

COURS #10

Concepts divers & clôture cours

Introduction aux réseaux 2023 (Bloc 2)

Corentin Badot-Bertrand

PARTIE #1

Derniers protocoles applicatifs

Découvrons les derniers protocoles L7 pour ce cours



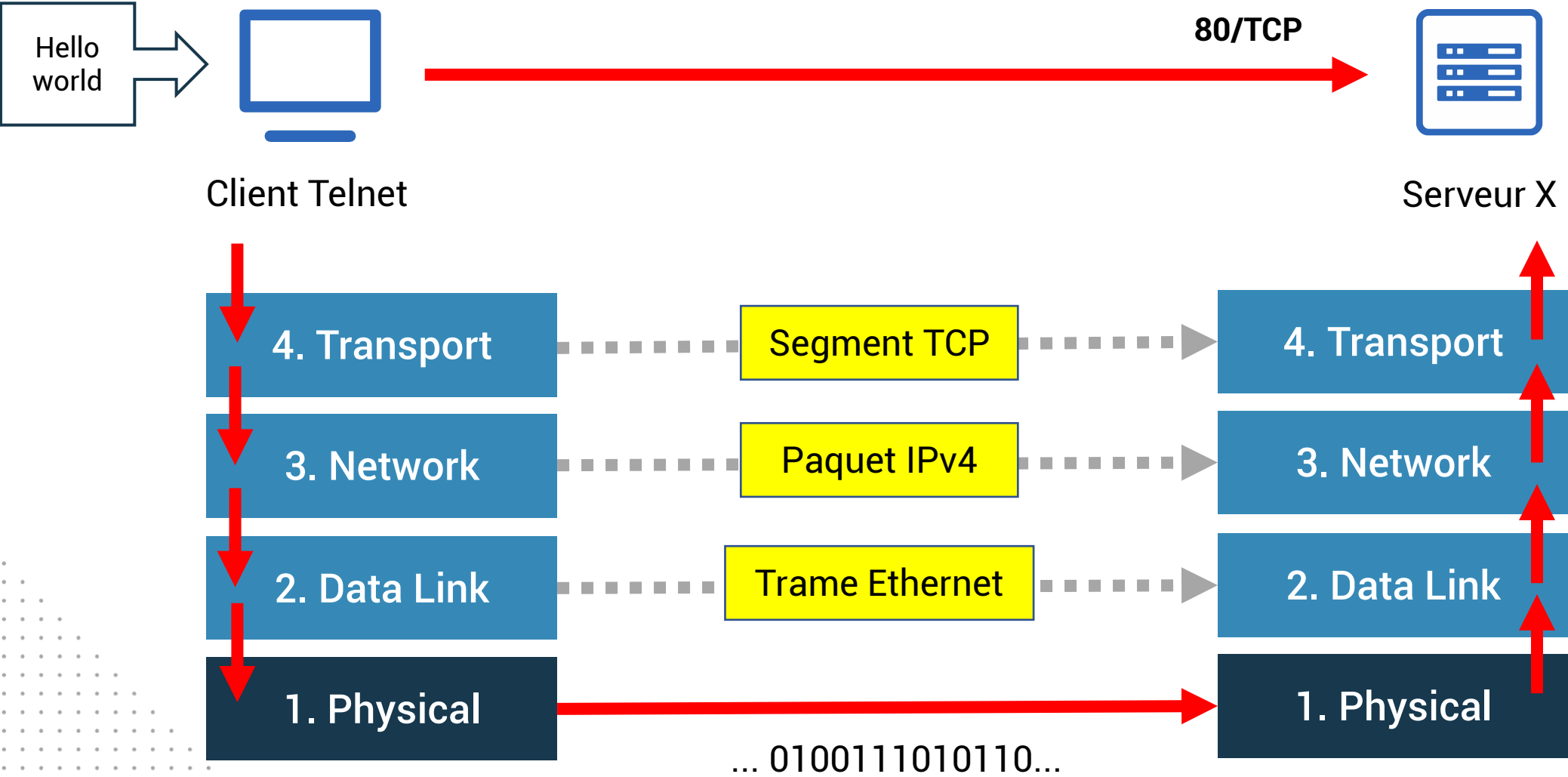
Telnet

Permet d'établir une **connexion TCP interactive** avec des services distants

- TErminaL NETwork
- Historiquement, un serveur telnet utilisait le port **23 (TCP)**
- Un serveur telnet **donne accès** à une machine distante
- Le client telnet permet de s'y connecter... ou d'établir une **connexion TCP**

