Computer Measurement Group 2001

TCP/IP Basics For The IS Professional

Michael S. Recant MGS, Inc.



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 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

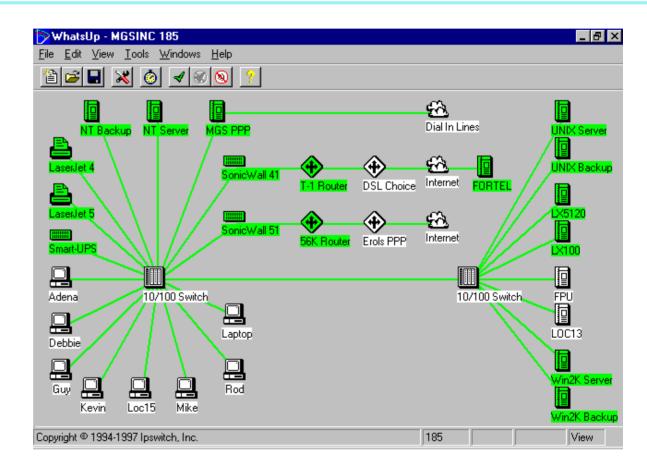


🏷 WhatsUp - MGSINC1				_ 🗆 🗵
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>T</u> ools <u>W</u> indows <u>H</u> elp				
1				
Mike Lantastic Bkup	Poll/Sel Gates	way LaserJe	ļ	
Dial In Line Lantastic Server	Micro-A Dial In Lines		Rod	
LaserJet 4			Prab	
Admin			Maintenance	
Copyright © 1994-1998 Ipswitch, Inc.		Inactive	Modified	View //



- 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







- 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



- 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)



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



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



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



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

Hardware	IP	Session	Protocol	Data
	IP	TCP	HTTP	HTML
	Header	Header	Header	Data

Link |

Network

Application

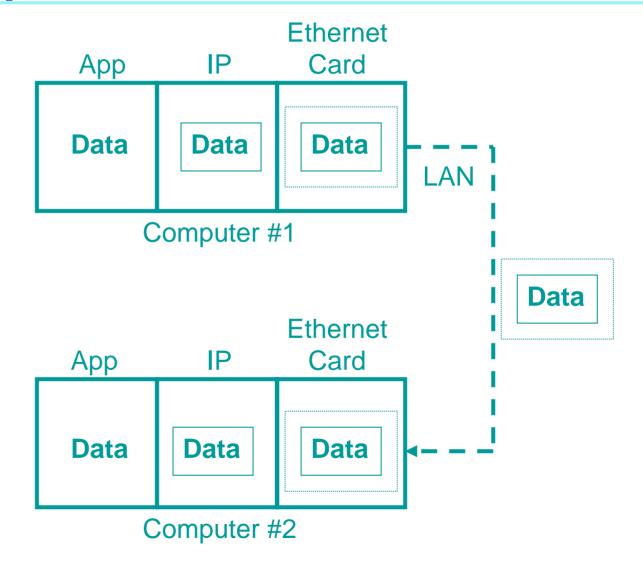


IP Communication -Overview

- 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)



IP Communication -Example



MGS

IP Addressing -Overview

- Not associated with hardware
- 32-bit Unique Host Address
- Dotted-decimal Notation: 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



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

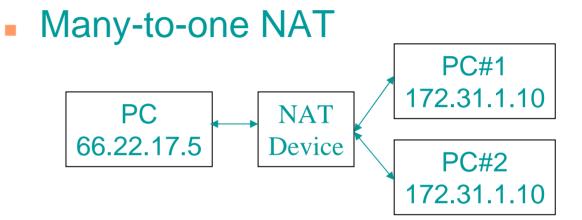


IP Addressing -Network Address Translation

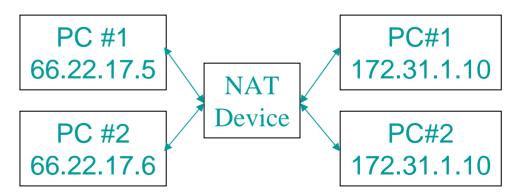
- Referred to as NAT
- Maps Internet IP Addresses to Private LAN IP Addresses
- Many-to-one NAT
 - Maps many private LAN IP Addresses to a single Internet address
 - Limited use for Servers
- One-to-one NAT
 - Maps one private IP Address to one Internet IP Address



