Jalon 7 :

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

Le scan de port pouvant être utilisé à des fins légitime (comme un administrateur réseau voulant scanner ses machines pour repérer des logiciels indésirables sur son réseau) cependant le scan de port permet à une personne malintentionnée d'obtenir des informations sur des failles de sécurité par exemple.
C'est pour cela que nous pouvons seulement utiliser des applications de scan réseau dans notre propre réseau local dans lequel nous avons le droit d'en faire.
La condamnation pour l'utilisation d'un outil de scan de port tel que nmap dans un cadre non « légal » reste encore compliqué à sanctionné puisqu'il ne s'agit pas clairement d'un accès frauduleux malgré qu'il puisse signifier une étape préliminaire à une intrusion.

- **Scan des ports et IP avec nmap** :

  - Scan des ports de tous les appareils du réseau = *nmap 192.168.33.0/24*

  - Pour trouver les machines à découvrir (IP et ports) = *nmap 192.168.33.1-100* (d'IP 1 à 100).

  - Voir les ports ouverts d'une machine en particulier : *nmap 192.168.33.90* (par exemple).

- **Adresse IP et numéro des ports ouverts sur le PC, le RPI ainsi que les 4 machines connectés à découvrir** :

  - Sur le PC : *nmap* ***@IpduPC***

IP : 192.168.33.131
Les ports ouverts : 22 (ssh)

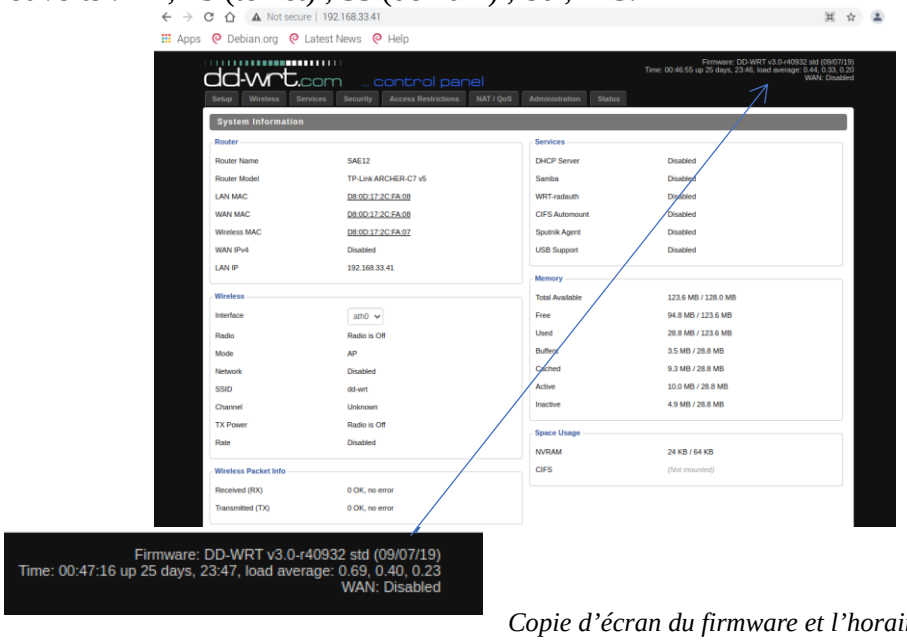
  - Sur le rspi : *nmap* ***@IpduRSPI***

Les ports ouverts : 22 (ssh) ; 80 (http) ; 139 (netbio-ssn) ; 145 (microsoft-ds) ; 5900 (vnc).
IP : 192.168.33.194

