

NETWORK MANAGEMENT

Mohammad S. Hasan

Lecture Outline

2

- The Need for Network Management
- The ISO network management model
- Network Management Tools
- Network Troubleshooting
 - ▣ Procedure
 - ▣ Commands

The Need for Network Management

3

- ❑ To keep the number of problems to a minimum
- ❑ To prevent problems that cause inconvenience
- ❑ To stop any damage spreading



Network Management

Network Management

4

- Network manager or network administrator's role
 - ▣ Designs and implements efficient and robust network infrastructure
 - ▣ Identifies and corrects problems as they arise
 - ▣ Knowledge on both hardware and software
- Why is network management hard?
 - ▣ Most internets heterogeneous
 - ▣ Most internets large

The ISO Network Management Model

5

- ❑ Configuration management
- ❑ Fault management
- ❑ Performance management
- ❑ Accounting management
- ❑ Security management

Configuration Management

6

- Monitoring and controlling normal operations in a network
- Collecting and maintaining the network configuration
- The administrators need to know
 - ▣ The components of the network
 - ▣ Component names and addresses
 - ▣ Routing details
 - ▣ Relationship between these components
 - ▣ Component operational characteristics

Configuration Management

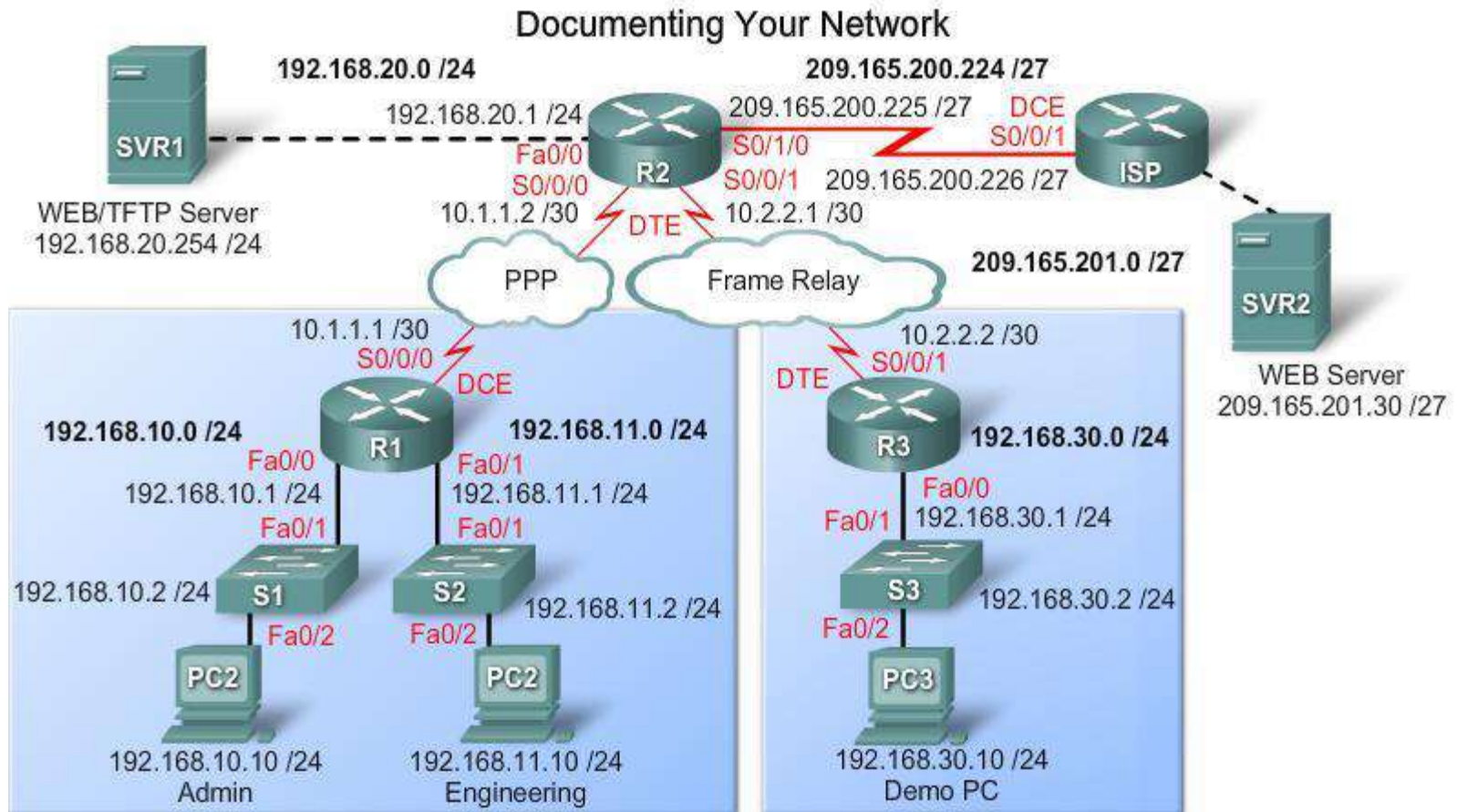
7

Device Name, Model	Interface Name	MAC Address	IP Address/Subnet Mask	IP Routing Protocol(s)
R1, Cisco 2611XM	fa0/0	0007.8580.a159	192.168.10.1 /24	EIGRP 10
	fa0/1	0007.8580.a160	192.168.11.1 /24	EIGRP 10
	s0/0/0	---	10.1.1.1/30	OSPF
	s0/0/1	---	Not Connected	
R2, Cisco 2611XM	fa0/0	0007.8580.a159	192.168.20.1 /24	EIGRP 10