IP Addressing -Network Address Translation









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



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



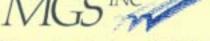
IP Communication -Summary

- 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



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



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)

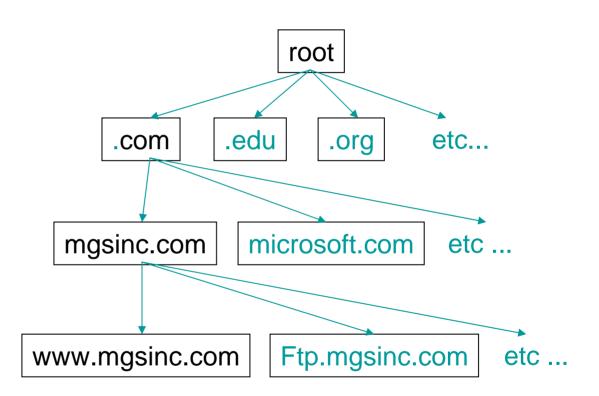


The Domain Name System - DNS



- 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

The Domain Name System - DNS Tree





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



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



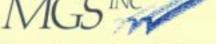
The Domain Name System - DNS Resolver

- 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-toapplication 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



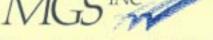
IP Based Services -LPD/LPR - Remote Printing

- 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



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



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



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



Computer Business Solutions

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



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 v	www.forte	el.com	
Trad	cing route	e to www	.fortel.co	om [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]
Trad	ce compl	ete.		



TCP/IP Diagnostic Tools -WinIPCfg and IpConfig

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

P Configuration							
Host Information							
Host Name	LOC12.mgsinc.com	ı					
DNS Servers	172.31.1.2						
Node Type	Broadcast						
NetBIOS Scope Id							
IP Routing Enabled	WINS Proxy Enabled						
NetBIOS Resolution Uses DNS	V						
Ethernet Adapter Information							
ļ	Xircom Ethernet 10/100 PC	Card 🔻					
Adapter Address	00-10-A4-A9-4C-46						
IP Address	172.31.1.12						
Subnet Mask	255.255.255.0						
Default Gateway	172.31.1.41						
DHCP Server							
Primary WINS Server							
Secondary WINS Server							
Lease Obtained							
Lease Expires							
OK Releage Re	new Release All Re	ne <u>w</u> All					