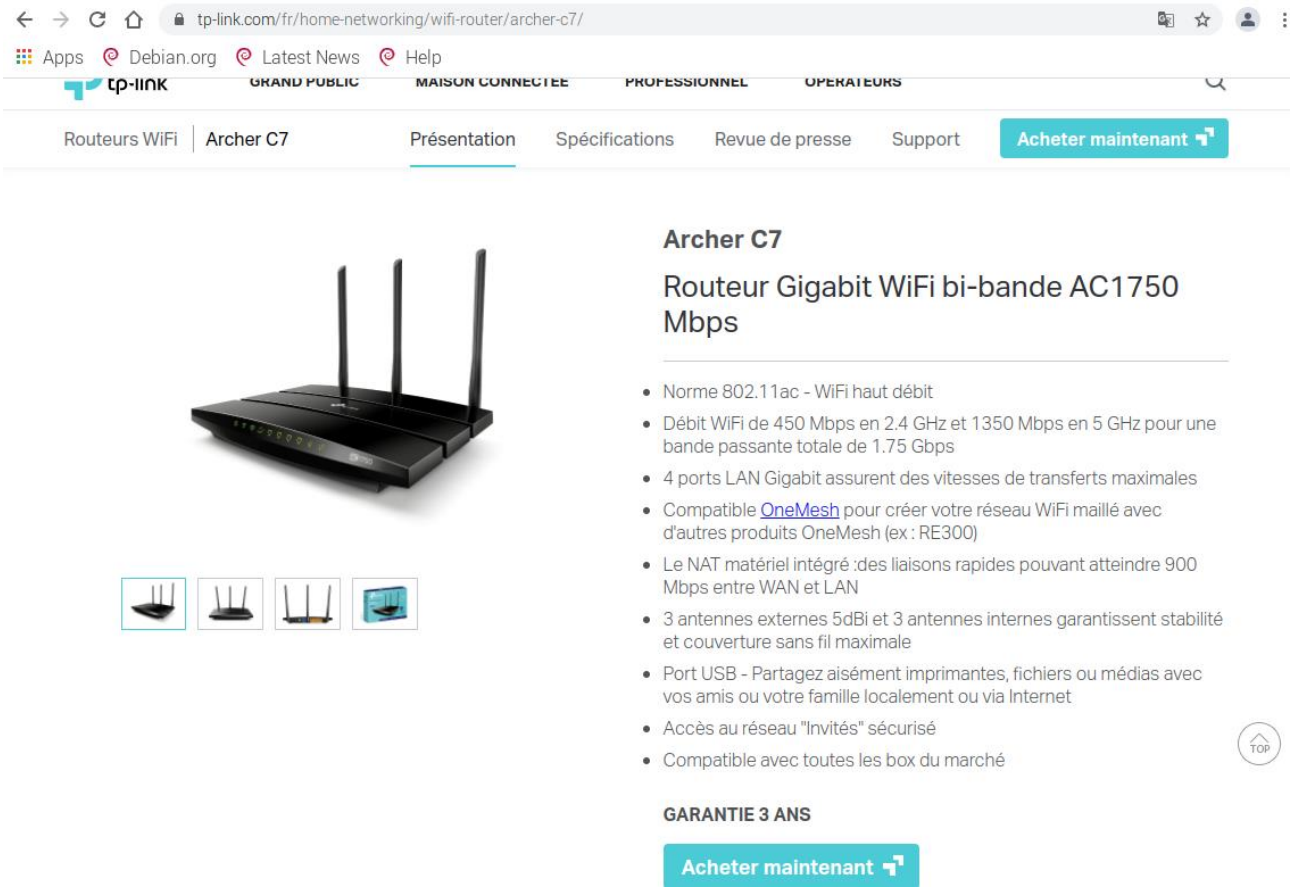
- Les 4 machines avec les commandes qui est *nmap* ***@IP*** :

1ère : 192.168.33.90 (CAMERA)
Les ports ouverts : 21 (FTP) ; 80 ; 443 (https) ; 554 (rtsp) ; 49152 (unknow)

2ème : 192.168.33.41 (BORNE WIFI)
Les ports ouverts : 22 ; 23 (telnet) ; 53 (domain) ; 80 ; 443.



Copie d'écran du firmware et l'horaire



Doc du constructeur avec les caractéristiques essentielles de cette borne

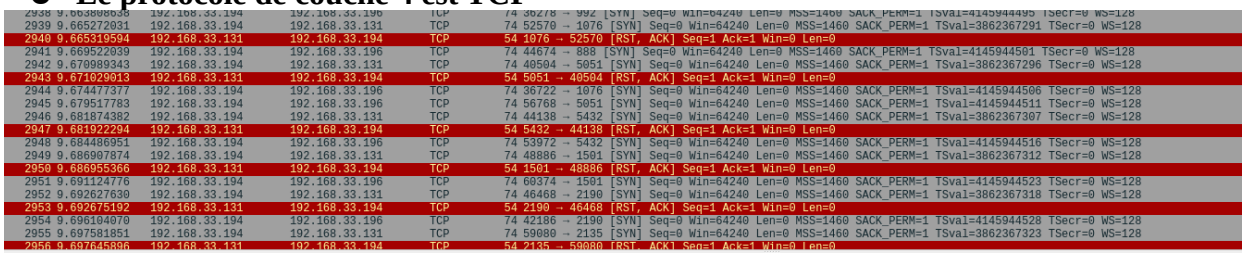
- 3ème : 192.168.33.33 (serveur multimédia)

