



Communications Debugging Techniques and Tools



Making Electric Power Safer, More Reliable, and More Economical®

Why Learn Debugging Techniques?

- Reduce installation times
- Diagnose issues faster
- Improve communications infrastructure
- Increase reliability

Debugging Overview

- Communications
- How does it work?
- Common issues
- Tools
- Bruce's Bag O' Tricks
- Real world examples

What Is Communication?

The exchange of thoughts, messages, or information, as by speech, signals, writing, or behavior

Electronic Communications

Series of bytes, or bits, transmitted and received along a media

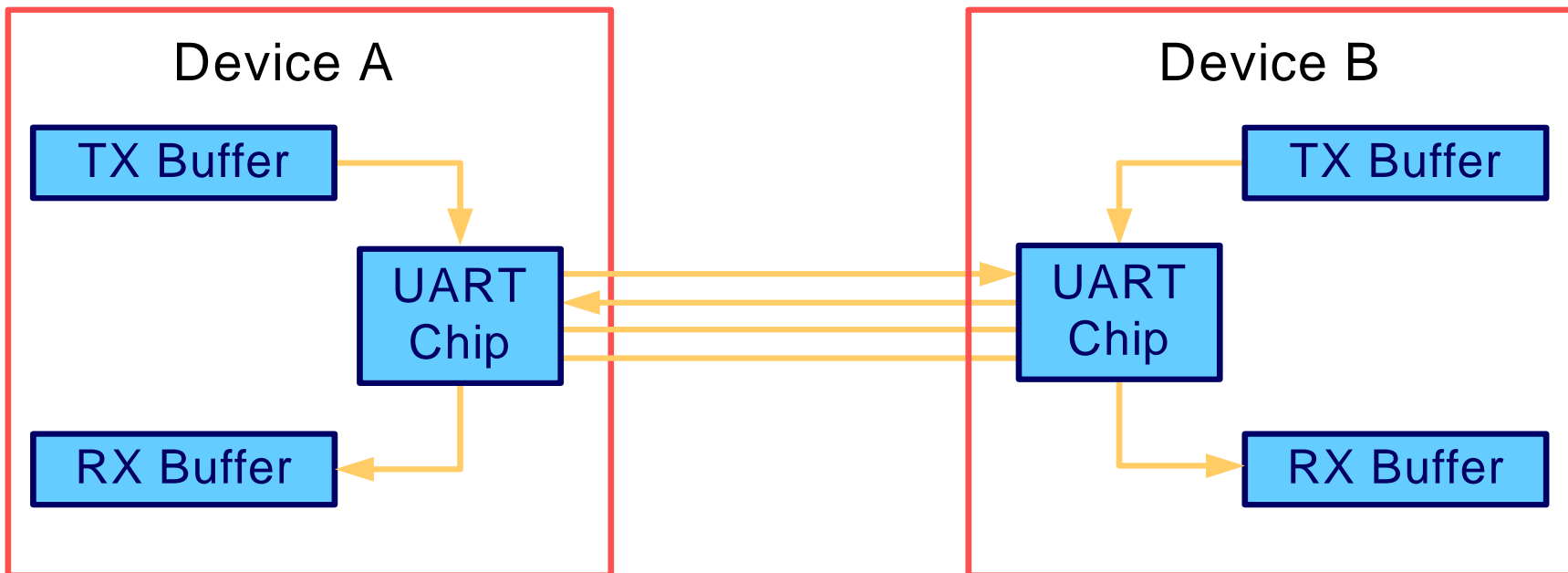
- Serial
- Ethernet network
- Phone lines
- Radio, cell networks
- Fiber optics

Technique

- Define problem
 - ◆ Isolate equipment, events
 - ◆ Toggle problem
 - ◆ Understand controlling factors
- Determine solution
- Test and verify solution
- Take notes

