Recap Guide 1: Binary (Base 2), IP Address, Subnet Masks

Recording is here

This recap guide is designed to help you quickly revisit and build confidence in all the concepts, commands and practical frameworks covered in your session led by Mark McGinley.

Use this as a reference to strengthen your understanding and as a checklist for your independent study. Let's break it down step by step.

Timestamps

00:00 Preview of Security Course Labs

15:27 "Intro to IP Addressing"

28:20 IP Address and Network Explanation

37:40 Weekend Binge: Network Protocols Prep

44:08 Data Quality Influences Search Accuracy

01:01:08 Network Simulator Introduction

01:12:59 Practice Labs Build Job Confidence

01:21:54 "Saving NMAP Output"

01:33:44 "Exploring Network Tools Tutorial"

01:38:18 Cisco Learning: Packet Tracer Tool

01:48:59 Switch Management IP Setup

01:57:42 Coordination in Collaborative Environments

02:12:42 Understanding VLANs and Native VLAN Setup

02:17:39 VLAN Tagging Discussion

Videos Mark Recommends To Watch

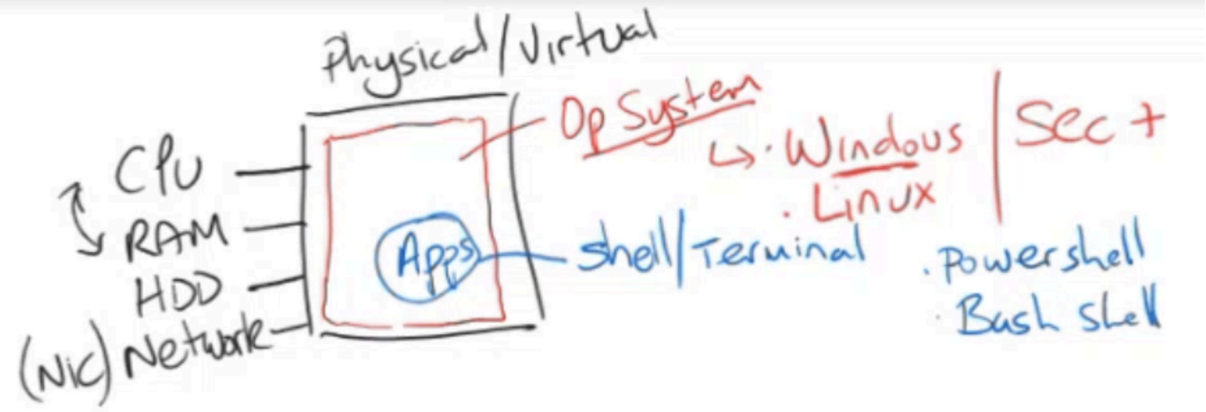
1. How do Hard Disk Drives Work? 💻💿🛠
2. How does Computer Memory Work? 💻🛠
3. How are Microchips Made? 🖥🛠 CPU Manufacturing Process Steps
4. How do Graphics Cards Work? Exploring GPU Architecture
5. How do Transistors Build into a CPU? 🖥🤔 How do Transistors Work? 🖥🤔
6. Operating Systems: Crash Course Computer Science #18
7. you NEED to learn Windows RIGHT NOW!!
8. EVERYONE needs to learn LINUX

1. Understanding Basic Computer Components in Networking

What are the main components of a computer in a network?

- **CPU (Central Processing Unit):** The 'brain' of the computer; handles processing tasks.
- **RAM (Random Access Memory):** Temporary memory the CPU uses for fast data access.
- **Storage:** Hard Drive (HDD) or Solid State Drive (SSD) for permanent data storage.
- **NIC (Network Interface Card):** Allows the computer to connect to a network.

Why do you need to know this?
These are the hardware pieces every networked device has, and understanding them is fundamental for troubleshooting, lab work, and security tasks.



2. Operating Systems in Networking

What operating systems are used?

- **Windows:** Most common in office/business environments (very graphical).
- **Linux:** Modern version of UNIX, widely used for servers and security.
- **Ubuntu:** A Linux-based operating system that’s friendly, stable and widely used for general computing.
- **Kali Linux:** Another Linux-based operating system, but focused on cybersecurity, penetration testing and ethical hacking tools.

Why is this important?

You will encounter all OS environments in labs and on the job. You must recognise and operate in both, especially using their respective command-line interfaces (CLI).

