SOMMAIRE

I) LE MODELE OSI

Définition

Le modéle OSI est composé de 7 couches qui permettent de modéliser le fonctionnement d'un réseau

La couche 1 :

est la **couche physique** qui est associé à tout les éléments matériels et physiques permettant au réseau de fonctionner c'est à dire:

Les câbles (**paire torsadée, paire torsadé blindé, connecteur RJ45, fibre optique, sans fil, le hub**)

La couche 2:

Est la **couche liaison de donnée** qui permet de faire la liaison entre la couche physique et la couche réseau. sur le plan matériel la carte réseau est situé à ce niveau et elle permet de faire la liaison entre **l'adresse IP** et l'adresse physique (adresse **mac**). Le protocole **ARP** se trouve à ce niveau. Les switchs conservent des tables dans leur mémoire permettent de faire la correspondance entre les **adresses mac** et les **ports matériel** sur lesquels sont connectés les ordinateurs .

Travail pratique: essayez la commande **arp -a** vous constatez qu'elle permet d'obtenir une table de correspondance adresse IP adresse MAC. Essayer la commande **arp -d** elle va effacer le cache arp,

La couche 3:

C'est la **couche réseau** qui est responsable de l'acheminement de paquets de donnée de bout en bout. Les paquets ip traverse des routeurs. C'est à ce niveau que l'on trouvent les **routeurs** qui permettent d'envoyer les **paquets de données** sur un interface donnée en fonction de table de routage.

Travail pratique: Essayer les commandes suivantes:

ping (adresse ip): Qui permet de s'assurer qu'un ordinateur est bien connecté au réseau

ipconfig/ all :qui permet d'avoir la configuration reseau d'un ordinateur c'est à dire que l'on obtient (l'adresse ip, le masque de reseau, la passerelle, le dns, l'adresse mac)

ipconfig/renew: Pour libérer une adresse ip

ipconfig/release: pour obtenir une adresse IP

tracert (adresse ip): pour savoir quelles sont tous les routeurs qui sont traversé par un paquet IP afin d'atteindre sa destination

ipconfig/registerdns: Pour forcer l'enregistrement d'une machine dans un serveur dns

nslookup (nom de domaine): Permet de tester le fonctionnement d'un serveur DNS

La couche 4:

c'est la **couche transport** qui est responsable de s'assurer du fait que les paquets d'information sont arrivés à destination. Il y a deux protocoles de transport le protocole **UDP** et le protocole **TCP** . Le protocole TCP est un protocole qui s'assure que le paquet est arrivé à destination en faisant en sorte que la machine de destination envoie un message d'aquitement à la machine source. Le protocole UDP ne permet pas l'envoi d'un message d'acquitement.

Exemple: Le protocole **HTTP** se base sur le protocole de transport **TCP**

Le protocole **FTP** se base sur le protocole **UDP**

La couche 5:

C'est la **couche session** qui se charge de gérer la session de communication

La couche 6:

c'est la **couche présentation** qui se charge de mettre en forme les données pour qu'elles soient lisibles par toutes les machines et tous les systémes d'exploitation.

La couche 7:

C'est la couche application qui met à disposition des applications voulant communiquer sur le réseau des outils réseau comme:

HTTP: qui permet la communication entre un serveur web (**Apache, IIS**) et un client de navigation (**mozilla, internet explorer, chrome**)

FTP: qui permet la communication entre un serveur **FTP** (**Fizilla serveur, IIS**) et un client **FTP fizilla client**

SMTP : qui permet l'envoi de message entre un serveur de messagerie (exchange) et un client de messagerie (outlook, thunderbird)

POP: Qui permet la reception de message entre un serveur de messagerie (exchange) et un client de messagerie (outlook, thunderbird)

SIP: qui permet la VOIP entre un serveur de téléphonie SIP (tribox) et un client de Voip

I.1) LE FONCTIONNEMENT D'UN RESEAU PAR RAPPORT AU MODELE OSI ?

Lorsqu'un ordinateur A envoie un paquet d'information sur le réseau a destination d'un autre ordinateur B le paquet d'information va traverser toutes les couches du modéle OSI sur l'ordinateur A de la couche 7 jusqu'a la couche 1 . A chaque couche il y a des informations qui s'ajoutent c'est ce que l'on appelle **l'encapsulation**. Puis lorsque la trame d'information arriv chez l'ordinateur B c'est l'inverse qui se produit le paquet monte de la couche 1 à la couche 7 c'est la **desencapsulation**.

II) DESCRIPTION DES MATERIELS D'INTERCONNEXION

II.1) Le HUB:

Permet de brancher plusieurs ordinateurs avec une topologie physique en etoile , lorsqu'un ordinateur envoie une trame de donnée vers un autre le signal est regénéré sur tous les ports , seul l'ordinateur concerné conserve le paquet d'information.

II.2) LE SWITCH

Permet de brancher plusieurs ordinateurs avec une topologie physique en etoile , lorsqu'un ordinateur envoie un paquet de donnée vers un autre , le switch grace à une table en mémoire qui permet d'etablir la correspondance entre chacun de ses ports matériel et les adresses mac branchés sur chacun de se

ports matériels va pouvoir envoyer le paquet vers le bon ordinateur.

