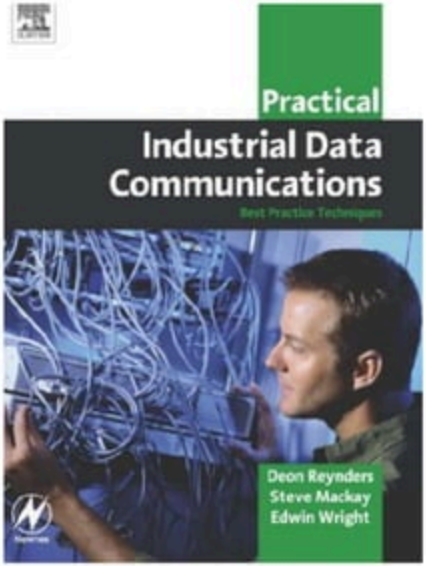
Modbus Data communications systems

by

Steve Mackay



EIT Micro-Course Series

- Every two weeks we present a 35 to 45 minute interactive course
- Practical, useful with Q & A throughout
- PID loop Tuning / Arc Flash Protection, Functional Safety, Troubleshooting conveyors presented so far
- Upcoming:
  - Electrical Troubleshooting and much much more.....
- Go to

http://www.eit.edu.au/free-courses

- You get the recording and slides

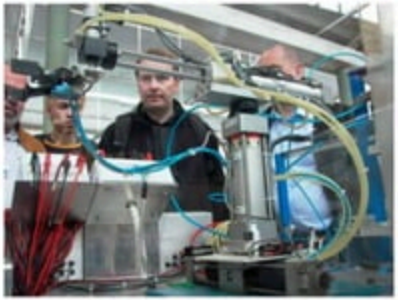
Overall Presentation

A review of the Modbus Protocol and related some troubleshooting issues.