Serial Communications

- Byte at a time
- Control lines RTS / DTR / CTS



Common Serial Problems

- Port settings
 - ◆ Speed
 - ◆ Parity
- Cabling
- Buffer overruns
- PC UARTs

Serial Devices

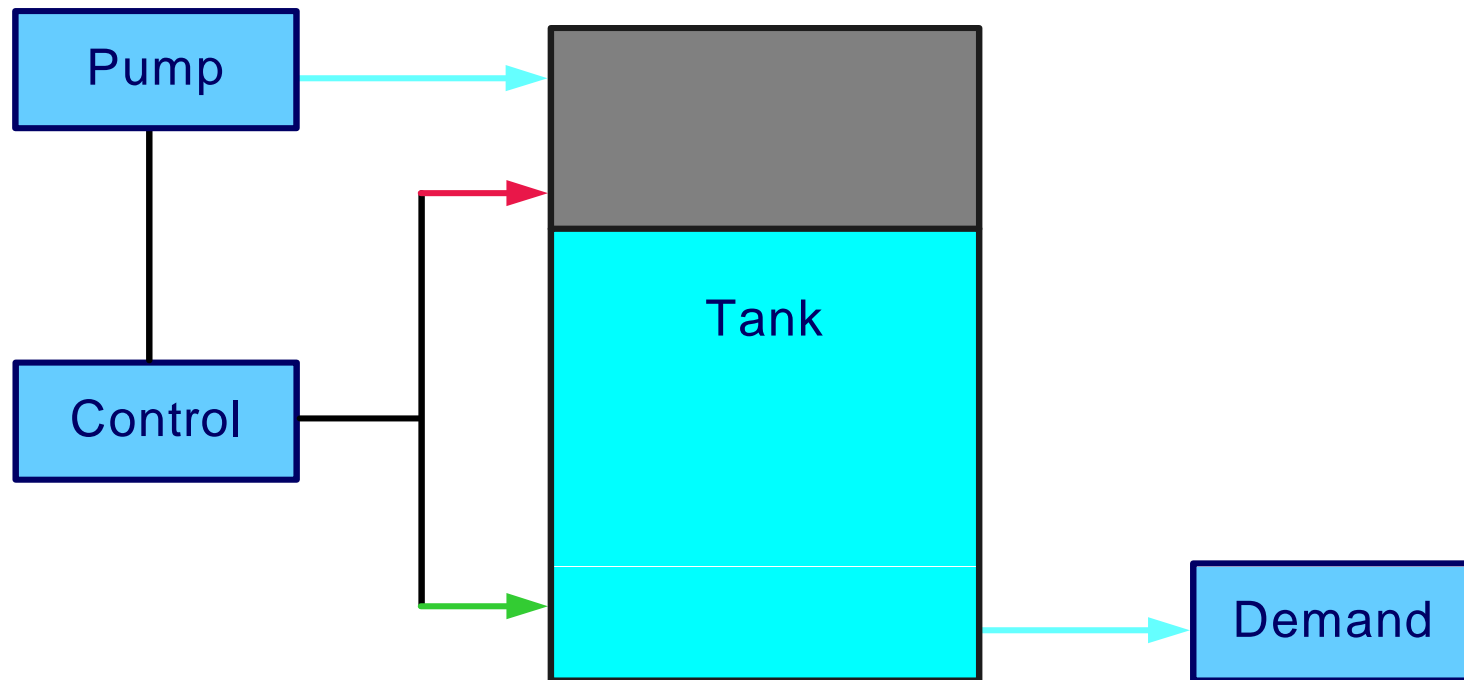
- DCE
 - ◆ Data Communications Equipment
 - ◆ Modems
 - ◆ Channel Cards
- DTE
 - ◆ Data Terminal Equipment
 - ◆ Relays
 - ◆ Computers

Device Connections

- Crossover Cable
 - ◆ DTE to DTE
 - ◆ DCE to DCE
- Straight Cable
 - ◆ DTE to DCE

