

SAE 1.2

S'initier aux réseaux informatiques



Sébastien Couderc

IUT de Poitiers – Site de Châtellerault

Département Réseaux et Télécoms

2023 - 2024

Table des matières

| | |
|---|-----------|
| Introduction..... | 3 |
| Présentation du sujet | 4 |
| Organisation de la SAE..... | 4 |
| Partie 1: Découverte du réseau domestique..... | 6 |
| 1. Moyens d'accès à Internet | 6 |
| 1.1. Etude du lien internet vers le fournisseur d'accès (FAI)..... | 6 |
| 1.2. Evaluation de la latence du réseau..... | 7 |
| 1.3. Etude de la connectique de la Box | 9 |
| 2. Outils pour caractériser le réseau | 10 |
| 2.1. Etude de la configuration des périphériques finaux | 10 |
| 2.1.1. Recherche de la configuration de l'ordinateur sous Windows | 10 |
| 2.1.2. Recherche de la configuration du smartphone sous Android..... | 12 |
| 2.2. Recherche d'informations complémentaires sur le réseau | 13 |
| 2.2.1. Recherche des caractéristiques de la liaison Wi-Fi | 13 |
| 2.2.2. Recherche d'informations sur de la liaison WAN et le FAI..... | 14 |
| 2.3. Recherche des services installés..... | 16 |
| 2.4. Schémas de la topologie du réseau..... | 17 |
| Partie 2: Installation d'un réseau domestique sous Packet Tracer..... | 18 |
| 1. Construire un réseau domestique sous Packet Tracer..... | 18 |
| 1.1. Topologie | 18 |
| 1.1. Installation du routeur sans fil et utilisation avec les paramètres par défaut | 18 |
| 1.1.1. Câblage des équipements | 18 |
| 1.1.2. Configuration des périphériques finaux..... | 18 |
| 1.2. Configuration du routeur sans fil | 19 |
| 1.2.1. Modification des paramètres d'adressage..... | 19 |
| 1.2.2. Modification des paramètres du réseau sans fil | 20 |
| 1.3. Configuration des hôtes | 20 |
| 2. Analyse protocolaire..... | 21 |
| Partie 3: Déploiement d'un réseau informatique et mise en place d'un service de vidéo surveillance ... | 24 |
| 1. Topologie du réseau | 24 |
| 1.1. Le réseau de l'opérateur | 24 |
| 1.2. Le réseau du particulier | 25 |
| 1.3. Les services de l'opérateur | 25 |
| 2. Matériel | 25 |
| 3. Travail à réaliser | 26 |
| 3.1. Configuration des équipements du réseau local..... | 26 |

| | | |
|---|--|-----------|
| 3.2. | Mise en place d'un site web de vidéosurveillance | 26 |
| 3.3. | Accéder au flux vidéo de la caméra IP depuis Internet..... | 27 |
| Partie 4: Annexes..... | | 28 |
| Progression pédagogique – SAE1.2 « S'initier aux réseaux informatiques » | | 28 |

SAE1.2 – S’initier aux réseaux informatiques

Objectifs et problématique professionnelle

Dans cette SAÉ vous serez confronté à la découverte et à la mise en œuvre d’un premier réseau informatique. Vous appréhendez la diversité de ses constituants et vous serez amenés à comprendre leurs interactions. Les phases de recherche et d’analyse de l’existant sont nécessaires avant toute intervention sur un élément constitutif d’un réseau informatique. Cette démarche constitue le quotidien d’un technicien réseau.

Introduction

Les réseaux et Internet ont modifié notre façon de communiquer, d’apprendre, de travailler et de nous divertir. Ils peuvent être dessinés pour une utilisation locale, à l’échelle d’une ville, d’un pays ou à l’international. Ils sont répartis en 3 catégories :

- Les réseaux domestiques ou les petits réseaux de bureau représentent l’installation traditionnelle d’une habitation connectée à Internet. Ils relient quelques ordinateurs et périphériques sans fil entre eux et à Internet par l’intermédiaire d’une Box (CPE). Cet équipement intègre à minima un modem ou adaptateur, un commutateur, un point d’accès Wifi, un routeur et un pare-feu logiciel. La connexion à Internet s’effectue dans la majorité des cas grâce une technologie dite « cuivre » comme l’ADSL ou « fibre » comme le FTTH mais il existe aussi d’autres technologies pour relier l’usager à Internet.
- Les moyens et grands réseaux représentent des installations d’entreprises, reliées ou non à Internet et qui peuvent être déployées sur un seul site (Siège social) ou sur plusieurs sites (siège social et filiales). Les équipements réseau d’entreprise sont sécurisés, redondants et résilients pour assurer la continuité de service. Les employés peuvent se connecter au réseau filaire ou sans fil, selon la politique de sécurité de l’entreprise. Ils ont généralement la possibilité de se connecter depuis chez eux au réseau interne de l’entreprise via une technologie nommée VPN (Virtual Private Network).
- Les réseaux mondiaux sont des architectures qui s’étendent sur toute la surface du globe et permettent la communication internationale. Internet est littéralement un ensemble de réseaux privés et publics interconnectés, tels que ceux décrits ci-dessus.

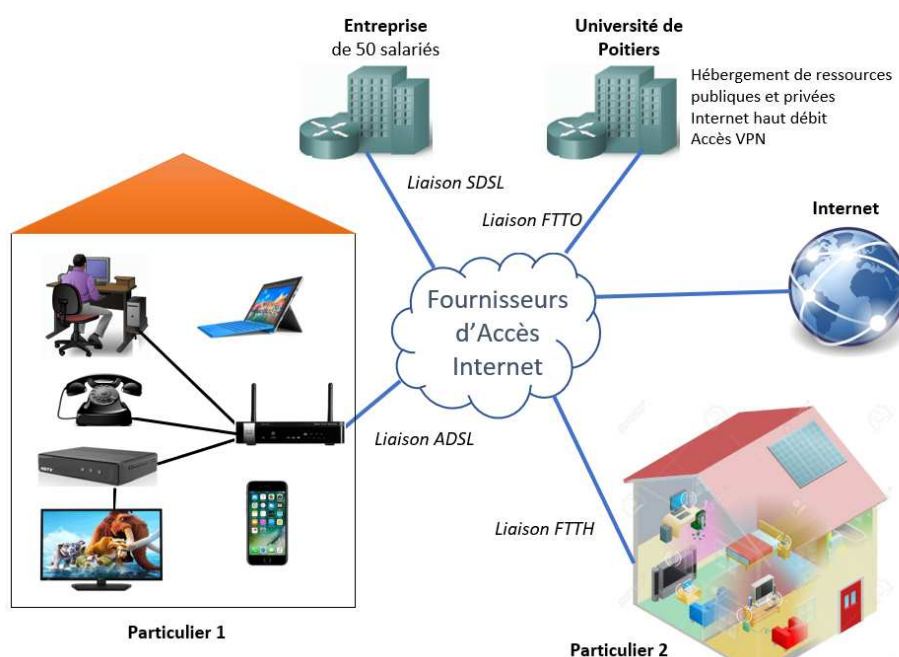


Fig 1 : Architecture globale du réseau étendu

Présentation du sujet

Le but de cette activité est de découvrir votre réseau informatique domestique. Vous allez en extraire les principales données techniques, les analyser afin de produire un schéma de la topologie physique et de la topologie logique. Vous utiliserez des applications web, des logiciels spécifiques à installer sur votre ordinateur et sur votre smartphone et les commandes de base fournies avec le système d'exploitation afin de consulter, configurer et établir des diagnostics sur les périphériques finaux installés dans votre réseau. Vous serez également amenés à vérifier des éléments de sécurité informatique de votre réseau.

Dans un deuxième temps, vous devrez installer et configurer un réseau domestique sous Packet Tracer. Une fois le réseau fonctionnel, vous simulerez un échange entre un ordinateur du réseau et un serveur de l'internet afin de comprendre comment sont réalisés les échanges d'information et vous en déduirez la modélisation en couche de cet échange.

Enfin, vous construirez un réseau domestique en salle de TP. Vous installerez les différents équipements, vous les configurerez et les sécuriserez. Vous ajouterez à votre réseau domestique une surveillance vidéo accessible via une page web depuis un réseau externe comme Internet.

Organisation de la SAE

Voici le planning prévisionnel du travail demandé pour cette SAE.

| Partie 1 – Découverte du réseau domestique | | | |
|--|----------|---|--|
| Séances | Type | Description | Outils / Ressources |
| S1 (1h) | CM | Présentation de la SAE | |
| S2 (2h) | TP NE | Recherche des différents moyens permettant à un particulier d'accéder à Internet. Utilisation d'un outil pour caractériser la liaison WAN (débit, latence ...) et la comparer à d'autres technologies disponibles à votre adresse Evaluation de la couverture du réseau d'accès FTTH à votre adresse Evaluation de la latence du réseau à la manière de Degrouptest.com Rédaction d'un compte-rendu | degrouptest.com cartefibre.arcep.fr ping, tracert |
| S3 (2h) | TP NE | Etude de la connectique de la Box Réalisation d'un schéma de la topologie physique | Guide d'utilisation de la Box lucidchart.com app.diagrams.net |
| S4 (2h) S5 (2h) | TP NE | Utilisation d'outils de diagnostics (sous Windows, Android, web) pour caractériser le réseau domestique (adressage MAC, IPv4 statique / dynamique, masque de sous-réseau, préfixe réseau, passerelle par défaut, serveurs DNS, adresse IP privée et publique, localisation IP, service DHCP, test de débit, canaux WiFi, méthode d'authentification...) Consigner les différents résultats de diagnostics dans un tableau. | Environnement PowerShell Terminal Emulator for Android Net Analyser for Android inSSIDer www.monip.org ip.lafibre.info www.hostip.fr www.iana.org/numbers www.ripe.net What_is_the_RIPE_NCC.mp4 |

| | | | |
|---|-------------|---|--|
| | | | apps.db.ripe.net/db-web-ui/query dnschecker.org nmap.org nmap.org/man/fr nmap.org/man/fr/man-briefoptions.html |
| S6 (1h30) | TD | Analyse des résultats obtenus et réalisation d'un schéma de la topologie complètement renseigné Evaluation du travail réalisé | app.diagrams.net |
| Partie 2 – Installation d'un réseau domestique sous Packet Tracer et analyse des couches protocolaires | | | |
| Séances | Type | Description | Outils / Ressources |
| S7 (2h) | TP NE | Installation d'un réseau domestique sous Packet Tracer Configuration du routeur sans fil avec les paramètres fournis afin d'assurer un accès filaire et sans fil Modélisation du réseau domestique Mise en évidence du principe d'encapsulation Analyse protocolaire Modélisation d'un échange entre deux périphériques | Packet Tracer |
| S8 (1h30) | TD | Réalisation d'un schéma modélisant un échange entre deux périphériques Introduction à l'analyse de flux réseau avec Wireshark | |
| Partie 3 – Déploiement d'un réseau informatique et mise en place d'un service de vidéo surveillance | | | |
| Séances | Type | Description | Outils / Ressources |
| S9 (2h) | TP NE | Etude du cahier des charges en vue de déployer un réseau domestique dans la salle de TP Conception du réseau : adressage IP, plage DHCP, SSID, méthode d'authentification Services à mettre en place : service de vidéo surveillance | Wireshark |
| S10 (3h) | TP | Déploiement du réseau filaire et sans fil Mise en place d'une caméra de vidéo surveillance | Cisco RV215W Caméra IP D-Link / Axis |
| S11 (3h) | TP | Mise en place du service de vidéo surveillance sur le serveur HTTP du FAI Capture du flux video avec Wireshark et identification des couches selon le modèle OSI. Capture du flux lors de l'authentification au service de vidéo surveillance non sécurisé et explantation pour retrouver les identifiants de l'utilisateur Evaluation : Démonstration du fonctionnement / Explications / Questions orales / QCM | Wireshark |

Partie 1: Découverte du réseau domestique

1. Moyens d'accès à Internet

Dans cette partie, vous allez étudier le moyen qui vous permet d'accéder à Internet, caractériser le réseau étendu par des tests de débit et de latence et étudier la connectique de votre Box. Le but étant de réaliser le schéma de la topologie physique de votre réseau domestique.