Switch Name, Model, Management IP Address	Port Name	Speed	Duplex	STP State (Fwd / Block)	Port Fast (Yes / No)	Trunk Status	Ether Channel (L2 or L3)	VLANs	Key
S1, Cisco WS-C3550-24-SMI, 192.168.10.2 /24	fa0/1	100	Auto	Fwd	No	On	L2	1	Connects to R1
	fa0/2	100	Auto	Fwd	No	On	L2	1	Connects to PC1
	fa0/3								Not Connected
	fa0/4								Not Connected

Configuration Management

8



Fault Management

9

- Fault conditions must be detected, logged, isolated and dealt with
- Three areas – GP diagnosis
 - ▣ Fault / error detection
 - ▣ error diagnosis
 - ▣ error recovery



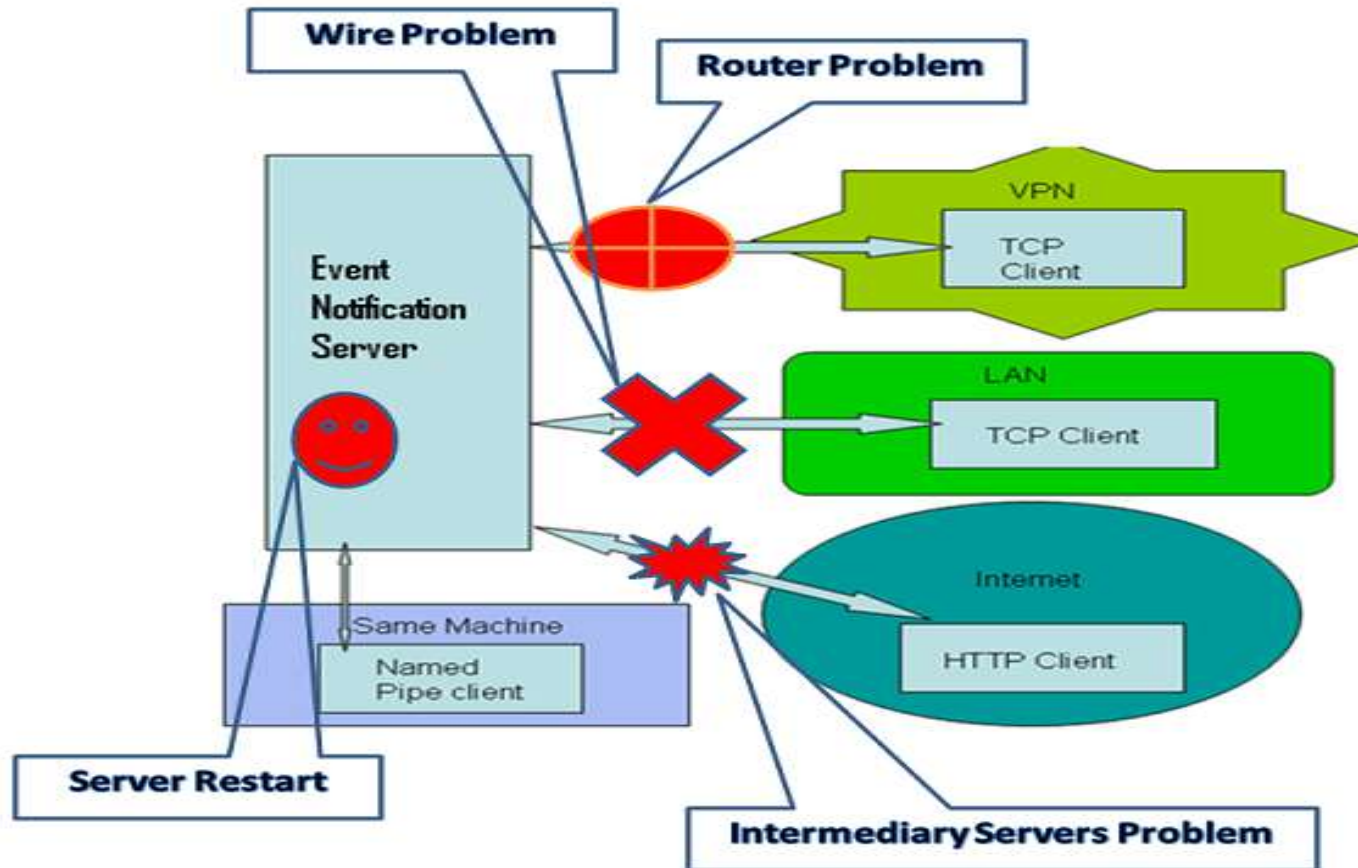
Fault Management

10

- Fault / error detection
 - ▣ Users may discover faults
 - ▣ Special reliability tests may reveal faults
- Error diagnosis
 - ▣ Analysing logs
 - ▣ Running diagnostic programs
- Error recovery
 - ▣ Resetting devices
 - ▣ Replacing faulty hardware or software

Fault Management

11



Performance Management

12

- Analyses and controls network performance
- Parameters measured, analysed and controlled
 - ▣ Throughput
 - ▣ Utilisation
 - ▣ Error rates etc.
- Making sure the network performs optimally
- The SNMP plays an important part in performance management

Performance Management – Establishing the Baseline

13

- A baseline sets the acceptable level of performance of the network
- Without a baseline, it will not be possible to tell whether performance is improving or declining
- If the network is expanded or updated, the baseline itself will need to be updated
- Baselining involves measuring and recording how a network operates over a certain period of time
- It can be used to find out how the network is performing currently and what the future needs are

Baselining

14

- Info on network devices
 - ▣ Workstations
 - ▣ Server computers
 - ▣ Hubs
 - ▣ Switches
 - ▣ Routers etc.
- Further information
 - ▣ Model numbers
 - ▣ Serial numbers
 - ▣ NIC MAC address
 - ▣ IP addresses
 - ▣ Protocols
 - ▣ Network applications etc.

