المرجو الدعوة لمن ساهم بنشر هذه الملخصات
بالنجاح و الرحمة للوالدين

Résumer par : Team YAAKOUB

Les types de routages dynamique ipv4 :

RIPV1 -RIPV2 -OSPFV2

Les protocoles de routage dynamique IPV6 :

RIPng – OSPFV3

La déférence entre vecteur de distance et état de liens :

+ **Vecteur de distance : en utilise comme poteaux indicateurs la longue topologie du réseau**
+ **Etat de liens : en utilise comme une carte complétée de la topologie du réseau**

Comparer le Routage Statique et Routage Dynamique :

Routage Statique :

+ **Configuration manuel**
+ **Plus sécurisé**
+ **La route vers la destination est toujours la mêmes**
+ **Moins de bande passante.**

Routage Dynamique :

+ **Configuration automatique**
+ **Moins sécurisé**
+ **La route dépend de la topologie en cours**
+ **Plus de bande passante**

RIP

Les Avantages RIP :

+ **Plus simple**
+ **Configuration est aisée**
+ **supporte L'authentification**

Les inconvénients RIP :

+ **Nombre de saut limite 15**
+ **Convergence lent**
+ **Moins sécurisée**

ملخص وحدة لينكس شامل لجميع فقرات الدرس

Routage Statique

Les avantages routage statique :

+ **Plus sécurité**
+ **Economie de bande passante**
+ **Ne consomme pas les ressources**

Les inconvénients routage statique :

+ **Mise à jour manuel**
+ **Boucles de routage**
+ **Pas de redondance**

Les types de routage statique :

+ **Route statique par défaut : est une route qui correspond à tous les paquets**
+ **Route statique flottante : est une route secondaire en cas de panne**
+ **Route statique récapitulative : pour résumé ou réduire le nombre d'entrées de la table de routage.**
+ **Route statique standard :**

Routage Dynamique

Les avantages routage dynamique :

+ **Configuration automatique**
+ **Moins les tâches administratives**
+ **Convient à toutes les topologies**

Les inconvénients de routage dynamique :

+ **moins sécurisé**
+ **Consommation les ressources**
+ **La route dépend de la topologie en cours**

Les fonctions de routage dynamique :

+ **La détection des réseaux distants**
+ **Le choix du meilleur chemin**

Protocole OSPF

Les avantages OSPF :

+ Convergence plus rapide
+ support de l'authentification
+ métrique de la bande passante

Les inconvénients OSPF :

+ Plus complexe
+ Configuration difficile
+ Moins sécurisé

le protocole OSPF à zones multiples:

Utilisé pour diviser en plusieurs zones un réseau OSPF de grande taille

Les types zones :

+ Zones fédératrice (transit)
+ Zones normale (non fédératrice)

Les types routeur OSPF multizones :

+ Routeur interne
+ Routeur fédérateur
+ Routeur ABR
+ Routeur ASBR

Les avantages du protocole OSPF multizones :

+ Réduction de la taille des tables de routage
+ Réduction de la fréquence des calculs SPF
+ Réduction de la surcharge liée aux mises à jour d'état de liens

Les types de LSA OSPF :

LSA 1 : LSA de routeur
LSA 2 : LSA de réseau
LSA 3 et 4 : LSA de récapitulation
LSA 5 : LSA externe du système autonome

Le rôle DR :

+ le protocole OSPF sélectionne le routeur DR comme point de collecte et distribution les paquets LSA envoyés et reçus
+ Eviter création de contiguïtés multiples
+ Eviter diffusion Passive de paquets

les critères de choix DR :

+ Priorité OSPF des interfaces plus élevées
+ ID routeur plus élevées
+ Adresse bouclages
+ Adresse interface plus élevées

Les types réseaux OSPF :

Point à point / accès multiple

le rôle BDR :

Un routeur BDR est également choisi au cas où le routeur DR est défaillant

Comment calculs les couts OSPF :

BANDE PASSANTE DE REFERENCE / BANDE PASSANTE DE INTERFACE

Comparaison entre OSPF et RIP :

OSPF	RIP
Convergence rapide	Convergence lent
Plus complexe	Plus simple
En fonction de la bande passante	En fonction du nombre de sauts
Algorithme de Dijkstra	Algorithme de BELLMAN-FORD

États opérationnels OSPF

État Down *État *État Two-Way *État ExStart *État Exchange *État Loading *État Full

Bases de données OSPF

Base de données de contiguïté / Base de données de Réacheminement / Base de données d'états de liens (LSDB)

Types de paquets OSPF

Hello / DBD / LSR / LSU / LSAck

DHCP

DHCP est un protocole réseau qui permet l'attribution automatique des adresses IP et des autres informations aux clients.