Les ports ouverts : 23 ; 80

- 4ème : 192.168.33.10 (téléphone IP)

Les ports ouverts : 23 ; 80 ; 5060 (sip) ; 5061 (sip-tls)

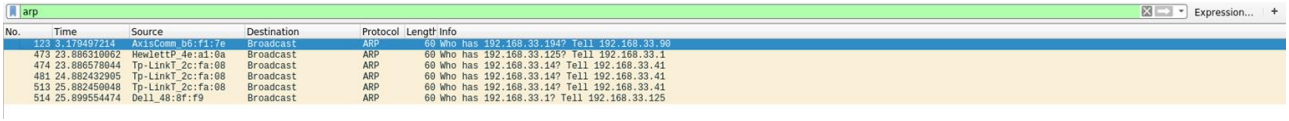
- **Le protocole de couche 4 est TCP**



2939	9.665272031	192.168.33.194	192.168.33.131	TCP	74 52570 → 1076 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3862367291 TSecr=0 WS=128
2940	9.665319594	192.168.33.131	192.168.33.194	TCP	54 1076 → 52570 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2941	9.669522039	192.168.33.194	192.168.33.196	TCP	74 44674 → 888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4145944501 TSecr=0 WS=128
2942	9.670009343	192.168.33.194	192.168.33.131	TCP	74 40504 → 5051 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3862367296 TSecr=0 WS=128
2943	9.671029013	192.168.33.131	192.168.33.194	TCP	54 5051 → 40504 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2944	9.674477377	192.168.33.194	192.168.33.196	TCP	74 36722 → 1076 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4145944506 TSecr=0 WS=128
2945	9.679517783	192.168.33.194	192.168.33.196	TCP	74 56768 → 5051 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4145944511 TSecr=0 WS=128
2946	9.681874382	192.168.33.194	192.168.33.131	TCP	74 44138 → 5432 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3862367307 TSecr=0 WS=128
2947	9.681922294	192.168.33.131	192.168.33.194	TCP	54 5432 → 44138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2948	9.684486951	192.168.33.194	192.168.33.196	TCP	74 53972 → 5432 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4145944516 TSecr=0 WS=128
2949	9.686907874	192.168.33.194	192.168.33.131	TCP	74 48886 → 1501 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3862367312 TSecr=0 WS=128
2950	9.686955366	192.168.33.131	192.168.33.194	TCP	54 1501 → 48886 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2951	9.691124776	192.168.33.194	192.168.33.196	TCP	74 60374 → 1501 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4145944523 TSecr=0 WS=128
2952	9.692627630	192.168.33.194	192.168.33.131	TCP	74 46468 → 2190 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3862367318 TSecr=0 WS=128
2953	9.692675192	192.168.33.131	192.168.33.194	TCP	54 2190 → 46468 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2954	9.696104070	192.168.33.194	192.168.33.196	TCP	74 42186 → 2190 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4145944528 TSecr=0 WS=128
2955	9.697581851	192.168.33.194	192.168.33.131	TCP	74 59080 → 2135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3862367323 TSecr=0 WS=128

On voit clairement que c'est le protocole TCP à la couche 4.