Baselining

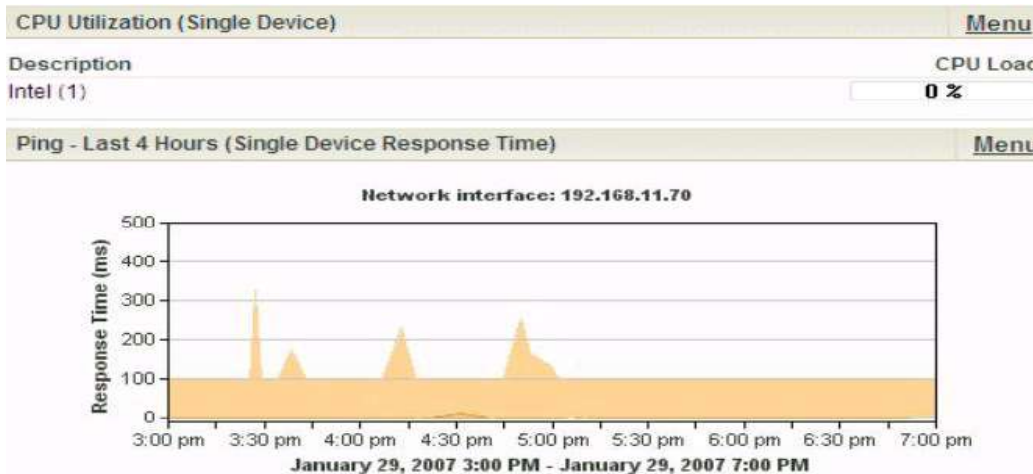
15

- The administrator will also need to record figures
 - ▣ the average and peak network utilisation
 - ▣ the average and peak frame size
 - ▣ the average and peak number of frames per second
 - ▣ the number of broadcasts
 - ▣ the number of collisions per second
 - ▣ the number of CRC errors
 - ▣ the number of illegally short and long frames

Baselining and Record Sheet

16

Hardware Device Documentation		
Type of equipment:		
Serial no.:		
Date purchased:		
Warranty expiration data:	Vendor:	Phone:
Service contract:	Vendor:	Phone:
Problems:		
Date:	Problem:	Solution:



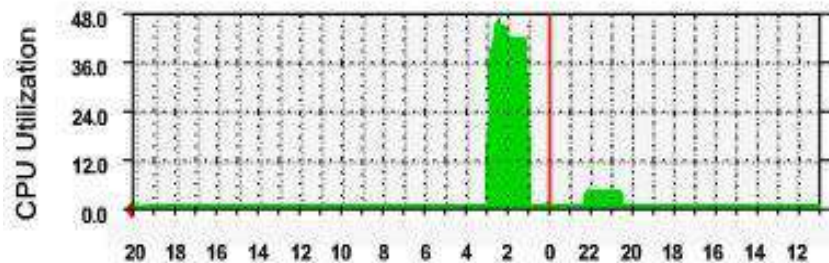
Network Management

- Manual maintenance
 - ▣ A simple record sheet may be utilised
- Automated maintenance
 - ▣ Software can be used to record the data

Baselining

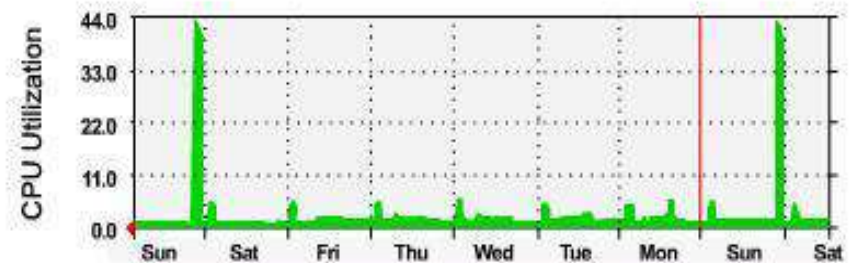
17

'Daily' Graph (5 minute Average)



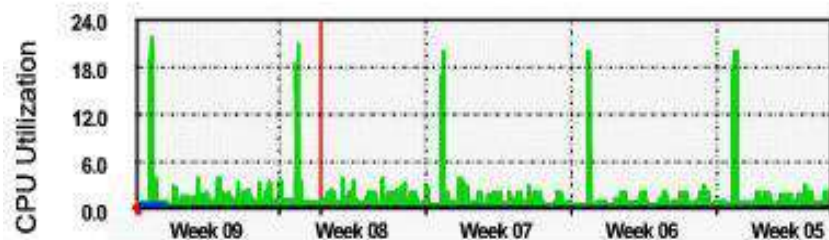
Max Load: 46% Average Load: 3% Current Load: 1%

'Monthly' Graph (2 Hour Average)