II.3) LE ROUTEUR

Le routeur est un méteriel qui permet de relier plusieurs reseaux différents entre eux (un reseau local avec internet , plusieurs segments de reseau locaux entre eux). Un routeur posséde plusieurs interfaces c'est à dire plusieurs carte réseau. Lorsqu'un paquet d'information parvient au routeur , le routeur va analyser vers quel reseau doit être envoyé le paquet et grace à une table de routage qui permet d'etablir la correspondance entre le reseau de destination et les interfaces le routeur sait vers quelles carte reseau il envoie le paquet de données. Deux protocoles sont utilisés par les routeurs le protocole RIP et le proctocole OSPF.

II.4) Les VLAN

Les VLAN sont des réseaux locaux virtuels , on utilise un switch paramétrable pour les créer Par exemple sur les switch de niveau 3 on peut paramétrer les ports du swicth pour qu'ils soient associés à un réseau bien determiné.

II.5) Le répéteur

Le répeteur est un dispositif qui permet de regenerer le signal . Les cables ethernet ne permettent pas de créer des cables de plus de 100 metres , donc chaque 100 metres il faut les brancher à un répéteur qui va regenerer le signal..

III) LES TYPES DE RESEAU

III.1) Les réseaux ETHERNET

Les réseaux ethernet sont des réseaux qui utilise la méthodes de communication **CSMA/CD** (acces multiple avec ecoute de porteuse et detection de collision). Sur les reseaux ethernet les ordinateurs communiquent tous en même temps ce qui entrâinent qu'il peut y avoir des coliisions sur un reseau ethernet et donc les ordinateurs sont appelés à renvoyer le paquet d'information. Pour cela les cartes reseaux ecoutent le reseau si ils constatent qu'un signal anormal leur parvient ils renvoit le paquet de données.

III.2) Les réseau novell ?

Les reseaux novel eux sont disciplinées. Une trame d'information circule sans arrêt sur le réseau, dés qu'un ordinateur veut communiquer il s'empare de cette trame que l'on appelle le jeton et il envoie ses paquets d'information sur le

reseau. Quand il a terminé il remet le jeton en ciculation pour qu'un autre ordinateur qui veut communiquer puisse s'emparer du jeton.

IV) Les supports de connexion

IV.1) Les câbles croisés

Si on veut relier deux ordinateurs entre eux on utilise un câble croisés en effet les données sont transmises sur les fils 1 et 2 d'un cable puis receptionné sur les fils 3 et 4,

IV.2) Les câbles droits

Si on veut relier des ordinateurs via un switch ou un hub on utilise un câble droit car le hub ou le switch utilisent les fils 1 et 2 pour la reception

IV.3) Les types de câbles ethernet

Protocole Ethernet standardisé par la norme IEEE 802.3
802.3 utilise les services de la couche **LLC** , la méthode d'accès au support est par contention csma/cd
Plusieurs options en fonction du débits (**mbits/s**, bande de base (large bande), longueur maximum d'un segment (100 mètres))
Codage : manchester, carte réseau 20 Mhz, longueur minimale trame 64 octets , maximum 1518 octets
Ethernet : regle des 5-4-3 Maximum 5 segments avec 4 répéteurs , seuls 3 segments comporte des stations.

Denomination	Caracteristiques
10 Base 2	• Câble coaxial fin (RG58), connecteur BNC • Distance minimale entre 2 connecteurs 0.5m • Etendue du réseau 925 mètres (5 segments maximum avec répéteur) • 30 stations maximum par segment • 10 mbps, signaux numériques, 185 mètres pour un segment
10 Base 5	• Câble coaxial épais (RG11) • Environnement avec perturbations électromagnétiques • 500 mètres par segment • 2500 mètres maximum • Emetteur-récepteur (transceiver) • Cordon reliant le connecteur Access Unit Interface (AUI) de la

	carte au receveur est le câble émetteur - récepteur
10 Base T	Ethernet en paire torsadée (T twisted pair), 10 Mbps
100 Base T	100 mbps (catégorie 5)
1000 Base T (IEEE 802.3ab)	Paire torsadée UTP (catégorie 5e) 100 mètres, 1000 Mbps
10 G base T (IEEE 802.3an)	10 Gbp/s paire torsadée 100 mètres
10 Base FL	Fibre optique 2 km 10 mbps
100 Base T4	4 paires torsadée UTP au moins de catégorie 3 Codage 8B/6T 3 paire pour la transmission , 1 détection de collision
100 Base TX	Paires torsadée blindée ou pas Cat 5
100 Base FX	Fibres optiques, multimode, 100 Mbps
1000 Base TX	Paires torsadee 5e, 6 1000 MBPS 100 Mètre
1000 Base SX	Fibre optique mutlimode 550 mètres maximum
1000 Base LX	Fibre optique multimode ou monomode sur 2 a 5 km