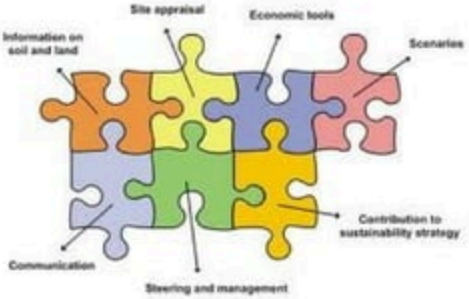
Objectives

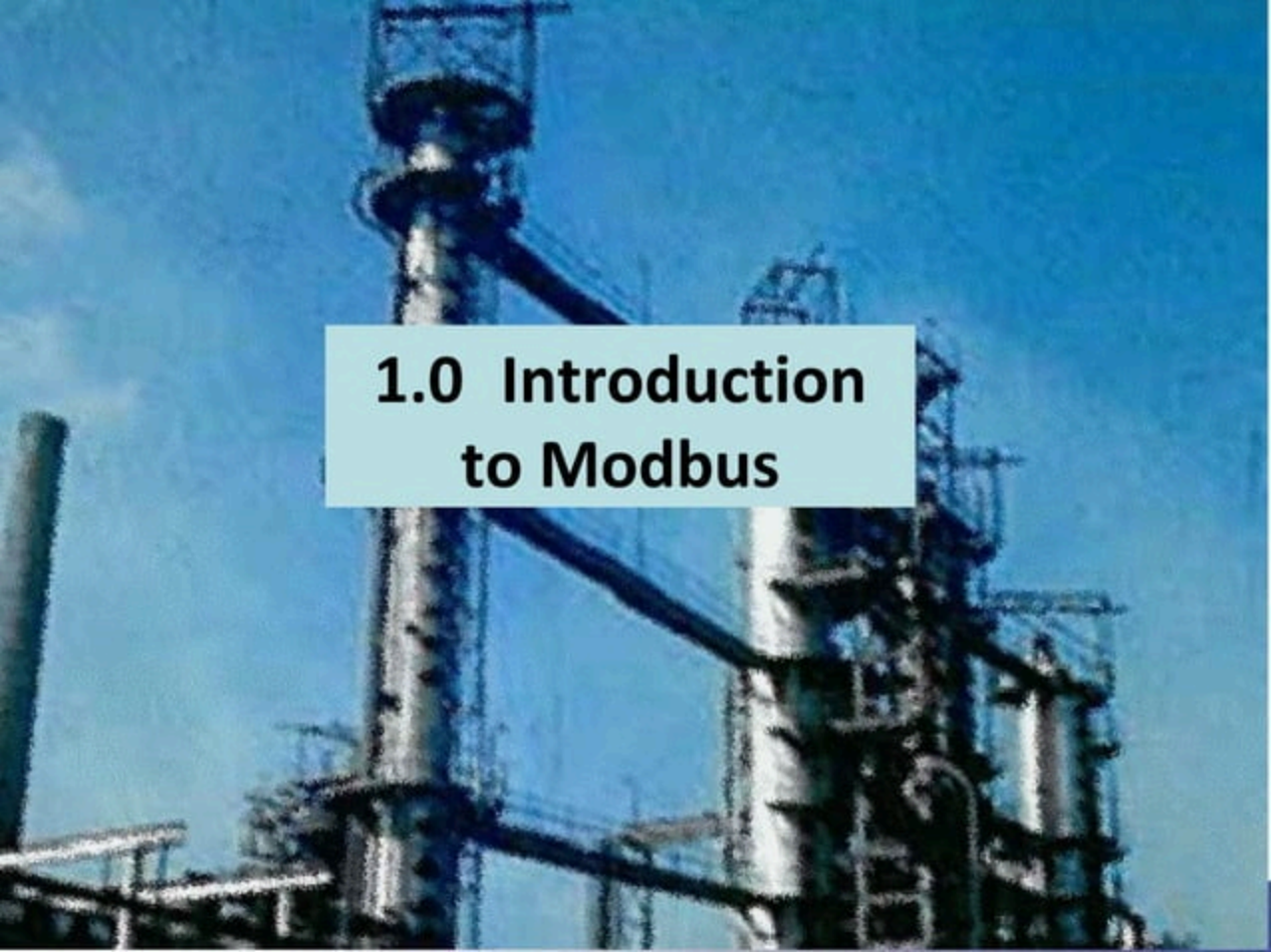
- Give an introduction to Modbus
- Review simple troubleshooting steps

Topics



- Introduction to Modbus protocol
- Troubleshooting Modbus
- Conclusion




1.0 Introduction
to Modbus

Objective

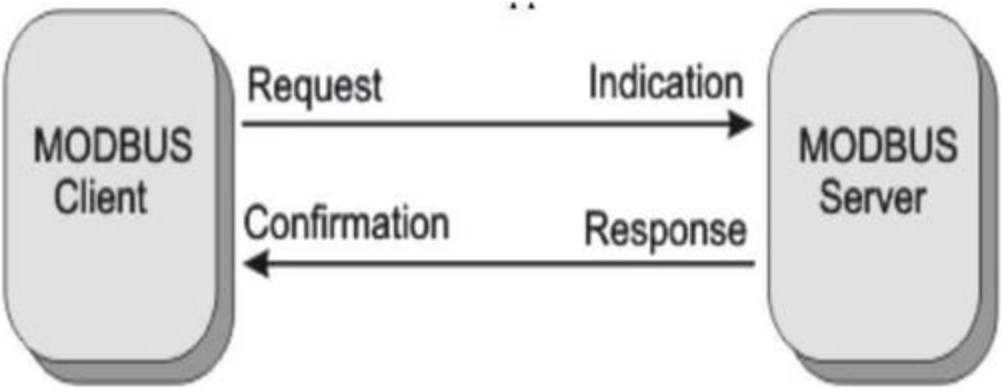
- The Modbus Messaging protocol
- The transportation of Modbus requests and responses on serial networks
- Modbus memory allocation
- Modbus Function Codes and their application
- The difference between Modbus RTU and ASCII
- Troubleshooting Modbus systems in terms of:
  - No response to requests
  - Exception responses

