TD4 – Sujet de synthèse

MARS ESCAPE ... Quelque part dans l'espace à des centaines de milliers de kilomètres de la terre

"Radio: ....

Vous: Pfff... la radio est endommagée également...je crois que je n'ai plus le choix je vais activer la capsule d'évacuation d'urgence pour rejoindre la Terre

(Vous cherchez votre xDroidPhone)

Vous: Heureusement que j'ai noté le code d'activation de la capsule dans ma mémoire externe...et dire que nos ancêtres utilisaient leurs cerveaux pour retenir des informations; quel gâchis...

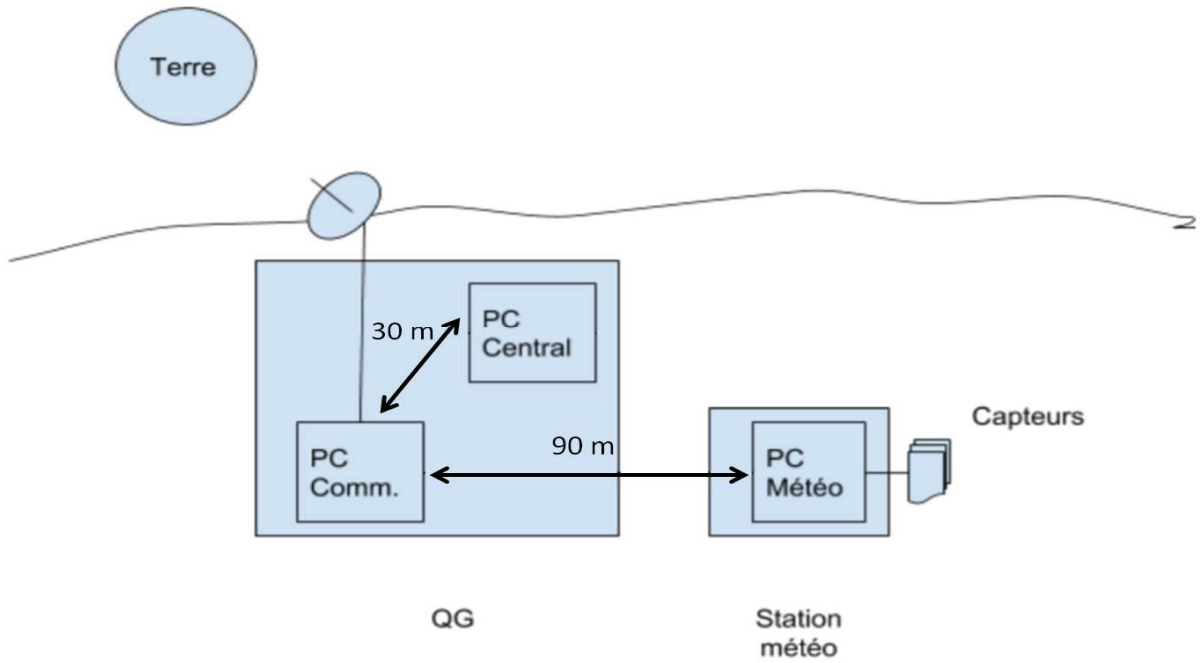
(L'écran du xPhoneDroid reste inactif)
Vous: il ne s'allume pas il est également endommagé... je dois absolument avoir le code d'activation de la capsule sinon je vais crever ici !

Vous: alors la station est composée d'une station météo autonome avec un vieux PC linux et de différents capteurs. La station météo est reliée par une connexion filaire à un différent PC de communication qui transmet périodiquement les données vers la terre. D'après le diagnostic de l'ordinateur de bord, le PC de communication semblerait OK; par contre la station météo est down....Je vais lancer un diagnostic avancé sur la station météo....

Vous: OK je vois le problème; si j'arrive à mettre en place un nouveau gestionnaire de fichiers sur la station météo elle sera capable d'envoyer des bulletins météo et je suis sûr que je pourrai hacker les messages météo pour transmettre un SOS à la terre et demander le code de la capsule..."

La situation actuelle :

Plan de la station et des équipements :



Le système de fichier est OK ,mais aucune donnée n'est transmise par le PC Comm, il faut vite identifier le problème et le résoudre.

