Link Layer Devices and Protocols

2.4 Link Layer Devices and Protocols

+ **How does this support my pentesting career?**

  - MAC spoofing
  - Testing switches security
  - Sniffing techniques
  - Man in the middle attacks

2.4 Link Layer Devices and Protocols

+ Packet forwarding also happens in the **lowest layer** of the TCP/IP stack: the **link layer**.

+ While routers are aware of the best overall path to the destination, link layer devices and protocols deal only with the next hop.

2.4 Link Layer Devices and Protocols

+ In this section you will see:
    - How switches work
    - Network card's MAC addresses
    - The Address Resolution Protocol (ARP)

2.4.1 Link Layer Devices

+ Hubs and switches are network devices that forward **frames** (layer 2 packets) on a local network.

+ They work with link layer network addresses: **MAC addresses**.

2.4.2 Mac Addresses

- IP addresses are the Layer 3 (Network layer) addressing scheme used to identify a host in a network, while **MAC addresses** uniquely identify a network card (Layer 2).

- A MAC (Media Access Control) address is also known as the **physical address**.

2.4.2 Mac Addresses

- MAC addresses are 48 bit (6 bytes) long and are expressed in hexadecimal form (HEX).

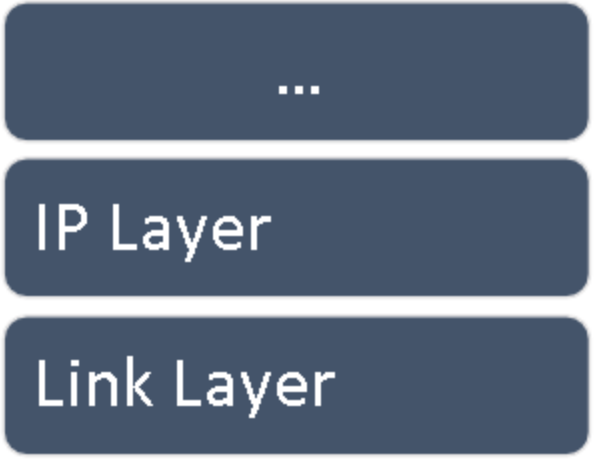
```
00:11:AA:22:EE:FF
```

2.4.2 Mac Addresses

- To discover the MAC address of the network cards installed on your computer, you can use:
  - `ipconfig /all` on Windows
  - `ifconfig` on *nix operating systems, like MacOS
  - `ip addr` on Linux

2.4.2 Mac Addresses

- Every host on a network has both a MAC and an IP address.
- Let us see how they are used together to send packets.
- **Remember:** the lower layer serves the layer above.



2.4.3 IP and MAC Addresses

- Let's take a look at an example to see how MAC addresses are used.

2.4.3 IP and MAC Addresses

- Two different networks are connected together by a router:
  - 10.32.1.0/24
  - 192.168.2.0/24

2.4.3 IP and MAC Addresses

+ Every host on the network has both an IP and a MAC address. The router has two interfaces, each with its own addresses.

2.4.3 IP and MAC Addresses

- If workstation A wants to send a packet to workstation B, which IP and MAC addresses will it use?

2.4.3 IP and MAC Addresses

- Workstation A will create a packet with:
  - The **destination IP address of workstation B** in the IP header of the datagram.
  - The **destination MAC address of the router** in the link layer header of the frame.
  - The **source IP address of workstation A**
  - The **source MAC address of workstation A**

2.4.3 IP and MAC Addresses

- The router will then take the packet and forward it to B's network, **rewriting the packet's MAC addresses**:
  - The **destination MAC address** will be B's
  - The **source MAC address** will be the router's

- The router will not change the source and destination IP addresses.

2.4.3 IP and MAC Addresses

- When a device sends a packet:
  - The destination MAC address is the MAC address of the **next hop**; this ensures that, locally, the network knows where to forward the packet.
  - The destination IP address is the address of the **destination host**; this is global information and remains the same along the packet trip.

2.4.3 IP and MAC Addresses

- This method, in a way, recalls how you send a letter to a friend.
- You need to know his or her home address (IP address) and the address of the nearest post office (MAC address) where you can drop the letter.

2.4.4 Broadcast MAC Address

- There is also a special MAC address

`FF:FF:FF:FF:FF:FF`

...which is the **broadcast** MAC address.

- A frame (the name of the packets at Layer 2) with this address is delivered to all the hosts in the local network (within the same broadcast domain).

2.4.5 Switches

- While routers work with IP addresses, switches work with MAC addresses. Switches also have multiple interfaces, so they need to keep a **forwarding table** that binds one or more MAC addresses to an interface.

MAC	Interface	TTL
00:11:22:33:44:55	1	30
AA:BB:CC:DD:EE:01	2	5
AA:CC:FF:0A:0C:12	2	5
11:22:33:1D:CC:0A	3	7

2.4.5 Switches

- The forwarding table is called Content Addressable Memory (CAM) table. Many hosts can connect to a switch. Let's see how.

MAC	Interface	TTL
00:11:22:33:44:55	1	30
AA:BB:CC:DD:EE:01	2	5
AA:CC:FF:0A:0C:12	2	5
11:22:33:1D:CC:0A	3	7

2.4.5 Switches

- The smallest switches you can encounter are home switches, usually integrated into a DSL home router. They usually have 4 ports.

