Computer Measurement Group 2001

TCP/IP Basics For The IS Professional

Michael S. Recant
MGS, Inc.

MGS INC
Computer Business Solutions

Introduction

- MGS, Inc. - a small consulting and software development firm in the Unisys ClearPath market space
- We extensively use network communications to solve our business problems
- This presentation is based on our actual experiences from 1993 until today

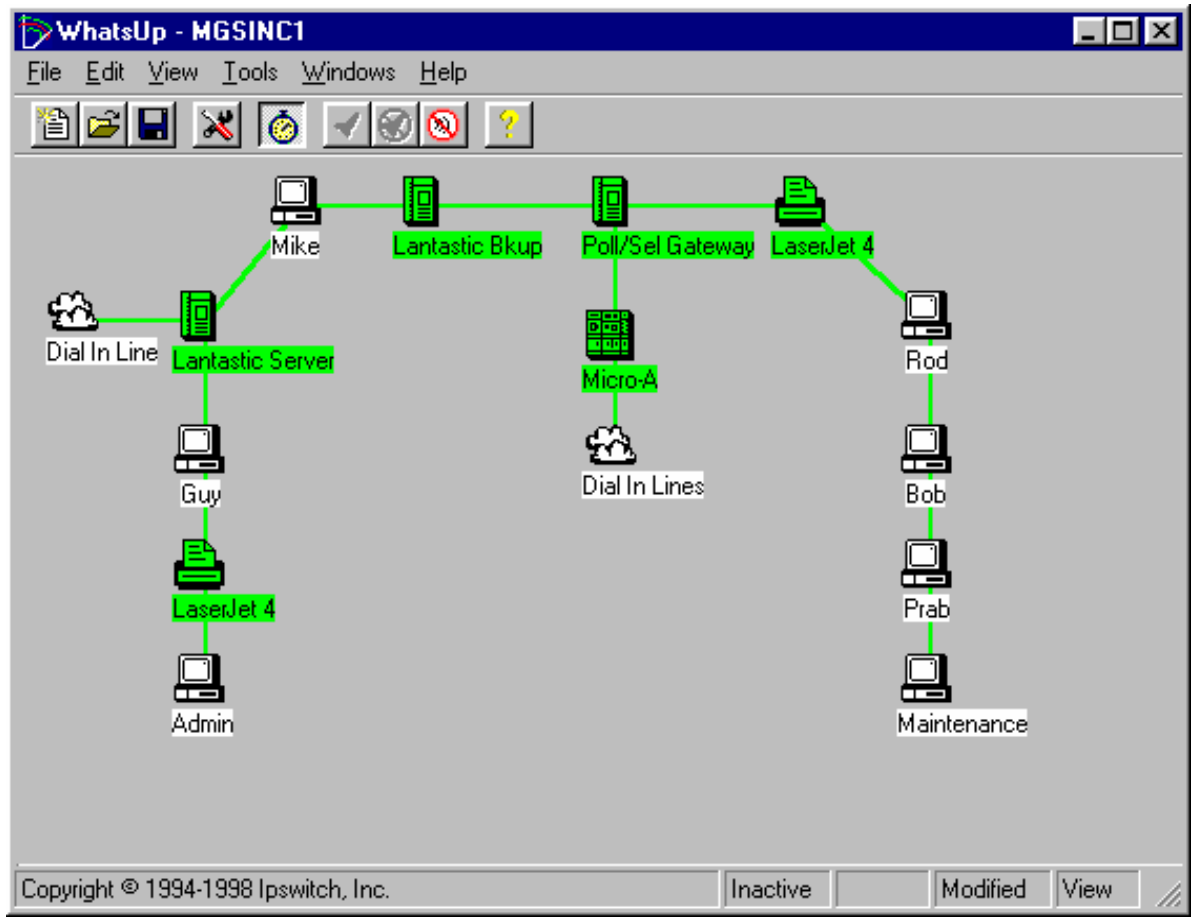
MGS INC
Computer Business Solutions

MGS Network - Requirements

- Required services
  - File/Print sharing
  - Unisys mainframe access
  - Electronic mail
  - Remote Access
  - ***Reliability***
- Standard software products (no programming)
- Limited administration time
- Low-to-moderate cost