1.1. Etude du lien internet vers le fournisseur d'accès (FAI)

Généralement, c'est la « Box internet » qui permet de connecter le réseau local du particulier à Internet. A l'aide du site DegroupTest.com, faites des recherches et lancer des tests pour répondre aux questions suivantes :

Q1. Se rendre sur le site <https://www.degrouptest.com/>, réaliser des recherches et lancer des tests pour répondre aux questions suivantes :

- 1) Quelles sont les différentes technologies utilisées pour connecter le réseau local d'un particulier à Internet ?
- 2) Quel est la technologie utilisée à votre domicile ? Etes-vous éligible à d'autres technologies de connexion ? Si oui, lesquelles ? Si non, pourquoi ?
- 3) Quels sont les opérateurs nationaux pouvant raccorder un particulier à Internet ? Quel est le vôtre ?

Q2. Utiliser le site DegroupTest.com pour réaliser des tests de performance de votre liaison WAN

- 1) Quelles sont les performances de votre liaison Internet ? Compléter le tableau suivant :

| Opérateur | Technologie de connexion | Débit descendant | Débit montant | Latence | Gigue |
|-----------|--------------------------|------------------|---------------|---------|-------|
| | | | | | |

- 2) Est-ce que la technologie utilisée pour votre liaison Internet est dite « symétrique » ou « asymétrique » ?
- 3) Pourquoi 2 tests de débit réalisés à quelques minutes d'intervalle peuvent fournir des résultats différents ?
- 4) Combien de temps faut-il pour télécharger un film en haute résolution de 440 Mio avec votre liaison internet ?

Q3. Utiliser le site DegroupTest.com et le site de l'ARCEP pour définir ce qu'est le débit minimal requis pour un particulier et ce que l'on appelle le « Très Haut débit »

- 1) Quel est le débit minimal requis pour surfer sur internet, relever ses mails ou encore regarder la TV via la box du FAI ? Est-il suffisant pour visualiser un film en 4K sur son téléviseur connecté ?
- 2) Qu'est-ce que le « Très Haut Débit » ? A partir de quelle valeur de débit parle-t-on de très haut débit ? Quelles sont les technologies qui permettent d'obtenir un très haut débit ?

Q4. Se rendre sur le site <https://cartefibre.arcep.fr/> pour relever des informations concernant la connexion FTTH actuelle (vous avez un abonnement), possible (vous pouvez vous abonner mais vous avez conservé une autre technologie) ou en cours de déploiement (vous pourrez en bénéficier plus tard) à l'adresse de votre logement.

- 1) Quel est l'état de couverture du réseau d'accès FTTH à votre adresse ?
- 2) Quels sont les opérateurs qui peuvent vous fournir un accès fibre à votre adresse ?
- 3) Quels sont les plages de débits théoriques montant et descendant proposés à votre adresse ?
- 4) Quelles sont les autres technologies pour lesquelles votre logement est éligible ? Quels sont les opérateurs ?

1.2. Evaluation de la latence du réseau

Dans cette partie, vous allez mesurer et évaluer la latence du réseau à différents moments de la journée (matin et après-midi par exemple) afin d'obtenir des données représentatives de l'activité sur le réseau. Pour cela, vous analyserez le délai de retour d'un serveur distant à l'aide de la commande `ping`. Les valeurs de ces délais mesurés seront ensuite copiées dans un tableur (Excel ou autre) pour être interprétés facilement.

Il faut choisir un serveur suffisamment éloigné pour que la mesure de la latence soit significative. Nous utiliserons le serveur www.google.fr. La commande `tracert` sera également utilisée pour afficher l'itinéraire emprunté par les paquets entre votre ordinateur et le serveur. Chaque ligne affichée correspond à un routeur qui a été traversé.

Q5. Exécuter la commande `tracert www.google.fr` dans un terminal sous Windows.

- 1) Combien de routeurs ont été traversés pour atteindre la destination ?
- 2) Pensez-vous que cela soit suffisant pour faire des mesures de latences ? Pourquoi ?

La commande `ping` sera utilisée pour documenter la latence du réseau. Vous pouvez obtenir de l'aide sur cette commande en utilisant `ping /?`.

Q6. Vérifier la connectivité entre votre ordinateur et celle du serveur distant en utilisant la commande `ping -n 1 www.google.fr`.

- 1) Le test a-t-il réussi ?
- 2) Quelles sont les fonctions de l'option `-n` et de l'argument `1` ?
- 3) Quelle option et quel argument permettent de définir la taille par défaut sur 100 octets ?
- 4) Relancer le test et vérifier le résultat affiché par la commande. Combien de paquets ont été envoyés ? Combien ont été reçus ? Combien d'octets ont été envoyés ?

Nous allons poursuivre en réalisant un test de latence à la manière du site DegroupTest. Pour cela, vous allez construire une commande `ping` qui permet d'envoyer 100 requêtes Echo Request de 100 octets de données et rediriger les résultats de la commande vers un fichier `data_latence.txt`. Pour cela, il faut rajouter `> data_latence.txt` à la suite de la commande `ping`. Ensuite, vous éditez un graphique à l'aide du tableur Excel ou Calc (LibreOffice).

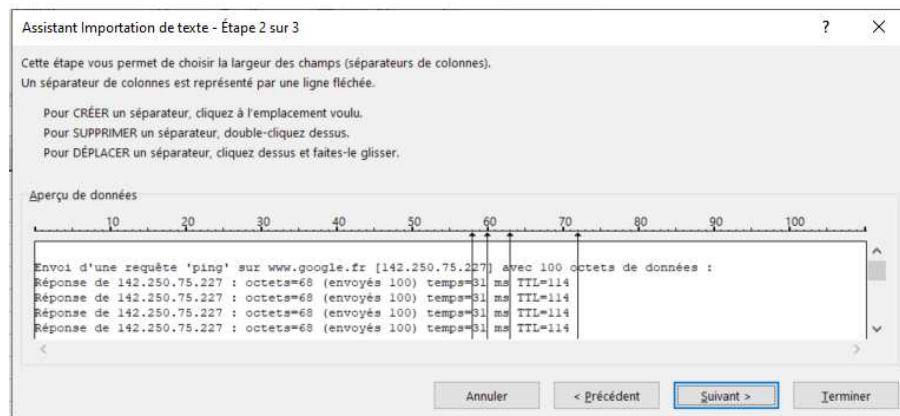
Q7. Lancer la commande `ping` afin d'envoyer 100 requêtes Echo de 100 octets vers le serveur distant. Cela peut durer quelques minutes.

- 1) Quelle commande `ping` avez-vous saisie (option, argument, redirection) pour envoyer les requêtes et récupérer les réponses dans un fichier ?
- 2) Est-ce que les résultats apparaissent à l'écran ? Pourquoi ?
- 3) Est-ce que le fichier `data_latence.txt` contient les résultats de la commande `ping` ?

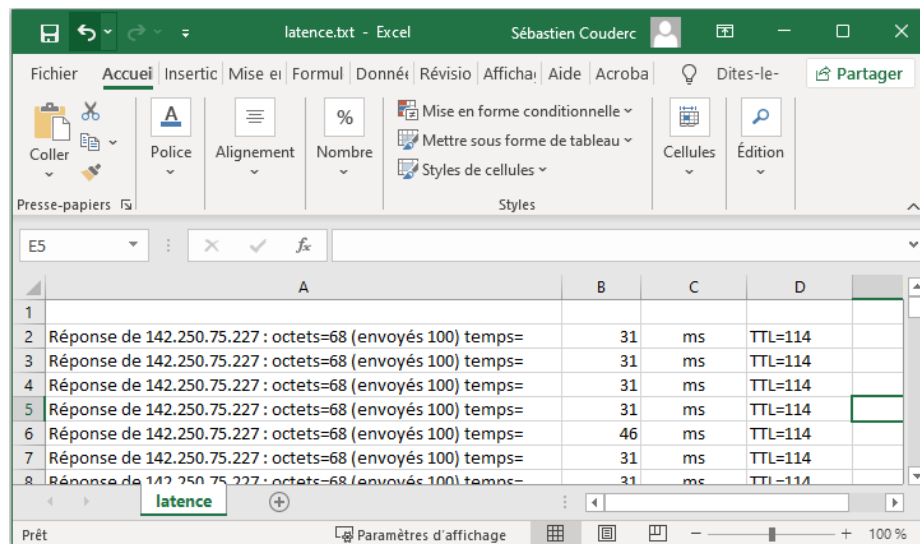
Q8. Lancer le tableur Microsoft Excel ou autre puis ouvrir le fichier `data_latence.txt`. Un assistant d'importation du texte va vous permettre de formater votre fichier pour le rendre exploitable par le tableur. Ensuite, suivre les étapes suivantes de l'assistant :

- Etape 1 : Sélectionnez « Largeur fixe » puis cliquez sur « Suivant »

- Etape 2 : Suivez les instructions pour placer les curseurs afin de séparer les valeurs numériques du texte puis cliquez sur « Suivant »



- Etape 3 : Choisissez un format de colonne « Standard » puis cliquez sur « Terminer »



- Etape 4 : Calculez la latence moyenne en utilisant la formule =MOYENNE(B2:B84)
- 1) Est-ce que votre résultat correspond approximativement à celui indiqué par la commande ?
 - 2) Comment exprimer la valeur de la latence la plus fréquente dans la plage de données (valeur modale) ? Quelle est sa valeur ?

Nous allons poursuivre et se demander si l'envoi de requêtes Echo contenant de plus en plus de données influent sur la latence du réseau. Pour cette analyse, vous enverrez 20 requêtes Echo et chaque requête sera incrémentée de 100 octets de données.