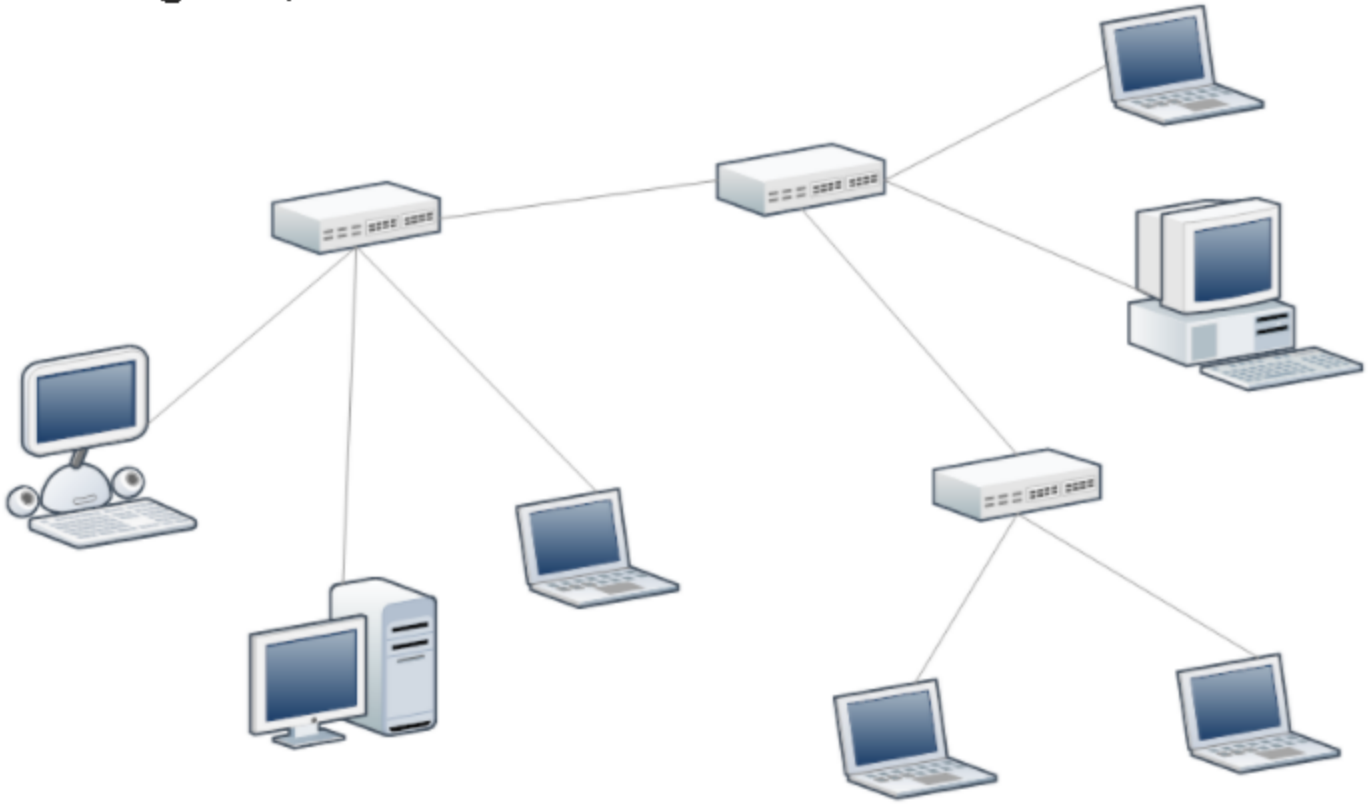
- Corporate switches may have up to 64 ports, and system administrators can connect multiple switches together to accommodate more hosts.

2.4.5 Switches

- The main difference between one switch and another is the packet forwarding speed.
- The speed of a switch varies from 10Mbps (megabits per second) to 10Gbps (gigabits per second). Nowadays, 1Gbps is the most common forwarding speed in commercial switches.