Modbus messaging

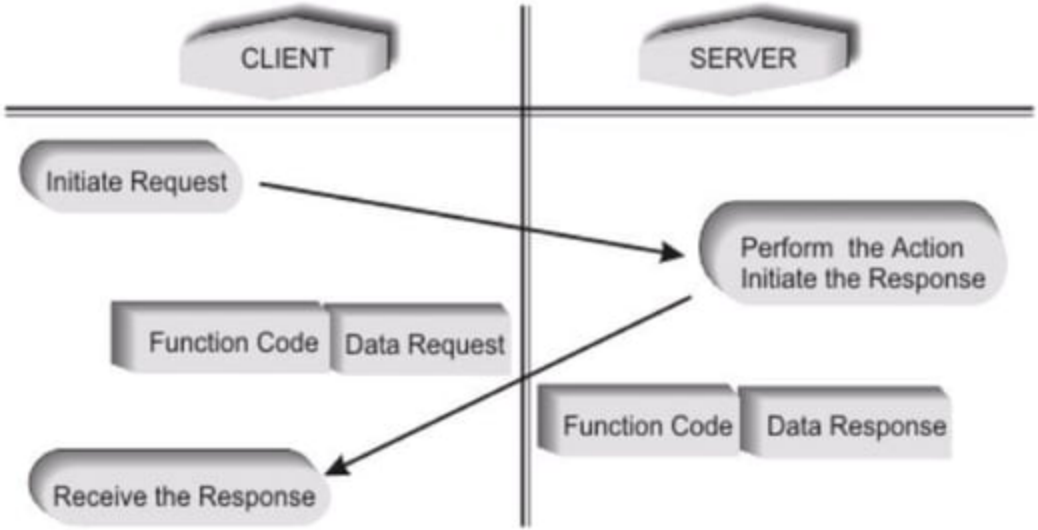
- Application layer (OSI layer 7) protocol that provides client/server communication between devices connected to different types of buses or networks

