Cours 7 :

Phase 2 : Le scanning réseau

JACQUEMIN Mathieu

Disclaimer

- Ce cours a été créé dans le but d'informer et d'éduquer les participants sur les sujets liés à la cybersécurité. L'ensemble des techniques présentées le sont à titre pédagogique et préventif afin de pouvoir se prémunir d'attaque potentiel.
- Certaines des techniques présentées sont illégales et dangereuses si elles sont utilisées à mauvais escient, sans maitrise, et sans consentement.
- Il est interdit d'utiliser ces techniques contre toute entité dont vous ne disposez pas le consentement. Dans le cadre d'un accord pour audit, il est obligatoire d'agir dans le cadre d'un contrat parfaitement défini, écrit, et signé par les deux parties.
- Vous devez respecter la loi en vigueur ainsi qu'utilisez les techniques avec éthique et responsabilité.
- Je me dédouane de toute responsabilité en cas de problème ou d'incidents à la suite de ce cours.
- Vous êtes seul responsable de l'usage fait des connaissances enseignées.

Le scanning réseau

Il suit l'étape de la reconnaissance et se base donc sur les infos récupérées précédemment

Etape où l'on cherche plus d'informations et plus précise. (protocoles, ports)

Le scanning réseau

Que scanner et comment ?

Quels services sont sur les serveurs

Quel système d'exploitation

Quelle défense en place

L'énumération

Etape qui suit le scan de port qui sert à énumérer les processus et services qui tournent derrière les ports découverts lors du scanning

Cela peut être :

- **Les noms d'utilisateurs ou de groupes**
- **Les noms des machines**
- **Les ressources du réseau ou partages**
- **Certains paramètres**