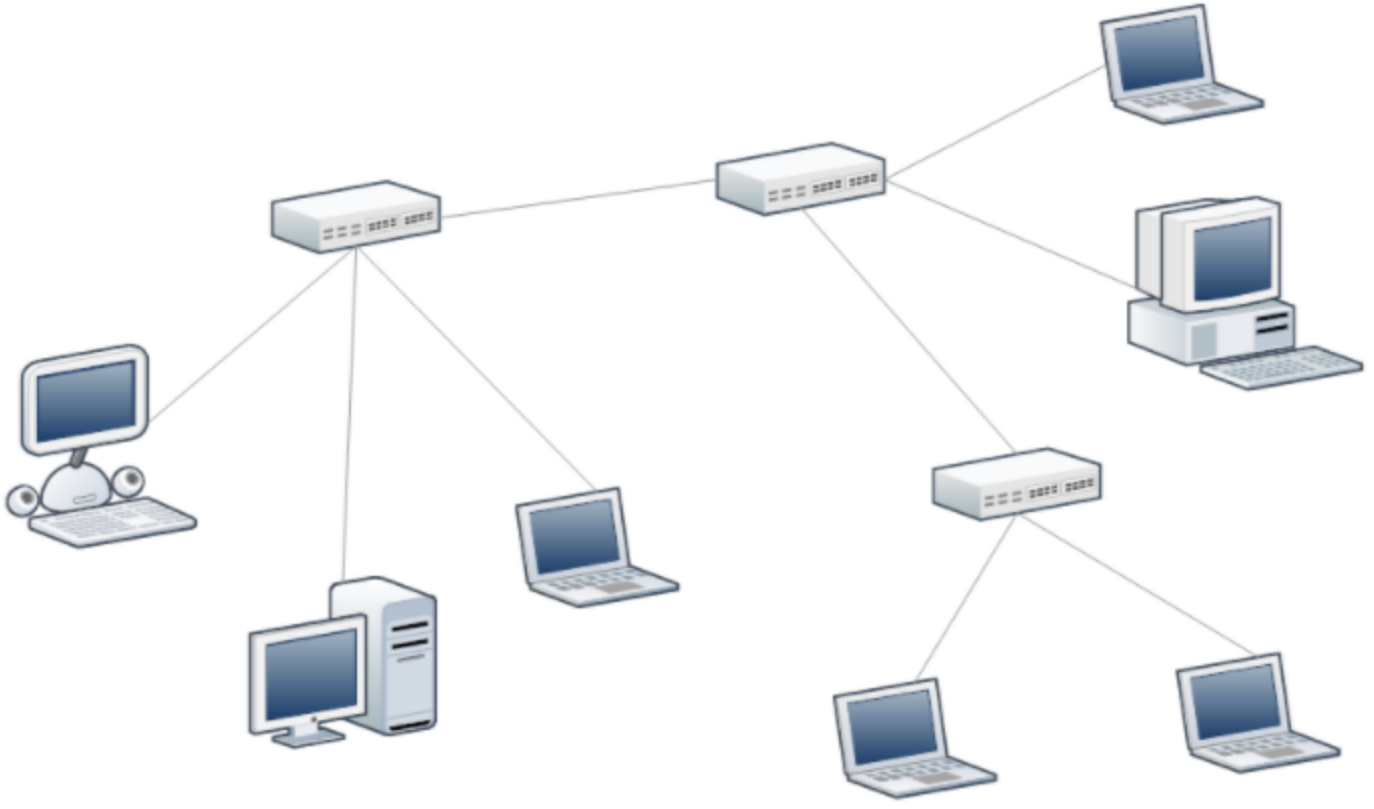
2.4.5.1 Multi-switch Network

- In this diagram, all the machines are **on the same network.**



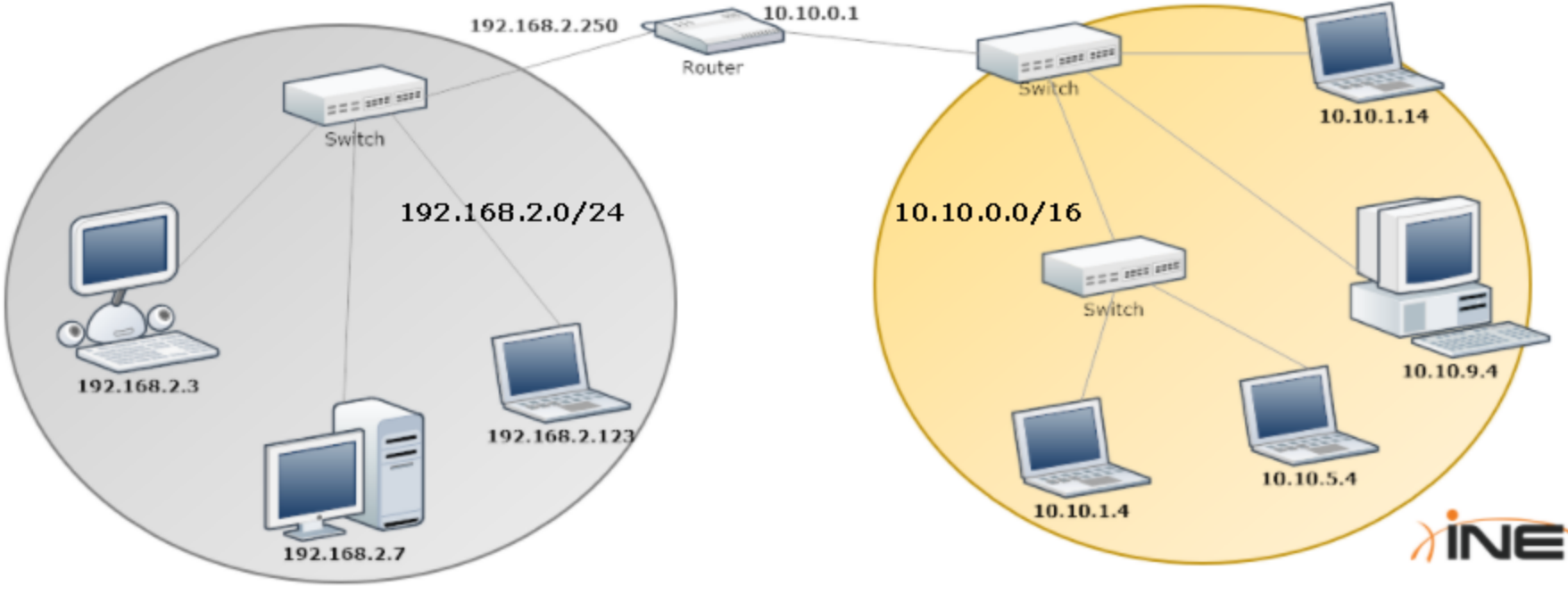
2.4.5.1 Multi-switch Network

+ Switches let all the computers talk to each other.



2.4.5.2 Segmentation

+ Switches, without VLANs, do not **segment** networks. Routers do.

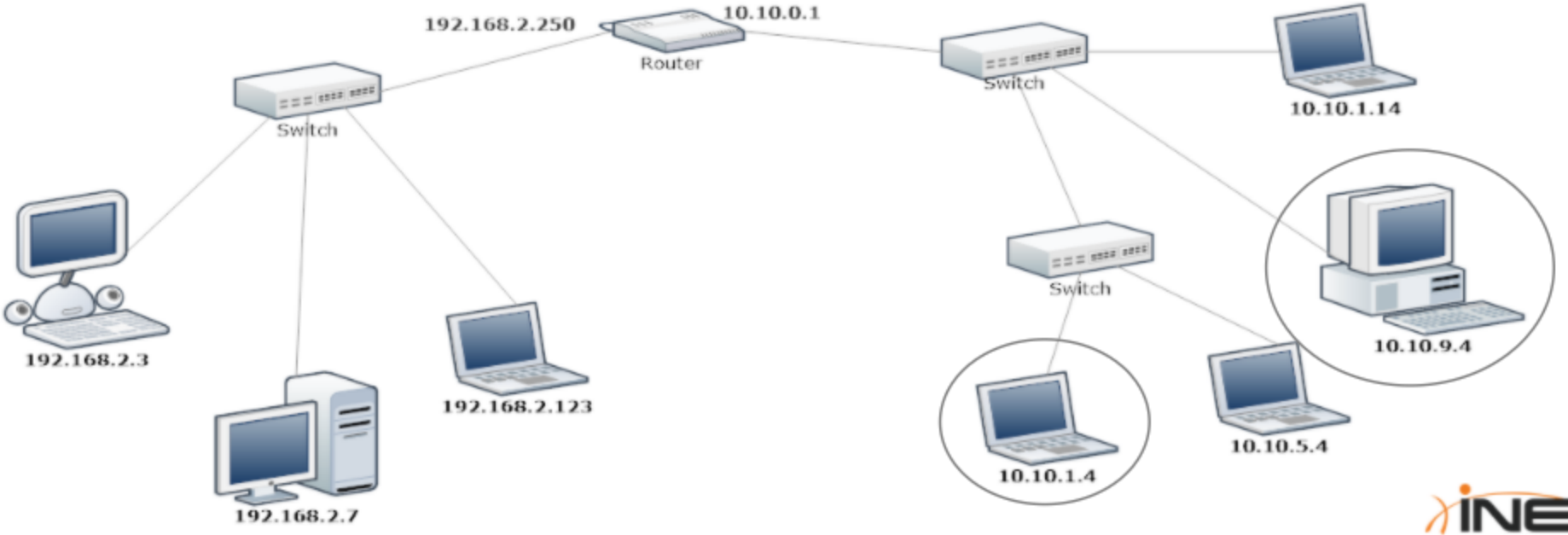


2.4.5.2 Segmentation

- Usually, every interface of a router is attached to a different subnet with a different network address.
- Also, routers do not forward packets coming from one interface if they have a ff:ff:ff:ff:ff:ff broadcast MAC address (imagine if they did!).