TCP/IP Diagnostic Tools -NetMON

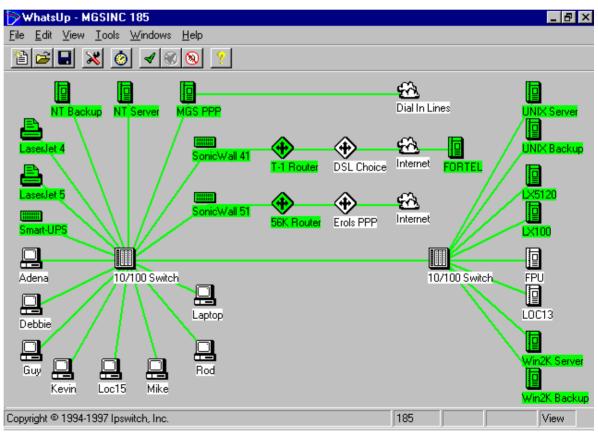
Monitor Network Packets

And I wanted	24 0	inter [Capture]		t:			1
2210		NUMBER		Conceptual and the second	1 · · · · · · · · · · · · · · · · · · ·		
1			and a second of the second of the	succession in the local division in the loca	terrained terrained terrained terrained		215
Frank			Dyt BAC Addr.			fre Sther Add	tr Dat. Other 1
	35,721	000007389285	LOCIE SCORTAPPERS	109_1437	AND: Reply, Target IF: 172.01.1.12 Target Hdwr Addr: 001084A94C4 S., 1en: 24, seg: 7601024-7601047, ads: 0, uts:		172. 31. 2. 21
10		000007455285		102			LOCIE
10		10212	BEDGETAFF285	110	.A. 5., Len: 24, seq: 85080566-85080589, ack: 7601325, wir .A, Len: 17, seq: 7601325-7601338, ack: 893833667, win.		172.31.1.21
11	16, 320		000087858205			ROOM	178.01.0.4
43		DODDE7AFF288		STTP.		172.31.1.21	LOCIE
14		000087459286		8778		170.01.0.01	LOCIE
18	38,728		OCCUPTAFF285			LOCIZ	172.31.1.21
16		000007357285		ATTR		172.91.1.21	LOCIE
17		000.087455285		STTR		172.31.1.21	LOCIZ
19	\$5.731	000.007459285		ATTR		172.31.1.21	LOCLE
19	35,712		OCCORTAFF205	109	A, 1an: 12, seg: 7601510-7601529, ack: 093039905, win:		172.31.1.21
20	37.893		ODDOR'TAFFICES	STTR		10012	172.31.1.2
21	37.896	000087455285	LOCIZ	11777	Response (to client using port 1845)	172.01.1.21	LOCIZ
22	37.887	000087488288	LOCLI	1177.0	Basponse (to client using port 1888)	172.31.1.21	LOCAR
2.5	37.090	000007489200	LOCLE	10772	Berponse (to client using part 1045)	172.01.1.21	LOCIE
24	37.899	000087487288	LOCLT	1477.8	Barponsa (to client using port 1845)	172.31.1.21	LOCIE
2.5	17.900	10012	OCDORTAFFEOS	103	.A, Jan: 12, seq: 7601764-7601775, ack: 090045727, win:	LOCLE	372.01.1.2
◆87H82 ◆32: 3	887: 83 D = 013	MAIP: Proto -	: Protocol = 1 TCF; Len: 245		Internet Frotocol ack: 835833567, win: 8760, arc: 1045 dat: 80		
 FRAME FRAME FRAME FRAME FRAME FRAME FRAME 	0111: 13 D = 013 .AP	TYPE = De0800 ALP: From =	: Protocol = 1 TCP; Lem: 245 eq: 7601025	-7601529.	ack: 030033567, win: 0760, arc: 1045 dat: 00		
• FRAME • ETHER • 19: 1 • TCF: • TCF: • TCF:	011: 13 D = 013 AP	MIF: Proto - Lin: 205, s 2003 Fond	: Probacol = TCP; Lea: 245 eq: 7601325 Heat Colory	-7601529, art 1845)	ack: 030033567, win: 0760, stc: 1045 dst: 00		
	011: 13 D = 013 AP.	1778 - De0800 MAR, Frons - , Len: 205, s 22200 - Form -	: Protocol = TCP; Les: 245 eq: 7601325 FETE OFFICE 0 5 00 10 A4 A9	-7601529,	ack: 830833567, win; 8768, stc: 1045 dst; 80		
	6117: 13 D = 013 AP. 017 P	TYPE - Decision MAIP: Prots - . Len: 205, s Typete Frence For an arr and the FS 3a AF 40 CC	: Protocol = TCP; Lem: 245 eq: 7401025 History CHANNES 5 00 10 A4 A5 1 80 56 45 78	-7601529, 010 40441 02 44 00 AC 17 D1	ack: 850833567, win; 8768, arc: 1048 dat; 80		_
