Préparation EFM Architecture et fonctionnement d’un réseau informatique

Conseil : Résumez les définitions apprenez les abréviations et comprenez les concepts propres à chaque couche fonctionnelle OSI ou TCP/ IP.

Généralités : LAN MAN WAN Intranet Extranet Réseau égal à égal Réseau client-serveur Internet

Commandes réseaux :

ping : test ICMP de connectivité ip de bout en bout.

tracert : Traçage ICMP des sauts d’une route entre une source et une destination

Netstat –R : Affichage de la table de routage sur un hôte

Route print :Idem

Netstat –n :Affichage des conversations TCP et UDP en cours (sources et destinations en chiffre @ip et num de port)

Netsat –a : Affichage des conversations TCP et UDP en cours (sources et destinations en nom de domaine et abréviation des protocole)

nslookup : Résolveur DNS test du serveur DNS et de la résolution des addresses

ipconfig /all : affichage exhaustif des configuration TCP/IP de toutes les cartes réseaux du système (@IP, MSR, PPD, statique ou DHCP, @MAC pour carte ethernet…)

/renew : renouvelement de l’addresse IP auprès d un serveur DHCP

/release : liberer une addresse IP pour un serveur DHCP

 /displaydns : Afficher le cache DNS (résolution @IP------nom de domaine)

 /flushdns : Vider le cache DNS

Arp –a : Afficher le cache ARP

Arp –d :Vider le cache ARP

Couche 7 : couche exécutant les services et interface avec les utilisateurs du réseau

Définition et fonctionnement des protocoles :

http FTP Telnet DNS DHCP SMTP/POP

Couche 6 : Présentation et préparation des données (codage cryptage compression, ASCII codecs…)

Couche 5 : Gestion des sessions de bout en bout (SSL , SSH…)

Couche 4 : Gestion et suivi du transport des données de bout en bout , la connexion des différents services et application grâce aux numéros de port(segmentation étiquetage réassemblage)

Port d’écoute : emplacement RAM 16bits réservé par l’application (serveur ou client) pour identifier les conversations réseaux en cours. (ports réservés 0 à 1023 fixes et connus ; inscrits 1024 à 49151 aléatoires ; dynamiques 49152 à 65535) http 80 FTP 20 et 21 DNS 53 HTTPS 443 TELNET 23 SMTP 25 POP 110…..

TCP : Protocol de control de transmission par les mécanismes : établissement de session (mode connecté ou orienté connexion) ; Fiabilité (accusé de réception et retransmission TCP le cas échéant ACK=SEQ+1) ; Control de flux ou gestion des encombrements (équilibrage de charge entre l’émetteur et le récepteur grâce au fenêtrage TCP ) ; Livraison dans l’ordre (les segments sont mis dans des paquets ip couche 3 et subiront le routage et les conditions d’acheminement et arriverons a fortiori ds un ordre différent , grâce au num d’ordre SEQ les segments sont remis et livrés dans l’ordre)

Segment TCP : donnée de la couche application (après segmentation) et entête de 20 octets (port src, port dst, long, somme de control , SEQ, ACK, fenêtre, Indicateur SYN ACK URG FIN RST PSH)

Protocol utilisant TCP : http smtp pop telnet ftp dns

UDP : User Datagramme protocol ; protocol de transport orienté non connexion , non fiable sans control de flux ; mais donc très rapide entête simple de 8 octets (faible surcharge : PS,PD,SC,LONG)

Protocol utilisant UDP : dhcp tftp dns snmp

Couche 3 ; couche réseau responsable de l’acheminement des paquets entre les réseaux grâce a un protocole routé (IP IPX ou AppleTalk) en utilisant des services de routage et d’adressage propre au protocole.

IP : Internet Protocol Protocole routé de couche 3 pour la communication inter réseaux (adressage acheminement routage) : protocole non fiable , fait son travail « au mieux » et indépendant des médias (le paquet est l’élément de voyage entre les réseaux il ne change pas qlq soit le média cuivre fibre wifi adsl sat 3G …

Adressage IP : espace de 32 bits utilisé pour exprimer une adresse internet (inter réseaux) et composée d’une partie réseau (gauche) et une partie hôte (droite) ; ces parties sont identifiées grâce a un chiffre binaire de 32 bits composé d’une suite de UN (partie réseau) et d’une suite de ZERO (partie hôte) c’est le MASQUE de SOUS RESEAU .Cet adressage comme toute numérotaion réseau (num de port adressage MAC adresses multicast ..)est geré par un organisme international dit IANA(iana.net ou iana.org). Il est passé par plusieurs stations et améliorations forcée par la pénurie et la crise d’adressage (découpage de sous réseau CIDR VLSM DHCP adressage privé public et services NAT et PAT) dont les principales sont :

