Protocol Trouble Shooting

Amir A. Khan

aakhan@ccse.kfupm.edu.sa
Department of Computer Engineering
King Fahd University of Petroleum and Minerals
Dhahran, Saudi Arabia

Overview

- Objectives of LAN Analysis
- Tools used for LAN Analysis
  - » LAN Analyzers
    - ï Netsight Analyst
    - ï Cable Tester
- How To Analyze / Resolve Network Problems
- Trouble shooting specific protocol suites
  - » TCP/IP Network Utilities

    Note : These TCP/IP commands are available on both UNIX and with some variation on Windows NT (Windows NT version is discussed here)
  - » Some TCP/IP Trouble Shooting scenarios
  - » Example of transaction analysis (TCP/IP)

Objectives Of LAN Analysis

Better Utilization Of Resources

- Improve Performance and Response Times
- Improve Security
- Trouble Shooting

Other Uses

- Protocol Design
  - Distributions
  - Protocol Efficiency Analysis /Comparison

Some Definitions

- Utilization
  - » Ratio of actual number of bits transmitted to maximum total number of bits possible.
- Traffic
  - » Number of frames exchanged between source and destination pair.
- Throughput
  - » Number of frames passing through network.
- Delays
  - » Time taken to respond. Delays may be due to propagation times, device latencies, disk seek times
- Errors
  - » Incomplete frames resulting from collisions, called runts and stubs
- Interconnecting Devices
  - » Like Routers, Bridges and Gateways

Some Common Protocol Suites

- Higher layers
  - IPX / SPX
  - TCP/IP
  - NetBEUI
- DLC Layer Protocols
  - IEEE standards
  - DIX framing

Protocol Analyzers

Tools to analyze and trouble shoot network problems.

Å Examples:

- ï Software Analyzers:
  - » LANwatch by FTP software Inc..
  - » Netsight analyst.
- ï Software and Hardware Analyzers:
  - » LANvista by Digilog Inc..
  - » LANalyser by NOVELL.
  - » HP4972A test equipment by HP.
  - » Sniffer by Network General Corp..

Netsight Analyst

- Capturing packets
- Defining filters
- Address aliasing
- Generating traffic
- Trouble shooting

