

Jalon 7

7.1

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

Avant d'utiliser des outils de scan réseau comme Nmap, il est essentiel de se rappeler qu'il est illégal de scanner des réseaux et des dispositifs sans autorisation explicite. L'utilisation de ces outils doit se faire dans un cadre légal, comme sur des réseaux de test ou avec l'accord des propriétaires des systèmes à scanner.

7.2

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

Scan des ports :

Pour scanner les ports ouverts sur une adresse IP spécifique :

```
nmap <adresse_ip>
```

Pour scanner des ports spécifiques :

```
nmap -p <port1>,<port2>,<port3> <adresse_ip>
```

Scan des adresses IP :

Pour scanner un sous-réseau entier :

```
nmap <plage_ip>/24
```

Exemple pour scanner un sous-réseau local :

```
nmap 192.168.1.0/24
```

7.3

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

sur le PC (192.168.33.88)

PORT	
22	SSH
111	RPCbind
445	SMB
631	IPP

Sur le RPI (192.168.33.125)

PORT	SERVICE
22	SSH
80	http
111	RPCbind
2049	nfs
5900	vnc

Pour les 4 machines a découvrir

Routeur (192.168.33.49)

PORT	SERVICE
22	ssh
111	rpcbind

webcam (192.168.33.215)

PORT	SERVICE
21	ftp
80	http
443	https
554	rtsp
49155	unknow

téléphone (192.168.33.185)

PORT	SERVICE
23	telnet
80	http
5060	sip
5061	sip-tls

serveur multimédia(192.168.33.133)

PORT	SERVICE
23	telnet
80	http

7.4

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.

figure (32)




figure(33)

Linksys Accueil Affaires Assistance

Routeur sans fil G WRT54GL Linksys

Article n° WRT54GL



[GUIDE D'UTILISATION EN PDF](#) [TÉLÉCHARGEMENTS / MICROCODES](#)

[Enregistrer un produit](#)

1-800-326-7114

figure(34)

dd-wrt.com ... control panel

Micrologiciel: DD-WRT v24-sp2 (10/10/09) mini
Heure: 22:11:36 up 2 days, 22:11, load average: 1.38, 1.63, 1.51
WAN: D+activ

Configuration Sans fil Services Sécurité Restrictions d'accès NAT / QoS Administration État

Information du Système

Routeur		Services	
Nom du routeur	SAE12	Serveur DHCP	Désactivé
Modèle du Routeur	Linksys WRT54G/GL/GS	WRT-radauth	Désactivé
LAN MAC	C0:56:27:19:B4:C5	Agent Sputnik	Désactivé

rouge = horaire

7.5

Identification du protocole (couche 4) permettant de scanner le port ouvert (capture d'écran de Wireshark)
figure (35)