IV.4) Categorie et type de cable en paire torsadee

Categorie	**Type de cable**	**Caracteristiques**
1		Telephonique
2		UTP 4 paires (4mbps)
3	UTP	UTP 4 paires 3 torsions par pied (33cm). 10 mbps telephonique
4	UTP	UTP 4 paires 16MBPS
5	UTP	UTP,STP,FTP 4 paires100 MBPS
5e	UTP	UTP,STP,FTP 4 paires 1 Gbps
6	UTP	UTP classe E 1 gbps
6a	F/FTP	1 a 10 gbps
7	F/FTP	F/FTP 10 Gpbs
7a	F/FTP	100 gbps
8.1	U/FTP F/UTP	40 gbps (autonegocaition)
8.2	F/FTP S/FTP	40 gbps

V.5) Criteres de choix

Caracteristiques	**Paire torsadee non blindee (UTP)**	**Paire torsadee blindee (FTP)**	**Fibre optique**
Prix	Peu cher	Peu cher >UTP	Plus cher
Longueur d'un segment	100 metres	Un peu plus	2000 m
Debits	100 (cat 5) 1 GBPS (Cat 5e et 6) 10 GBPS (6a et 7)	1000 Mbps (cat 5) 1 Gbps (cat 5e et 6) 10 gbps (6a et 7) Environnements perturbes	100 mbps a 1 gbps
Installation	Simple	Simple	Complexe (rayon de courbure, ne pas obtsruer passage de lumiere)
Attenuation	Elevee	Faible	aucune
Sensibilite aux interferences	Sensible	Peu sensible	aucune
Utilization habituelle	Reseaux de bureau de taille moyenne	Environnements perturbe de grande taille	Necessite de forts debits interconnexion entre repartiteurs ou batiments

VI) Le serveur DNS

LE DNS: LE DNS permet la resolution d'adresse ip en nom d'hôte , Sur un serveur DNS on trouve la zone de recherche directe permettant la correspondance nom d'hôte en adresse IP et la zone de recherche inversé permettant l'inverse,

VI.1) les enregistrements de ressource existant sur un serveur DNS

SOA: Start of authority indique l'adresse du serveur DNS ayant autorité sur la zone c'est à dire celui qui gére la zone pour la correspondance des noms d'hôtes en adresse IP.

NS: Name service , indique l'adresse du serveur DNS

A: Hôte enregistré dans le DNS

AAAA: Hôte pour les adresses IPV6

SRV:Enregistrement representant un service par exemple pour un contrôleur de domaine il y a le service kerberos qui permet l'authentification, Dés qu'un contrôleur de domaine est crée plusieurs enregistrement de service utilisé par le contrôleur de domaine sont crée,

MX: Enregitrement representant un serveur de messagerie

CNAME: Enregistrement representant un alias c'est à dire que l'on peut associer 2 noms à une même adresse IP cela sert dans le cas ou un ordinateur est serveur web on peut lui donner le nom www par exemple pour qu'il soit reconnu en fonction du service qu'il offre.

PTR: Enregistrement de type pointeur existant dans la zone de recherche inversé qui permet de trouver un nom d'hôte en fonction de l'adresse IP

VII) Le serveur DHCP ?

LE DHCP: Le serveur DHCP permet d'attribuer des adresses dynamiquement, Il permet de définir des etendues d'adresses IP, des exclusions , des reservations d'adresses IP, des options d'etendue,

VIII) Les Domaines

LE DOMAINE

Le domaine est une limite de sécurité. Dans un domaine la gestion des ordinateurs est centralisé grâce à un contrôleur de domaine contrairement au workgroup ou l'administration des ordinateurs est decentralisé et se fait sur chaque poste.

IX) les principales menaces pour le poste de travail d'un utilisateur ou le pc d'un particulier ?

Virus, troyens, malware, spams, phishing,...pouvant causer des intrusions , des pertes de données, des vols de données confidentielles, des usurpations d'identité , des utilisation de poste à des fins illicites .

IX) Comment peut on se protéger efficacement de ces menaces ?

On réalise des sauvegardes régulieres, des mises à jour réguliéres, on met des mots de passe complexe, des anti-vrius, des antispam, des antispy, des pare-feu.

X) Communication avec du matériel mobile

Quelles sont les différents moyens possible pour la communication locale entre un PDA ou SMARTPHONE et un PC sont Le bluetooth, l'USB, le WIFI

On peut synchRoniser les données entre un PC et un equipement windows mobile (Pocket PC, Smartphone...) avec le logiciel **microsoft Activesync**

XI) Le devis

Le devis a valeur de contrat une fois signe entre le vendeur et le client, il engage le vendeur et le prestataire il est reconnu par la justice en cas de litige il a une duree de validite limitée dans le temps il est obligatoire pour toute reparation superieure à 150 euros tout depassement doit faire l'objet d'un avenant accepte par le client.

XII) avantage qu'il y a pour un service informatique a assurer le suivi logiciel du parc informatique ?

Inventaire a jour des materiels et des logicielles, historique des mises a jour et des interventions, gestion des licences, gestion financiere, couplage avec le helpdesk .

XIII) quels sont les services fournis par un boitier boitier triple play ?