MGS INC
Computer Business Solutions

MGS Network - 1993



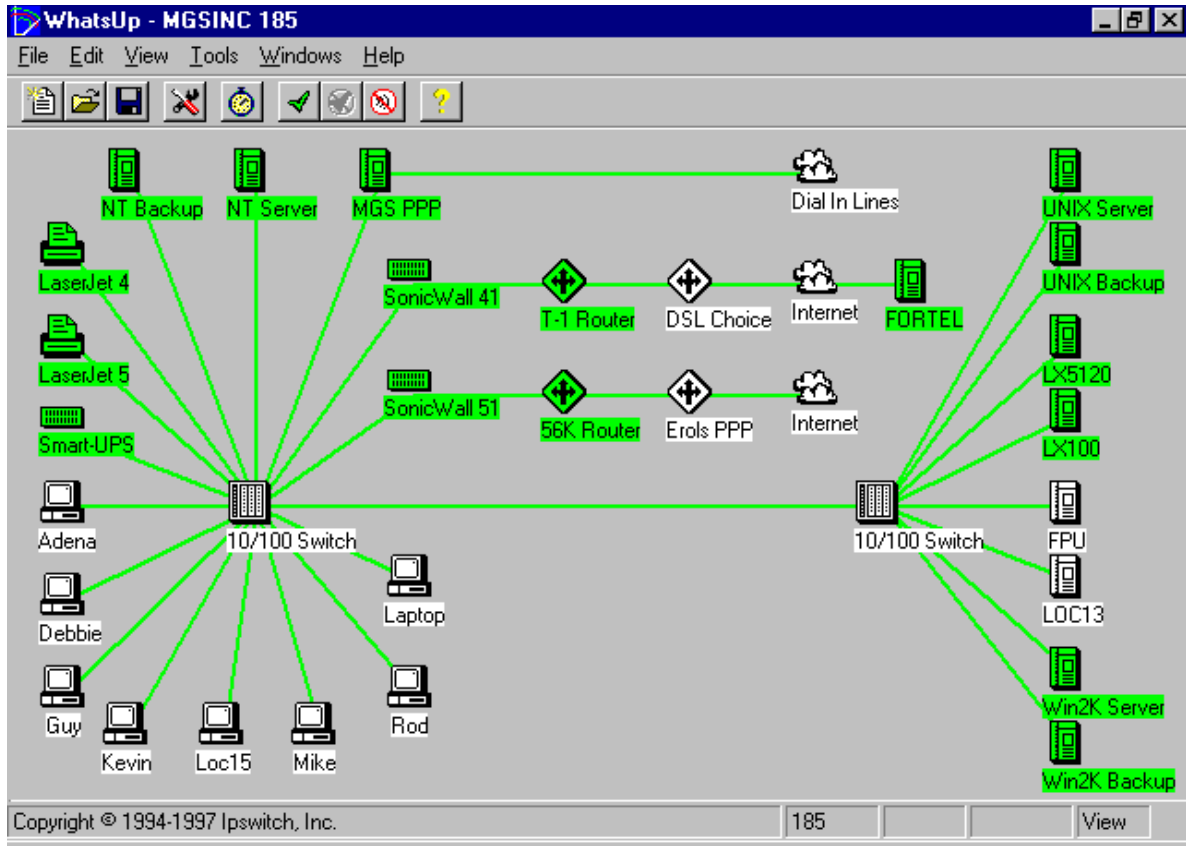
MGS INC
Computer Business Solutions

MGS Network - 1993

- DOS/Win 3.1, DOS/LANtastic
- Services
  - Unisys mainframe access
  - File/Print sharing
  - Limited dial-in access (direct to server/mainframe)
  - Electronic mail (dial out to CompuServe)
- No Internet
- Minimal redundancy

MGS INC
Computer Business Solutions

MGS Network - 2001



MGS INC
Computer Business Solutions

MGS Network - 2001

- Win9x, Win NT/2K, BSDI UNIX
- Services
  - Unisys mainframe access
  - File/Print sharing
  - “Generic” dial-in access
  - Electronic mail
  - Internet access (in & out)
  - WEB and FTP
  - Virtual Private Network
  - DNS and Time
- Fully redundant capabilities

MGS INC
Computer Business Solutions

MGS Network - 2001

- How can a small company do all this?
  - Simple/reliable hardware
  - Software with integrated advanced communications capabilities
  - High speed wide-spread connectivity
  - Commodity pricing
  - ***Unparalleled communication standards*** *(like TCP/IP)*

MGS INC
Computer Business Solutions

What is TCP/IP and Where Did It Come From?

- Designed as part of an effort by the military to develop robust, reliable vendor-independent data communications
- Standards published as Request for Comment (RFCs)
- You can download RFCs for all the protocols discussed in this presentation from:

http://www.cis.ohio-state.edu/Services/rfc/index.html

What is TCP/IP and Where Did It Come From?

- TCP/IP and Internet history
  - 1969 - ARPANET research started
  - 1975 - ARPANET made operational
  - 1983 - TCP/IP added to BSD UNIX
  - 1983 - Term Internet is first used
  - 1989 - Most major US/Canadian Universities
  - 1992 - Most countries inter-networked
  - 1994 - Commercial use takes over the Internet
  - 1995 - Microsoft integrates TCP/IP into Windows
  - 1998 - TCP/IP surpasses IPX/SPX as the most common network protocol

What is TCP/IP and Where Did It Come From?

- TCP - Transmission Control Protocol
  - Breaks application data streams into packets
  - Insures reliable delivery of packets in the correct order
  - Does data stream Re-assembly
- IP - Internet Protocol
  - Packet based
  - Implements the network addressing scheme
  - Packets are routable
  - The networking layer for the Internet

MGS INC
Computer Business Solutions

TCP/IP Communication - Architecture

- Based on the 7 level OSI Model
  - Application
    - OSI Application
    - OSI Presentation
  - Network
    - OSI Session
    - OSI Transport
    - OSI Network
  - Link
    - OSI Data link
    - OSI Physical

TCP/IP Communication - A Layered Implementation

- Application data (business)
  - User Information
- Application Protocol (service)
  - Telnet, HTTP,FTP
- Network Session (connection)
  - TCP, UDP, ICMP
- Network (packet movement)
  - IP (vs IPX, NetBEUI)
- Link (physical transport)
  - Ethernet, ATM, FDDI

MGS INC
Computer Business Solutions

TCP/IP Communication - The Link Layer

- Supported by a variety of physical transports
- Most frequently used
  - Ethernet (IEEE 802.3)
  - Serial Port (PPP)
- Network topologies dependant on hardware
  - 100BaseT star
  - ThinNet bus
  - Token Ring ring
  - PPP point-to-point
- Link layer encapsulates the IP packet

TCP/IP Communication - The Networking Layer

- Provides Connection (TCP only)
- Breaks the data stream down into small packets (TCP only)
- IP packet encapsulates the higher layers
  - Application protocol
  - Application data
- Provides logical addressing
- Provides packet routing

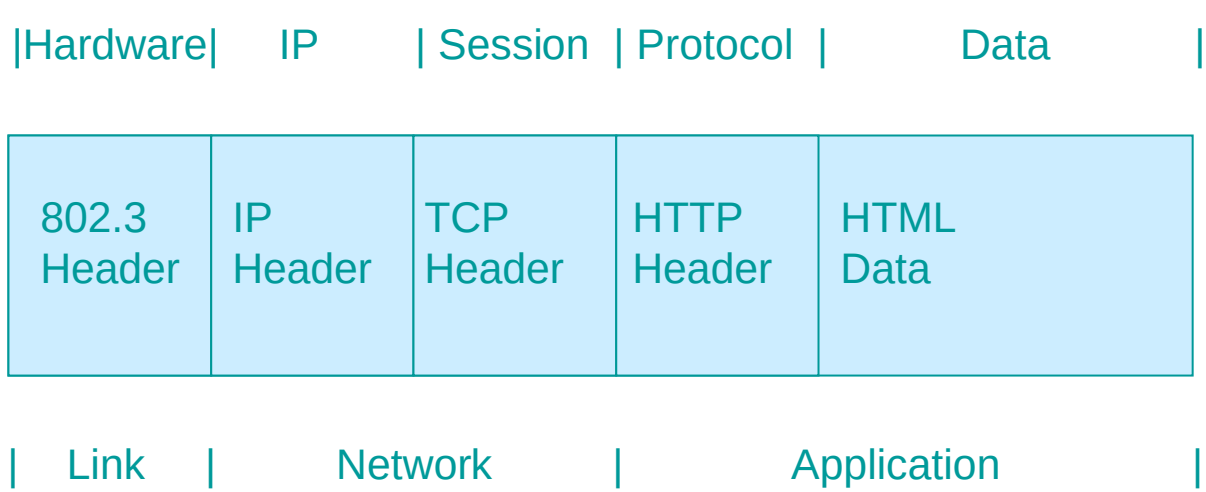
MGS INC
Computer Business Solutions

TCP/IP Communication - The Application Layer

- Application programs use the system's TCP/IP interface
  - BSD Sockets (UNIX)
  - Winsock (Windows)
- Application level processing
  - Service - message communication based on an application-to-application protocol
  - Data - business information communicated using the Service

