AMGHAR MOURAD GROUPE 10

DAKHOUCHE BILAL

Jalon 7 :

Rappels des conditions légales d'utilisation d'une application de scan :

Respect de la vie privée : Il est important de ne pas utiliser une application de scan de réseaux pour collecter des informations sur les utilisateurs sans leur consentement.

Utilisation légale : Il est illégal d'utiliser une application de scan de réseaux pour pénétrer dans des systèmes informatiques sans autorisation.

Responsabilité : Vous êtes responsable de l'utilisation que vous faites de l'application de scan de réseaux et de toute violation des lois et des règlementations.

Utilisation à des fins de sécurité : Il est important de rappeler que l'utilisation d'une application de scan de réseaux est légale uniquement à des fins de sécurité.

Respect de la propriété intellectuelle : Il est important de respecter les droits de propriété intellectuelle et de ne pas utiliser l'application de scan de réseaux pour violer les droits d'autrui.

Syntaxe des commandes NMAP permettant le scan des ports et des adresses IP :

Pour scanner un seul hôte ou un domaine :

nmap www.example.com

nmap 192.168.1.1

Pour scanner une plage d'adresses IP :

nmap 192.168.1.1-100

nmap 192.168.1.0/24

Pour spécifier les ports à scanner :

nmap -p 80,443 www.example.com

nmap -p 1-1000 www.example.com

Pour plus de commande :

nmap –help

Adresses IP et Numéro des ports ouverts sur le PC, le Rpi ainsi que les 4 machines connectés à découvrir. Liste des services des 4 machines à découvrir.

```
pi@rpi:~ $ nmap 192.168.33.16
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-10 11:11 CET
Nmap scan report for 192.168.33.16
Host is up (0.00064s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
pi@rpi:~ $ nmap 192.168.33.180
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-10 11:12 CET
Nmap scan report for 192.168.33.180
Host is up (0.00055s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2049/tcp open  nfs
5900/tcp open  vnc
```

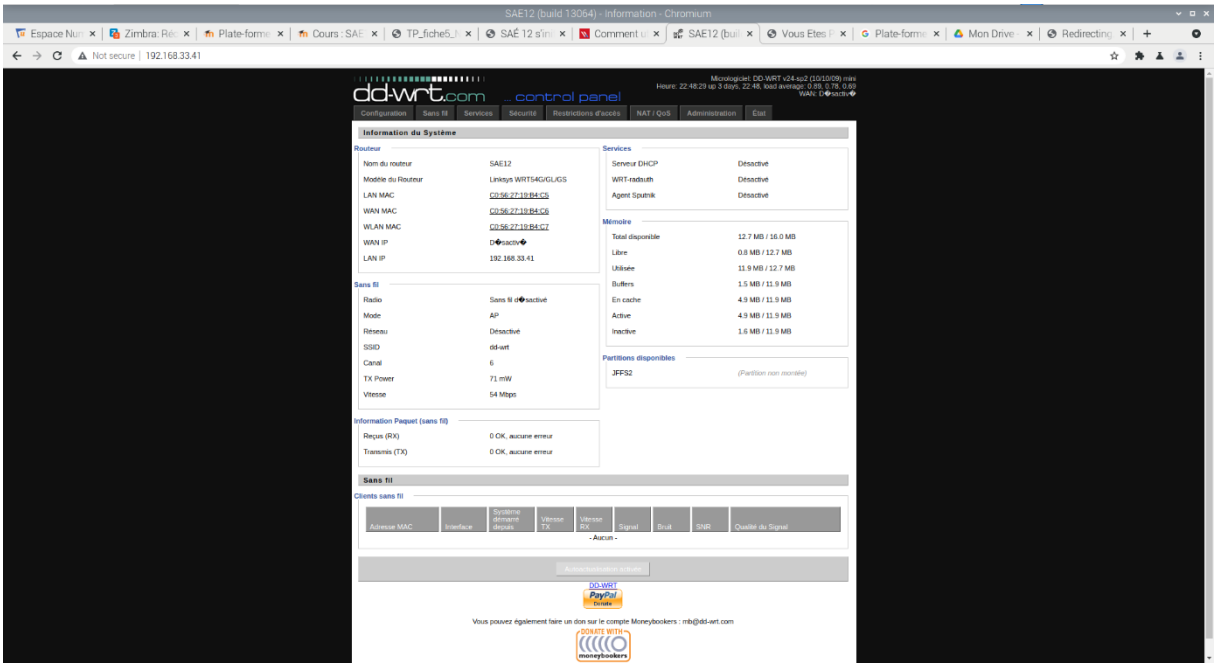
Le téléphone IP correspond à l'IP :192.168.33.10

