SOC ANALYST SERIES

1. NETWORKS

https://academy.maikroservice.com

30 DAYS - 30 TOPICS

1 GOAL

GET READY TO BE A SOC ANALYST

@maikroservice

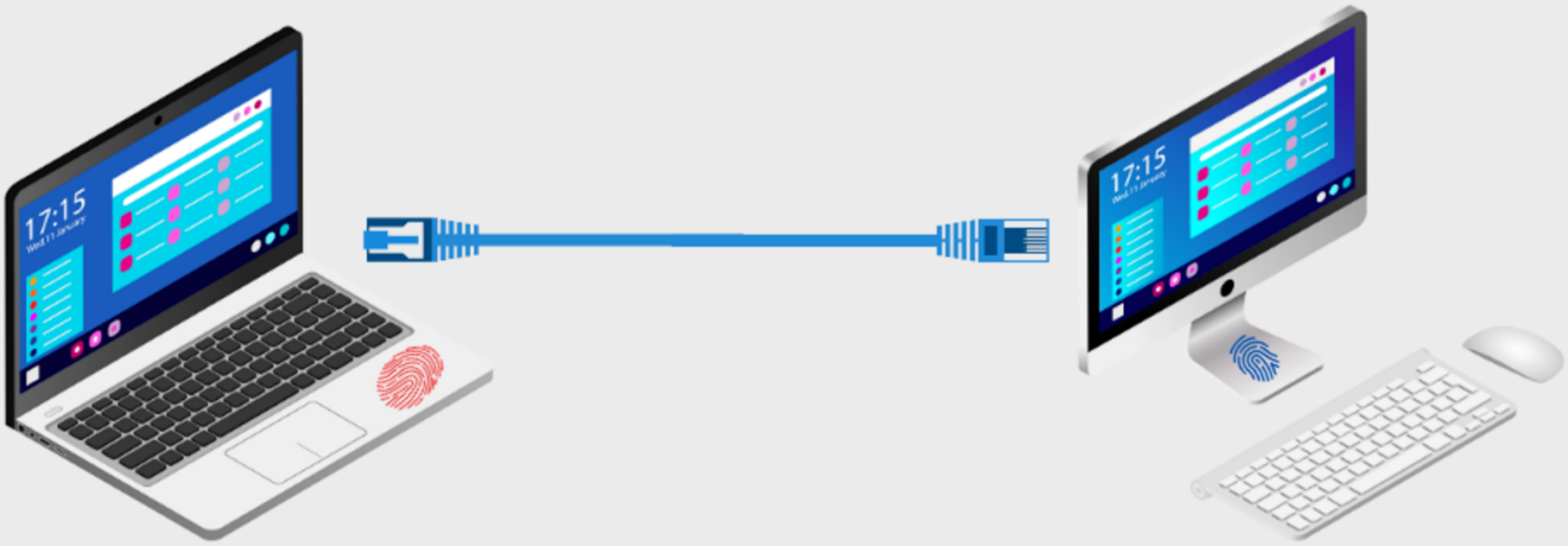
Networks

The smallest possible network is peer-to-peer

that means 1 computer to 1 computer (directly)

computer1 ⟷ computer2

P2P Network



In order to connect them you need:

- a cable
- and one network interface controller (NIC)

each

(sometimes they are also called network cards)

Back in my days

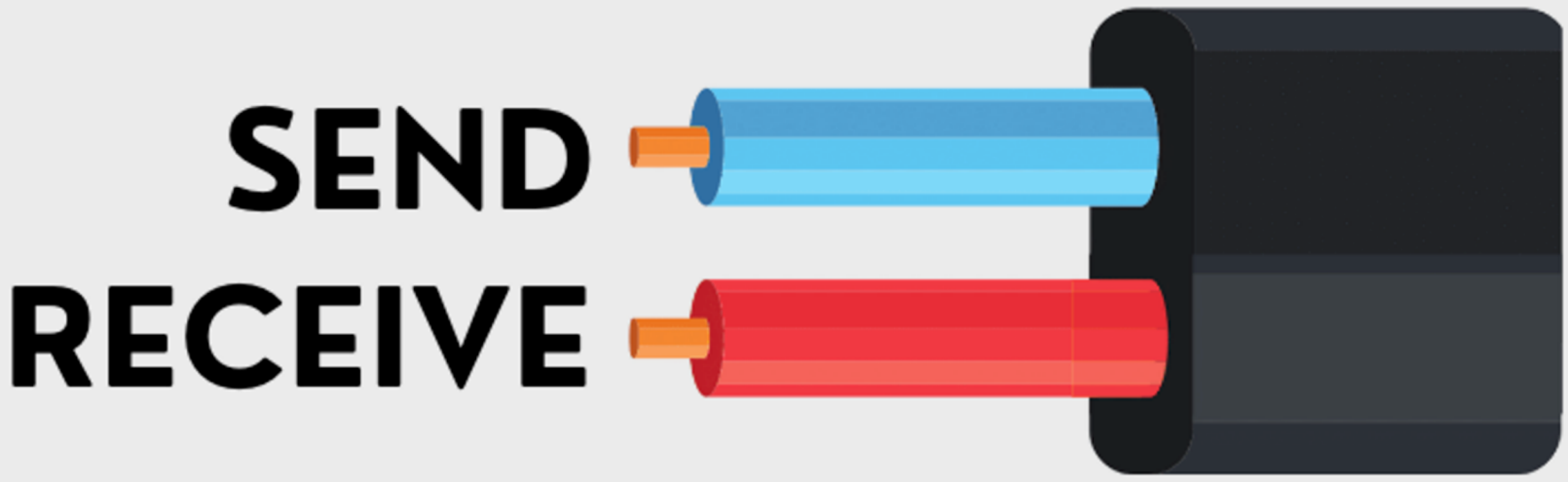
you needed to have a special type of ethernet cable to directly connect 2 computers:

Cross-Over cables

Cross-what?

In order to understand this concept better

let's use a reduced proof of concept (POC)



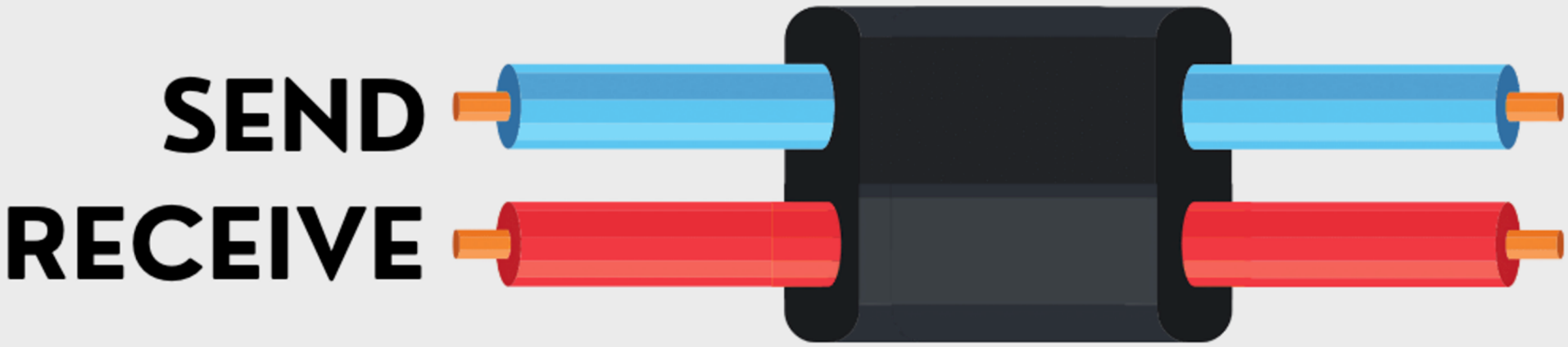
We have a 2 pole cable that shall connect two devices

You plug it into one device on the left side and another one on the right

HOW DO YOU MAKE SURE THEY CAN EXCHANGE INFORMATION?

🤔

@maikroservice



First try:

Machine 1 on the left sends data

via the Send cable (blue)

and that one is plugged into the Send (blue) on the other side


HACKER

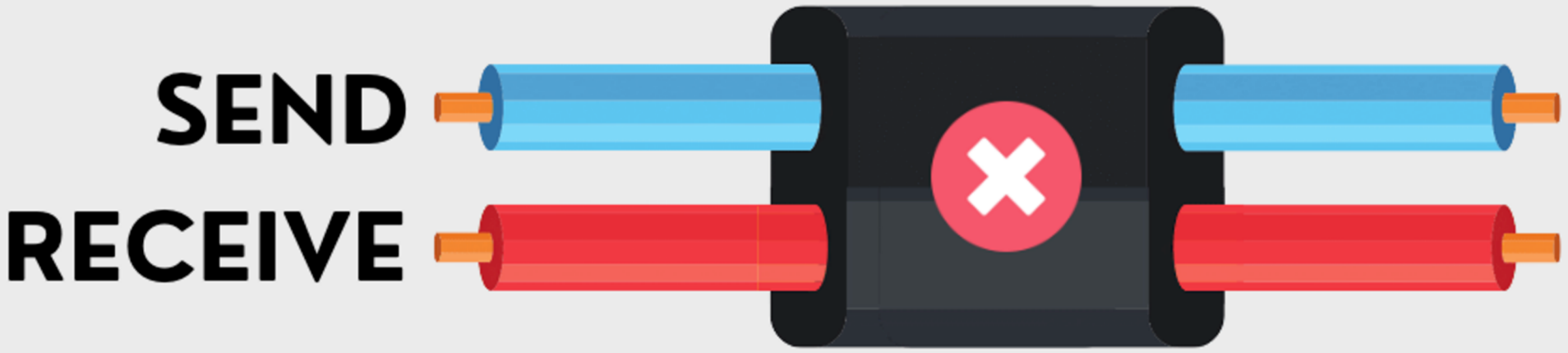
Well ... That wont work, right?!

