Video Lecture # 33
Overview of TCP/IP Architecture and Services

Course: SYSTEM PROGRAMMING

Instructor: Arif Butt
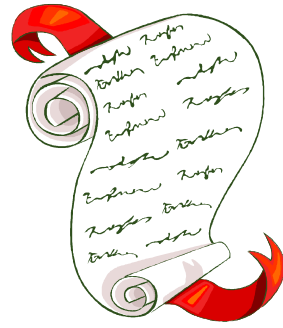
Punjab University College of Information Technology (PUCIT)
University of the Punjab

Today's Agenda

- TCP/IP Stack
- Addressing on TCP/IP Layers
- Important NW Services
- Hands on Linux Network Configuration Tools
- Configuring and using Linux Servers
  - SSH/Telnet
  - Echo
  - Daytime
  - Time
  - Chargen
  - Discard
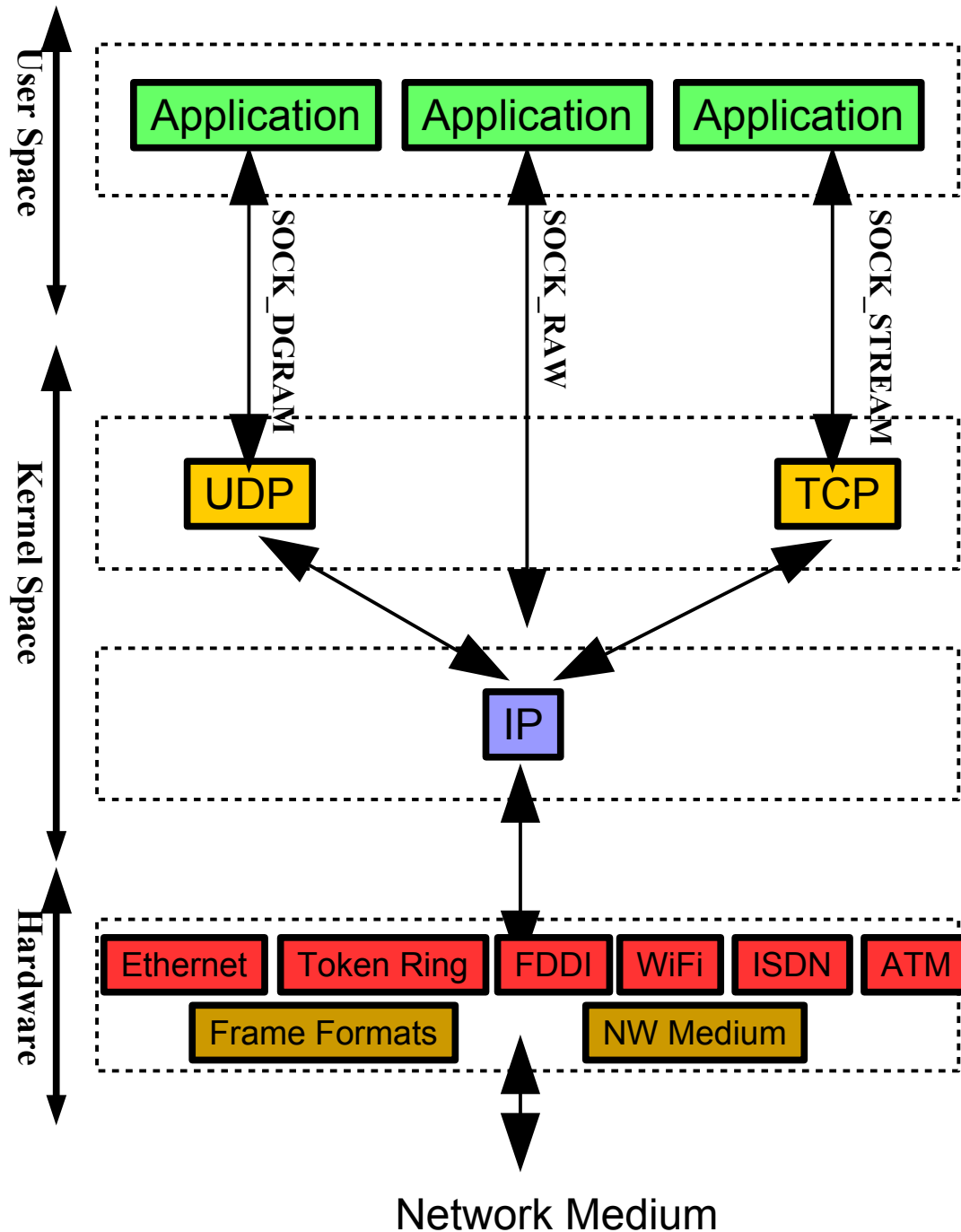
Internetworking with Linux:
https://www.youtube.com/playlist?list=PL7B2bn3G_wfD6_mhy-eLdn_mFgQ_mOyLl

