TCP/IP overview

TCP/IP: The Internet Language

- It is the protocol used for all major networking services like World Wide Web and email systems
- Thus, it is used to interconnect machines across small, medium-sized, and huge networks. It is also the protocol that powers high level Internet services like HTTP, FTP, POP, and SMTP to name a few
- All network-aware machines (and devices in general) talk and understand TCP/IP, which makes data exchange among different nodes easy
- The following reasons made TCP/IP the de facto language of the Internet:
  - Adaptive architecture
  - Not being owned by a company or person (non-proprietary)

How do packets find their way around the network?

- Every network adapter has a Media Access Control number (MAC address). It is a unique value supplied to the adapter at manufacturing time. Using MAC addresses to identify network devices is called Physical Addressing
- On very small networks, adapters listen for all the traffic passing through to determine whether or not data is intended for their own MAC addresses. Devices are joined by a device called hub (rarely used now).
- As networks get larger, a device is installed to ensure that packets get addressed only to their intended recipients. It is called a switch.
- As networks get larger, physical addressing becomes less effective. Networks are segmented using Logical Addressing.
- In logical addressing, each device is assigned a number called IP address. This number is unique across the *subnet*. Different subnets are connected through a device called a router.
- TCP/IP supports both types of addressing

What is a protocol?

- A set of common rules that controls communication between two or more devices on a specific medium
- This medium could be a wire or a radio wave
- A protocol uses the networking components and daemons on the operating system, the network hardware, and the transmission medium to send or receive a message from a remote device.
- A network-aware application uses the TCP/IP stack to communicate with other applications. It takes the route from up to bottom as in shown in the next slide
- The protocol defines the contents of each packet in a standard way that can be interpreted by the receiving device.

TCP/IP skeleton

- It stands for Transmission Control Protocol/Internet protocol; a set of network protocols stacked over each other and designed to work with each other:
  - Application layer: it is where the network-aware application resides. For example SSH and FTP programs.
  - Transport layer: where TCP and UDP exist. TCP provides a two-way, reliable data transfer with error correction mechanisms. UDP provides a faster data transfer but one way and with no verification mechanisms.
  - Network layer: contains the Internet Protocol (IP) and Internet Control Message Protocol (ICMP). Both of which provide low level support for routing and error correction.
  - Link layer: where network drivers operate. It also contains the ARP (Address Resolution Protocol), which is responsible for translating logical addresses (IP) to hardware addresses (MAC).
  - Physical layer: the network medium where data travels (copper wires, radio waves…etc.).
- As data travels from the top layer to the bottom before it enters the transfer medium, each layer adds a *header* information. This is called *encapsulation*. When received, this data is interpreted from the bottom layer upward.

The Link layer

- To enable TCP/IP to support different kinds of networks (Ethernet, token ring…etc.) there had to be an abstraction between differnt layers. The Link layer, for example, is responsible for managing the low level harware details of the specific network. It is where the drivers decide the way data will be sent and received. Other layers do not and should not care about the network medium as it is abstracted by the Link layer.
- The link layer determines the maximum length of the *packet*, which is the unit of data transferred over the network. This is governed by the hardware limits and the protocol specification.
- For example, an Ethernet packet is about 1500 bytes, a PPP modem link packet is between 512 and 576, and a Point-to-Point WAN link could be between 1500 and 4500 bytes.

How do packets know their destinations?

- Several methods are used in conjunction: MAC addressing, IP (v4 or v6) addressing, and hostnames.
- MAC address
  - it is a 6-byte address assigned to the network adapter at time of manufacture. It is unique among all network adapters.
  - It represented in hex format in pairs separated by colons. For example: `00:0a:95:9d:68:16`. The first 3 bytes identify the vendor. For example: `00:0a:95` is for Apple Computers Inc. A comprehensive list can be found at http://iana.org/assignments/ethernet-numbers
  - Although MAC address were intended to be unique, many adapters offer a way to change them, especially if you are on a virtual machine.
- IP addressing
  - An IP address consists of 32 bits that can be represented as four numbers separated by dots. For example 192.168.1.100. The ARP protocol on the link layer translates this IP address to the physical MAC address to enable communication.
- Hostnames
  - Human-readable names of machines. Translation from hostnames to IP addresses can be done through several systems from machine hosts files to LDAP databases or DNS systems.
  - The application running on the host uses a 16-bit number called a port so that the operating system can correctly direct messages to the intended recipient application.

