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	rstp
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)

Chapter 1 Product Overview

Chapter 1: Product Overview

Thank you for choosing the Linksys Wireless-G Broadband Router. The Router lets you access the Internet via a wireless connection, broadcast at up to 54 Mbps, or through one of its four switched ports. You can also use the Router to share resources such as computers, printers and files. A variety of security features help to protect your data and your privacy while online. Security features include WPA2 security, a Stateful Packet Inspection (SPI) firewall and NAT technology. Configuring the Router is easy using the provided browser-based utility.

Front Panel

SecureEasySetup (Orange/White) The Cisco logo is the Router's SecureEasySetup button. It lights up and will stay orange when the Router is powered on. The color orange indicates that the Router is not using the SecureEasySetup feature, while the color white indicates that the Router is using the SecureEasySetup feature. When the Router enters SecureEasySetup mode, the Cisco logo will turn white and start flashing. After the Router has generated the SSID and WPA Personal key, the Cisco logo will stop flashing and stay white.

To clear the SSID and WPA Personal key, press and hold down the Cisco logo for five seconds. The Cisco logo will flash slowly as the Router resets itself. The Cisco logo will turn orange to indicate a successful reset.

NOTE: SecureEasySetup is a feature that makes it easy to set up your wireless network. If you have SecureEasySetup devices, run the Router's Setup Wizard CD-ROM and follow the on-screen instructions to use SecureEasySetup.

Power (Green) The Power LED lights up and will stay on while the Router is powered on. When the Router goes through its self-diagnostic mode during every boot-up, this LED will flash. When the diagnostic is complete, the LED will be solidly lit.

DMZ (Green) The DMZ LED indicates when the DMZ function is being used. This LED will remain lit as long as DMZ is enabled.

WLAN (Green) The WLAN LED lights up when the wireless feature is enabled. If the LED is flashing, the Router is actively sending or receiving data over the network.

1, 2, 3, 4 (Green) These numbered LEDs, corresponding with the numbered ports on the Router's back panel, serve two purposes. If the LED is continuously lit, the Router is successfully connected to a device through that port. A flashing LED indicates network activity over that port.

Internet (Green) The Internet LED lights up when there is a connection made through the Internet port. A flashing LED indicates network activity over the Internet port.

Back Panel

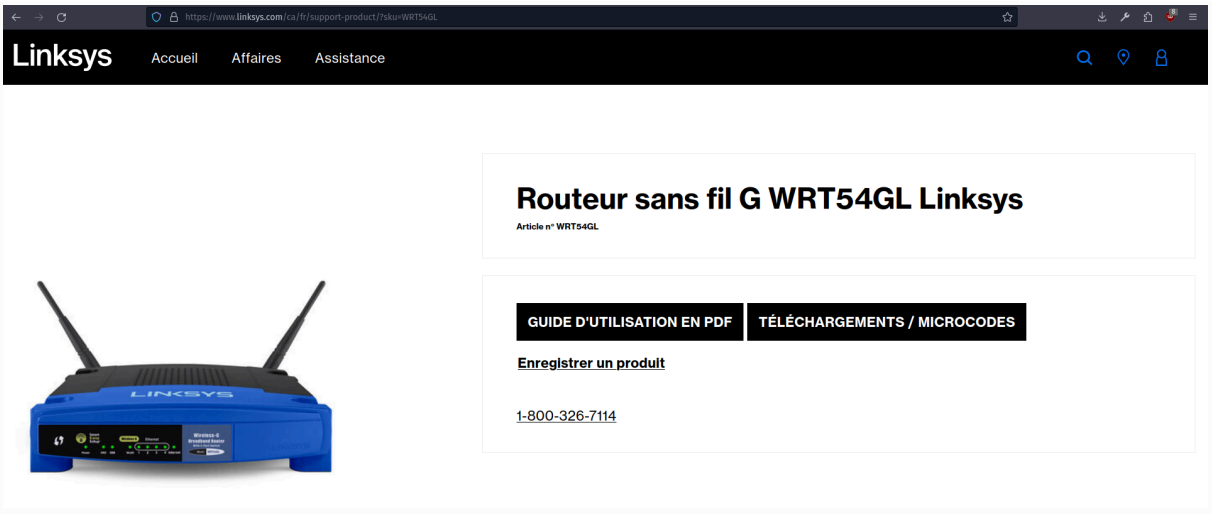
Reset There are two ways to reset the Router's factory defaults. Either press and hold the Reset Button for approximately five seconds, or restore the defaults from Administration > Factory Defaults in the Router's web-based utility.