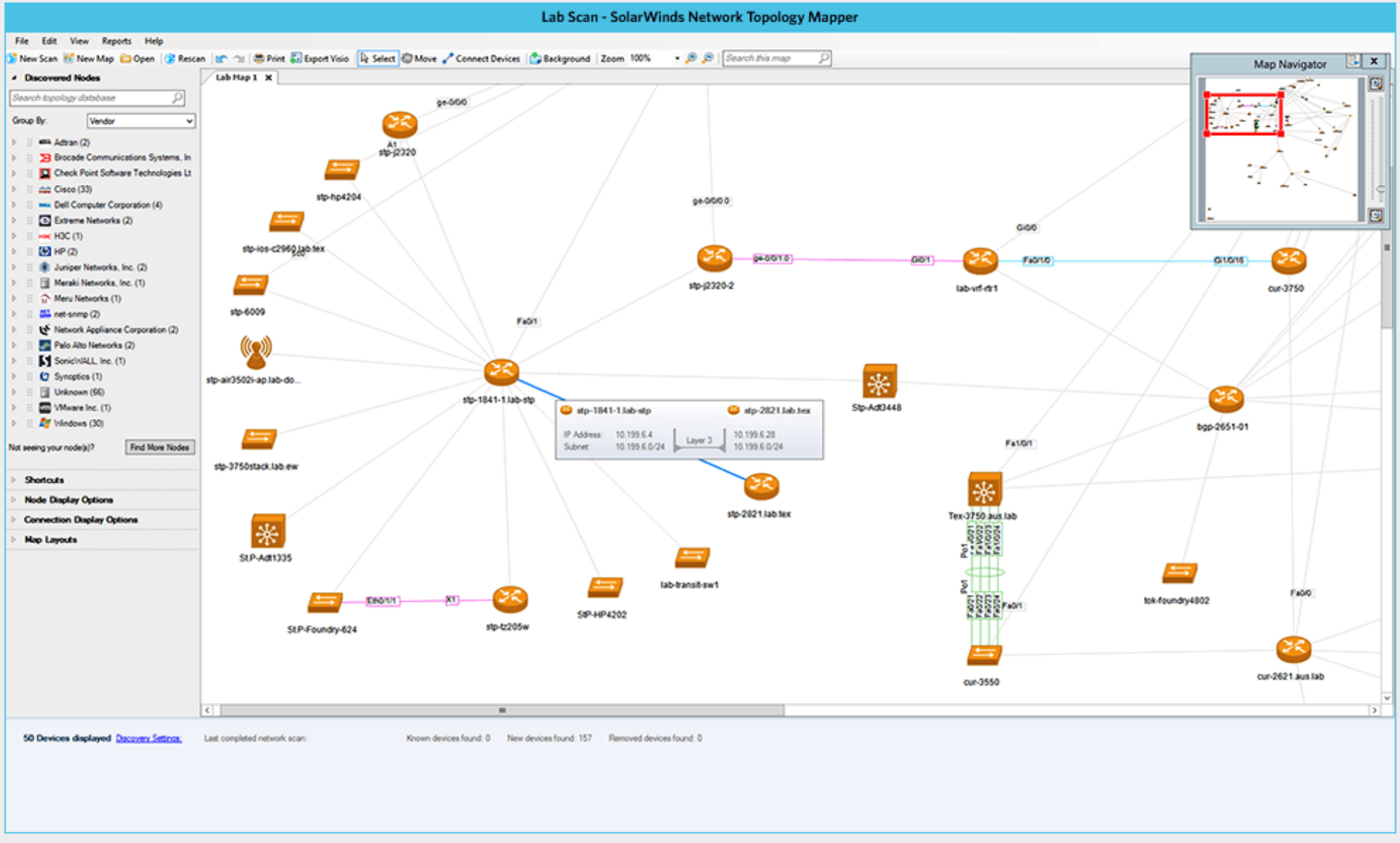
Disclaimer N°2

- Attention à ne pas tout scanner sans réflexion !!!
- Jusqu'à présent on était dans une phase de reconnaissance, plus généralement passive, ou l'on ne faisait que récupérer des informations sur le web. Mais à partir de maintenant, la recherche d'informations devient vraiment active, plus volontaire, et de ce fait des défenses en place risquent de signaler les tentatives de scanning ou d'intrusion.
- Scan non autorisé par défaut : Il est souvent pris pour une action malveillante car elle est volontaire et vise à récupérer des informations précises sur une entreprise, sur un serveur donné
- Peut faire réagir des systèmes de détection d'intrusion : Ca ne pose pas de problème si on a les autorisations nécessaires mais dans le cas contraire, ça peut vous retomber dessus.

Types de scans

- Ping sweep
- Scan de ports
- Network mapping
- OS Fingerprinting

Network mapping



Se protéger

Utilisation d'un pare-feu qui permet d'autoriser ou de bloquer des ports

Utilisation d'IDS (Intrusion Detection System)