DEMO

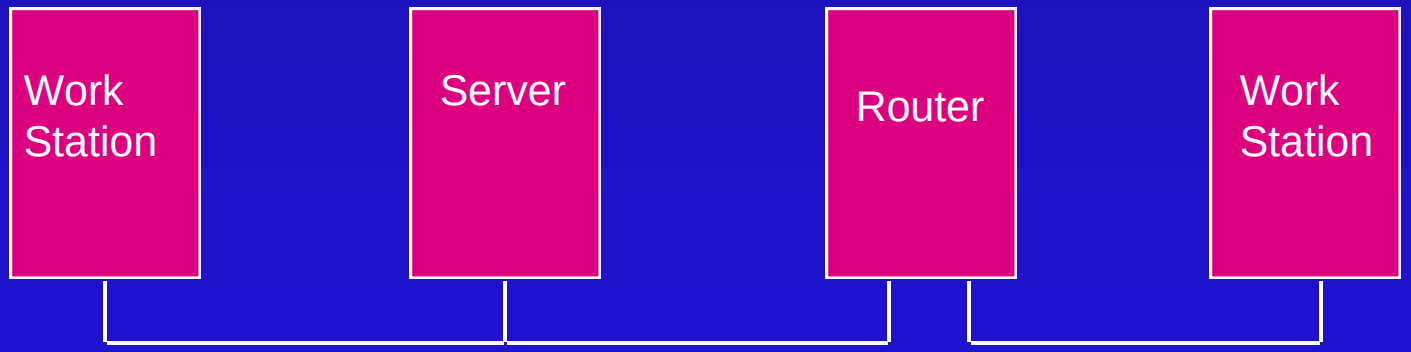
Netsight Analyst

Capabilities and usage

Performance Improvement

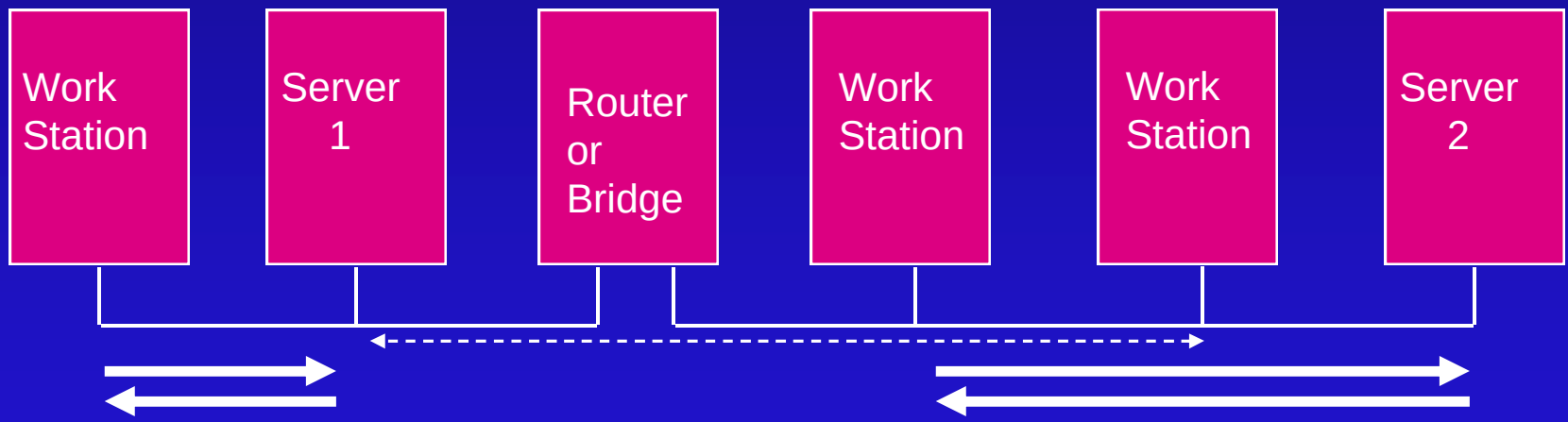
- Analyse network traffic loads and distribution on different segments
- Segregate traffic and establish preferred paths i.e. reorganize topology

This process is common to all protocols



mance Improvement (contd.)

- Analyze loads and distribution on different segments
- Segregate traffic and establish preferred paths

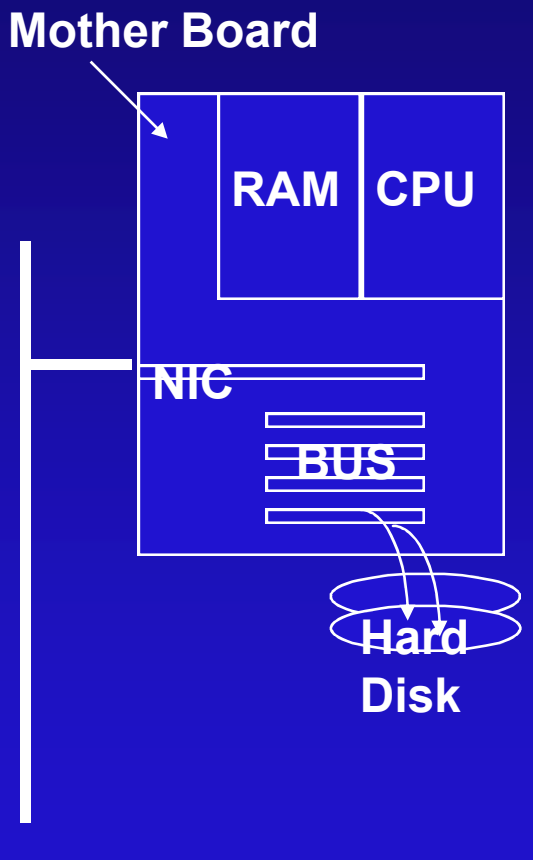


DEMO

Using Netsight Analyst to determine traffic flows and to determine best topology to minimize traffic flows in various segments

Performance Improvement

- Identify the bottleneck
- Factors affecting performance:
  - » CPU Speed
  - » Motherboard speed
  - » RAM
  - » Disk access
  - » I/O BUS
  - » NIC
  - » LAN cable bandwidth
  - » Operating system design / configuration
- Determine actual network bottle neck i.e CPU, interface, disk, cable etc. and improve it



DEMO

Using Netsight Analyst to determine average network response times (use Netsightôs timestamps) to identify bottleneck e.g. disk, cable, CPU etc.

(You must devise your own test on the basis of your understanding and resources available.)

Example: Compare results of multiple transfers of a small size file (perhaps a single byte) to that of multiple transfers of a very large file.

Note : The single file transfer will be serviced from the the serverôs cache (no disk access) but the large file transfer comes from the serverôs hard disk. Therefore you get some measure of the server hard disk response.

Improve Security

- Determine secure paths using :
  - » static routes
  - » filters
  - » firewalls
- Monitor network traffic to determine potential security loopholes

  Example use Netsight Analyst and configure ñtriggersò on certain types of transactions

Trouble Shooting

- Cable faults
  - » Breaks / kinks
  - » Line impedance
  - » Ground loops
  - » Below specification cabling
- Network Interface Card (NIC) faults
  - » Partial / complete failure
- Configuration errors
  - » Operating System / Protocol
  - » Interconnecting devices

