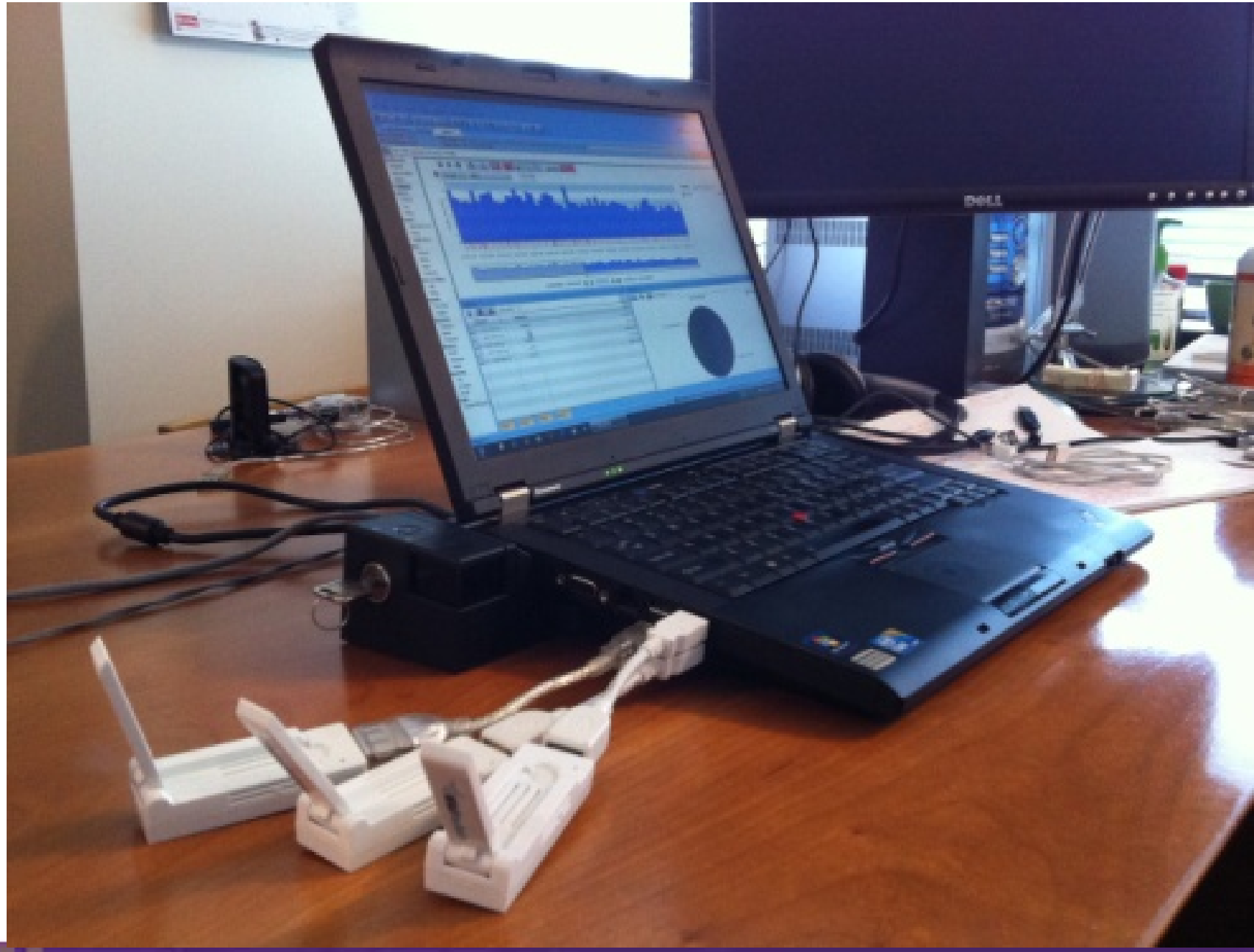
Packet Capture and Analysis in the MU-MIMO 11ac World

Jay Botelho, Director of Product Management, Savvius Inc.