TCP/IP Stack

Protocols in TCP/IP Suite

User Space

Kernel Space

Hardware

Application   Application   Application

SOCK_DGRAM   SOCK_RAW   SOCK_STREAM

UDP   TCP

IP

Ethernet   Token Ring   FDDI   WiFi   ISDN   ATM

Frame Formats   NW Medium

Network Medium

Application Layer
- Consist of processes that uses the NW
- Provides programming interface used for building a program
- Protocols used are http, telnet, ftp, smtp, ssh
- Addresses are string based URIs (URL, URN)

Transport Layer
- Provides host-to host communication
- Protocols used are TCP, UDP, RAW
- 16 bits Port numbers are used for addressing

Internet Layer
- Break data into fragments small enough for transmission via link layer
- Routing data across internet
- Protocols used are IP, ICMP, IGMP
- IPv4 and IPv6 are used for addressing

Link Layer/ Physical Layer
- Place packets on the NW medium and receiving packets off the NW medium
- Protocols used are Ethernet, Token ring, FDDI, ISDN, SONET, ATM
- 48 bit Mac address are used for addressing

4

Addressing Schemes Used On TCP/IP Layers

Addressing on the Application Layer

- A host on the Internet can be uniquely identified by a Fully Qualified Domain Name (FQDN), having two parts

<p align="center"><code>hostname.domain-name</code></p>

- A central authority (`iana.org`) manages the assignment of domain-names to organizations, which can be two or more strings separated by a period. A mapping of these hostnames with their corresponding IP addresses is kept in a hierarchical decentralized database and the service that performs a look up is called DNS/BIND (RFC:882, RFC:883)

- The organization can add prefixes to its domain name to define its hosts:

<p align="center"><code>pucit.pu.edu.pk</code></p>

- The organization can add suffixes to its domain name to define its resources:

<p align="center"><code>pucit.pu.edu.pk/academics/timetable-pucit.html</code></p>

- URL: A uniform resource locator is a string of characters used to identify a resource located on a specific host, on a specific domain on the Internet

`protocol://hostname.domain-name[:port]/pathtoresource`

`http://pucit.pu.edu.pk:80/academics/timetable-pucit.html`

Addressing on the Transport Layer

The transport layer addresses are called Port Numbers. A 16 bit integer used to identify a specific process to which a NW message is to be forwarded when it arrives at a host. There may be a machine which is running both the `http` and `ssh` service. The `http` process will be listening on port 80, while `ssh` process will be listening on port 22

- **Well Known / Reserved Ports (0 to 1023):** These are permanently assigned to specific applications (also known as services). For example, ssh daemon uses port 22. Well known ports are assigned numbers by a central authority the Internet Assigned Number Authority (`http://www.iana.org`)

- **Registered Ports (1024 to 49151):** IANA also records registered ports, which are allocated to application developers on a less stringent basis

- **Dynamic/Private/Ephemeral Ports (49152 to 65535):** IANA specifies the ports in the range 49152 to 65535 as dynamic or private, with the intention that these ports can be used by local applications. If an application doesn't select a particular port (i.e., it doesn't `bind()` its socket to a particular port), then TCP and UDP assign a unique ephemeral port (i.e., short-lived) number to the socket