DEMO

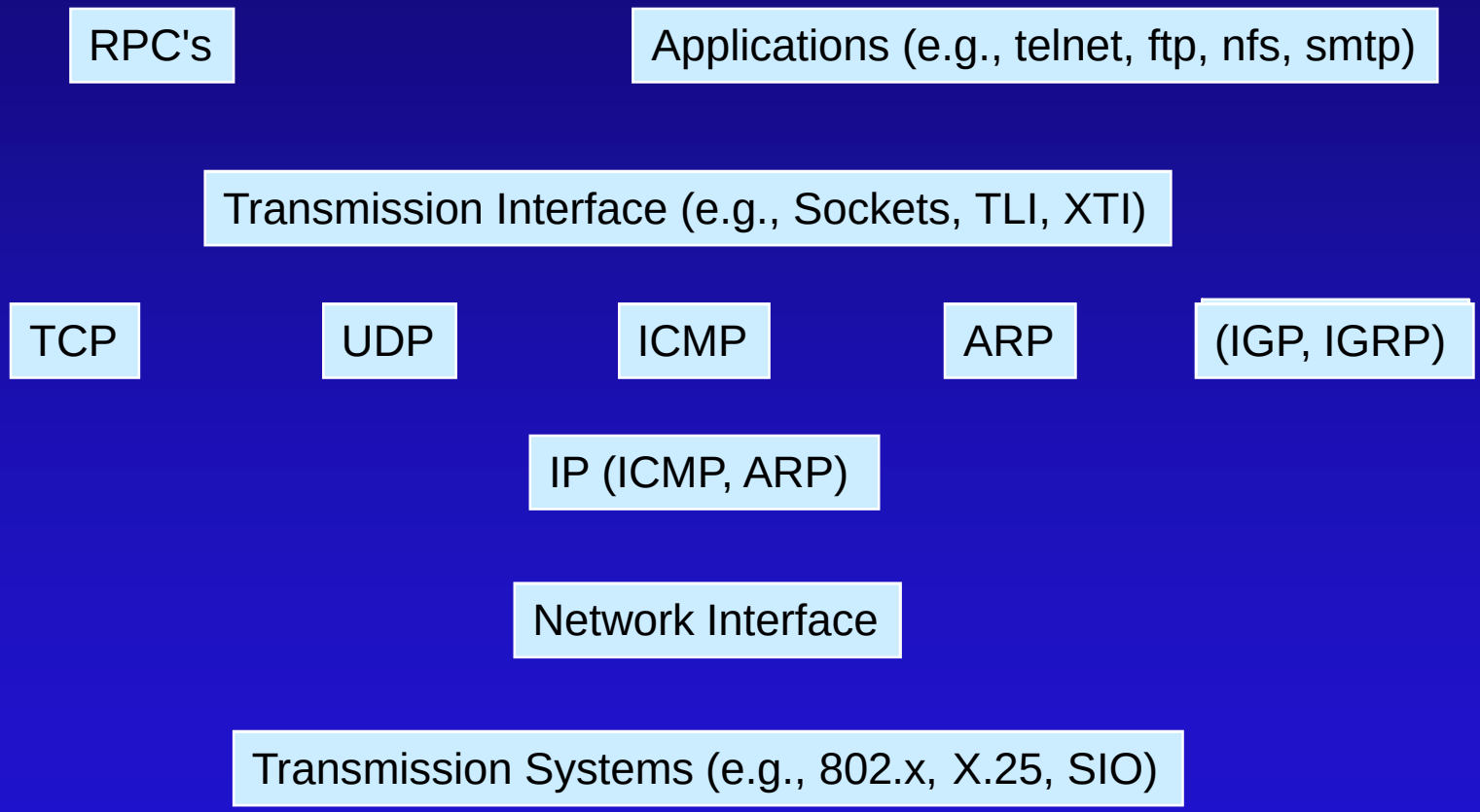
Using cable tester to cable integrity and specifications

Use NICôs diagnostic facilities (if available)

ble shooting specific protocol suites

- TCP/IP Protocol Suite
- TCP/IP Network Utilities

TCP/IP Protocol Suite



TCP/IP Protocol Suite (contd.)

Following is a one line description of the services that some of the TCP/IP protocols provide :

- **ARP** : Address resolution protocol is used to determine the Ethernet (physical) address based on the IP address
- **IP** : Is a Best Effort Datagram Delivery Service (corresponds to OSIûs network layer)
- **ICMP** : Internet Control Message Protocol is used by IP to pass control information
- **TCP** : Provides Reliable Stream Oriented delivery by using IP. (TCP corresponds to OSIûs transport layer)

TCP/IP Protocol Suite (contd.)