Le plus simple consiste à utiliser la commande de boucle FOR de Windows. La syntaxe est la suivante : `FOR /L %%variable IN (début,pas,fin) DO commande [paramètres]`

L'ensemble est une séquence de chiffres allant de début à fin, incrémenté de pas. Ainsi (1, 1, 5) génère la séquence 1 2 3 4 5 et (5, -1, 1) génère la séquence 5 4 3 2 1.

Les résultats de la commande seront redirigés vers le fichier `data_variable_latence.txt`. Pour cela, il faut rajouter le symbole de redirection `>>` suivi du nom du fichier `data_variable_latence.txt` à la suite de la commande `ping`. Remarque : l'opérateur de redirection normal (`>`) écrase le fichier à chaque exécution de la commande `ping`.

Q9. A l'aide des informations sur la boucle FOR, compléter la commande `FOR /L %i IN (debut,pas,fin) DO ping -n 1 -l %i www.google >> data_variable_latence.txt` en indiquant les valeurs de *début*, *pas* et *fin* puis exécuter cette commande dans le terminal (cmd) de Windows.

Q10. Ouvrir le fichier avec l'assistant d'importation, placer les curseurs pour isoler les valeurs numériques des durées et calculer la valeur moyenne de la latence. Si vous avez du temps, vous pouvez aussi réaliser un graphique avec en abscisse la taille du datagramme envoyé et en ordonnée la latence.

- 1) Quelle est la valeur moyenne de la latence ?
- 2) Comment évolue la latence en fonction de la taille des requêtes Echo ?

1.3. Etude de la connectique de la Box

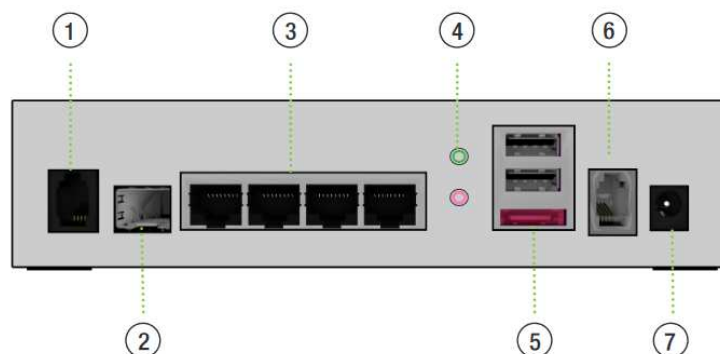
La Box internet est un équipement qui intègre différents périphériques intermédiaires et notamment un routeur qui permet d'interconnecter le réseau local privé de l'utilisateur au réseau public internet.

Dans cette partie, il s'agit de détailler les différentes fonctionnalités de votre Box ainsi que les différents ports physiques sur lesquels sont raccordés les périphériques. L'idéal serait de télécharger le guide d'utilisation de votre Box et de vous y référer.

Q11. Réaliser l'inventaire des périphériques finaux présents dans votre réseau local domestique. Quels sont les périphériques intermédiaires qui réalisent leur connexion ? Quels types de supports sont utilisés ? A quels ports sont-ils connectés (cas des connexions filaires) ?

Q12. Quel est l'équipement intermédiaire qui permet d'interconnecter le réseau local (LAN) et le réseau étendu (WAN) ? Quel support est utilisé pour la liaison avec le FAI ? Quel port physique est utilisé ? Quelle est la nature des informations (électrique, lumineuse, onde radio) véhiculées sur le support ?

Voici la connectique standard que l'on trouve généralement sur une Box.



Q13. Télécharger la documentation de votre Box et compléter le tableau suivant :

| Repère | Rôle des ports | Technologie | Support | Connecteur |
|--------|--|-------------|---------|------------|
| | Raccordement au réseau du FAI | | | |
| | Raccordement d'un équipement numérique et / ou d'un périphérique de stockage | | | |

| | | | | |
|--|--|--|--|--|
| | Raccordement des PC | | | |
| | Raccordement du téléphone | | | |
| | Raccordement au bloc d'alimentation secteur | | | |
| | Raccordement d'un casque ou d'un lecteur audio | | | |

Q14. Dans quel cas utilise-t-on des boîtiers de courants porteurs en ligne (CPL) ?

Q15. Si vous disposez d'un « Player TV » (une Set-top Box), précisez comment ce boîtier est relié à la Box TV.

Q16. A l'aide de l'application en ligne <https://www.lucidchart.com> ou <https://app.diagrams.net/> et de la bibliothèque « Network », réaliser le schéma de la topologie physique de votre réseau domestique. Demandez-vous quelles sont les informations qui doivent apparaître sur la topologie physique. Vous ferez apparaître tous les périphériques finaux et intermédiaires ainsi que la connexion WAN. La Box sera représentée par un seul périphérique. Vous indiquerez à minima le nom des équipements et des ports utilisés.

2. Outils pour caractériser le réseau

A ce stade, vous avez connaissance de la topologie physique de votre réseau. Dans cette partie, vous allez utiliser des outils de diagnostics afin de relever les paramètres de configuration de vos périphériques finaux et les différents services applicatifs accessibles sur votre réseau.

2.1. Etude de la configuration des périphériques finaux

L'ordinateur, la tablette ou encore le smartphone doivent être connectés au réseau local. Les commandes de diagnostics peuvent être différentes selon le système d'exploitation utilisé. Dans cette partie, l'ordinateur est doté d'un système d'exploitation Windows et tablette / smartphone sont équipés d'un système d'exploitation Android. Si vous utilisez un autre système, recherchez des outils équivalents ou demandez à votre enseignant.

2.1.1. Recherche de la configuration de l'ordinateur sous Windows

Il existe différentes commandes sous Windows pour afficher les paramètres de la connexion réseau de l'ordinateur. En TP, vous avez utilisé la commande `ipconfig` dans l'invite de commandes. Dans cette SAE, vous utiliserez l'interpréteur de commandes PowerShell (<https://docs.microsoft.com/fr-fr/powershell/scripting/overview?view=powershell-7.1>) et les commandes de ce langage de script pour déterminer les paramètres IP de votre ordinateur. Pour obtenir de l'aide sur l'utilisation d'une commande, il faut saisir `Get-Help <nom_de_la_commande>`

Q17. Lister les interfaces présentes sur votre ordinateur en utilisant la commande `Get-NetAdapter`

- 1) Quel est le nom des interfaces présentes sur votre machine ?
- 2) Quel est le nom de l'interface physique active ? Quel est son numéro d'index ?

Q18. Afficher les paramètres IP des interfaces en utilisant la commande `Get-NetIPConfiguration` ou bien à partir de son alias `gip`. Vous pouvez aussi ajouter à la commande l'argument `-interfaceindex <numéro_interface_active>` pour n'afficher que les paramètres IP de cette interface.

- 1) Quelle est l'adresse IP et le masque de sous-réseau de l'interface active ?

- 2) Quelle est l'adresse du réseau correspondant ?
- 3) Quelle est l'adresse de diffusion ?
- 4) Quelle est la notation CIDR (préfixe) de ce réseau ?
- 5) S'agit-il d'une adresse privée ou publique ? Pourquoi selon vous ?

Votre ordinateur accède aux ressources de l'internet. Cela signifie qu'une adresse de passerelle par défaut a été définie. Elle se matérialise par une route par défaut (0.0.0.0 /0 ou default) dans la table de routage de votre ordinateur.

Q19. Afficher la route par défaut contenue dans la table de routage en utilisant la commande `Get-NetRoute -destinationprefix 0.0.0.0/0`. Vous pouvez aussi l'ancienne commande `route print` en indiquant l'éléments de recherche 0.0.0.0*

- 1) Quelle est l'adresse IP de la passerelle ?
- 2) Est-ce qu'elle appartient au réseau local ?
- 3) Quel équipement joue le rôle de passerelle ?

Généralement, les paramètres IP comme l'adresse IP, le masque de sous-réseau, l'adresse de passerelle et l'adresse du serveur DNS sont transmis à l'ordinateur lorsque celui-ci en fait la demande à un serveur DHCP. Vous utiliserez la commande `ipconfig /all` pour déterminer les paramètres qu'il vous manque.

Q20. Afficher les informations du service DHCP en utilisant la commande `Get-NetworkAdapter -indexinterface <numéro_index_interface>` puis la commande `ipconfig /all`

- 1) Est-ce que le service DHCP est activé ?
- 2) Quelles est la durée de validité de l'adresse IP obtenue ?
- 3) Quelle est l'adresse IP du serveur DHCP ?
- 4) Sur quel périphérique ce service est-il installé ?

En principe, le serveur DHCP est installé sur la Box. Vous pouvez vous connecter à la page de configuration via votre navigateur web et consulter les paramètres réseau qui ont été configurés. ATTENTION : Ne modifiez pas les paramètres de configuration de votre Box.

Q21. Accéder à la page de configuration de votre Box à partir d'une URL sous la forme <http://<adresse IP passerelle>>

- 1) Quelle est la plage d'adresse IP définie sur le serveur DHCP ?
- 2) Quels sont les « Baux actifs » (les équipements du réseau qui ont reçus une adresse IP du serveur) ?

En général, le client DNS de votre ordinateur est configuré avec l'adresse du serveur DNS de votre FAI ou bien avec l'adresse IP de la passerelle (Box). Dans le premier cas, c'est le client DNS de l'ordinateur qui contacte directement le serveur DNS de votre FAI alors que dans le deuxième cas le client DNS s'adresse à la Box pour que cette dernière relaye la requête au serveur DNS du FAI. La Box joue ainsi le rôle de mandataire (proxy DNS).

Q22. Afficher les adresses du client DNS en utilisant la commande `Get-DnsClientServerAddress -indexinterface <numéro_index_interface>`

- 1) Quelle est l'adresse IP du serveur DNS configuré sur votre ordinateur ?
- 2) Est-ce que cette adresse IP correspond à celle du DNS de votre FAI ou à la passerelle ?

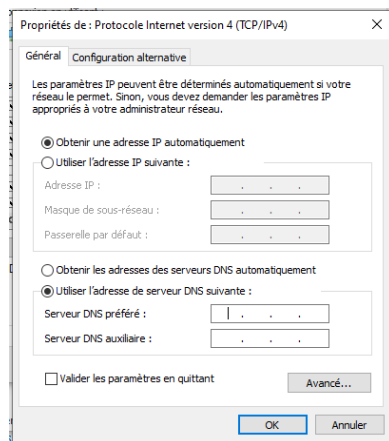
Pour déterminer l'adresse du serveur DNS utilisée par votre ordinateur, vous pouvez utiliser la commande `nslookup` pour l'interroger.

Q23. Interroger le serveur DNS en exécutant la commande `nslookup` et en précisant le nom de domaine totalement qualifié à résoudre (www.univ-poitiers.fr)

- 1) Quel est le nom du serveur DNS ? Quelle est son adresse IP
- 2) Quelle est l'adresse IP du serveur qui héberge le site web de l'université ? Quel est son nom ? Porte-t-il un alias ?

C'est également possible d'utiliser un serveur DNS public comme Google Public DNS (8.8.8.8), Cloudflare (1.1.1.1) ou encore Quad9 (9.9.9.9). Cependant, il est recommandé d'utiliser celui de votre FAI.