	HT: 17 D = 013 AP 0 = 0 1 0 00 1 10 00 1	TYPE - Decision IA19; Froms - . Len: 205, s Specie From 0 10 37 AF F2 01 F5 38 19 40 00 15 07 35 00 50	: Protocol = TCP; Les: 245 eq: 7601925 Histor Clinit ; 5 00 10 A4 A5 5 00 56 46 76 1 00 79 FC AD	-7601529, 010 40441 02 44 00 A2 19 01 95 46 51	ack: 0300330567, win: 0760, stt: 1045 dst: 00 00 45 4245*8.:5*4FE. 00 45 17 .).0.0.0.00 57 00 10 .5.5.P.m.(SP_0.		
	HT: 17 D = 013 AP 0 00 1 0 00 1 0 01 1 0 01 1	TYPE = Duc0800 hA19; Froms = , 140; 205, s proto 1544 a 1544 a 15 0 7 AF 32 01 15 07 AF 32 00 15 07 35 00 50 16 64 86 00 00	: Protocol = TCP; Less: 245 eq: 7601325 Hints Million y 5 00 10 A4 A5 0 80 D6 46 78 1 00 73 37 A0 0 01 01 06 0A	-7601529, 210 10435 40 46 00 AC 17 01 95 46 51 05 01 11	ack: 833833567, win; 8768, stc: 1045 dst; 80 50 45 12+s=k.:b=1FE. 50 A5 17 .).8.C.eeMCMD 57 80 185.2.mi;6F_C.		
P3/25 FT(F) T(F) T(F)	HTT: 17 D = 013 AP 0 00 1 10 00 1 10 01 1 10 22 1 10 00 1	TYPE = Dw0100 M19: Froms = . Len: 205, F TYPES Form = 10 7 AF 72 01 F5 34 1P 40 02 15 07 35 00 50 16 4A FE 03 00 10 77 45 14 20	: Protocol =) 3CP; Lew: 245 eq: 7401325 Hints Hinty p 5 00 10 A4 A9 9 80 56 48 78 1 00 73 FC A0 0 L 51 58 0A	-7601529, 011 10445) 40 46 00 AC 17 01 95 46 01 95 46 01 95 01 31 24 50 17	ack: 830833567, win; 8768, stc: 1048 dst; 80 50 45 12+to-4a.:5-1FE. 50 AC 17 -:		
	HTT: 17 D = 013 AP 0 00 1 10 00 1 10 00 1 10 01 1 10 00 1 10 00 1 10 00 1 10 00 1	TYPE DuroBio ALIF: Fronts . Len: 205. *	: Protocol = TCP: Leas: 245 eq: 7401325 Field Million F 5 00 10 A4 A9 5 00 10 A4 A9 1 00 70 FC A0 1 01 70 FC A0 1 01 70 46 54 1 70 74 34 20	-7601529, 407 40451 407 40 40 407 40 40 407 40 11 54 50 21 54 50 21 55 50 21 5	ack: 4300330567, win; 5769, src: 1045 dst; 80 50 45 12+torkD+LFI. 50 45 17		
	HT: 13 D = 013 AP 00 00 1 10 00 1 10 00 1 10 01 1 10 00 1	TYPE = De0100 hilfs; Frocs = len; 205, s 100 7 AF 92 01 F5 3A 19 40 00 15 07 35 00 50 15 4A 95 03 00 10 97 45 54 35 10 41 53 03 65 44 53 05 74 32	: Protocol =) 3CP; Lew: 248 eq: 7601325 5 00 10 A4 A9 5 00 06 45 76 1 00 72 FC A0 0 01 01 48 0A 1 17 20 49 54 70 74 35 40 40 41 42 47	-7601529, art 14451 40 46 00 AC 17 01 05 46 01 24 60 17 24 60 17 25 61 60 17 25 60 17 2	ack: 433033567, win; 5769, stc: 1045 dst; 80 50 45 12tork0-1F1. 50 A5 17		
