

# BASES DES RÉSEAUX

Objectifs du module

## OBJECTIFS

- Connaître les couches du modèle OSI
- Manipuler les unités de mesure informatique
- Appréhender l'adressage IP
- Connaître la communication au sein d'un réseau
- Découvrir les premières commandes
- Comprendre pourquoi un équipement arrive à communiquer avec un autre

Plan du module

# SOMMAIRE

- Module 1 : Le modèle OSI
- Module 2 : Les unités informatiques
- Module 3 : L'adressage IPv4
- Module 4 : La communication
- Module 5 : Les premières commandes
- Module 6 : L'adressage IPv6

# BASE DES RÉSEAUX

## 01 – LE MODÈLE OSI



## Objectifs

- Représenter le modèle OSI
- Expliquer le principe d'encapsulation
- Expliquer le principe de désencapsulation
- Illustrer la communication entre ordinateurs
- Connaître le fonctionnement des couches du modèle OSI

# Présentation du modèle OSI

- **Modèle OSI** (*Open Systems Interconnection*)
  - Présenté en 7 couches indépendantes et communicantes
  - Représente la communication entre systèmes d'information en réseau
  - Proposé par l'organisme de normalisation ISO (International Organization for Standardization)
- **Protocole**
  - Ensemble de règles à respecter permettant la communication entre systèmes d'information en réseau
  - Exemple : **I**nternet **P**rotocol (ensemble de protocoles utilisés sur Internet puis dans les réseaux locaux)

- **PDU** (Protocol Data Unit / Unité de données de Protocole)
  - Unité de mesure des données échangées dans un réseau
  - Constitué de plusieurs éléments distincts :
    - Des informations de contrôle de protocole (**PCI** : **P**rotocol **C**ontrol **I**nformation)
    - Des unités de données de service (**SDU** : **S**ervice **D**ata **U**nit)



- Les couches OSI

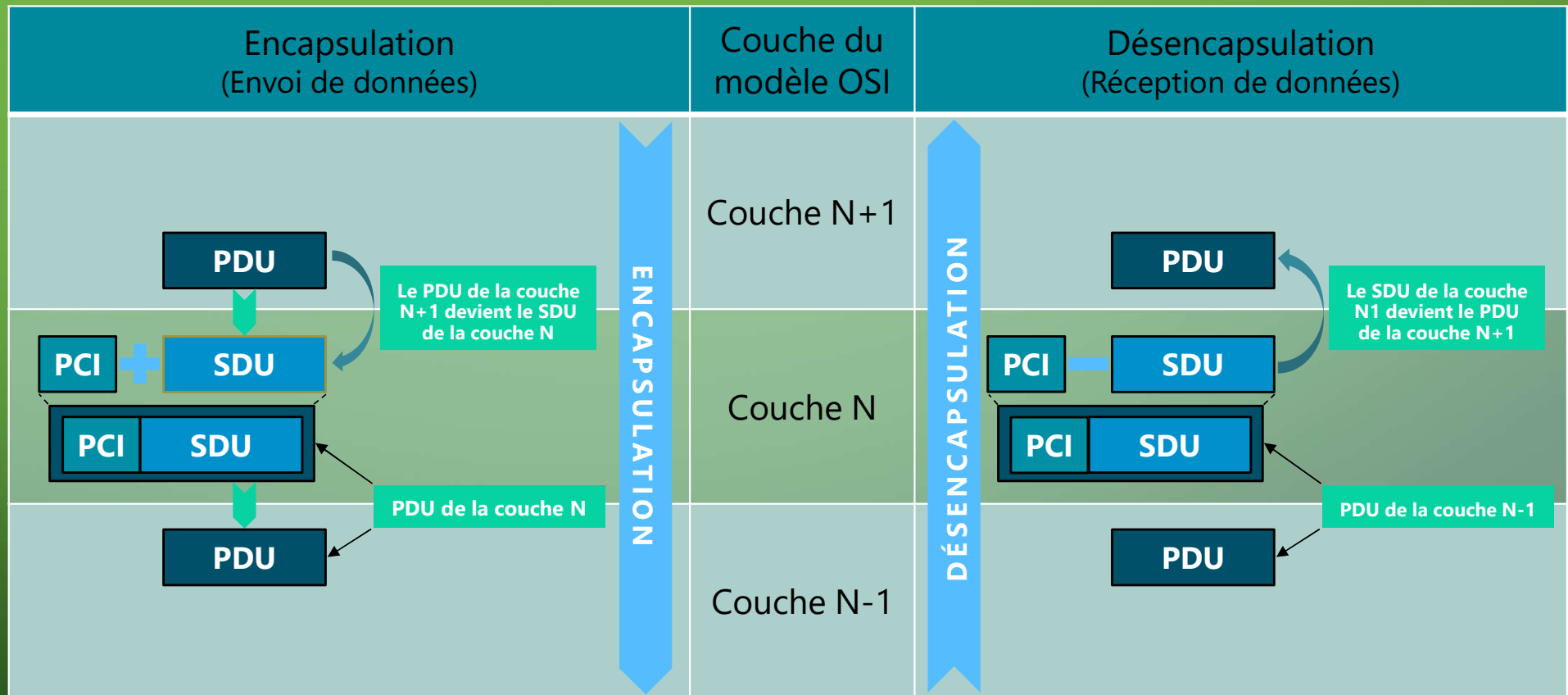
Couches OSI	Rôle	
<b>Application</b>	<i>Point d'accès au réseau</i>	<ul style="list-style-type: none"> <li>Communication entre applications</li> <li>Communication entre l'utilisateur et les applications</li> <li>Entrée et sortie des données</li> </ul>
<b>Présentation</b>	<i>Traduction des données</i>	<ul style="list-style-type: none"> <li>(Dé)Chiffrement / (Dé)Compression</li> <li>Formatage des données (dédiées &lt;—&gt; non-dédiées)</li> </ul>
<b>Session</b>	<i>Fiabilisation de la communication</i>	<ul style="list-style-type: none"> <li>Authentification entre les PC</li> <li>Synchronisation des échanges</li> <li>Création de points de contrôle</li> </ul>
<b>Transport</b>	<i>Transmission de bout en bout entre applications / Segmentation des données</i>	<ul style="list-style-type: none"> <li>Contrôle de flux (segmentation et réduction de l'encombrement)</li> <li>Communication entre même type applications (ports)</li> </ul>
<b>Réseau</b>	<i>Transmission de bout en bout entre PCs Routage</i>	<ul style="list-style-type: none"> <li>Communication entre les PC expéditeur et destinataire</li> <li>Choix de la meilleure route (routage)</li> <li>Adressage logique (adresses IPv4 &amp; IPv6)</li> </ul>
<b>Liaison</b>	<i>Transmission de point à point</i>	<ul style="list-style-type: none"> <li>Communication entre nœuds adjacents</li> <li>Contrôle d'erreurs et de flux</li> <li>Adressage physique (adresses Mac)</li> </ul>
<b>Physique</b>	<i>Transmission du signal</i>	<ul style="list-style-type: none"> <li>Conversion des données informatiques en bits</li> <li>Mis en forme de signal en fonction de média (Modulation)</li> </ul>

# PRÉSENTATION DU MODÈLE OSI

Couches OSI	Protocoles - Ports											Matériels			
Application	FTP File Transfer Protocol 21	HTTP Hyper Text Transfer Protocol 80	HTTPS Hyper Text Transfer Protocol Secure 443	SMTP Simple Mail Transfer Protocol 25	SSH Secure Shell 22	IMAP Internet Message Access Protocol 143	LDAP Lightweight Directory Access Protocol 389	RDP Remote Desktop Protocol 3389	DNS Domain Name System 53	DHCP Dynamic Host Configuration Protocol 67-68	SNMP Simple Network Management Protocol 161-162				PARE-FEU
Présentation															
Session															
Transport	TCP								UDP						
Réseau	ICMP IPv4 – IPv6 ARP														
Liaison	Adresse MAC – Contrôle d'erreurs												SWITCH	ROUTEUR	
Physique	Bits											HUB			