- 'Request/Response' type protocol and not a 'master/slave' type protocol

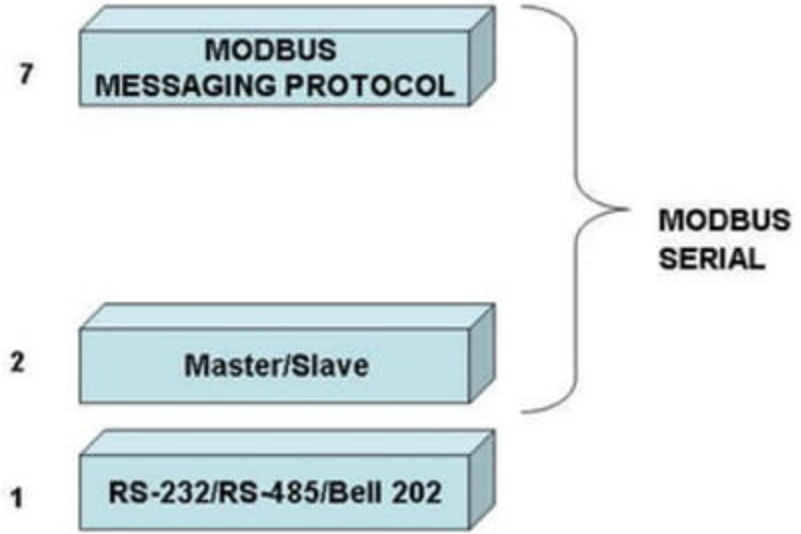
Master-slave interaction



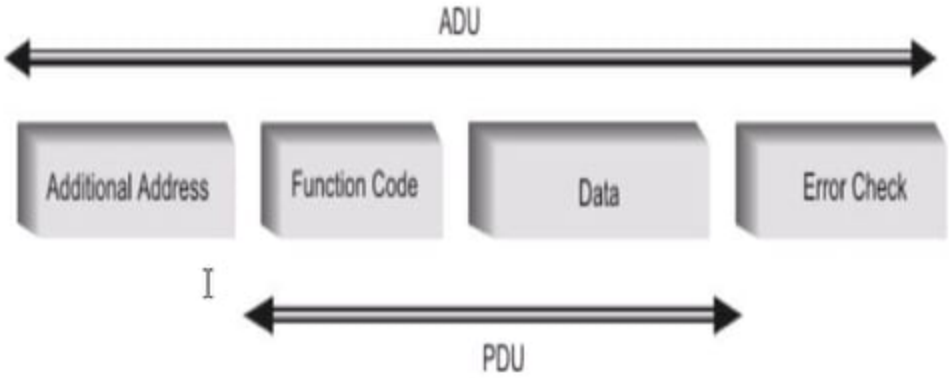
Modbus transaction



Modbus Serial communication stack



Modbus Serial ADU



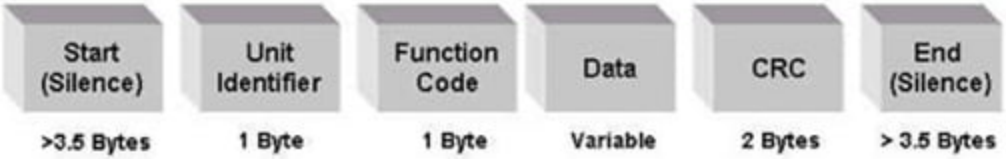
Modbus....

- The Address field
- The Function field
- The Data field
- The Error Check field

Allocation of Modicon memory address blocks

RTU mode

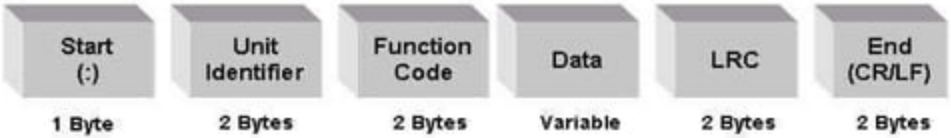
- 8 data bits, even, odd or no parity, 1 or 2 stop bits
- Gap of 3 ½ character lengths used for header (3 ½ mS)
- Same for trailer
- Gap in transmission >1,5ms causes frame to be discarded
- CRC error checking
- 999810 transmitted as <0x27><0x0E> (2 bytes)



RTU message frame

ASCII Mode

- 7 data bits, even, odd or no parity, 1 or 2 stop bits
- Header = : (colon)
- Trailer = <CR> <LF>
- Gaps of 1 second in frame acceptable
- LRC error checking (not CRC)
- 999810 (0x270E) transmitted as the ASCII string 270E i.e. <0x32><0x37><0x30><0x45> (4 bytes)



ASCII message frame

Function Code

- **FC01- reading coils-RTU mode :**

Request message

Unit Identifier	Function Code	Reference Number	Bit Count	CRC
01	01	00 0A	00 02	9D C9

Response message

Unit Identifier	Function Code	Byte Count	Bit Values	CRC
01	01	01	03	11 89

- **Read input discrete :**

Request message

Unit Identifier	Function Code	Reference Number	Bit Count	CRC
01	02	00 00	00 02	F9 CB

Response message

Unit Identifier	Function Code	Byte Count	Bit Values	CRC
01	02	01	02	20 49

Function Codes....

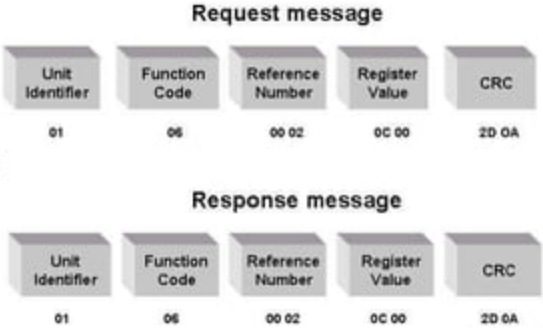
- **Read multiple registers :**

- **FC04-reading input register**

Function Codes....