No.	Time	Source	Destination	Protocol	Length	Info
23095	10.233662824	192.168.33.88	192.168.33.215	TCP	66	50110 → 80 [ACK] Seq=1 Ack=6127716 Win=666 Len=0 TSval=4043145711 TSecr=639654
23096	10.233778909	192.168.33.215	192.168.33.88	TCP	1514	80 → 50110 [ACK] Seq=6127716 Ack=1 Win=1745 Len=1448 TSval=639654 TSecr=4043145711
23097	10.233847484	192.168.33.215	192.168.33.88	TCP	1918	80 → 50110 [ACK] Seq=6129164 Ack=1 Win=1745 Len=852 TSval=639654 TSecr=4043145711
23098	10.233860655	192.168.33.88	192.168.33.215	TCP	66	50110 → 80 [ACK] Seq=1 Ack=6130116 Win=666 Len=0 TSval=4043145711 TSecr=639654
23099	10.234179982	192.168.33.37	192.168.33.88	TCP	74	51958 → 35938 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2901877953 TSecr=0 WS=1024
23100	10.234179112	192.168.33.215	192.168.33.88	TCP	1514	80 → 50110 [ACK] Seq=6130116 Ack=1 Win=1745 Len=1448 TSval=639654 TSecr=4043145711
23101	10.234188539	192.168.33.88	192.168.33.37	TCP	54	35938 → 51958 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23102	10.234390521	192.168.33.215	192.168.33.88	TCP	1514	80 → 50110 [ACK] Seq=6131564 Ack=1 Win=1745 Len=1448 TSval=639654 TSecr=4043145711
23103	10.234314988	192.168.33.88	192.168.33.215	TCP	66	50110 → 80 [ACK] Seq=1 Ack=6133012 Win=666 Len=0 TSval=4043145712 TSecr=639654
23104	10.234422578	192.168.33.215	192.168.33.88	TCP	1514	80 → 50110 [ACK] Seq=6133012 Ack=1 Win=1745 Len=1448 TSval=639654 TSecr=4043145711
23105	10.234553249	192.168.33.215	192.168.33.88	TCP	1514	80 → 50110 [ACK] Seq=6134460 Ack=1 Win=1745 Len=1448 TSval=639654 TSecr=4043145711
23106	10.234659574	192.168.33.88	192.168.33.215	TCP	66	50110 → 80 [ACK] Seq=1 Ack=6135908 Win=666 Len=0 TSval=4043145712 TSecr=639654
23107	10.234676096	192.168.33.215	192.168.33.88	TCP	1514	80 → 50110 [ACK] Seq=6135908 Ack=1 Win=1745 Len=1448 TSval=639654 TSecr=4043145711
23108	10.234736559	192.168.33.37	192.168.33.88	TCP	74	54202 → 23964 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2901877954 TSecr=0 WS=1024
23109	10.234744637	192.168.33.88	192.168.33.37	TCP	54	23964 → 54202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23110	10.234758533	192.168.33.215	192.168.33.88	TCP	1618	80 → 50110 [ACK] Seq=6137556 Ack=1 Win=1745 Len=1448 TSval=639654 TSecr=4043145711
23111	10.234808354	192.168.33.88	192.168.33.215	TCP	66	50110 → 80 [ACK] Seq=1 Ack=6138308 Win=666 Len=0 TSval=4043145712 TSecr=639654
23112	10.235104632	192.168.33.88	192.168.33.88	TCP	1514	80 → 50110 [ACK] Seq=6138308 Ack=1 Win=1745 Len=1448 TSval=639654 TSecr=4043145712
23113	10.235272438	192.168.33.37	192.168.33.88	TCP	74	36012 → 12413 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2901877954 TSecr=0 WS=1024
23114	10.235274055	192.168.33.88	192.168.33.37	TCP	54	12413 → 36012 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23115	10.235395426	192.168.33.216	239.255.255.250	SDP	218	M-SEARCH * HTTP/1.1
23116	10.235395453	192.168.33.215	192.168.33.88	TCP	1514	80 → 50110 [ACK] Seq=6139756 Ack=1 Win=1745 Len=1448 TSval=639655 TSecr=4043145712