# PRÉSENTATION DU MODÈLE OSI

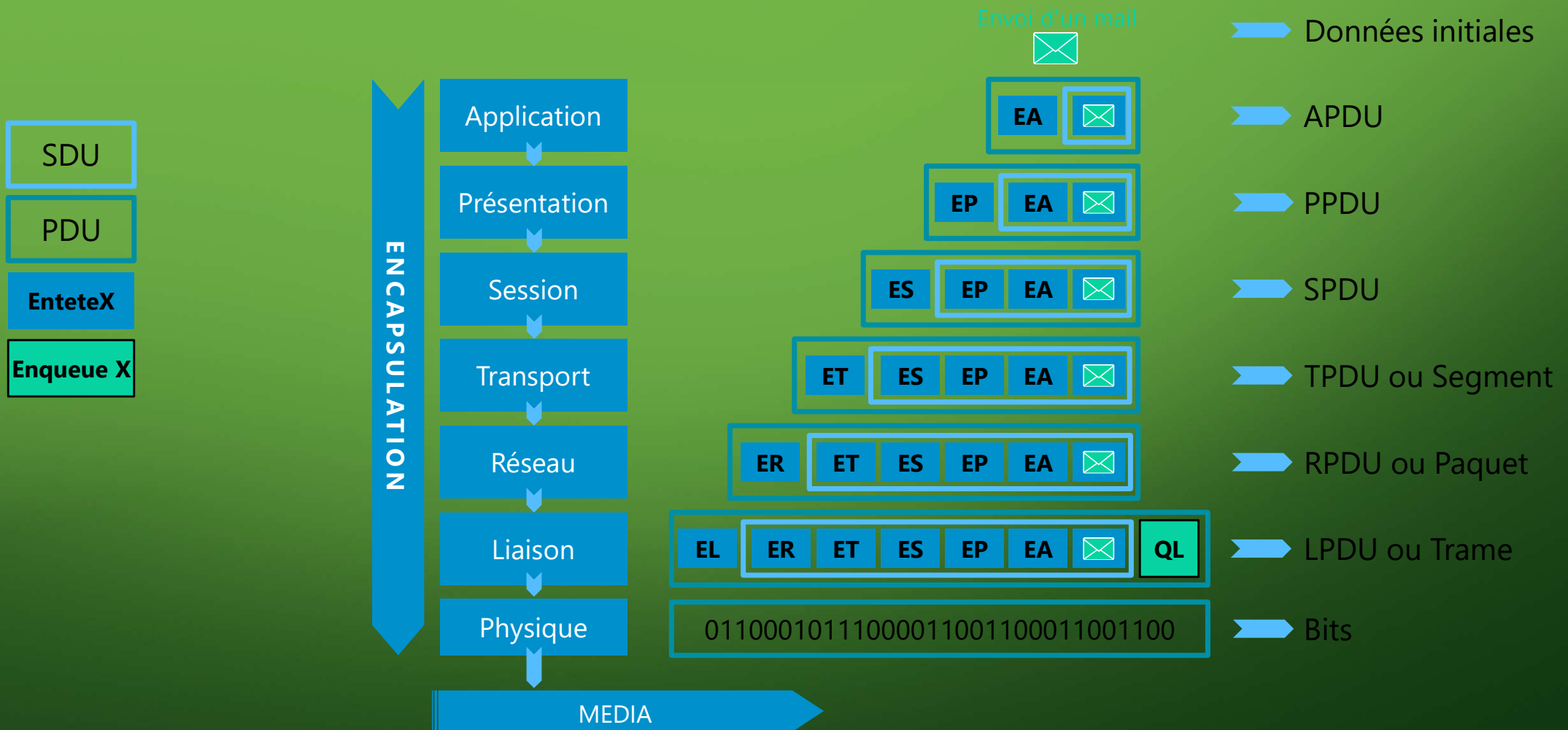
## Communication entre les couches



# Encapsulation

# • Comment ça marche ?

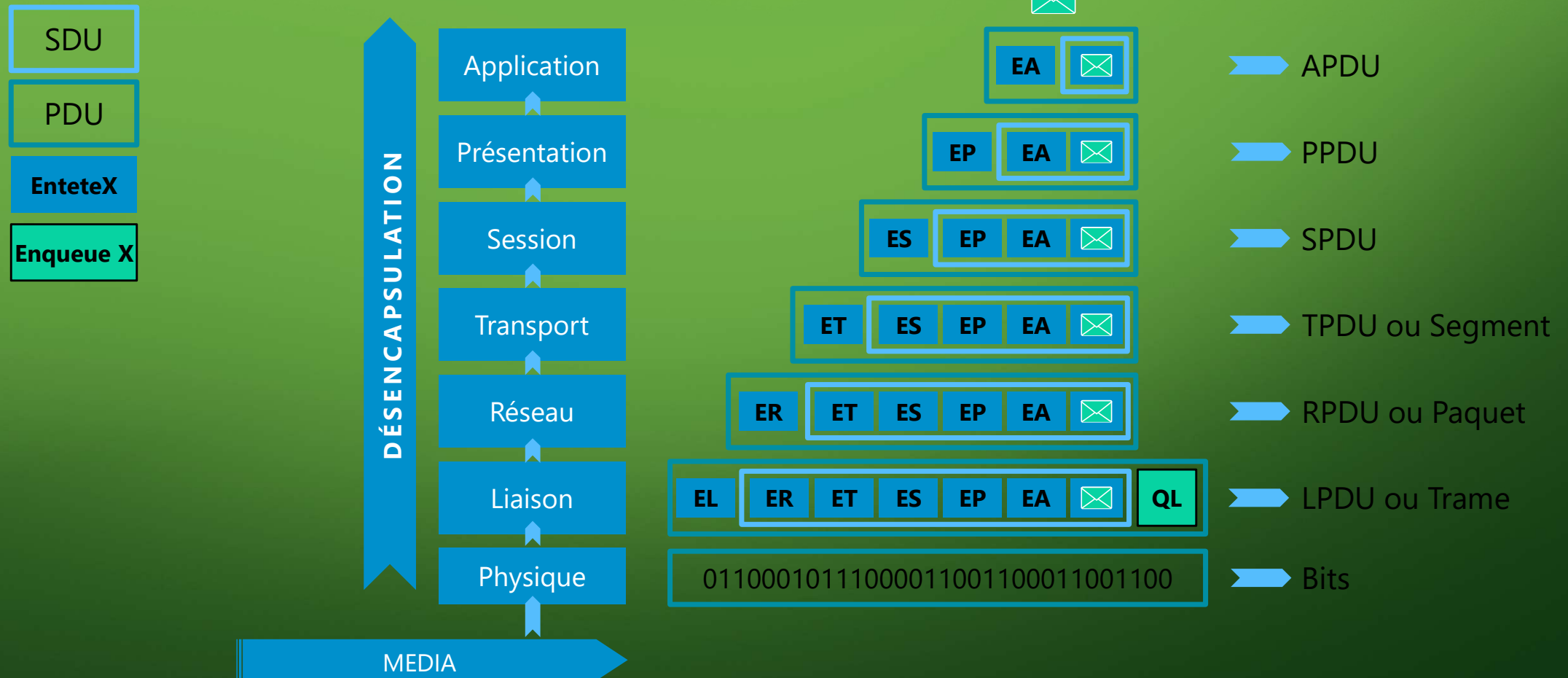
## ENCAPSULATION



# Désencapsulation

# • Comment ça marche ?

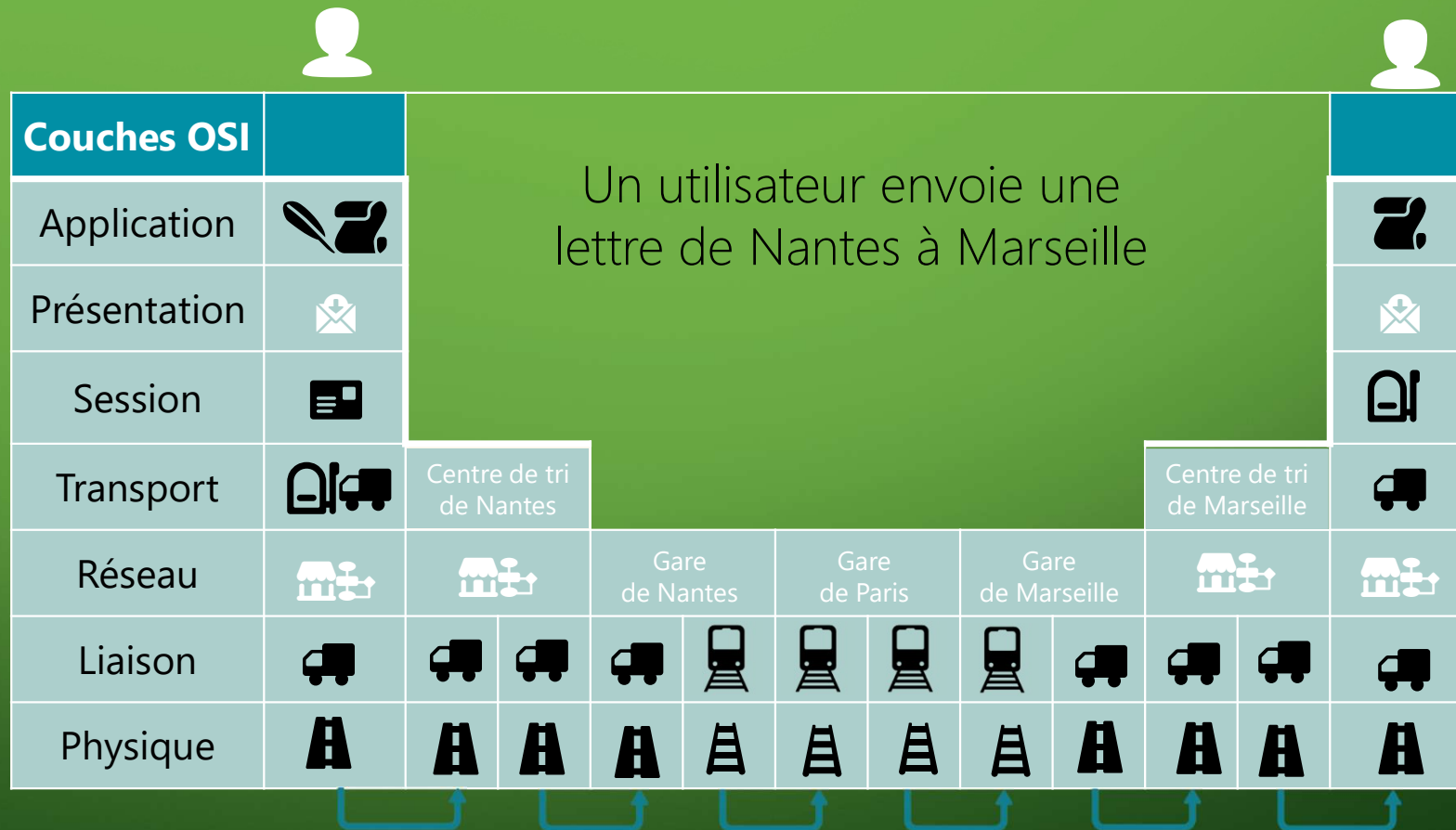
## DÉSENCAPSULATION



# Analogie avec La Poste



- Scénario

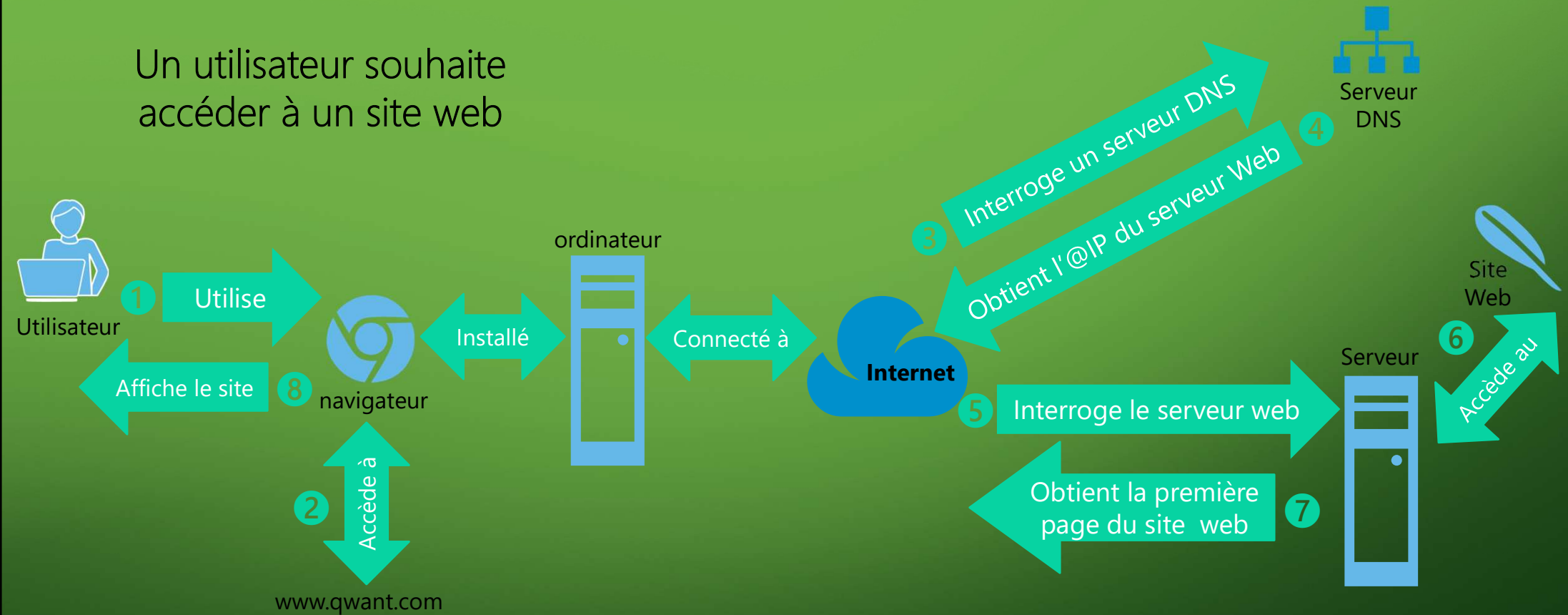


# Modèle OSI et communication

- Exemple de communication

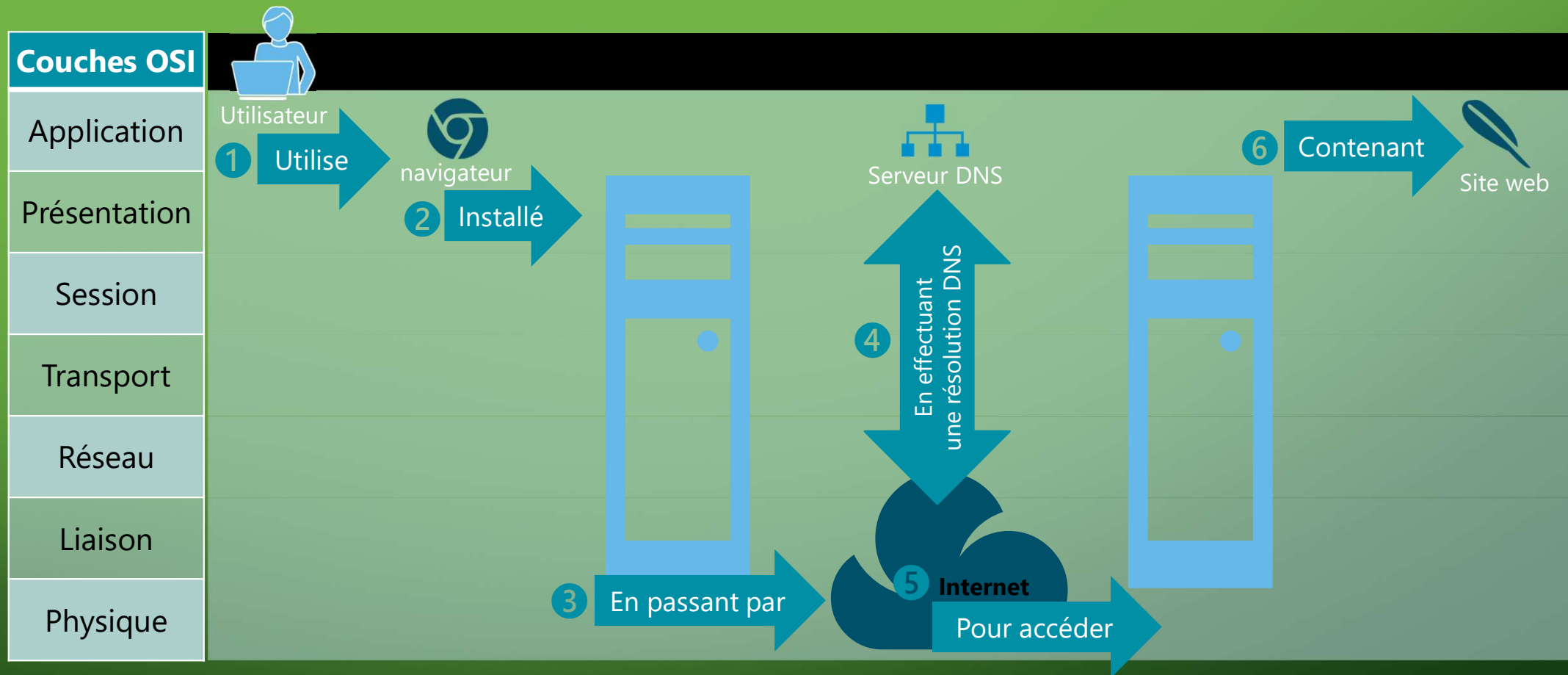
## MODÈLE OSI ET COMMUNICATION

Un utilisateur souhaite accéder à un site web



- Exemple de communication






## MODÈLE OSI ET COMMUNICATION



Un utilisateur souhaite accéder à un site web

## • Exemple de communication

## MODÈLE OSI ET COMMUNICATION

 <b>Utilisateur</b> 		<b>Serveur WEB</b>		 
Couches OSI				
Application	Utilisation du navigateur	 Accès au site web Envoi de la première page du site		Réception de la page web
Présentation	Chiffrement (certificat client) Compression	Comparaison des certificats Déchiffrement Décompression	Chiffrement (certificat client) Compression	Déchiffrement Décompression
Session	Authentification Synchronisation	Authentification Synchronisation	Authentification Synchronisation	Authentification Synchronisation
Transport	Segmentation des données + port du service (TCP:443) + port de réponse (> 1024)	Assemblage des données - port du service (TCP:443) - port de réponse (> 1024)	Segmentation des données + port de réponse (> 1024) + port du service (TCP:443)	Assemblage des données - port de réponse (> 1024) - port du service (TCP:443)
Réseau	+ @IP du serveur Web + @IP du PC local	Lecture et vérification adresse - @IP du serveur Web - @IP du PC distant	+ @IP du PC distant + @IP du serveur Web	Lecture et vérification adresse - @IP du PC - @IP du serveur Web
Liaison	Requête ARP / MAJ Cache ARP + @Mac de la box + @Mac du PC	Lecture et vérification adresse - @Mac du Srv WEB - @Mac de la box	Requête ARP / MAJ Cache ARP + @Mac de la box + @Mac du Srv WEB	Lecture et vérification adresse - @Mac du PC - @Mac de la box
Physique	10100 Conversion des données en Bits 🔌 Envoi des bits sur le média	10100 Conversion des Bits en données 🔌 Reçoit des bits	10100 Conversion des données en Bits 🔌 Envoi des bits sur le média	10100 Conversion des Bits en données 🔌 Reçoit des bits

