Reconnaissance partie 1 :

Les Ports

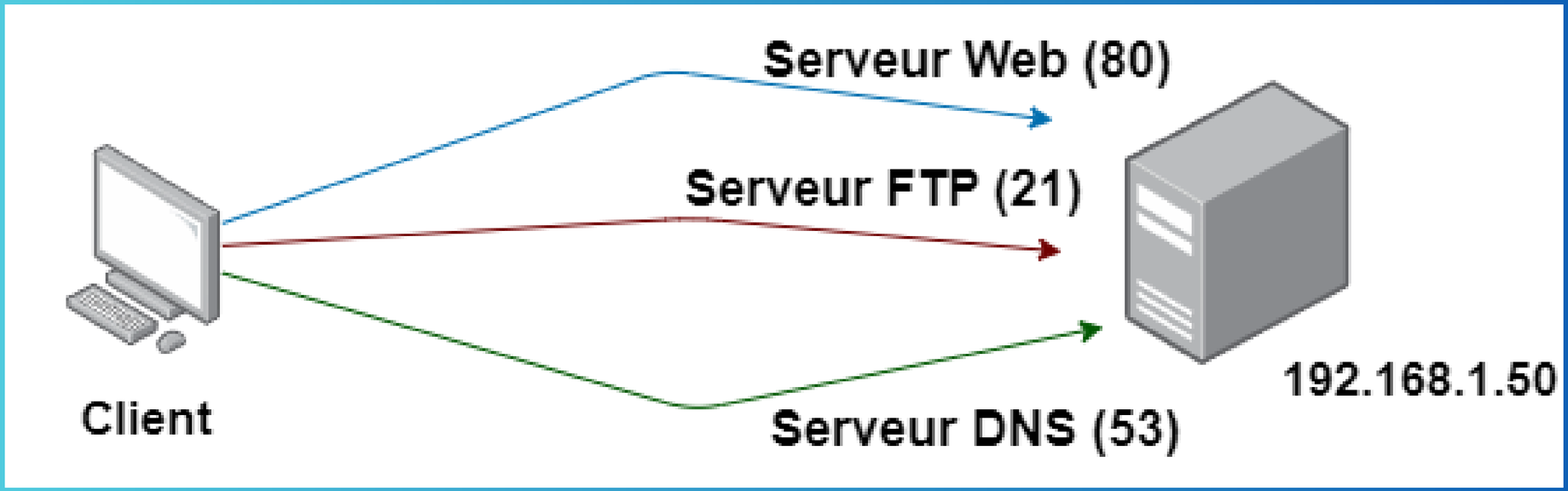
Qu’est ce qu’un port réseau ?

Un port réseau est un numéro logique attribué à un processus ou à un service spécifique sur un périphérique réseau.