La calculatrice à pour IP :192.168.33.33

La borne wifi à pour IP : 192.168.33.41

La caméra de surveillance correspond à l'IP : 192.168.33.90

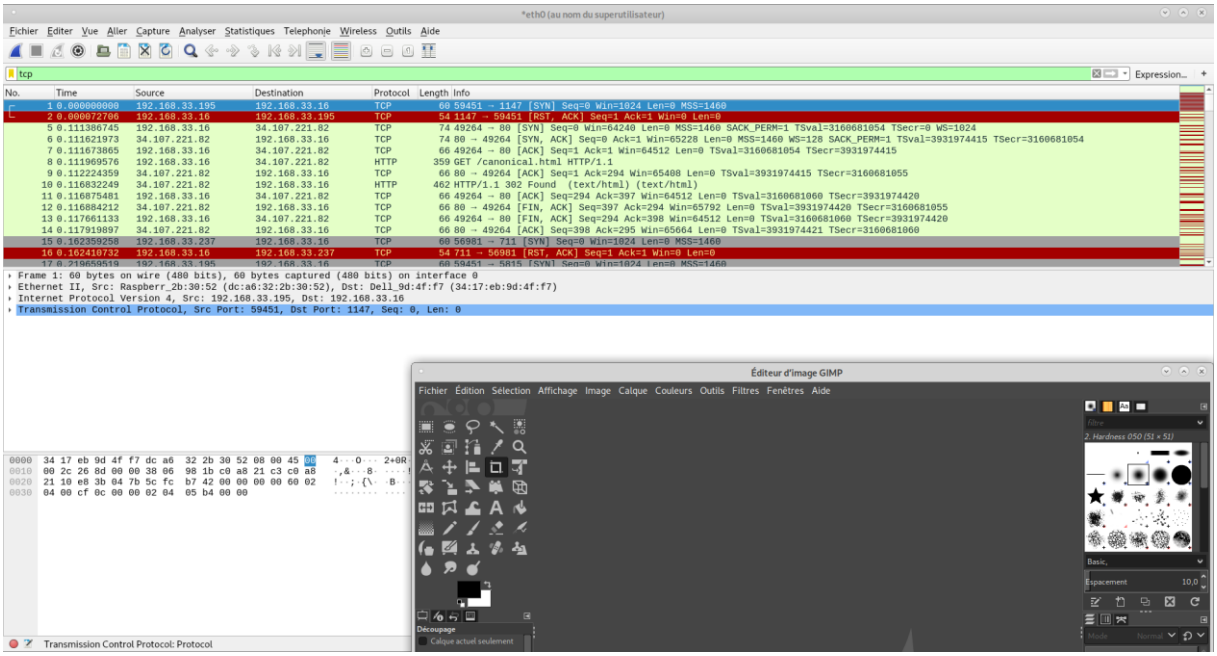
Jalon borne wifi=> copie écran du firmware et l'horaire. Rechercher dans la doc du constructeur, les caractéristiques essentielles de cette borne. Fournir une photo correspondant à ce matériel.