Accès au site web après résolution DNS

# Les couches du modèle OSI

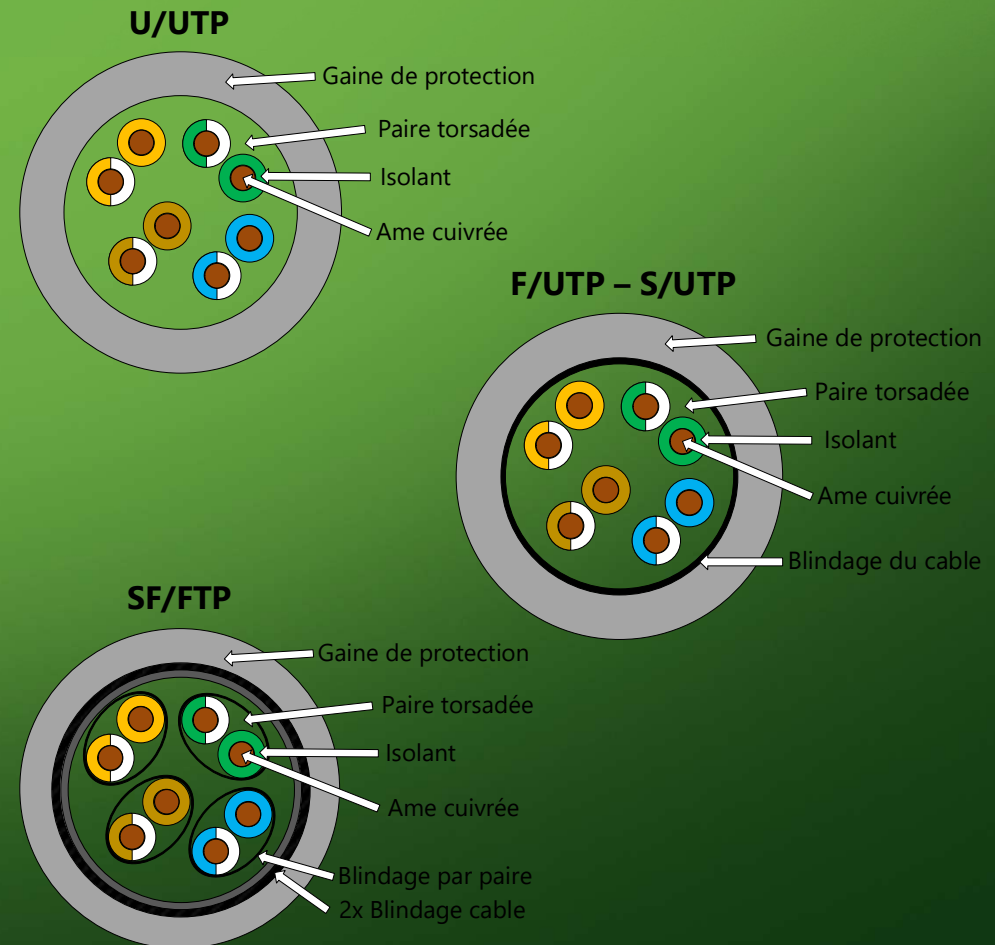
- Connexion physique entre les nœuds réseau
- Connexion garantie par la carte réseau
  - *La carte réseau est présente sur les couches 1 et 2 du modèle OSI*
    - Couche 1 : connectique et modulation de données
    - Couche 2 : adresse physique (adresse MAC)

# LES COUCHES DU MODÈLE OSI

## Couche 1 Physique

### La paire torsadée

ISO 11801	Blindage du câble	Blindage de paire
U/UTP	aucun	aucun
U/FTP	aucun	feuillard
F/UTP	feuillard	aucun
S/UTP	tresse	aucun
SF/UTP	tresse, feuillard	aucun
F/FTP	feuillard	feuillard
S/FTP	tresse	feuillard
SF/FTP	tresse, feuillard	feuillard















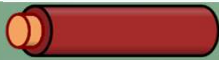



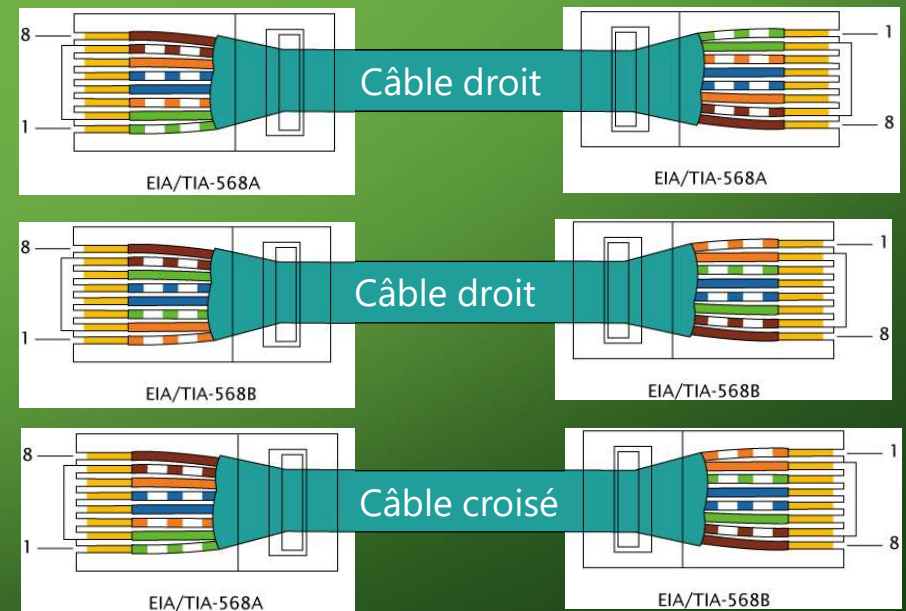


# LES COUCHES DU MODÈLE OSI

## Couche 1 Physique

La paire torsadée

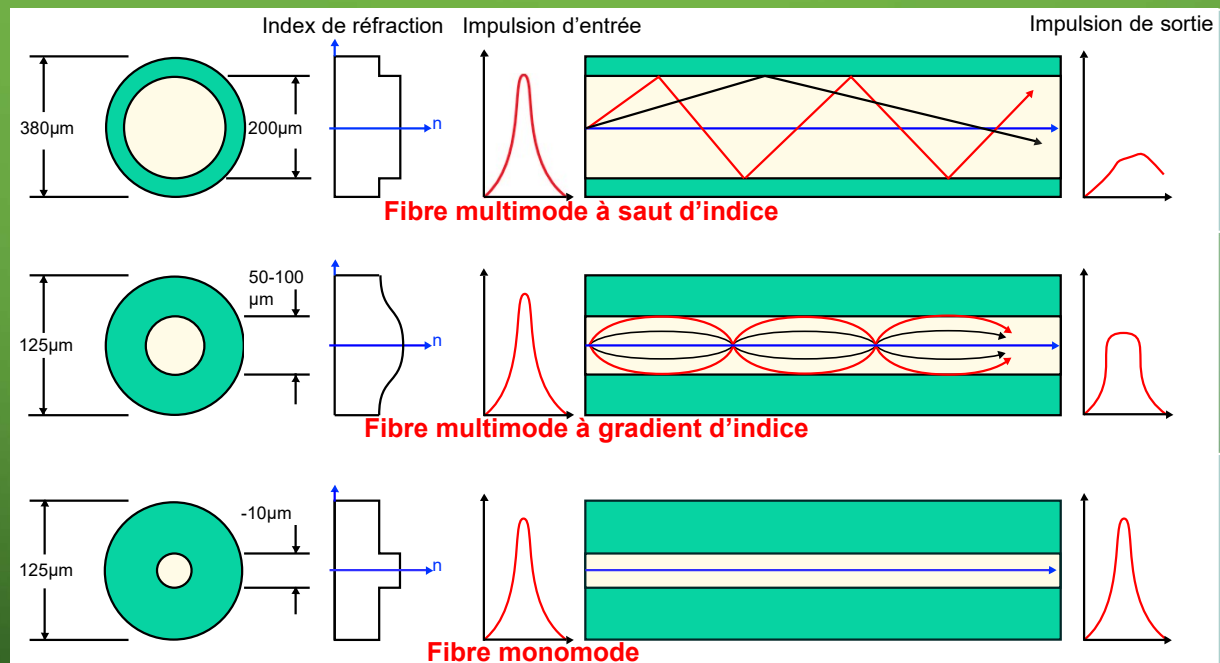
568A			568B
	1	Transmission +	
	2	Transmission -	
	3	Réception +	
	4	N/A	
	5	N/A	
	6	Réception -	
	7	N/A	
	8	N/A	



## LES COUCHES DU MODÈLE OSI

### Couche 1 Physique

#### Fibre optique



- Gigabit
- 200 m maximum
- Émis par D.E.L
- Plusieurs signaux

- Gigabit
- 275 m maximum
- Émis par D.E.L
- Plusieurs signaux

- Gigabit
- 10 km maximum
- Émis par laser
- Un signal

- Les ondes électromagnétiques
  - Ondes à étalement de spectre par saut de fréquence ( FHSS )
    - 802.11 – fréquence 2,4 Ghz à 2,4835 Ghz
    - 79 canaux de 1 Mhz
    - Chaque canal utilisé pendant 400 ms
    - Moins sécurisées que le cable

- Adresse physique d'un nœud réseau
  - *Adresse MAC gérée par OUI (Organizationally Unique Identifier)*
    - *48 bits hexadécimaux (6 octets)*

Adresse MAC											
C0		3E		BA		8F		50		92	
1100	0000	0011	1110	1011	1010	1000	1111	0101	0000	1001	0010
ID_Constructeur						ID_Peripherique					

- Contrôle d'erreurs (CRC control...)
  - *Cyclic Redundancy Check*
  - *Garantir la fiabilité de la trame reçue*

## Les protocoles

- *ARP (Address Resolution Protocol) : résolution de l'adresse MAC à partir de l'adresse logique*
- *DHCP (Dynamic Host Configuration Protocol) : fournit une configuration réseau aux postes clients (bail)*
- *PXE (Pre-boot eXecution Environment) :*
  - *Serveur TFTP (Trivial File Transfer Protocol)*
  - *Serveur DHCP*
  - *Démarrer un poste à partir de sa carte réseau*

## LES COUCHES DU MODÈLE OSI

### Couche 2 Liaison

- Communication du poste A vers poste B avec l'adresse Physique

Envoi de la requête de A vers B		
Adresse MAC		
Destination	Source	
FF:FF:FF:FF:FF:FF	00:11:22:33:44:55	Requête ARP

Réponse à la requête de B vers A		
Adresse MAC		
Destination	Source	
00:11:22:33:44:55	AA:BB:CC:DD:EE:FF	Réponse ARP

- Mise à jour du cache ARP

- Adresse logique d'un nœud réseau
  - *ID\_Réseau + ID\_Hôte*
  - *Unique sur un réseau logique*
- Adresse IP + Masque de sous-réseau = Adresse de réseau logique
  - *Utilisation d'opérateur « & logique »*

## LES COUCHES DU MODÈLE OSI

### Couche 3 Réseau

- Communication du poste A vers poste B (Ping) dans le réseau 1

Envoi de la requête de A vers B				
Adresse MAC		Adresse Logique		
Destination	Source	Destination	Source	
00:1A:2B:3C:4D:5E	00:11:22:33:44:55	@IP: 1B	@IP: 1A	Ping 1B

Envoi de la requête de B vers A				
Adresse MAC		Adresse Logique		
Destination	Source	Destination	Source	
00:11:22:33:44:55	00:1A:2B:3C:4D:5E	@IP: 1A	@IP: 1B	Réponse de 1B