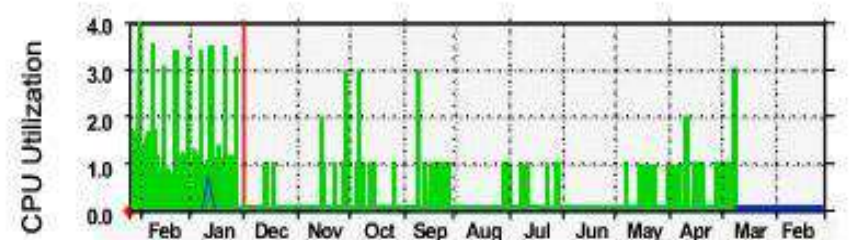
Max Load: 43% Average Load: 2% Current Load: 1%

'Weekly' Graph (30 Minute Average)



Max Load: 43% Average Load: 2% Current Load: 1%

'Yearly' Graph (1 day Average)



Max Load: 43% Average Load: 0% Current Load: 1%

Usual Parameters for Performance Management

18

- Parameters useful for demonstrating current system demands and predicting future needs
 - ▣ Mean Time Between Failures (MTBF)
 - 5 failures in 20 hours
 - ▣ Mean Time To Repair (MTTR) and
 - 5 failures took 5 hours repair time
 - ▣ Availability
 - 19 hours available in 24 hours

MTBF, MTTR & Availability

19

- The MTBF
 - ▣ the mean (average) time a device or system will operate before it fails
- The MTTR
 - ▣ the average time necessary to repair a failure within the computer system
- The availability
 - ▣ the probability that the component or system will be available during a fixed time period

Availability

20

- The formula for availability is given below:
 - ▣ $\text{Availability} = \text{MTBF} / (\text{MTBF} + \text{MTTR})$
- Example
 - ▣ Suppose that
 - MTBF = 5000 hours
 - MTTR of 20 hours
 - Availability = ?
 - ▣ $\text{Availability} = 5000 / (5000 + 20) = 99.6\%$

Availability

21

- The availability of a system
 - ▣ availability of each of its components
- if the system availability is A_{system} , the availabilities of device 1, 2, ..., n are $A_1, A_2 \dots, A_n$ then
 - ▣ $A_{\text{system}} = A_1 \times A_2 \times \dots \times A_n$
- A network has five components with an average availability of 0.96, then
 - ▣ $A_{\text{network}} = 0.96 \times 0.96 \times 0.96 \times 0.96 \times 0.96 = 0.815$

Accounting Management

22

- Collecting data on how resources are being consumed by users and devices
- The administrator can work out how much to charge for the network services
- It will facilitate analysis of current network capacity and analysis of trends
- Accounting management deals with
 - ▣ adding and deleting users
 - ▣ setting their usage quotas – student 40 MB h-drive
 - ▣ granting them privileges to access resources etc.

Security Management

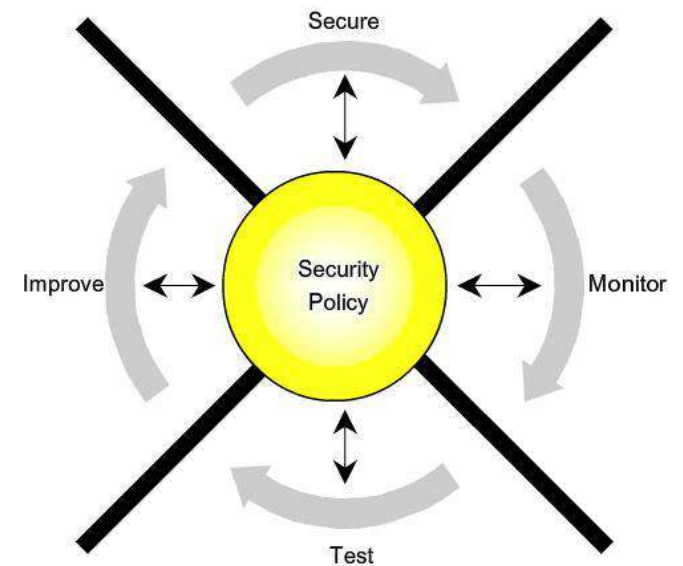
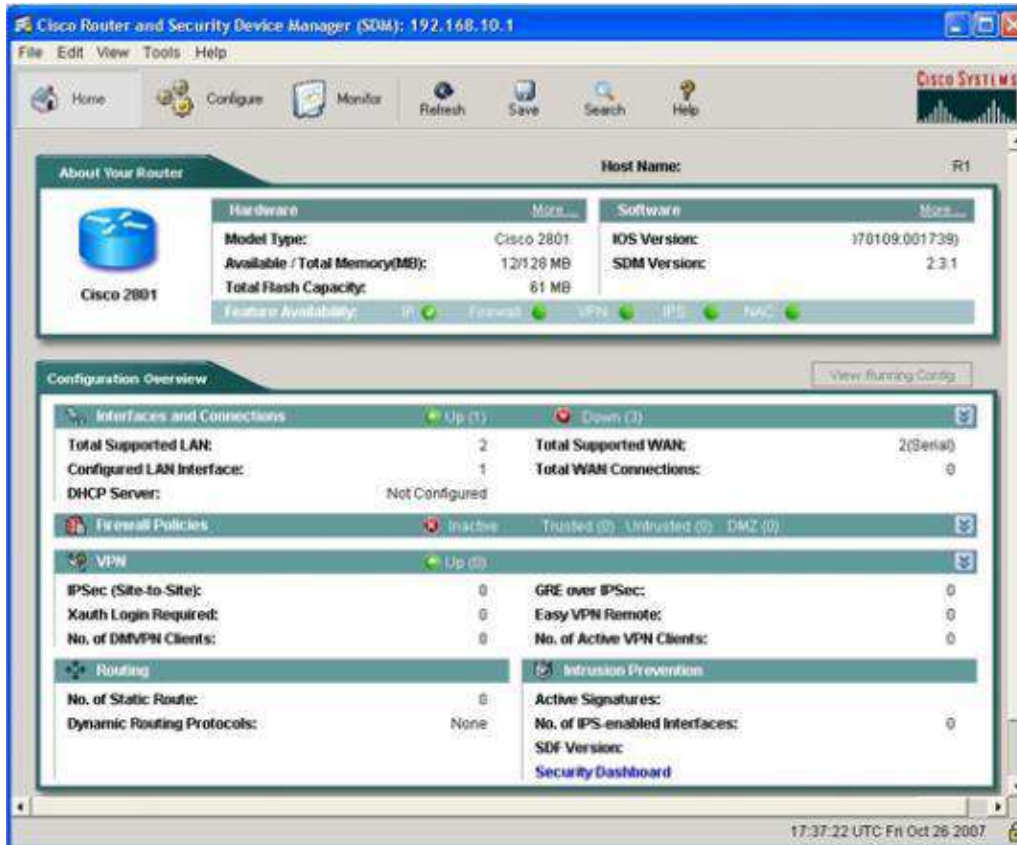
23