	HIT: 17 D = 013 AP. 00 00 1 10 00 1 10 01 2 10 00 1 10 01 2 10 00 1 10 00 1 10 01 2 10 00 1 10 00 00 1 10 00 00 00 00 00 00 000 0	TYPE = Dec01000 ALIS: Froms = Les: 205, s Plant IF and F2 01 F7 AF F2 01 F7 AF F2 01 F7 AF F3 00 50 15 07 35 00 50 15 07 35 00 50 15 07 35 00 50 15 54 35 00 47 45 54 35 00 47 45 54 35 00 47 45 73 00 14 67 07 73 16 20 70 73 00 16 20 70 73 00 17 75 73 00 16 20 70 73 00 16 20 70 73 00 17 75 73 00 16 20 70 70 16 20 70 70 16 20 70 70 16 20 70 70 16 20 70 10	: Protocol = TCP; Lew: 248 eq: 7601325 11mmL 041109 p 5 00 10 A4 A5 5 00 10 A4 A5 5 00 10 A4 A5 1 00 72 9C A5 1 00 72 9C A5 1 00 74 34 20 1 4C 61 62 67 1 4C 61 63 63	-7601529, art 1445; 40 46 00 AC 17 01 95 46 01 95 46 01 95 46 01 95 10 11 14 00 13 14 00 15 14 00 15 14 10 15 14 10 15 15 15 15 15 15 15 15 15 15	ack: 850833567, win; 8768, stc: 1048 dst; 80 50 45 1240-05-1F1. 50 45 17 -01.8.C.en4040 57 80 18 -5		
	HIT: 13 D = 013 AP. 014 10 10 00 1 10 01 1 10 02 2 10 00 1 10 00 100 1	TYPE = De0100 TALE: From: - Len: 205, s bylet5 From: - bylet5 From: - 15 07 AF F2 01 5 07 35 00 50 36 5A DE 09 00 50 47 45 54 20 50 41 63 75 73 00 64 20 75 73 00	: Protocol =) 3CP; Lew: 245 eg: 7601325 Hind 40509 p2 5 00 10 A4 A5 5 00 10 A6 A5 5 00 10 A6 A5 1 00 75 27 A5 1 00 75 27 A5 1 00 75 45 54 70 74 45 45 70 74 45 45 0 04 41 63 63 0 24 20 47 7A	-7601525, 46 46 00 46 10 11 10 11 10 11 10 11 11 14 10 13 14 10 10 10 10 10 10 10 10 10 10 10 10 10	ack: 4300330567, win; 5769, src: 1045 dst; 80 50 45 12+to=hfs-LFI. 50 45 12+to=hfs-LFI. 50 45 12+to=hfsg. 51 00 00+to=hfsg. 51 00 00 00+to=hfsg. 51 00 00 00 00 00 00 00 00 00 00 00 00 00		
	HIT: 17 D = 013 AP OT 00 1 10 00 1 10 01 1 10 00 1 100 000 1 10 00 100 1	TYPE = Dec01000 ALIS: Froms = Les: 205, s Plant IF and F2 01 F7 AF F2 01 F7 AF F2 01 F7 AF F3 00 50 15 07 35 00 50 15 07 35 00 50 15 07 35 00 50 15 54 35 00 47 45 54 35 00 47 45 54 35 00 47 45 73 00 14 67 07 73 16 20 70 73 00 16 20 70 73 00 17 75 73 00 16 20 70 73 00 16 20 70 73 00 17 75 73 00 16 20 70 70 16 20 70 70 16 20 70 70 16 20 70 70 16 20 70 10	: Protocol =) 3CP; Lew: 248 9CP; Lew: 248 9CP; Active a 00 10 A4 A9 00 00 645 76 00 10 072 97 A0 01 01 08 0A 17 74 34 20 40 41 63 63 2A 20 47 7A 0A 55 73 65	-7601529, act 104451 46 46 00 Ac 17 04 95 46 01 11 54 00 27 28 21 27 28 21 27 28 21 67 45 70 20 72 20 41	ack: 4550335567, win; 5768, stc: 1045 dst; 80 50 45 12+ts=k.:D+1FE. 50 A5 17 .).8.9.ex4540 57 80 14 .5.9.mi(5540 57 80 14 .5.9.mi(5540 51 28 01 .5.9.mi(5540 .5.1 28 01 .5.9.mi(5540 .5.1 28 01 .5.1 28 01 .5.2 mi(5540 .5.1 28 01 .5.2 mi(5540 .5.1 28 01 .5.2 mi(5540 .5.1 28 01 .5.2 mi(5540 .5.1 28 01 .5.2 mi(5540 .5.2 mi(5540) .5.2 mi		
	HT: 17 D = 012 AP 017 P 017 P	TYPE = De0100 hilfs; Frocs = les: 205, s 100 7 AF 72 01 F5 3A 19 40 00 15 07 35 00 50 15 07 35 00 50 15 07 45 54 50 10 47 45 54 50 10 47 45 54 50 14 53 01 41 15 57 73 00 15 64 49 48 45 15 65 00	: Protocol = 3CP; Lew: 248 9C); Lew: 248 9C); Advisor 110000 0010 A4 A59 80 D6 46 78 100 72 FC A2 101 72 FC A2 101 72 FC A2 101 72 FC A2 17 720 45 54 170 74 34 20 4C 41 4E 47 2 A 20 47 74 0 A 11 45 47 0 A 12 57 36 0 A 12 57 74	-7601529, 46 46 00 46 46 00 46 17 01 54 60 13 54 60 13 54 60 13 54 60 27 65 70 74 65 70 74 65 70 24 77 200 41 57 94 23	ack: 853833567, win; 8768, stc: 1048 dst; 80 50 45 1240-40-1F1. 50 45 1210 000 59 80 10 -5.5.P. m(5F_0. 51 00 00 -5.5.P. m(5F_0.		
