NETWORK FUNDAMENTALS

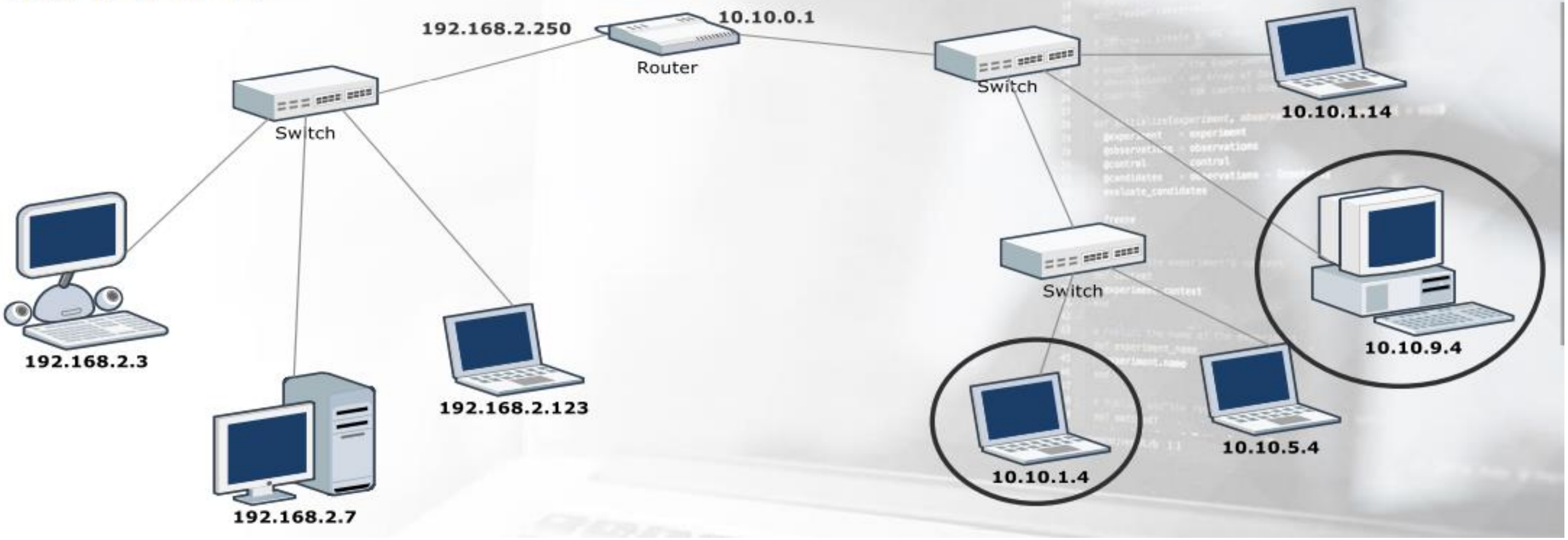
BY

SURAJKARTHIC

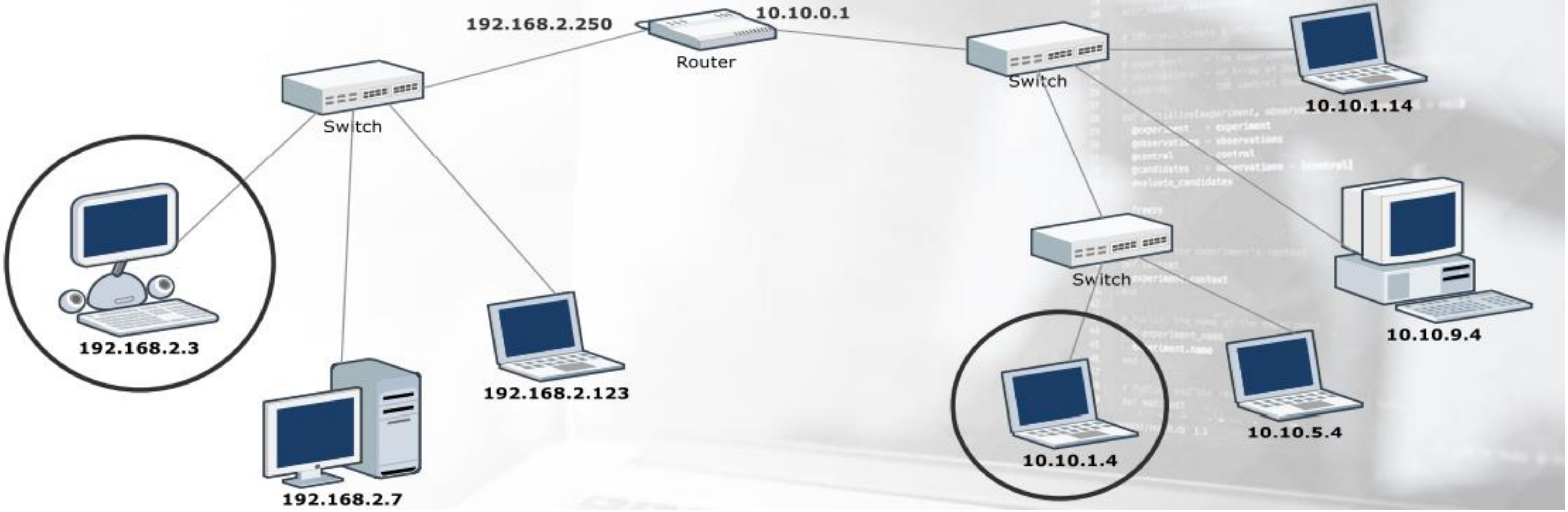
FORWARDING

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

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



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



