Intro to Networking

M. Baricevic
CNR-INFM Democritos
Trieste
Italy
INTRO TO NETWORKING

PART 1: Basic concepts
Agenda

- Connections
- Concept of Packet
- Network Stack Models (TCP/IP - ISO/OSI)
- Internet Protocol and IP Address Space
- Ethernet and Physical Address
- Speed, Bandwidth, Latency, Throughput
- High Speed (and Low Latency) Networks
- **LINUX commands** (configuration and diagnostic)
Connections
**Connections**

```
host-1.site-A$ ssh host-2.site-A

host-X.site-A$ ssh host-Y.site-B
```
Example: the lab network

INTERNET

SMR2068.ictp.it
NEXUS.lab

BORG.hwlab

IOSRV.hwlab

CL1.hwlab

CL2

CL3

CL4

node1.hpc

nodeX.cl1

nodeX.cl2

nodeX.cl3

nodeX.cl4

HPC2068.lab

EKLUND-X.lab

INFOLAB-X.lab

nodeX.hpc

HUB (switch)

HOST

SERVER/GATEWAY
Concept of Packet
Addressing and Multiplexing

From Address:
Country
City
Street and Number
Name

To Address:
Country
City
Street and Number
Name/Apartment/Floor

Source Address:
hostname: host-a
domain: example.com
IP address: 192.0.32.10
protocol: TCP
port: 35432

Destination Address:
hostname: host-b
domain: example.org
IP address: 192.0.2.44
protocol: TCP
port: 25 (SMTP)
Fragmentation and Windowing

NETWORK CONNECTIONS ARE (OFTEN) NOT RELIABLE
BANDWIDTH IS NOT FREE AND IS NOT UNLIMITED

In case of failure, sending twice a large amount of data has a cost, both in terms of money and time. Network protocols split and fragment the data stream, TCP uses sequence numbers to reassemble the data in case they reach the destination out of order (retransmission, timeout, different routes,...).
Network Stack
Network Stack Models

TCP/IP Model

- Application
- Transport
- Internet
- Network Access
- Protocols
- Networks

ISO/OSI Model

1. Physical
2. Data Link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

Logical Addressing
- objects (e-mails, web pages, ...)
- streams (segments, packets, frames)

Physical Addressing
- bits (voltage levels, light impulses, ...)
TCP/IP Model

Protocols

- **Application**
  - E-Mail (SMTP),
  - Web (HTTP), ...
- **Transport**
  - TCP, UDP
- **Internet**
  - IP, ICMP, ...
- **Network Access**
  - ETHERNET (10/100/1G/10G), ...

11
Encapsulation/De-encapsulation

TCP/IP

Application Layer

Transport Layer (TCP)

Internet Layer (IP)

Net. Access Layer (Ethernet)

Media (copper/fiber/air/...)

USER DATA

App. Header

USER DATA

TCP Header

APPLICATION DATA

TCP Segment

IP Datagram/Packet

Ethernet Frame

Ethernet Header

IP Header

TCP Header

APPLICATION DATA

Ethernet Trailer

00100110101001000111100101001
Data flow

host X → switch → router → router → switch → host Y

- Switches inspect the traffic for layer 2 info (MAC)
- Routers inspect the traffic for layer 3 info (IP)
End-to-end connection

[1]
Src IP: 10.1.0.1
Src Port: 1234
Dst IP: 10.2.0.1
Dst Port: 22

[2]
Src IP: 10.2.0.1
Src Port: 22
Dst IP: 10.1.0.1
Dst Port: 1234
Internet Protocol and IP Address Space
Internet Protocol

The **Internet Protocol (IP)**:

- provides network connectivity at **layer 3**
- it's a **hierarchical network-addressing scheme**
- **addresses are used to route packets** from a source to a destination through the **best available path**
- is a **connectionless, unreliable, best-effort delivery protocol** (verification handled by upper protocols)
The **IP address** is:

something like this: **10.1.2.3**

- a **numerical label** which **uniquely identify each host on a network**
- logically divided in two parts, the *network* portion and the *host* portion
- obtained by the ISP (public IPs) or the system/network administrator (private IPs)
- **assigned** to a host **statically or dynamically** (BOOTP/DHCP)
- a 32bits/4bytes unsigned integer number, usually **represented in a dotted-decimal notation**, as four 8bits/1byte numbers (0-255), called “octets”, separated by a dot '.'
Netmask, Network and Broadcast

The **network address**:
- identifies the network itself
- defines the group of IP addresses that belongs to the same broadcast domain, hosts that can communicate with each other without the need of a layer 3 device
- is an IP address with the **host portion filled by 0s** (10.1.2.0)

The **netmask address** is:
- a bit-mask of contiguous 1s (starting from the MSB) that separates the host portion from the network portion of an IP address (1s on the network portion, 0s on the host portion)
- often represented in the “slash format” as the total number of bits used for the network and subnetwork portion of the mask (/8, /16, /24, /32, ...)
- something like this: 255.255.255.0