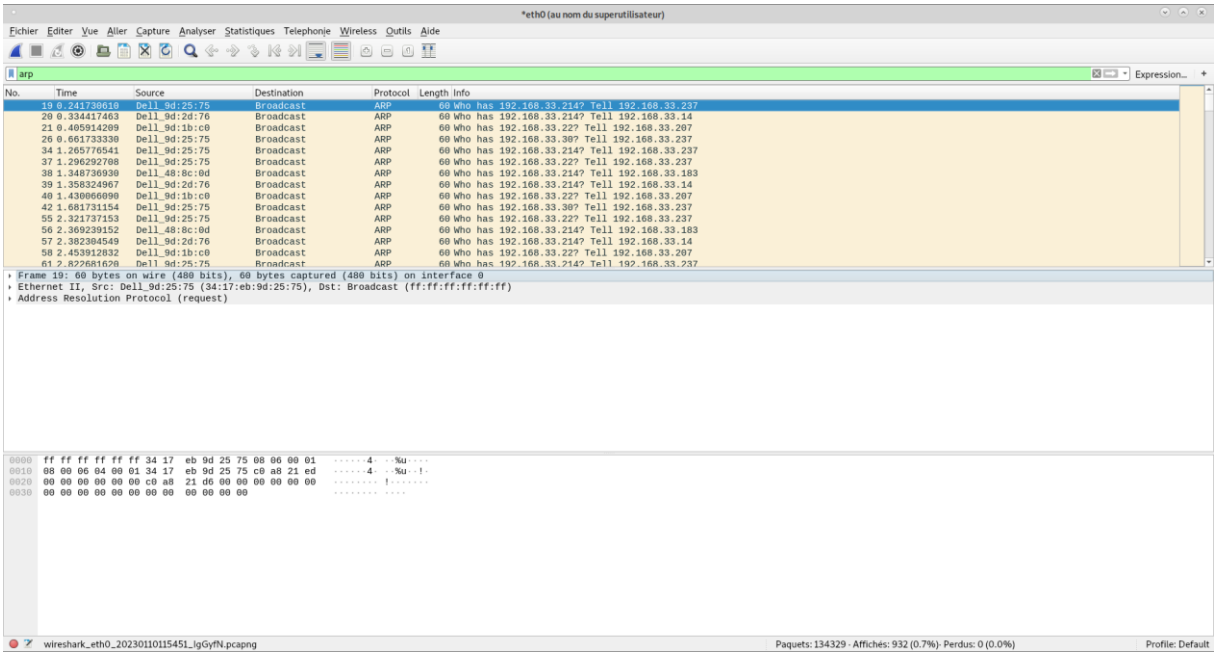


- Doté de SecureEasySetup (SES) - Bouton poussoir de sécurité;
- Compatible avec 802.11g et 802.11b (2.4GHz) Standards;
- Prend en charge Wired Equivalent Privacy™ (WEP), Wi-Fi Protected Access™ (WPA) et Wi-Fi Protected Access™2 (WPA2);
- Doté de fonctionnalités améliorées de Gestion de Sécurité Internet, Politiques d´Accès à Internet avec les horaires de travail;
- Prise en charge de la liaison par tous les ports LAN Autocroisés / Aucun câble croisé (MDI/MDI-X) n´est requis
- Dispose d´une interface basée sur le Web pour une configuration facile.

Identification du protocole (couche 4) permettant de scanner le port ouvert (capture d’écran de Wireshark)

Identification du protocole (couche 3) permettant de scanner l'adresse IP (capture d'écran de Wireshark)





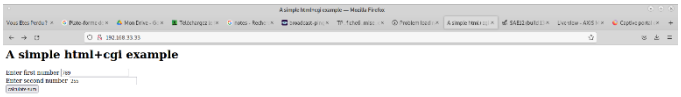
Copie d'écran des réponses des différentes broadcast.

```
tp@rt: ~
Fichier  Editer  Affichage  Rechercher  Terminal  Aide
tp@rt:~$ ping -b 255.255.255.255
WARNING: pinging broadcast address
PING 255.255.255.255 (255.255.255.255) 56(84) bytes of data.
64 bytes from 192.168.33.10: icmp_seq=1 ttl=64 time=0.690 ms
64 bytes from 192.168.33.33: icmp_seq=1 ttl=64 time=0.724 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=1 ttl=64 time=1.20 ms (DUP!)
64 bytes from 192.168.33.41: icmp_seq=1 ttl=64 time=1.23 ms (DUP!)
64 bytes from 192.168.33.108: icmp_seq=1 ttl=255 time=1.59 ms (DUP!)
64 bytes from 192.168.33.10: icmp_seq=2 ttl=64 time=0.561 ms
64 bytes from 192.168.33.33: icmp_seq=2 ttl=64 time=0.594 ms (DUP!)
64 bytes from 192.168.33.41: icmp_seq=2 ttl=64 time=0.601 ms (DUP!)
64 bytes from 192.168.33.108: icmp_seq=2 ttl=255 time=0.996 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=2 ttl=64 time=1.03 ms (DUP!)
64 bytes from 192.168.33.10: icmp_seq=3 ttl=64 time=0.596 ms
64 bytes from 192.168.33.33: icmp_seq=3 ttl=64 time=0.633 ms (DUP!)
64 bytes from 192.168.33.41: icmp_seq=3 ttl=64 time=0.887 ms (DUP!)
64 bytes from 192.168.33.108: icmp_seq=3 ttl=255 time=0.908 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=3 ttl=64 time=0.914 ms (DUP!)
64 bytes from 192.168.33.33: icmp_seq=4 ttl=64 time=0.568 ms
64 bytes from 192.168.33.10: icmp_seq=4 ttl=64 time=0.613 ms (DUP!)
64 bytes from 192.168.33.41: icmp_seq=4 ttl=64 time=0.860 ms (DUP!)
64 bytes from 192.168.33.108: icmp_seq=4 ttl=255 time=0.877 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=4 ttl=64 time=0.883 ms (DUP!)
64 bytes from 192.168.33.33: icmp_seq=5 ttl=64 time=0.602 ms
```