192.168.1.50:80

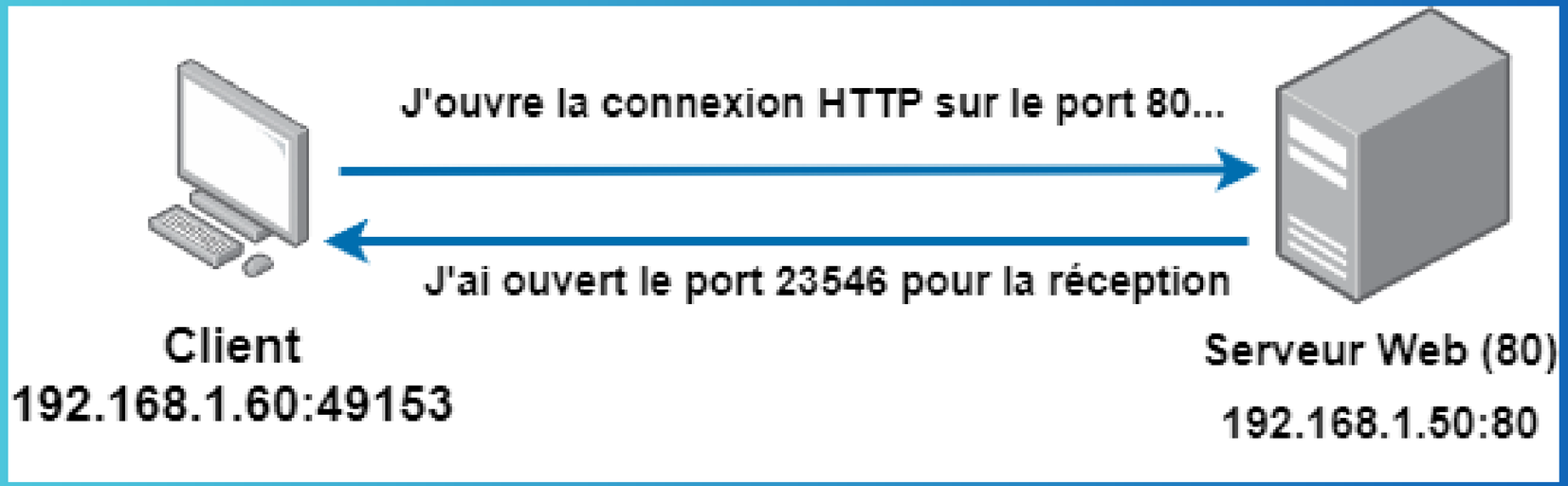
À quoi ça sert ?

Les ports sont cruciaux car ils facilitent l'acheminement correct des données vers les applications appropriées sur un dispositif. Ils permettent de multiplexer différentes applications sur une seule adresse IP



Concrètement :

Les ports sont utilisés par les protocoles de communication pour établir des connexions entre les applications. Ils définissent des points finaux pour la communication.



Combien de ports ?

Les ports sont des numéros qui peuvent prendre jusqu'à 16 bits (soit 2 octets).
On a donc 2^16-1 ports disponibles soit 65536. (un port ne pouvant pas être égal à 0)

Services	Ports
Modbus	502
Telnet	23
FTP	21
SMTP	25
NTP	123
BOOTP	67
DHCP	67
HTTP	80
DNS	53
POP	110
SNMP	161

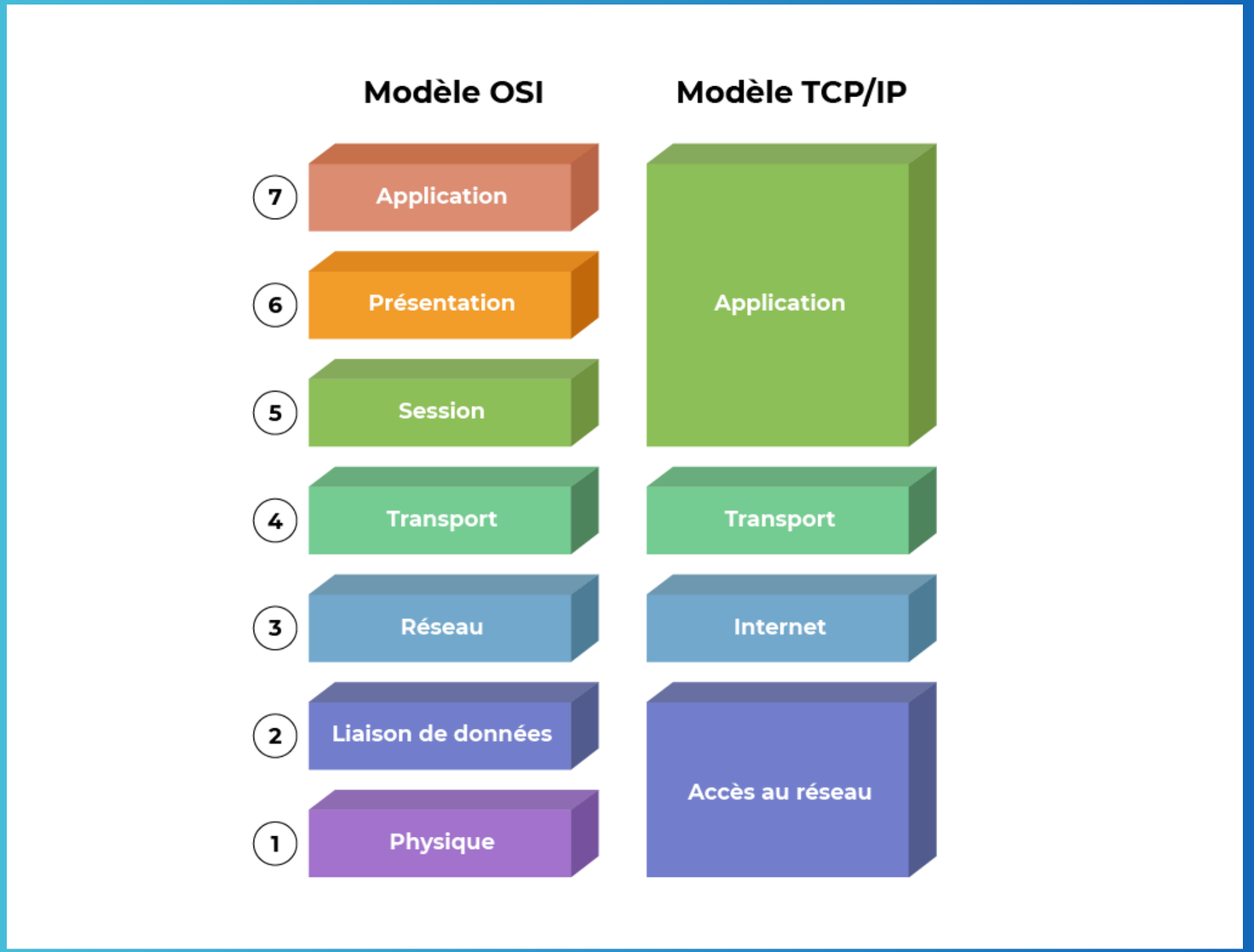
La réglementation :

