Intitulé de l'épreuve : Réseaux et Télécommunications

Nombre de copies : 4

Numérotez chaque page (dans le cadre en bas de la page) et placez les feuilles dans le bon sens.

Partie 1

Exercice 1a.

1) Le modèle osi est une norme décrivant un réseau en le modélisant par couches. Chaque couche inférieure est responsable du traitement des données nécessaire aux couches supérieures, ce qui permet un raffinement dans le traitement dans les couches les plus hautes.

La couche 1 : physique, décrit la façon dont deux équipements voisins communiquent du point de vue de leurs signaux.
Ils échangent en bits.

La couche 2 : liaison, décrit comment deux équipements voisins échangent de façon ~~sécurisée~~ à vérifier l'intégrité des échanges.
L'unité de données est la ~~datagramme~~ trame

La couche 3 : réseau, ~~décrit~~ permet grâce à une introduction d'adressage, de faire communiquer des équipements distants.
L'unité de donnée est le datagramme.

N° 1/4.

La couche 4 - Transport. Elle permet de prendre en compte la finalité d'un ~~est~~ datagramme échangé (pour quel type d'application le paquet est destiné). Elle a également pour rôle d'assurer un contrôle de flux entre 2 hôtes.
L'unité de données est le paquet.

La couche 5 - Session : Elle permet d'assurer quelques mécanismes d'authentification à un échange.
L'unité est le datagramme de couche session.

La couche 6 - Présentation : Elle permet d'ajouter un niveau d'abstraction entre des hôtes qui n'ont pas forcément les mêmes systèmes de données (par exemple la façon de mémoriser des entiers, mais également des tables de caractères, les dates ...)
L'unité est le datagramme de couche présentation.

La couche 7 - Application : La couche la plus haute, c'est celle qui a besoin d'échanger, et qui traite les données grâce aux couches inférieures.

2) Dans la couche 1, ARP (adresse resolution Protocol, situé entre les couches 2 et 3) et ATM (protocole réseau et transport) sont à rayer.

Dans la couche 2, tous les protocoles sont bons.

Dans la couche 3, UDP est mal placé (protocole de niveau transport)

Dans la couche 4, IP v6 est de couche réseau, ~~ainsi que~~ et PPP (point-to-point protocol), de couche liaison.

N° 1/4..

Dans la couche 5, Netbios est un protocole de couche réseau, et UDP aussi. RPC et SMB, servent à des applications et offrent des mécanismes de l'authentification, peuvent être considérés comme des protocoles de couche session

Dans la couche 6, on parle en effet de normes permettant à des hôtes de conception différentes de communiquer. ASCII et MIME sont donc accepté, SMB et HTTP non.

Enfin, dans la couche 7, tous ces protocoles sont également des applications et peuvent donc être considérés comme de couche applicative. Cependant, SNMP est clairement destiné à auditer les couches réseau et devrait donc être rangé,
3)

4) Le protocole ARP (address resolution Protocol) est un lien entre la couche liaison et IPv4 qui permet pour un hôte, à partir de son adresse IPv4 et d'envoi d'une trame multicast, de connaître l'adresse physique de l'hôte recherché présent sur le même réseau local.

Il existe un protocole inverse : R-ARP (Reverse Adress Resolution Protocol) permettant, à partir d'une adresse physique, de demander l'adresse IPv4 d'un hôte du réseau.

Exercice 1 b :

Signal physique	Support de transmission
Onde électrique	Câble réseau en métal.
Onde électromagnétique	Vide, air, fibre optique
Onde mécanique	Matériau solide, eau...

N° A.1.4

Exercice 1 c.

1) Le Wifi est classé en normes dans la famille 802.11 Celle-ci est déclinée en versions par des lettres, comme 802.11b, 802.11i, 802.11ac...

Les normes définissent les caractéristiques matérielles permettant d'atteindre des vitesses de transmission théoriques et des distances maximales de signal.