Internet - téléphonie sur IP-Television
Les connecteurs que l'on trouve le plus couremment sur un boitier triple play Sont l' ADSL sur rj11- telephone sur rj11-ethernet sur rj45-television selon standard-USB

XIV) points forts respectifs de la téléphonie classique et de la voix sur IP

Pour la téléphonie classique on a une qualité constante du son, l'independance vis à vis de l'acces à internet, le téléphone peut -être alimentée directement par la ligne.

Pour la voix sur IP Le cout est trés faible ou gratuit, n'impose pas un terminal dédie on peut utiliser un softphone , et peut être couplé à l'image (visiophonie par webcam)

XVII) PANNE POSSIBLE SUR UN RESEAU ET METHODE DE RESOLUTION

A) Vous constatez que vous n'arrivez pas à communiquer avec un ordinateur ?

1) assurez vous que le cable est bien branché sur la carte réseau et que celle ci clignote, assurez vous egalement que le cable ethernet est bien placé sur le switch ou la prise murale , si la carte réseau ne clignote pas assurez vous de bien enficher le cable des deux côtés sinon changer de cable . Si malgré que la carte réseau clignote cela continue toujours à ne pas communiquer passer à l'étape 2

2) Faites un ping vers l'adresse ip de l'ordinateur de destination a partir de votre machine ?

Si il n'y pas de réponse , faire un **ipconfig /all** sur les deux ordinateurs et assurez vous que les deux ordinateurs sont sur le même réseau ? Si ils ne sont pas sur le même réseau corriger l'adresse IP sur votre machine sinon desactivez entiérement le pare-feu sur les deux ordinateurs si le ping passe , alors remettre le pare-feu et le paramétrer pour laisser passer les ping sur les deux machines et refaire le ping ? Si les deux ordinateurs ne communiquent toujours pas alors configurer le pare-feu de tel maniére à laisser passer le programme que vous souhaiter utiliser (tightvnc, bureau a distance,...). si on ne passe toujours pas , alors passer à l'étape 3.

3) Vider le **cache arp** en effet parfois il y a une mauvaise correspondance entre l'adresse ip d'un poste et son adresse mac du fait que celle ci a changé et le cache n'a pas encore été mis à jour .

Pour vider le cache ARP faites la commande suivante: **arp -d**

Pour afficher le cache ARP faites la commande suivante: **arp -a**

B) Vous constater que vous n'arriver pas à aller sur internet ?

1) Faire un **ipconfig /all** sur la machine et regarder si le DNS est bien celui défini sur le réseau si non alors si l'adressage de la carte réseau s'est fait manuellement attribuer manuellement la bonne adresse DNS sinon, allez vérifier dans le DHCP que les options d'etendu ont été bien configuré. Si aprés cela on ne parvient pas aller sur internet passer à l'étape 3.

2) Vérifier que la connexion au serveur proxy est bien configuré dans les paramétres du navigateur si il y a un proxy.

3) Verifier que l'adresse de la passerelle est la bonne et que vous pinguer bien la passerelle, sinon changez l'adresse de la passerelle et allez vérifier que la passerelle c'est à dire le routeur est bien en marche et qu'un cable relie le routeur au reseau ou se situe votre ordinateur.

4) vérifier que l'URL que vous avez saisi est bien définie

5) si le probléme persiste un virus peut empêcher d'aller sur internet , redemarrer l'ordinateur en mode sans echec avec prise en charge réseau et tenter d'aller sur internet si cela passe alors cela signifie qu'un service est monté en mémoire en mode normal qui peut être un virus il faut alors déviruser l'ordinateur avec un scan au demarrage par exemple avec avast .

XVIII) L'ADRESSAGE IP

a) les classes d'adresse possibles

Classe A: Le premier bit de poids fort est 0 le masque par deaut est 255.0.0.0

Classe B: Les deux premiers bits de poids fort est 10 le masque par defaut est 255.255.0.0

Classe C: Les trois premiers bits de poids fort sont 110 le masque par defaut est 255.255.255.0

Classe D: Les quatres permiers bits de poids fort sont 1110

Classe E: les cinq premiers de poids forts sont 11110

port logicielle: C'est un numéro attribué à un programme

socket: c'est la combinaison adresse IP :port (192.168.1.1:80)

masque de reseau: C'est une information qui combiné avec l'adresse IP permet d'obtenir l'adresse du réseau

adresse unicast: elle ne concerne qu'un ordinateur

adresse de broadcast: concerne toutes les machines du réseau

adresse multicast: elle ne concerne qu'un ensemble de machine

QUESTION - REPONSE

1) **La technique du spoofing IP consiste à:**

Réponse:

Usurper une adresse IP pour faire passer un ordinateur pour un autre

2) **Quel type de journal n'existe pas dans les journaux windows de l'observateur d'événements**

Réponse:

Systéme

3) **A Quoi sert un NAS**

Réponse:

Un NAS network **attached storage** est un serveur de fichier autonome relié à un réseau dont la principale fonction est le stockage de données en un volume centralisé pour des clients réseau fonctionnant sous différents systéme,Un serveur NAS est accessible via une adresse IP en utilisant le protocole **SMB, FTP,NFS**, Il permet de gérer la sauvegarde des données d'un réseau,

4) **Lors d'une sauvegarde incrementielle le bit d'archive est:**

   Réponse:

   Le bit d'archive est modifié (remis à zéro).