- Ajout des ports
  - *Port de destination (Application à contacter)*
  - *Port local d'écoute (Port local aléatoire ouvert pour la réponse)*
- Deux protocoles
  - *TCP (Transmission Control Protocol) : mode connecté avec accusé de réception*
  - *UDP (User Datagram Protocol) : mode non connecté sans accusé de réception*

## LES COUCHES DU MODÈLE OSI

### Couche 4 Transport

- Communications entre deux postes
  - Un poste joue le rôle de client
  - Un poste joue le rôle de serveur
- Plusieurs communications simultanées pour un poste

Un socket de communication vers le serveur

Un socket de communication pour la réponse

Adresse IP

Adresse IP

Protocole de couche 4

Protocole de couche 4

Port

Port

## LES COUCHES DU MODÈLE OSI

### Couche 4 Transport

- Exemple de communications entre deux postes

Je cherche à contacter le site : 173.194.34.31

173.194.34.31 : TCP : 80



Je suis 80.10.20.30 et j'attends la réponse sur le port 44800

80.10.20.30 : TCP : 44800

└─> Port aléatoire > 1024

TP

# BASE DES RÉSEAUX

02 – LES UNITÉS INFORMATIQUES

## Objectifs

- Connaître le principe de numération
- Effectuer des conversions
- Comprendre les unités informatiques

# La numération

- Les bases de numération

Base 2 (binaire)

Valeurs utilisées	
0	1

Base 8 (octal)

Valeurs utilisées							
0	1	2	3	4	5	6	7

Base 10 (décimal)

Valeurs utilisées									
0	1	2	3	4	5	6	7	8	9

Base 16 (hexadécimal)

Valeurs utilisées															
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F



- Principe de numération décimale

# LA NUMÉRATION

## Base 10

0	0
0	1
0	2
0	3
0	4
0	5
0	6
0	7
0	8
0	9

Valeurs possibles

Reprise des valeurs

Combinaison avec la valeur suivante

1	0
1	1
1	2
1	3
1	4
1	5
1	6
1	7
1	8
1	9

Reprise des valeurs

Combinaison avec la valeur suivante

2	0
2	1
2	2
2	3
2	4
2	5
2	6
2	7
2	8
2	9

Reprise des valeurs

Combinaison avec la valeur suivante

3	0
3	1
3	2
3	3
3	4
3	5
3	6
3	7
3	8
3	9

- Principe de numération binaire



- Principe de numération octale

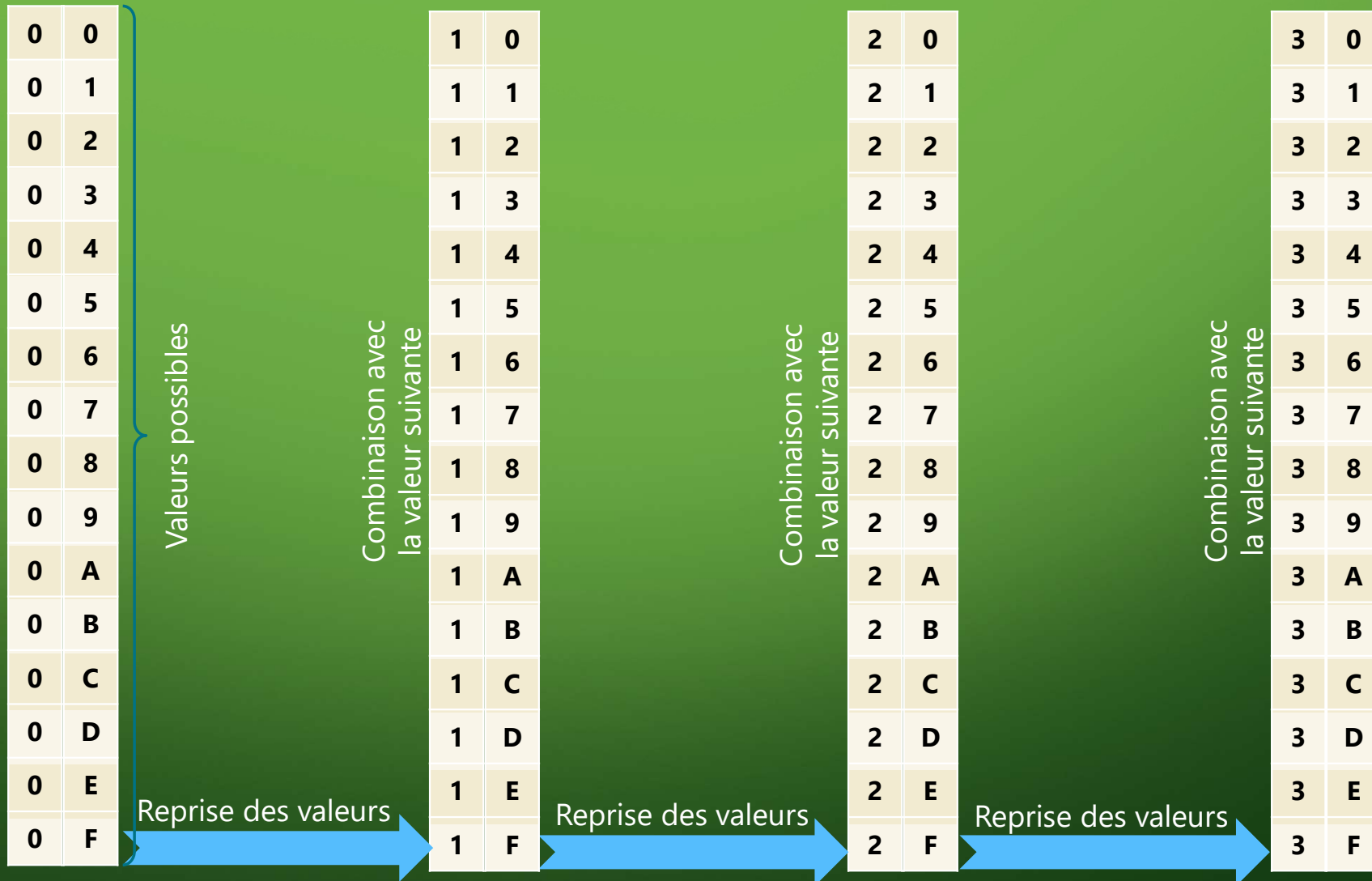
## LA NUMÉRATION



## Base 16

### • Principe de numération hexadécimale

## LA NUMÉRATION



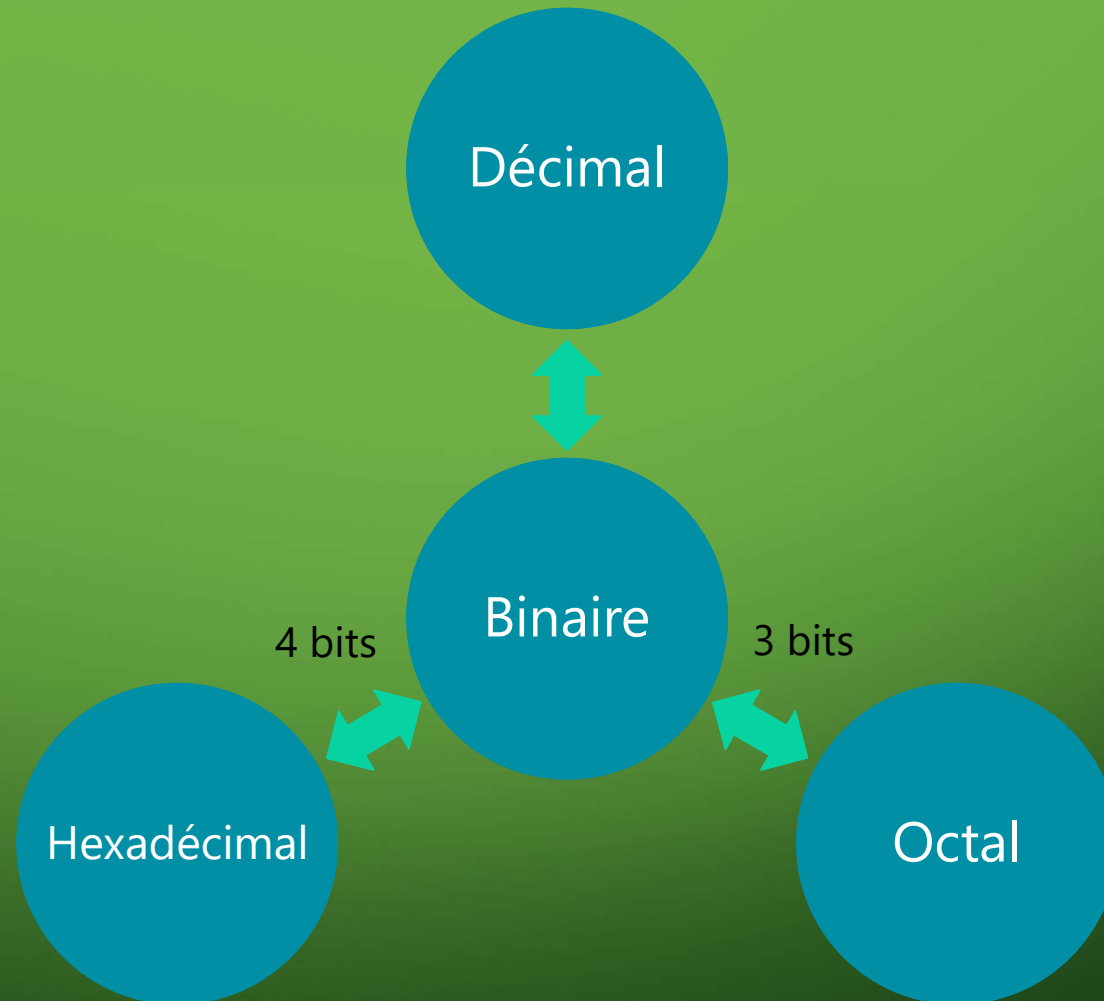
- Quelques équivalence des valeurs

Base 2	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111	10000	10001
Base 8	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17	20	21
Base 10	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Base 16	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11

# La conversion

- Introduction

## LA CONVERSION



- ## LA CONVERSION

			1 octet												
	$2^{10}$	$2^9$	$2^8$	$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$				
	1024	512	256	128	64	32	16	8	4	2	1				
$(10\ 0111\ 0110)_2$		1	0	0	1	1	1	0	1	1	0				
		512	+		64	+	32	+	16	+	4	+	2	=	630
	$(10\ 0111\ 0110)_2$					=	$(630)_{10}$								
$(101\ 0111)_2$				0	1	0	1	0	1	1	1				
					64	+	16	+	4	+	2	+	1	=	87
	$(101\ 0111)_2$					=	$(87)_{10}$								



- La conversion octale/décimale

En passant par le binaire

	<b>(2631)<sub>8</sub></b>			
<b>Séparation</b>	<b>2</b>	<b>6</b>	<b>3</b>	<b>1</b>
<b>Conversion binaire</b>	<b>10</b>	<b>110</b>	<b>11</b>	<b>1</b>
<b>Ecriture (3 bits)</b>	<b>010</b>	<b>110</b>	<b>011</b>	<b>001</b>
<b>Regroupement</b>	<b>0101 1001 1001</b>			
<b>Conversion décimale</b>	<b>(1433)<sub>10</sub></b>			

- La conversion hexadécimale/décimale

## LA CONVERSION

En passant par le binaire

	<b>(C1A6)<sub>16</sub></b>			
<b>Séparation</b>	<b>C</b>	<b>1</b>	<b>A</b>	<b>6</b>
<b>Conversion binaire</b>	<b>1100</b>	<b>1</b>	<b>1010</b>	<b>110</b>
<b>Ecriture (4bits)</b>	<b>1100</b>	<b>0001</b>	<b>1010</b>	<b>0110</b>
<b>Regroupement</b>	<b>1100 0001 1010 0110</b>			
<b>Conversion décimale</b>	<b>(49 574)<sub>10</sub></b>			

- La conversion décimale/hexadécimale

## LA CONVERSION

En passant par le binaire

	<b>(51966)<sub>10</sub></b>			
<b>Conversion binaire</b>	<b>1100 1010 1111 1110</b>			
<b>Regroupement (4bits)</b>	<b>1100</b>	<b>1010</b>	<b>1111</b>	<b>1110</b>
<b>Conversion décimale</b>	<b>12</b>	<b>10</b>	<b>15</b>	<b>14</b>
<b>Conversion hexadécimale</b>	<b>C</b>	<b>A</b>	<b>F</b>	<b>E</b>
	<b>(CAFE)<sub>16</sub></b>			

# Comprendre les unités informatiques

- Les différentes unités informatiques

## COMPRENDRE LES UNITÉS INFORMATIQUES

### Unité de base

#### Le bit (**B**inary **Dig**it)

- Valeurs possibles **0** et **1**
- Symbole : **b**

#### Les multiples du bit

- Le Kibibit (Kibit)
- Le Mebibit (Mibit)
- Le Gibibit (Gibit)
- Le Tebibit (Tibit)

#### L'octet ou Byte (anglais)

- Ensemble de 8 bits
- Symbole octet : **o**
- Symbole Byte : **B**

#### Les multiples de l'octet (10)

- Le Kiloctet (ko)
- Le Mégaoctet (Mo)
- Le Gigaoctet (Go)
- Le Téraoctet (To)