Certains ports sont réservés : de 1 à 1023, réservés pour les services réseau standard tels que HTTP (port 80) et FTP (port 21).

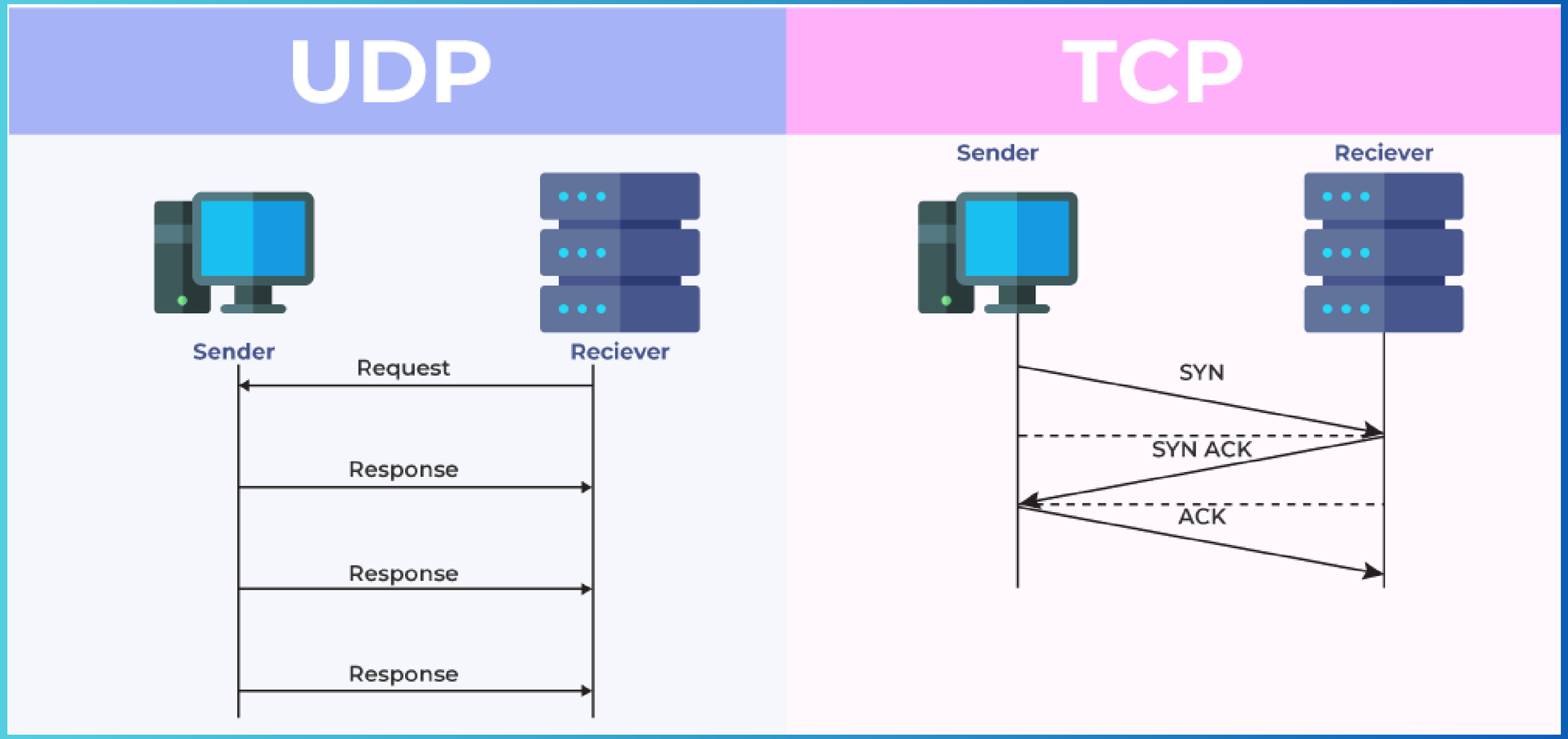
Numéros de port de 1024 à 49151, alloués par l'Internet Assigned Numbers Authority (IANA) aux applications spécifiques. (Minecraft = 25565)

Numéros de port de 49152 à 65535, utilisés de manière dynamique par les systèmes d'exploitation pour les connexions temporaires.

Les protocoles :



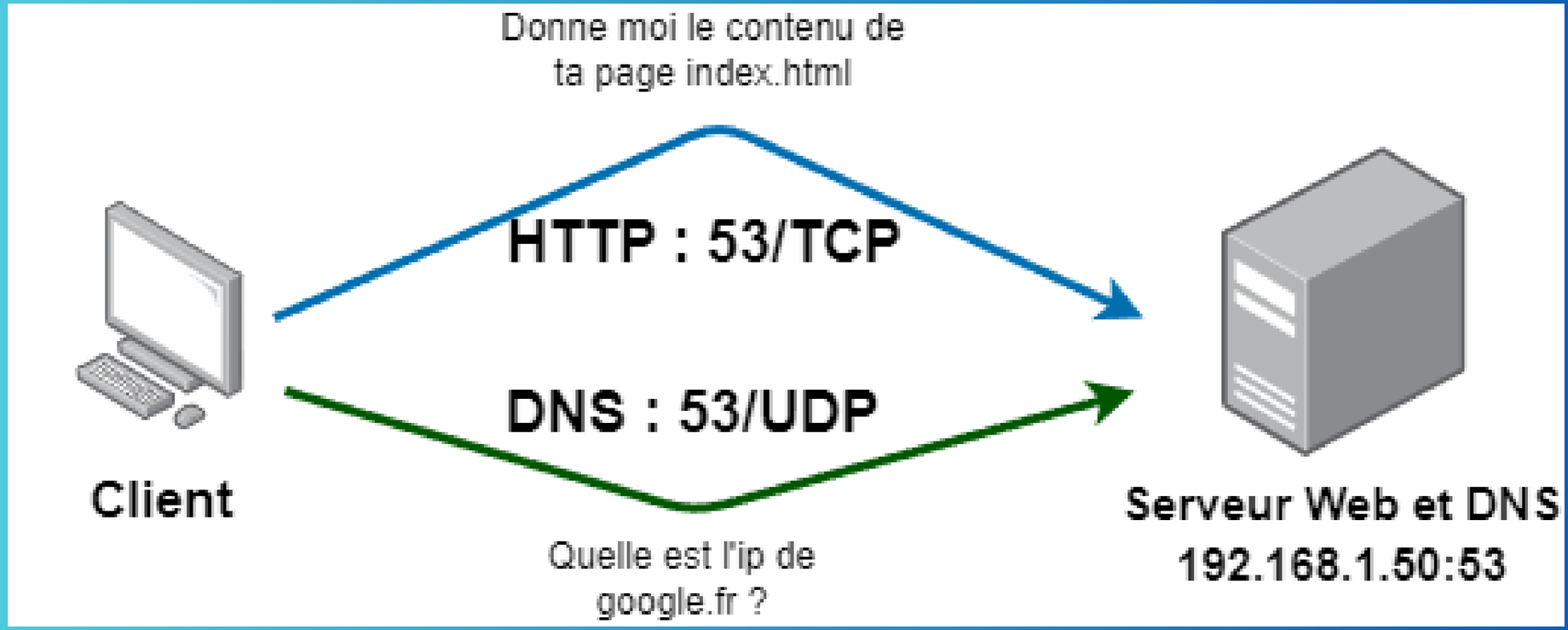
TCP / UDP :