View `/etc/services` file on your UNIX machine for details

Famous Well Known Ports

Protocol	Port	Service
echo	7	IPC testing
daytime	13	Provides current date and time
ftp-data, ftp	20, 21	File Transfer Control (TCP)
ssh	22	Secure Shell for secure Remote Login facility (TCP)
telnet	23	Remote login facility (TCP)
smtp	25	Simple Mail Transfer Protocol (TCP)
time	37	Provides standard time
bootps, bootpc	67, 68	Bootp server and client (UDP)
tftp	69	Trivial File Transfer Protocol (UDP)
finger	79	Provides information about a user
http	80, 8080	Web Server (TCP)
sunrpc	111	Sun Remote Procedure Call
NTP	123	Network Time Protocol (UDP)
https	443	Secure Web Server (TCP)
RMI Registry	1099	Registry for Remote Method Invocation
NFS	2049	Network File Server (UDP)

Class Full Addressing on the Internet Layer (IPv4)

Class A IP Addresses:

| 0 | Net ID (7) | Host ID (24) |

Total Addresses: $2^7 - 2$ (1.0.0.0 to 126.0.0.0)

Hosts per Address: $2^{24} - 2$

Subnet Mask: 255.0.0.0 or /8

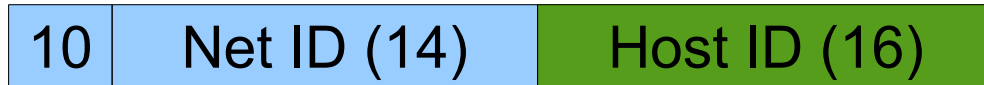**Example:**
NW Addr: 1.0.0.0
Host Addr Range: 1.0.0.1 to 1.255.255.254
Broadcast Addr: 1.255.255.255

Class B IP Addresses:

| 10 | Net ID (14) | Host ID (16) |

Total Addresses: $2^{14} - 2$ (128.0.0.0 to 191.255.0.0)
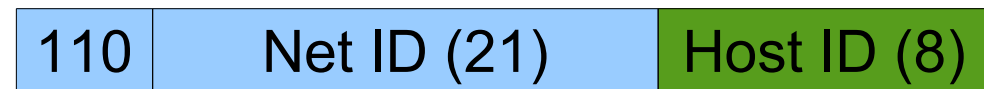
Hosts per Address: $2^{16} - 2$

Subnet Mask: 255.255.0.0 or /16

Example:
NW Addr: 128.0.0.0
Host Addr Range: 128.0.0.1 to 128.0.255.254
Broadcast Addr: 128.0.255.255

Class C IP Addresses:

| 110 | Net ID (21) | Host ID (8) |

Total Addresses: $2^{21} - 2$ (192.0.0.0 to 192.255.255.0)

Hosts per Address: $2^8 - 2$

Subnet Mask: 255.255.255.0 or /24

Example:
NW Addr: 192.0.0.0
Host Addr Range: 192.0.0.1 to 192.0.0.254
Broadcast Addr: 192.0.0.255

Classless Addressing on the Internet Layer (IPv4)

- There are about 4 billion IPv4 addresses, and this address space has gone full. ICANN is using a scheme called Classless Internetwork Domain Routing (CIDR), which has significantly extended the useful life of IPv4

- ICANN has taken away many class A and class B addresses from organizations and is using them to create IP addresses with lesser number of host computers and then issuing these classless IP addresses to organizations

- **Example:** In /28 networks, ICANN controls the leftmost 28 bits for the NW part with remaining 4 bits under the control of the organization it is issued to. This gives the organization 2^4 - 2 IP addresses to use as hosts

- **Problem:** What if the organization is having more than 14 hosts?

- **Solution:** Private IP addresses

Private IP Addresses (IPv4)

- IETF has designed three address ranges as private. These are non routable, and can only be used either on a fully disconnected NW or on a NW behind firewall

- Firewalls translates private IP addresses to public IP addresses using a process called NW Address Translation (NATing)

- NAT allows a single device called gateway computer (router) having a public IP address to act as an agent between the Internet and the private NW

- So this means that a single public IP address can represent an entire group of computers

- CIDR and NATing has significantly extended the useful life of IPv4

Class	IP Address Range	Count	Subnet Mask
A	10.0.0.0 to 10.255.255.255	2^{24}	/8
B	172.16.0.0 to 172.31.255.255	2^{20}	/12
C	192.168.0.0 to 192.168.255.255	2^{16}	/16