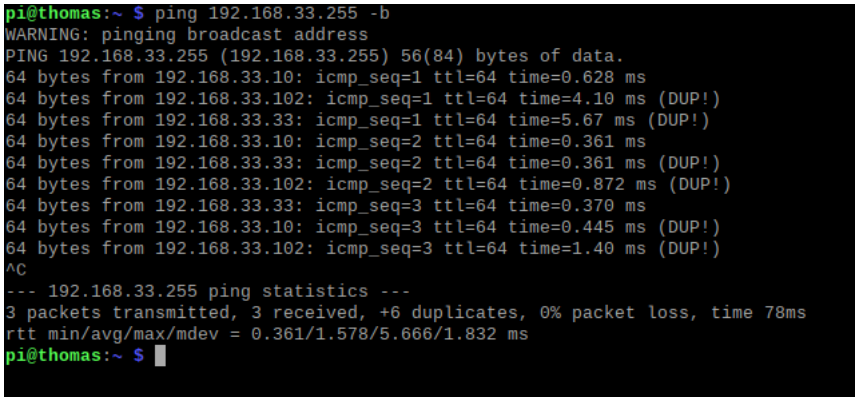
- **Le protocole de couche 3 est ARP**



No.	Time	Source	Destination	Protocol	Length	Info
123	3.170497214	AxisComm_b6:f1:7e	Broadcast	ARP	60	Who has 192.168.33.194? Tell 192.168.33.90
473	23.886310062	HewlettP_4e:a1:0a	Broadcast	ARP	60	Who has 192.168.33.125? Tell 192.168.33.1
474	23.886578044	Tp-LinkT_2c:fa:08	Broadcast	ARP	60	Who has 192.168.33.14? Tell 192.168.33.41
481	24.882432905	Tp-LinkT_2c:fa:08	Broadcast	ARP	60	Who has 192.168.33.14? Tell 192.168.33.41
513	25.882450048	Tp-LinkT_2c:fa:08	Broadcast	ARP	60	Who has 192.168.33.14? Tell 192.168.33.41
514	25.899554474	Dell_48:8f:f9	Broadcast	ARP	60	Who has 192.168.33.1? Tell 192.168.33.125

- **Copie d'écran des réponses des broadcast :**

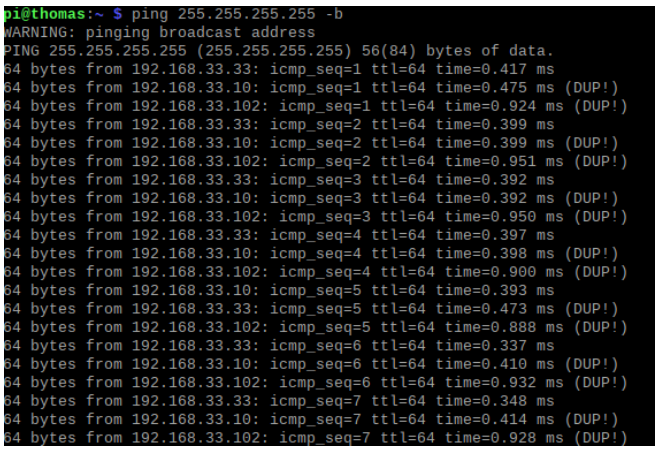
  - Broadcast réseau



```
pi@thomas:~ $ 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 192.168.33.10: icmp_seq=1 ttl=64 time=0.628 ms
64 bytes from 192.168.33.102: icmp_seq=1 ttl=64 time=4.10 ms (DUP!)
64 bytes from 192.168.33.33: icmp_seq=1 ttl=64 time=5.67 ms (DUP!)
64 bytes from 192.168.33.10: icmp_seq=2 ttl=64 time=0.361 ms
64 bytes from 192.168.33.33: icmp_seq=2 ttl=64 time=0.361 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=2 ttl=64 time=0.872 ms (DUP!)
64 bytes from 192.168.33.33: icmp_seq=3 ttl=64 time=0.370 ms
64 bytes from 192.168.33.10: icmp_seq=3 ttl=64 time=0.445 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=3 ttl=64 time=1.40 ms (DUP!)
^C
--- 192.168.33.255 ping statistics ---
3 packets transmitted, 3 received, +6 duplicates, 0% packet loss, time 78ms
rtt min/avg/max/mdev = 0.361/1.578/5.666/1.832 ms
pi@thomas:~ $
```

→ Les adresses qui répondent sont 192.168.33.10 // 192.168.33.102 // 192.168.33.33