- **Write coil :**

- **Write single register :**



Force multiple coils

Request message

Unit Identifier	Function Code	Reference Number	Bit Count	Byte Count	Data	CRC
01	0F	00 01	00 03	01	07	.. ..

Response message

Unit Identifier	Function Code	Reference Number	Bit Count	CRC
01	0F	00 01	00 03	.. ..

- **Write multiple registers :** →

Request message

Unit Identifier	Function Code	Reference Number	Word Count	Byte Count	First Register	Second Register	CRC
01	10	00 0A	00 02	04	AB CD	01 02	.. ..

Response message

Unit Identifier	Function Code	Reference Number	Word Count	CRC
01	10	00 0A	00 02	.. ..

2.0 Modbus - Troubleshooting

Typical problems

- **Hardware or software problems :**

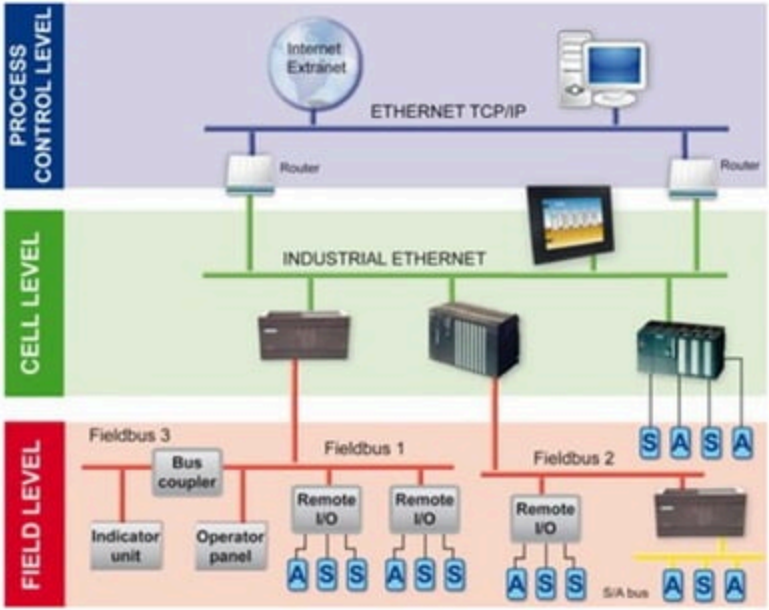
- Hardware problems → Mis-wired communication cabling and faulty communication interfaces

- Software (protocol) related problems → Controller application tries to access non-existent target devices nodes or use invalid Function Codes, address non-existent memory locations in the target devices, or specify illegal data format types

Tools used

- **Hardware tools :** → RS-232 breakout boxes, RS-232 to RS-485 converters, continuity testers, voltmeters, screwdrivers, pliers, crimping tools and cabling tools.
- **Software tools** → Protocol analyzer
- **Hardware troubleshooting**
- **Software troubleshooting**

Overall Concept



Tools of the trade

- Cable tester
- TCP/IP (and other third party) Utilities
- Protocol Analyzer (e.g. Wireshark)

