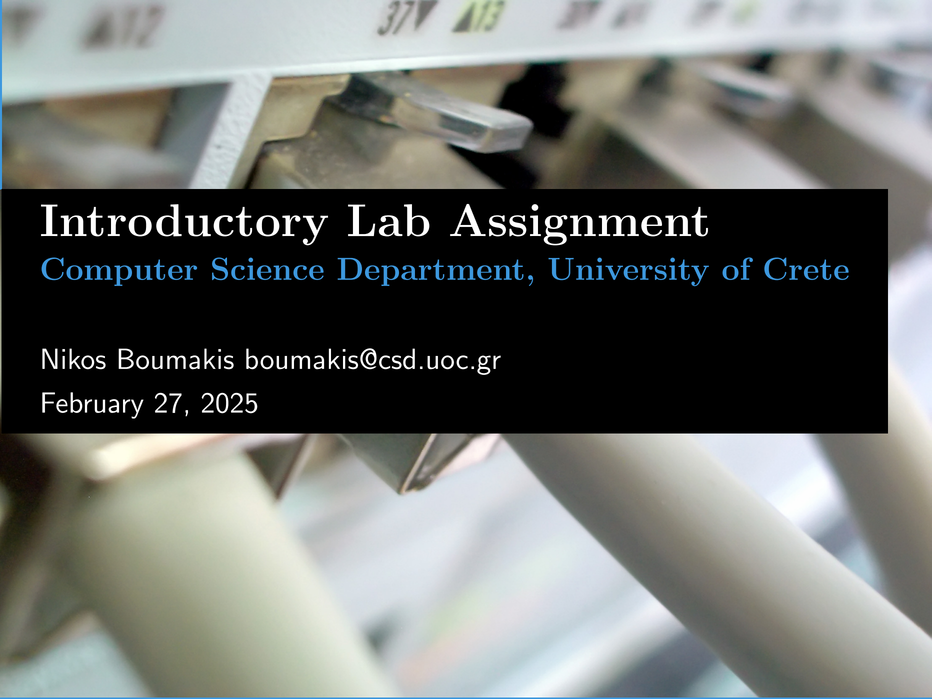


Introductory Lab Assignment

Computer Science Department, University of Crete

Nikos Boumakis boumakis@csd.uoc.gr

February 27, 2025

Original slides by Manolis Surligas surligas@csd.uoc.gr

Outline

Goal of the first assignment

- Prepare the environment that you are going to work (PCs, OS etc)
- Get familiar with different fundamental network software tools
- Use different hardware equipment and understand their key features
- Play with the parameters of the hardware/software and observe performance changes
- Understand communication within a network segment

Computers and Operating System

- The Lab provides several computers that are connected together
- The distribution used is Debian (`https://www.debian.org`)
- Tools for development, network monitoring, testing and security are already installed
- KDE graphical environment due to no-longer limited resources (Also, it looks good!)

Note!

If you need more packages or tools contact the TA

Software Tools

- In order to accomplish your tasks several software tools are necessary
- It is essential to get familiar with them
- Many of them are not required by the assignments but are vital for troubleshooting and debugging (e.g. **nmap, arp**)
- Some of them:
  - ip
  - iperf3
  - wireshark
  - nmap
  - ping
  - ethtool
  - traceroute
  - route
  - arp
  - arping
  - wireshark (again)
  - And many, many others

The ip tool

- A tool for configuring network interfaces and getting information about them
- The recommended way for configuration in recent Linux kernels
- Statically assign the IP address, subnet of a host, configure routes etc

Note!