Flow Control

- Prevents buffer overruns
- Red light – green light

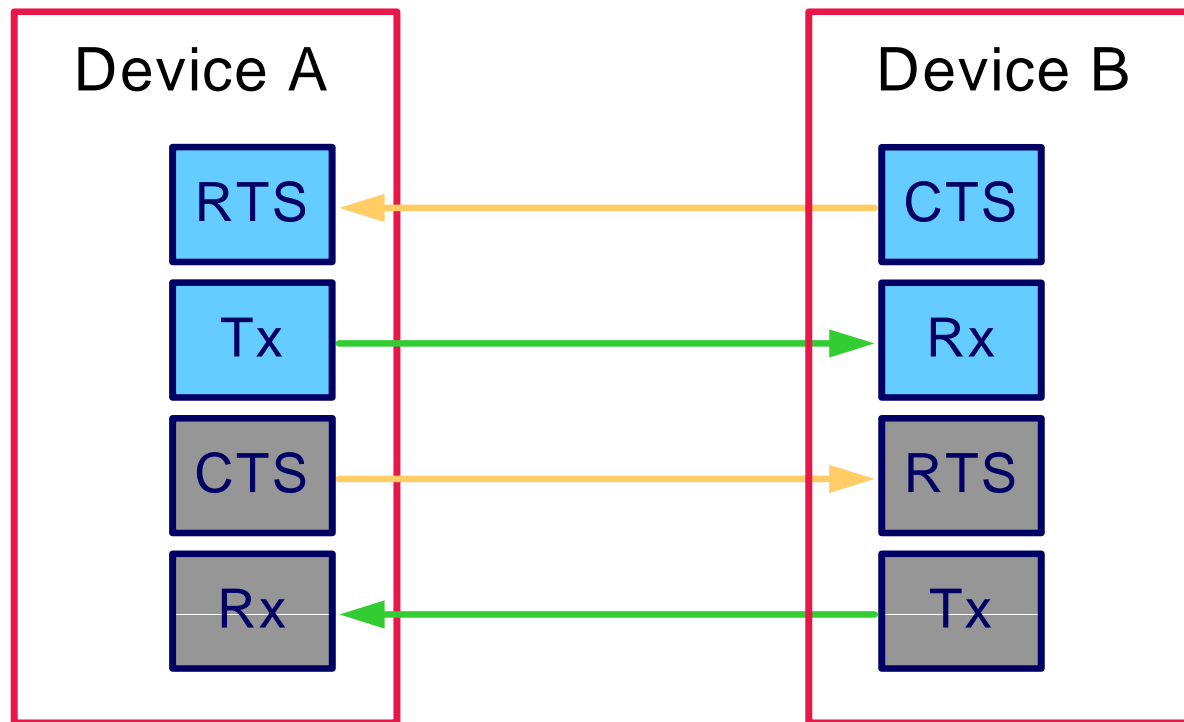


Software Flow Control

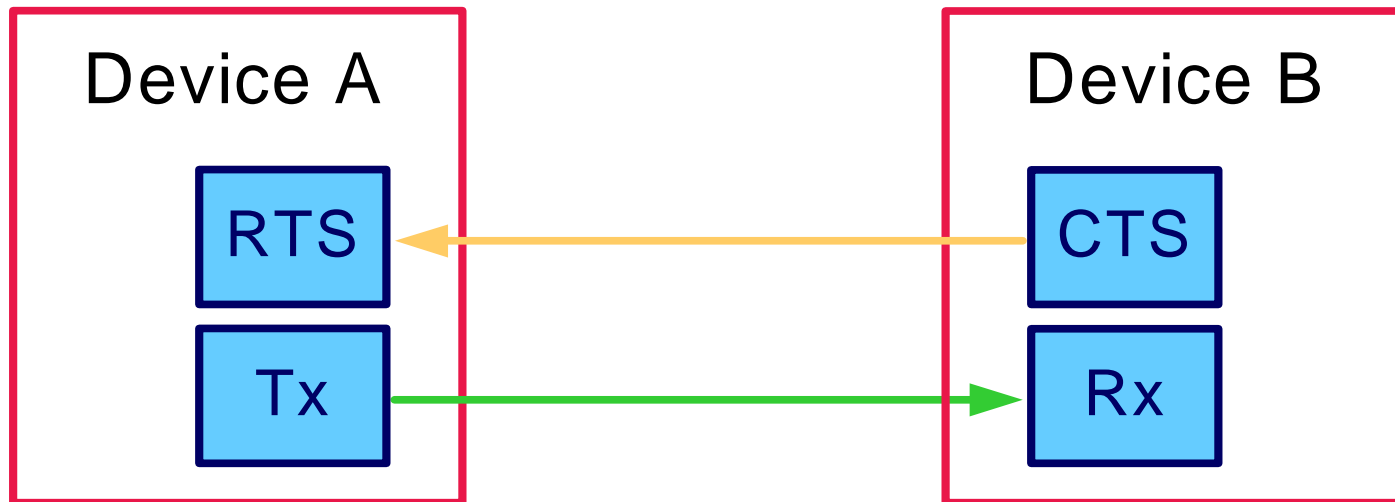
- XON 0x11
- XOFF 0x13

Hardware Flow Control

- RTS – Ready To Send
- CTS – Clear To Send



Hardware Flow Control



Common Flow Control Problems

- Software
 - ◆ Binary data
 - ◆ Noise – no shield
 - ◆ Dropped characters
- Hardware – cabling