TCP/IP Communication - Example Packet

- Typical Communications Packet



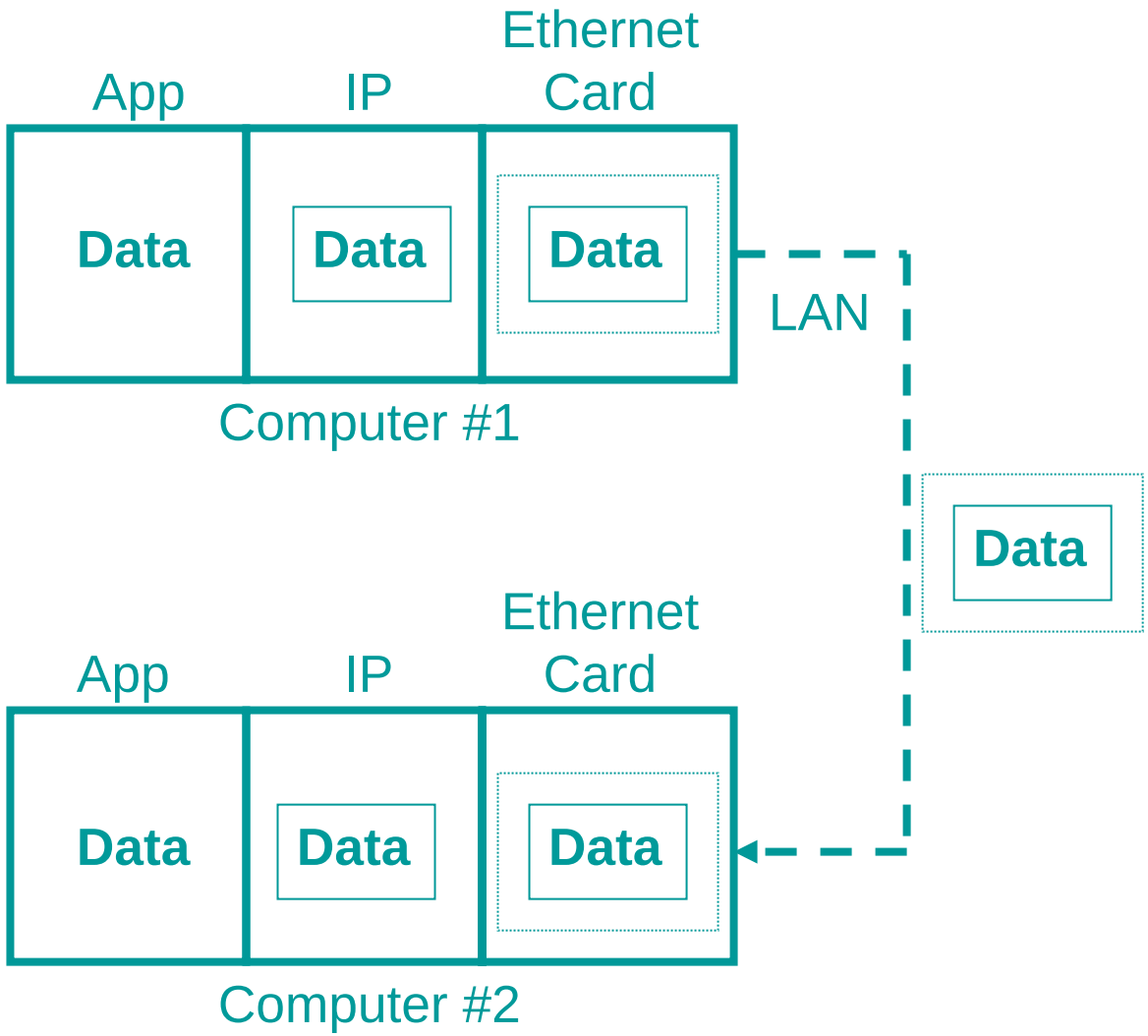
MGS INC
Computer Business Solutions

IP Communication - Overview

- IP implemented based on a Packet Concept
- Physical transport independent architecture
- Unreliable and connectionless (at this layer)
- Routable
- Superior to older protocols (Novell IPX, Microsoft NetBEUI)

MGS INC
Computer Business Solutions

IP Communication - Example



MGS INC
Computer Business Solutions

IP Addressing - Overview

- Not associated with hardware
- 32-bit Unique Host Address
- Dotted-decimal Notation: nnn.nnn.nnn.nnn (where nnn is 0 to 255)
- Represents a combined LAN number and HOST number
- HOST 0 refers to the entire LAN
- HOST all-bits-on (example 255) is for broadcast to all hosts

IP Addressing - Address Conventions

- IP Address Class Ranges
  - Class A - 1.n.n.n to 127.n.n.n
  - Class B - 128.n.n.n to 191.n.n.n
  - Class C - 192.n.n.n to 223.n.n.n
- IP Address Class Sizes
  - Class A - 16,777,216 addresses
  - Class B - 65,636 addresses
  - Class C - 256 addresses
- Special IP Addresses
  - Loop back - 127.0.0.0 to 127.255.255.255
  - Private
    - 10.0.0.0 to 10.255.255.255
    - 172.16.0.0 to 172.31.255.255
    - 192.168.0.0 to 192.168.255.255

IP Addressing - Where does it come from?