- Monitoring security
 - ▣ intrusion detection
 - ▣ user security management (passwords)
- Security configuration management
 - ▣ Example: firewalls and proxies
- Security audits - Vulnerability disclosure
 - ▣ Manual
 - ▣ Automated or software



Security Management

24



Monitor - Log analysis

Test - PoD or Smurf attack

Tools for Network Management

25

- Cable faults are the most common error on networks
 - ▣ Physical layer - cable testers
 - ▣ an LED lights up if a wire of a copper cable has a good connection
- Testers are also available for
 - ▣ Fibre optic cable and
 - ▣ Wireless



Cable Tester - Time Domain Reflectometry (TDR)

26

- A pulse of energy is sent along the cable - BAT
- The energy pulse is reflected back to the cable tester when the pulse reaches
 - ▣ the end of the cable or
 - ▣ the place where there is a fault
- The instrument measures the time to receive the reflected signal
- From the time taken, the tester works out the distance and displays it

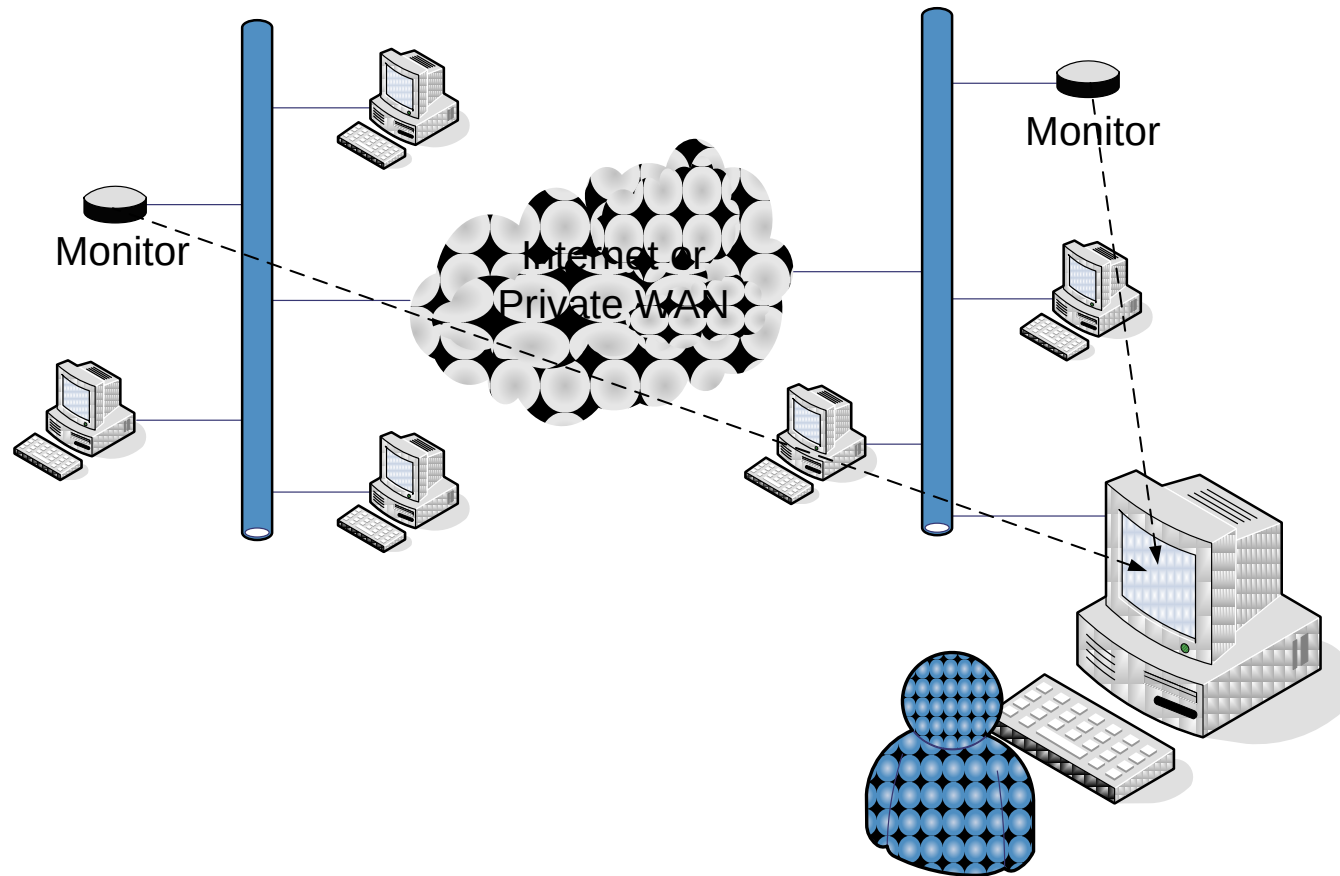
Network Monitors - Probes

27

- Network monitors (or probes) are installed on each segment
- The monitors observe and record events on the network
 - ▣ how much the network is utilised,
 - ▣ how many frames are sent and received etc.
- The information that the monitors provide can be viewed from a central point
- Network monitors are often a part of an integrated network management system
- These generally use remote monitoring (RMON)

