Twisted Taps

TWISTED PAIR ETHERNET AND TAPPING THE WIRE

The Open Systems Interconnection (OSI) Model - Refresher

7
- **Application Layer**
- Provides Data to the Application

6
- **Presentation Layer**
- Represents the data and provides Encryption

5
- **Session**
- Establish and maintain host communication

4
- **Transport**
- Breaks DATA into SEGMENTS, handles End-to-end connections and Error checking.

3
- **Network**
- Breaks SEGMENTS into PACKETS, handles Network Addressing, Routing, Pathing & Logical Addressing (IP Addresses)

2
- **Datalink**
- Breaks PACKETS into FRAMES, handles bitrate flow control and Physical Addressing (MAC Addresses)

1
- **Physical**
- Breaks FRAMES into raw BINARY Bits. Provides the electrical signalling of media.

The TCP/IP Model - Refresher

5
- **Application Layer**
- Protocols: Telnet, SSH, FTP, HTTP, POP, IMAP, LDAP, NTP, SMTP, DHCP

4
- **Transport**
- Protocols: TCP, UDP.

3
- **Network**
- Protocols: ICMP, IGMP, IPsec, IPv4, IPv6, IPX, RIP

2
- **Data Link**
- Protocols: ARP, RARP, ATM, CDP, FDDI, HDLC, MPLS, PPP, STP, 802.5 (Token Ring)

1
- **Physical Link**
- Protocols: 802.3 (Ethernet), DSL, ISDN, 802.11 (WiFi), 802.15 (Bluetooth), 802.16 (WiMAX)

Physical Cabling – Part 1

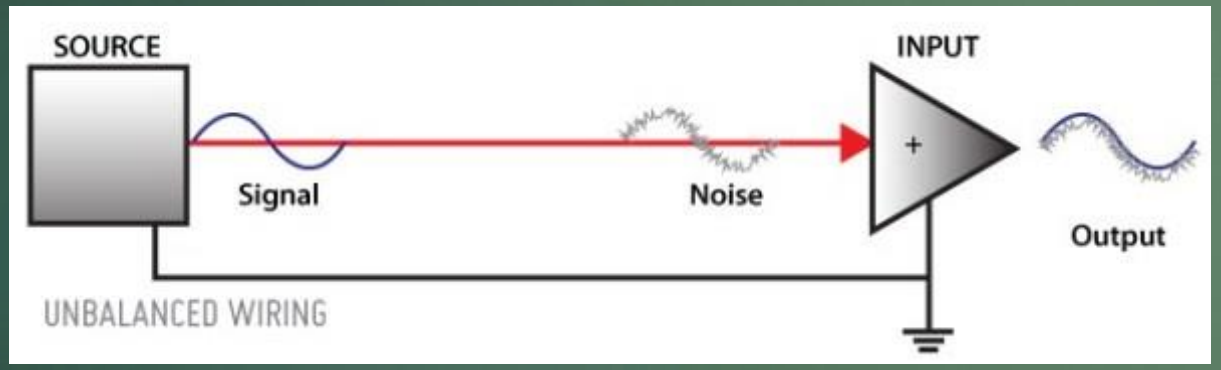
- Coaxial (Baseband)
  - One conductor, surrounded by a second conductive braid
  - 10BASE5 – 10Mbit over 500m
  - 10BASE2 – 10Mbit over 200m (185m)
- Power Line Transmission
  - Carried by Extra Low-Volt/Low-Volt Alternating Current
  - Low-speed Narrow Band – 200 to 800 bps
  - Medium-speed Narrow Band – 576 kbps
- Optical Fiber
  - One or more light transmissive waveguide cores
  - Multi-Mode: 100Mbps @ 2km, 1Gbps @ 1km, 10Gbps @ 550m
  - Single-Mode: 100Mbps @ 40km, 1Gbps @100km, 10Gbps @ 40km

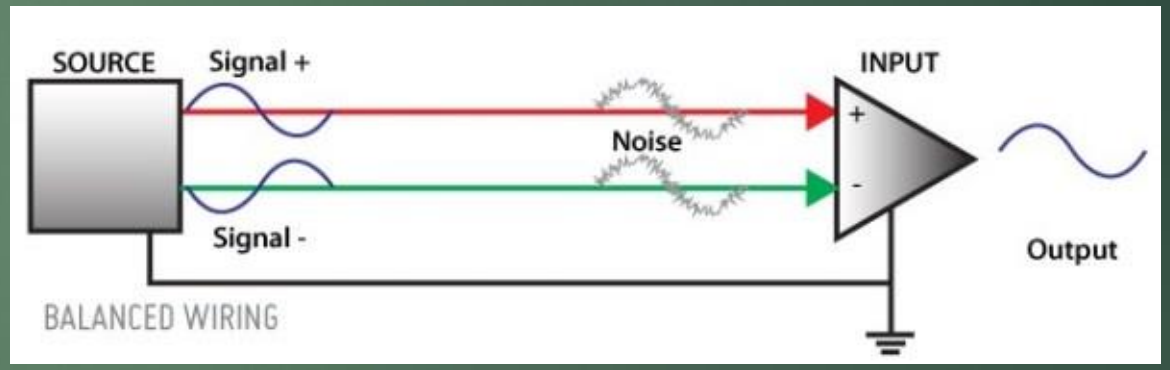
Physical Cabling – Part 2

- Twisted Pair Cable Standards (Maximum Speed @ Bandwidth)
  - CAT1 (UTP) 1Mbps @100 KHz (POTS)
  - CAT2 (UTP) 4Mbps @1000 KHz (Token Ring)
  - CAT3 (UTP) 10Mbps @16 MHz (Token Ring & 10BASE-T)
  - CAT4 (UTP) 16Mbps @20 MHz (Token Ring)
  - CAT5 (UTP) 100Mbps @100 MHz (Token Ring & Fast-Ethernet)
  - CAT5e (UTP&STP) 1,000Mbps @100 MHz
  - CAT6 (STP) 1,000Mbps @ 250 MHz
  - CAT6a (STP) 10,000Mbps @ 500 MHz
  - CAT7 (SSTP) 10,000Mbps @ 600 MHz
  - CAT7a (SSTP) 40,000Mbps @ 1000 MHz

Unbalanced vs Balanced

Why Twisted Pair?