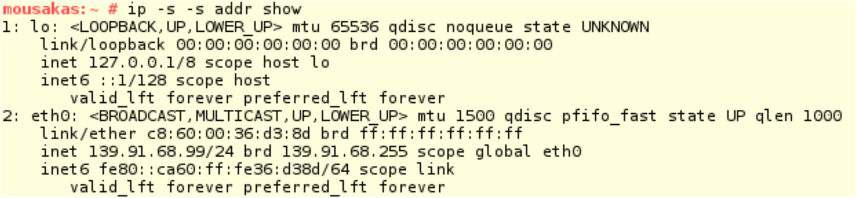
For this assignment only, a **DHCP** server automatically provides IP addresses to all hosts when they are connected to the switch. In the next assignments and for the switch topology you will have to do it yourselves using **ip**!

Hint!

Every time you unplug a cable, the IP address settings are lost!

The ip tool

- Lets see some examples!
- To show the available network interfaces use the command:



```
mousakas:~ # ip -s -s addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether c8:60:00:36:d3:8d brd ff:ff:ff:ff:ff:ff
    inet 139.91.68.99/24 brd 139.91.68.255 scope global eth0
    inet6 fe80::ca60:ff:fe36:d38d/64 scope link
       valid_lft forever preferred_lft forever
```

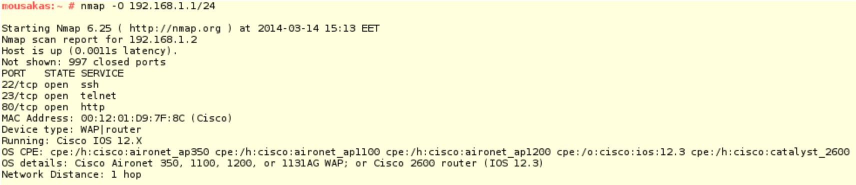
- To assign the 192.168.1.203 IP address in a /24 subnet at the interface **eth1** you can use the command:

```
ip addr add 192.168.4.101/24 broadcast 192.168.4.255 dev eno1
```

- For more info **man ip** or **ip OBJECT help**

The nmap tool

- A network exploration/reconnaissance tool
- Scans a given range of IP addresses and/or ports
- Very useful in cases that we do not know the IP of a device
- We can get the number of connected hosts in a network
- We can get also the services that end hosts are running
- Many, many options



```
mousakas:~ # nmap -O 192.168.1.1/24

Starting Nmap 6.25 ( http://nmap.org ) at 2014-03-14 15:13 EET
Nmap scan report for 192.168.1.2
Host is up (0.0011s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet
80/tcp open  http
MAC Address: 00:12:01:D9:7F:8C (Cisco)
Device type: WAP|router
Running: Cisco IOS 12.X
OS CPE: cpe:/h:cisco:aironet_ap350 cpe:/h:cisco:aironet_ap1100 cpe:/h:cisco:aironet_ap1200 cpe:/o:cisco:ios:12.3 cpe:/h:cisco:catalyst_2600
OS details: Cisco Aironet 350, 1100, 1200, or 1131AG WAP; or Cisco 2600 router (IOS 12.3)
Network Distance: 1 hop
```

ethtool

- Query and control network device driver and hardware settings, particularly for wired Ethernet devices
- Very useful to set a fixed speed (10 Mbps, 100 Mbps etc.) and operation mode (Full Duplex, Half Duplex)
- Get information about devices

Wireshark

- Open-source, extendable packet analyzer
- Fan-favourite for debugging
- Analyzes local and remote networks (over SSH)
- Nice GUI. Use tcpdump, tshark for terminal operations

Traceroute

- Determines the path between two connections.
- Returns the names or IP addresses of all the routers in the path
- ICMP (Internet Control Message Protocol) echo packets with variable TTL (Time to Live) values.
- How exactly?
- How accurate?

ARP

- Address Resolution Protocol: Map an IP address to a MAC address in a local area network
- Basically, ARP is a program used by a computer system to find another computer's MAC address based on its IP address
- What are the messages used?