Network Monitors - Probes

28

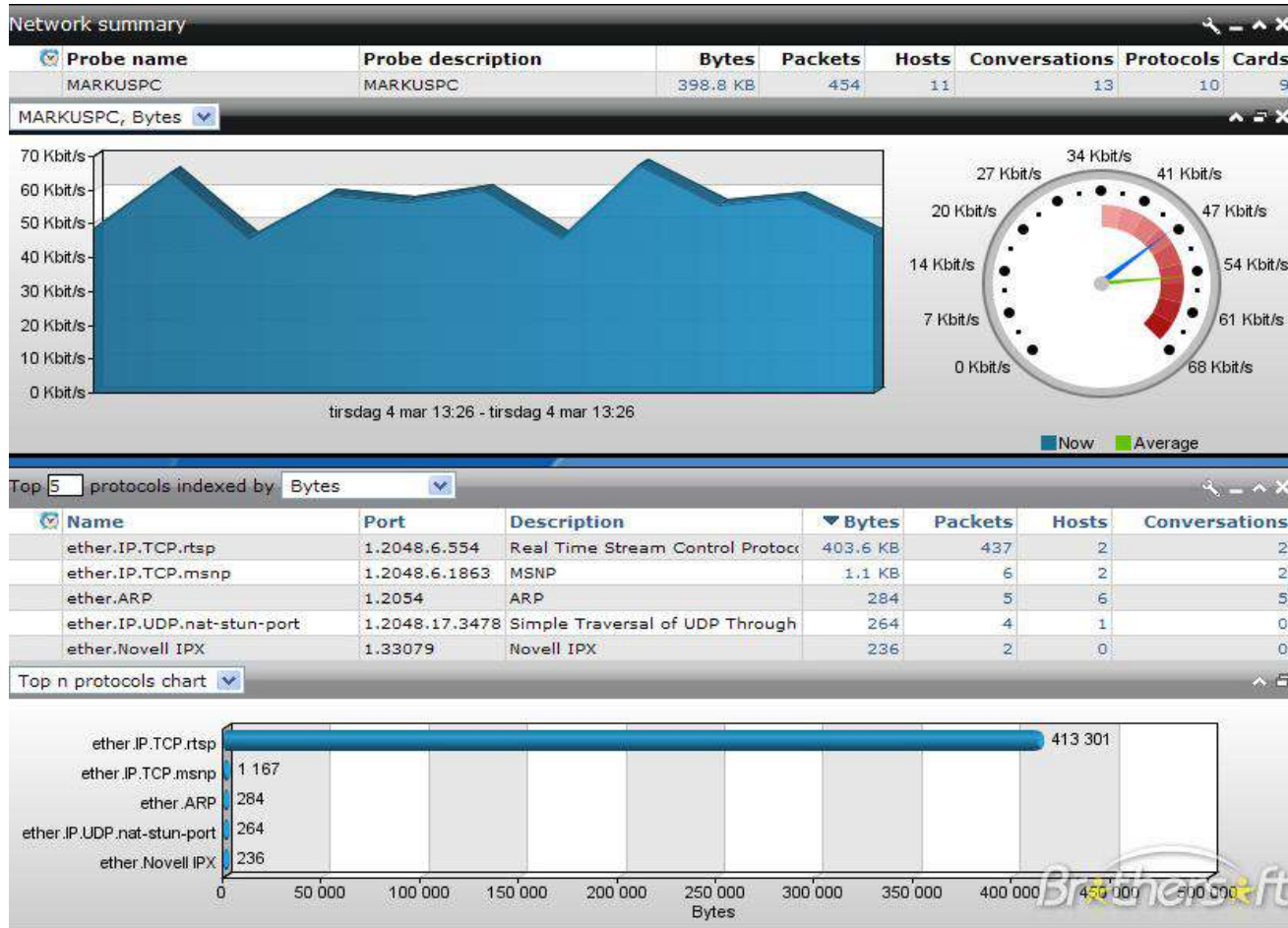


Network Administrator

Network Management

Network Monitors - Probes

29



Network Management

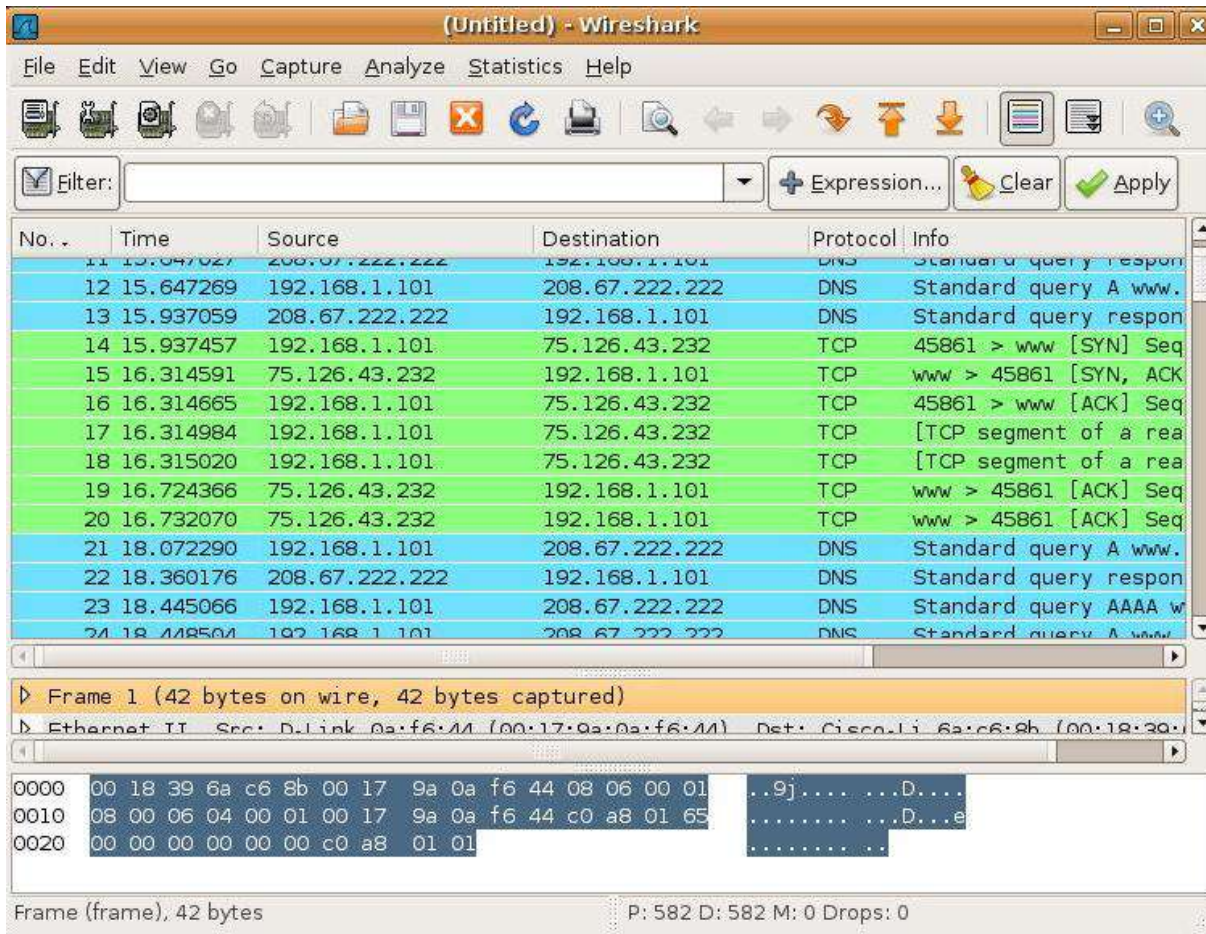
Protocol Analyser

30

- A protocol analyser or packet sniffer can capture and interpret network frames and packets
- The protocol analyser
 - ▣ Hardware: specialised portable computer with built-in software
 - ▣ Software: designed to run on a general-purpose computer
- Wireshark (formerly known as Ethereal) is a free protocol analysis software
 - ▣ Available from <http://www.wireshark.org/>

Protocol Analyser – Security Issues

31



- Privacy violation
- Username and password viewing if in plain text

Network Troubleshooting

32

- ❑ Troubleshooting involves finding out the cause of a problem on the network and sorting it out
- ❑ The tools discussed before can be used for this, along with other tools and techniques
- ❑ Sometimes very hard to detect the problem