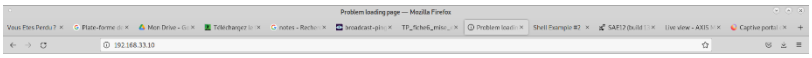
```
tp@rt: ~
Fichier  Editer  Affichage  Rechercher  Terminal  Aide
tp@rt:~$ ping 192.168.33.255 -b
WARNING: pinging broadcast address
PING 192.168.33.255 (192.168.33.255) 56(84) bytes of data.
64 bytes from 192.168.33.33: icmp_seq=1 ttl=64 time=0.646 ms
64 bytes from 192.168.33.10: icmp_seq=1 ttl=64 time=0.679 ms (DUP!)
64 bytes from 192.168.33.41: icmp_seq=1 ttl=64 time=0.686 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=1 ttl=64 time=1.63 ms (DUP!)
64 bytes from 192.168.33.33: icmp_seq=2 ttl=64 time=0.638 ms
64 bytes from 192.168.33.10: icmp_seq=2 ttl=64 time=0.669 ms (DUP!)
64 bytes from 192.168.33.41: icmp_seq=2 ttl=64 time=0.676 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=2 ttl=64 time=0.870 ms (DUP!)
64 bytes from 192.168.33.33: icmp_seq=3 ttl=64 time=0.708 ms
64 bytes from 192.168.33.10: icmp_seq=3 ttl=64 time=0.742 ms (DUP!)
64 bytes from 192.168.33.41: icmp_seq=3 ttl=64 time=0.749 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=3 ttl=64 time=1.05 ms (DUP!)
64 bytes from 192.168.33.33: icmp_seq=4 ttl=64 time=0.604 ms
64 bytes from 192.168.33.10: icmp_seq=4 ttl=64 time=0.635 ms (DUP!)
64 bytes from 192.168.33.41: icmp_seq=4 ttl=64 time=0.642 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=4 ttl=64 time=0.980 ms (DUP!)
^C
--- 192.168.33.255 ping statistics ---
4 packets transmitted, 4 received, +12 duplicates, 0% packet loss, time 34ms
rtt min/avg/max/mdev = 0.604/0.787/1.628/0.250 ms
tp@rt:~$
```

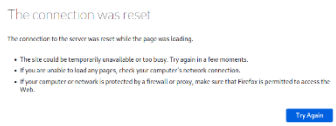
Copie d’écran de chaque service auquel vous aurez accédé. Dans le cas du serveur multimédia, une copie d’écran du résultat de l’addition est demandée.

