EtherSniff

How to stealthily monitor an established Ethernet network

by Mark Smith, aka Smitty

Introduction

- Hardwired network paths are secure.
- No encryption needed internally.
- A physical sniffer insertion would break link on network interfaces, triggering alarms.

Right?

- …maybe not…

Introduction: Me

- Mark Smith, aka Smitty
- By day: Network engineer and system administrator for over 15 years
- By night: Maker, ham radio nerd, musician, podcaster, husband, father, closet tree hugger
- Contact me:
  - Email: mark {at} halibut {dot} com
  - @SmittyHalibut just about everywhere else.

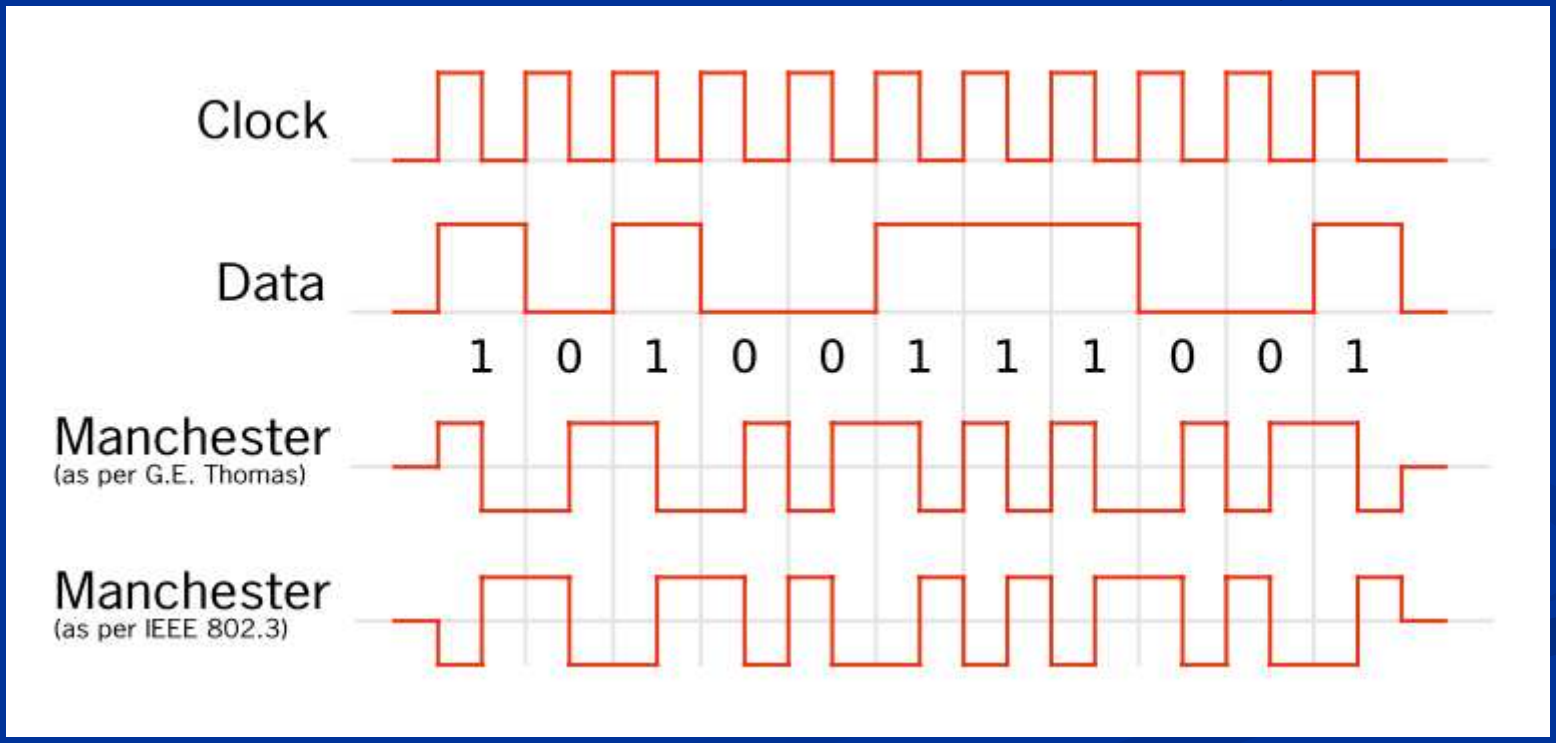
Encoding Techniques: 10baseT

- 10Mbps, baseband (not carrier modulated), Twisted pair.
- 10Mbps data stream, Manchester coded, produces 20MHz square wave signal.
- Bi-state output: +2.5v and -2.5v.
- Full duplex done with two separate simplex pairs: TX and RX

http://en.wikipedia.org/wiki/10BASET

Encoding Techniques: 10baseT

- Manchester coding: Output = Data XOR Clock
- Guarantees a state transition with every bit.