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.

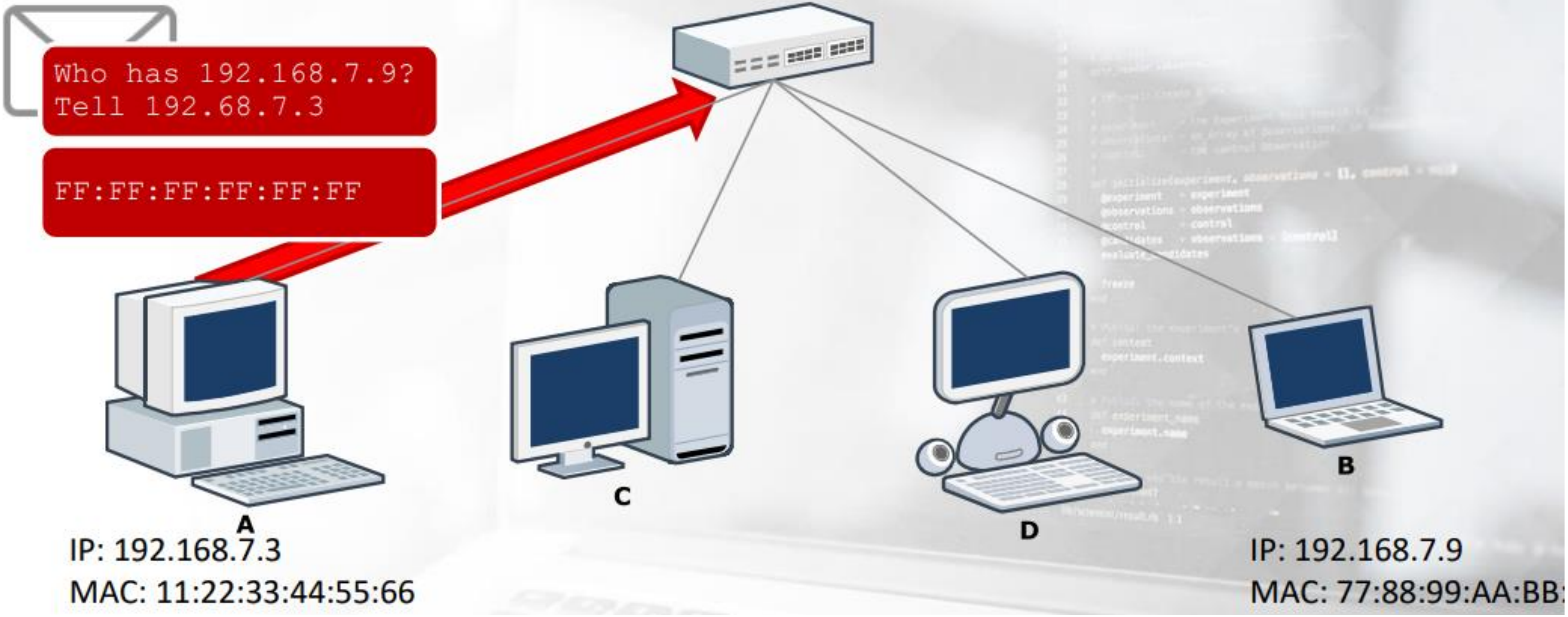
- You wouldn’t be able to send your friend a letter if you don’t know his/her address, right? What happens if the source host knows the IP address, but not the MAC address of the destination host?