Telnet n'est PAS sécurisé et le client « telnet » doit seulement être utilisé pour des tests réseau

Le protocole Telnet



Les trois piliers de la sécurité



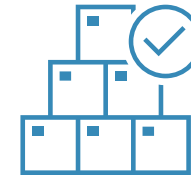
Confidentialité

Seul les utilisateurs
de confiance
accèdent au système



Disponibilité

Le système est
disponible pour les
utilisateurs



Intégrité

Les données sur le
système ne sont pas
compromises

Un **système sécurisé** garantit la
confidentialité, l'intégrité et la disponibilité

Le chiffrement

Garantir la **confidentialité** d'un message transmis sur le réseau

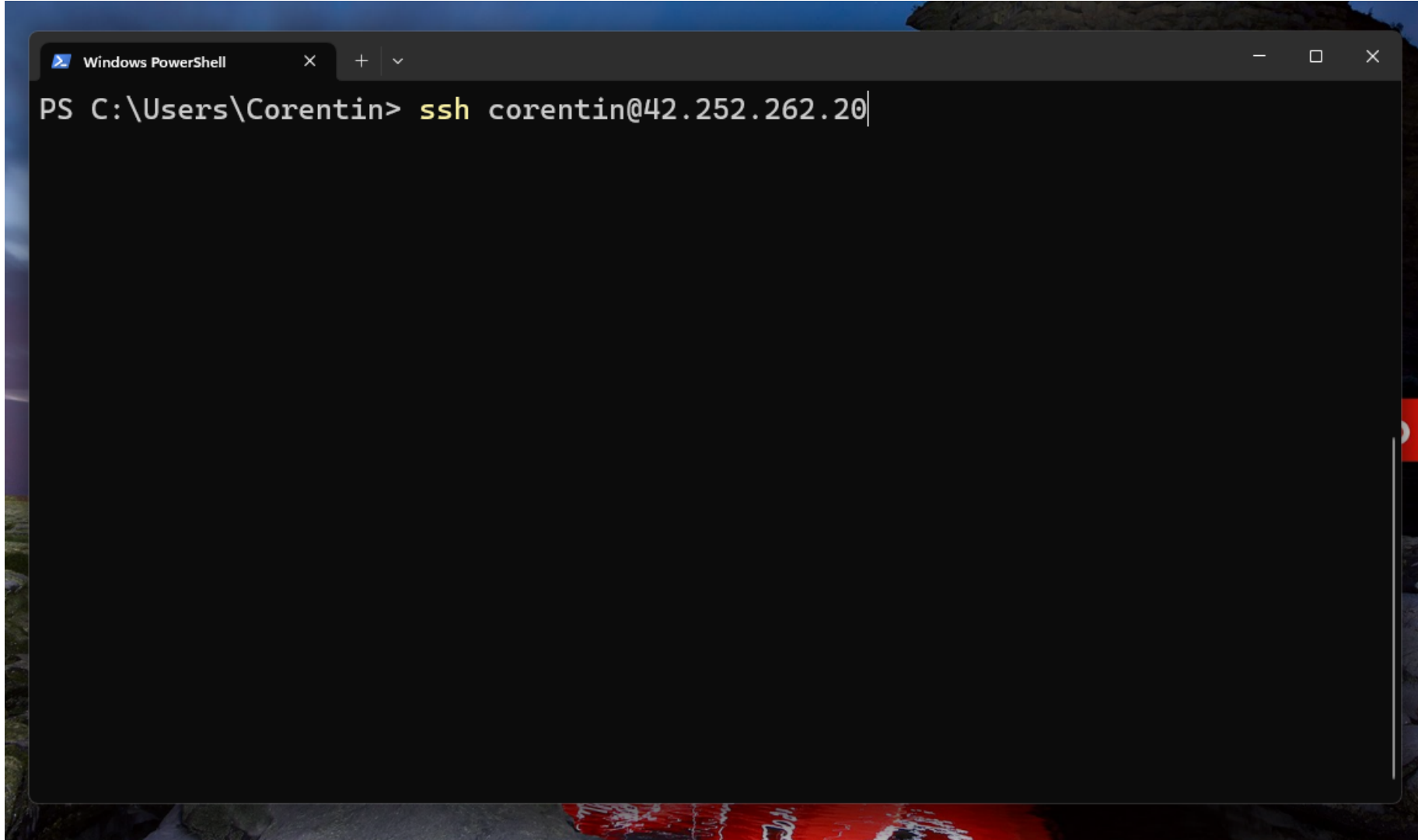
- Une fois les données **chiffrées** – elles ne peuvent être que lues par les personnes autorisées
- La personne autorisée peut alors **déchiffrer** les données
- Utilisation d'une **clé** pour chiffrer & déchiffrer le message
- Chiffrement **symétrique** = l'envoyeur et le receveur se partagent une clé
- Chiffrement **asymétrique** = système de clé publique et privée

