**Résolution du travaux pratique**

Partie 1

1 .

1. Le masque de sous réseau est : 255.255.255.240
2. Réseau: 28 bits,Hôte: 32 - 28 = 4 bits
3. Le nombre total d’adresse est 16 adresses
4. 16 – 2 = 14, on aura 14 hôtes utilisataires

2.

|  |  |  |  |
| --- | --- | --- | --- |
| **Sous-Réseau** | **Adresse Réseau** | **Plage utilisable** | **Adresse Broadcast** |
| 1 | 192.178.12.0 | 192.178.12.1 → 192.178.12.14 | 192.178.12.15 |
| 2 | 192.178.12.16 | 192.178.12.17 → 192.178.12.30 | 192.178.12.31 |
| 3 | 192.178.12.32 | 192.178.12.33 → 192.178.12.46 | 192.178.12.47 |
| 4 | 192.178.12.48 | 192.178.12.49 → 192.178.12.62 | 192.178.12.63 |

Partie 2 :

1.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N° | Nom | Ancienne IP | Remarque | Nouvelle IP attribuée |
| 01 | Laptop | 192.178.12.0 ❌ | adresse réseau (interdite) | ✅ 192.178.12.1 |
| 02 | Desktop | 192.178.12.1 ✅ | OK | ✅ 192.178.12.2 |
| 03 | Desktop | 192.178.12.3 ✅ | OK | ✅ 192.178.12.3 |
| 04 | Desktop | 192.178.12.6 ✅ | OK | ✅ 192.178.12.4 |
| 05 | Laptop | 192.178.12.11 ✅ | OK | ✅ 192.178.12.5 |
| 06 | Imprimante | 192.178.12.17 ❌ | hors réseau /28 | ✅ 192.178.12.6 |
| 07 | Serveur | 192.178.12.13 ✅ | OK | ✅ 192.178.12.7 |
| 08 | Serveur | 192.178.12.11 ❌ | doublon | ✅ 192.178.12.8 |
| 09 | Laptop | 192.178.12.14 ✅ | dernière IP valide | ✅ 192.178.12.9 |
| 10 | Imprimante | 192.178.12.15 ❌ | adresse de broadcast (interdite) | ✅ 192.178.12.10 |

2. Je l’ai mis dans cisco en mode pratique

3. tout est connecté

4.

* **Machine n°6 (Imprimante)** a une IP = 192.178.12.17

Mais mon réseau est : 192.178.12.0/28

* + Plage valide : 192.178.12.1 → 192.178.12.14

Conclusion :  
→ **L’imprimante n°6 est dans un autre réseau !**  
→ C’est **la machine infiltrée**

**L’adresse du réseau et le broadcast**

**Adresse réseau = 192.178.12.16**

**Adresse broadcast = 192.178.12.31**

**Machine infiltrée : fait partie du réseau 192.178.12.16/28**

**.**

**trouvons**

**31 = 00011111 en binaire   
 C’est la première moitié de la clé**

La suite du code est 5c qui est les premier prefix de l’adresse MAC

**Cryptage**

* cryptage

La suite du code est 5c qui est les premier prefix de l’adresse MAC

Partie 3

**1. Nouveau département de 20 hôtes uniques**

**Pourquoi un sous-réseau en /28 ne suffit pas ?**

Un réseau en /28 donne :

* 32 - 28 = **4 bits pour les hôtes**
* Nombre total d’adresses : 2⁴ = **16 adresses**
* Mais attention :
  + 1 pour l’adresse réseau
  + 1 pour le broadcast
* Donc **14 hôtes utilisables**

**14 < 20** → pas suffisant

**Quel masque de sous-réseau faut-il alors ?**

On cherche au minimum **20 hôtes utilisables**.

🔢 Calcul :

* 2⁵ = 32 adresses → 30 hôtes (car 32 - 2 pour réseau/broadcast)
* Donc **/27** est le plus petit masque suffisant

| **Masque** | **Adresses totales** | **Hôtes utilisables** |
| --- | --- | --- |
| /28 | 16 | 14 |
| /27 ✅ | 32 | 30 |
| /26 | 64 | 62 |

🧠 **Justification :**

Avec un masque /27, on obtient 5 bits pour les hôtes :

2^5 = 32 adresses totales, soit 30 hôtes possibles.

C’est donc le masque le plus optimisé pour au moins 20 hôtes.

**2. Optimisation IP : 10 sous-réseaux de 14 hôtes en /28**

**Quel est le risque avec le temps ?**

Tu veux créer **10 sous-réseaux en /28** à partir de 192.178.12.0/24 :

* Chaque /28 = 16 adresses → 14 hôtes
* 256 adresses en tout (car /24)
* 256 ÷ 16 = **16 sous-réseaux max**

Tu veux en utiliser 10 sur 16 → ça passe **au début**  
❗ Mais...

**⚠️ Problème potentiel :**

Avec l’évolution de l’entreprise, si un sous-réseau a besoin de plus de 14 hôtes, le /28 sera insuffisant.

On sera obligé de fusionner ou réorganiser, ce qui implique une reconfiguration complexe.

**Conclusion :** ce plan n’est pas **scalable** (pas évolutif)

**3. Sécurité : adresse réseau & broadcast**

**Pourquoi on ne les attribue pas ?**

* **Adresse réseau** (ex: 192.178.12.0) : identifie le **sous-réseau lui-même**. Utilisée dans les tables de routage.
* **Adresse broadcast** (ex: 192.178.12.15) : utilisée pour **envoyer un message à tous les hôtes** du sous-réseau.

Elles ont une fonction **réseau**, pas d’hôte. Si tu les attribues à un hôte → conflit.

**Pourquoi bien planifier son sous-réseautage ?**

1. **Évite le gaspillage d’adresses IP**  
   → Tu donnes juste ce qu’il faut à chaque département
2. **Améliore la sécurité**  
   → En isolant les départements critiques dans des VLAN ou sous-réseaux dédiés, tu limites les failles de propagation
3. **Simplifie le dépannage**  
   → Si un problème survient, tu sais exactement dans quel bloc il est

**4. Dépannage : PC3 ne ping pas les autres**

**Hypothèse : PC1 et PC2 communiquent → réseau OK**

Mais PC3 est isolé. Donc problème **local à PC3**

**Démarche de diagnostic :**

**a. Vérifier la configuration IP de PC3 :**

ipconfig (Windows)

ifconfig (Linux)

**b. Tester la connectivité locale :**

ping 127.0.0.1

→ Vérifie si la carte réseau fonctionne

**c. Ping vers un voisin :**

ping 192.178.12.3 (adresse de PC1 ou PC2)

**d. Vérifie la table ARP :**

arp -a

→ Est-ce que PC3 apprend les adresses MAC de ses voisins ?

**e. Vérifie le câblage / carte réseau :**

* Le câble ou l’interface réseau est-elle activée ?
* LED verte sur la carte ?

**f. Optionnel : traceroute**

tracert 192.178.12.X