Activité 6 : IP et TCP

Visionner la vidéo sur le protocole IP et TCP

Question 6.1. A quel système de distribution ressemble Internet ?

Question 6.2. Indiquer par une croix le rôle de chacun des protocoles d'internet

	Renseigne des informations Complémentaires sur les messages	Découpe les messages en paquets et les regroupe pour l'envoi
Protocole TCP		
Protocole IP		

La commande ipconfig /all a été faite à partir d'un ordinateur voici la capture d'écran correspondante

```
Configuration IP de Windows

        Nom de l'hôte . . . . . . . . . . . . : portable6400
        Suffixe DNS principal . . . . . . . :
        Type de noud . . . . . . . . . . . . : Inconnu
        Routage IP activé . . . . . . . . . . : Oui
        Proxy WINS activé . . . . . . . . . . : Non
        Liste de recherche du suffixe DNS : home
                                            home

Carte Ethernet Connexion réseau sans fil 4:

        Suffixe DNS propre à la connexion : home
        Description . . . . . . . . . . . . : Intel(R) PRO/Wireless 3945ABG Networ
k Connection
        Adresse physique . . . . . . . . . . : 00-18-DE-8A-9D-DF
        DHCP activé. . . . . . . . . . . . . : Oui
        Configuration automatique activée . . . . : Oui
        Adresse IP. . . . . . . . . . . . . . : 192.168.1.18
        Masque de sous-réseau . . . . . . . . : 255.255.255.0
        Passerelle par défaut . . . . . . . . : 192.168.1.1
        Serveur DHCP. . . . . . . . . . . . . : 192.168.1.1
        Serveurs DNS . . . . . . . . . . . .  : 192.168.1.1
        Bail obtenu . . . . . . . . . . . . . : mercredi 9 juillet 2008 21:40:27
        Bail expirant . . . . . . . . . . . . : mercredi 16 juillet 2008 21:40:27

Carte Ethernet Connexion au réseau local:

        Suffixe DNS propre à la connexion : home
        Description . . . . . . . . . . . . : Broadcom 440x 10/100 Integrated Cont
roller
        Adresse physique . . . . . . . . . . : 00-15-C5-B4-8A-42
        DHCP activé. . . . . . . . . . . . . : Oui
        Configuration automatique activée . . . . : Oui
        Adresse IP. . . . . . . . . . . . . . : 192.168.1.12
        Masque de sous-réseau . . . . . . . . : 255.255.255.0
        Passerelle par défaut . . . . . . . . : 192.168.1.1
        Serveur DHCP. . . . . . . . . . . . . : 192.168.1.1
        Serveurs DNS . . . . . . . . . . . .  : 192.168.1.1
        Bail obtenu . . . . . . . . . . . . . : mercredi 9 juillet 2008 21:26:10
        Bail expirant . . . . . . . . . . . . : mercredi 16 juillet 2008 21:26:10
```

Questions 6.3. Relevez les éléments suivants de la configuration réseau de votre poste :

Adresse IP		Adresse physique*	
Masque de sous-réseau		Serveur DHCP	
Passerelle par défaut		Serveur DNS	

* Adresse MAC est synonyme de « Adresse physique »

En vous aidant de recherches sur internet,

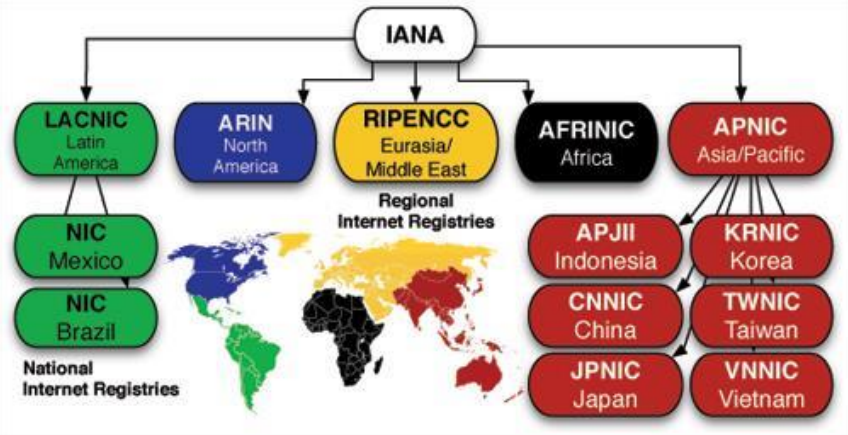
Question 6.3 bis. Pour chaque ligne, Entourez la réponse concernant les adresses proposées

	Adresse IP (version 4)	**Adresse MAC**
00 :37 :6C : E2 : EB :62	OUI - NON	OUI - NON
1 Avenue Pierre Mendès France, 77186 Noisiel	OUI - NON	OUI - NON
01.60.37.56.56	OUI - NON	OUI - NON
168.212.226.204	OUI - NON	OUI - NON

Aller sur https://www.mon-ip.com/ puis cliquer sur « mon adresse IP publique » Relever l'adresse déterminée par le site internet.