http://en.wikipedia.org/wiki/Manchester_code

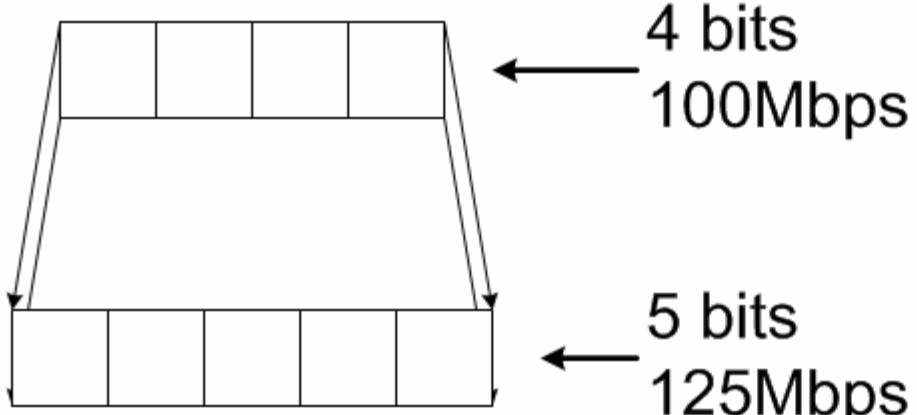
Encoding Techniques: 100baseT

- 100Mbps, baseband, Twisted pair.
- 100Mbps data stream, 4B5B line coding to ensure sufficient clocking, produces 125Mbps symbol rate.
- MLT-3 encoding produces 31.25MHz tri-state output: +1v, 0v, and -1v.
- Full duplex done with two separate simplex pairs: TX and RX

http://en.wikipedia.org/wiki/Fast_Ethernet

Encoding Techniques: 100baseT

- 4B5B line coding ensures sufficient 1s density for 0v DC offset. Includes signaling.

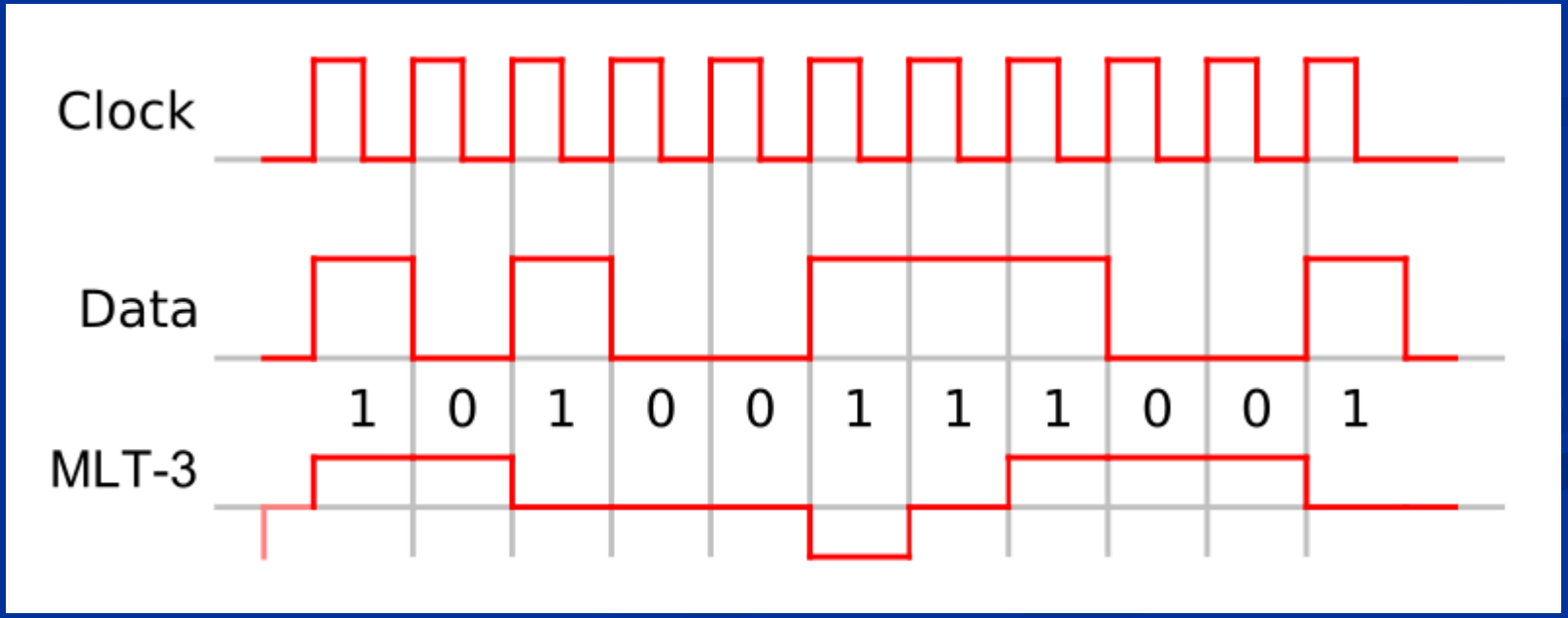


4 bits	5 bits	Description
0000	11110	
0001	01001	
0010	10100	Hex Data
...	...	
1111	11101	
-NONE-	00000	Quiet (signal lost)
-NONE-	11111	Idle
-NONE-	11000	Start #1
-NONE-	10001	Start #2
-NONE-	01101	End
-NONE-	00111	Reset
-NONE-	11001	Set
-NONE-	00100	Halt

http://en.wikipedia.org/wiki/4B5B

Encoding Techniques: 100baseT

- MLT-3 coding. 3 voltage levels, 4 states. Moves to next state on 1, stays on current state on 0.
- Max base frequency is ¼ the data rate.