**\*Adressage CLASSFULL (A/8 , B/16 et C/24) : Adressage avec respect de la classe (masque par défaut) et du masque fixe en cas de découpage de sous réseaux (les sous réseaux issus d’un découpage ont tjrs le même masque)**

**\*Adressage Classless (sans respects du masque de la classe) CIDR et VLSM ds les années 90**

CIDR : Classless Inter Domain Routing (notation / au lieu du masque 255.255. ;;;;)

VLSM : Variable Lenght Subnet Mask (Découpage avec possibilité de sous réseaux avec des masques différents)

**\*Adressage IPv6 (en cours de déploiement solution finale pour la crise on passe de 32 bits à 128 bits) en 1997**

Les protocoles et services

DHCP : Dynamic Host Configuration Protocol :protocol d’attribution automatique d’adresses IP on parle d’adressage automatique utilisé par les stations utlisateur(PC mobile labtop …) l’adressage statique ou fixe ou manuel étant utlisé pour les Serveurs, les routeurs(passerelles) switchs (adresse du VLAN de gestion) ou imprimantes réseaux .

Adressage privé et publique : Des adresses privées non routables qui ne sont pas visible sur le réseau publique ont été réservées pour l’utilisation privée interne et gratuite (une adresse publique étant payante) des réseaux d’entreprise . (Classe A : 10.0.0.0/8 ; Classe B : 172.16.0.0/12 ; Classe C : 192.168..0.0/16)

NAT : Network Address Translation ; service de traduction d’adresses IP privé en adresse publique (connexion sortante) et publique en privée (connexion sortante). Une table de NATAGE de traduction est utilisé par le routeur pour remplacer les adresses ip sources privées (ex : 192.168.1.3) en adresse sources publique fournie par l’opérateur Telecom (ex :180.134.3.2) .on parle de NAT statique ou la correspondance entre l @ privée et publique est statique et ne change pas . On parle de NAT dynamique lorsque la correspondance entre l’@ privée et publique est dynamique et se fait a partir de pool (intervalles) d’adresses privées et publiques.

PAT : ou NAT en surcharge ;Port Adress Translation est le cas de figure le plus utilise dans le NAT et ou on utlise les numéro de ports pour distinguer les différentes conversation du reseau local (ex 192.168.1 .1 ; .2 ; .3 .4 .5 ……) avec une seule adresse publique internet.

Les classes

A 1 a 126 .0.0.0/8 (0.0.0.0 est la route par défaut . 127.0.0.0 est l @ de bouclage interne : on utlise le ping 127.0.0.1 pour tester la pile TCP/IP du système protocole du système d’exploitation et pilote de la carte réseau.

B 128 à 191. 0.0.0 /16 (169.254.0.0 est le réseaux local liens utilisée automatiquement par toute les machine n’ayant pas d’@ statiques (manuelles) et n’ayant pas résussi a voir d’@ IP automatique par DHCP. Ce sont des adresse locales non routables.

C 192 à 223 .0.0.0 /24

D 224 à 239.0.0.0 pas de notion de masque car pas de notion de réseaux, les adresse sont déjà la pour désigner un groupe de machine (abonnés) on parle d’@ multicast

E 240 à 255 (classe expérimentale) 255.255.255.255 est l@ de broadcast limité ou diffusion limitée (DHCP ARP ) qui est effectivement limitée ou bloquée inévitablement par le Routeur (Segmentation des domaine de diffusion)

Types de communications :

\*Monodiffusion , unicast vers une seule machine

\*Multidiffusion , Multicast vers un groupe de machine (un groupe d’abonnés ayant déjà installé un client ou service ou application préconfigurés pour s’ajouter ou s’abonner au groupe et traiter les paquets a destination de ce dernier ex : Multidiffusin tv en ligne les jeux en lignes , protocoles de routage….)

\*Braodcast ou diffusion ; soit dirigée (192.168.1.255) ou limitée (255.255.255.255) correspond à la communication avec toute les machines du réseau (domaine de diffusion) en général pour un mappage d’adresses locale (ARP) ou de recherche de serveur (DHCP) ou de configuration automatique (protocoles de routage)

Le routage : acheminement des paquet et recherche de la meilleur route pour atteindre la destination. Mécanisme de routage se base sur la recherche du réseau (@ réseau) dans la table de routage correspondant à l’@ réseau de destination du paquet IP et ce en utilisant le ET logique (AND) entre l@ ip de destination et MASQUE de sous réseau du réseau de destination si la correspondance réussie le paquet est routé et envoyé au prochain saut.