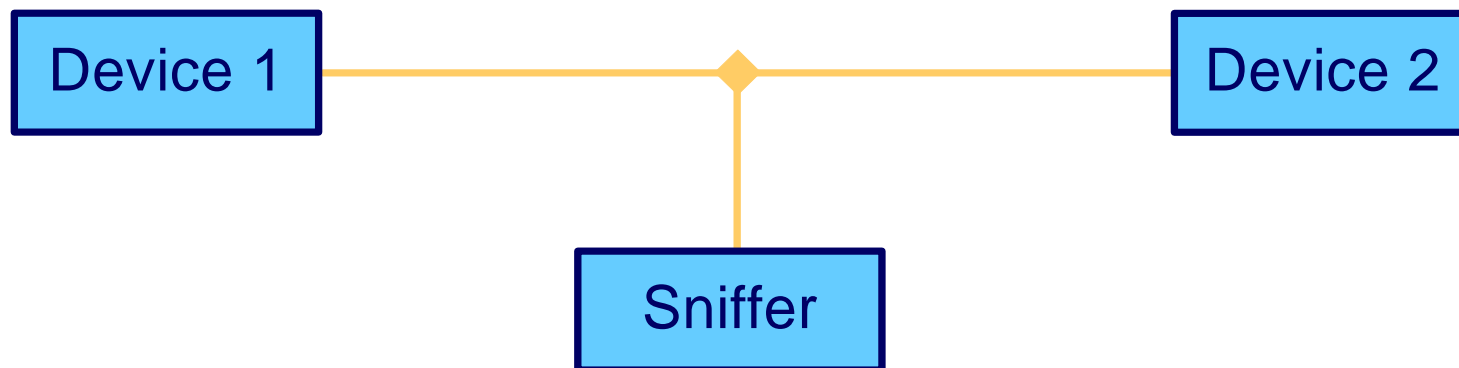
Serial Parallel Tools

PROS

- Protocol decoding
- Does not alter the line
- Detailed capture

CONS

- More costly
- Special cabling
- Special drivers



Serial In-Line Tools

PROS

- Simpler hardware setup
- Less costly

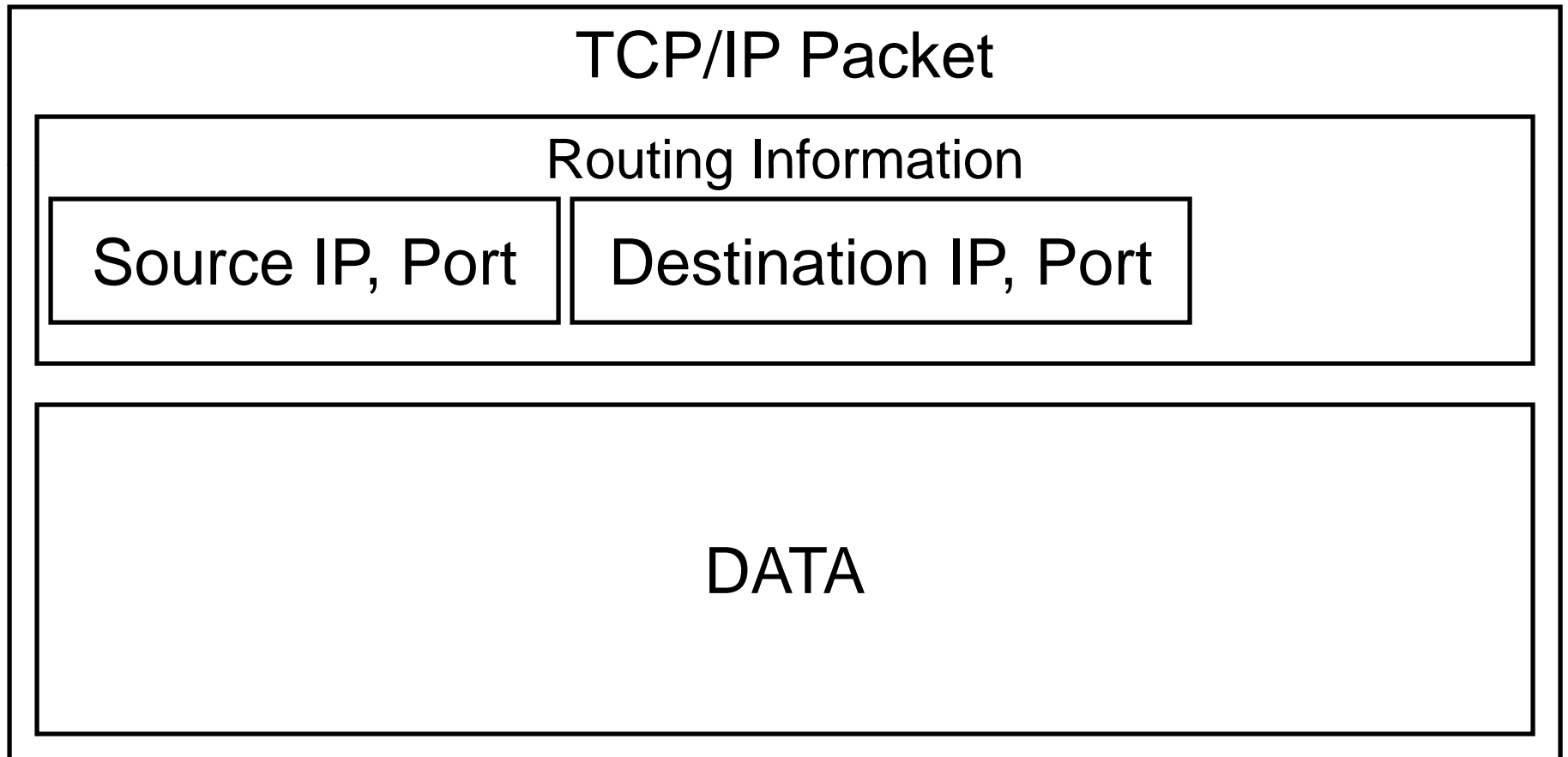
CONS

- Alters buffering
- Alters timing