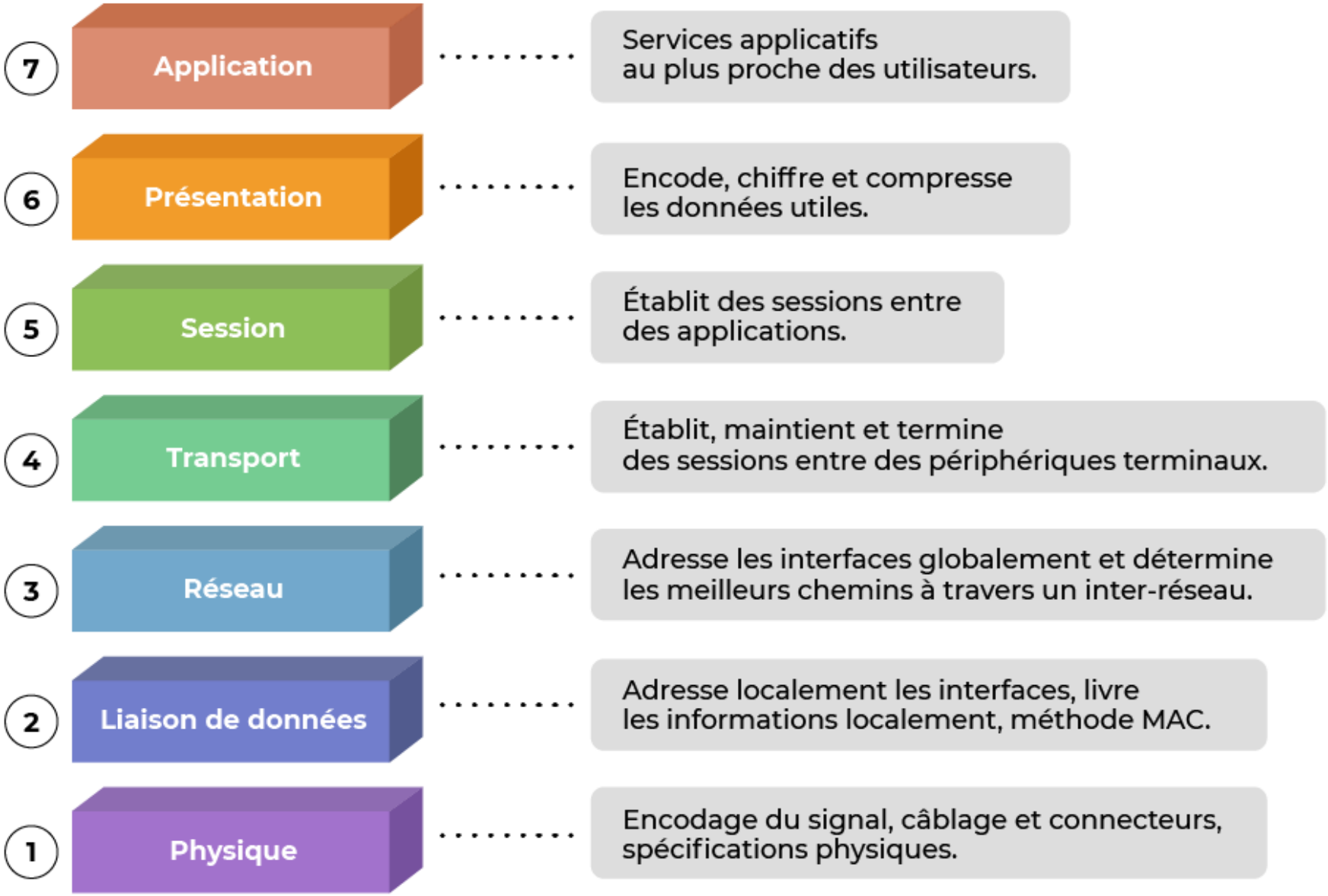
Qu'est-ce que le modèle OSI

Le modèle OSI est un standard de communication réseau, qui vient