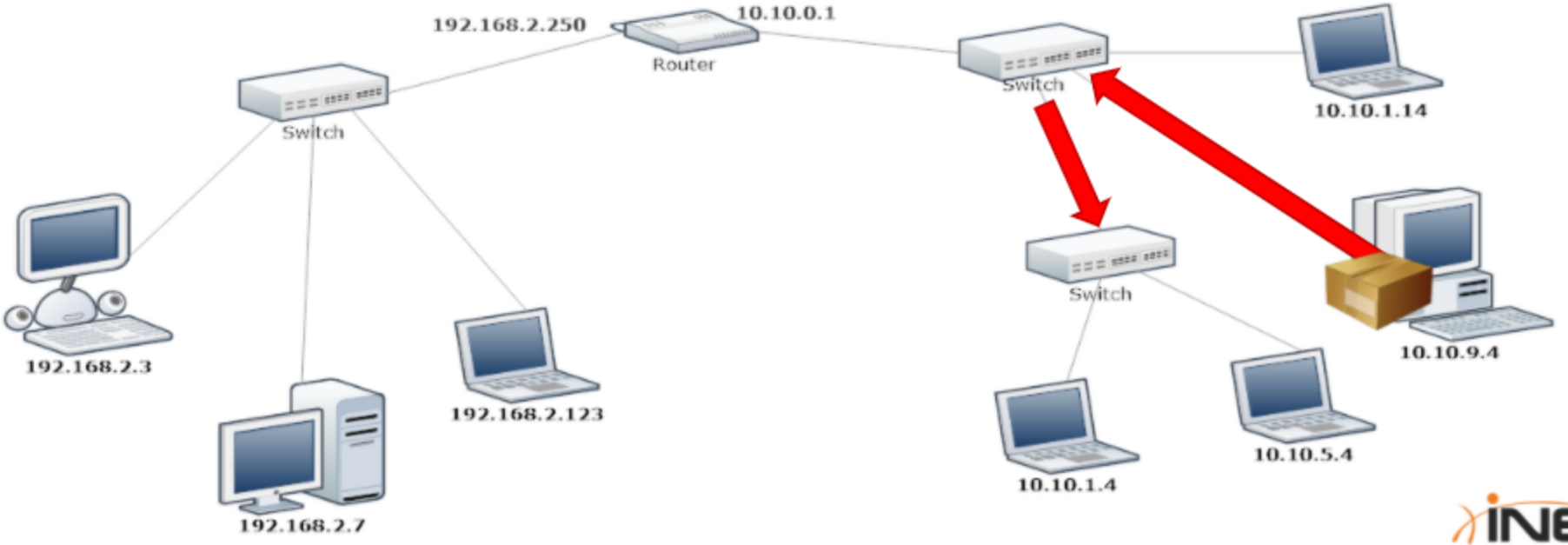
2.4.5.3 Multi-switch Example

+ What happens if 10.10.9.4 wants to send a packet to 10.10.1.4?



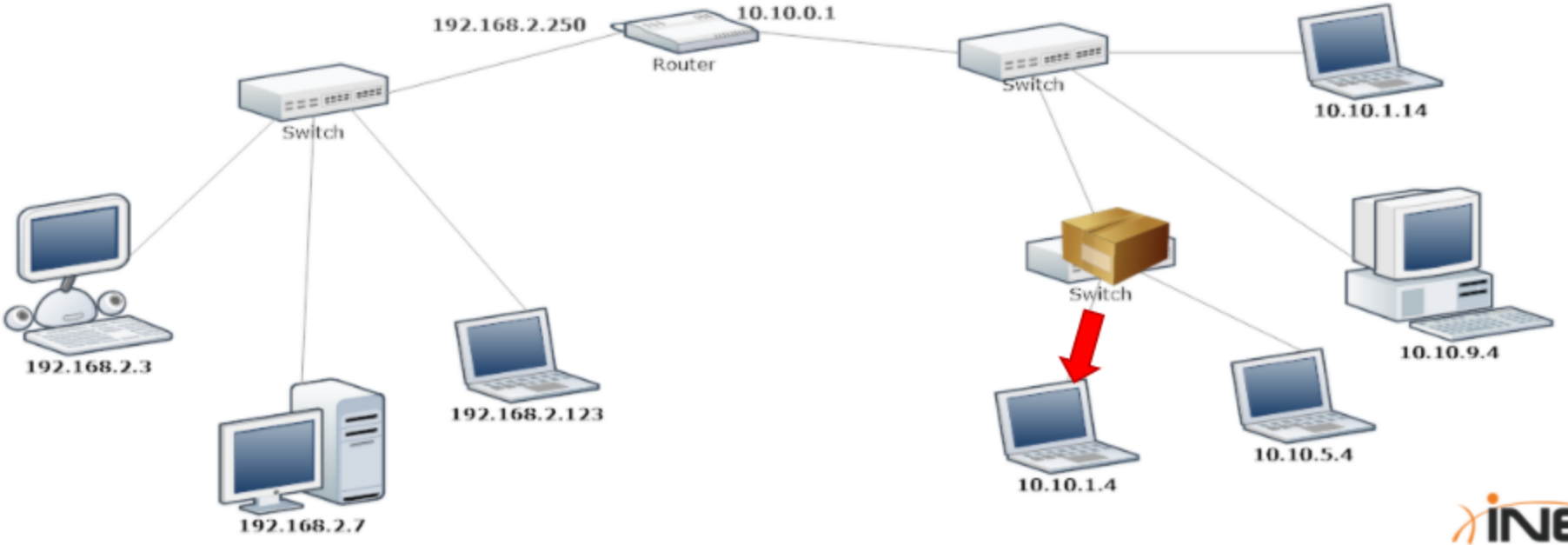
2.4.5.3 Multi-switch Example

- The first switch receives the packet, performs a look-up in the CAM table and forwards it to the next switch.



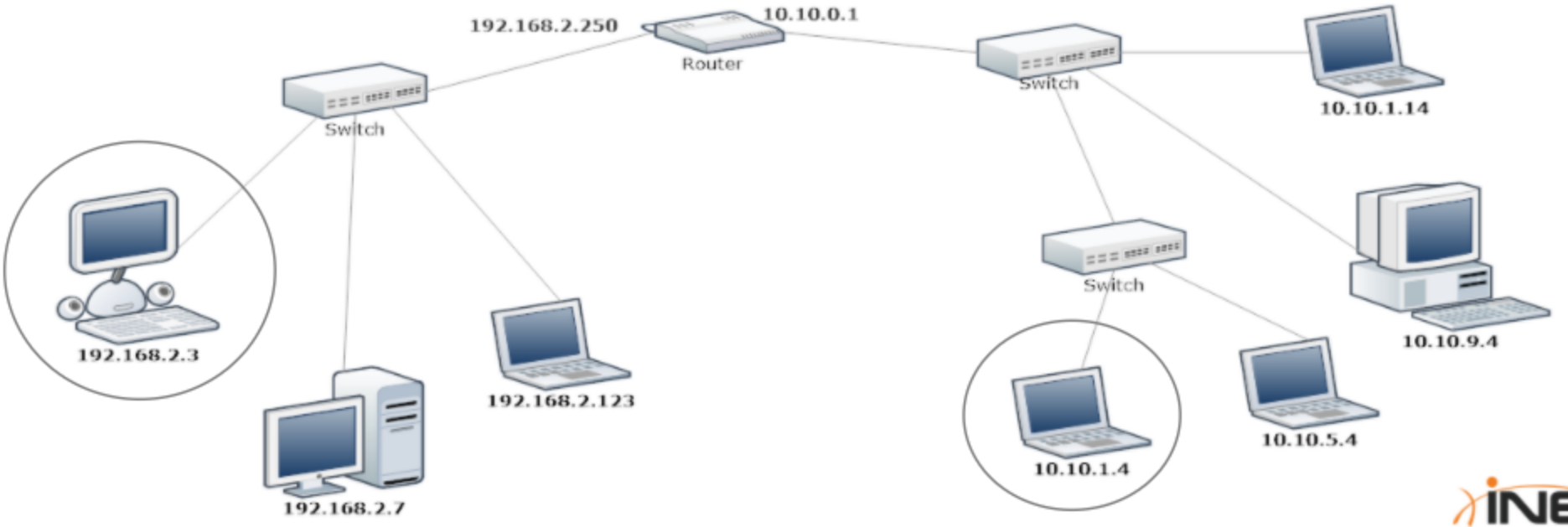
2.4.5.3 Multi-switch Example

- The second switch forwards the packet to 10.10.1.4.