Hardware and Physical Cabling

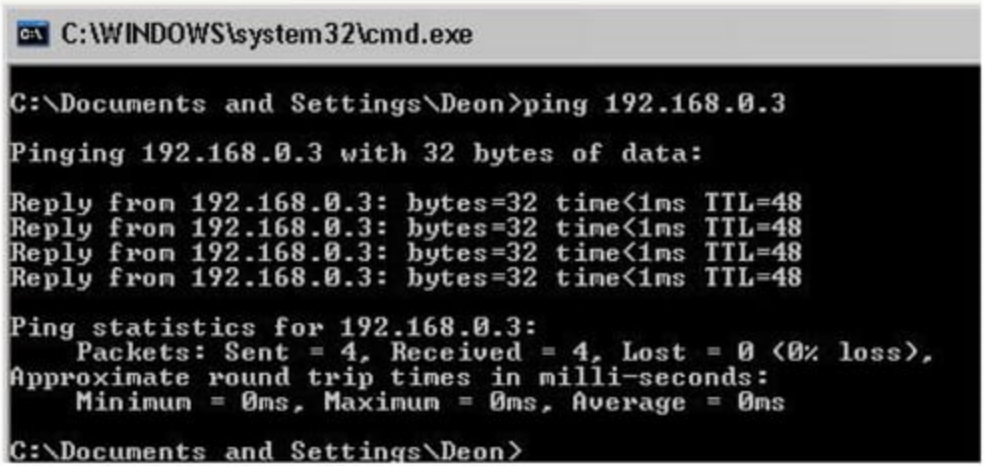
- Check cable on both sides of connection
- Switch lights
- Incorrect wire type and components
- Straight versus cross over cable
- Excessive untwists
- Damaged RJ-45 connector
- Electrical noise and shielding

TCP/IP Utilities

- Ping
- Arp
- Netstat
- Nbtstat
- Ipconfig
- Tracert

Ping -t

- Easiest ways to test connectivity across the network and confirm that an IP address is reachable

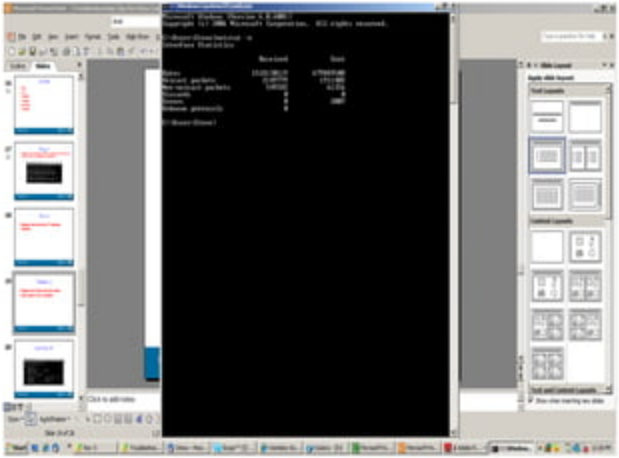


Arp -a

- Displays hardware and IP address mapping

Netstat -e

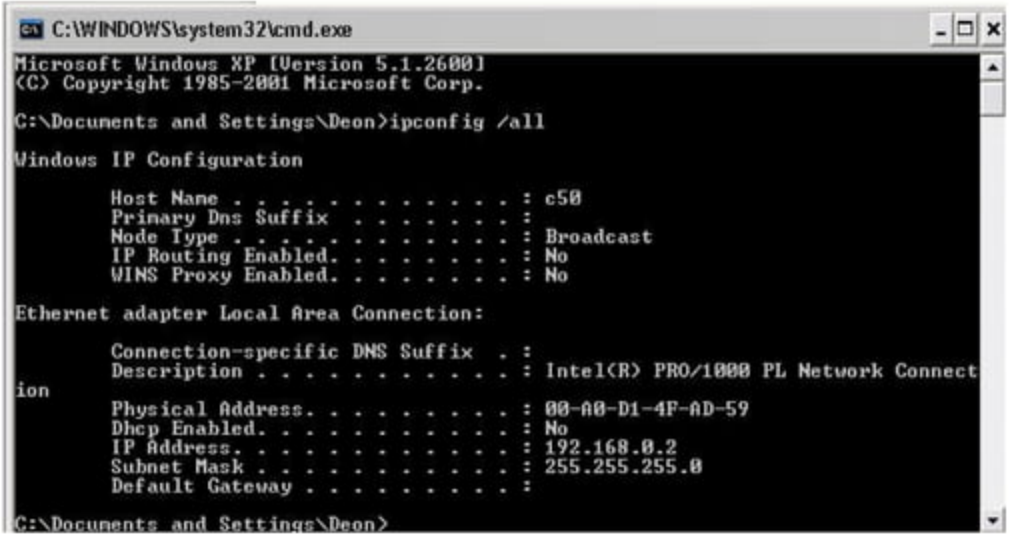
- Displays activities since last reboot
- Useful data on any problems