Calculatrice :

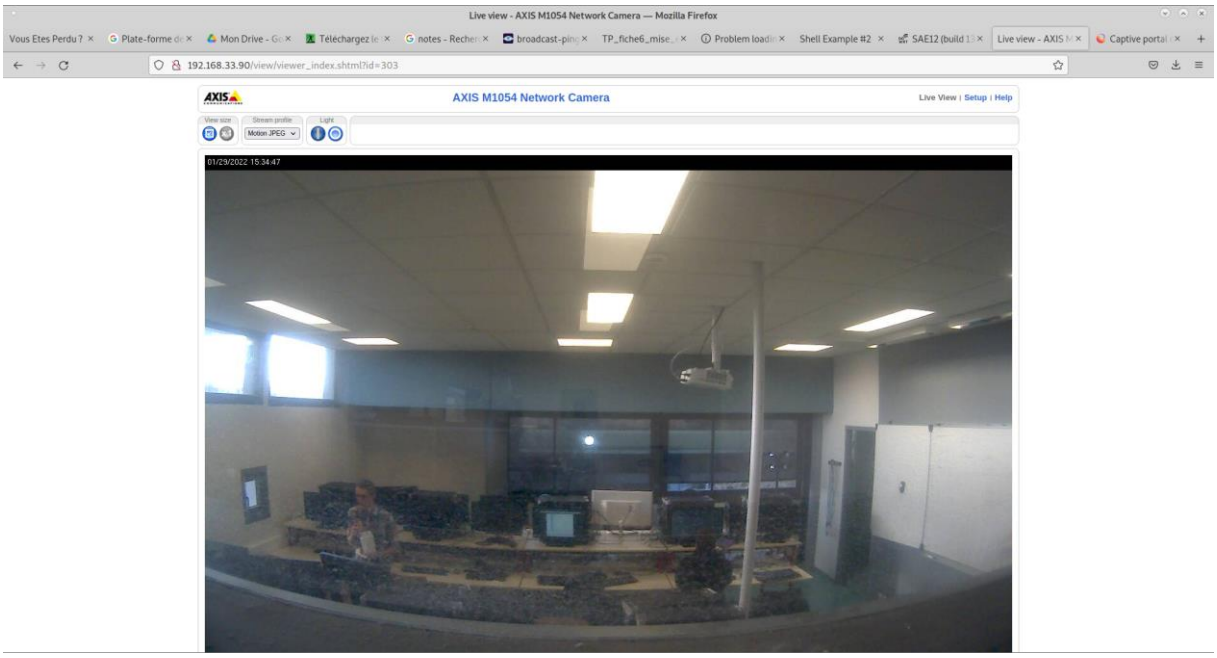


Téléphone IP : (page surdemandé)