Internet The Internet port is where you will connect your cable or DSL Internet connection.

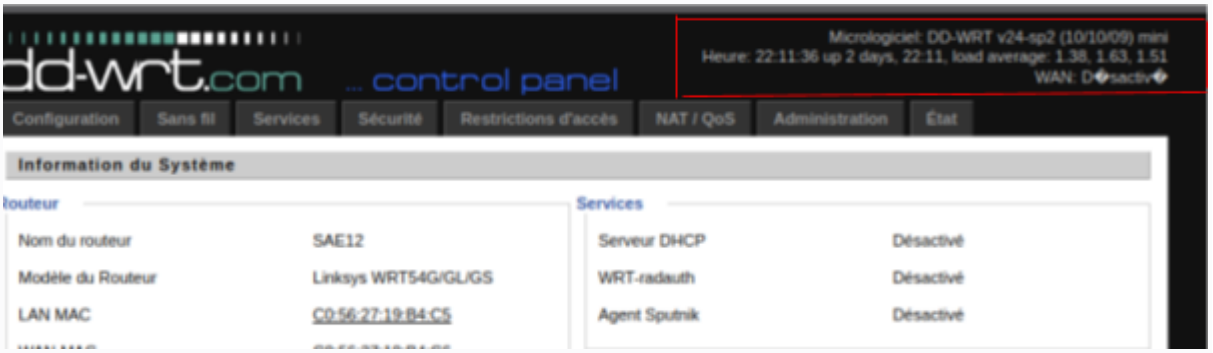
1, 2, 3, 4 These Ethernet ports (1, 2, 3, 4) connect the Router to PCs on your wired network and other Ethernet network devices.

Power The Power port is where you will connect the power adapter.

figure(33)



figure(34)