5) **Lors d'un sauvegarde différentielle le bit d'archive est:**

   Réponse:

   non modifié

6) **Lors d'un sauvegarde normale le bit d'archive est :**

   Réponse:

   Modifié (remis à 0)

7) **Vous êtes technicien chez un assembleur , Un collegue assemble des machines pour des clients il vous demande quel type de licence il peut installer pour le systéme microsoft, Que lui proposez vous ?**

Réponse:

La licence OEM

8) **<u>Indiquez le masque de sous -reseau de l'adresse IP 192.168.1.1/30 en notation decimale et combient d'adresse d'hôtes peuvent être attribuées dans ce réseau ?</u>**

<u>Rappel concernant le binaire:</u>

Pour convertir un nombre binaire sur 8 bit c'est à dire 1 Octet en decimal vous devez utiliser le tableau suivant:

128	64	32	16	8	4	2	1

Ainsi si vous devez convertir un nombre binaire en decimal vous disposez les chiffres du nombre binaire dans la ligne du dessous, par exemple:

Supposons que l'on doit convertir 11111111 en decimal on va avoir:

128	64	32	16	8	4	2	1
1	1	1	1	1	1	1	1

Puis on additionne toutes les cellules qui sont marqués par un 1 on obtient:7

128+64+32+16+8+4+2+1=255

Ce rappel etant fait revenons à la question on a l'adresse 192,168,1,1/30 et on doit ecrire le masque en notation decimal, Le masque de réseaux s'ecrit:

11111111.11111111.11111111.11111100= 255.255.255.252

Le nombre d'hôte de ce réseau est egale à 2^2-2=4-2=2

On doit enlever l'adresse du réseau et l'adresse de broadcast Donc la réponse est:

Réponse:

Masque en decimal: 255.255.255.252

Nombre d'hôte: 2

9)Vous devez relier deux switches par un cordon ethernet selon le statut des ports à connecter quel type de cordon va t'on pouvoir brancher ?

Explication:

Les câbles ethernet en paire torsadée possédent 8 Fils et un ordinateur emet sur les fils 1 et 2 et receptionnent les données sur les fils 3 et 4 pour la reception. Les ports normaux d'un switch utilisent les fils 1 et 2 pour la reception, Donc d'un port normal vers un port normal on utilise un cable croisé,

Le port uplink croise les fils c'est à dire que les fils utilisé pour la transmission vont pouvoir etre utilisé pour la reception, donc d'un port normal vers uplink on utilise un cable droit, entre deux ports uplink comme il croisent tous les deux donc on utilise un cable croisé,

Le port automdx detecte quel type de périphérique est connecté (normal, uplink, automdx) et donc il croise ou non en fonction , donc on peut utiliser le cable que l'on veut ,

La réponse est:

Switch 1	Switch 2	Type de cordon DROIT, Croisé ou les deux
Normal	Normal	CROISE
Uplink	Normal	DROIT
Uplink	Auto MDX	LES DEUX
Auto MDX	Normal	Les DEUX
Uplink	Uplink	CROISE

Auto mdx	Auto MDX	Les DEUX

10) **Indiquez pour les adresses suivantes: leur classe d'adresse, si elles peuvent être attribués à un hôte si elles sont publiques ou privées**

IP	Valide pour un hôte	Publique ou privée	Classe
165 .10.14.24	Oui	Publique	B
127.144.156.20	Non	aucun	Aucun
10.255.0.0	Non	privee	A
172.30.255.255	Non	privee	B

Rappel:

Les adresses de la classe A: 0.0.0.0 A 126.255.255.255

Les adresses de la classe B:128.0.0.0 A 191.255.255.255

Les adresses de la classe C: 192.0.0.0 A 255.255.255.255

Les adresses de la classe D: 224.0.0.0 A 239.255.255.255

Les adresses de la classe E: 240.0.0.0 A 255.255.255.255

Les adresses privees de la classe A : 10.0.0.0 A 10.255.255.255

Les adresses privees de la classe B: 172.16.0.0 A 172.31.255.255

Les adresses privées de la classe C : 192.168.1.0 A 192.168.255.255

QUESTION

Question 1 :
Dans un environnement réseau il y a des perturbations électromagnétiques et on souhaite un débit à 100 mbit/s , proposer un type de câblage ?

Réponse :
perturbations électriques faibles : un câble paire torsadée catégorie 5 blindé
fibre optique débit immunité aux interférences.

Question 2 :
comment fonctionne un pont filtrant

Réponse
Le pont est un élément d'interconnexion de réseaux locaux. Se situant au niveau 2 du modèle OSI, il a la capacité d'étudier l'adresse des trames qu'il reçoit et d'y appliquer un filtrage. Pour cela, le pont construit une table associant à l'adresse de chaque équipement du réseau le numéro de port correspondant.
Dès qu'un poste de travail se connecte sur le réseau, le pont stocke son adresse dans la table avec le numéro du port correspondant.
Chaque nouveau message est étudié :

- Si l'adresse du destinataire est connue et est du même côté du pont, le message est filtré.
- Si l'adresse du destinataire est connue et est de l'autre côté du pont, le message est passé.
- Si l'adresse du destinataire est inconnue, le message est passé.
- Par ailleurs, si l'adresse de l'expéditeur n'est pas connue dans la table, le pont ajoute une nouvelle entrée avec l'adresse de l'expéditeur et le numéro du port d'où le message arrive.