23117	10.235408910	192.168.33.215	192.168.33.88	TCP	66	50110 → 80 [ACK] Seq=1 Ack=6141204 Win=666 Len=0 TSval=4043145713 TSecr=639654
23118	10.235517754	192.168.33.215	192.168.33.88	TCP	1514	80 → 50110 [ACK] Seq=6141204 Ack=1 Win=1745 Len=1448 TSval=639655 TSecr=4043145712
23119	10.235593922	192.168.33.215	192.168.33.88	TCP	1514	80 → 50110 [ACK] Seq=6142652 Ack=1 Win=1745 Len=1448 TSval=639655 TSecr=4043145712
23120	10.235606837	192.168.33.88	192.168.33.215	TCP	66	50110 → 80 [ACK] Seq=1 Ack=6144100 Win=666 Len=0 TSval=4043145713 TSecr=639655
23121	10.235722525	192.168.33.215	192.168.33.88	TCP	1514	80 → 50110 [ACK] Seq=6144100 Ack=1 Win=1745 Len=1448 TSval=639655 TSecr=4043145712
23122	10.235796988	192.168.33.37	192.168.33.88	TCP	74	36272 → 46986 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2901877955 TSecr=0 WS=1024
23123	10.235804658	192.168.33.88	192.168.33.37	TCP	54	46986 → 36272 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23124	10.235826258	192.168.33.37	192.168.33.88	TCP	74	33210 → 33210 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2901877955 TSecr=0 WS=1024
23125	10.236326545	192.168.33.88	192.168.33.37	TCP	54	19236 → 33218 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23126	10.236342774	192.168.33.37	192.168.33.88	TCP	74	33548 → 52768 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2901877956 TSecr=0 WS=1024
23127	10.236371767	192.168.33.88	192.168.33.37	TCP	54	52768 → 33548 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23128	10.237431538	192.168.33.37	192.168.33.88	TCP	74	44012 → 19348 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2901877956 TSecr=0 WS=1024
23129	10.237454174	192.168.33.88	192.168.33.37	TCP	54	10848 → 44812 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23130	10.238061177	192.168.33.37	192.168.33.88	TCP	74	33268 → 33297 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2901877958 TSecr=0 WS=1024
23131	10.238084133	192.168.33.88	192.168.33.37	TCP	54	33297 → 33268 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23132	10.239180628	192.168.33.88	192.168.33.88	TCP	74	52938 → 31081 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2901877959 TSecr=0 WS=1024
23133	10.239183392	192.168.33.88	192.168.33.37	TCP	54	31081 → 52938 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23134	10.239191173	192.168.33.37	192.168.33.88	TCP	74	41019 → 58710 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2901877959 TSecr=0 WS=1024
23135	10.239802408	192.168.33.88	192.168.33.37	TCP	54	41019 → 58710 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23136	10.240282178	192.168.33.37	192.168.33.88	TCP	74	42264 → 3596 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2901877959 TSecr=0 WS=1024
23137	10.240286042	192.168.33.88	192.168.33.37	TCP	54	3596 → 42264 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23138	10.241035963	192.168.33.88	192.168.33.88	TCP	74	47626 → 60761 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2901877960 TSecr=0 WS=1024
23139	10.241038088	192.168.33.88	192.168.33.37	TCP	54	60760 → 47626 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