The **broadcast address** is:
- a network address that allows information to be sent to all nodes on a network, rather than to a specific network host (unicast)
- an IP address with the **host portion filled by 1s** (10.1.2.255)
**IP Address Notation**

- **Dotted Quad Notation** *(four-octet dotted-decimal, numbers-and-dots)*
  - 10.240.27.73 / 255.255.255.0 (10.240.27.73/24)

- **Hexadecimal Notation**
  - 0AF01B49 / FFFFF00

- **Binary Notation**
  - 00001010 11110000 00011011 01001001 / 11111111 11111111 11111111 00000000

```
  NETWORK PORTION      HOST PORTION
  +-------------------+-------------------+
  | 11111111 11111111 11111111 | 00000000 00000000 |
  | 00001010 11110000 00011011 | 01001001 00000000 |
  | 00001010 11110000 00011011 | 0AF01B49 0AF01B00 |
  | 00001010 11110000 00011011 | 11111111 0AF01BFF |
  +-------------------+-------------------+
  | 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 |
  | 10.240.27.73 10.240.27.73 10.240.27.73 10.240.27.73 |
  | 73 73 73 73 |
```
Reserved IP Addresses

- “This” network: 0.0.0.0/8
- Loopback: 127.0.0.0/8
- Private addresses:
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
- “TEST-NET” (example.com, org, net): 192.0.2.0/24
- 6to4 Relay: 192.88.99.0/24
- “Link local” (zeroconf): 169.254.0.0/16
- Multicast: 224.0.0.0/4
Host names, Domain names and DNS

- **hostname**
  - `cerbero.hpc.sissa.it`

- **first level domain**
  - `cerbero.hpc.sissa.it`

- **second level domain**
  - `cerbero.hpc.sissa.it`

- **third level domain**
  - `cerbero.hpc.sissa.it`

- **Fully Qualified Domain Name (FQDN)**
  - `cerbero.hpc.sissa.it`

- **DNS**
  - `cerbero.hpc.sissa.it` --> 147.122.17.62
  - 147.122.17.62 --> `cerbero.hpc.sissa.it`
Routing

- **routers** are layer 3 devices that **use the IP address to move data packets between networks**.
- when packets arrive at an interface, the router uses the **routing table** to determine where to send them.
- each router that the packet encounters along the way is called a **hop**, the **hop count** is the distance traveled.
- routing **metrics** are used to determine the **best path** (hop count, load, bandwidth, delay, cost, and reliability of a network link).
Best path determination

Host A

Host B

Hop Count = 1

Host A -> Host B  cost = 1

Host A -> Host C  cost = 3

Host C

Hop Count = 5  

Hop Count = 4  

Hop Count = 3  

23
End-to-end connection (try 2)

[1]
Src IP: 10.1.0.1
Src Port: 1234
Dst IP: 10.2.0.1
Dst Port: 22
Protocol: TCP

- Clients use random source ports (> 1023)
- Servers are bound to fixed ports

[2]
Src IP: 10.2.0.1
Src Port: 22
Dst IP: 10.1.0.1
Dst Port: 1234
Protocol: TCP
Protocols, Ports and Services

TCP

UDP

IP

Internet

LAN

WAN

FTP

SSH

SMTP

HTTP

DNS

DNS

DHCP

TFTP

NTP
Summary (so far)

- fragmentation
- protocols
- IP addresses
- DNS
- routing
- ports
Ethernet and Physical Address
MAC Address

The *Media Access Control Address* is:

- a **physical address, globally unique**
- **assigned by the manufacturer** of the NIC and **burned-in into the PROM of the NIC** (in some cases, can be administratively assigned)
- part of the Ethernet protocol and **operates at Layer 2**
- sometimes called **Ethernet Hardware Address** (EHA)
- **used by DHCP to dynamically assign IP Addresses**
- a 48bits number represented as a 6 groups of two hexadecimal digits (6 bytes) separated by `:'` (00:1d:09:d7:3b:25), made of two parts, 3 bytes each:
  - the OUI (Organizationally Unique Identifier)
  - the production number
Cables and connectors

- bandwidth varies depending upon the type of media as well as the technologies used, the physics of the media account for some of the difference
- signals travel through twisted-pair copper wire, coaxial cable, optical fiber, and air
- the physical differences in the ways signals travel result in fundamental limitations on the information-carrying capacity of a given medium
- actual bandwidth of a network is determined by a combination of the physical media and the technologies chosen for signaling and detecting network signals.
That's All Folks!

“Network is down.”

(questions; comments) | mail -s uheilaaa baro@democritos.it

(complaints; insults) &>/dev/null
REFERENCES AND USEFUL LINKS

SOFTWARE:
- Linux Kernel [http://www.kernel.org]
- Netfilter [http://www.netfilter.org]
- nmap [http://www.insecure.org/nmap/]
- hping [http://www.hping.org/]
- netcat [http://netcat.sourceforge.net/]
- iptstate [http://www.phildev.net/iptstate/]
- ss [http://linux-net.osdl.org/index.php/lproute2]
- lsof [ftp://lsof.itap.purdue.edu/pub/tools/unix/lsof/]
- netstat [http://www.tazenda.demon.co.uk/phil/net-tools/]
- tcpdump [http://www.tcpdump.org]
- wireshark [http://www.wireshark.org]
- ethereal [http://www.ethereal.com (see wireshark)]
- iptraf [http://iptraf.seul.org/]
- ethtool [http://ethtool.sourceforge.net]
- dnsns [http://www.monkey.org/~dugsong/dsniff/]
- tcptraceroute [http://michael.toren.net/code/tcptraceroute/]
- (telnet, traceroute, ping, ...)