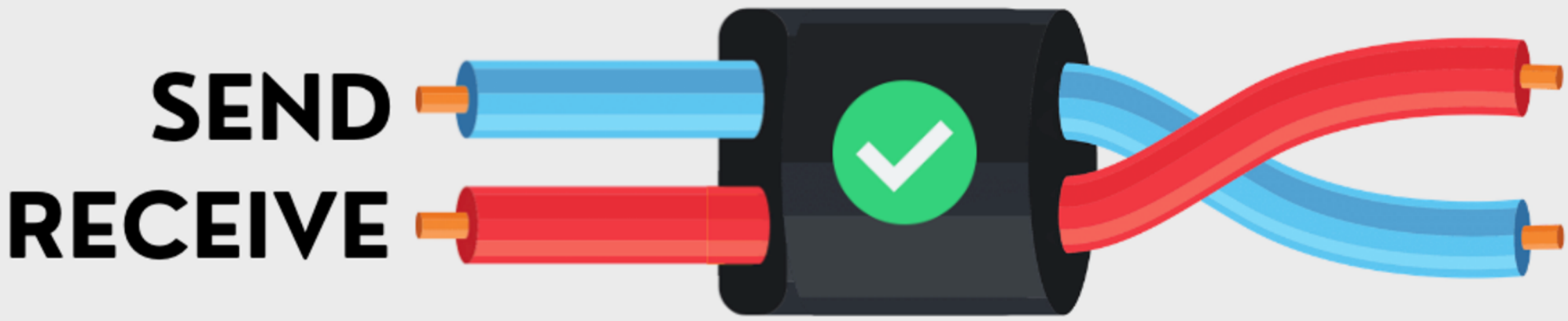
Exactly!

If we push data over the “Send” cable the data will not be received because...

well it is not hitting the receive cable 🤷

How about:





@maikroservice


WINNER


HACKER

DING DING DING, we have a winner. 🙌🏆

If we swap the positions of Send and Receive
the devices can exchange information

because they each get the correct data on the port they expect it

uh… What's a port?

Good question!

As you probably know, a cable needs to be plugged in somewhere

No plug, no need for a cable - much like wifi cable 😎

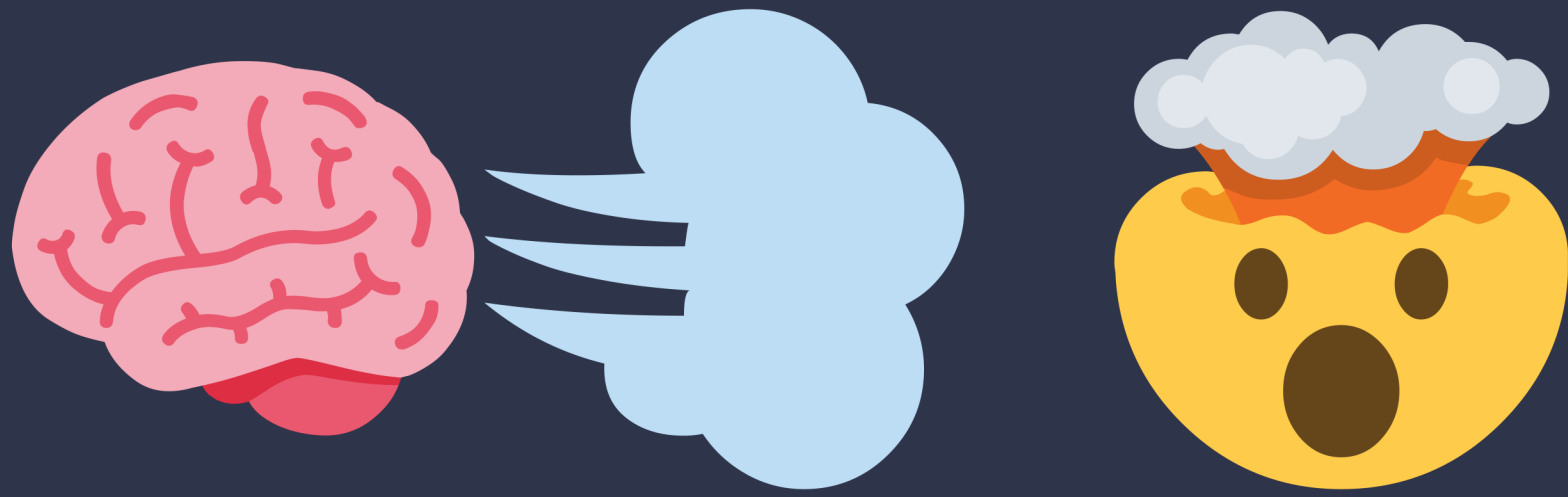
Wifi cable

A physical port is the connector
that you plug your cable into

It might also be broken down
into many ports,
one for each of the poles inside
the cable