http://en.wikipedia.org/wiki/MLT-3

Encoding Techniques: 1000baseT

- …uhh… I'll get back to this later in the talk…

http://www.ieee802.org/3/ab/index.html

http://en.wikipedia.org/wiki/Gigabit_Ethernet

http://en.wikipedia.org/wiki/Pulse_amplitude_modulation

http://en.wikipedia.org/wiki/Trellis_modulation

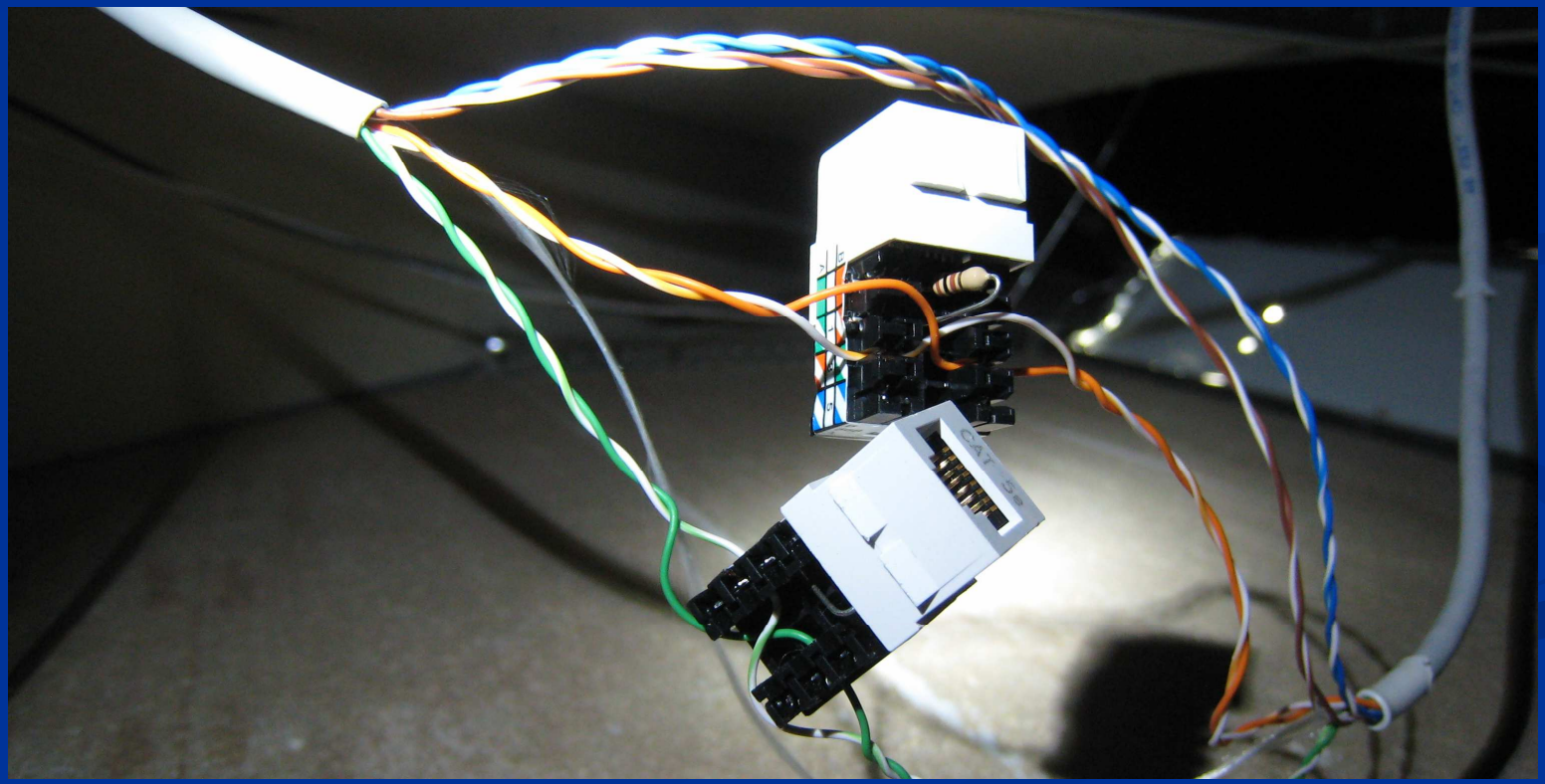
http://en.wikipedia.org/wiki/Linear_feedback_shift_register

Tapping methods

- DC coupling
- Inductive coupling

Tapping Methods: DC coupling

- A direct copper connection between the wires being monitored and the monitoring device.