7.6

Identification du protocole (couche 3) permettant de scanner l'adresse IP (capture d'écran de Wireshark)
figure (36)

No.	Time	Source	Destination	Protocol	Length	Info
563	0.772161889	00:11:45:97:3b	00:00:00:00:00:00	ARP	60	Who has 192.168.33.182? Tell 192.168.33.20
564	0.818499069	FsCom_1f:93:08	Broadcast	ARP	60	Who has 192.168.33.17? Tell 192.168.33.159
838	1.152748319	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.17? Tell 192.168.33.88
839	1.152769050	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.27? Tell 192.168.33.88
840	1.152776822	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.37? Tell 192.168.33.88
841	1.152783950	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.47? Tell 192.168.33.88
842	1.152790336	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.57? Tell 192.168.33.88
843	1.152796333	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.67? Tell 192.168.33.88
844	1.152802140	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.77? Tell 192.168.33.88
845	1.152808037	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.87? Tell 192.168.33.88
846	1.152813816	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.97? Tell 192.168.33.88
847	1.152820025	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.107? Tell 192.168.33.88
848	1.152997209	4c:d7:17:9f:18:78	00:be:43:8c:43:12	ARP	60	192.168.33.1 is at 00:00:5e:00:01:02
849	1.152997331	4c:d7:17:9f:18:78	00:be:43:8c:43:12	ARP	60	192.168.33.2 is at 4c:d7:17:9f:18:78
850	1.152997413	4c:d7:17:9f:18:05:d9	00:be:43:8c:43:12	ARP	60	192.168.33.3 is at 4c:d7:17:9f:18:05:d9
851	1.153059337	00:11:45:97:3b	00:be:43:8c:43:12	ARP	60	192.168.33.10 is at 34:17:eb:9d:18:d3
852	1.153059424	28:87:ba:92:be:e0	00:be:43:8c:43:12	ARP	60	192.168.33.4 is at 28:87:ba:92:be:e0
987	1.342666091	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.57? Tell 192.168.33.88
988	1.342629740	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.67? Tell 192.168.33.88
989	1.342637184	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.77? Tell 192.168.33.88
990	1.342644667	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.87? Tell 192.168.33.88
991	1.342651196	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.97? Tell 192.168.33.88
992	1.342715484	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.137? Tell 192.168.33.88
993	1.342723610	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.147? Tell 192.168.33.88
994	1.342730593	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.157? Tell 192.168.33.88
995	1.342737161	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.167? Tell 192.168.33.88
996	1.342744551	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.177? Tell 192.168.33.88
997	1.342751325	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.187? Tell 192.168.33.88
998	1.342757272	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.197? Tell 192.168.33.88
999	1.342763117	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.207? Tell 192.168.33.88
1000	1.342768943	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.217? Tell 192.168.33.88
1001	1.342775840	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.227? Tell 192.168.33.88
1002	1.342908832	00:11:45:97:3b	00:be:43:8c:43:12	ARP	60	192.168.33.14 is at 34:17:eb:9d:18:95
1003	1.342909949	00:11:45:97:3b	00:be:43:8c:43:12	ARP	60	192.168.33.17 is at 34:17:eb:9d:4f:b9
1004	1.342913021	00:11:45:97:3b	00:be:43:8c:43:12	ARP	60	192.168.33.20 is at 34:17:eb:9d:05:0f
1092	1.443206242	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.137? Tell 192.168.33.88
1093	1.443229950	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.147? Tell 192.168.33.88
1094	1.443237284	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.157? Tell 192.168.33.88
1095	1.443244282	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.167? Tell 192.168.33.88
1096	1.443251658	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.177? Tell 192.168.33.88
1097	1.443259471	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.187? Tell 192.168.33.88
1098	1.443265952	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.197? Tell 192.168.33.88
1099	1.443272324	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.207? Tell 192.168.33.88
1100	1.443278801	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.217? Tell 192.168.33.88
1101	1.443285450	00:be:43:8c:43:12	Broadcast	ARP	42	Who has 192.168.33.227? Tell 192.168.33.88

7.7

Copie d'écran des réponses des différents broadcast.
figure (37) avec la commande ping -b 192.168.33.255 -c 2

```
root@rt:~# ping -b 192.168.33.255 -c 2
WARNING: pinging broadcast address
PING 192.168.33.255 (192.168.33.255) 56(84) bytes of data.
64 bytes from 192.168.33.185: icmp_seq=1 ttl=64 time=0.409 ms
64 bytes from 192.168.33.41: icmp_seq=1 ttl=64 time=0.846 ms (DUP!)
64 bytes from 192.168.33.133: icmp_seq=1 ttl=64 time=4.89 ms (DUP!)
64 bytes from 192.168.33.221: icmp_seq=1 ttl=255 time=5.25 ms (DUP!)
64 bytes from 192.168.33.185: icmp_seq=2 ttl=64 time=0.673 ms

--- 192.168.33.255 ping statistics ---
2 packets transmitted, 2 received, +3 duplicates, 0% packet loss, time 2ms
rtt min/avg/max/mdev = 0.409/2.413/5.253/2.176 ms
root@rt:~#
```

7.8

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.

figure (38) Pour la webcam (192.168.33.215)