UDP
Sender
Reciever
Request
Response
Response
Response
TCP
Sender
Reciever
SYN
SYN ACK
ACK

Particularité des protocoles

Protocole	TCP/UDP	Description
HTTP	TCP	Protocole de transfert hypertexte pour les pages web.
HTTPS	TCP	HTTP sécurisé, utilise le chiffrement TLS/SSL.
FTP	TCP	Protocole de transfert de fichiers.
SSH	TCP	Protocole de connexion sécurisée pour l'accès distant.
Telnet	TCP	Protocole d'émulation de terminal sur réseau.
DNS	UDP	Système de noms de domaine pour la résolution d'adresses IP.
DHCP	UDP	Protocole de configuration automatique des paramètres IP.
SNMP	UDP	Protocole simple de gestion de réseau.
SMTP	TCP	Protocole de transfert de courrier électronique.
POP3	TCP	Protocole d'office de poste pour la réception de courrier électronique.
IMAP	TCP	Protocole d'accès aux messages Internet pour la récupération de courrier électronique.

C’est dégueulasse mais c’est possible



En bref...

1 port = 1 service

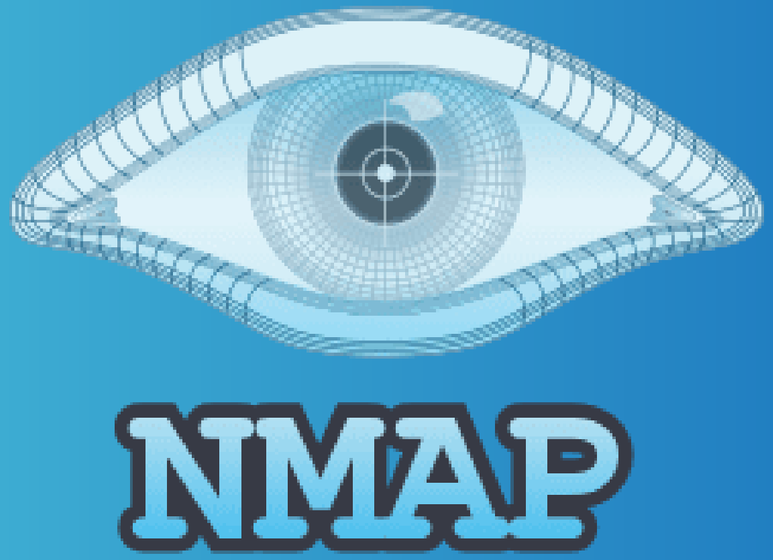
1 service sur 1 port se repose sur une méthode de transport : UDP ou TCP

Les ports sont généralement attribués à des services fixes, mais ce n’est pas toujours le cas.