Les étapes de processus DHCP :

+ **DHCP DISCOVER**
+ **DHCP OFFER**
+ **DHCP REQUEST**
+ **DHCP ACK**

Fonctionne renouvellement d'Un bail

DHCPREQUEST – DHCPACK

Les différents types DHCP pour IPV6:

+ **DHCPV6 SANS ETAT = SLAAC + DHCP**
+ **DHCPV6 AVEC ETAT = DHCP uniquement**
+ **SLAAC = SLAAC uniquement**

NAT

La définition du NAT :

NAT permet de traduire une adresse IP privée en une adresse IP publique et routable.

Les avantages NAT / Le rôle NAT :

+ **Augmente la souplesse des connexions aux réseaux publics**
+ **Elle garantit la sécurité**
+ **Cohérence des schémas d'adressage du réseau interne**

Les inconvénients NAT :

+ **Perte de la traçabilité IP de bout en bout**
+ **L'adressage de bout en bout est perdu**
+ **Complexité de la transmission tunnel**

Les types de NAT :

+ **NAT statique : mappages un à un des adresses IP privées en adresses IP publiques**
+ **NAT dynamique : mappages de plusieurs adresses locales en adresses globales**
+ **PAT : mappages de plusieurs adresses locales en une adresse globale**

Types li adresse NAT

Adresse locale interne -adresse globale interne – adresse locale externe – adresse globale externe

SNMP :

Est un protocole de couche Application qui procure un format pour les messages de communication entre les gestionnaires et les agents

Le role SNMP :

permet aux administrateurs de gérer les périphériques sur un réseau IP. Ces derniers peuvent ainsi contrôler et gérer les performances du réseau, identifier et résoudre les problèmes et anticiper la croissance du réseau.

les types de requêtes SNMP :

get-request *get-next-request *get-bulk-request *get-respons *set-requeste

Versions SNMP

+ SNMPv1 : Utilise une méthode d'authentification basée sur une chaîne de communauté simple.Ne doit pas être utilisé en raison de risques de sécurité.

+ SNMPv2c : Utilise une méthode d'authentification basée sur une chaîne de communauté simple. Fournit des options de récupération en bloc ,ainsi que des messages d'erreur plus détaillés.

SNMPv3 : Utilise l'authentification par nom d'utilisateur, assure la protection des données à l'aide de HMAC MD 5 ou HMAC SHA et le chiffrement à l'aide du chiffrement DES, 3DES ou AES

Sécurité des ports :

La sécurité des ports peut être configurée pour autorisée une ou plusieurs adresses MAC.

Les type d'adresses MAC sécurisées :

+ MAC statiques
+ MAC dynamiques
+ MAC rémentes

Modes violations de la sécurité des ports :

SHUTDOWN : le port passe immédiatement à l'état désactiver par erreur
RESTRICT : le port supprime les paquets dont l'adresse source est inconnue. Un message SYSLOG généré.
PROTECT : le port supprime les paquets avec des adresses source MAC inconnues. Aucun message SYSLOG n'est envoyé.

Obsolescence de la sécurité des ports :

+ Absolue : les adresses sécurisées sur le port sont supprimées après le temps d'obsolescence spécifié.
+ Inactivité : les adresses sécurisées sur le port sont supprimées si elles sont inactives pendant une durée spécifiée.

Les techniques d'atténuation des attaques de commutateur

+ Sécurité des ports : Empêche de nombreux types d'attaques, y compris les attaques d'inondation d'adresses MAC et les attaques d'insuffisance DHCP
+ Espionnage (snooping) DHCP : Empêche l'insuffisance DHCP et les attaques d'usurpation du DHCP.
+ Inspection ARP dynamique (DAI) : Empêche l'usurpation d'ARP et les attaques d'empoisonnement d'ARP.
+ Protection de la source IP (IPSG) : Empêche les attaques d'usurpation d'adresse MAC et IP.