de Open Systems Interconnection

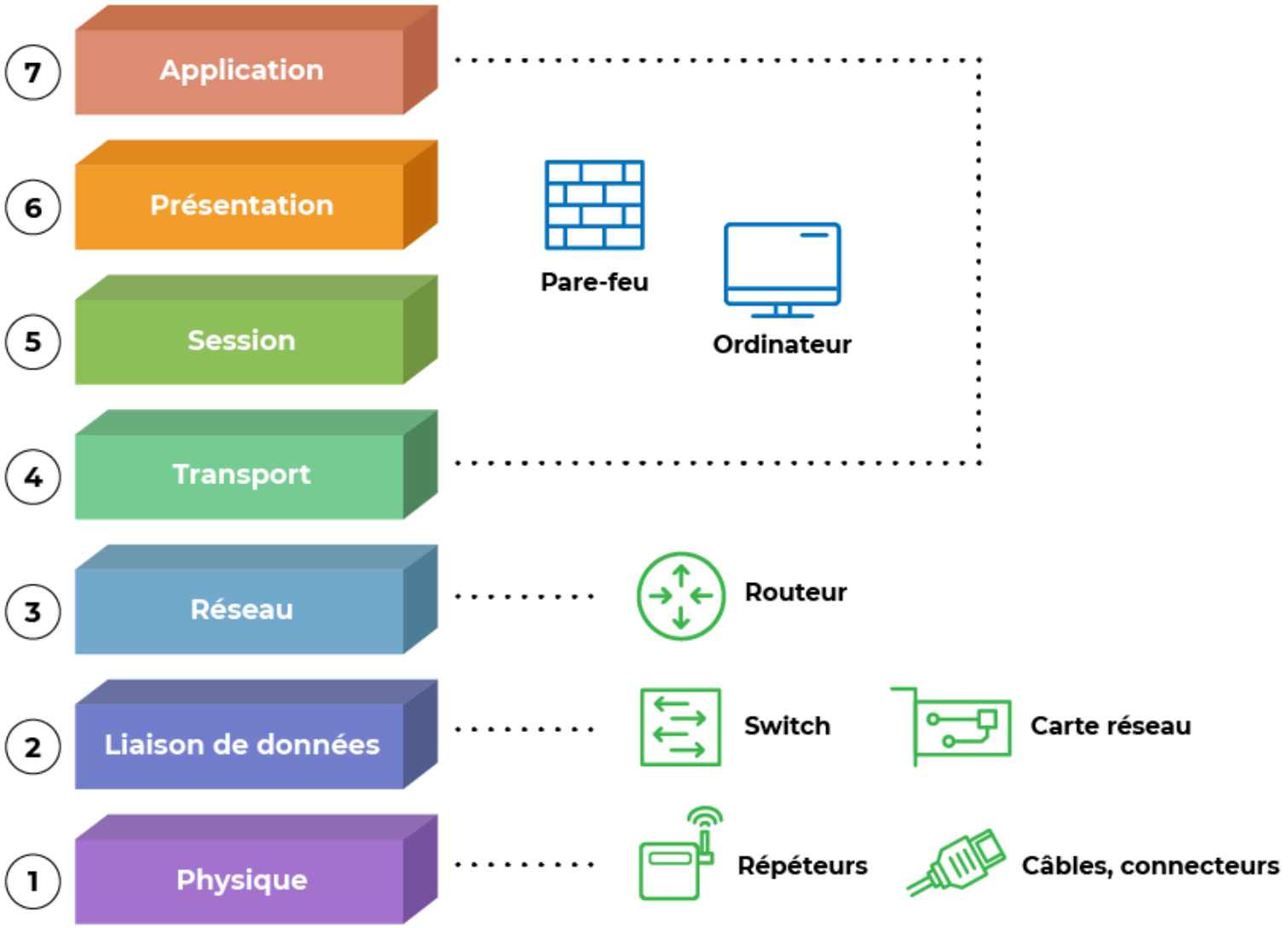
Il a été standardisé par l'organisme de standardisation ISO