Addressing on the Network Layer (IPv6)

- Using IPv4 address format (32 bits) we can assign 4 billion addresses. Using IPv6 address format (128 bits) we can assign over 340 trillion trillion trillion addresses. (means one million IPv4 addresses to every star in this universe)
- IPv6 addresses are typically written as a series of 16-bit hexadecimal numbers separated by colons, as in the following:

`F000:0:0:0:0:0:A:1`

- IPv6 addresses often include a sequence of zeros and, as a notational convenience, two colons (::) can be employed to indicate such a sequence. Thus, the above address can be rewritten as:
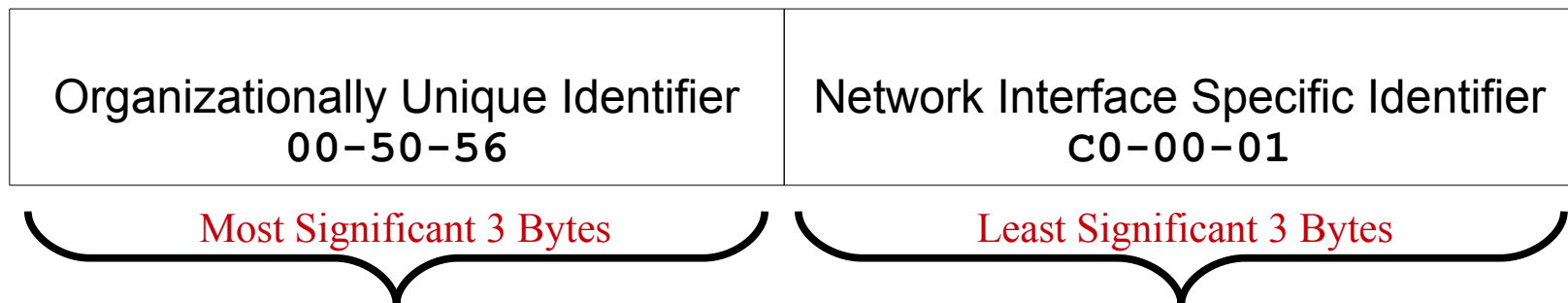
`F000::A:1`

- Only one instance of the double-colon notation can appear in an IPv6 address; more than one instance would be ambiguous
- IPv6 also provides equivalents of the IPv4's loopback address (127.0.0.1 is equivalent to ::1) and wildcard address (0.0.0.0 is equivalent to either 0::0 or ::)
- When writing an IPv4-mapped IPv6 address, the IPv4 part of the address (i.e., the last 4 bytes) is written in IPv4 dotted-decimal notation. Thus, the IPv4-mapped IPv6 address equivalent to 204.152.189.116 is ::FFFF:204.152.189.116