Routage sur un équipement final :ex : PC : L’équipement final a une table de routage en général très simple comportant la route vers le réseau local du pc lui-même et en cas de présence de passerelle par défaut configurée on trouvera la route correspondante et qui est la route par défaut et donc deux cas de figurent se présentent :

 \*L’@ de destination correspond (avec ET logique) au réseau local donc ARP va aller rechercher l’@ MAC de la destination (sur le même réseau)

 \*L’@ de destination ne correspond pas au réseau local et donc correspondra forcément a la route par défaut (puisque ET logique avec 0.0.0.0 donne tjrs 0.0.0.0) , la destination appartient alors à un autre réseau autre que celui local, ARP ira rechercher l’@ MAC de la passerelle par défaut (routeur : prochain saut pour atteindre un autre réseau).

Routage sur un équipement inter-réseaux (le routeur) : comme pour un pc la recherche se fait séquentiellement d’une route a une autre pour rechercher la correspondance avec l’adresse ip de destination (avec ET logique) trois cas de figure se présentent :

 \*la correspondance est trouvée et le paquet est envoyé vers le prochain saut pour atteindre la destination.

 \*Aucune correspondance n’existe sur la table mais il y a une route par défaut qui servira comme dernier recours et se chargera des paquet pour atteindre leur destination.

 \*Ni correspondance de route ni de route par défaut n’existent..le paquet est supprimé

La configuration de routage : alimentation de la table de routage en utilisant les deux techniques :

Routage statique : Ajout de route manuellement par l’administrateur

Routage Dynamique : Ajout de route automatiquement par des protocoles de routage (ex RIP ou OSPF)

Protocole ICMP : Internet Control Message Protocol : Protocole de messagerie de notification du contrôle de la connectivité ip de couche réseau (3). Ip est un protocole non fiable mais qui utilise la messagerie ICMP pour notifier un echec aux systèmes sources (destination inaccessible (réseau) ; hôte inaccessible ou (machine) ou service inaccessible (le port est indisponible). Le protocole ICMP est utilisé par les commandes ping et TRACERT.

Ping : commande ICMP de test de connectivité de couche 3 de bout en bout envoyant des paquets ICMP Echo request et recevant des paquets ICMP echo replay avec un rapport de connectivité contenant le délai de réponse le TTL ainsi que le pourcentage des paquets perdus et reçus. La commande peut être utilisé avec des commutateur / pour personnaliser le ping (nombre de paquets ; durée TTL …)

Tracert (Traceroute sur shell linux) : Commande ICMP utilisée classiquement après un echec d’un ping distant (entre des hôtes séparés par un ou plusieurs routeurs) . La commande permet de tracer la route entre la source et la destination avec des réponses à chaque saut (routeur) tracé par le paquet ip et de définir ainsi le dernier routeur (saut) qui répondra à la requête.

Protocole ARP : Address Resolution Protocol : protocole de couche 3 se charge du mappage (resolution) d’une adresse IP connue sur une adresse de couche 2 MAC inconnue. Au besoin d’une adresse MAC de destination de couche 2 ARP envoi une requête ARP-request à l’adresse 12F (diffusion : who is 192.168.1.1 par exemple) et attend la réponse de cet hôte ARP-replay (monodiffusion : 192.168.1.1 is 34 :7A : 55 :EE :8B :AA) comportant la résolution qui sera conservé dans le cache ARP (table de correspondance entre MAC et IP du réseau local)

Les commandes ARP : Arp –a pour afficher le cache arp

 Arp –d pour vider le cache arp

Découpage d’adresse de sous réseaux (nouveau masques) et calculs de schémas d’adressage (@R, 1ere @, Der @, @ BC et nombre d’hôte par S/R):

Pourquoi on découpe : Organisation ; performance (découpage des domaines de diffusion) ; sécurité (identité différente des sous réseaux)

Les règles de découpage : 2puissance n (possibles) ou 2 puissance n-2 (utilisables) n étant le nombre de bits à emprunter de la partie hôte pour l’ajouter à la partie réseau.

Les calculs réseaux : **NB : Ne jamais toucher à la partie réseau pour les calculs réseaux**

@Réseau : Mise à zéro de la partie hôte (s’obtient par AND logique avec le MSR)

1 ère @ machine : l’ajout de 1 binaire (bit faible) à droite de l’@ réseau

Dernière @machine : la soustraction de 1 binaire (remplacement par 0)(bit faible) à droite de l’@ de BC

@BC ou de diffusion : La mise à un de la partie hôte .