Cabling Colour Standards

- Australian Standard AS/ACIF S009:2006
- Minor colour names (left)
  - Blue
  - Orange
  - Green
  - Brown
  - Slate

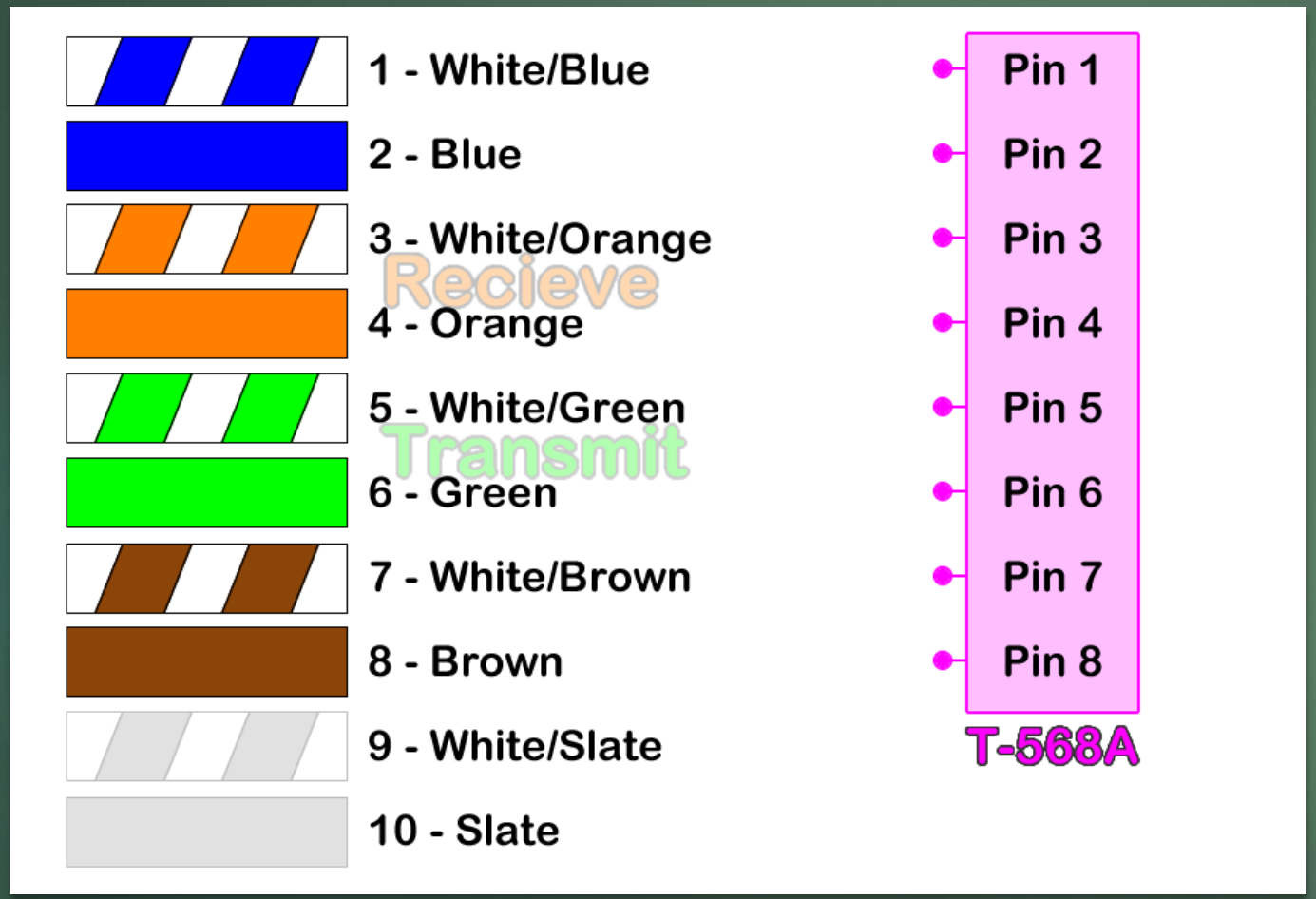
Ethernet Conductors

- Major colour groups
  - White (shown left)
  - Red
  - Black
  - Yellow
  - Violet
- Ethernet only uses the first four pairs (8 conductors)

Fast Ethernet Connectivity

- Only uses Two Pairs
- Receive – Pair 2
  - ORANGE (**WHITE**)
  - ORANGE (mate)
- Transmit - Pair 3
  - GREEN (**WHITE**)
  - GREEN (mate)

The Modular Jack Connector



- RJ45
  - Registered Jack 45
- 8P8C
  - 8 Position (size)
  - 8 Contacts (in positions)