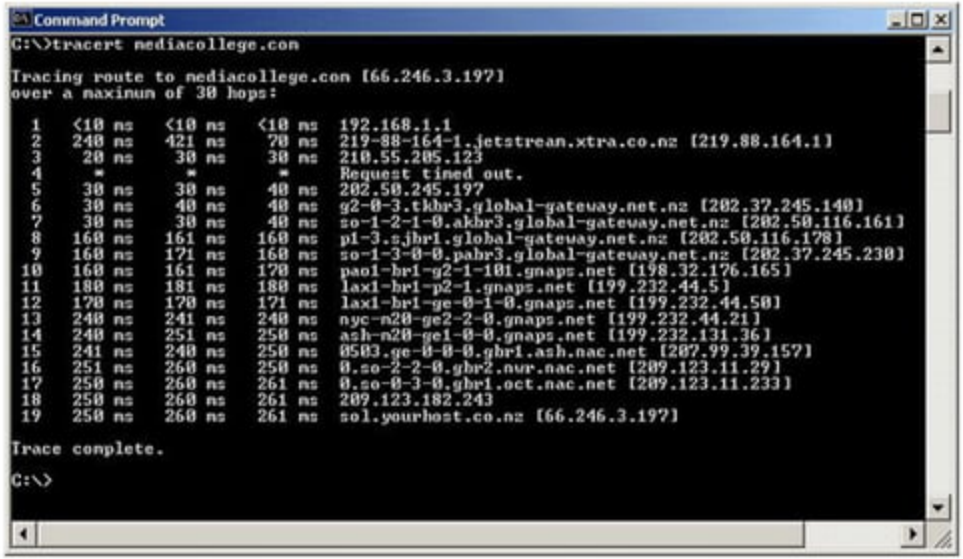
Nbtstat

- Protocol Stats & TCP/IP connections

Ipconfig /all

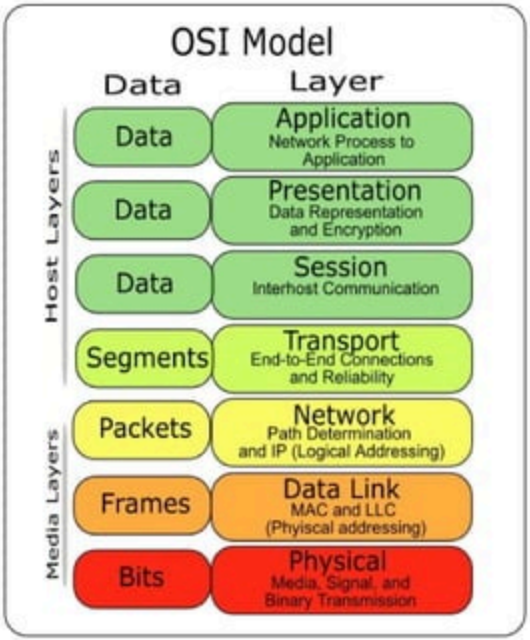


Tracert

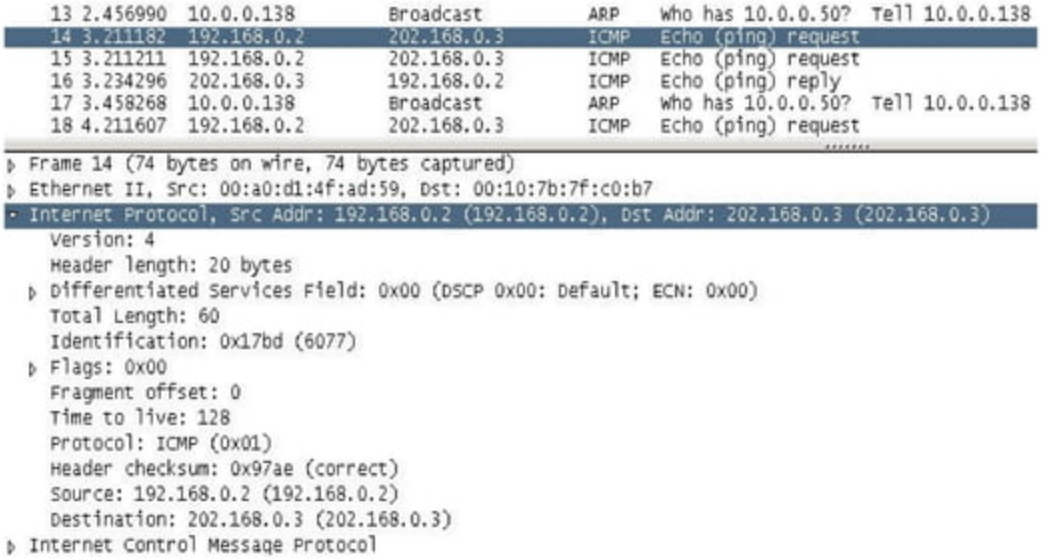

Command Prompt
C:\>tracert mediacollege.con
Tracing route to mediacollege.con [66.246.3.197]
over a maximum of 30 hops:
1 <10 ms <10 ms <10 ms 192.168.1.1
2 240 ms 421 ms 70 ms 219-88-164-1.jetstream.xtra.co.nz [219.88.164.1]
3 20 ms 30 ms 30 ms 210.55.205.123
4 * * * Request timed out.
5 30 ms 30 ms 40 ms 202.50.245.197
6 30 ms 40 ms 40 ms g2-0-3.tkbr3.global-gateway.net.nz [202.37.245.140]
7 30 ms 30 ms 40 ms so-1-2-1-0.akbr3.global-gateway.net.nz [202.50.116.161]
8 160 ms 161 ms 160 ms pl-3.sjbr1.global-gateway.net.nz [202.50.116.178]
9 160 ms 171 ms 160 ms so-1-3-0-0.pabr3.global-gateway.net.nz [202.37.245.230]
10 160 ms 161 ms 170 ms pao1-br1-g2-1-101.gnaps.net [198.32.176.165]
11 180 ms 181 ms 180 ms lax1-br1-p2-1.gnaps.net [199.232.44.5]