- Alters control lines



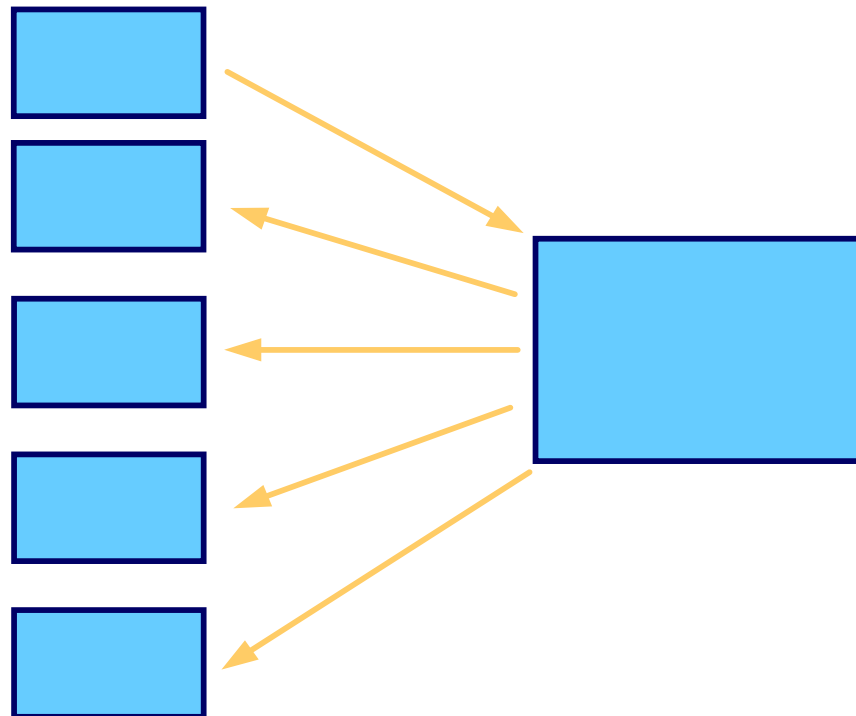
TCP/IP Communications

Frames / Packets



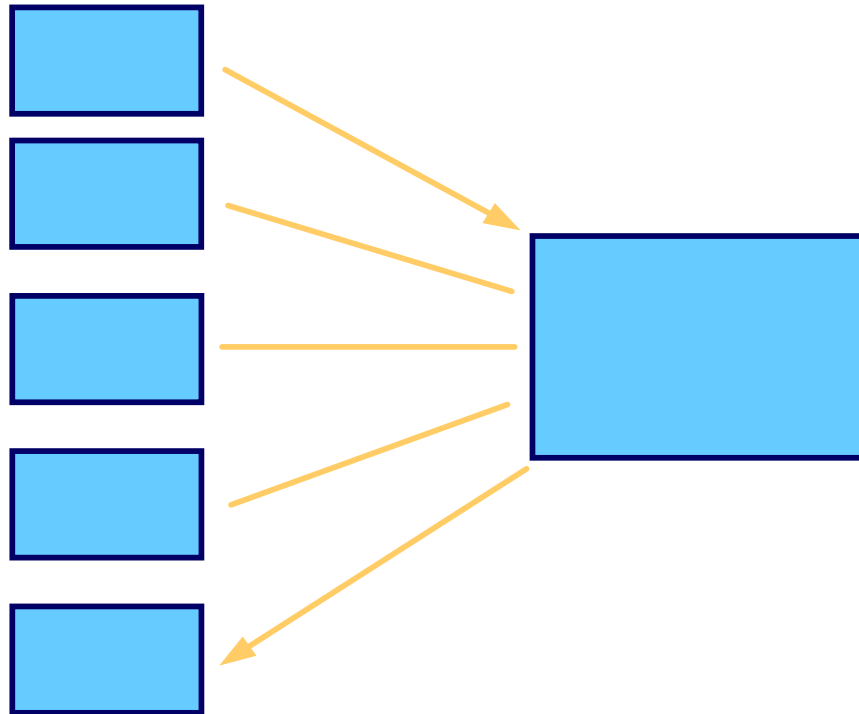
Hubs

- Move data along network
- Rebroadcast – every node sees all traffic
- Simple



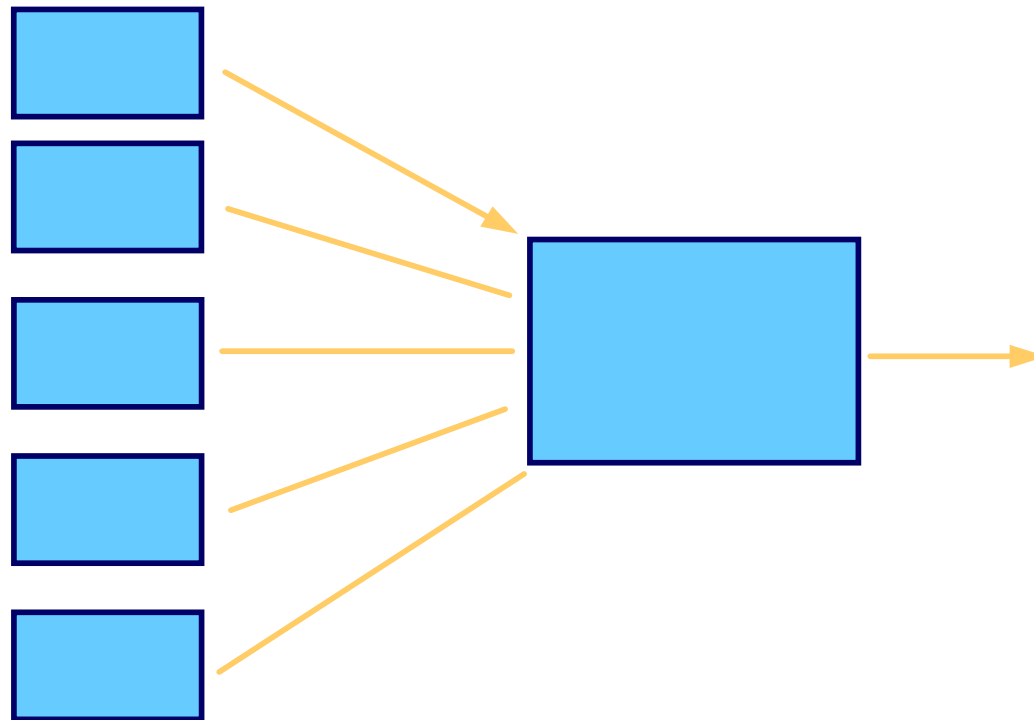
Switches

- Move data from node to node
- Direct traffic



Routers

- Move data, gateway between networks
- Switch internal network data



Common Network Problems

- Network settings
 - ◆ Duplicate IPs
 - ◆ Subnet, router settings
- Firewalls

Network Tools

- Wireshark and WinPCap applications
- Require vision of network traffic
 - ◆ Run on PC being debugged
 - ◆ Hubbed alongside
 - ◆ Mirrored port(s)
- Filtering of packets, protocols