The Modular Jack Connector

- Pair 1 – Commonly used for Phone

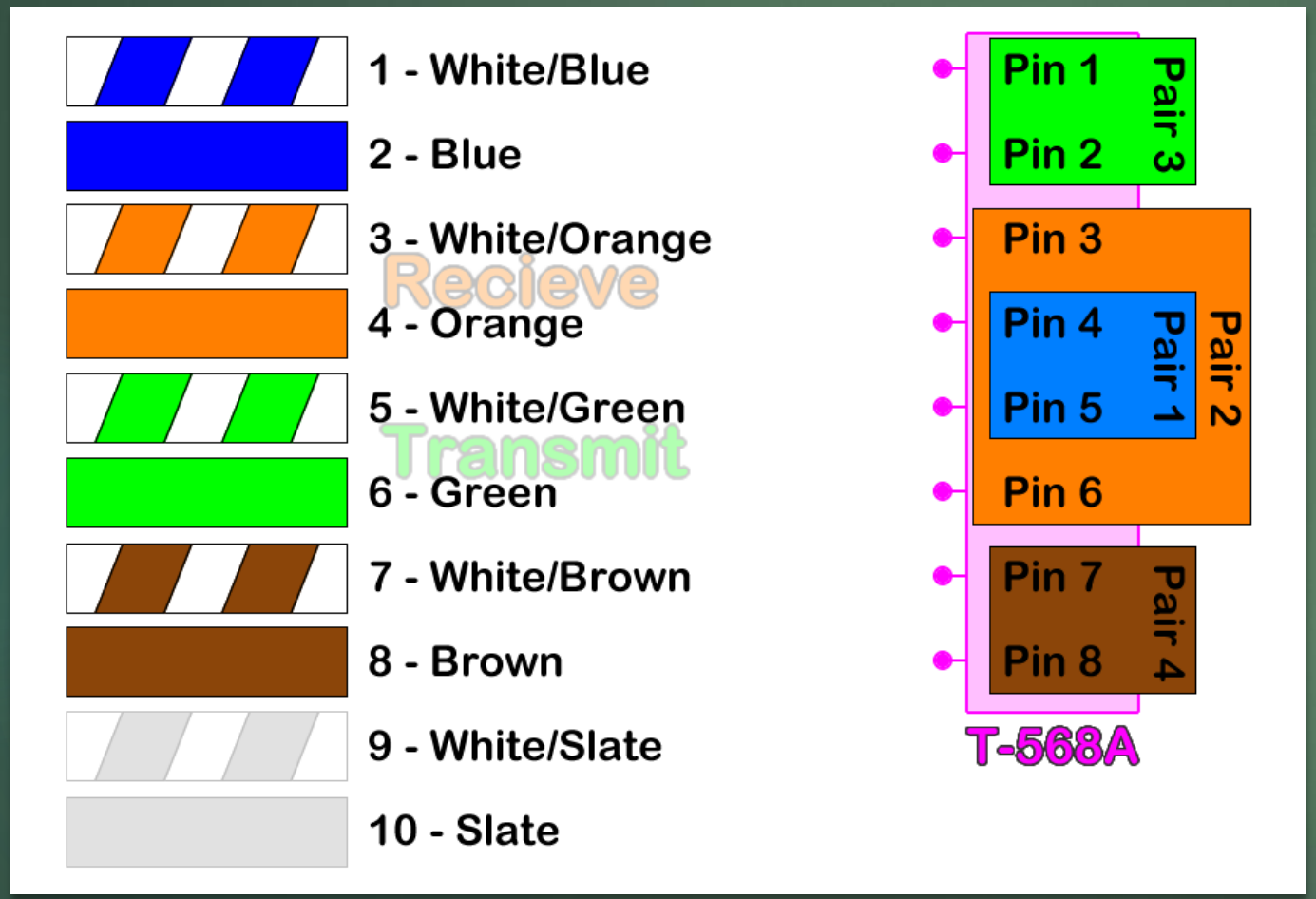
The Modular Jack Connector

- Pair 1 – Commonly used for Phone
- Pair 2 – Receive Pair

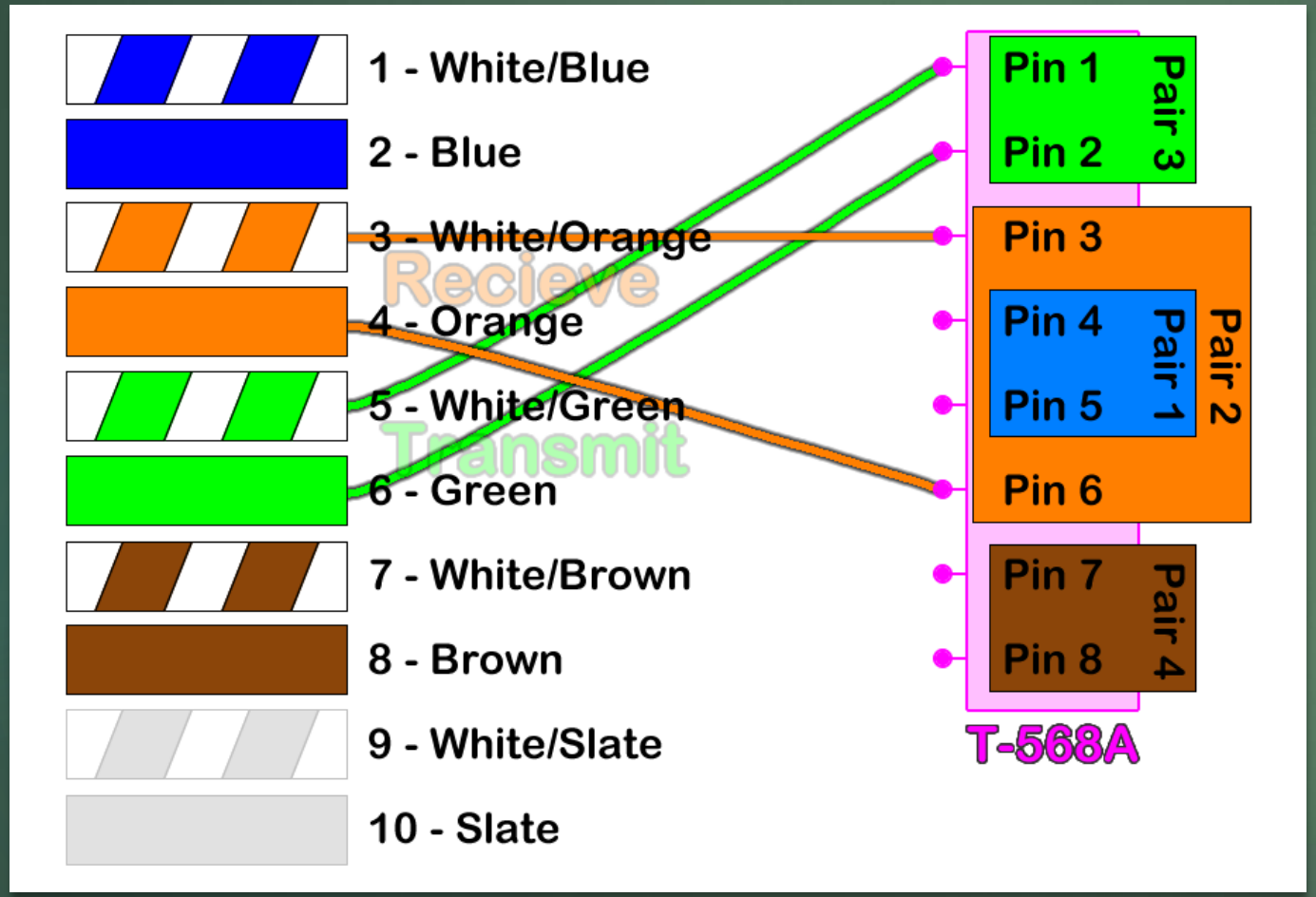
The Modular Jack Connector

- Pair 1 – Commonly used for Phone
- Pair 2 – Receive Pair
- Pair 3 – Transmit Pair