  - Broadcast universel



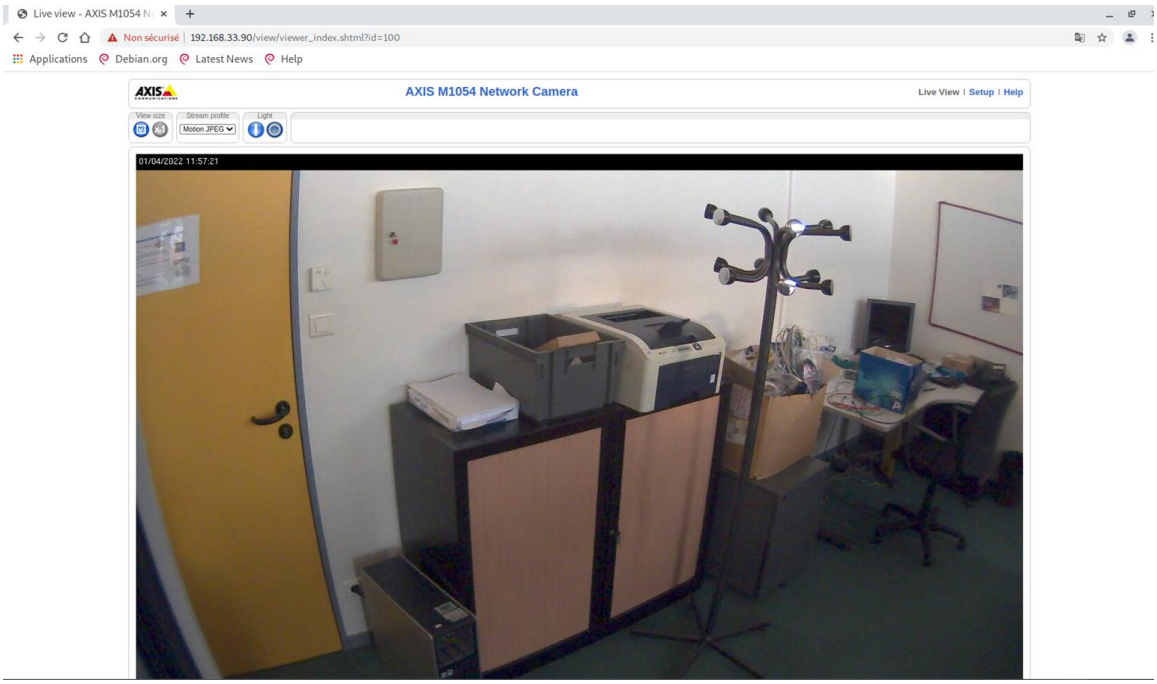
```
pi@thomas:~ $ ping 255.255.255.255 -b
WARNING: pinging broadcast address
PING 255.255.255.255 (255.255.255.255) 56(84) bytes of data.
64 bytes from 192.168.33.33: icmp_seq=1 ttl=64 time=0.417 ms
64 bytes from 192.168.33.10: icmp_seq=1 ttl=64 time=0.475 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=1 ttl=64 time=0.924 ms (DUP!)
64 bytes from 192.168.33.33: icmp_seq=2 ttl=64 time=0.399 ms
64 bytes from 192.168.33.10: icmp_seq=2 ttl=64 time=0.399 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=2 ttl=64 time=0.951 ms (DUP!)
64 bytes from 192.168.33.33: icmp_seq=3 ttl=64 time=0.392 ms
64 bytes from 192.168.33.10: icmp_seq=3 ttl=64 time=0.392 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=3 ttl=64 time=0.950 ms (DUP!)
64 bytes from 192.168.33.33: icmp_seq=4 ttl=64 time=0.397 ms
64 bytes from 192.168.33.10: icmp_seq=4 ttl=64 time=0.398 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=4 ttl=64 time=0.900 ms (DUP!)
64 bytes from 192.168.33.10: icmp_seq=5 ttl=64 time=0.393 ms
64 bytes from 192.168.33.33: icmp_seq=5 ttl=64 time=0.473 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=5 ttl=64 time=0.888 ms (DUP!)
64 bytes from 192.168.33.33: icmp_seq=6 ttl=64 time=0.337 ms
64 bytes from 192.168.33.10: icmp_seq=6 ttl=64 time=0.410 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=6 ttl=64 time=0.932 ms (DUP!)
64 bytes from 192.168.33.33: icmp_seq=7 ttl=64 time=0.348 ms
64 bytes from 192.168.33.10: icmp_seq=7 ttl=64 time=0.414 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=7 ttl=64 time=0.928 ms (DUP!)
```

→ Les adresses qui répondent sont 192.168.33.10 // 192.168.33.102 // 192.168.33.33