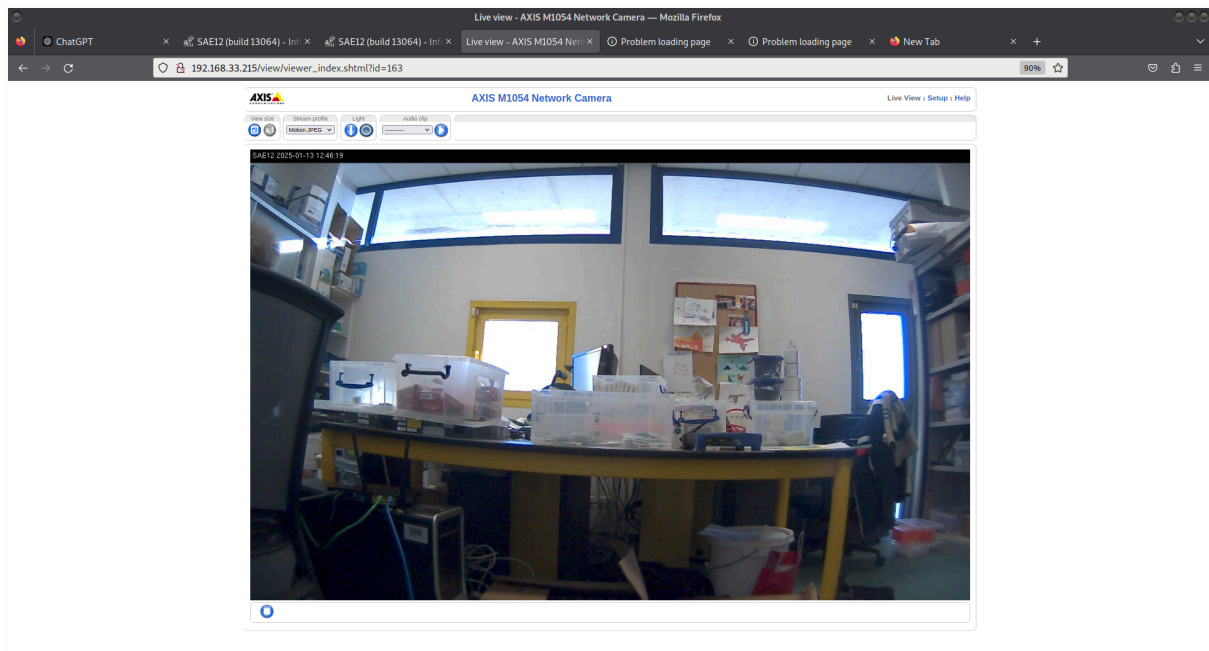


figure (39) Pour le routeur