Q24. Configurer le client DNS de votre ordinateur avec l'adresse IP d'un serveur DNS public en utilisant l'environnement de configuration graphique de Windows suivant ou bien en utilisant la commande `Set-DnsClientServerAddress`.



- 1) Afficher l'adresse du client DNS avec la commande `Get-DnsClientServerAddress -indexinterface <numéro_index_interface>`. Est-ce l'adresse que vous avez configurée ?
- 2) Vider le cache DNS de votre ordinateur avec la commande `Clear-DnsClientCache` ou bien encore `ipconfig /flushdns`.
- 3) Interroger le serveur DNS pour résoudre www.univ-poitiers.fr. Est-ce bien le serveur DNS configuré qui a fait la résolution ?
- 4) Revenir à votre configuration de départ et cocher « Obtenir les adresses des serveurs DNS automatiquement ».

2.1.2. Recherche de la configuration du smartphone sous Android

Le smartphone est connecté au réseau local et au réseau 4G (Données mobiles activées). Pour dialoguer en mode commande avec le système d'exploitation, vous utiliserez l'application « Terminal Emulator for Android ».

Q25. Installer l'application « Terminal Emulator for Android » sur votre smartphone si ce n'est pas déjà fait et la lancer. Dans le terminal, saisissez les commandes `ls`, `id`, `pwd` ... puis la commande `ip address`

- 1) A quel système d'exploitation cela vous fait-il penser ?
- 2) Quelle est l'adresse IPv4 affectée à l'interface WLAN de votre smartphone ?
- 3) Appartient-elle à votre réseau IP ? Est-elle issue de la plage DHCP de votre serveur ?

Q26. Relever l'adresse des serveurs DNS configurés sur votre smartphone en utilisant la commande `getprop | grep dns`. Vérifier que l'adresse est bien identique à celle configurée sur l'ordinateur.

Q27. Tester la connectivité entre votre smartphone et votre ordinateur à l'aide de la commande `ping`. Vérifier que le test est concluant.

Sur le réseau 4G, le smartphone reçoit en général 2 adresses IPv6. Ce sont des adresses de 128 bits, codées en hexadécimal.

Q28. Relever les deux adresses IPv6 associées à l'interface `rmnet0`.

2.2. Recherche d'informations complémentaires sur le réseau

A ce stade, vous avez rassemblé les informations qui caractérisent votre réseau local (LAN). Il vous manque encore celles du réseau local sans-fil (WLAN) et celles du réseau étendu (WAN).

2.2.1. Recherche des caractéristiques de la liaison Wi-Fi

Le point d'accès Wi-Fi de votre Box permet de connecter les différents équipements sans fil (smartphone, ordinateur, TV connecté...) de votre réseau local selon la norme IEEE 802.11.

Selon la norme utilisée, la bande de fréquence des 2,4 GHz et / ou celle des 5 GHz peuvent être utilisées. Par exemple, un point d'accès configuré en mode mixte « B/G/N Mixed » permet aux périphériques sans fil équipés d'une interface compatible 802.11b, 802.11g ou 802.11n (2,4 GHz) de se connecter.

Le SSID (Secure Set IDentifier) est le nom donné au réseau et sert d'identifiant unique.

Dans la bande des 2,4 GHz, le canal permet aux appareils sans fil de communiquer sur des plages de fréquence spécifiques. En Europe, il y a 13 canaux disponibles dans la bande des 2,4 GHz.

La sécurité du réseau sans fil est assurée par un système d'authentification et de chiffrement des données échangées entre le client sans fil et le point d'accès. Les techniques d'authentification à clé partagée comme WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) et WPA2 (norme IEEE 802.11i) peuvent être utilisées. Actuellement, la méthode la plus sûre est WPA2 avec l'algorithme de chiffrement AES. Aujourd'hui, WEP n'est pas recommandé car les clés partagées n'offrent pas une protection suffisamment robuste.

Le niveau de puissance du signal Wi-Fi reçu est un paramètre important pour qualifier la qualité de la liaison. Consultez le site suivant pour obtenir davantage d'informations :
<https://desk.zoho.com/portal/tplinkfrance/en/kb/articles/orientation-en-mode-repeteur>

Dans cette partie, vous allez rechercher les caractéristiques de votre réseau sans fil à l'aide de votre smartphone et/ou de votre ordinateur portable. Assurez-vous que ces équipements sont bien connectés au réseau sans fil de votre domicile.

Q29. Installer et exécuter l'application « Net Analyser » sur votre smartphone. Parcourir les différents menus pour rechercher les informations demandées.

- 1) Quel est le nom de votre réseau Wi-Fi ?
- 2) Quelle est la norme 802.11 (mode b, g, n, ac) utilisée ? Quelle bande de fréquence est utilisée ?
- 3) Quel canal est utilisé ?

- 4) Quelle est la puissance du signal reçue ? Est-ce que cela a une influence sur le débit ? Comment procédez-vous pour le vérifier ? A partir de quel niveau de puissance la connexion devient inutilisable ?
- 5) Quel est la méthode d'authentification et de chiffrement utilisées ?
- 6) Y-a-t-il d'autres canaux Wi-Fi utilisés ? Si oui, quel est leur nom ?
- 7) Quels sont les paramètres de configuration IP de l'interface sans-fil ?

Vous pouvez également utiliser votre ordinateur portable pour caractériser votre réseau Wifi.

Q30. Installer et lancer l'application inSSIDer puis dans le terminal PowerShell, exécuter la commande `netsh wlan show interface`. Exploiter les résultats obtenus pour compléter / confirmer les résultats obtenus à la question précédente.

- 1) Quel est le nom de votre réseau Wi-Fi ?
- 2) Quelle est la norme 802.11 (mode b, g, n, ac) utilisée ? Quelle bande de fréquence est utilisée ?
- 3) Quel canal est utilisé ?
- 4) Quelle est la puissance du signal reçue ? Est-ce que cela a une influence sur le débit ? Comment procédez-vous pour le vérifier ? A partir de quel niveau de puissance la connexion devient inutilisable ?
- 5) Quel est la méthode d'authentification et de chiffrement utilisées ?
- 6) Y-a-t-il d'autres canaux Wi-Fi utilisés ? Si oui, quel est leur nom ?
- 7) Quels sont les paramètres de configuration IP de l'interface sans-fil ?

2.2.2. Recherche d'informations sur de la liaison WAN et le FAI

Les aspects physiques de la liaison WAN ont été étudiés dans la première partie. Il s'agit ici de relever l'adresse IP associée à l'interface WAN de votre Box et de rechercher différents types d'informations : Où est-elle localisée ? Qui exploite cette adresse ? Est-elle associée à un nom de domaine ?

Q31. Relever l'adresse IP associée à l'interface WAN de votre Box en utilisant les deux sites suivants : <https://www.monip.org/> et <https://ip.lafibre.info/>

- 1) Quelle est l'adresse IPv4 de l'interface WAN ?
- 2) Est-ce une adresse IP publique ? Pourquoi ?
- 3) Y-a-t-il une adresse IPv6 associée à votre interface WAN ? Si oui, laquelle ?

Q32. Relever les informations sur la localisation de l'adresse IP (IPv4 et / ou IPv6) de votre Box en utilisant le lien <https://www.hostip.fr/>.

- 1) Quel est sa localisation ? Est-ce que cette information est fiable ?
- 2) Quelle est la signification du champ « Host » ?

Les adresses IP publiques sont gérées par l'IANA (Internet Assigned Numbers Authority). Cette organisation délègue l'attribution des adresses à des RIR (Regional Internet Registries) qui se chargent d'organiser la distribution de blocs d'adresses aux opérateurs et aux entreprises.

Q33. Se rendre sur le site de l'IANA à l'adresse <https://www.iana.org/numbers>

- 1) Quel est le nom des différents RIR ?
- 2) Quelles sont les régions gérées par ces RIR ?

Le RIPE NCC (RIPE Network Coordination Center) est le centre de gestion des adresses IP pour l'Europe, le Moyen-Orient et l'Asie centrale. Il maintient une base de données de toutes les adresses IP allouées ainsi que des informations sur les propriétaires de ces adresses.

Q34. Se rendre sur le site du RIPE NCC, visualiser la vidéo https://www-static.ripe.net/static/videos/misc/What_is_the_RIPE_NCC.mp4 et retrouver les éléments indiqués ci-dessus.

Le Whois est un service de recherche d'informations sur le propriétaire d'une adresse IP ou d'un nom de domaine Internet.

Q35. Se rendre sur la page de consultation de la base de données du RIPE en utilisant l'adresse <https://apps.db.ripe.net/db-web-ui/query> et saisir l'adresse IP publique de votre Box. Les résultats qui apparaissent de couleur verte sont des liens vers des informations complémentaires. Vous pouvez aussi compléter avec vos propres recherches sur internet.

- 1) Quelle est la structure (organisation) qui a la responsabilité de votre adresse ? A qui appartient cette structure ? Dans quelle ville est-elle implantée ? En quelle année a-t-elle été créée ? Quel est son nom commercial ?
- 2) Quelle est la plage d'adresse affectée à votre FAI ? Combien d'adresses votre FAI exploite-t-il ?

La majorité des entreprises possède un nom de domaine qui leur permet de mettre en place différents services informatiques (sites web, messagerie...) qui doivent être accessibles publiquement. Un certain nombre d'informations sur leurs systèmes d'informations sont donc disponibles au grand public. A titre d'exemple, vous allez utiliser le site DNS Checker pour rechercher l'adresse IP du serveur web de l'université de Poitiers à partir de son URL. Vous utiliserez également ce site pour vérifier si votre adresse IP publique est associée ou non à un nom de domaine.

Q36. Se rendre sur le site <https://dnschecker.org/>, sélectionner « DNS Lookup » dans le menu puis saisir l'adresse URL du site web de l'université de Poitiers.

- 1) Quelle est l'adresse IP associée au nom de domaine complètement qualifié www.univ-poitiers.fr ?
- 2) Quel est le nom d'hôte du serveur ? Quel est son alias ?

Q37. Toujours sur le site <https://dnschecker.org/>, sélectionner « All Tools » puis « Reverse IP Lookup » dans le menu et saisir l'adresse IP du serveur web de l'université.

- 1) Quel est le nom d'hôte du serveur ?
- 2) Vérifier la réponse à la question précédente.

Q38. A partir des fonctions de recherche « DNS Lookup » et « Reverse IP Lookup » du site <https://dnschecker.org/>, rechercher le nom d'hôte de votre Box.

- 1) Quel est le nom d'hôte de votre Box ? Quel est le nom de domaine complètement qualifié associé à votre Box ?
- 2) Pourquoi ce nom d'hôte n'est-il pas enregistré dans les DNS public ?

En général, l'adresse IP de l'interface WAN de la Box est publique. Cela signifie qu'un test de connectivité entre un smartphone connecté au réseau mobile (4G) par exemple et votre adresse IP doit être fonctionnel.