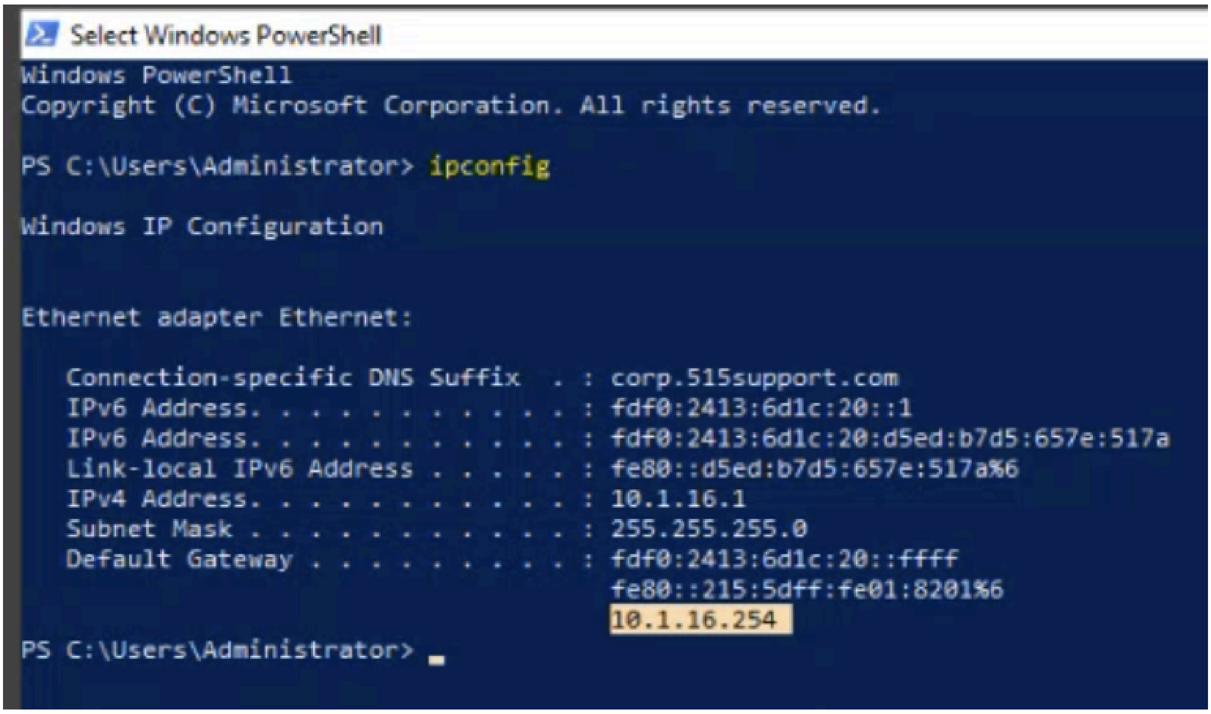
3. Shells & Command-Line Interfaces

- **Windows PowerShell** (for Windows environments)
- **Bash Shell** (for Linux environments)

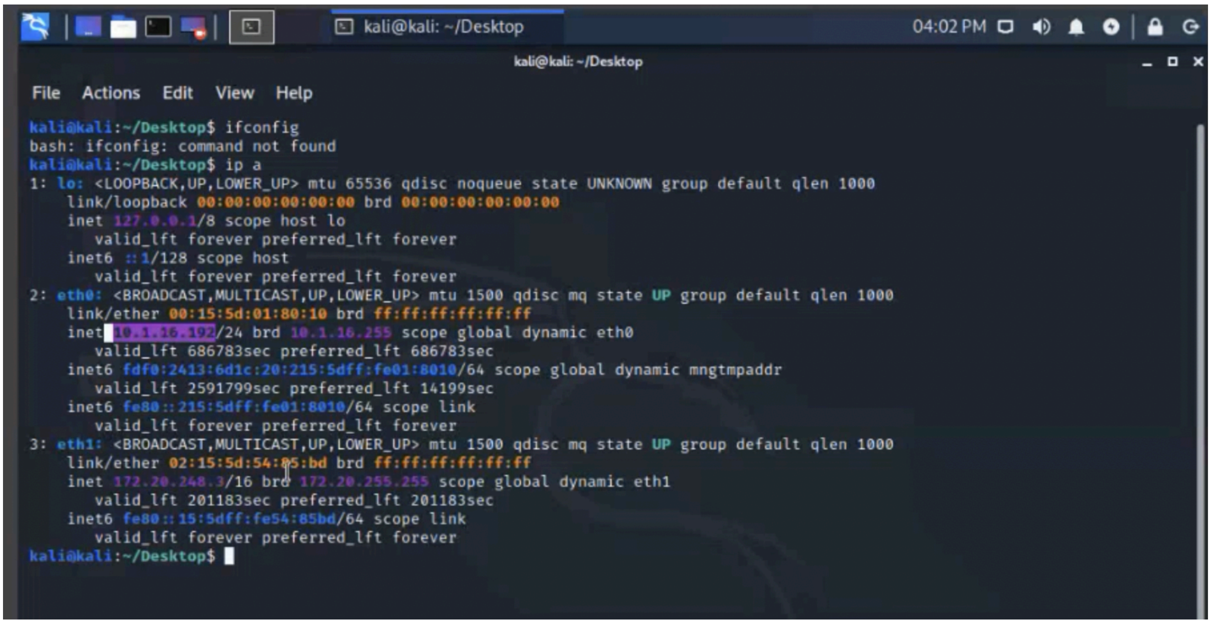
What is it? These are command-line programs (CLI) that let you interact directly with the OS to control devices, gather information, and run scripts.