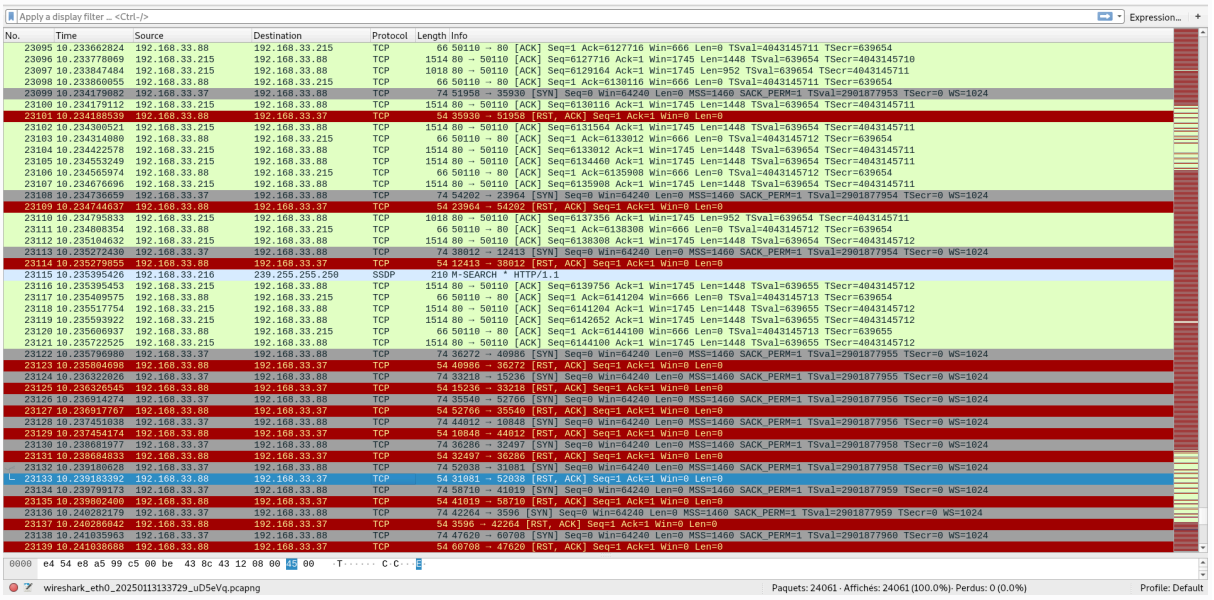


rouge = horaire

7.5

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

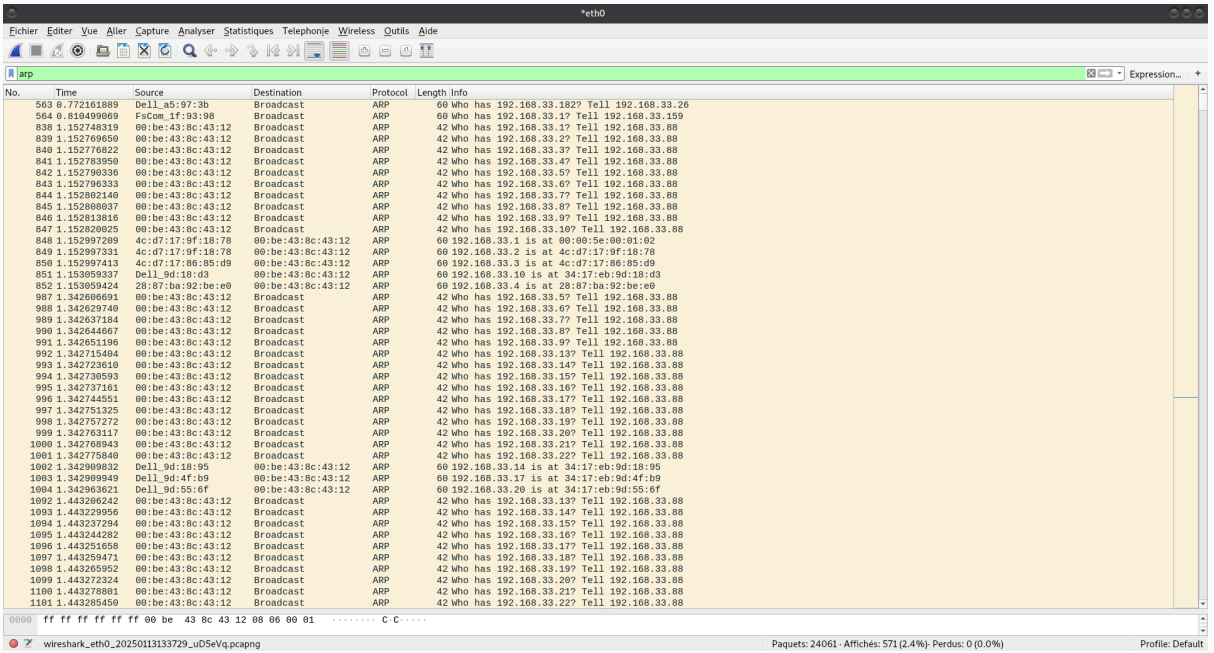
figure (35)