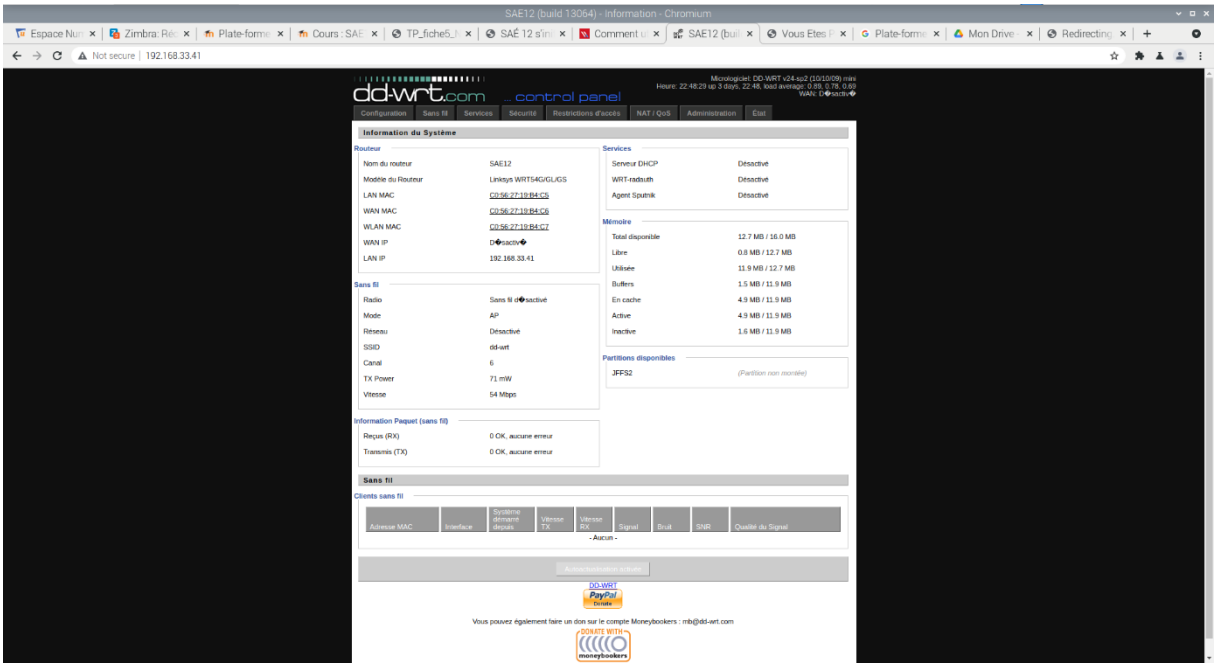




Caméra :



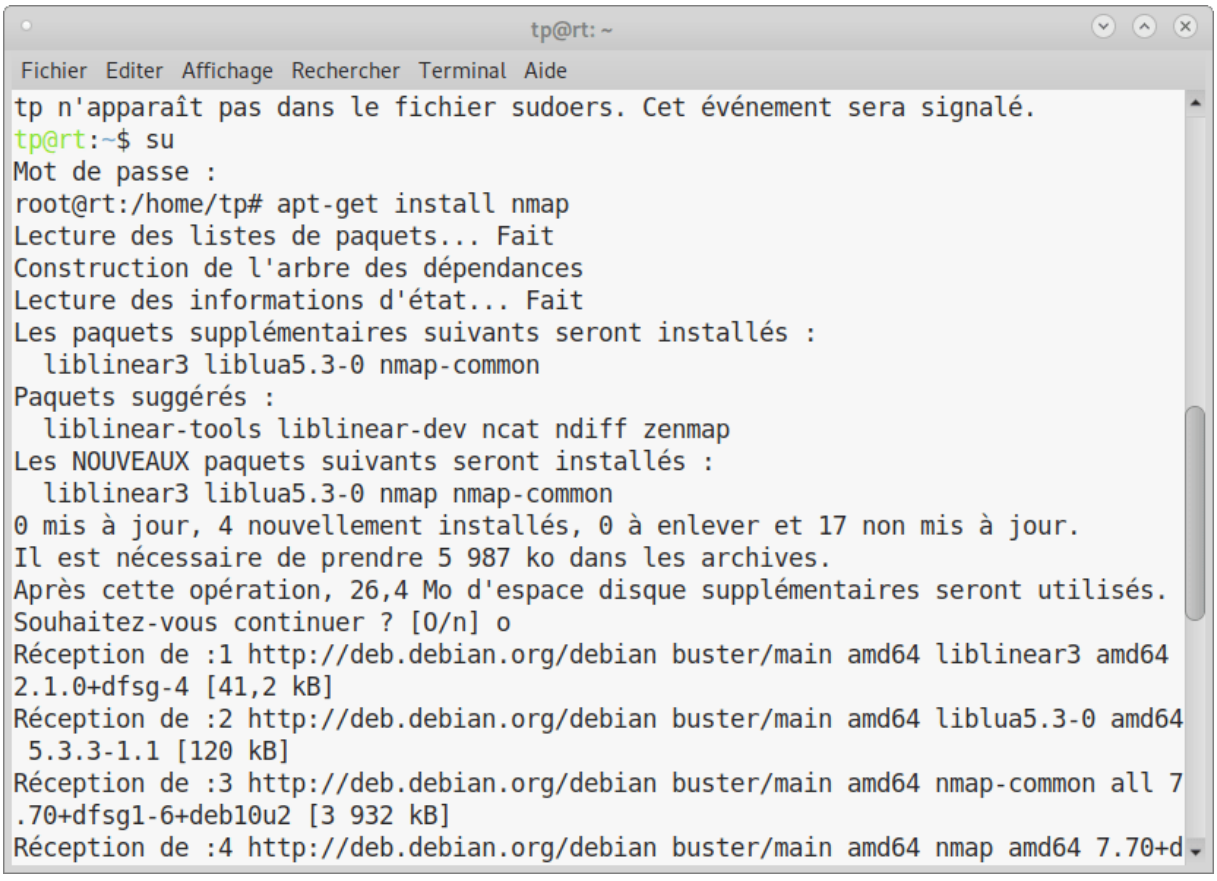
Routeur wifi :