Question 3 :
on veut faire communiquer ensemble des reseaux locaux de topologie et de protocole différents quel matériel doit on utiliser ?

Réponse
Il s'agit ici d'interconnecter des réseaux locaux de topologie et de protocole différents. Une passerelle est donc le dispositif indispensable. Elle travaille jusqu'au niveau 7 du modèle OSI et permet d'assurer les conversions des protocoles de réseaux locaux avec des protocoles propriétaires.

Question 4 :
Comment peut on faire un partage d'imprimante

Réponse
On attache l'imprimante au serveur.
• L'imprimante est directement connectée au réseau.
• L'imprimante est connectée à un poste de travail qui sert de serveur d'impression.

Question5 :
Expliquer la méthode d'accés au média utilisé sur un réseau ethernet

Reponse
La méthode d'accès utilisée sur réseau Ethernet est CSMA/CD : détection des collisions par écoute du canal de transmission. Il s'agit d'une méthode probabiliste.

Question 6 : Décrire les normes de câblage qui autorisent un débit de 100 Mbit/s sur les réseaux Ethernet. Donner leur nom et leurs principales caractéristiques techniques

Réponse :
- **Fast Ethernet 100 Base TX** : câble UTP catégorie 5 sur 2 paires.
- **Fast Ethernet 100 Base T4** : câble UTP catégorie 3, 4 ou 5 sur 4 paires.
- **100 Base FX** : fibre optique à une paire.

Question7 :
Expliquer ce qu'est un intranet.

Reponse
Intranet : utilisation des standards de l'internet (HTML, HTTP, CGI, SMTP, NNTP) pour développer des applications internes à l'entreprise, que le réseau soit local ou étendu.

Question12 :
Citer les spécificités du développement d'un intranet par rapport à d'autres types d'architectures client-serveur.

Reponse :
Les spécificités du développement d'un intranet sont :
- Davantage de *middleware* standard, accès universel, pas de déploiement spécifique sur chaque type de plate-forme.
- L'application est développée sur le serveur, une mise à jour de l'application est immédiate
pour tous les clients quelle que soit leur plate-forme.

Question 13 :

préciser à quels niveaux du modèle OSI interviennent les éléments d'interconnexion suivants :

Hub, Routeur, Switch, Passerelle

Réponse

Hub	couche 1 – physique
Routeur 4	couche 3 – réseau
Switch 4	couche 2 - liaison
Passerelle	couche 7 – transport, session, présentation, application (on accepte les solutions de 4 à 7)

Question 14 :

Expliquer en quelques lignes le principe de la création de sous-réseaux dans un réseau TCP/IP. *Vous illustrerez votre propos par un exemple utilisant une adresse de classe C.*

Réponse :
Le principe des sous-réseaux repose sur la définition d'un masque de sous-réseau indiquant un découpage de l'adresse IP en réseau/machine plus long pour la partie réseau que ne l'exige la classe d'adresse retenue. En pratique, on prélève un certain nombre de bits sur la partie machine, ces bits contiendront le numéro identifiant un sous-réseau particulier.

Question 15 :
Lister au moins deux avantages liés à l'utilisation de sous-réseaux

Réponse
création de domaines de collision indépendants (segmentation) ;
• diffusions limitées au sous-réseau (les trames de diffusions ne sont pas routées) ;
• un seul identificateur de réseau vu du monde extérieur ;
• une sécurité accrue entre les sous-réseaux.

Question 16 :
Sur le réseau on a le message suivant :
« Le système a détecté un conflit entre l'adresse IP 195.10.228.116 et l'adresse matérielle 00 :13 :B8 :3C :F7 :B2 »
« Le système a détecté un conflit entre l'adresse IP 195.10.228.116 et l'adresse matérielle 00 :13 :B8 :3C :F4 :D5 7
Comment regler le probléme ?

Réponse :
On est dans la situation où 2 machines utilisent la même adresse IP dans le même sous-réseau.
Il faut donc changer l'adresse du poste pour qu'elle sorte de cette plage, sous réserve d'adresses disponibles (par exemple 195.10.228.126).

Question 17 :
Expliquer quel est l'intérêt d'empiler des commutateurs plutôt que de les « cascader ».

Réponse
Cascader baisse le coût de l'équipement mais chaque équipement est autonome. La cascade augmente le temps de transmission entre les différents composants en générant un goulot d'étranglement.
Empiler permet de faire une seule entité des différents composants partageant ainsi les différents services tel que SNMP.

Question 18 :
Préciser les commandes à utiliser pour vérifier que les postes peuvent effectivement communiquer entre eux et pour connaître la route empruntée lors d'un échange.