The Modular Jack Connector

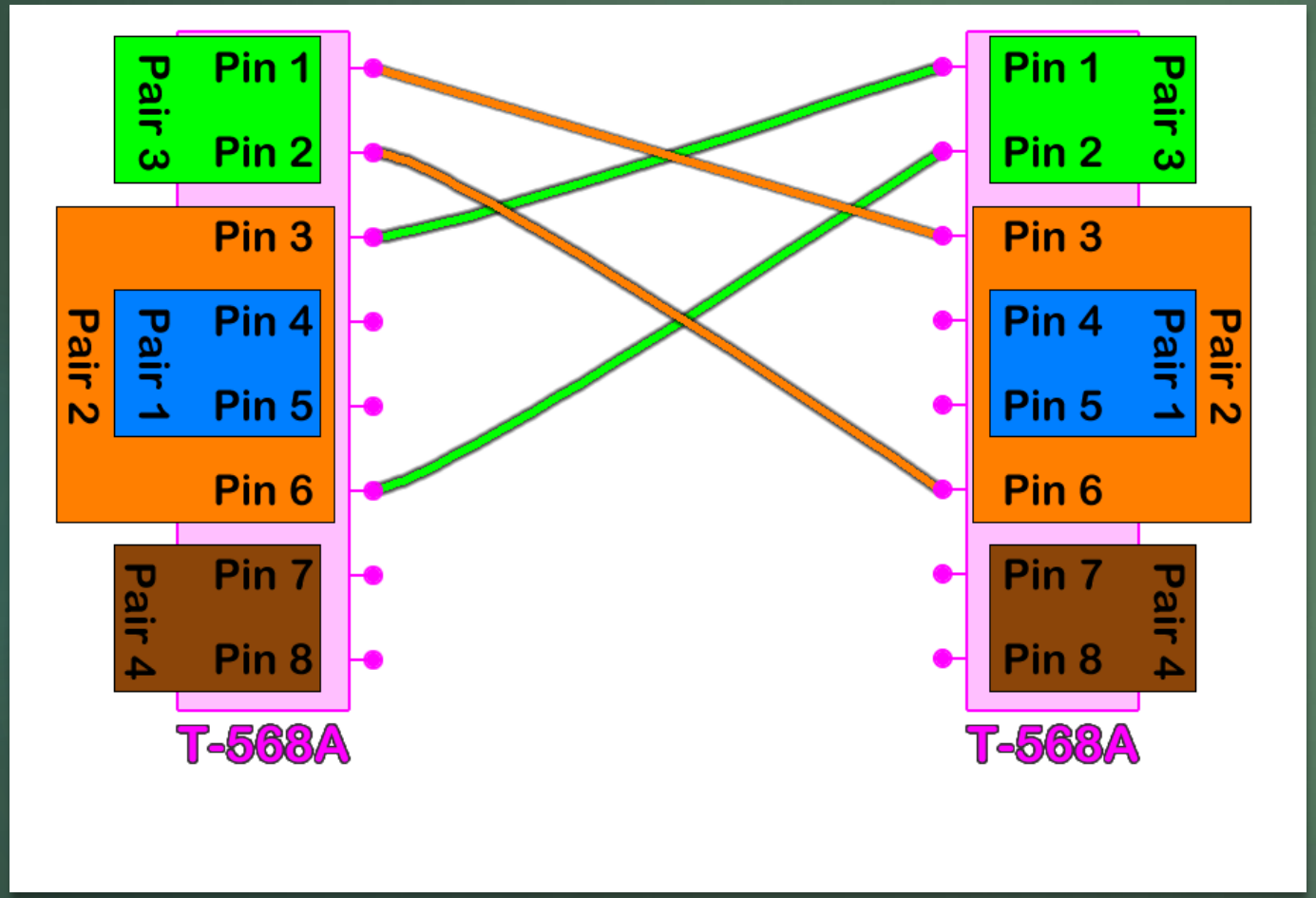


- Pair 1 – Commonly used for Phone
- Pair 2 – Receive Pair
- Pair 3 – Transmit Pair
- Pair 4 - Unused



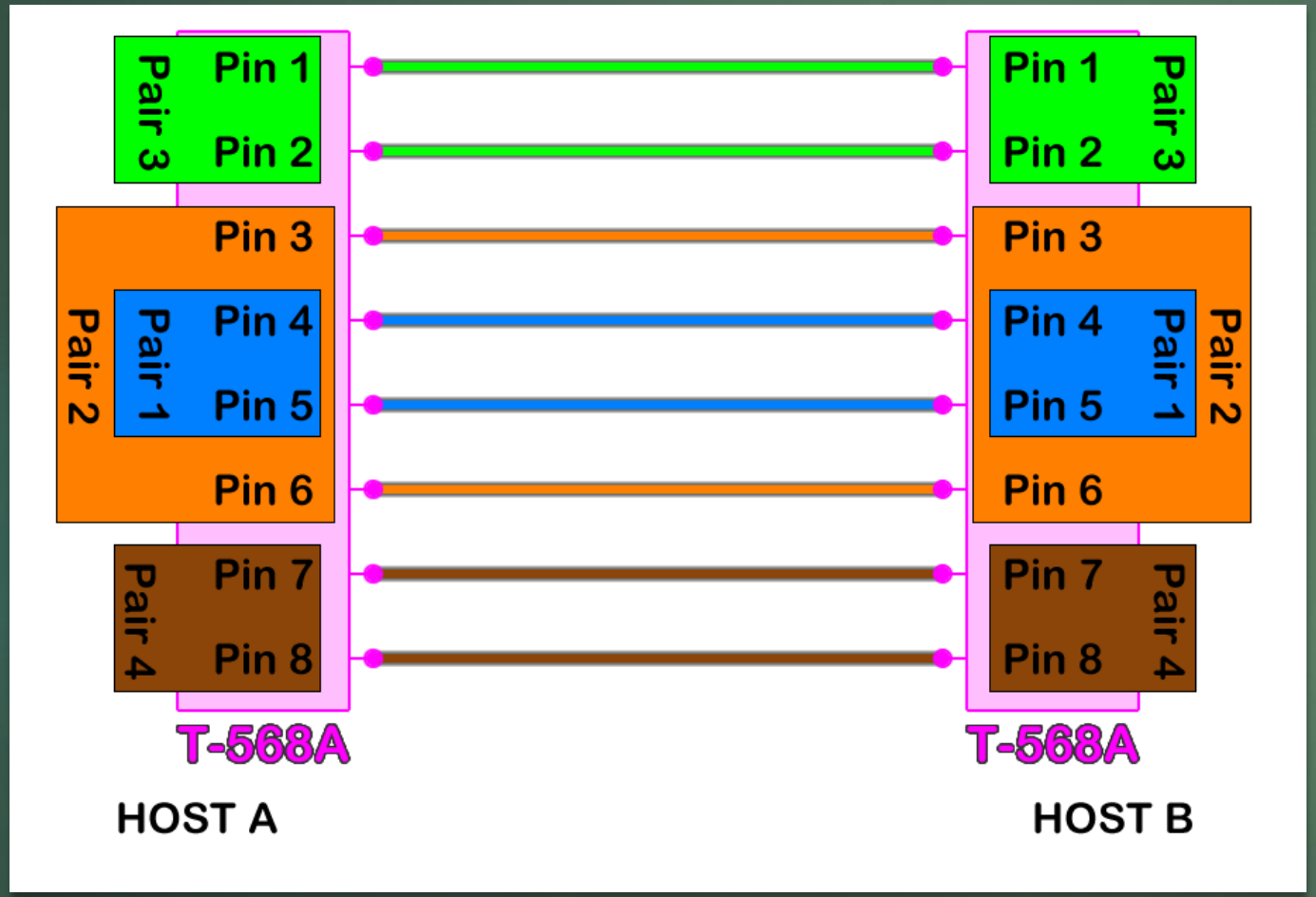
The Modular Jack Fast Ethernet Conductor Pinout