Wireshark

No. ↓	Time	Source	Destination	Protocol	Info
91	15.000000	10.200.0.1	10.200.0.144	HTTP	Conn. Reset = 6192/00:04:4e:3d:8b:bc
92	15.241579	10.200.0.253	10.200.255.255	BROWSER	Host Announcement JIANCHPC4, work
93	15.550879	10.200.0.144	10.201.12.12	Modbus/TCP	query [1 pkt(s)]: trans:
94	15.578629	10.201.12.12	10.200.0.144	Modbus/TCP	response [1 pkt(s)]: trans:
95	15.691448	10.200.0.144	10.201.12.12	TCP	2286 > 502 [ACK] Seq=13 Ack=254 w
96	15.722795	10.200.0.144	10.201.12.12	Modbus/TCP	query [1 pkt(s)]: trans:
97	15.730867	10.201.12.12	10.200.0.144	Modbus/TCP	response [1 pkt(s)]: trans:

Frame 94 (307 bytes on wire, 307 bytes captured)
 Ethernet II, Src: 10.200.0.1 (00:04:4e:3d:8b:bc), Dst: 10.200.0.144 (00:0b:db:cd:89:fd)
 Internet Protocol, Src: 10.201.12.12 (10.201.12.12), Dst: 10.200.0.144 (10.200.0.144)
 Transmission Control Protocol, Src Port: 502 (502), Dst Port: 2286 (2286), Seq: 1, Ack: 13, Len: 253
 Modbus/TCP

- transaction identifier: 1
- protocol identifier: 0
- length: 247
- Modbus
 - unit identifier: 1
 - function 3: Read multiple registers
 - byte count: 244
 - Data

0000	00 0b db cd 89 fd 00 04 4e 3d 8b bc 08 00 45 00 N=....E.
0010	01 25 8a d2 00 00 3b 06 d1 d4 0a c9 0c 0c 0a c8	.%.....;
0020	00 90 01 f6 08 ee c6 e3 2e a2 c7 fa e3 c5 50 18P.
0030	11 10 48 6a 00 00 00 01 00 00 00 f7 01 03 f4 53	..Hj....S
0040	45 4c 2d 37 33 34 2d 58 31 38 58 2d 56 30 2d 5a	EL-734-X 18X-V0-Z
0050	30 30 36 30 30 31 2d 44 32 30 30 35 31 32 32 32	006001-D 20051222
0060	00 00 00 00 00 00 00 32 32 37 30 20 4e 00 00 002 270 N...
0070	00 00 00 00 00 00 00 00 00 00 00 00 53 45 4cSEL
0080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090	00 00 00 00 00 00 00 00 00 00 00 00 80 00 80
00a0	00 80 00 00 00 00 05 4d 57 33 44 49 00 00 00 00M W3DI....
00b0	00 00 00 00 00 4d 57 48 33 49 00 00 00 00 00 00MWH 3I.....
00c0	00 00 00 4d 56 41 33 44 49 00 00 00 00 00 00 00	...MVA3D I.....
00d0	00 4d 56 52 33 44 49 00 00 00 00 00 00 00 56	.MVR3DI.V
00e0	48 33 49 00 00 00 00 00 00 00 00 00 50 46 33	H3I.....PF3
00f0	00 00 00 00 00 00 00 00 00 00 56 48 33 49 00VH3I.
0100	00 00 00 00 00 00 00 00 00 4d 57 33 4d 58 00 00MW3MX..
0110	00 00 00 00 00 00 00 4d 57 33 50 49 00 00 00 00M W3PI....
0120	00 00 00 00 00 4d 57 33 50 4f 00 00 00 00 00 00MW3 PO.....
0130	00 00 00	...