- 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).

- 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.
- Every host on the network will receive the request.
- B replies with an ARP reply, telling A its MAC address.

‘A’ sends a packet to the broadcast MAC address, asking for the MAC address of B.



```
Who has 192.168.7.9?
Tell 192.68.7.3
```

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

A

IP: 192.168.7.3
MAC: 11:22:33:44:55:66

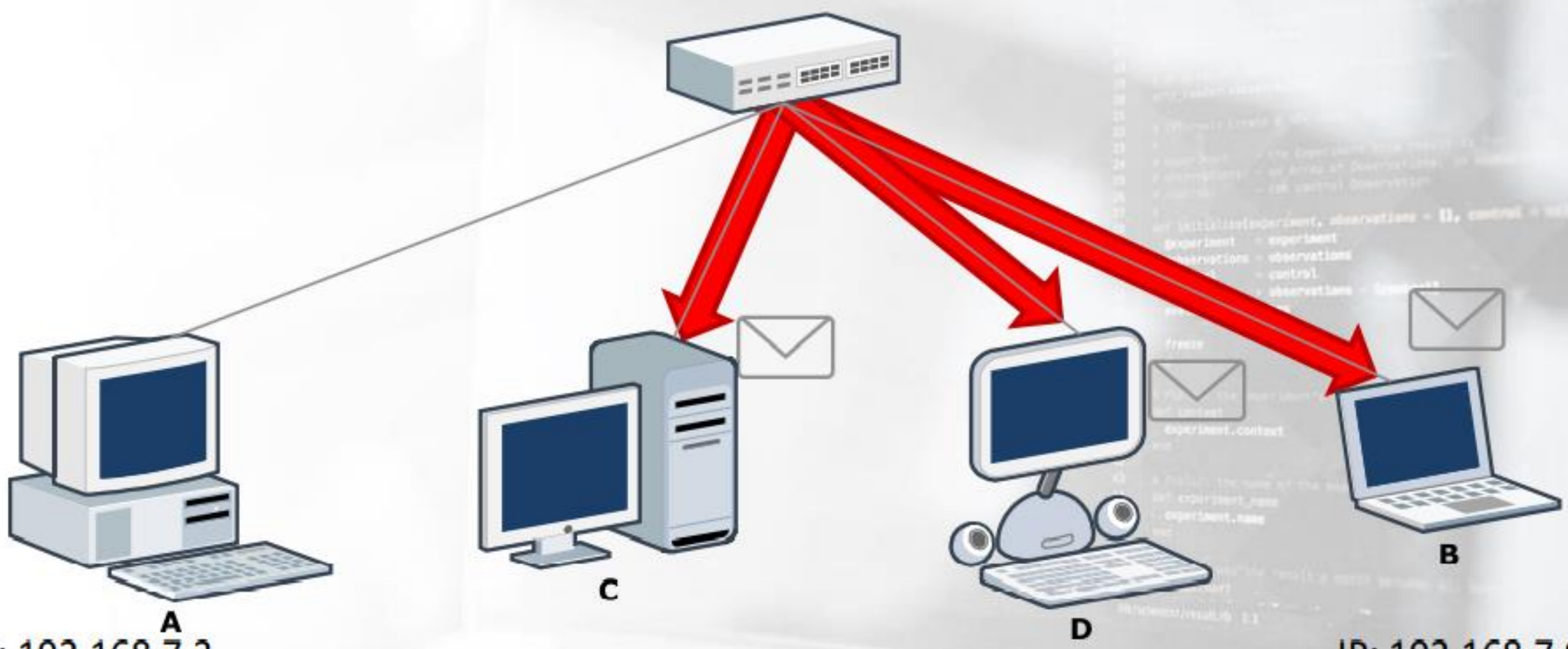
C

D

B

IP: 192.168.7.9
MAC: 77:88:99:AA:BB:

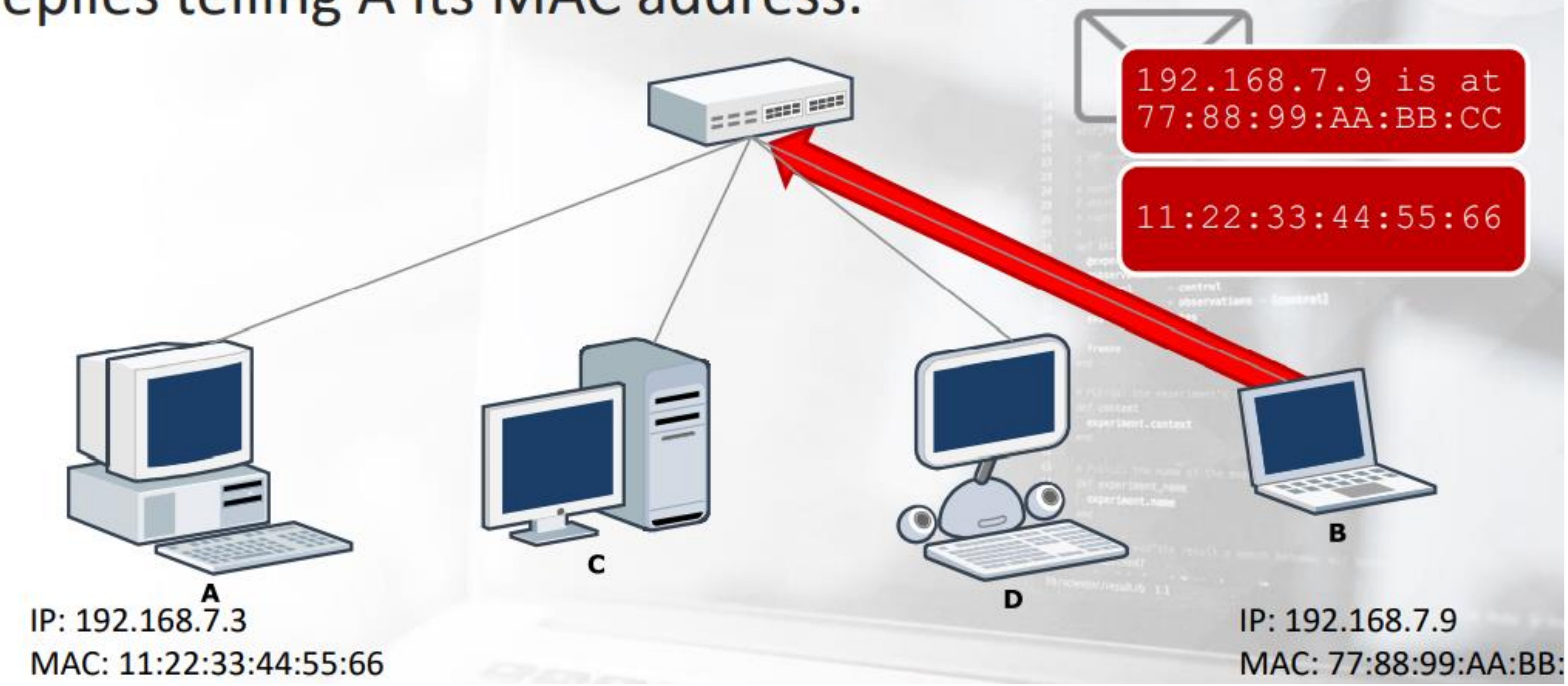
The switch forwards the packet to all its ports.



IP: 192.168.7.3
MAC: 11:22:33:44:55:66

IP: 192.168.7.9
MAC: 77:88:99:AA:BB:

B replies telling A its MAC address.