- 10/100 Mbps
- Can't carry Gigabit
- Only uses two pairs
- Unused pairs can/could be used to share more services



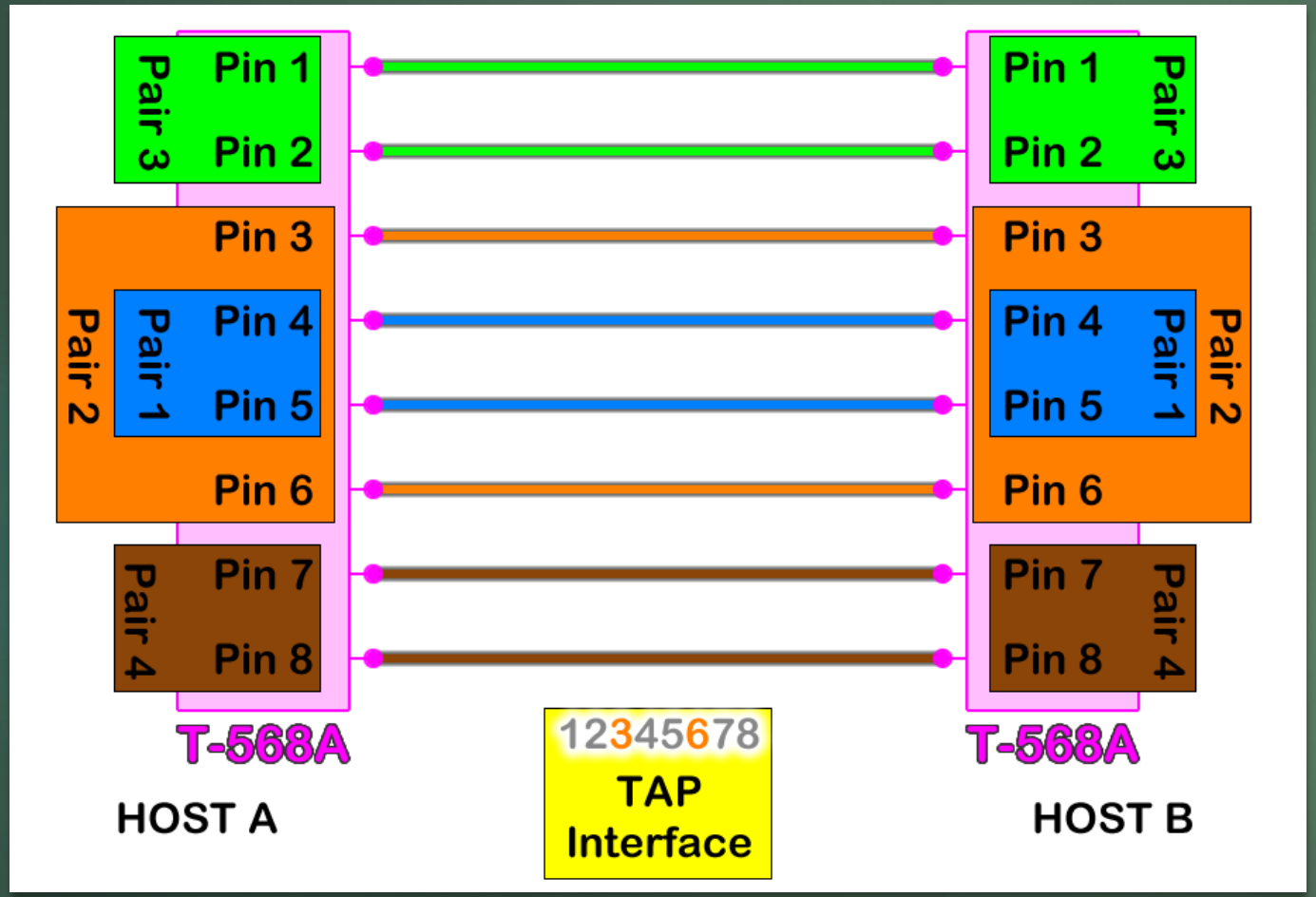
Fast Ethernet Crossover Cable

- Transmit to Receive
- Receive to Transmit
- Host to Host Ethernet
- Non Auto-Crossover Ports



