**SESSION 1\_DESS**

**Cours: Architecture des Réseaux**

**TD/TP 3**

1. **Commutation de niveau 2** La description est correcte : la commutation de la couche liaison (niveau 2) gère bien le transfert des trames via les adresses MAC et l’utilisation de tables de commutation pour acheminer les données est exacte. Le fait que les switches Ethernet segmentent les domaines de collision et permettent la mise en œuvre de VLANs est tout à fait pertinent. À noter toutefois qu’en mode full-duplex, les collisions ne se produisent plus, et cette segmentation aide surtout à organiser le trafic et à améliorer la sécurité.
2. **Commutation de niveau 3** Tu décris bien le fonctionnement de la couche réseau qui repose sur le routage IP avec l’utilisation de tables de routage et de protocoles tels qu’OSPF ou EIGRP. L’intégration de la QoS et du filtrage pour optimiser le trafic inter-sous-réseaux est également appropriée
3. **Adressage de réseau à valeur ajoutée** L’idée que le DHCP permet une gestion dynamique des adresses IP et que l’adressage hiérarchique facilite la gestion des sous-réseaux est bien expliquée. La segmentation par VLANs à ce niveau renforce la sécurité et la performance en isolant logiquement le trafic.
4. **Segmentation de réseau** La segmentation via VLANs et sous-réseaux permet effectivement de réduire les domaines de broadcast et d’isoler des groupes d’utilisateurs pour améliorer la sécurité et limiter le trafic superflu. La mention de politiques d’accès granulaires est également bien placée.
5. **Diffusion broadcast et multicast** Tu expliques correctement que le broadcast envoie des paquets à tous les hôtes (par exemple utilisé par ARP), tandis que le multicast cible un groupe spécifique, comme dans le cas du streaming vidéo. L’évocation d’IGMP pour gérer les adhésions aux groupes multicast est pertinente, même si IGMP contrôle plutôt la gestion des membres que la diffusion en elle-même.
6. **Services de noms, proxy et cache local** Le rôle des DNS, des proxies pour filtrer/rediriger le trafic, et du cache pour réduire la latence est bien résumé.
7. **Sécurité de l’accès au média** Tu cites des mécanismes courants comme 802.1X, le filtrage MAC et la sécurisation des ports pour prévenir les accès non autorisés et le MAC flooding..
8. **Découverte de routeurs** La mention d’ARP et d’ICMP dans le cadre de la découverte des gateways est correcte, tout comme l’introduction de protocoles de redondance comme HSRP (bien que des alternatives comme VRRP ou GLBP existent aussi).
9. **Gestion de la bande passante** L’application de la QoS pour prioriser certains flux (comme la VoIP) et le traffic shaping pour contrôler le trafic montant/descendant au niveau de la distribution est bien décrite.
10. **Filtrage de zones et de services** L’utilisation d’ACLs pour filtrer le trafic inter-VLANs et la fonction des firewalls dans la couche distribution pour bloquer les intrusions sont correctement détaillées.
11. **Distribution stratégique** L’implémentation de politiques de routage via des route-maps pour diriger le trafic selon des critères spécifiques est bien résumée. Ce rôle dans la gestion des coûts et de la performance est une notion clé dans la couche de distribution.
12. **Services de passerelle** La fonction des routeurs de distribution en tant que passerelles inter-sous-réseaux, avec des mécanismes comme le NAT ou la traduction inter-protocoles (IPv4/IPv6), est expliquée de façon adéquate.
13. **Redistribution de routes interprotocoles** Tu décris bien la redistribution entre différents protocoles de routage (par exemple OSPF vers EIGRP), en insistant sur la nécessité de gérer les métriques pour éviter les boucles de routage.
14. **Traduction du format de trame** La conversion d’un format de trame à un autre (comme Ethernet vers PPP pour les WANs) et l’encapsulation dans des technologies telles que MPLS pour assurer la compatibilité entre différents types de réseaux sont évoquées. Il est toutefois à noter que l’encapsulation MPLS est souvent associée à la transmission dans le cœur de réseau, et la traduction de format peut être réalisée par des dispositifs d’agrégation ou de médiation.
15. **Optimisation du chemin** L’utilisation de protocoles de routage dynamique tels que BGP et d’algorithmes comme SPF dans OSPF pour sélectionner le chemin le plus performant est bien recherchée.
16. **Priorité du trafic** La QoS via Demux DiffServ ou MPLS pour marquer les paquets (DSCP) et réserver de la bande passante afin d’assurer un SLA pour des flux critiques (comme la voix) est correctement énoncée.
17. **Équilibrage de charge** La répartition du trafic sur plusieurs liens (ECMP) et l’utilisation de mécanismes tels que l’anycast dans certains déploiements (souvent associé à BGP) sont bien détaillées. Quelques nuances pourraient être apportées sur l’usage de l’anycast, qui est surtout employé pour rapprocher les utilisateurs d’un serveur plutôt que pour un load balancing classique entre liens.
18. **Chemins alternatifs** L’emploi de la redondance via les protocoles FHRP et des liens redondants, ainsi que la capacité d’un protocole de routage à recalculer automatiquement les routes en cas de panne, est correctement exposé.
19. **Accès commuté** La mention des connexions commutées (dial-up, ISDN) et l’utilisation de PPPoE pour adapter le trafic aux infrastructures legacy illustrent bien les technologies plus anciennes qui peuvent être prises en charge, notamment à des fins de backup ou d’accès distant. Il faut toutefois noter que ces technologies sont aujourd’hui largement remplacées par des solutions plus récentes (ADSL, fibre, VPN via IP).
20. **Encapsulation (tunneling)** La description des tunnels IPsec ou GRE pour encapsuler des paquets et permettre le passage de données à travers des réseaux non fiables, en facilitant l’implémentation des VPN et l’interconnexion de réseaux privés via Internet, est tout à fait appropriée.