- **UDP** : Provides unreliable datagram delivery by using IP. (UDP also corresponds to OSIûs transport layer)
- **DNS** : Domain Name System is used to find the network layer or IP address of a machine from itûs name or alias

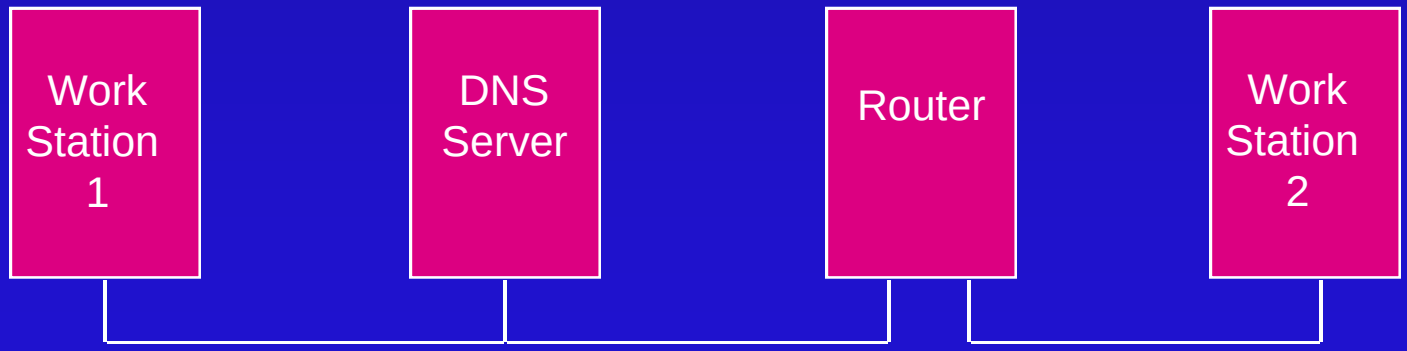
All the protocols in the TCP/IP suite co-operate to perform a communication task

- **Router** : Is a relay used to link two networks together at the network layer