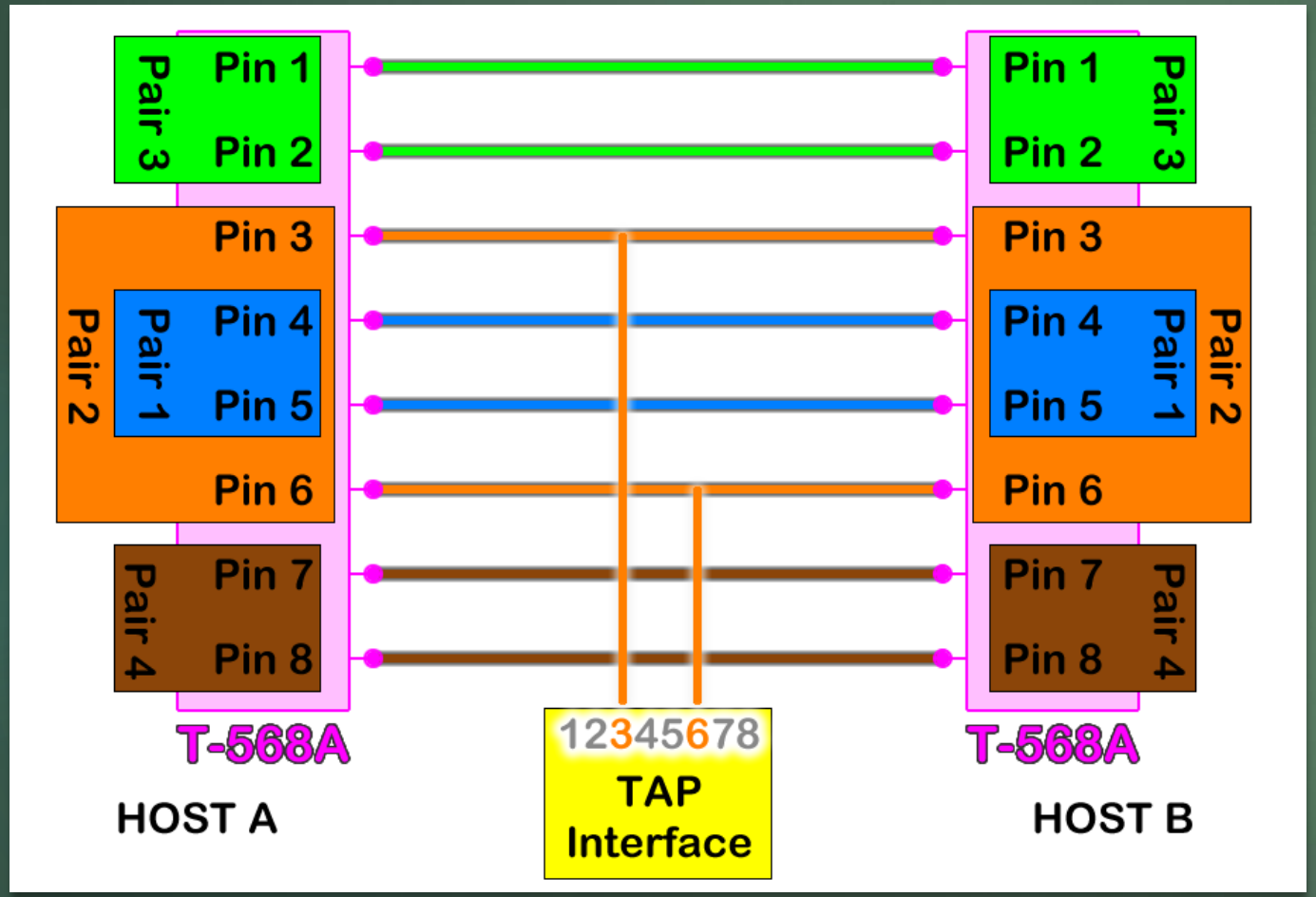
Straight Through Networking Cable

- Straight though connection between Network Nodes
- Host to Switching Equipment
- Structured Cabling
- Fly leads
- Can carry higher bitrate network speeds



Building a Fast Ethernet Tap

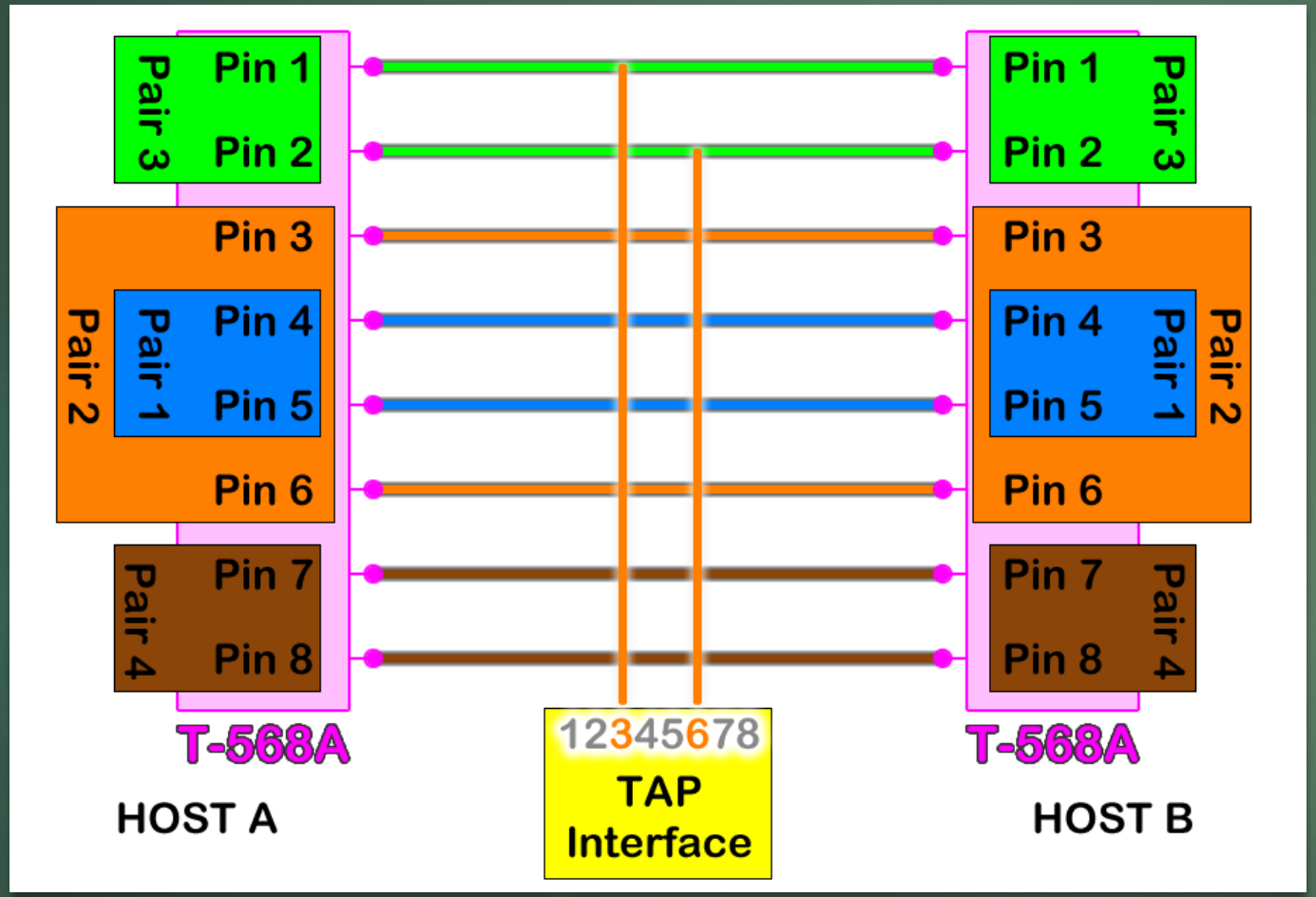
- Tap Interface only needs to Listen to communication
- Pair two (Receive) uses:
  - Pin 3 = Receive +
  - Pin 6 = Receive –
- Tap Interface is a Sensor