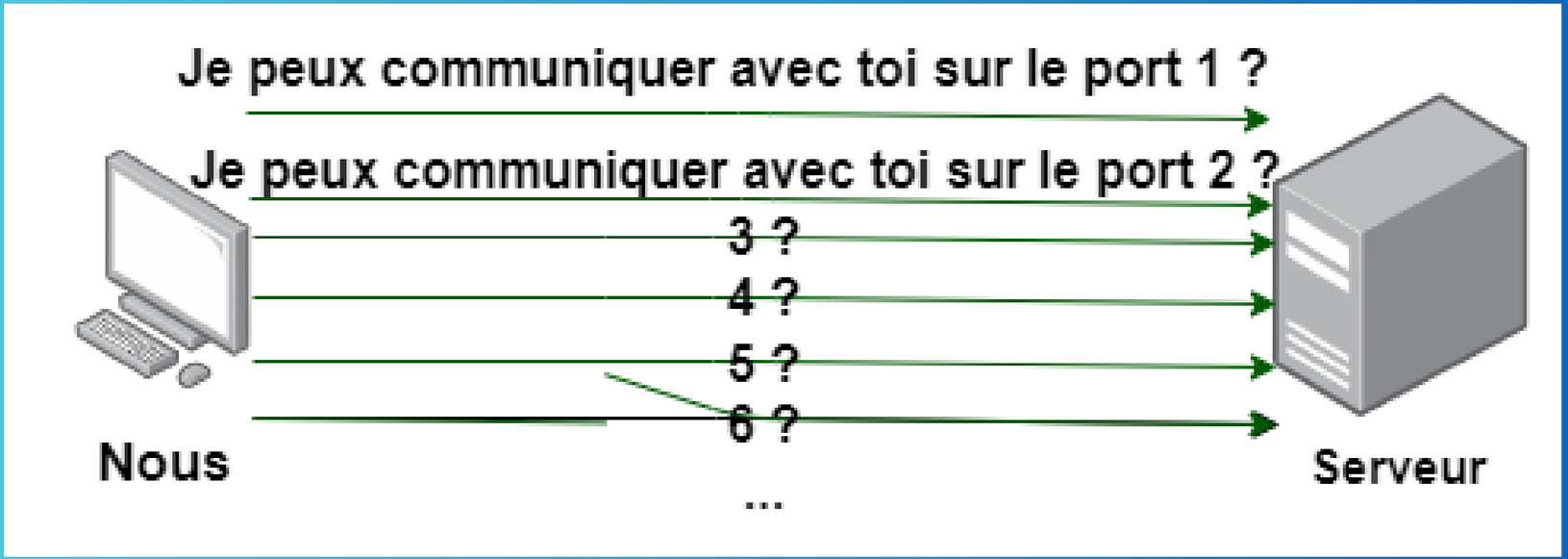
Les plus connus

Service	Protocole	Port	Description
HTTP	TCP	80	Protocole de transfert hypertexte (non sécurisé).
HTTPS	TCP	443	Protocole de transfert hypertexte sécurisé.
FTP (Contrôle)	TCP	21	Contrôle des sessions FTP.
FTP (Données)	TCP	20	Transfert des données FTP.
SSH	TCP	22	Connexion sécurisée à distance.
Telnet	TCP	23	Accès distant non sécurisé.
DNS	UDP/TCP	53	Système de noms de domaine pour la résolution d'adresses IP.
DHCP	UDP	67/68	Protocole de configuration automatique des paramètres IP.
SMTP	TCP	25	Protocole de transfert de courrier électronique.
POP3	TCP	110	Protocole d'office de poste pour la réception de courrier électronique.

Comment connaître les services ouverts sur une machine ??