7.6

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

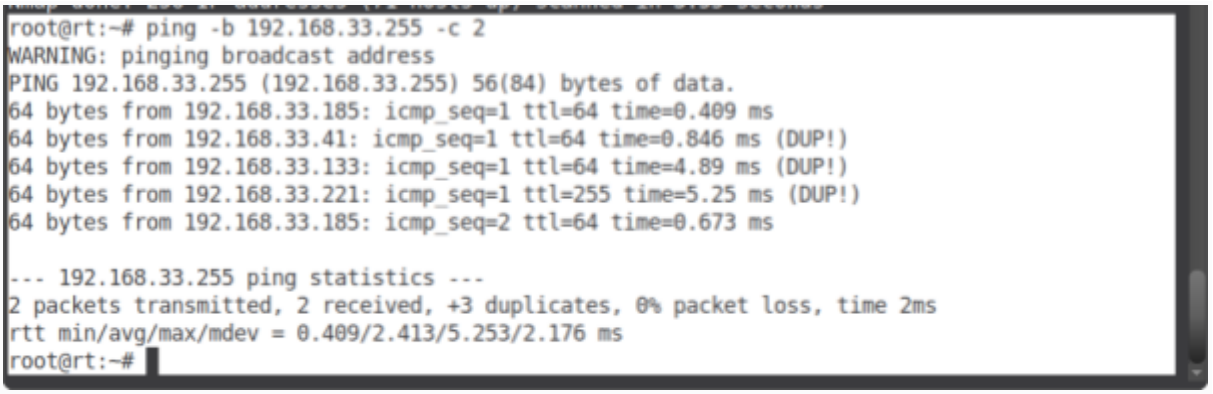
figure (36)



7.7

Copie d’écran des réponses des différents broadcast.

figure (37) avec la commande ping -b 192.168.33.255 -c 2



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)