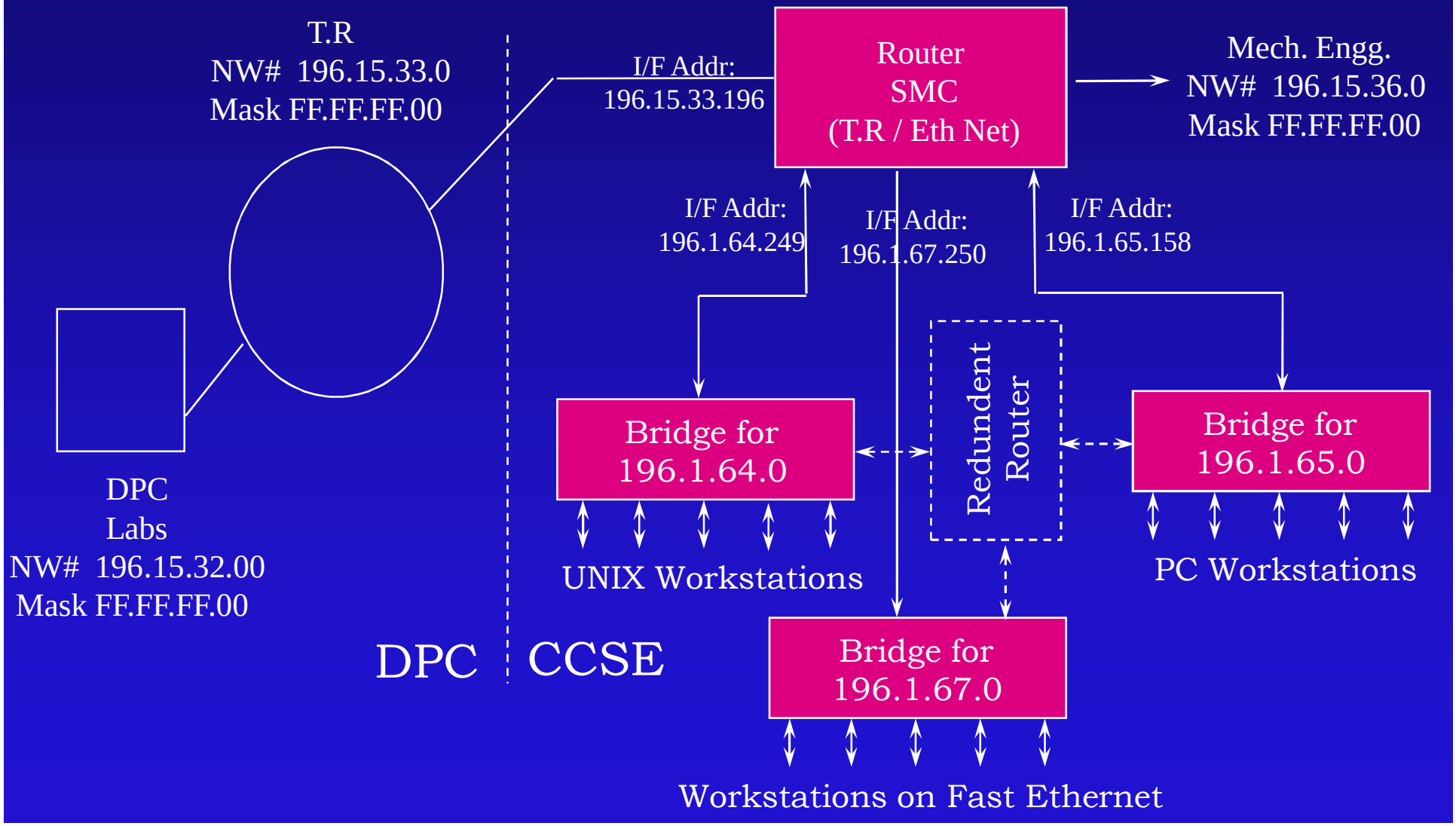
A TCP/IP Transaction

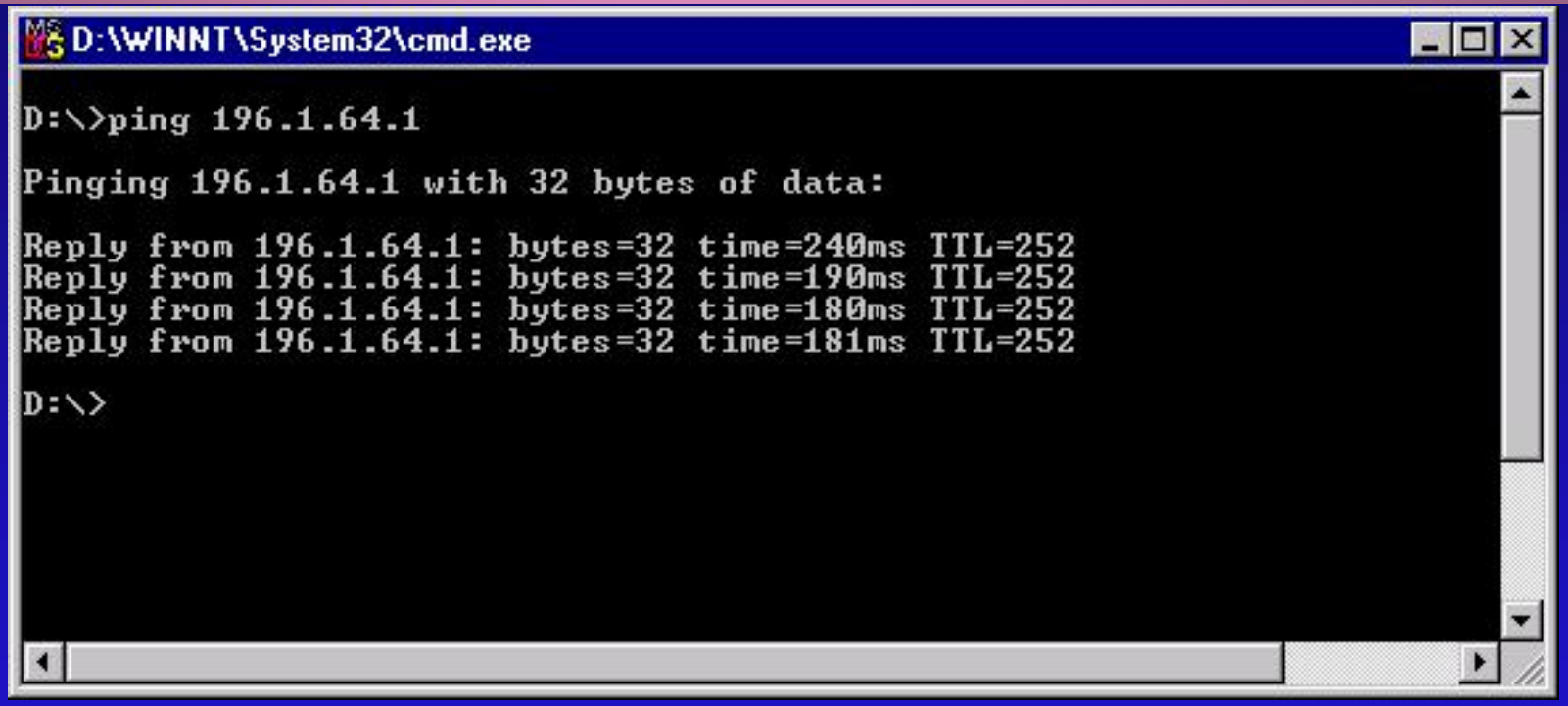
Workstation 1 wants to telnet to Workstation 2

- Workstation 1 sends an ARP request to ask EA of DNS server, which replies.
- Workstation 1 asks DNS server for Workstation 2ôs IP addr (DNS protocol), which replies.
- Workstation 1 sends an ARP to ask EA of router if EA of router is not available in ARP cache.
- Workstation 1 sends data frame for Workstation 2 to router.
- Router sends an ARP to ask EA of Workstation 2.
- Router sends Workstation 1ós data to Workstation 2.