	HIT: H D = AP -	TYPE = Dec01000 hills: Frots = Les: 205, s Friend - 15 and - 10 7 AF 72 01 15 07 35 00 52 15 07 35 00 52 15 07 35 00 52 15 07 35 00 52 15 84 55 02 00 14 41 52 67 65 42 45 20 74 54 42 45 77 70 44 45 45 70 44 45 45 70 44 45 45 70 44 45 45 70 44 45 77 44 55 70 45 44 55 70 45 45 77 45 45	: Protocol =) 3CP; Lew: 245 9C01325 1000 10 A4 A5 000 10 A4 A5 000 10 A4 A5 100 73 FC A0 100 73 FC A0 100 73 FC A0 100 73 FC A0 100 74 A 20 04 C 41 62 67 04 41 63 63 04 C 41 63 63 04 55 73 66 69 6C 45 69 6C 45 70 74 100 73 100 73 100 73 100 73 100 74 100 74	-7601529, 40 446 00 40 446 00 40 17 01 25 46 01 25 46 01 25 46 01 24 50 17 24 50 17 24 50 17 24 50 17 24 57 0 27 75 10 41 27 10 41 27 10 40 20 10 40 2	ack: 4300330567, win; 5769, src: 1045 dst; 80 50 45 42+to-AD-AFT. 50 45 42+to-AD-AFT. 50 45 12+to-A 51 80 14+to-A 51 80 14+to-A 51 80 14+to-A 51 14 01+to-A 51 15		
	HIT: T D = 0.2 AP 0.0 0.1 OIT 0.0 0.1 IOT 0.0 0.1	TYPE = De0100 TALE: From: Ien: 205, s TALE: 105, s TAL	: Protocol = TCP; Lew: 245 eq: 7401325 lised: 041509 p 5 00 10 A4 A5 5 00 10 A4 A5 10 07 2 FC A5 0 0 01 0 A4 A5 10 07 2 FC A5 0 0 01 0 A4 A5 10 07 2 FC A5 0 0 01 0 A4 A5 10 07 2 FC A5 10 07 4 34 20 4C 41 45 63 24 20 47 34 46 4C 41 45 46 4C 41 45 46 4C 41 45 47 7 3 4C 45 47 4 45 45 47 4 45 45 48 45 45 45 48 45 45 48 45 45 48 45 45 48 45 45 48 45 45 48 45 45 48 45 45 48 45 45 48 45 45	-7601525. 40 46 00 40 46 00 40 19 01 51 46 01 40 01 11 54 60 02 54 60 12 54 60 02 54 67 03 54 70 74 55 70 74 55 70 74 51 94 23 52 94 23 54 67 72 20 41 59 94 23 50 40 69 77 73 60 77 50 40 50 77 50 40 50 77 50 40 50 77 50 40 50 40 50 40 50 40 50 40 50 50 50	ack: 4550532567, win; 5768, stc: 1045 dst; 80 50 45 124s-A.:DelFE. 50 A5 17 -0.:B.Q.exMCMD 57 80 14 -5.5.7.mp;5F_Q. 51 80 05 -784 51 28 51 -542		
	HIT: T D = 0.23 AP AP AP GIT Id	TYPE Dec01000 Lim: 2005.0 Lim: 2005.0 Maile: From:	Protocol = 3CP; Lew: 248 3CP; Lew: 248 3CP; Advisor 24 11000 10 A4 A9 5 00 10 A4 A9 5 00 10 A4 A9 5 00 20 65 78 10 72 FC A2 10 72 FC A2 10 72 FC A2 10 74 34 20 4C 41 4E 47 2 A 20 47 74 0 A 41 43 43 2 A 20 47 74 0 A 55 73 65 157 49 45 43 157 49 45 45 45 157 49 45 45 45 157 49 45 45 157 45 45 45 157 45 45 45 45 45 1	-7601522, ort 1045; 42 46 00 Ac 17 01 25 46 01 26 45 10 05 01 11 54 00 27 55 70 74 49 70 20 75 70 20 20 40 47 77 72 20	ack: 4330330567, win; 5769, src: 1045 dst; 80 50 45 12+br%fc4Ff. 50 45 12br%fc4Ff. 50 45 17 -21.8 C end(740 57 80 14 -5.5.P.m)59-C. 51 00 05 -755 51 00 05 -755 51 00 05 -755 51 00 05 -755 51 00 05 -655 52 40 40 moding: g452 40 67 65 61 filmsTwar.Agen 10 15 41 -5 51 Mardows 98 67 65 61 filmsTwar.Agen 10 15 41 -5 51 Mardows 98 60 67 73 8 5.5 Mardows 98		