How We Work Today

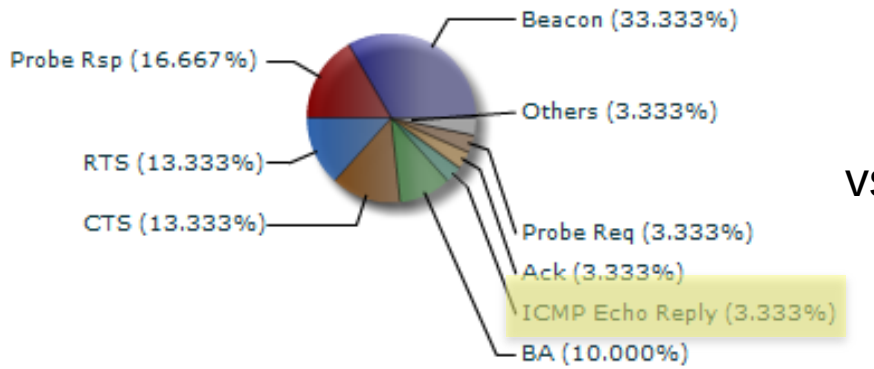


USB WLAN Adapters Are Not Keeping Up

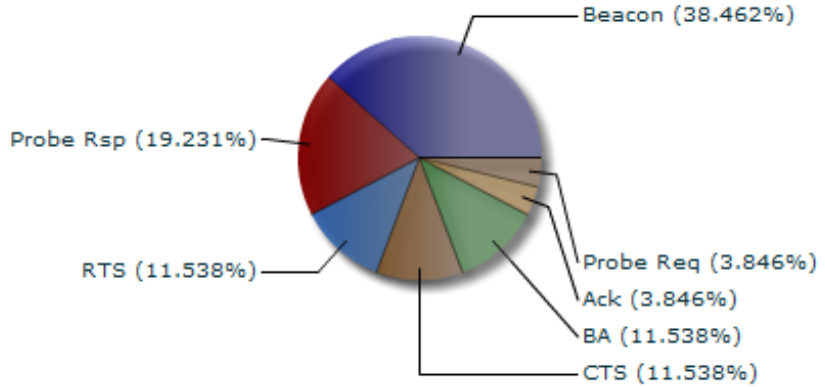
1,733Mbps vs. 866Mbps

The Real World

1,733Mbps vs. 866Mbps



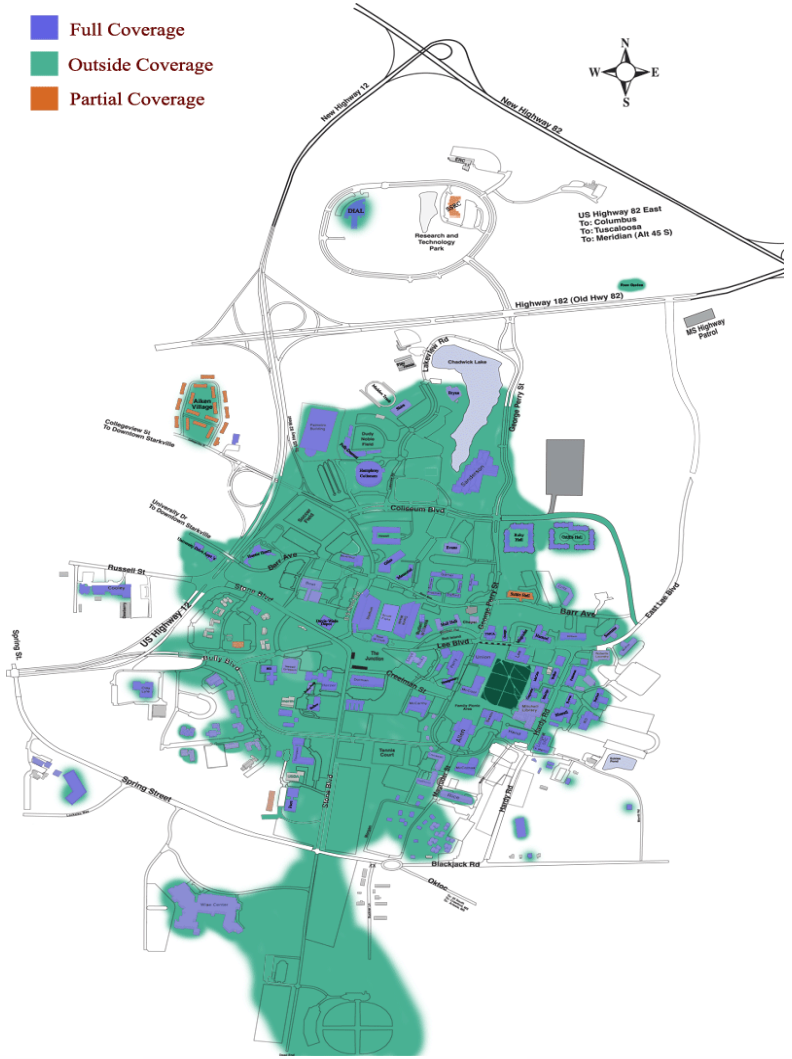
vs.



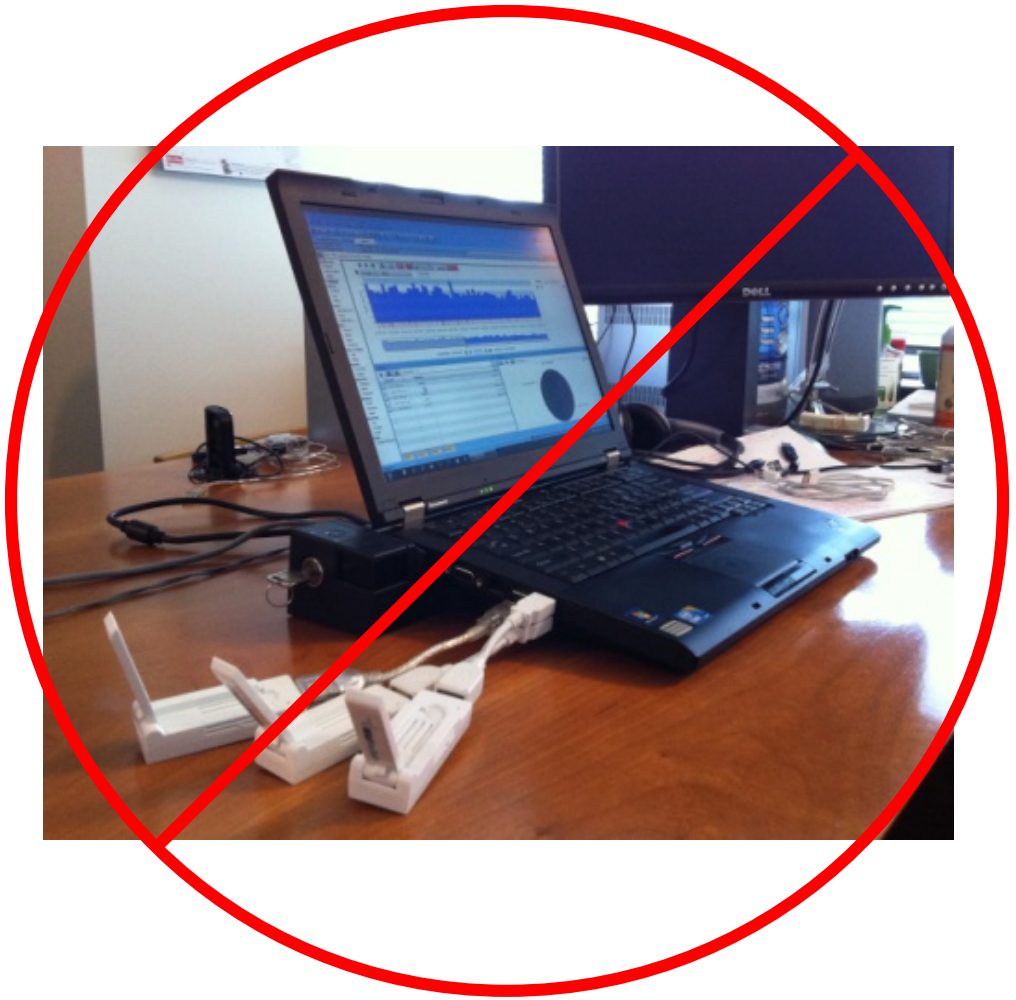
What happened to my ping data?