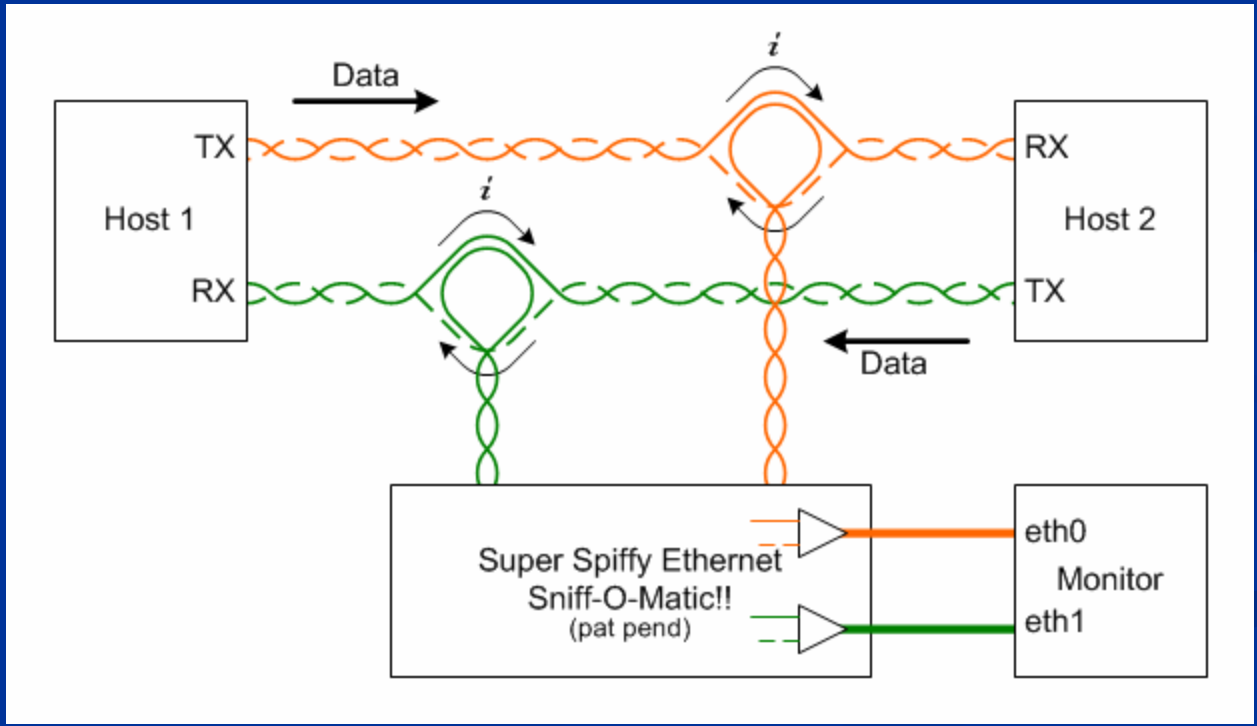


Tapping Methods: DC coupling

- Pros:
  - Easy to construct and connect.
  - Hardware is cheap and passive; no power required.
- Cons:
  - Accidental DC short, could break link.
  - Tap and branch cause reflections, could break link.
  - Accidental reversal of TX/RX, or auto-negotiation of MDI state will transmit, could break link.

Tapping Methods: Inductive Coupling

- Build a small transformer with the pair being monitored, pull a bit of the power.



Tapping Methods: Inductive Coupling

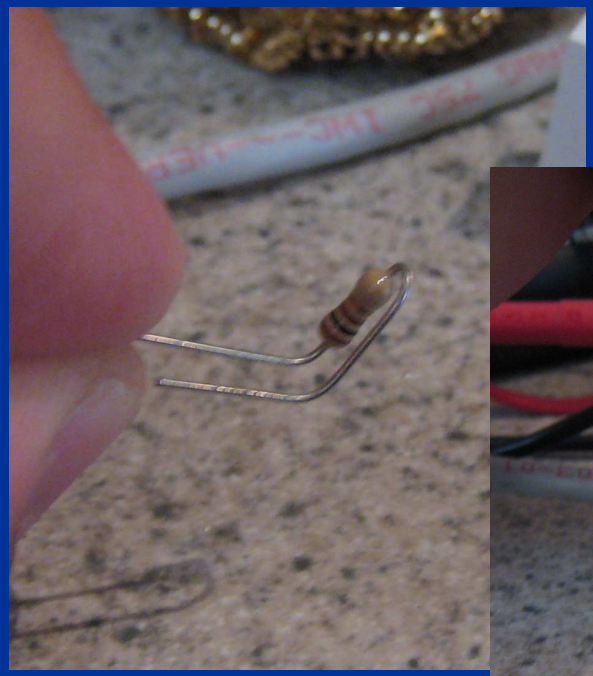
- Pros:
  - Minimal impedance change, hard to detect.
  - Insulation intact, won't accidentally DC short.
  - The receiver amplifier acts as a buffer, prevents accidental transmission.
- Cons:
  - Inductively coupled signal is high impedance; requires amplifier.
  - Transformers are finicky, hard to get right.

