius
 - Public SSL site where people can create radios accounts and download the CA File
- Open Wifi Network
 - Traditional open wifi
- Mosh Pit Network
 - Various old and crufty things running for people to play with
- All networks are virtual SSIDs trunked and delivered through the same access points



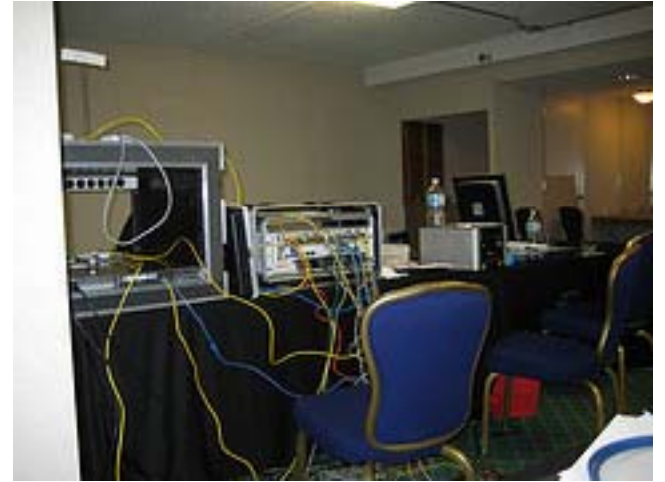
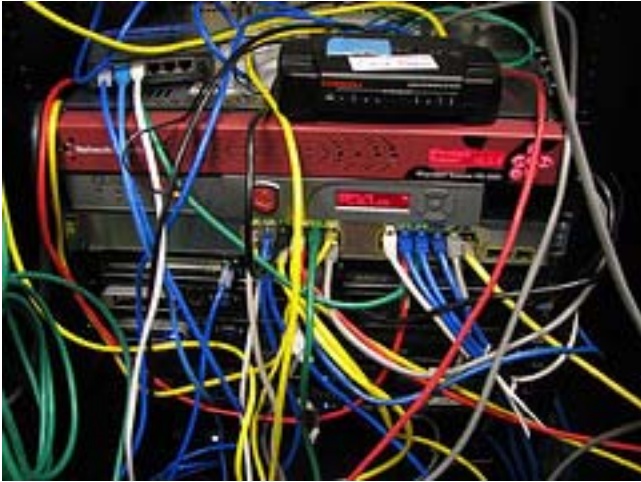
Shmocon '07
3/23/07 - 5pm edt

Issues?



Issues

- Hotel IT issues
 - Needs not always understood
 - Confusion, “Your wireless network is breaking a guests EVDO card!”
- Interop problems
 - Multiple vendors show up with gear we have never seen before
- Complexity and the number of people
- Strange bugs
 - FreeBSD network driver bug that drops frames over 1500 bytes (Pfsense)



Questions??