2) Le SSID (Identificateur de signal) est le nom donné à un réseau Wifi. C'est celui qui sera visible de l'utilisateur qui le choisira parmi les réseaux disponibles à son emplacement.

Le canal est la bande de fréquence choisie par un point d'accès Wifi pour émettre. Il existe deux grandes bandes autour de 2,4 GHz et 5 GHz, utilisables selon la norme Wifi, et chacune d'elles est divisée en canaux (respectivement une dizaine et une vingtaine)
Pour de performances Wifi optimales, un point d'accès devra choisir un canal vide, ou du moins pas trop utilisé, ainsi que laisser un canal libre ~~entre~~ de distance fréquentielle avec les canaux voisins.

3) Le Wifi a connu deux ~~grandes~~ grandes familles de protocoles de sécurisation :

- le WEP est le plus ancien, et repose sur des vieux algorithmes. Non évolutif, il contient de nombreuses failles qui l'ont rendu obsolète et abandonné.

- le WPA est un protocole évolutif, paramétrable selon divers protocoles d'authentification et de chiffrement. Il a évolué en WPA2

N°

Intitulé de l'épreuve : Réseaux et Télécommunications

Nombre de copies : 4

Numérotez chaque page (dans le cadre en bas de la page) et placez les feuilles dans le bon sens.

Exercice 1d.

$(252)_{10} = (11111100)_2$

$(48)_{10} = (30)_{16}$

Exercice 1e.

1) Le MTU (Maximum Transmission Unit) est la taille maximale convenue entre deux équipements voisins pour échanger dans la couche liaison.

2) Le MTU peut être mis à défaut si les couches supérieures définissent des paquets plus grands que le dépassement de ce MTU. Normalement, ces paquets sont automatiquement fragmentés par la couche liaison, mais il se peut qu'il soit impossible de le faire. C'est notamment le cas avec des protocoles de tunnel tels qu'IPSec. Dans ce cas, les paquets sont perdus.

3) Ces erreurs entraînent des tunnels IPsec inutilisables : ils paraissent bien ouverts, mais ils sont inexploitables, les paquets y transitant étant rejetés par la couche physique.

N° 2.1.4.

4) Des logiciels d'analyse de trames tels que tcpdump ou wireshark sont toujours utiles pour visualiser des paquets perdus à cause du MTU. IPSec complique hélas l'analyse.

Il est également possible d'émettre avec des commandes SNMP des paquets non fragmentables pour simuler des erreurs de MTU

Partie 2

Exercice 2.1.

1) Il y a manifestement un problème d'organisation dans le plan d'adressage de cette entreprise :

- les différents service ont des réseaux qui se télescopent autour des adresses 192.168.10.1 à 192.168.10.31.
- le plan ne peut pas tenir la route car les seuls services techniques et client se partagent déjà l'ensemble du réseau, ne laissant aucune adresse aux 2 autres services et aux routeurs.

Voici un plan d'adressage viable et optimisé au plus juste pour les tailles des services :

Sous-Reseau	Adresse	Masque	CIDR	1° adresse	Dernière adresse
Interco	192.168.10.0	255.255.255.248	29	192.168.10.2	192.168.10.6
Administratif	192.168.10.16	255.255.255.240	28	192.168.10.18	192.168.10.30
Comptabilité	192.168.10.32	255.255.255.224	27	192.168.10.34	192.168.10.62
Client	192.168.10.128	255.255.255.192	26	192.168.10.130	192.168.10.190
Technique	192.168.10.192	255.255.255.192	26	192.168.10.194	192.168.10.254