On ne dit pas « crypter » - abus de langage

SSH

Permet d'établir une session à distance sécurisée (chiffrement des données)

- Secure SHell
- Successeur de Telnet
- Utilise le port 22 (TCP)
- Permet à un utilisateur de se connecter sur une machine distante
 - Pour administrer la machine
 - Pour utiliser les services présents
 - Pour établir un tunnel SSH
 - (...)
- Le client « ssh » sur Linux/Mac peut être utilisé, « Putty » sur Windows

A screenshot of a Windows PowerShell terminal window. The window has a dark gray title bar with the text "Windows PowerShell" and standard window controls (minimize, maximize, close). The terminal content shows the prompt "PS C:\Users\Coreentin>" followed by the command "ssh corentin@42.252.262.20" which is currently being typed, with a cursor at the end of the line. The background of the terminal is black, and the text is white. The window is set against a desktop background that appears to be a scenic image of a body of water and a red boat.

```
Windows PowerShell
PS C:\Users\Coreentin> ssh corentin@42.252.262.20
```


SFTP

Protocole de **transfert de fichiers sécurisé**, basé sur SSH

- Secure File Transfer Protocol
- Successeur du FTP
- Utilise le port **22 (TCP)**
- N'utilisez plus FTP – risque d'interception des communications

SMTP

Protocole de communication pour l'envoi des emails

- Simple Mail Transfer Protocol
- Utilise le port 25 (TCP)
- Prends en charge le transfert des emails vers des serveurs de messagerie
- Un « serveur SMTP » prends en charge le transfert des emails
- Protocole non-sécurisé

IMAP & POP3

Protocoles de communication pour la réception des emails

- POP3 utilise le port 110 (TCP)
- IMAP utilise le port 143 (TCP)
- POP3 supprime les messages après lecture sur le serveur
- IMAP permet de lire les messages sur le serveur sans destruction
- Protocoles non-sécurisés