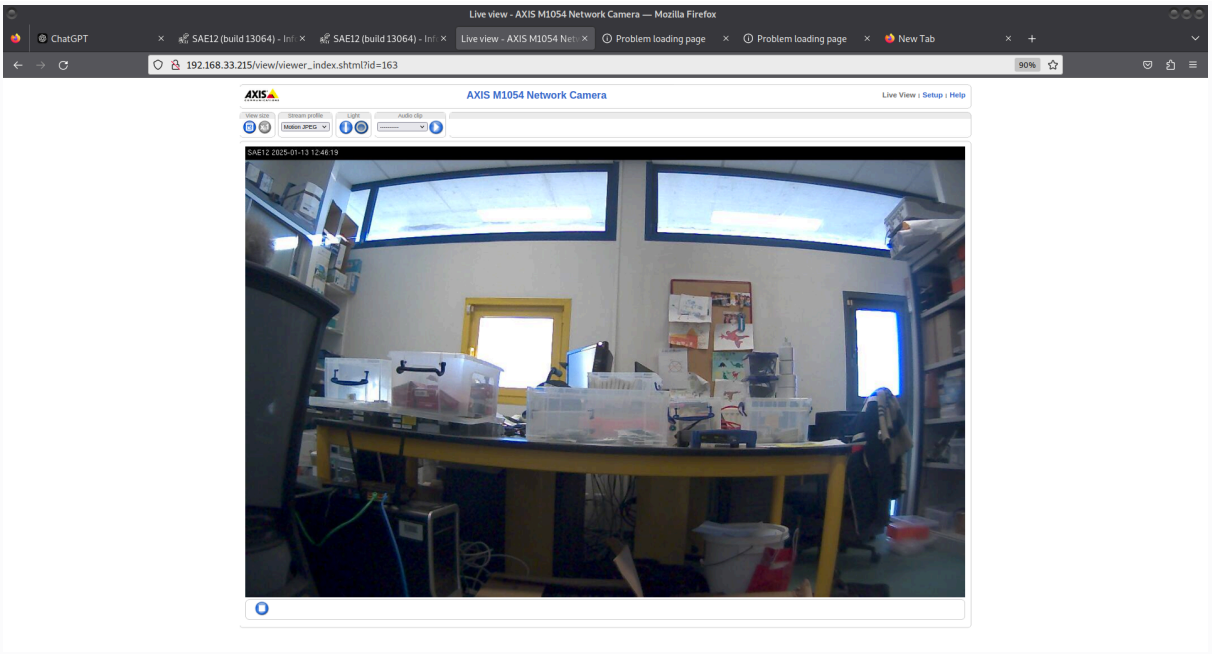


figure (39) Pour le routeur

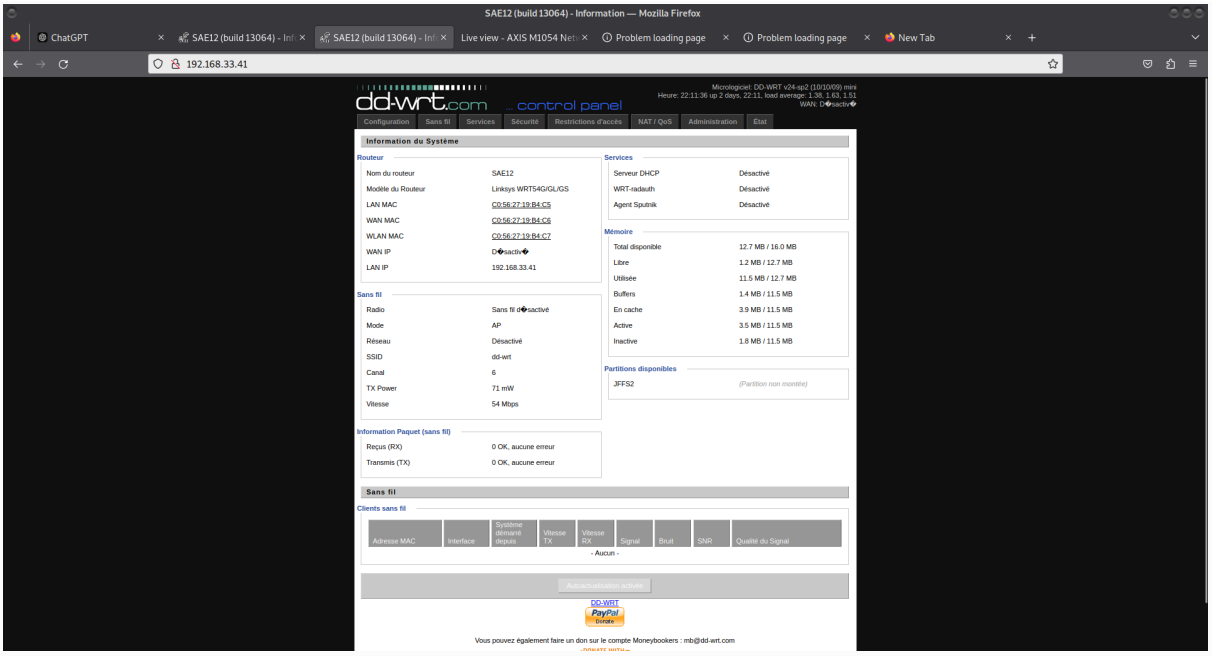


figure 40)Pour le téléphone (192.168.33.185)