How to Access:

- In Windows: Use the 'PowerShell' application.
- In Linux: Use 'Terminal' or 'Shell.'



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : corp.515support.com
   IPv6 Address. . . . . . . . . . . : fdf0:2413:6d1c:20::1
   IPv6 Address. . . . . . . . . . . : fdf0:2413:6d1c:20:d5ed:b7d5:657e:517a
   Link-local IPv6 Address . . . . . : fe80::d5ed:b7d5:657e:517a%6
   IPv4 Address. . . . . . . . . . . : 10.1.16.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fdf0:2413:6d1c:20::ffff
                                       fe80::215:5dff:fe01:8201%6
                                       10.1.16.254

PS C:\Users\Administrator> _
```



```
kali@kali:~/Desktop$ ifconfig
bash: ifconfig: command not found
kali@kali:~/Desktop$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:01:80:10 brd ff:ff:ff:ff:ff:ff
    inet 10.1.16.192/24 brd 10.1.16.255 scope global dynamic eth0
       valid_lft 686783sec preferred_lft 686783sec
    inet6 fdf0:2413:6d1c:20:215:5dff:fe01:8010/64 scope global dynamic mngtmpaddr
       valid_lft 2591799sec preferred_lft 14199sec
    inet6 fe80::215:5dff:fe01:8010/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 02:15:5d:54:85:bd brd ff:ff:ff:ff:ff:ff
    inet 172.20.248.3/16 brd 172.20.255.255 scope global dynamic eth1
       valid_lft 201183sec preferred_lft 201183sec
    inet6 fe80::15:5dff:fe54:85bd/64 scope link
       valid_lft forever preferred_lft forever
kali@kali:~/Desktop$ █
```

4. Virtual Machines & Labs

- **Virtual Machine (VM):** A simulated computer running within your actual system, used for hands-on practice labs.
- **Why?** VMs let you experiment, break things and learn without risking your real system.

Tip: You'll use VMs extensively for hands-on Security+ and networking labs.

5. Networking Essentials

IP Addressing

- **IP Address:** The unique identifier for each device on a network (like a house's street address).
    - Format: Four blocks (octets) of numbers, separated by periods, e.g., `10.1.16.1`
    - **IPv4:** Most common (uses 32 bits total; four 8-bit numbers)
    - **IPv6:** Next-generation IP addresses
- **Subnet Mask:** Used alongside IP addresses to determine what amount of the address refers to the 'network' vs. the specific 'host' (device).
    - Examples: `255.255.255.0` (`/24`), `255.255.0.0` (`/16`)
    - **Why?** It defines the boundaries of your network ('which devices are neighbors').

Example:

If your IP is `10.1.16.192` and subnet mask is `255.255.255.0`, then:

- **Network Portion:** `10.1.16`
- **Host Portion:** `.192` (for your device)

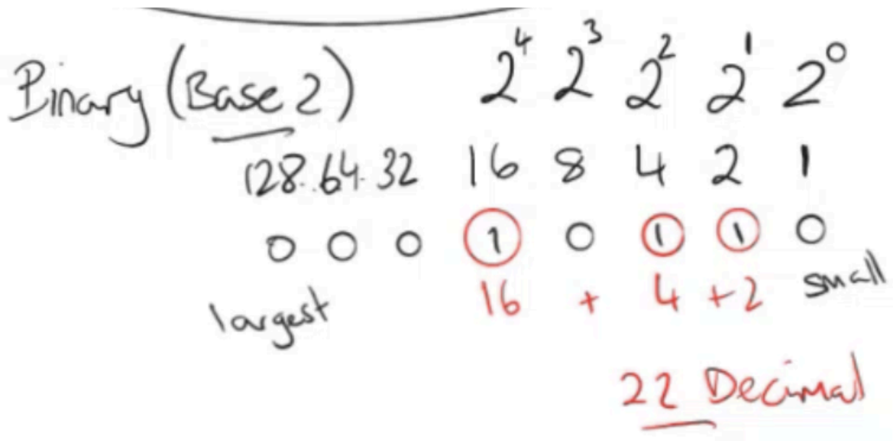
6. Binary (Base 2) & IP Addressing

Binary System: Computers use base-2 (0s and 1s) to represent data, including IP addresses.

How to Interpret Binary:

- Each bit (from right to left) has a value:
  `128 64 32 16 8 4 2 1`
- **Examples:**
  `00010110` = 0+0+0+16+0+4+2+0 = 22

Base 2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Calculation	2X2X2X2X2X2X2	2X2X2X2X2X2	2X2X2X2X2	2X2X2X2	2X2X2	2X2	2X1	2÷2
Total of all = 255	128	64	32	16	8	4	2	1
Binary	0	0	0	1	0	1	1	0
Total of 1 = 22				16		4	2	



Why do this?
Subnetting, IP address ranges and mask calculations use binary!

7. Key Networking Commands

On Windows (PowerShell):

To find out the IP address for your machine, type in the PowerShell:

- `ipconfig`

On Linux (Terminal or Bash):

To find out the IP address for your machine, type in the Terminal or Bash:

- `ifconfig`
- `ip addr` **(or** `ip a`**) =** Shows network interfaces and addresses.
- `ping [IP address]=` Tests network connectivity.
- `ls` / `ls -l =` List directory contents
- `cd [directory]` = Change directory.
- `cat [filename]` = Print the contents of a file.
- `nmap = Network mapper` scans hosts and services on a network.
- **Piping (**`|`**):**
  E.g., `ls -l | more =` (useful for long outputs, one page at a time)
  - **Note:** When using virtual keyboards in labs, sometimes the ‘pipe’ (|) character isn’t where you expect on your actual keyboard. Use the virtual keyboard's shift function to find it!
- **Redirect (use** `>`**):**
  - E.g., `nmap 10.1.16.12 > nmap.txt`
  - **To append:** use `>>`

8. Tools You’ll Use

NMap: Network Mapper, scans hosts and services on a network.

- Example: `nmap 10.1.16.12`
- Why? Quickly see what services/ports are open on a device.

Wireshark: Captures and analyses network traffic.

- Why? See what’s happening on the wire; used for packet/protocol analysis.

TCPDump: CLI tool for capturing traffic (Linux).

- Why? Similar to Wireshark, but CLI-based.

9. Interpreting Output & Practical Tasks

Yeah — that little block is describing how your local network carves up and organizes IP space. Here's what's going on underneath:

Default Gateway

- It's the "exit door" from your network, usually your router's IP.
  When your computer wants to reach the internet or another network, traffic goes to that gateway first (e.g. `10.1.16.254`).

Subnet Mask

- The `/24`, `/16`, `/8` defines how many bits of the **32-bit IP address** are for the **network** vs. the **hosts**.
  - `/24` → 24 bits for network, 8 bits left for hosts. = **24+8=32**
  - So `192.168.1.0/24` means every address from `192.168.1.1` to `192.168.1.254` belongs to that same network.

Network & Broadcast Addresses

- Every subnet has **two reserved addresses**:
  - **Network address (.0)** → identifies the subnet not a device.
  - **Broadcast address (.255)** → sends messages to *all* hosts in that subnet.

So if you have `192.168.1.0/24`:

- Network address → `192.168.1.0`
- Broadcast → `192.168.1.255`
- Usable host range → `192.168.1.1 – 192.168.1.254`

