What's on your Network?

Mark Jeffries
Favarger Consulting
mark@favarger.net

Monitoring vs. Managing

- Who's on your network?
- Why do you care?
- Servers, Clients, Mobile Devices, FileServers, WAPs
- Going in Blind
- Mapping out network - are results what you expect?

MACTECH

How do you Identify What's on your Network

- Scan the network
  - iNet / subnet insight
  - Network Utilities
  - Wireshark (and other big guns)
- Use the Network
  - Gateway - DHCP & DNS
  - Switches
  - SNMP

MACTECH

How do you Identify What's on your Network

- Analyze the Data
  - Break it down
  - Follow a path
  - Look for Patterns
  - Test your theory

MACTECH

Scanning with GUI

- iNet
- Subnet Insight
- Network Utility
- Scan any IP range
- Services available on host
- Bonjour Browser

MACTECH

Scanning with CLI

- ping
- host
- arp -a vs. arp
- netttop
- tcpdump
- ping broadcast IP

Hidden CL Tools

- airport -s
- ./stroke

Command Line Resources

- man command
- Bwana - http://www.bruji.com
- Google
- Wikipedia

MACTECH

Wireshark

- Make sense of all those packets
- “it just cuts out”
- “it’s consistently inconsistent”
- Capture data and look for pattern

MACTECH

SNMP

- Simple Network Management Protocol
- Layer7
- iNet
- InterMapper

MACTECH

QoS

- Weighting
- Different separations of “classes” of service
  - IP/port based
  - Layer 7
- All devices on route must respect QoS
- Time sensitive traffic

Resources

- Software mentioned:
  - iNet - AppStore
  - Subnet Insight - AppStore
  - Wireshark - www.wireshark.com
  - InterMapper - www.intermapper.com
  - AppleRemote Desktop - AppStore
  - Bonjour Browser - AppStore

MACTECH