Les catégories d'attaque de commutateurs

+ Les Attaques de table MAC : Il comprend les attaques par inondation de l'adresse MAC.
+ Attaques de VLAN : Il comprend les attaques par saut et par revérifier VLAN. Il aussi comprend les attaques entre les périphériques sur un VLAN commun.
+ Attaques DHCP : Il comprend les attaques d'insuffisance DHCP et les attaques d'usurpation DHCP.
+ Les attaques ARP : Il comprend les attaques d'usurpation ARP et les attaques d'empoisonnement ARP.
Les attaques STP : Il comprend les attaques de manipulation du protocole Spanning-Tree.
Attaques par usurpation d'adresse Il comprend les attaques d'usurpation d'adresse MAC et d'adresse IP.

NTP

Le NTP peut être configuré pour se synchroniser avec une horloge maîtresse privée,

CDP :

Est un protocole de couche 2 propriétaire de Cisco qui est utilisé pour recueillir des informations sur les appareils Cisco qui partagent la même liaison de données.

LLDP :

est un protocole de détection voisin ouvert semblable au protocole CDP. LLDP fonctionne avec des périphériques réseau, tels que des routeurs, des commutateurs et des points d'accès LAN sans fil.

Réseau local sans fil (WLAN) :

Est un type de réseau sans fil couramment utilisé dans maisons, les bureaux et les campus.

Le rôle WLAN :

Les WLAN rendant la mobilité possible dans les environnements domestiques et professionnels.

Quelles sont les normes 802.11 compatibles avec la bande de fréquence 2,4 GHZ ?

802.11 N * 802.11 G * 802.11 B * 802.11 AX * 802.11

Expliquez les interférences pour la bande 2.4 GHZ. Donnez des exemples de dispositifs causant ces problèmes

- **Le four à micro-ondes**
- **téléphones sans fi**
- **webcams sans fi**
- **appareils Bluetooth**

Quelles sont les normes 802.11 compatibles avec la bande de fréquence 5 GHZ ?

802.11 A * 802.11 N * 802.11 AC * 802.11 AX

Types d'antennes externes:

+ Omnidirectionnel : Fournit une couverture à 360 degrés. Idéal dans les maisons et les bureaux.

+ Directionnel : Concentrez le signal radio dans une direction spécifique. Les exemples sont le Yagi et le plat parabolique.

+ Entrées multiples Sorties multiples (MIMO) : Utilise plusieurs antennes (jusqu'à huit) pour augmenter la bande passante.

Modes topologies sans fil 802,11 :

- **Mode infrastructure**
- **Partage de connexions**

CAPWAP est un protocole standard IEEE qui permet à un WLC de gérer plusieurs AP et WLAN.

Le rôle CAPWAP :

Encapsule et transfère le trafic client WLAN entre un AP et un WLC sur des tunnels sen utilisant les ports UDP 5246 et 5247.

Le mode infrastructure définit deux blocs de topologie:

+ Ensemble de services de base (BSS) : Un BSS consiste en un seul AP interconnectant tous les clients sans fil associés.
Les clients de différents BSS ne peuvent pas communiquer.

+ Ensemble de service étendu (ESS) : Union de deux ou plusieurs BSS interconnectés par un système de distribution câblé.
Les clients de chaque BSS peuvent communiquer via l'ESS.