Putting It Together

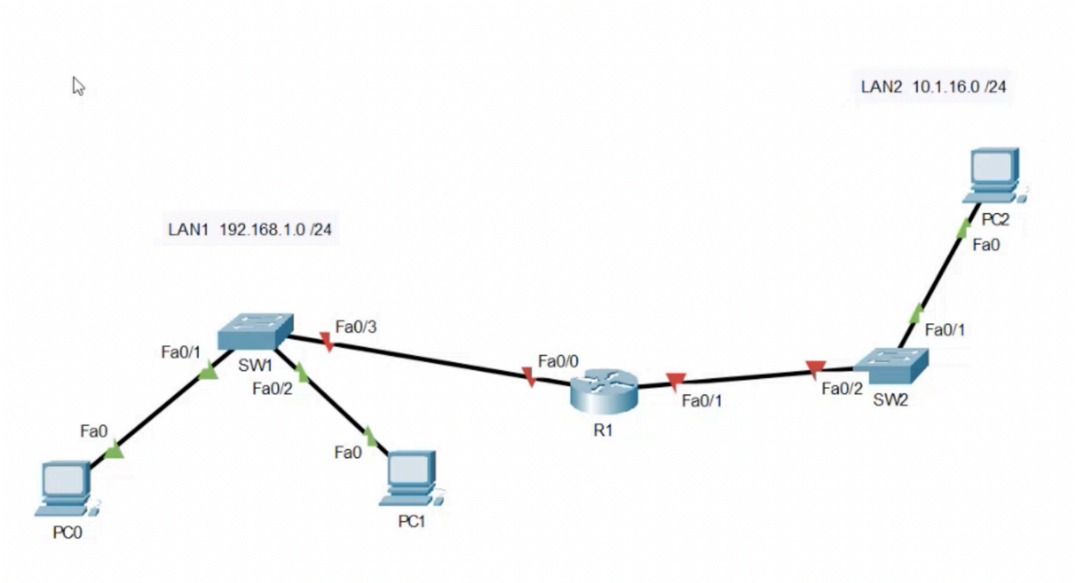
When your computer connects:

- It gets an IP (example: `192.168.1.5`)
- It knows the subnet mask (`255.255.255.0`) = 8 + 8+ 8 = 24 bits
- It knows the gateway address (`192.168.1.1`)

That info lets it figure out who’s “local” and who needs to go out through the router.

In plain terms:
Your subnet mask draws the borders of your digital neighborhood.
`.0` marks the street sign (the network), `.255` is the loudspeaker (broadcast), and the gateway is the door leading out of town.

10. Step-by-Step Guide: Creating a Basic Network in Packet Tracer



Download & Open Packet Tracer

- Follow this guide to download

Set Up a Label for Your Network

- Click the label icon (looks like a castle at the top).
- Click inside the workspace to place the label.
- Give your network a name (e.g., “LAN1”) and add your chosen network address (Mark used `192.168.1.0/24`).
- Resize and move the label as needed for clarity.

Add a Switch

- Click the "Network Devices" icon at the bottom.
- Choose "Switches" (it looks like a little box).
- Drag a 2960 switch (or default switch) into the workspace.

- Optionally, rename the switch (e.g., "SW1") by clicking on it and editing the name.

Add Computers (PCs)

- Click on "End Devices" (little PC icon) in the device list.
- Drag two PCs (e.g., "PC0" and "PC1") into the workspace.
- Rename them if you wish.

Connect Devices with Cables

- Click the lightning bolt icon for connections.
- Select "Copper Straight-Through" cable.
- Click the first PC, connect via FastEthernet0.
- Connect to Switch port FastEthernet0/1.
- Repeat the process for the second PC, using the next switch port.

Assign IP Addresses

- Click on a PC, go to the "Desktop" tab.
- Click "IP Configuration."
- Uncheck "DHCP" (set to Static).
- Enter the IP address (e.g., `192.168.1.2` for PC0, `192.168.1.3` for PC1), with subnet mask `255.255.255.0`.
- (Optional) Set Default Gateway as `192.168.1.1`—this is useful when you eventually add a router.
- Close the configuration window.

Check Network Functionality

- With both PCs configured, open the “Command Prompt” on PC0.
- Type `ping 192.168.1.3` to test connectivity to PC1
- You should see replies, confirming the switch and configuration are working.

Add a Router (Optional)
- Drag a router from "Network Devices" into the workspace.
- Connect the switch’s unused port to the router’s FastEthernet port.
- (When ready) Set the router’s interface IP (e.g., `192.168.1.1`) to serve as a gateway.

11. Next Steps

- Review this guide before every hands-on lab.
- Re-watch sections of the recording when you’re stuck.
- Work through Capture-The-Flag style exercises (e.g. HackTheBox) for extra practice.
- Ask questions in chat or during your next session if something is unclear.