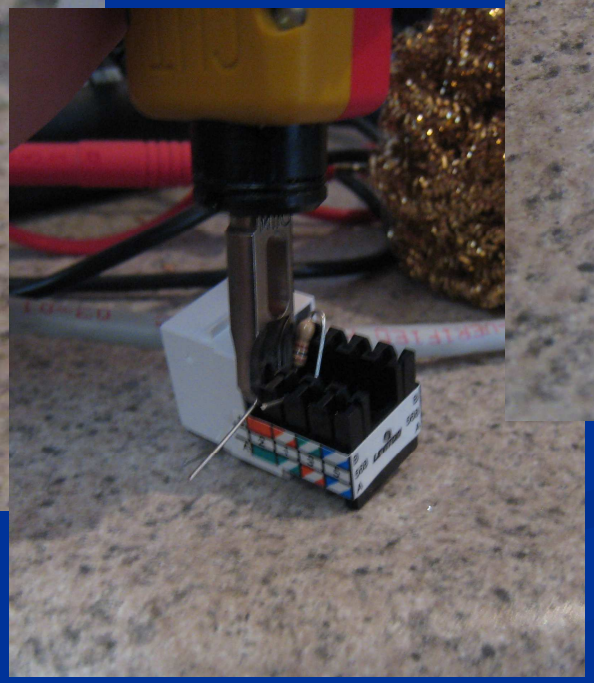
Hardware Assembly

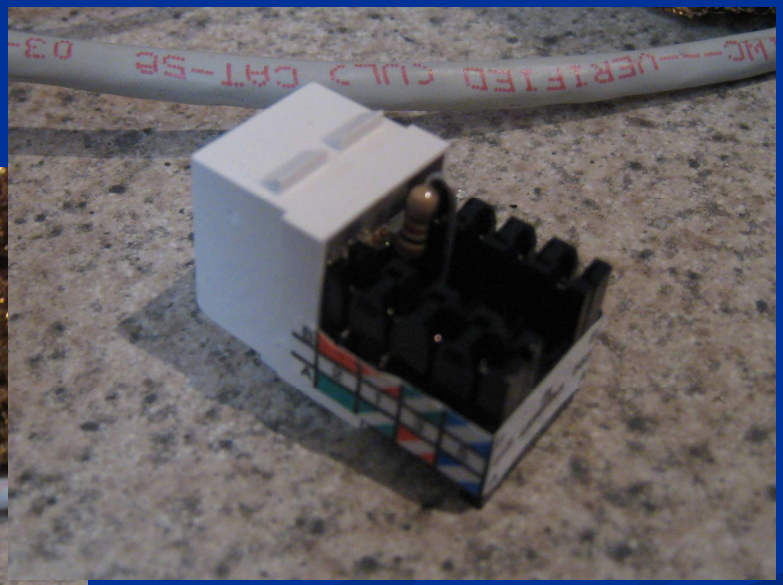
- Because of its simplicity, we'll be using a DC coupled system for today's demonstration.

Hardware Assembly: DC Coupled

- Punch a 100 ohm resistor across Orange pair of two 568B RJ-45 wall jacks.