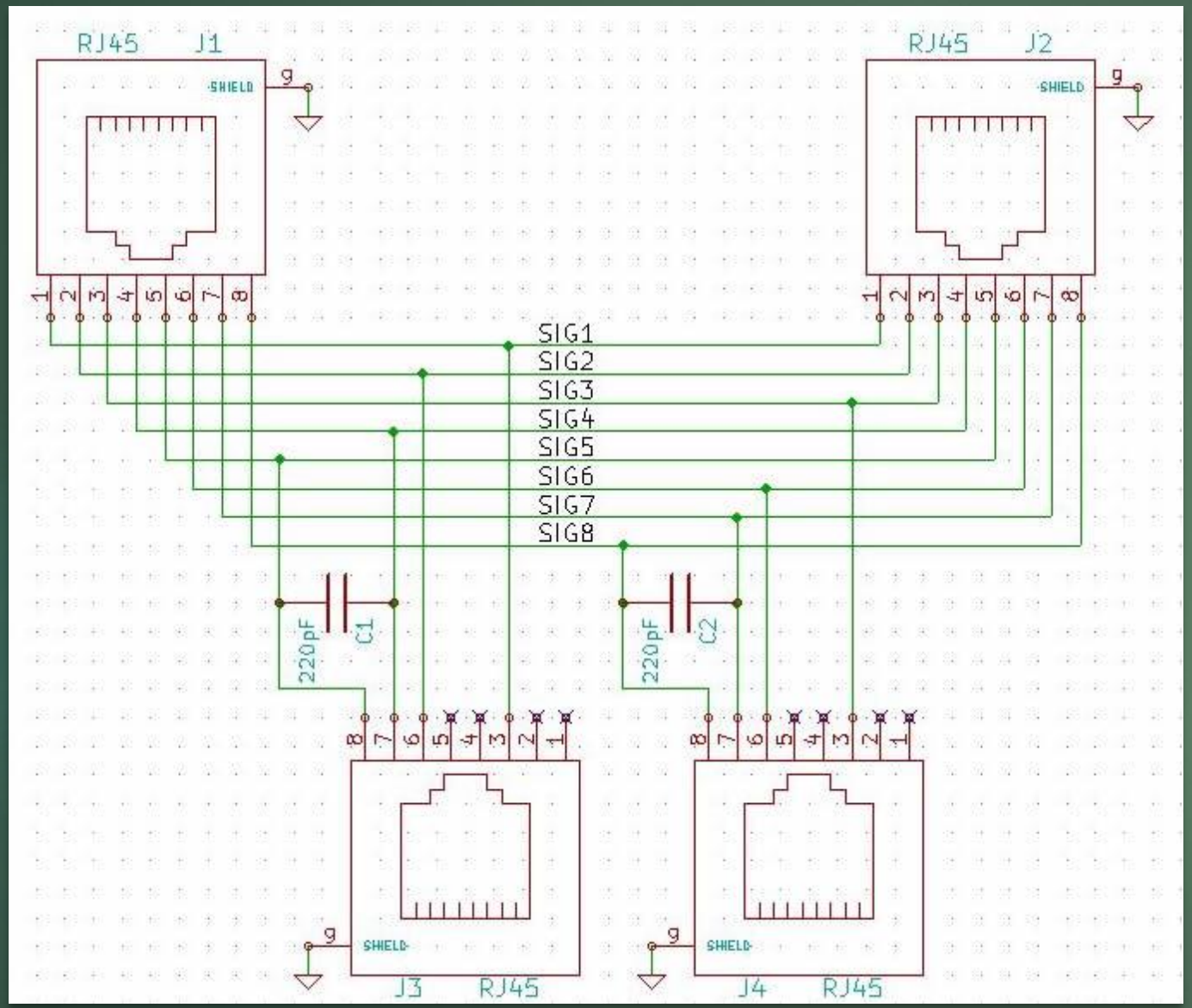
Building a Fast Ethernet Tap

- Connecting to Pair 2
- TAP Interface will see RECEIVED packets

Building a Fast Ethernet Tap



- Connecting to Pair 3
- TAP Interface will see TRANSMITTED Packets

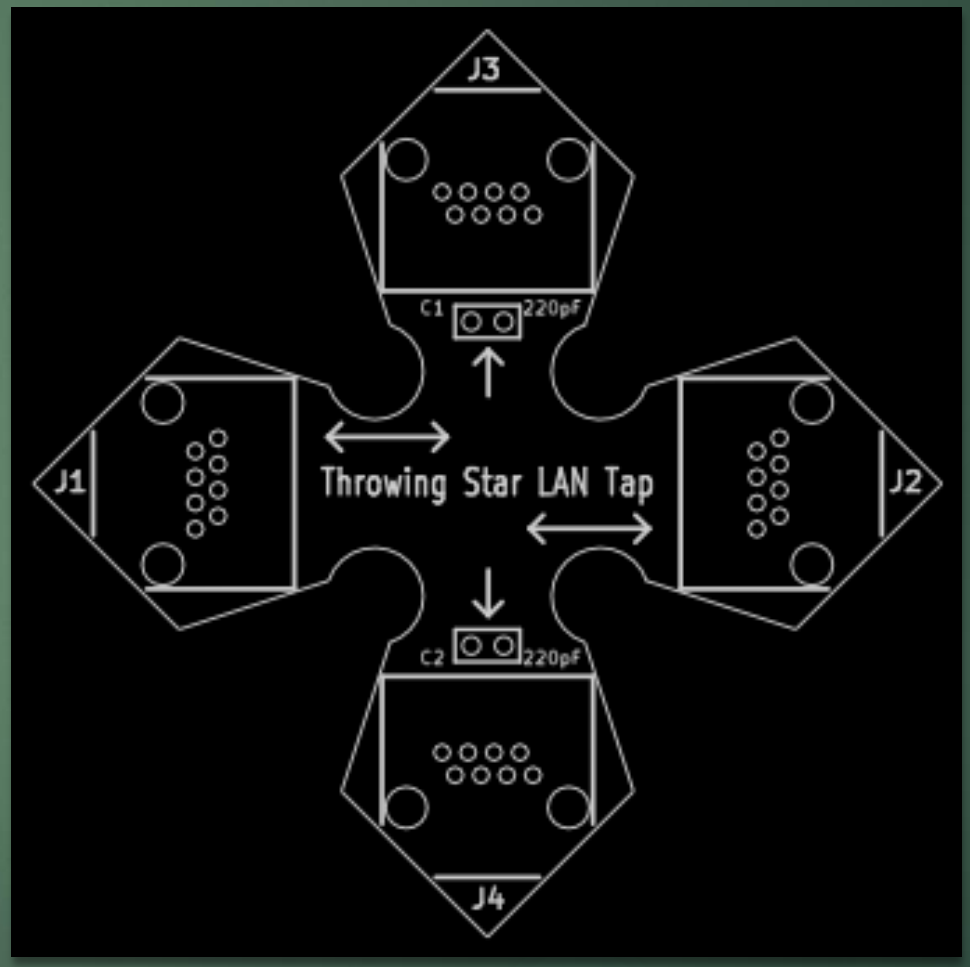


Building a Fast Ethernet Tap

- Basic Schematic
- J1 is the Target System
- J2 is the upstream network
- J3 listens to Transmit Signals
- J4 listens to Receive Signals
- 220pF Capacitors filter out high-frequency signals

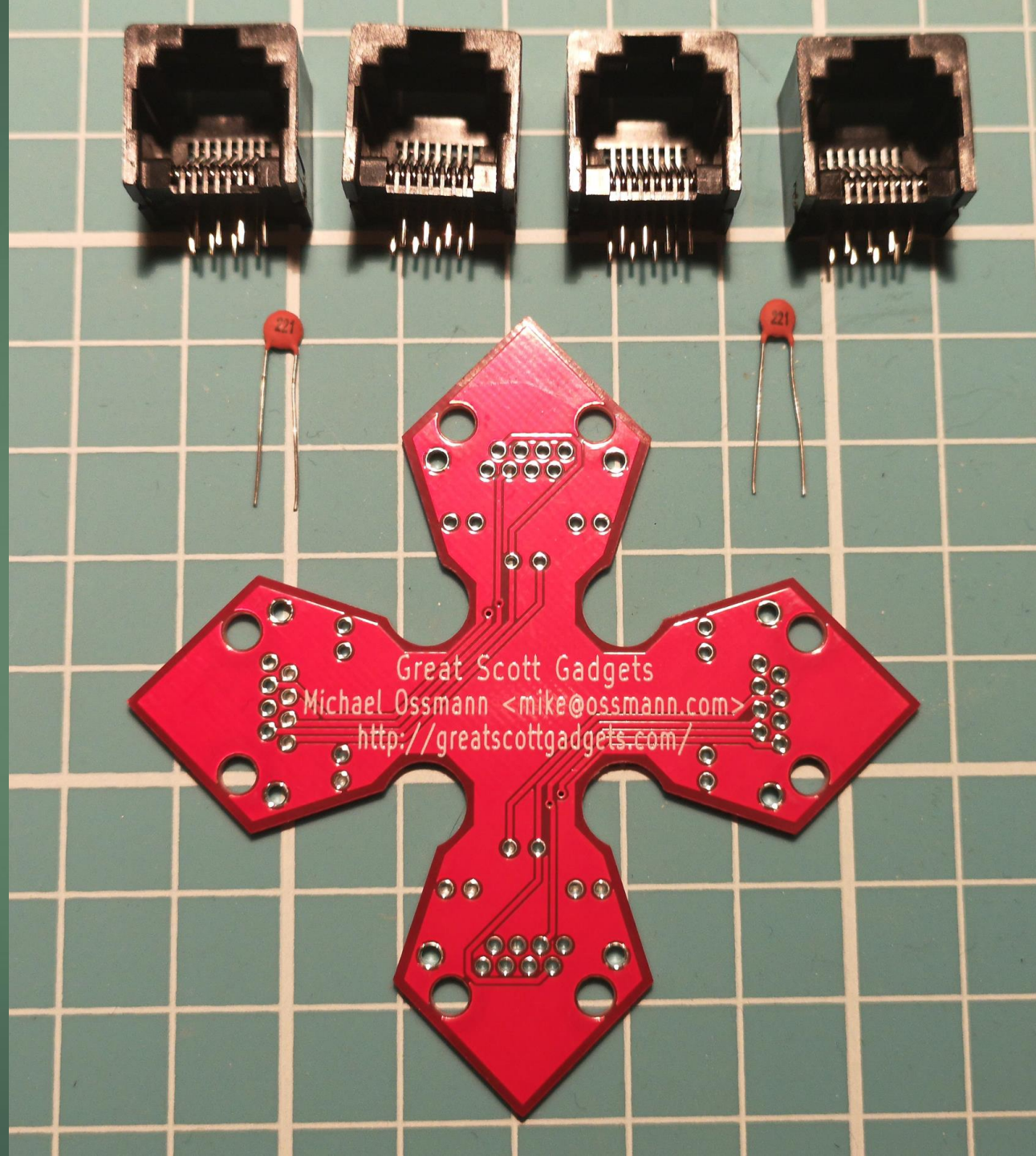
Throwing Star LAN Tap

- Passive Ethernet Tap
- Fast Ethernet ONLY (10/100):
  - 10BASE-T
  - 100BASE-T1
  - 100BASE-TX
- Great Scott Gadgets
- Michael Ossmann
- https://greatscottgadgets.com/throwingstar/
- https://github.com/greatscottgadgets/throwing-star-lan-tap



Throwing Star LAN Tap

- CrikeyCon Badge Edition
- Parts required:
  - Single-sided circuit board
  - 4x 8P8C PCB-mount Sockets
  - 2x Ceramic 220pF Capacitors
- Tools:
  - Soldering Iron
  - Side cutters
  - You, with 10 minutes free



Throwing Star Alternative Options

- Passive Taps
- Custom Flyleads
- Active Taps
- Switch Port Replication
- Ethernet Hubs
- Clipping the wire itself
- Induction pickups

Throwing Star Live Demo

- Connect throwing star tap inline
- Sniff packets with Wireshark
- Listen to Transmit
- Listen to Receive

Twisted Taps – Questions

- Twitter: @Joflixen
- Email: james@mouat.net.au
- Website: https://mouat.net.au
- https://github.com/Joflixen
- https://www.linkedin.com/in/jamesmouat/

- Great Scott Gadgets – Throwing Star Tap
  - https://greatscottgadgets.com/throwingstar/
  - https://github.com/greatscottgadgets/throwing-star-lan-tap