- LAN numbers are assigned by the Internet Network Information Center (InterNIC)
- LAN numbers are unique within the Internet
- Host numbers are are assigned by local network administrator
- Host numbers are unique within a LAN
- IP Address is always paired with an associated Network Mask

IP Addressing - Networks of Addresses

- IP address has two parts:
  - LAN Number
  - Host Number
- LAN Number calculated by:

  (IP Address **AND** Network Mask)
- Host Number calculated by:

  (IP Address **AND NOT**(Network Mask))
- Example:

  IP Address: 172.31.1.25
  Network Mask: 255.255.255.0
  LAN Number: 172.31.1.0
  Host Number: .25

MGS INC
Computer Business Solutions

IP Addressing - Setting The Host IP Address

- Manually: by setting IP Address and Network Mask
- Automatically: by Dynamic Host Configuration Protocol (DHCP)
- DHCP requires one or more DHCP servers provisioned with the available IP Address ranges

IP Addressing - Private LAN Addressing

- A Private LAN is where the LAN is not connected to the Internet
- Technically any IP Address range can be used but one of the InterNIC “private” LAN numbers is recommended
- Often used for isolated Intranets
- When used with NAT, simplifies changing your company’s Internet IP Address range

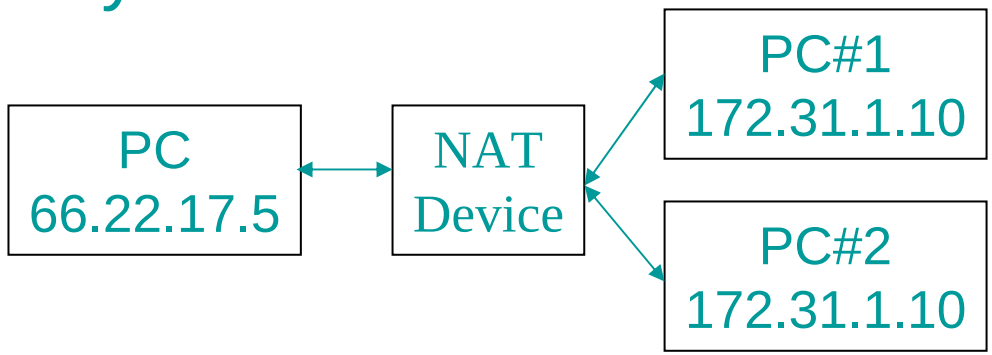
IP Addressing - Network Address Translation

- Referred to as NAT
- Maps Internet IP Addresses to Private LAN IP Addresses
- Many-to-one NAT
  - Maps many private LAN IP Addresses to a single Internet address
  - Limited use for Servers
- One-to-one NAT
  - Maps one private IP Address to one Internet IP Address

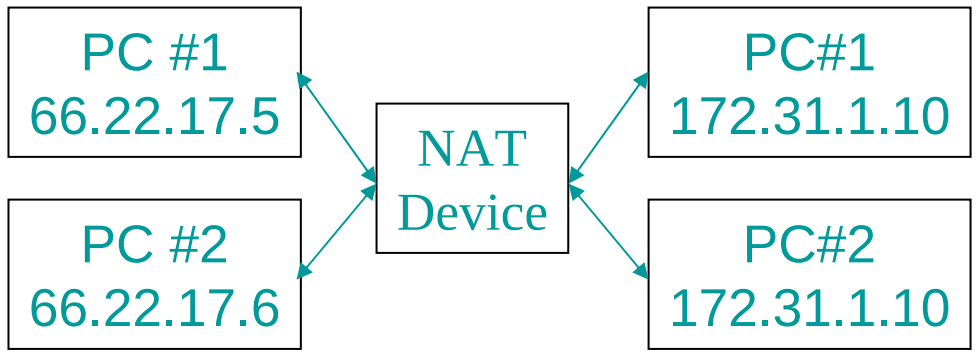
MGS INC
Computer Business Solutions

IP Addressing - Network Address Translation

- Many-to-one NAT



- One-to-one NAT



MGS INC
Computer Business Solutions

IP Communication - Local-LAN

- Communication protocol used when the destination is on the same LAN
- Address Resolution Protocol (ARP) maps IP Address to hardware address
  - IP Address in ARP table?
  - Broadcast ARP-request
  - Receive ARP-reply with both IP Address and associated MAC hardware address
  - Store ARP-reply in ARP table
  - Send packet to responder MAC address

IP Communication - Off-LAN Routing

- Communication protocol used when the destination is on a different LAN
- A routing table is used to define paths to Off-LAN IP Addresses
- All Off-LAN routes are defined in the Host's routing table
- Routing table identifies IP address of the router associated with a route

MGS INC
Computer Business Solutions

IP Communication - Off-LAN Routing

- Automatic updates received from routers on the LAN
- A default routing entry is needed to send off-LAN packets to unknown routes (Internet)
- Manual entries can entered in the routing table to deal with complex topologies

IP Communication - Summary

- Only three settings are required for successful communications
  - IP Address
  - Network Mask
  - Default Router
    (only needed for off-LAN traffic)
- DHCP can set all three automatically

MGS INC
Computer Business Solutions

IP Communications - Connecting to the Internet

- Internet Service Provider (ISP)
- Provides physical connectivity
  - PPP (28-56 Kbaud)
  - ISDN / IDSL (128 Kbaud)
  - SDSL (384 to 768 Kbaud)
  - T1 (1 Mbaud)
  - Cable Modem (1-3 Mbaud)
- Provides logical connectivity
  - Floating IP Address
  - Fixed IP Address
  - Range of fixed IP Addresses
- Note that providing a service requires a fixed IP Address

IP Communications - Connecting to the Internet

- There are critical security issues to be addressed before putting any server on the Internet
- ISPs can provide additional customer services
  - DNS
  - Mail
  - News
  - WEB

MGS INC
Computer Business Solutions

IP Communication - Additional Capabilities

- Internet Control Message Protocol (ICMP)
  - IP communication service messages like PING, TRACEROUTE and ROUTER
- Internet Group Message Protocol (IGMP)
  - IP communications based on multicasting (sending to groups of hosts)