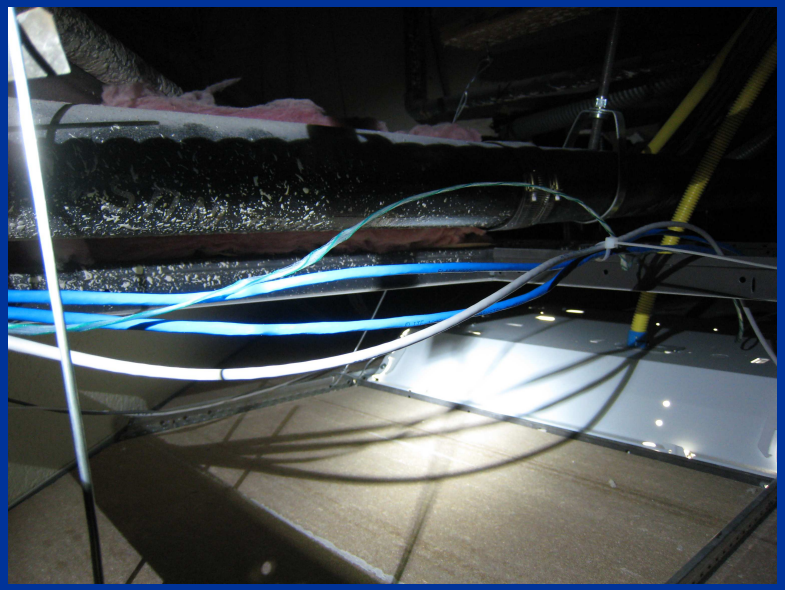


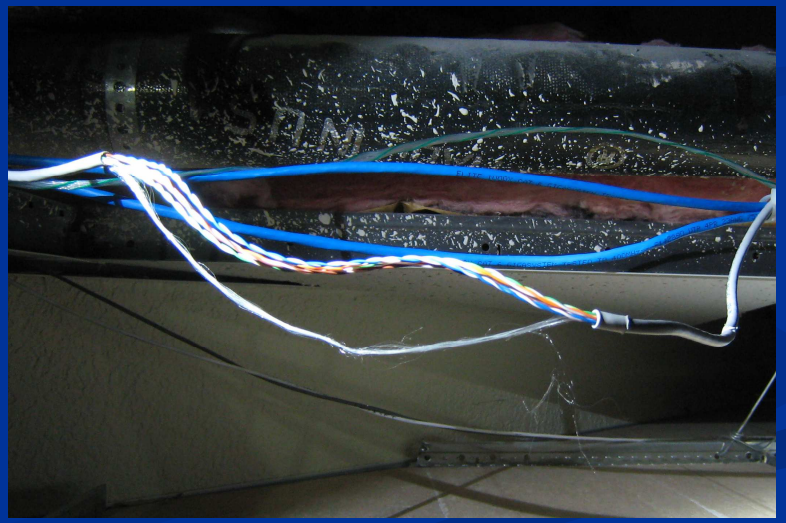




Hardware Assembly: DC Coupled

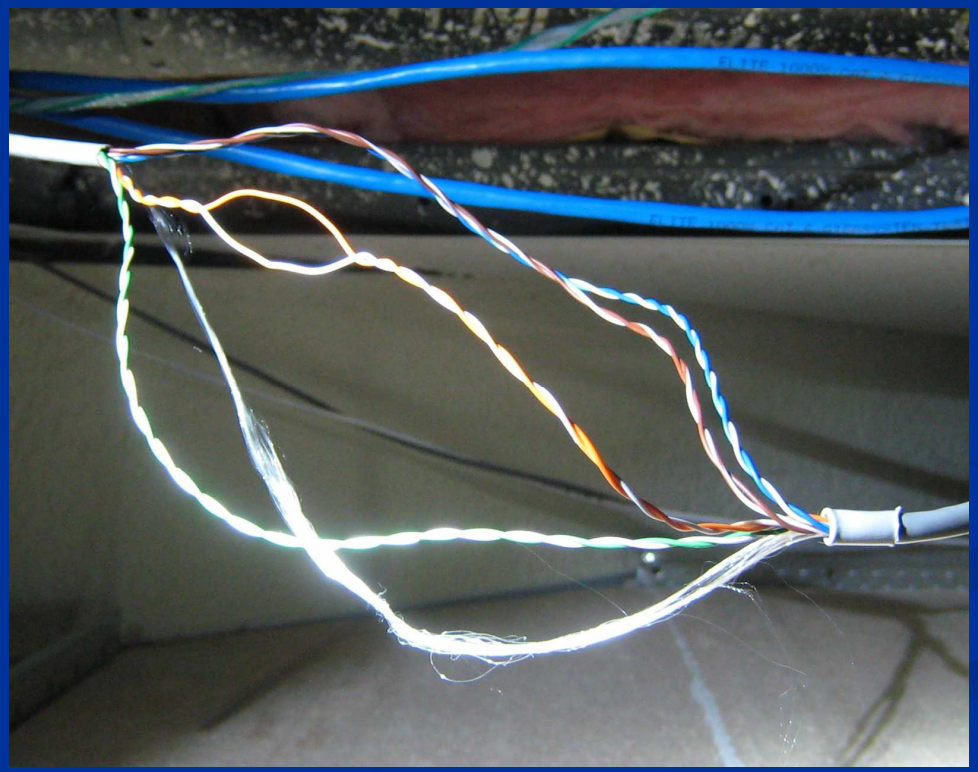
- Carefully cut about 12 inches of the **outer jacket** off the Ethernet cable to be monitored.





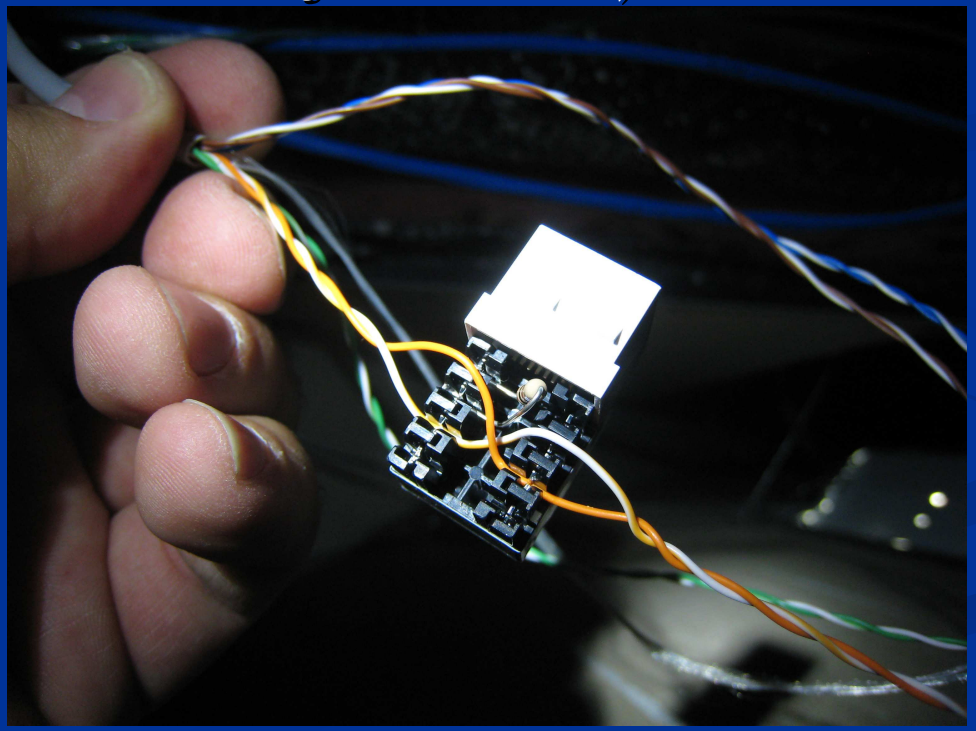
Hardware Assembly: DC Coupled

- Untwist the Orange pair a bit to give yourself about an inch of straight wires.