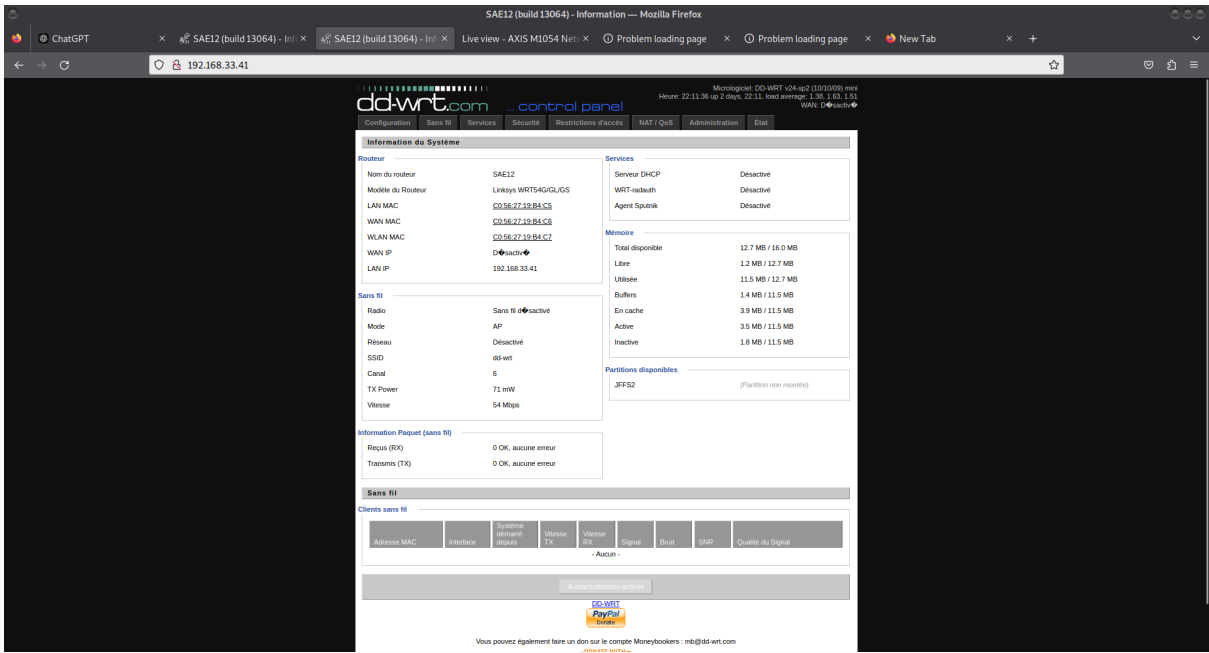


figure 40)Pour le téléphone (192.168.33.185)