PARTIE #2

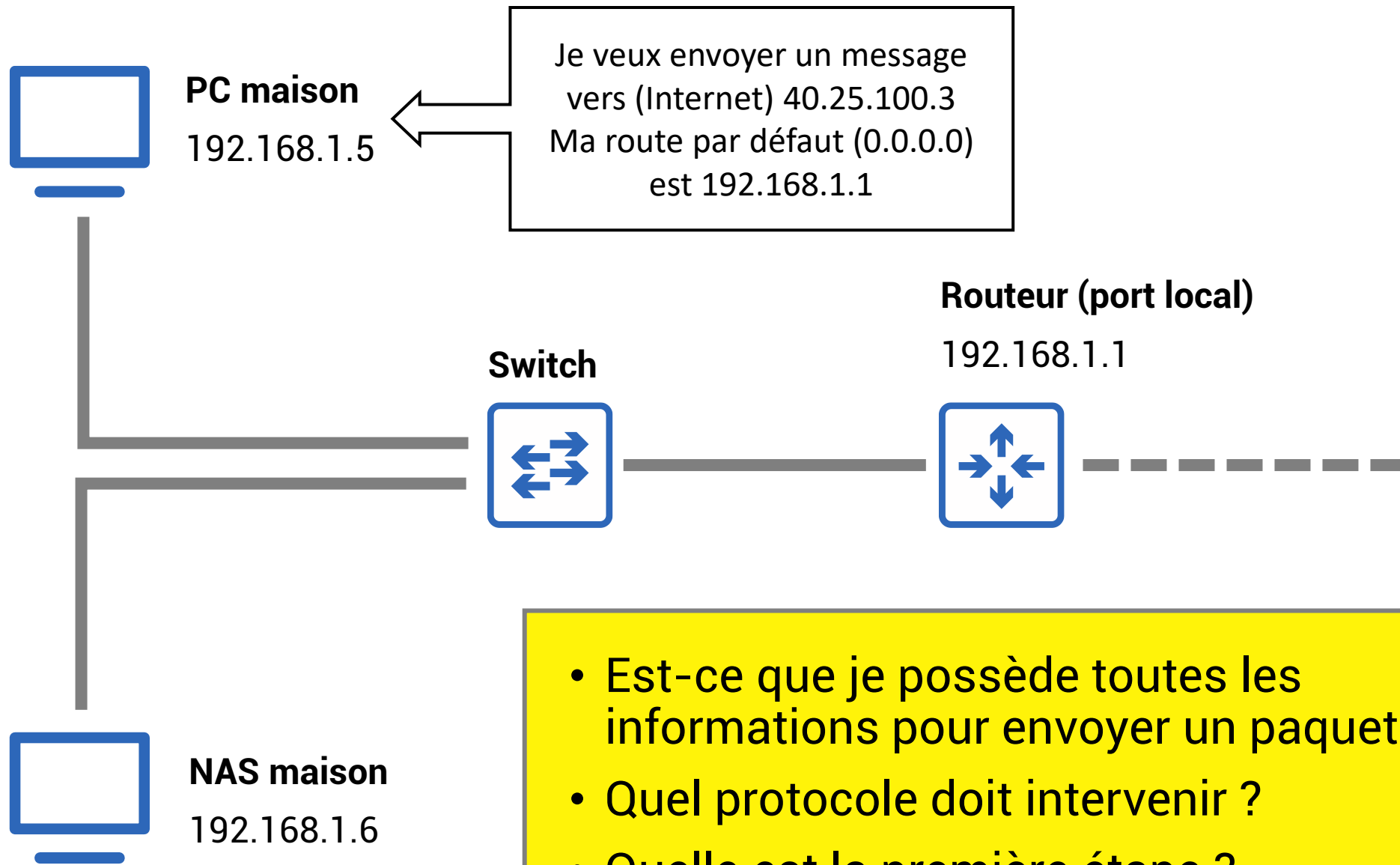
Quelques conseils



Pour préparer l'examen

L'examen sera un QCM (sans points négatifs)

- Sur papier – 2h – pas de supports
- Révissez les **supports** de cours
- Réfléchissez en termes de **couches OSI**
 - Un switch voit seulement des adresses MAC, car c'est la couche OSI ...
 - Un routeur manipule des paquets dans la couche OSI ...
- Révissez quelques **scénarios**
 - Calcul des adresses IP (masque réseau)
 - Fonctionnement d'un switch quand il reçoit une « frame »
 - Construction de la table de routage





- Quelles sont les fonctions de cette machine ?
- Un broadcast storm... Que signifie ce terme et quel protocole sur cette machine peut gérer ce scénario ?



**Courage pour les
projets & examens !**