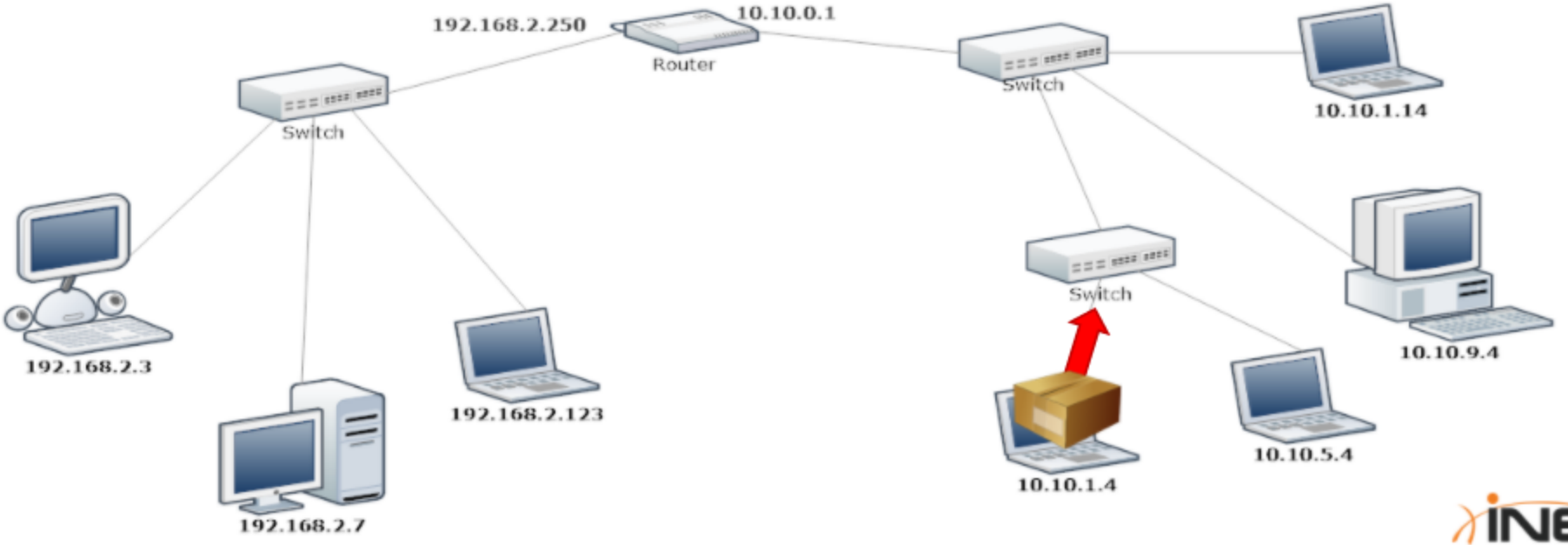
2.4.5.4 Multi-switch and Router Example

- What happens if 10.10.1.4 wants to send a packet to 192.168.2.3?



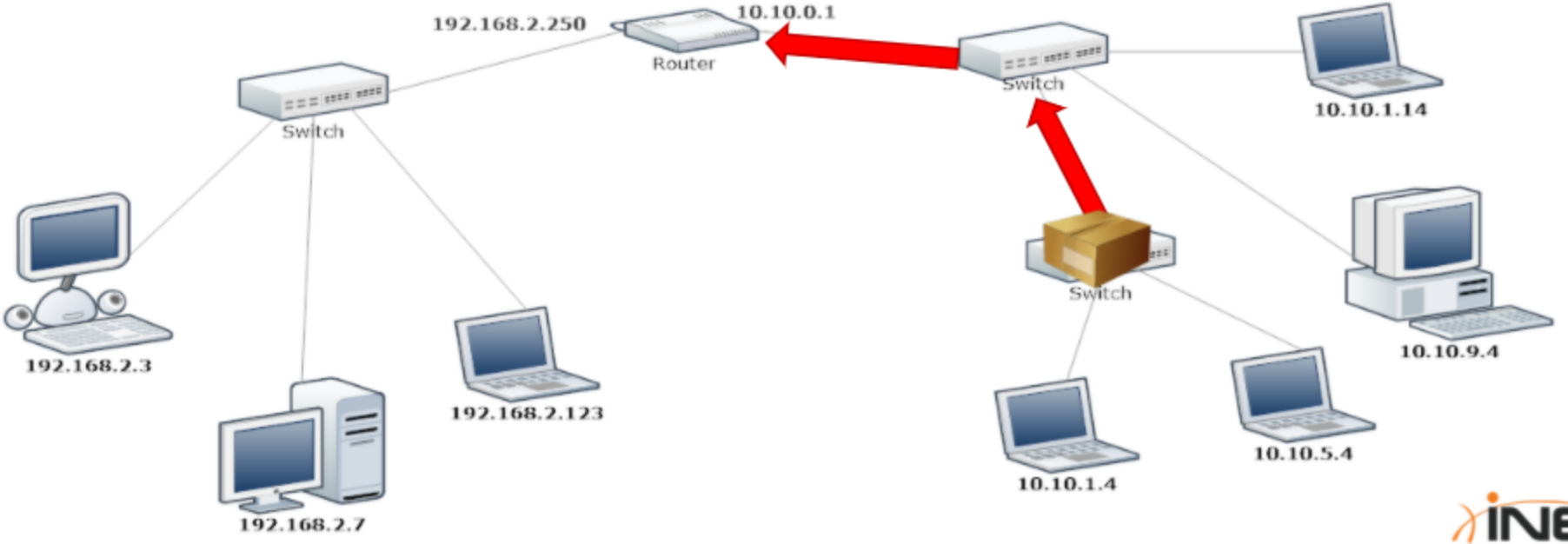
2.4.5.4 Multi-switch and Router Example

- 10.10.1.4 needs to send the packet to the router so that the first switch will forward the packet to the next one.