	HIT: 13 D 413 AP. 141 CIT	TYPE = De01000 hills: Froms = Less: 205, s Friend 15 trans 1 10 7 AF 32 01 15 07 35 00 52 15 07 35 00 52 15 07 35 00 52 15 42 54 20 14 41 63 63 65 15 17 46 50 16 44 49 48 67 17 46 50 17 46 50 17 46 50 17 46 70 61 74 18 28 28 38 28 28 38 77 28 28 38 38 28 28 38 77 28 28 38 28 28 38	: Protocol =) TCP; Lew: 245 TCP; Lew: 245 Filest 445 500 10 A4 A5 500 10 A4 A5 500 10 A4 A5 10 73 FC A0 10 73 FC A0 10 73 FC A0 10 73 A5 00 A1 65 73 00 A1 65 73 00 A5 73 65 10 65 65 55 17 49 45 64 17 43 20 07 10 74 45 64 10 75 73 65 10 76 45 65 17 49 45 64 17 43 45 07 10 76 45 64 17 43 45 07 10 76 45 77 10 76 10 76 44 10 76 44 10 76 77 10	-7601529, act 4465 45 446 00 Ac 14 01 5 446 10 Ac 14 01 5 440 12 4 00 01 11 54 00 12 54 10 12 54	ack: 830833567, win; 8768, src: 1045 dst; 80 50 45 42+b=45+4F1. 50 45 42+b=45+4F1. 50 45 17		
	HIT: T D = 0.23 AP AP AP CLT AP	TYPE = De0100 TALE: Proce. Les: 205, s protect Free 4 10 27 AF 72 01 78 34 19 40 00 10 41 63 00 50 10 41 63 00 50 10 41 63 07 55 42 45 20 74 52 00 44 44 64 48 42 44 49 48 49 44 69 48 49 44 69 48 49 44 69 48 49 44 69 48 49 45 75 70 61 74 55 40 49 48 49 46 49 48 49 46 49 48 49 48 49 48 48 49 48 49 48 49 48 48 49 48 40 40 40 40 40 40 40 40 40 40	: Protocol =) TCP; Lew: 245 TCP; Lew: 245 Filest 445 500 10 A4 A5 500 10 A4 A5 500 10 A4 A5 10 73 FC A0 10 73 FC A0 10 73 FC A0 10 73 A5 00 A1 65 73 00 A1 65 73 00 A5 73 65 10 65 65 55 17 49 45 64 17 43 20 07 10 74 45 64 10 75 73 65 10 76 45 65 17 49 45 64 17 43 45 07 10 76 45 64 17 43 45 07 10 76 45 77 10 76 10 76 44 10 76 44 10 76 77 10	-7601529, act 4465 45 446 00 Ac 14 01 5 446 10 Ac 14 01 5 440 12 4 00 01 11 54 00 12 54 10 12 54	ack: 830833567, win; 8768, src: 1045 dst; 80 50 45 42+b=45+4F1. 50 45 42+b=45+4F1. 50 45 17		
	HIT: T D = 0.23 AP AP AP CLT AP	TYPE Dec01000 Lim: 2005.0 Lim: 2005.0 Maile: From:	: Protocol =) TCP; Lew: 245 TCP; Lew: 245 Filest 445 500 10 A4 A5 500 10 A4 A5 500 10 A4 A5 10 73 FC A0 10 73 FC A0 10 73 FC A0 10 73 A5 00 A1 65 73 00 A1 65 73 00 A5 73 65 10 65 65 55 17 49 45 64 17 43 20 07 10 74 45 64 10 75 73 65 10 76 45 65 17 49 45 64 17 43 45 07 10 76 45 64 17 43 45 07 10 76 45 77 10 76 10 76 44 10 76 44 10 76 77 10	-7601529, act 4465 45 446 00 Ac 14 01 5 446 10 Ac 14 01 5 440 12 4 00 01 11 54 00 12 54 10 12 54	ack: 830833567, win; 8768, src: 1045 dst; 80 50 45 42+b=45+4F1. 50 45 42+b=45+4F1. 50 45 17		