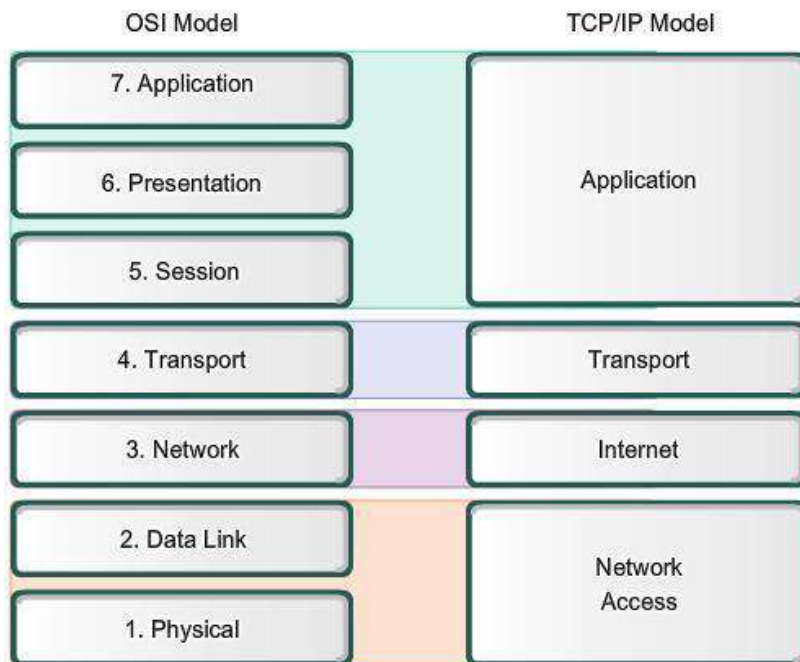
Systematic Method of Troubleshooting

33

- ❑ Collect symptom information and analyse it
- ❑ Narrow down to a particular area, e.g. a network segment or a network device
- ❑ Narrow down further, e.g. to an item of software or hardware within the troublesome network device
- ❑ Identify the problem and correct it
- ❑ Check if the problem really has been solved completely
- ❑ Document the problem and the solution
- ❑ Inform the network support team

Procedures for Troubleshooting

34



- Bottom-Up approach
 - ▣ Layer 1 to Layer 7 of the OSI model
- Top-Down approach
 - ▣ Layer 7 to Layer 1 of the OSI model

Troubleshooting – Possible Layer 1 (Physical Layer) errors

35

- ❑ Disconnected or broken data or power cables
- ❑ A device is NOT powered up
- ❑ Selection of wrong cable straight-through, crossover
- ❑ Cables plugged into the wrong port on a device
- ❑ A NIC, router, switch might be faulty

Troubleshooting at Layer 1

36

- ❑ Check indicator lights - if a NIC is physically connected and working a green light may be visible
- ❑ There may also be lights that show network transmission or reception
- ❑ No green light might also indicate a symptom of a cable problem
- ❑ It is advisable to check for basic faults before trying more sophisticated troubleshooting

Troubleshooting - Possible Layer 2 (Data Link Layer) errors

37

- ❑ Wrongly configured Ethernet or WAN interfaces
- ❑ Wrong type of Layer-2 encapsulation
- ❑ Frame Relay: the wrong DLCI (permanent virtual circuit number) may have been set
- ❑ Wrong MAC and IP address association
 - ▣ Purging (emptying) the ARP cache will often cure this
- ❑ Wrong VLAN configuration
 - ▣ NO communication between different VLANs

Troubleshooting - Possible Layer 3 (Network Layer) errors

38

- Addressing error
 - ▣ e.g. wrong IP address or subnet mask
- No routing protocol (such as RIP)
- Wrong routing protocol or version
- Wrong networks are being advertised

Commands for Troubleshooting

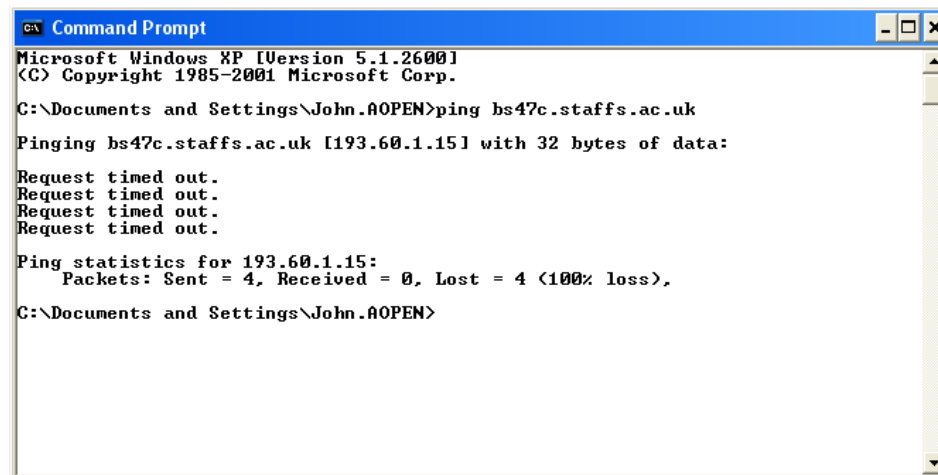
39

□ Ping

- To test network connectivity
- Shows the min, average and max round-trip time for a remote device

□ Traceroute / tracert

- To show the route from A to B
- Delay information
- Sequence of router from source to destination



```

C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\John.AOPEN>ping bs47c.staffs.ac.uk

Pinging bs47c.staffs.ac.uk [193.60.1.15] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 193.60.1.15:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\John.AOPEN>
```

Use of Telnet for Troubleshooting

40

- For troubleshooting at Layer 7
- Telnet is a virtual terminal protocol that works at the Application Layer of TCP/IP
- If Telnet functions OK, it shows that the TCP/IP protocol stack from Telnet downwards is working correctly
 - ▣ If Telnet to a server fails from a particular client host, try from another device
 - ▣ If the name of the server does not produce a login prompt, try server's IP address instead
 - ▣ If telnet still fails, it is possible that the Telnet service is not running or is running on a different port

The nslookup Command

41

- Gives the IP address of a domain name e.g. `www.google.co.uk`
- The command is issued on a PC with name “bsussoc1”
 - ▣ `bsussoc1 > nslookup www.google.co.uk`
 - ▣ Server: `bsus.staffs.ac.uk`
 - ▣ Address: `193.60.1.17`
 - ▣ Non-authoritative answer:
 - ▣ Name: `www.l.google.com`
 - ▣ Addresses: `66.102.9.147, 66.102.9.99, 66.102.9.104`
 - ▣ Aliases: `www.google.co.uk, www.google.com`