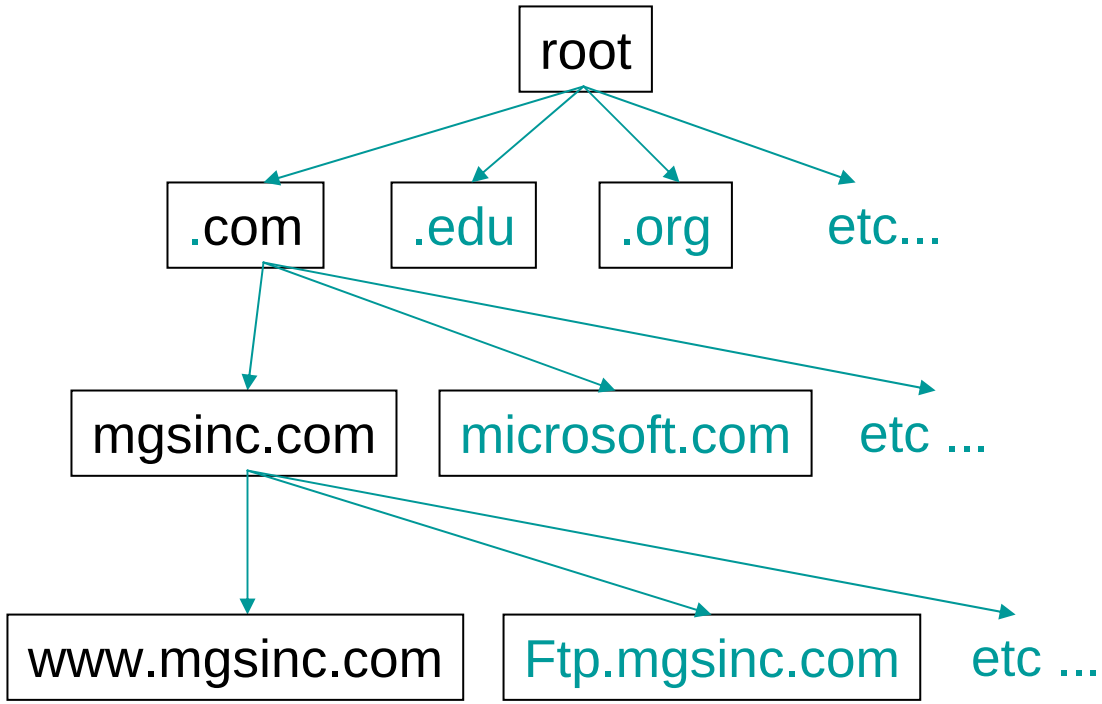
The Domain Name System - DNS

- The Domain Name System insulates applications from specific IP Addresses
- Format: host.domainname.domain
- “domainname.domain” assigned by InterNIC
- “host” assigned by network administrator and designates a specific computer
- “host” can be a multi-level name

  aaa.bbb.domainname.domain

MGS INC
Computer Business Solutions

The Domain Name System - DNS Tree



MGS INC
Computer Business Solutions

The Domain Name System - DNS Domain Entry

Registrant: MGS, Inc (MGSINC-DOM)
10901 Trade Road, Suite B
Richmond, VA 23236, USA

Domain Name: MGSINC.COM

Record last updated on 21-Jun-2001.
Record expires on 29-Mar-2010.
Record created on 28-Mar-1995.
Database last updated on
13-Sep-2001 01:15:00 EDT.

Domain servers in listed order:

NS1.MGSINC.COM	64.23.177.43
NS2.MGSINC.COM	208.58.172.236
NS3.MGSINC.COM	24.7.183.76

MGS INC
Computer Business Solutions

The Domain Name System - DNS Servers

- Provides service to convert domain names to IP Addresses
- If necessary, it goes back to the InterNIC “root” server for info
- DNS tables are maintained by the site’s network administrator
- Can provide both Forward DNS and Reverse DNS
- May cache name/IP Address association for a period of time

MGS INC
Computer Business Solutions

The Domain Name System - DNS Resolver

- Client software which requests a DNS Server to resolve name
- All systems running TCP/IP run a resolver
- DNS Server(s) IP Address must be specified to the resolver

IP Based Services - Overview

- Services are built on top of IP networking
- Services use TCP/IP Sessions
  - TCP
  - UDP
- Services are addressed by:
  - Host name or IP Address
  - Port number
- Service protocols also defined by RFC standards
- These are Different from Microsoft Networking Services

IP Based Services - Overview

- TCP/IP Applications have the responsibility for the following
  - Establishing the application-to-application connection
  - Operating the Service protocol
  - Identifying where messages start/end based on the Service protocol
  - Processing the data in the message(s)

IP Based Services - Sessions

- TCP/IP supports two types of application-to-application sessions
- User Datagram Protocol (UDP)
  - No reliability, no message ordering
  - Connectionless data path
  - Application must fragment messages
  - Specify Hostname and Port
- Transmission Control Protocol (TCP)
  - Reliable
  - Automatic message fragmentation
  - Single connection data path
  - Specify Hostname and Port

IP Based Services - Services

- A server can offer (run) one or more TCP/IP services
- Each service uses a specific protocol over a specific TCP/IP Port
  - Ports 1-1023 are reserved as well known ports
  - Only authorized applications should use the well known ports
  - All ports above 1023 can be used by normal applications

IP Based Services - Services

- The documented well known port numbers can be found at:

  http://www.iana.org/assignments/port-numbers

- Common IP based services
  - Telnet - Terminal
  - FTP - File Transfer
  - LPD/LPR - Printing
  - SMTP/POP3 - Electronic Mail
  - HTTP - Web
  - Misc. Service Protocols

IP Based Services - Telnet - Terminal Interface

- Provides traditional terminal access
- The client and server can negotiate the terminal characteristics
- Typical implementation uses clear-text password for logon
- Capabilities and characteristics are specific to the server operating system

IP Based Services - FTP - File Transfer

- Provides both text and binary file transfer
- Client can connect either on an Anonymous basis or can use a defined UserID/Password
- Note that the password is sent as clear-text.
- File access is controlled through the server operating system's permissions

MGS INC
Computer Business Solutions

IP Based Services - LPD/LPR - Remote Printing

- Provides remote printing services in both directions
  - LPD Server (incoming)
  - LPR Client (outgoing)
- The following specifications are needed to connect an LPR client to an LPD server printer
  - Host name or IP Address
  - Port number (well known port 515)
  - Printer name

MGS INC
Computer Business Solutions

IP Based Services - SMTP/POP3 - Mail Services

- Provides electronic mail services
- SMTP (send mail) is used to transmit an email
- POP (receive mail) is used to acquire a received email
- There are alternate services for managing receipt of email sent via SMTP
  - IMAP
  - WEB based email

MGS INC
Computer Business Solutions

IP Based Services - HTTP - Web Services

- Provides Web services
- The HTTP command structure allows the browser client to request information
- The Web server responds by either retrieving the requested file or invoking execution of the requested program or script
- The information sent back to the client may contain elements that will execute on the client

IP Based Services - Service Protocols

- SNMP
  - Simple Network Management Protocol
  - The service is used to provide status and usage information about a server
  - Information is provided in a generic data structure called a MIB
- Echo
  - Echoes every character sent
  - Useful for confirming speed and reliability of a TCP/IP data path
- Time
  - Used to synchronize a server's clock to a standard source