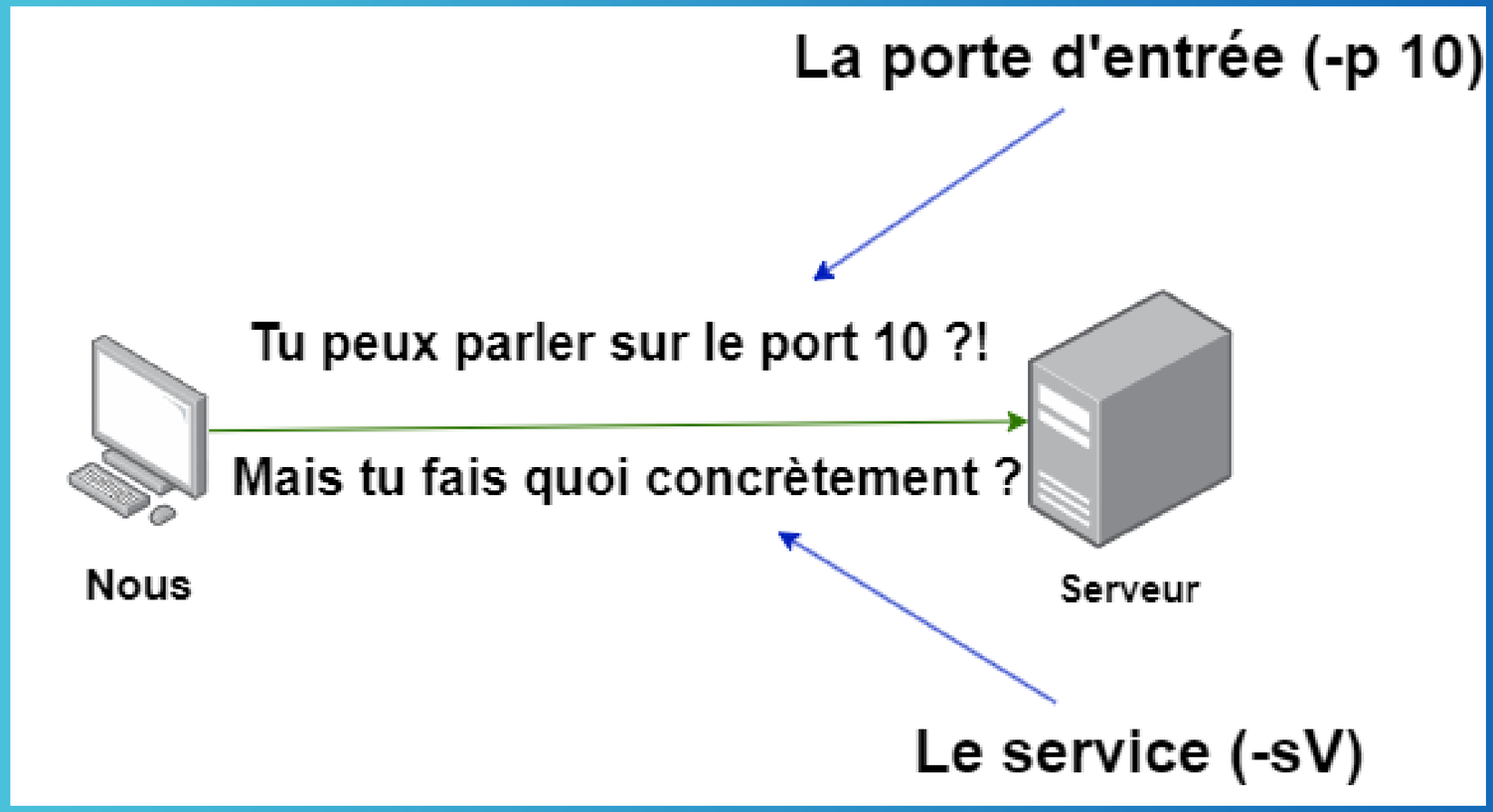


Un harceleur de rue



sudo nmap -p- 192.168.1.1

Un harceleur de rue partie 2



sudo nmap -sV -p 10 192.168.1.1

À vous !

Quel port est ouvert sur la machine ?

Quel service tourne sur la machine ?

10.214.50.50

sudo nmap -p-

sudo nmap -sV


Kahoot!