- Q39.** Connecter votre smartphone au réseau 4G, lancer l'application « Terminal Emulator for Android » et réaliser un test de connectivité en utilisant la commande ping. Le résultat est-il concluant ?

2.3. Recherche des services installés

Dans cette partie, vous allez rechercher si des services applicatifs sont actifs sur les équipements de votre réseau local et potentiellement détecter des vulnérabilités. Pour cela, vous utiliserez la méthode du scan de port qui consiste à identifier les adresse IP des périphériques présents dans le réseau local et à découvrir si des services réseaux sont actifs sur ces différents équipements.

On distingue généralement 2 types d'hôtes dans un réseau IP : les clients et les serveurs.

Les serveurs sont des hôtes sur lesquels des applications réseaux ont été installées. Nous avons vu en cours par exemple, le service DHCP qui fournit un paramétrage réseau, le service DNS qui fournit une correspondance entre un nom d'hôte et une adresse IP ou encore le service http qui permet de mettre en ligne un site Web.

Un serveur est joignable sur un réseau IP via son adresse IP et peut déployer simultanément plusieurs services. L'utilisation seule de l'adresse IP pour établir une communication avec un service spécifique n'est donc pas suffisant. La « porte d'entrée » de communication à destination d'un service est un triplet {adresse IP ; n° de port ; protocole}. Une application (un service) est alors en écoute permanente d'une requête (une question) sur son n° de port.

Par exemple, le service DNS écoute sur son port 53 dans l'attente d'une requête en UDP, un serveur HTTP sur le port 80 en TCP et DHCP sur le port 67 en UDP.

Vous utiliserez l'outil Nmap pour découvrir les différents hôtes du réseau local et lister les éventuels services présents sur ces équipements. Pour des informations sur cet utilitaire, rendez-vous sur le site <https://nmap.org/> et suivez le lien <https://nmap.org/man/fr/> pour obtenir sa documentation. Les options de la commande sont accessibles à la page <https://nmap.org/man/fr/man-briefoptions.html>

- Q40.** Télécharger puis installer le logiciel nmap à partir du lien <https://nmap.org/dist/nmap-7.92-setup.exe>

Vous pouvez lancer l'outil graphique Zenmap ou bien encore saisir la commande nmap directement dans un terminal de commande.

- Q41.** Lancer le logiciel Zenmap et saisir la commande `nmap -O 127.0.0.1` afin de scanner votre ordinateur. L'adresse 127.0.0.1 est l'adresse « local host », c'est l'adresse de bouclage de l'ordinateur.

- 1) Combien de ports sont actuellement ouverts sur votre ordinateur ?
- 2) A quels services sont-ils associés ?
- 3) Quelles informations avez-vous obtenues sur système d'exploitation de votre ordinateur ?

- Q42.** Saisir la commande `nmap -sP <adresse_ip_reseau> <prefixe_reseau>` afin de scanner le réseau local.

- 1) Combien d'hôtes ont été détectés ?
- 2) Retrouver l'adresse MAC et l'adresse IP de votre ordinateur

Maintenant, vous allez scanner votre Box pour déterminer son système d'exploitation, sa version, lister les ports ouverts et les services installés.

- Q43.** Saisir la commande `nmap -sV --version-light <adresse_IP_Box>` afin de scanner le réseau local.

```

Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-15 20:51 Paris, Madrid (heure d'été)
Nmap scan report for 192.168.0.254
Host is up (0.022s latency).
Not shown: 973 filtered tcp ports (no-response), 11 filtered tcp ports (port-unreach)
PORT      STATE SERVICE      VERSION
21/tcp    closed ftp
53/tcp    open  domain       dnsmasq 2.85
80/tcp    open  http         nginx
139/tcp   closed netbios-ssn
443/tcp   open  ssl/http     nginx
445/tcp   open  microsoft-ds
548/tcp   closed afp
554/tcp   open  rtsp         Freebox rtspd 1.2
1723/tcp  closed pptp
5000/tcp  open  rtsp
5001/tcp  closed complex-link
5357/tcp  open  tcpwrapped
5678/tcp  open  upnp         fbzigdd 1.1 (AliceBox PM203 UPnP; UPnP 1.0)
6000/tcp  closed X11
8090/tcp  open  http         nginx
9091/tcp  open  http         nginx
MAC Address: (Freebox SAS)
Service Info: OS: Linux 2.6; Devices: media device, WAP; CPE: cpe:/o:linux:linux_kernel:2.6

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 44.73 seconds

```

- 1) Quel est le système d'exploitation de votre Box ? Quelle est sa version (version du noyau) ?
- 2) Quels sont les ports ouverts ? Quel protocole est identifié par le port 80 ? A quel service correspond -t-il ? Quelle est le nom de l'application serveur qui fournit ce service (vous pouvez faire une recherche à partir du nom pour vous aider) ?
- 3) Connectez-vous à ce service en utilisant le navigateur de votre ordinateur. Que constatez-vous ? Quel est l'intérêt d'avoir intégré ce service dans la Box ?
- 4) Quels sont les autres services accessibles sur votre Box ? Quelles sont les applications installées qui fournissent ces services ?

2.4. Schémas de la topologie du réseau

A ce stade, vous disposez d'un grand nombre d'informations qui vont vous permettre de réaliser le schéma de la topologie de votre réseau. Vous représenterez la Box par ses éléments internes, vous ferez apparaître l'ensemble des hôtes avec leur adresse MAC et IP, vous indiquerez l'adresse de réseau et les services internes à la Box.

Q44. A l'aide du logiciel en ligne <https://app.diagrams.net/> et de la bibliothèque Cisco 19, réaliser le schéma de la topologie de votre réseau domestique.

Pour réaliser la topologie logique de votre réseau domestique, vous réaliserez un autre schéma à l'aide de l'outil en ligne <https://app.diagrams.net/> et vous représenterez la Box seulement par un routeur.

Q45. Réaliser du schéma de la topologie logique de votre réseau domestique. Demandez-vous quelles sont les informations qui doivent apparaître sur cette topologie logique.

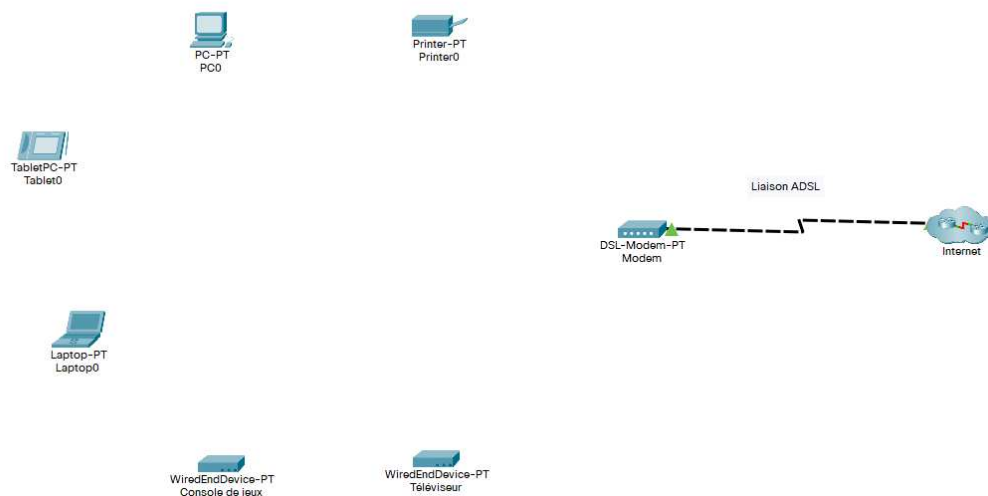
Partie 2: Installation d'un réseau domestique sous Packet Tracer

1. Construire un réseau domestique sous Packet Tracer

Dans cette partie, vous allez prendre le rôle d'un technicien dont les missions consistent à intervenir chez les clients de l'opérateur national Liberty. Aujourd'hui, votre tâche consiste à installer et configurer un réseau informatique domestique chez un particulier.

Vous utiliserez le logiciel Packet Tracer pour construire le réseau domestique et le configurer conformément aux directives de sécurité imposées par votre entreprise.

1.1. Topologie



1.1. Installation du routeur sans fil et utilisation avec les paramètres par défaut

1.1.1. Câblage des équipements

Vous utiliserez le routeur sans fil WRT300N.

Q46. Télécharger le fichier `reseau_domestique.pkt` sur la plateforme *UPdago* et ouvrir ce fichier avec *Packet Tracer*.

Q47. Placer le routeur sans fil WRT300N dans l'espace de travail.

Q48. Quels sont les ports à utiliser pour le LAN et celui à utiliser pour le WAN ? Connecter tous les périphériques filaires au routeur sans fil WRT300N.

Q49. Installer la carte réseau sans fil *WPC-300N* (2,4GHz) dans l'emplacement réservé du Laptop afin d'assurer la connexion au routeur sans fil. Pensez à mettre l'ordinateur sous tension.

1.1.2. Configuration des périphériques finaux

La plupart des routeurs sans fil utilisés au domicile ou dans les petits réseaux de bureau sont prêts à l'emploi. Ils sont configurés pour attribuer de manière dynamique une adresse IP aux périphériques finaux qui lui sont rattachés par l'intermédiaire du protocole DHCP.

Q50. Configurer l'ordinateur PC0 afin qu'ils reçoivent les paramètres IP (Adresse IP, masque de sous réseau, adresse de passerelle) du serveur DHCP. Utiliser la commande `ipconfig` pour vérifier la configuration.

- 1) Quelle est l'adresse IP et le masque de sous réseau de PC0 ?
- 2) Quelle est l'adresse du réseau IP ?
- 3) Quelle est l'adresse IP de la passerelle par défaut ?
- 4) Quelle est l'adresse IP du serveur DNS ?

Q51. Vérifier que vous pouvez atteindre le serveur web à l'adresse `200.123.211.1` par un test de connectivité initié depuis PC0. Lorsque le test est lancé pour la première fois, les 3 premières requêtes ICMP échouent. Vous pouvez également vérifier que la page web s'affiche correctement en saisissant l'adresse www.liberty.net dans le navigateur de PC0.

1.2. Configuration du routeur sans fil

Votre réseau est maintenant opérationnel mais utilise les paramètres de configuration par défaut du routeur sans fil. Cela pose un problème de sécurité car les informations comme le nom d'utilisateur, le mot de passe, l'adressage, le SSID se trouvent facilement sur Internet. Une bonne pratique consiste à changer ces paramètres de configuration.

Les routeurs domestiques sans fil sont conçus pour être facilement configurés. Ils contiennent généralement une interface web accessible via un ordinateur connecté au réseau local. Dans cette étape, vous allez utiliser l'ordinateur PC0 pour effectuer la configuration du routeur sans fil WRT300N.

Q52. Accéder à l'interface web de configuration du routeur à partir du navigateur web de PC0. Pour cela, vous saisissez l'adresse IP du routeur dans le champ URL pour accéder à la page d'authentification du routeur puis saisissez l'identifiant `admin` et le mot de passe `admin` pour charger la page de configuration.