Network Management - Proxy Servers

- Proxy Servers “front end” servers providing well known services
- Requests are forwarded to the real server for processing
- Benefits
  - Security
  - NAT
  - Data caching
  - Workload distribution
- Problems
  - Slows performance (bottleneck)
  - Client may require knowledge of proxy

Network Management - Security - General

- Don’t just put your corporate servers on the Internet
- Only allow Internet access to specific services on a specific system
- Limit to access from fixed locations if possible (not the whole Internet)
- Audit ***ALL*** Internet access

MGS INC
Computer Business Solutions

Network Management - Security - Firewalls

- Firewalls
  - Restrict access to/from a LAN
  - Limit packets based on packet type, IP Address and port, or service
  - Software like Microsoft Proxy Server
  - Black-box like SonicWALL
- Guidelines
  - Allow connections from internal systems to systems on the Internet
  - Allow connections from systems on the Internet to “public” services (Web, SMTP)
  - Minimize or eliminate connections from systems on the Internet to non “public” services

Network Management - Security - VPN

- Virtual Private Networking
  - Provides a secure, private path from a workstation to the servers on your LAN, through the Internet or an Intranet
  - Works in a similar fashion to a dial-in PPP connection to your LAN
  - Requires special workstation software
  - Needs a Path through through Firewall on a known port
  - Needs both logon security and data encryption
  - VPN Client/Server acts like two routers that use IP/Internet for “physical communication” rather than a private phone connection

Network Management - Reliability

- Internet IP Communication
  - Redundancy must come from your ISP
  - Multiple-ISP redundancy is difficult (IP Addresses change)
- Workstations
  - NAT makes switching LANs transparent by insulating the workstation from the Internet IP address
- Services
  - TCP/IP Services have limited built-in reliability
  - Only DNS and MAIL have fail-over designed into the protocols

MGS INC
Computer Business Solutions

TCP/IP Diagnostic Tools - Overview

- Useful Diagnostic Utility Programs
  - Ping
  - TraceRoute
  - Microsoft WinIPCfg & IpConfig
  - Microsoft NetMON
  - IPSwitch WhatsUp
  - IPSwitch WS_Ping ProPack

TCP/IP Diagnostic Tools - Ping

- Always use to confirm basic end-to-end communication

```
[C:\] PING WWW.CMG.ORG

Pinging CMG.ORG [209.66.0.64] with 32 bytes of data:

Reply from 209.66.0.64: bytes=32 time=54ms TTL=241
Reply from 209.66.0.64: bytes=32 time=54ms TTL=241
Reply from 209.66.0.64: bytes=32 time=39ms TTL=241
Reply from 209.66.0.64: bytes=32 time=38ms TTL=241

Ping statistics for 209.66.0.64:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 38ms, Maximum =  54ms, Average =  46ms
```

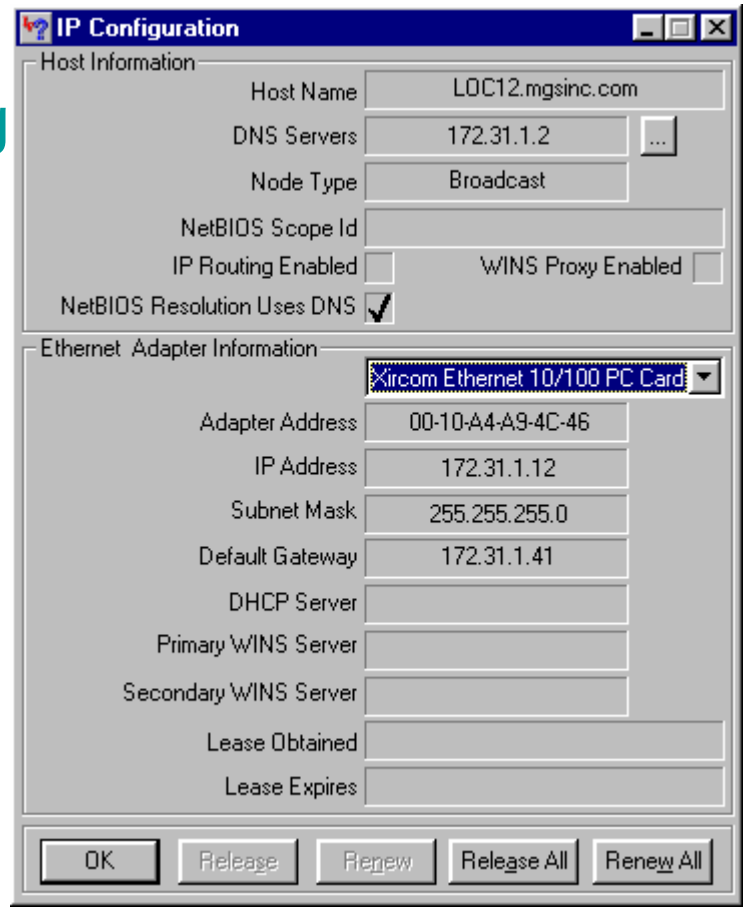
TCP/IP Diagnostic Tools - TraceRoute

- Use to check the path through which packets are routed

```
[C:\] tracert www.fortel.com
Tracing route to www.fortel.com [207.217.96.33]
 1     8 ms     4 ms     4 ms  gateway.mgsinc.com [66.22.17.1]
 2    21 ms    18 ms    19 ms  66.22.7.1
 3    20 ms    18 ms    20 ms  fe1-0crva003.volocom.net [207.233.168.6]
 4    18 ms    19 ms    19 ms  core2.washington1.level3.net [209.244.11.45]
 5    20 ms    19 ms    18 ms  washington1.level3.net [209.247.10.77]
 6    82 ms    83 ms    84 ms  losangeles1.level3.net [64.159.1.126]
 7    86 ms    84 ms    84 ms  hsipacc1.losangeles1.level3.net [209.244.2.98]
 8    86 ms    83 ms    83 ms  unknown.level3.net [209.245.88.34]
 9    85 ms    84 ms    83 ms  neteng.itd.earthlink.net [207.217.2.29]
10    84 ms    83 ms    84 ms  www.fortel.com [207.217.96.33]
Trace complete.
```