Wi-Fi Is Everywhere Today

- WLANs are everywhere
  - Lots of AP's
  - Lots of physical distance to cover
- WLAN troubleshooting ***still*** requires a point-of-presence



Portable analysis of enterprise WLANs is no longer feasible



Portable analysis of enterprise WLANs is feasible
only under certain conditions

When Is Portable Wireless Packet Analysis Feasible?

1. It is convenient, or at least feasible, to be where the measurements need to be made
2. You are 100% sure of the environment
3. Only short-term measurement is required
4. The problem is repeatable, or frequent enough to capture quickly
5. Long-term packet retention is not required
6. Measurement from a single location is sufficient
7. You are only interested in a subset of the data, and this data can be captured within the limitations of portable analysis

USB Adapter Capabilities

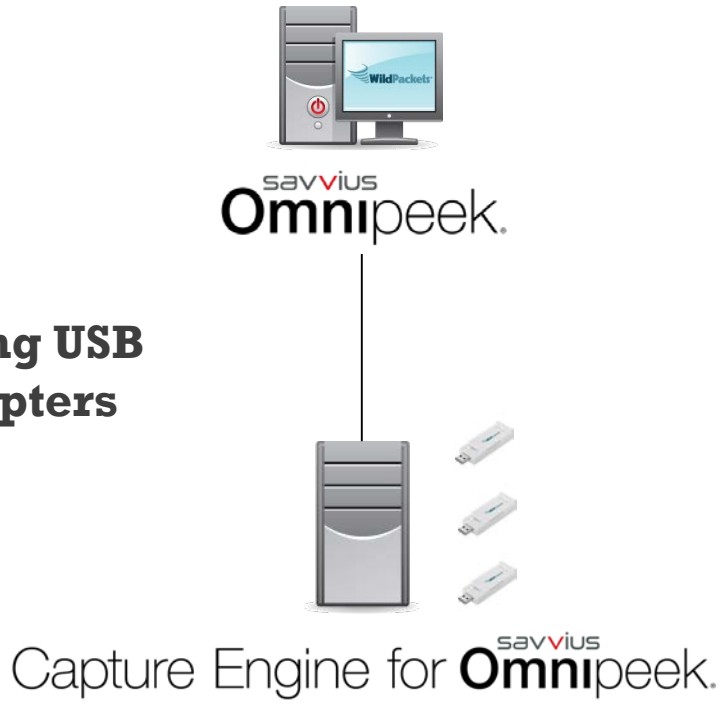
- Product features:
  - USB device with extension cable
  - Dual band operation – 2.4GHz/5GHz
  - All standard international 802.11 channels (a/b/g/n)
  - ***Supports 802.11n - 3 transmit/receive streams (450Mbps)***
  - ***20MHz and 40MHz channel operation***
  - Supports multi-channel aggregation and roaming
- Driver included with Omnipeek
- Tested and supported with OmniPeek and Capture Engine
- Capture Only – no network services
- $59 on Amazon

- Product features:
  - USB device with extension cable
  - Dual band operation – 2.4GHz/5GHz
  - All standard international 802.11 channels (a/b/g/n/ac)
  - ***Supports 802.11ac - 2 transmit/receive streams (867Mbps)***
  - ***20/40/80MHz channel operation***
  - Supports multi-channel aggregation and roaming
- Driver included with Omnipeek
- Tested and supported with OmniPeek and Capture Engine
- Capture Only – no network services
- $149 on Amazon