(Pour les adresses utilisables, j'ai enlevé l'adresse de réseau ainsi que

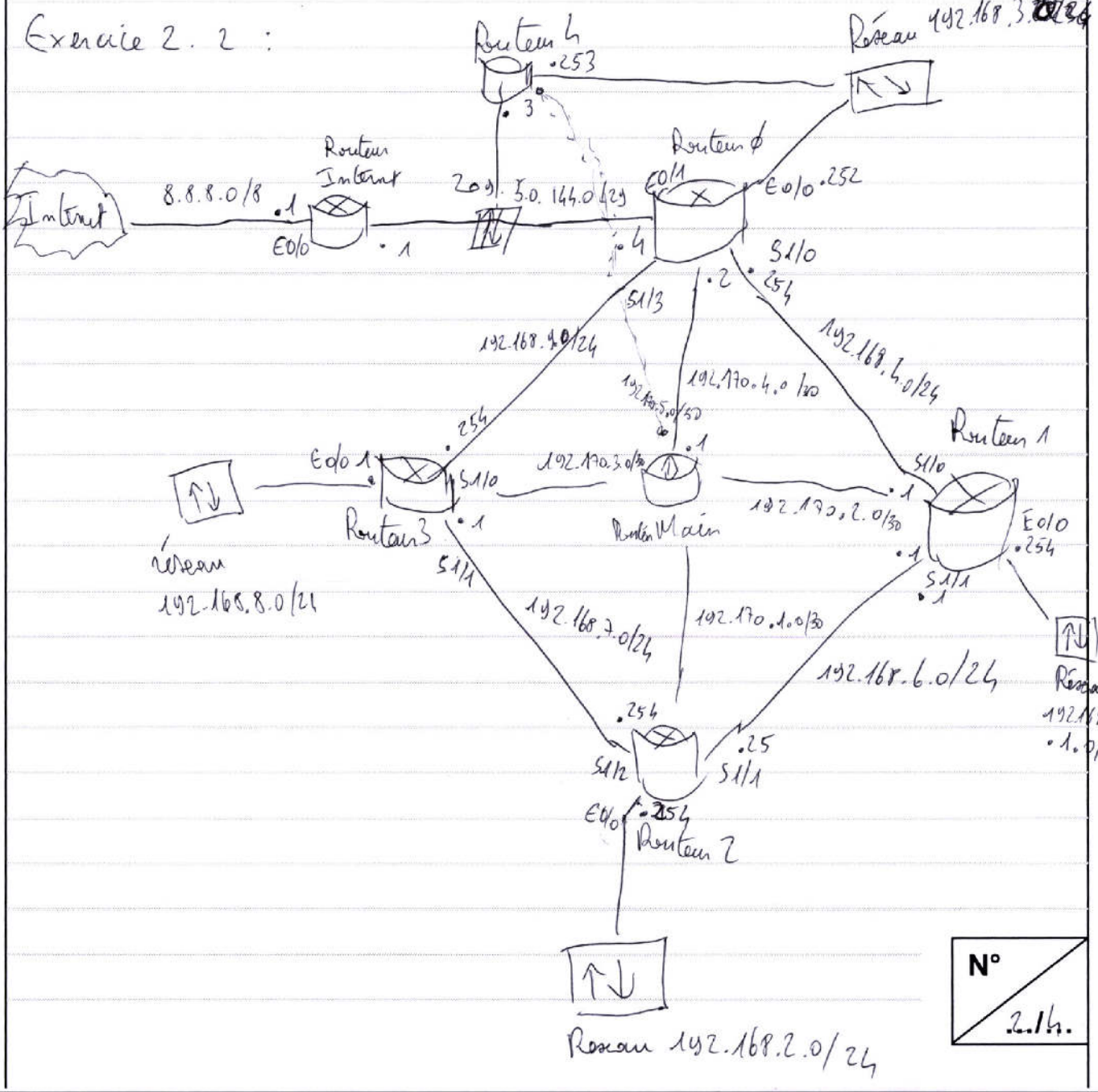
N° T.I.b

la première adresse dédiée au routeur au début de chaque plage. Dans les fins de plage, il faut retirer la dernière adresse désignée au multicast)

2) Le plan d'adressage précédent laisse une plage de 64 adresses utilisables qui pourra être exploitée pour un service supplémentaire. Le sous-réseau serait :

Adresse : 192.168.10.64
Masque : 255.255.255.192
CIDR = 26
Première adresse utilisable (sans compter le routeur) : 192.168.10.66
Dernière adresse : 192.168.10.126.