All zeros	FFFF	IPv4 address
80 bits	16 bits	32 bits

Addressing on the Physical Layer

- The 48 bit addresses used on the Physical layer are called MAC address
- Before a manufacturer can build Ethernet products, it asks the IEEE to assign the manufacturer a universally unique 3-byte code, called the organizationally unique identifier (OUI). The manufacturer agrees to give all Ethernet products a MAC address that begins with its assigned 3-byte OUI. The manufacturer also assigns a unique value for the least significant 3 bytes, a number that manufacturer has never used with that OUI, thus making the address of that device unique
- If the destination IP address of a NW message is not in the same local area NW then the packet is sent to the configured gateway computer for routing
- If the destination IP address of a NW message is in the same local area NW then the source computer uses Address Resolution Protocol to get the destination MAC address from the destination IP address
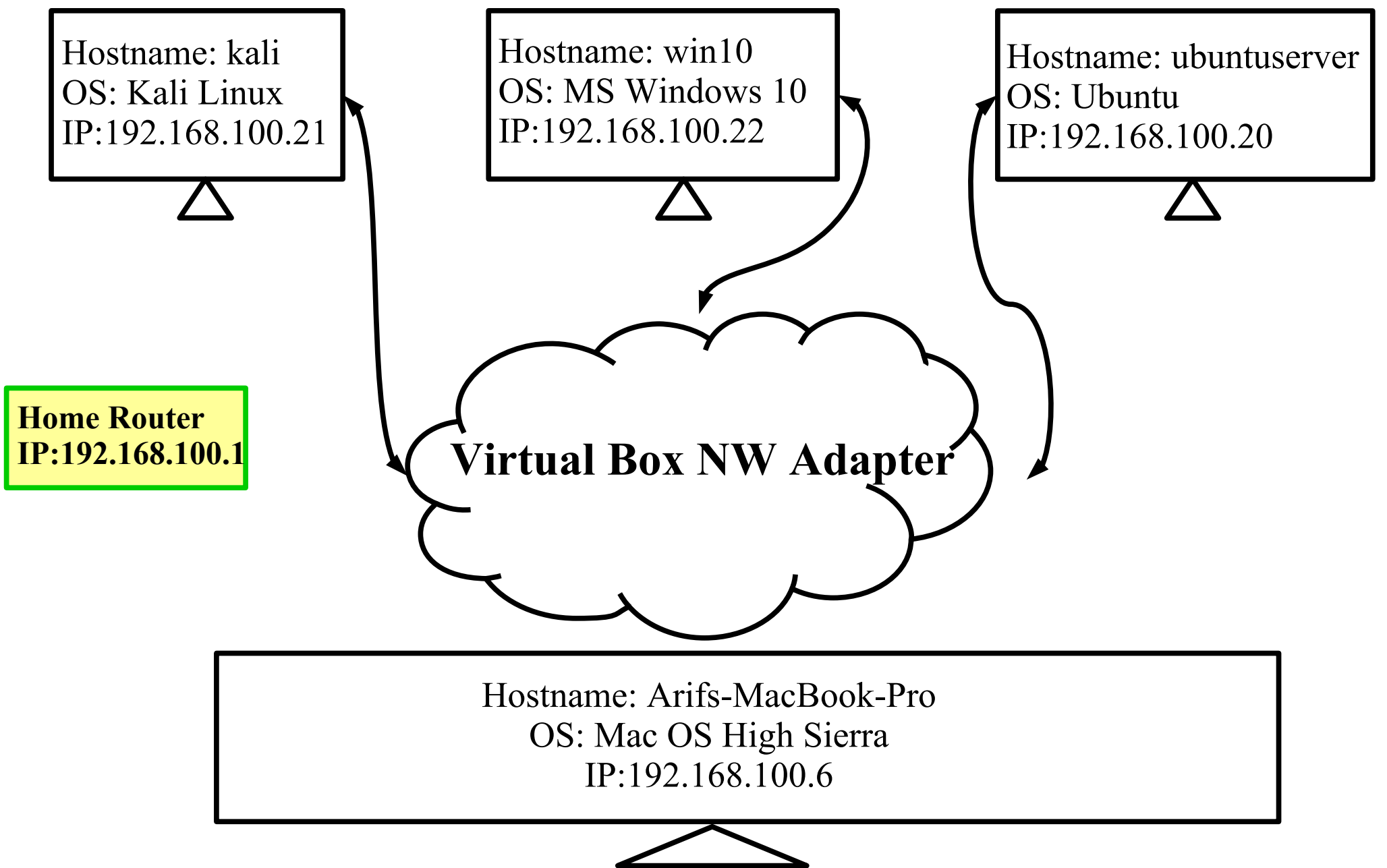
Organizationally Unique Identifier 00-50-56	Network Interface Specific Identifier C0-00-01
Most Significant 3 Bytes	Least Significant 3 Bytes

Lab Setup

Lab Scenario

Hostname: kali
OS: Kali Linux
IP:192.168.100.21

Hostname: win10
OS: MS Windows 10
IP:192.168.100.22

Hostname: ubuntuserver
OS: Ubuntu
IP:192.168.100.20

Home Router
IP:192.168.100.1

Virtual Box NW Adapter

Hostname: Arifs-MacBook-Pro
OS: Mac OS High Sierra
IP:192.168.100.6

NW Configuration Lab Environment Proof of Concept

Things To Do

If you have problems visit me in counseling hours. . . .