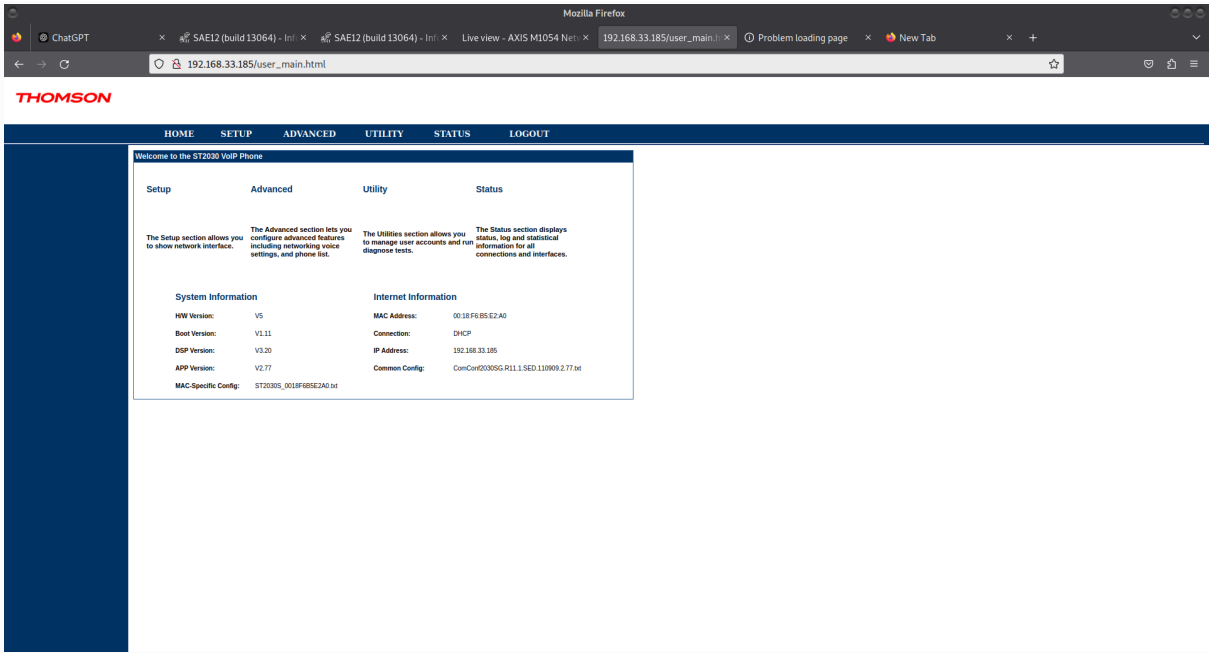
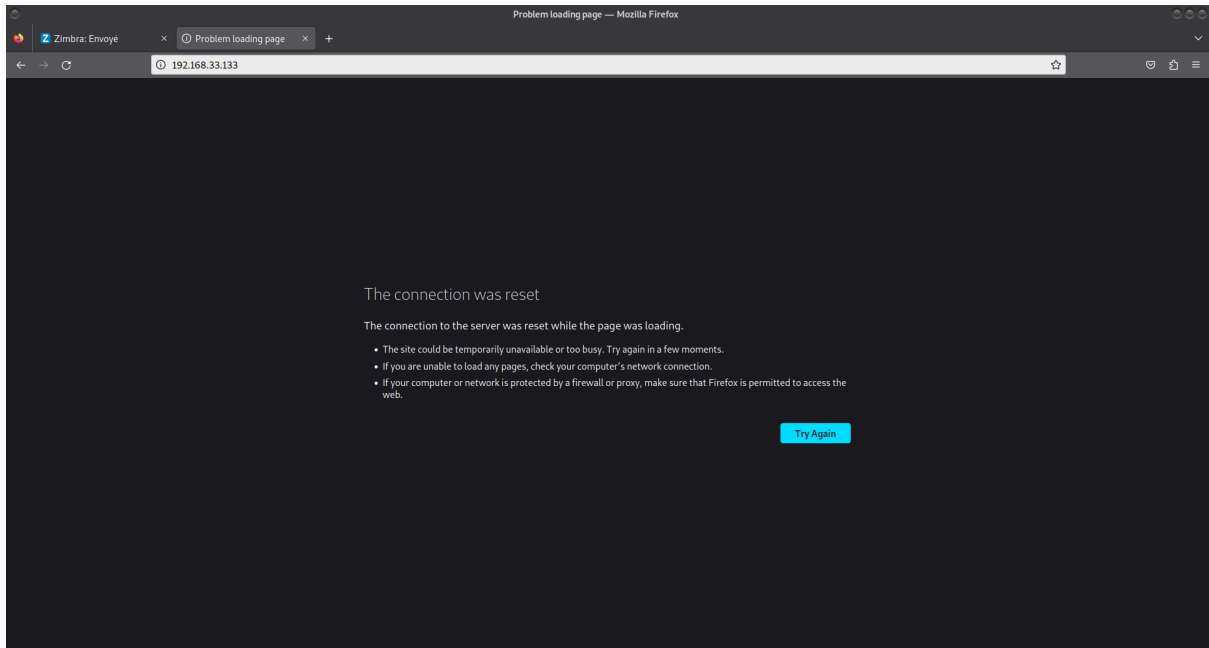