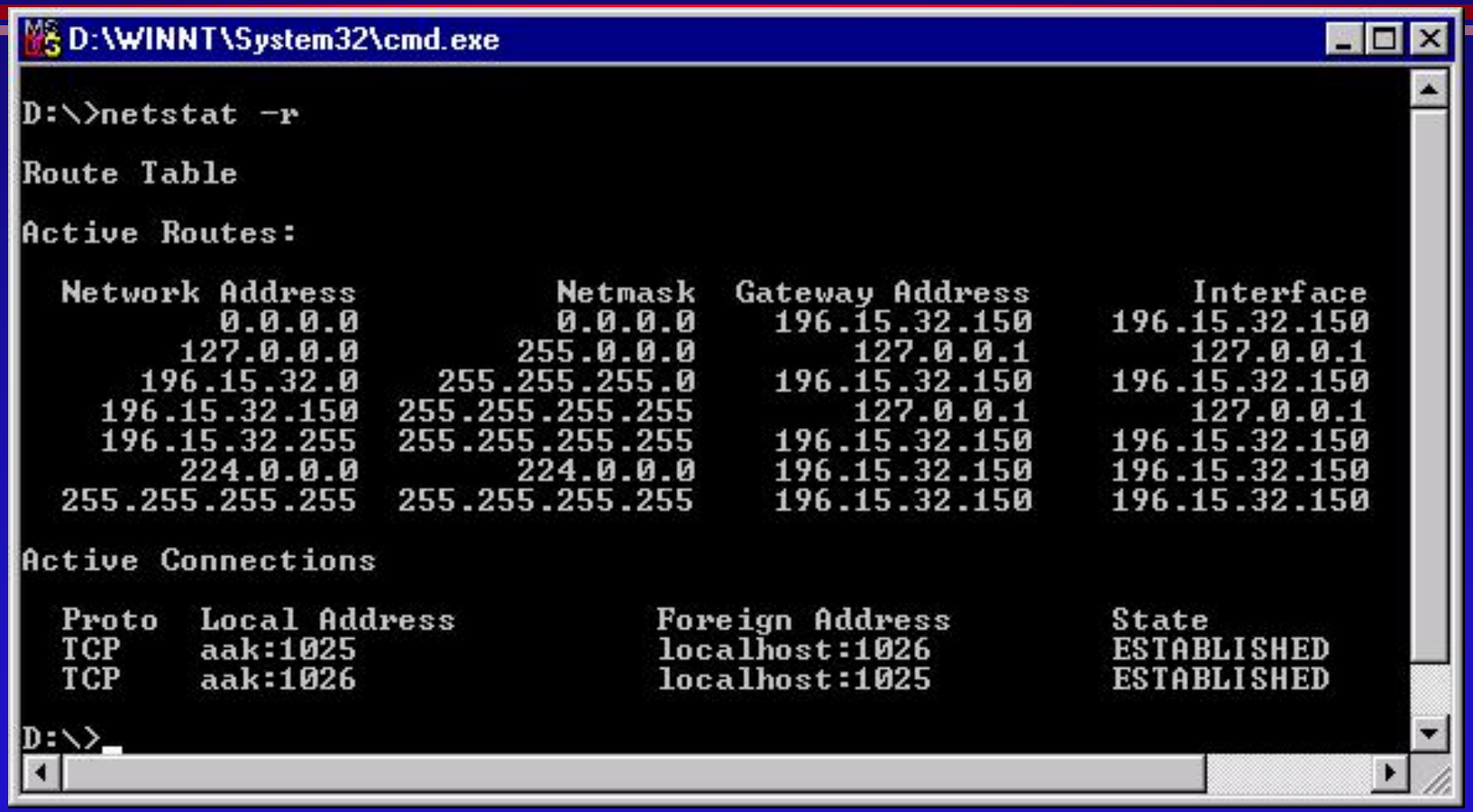
CCSE Network IP Addresses





- ping hostname (or IP address)
  - » Sends ICMP Echo_Request and expects Echo_Reply : Tests connectivity, routing, delay