Exercice 2.2 :



N° 2.1b.

2) Quand l'utilisateur du site B fera un PING 209.50.144.1 ;

- Le paquet sera d'abord traité par sa passerelle par défaut, maintenant le routeur 1, en 192.168.1.254.

- Sur le routeur 1, il n'y a pas de règle traitant le réseau 209.50.144.0. Il empruntera donc la passerelle par défaut du routeur, 192.170.1.1, donc le routeur "Main".

- Sur le routeur main, il y a un protocole OSPF mis en place. Il a donc reçu de routeur 4 son message, à savoir sa proximité avec le réseau 209.50.144.0/29 ~~transmettant~~.

- Le paquet est donc traité par le routeur 4. Le paquet étant destiné à une adresse traitée par l'une de ses interfaces, une route implicite existe donc, et sa table ARP permettra de délivrer le paquet à "Routeur Internet", le destinataire de cette requête SNMP

N° 2.1.4

Intitulé de l'épreuve : Réseaux et Télécommunications

Nombre de copies : 4

Numérotez chaque page (dans le cadre en bas de la page) et placez les feuilles dans le bon sens.

Partie 2.

3) La commande de recherche des voisins directs montre que cet hôte a pour voisins actifs les hôtes 192.168.4.1, 192.168.3.253, 192.168.9.254 et 192.170.4.1

D'après le schéma, on est donc ici sur le routeur 0, qui montre ses voisins routeur 1 (192.168.2.1) et routeur 3 (192.168.9.254), ainsi qu'un routeur ~~[illegible]~~ Main sur Serial 1/1 et le réseau local désservi par Routeur 0.

Le grand absent de cette commande est le voisin Routeur Internet. Une panne est peut-être en cours sur le réseau entre Routeur 0 et Internet.

4) En OSPF, le "Designated routeur" est désigné automatiquement grâce à des mesures de performances régulières mises en place entre deux voisins. Cette situation peut être administrée en définissant d'autres valeurs.

5) Certaines interfaces des routeurs 0 et 4 ont des adresses secondaires en "Standby".

Ces interfaces peuvent être activées en cas de détection de panne sur l'hôte portant réellement cette adresse. Ainsi, les routeurs 0 et 4 agissent en continuité d'activité l'un avec l'autre vis à vis

N° 3.1.4

[redacted]

de réseaux 192.168.3.0 et 209.50.144.3.

Partie 3 :

1) Je propose pour l'infrastructure de câblage une modèle en simple étoile, l'ensemble de toutes les prises étant liées à une armoire de répartition dans le local technique TO.

Il n'est en effet pas fait mention d'autre locaux techniques, et la sécurité impose donc de faire déboucher les câblages dans un local sécurisé.

A raison de 3 prises réseau par bureau, cela amène donc à un répartiteur de 90 prises.
Selon la taille des bureaux, il faudra peut-être en prévoir 6, ce qui peut amener à 180 prises. En fonction du nombre d'equipements, il faudra prévoir assez de commutateurs (assez de prises pour chaque agent) physiques.
Niveau services, il faudra au moins prévoir 3 hôtes dans le cadre d'une virtualisation complète : ce sont les recommandations des fournisseurs de virtualiseurs pour se premunir de pannes sur l'infrastructure : ceux-ci devraient être dans une DMZ.
Enfin, le Wifi, si nécessaire, devrait faire l'objet d'un réseau dédié afin de limiter une attaque.

L'ensemble devrait être protégé par des onduleurs, 2 au minimum.

N° 3.14.