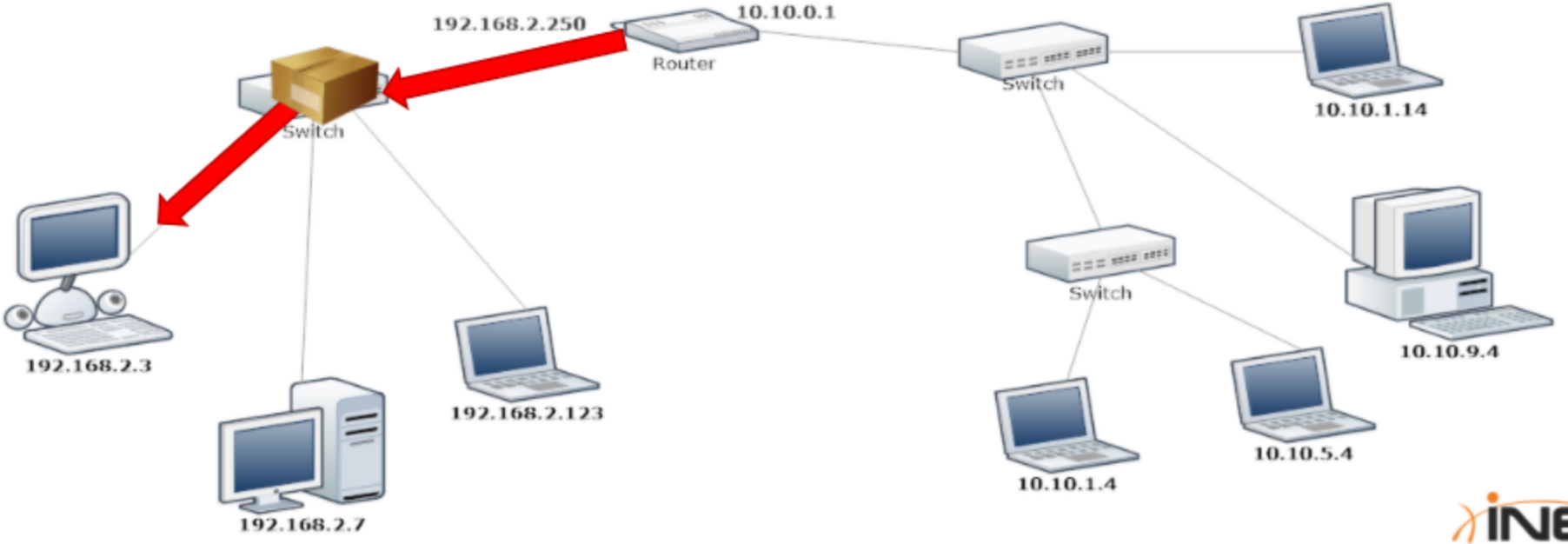
2.4.5.4 Multi-switch and Router Example

- The packet then arrives at the router that, after a look up in the routing table, forwards it to the 192.168.2.0/24 network.



2.4.5.4 Multi-switch and Router Example

+ Finally, the packet is delivered.



2.4.5.5 Forwarding Tables

- A forwarding table binds MAC addresses to interfaces.

- In the following slides you will see:
  - The structure of the table
  - The way a switch constructs the MAC address – interface binding
  - How forwarding works

2.4.5.5 Forwarding Tables

+ A typical forwarding table contains:
  - The MAC address
  - The interfaces the switch can use to deliver packets to a specific MAC address
  - A time to live (TTL)

MAC	Interface	TTL
00:11:22:33:44:55	1	30
AA:BB:CC:DD:EE:01	2	5
AA:CC:FF:0A:0C:12	2	5
11:22:33:1D:CC:0A	3	7

2.4.5.5 Forwarding Tables

- The forwarding table, or Content Addressable Memory table (CAM table), is stored in the device's RAM and is constantly refreshed with new information.

MAC	Interface	TTL
00:11:22:33:44:55	1	30
AA:BB:CC:DD:EE:01	2	5
AA:CC:FF:0A:0C:12	2	5
11:22:33:1D:CC:0A	3	7

2.4.5.5 Forwarding Tables

+ Looking at the table you can tell that:
  - A single host is attached to Interface 1 and 3 respectively
  - Two hosts are attached to interface 2 (probably via another switch).

MAC	Interface	TTL
00:11:22:33:44:55	1	30
AA:BB:CC:DD:EE:01	2	5
AA:CC:FF:0A:0C:12	2	5
11:22:33:1D:CC:0A	3	7

2.4.5.5 Forwarding Tables

- There might be multiple hosts on the same interface and interfaces without any host attached.

- In our example interface, 4 has no hosts attached.

MAC	Interface	TTL
00:11:22:33:44:55	1	30
AA:BB:CC:DD:EE:01	2	5
AA:CC:FF:0A:0C:12	2	5
11:22:33:1D:CC:0A	3	7

2.4.5.5 Forwarding Tables

- The TTL determines how long an entry will stay in the table. This is important because the **CAM table has a finite size**.

- So, as soon as an entry expires it is removed from the table.

MAC	Interface	TTL
00:11:22:33:44:55	1	30
AA:BB:CC:DD:EE:01	2	5
AA:CC:FF:0A:0C:12	2	5
11:22:33:1D:CC:0A	3	7

2.4.5.6 CAM Table Population

- Switches learn new MAC addresses dynamically; they inspect the header of every packet they receive, thus identifying new hosts.

- While routers use complex routing protocols to update their routing rules, switches just use the source MAC address of the packets they process to decide which interface to use when forwarding a packet.

2.4.5.6 CAM Table Population

- The source MAC address is compared to the CAM table:
  - If the MAC address is not in the table, the switch will add a new MAC-Interface binding to the table
  - If the MAC-Interface binding is already in the table, its TTL gets updated
  - If the MAC is in the table but bound to another interface the switch updates the table

2.4.5.7 Forwarding

- To forward a packet:
  1. The switch reads the destination MAC address of the frame.
  2. It performs a look-up in the CAM table.
  3. It forwards the packet to the corresponding interface.
  4. If there is no entry with that MAC address, the switch will forward the frame to all its interfaces.

2.4.6 ARP

- When a host wants to send a packet to another host, it needs to know the IP and the MAC address of the destination in order to build a proper packet.

- You wouldn't be able to send your friend a letter if you don't know his/her address, right? What happens if the source host knows the IP address, but not the MAC address of the destination host?

2.4.6 ARP

- This situation occurs in many circumstances, for example at every power up.
  - A PC in an office knows a bunch of IP addresses, like the fileserver, the printers, and the webserver, but not their corresponding MAC addresses.

- The host needs to know the MAC addresses of the other network nodes, and it can learn them by using the **Address Resolution Protocol (ARP)**.

2.4.6 ARP

- With ARP a host can build the correct IP Address – MAC address binding.
- This is one of the most fundamental protocols any modern network uses, so make sure to fully understand it.