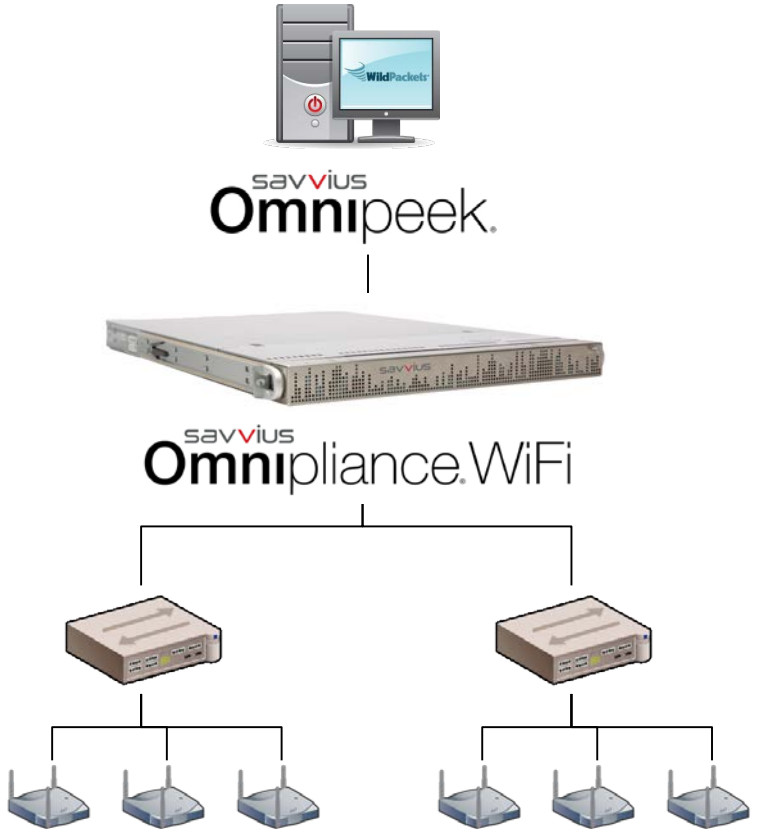
When Portable Isn’t Enough

WLAN Analysis Without Leaving Your Desk

Using USB Adapters



Remote Software Probe for 24x7 Operation



Using APs

Omnipliance WiFi

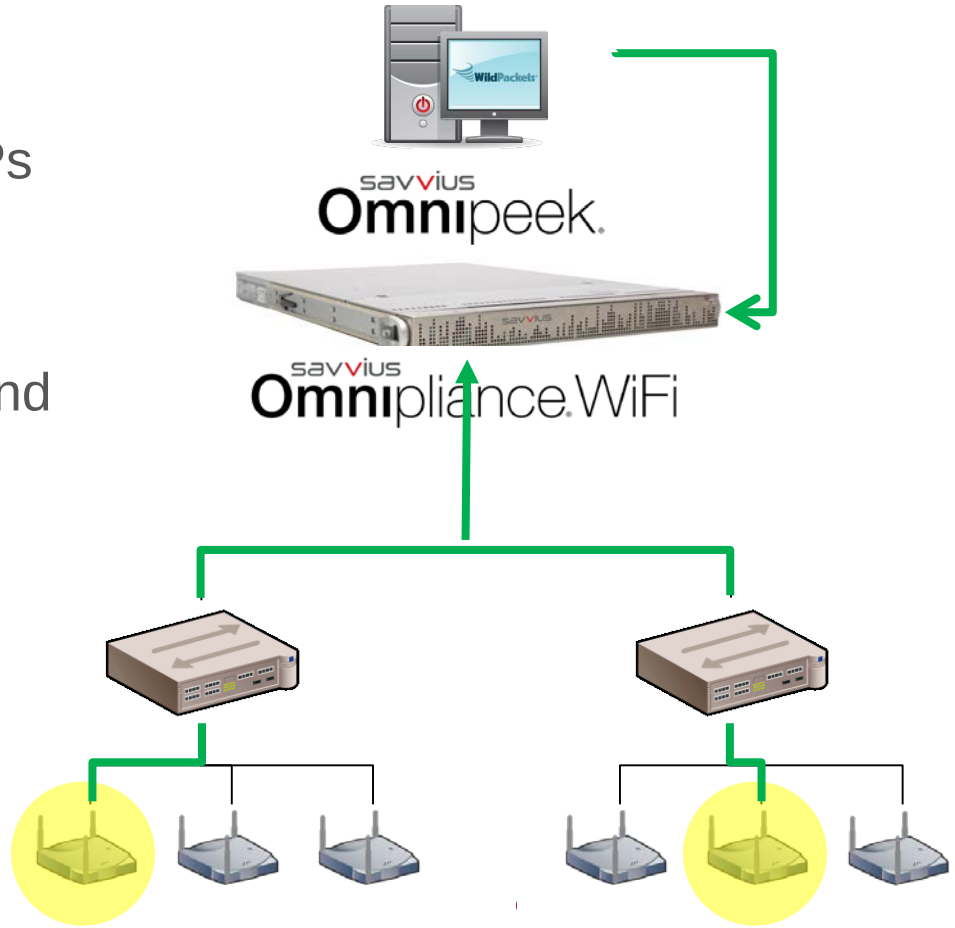
- The first and only dedicated appliance for distributed, 24x7 wireless packet capture and analysis
- Supports multi-gigabit capture rates
- Supports both real-time and forensic analysis simultaneously
- 8TB of storage for recording hours/days of high-speed WLAN traffic
- Captures packets from existing, or dedicated, APs
- Analysis performed locally – no extra traffic on network
- Tested with industry-leading wireless equipment vendors

aruba NETWORKS

CISCO

How Omnipliance WiFi Works

1. Using the WLAN controller UI, put the desired APs in “sniffer” mode, and direct the packets to Omnipliance WiFi – packets start flowing
2. Using Omnipeek, connect to Omnipliance WiFi and configure your Remote Adapter capture
3. Start the capture – analysis (and storage) of all packets from the APs begin immediately