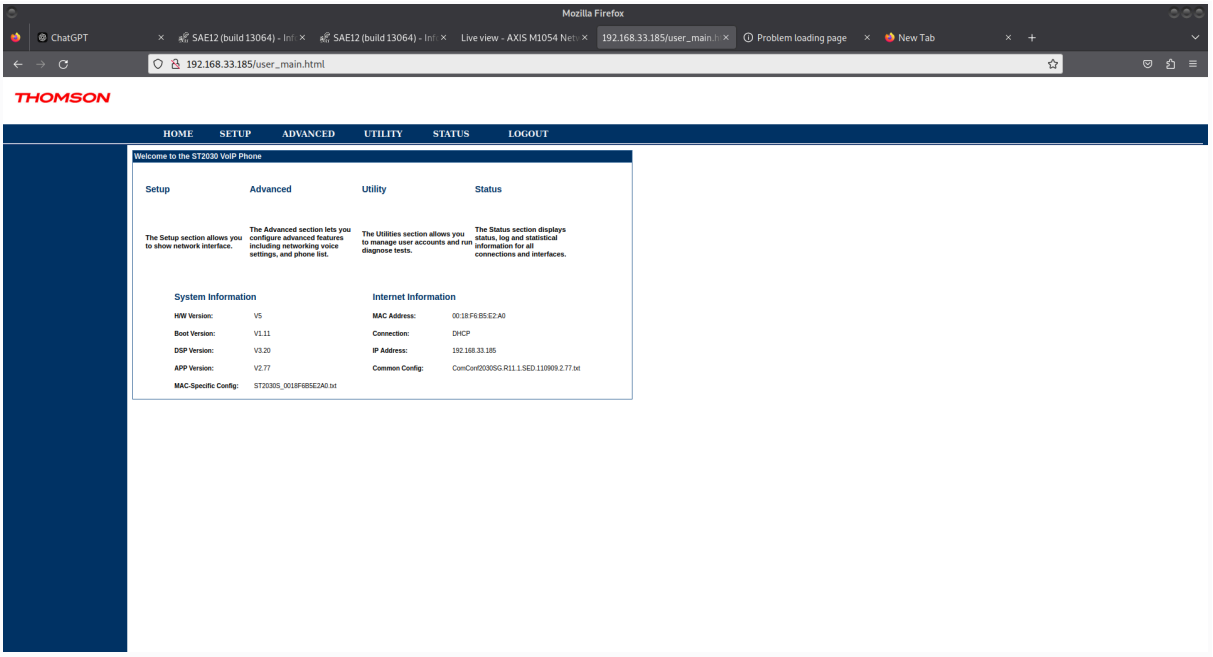
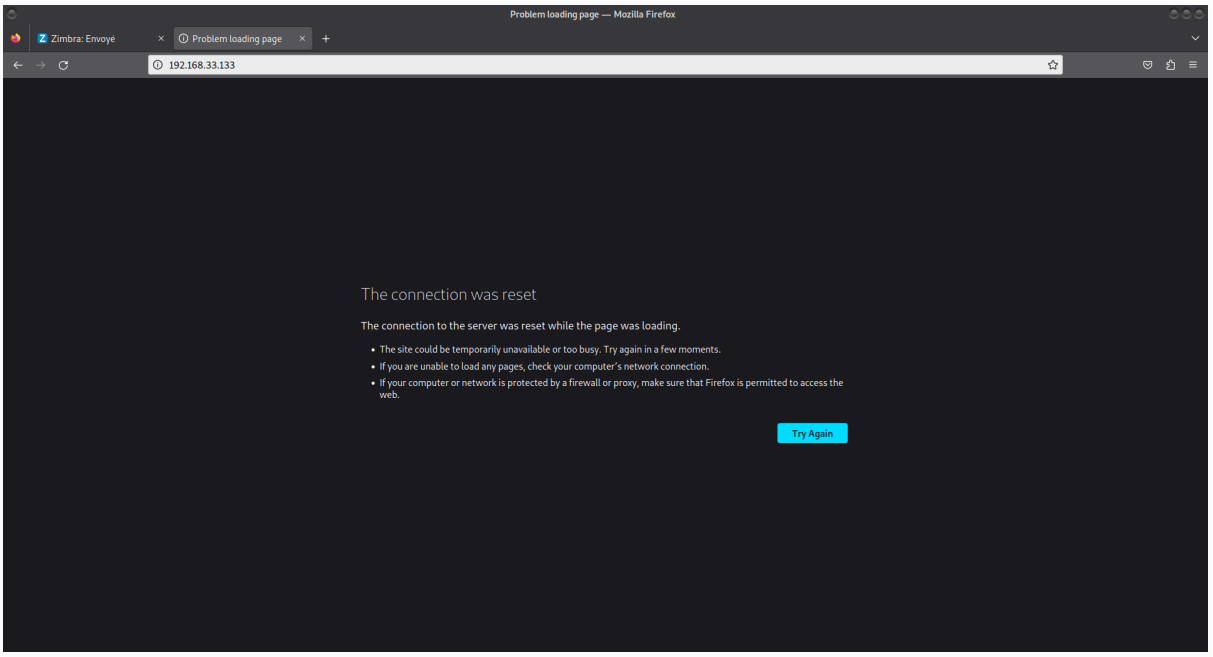
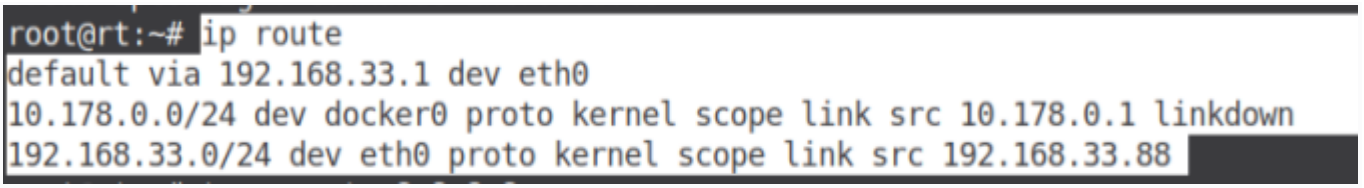