- Les préfixes

## COMPRENDRE LES UNITÉS INFORMATIQUES

Préfixes binaires (bits)			
Nom	Symbole	Nbre de bits	
Kibibit	Kibit	$2^{10}$	1024 bits
Mebibit	Mibit	$2^{20}$	1024 Kibit
Gibibit	Gibit	$2^{30}$	1024 Mibit
Tebibit	Tibit	$2^{40}$	1024 Gibit
Pebibit	Pibit	$2^{50}$	1024 Tibit
Exbibit	Eibit	$2^{60}$	1024 Pibit
Zebibit	Zibit	$2^{70}$	1024 Eibit
Yobibit	Yibit	$2^{80}$	1024 Zibit

Préfixes binaires (usage informatique)			
Nom	Symbole	Nbre d'octets	
Kibiocet	Kio	$2^{10}$	1024 o
Mebiocet	Mio	$2^{20}$	1024 Kio
Gibiocet	Gio	$2^{30}$	1024 Mio
Tébiocet	Tio	$2^{40}$	1024 Gio
Pébiocet	Pio	$2^{50}$	1024 Tio
Exbiocet	Eio	$2^{60}$	1024 Pio
Zébiocet	Zio	$2^{70}$	1024 Eio
Yobiocet	Yio	$2^{80}$	1024 Zio

TP

# BASE DES RÉSEAUX

## 03 – L'ADRESSAGE IPV4



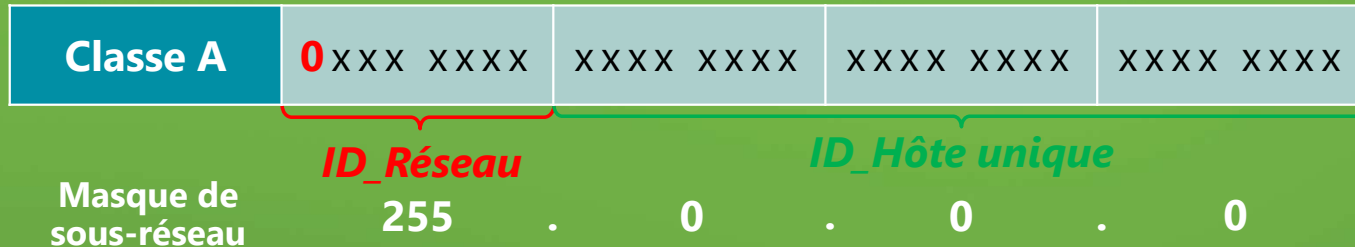
## Objectifs

- Connaître l'adressage IPv4
- Identifier les classes IPv4
- Calculer les différentes adresses
- Appréhender l'utilisation de la notation CIDR
- Calculer les adresses de sous-réseaux

# Présentation de l'adressage IPv4

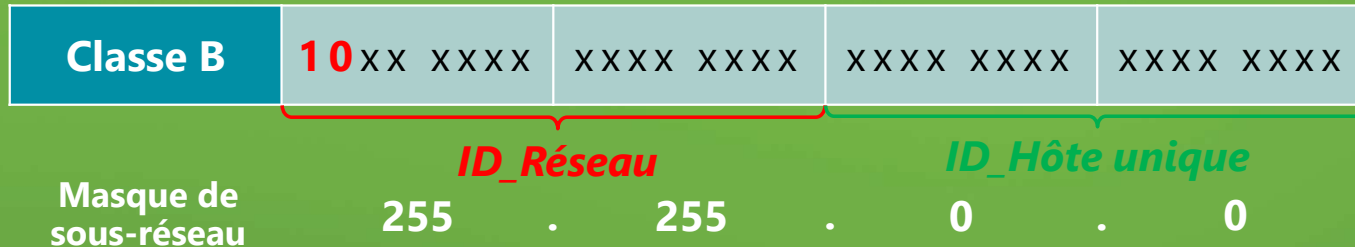
- Une adresse IPv4 est constituée de 32 bits découpés en 4 octets distincts.
- Une adresse IPv4 est composée :
  - *d'un identifiant réseau (**ID\_Réseau**)*
  - *d'un identifiant d'hôte unique sur le réseau logique (**ID\_Hôtes**)*
- Pour communiquer avec d'autres hôtes sur son réseau logique, un hôte réseau a besoin :
  - *d'une adresse IP*
  - *d'un masque de sous-réseau.*
- À partir de son adresse IP et son masque de sous-réseau, l'hôte réseau va calculer :
  - *son adresse de réseau logique*
  - *son adresse de diffusion*

# Les classes



	2 <sup>7</sup> 128	2 <sup>6</sup> 64	2 <sup>5</sup> 32	2 <sup>4</sup> 16	2 <sup>3</sup> 8	2 <sup>2</sup> 4	2 <sup>1</sup> 2	2 <sup>0</sup> 1
<b>0</b>	<b>0</b>	0	0	0	0	0	0	0
<b>127</b>	<b>0</b>	1	1	1	1	1	1	1

- Réseau de classe A , l'ID\_Réseau est compris entre :
  - Classe entière : **0** et **127**
  - Classe utilisable : **1** et **126**
- Nombre d'hôtes, l'ID\_Hôte unique contient :
  - Nbre bits @IP – Nbre bits ID\_Réseau
  - $32 - 8 = 24$
  - $2^{24} - 2 = 16\ 777\ 214$  hôtes possibles



	2 <sup>7</sup> 128	2 <sup>6</sup> 64	2 <sup>5</sup> 32	2 <sup>4</sup> 16	2 <sup>3</sup> 8	2 <sup>2</sup> 4	2 <sup>1</sup> 2	2 <sup>0</sup> 1
128	1	0	0	0	0	0	0	0
191	1	0	1	1	1	1	1	1

- Réseau de classe B , l'*ID\_Réseau* est compris entre :
  - Classe entière et utilisable : **128 et 191**
- Nombre d'hôtes, l'*ID\_Hôte unique* contient :
  - Nbre bits @IP – Nbre bits *ID\_Réseau*
  - $32 - 16 = 16$
  - $2^{16} - 2 = 65\ 534$  hôtes possibles



- Réseau de classe C , l'*ID\_Réseau* est compris entre :
  - Classe entière et utilisable : **192** et **223**

	2 <sup>7</sup> 128	2 <sup>6</sup> 64	2 <sup>5</sup> 32	2 <sup>4</sup> 16	2 <sup>3</sup> 8	2 <sup>2</sup> 4	2 <sup>1</sup> 2	2 <sup>0</sup> 1
<b>192</b>	1	1	0	0	0	0	0	0
<b>223</b>	1	1	0	1	1	1	1	1

- Nombre d'hôtes, l'*ID\_Hôte unique* contient :
  - Nbre bits @IP – Nbre bits *ID\_Réseau*
  - $32 - 24 = 8$
  - $2^8 - 2 = 254$  hôtes possibles

## LES CLASSES

Classe D	1110	xxxx	xxxx	xxxx	xxxx	xxxx
----------	------	------	------	------	------	------

*ID\_Réseau*

Masque de sous-réseau      240 . 0 . 0 . 0

	2 <sup>7</sup> 128	2 <sup>6</sup> 64	2 <sup>5</sup> 32	2 <sup>4</sup> 16	2 <sup>3</sup> 8	2 <sup>2</sup> 4	2 <sup>1</sup> 2	2 <sup>0</sup> 1
224	1	1	1	0	0	0	0	0
239	1	1	1	0	1	1	1	1

- Réseau de classe D , l'*ID\_Réseau* est compris entre :
  - Classe entière et utilisable : **224** et **239**
- Nombre d'hôtes, la classe D ne contient pas d'hôtes



## LES CLASSES

						Valeurs 1 <sup>ier</sup> octet	Nbre d'hôtes
Unicast	Classe A	0xxx xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	1 - 126	$2^{24} - 2 = 16\,777\,214$
	Masque sous-réseau	255	0	0	0		
	Classe B	10xx xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	128 - 191	$2^{16} - 2 = 65\,534$
	Masque sous-réseau	255	255	0	0		
	Classe C	110x xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	192 - 223	$2^8 - 2 = 254$
	Masque sous-réseau	255	255	255	0		
Multicast	Classe D	1110 xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	224 - 239	0
	Masque sous-réseau	240	0	0	0		

TP

# Calcul des adresses

## CALCUL DES ADRESSES

### Calcul de l'adresse réseau

- L'adresse de réseau logique est une sorte d'identifiant commun
- La fonction **&logique** permet de calculer l'adresse de réseau logique

#### Configuration IP d'un hôte

- @IP : 192.168.76.150
- Masque : 255.255.255.0

Table de vérité de la fonction & logique

a	b	a.b
0	0	0
0	1	0
1	0	0
1	1	1

Octet 1	Octet 2	Octet 3	Octet 4	Octet 1	Octet 2	Octet 3	Octet 4
192	168	76	150	1100 0000	1010 1000	0100 1100	1001 0110
255	255	255	0	1111 1111	1111 1111	1111 1111	0000 0000
192	168	76	0	1100 0000	1010 1000	0100 1100	0000 0000

L'@IP **192.168.76.150** avec le masque **255.255.255.0**  
appartient donc au réseau logique **192.168.76.0**

## CALCUL DES ADRESSES

### Calcul de l'adresse réseau

Un hôte

- @IP : 192.168.76.150
- Masque : 255.255.255.0

Octet 1	Octet 2	Octet 3	Octet 4	Octet 1	Octet 2	Octet 3	Octet 4
192	168	76	150	1100 0000	1010 1000	0100 1100	1001 0110
255	255	255	0	1111 1111	1111 1111	1111 1111	0000 0000
192	168	76	0	1100 0000	1010 1000	0100 1100	0000 0000

- Identifier, les deux parties ( **ID\_Réseau** & **ID\_Hôtes** ) en fonction du masque de sous-réseau
- Passer toutes les valeurs de l'**ID\_Hôtes** à 0 pour obtenir l'**adresse de réseau**

L'@IP **192.168.76.150** avec le masque **255.255.255.0**  
provient du réseau logique **192.168.76.0**

## CALCUL DES ADRESSES

### Calcul de l'adresse de diffusion (broadcast)

#### Un hôte

- @IP : 192.168.76.150
- Masque : 255.255.255.0

Octet 1	Octet 2	Octet 3	Octet 4	Octet 1	Octet 2	Octet 3	Octet 4
192	168	76	150	1100 0000	1010 1000	0100 1100	1001 0110
255	255	255	0	1111 1111	1111 1111	1111 1111	0000 0000
192	168	76	255	1100 0000	1010 1000	0100 1100	1111 1111

- Identifier, les deux parties ( **ID\_Réseau** & **ID\_Hôtes** ) en fonction du masque de sous-réseau
- Passer toutes les valeurs de l'**ID\_Hôtes** à 1 pour obtenir l'adresse de diffusion

L'@IP **192.168.76.150** avec le masque **255.255.255.0**  
a pour adresse de broadcast **192.168.76.255**

## CALCUL DES ADRESSES

### Calcul du nombre d'hôtes

#### Un hôte

- @IP : 192.168.76.150
- Masque : 255.255.255.0

Octet 1	Octet 2	Octet 3	Octet 4	Octet 1	Octet 2	Octet 3	Octet 4
192	168	76	150	1100 0000	1010 1000	0100 1100	1001 0110
255	255	255	0	1111 1111	1111 1111	1111 1111	0000 0000

- Identifier, les deux parties ( **ID\_Réseau** & **ID\_Hôtes** ) en fonction du masque de sous-réseau
- Prendre le nombre de bits de l'**ID\_Hôtes**, pour l'exemple **8 bits**
- Utiliser la formule :  $2^{\text{bits\_ID\_Hôte}} - 2$  (les adresses de réseau et de diffusion)


$$2^8 - 2 = 254 \text{ hôtes possibles}$$

- **Obtenir l'adresse de réseau** : passer tous les **bits** de l'**ID\_Hôtes** à 0
- **Obtenir l'adresse de diffusion** : passer tous les **bits** de l'**ID\_Hôtes** à 1
- **Obtenir le masque de sous-réseau** : passer tous les **bits** de l'**ID\_Réseau** à 1
- **Obtenir le nombre d'hôtes** : prendre le **nombre de bits (n)** de l'**ID\_Hôtes**

Utiliser la formule : **Nbre d'hôtes** =  $2^n - 2$



TP

# La notation CIDR

## LA NOTATION CIDR

### Présentation

- La notation CIDR (Classless Inter Domain Routing) publiée en septembre 1993 (RFC 1518 et 1519)
- Suppression du fonctionnement par classes car :
  - *devenu obsolète,*
  - *trop restrictif,*
  - *peu évolutif*
- Suppression du masque de sous-réseau, remplacer par le préfixe
- Le préfixe représente le nombre de bits de l'**ID\_Réseau**

**Classe A : 255.0.0.0**  **devient /8**

**Classe C : 255.255.255.0**  **devient /24**

**Classe B : 255.255.0.0**  **devient /16**

**Classe D : 240.0.0.0**  **devient /4**

- Calcul du préfixe en fonction du masque de sous-réseau

LA NOTATION CIDR

@IP : 192.168.150.68  
Masque : 255.255.248.0

Masque de sous-réseau :  
255.255.248.0

- ➡ Convertir les octets en binaire
- ➡ Additionner le nombre de bits à « 1 »
- ➡ ce qui représente l'**ID\_Réseau** donc le préfixe

	Octet 1	Octet 2	Octet 3	Octet 4
255.255.248.0	1111 1111	1111 1111	1111 1000	0000 0000
Nbre de bits	8	8	5	0
Le masque 255.255.248.0 devient /21 en notation CIDR				

- Calcul du masque de sous-réseau en fonction du préfixe

LA NOTATION CIDR

@IP : 192.168.150.68 /20

Préfixe : /20

- Dans un tableau représentant une adresse IP découpée en octets
- Mettez **1** dans les **20** premiers bits (**ID\_Réseau**)
- Mettez **0** dans les **12** bits suivants (**ID\_Hôtes**)
- Convertissez chaque octet **en décimale** (**Masque de sous-réseau**)

	Octet 1	Octet 2	Octet 3	Octet 4
/ 20	1111 1111	1111 1111	1111 0000	0000 0000
Masque de sous réseau	255	255	240	0
Le préfixe /20 devient le masque 255.255.240.0				

TP

# Les adresses privées

- Les adresses privées ont été définies en février 1996.
- Elles sont utilisables seulement dans les réseaux locaux privés.
- Elles ne sont pas routables sur Internet.