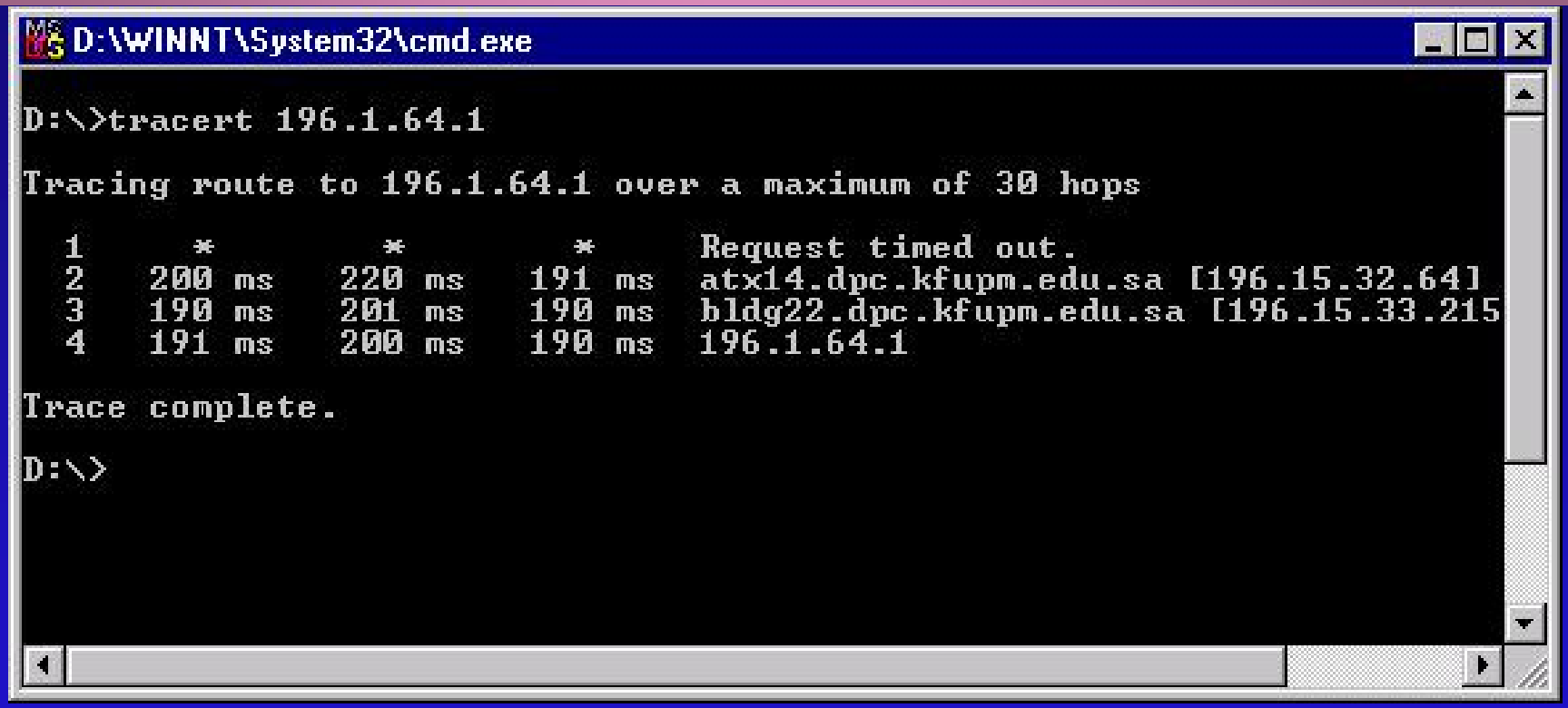
TCP/IP Utilities : netstat



- netstat (option)
  - » Used to query network subsystem for information

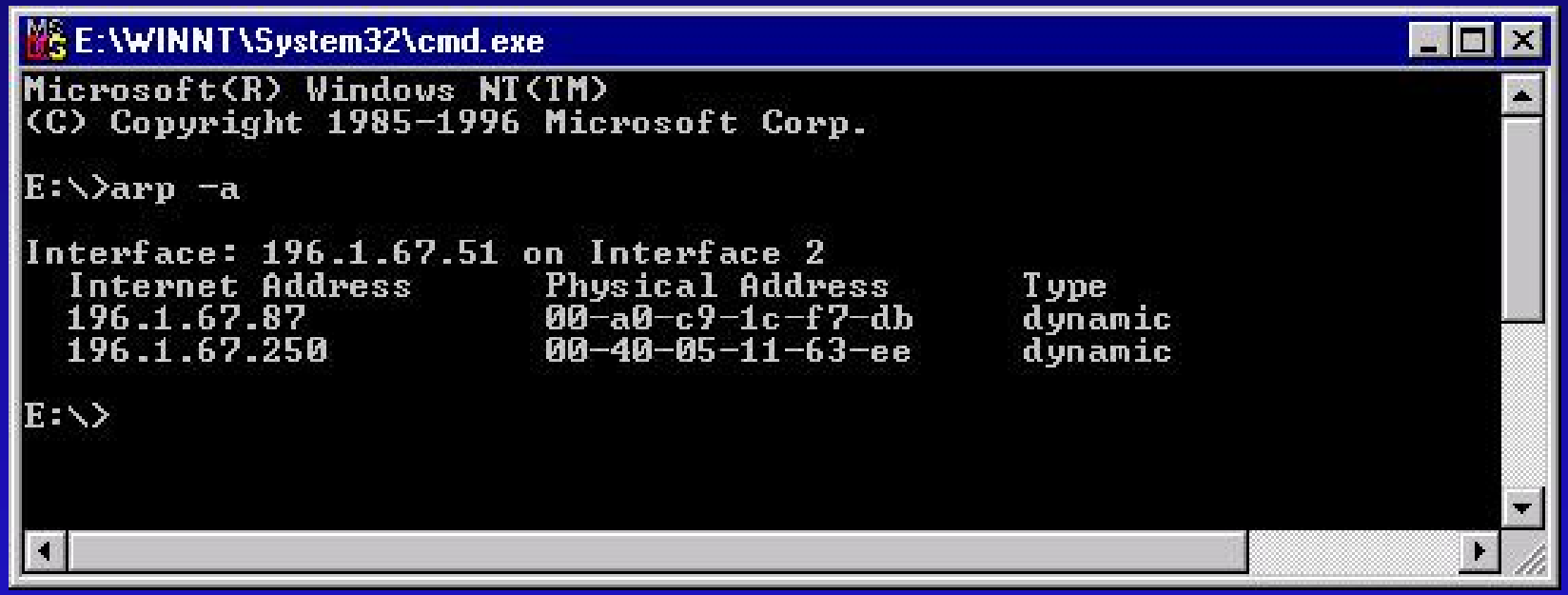
Options: -i : interface, -a : all sockets, -r : routing table, -m : memory allocation