Full Duplex - Half Duplex

- **Full duplex**: Data can be transmitted simultaneously in both directions
  - Faster and more efficient communication
  - Requires two communication channels, one for transmitting data and one for receiving data
  - Requires support from both devices and appropriate cables
- **Half duplex**: Data can be transmitted in both directions but not at the same time
  - One device is transmitting, the other device must wait until the transmission is complete
  - Slow and inefficient
  - Less cable strands, inherently supported

Hardware that is going to be used

- For the first assignment you have to use two different network devices
  - A Hub
  - A 1 Gigabit managed switch

Attention!!

Take care of the power supplies!!!! The switch and the routers use a 12V DC adapter whereas the Hub uses a 12V AC adapter!!

Note!

When you finished with your work, reset every device in the default settings and connect the computers at their initial network setup.

Our Lab

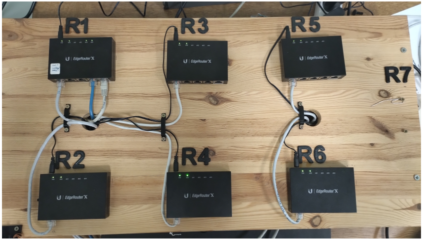
- 10 Lenovo Thinkcentre
- 6 Ubiquity routers, running the latest EdgeOS
- 1 Ubiquity switch, 24 ports
- 1 hub, 16 port
  - Almost museum piece, why?

Hosts

- Brand-new hardware (those on the desks)
- Up-to-date OS & software
- No Internet access
- Credentials per team

Routers

- What's a router? At which Layer?
- 6 Ubiquity ER-X, latest firmware
- Write access only to R2-6 (add cables as needed)
- hy435/hy435@csd

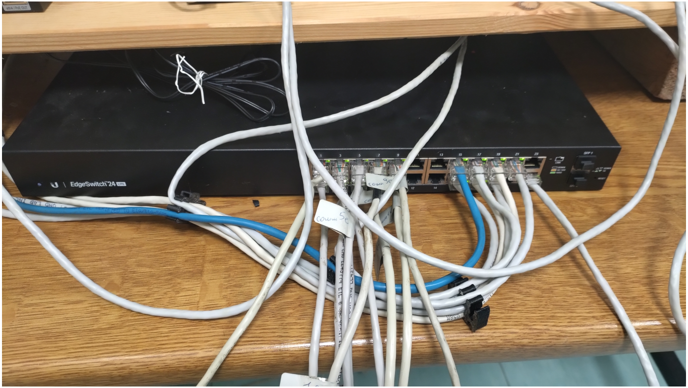


Routers (cont.)

- Networking device that forwards packets between networks
- Layer 3 device
- Reads the IP address, routes accordingly
- Can be generic computers, software-based, ASICs etc.

Switch

- What's a switch? At which Layer?
- 1 Ubiquity ES-24-Lite, latest firmware
- Read-only access



Switch (cont.)

- Forwards data frames between ports
- Layer 2 device
- Decisions based on the destination MAC address
- Segment collision domain
- More secure than hubs, since packets can be forwarded selectively
- Multiple devices can communicate with no congestion problem
- Coolest devices ever

Hub

- What's a hub? At which Layer?
- 1 unknown brand with 16 ports
- +another, a Micronet (broken?)
- No access (of course)

Hub (cont.)

- Broadcasts all data packets received on one port to all other ports
- Layer 1, no addresses
- Creates a collision domain
- Insecure, easy to congest
- Unsupported by latest standards, couldn't find any produced

Assignment 1

- Measurements across various configurations
- Understanding communication in a network segment

Measurements

- Switch to ”Network Measurements” slideset

Understanding communication

- Demonstrate every step needed for communication between devices
- Use Wireshark on a few hosts
- Cause communications, observe the packets exchanged
- Take screenshots and report
- Remember to empty as many caches as possible

Note

There is no guarantee that the packets exchanged will be only those relevant to the assignment. Reasonable steps have been taken to limit packets to the necessary but it is your responsibility to classify the packets you do see.