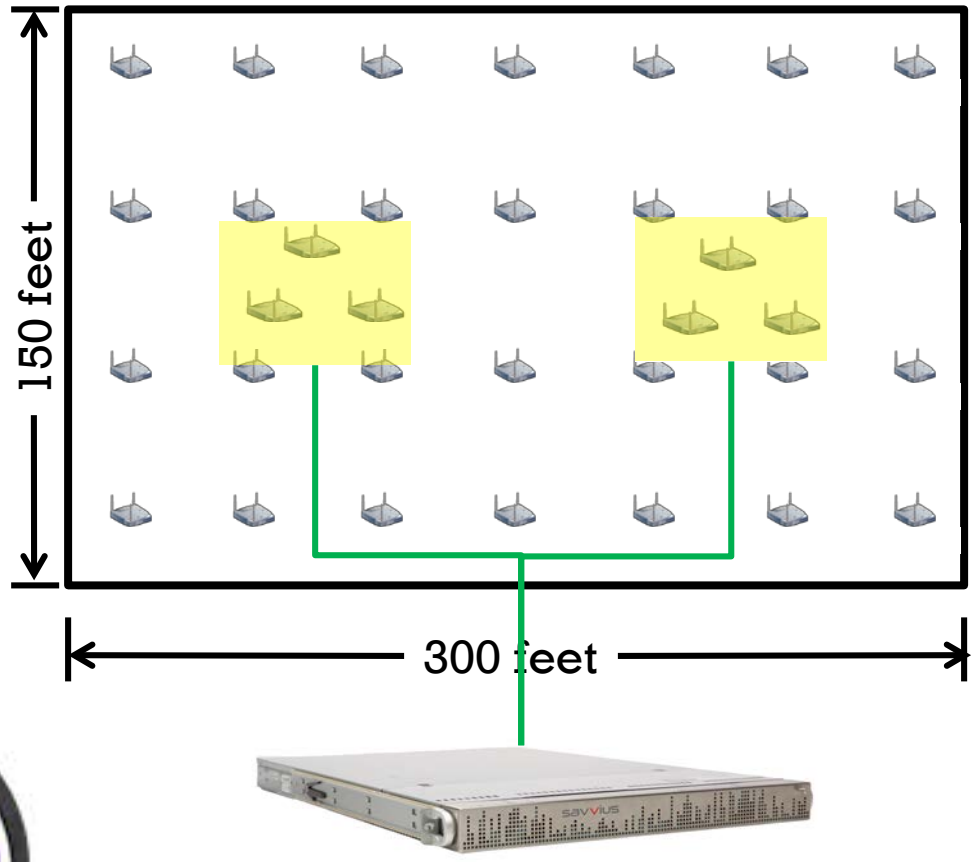


http://www.youtube.com/embed/BcWWeufQn7Q

Example: Mission-Critical Financial Trading

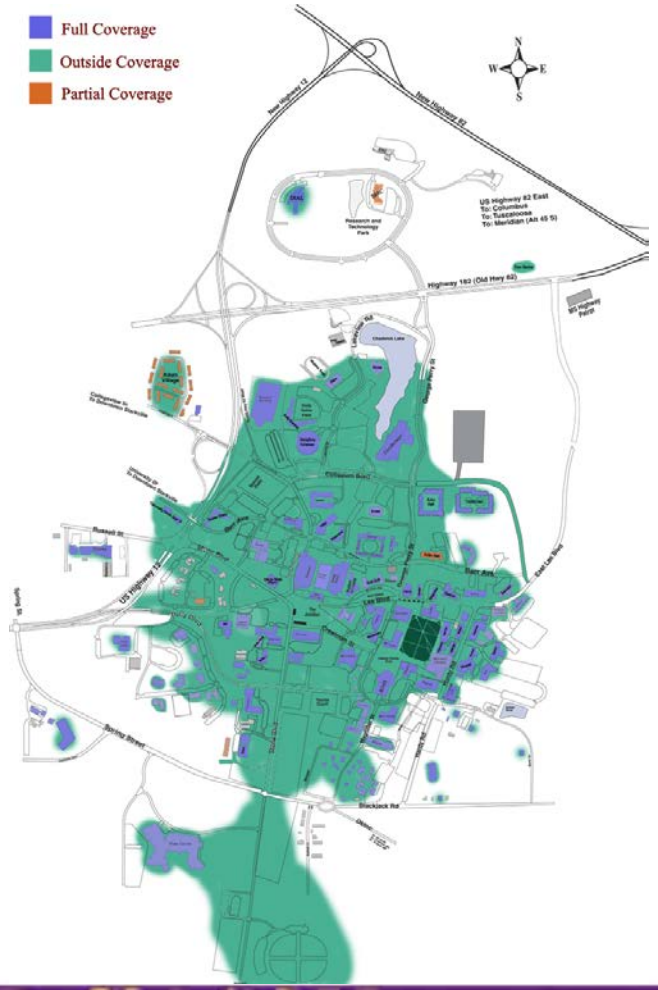
- All users on Wi-Fi; BYOD
- 100’s of simultaneous users
- 100’s of trades per second
- Deliver, verify that each individual gets the same QOS to guarantee fair trading
- Single appliance solution
- 24x7 forensics data capture with additional real-time captures to handle spot problems

