An Overview of TCP/IP
(and speaking “network”)

Samuel D. Cohen
IBM z Consultant
Levi, Ray & Shoup, Inc.
Contact: sam.cohen@lrs.com

Why Should I Care?

- Your customers/end-users think that a network interruption means the mainframe is down
- As an administrator for an IBM z Operating System, you should know basic troubleshooting for network issues
- To do basic troubleshooting, you should have an understanding of the network concepts and terminology

Internet Protocol (IP)

- Layered Protocol
  - 1 – Physical/Link Layer (wiring and transmission protocol)
  - 2 – Internet Layer (IPv4, IPv6, ICMP)
  - 3 – Transport Layer (TCP, UDP)
  - 4 – Application Layer (Telnet, FTP, SMTP, SNMP, etc.)

Layer 2 vs. Layer 3 Communications

- Layer 2 communications uses a hardware-based address (Media-Access Control Address or MACADDR) to identify the sender and the receiver
- Layer 3 communications uses an IP address (IPv4 consists of 4 decimal digits in the range of 0-255 separated by ‘.’)
  - Uses ARP (Address Resolution Protocol) to map an IP address to a target MACADDR

Internet Layer

- Local Area Network (LAN)
  - Physical Infrastructure
    - Network Interface (NIC) - LAN interface connection
    - Hub – Layer 1 dumb connections to machines in a single LAN
      - Bridge – connects multiple hubs together in a single LAN
    - Switch – Layer 2 smart connections to machines in a single LAN
    - Router – Layer 3 provider of connections between LANs

Internet Layer

- Local Area Network (LAN)
  - Logical Infrastructure
    - Host
    - Network
    - Network Mask
    - Routing

IPv4 Addressing

- An IPv4 address has 4 bytes presented as digital numbers with ranges *0-255.0-255.0-255.0-255*
  - This corresponds to hex values *00-FF.00-FF.00-FF.00-FF*
  - Note the ‘.’ separating each byte
- In a single network, each IP address on the network must be unique
- Each IP address represents a combination of “host” and “network”

Host

- A host refers to a unique IP address on specific LAN
- A host does not necessarily have a 1:1 relationship with a NIC
  - For example, an IBM z Open Systems Adapter (OSA) can have many host addresses
  - This tends to confuse network engineers who only see 1 NIC = 1 Host on a regular basis

Network

- A network refers to a set of IP host addresses in a unique LAN
  - You can not have duplicate networks in a set of connected LANs
  - You can have duplicate networks if those networks are isolated from each other
    - Good luck managing those

Network Mask

- In a given IPv4 address, how do you know what part is "network" and what part is "host"?
  - Network Mask – a parallel IPv4-type construct separating network from host
    - Network Mask bit = 1 – Network
    - Network Mask bit = 0 – Host
  - Coding of Network Mask
    - In IPv4 construct, in the range *0-255.0-255.0-255.0-255*
    - Number of consecutive network bits starting from the leftmost part of the IPv4 address
      - Separated from the IPv4 address by "/"

Example of Host/Network

- The IPv4 address is 192.168.0.254
- The network mask is 255.255.0.0
- The combined address/mask is 192.168.0.254/16
- The network address is determined by ANDing the address by the mask (after conversion to binary (shown here in dotted decimal)):

  192.168.0.254 & 255.255.0.0 = 192.168.0.0
- The network address is determined by XORing the address by the mask (after conversion to binary (shown here in dotted decimal)):

  192.168.0.254 ∧ 255.255.0.0 = 0.0.0.254

Routing

- Every host in a LAN can automatically communicate with every other host that is connected to the LAN
- If you want to connect to a host in a different LAN, you must specify how to get to that host by specifying the IP address of a router that is connected to both LANs (yours and the other hosts')
- You can also specify the IP address of a router for any LAN not otherwise specified
  - This is called the "default" router or gateway

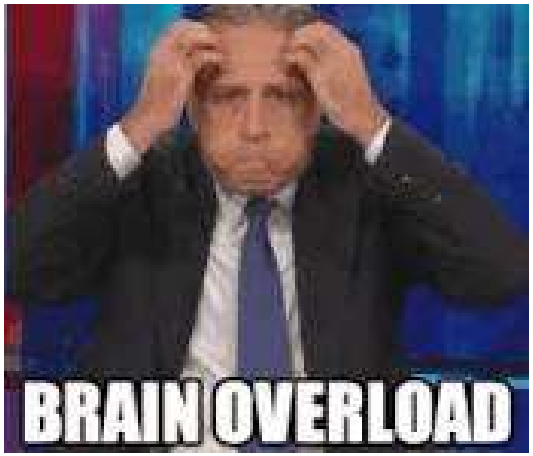
Transport Layer

- Maintains end-to-end connections in a conversation between hosts
  - Connection-oriented (called Transport Control Protocol or TCP)
  - Connectionless (called Unformatted Datagram Protocol or UDP)
- TCP is used when a client sends a request to a server
- UDP is used to broadcast a message out from the server
- Sockets (like electrical sockets in your home) are provided for applications to plug into the IP stack for communications

Applications

- Applications using IP communication plug into a socket (via socket or port number: 1-65535)
- Some applications will listen for incoming traffic, others will send outgoing traffic to a specific host and a specific port

Are you here?



Those are the basics

- Why are there network problems?
  - IF you follow all the rules, everything should interconnect seamlessly
    - IF you have a complete and consistent network architecture
    - IF you have no typos in any configuration file
    - IF you have the same manufacturer of network hardware with the same levels of software (since today's equipment is more software than hardware)
    - IF things don't break for reasons unknown
    - IF there was unrestricted transmission between hosts/networks
    - IF there weren't any bad guys out there

What are common issues?

- Can’t initially connect to your LAN
- Can’t reach a particular network destination
- Sometimes works, sometimes doesn’t work
- What changed??
  - “Nothing”
    - “Well, maybe something in the next building….”

Easy to use test tools

- Ping – sends ICMP message to target IP address
- Traceroute – sends ICMP message (perhaps via UDP) and reports each router transited enroute to the target IP address
- Headache: Many network teams disable responding to ICMP
  - Fine for communicating outside the business
  - Pain when troubleshooting inside the business

Ping command

- z/VM: CMS command (on TCPMAINT 592): **ping *ip-address***
- Linux: **ping *ip-address***
- z/OS: **TSO ping *ip-address***
- VSE^{n}: CSI via CICS: **ping *ip-address***

  BSI via batch job

Traceroute command

- z/VM: CMS command (on TCPMAINT 592): **tracerte *ip-address***
- Linux: **traceroute *ip-address***
- z/OS: **TSO tracerte *ip-address***
- VSE^{n}: CSI via CICS: **tracert *ip-address***

Common Challenges

- Isolation of network team from systems and business units
  - Chasing network problems requires expertise on both ends of the connection
- Lack of complete/consistent network architecture
  - Or no one has access to the documents and drawings
- Not seeing the big picture and where you fit in
  - Applications teams knowing little about the platforms they run on and why
  - Systems teams not knowing what the application teams are doing
  - Network teams not knowing applications or systems

Solution Approaches

- Network problem resolution require a team approach:
  - Expertise at both ends of the connection, and
  - Expertise along the connection path
- IBM z SysProgs must have some understanding of how the underlying applications and middleware use network resources for capacity planning and problem resolution
- Application architects need to understand how their applications use system and network resources
- Despite the “zero trust” mantra, the knowledge resources must have unfettered access to systems for PD/PSI to resolve problems quickly

Exhausted Yet?

Have a good break