Question 6.4. Comparez vos 2 adresses trouvées avec celles de votre voisin. Avez-vous une adresse commune identique ? Si ce n'est pas votre adresse IP, de quelle adresse pourrait-il s'agir ?

Les adresses IP publiques étant visibles au monde connecté, il est intéressant de savoir que l'organisme régulant la distribution des adresses publiques est l'IANA.



Question 6.5. A l'aide d'internet et du schéma ci-dessus, recherchez a. la définition de l'IANA

b. la définition de l'entité qui distribue les adresses IP publiques pour la France

A retenir :

L'information ne voyage pas seul. Il lui faut des données complémentaires (ex : expéditeur, destinataire, accusé réception). C'est le protocole IP qui gère cela. De plus, pour s'adapter aux capacités de transmission des réseaux, l'information est fragmentée et identifiée au départ, pour être ensuite reconstituée à l'arrivée. C'est le protocole TCP qui gère cela.

Les adresses IP sont les numéros qui permettent aux ordinateurs et aux objets connectés de communiquer les uns avec les autres. Une adresse IP peut être publique (visible sur Internet) ou privée (visible sur le sous). Les blocs d'adresses publiques sont attribués par l'IANA de façon internationale, aux cinq zones régionales (RIPE NC pour l'Europe).

Activité 7 : découverte du DNS

Ouvrir un navigateur web, puis tapez dans l'URL l'adresse: www.qwant.fr

Ouvrir de nouveau un navigateur web, puis tapez dans l'URL l'adresse IP: **194.187.168.99**

(Vous devrez probablement à autoriser la page dans le bouton « Avancé ») ❼

Ce que vous observez alors est l'effet du serveur DNS.

Question 7.1. D'après cette observation, quel est le rôle apparent du serveur DNS?

□ Un répétiteur, envoyant à multiples reprises la requête IP au navigateur web

□ Un annuaire, traduisant l'adresse symbolique en adresse IP pour le navigateur web

□ Un explorateur, recherchant constamment les sites web pour trouver celui de la requête

Visionner la vidéo sur les actions du DNS

Question 7.2. En combien d'étapes (ou serveurs) la requête se réalise-t-elle ?

❼ Prendre connaissance du tableau de noms de domaines, ainsi que faire une recherche avec un moteur de recherche web sur la « *liste des noms de domaines par pays* »

Question 7.3. A partir de ces informations, déterminez la classification correspondant à l'extension :

- ".com" : _____
- ".edu" : _____
- ".fr" : _____
- ".de" : _____
- ".us" : _____

Les serveurs correspondant aux domaines de plus haut niveau sont appelés « serveurs de noms racine » et possèdent les noms « a.root-servers.net » à « m.rootservers.net ».

❼ Ouvrir le navigateur de votre ordinateur et visiter le site internet https://root-servers.org/

Question 7.4. A partir de votre recherche sur le site internet, Relevez le nombre de serveurs racines de DNS total en France, ainsi que les principales grandes villes auxquelles ils sont rattachés.

Activité 8 : Vulnérabilité des IP et DNS

Visionner la vidéo sur la cyberattaque sur DNS de 2016

Question 8.1. Comment l'attaque « par déni de service » a-t-elle fonctionné?

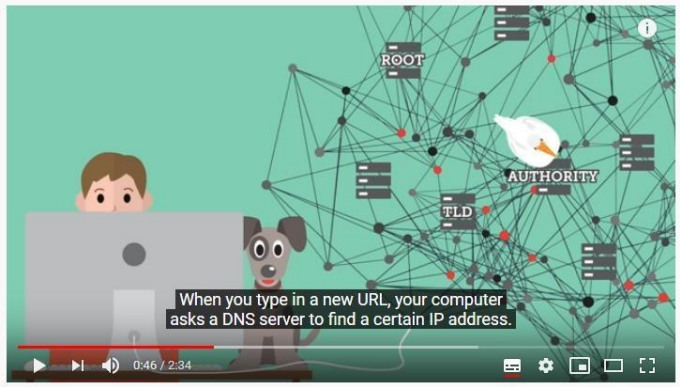
□ par refus de faire fonctionner internet en bloquant l'accès des internautes

□ par arrêt total des serveurs web, en coupant physiquement l'alimentation électrique

□ par saturation du serveur DNS avec des milliards de requêtes

Question 8.2. Quels systèmes électroniques mériteraient d'être mieux protégés?