High Density/Small Physical Footprint Deployment



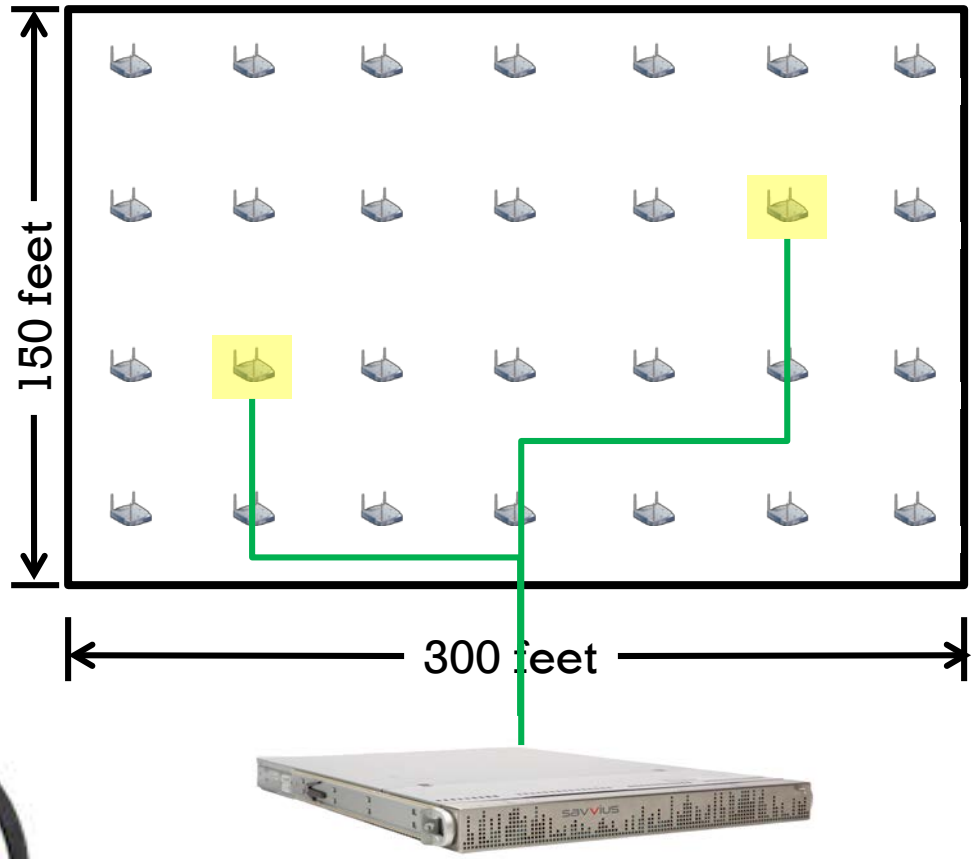
- Dense deployment – 28 APs per trading floor
- Sensor APs – 2 groups of 3
- Provides dedicated, 24x7 monitoring

Example 2: Highly Distributed, Multi-Campus



- All users with multiple devices on Wi-Fi; BYOD
- Wide mix of device capabilities
- 10’s of thousands of users; 1000’s simultaneously
- 10,000 APs
- High bandwidth apps, eg. video

Highly Distributed, Multi-Campus Deployment



- Dense deployment ~ 28 APs per building floor
- 100’s of building floors
- Reactive capture and analysis

24x7 WLAN Analysis Value Proposition

Reduce MTTR	• Begin analyzing issues immediately • Aggregate data from multiple APs • Wi-Fi forensics - No need to reproduce a problem
Gigabit Speed	• Analysis as fast as your 802.11ac Wi-Fi networks
Time-saving Analytics	• Complete 802.11 protocol analysis • VoFi • Roaming
24x7 Enterprise-wide Visibility	• APs represent the maximum capability of your WLAN vs. using USB WLAN adapters
Lower IT Costs & Resources	• Less resources required to manage and troubleshoot • Save travel expenses • Troubleshoot in real time without leaving your desk

And What About MU-MIMO?