12 170 ms 170 ms 171 ms lax1-br1-ge-0-1-0.gnaps.net [199.232.44.50]
13 240 ms 241 ms 240 ms nyc-n20-ge2-2-0.gnaps.net [199.232.44.21]
14 240 ms 251 ms 250 ms ash-n20-ge1-0-0.gnaps.net [199.232.131.36]
15 241 ms 240 ms 250 ms 0503.ge-0-0-0.gbr1.ash.nac.net [207.99.39.157]
16 251 ms 260 ms 250 ms 0.so-2-2-0.gbr2.nvr.nac.net [209.123.11.29]
17 250 ms 260 ms 261 ms 0.so-0-3-0.gbr1.oct.nac.net [209.123.11.233]
18 250 ms 260 ms 261 ms 209.123.182.243
19 250 ms 260 ms 261 ms sol.yourhost.co.nz [66.246.3.197]
Trace complete.
C:\>

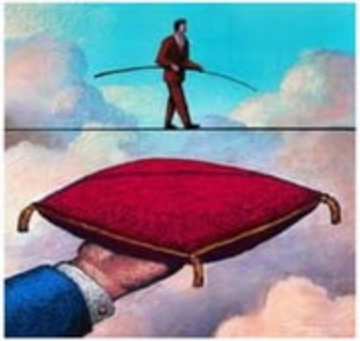
Packet Analysis

OSI Model


OSI Model
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Packets
Network
Path Determination and IP (Logical Addressing)
Frames
Data Link
MAC and LLC (Phyiscal addressing)
Bits
Physical
Media, Signal, and Binary Transmission

Packet Structure





Section 3
Conclusion

Thank You For Your Interest

If you are interested in further training, please visit:
http://www.idc-online.com/slideshare