Le nombre de machine par sous réseau : 2 puissance n -2 (moins deux pour éliminer les adresses particulières réseau et broadcast)

Ce qui change sur le paquet IP en voyage vers la destination :

Le TTL (time to leave) : durée de vie codée sur 8 bits (2puissace8 : 256 sauts ou routeurs comme durée maximale) décrémente de un (-1) sur chaque routeur avant son transfert vers un autre routeur.

La fragmentation ou défragmentation : En passant d’un support LAN (grande MTU : maximal transfert Unit) vers un support WAN (petite MTU) le paquet est fragmenté pour correspondre à la capacité de la trame adaptée à ce dit support.

Le NAT et PAT : L’@ ip source privée (gratuite non routable) est remplacée par une autre publique (payante routable) en sortant vers internet, et vice versa en revenant d’internet vers le réseau local.

La couche 2 : Couche de liaison entre le logiciel et le matériel des composants réseau, reçoit le paquet IP (sous couche LLC :mise en trame et adressage MAC pour Ethernet par exemple) et se charge de la mise de la trame sur le support (sous couche MAC : début et fin de la trame et control des erreurs grâce au champs FCS : technique CRC)

A développer ……

Sous couche MAC et LLC ,

Domaine de diffusion

Domaine de collision

pont (bridge)

commutateur (switch)

Ethernet @MAC (unicast ; broadcast et multicast),

Topologie logique : ou méthodes d’accès :Correspond au mode de circulation des donnée entre une source et une destination, deux grandes approches

\*Basée sur le conflit (CSMA/CD sur cuivre , CSMA/CA sur wifi)

\*Basée sur le contrôle (passage du jeton : Token ring sur cuivre ou FDDI sur fibre optique)

CSMA/CD :

Passage du jeton :

Contrairement au paquet de couche 3 (en général IP) qui est indépendant des médias (câble ou support) ; La trame est très dépendante du support (méthodes d’accès différentes) on retrouve Trame ethernet LAN ; trame Token ring, trame WIFI ; trame PPP ; trame 3G etc……

La couche 1 : Couche de codage de la trame et de sa signalisation pour la mise sur le support ; signalisation électrique (cuivre) ; optique lumineuse (fibre) ou hertzienne pour le sans fil

Tableau comparatif des 3 types de supports sur : longueur du segment ; facilité d’installation ; coût ; sensibilité aux interférences électromagnétique (à remplir)

|  |  |  |  |
| --- | --- | --- | --- |
|  | Cuivre | Fibre optique | Sans fil |
| Longueur du segment sans répéteur |  |  |  |
| Facilité d installation |  |  |  |
| Coût |  |  |  |
| Sensibilité aux interférences électromagnétiques |  |  |  |

Topologie physique : Emplacement physique des postes et du câblage les uns par rapport aux autres. Sur les réseaux locaux elle a évolué pour les réseaux ethernet du BUS (10 base 2 et 10 base 5) vers l’étoile (10 base T sur un concentrateur : HUB) puis 100 base TX (fullduplex)puis 1000 base T….

Tableau des normes Ethernet (10 base 2 10 base 5 10 base T 100baseTx ; 1000baseT ; 100baseFX ; 1000baseCX, 10000baseSX, 1000baseLX ; 1000base ZX ; 1000 baseZR)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Half duplex :

Full duplex :

Norme de couleurA :

Norme de couleur B :

Interface MDI : Périphériques finaux (PC) ou inter réseaux (routeurs)

Interface MDIX : Périphérique intermédiaires (répéteur ; pont ; concentrateur, commutateur)

Câblage UTP:

Câblage droit ou direct (AA ou BB) utilisé entre des Interfaces différentes MDI-----MDIX

Câblage croisé (AB ou BA) : utilisé entre des Interfaces de même type MDI-----MDI ou MDIX-----MDIX

Bande passante :Capacité théorique maximale d’un réseau a transférer l infomation

Débit : Vitesse réelle de transfert mesurée (pratique)

Débit applicatif : le débit réel des données applicatives (reçus par la couche ou Protocol applicatif de couche 7) le temps et surcharge d’encapsulation et de désencapsulation sont pris encompte.

Calcul de la durée de transfert d’un fichier (10 Moctets) avec un débit de 10 Mbits/secondes.

(règle de trois n’oubliez pas que 1octet=8bits)