Réponse
Pour vérifier la communication : commande *Ping* sur l'un des postes, avec l'adresse IP du poste à atteindre. Pour chercher la route : commande *Tracert* (sous DOS/Windows) ou *traceroute* (sous UNIX) sur l'un des postes, avec l'adresse IP du poste à atteindre. Éléments

Question 20 :

Un utilisateur semble rencontrer quelques dysfonctionnements à partir de la machine 192.168.62.11 alors que **tout fonctionne normalement sur les autres machines**. Il peut accéder à tous les services Internet, mais n'arrive pas à accéder aux applications situées sur la machine 172.16.0.10 de nom *medianet.serveur.fr*.
Afin de déterminer la cause du dysfonctionnement entre ces deux nœuds, vous souhaitez,

à partir du poste 192.168.62.11, utiliser la commande « ping » pour vérifier le

fonctionnement des éléments suivants :

8) pile de protocoles TCP/IP sur lui-même,
9) couche Physique et Liaison de données sur le réseau de la société
10) couche Réseau entre le réseau de la société entre les deux reseaux
11) résolution de nom en utilisant le protocole DNS.

Pour chacune des vérifications souhaitées, indiquer la commande « ping » à exécuter.

Réponse :

ping 172.16.0.10 » sur la machine qui ne fonctionne pas. La consultation du cache **arp** de cette machine donne le résultat suivant :

Adresse internet	***Adresse physique***	***Type***
192.168.62.253	00:D0:59:86:3B:68	dynamique

commande « **ping 172.16.0.10** », depuis une autre machine d'adresse **192.168.62.12**. Après quoi, la consultation du cache **arp** de cette autre machine donne le résultat suivant :

Adresse internet	***Adresse physique***	***Type***
192.168.62.254	00:D0:59:82:2B:86	dynamique

Vérification 1 : « *Pile de protocoles TCP/IP sur lui-même* »

La commande **ping 127.0.0.1** permet de tester la pile TCP/IP de la machine, sans «

Vérification 2 : « *Couche Physique et Liaison de données sur le réseau de la société*

La commande **ping 192.168.62.254** permet de déterminer que la liaison fonctionne sur 2 noeuds adjacents. *Cette commande permet de tester la carte réseau, le concentrateur et le câble de liaison.*.

Vérification 3 : « *Couche Réseau entre les deux reseaux*

Il s'agit de vérifier ici si le « routage » « *…couche réseau…* » se fait bien. Il faut donc un ping qui « concerne » les routeurs intermédiaires aux deux réseaux intéressés. Les commandes **ping 172.16.1.254** ou **ping 172.16.0.10**

Vérification 4 : « *Résolution de nom en utilisant le protocole DNS* »

Pour provoquer la résolution de nom en son adresse IP, il faut faire un ping qui utilise le nom d'hôte du poste. Ce nom est précisé dans le texte du sujet *« …la machine 172.16.0.10 de nom medianet.serveur.fr…* ». On fera donc un **ping *medianet.serveur.fr***.

Question 21 :
Expliquer le rôle du protocole **arp ?**

Réponse :

Le protocole **arp** permet la résolution (traduction, translation, mappage…) d'adresse IP en adresse MAC (*Media Access Control*), adresse physique ou adresse Ethernet.

Question 22 :
Indiquer comment procéder pour que le serveur d'impression obtienne toujours la même adresse IP de la part du serveur DHCP ?

Réponse :
Au niveau du serveur DHCP, il faut procéder à une **réservation**, c'est à dire associer l'adresse MAC de la carte réseau du serveur d'impression à l'adresse IP souhaitée.
On autorisera un bail illimité

Question 24
Expliquer le principe et l'intérêt de la délégation de zone dans le système de résolution de nom DNS.

Réponse :
Permet de diviser l'espace de noms et de déléguer la gestion d'une partie de l'espace de nom DNS à chaque Division. L'extension de l'espace de noms sera ainsi simplifiée et sous la responsabilité de chaque Division. La modification d'un nom d'hôte sera réalisée par la division qui gère la zone concernée.

Question 22
Donner le nombre de domaines de collision et le nombre de domaines de diffusion d'un hub a 8 ports et d'un switch a 8 ports

Réponse :
Un domaine de diffusion (*broadcast domain*) est une aire logique d'un réseau informatique où n'importe quel ordinateur connecté au réseau peut directement transmettre à tous les autres.
Un domaine de collision est une zone logique d'un réseau informatique où les trames de données peuvent entrer en collision entre elles. Dans le cas du réseau Ethernet, le domaine de collision comprend l'ensemble des segments connectés par des concentrateurs ou répéteurs.

Question 23 :
Indiquer précisément le protocole de la famille TCP/IP exploité par la commande *ping*.

Réponse
Le *ping* appartient à la couche protocolaire IP et le protocole précisément mis en oeuvre est **ICMP**. Le *ping* repose en fait sur deux commandes *« Echo Request »* et *« Echo Reply »*.

Question 24 :

Expliquer ce qu'est une « tempête de diffusion » et sa cause. quel protocole (ou algorithme) l'administrateur doit activer sur les commutateurs pour résoudre ce problème

probléme :

Le commutateur segmente le domaine de collision, il laisse cependant passer les diffusions de trames Ethernet (MAC FF-FF-FF-FF-FF-FF).
Conséquences :
Les commutateurs mettent à jour leur table de correspondance port source = @mac à partir de la trame qui arrive. Les trames de diffusion et de multidiffusion sont acheminées par inondation vers tous les autres ports du commutateur et donc vers tous les commutateurs interconnectés. La trame boucle indéfiniment (pas de TTL), il y a inondation de la bande passante et surcharge de tous les noeuds connectés sur tous les ports.