MU-MIMO Setup

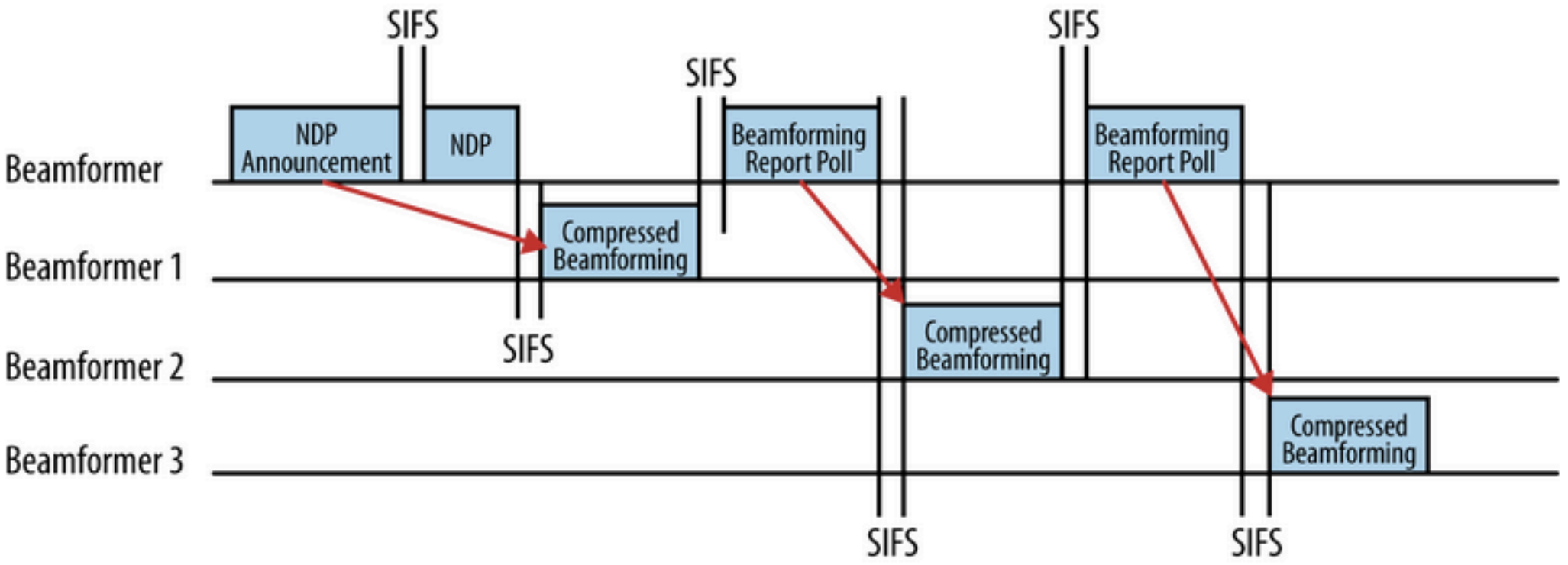


Figure 4-10. Multi-user channel sounding procedure

802.11ac: A Survival Guide;
Matthew Gast, O'Reilly Media, 2013

MU-MIMO Data Transmission

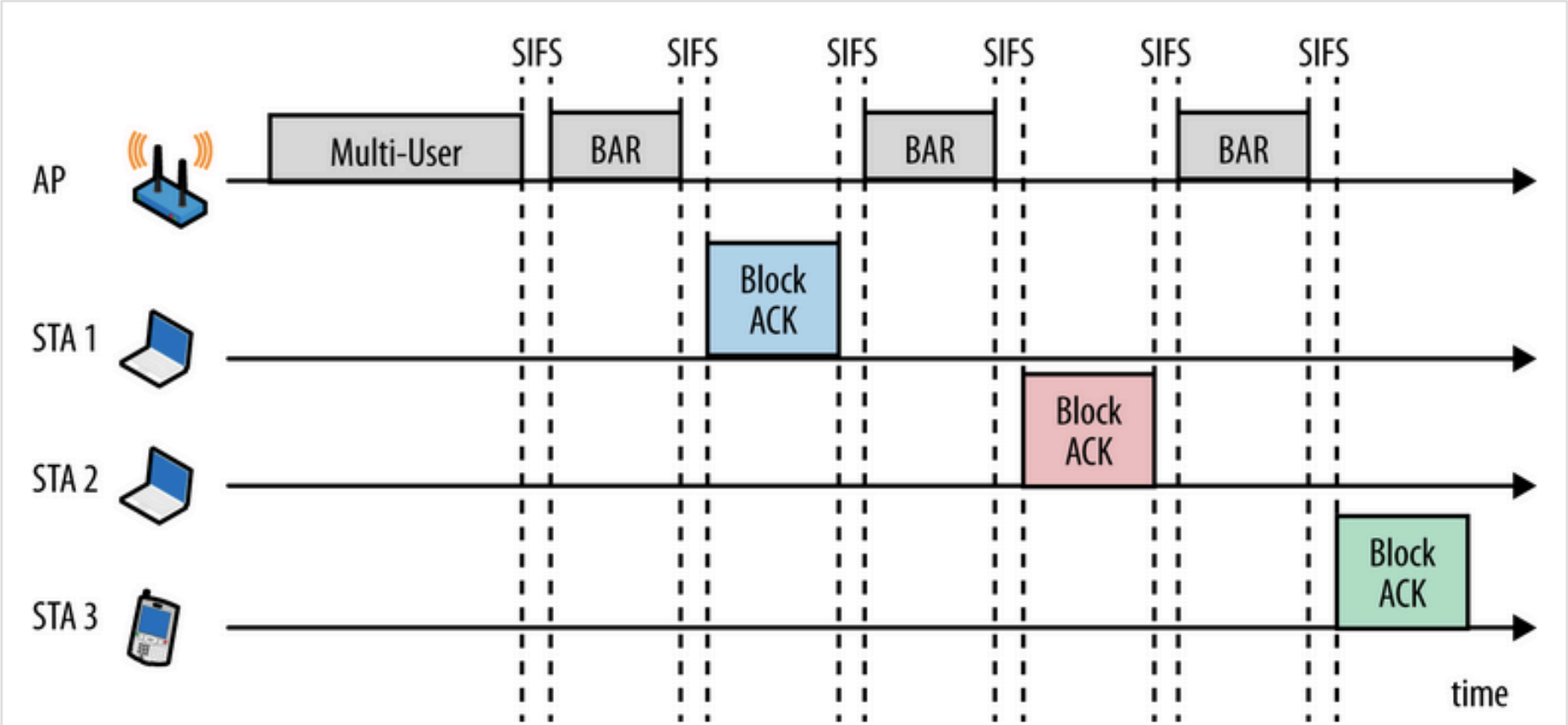


Figure 4-19. Acknowledgement in multi-user MIMO

802.11ac: A Survival Guide; Matthew Gast, O'Reilly Media, 2013

What Can a Sniffer See?