IP addressing

- An IP address is divided into the network (subnet) and the physical host.
- When an IP address starts with 127 this means it is referring to the loopback network. If the IP address is 127.0.0.1, it is referring to the current host (the loopback address)
- Classes were introduced to define which part of the IP address represent the host address and which represent the network id.
- The number 0 is used as a network id and 255 is used as a broadcast address so they are excluded from any network range.
- A netmask is used to specify the network and host portion of an IP address. For example: 192.168.5.10/24 is a class C IP address.
- Classful IP addressing can be summarized as follows:

Class	Range	Network/Host representation (binary format)	Possible hosts	Possible networks	Netmask
A	1 – 127	0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH	16,777,214	126	8
B	128 – 191	10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH	65,534	16,384	16
C	192 - 223	110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH	254	2,097,152	24

Classless Inter Domain Routing (CIDR)

- As depicted in the table, default subnet classes wasted a lot of addresses. Note that 127 is reserved for loop back addresses.
- To make better use of the wasted space, subnetting was introduced to divide a single octet between the network and the host instead of being assigned exclusively to one of them.
- For this reason CIDR was introduced. It allows the octet to be shared between the network id and the host id
- You can use the following online tool to calculate CIRD notation address spaces: http://jodies.de/ipcalc
- It can be applied using the following mechanism:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Class	Possible network bits	Possible subnets	Possible hosts
A	8 – 30	1 – 4,194,304	2 – 16,777,214
B	16 – 30	1 – 16,384	2 – 65,534
C	24 – 30	1 – 64	2 – 254

Private address spaces and NAT

- Private address spaces were introduced to address the problem of growing number of hosts requiring unique addresses.
- Those addresses should not *directly* access the Internet. Accordingly, they can be assigned multiple times at the same time
- They can be listed as follows:
  - 10.0.0.0 – 10.255.255.255 (class A)
  - 172.16.0.0 – 17.31.255.255 (class B host id is talking 20 bits)
  - 192.168.0.0 – 192.168.255.255 (Class C. Host id is taking 16 bits)
- To access the Internet, a protocol called NAT (network address translation) is used. It translates the internal IP address to one public address used to access the Internet. When the response is returned from the Internet, NAT routes this response to the internal IP that initiated the request.
- NAT uses port forwarding to enable internal addresses to receive requests from the outside
- NAT is not and cannot replace a firewall solution.

Routing

- It is the method by which a packet finds its way from source IP to destination IP through a set of one or more networks (or subnets).
- Paths (routes) are defined in a routing table that is stored in the kernel.
- If there are no defined routes for a packet, it is directed to a “default route”
- If there are no defined routes for the packet and no default route, “network unreachable” message is returned, which is an ICMP error.
- Routing table can be displayed using the `netstat -r` command. –n can be added to avoid DNS lookups:
  - The destination address may be a network or a host
  - The IP 0.0.0.0 indicates the default route
  - The default gateway must be a device that exists on the same network
- A route can be added statically, for example:

  ```
  route add –net 8.8.8.8 netmask 255.255.255.254 gw 192.168.0.1
  ```
- Dynamic routing is done through routing daemons that manages the routing tables.

ARP: Address Resolution Protocol

- It is used for translating the IP address of a machine to the physical MAC address of the adapter so that data can flow between source and destination devices
- If the target machine is not on the same network, the routing table is consulted to determine the next hop and ARP is used to find the router's MAC address
- When the source machine wants to send data to the target machine, it broadcasts a message on Ethernet asking other machines on the network "Who is using this IP x.x.x.x?" the taget machine replies with it's MAC address. The request includes the IP address and MAC address of the source machine so that the target one does not have to do the same broadcast message to reply.
- Accordingly, one request makes two machines learn the MAC addresses of each other. Other machine on the network receives this request and may save it in their *ARP cache*. This helps reduce the overall network traffic.

DHCP: Dynamic Host Configuration Protocol

- It is a service/protocol that ensures that every device on the network gets *at least* an IP and a default gateway. DHCP can also be used to provide default DNS servers, NTP servers and other parameters.
- When a device receives its address information, it keeps it for the duration of a lease period (which is configurable on the server side). Within this lease, the machine must periodically contact DHCP server to renew it (when lease is half over). If the lease is not renewed it expires and the address can be reassigned to a new device.
- When a new device gets attached to the network, it sends a broadcast message to the broadcast IP address (like 192.168.1.255). If a DHCP server is present on the same network, it starts communicating information to the client. Otherwise, the message can traverse networks through DHCP *relay* until it reaches the DHCP server.
- Clients should keep their DHCP information persistent across reboots.