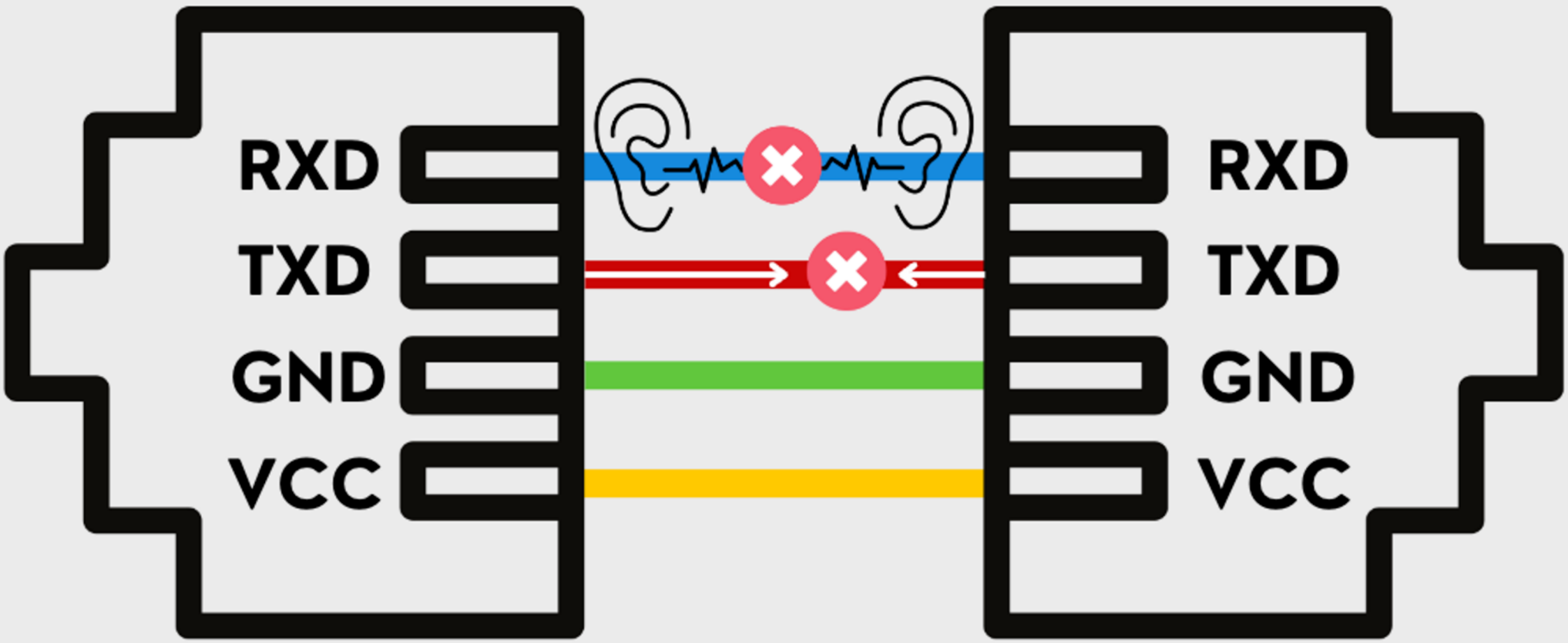
Let us also visualize this concept a little more with some bare-minimum concepts.

OK MY MIND IS YOURS



@maikroservice

Port Traffic Jam



@maikroservice

A cable can be imagined similar to a railway 🚃

its one-way only and if you turn around you will face a lot of trouble
+ at some point jail time because you should not be driving (anymore) 💫😵

By the way, another tragedy would happen on the RECEIVE (RXD) lane, both devices would listen...

But none of them would ever receive anything.

Sad little ears 🦻❌

You should now understand a little better why we need(ed) a cross-over cable to begin with

back when no hardware was sitting in the middle between the two computers

LOOKING FOR MORE CYBER CONTENT?

THE PURPLE TEAM COACH

@maikroservice

FOLLOW ME

+

SHARE THIS POST WITH YOUR FRIENDS / COLLEAGUES

save for later →