Physiquement, le Répétiteur ressemblerait à ça :

Les réseaux se devront d'être séparés les uns les autres, avec des routes entre eux pour ne garantir que les flux essentiels.

2) Avec 30 agents, en imaginant qu'ils ont chacun 4 équipements réseau, il faudrait une nombre de 120 adresses, plus la dizaine de mieux.

Un masque de 25 (128 adresses) conviendrait, néanmoins choisissons un masque de 24 (256 adresses pour plus de confort)

On pourrait avoir, sur le réseau privé classique 192.168.0.0/24 :

Rés1 : 192.168.0.0/29 : routeur internet, équipements réseau

Rés2 : 192.168.0.16/28 : équipements de service, routeurs

Rés3 : 192.168.0.128/26 : équipements des utilisateurs, réseau filaire

Rés4 : 192.168.0.192/26 : équipements des utilisateurs en Wifi

Ces quatre réseaux sont choisonnés, et il faudrait définir

N° 3.1.5.

des règles entre eux :

ex : Res 3 → Rés 0 : autoriser HTTPS, Protocoles Mail, Protocoles des applications propriétaires.

Res 4 → Res 0 : autoriser l'accès Web.

Res 0 → Internet : autoriser uniquement certains accès pour les besoins des applications.

~~Internet~~ → Res 0 : autoriser l'accès au webmail de l'entreprise

Exercice 3 b :

1) Une manière économique pour interconnecter A et B serait d'ouvrir un accès à Internet ~~entre les~~ sur B et de mettre en place un tunnel VPN entre les deux.

L'inconvénient est le manque de robustesse et d'évolutivité de cette solution : un accès internet tombe, ou le VPN tombe en panne, et l'interconnexion est rompue
Une alternative intéressante serait de souscrire une offre de M2PS (Multi Layer). Cela permet d'avoir un niveau d'abstraction entre le réseau et les besoins, de définir au mieux ce que l'on souhaite échanger entre les sites.

2) En règle générale, cette interconnexion provoquera des transits de données entre deux sites distants, via internet ou le réseau d'un opérateur.

Il faudra donc veiller à ce qu'un chiffrement de bout en bout soit mis en place.
Le protocole IP Sec permet des chiffrements sur la liaison, ou on peut acquérir des équipements dédiés.

On veillera aussi à ne pas ouvrir des flux plus que nécessaires entre les sites

N° 3.14.

Intitulé de l'épreuve : Réseaux et Télécommunications

Nombre de copies : 4

Numérotez chaque page (dans le cadre en bas de la page) et placez les feuilles dans le bon sens.

Exercice 3 - suite.

1) La VoIP peut avoir des impacts de deux ordres sur le réseau de l'entreprise :

- Des impacts de performance d'abord : la VoIP, notamment si elle transporte aussi l'image, peut être source de congestionnements de réseaux, ou tout le moins avoir un net impact.

La mise en place devrait donc s'accompagner sur les équipements réseau de configurations de Qualité de Service (QoS), permettant de marquer les flux selon leur importance, maîtrisa par exemple la VoIP pour qu'elle empêche de nuire au reste des applications quitte à baisser sa qualité.

- L'autre impact est évidemment la sécurité. Selon l'organisation choisie, il sera nécessaire d'ouvrir des flux entrants sur Internet.

Là encore, une maîtrise des règles de firewall doit permettre de contenir la menace

N° 4 1.4

2) Pour permettre de la mobilité aux utilisateurs, il sera nécessaire d'ouvrir un point d'accès VPN. Chiffré, celui-ci permettra aux utilisateurs d'accéder à leurs données de manière confidentielle.

Attention cependant, cette ouverture nécessitera une sécurisation accrue du poste client, afin d'éviter une compromission par l'un d'eux. Les collaborateurs devront en outre être responsabilisés à la sécurité de leur matériel et à signaler rapidement toute perte ou anomalie constatée

N° 4.1.4

N°

... /...

N°

... /...