Fonctions MAC AP

- **Balises et réponses des sondes**
- **Accusé de réception et retransmissions de paquets**
- **Mise en file d'attente des trames et priorisation des paquets**
- **Cryptage et décryptage des données de la couche MAC**

Fonctions MAC WLC

- **Authentification**
- **Association et réassociation de clients itinérants**
- **Traduction de trame vers d'autres protocoles**
- **Arrêt du trafic 802.11 sur une interface filaire**

Les attaques visant le WLAN :

- **Les Attaques DoS**
- **Les Points d'Accès Non Autorisés**
- **Attaque d'Homme-au-Milieu**

Mécanismes de sécurité WLAN

- **Masquage SSID et filtrage des adresses MAC**
- **Méthodes d'authentification d'origine du 802.11**

MPL5

technologie de routage WAN de fournisseur de services haute performance pour interconnecter les clients sans tenir compte de la méthode d'accès ou de la charge utile

DWDM : est une technologie plus récente qui augmente la capacité de charge des données de SDH et SONET

WAN (Un réseau étendu)

est un réseau de télécommunications qui s'étend sur une zone géographique relativement vaste et qui doit se connecter au delà des limites du réseau local

Les type de WAN

* **Un WAN privé :** est une connexion dédiée à un seul client.
* **WAN publique :** est généralement fournie par un FAI ou un fournisseur de services de télécommunication utilisant l'internet.

AVANTAGE WAN PRIVE

+ Niveau de service garanti + Bande passante cohérente + Sécurité

Li topologie de WAN

+ Topologie point à point

Utilise un circuit point à point pour relier deux terminaux.

+ Topologie en étoile

Permet de partager une interface unique sur le routeur du concentrateur avec tous les Circuits en étoile

+ Topologie à double résidence

Elle offre une meilleure redondance du réseau, un équilibrage des charges, un calcul et un traitement distribués

+ Topologie à maillage global

- Utilise plusieurs circuits virtuels pour connecter tous les sites
- La topologie la plus tolérante aux pannes

+ Topologie partiellement maillée

Connecte de nombreux sites mais pas tous

WAN dans le modèle OSI

+ Protocoles de couche 1

Exemple

+ Synchronous Digital Hierarchy (SDH)
+ Synchronous Optical Networking (SONET)
+ Multiplexage en longueur d'onde dense (DWDM)

+ Protocoles de couche 2

Exemple

+ Sans-fil
+ WAN Ethernet (Metro Ethernet)

Types d'appareils spécifiques aux environnements WAN

DTE / DCE

- Communication commutée par circuits

Un réseau à commutation de circuits établit un circuit (ou canal) dédié entre les points d'extrémité avant que les utilisateurs puissent communiquer.

- Communication commutée par paquets

La communication réseau est le plus souvent implémentée à l'aide de la communication commutée par paquets

Normes OSI de fibre optique de couche 1

SDH : est une norme mondiale pour le transport de données sur un câble à fibre optique

SONET : est la norme nord-américaine qui fournit les mêmes services que SDH

Les Réseaux de fournisseurs de services utilisent

SDH / SONET / DWDM

Ligne louée

AVANTAGE Simplicité / Qualité / Disponibilité

Inconvénients Coût / Flexibilité limitée

Les connexions à commutation de paquet

+ Mode de transfert asynchrone (ATM) : peut transférer de la voix, de la vidéo et des données sur des réseaux privés et publics.

Les connexions à commutation de circuits

+ Réseau téléphonique public commuté (RTPC)
+ RNIS (Réseau Numérique à Intégration de Services)

Options de connectivité WAN moderne

Haut débit dédié / Commutation de paquets / Haut débit sur l'internet

SWITCH

Un switch est un équipement qui fonctionne comme un pont multiport et qui permet de relier plusieurs segments d'un réseau informatique entre eux

VLAN

Un vlan est une partition logique d'un réseau de couche 2

Les avantages vlan :

+ Sécurité + Réduction des couts + Réduire les domaines de diffusion
+ Efficacité accrue des équipes informatiques

Les types de vlan :

+ Vlan de gestion : est un réseau local virtuel configuré pour accéder aux fonctionnalités de gestion
+ Vlan natif : est affect a un port trunk 802.1Q, le vlan natif c'est le vlan 1 par default
+ Vlan par défaut : jouer le rôle vlan natif et vlan de gestion
+ Vlan de données : configurée pour transmettre le trafic génère par l'utilisateur

Le routage inter-vlan

Une technique d'acheminement du trafic réseau d'un VLAN à un autre qui repose sur l'utilisation d'un routeur.

Les méthodes le routage INTER-VLAN :

Routage existant : il s'agit une solution héritée. Il n'est pas bien dimensionné

Router-on-a-stick: c'est une solution acceptable pour un réseau de petite a moyenne taille.