La solution :

Les liaisons redondantes doivent être invalidées (suite à la formation de liaison inter-commutateur) sous peine de diffuser en plusieurs exemplaires des trames de broadcast et d'autres trames.
Pour y remédier il faut s'assurer que les commutateurs gèrent un algorithme de gestion des redondances comme **STP** (*Spanning Tree Protocol*) ou protocole **802.1d** et l'activer sur tous les commutateurs.
Gestion des redondances*, Spanning Tree* ou protocole 802.1d, *une seule de ces trois réponses est suffisante.*

Question 25 :

Expliquer pourquoi les ports d'interconnexion entre commutateurs doivent être étiquetés (*taggés*).

Réponse :

Les ports d'interconnexion appartiennent à plusieurs VLAN. Pour pouvoir associer une trame à un VLAN il faut donc rajouter l'étiquette 802.1q dans la trame.

Question 26 :

Présenter les critères qui plaident en faveur de l'utilisation de réseaux locaux virtuels.

Réponse :

isoler les flux entre les différents services
améliorer ainsi la sécurité des échanges
optimiser l'utilisation de la bande passante (*broadcast*).

Question 27 :
Expliquer les principales différences techniques qui existent entre l'ADSL et le SDSL

Réponse :

ADSL
allant de l'abonné vers le réseau et la voie montante allant du réseau vers l'abonné) sont asymétriques c'est-à-dire que leur débit est différent.

SDSL (*Symetric* DSL ou *Single line* DSL) est une version monoligne de HDSL. Les canaux (la voie descendante allant de l'abonné vers le réseau et la voie montante allant du réseau vers l'abonné) sont symétriques c'est-à-dire que leur débit est identique

Question 28 : Expliquer la démarche que doit suivre l'administrateur du réseau pour obtenir une adresse IP publique fixe.

Réponse :
Faire une demande d'adresse IP Publique fixe auprès du fournisseur d'accès Internet.

Question 29 : Quelle est la configuration matérielle et les protocoles que devra supporter un commutateur dont les fonctionnalités devront être les suivantes :
Gérer les VLAN et la priorité des flux ;
Éviter les tempêtes de diffusion ;
Supporter la redondance de liens avec un autre commutateur de même type ;
Administrer à distance le commutateur en mode console ainsi qu'à l'aide d'outils de supervision de réseau

Réponse :
Fonctions/protocoles Rôle, explication
Éviter les tempêtes de diffusion ;
Supporter la redondance de lien en évitant les tempêtes de diffusion
Protocole 802.1D, STP Arbre de recouvrement (Spanning tree)
Supporter la redondance de liens avec un autre commutateur de même type ;
Tolérance de panne par agrégation de liens
Gérer les VLAN
Protocole 802.1q Marquage de trames pour identifier les VLAN
Gérer la priorité de flux
Protocole 802.1p
Administrer à distance le commutateur en mode console ainsi qu'à l'aide d'outils de supervision de réseau
Protocoles SNMP, Telnet, HTTP Accès en mode administrateur

Question 30 *:*
Expliquer le rôle d'un agent relais DHCP

Réponse :
L'échange entre un client et un serveur DHCP utilise des trames de diffusion (broadcast) et des paquets IP de diffusion. Ces paquets ne passent pas les routeurs. Un agent relais DHCP récupère l'échange DHCP et l'encapsule dans un paquet UNICAST qui pourra être routé, destiné au serveur DHCP.

Question 31 :
Expliquer le rôle d'un fichier de zone DNS et préciser quel est le type des serveurs DNS qui ont autorité sur ces fichiers.

Reponse : Un fichier de zone DNS associe les noms d'hôtes à leur(s) adresse(s) IP. Les fichiers de zones sont gérés par les serveurs primaires (ou maîtres) qui ont autorité sur la zone

Question 32 :

Justifier le choix du cryptage WPA par rapport au cryptage WEP.

Réponse

Il s'agit de deux techniques de chiffrement des trames. WPA est plus performant que WEP, considéré aujourd'hui comme insuffisant en terme de sécurité (trop facile à « craquer »). WEP s'appuie sur des clés relativement courtes (de 64, 128 ou 256 bits) mais surtout sur un cryptage de flux par un vecteur d'initialisation de 24 bits, ce qui permet de découvrir la clé après une écoute passive de quelques heures seulement. WPA peut utiliser le protocole TKIP (Temporal Key Integrity Protocol) qui échange les clés dynamiquement au cours de l'utilisation du réseau et peut utiliser soit le mode PSK (PreShared Key) qui consiste en la saisie par l'utilisateur d'une phrase de passe (plus longue et donc plus difficile à retrouver qu'un mot de passe), soit un serveur d'identification 802.1X (à base de serveur RADIUS, par exemple) qui distribue les clés à chaque utilisateur selon ses