- Classe A

	Plage d'adresses globale	Plage d'adresses utilisable	Masque sous-réseau	Notation CIDR
Privée de Classe A	<b>10.0.0.0 10.255.255.255</b>	<b>10.0.0.1 10.255.255.254</b>	<b>255.0.0.0</b>	<b>10.0.0.0 /8</b>

- Classe B

	Plage d'adresses globale	Plage d'adresses utilisable	Masque sous-réseau	Notation CIDR
Privée de Classe B	<b>172.16.0.0</b> <b>172.31.255.255</b>	<b>172.16.0.1</b> <b>172.31.255.254</b>	<b>255.240.0.0</b>	<b>172.16.0.0 /12</b>

- Classe C

	Plage d'adresses globale	Plage d'adresses utilisable	Masque sous-réseau	Notation CIDR
Privée de Classe C	<b>192.168.0.0</b> <b>192.168.255.255</b>	<b>192.168.0.1</b> <b>192.168.255.254</b>	<b>255.255.0.0</b>	<b>192.168.0.0 /16</b>

## LES ADRESSES PRIVÉES

### Résumé

Définies en  
février 1996

	Plage d'adresses globale	Plage d'adresses utilisable	Masque sous-réseau	Notation CIDR
Privée de Classe A	<b>10.0.0.0</b> <b>10.255.255.255</b>	<b>10.0.0.1</b> <b>10.255.255.254</b>	<b>255.0.0.0</b>	<b>10.0.0.0 /8</b>
Privée de Classe B	<b>172.16.0.0</b> <b>172.31.255.255</b>	<b>172.16.0.1</b> <b>172.31.255.254</b>	<b>255.240.0.0</b>	<b>172.16.0.0 /12</b>
Privée de Classe C	<b>192.168.0.0</b> <b>192.168.255.255</b>	<b>192.168.0.1</b> <b>192.168.255.254</b>	<b>255.255.0.0</b>	<b>192.168.0.0 /16</b>

# Les adresses APIPA

- Les adresses d'autoconfiguration ont été définies en mai 2005
- APIPA : Automatic Private Internet Protocol Addressing
  - *Adressage Privé IP Automatique*
- Adresse de réseau logique : **169.254.0.0 /16**
- Caractéristiques de ses adresses
  - *Pas routables sur Internet*
  - *Pas distribuables par un serveur DHCP*
  - *Pas déclarées dans un serveur DNS*

# Les sous-réseaux

## La création de sous-réseaux (RFC 1878)

- **La création de sous-réseaux :**
  - *Permettre de limiter l'impact des diffusions ARP*
  - *Équilibrer le trafic réseau*
  - *Isoler des machines*
  - *Mettre en place un peu de sécurité*
  - *Optimiser l'utilisation des adresses IP*
- Nouvelle partie dans l'adresse IP :
  - **ID\_Réseau**
  - **ID\_ss-réseau** (créé à partir de bits issus de l'**ID\_Hôtes**)
  - **ID\_Hôtes**



# Calculs des sous-réseaux

• Exemple 1 : calcul du nombre de bits ID<sub>ss-réseau</sub>

CALCUL DES SOUS-RÉSEAUX

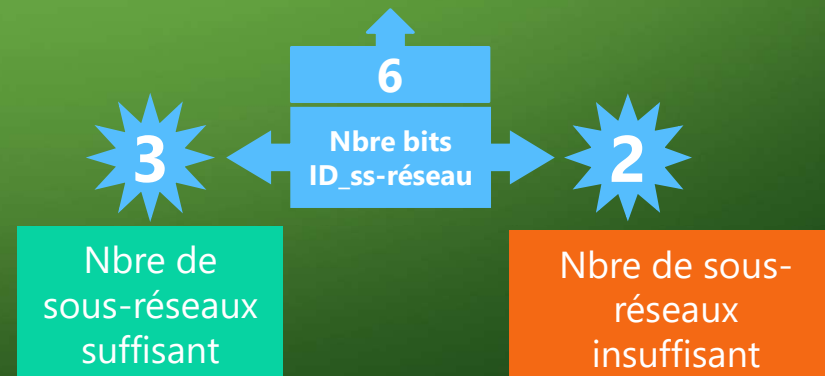
@ du réseau : 192.168.0.0 /16  
Découpage du réseau en 6 SR

Nombre de bits de l'**ID<sub>ss-réseau</sub>**

- Nbre ss-réseau  $\leq 2^n$
- $n$  représente le nbre de bits

Tableau binaire										
2 <sup>10</sup>	2 <sup>9</sup>	2 <sup>8</sup>	2 <sup>7</sup>	2 <sup>6</sup>	2 <sup>5</sup>	2 <sup>4</sup>	2 <sup>3</sup>	2 <sup>2</sup>	2 <sup>1</sup>	2 <sup>0</sup>
1024	512	256	128	64	32	16	8	4	2	1

L'**ID<sub>ss-réseau</sub>** est  
composé de **3 bits** pris  
sur l'**ID<sub>Hôte</sub>**



## CALCUL DES SOUS-RÉSEAUX

@ du réseau : 192.168.0.0 /16  
Découpage du réseau en 6 SR

Decoupage du reseau en 6 SR

Octet 1 = 192								Octet 2 = 168								Octet 3 = 0								Octet 4 = 0								
128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	
1	1	0	0	0	0	0	0	1	0	1	0	1	0			0	0	0														
192								168								SR0				0	0	0										
																SR1				0	0	1										
																SR2				0	1	0										
																SR3				0	1	1										
																SR4				1	0	0										
																SR5				1	0	1										
																SR6				1	1	0										
																SR7				1	1	1										

ID\_Réseau

+ ID\_ss-réseau =

Nouveau masque (/19)

**ID\_ss-réseau**

ID\_Hôtes

TP

*M03-04-TP-Sous-réseaux*

*M03-05-TP-Packet-Tracer\_Adressage\_IPv4*

# BASE DES RÉSEAUX

04 – LA COMMUNICATION

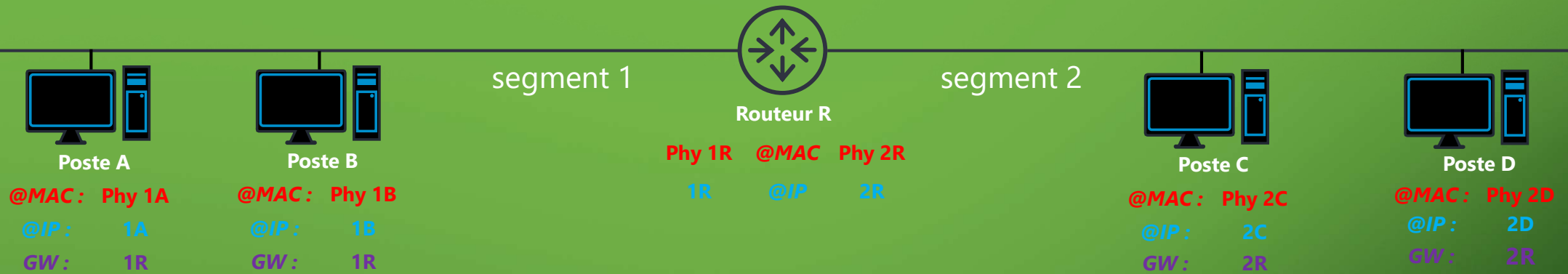
## Objectifs

- Expliquer la communication entre ordinateurs
- Présenter le routage
- Calculer des adresses de sur-réseaux

# La théorie

# • Communication entre deux PC

LA THÉORIE



Si ping de A vers B

ping 1A vers 1B  
Réseau identique



Envoi de la requête Ping

Si ping de A vers D

ping 1A vers 2D  
Réseau différent



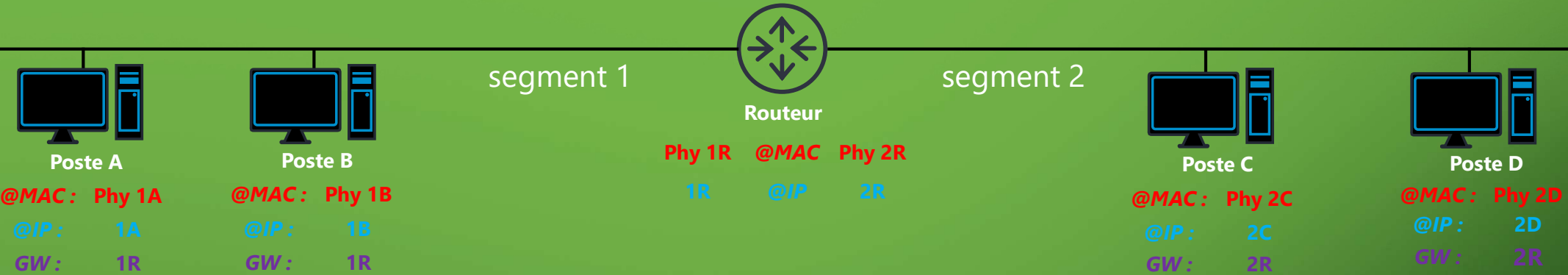
Pas d'envoi de la requête Ping

**Pour accéder à un segment différent, il faut paramétrer la passerelle par défaut**



• Communication entre deux PC (ping)

LA THÉORIE



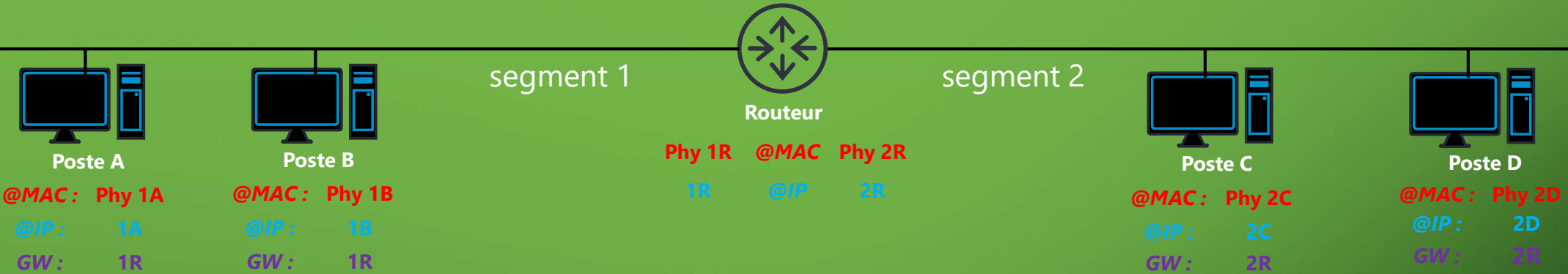
Recherche de l'adresse de physique de R				
Adresse physique		Adresse logique		
Destinataire	Source	Destinataire	Source	
FF:FF:FF:FF:FF:FF	Phy1A	1R	1A	Requête ARP

Envoi de la trame Ping au routeur				
Phy1R	Phy1A	2D	1A	Ping D

Réponse du routeur				
Phy1A	Phy1R	1A	1R	Réponse ARP

• Communication entre deux PC (ping)

LA THÉORIE



Recherche de l'adresse de physique de D				
Adresse physique		Adresse logique		
Destinataire	Source	Destinataire	Source	
FF:FF:FF:FF:FF:FF	Phy2R	2D	2R	Requête ARP