NDP is "invisible"

MU A-MPDU "Signature"

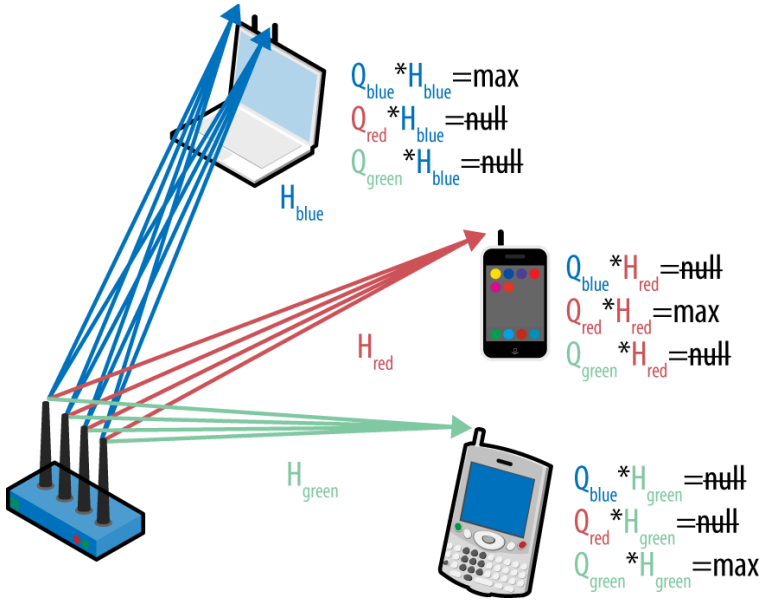
MU Sounding Exchange

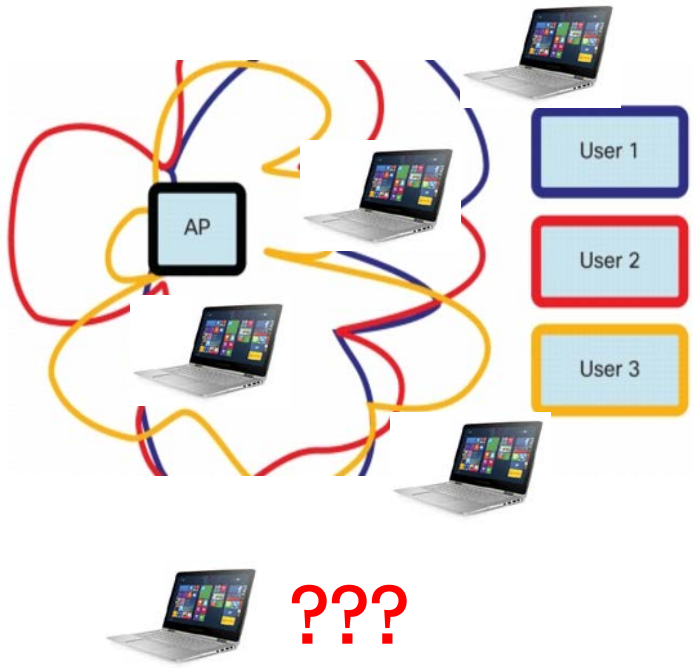
Data TX

Data TX

Data...	Size	Protocol	Decode: Subtype		Delta Time
6.0	27	802.11 Control	%0101	*VHT NDP Announcement*	
29.3	1499	802.11 Management	%1110	*Action No Ack*	0.000542
6.0	21	802.11 Control	%0100	*Beamforming Report Poll*	0.000008
29.3	1499	802.11 Management	%1110	*Action No Ack*	0.000474
6.0	21	802.11 Control	%0100	*Beamforming Report Poll*	0.000009
29.3	1499	802.11 Management	%1110	*Action No Ack*	0.002026
24.0	32	802.11 BA	%1001	*Block Acknowledgement (BlockAck)*	0.001834
24.0	24	802.11 BAR	%1000	*Block Acknowledgement Request (BlockAckReq)*	0.000008
24.0	32	802.11 BA	%1001	*Block Acknowledgement (BlockAck)*	0.000005
24.0	24	802.11 BAR	%1000	*Block Acknowledgement Request (BlockAckReq)*	0.000004
24.0	32	802.11 BA	%1001	*Block Acknowledgement (BlockAck)*	0.000027
6.0	14	802.11 CTS	%1100	*Clear To Send (CTS)*	0.000185
24.0	32	802.11 BA	%1001	*Block Acknowledgement (BlockAck)*	0.001865
24.0	24	802.11 BAR	%1000	*Block Acknowledgement Request (BlockAckReq)*	0.000008
24.0	32	802.11 BA	%1001	*Block Acknowledgement (BlockAck)*	0.000005
24.0	24	802.11 BAR	%1000	*Block Acknowledgement Request (BlockAckReq)*	0.000031
24.0	32	802.11 BA	%1001	*Block Acknowledgement (BlockAck)*	0.000004
6.0	14	802.11 CTS	%1100	*Clear To Send (CTS)*	0.000207

Where Does the Sniffer Go?
Are There Conditions Under Which It Will Work?





- The sniffer doesn't participate in the beam forming
- The sniffer is still isotropic
- The sniffer must be in line to see both the AP and client transmission
- An in line position is likely a noisier one
- The sniffer can only be in one place at a time

Questions?