Q53. Changer le mot de passe par défaut de connexion du routeur par `gtrnet`. Sauvegarder votre configuration en cliquant sur « Save Settings » en bas de la page de configuration.

1.2.1. Modification des paramètres d'adressage

Votre société a établi le plan d'adressage suivant :

| | |
|------------------------------------|-----------------------------|
| Adresse de l'interface WAN | Adressage dynamique |
| Adresse du réseau LAN | 172.20.0.0 /24 |
| Plage d'adresses de l'étendue DHCP | 172.20.0.150 à 172.20.0.189 |
| Adresse de passerelle par défaut | 172.20.0.254 |
| Adresse du serveur DNS | 197.54.122.1 |

Q54. Dans la section *Setup*, vérifier que l'interface WAN (Internet) du routeur est configuré pour obtenir automatiquement une adresse IP du FAI via le protocole DHCP.

Q55. Dans la section *Setup*, configurer l'adresse IP du routeur et son masque de sous-réseau.

Q56. Dans la section *Setup*, configurer le service DHCP pour que les périphériques du LAN puisse obtenir une adresse IP, un masque de sous-réseau, une adresse de passerelle et une adresse de serveur DNS automatiquement. Enregistrer les nouveaux paramètres en cliquant sur Save Settings en bas de la page.

La sauvegarde de la configuration a entraîné le redémarrage du routeur sans fil. A ce stade, vous ne pouvez plus accéder à la page de configuration car l'adresse IP du routeur a été modifiée et votre ordinateur ne se trouve plus dans le même réseau IP que le routeur.

Q57. Libérer puis renouveler les paramètres IP de l'ordinateur PC0 afin d'obtenir une nouvelle adresse IP dans le réseau 172.20.0.0/24. Pour cela, vous pouvez utiliser les commandes `ipconfig /release` et `ipconfig /renew` ou bien en sélectionner « *Static* » puis « *DHCP* » à partir de l'onglet *Desktop – IP Configuration* dans la fenêtre de configuration de PC0.

Q58. Se reconnecter à nouveau à l'interface de configuration du routeur à partir de PC0.

1.2.2. Modification des paramètres du réseau sans fil

Les paramètres concernant le réseau sans fil sont les suivants :

| | |
|--|----------------------|
| Nom du réseau sans fil (SSID) | Perso_wifi |
| Type de chiffrement du réseau sans fil | WPA2-Personnel / AES |
| Clé de sécurité du réseau sans fil | gtrnetgtrnet |

Q59. A partir de la section *Wireless*, saisir le nom du réseau sans fil (SSID) et vérifier que celui-ci est autorisé à être diffusé par le routeur sans fil.

Q60. A partir de la section *Wireless*, activer la sécurité du réseau sans fil en choisissant le mécanisme approprié pour l'authentification et le chiffrement. Enfin, renseigner la clé de sécurité (Passphrase).

1.3. Configuration des hôtes

Le routeur sans fil est maintenant configuré. Il ne reste plus qu'à paramétrer les hôtes du réseau à l'exception de PC0 qui a permis la configuration de l'équipement. Il est nécessaire de renouveler les paramètres IP des hôtes car ils ont conservé les paramètres de la précédente configuration.

Q61. Renouveler les paramètres IP des différents périphériques filaires du LAN en utilisant les commandes `ipconfig /release` et `ipconfig /renew` ou bien en sélectionnant « *Static* » puis « *DHCP* » à partir de l'onglet *Desktop – IP Configuration* dans la fenêtre de configuration des ordinateurs. Avez-vous une adresse comprise dans la plage imposée ? L'adresse de la passerelle par défaut et du DNS sont-elles correctes ?

Q62. Vérifier que vous pouvez communiquer avec le serveur web situé à l'adresse 200.123.211.1 à partir des tests suivants :

- 1) Vérifier la connectivité entre PC0 et le serveur à l'aide de la commande `ping`. Quelles couches du modèle TCP/IP sont utilisées ? Quels sont les protocoles qui ont été vérifiés ?
- 2) Afficher la page web située à l'adresse <http://200.123.211.1> à l'aide du navigateur de PC0. Quelles couches du modèle TCP/IP sont utilisées ? Quels sont les protocoles mis en jeu ? Quel service a été vérifié ?
- 3) Afficher la page web située à l'adresse <http://www.liberty.net> à l'aide du navigateur de PC0. Quel service autre que le service HTTP avez-vous vérifié ?

Q63. Connecter l'ordinateur Laptop au réseau sans fil à partir de l'onglet *Desktop > PC Wireless* ou bien en utilisant l'assistant de configuration PC Wireless. Connecter également la tablette. Valider votre configuration par un test de connectivité.

2. Analyse protocolaire

Les protocoles sont un ensemble de règles qui régissent les communications entre les différents ordinateurs d'un réseau. Les spécifications de protocole définissent le format des messages échangés.

Un modèle de référence a permis de normaliser la manière dont les périphériques communiquent sur le réseau. Il sépare les communications réseau en 7 couches distinctes. Le modèle couramment utilisé pour Internet regroupe les couches 5, 6 et 7 sous le terme de couche Application et les couches 1 et 2 sous le nom de couche Accès réseau.

| Modèle OSI | PDU | Description | Modèle TCP/IP | Pile de protocoles |
|-----------------------|---------|---|---------------|----------------------------|
| 7- Application | Données | Responsable des services réseau pour les applications | Application | HTTP, DNS, DHCP, SMTP, POP |
| 6- Présentation | Données | Adapte les formats de données | | |
| 5- Session | Données | Etablit, gère et interrompt les connexions entre l'application locale et distante | | |
| 4- Transport | Segment | Gère le transport des données entre application sur tout le réseau grâce aux numéros de ports | Transport | TCP / UDP |
| 3- Réseau | Paquet | Responsable de l'adressage logique et du routage | Réseau | IP, ICMP |
| 2- Liaison de données | Trame | Assure l'adressage physique et l'accès au support | Accès réseau | Ethernet |
| 1- Physique | Bit | Définit toutes les spécifications électriques et physiques des équipements | | |

PDU (Protocol Data Unit) : Unité de données de protocole

Lors de l'envoi de messages sur le réseau, les données de la couche Application traversent les différentes couches pour atteindre le support physique. A chaque couche, les informations de la couche supérieure sont encapsulées dans le champ Données du protocole de la couche sous-jacente.

Dans cette partie, vous allez utiliser le mode Simulation pour identifier les protocoles mis en jeu lorsque PC0 demande une page web au serveur du FAI.

Pour obtenir une simulation fluide, réaliser au préalable un test de connectivité entre PC0 et les serveurs DNS et Web. Plusieurs requêtes ICMP sont nécessaires.

Q64. Passer en mode « Simulation » et vérifier que le filtre ne laisse passer que les événements liés aux protocoles ICMP, HTTP et DNS.

Q65. Accéder à la page web www.liberty.net à partir du navigateur de PC0, jouer la simulation et observer le chemin emprunté par le paquet. Les informations contenues dans le panneau de simulation doivent correspondre à celles-ci :

| Event List | | | | |
|------------|-----------|------------------|------------------|------|
| Vis. | Time(sec) | Last Device | At Device | Type |
| | 0.000 | -- | PC0 | DNS |
| | 0.001 | PC0 | Wireless Router0 | DNS |
| | 0.002 | Wireless Router0 | Modem | DNS |
| | 0.003 | Modem | Operateur | DNS |
| | 0.008 | Operateur | Modem | DNS |
| | 0.009 | Modem | Wireless Router0 | DNS |
| | 0.010 | Wireless Router0 | PC0 | DNS |
| | 0.020 | -- | PC0 | HTTP |
| | 0.021 | -- | PC0 | HTTP |
| | 0.022 | PC0 | Wireless Router0 | HTTP |
| | 0.023 | Wireless Router0 | Modem | HTTP |
| | 0.024 | Modem | Operateur | HTTP |
| | 0.029 | Operateur | Modem | HTTP |
| | 0.030 | Modem | Wireless Router0 | HTTP |
| | 0.031 | Wireless Router0 | PC0 | HTTP |

Q66. Analyser le premier message émis par PC0 (premier carré coloré) et répondre aux questions suivantes :

- 1) Quel protocole applicatif est encapsulé par PC0 ?
- 2) Que signifie DNS Query (Name=www.liberty.net) ?
- 3) Quel est le protocole de transport utilisé avec ce protocole applicatif ? Quel est le port d'écoute du service serveur ?
- 4) Quelle est l'adresse IP de destination du paquet ? A quel équipement appartient cette adresse ? Est-ce que cette adresse IP sera modifiée durant le transit ?
- 5) Quelle est l'adresse MAC de destination de la trame ? A quel équipement correspond-elle ? Sera-t-elle conservée durant le transit ?

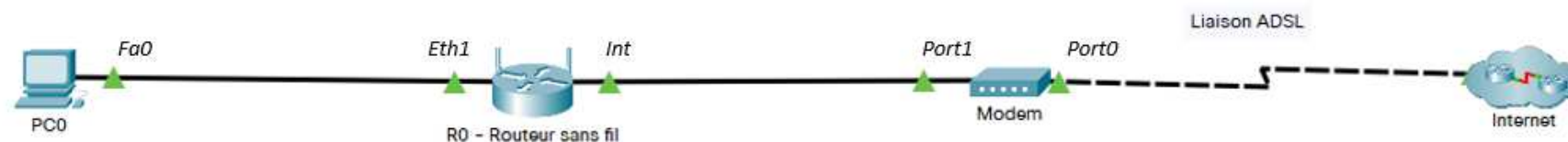
Q67. Analyser la réponse reçue par PC0 (7ème carré coloré) et répondre aux questions suivantes :

- 1) Quel protocole applicatif est encapsulé dans la réponse ?
- 2) Quelle information utile est contenue dans le champ DNS Answer ?
- 3) Quelles est la valeur du port source ? Pourquoi cette valeur ?
- 4) Quelle est l'adresse IP source du paquet ? A quel équipement appartient-elle ?
- 5) Quelle est l'adresse MAC source ? A quel équipement appartient-elle ?

Q68. Décrire le processus d'encapsulation lorsque l'ordinateur PC0 envoie une requête HTTP au serveur web et compléter le schéma représentant les couches du modèle OSI utilisées par chaque périphérique.