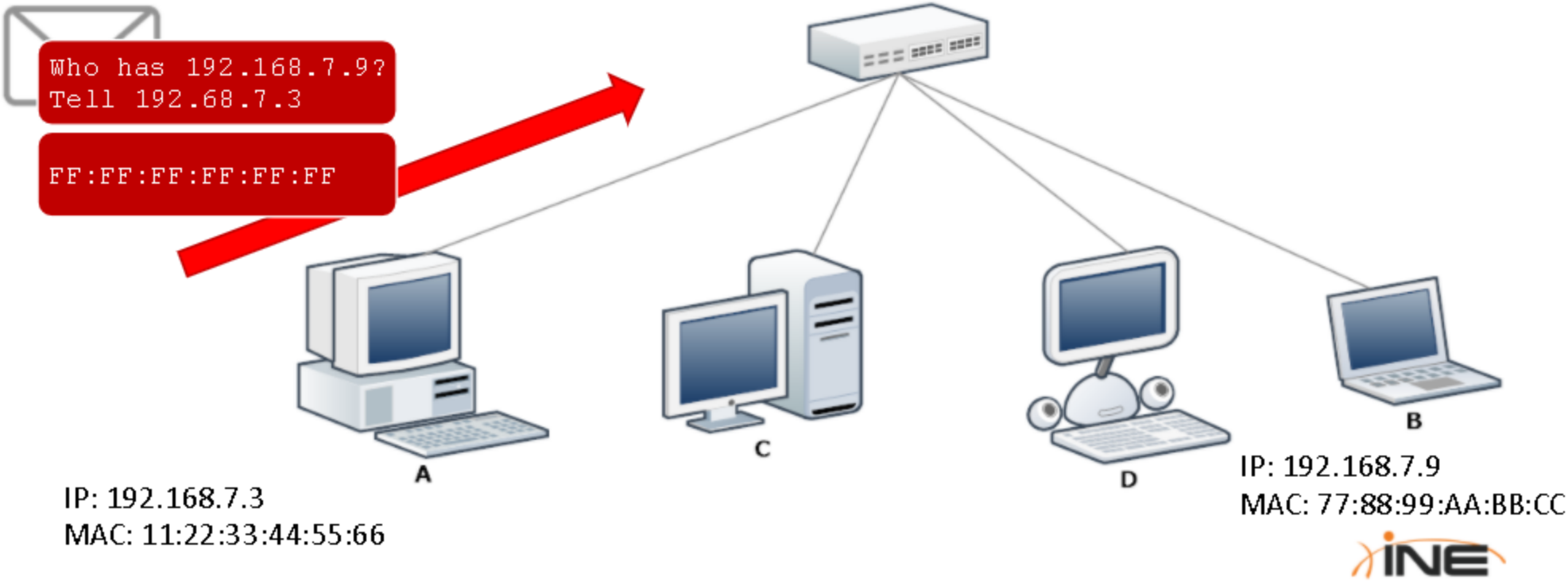
2.4.6 ARP

- When a host (*A*) wants to send traffic to another (*B*), and it only knows the IP address of *B*:
  1. *A* builds an **ARP request** containing the IP address of *B* and FF:FF:FF:FF:FF:FF as destination MAC address.
     This is fundamental because the switches will forward the packet to every host.
  2. Every host on the network will receive the request.
  3. B replies with an **ARP reply**, telling *A* its MAC address.

2.4.6 ARP

1

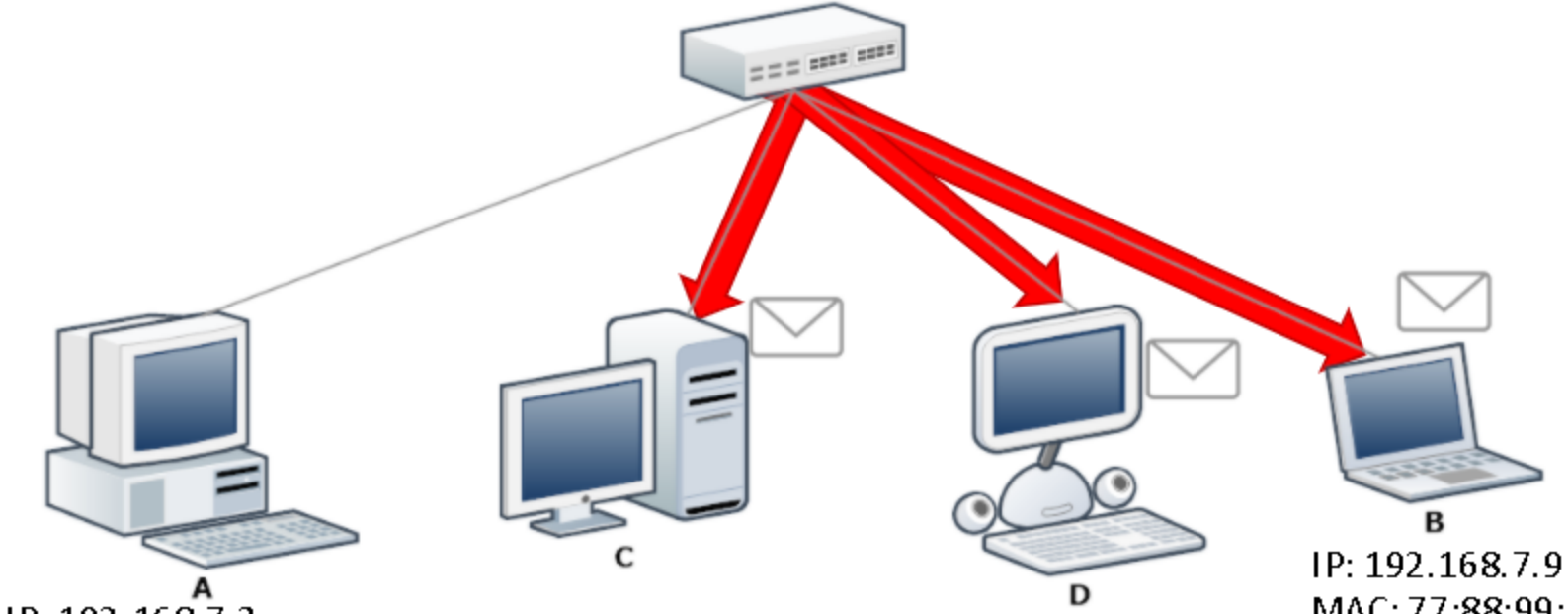
+ 'A' sends a packet to the broadcast MAC address, asking for the MAC address of B.



2.4.6 ARP

2

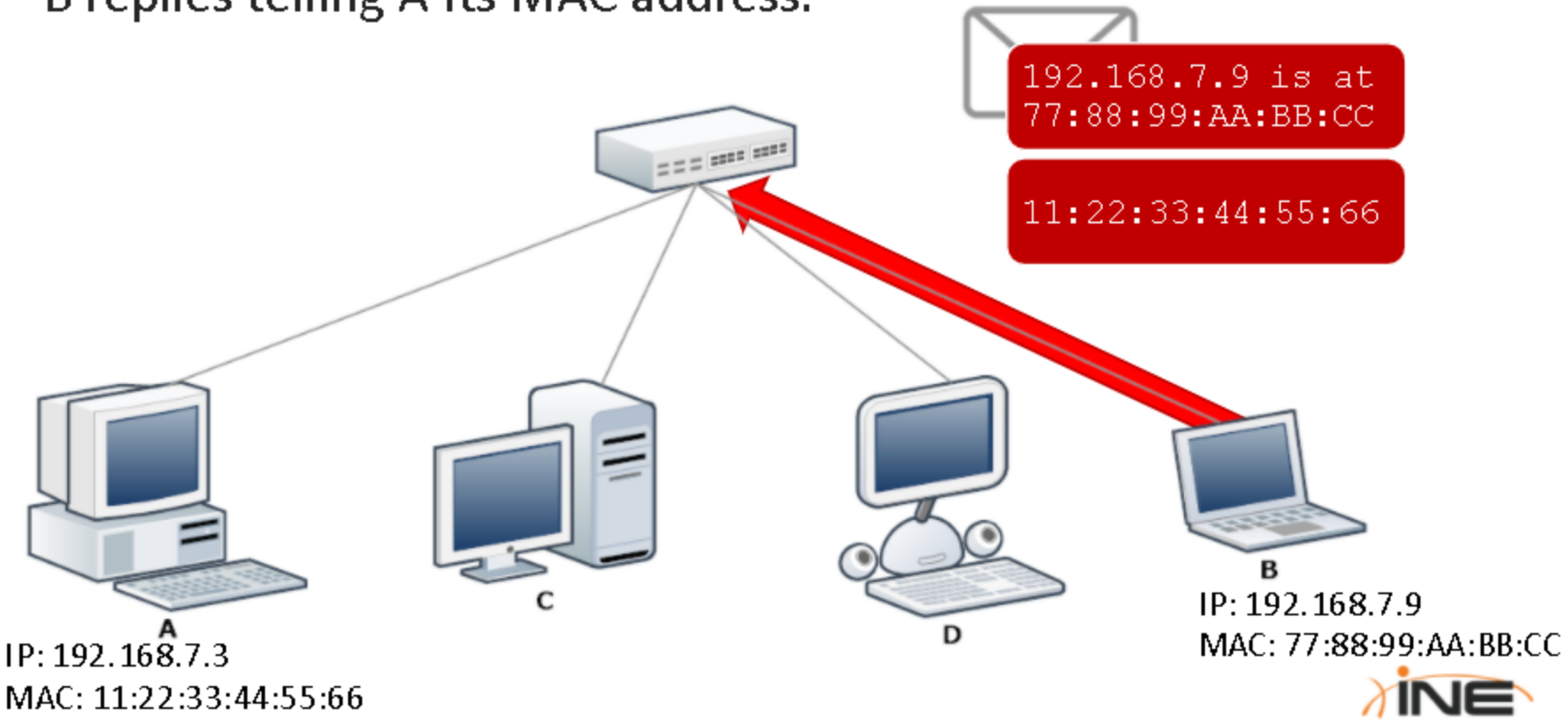
+ The switch forwards the packet to all its ports.