Commutateur MUTICOUCHE : il s'agit de la solution la plus évolutive pour les moyennes et grandes entreprises.

Les problèmes courants d'inter-Vlan :

+ Problèmes de configuration de routeurs
+ Problèmes de port de TRUNK de commutateur
+ Problèmes lies aux ports de commutateurs

les deux méthodes de transmission pour la commutation :

+ Store-And-FORWARD : est une méthode de transmission des données fiable qui permette la détection le contrôle de FCS
+ CUT-THROUGH : est une méthode de transmission plus rapide mais ne contient pas le contrôle FCS

Caractéristiques des commutateurs multicouches :

+ Routage plus rapide par rapports aux routeurs
+ Les ports peuvent être configurés en ports « routés »
+ Prennent en charge certains protocoles de routage

Les avantages des commutateurs multicouches :

+ Plus rapides que les routeurs on-a-stick
+ Ils ne sont pas limités a une liaison
+ La latence est bien plus fiable

Quel est l'équipement qui peut remplacer un routeur pour effectuer le routage inter-vlan ? Switch multicouche

Les inconvénients des commutateurs multicouches : Sont plus chers

ACL

Une ACL permet de vérifier le flux traversant un routeur. Elle peut également permettre de restreindre l'accès aux lignes virtuelles (VTY).

Type une ACL

+ Les ACL Standard (de 1 à 99) : bloque tous le trafic
+ Les ACL étendues (de 100 à 199) : bloque un ou plusieurs trafics
+ Les ACL nommées : peut-être de type standard ou étendue

Les Avantage ACL

ACL est donc de fournir une base de sécurité réseau en filtrant les trafics traversant un routeur

Les Inconvénient ACL

Le principal inconvénient est malheureusement un traitement supplémentaire à effectuer pour chaque paquet entrant et ou sortant du router

Spanning Tree

Est un protocole qui permit bloque logiquement les boucles physiques dans un réseau de couche 2 empêchant les trames d'encercler le réseau pour toujours.

Les avantages de STP

+ Eviter tempête de diffusion
+ Eviter boucles de commutation
+ Eviter trames de monodiffusion en double
+ Eviter instabilité de la base de données MAC
+ REDONDANCE LAN

Les problèmes d'une boucle de la couche liaison de données / Les inconvénients :

+ Tempête de diffusion
+ Boucles de commutation
+ Trames de monodiffusion en double
+ Instabilité de la base de données MAC

Les étapes de l'algorithme STP :

+ Election du pont racine
+ Election des ports racines
+ Choix des ports désignés
+ Choix des ports alternatifs

Le rôle le pont racine :

Sert de point de référence pour tous les calculs de l'algorithme STA afin de déterminer les chemins d'accès redondants devant être bloqués

Critères de choix pont racine :

+ La priorité plus fiable
+ L'adresse MAC la plus fiable

Une BPDU : est une trame de message échangée par les commutateurs pour le protocole STP.

Les types protocoles STP / Les variantes STP :

Protocole	Norme	Ressources nécessaires	convergence	Calcul d'arborescence
STP	802.1D	Fiable	Lente	Tous les vlan
PVST+	CISCO	Elevée	Lente	Par vlan
RSTP	802.1W	Moyenne	Rapide	Tous les vlan
Rapide PVST+ -MSTP	CISCO -802.1S CISCO	Très Elevée -moyenne Ou élevée	Rapide -Rapide	Par vlan -par instance

Rôles des ports :

Décrivent la relation entre les ports du réseau et le pont racine, et indiquent s'ils sont autorisés à réacheminer du trafic de données.

Li types rôles des Port

+ Ports racine (PR) : il s'agit des ports de commutation les plus proches du pont racine.
+ Ports désignés (PD) : il s'agit de tous les ports non racine qui sont autorisés à acheminer le trafic sur les réseaux.
+ Ports alternatifs et ports de sauvegardes (PA) : sont configurés avec un état de blocage, pour éviter la formation de boucles.