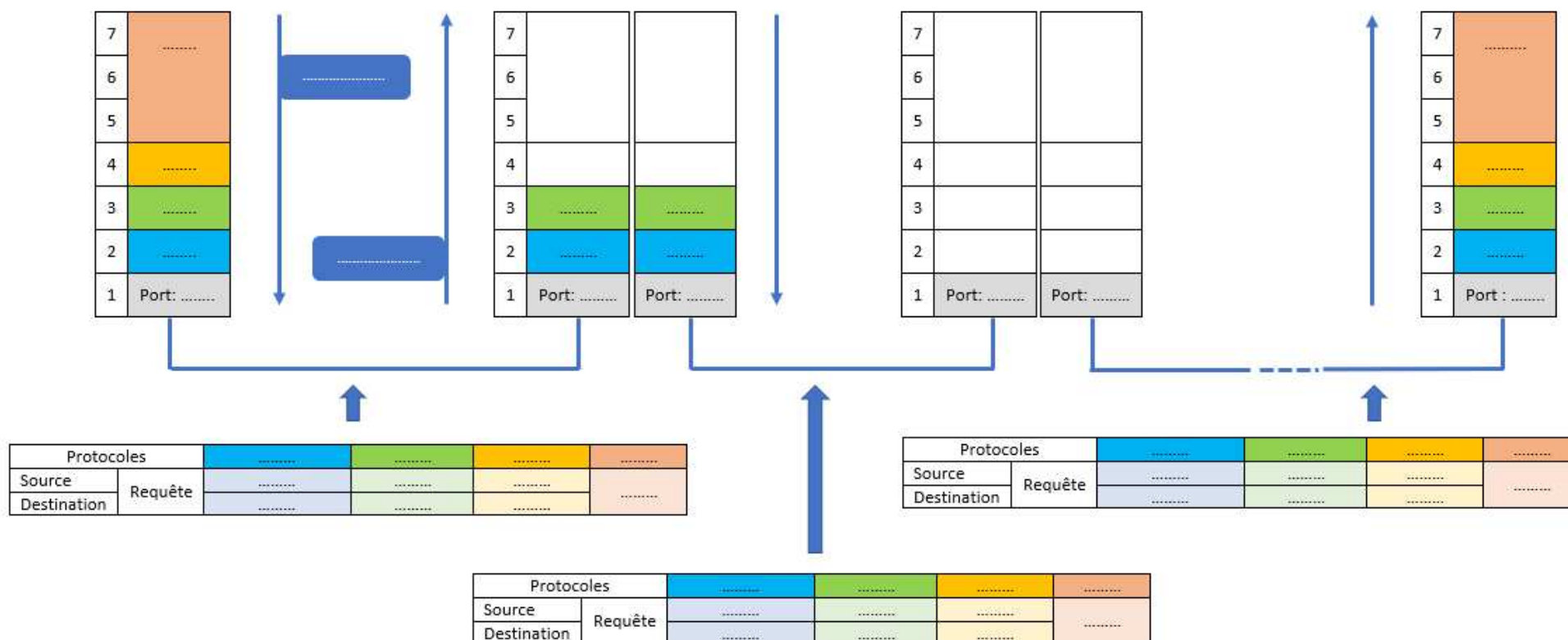
- 1) Extraire les informations relatives à chaque couche : protocoles, adresse IP, adresse MAC
- 2) Reporter ces informations sur le schéma fourni en annexe 1 : les adresses seront notées MAC-PCx et IP-PCx où x représente le numéro de l'ordinateur concerné. Indiquer les processus d'encapsulation et de désencapsulation sur le schéma.
- 3) Quelles sont les couches gérées par le routeur ? Peut-il porter le nom d'équipement de couche 3 ?

Annexe 1 : Modélisation d'un échange entre PC0 et le serveur www.liberty.net



Processus de routage : examen IP Dst et choix du meilleur chemin pour atteindre la destination
 Processus NAT : translation de l'adresse IP Src privé par une adresse IP Src publique

Le modem est un dispositif qui permet d'adapter le signal provenant du routeur à celui de la liaison ADSL et inversement.

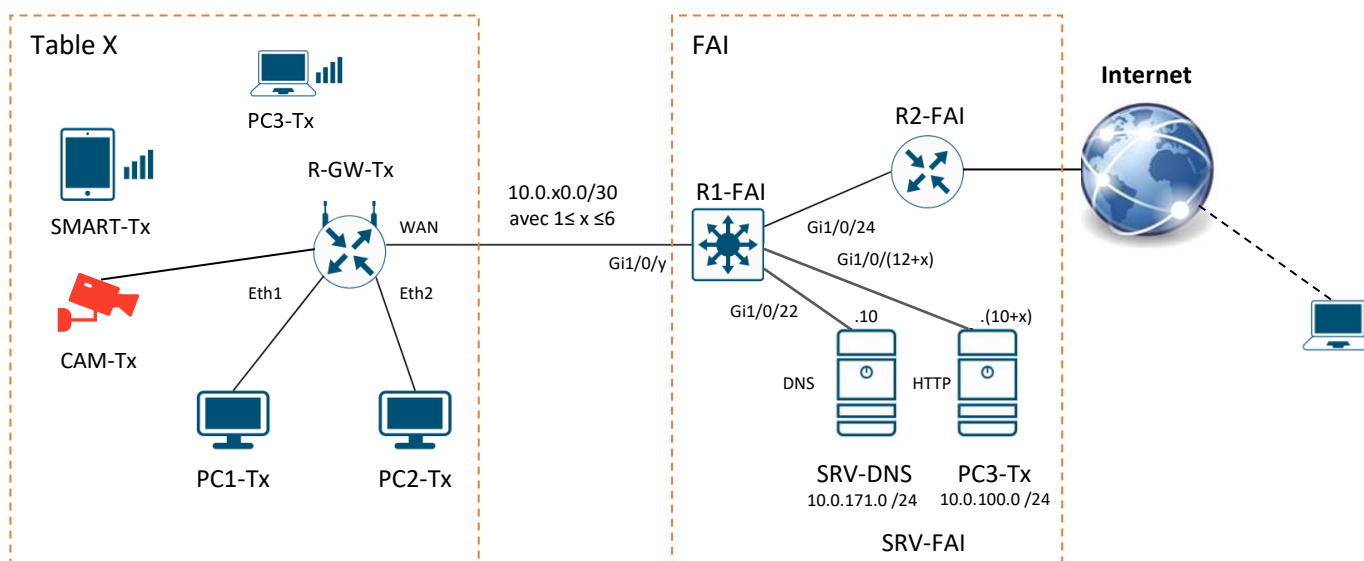


Partie 3: Déploiement d'un réseau informatique et mise en place d'un service de vidéo surveillance

Dans ce TP vous allez mettre en place l'infrastructure d'un réseau domestique. Vous réaliserez le câblage de la topologie, la configuration de l'équipement Cisco RV215W pour permettre un accès à Internet à partir de périphériques filaires et sans fil, l'intégration d'une caméra IP Axis ou D-Link pour assurer la vidéo surveillance et l'installation d'un service web pour visualiser le flux vidéo depuis Internet.

1. Topologie du réseau

Le schéma de la topologie du réseau que vous allez utiliser lors des travaux pratiques est le suivant :



Dans cette topologie, les 6 réseaux domestiques ($1 \leq x \leq 6$) sont connectés à Internet par l'intermédiaire d'une infrastructure qui simule le réseau du fournisseur d'accès à Internet (FAI). Le routeur R2-FAI est connecté au réseau de la salle de TP et permet ainsi l'accès à Internet.

Chaque table de TP représente un réseau domestique. Le CPE (Box) du particulier est un équipement Cisco RV215W qui intègre un commutateur, un routeur passerelle et un point d'accès sans fil. Les ordinateurs et la caméra IP seront connectés au réseau à partir d'une connexion filaire ou bien à l'aide d'un adaptateur sans fil (Wi-Fi).

Remarque : x représente le numéro de la table de TP.

1.1. Le réseau de l'opérateur

Dans la réalité, l'interconnexion entre le réseau domestique et le fournisseur d'accès Internet est réalisée par la boucle locale (cuivre ou fibre) et par le réseau de collecte / transport composés d'équipements spécifiques. Pour le TP, le réseau de l'opérateur se limite à un lien qui relie l'interface WAN du routeur passerelle à celle du routeur du FAI. Il n'y a donc pas besoin d'utiliser de modem xDSL pour le réseau domestique dans notre cas.

Le tableau ci-dessous donne les éléments de câblage et de configuration concernant l'interconnexion entre le réseau du particulier et celui du FAI.

| Abonnés | Routeur R-GW-Tx | | Routeur R1-FAI | | |
|----------------|-----------------|-------------------|----------------|------|-------------------|
| | Interface | Adresse / Préfixe | Interfaces | VLAN | Adresse / Préfixe |
| Table 1 | WAN | dhcp | Gi1/0/1-2 | 10 | 10.0.10.1 /30 |

| | | | | | |
|----------------|-----|------|-------------|----|---------------|
| Table 2 | WAN | dhcp | Gi1/0/3-4 | 20 | 10.0.20.1 /30 |
| Table 3 | WAN | dhcp | Gi1/0/5-6 | 30 | 10.0.30.1 /30 |
| Table 4 | WAN | dhcp | Gi1/0/7-8 | 40 | 10.0.40.1 /30 |
| Table 5 | WAN | dhcp | Gi1/0/9-10 | 50 | 10.0.50.1 /30 |
| Table 6 | WAN | dhcp | Gi1/0/11-12 | 60 | 10.0.60.1 /30 |

Le réseau du fournisseur d'accès est basé sur le routeur R1-FAI (Cisco 3650) qui assure l'interconnexion entre les différents réseaux domestiques. Le routeur R1-FAI est un commutateur doté de fonctions de routage qui utilise des réseaux locaux virtuels (VLAN).

1.2. Le réseau du particulier

Le réseau LAN du particulier doit disposer :

- D'un service DHCP :
 - Adresse réseau : 172.20.x.0 /24
 - Adresse de l'interface interne : 172.20.x.254 /24
 - Plage pour l'attribution des adresses dynamiques : 172.20.x.100 à 172.20.x.199
 - Durée du bail : 3 jours
 - Adresse du serveur DNS : 10.0.171.10
- D'un adressage statique pour la caméra IP
- D'un accès sans fil sécurisé 802.11n
 - SSID : lab-sae-x avec x représente le numéro de table
 - WPA2-Personnal / AES pour l'authentification et le chiffrement
 - Canal à utiliser : C1 – Table 1 ; C4 – Table 2 ; C6 – Table 3 ; C8 – Table 4 ; C10 – Table 5 ; C13 – Table 6
- D'un service de translation d'adresse NAT
- D'un service de filtrage des flux (Pare-feu)

1.3. Les services de l'opérateur

Le FAI dispose d'un service d'hébergement de sites web (Apache) et d'un service DNS (Bind) qu'il met à disposition des abonnés. Le serveur DNS est commun à tous les abonnés alors que le serveur Web sera installé et configuré à la demande. Les informations suivantes concernent le serveur DNS du FAI :

- Connexion distante au serveur DNS du FAI :
 - Protocole : SSH
 - Nom d'utilisateur : etudiant
 - Mot de passe : etudiant
- Elévation des privilèges via la commande `sudo`
- Nom complet du site (FQDN) : www.tx.lab.rt avec x le numéro de la table de TP.
- Fichier de résolution du nom du site : `/etc/bind/db.tx.lab.rt`

2. Matériel

Le matériel utilisé est le suivant :

- Routeur sans fil : Cisco RV215W
- Caméra IP : D-Link DCS 2132L ou AXIS M1011-W
- R1-FAI : Cisco 3650
- Adaptateur Wi-Fi : TP-Link Wireless USB Adapter TL-WN823N