figure 41) pour le serveur multimedia (192.168.33.133)



7.9

IP Passerelle

figure 42) réalisé avec la commande ip route

```
root@rt:~# ip route
default via 192.168.33.1 dev eth0
10.178.0.0/24 dev docker0 proto kernel scope link src 10.178.0.1 linkdown
192.168.33.0/24 dev eth0 proto kernel scope link src 192.168.33.88
```

7.10

IP réseau salle

comme le masque c'est 255.255.255.0 l'adresse ip réseau salle est 192.168.33.0

7.11

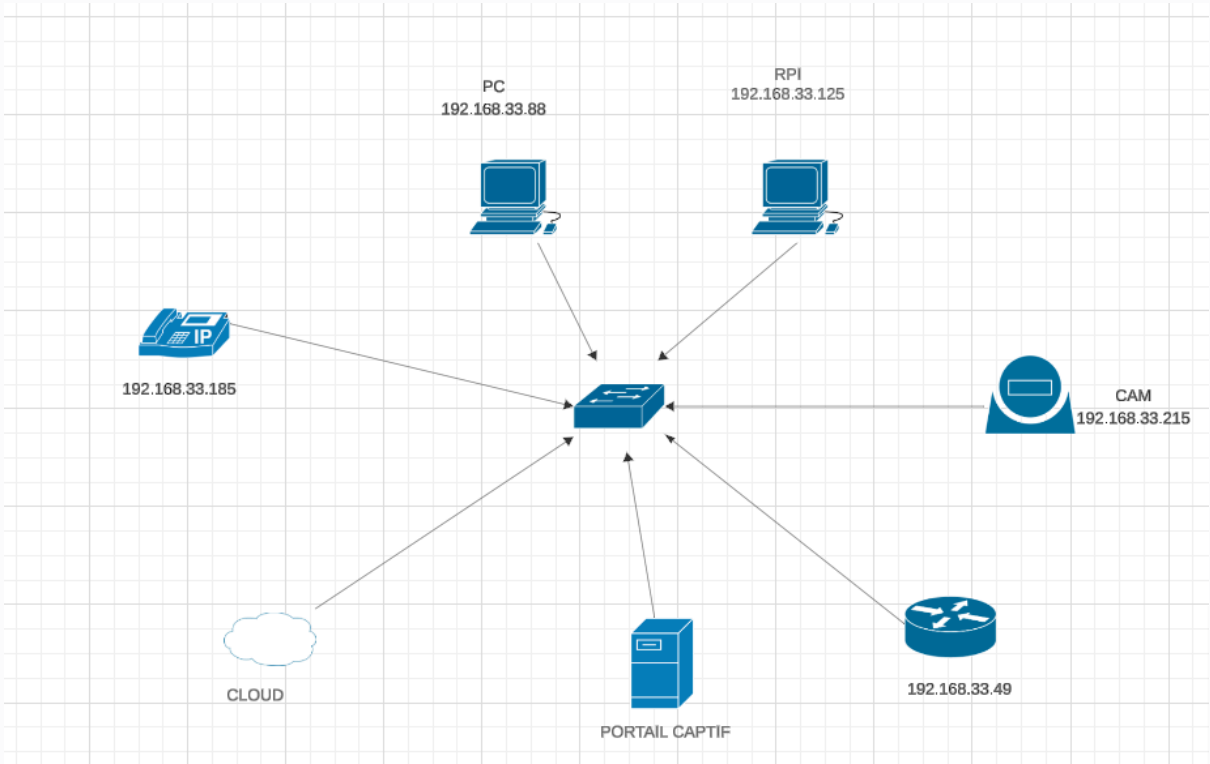
Procédure installation et utilisation Nmap

- Mettre à jour les paquets :
Exécutez la commande `sudo apt update` pour mettre à jour la liste des paquets disponibles.
- Installer Nmap :
Utilisez la commande suivante pour installer Nmap :
`sudo apt install nmap`.
- Vérifier l'installation :
Une fois installé, vérifiez la version de Nmap avec :
`nmap --version`.
- Scan d'une IP spécifique :
Pour scanner une adresse IP dans le sous-réseau `192.168.33.0/24`, utilisez :
`nmap 192.168.33.1`.
- Scan de tout le sous-réseau :
Pour scanner toutes les adresses du réseau `192.168.33.0/24` :
`nmap 192.168.33.0/24`.
- Scan de ports spécifiques :
Pour scanner des ports particuliers sur `192.168.33.1` :
`nmap -p 22,80 192.168.33.1`.
- Scan furtif (SYN scan) :
Pour effectuer un scan furtif (SYN scan) sur `192.168.33.1` :
`nmap -sS 192.168.33.1`.
- Détection de version des services :
Pour identifier les versions des services sur `192.168.33.1` :
`nmap -sV 192.168.33.1`.
- Scan de l'OS de la cible :
Pour détecter le système d'exploitation sur `192.168.33.1` :
`nmap -O 192.168.33.1`.
- Scan complet avec découverte d'OS et services :
Pour effectuer un scan complet (services et OS) sur le réseau `192.168.33.0/24` :
`nmap -A 192.168.33.0/24`.

7.12

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

figure (43)



7.13

Copie de l’agenda hebdomadaire réactualisé

figure 44)

	(1h)		
3	2 Le PC fixe est connecté au réseau de l'IUT et il accède sur l'extérieur : (1h)	1	1
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
11	10 Etude énergétique	1	1
12	11 Présentation finale: oral de 15mn en binôme	1	1
Total tâches		11	11