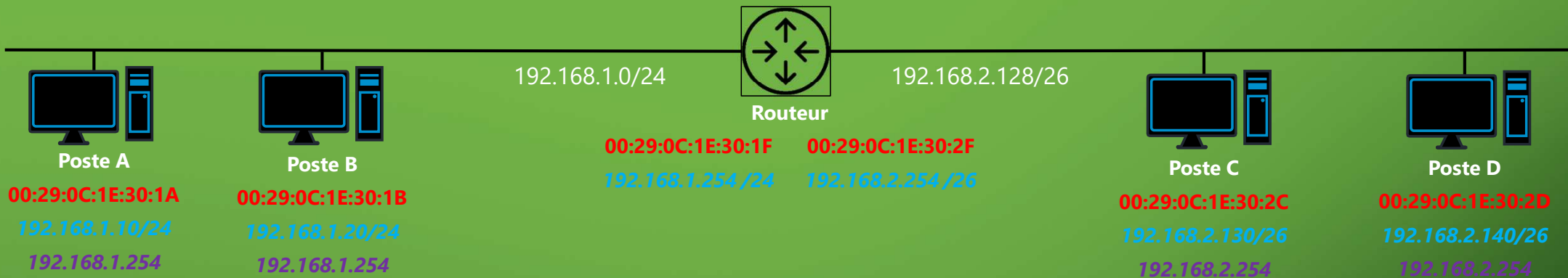
Envoi de la trame Ping au routeur				
Phy2D	Phy2R	2D	1A	Ping D

Réponse du poste D				
Phy2R	Phy2D	2R	2D	Réponse ARP

# La pratique

- Communication entre deux noeuds (ping)

LA PRATIQUE



Faire un ping du poste A vers le poste B

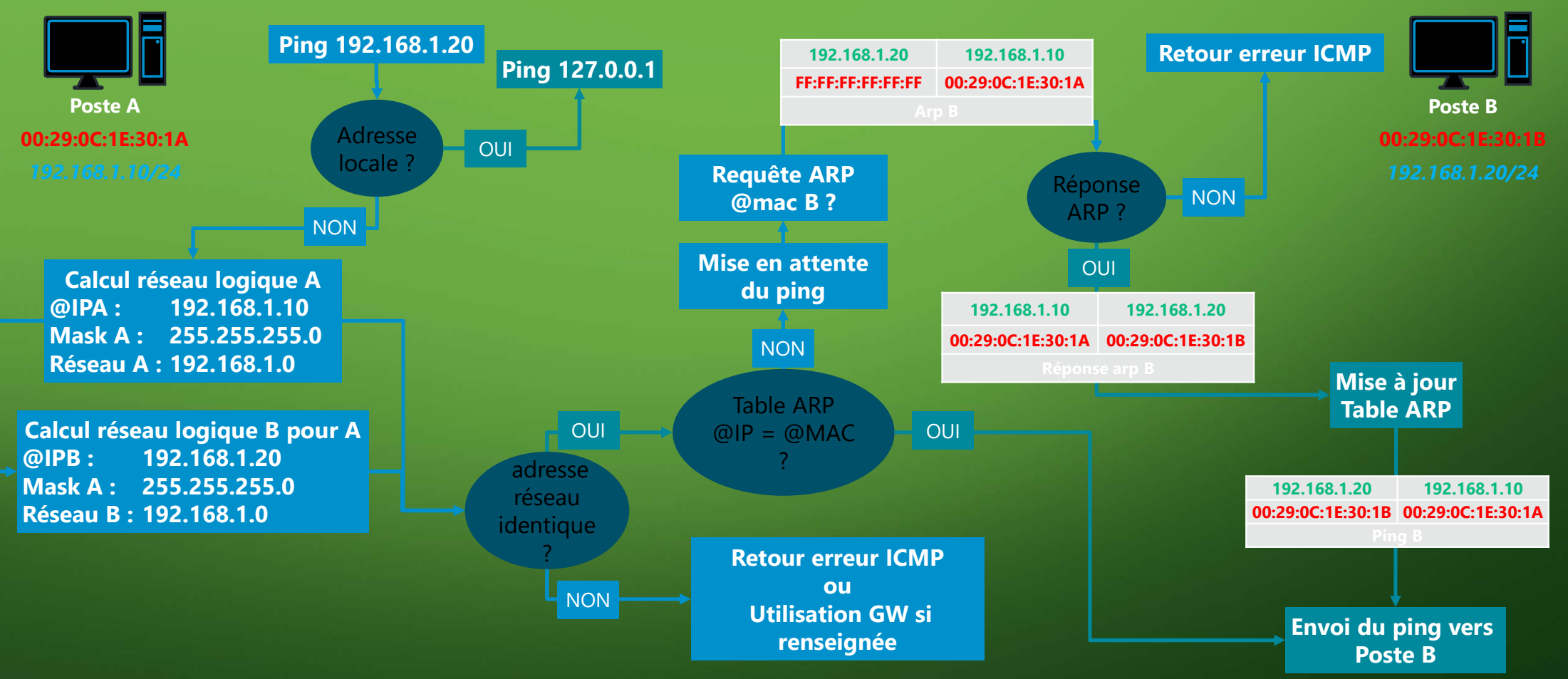
Faire un ping de 192.168.1.10/24 vers 192.168.1.20



C:\> ping 192.168.1.20

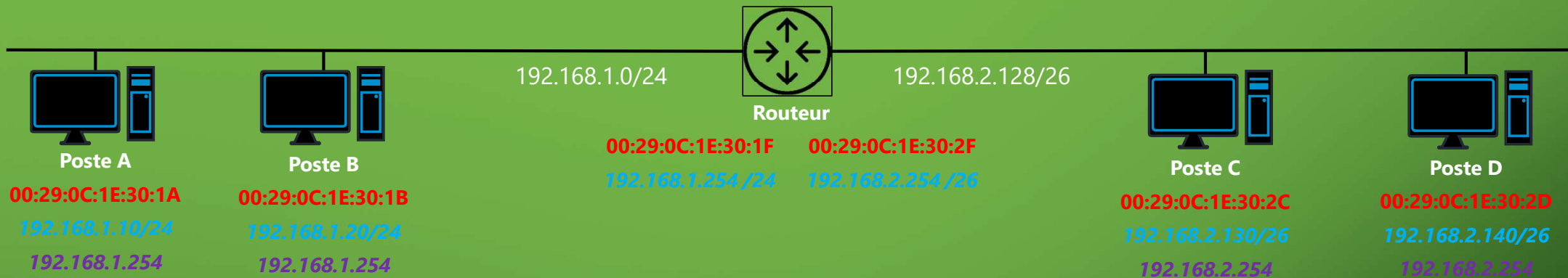
# • Communication entre deux PC

LA PRATIQUE



- Communication entre deux noeuds (ping)

LA PRATIQUE



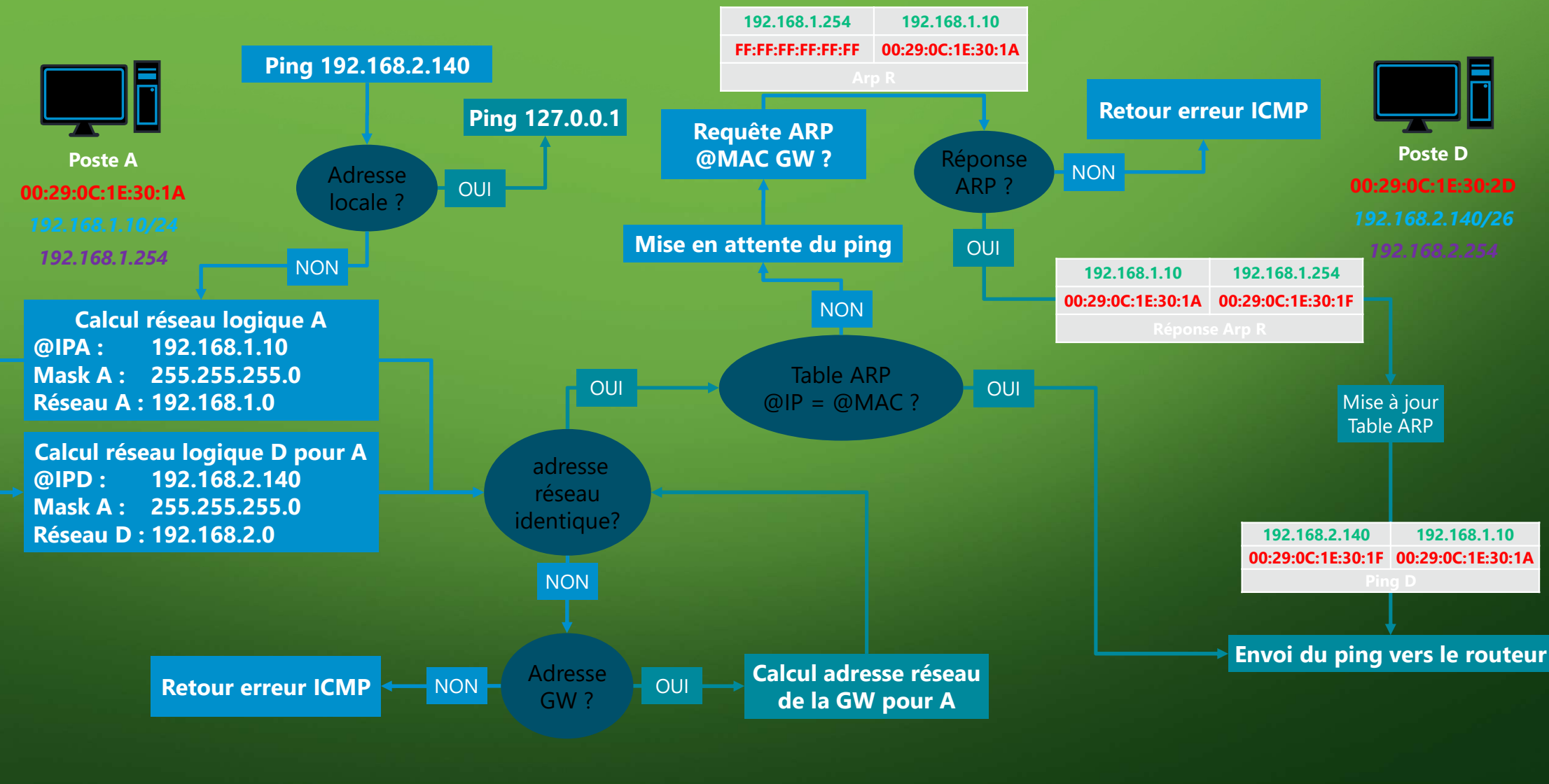
Faire un ping du poste A vers le poste D