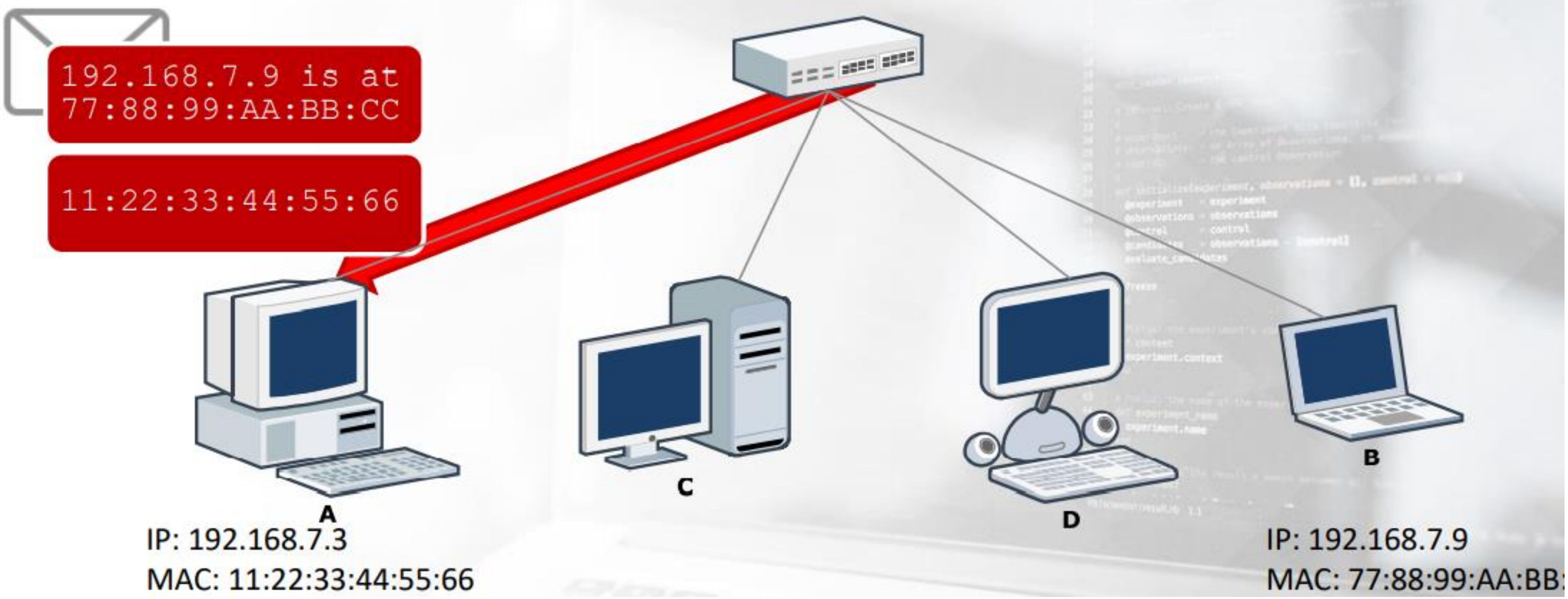
192.168.7.9 is at 77:88:99:AA:BB:CC

11:22:33:44:55:66

IP: 192.168.7.3
MAC: 11:22:33:44:55:66

IP: 192.168.7.9
MAC: 77:88:99:AA:BB:

Finally, the switch forwards the reply to A.



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

VLAN - VIRTUAL LAN

- Disadvantages of Subnetting
- - its time consuming - when we have more number of computers
- - it is configured at user end, so users can change the ip configuration of computers any time,. this is a security issue.

- VLAN
- - Subnetting depends on two factors - IP RANGE & CUSTOM SUBNET MASK
- - vlan doesnt depend on both of these, because we configure the ports of a switch and not computers.