DOC:
- IPTables HOWTO [http://www.netfilter.org/documentation/HOWTO/]
- IPTables tutorial [http://iptables-tutorial.frozentux.net/]
- Denial of Service [http://www.cert.org/tech_tips/denial_of_service.html]
- IPv4 Address space
  - [http://www.cymru.com/Documents/bogon-bn.html]
  - [http://www.iana.org/assignments/ipv4-address-space]
  - [http://www.oav.net/mirrors/cidr.html]
- IANA [http://www.iana.org]
- RIPE [http://www.ripe.net]
- RFC 3330 [http://www.ripe.net/rfc3330.html]
- SANS [http://www.sans.org/reading_room/whitepapers/firewalls/]
  [http://www.sans.org/reading_room/]

RFC:
- [http://www.rfc.net]
  - RFC 791 – Internet Protocol (IPv4) [http://www.rfc.net/rfc791.html]
  - RFC 793 – Transmission Control Protocol (TCP) [http://www.rfc.net/rfc793.html]
  - RFC 768 – User Datagram Protocol (UDP) [http://www.rfc.net/rfc768.html]
  - RFC 792 – Internet Control Message Protocol (ICMP) [http://www.rfc.net/rfc792.html]
  - RFC 1180 – A TCP/IP Tutorial [http://www.rfc.net/rfc1180.html]
  - RFC 1700 / IANA db – Assigned Numbers [http://www.rfc.net/rfc1700.html]
  - [http://www.iana.org/numbers.html]
  - RFC 3330 – Special-Use IPv4 Addresses [http://www.ripe.net/rfc3330.html]
  - RFC 1918 – Address Allocation for Private Internets [http://www.ripe.net/rfc1918.html]
  - Unofficial CIPWG [http://www.blug.linux.no/rfc1149/]
  - RFC 2549 – IP over Avian Carriers with Quality of Service [http://www.ripe.net/rfc2549.html]
  - Firewalls the CIP [http://www.tibonia.net/]
    [http://www.hotlink.com/wacky/dastrdy/]

32
Some acronyms...

**ICTP** – the Abdus Salam International Centre for Theoretical Physics  
**DEMOCRITOS** – DEMOCRITOS Modeling Center for Research in aTomistic Simulations  
**INFN** – Istituto Nazionale per la Fisica della Materia (Italian National Institute for the Physics of Matter)  
**CNR** – Consiglio Nazionale delle Ricerche (Italian National Research Council)

**IP** – Internet Protocol  
**TCP** – Transmission Control Protocol  
**UDP** – User Datagram Protocol  
**ICMP** – Internet Control Message Protocol  
**ARP** – Address Resolution Protocol  
**MAC** – Media Access Control

**OS** – Operating System  
**NOS** – Network Operating System  
**LINUX** – LINUX is not UNIX

**PING** – Packet Internet Groper

**FTP** – File Transfer Protocol – (TCP/21,20)  
**SSH** – Secure SHeIl – (TCP/22)  
**TELNET** – Telnet – (TCP/23)  
**SMTP** – Simple Mail Transfer Protocol – (TCP/25)  
**DNS** – Domain Name System – (UDP/53)  
**NTP** – Network Time Protocol – (UDP/123)  
**BOOTPS** – Bootstrap Protocol Server (DHCP) – (UDP/67)  
**BOOTP** – Bootstrap Protocol Server (DHCP) – (UDP/68)  
**TFTP** – Trivial File Transfer Protocol – (UDP/69)  
**HTTP** – HyperText Transfer Protocol – (TCP/80)  
**NTP** – Network Time Protocol – (UDP/123)  
**SNMP** – Simple Network Management Protocol – (UDP/161)  
**HTTP** – HyperText Transfer Protocol over TLS/SSL – (TCP/443)  
**RSH** – Remote Shell – (TCP/514,544)

**ISO** – International Organization for Standardization  
**OSI** – Open System Interconnection  
**TLS** – Transport Layer Security  
**SSL** – Secure Sockets Layer

**RFC** – Request For Comments  
**ACL** – Access Control List  
**PDU** – Protocol Data Unit

**TCP flags:**  
**URG**: Urgent Pointer field significant  
**ACK**: Acknowledgment field significant  
**PSH**: Push Function  
**RST**: Reset the connection  
**SYN**: Synchronize sequence numbers  
**FIN**: No more data from sender

**RFC 3168 TCP flags:**  
**ECN**: Explicit Congestion Notification  
**ECE**: ECN Echo  
**CWR**: Congestion Window Reduced

**ISN** – Initial Sequence Number