Faire un ping de 192.168.1.10/24 vers 192.168.2.140

C:\> ping 192.168.2.140

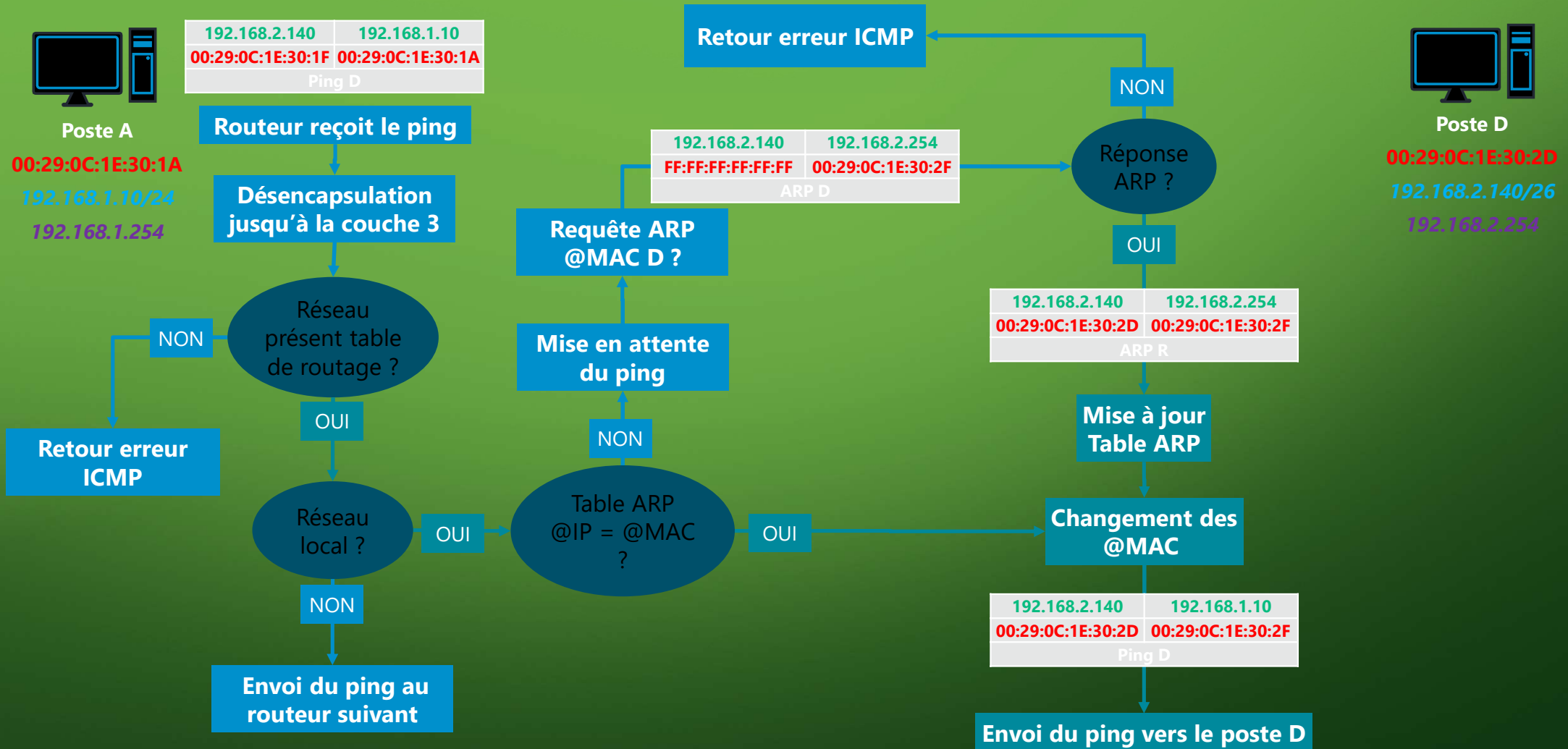
# • Communication entre deux PC

LA PRATIQUE



# • Communication entre deux PC

LA PRATIQUE

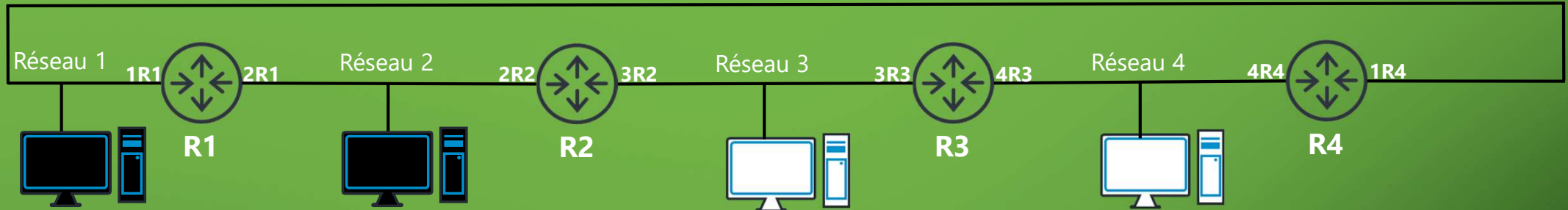




# Le routage

- La couche réseau

# LE ROUTAGE



Routeur R1		
R	P	M
1	1R1	1
2	2R1	1
3	2R2	2
4	2R2	3
3	1R4	3
4	1R4	2

Routeur R2		
R	P	M
2	2R2	1
3	3R2	1
1	2R1	2
4	3R3	2
1	3R3	3
4	2R1	3

Routeur R3		
R	P	M
3	3R3	1
4	4R3	1
1	3R2	3
2	3R2	2
1	4R4	2
2	4R4	3

Routeur R4		
R	P	M
4	4R4	1
1	1R4	1
2	1R1	2
3	4R3	2
2	4R3	3
3	1R1	3

TP

*M04-01-01-TP-La\_communication*

*M04-01-02-TP-Packet\_Tracer-La\_communication*

# BASE DES RÉSEAUX

05 – LES PREMIÈRES COMMANDES

## Objectifs

- Utiliser les commandes réseau
- Différencier les commandes

# Les premières commandes

## LES PREMIÈRES COMMANDES

### Commande ARP

- Visualiser le cache ARP
  - Correspondance @IP = @MAC
  - Enregistrements statiques (ajout dans le cache)
  - Enregistrements dynamiques (requêtes ARP)
- Modifier le cache
  - Ajout d'enregistrements statiques
- Vider le cache
  - Supprimer un enregistrement
  - Supprimer tous les enregistrements

#### Cache ARP

##### Table ARP

Interface 01

##### Table ARP

Interface 02

## LES PREMIÈRES COMMANDES

@IP ↔ @MAC	Windows
Affiche le cache	arp -a
Affiche la table d'une interface	arp -a -n @ipiface
Ajoute un enregistrement statique	arp -s @ip @mac
Ajoute un enregistrement statique dans la table ARP d'une interface	arp -s @ip @mac @ipiface
Vider le cache	arp -d
Vider le cache d'une interface	arp -d @ipiface



## LES PREMIÈRES COMMANDES

	Debian
Affiche le cache (Nom d'hôte ⇔ @MAC)	arp -a
Affiche le cache (@IP ⇔ @MAC)	arp -n
Affiche le cache pour une interface	arp -a -i <i>interface</i> arp -n -i <i>interface</i>
Ajoute un enregistrement statique	arp -s <i>hôte @mac</i>
Supprime un enregistrement	arp -d <i>hôte</i>

## LES PREMIÈRES COMMANDES

### Commande **IPCONFIG**

Afficher la configuration reseau Windows

Exemple sous Windows



```
C:\>ipconfig  
Configuration IP de Windows
```

```
Carte Ethernet Ethernet :  
Statut du média          : Média déconnecté  
Suffixe DNS propre à la connexion :
```

```
Carte Ethernet Ethernet 2 :  
Suffixe DNS propre à la connexion :  
Adresse IPv6               :2a01:cb05:8d6a:3000:148e:f75f:6574:5b0f  
Adresse IPv6 temporaire    : 2a01:cb05:8d6a:3000:bc4f:245a:384f:9bfc  
Adresse IPv6 de liaison locale :fe80::148e:f75f:6574:5b0f%8  
Adresse IPv4               : 192.168.1.31  
Masque de sous-réseau      : 255.255.255.0  
Passerelle par défaut      : fe80::da7d:7fff:fed1:b090%8  
                           : 192.168.1.1
```

- Commande IPCONFIG

ipconfig (Windows)	
ipconfig	Affiche la configuration réseau simplifiée
ipconfig /all	Affiche la configuration réseau complet
ipconfig /displaydns	Affiche le cache DNS
ipconfig /flushdns	Vide le cache DNS
ipconfig /renew	Demande de renouvellement de bail
ipconfig /release	Libération d'un bail

### Afficher la configuration reseau Debian

Exemple sous Debian



```
root@Client-deb:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:bf:29:f8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.255.100/24 brd 192.168.255.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet6 2a01:cb05:8d6a:3000:20c:29ff:febf:29f8/64 scope global dynamic mngtmpaddr
        valid_lft 1778sec preferred_lft 578sec
    inet6 fe80::20c:29ff:febf:29f8/64 scope link
        valid_lft forever preferred_lft forever
```

- Commande IP

ip (Debian)	
ip a ou ip addr ou ip address ou ip address show	Affiche la configuration réseau
ip address show <i>iface</i>	Affiche la configuration réseau complet
ip -4 addr	Affiche la configuration réseau IPv4
ip addr add <i>@ip/cidr</i> dev <i>iface</i>	Attribue une <i>@ip</i> à une interface
ip link set dev <i>iface</i> up	Active une interface
ip link set dev <i>iface</i> down	Désactive une interface

- Protocole ICMP
- Vérifier la « présence » d'un nœud informatique
  - Connecter à un réseau
  - Démarrer
  - Appartenant au réseau logique
  - Demande ICMP autorisée dans le pare-feu

## LES PREMIÈRES COMMANDES

Réponse reçue sous Windows	
Réponse de @ip : octets=32 .... Réponse de @ip : octets=32 .... Réponse de @ip : octets=32 .... Réponse de @ip : octets=32 ....	Réponse reçue de l'hôte @ip
Réponse de @ip : impossible de joindre l'hôte ... Réponse de @ip : impossible de joindre l'hôte ... Réponse de @ip : impossible de joindre l'hôte ... Réponse de @ip : impossible de joindre l'hôte ...	L'hôte @ip n'a pas répondu - L'hôte n'est pas démarré - L'hôte n'est pas connecté au réseau - Le pare-feu de l'hôte n'est pas paramétré - L'hôte n'existe pas
PING : échec de la transmission. Défaillance générale PING : échec de la transmission. Défaillance générale PING : échec de la transmission. Défaillance générale PING : échec de la transmission. Défaillance générale	L'hôte appartient à un réseau inconnu de l'ordinateur local

## LES PREMIÈRES COMMANDES

Réponse reçue sous Debian	
64 bytes from @ip : icmp_seq=1 ttl=64 time ... 64 bytes from @ip : icmp_seq=2 ttl=64 time ... 64 bytes from @ip : icmp_seq=3 ttl=64 time ... 64 bytes from @ip : icmp_seq=4 ttl=64 time ... ...	Réponse reçue de l'hôte @ip
From @ip icmp_seq=1 Destination Host Unreachable From @ip icmp_seq=2 Destination Host Unreachable From @ip icmp_seq=3 Destination Host Unreachable From @ip icmp_seq=4 Destination Host Unreachable ...	L'hôte @ip n'a pas répondu <ul style="list-style-type: none"><li>- L'hôte n'est pas démarré</li><li>- L'hôte n'est pas connecté au réseau</li><li>- Le pare-feu de l'hôte n'est pas paramétré</li><li>- L'hôte n'existe pas</li><li>- L'hôte appartient à un réseau inconnu de l'ordinateur local</li></ul>



## LES PREMIÈRES COMMANDES

### Commande **NETSTAT**

Afficher des informations réseau

Affichage dynamique	Windows
Afficher les connexions TCP actives et les ports TCP/UDP en écoute	netstat -a
Afficher le processus des connexions TCP actives et des ports TCP/UDP	netstat -b
Affiche les connexions pour un protocole (TCP, UDP, TCPv6, UDPv6)	netstat -p <i>proto</i>
Afficher les statistiques Ethernet (nbre d'octets, nbre de paquets)	netstat -E

Affichage instantané	Windows
Afficher les connexions TCP actives et les ports TCP/UDP en écoute	netstat -n
Afficher la table de routage	netstat -r
Afficher les statistiques par protocole	netstat -s

## LES PREMIÈRES COMMANDES

### Commande **NETSTAT**

Afficher des informations réseau

	Debian
Afficher les connexions TCP actives	netstat
Afficher la table de routage	netstat -r
Afficher les statistiques Ethernet	netstat -i
Afficher le processus des connexions TCP actives	netstat -p
Afficher les @IP des connexions TCP actives	netstat -n

## LES PREMIÈRES COMMANDES

### Commande **SS**

#### Afficher des informations réseau

	Debian
Afficher tous	ss -a
Afficher les connexions IPv4	ss -4
Afficher les connexions IPv6	ss -6
Afficher le processus des connexions actives	ss -p
Afficher les connexions TCP	ss -t
Afficher les connexions UDP	ss -u



ss (Sockets Statistics) remplaçant de netstat sous Debian

### Commande sous Windows

- Afficher le chemin vers une destination
  - Affiche les interfaces d'entrée des routeurs traversés
- tracert @IP/site
  - tracert 172.217.18.195
  - tracert [www.google.fr](http://www.google.fr)
- tracert -4 @IP/site
  - Pour forcer l'utilisation IPv4

## LES PREMIÈRES COMMANDES

### Commande **TRACEROUTE**

#### Commande sous Debian

- Afficher le chemin vers une destination
  - Affiche les interfaces d'entrée des routeurs traversés
- traceroute @IP/site
  - traceroute 172.217.18.195
  - traceroute [www.google.fr](http://www.google.fr)
- traceroute -4 @IP/site
  - Pour forcer l'utilisation IPv4

TP

# BASE DES RÉSEAUX

06 – L'ADRESSAGE IPV6

## Objectifs

- Distinguer une adresse IPv6



## Les bénéfices de l'adressage IPv6

- Constitué de 8 hextets de 16 bits
- Espace d'adressage plus grand
  - *Global :  $340 \times 10^{36}$  adresses soit 340 sextillions (340 trillions de trillions)*
  - *Par réseau local :  $18,4 \times 10^{18}$  adresses soit 18,4 milliards de milliards*
- Suppression de la traduction d'adresses publiques en adresses privées (NAT)
- Suppression des adresses de broadcast (adresses de diffusion)
- Amélioration du routage
- Amélioration de la mobilité et de la sécurité
- Simplification de la numérotation des préfixes
- Adresses multiples par interface
- Adresse d'auto-configuration sans DHCP
- Mécanismes de transition entre IPv4 et IPv6

## L'ADRESSAGE IPV6

Adresse IPv6	Écriture hexadécimale complète (8 hextets de 16 bits)																													
	2036		:	0001		:	2BC5		:	0000		:	0000		:	0000		:	087C		:	000A								
Adresse IPv6	Écriture séparée par octets (16 octets de 8 bits)																													
	20	36	:	00	01	:	2B	C5	:	00	00	:	00	00	:	00	00	:	08	7C	:	00	0A							
Adresse IPv6	Écriture binaire (128 bits)																													
	0010 0000		0011 0110	:	0000 0000		0000 0001	:	0010 1011		1100 0101	:	0000 0000		0000 0000	:	0000 0000		0000 0000	:	0000 0000		0000 0000	:	0000 1000		0111 1100	:	0000 0000	

## L'ADRESSAGE IPV6

Adresse IPv6

Écriture hexadécimale complète (8 hextets de 16 bits)

2036 : 0001 : 2BC5 : 0000 : 0000 : 0000 : 087C : 000A

Adresse IPv6

Écriture simplifiée sans les 0 non-significatifs

2036 : 1 : 2BC5 : 0 : 0 : 0 : 87C : A

Adresse IPv6

Écriture compressée

2036 : 1 : 2BC5 : : : : 87C : A

Adresse IPv6

2036 : 1 : 2BC5 :: 87C : A

TP