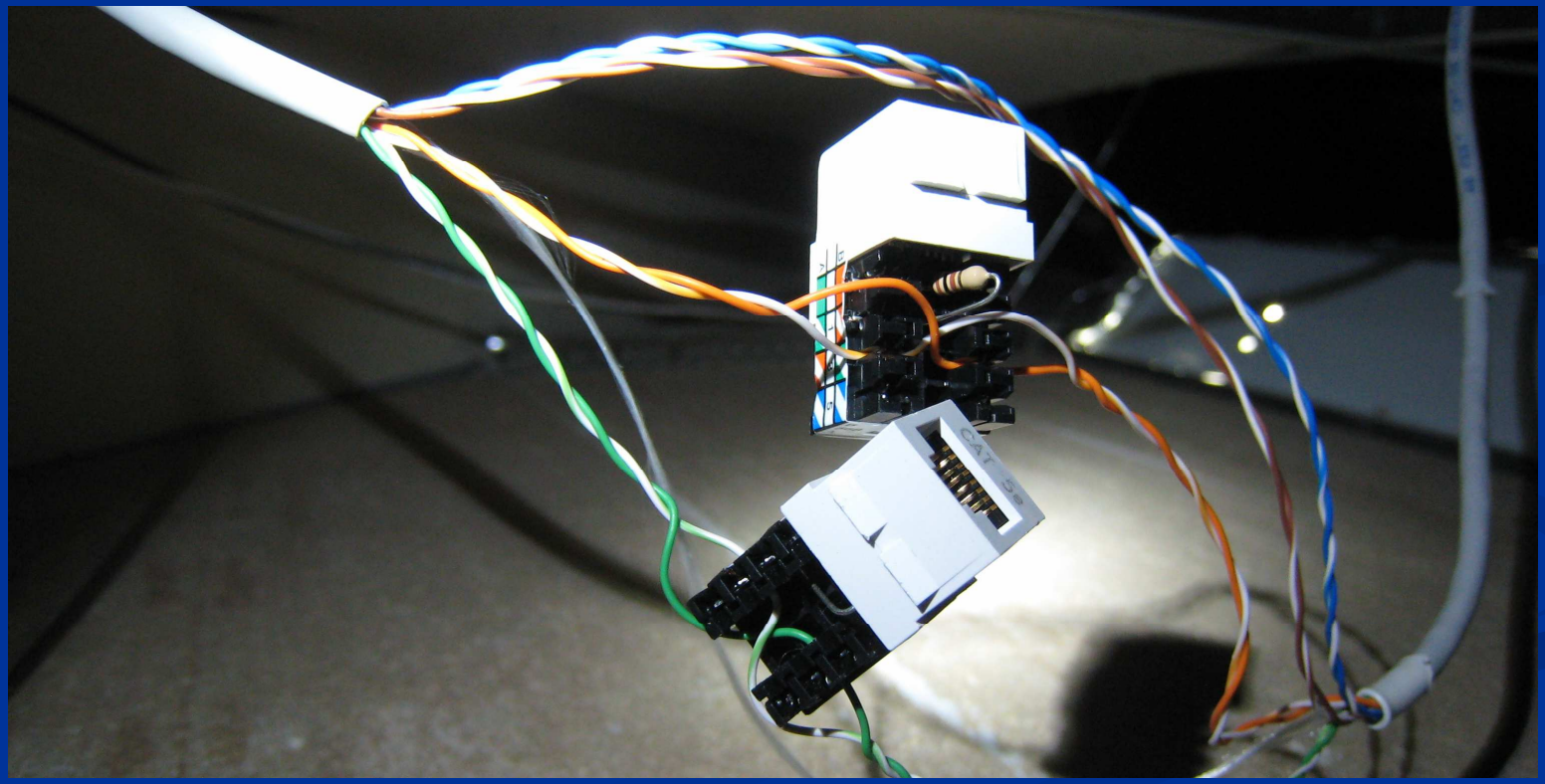
Hardware Assembly: DC Coupled

- Using the non-cutting side of a punch tool, punch the Orange wire into the Green pair of one of the 568B RJ-45 wall jacks.