Composé de 7 couches superposées

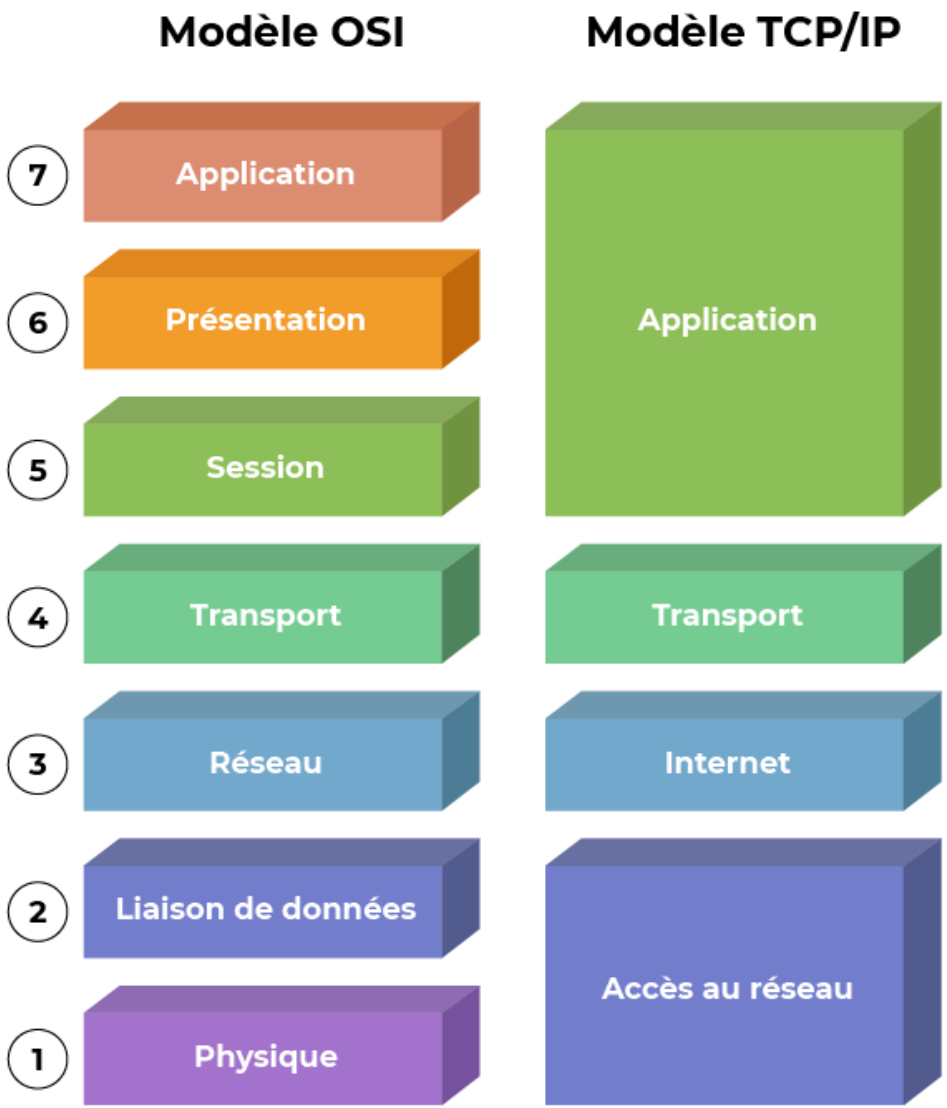
Modèle OSI


7
Application
Services applicatifs
au plus proche des utilisateurs.
6
Présentation
Encode, chiffre et compresse
les données utiles.
5
Session
Établit des sessions entre
des applications.
4
Transport
Établit, maintient et termine
des sessions entre des périphériques terminaux.
3
Réseau
Adresse les interfaces globalement et détermine
les meilleurs chemins à travers un inter-réseau.
2
Liaison de données
Adresse localement les interfaces, livre
les informations localement, méthode MAC.
1
Physique
Encodage du signal, câblage et connecteurs,
spécifications physiques.

Modèle OSI


7
Application
6
Présentation
5
Session
4
Transport
3
Réseau
2
Liaison de données
1
Physique
Pare-feu
Ordinateur
Routeur
Switch
Carte réseau
Répéteurs
Câbles, connecteurs

Modèle TCP / IP



Les Ports Réseaux

Dans le protocole TCP/IP, les applications utilisent différentes portes de communication en TCP ou en UDP, appelés ports réseaux.

Ces ports sont numérotés de 0 à 65635, tant en TCP qu'en UDP.

Ces numéros correspondent en général à un service applicatifs réseaux spécifiques.

Le port étant lié à une adresse IP, il est séparé par le caractère « : »

Exemple : « 192.168.1.14:443 »