3. Travail à réaliser

3.1. Configuration des équipements du réseau local

- 1) Etablir le plan d'adressage du réseau LAN
- 2) Remettre en configuration usine le routeur sans fil Cisco RV215W et se connecter au routeur
- 3) Brancher les différents équipements
- 4) Configurer le service DHCP sur le routeur et vérifier que les ordinateurs peuvent communiquer entre eux.
- 5) Configurer l'interface WAN du routeur et vérifier que vous avez obtenu une adresse IP du fournisseur d'accès
- 6) Configurer le mode « routeur passerelle » pour réaliser une translation d'adresses (NAT) et ainsi permettre aux hôtes du LAN de pouvoir accéder à Internet. Vérifier par un test de connectivité que votre ordinateur peut atteindre le serveur de Google.
- 7) Configurer le point d'accès sans fil en respectant les contraintes de normes, de SSID, de canal, et d'authentification.
- 8) Connecter un équipement sans fil au WLAN et vérifier la connectivité entre les postes et Internet
- 9) Utiliser l'outil InSSIDer pour vérifier le canal utilisé par votre réseau sans fil et évaluer la puissance du signal reçue.
- 10) Remettre en configuration usine la caméra IP et se connecter à l'équipement. Vérifier par un test de connectivité que vous arrivez à joindre la caméra.
- 11) Donner une adresse IP statique à la caméra IP.
- 12) Visualiser le flux de la caméra à partir de VLC. Les URL à utiliser avec une caméra D-LINK pour accéder au flux vidéo avec le protocole http ou RTSP sont les suivantes :
http://user:password@ip_address:port/video1.mjpg
rtsp://user:password@ip_address:port/live1.sdp
- 13) Réaliser une capture Wireshark du flux vidéo HTTP et RTSP, analyser la pile de protocoles utilisée pour chacun d'eux et les comparer.

3.2. Mise en place d'un site web de vidéosurveillance

Le site web à mettre en ligne se limite à une page HTML intégrant le flux vidéo de la caméra. Le fichier labx.html est à télécharger sur UPdago.

```
<!DOCTYPE html>
<html lang="fr">

<head>
  <title>Lab x</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" href="https://www.w3schools.com/w3css/4/w3.css">
</head>

<body>
  <div class="w3-container w3-teal">
    <h1>Atelier LAN - Site Lab x</h1>
    <h4>Visualisation du flux vidéo de la caméra</h4>
  </div>

  <div align="center">
    <section class="streaming">
      
    </section>
  </div>
</body>

</html>
```

- 14) Adapter le contenu HTML du fichier aux caractéristiques de votre réseau puis visualiser la page dans un navigateur web (Firefox).
- 15) Une machine virtuelle `debian` est utilisée pour fournir à l'abonné un service Web. Elle sera hébergée chez le FAI. Il faudra donc installer la VM sur l'ordinateur PC3-Tx présent sur votre table de TP et le connecter ensuite au commutateur / routeur (R1-FAI) du FAI en utilisant le n° de port indiqué sur le schéma de la topologie.
La VM sera créée à partir de l'image ISO de la distribution Debian 11, sans environnement de Bureau mais avec un accès distant SSH. Ensuite, vous installerez un service serveur web sur cette VM.
- 16) Transférer la page web sur le serveur du FAI à l'emplacement `/var/www/labx`. Vous utiliserez la commande `scp` ou l'application WinSCP.
- 17) Se connecter au serveur DNS à partir d'un ordinateur de la table de TP. Ajouter un enregistrement d'adresse IP dans le fichier `/etc/bind/db.tx.lab.rt` pour le serveur web situé dans le sous domaine `tx.lab.rt`. Redémarrer le service DNS (bind9).
- 18) Afficher la page web en saisissant l'URL du site dans le navigateur. La page web s'affiche car la caméra IP (serveur vidéo) est dans le même réseau local que votre ordinateur. Pouvez-vous afficher la page web de la table voisine (simule une connexion depuis Internet) ? Visualisez-vous leur flux vidéo ?

3.3. Accéder au flux vidéo de la caméra IP depuis Internet

La table voisine qui simule la connexion à votre site depuis Internet ne peut pas afficher votre flux vidéo car l'attribut `src` de la balise `img` de votre page web indique l'adresse IP (privée) de votre caméra. De plus, par défaut, le pare-feu du routeur (R-GW-Tx) bloque tous les accès externes vers les équipements internes lorsque la fonction NAT est activée.

```

```

Il est donc nécessaire d'autoriser l'accès à votre caméra IP depuis le réseau public. Le service HTTP doit être accessible depuis l'extérieur et atteindre votre caméra à l'adresse 172.20.0.y (172.20.0.50 dans l'exemple). C'est la fonction « Translation de ports » du pare-feu du routeur Cisco RV215W qu'il faut configurer.

| Service qui doit être accessible depuis l'extérieur | Port externe | Port interne | Protocole de transport utilisé par le service | Adresse IP de l'équipement interne |
|---|--------------|--------------|---|------------------------------------|
| HTTP | 80 | 80 | TCP | 172.20.0.y |
| HTTPS | 443 | 443 | TCP | 172.20.0.y |

Remarque : le numéro de port identifie le service serveur.

Le service HTTPS n'est pas nécessaire pour accéder au flux vidéo à partir du site web mais permet d'administrer la caméra depuis une connexion Internet.

- 19) Se connecter au serveur web, ouvrir votre page du site web de vidéo et remplacer l'adresse IP privée de la caméra par son adresse IP publique.
- 20) Configurer la translation de ports sur le routeur à partir du menu Firewall.
- 21) Vérifier depuis la table voisine que vous pouvez visualiser le flux vidéo de votre caméra.

Partie 4: Annexes

Progression pédagogique – SAE1.2 « S’initier aux réseaux informatiques »

| Partie 1 – Découverte du réseau domestique | | | | | | | |
|---|--------|--------------------------|--------------------------|---|---|---------|--|
| Date | Séance | Durée | Type | Groupe | Description | Repères | Outils / Ressources |
| 29-sept | S1 | 1h | CM | promo | Présentation de la SAE | | |
| 2-oct 3-oct | S2 | 2h | NE | TP3 ; TP4 TP2 ; TP1 | Recherche des différents moyens permettant à un particulier d’accéder à Internet. Utilisation d’un outil pour caractériser la liaison WAN (débit, latence ...) et la comparer à d’autres technologies disponibles à votre adresse Evaluation de la couverture du réseau d’accès FTTH à votre adresse Evaluation de la latence du réseau à la manière de Degrouptest.com Rédaction d’un compte-rendu | Q1-Q10 | degrouptest.com cartefibre.arcep.fr ping, tracert |
| 10- oct 11- oct | S3 | 2h | NE | TP4 ; TP2 TP3 ; TP1 | Etude de la connectique de la Box Réalisation d’un schéma de la topologie physique | Q11-Q16 | Guide d’utilisation de la Box lucidchart.com app.diagrams.net |
| 12-oct 16-oct 18-oct 20-oct 31-oct 02-nov 6-nov 7-nov 9-nov | S4, S5 | 2h 2h | NE NE | TP4 TP1 TP2 TP3 TP2 TP1 ; TP3 ; TP4 TP2 ; TP3 TP1 TP4 | Utilisation d’outils de diagnostics (sous Windows, Android, web) pour caractériser le réseau domestique (adressage MAC, IPv4 statique / dynamique, masque de sous-réseau, préfixe réseau, passerelle par défaut, serveurs DNS, adresse IP privée et publique, localisation IP, service DHCP, test de débit, canaux WiFi, méthode d’authentification...) Consigner les différents résultats de diagnostics dans un tableau. | Q17-Q43 | Environnement PowerShell Terminal Emulator for Android Net Analyser for Android inSSIDer www.monip.org ip.lafibre.info www.hostip.fr www.iana.org/numbers www.ripe.net What_is_the_RIPE_NCC.mp4 |

| | | | | | | | apps.db.ripe.net/db-web-ui/query dnschecker.org nmap.org nmap.org/man/fr nmap.org/man/fr/man-briefoptions.html |
|---|--------|-------|------|-----------------|--|---------|--|
| 8-nov | S6 | 1h30 | TD | TD1 TD2 | Analyse des résultats obtenus et réalisation d'un schéma de la topologie complètement renseigné Evaluation du travail réalisé | Q44-Q45 | app.diagrams.net |
| Partie 2 – Installation d'un réseau domestique sous Packet Tracer et analyse des couches protocolaires | | | | | | | |
| Date | Séance | Durée | Type | Groupe | Description | Repères | Outils / Ressources |
| 14-nov | S7 | 2h | NE | TP4 | Installation d'un réseau domestique sous Packet Tracer | Q46-Q68 | Packet Tracer |
| 23-nov | S8 | 2h | | TP4 ; TP3 ; TP2 | Configuration du routeur sans fil avec les paramètres fournis afin d'assurer un accès filaire et sans fil | | |
| 24-nov | | | | TP1 | Modélisation du réseau du réseau domestique | | |
| 28-nov | | | | TP2 ; TP3 | Mise en évidence du principe d'encapsulation | | |
| 29-nov | | | | TP1 | Analyse protocolaire Modélisation d'un échange entre deux périphériques | | |
| 21-nov | S9 | 1h30 | TD | TD1 ; TD2 | Synthèse de l'analyse de flux entre deux périphériques Introduction à l'analyse de flux réseau avec Wireshark | Q66-Q68 | Packet Tracer Wireshark |
| 1-dec | | | | TP4 | Analyse de flux entre deux périphériques, sous Packet Tracer et sous Wireshark | Q66-Q68 | Packet Tracer Wireshark |
| 4-dec | | | | TP3 | | | |
| 5-dec | | | | TP1 ; TP2 | | | |

| Partie 3 – Déploiement d’un réseau informatique et mise en place d’un service de vidéo surveillance | | | | | | | |
|---|----------|-------|------|--|--|---------|--|
| Date | Séance | Durée | Type | Groupe | Description | Repères | Outils / Ressources |
| 6-dec 11-dec 12-dec 14-dec | S10 | 2h | NE | TP4 TP2 TP1 TP4 TP3 TP3 TP1 TP2 | Etude du cahier des charges en vue de déployer un réseau domestique dans la salle de TP Conception du réseau : adressage IP, plage DHCP, SSID, méthode d’authentification Services à mettre en place : service de vidéo surveillance | | Wireshark |
| 22-dec 9-janv 12-janv 16-janv | S11, S12 | 6h | TP | TP1 TP3 TP2 TP4 | Déploiement du réseau filaire et sans fil Mise en place d’une caméra de vidéo surveillance Mise en place du service de vidéo surveillance sur le serveur HTTP du FAI Capture du flux video avec Wireshark et identification des couches selon le modèle OSI. Capture du flux lors de l’authentification au service de vidéo surveillance non sécurisé et explantation pour retrouver les identifiants de l’utilisateur Evaluation : Démonstration du fonctionnement / Explications / Questions orales / QCM | | Cisco RV215W Caméra IP D-Link / Axis Wireshark |