2.4.6 ARP

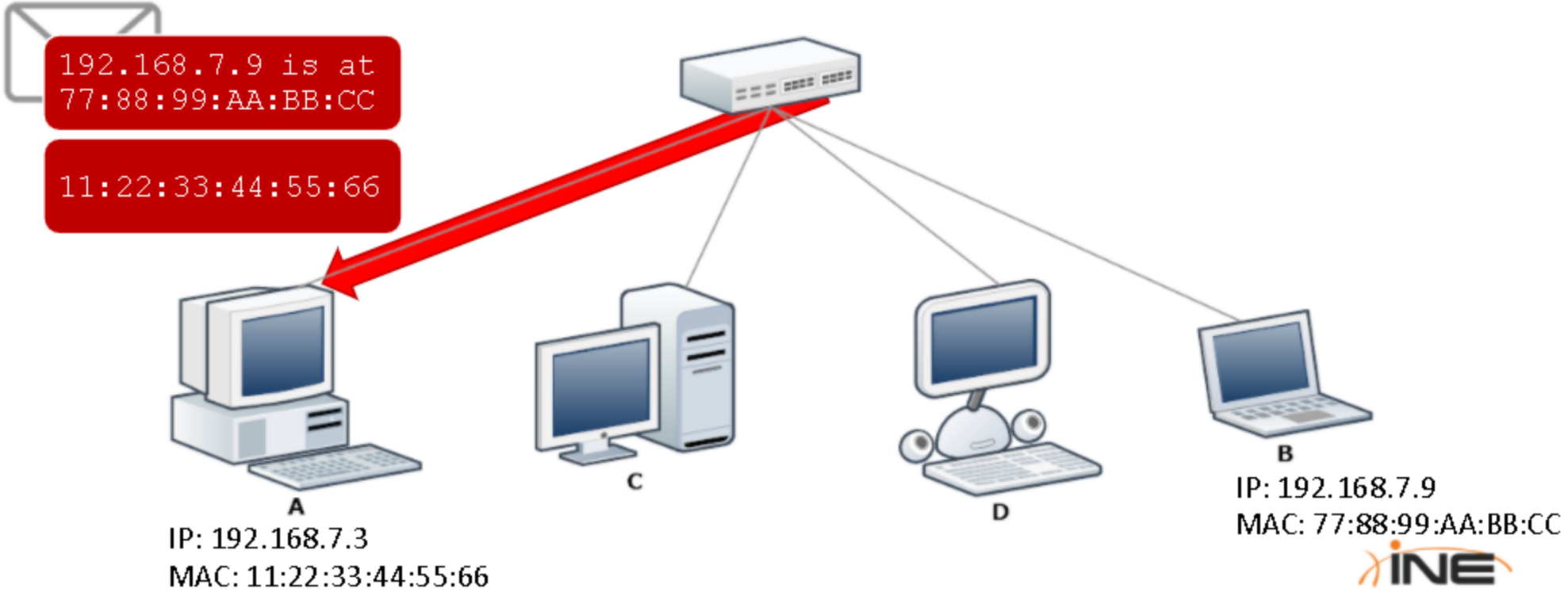
3

+ B replies telling A its MAC address.



2.4.6 ARP

- Finally, the switch forwards the reply to A.



2.4.6 ARP

- *'A'* will save the IP – MAC binding in its ARP cache. Further traffic to *'B'* will not need a new ARP resolution protocol round.

- ARP cache entries have a TTL too, as the size of the device RAM is finite. A host discards an entry at the power off or when the entry's TTL expires.

2.4.6.1 Checking the ARP Cache

- You can check the ARP cache of your host by typing:
  - arp -a on Windows
  - arp on *nix operating systems
  - ip neighbour on Linux

```
$ ip neighbour
192.168.17.202 dev eth0 lladdr d0:d4:12:e1:ef:5a STALE
192.168.17.1 dev eth0 lladdr 00:50:7f:78:fc:40 STALE
192.168.17.99 dev eth0 lladdr 00:d0:4b:92:2d:89 STALE
192.168.17.14 dev eth0 lladdr 60:a4:4c:a8:be:5b STALE
192.168.17.18 dev eth0 lladdr 20:cf:30:c7:ad:ae STALE
192.168.17.30 dev eth0 lladdr 20:cf:30:ea:22:13 STALE
192.168.17.66 dev eth0 lladdr a4:ee:57:e8:2e:0b STALE
192.168.17.254 dev eth0 lladdr c8:4c:75:a4:79:a6 REACHABLE
192.168.17.12 dev eth0 lladdr 60:a4:4c:a8:bd:1a STALE
192.168.17.19 dev eth0 lladdr 54:04:a6:a0:6e:ad STALE
192.168.17.24 dev eth0 lladdr bc:5f:f4:ef:63:51 STALE
```

2.4.7 Hubs

- **Hubs** were used in computer networks before switches. They have the same **purpose** but not the same **functionality**.

- Hubs are simple repeaters that do not perform any kind of header check and simply forward packets by just repeating electric signals. They receive electric signals on a port and repeat the same signals on all the other ports.

2.4.7 Hubs

- This means that every node on a hub-based network receives the same electric signals, thus the same packets.
- Nowadays, hubs are very rare as they have mostly been replaced by switches.