Les Ports Réseaux

Port 80 : HTTP

Port 21 : FTP

Port 443 : HTTPS

Port 161/162 : SNMP

Port 123 : NTP

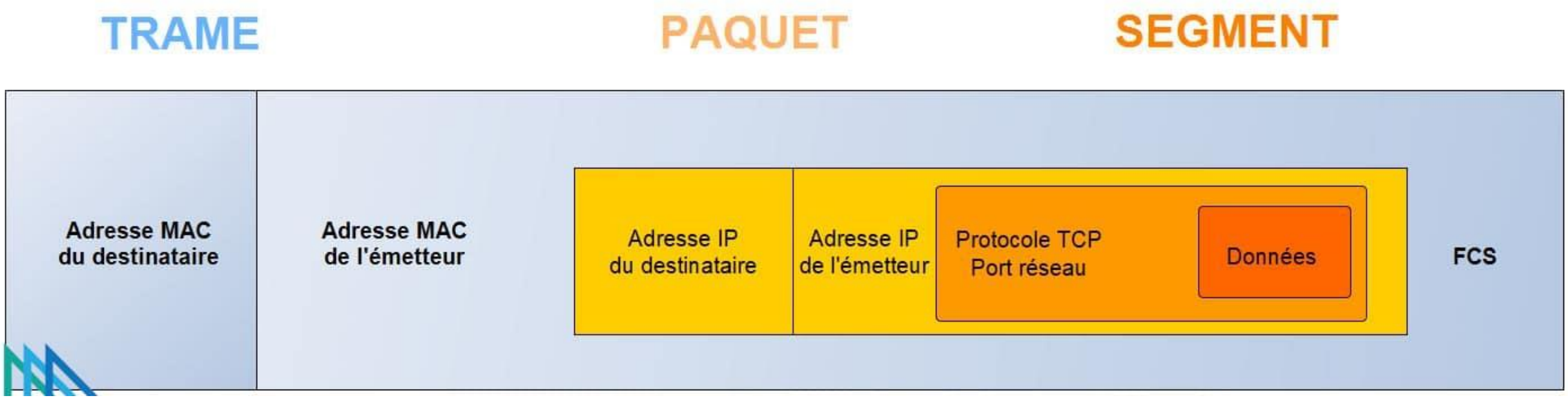
Port 22 : SSH

Port 25 : SMTP

Port 53 : DNS

Port 68 : DHCP

La trame TCP / IP

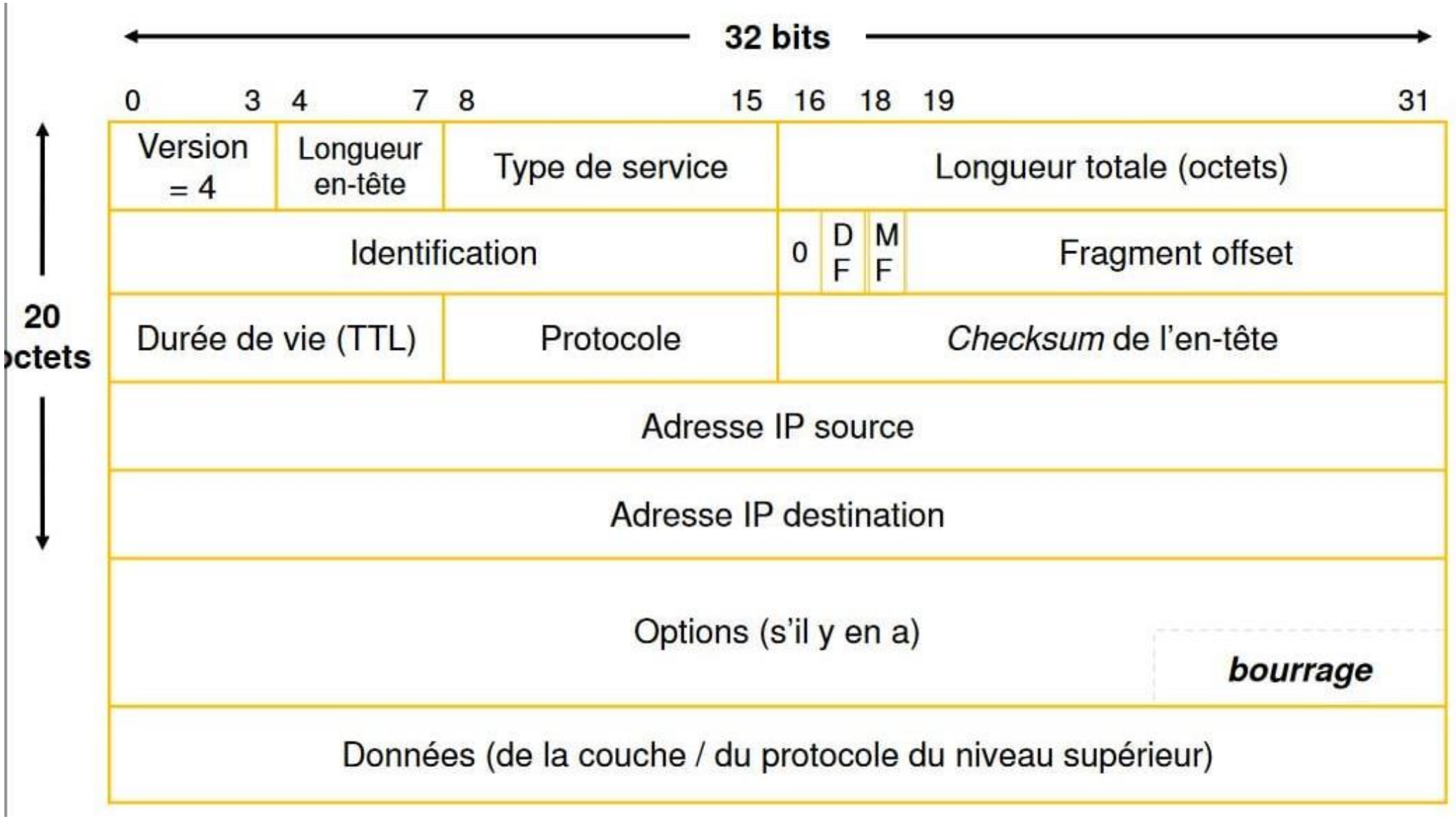


TRAME Ethernet
Couche 2 modèle OSI
Couche Liaison

PAQUET IP
Couche 3 modèle OSI
Couche Réseau

SEGMENT TCP
Couche 4 modèle OSI
Couche Transport

Le paquet IP



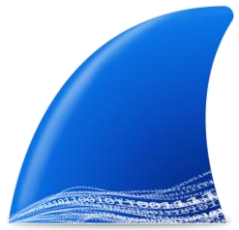
source http://www.i3s.unice.fr/~map/Cours/LPSILADMIN/C3_Reseau_IP_CIDR_LPSIL.pdf

Wireshark

Analyseur de paquets

Logiciel libre et gratuit

Il est utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie



En savoir plus

Liste des ports
https://fr.wikipedia.org/wiki/Liste_de_ports_logiciels

Vidéo Comprendre le modèle OSI de Cookie Connecté
https://www.youtube.com/watch?v=26jazyc7VNk

Vidéo Ports et protocoles de Cookie Connecté
https://www.youtube.com/watch?v=YSI6bordSh8

Logiciel Advanced IP SCAN et PORT SCANNER
https://www.advanced-port-scanner.com/fr/

Logiciel Wireshark
https://www.wireshark.org/download.html