Vous : Pas de panique, je vais essayer de remettre en état la liaison entre la station météo et le PC Comm puis, je profiterai de la connexion pour récupérer l'adresse IP et le numéro de port utilisé par le PC Comm et écrire une petit

client en C, pour envoyer mon message de SOS. Pour cela , j'aurais besoin de me connecter à partir de mon troisième PC central sur le même réseau que le PC Comm et la Station météo.

1 ère partie : Remise en état du réseau

A - Dans un premier temps vous vérifiez les connexions de votre réseau.

La commande : ping pc.comm.mars, donne le résultat ci-dessous :
Envoi d'une requête 'ping' sur pc.comm.mars [192.168.10.254] avec 32 octets de données :
Réponse de 192.168.10.254: octets=32 temps=52 ms TTL=51
Réponse de 192.168.10.254: octets=32 temps=55 ms TTL=51
Réponse de 192.168.10.254: octets=32 temps=54 ms TTL=51
Réponse de 192.168.10.254: octets=32 temps=55 ms TTL=51
Statistiques Ping pour 192.168.10.254: Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),

La commande : ping station.meteo.mars donne le résultat ci-dessous :
La requête Ping n'a pas pu trouver l'hôte station.meteo.mars . Vérifiez le nom et essayez à nouveau.

1 - Quel est le rôle de la commande ping ?

La commande IPCONFIG sur le PC COM donne le résultat ci-dessous :
Carte Ethernet Connexion au réseau local 1 :
Adresse IPv4. . . . . : 2.1.1.254
Masque de sous-réseau. . . .. : 255.255.0.0
Passerelle par défaut. . . ..: 2.1.1.1

Carte Ethernet Connexion au réseau local 2 :
Statut du média. . . . . : Média déconnecté
Suffixe DNS propre à la connexion. . . : pc.com.com

La commande IPCONFIG sur la station météo donne le résultat ci-dessous :
Carte Ethernet Connexion au réseau local 1 :
Statut du média. . . . . .: Média déconnecté
Suffixe DNS propre à la connexion. . . : station.meteo.com

2 - Quel est la rôle de la commande IPCONFIG ?
3 - A quoi correspondent les informations affichées ? Détaillez vos réponses et donnez «également les classes d'adresse utilisées
4 - Que déduisez vous de ces résultats ?
5 - Y-a-t-il un routeur dans ce réseau ?

B - Il y a de fortes chances que les équipements de transmission du réseau local soient endommagés.
Pour ne pas perdre trop de temps, vous envisagez de recâbler ce réseau local. Vous avez à disposition un Hub, un Switch et un routeur, ainsi que plusieurs segments de câble, type paire torsadée, d'une longueur de 50 mètres chacun.
Sachant que vous souhaitez relier les machines du site (cf plan ci-dessus).
6 - Déterminez quel(s) équipement(s) de connexion (HUB, Switch, Routeur, ...) sont nécessaires et pourquoi?

C - Après cette réorganisation du réseau vous souhaitez que la table de routage de la station météo soit configurée comme ci-dessous

Destination	Masque	Passerelle
0.0.0.0	0.0.0.0	192.168.10.254
192.168.10.0	255.255.255.0	192.168.10.10

127.0.0.0	255.0.0.0	127.0.0.1
255.255.255.255	255.255.255.255	192.168.10.10

7 - Déterminez le plan de câblage de votre réseau local

Sachant que la commande ipconfig peut s'utiliser pour configurer l'interface IP comme suit :
IPCONFIG SET interface ip-addr subnet-mask [dst-addr]
Remarque : dst-addr = passerelle par défaut, cette valeur est optionnelle

Exemple : IPCONFIG SET ETH1 162.38.10.1 255.255.0.0 162.38.1.1
Configure la carte Ethernet 1 avec comme adresse IP 162.38.10.1, un masque ayant la valeur 255.255.0.0 et comme passerelle la machine d'adresse 162.38.1.1

8 - Donner la liste des commandes qui permettront de reconfigurer chaque machine du réseau
9 - Quelle sera la table de routage du PC-COM après configuration ?