TCP/IP Utilities : tracert



- Tracert (options) destination [pktsize]
  - » Traces route taken by packets, generates ICMP Time_Exceeded (TTL) from all gateways in the path
  - » options: -n : numeric, -s : src addr, -r : route

TCP/IP Utilities : arp



- arp (options)
  - » Address resolution display and control program
  - » Used to manage ARP cache entries i.e. delete, add etc.
  - » options: -a, -d h_name, -s h_name eth_addr

Interface Configuration

- ifconfig
  - » Used to configure all interfaces except SLIP & PPP interfaces. Sets IP address, broadcast address, netmask, interface UP / DOWN, debug

Syntax:

ifconfig interface addr-fam address parameters

This is a UNIX only command. Only superuser can execute ifconfig

Problem Resolution

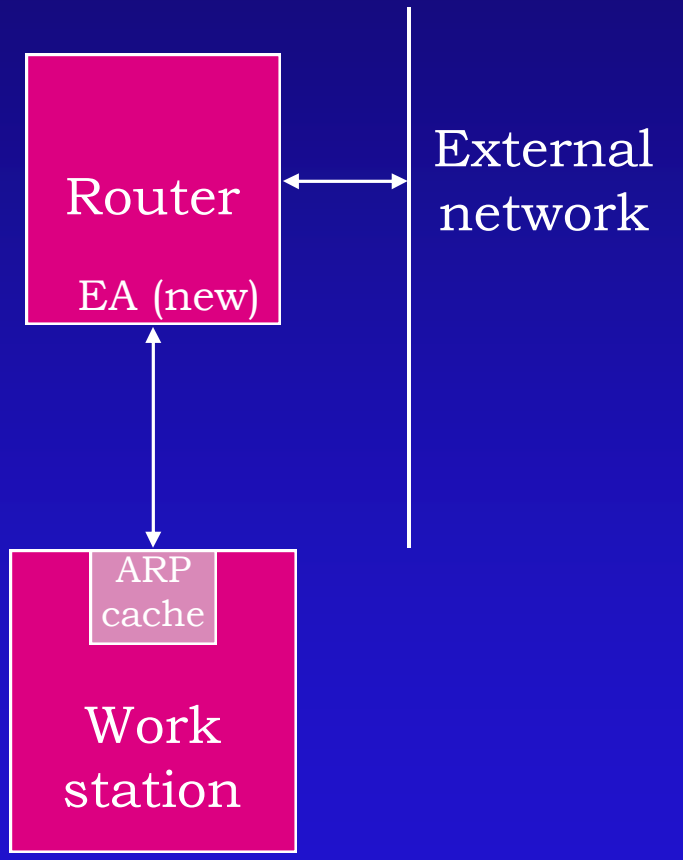
- Expected behavior of protocol MUST be known to troubleshoot
- Use TCP/IP utilities to isolate fault
- When all else fails use transaction analysis:
  - » Problem Resolution consists of recording erroneous transaction and then comparing with expected behavior to isolate fault
- Different implementations of protocols behave (slightly) differently

Assumption : In following slides it is assumed that there are no link level problems

Trouble Shooting Scenario 1

- You just replaced a software router with a new hardware device. Maintaining all the old configuration parameters. On testing the new system you find communication failure.

- Possible cause: Old Ethernet and IP address pair in ARP cache.
- Use arp utility to delete old entry ARP cache



Trouble Shooting Scenario 2

- Normal ping returns good response times but actual file transfer takes much longer
- Possible cause:

  Some network in the path does not support the MTU size you are using, forcing fragmentation or a different route.
- Use ping or tracert with different frame sizes to analyze the situation

Trouble Shooting Scenario 3

- Sometimes a remote system becomes too slow or even the connection is lost
- Possible cause:

  Your packets are being discarded by some intermediate gateway (during high load times).
- Use tracert to find out

Where to Obtain Information

- Magazines
- Books
- RFCs (Request for Comment)