- **Copie d'écran de chaque service auquel vous aurez accédé.**

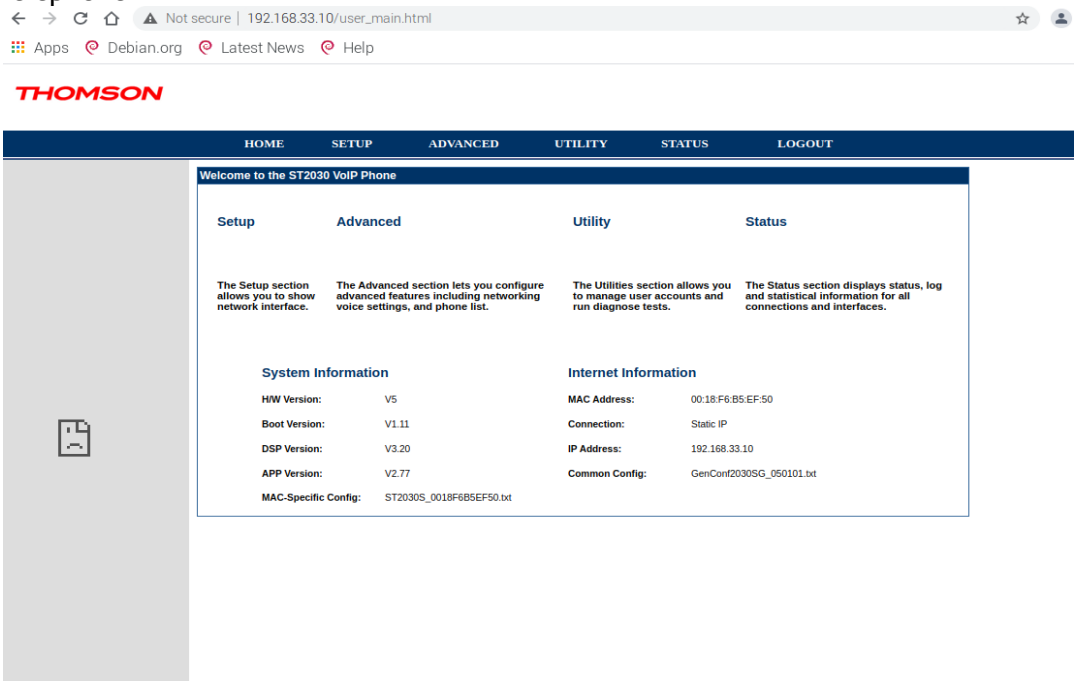
  - Serveur multimédia : (l'additionneur)