figure 41) pour le serveur multimedia (192.168.33.133)



7.9
IP Passerelle
figure 42) réalisé avec la commande ip route



7.10
IP réseau salle
comme le masque c'est 255.255.255.0 l'adresse ip réseau salle est 192.168.33.0

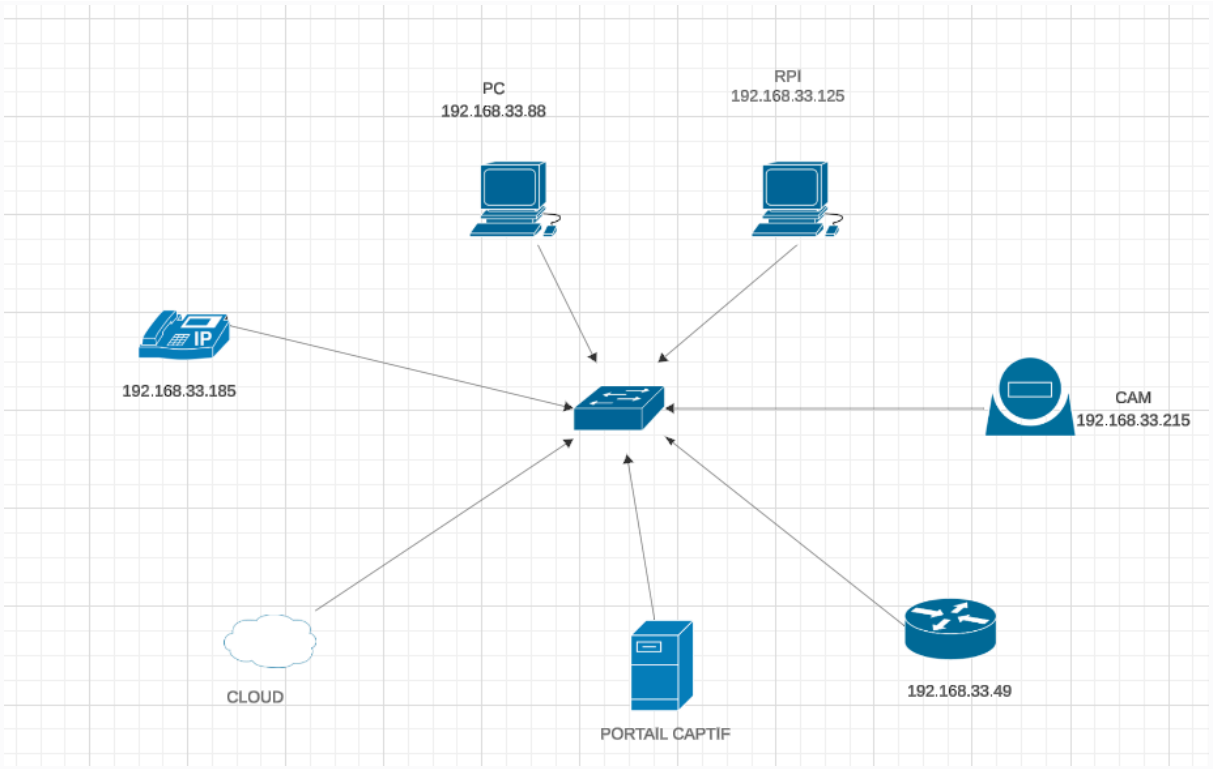
7.11
Procédure installation et utilisation Nmap

- 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