TCP/IP Diagnostic Tools -WhatsUp

Use to monitor presence of key network components/services





TCP/IP Diagnostic Tools -WS_Ping ProPack

Use to test key network services

e <u>E</u> dit <u>H</u> elp			1		с. л. ¹		<u> </u>
Info Time I Scan	HTML Ping SNMP	TraceRoute WinNet	Lookup	Finger Throughp	Whois out	LDAP	Quote out
IPSWITCH [™] Send comments about	WS_Ping ProPack, Internet Utilities Copyright © 1998 Ip This program may n Ipswitch, Inc. and n this program to sup	pswitch, Inc. All rig tot be redistributed	hts reserved. in any mann n conjunction	er without w	l license.	ission from	
Winsock Description: Winsock Status: Winsock Version: Local Hostname: Local IP Address: Domain: Name Server(s): Netmask: Default Gateway: Netmask: Netmask: Netmask:	Microsoft Wir Running on V 1.1 / 1.1 32767 (UDP: LOC12.mgsin 172.31.1.9 mgsinc.com 0.0.0.0 172.31.1.41 255.255.255. 0.0.0.0 0.0.00	65467) ic.com	rsion 1.1.				

MGSINC

Additional Questions?



Computer Business Solutions

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

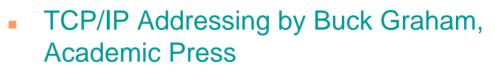
This presentation is available on our WEB site

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



- 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