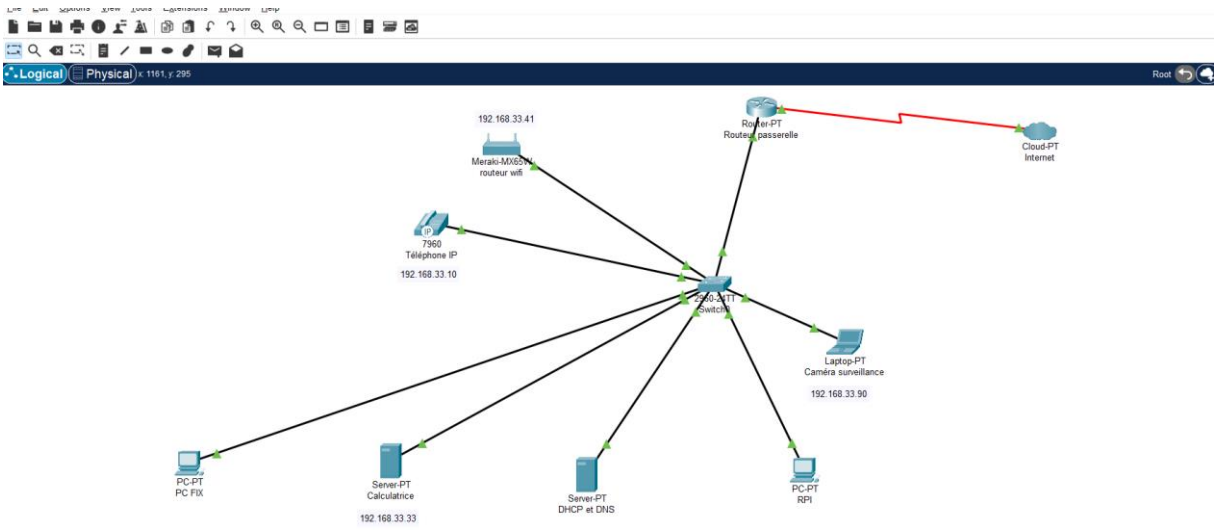
IP passerelle : 192.168.33.1

IP réseau de la salle : 192.168.33.0

Procédure installation et utilisation Nmap :



Simulation sous PT du réseau de la salle (IP du PC, IP du Rpi, IP passerelle) :



Voici *l'agenda hebdomadaire* réactualisé à la fin de notre septième jalon.

SAÉ_12_GANTT.mvdx*[récupéré]

			Planifi…	Nom de tâche	Durée	Début	Fin	Prédécess…	Progression
1				**Binôme 1-SAÉ 12 s'initier aux réseaux informatiques : 20 heures**	**2,87 jours**	**03/01/2022**	**05/01/2022**		**65%**
2				1. Outil de supervision: Mise en place d'un agenda hebdomadaire (1h)	0,24 jours	03/01/2022	03/01/2022		100%
3				2. Le PC fixe est connecté au réseau de l'IUT et il accède sur l'extéri…	0,12 jours	03/01/2022	03/01/2022	2	100%
4				3. Rpi connecté sur le réseau de l'IUT (2h)	0,23 jours	03/01/2022	03/01/2022	3	100%
5				4. Mise en place d'un serveur web Apache sur le Rpi	0,12 jours	03/01/2022	03/01/2022	4	100%
6				5. Certification de la connexion des 2 machines sur le même réseau…	0,22 jours	03/01/2022	03/01/2022	5	100%
7				6. Accès ssh établi entre le PC fixe et le Rpi(1h)	0,12 jours	04/01/2022	04/01/2022	6	100%
8				7. partage de ressources actif (3h)	0,36 jours	04/01/2022	04/01/2022	7	100%
9				8. réseau de la salle analysé (3h)	0,37 jours	04/01/2022	04/01/2022	8	75%
10				9. Infrastructure réseau de l'IUT analysé (3h)	0,36 jours	05/01/2022	05/01/2022		25%
11				10. Etude énergétique	0,12 jours	04/01/2022	04/01/2022		0%
12				11. Présentation finale: oral de 15mn en binôme	0,5 jours	05/01/2022	05/01/2022	10	0%

11. Présentation finale: oral de 15mn en binôme