TCP/IP Diagnostic Tools - WinIPCfg and IpConfig

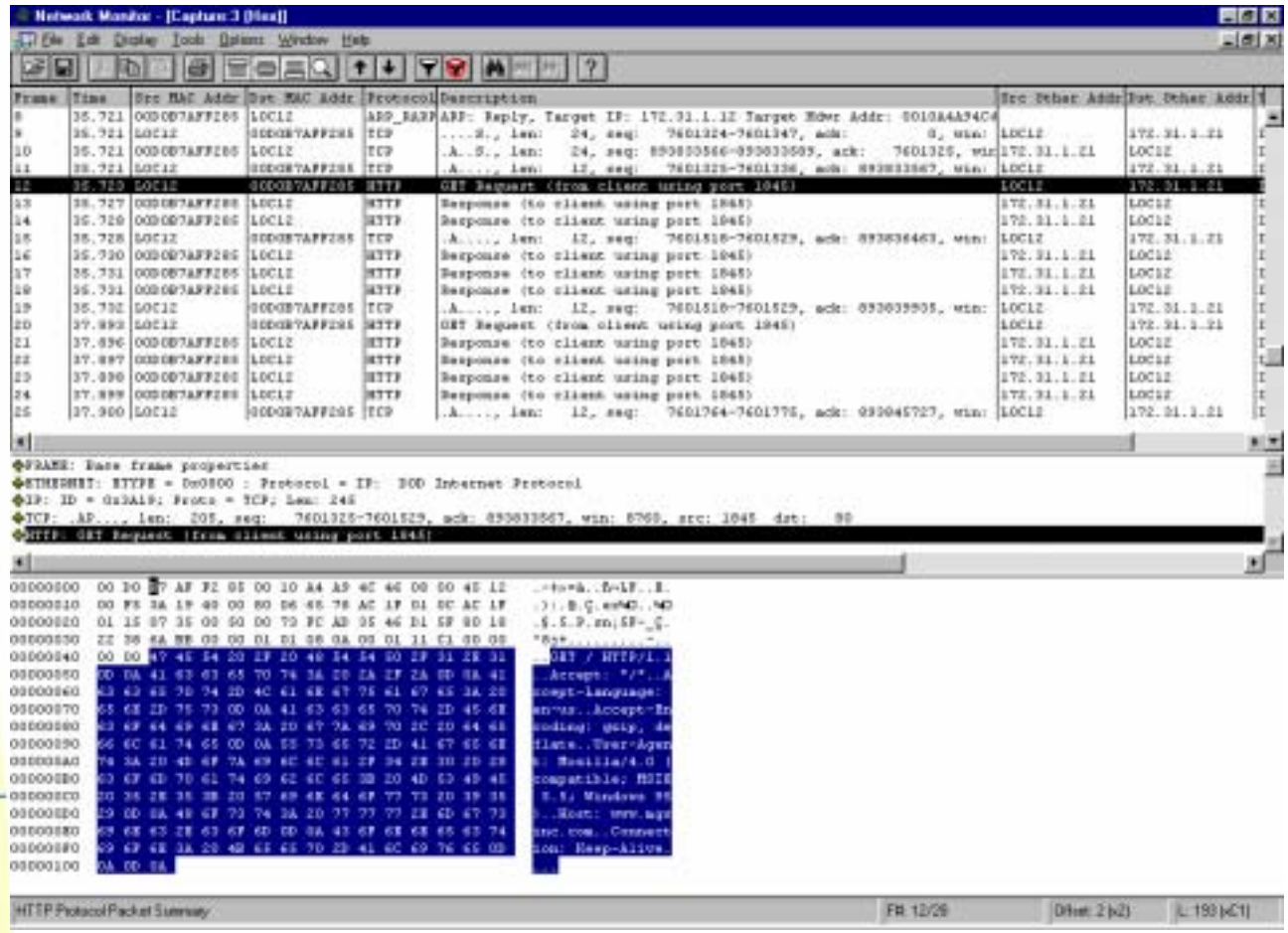
- Check current Windows TCP/IP Configuration
  - Win9x - WinIPCfg
  - NT/2K - IpConfig
  - Use /all option