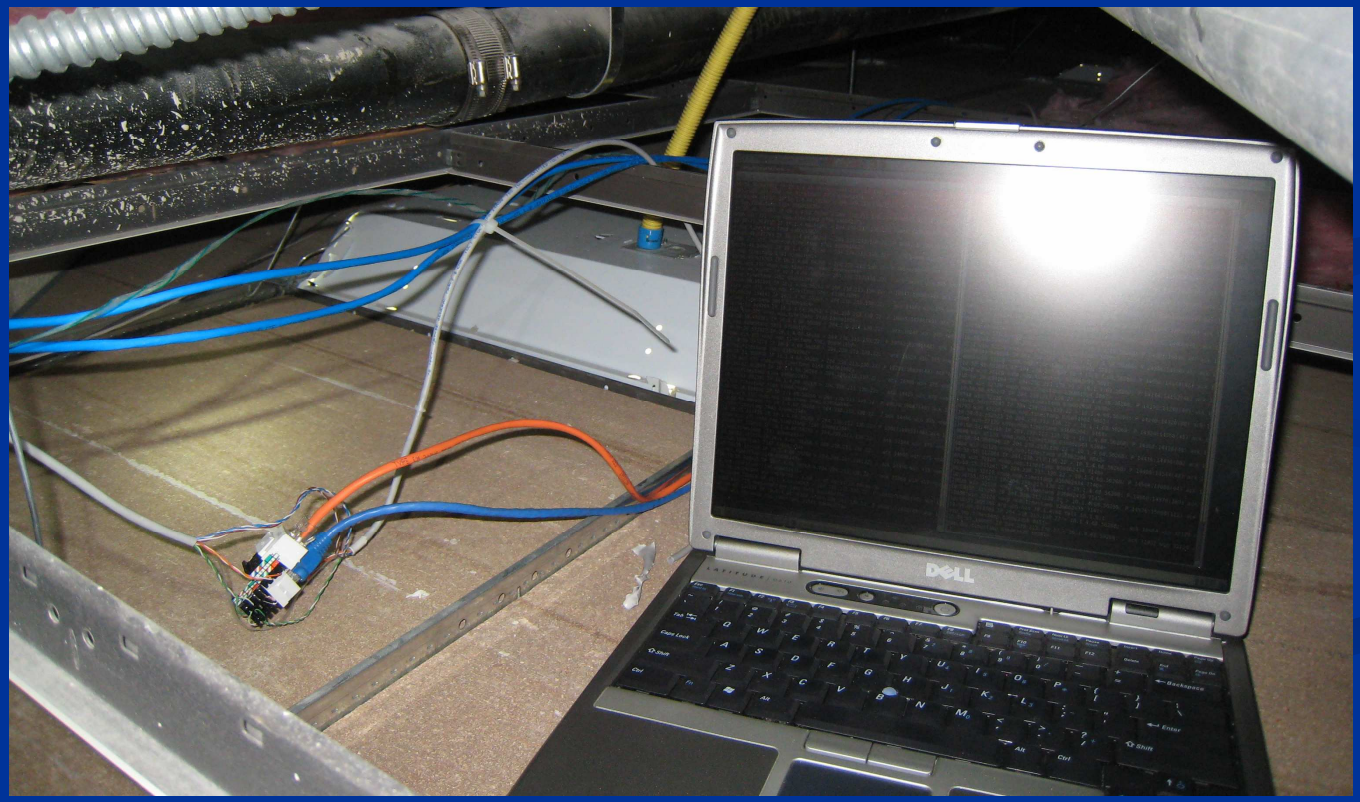
Hardware Assembly: DC Coupled

- Repeat last two steps with the Green pair.



Hardware Assembly: DC Coupled

- Connect two standard Ethernet cables from the RJ-45 wall jacks to your monitoring system.



Hardware Assembly: DC Coupled

- eth0 sees traffic one way, eth1 sees traffic the other way.
- Use tcpdump, WireShark or similar to capture and display the data.
- Capture with precise timestamps, add a bit of scripting, and you can have a single combined data flow.

Hardware Assembly: Inductively Coupled

- …come see me next year…

Thinking Black Hat

- Shared phone rooms and wiring closets
- Drop ceilings
- "Protected" conduits (got a pipe cutter from Home Depot?)
- Man holes, J-Boxes, etc.

Thinking White Hat

- Physical Security. (See other presentations here at DefCon.)
- Encryption. IPSec, TLS, etc.
- Heck, encrypt everything anyway; CPU is cheap.
- Periodic TDR measurements.
- Gigabit Ethernet (stick around…)

The Holy Grail: Gigabit Ethernet
…and why it's *REALLY* hard to sniff…

- 10baseT and 100baseT are easy to monitor:
  - Simple line coding techniques.
  - Relatively low signal rates (20MHz and 31.25MHz)
  - Individual TX and RX pairs (each pair is simplex.)
  - Auto-negotiation can be disabled and line settings configured manually.

The Holy Grail: Gigabit Ethernet
…and why it's *REALLY* hard to sniff…

- Gigabit Ethernet is none of those things:
  - Auto-negotiation is a requirement of the spec.
  - All four pairs are used *simultaneously* for TX and RX. Two unknowns, only one equation.
  - 1000baseT is far more susceptible to reflections and changes in impedance.

The Holy Grail: Gigabit Ethernet

…and why it's *REALLY* hard to sniff…

- Nothing public exists for this yet, but its not impossible.
- A more motivated and better funded organization has probably already figured this out.

Conclusion

- We've shown that:
  - A careful attacker with no budget can easily tap into unprotected 10baseT and 100baseT.
  - A decently funded attacker can probably do the same thing with 1000baseT.
- If you can't physically secure your network links, encrypt your traffic (IPSec, TLS, etc.)

Thanks!

- Thanks for listening!
  - Mark Smith, aka Smitty
  - mark {at} halibut {dot} com
  - @SmittyHalibut everywhere else

http://www.halibut.com/~mark/EtherSniff-v1.0.pdf