Visionner la vidéo sur les risques avec les serveurs DNS (ou : https://www.youtube.com/watch?time_continue=64&v=ot9BrVTzRBs&feature=emb_logo)



Question 8.3. Quels sont les 3 risques dans l'utilisation de serveurs DNS non cryptés?

- _____
- _____
- _____

Autre exemple : parfois il est prudent de ne pas se fier à l'adresse symbolique et de s'intéresser à l'adresse IP.

Imaginez, vous venez de recevoir un mail douteux qui dit ceci :

Cher(e) Client(e);

*Nous enregistrons ce Jeudi 04 février 2016 un chèque d'un montant de *€340*.00 EUR* *à l'ordre de MR LUSTIG VICTOR - 1 RUE ARSENE LUPIN - 39250 SHERWOOD – France émis par *M.VERGER BENOÎT - 18 ALLEE DES TILLEULS - 64122 URRUGNE- FRANCE **

*REMARQUE: Il est impératif de nous faire parvenir en répondant à ce mail (1) code de recharge PCS * de €100.00 EUR* pour vous acquitter des frais d'assurance. Dès réception et approbation du code après vérification, votre*

chèque vous sera expédié immédiatement. Vous le recevrez par courrier dans un (1) jour au maximum, à compter du jour de réception du code de la recharge PCS MASTERCARD. Christian SAINZ, Directeur Relation Client, DHL Finance

Vous n'êtes pas bien sûr de comprendre pourquoi on vous envoie ça (pourtant c'est bien vous, Victor Lustig) mais il semble facile de gagner les 240€ promis. Que faire ?

Il faut être prudent et vérifier la provenance exacte de ce message, vérifier si tout colle bien. Voici l'entête complet de ce mail (qu'on peut faire apparaître, par ex. dans Gmail, en cliquant sur les trois points verticaux en haut à droite du message, puis « Afficher l'original ») :

Delivered-To: isn.pourriel@gmail.com
Received: by 10.27.14.197 with SMTP id 66csp330398wlo;
Thu, 4 Feb 2016 00:23:13 -0800 (PST)
X-Received: by 10.55.15.199 with SMTP id 68mr2039057qkp.42.1454574192794;
Thu, 04 Feb 2016 00:23:12 -0800 (PST)
Return-Path: service.dhl.international@post.com
Received: from mout.gmx.com (mout.gmx.com. [74.208.4.200])
by mx.google.com with ESMTPS id a141si9579378qkb.16.2016.02.04.00.23.12
for isn.pourriel@gmail.com
(version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
Thu, 04 Feb 2016 00:23:12 -0800 (PST)
Received-SPF: pass (google.com: domain of service.dhl.international@post.com designates 74.208.4.200 as permitted sender) client-ip=74.208.4.200;
Authentication-Results: mx.google.com;
spf=pass (google.com: domain of service.dhl.international@post.com designates 74.208.4.200 as permitted sender) smtp.mailfrom=service.dhl.international@post.com
Received: from [192.168.1.100] ([41.191.68.245]) by mail.gmx.com (mrgmxus001) with ESMTPSA (Nemesis) id 0LrNUo-1a4NkD30Ga-01354l for isn.pourriel@gmail.com; Thu, 04 Feb 2016 09:23:11 +0100
From: "Service Expédition et Validation" service.dhl.international@post.com
To: isn.pourriel@gmail.com
Subject: CONFIRMATION DU DÉPÔT DE CHÈQUE DE BANQUE CERTIFIE

Nous pouvons distinguer ici l'adresse IP du serveur de prestataire DHL (74.208.4.200) et celui du serveur de l'expéditeur de l'email (41.191.68.245).

Allez sur le site https://ipgetinfo.com et cherchez des renseignements sur ces 2 adresses IP.

Question 8.4. Concluez alors si cette adresse est compatible avec l'expéditeur supposé

A retenir :

Le DNS convertit les adresses symboliques des sites web en adresses IP. Il fonctionne comme un annuaire réparti en plusieurs serveurs dans le monde, et qui ont chacun une partie en charge.

L'adressage IP est un élément clé sur internet car les tentatives de fraudes et les cyberattaques se basent essentiellement sur le détournement de ces adresses pour pirater.