Synthèse R3.06 - Architecture des Réseaux Ce document reprend l'ensemble des concepts expliqués dans le cours (CM), le TD1, et les commandes/configurations utilisées dans les TPs 0, 1, 2, 3, 4 et leurs corrections.

1. Modèles et Bases Réseaux (CM & TP0) Modèle OSI et TCP/IP +1

Couche 1 (Physique) : Transmission des bits (câbles, fibres).

Couche 2 (Liaison) : Adressage MAC, commutation (Switch).

Couche 3 (Réseau) : Adressage IP, Routage (Routeur).

Couche 4 (Transport) : TCP/UDP, Ports.

Couche 7 (Application) : HTTP, DNS, etc.

Adressage et Routage +1

IP & Masque : L'adresse IP identifie l'hôte, le masque sépare la partie réseau (NetID) de la partie hôte (HostID). Le routage permet l'interconnexion de réseaux.

Commandes de base (TP0) :

Activer une interface : ip link set eth0 up

Ajouter une IP : ip addr add 192.168.1.1/24 dev eth0

Ajouter une route : ip route add 172.20.11.0/24 via 192.168.1.253

Activer le forwarding (routeur) : sysctl net.ipv4.ip_forward=1

2. Couche Transport : TCP vs UDP (TD1 & CM) Protocoles +2

TCP (Fiable, Connecté) : Garantit l'ordre, sans perte, sans duplication. Utilise un mécanisme de fenêtre glissante et d'acquittements (ACK). Utilisé pour HTTP, SSH, FTP.

UDP (Non fiable, Non connecté) : Plus rapide, pas de garantie de livraison. Utilisé pour DNS, Streaming, Voip.

Analyse Wireshark (TD1) Connexion TCP (3-way handshake) :

SYN (Client -> Serveur)

SYN/ACK (Serveur -> Client)

ACK (Client -> Serveur)

Champs importants : Port source/dest, Numéro de séquence (pour remettre dans l'ordre), Flags (SYN, ACK, FIN, RST).

3. Service Web : Apache (TP1 & Correction) Installation et Commandes Installation : apt install apache2

Gestion du service : systemctl start|stop|reload apache2

Configuration des VirtualHosts (Sites) +1

Les sites sont définis dans /etc/apache2/sites-available/.

Par Nom : Plusieurs sites sur la même IP, différenciés par ServerName.

Apache

<VirtualHost *:80> ServerName www.monsite.com (http://www.monsite.com) DocumentRoot /var/www/html/site1 Par Port : Écoute sur des ports différents (ex: 8080). Nécessite la directive Listen 8080 dans ports.conf.

Directives Importantes +1

DocumentRoot : Dossier racine du site.

DirectoryIndex : Fichier par défaut (ex: index.html).

Options Indexes : Autorise le listing des fichiers si pas d'index.

Require all granted : Autorise l'accès.

Alias /url /chemin/physique : Mappe une URL à un dossier hors du DocumentRoot.

UserDir : Permet l'accès via ~user (module mod_userdir).

.htaccess

Permet une configuration décentralisée par dossier. Nécessite AllowOverride All dans la configuration principale.

4. Sécurité : Firewall & Netfilter (TP2 & Correction) Exploration réseau (Nmap)

Scanner une machine : nmap -A 192.168.0.1

Scanner un réseau : nmap 192.168.0.1-254

Scan de ports spécifiques : nmap -p 80,443 IP

Détecter l'OS : nmap -O IP

Iptables (Netfilter) +1

Le pare-feu Linux filtre les paquets via des chaînes (INPUT, OUTPUT, FORWARD).

Politique par défaut (Tout bloquer) :

Bash

iptables -P INPUT DROP iptables -P OUTPUT DROP iptables -P FORWARD DROP Autoriser le trafic local (Loopback) :

Bash

iptables -A INPUT -i lo -j ACCEPT Autoriser un service (ex: Serveur Web entrant) :

Bash

iptables -A INPUT -p tcp --dport 80 -j ACCEPT iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT (réponse)

Suivi de connexion (Stateful): Plus sécurisé, on accepte les réponses aux connexions qu'on a initiées. +1

Bash

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT 5. DNS : Domain Name System (TP3 & CM) Rôle

Traduit un nom de domaine (ex: www.univ-nantes.fr (http://www.univ-nantes.fr)) en adresse IP.

Configuration BIND9 (named.conf)

Zone Maître (Master) : La source de vérité.

DNS Zone file

zone "mazone.com" { type master; file "/etc/bind/db.mazone"; }; Zone Esclave (Slave) : Copie de sauvegarde, se synchronise avec le maître.

DNS Zone file

zone "mazone.com" { type slave; masters { IP_DU_MAITRE; }; }; Fichier de Zone (Enregistrements) +2

SOA : Start of Authority (paramètres de zone).

NS : Serveur de noms de la zone.

A : Nom -> IPv4.

CNAME : Alias (ex: www pointe vers serveur1).

PTR : IPv4 -> Nom (pour la zone inverse).

6. NAT : Network Address Translation (TP4 & CM) Masquerading (SNAT) +1

Permet aux machines d'un réseau privé d'accéder à Internet via une seule IP publique (celle du routeur).

Commande :

Bash

iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE Port Forwarding (DNAT)

Rend un service interne (ex: Serveur Web privé) accessible depuis l'extérieur.

Commande :

Bash

```
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to 10.0.0.10
```