MGS INC
Computer Business Solutions

TCP/IP Diagnostic Tools - NetMON

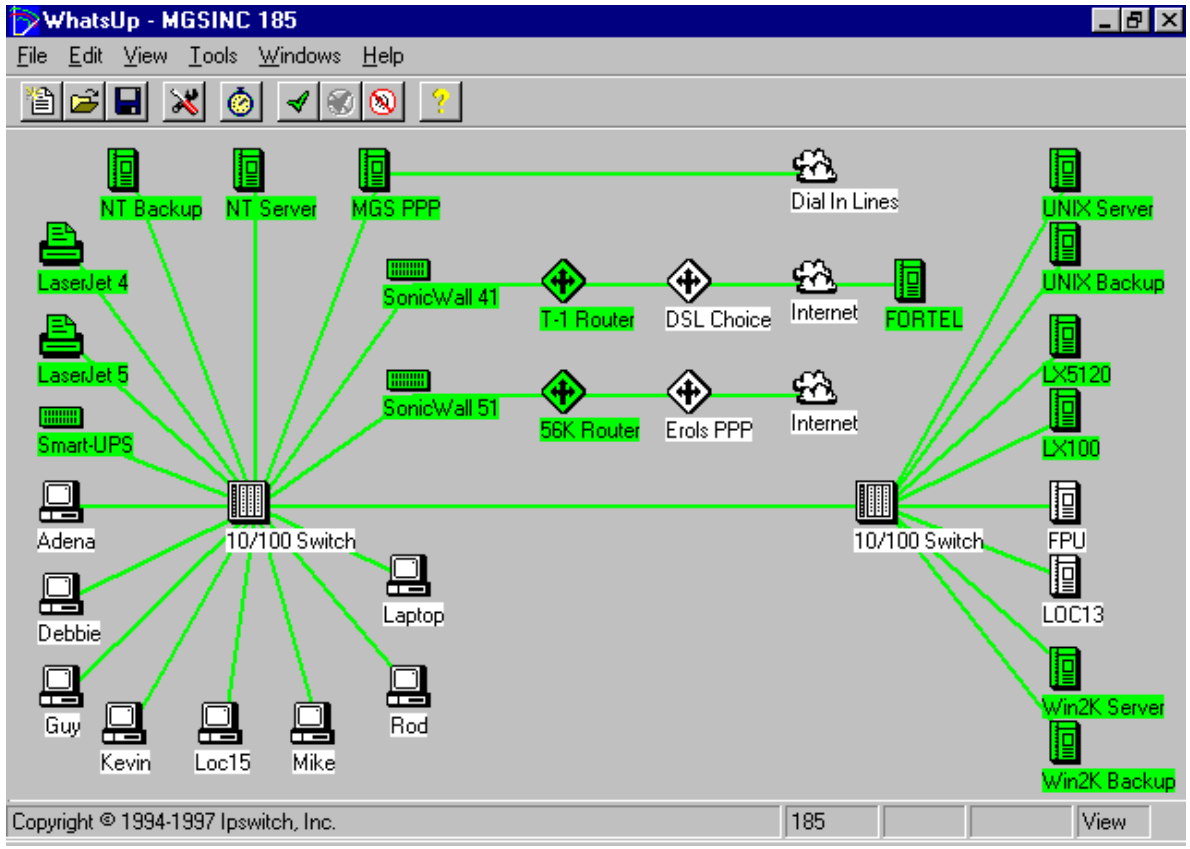
- Monitor Network Packets



MGS INC
Computer Business Solutions

TCP/IP Diagnostic Tools - WhatsUp

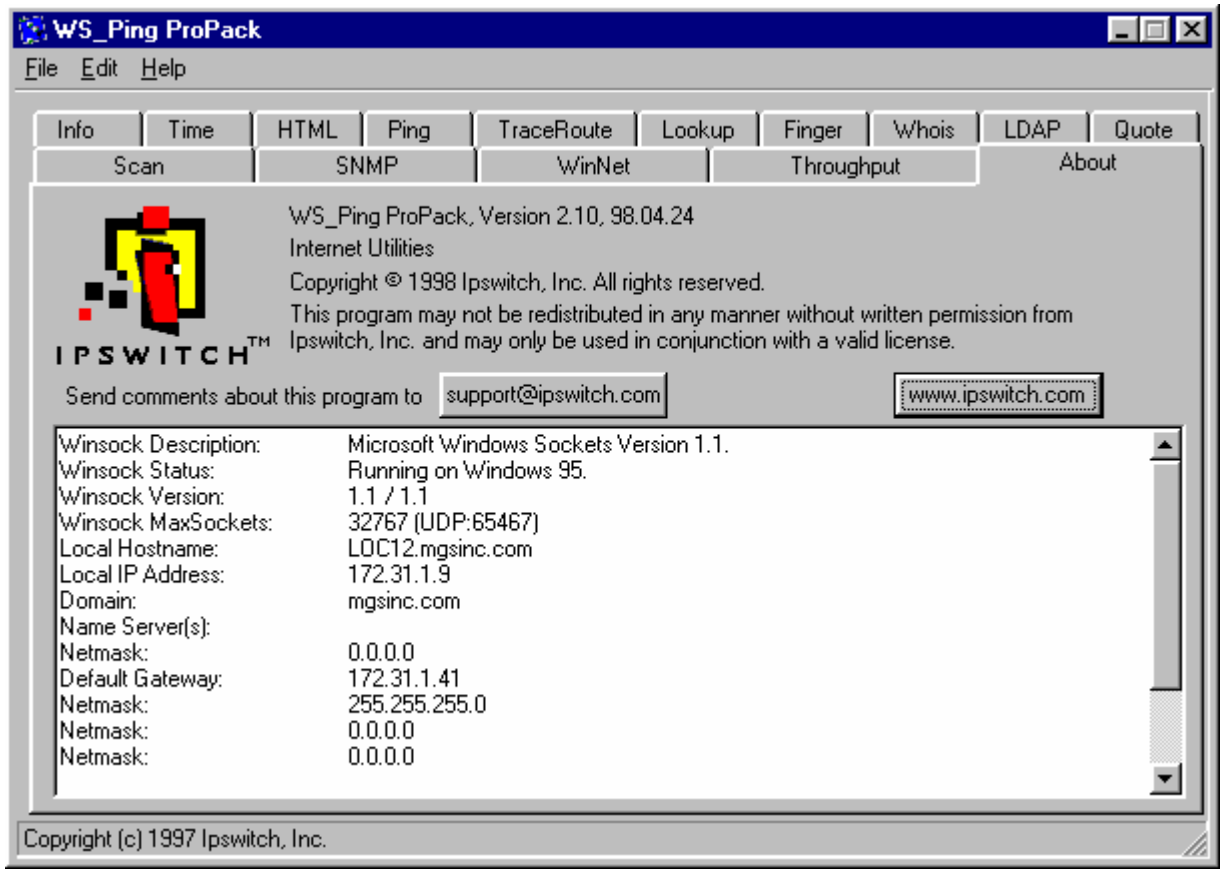
- Use to monitor presence of key network components/services



MGS INC
Computer Business Solutions

TCP/IP Diagnostic Tools - WS_Ping ProPack

- Use to test key network services



MGS INC
Computer Business Solutions

Additional Questions?

Michael S. Recant
VP Software Development

MGS, Inc.
10901 Trade Road, Suite B
Richmond, VA 23236

Voice: (804)379-0230
Fax: (804)379-1299
Email: Mike.Recant@mgsinc.com
Web: www.mgsinc.com

This presentation is available on our WEB site

MGS INC
Computer Business Solutions

Reference Material

- TCP/IP Illustrated, Vol 1 by W. Richard Stevens, Addison-Wesley
- TCP/IP Illustrated, Vol 2 by W. Richard Stevens, Addison-Wesley
- TCP/IP Network Administration by Craig Hunt, O'Reilly & Associates, Inc.
- Business Data Communications and Networking by Fitzgerald & Dennis, John Wiley & Sons, Inc.
- Microsoft Windows NT Server Networking Guide, Microsoft Press
- Windows 2000 TCP/IP by Karanjit Siyan, Ph.D., New Riders Publishing

Reference Material

- TCP/IP Addressing by Buck Graham, Academic Press
- Internetworking with TCP/IP Vol II: Design, Implementation, and Internals by Douglas E. Comer, Prentice Hall
- WhatsUp Gold Software by IPSwitch, Inc. www.ipswitch.com
- WS_Ping ProPack Software by IPSwitch, Inc. www.ipswitch.com
- SonicWALL Firewall by SonicWALL Inc. www.sonicwall.com
- BSDI UNIX, Berkeley Software Design, Inc www.bsdi.com

Computer Measurement Group 2001

TCP/IP Basics
For The
IS Professional

MGS INC
Computer Business Solutions