  - Caméra

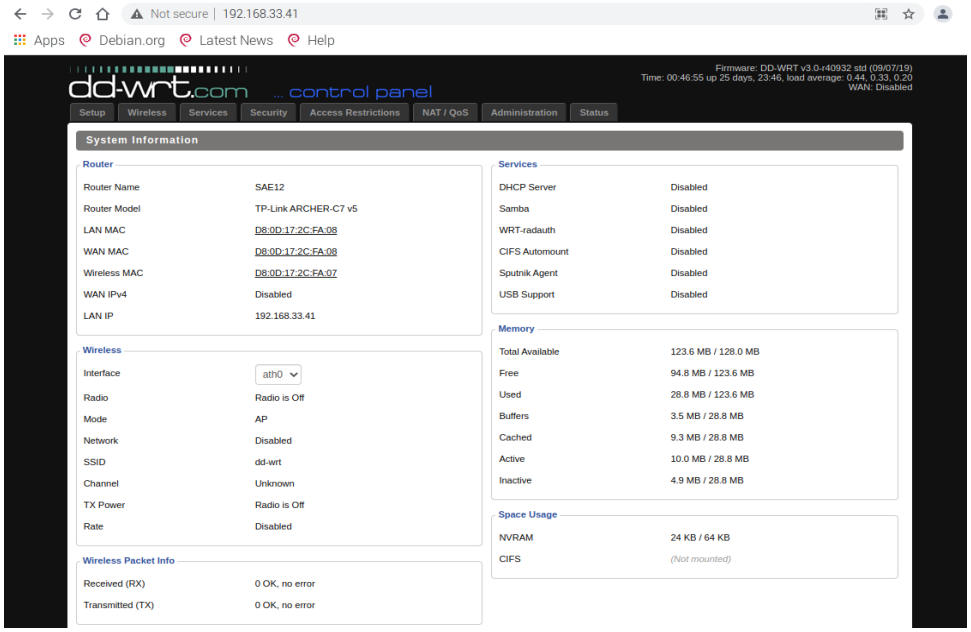


Thomas MIRBEY et RAYNAUD

- Téléphone IP



- Borne wifi



- IP Passerelle

L'IP est 192.168.33.1

- IP réseau salle

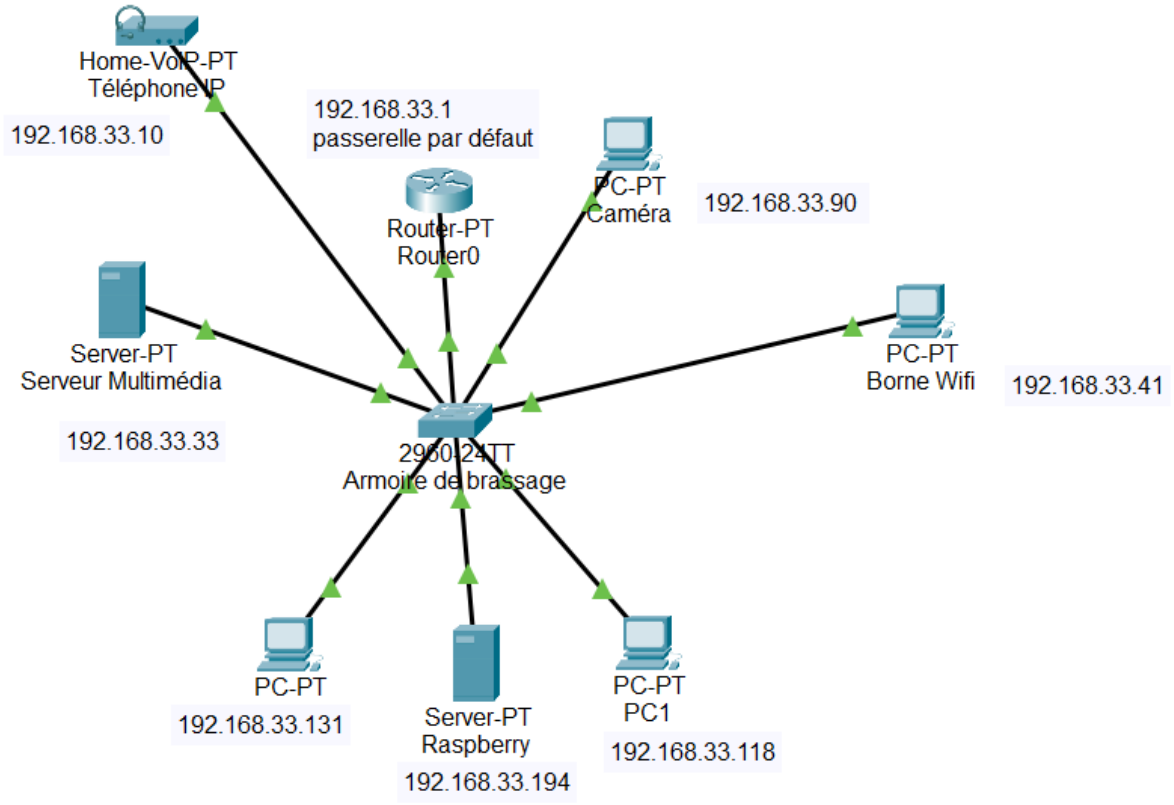
→ 192.168.33.0/24

- Procédure d'installation et utilisation de nmap

→ sudo apt install nmap
ou
→ sudo apt -get install nmap

Afin de l'utiliser il faut taper des commandes précises dans le terminal. Si l'on souhaite se renseigner sur des commandes, on peut écrire dans le terminal soit *nmap* soit *nmap –help.*
On peut aussi se renseigner sur des sites tels que : https://www.networklab.fr/scan-reseau-nmap/
Et utiliser les commandes que nous avons utilisé précédemment.

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



Il faut aussi prendre en compte de nombreuses autres machines qui sont connectées au réseau par le switch. Et aussi se rendre compte que pour se connecter au réseau chaque utilisateur doit passer par un portail captif sur www.perdu.com .

Thomas MIRBEY et RAYNAUD

- Copie de l’agenda hebdomadaire réactualisé :

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

	Le PC fixe est connecté au réseau de l'IUT et il accède sur l'extérieur : (1h)		
4	3 Rpi connecté sur le réseau de l'IUT (2h)	1	1
5	4 Mise en place d'un serveur web Apache sur le Rpi	1	1
6	5 Certification de la connexion des 2 machines sur le même réseau (2h)	1	1
7	6 Accès ssh établi entre le PC fixe et le Rpi(1h)	1	1
8	7 partage de ressources actif (3h)	1	1
9	8 réseau de la salle analysé (3h)	1	1
10	9 Infrastructure réseau de l'IUT analysé (3h)	1	1