STEPS TO CREATE VLAN

1

1. Create vlan name and number

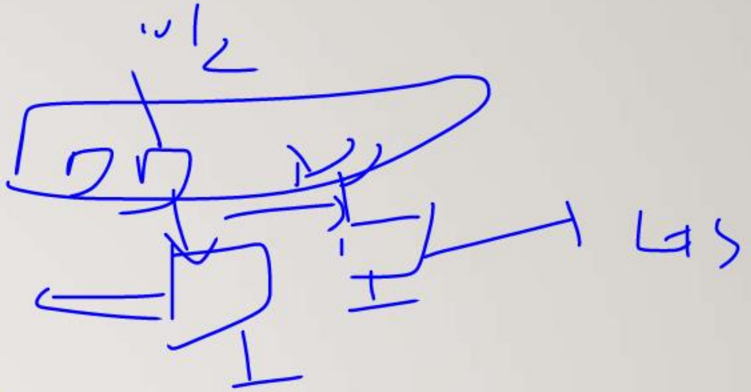
2

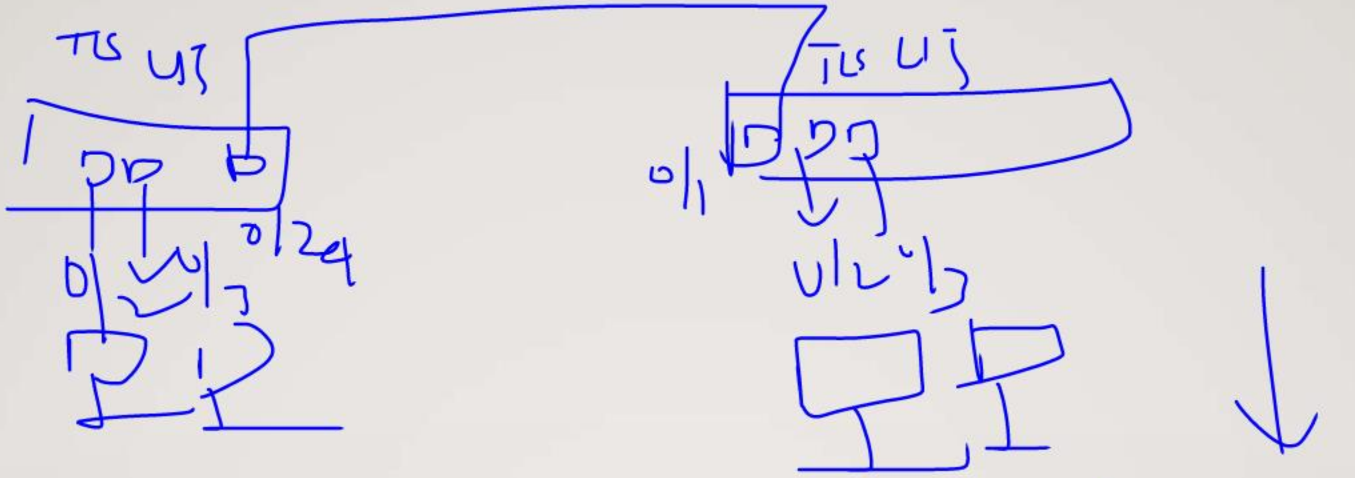
2. Configure switch port - Access port / Trunk port

3

3. VLAN membership - link the port with created vlan

```
en
conf
# vlan 1000 → 2000
# name ICS
# int fa 0/2  0/3
# switchport mode access vlan1000
# exit
```





[illegible]

0/1

~~#i Fast~~ 1/0/24

Switch port mode trunk

Switch port trunk allowed VLAN all

PORT SECURITY

- Disadvantages of VLAN
- When attacker computer from outside our LAN tries to connect to X vlan 100 of switch 1, what will happen?
- He will be able to connect and he can access all the documents of X vlan, this is a security risk and port security is used to stop this.

- - Port security assigns a particular mac address to a particular port.
- - Only computer with that mac address can access that port.
- - If a computer with different mac address tries to access, the port will be either blocked or shut down

Steps to configure PORT SECURITY

1. CHOOSE PORT/INTERFACE OF SWITCH
2. CONFIGURE PORT - ACCESS PORT / TRUNK PORT
3. ENTER PORT SECURITY CONFIGURATION
4. CHOOSE MAXIMUM NO OF COMPUTERS THAT CAN ACCESS THE PORT
5. ASSIGNING MAC ADDRESS - AUTOMATIC(STICKY) OR MANUAL
6. CONFIGURING VIOLATION RULE - RESTRICT,SHUTDOWN

RESTRICT - PACKET TRACER WILL KEEP THE PORT ON - GREEN, BUT ATTACKER WONT BE ABLE TO ACCESS ANYTHING FROM SALES VLAN

SHUTDOWN - PORT WILL BE DOWN, PACKET TRACER - RED

COMMANDS

- #INT FA0/2
- #SWITCHPORT MODE ACCESS
- #SWITCHPORT PORT SECURITY
- #SWITCHPORT PORT-SECURITY MAXIMUM 1
- #SWITCHPORT PORT-SECURITY MAC ADDRESS STICKY
- #SWITCHPORT PORT-SECURITY VIOLATION SHUTDOWN