2 ème partie : Création de l'application de communication

Voilà, après les quelques minutes nécessaires à la réinitialisation des équipements et des applications, la station météo se remet à transmettre les données au PC-Comm et ce dernier transmet à son tour les données vers la terre. Vous avez vérifié tout cela grâce à un analyseur de trames installé sur le PC-Comm

10 - Expliquez l'échange de données de l'annexe 1

Il ne vous reste plus qu'à créer une application client C, sur le PC Central, qui va envoyer à la terre le message :
SOS - Code d'activation de la capsule attendu !!

En vous aidant des fonctions C de l'annexe 2, créer une application cliente qui va transmettre ce message puis attendre et afficher la réponse.

11 - Expliquez la logique de votre application
12 - Proposer le code

Remarque : Vous disposez d'une fonction : init-sock-addrin (n°port, addr-IP-serveur, *sock_addr_serv); qui initialise le champ sock_addr_serv de type : struct sockaddr_in

3 ème partie : AIE, ca ne marche toujours pas ...

En fait après plusieurs tentatives , vous ne recevez aucune réponse, et là vous vous souvenez que l'application serveur est protégée pour ne traiter que des messages venant de la station météo et contenant une séquence particulière que vous ne connaissez pas.

Vous vous souvenez aussi, que les équipements sur terre sont protégés par un pare-feu qui émet des messages d'alerte lorsqu'il soupçonne un DoS.

13 - Qu'est ce qu'un pare-feu ? Comment fonctionne-t-il ?
14 - Qu'est ce qu'un DoS ? Quelle peuvent être les conséquences de ce type d'attaque sur un serveur ?

Aussi vous décidez de transformer votre application, pour qu'elle se transforme en une espèce de programme attaquant. Au lieu d'envoyer un message, elle va envoyer en parallèle plusieurs séquences de 2000 fois le message de SOS.

15 - Qu'elles modifications proposez vous dans le code précédent ?

Le dénouement ...

Ca à marché, le pare feu a signalé le comportement anormal de votre application. Le message d'alerte à été vu par les techniciens sur terre et ces derniers vous envoient les séquences de messages ci dessous :

UDP	2.1.1.1: 1111	2.1.1.254 : 2222	Code activation : #Activ-capsule-2018#
UDP	2.1.1.1: 1111	2.1.1.254 : 2222	Code activation : #Activ-capsule-2018#
UDP	2.1.1.1: 1111	2.1.1.254 : 2222	Code activation : #Activ-capsule-2018#
UDP	2.1.1.1: 1111	2.1.1.254 : 2222	Code activation : #Activ-capsule-2018#

...

Vous êtes sauvés !!!... Bon voyage de retour et bonnes fêtes de fin d'année

ANNEXE 1 - ANALYSE DE TRAMES

...

1.	TCP	192.168.1.1 : 1234	192.168.1.254: 8080	Flag=syn
2.	TCP	192.168.1.254: 8080	192.168.1.1: 1234	Flag=ack, syn
3.	TCP	192.168.1.1: 1234	192.168.1.254: 8080	Flag=ack
4.	TCP	192.168.1.1: 1234	192.168.1.254: 8080	Données de la station météo ....
5.	TCP	192.168.1.254: 8080	192.168.1.1: 1234	Flag=ack
6.	TCP	192.168.1.1: 1234	192.168.1.254: 8080	Flag=fin
7.	TCP	192.168.1.254: 8080	192.168.1.1: 1234	Flag=fin,ack

....

8.	TCP	2.1.1.254 : 2222	2.1.1.1: 1111	Flag=syn
9.	TCP	2.1.1.1: 1111	2.1.1.254 : 2222	Flag=ack, syn
10.	TCP	2.1.1.254 : 2222	2.1.1.1: 1111	Flag=ack
11.	TCP	2.1.1.254 : 2222	2.1.1.1: 1111	Transfert des données
12.	TCP	2.1.1.1: 1111	2.1.1.254 : 2222	Flag=ack
13.	TCP	2.1.1.254 : 2222	2.1.1.1: 1111	Flag=fin
14.	TCP	2.1.1.1: 1111	2.1.1.254 : 2222	Flag=fin,ack

...

ANNEXE 2 - Fonctions socket

```
int sock = socket (af, type, protocole)
int bind ( sock, p_struct_adress, long_struct_adress )
int listen (sock, nb)
int accept (sock, p_struct_adress, socklen_t )
int connect (sock, struct_adr, lgadr)
int send (sock, msg, lg,0)
int recv (sock, msg, lg,0)
int close (sock )
```