Converters Move Data Between Mediums

- Modems
- Radios
- Ethernet – serial
- Fiber optics – serial
- EIA-485 to EIA-232

General Issues

- Message did not get there
- Message did not get back
- Buffer overruns, slowdowns, changes
- Interrupted signal path
- Garbled noisy channel, mixed baud rates
- Complex communications paths
- It should be doing

Tools

- **Knowledge is POWER**
 - ◆ Protocols
 - ◆ Device
 - ◆ Information resources
 - ◆ System behavior, fail point
- Sniffers serial, network
- Log files
- Test sets
- Breakout box

Test Sets

Verify Device Settings

- ASE 2000
- Triangle MicroWorks

Bag O' Tricks

- Patterns
- Divide and conquer
- Compare
- Start small
- Make small, atomic changes
- What changed before it quit working?
- Check settings cabling
- Easiest problem is likely the issue
- Loopback messages
- Communications statistics

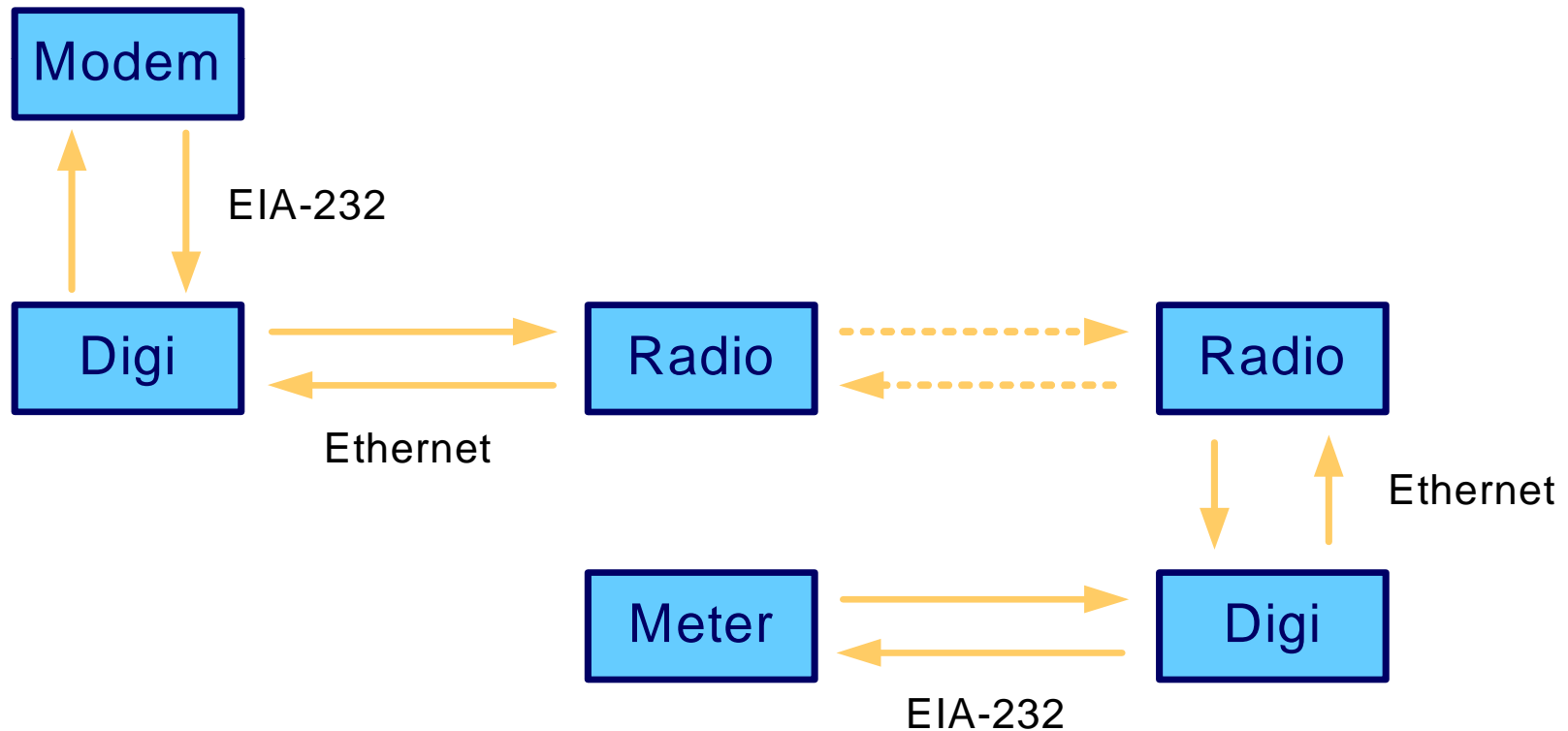
Real World Examples

- Rx and TX
- Ground



Real World Examples

- Modbus[®] protocol
- MV-90



SEL-734 Communications Debugging

- Modbus communications counters
- Supports loopback messages
- Modem in Use (MIU) Meter Word bit
 - ◆ Front-panel LEDs
 - ◆ SER