État du port

Blocage *Écoute *Apprentissage *Acheminement *Désactivé

La convergence STP nécessite trois minuteurs :

•Minuteur Hello •Minuteur Forward Delay •Minuteur Max Age

Comment la STA crée-t-elle une topologie sans boucle

- Sélection d'un pont racine
- Les chemins redondants bloqués
- Créer une topologie sans boucle
- Recalculer en cas de défaillance du

Etherchannel

Est une technologie d'agrégation de liens qui permet d'assembler plusieurs liens physiques Ethernet identiques en un seul lien logique.

L'agrégation de liaisons :

Est la capacité à créer une liaison logique en utilisant plusieurs liaisons physiques entre deux périphériques. Cela permet de partager la charge entre les liaisons physiques et d'éviter que STP bloque un ou plusieurs liaisons.

Les avantages l'agrégation de liaisons ETHERCHANNEL :

- **Amélioration de la bande passante**
- **Assurer la disponibilité en utilisant des liaisons redondantes**
- **L'équilibrage de charge**
- **Un ETHERCHANEEL repose sur les ports de commutation existants.**
- **ETHERCHANNEL crée une agrégation considérée comme une seule liaison logique.**

Restrictions et considérations ETHERCHANNEL :

- **8 ports aux maximums pour une liaison ETHERCHANNEL**
- **Prise en charge de 6 liaisons ETHERCHANNEL**
- **Même type ports**
- **Mode bidirectionnel simultané**
- **Cohérence de la configuration**

La déférence entre PAGP et LACP :

- **PAGP : est un protocole propriétaire de CISCO qui facilite la création automatique de liaisons ETHERCHANNEL**
- **LACP : est un protocole non propriétaire de CISCO permet de créer la liaison ETHE**

Les modes LACP :

S1	S2	Etablissement de canal
Activé	Activé	Oui
Active / Passive	Active	Oui
On (Activé)/Active (Actif)/Passive (Passif)	Non configuré	Non
Activé	Active	Non
Passive (Passif)/On (Activé)	Passif	Non

Les modes PAGP:

S1	S2	ETABLISSEMENT CANAL
Activé	Activé	Oui
Auto /Désirable (souhaitable)	Souhaitable	Oui
On (activé) / Auto/Désirable (souhaitable)	Non configuré	Non
Activé	Souhaitable	Non
Auto / On (Activé)	Désirable	Non

VTP

Est un protocole en utilise pour administrer et gérer des vlan
Pour des périphériques CISCO uniquement.

Le rôle VTP :

Permet de configurer les VLANS sur un seul commutateur, et ce dernier grâce à transfèrera ces informations aux autres commutateurs du même domaine.

Les avantages VTP :

+ Propager les informations vers les autres commutateurs
+ Renommer de VLAN sur des switches serveur
+ VTP permet de créer

Les modes VTP :

+ Server : permet de créer, supprimer ou modifier les informations des VLANS, ce commutateur enverra aux autres ces informations c'est le mode par défaut d'un commutateur
+ Client : accepte les modifications reçus du serveur et les applique (mettre à jour sa base de données)
+ Transparent : les commutateurs transparents transmettent les annonces VTP aux clients et serveurs VTP

Le numéro de révision :

C'est un numéro envoyé du serveur vers client pour mettre à jour sa base de données VLAN.

Pour réinitialiser le numéro de révision :

Changer le nom de domaine VTP par un nom inconsistant et remettre le nom correct.

Critère de choix de switch serveur :

+ Central
+ Puissant
+ Facile à gérer

Que fait le commutateur lorsqu'elle reçoit une annonce VTP avec un numéro de révision supérieure à celui qu'il contient :

Le commutateur n'est pas concerné par les annonces VTP du domaine, il est en mode transparent.

Les protocoles de premier saut

HSPR : pour les hôtes IP sur les réseaux configurés avec une adresse de passerelle virtuelle
GLBP : Il s'agit d'un FHRP propriétaire de Cisco qui protège le trafic de données d'un routeur ou d'un circuit défaillant
VRRP : qui attribue dynamiquement la responsabilité d'un ou plusieurs routeurs virtuels aux routeurs VRRP sur un réseau local IPv4.

États HSRP

Initial *Apprendre *Écouter *Parler * En attente

Les avantage HSPR :

*** Les protocoles de redondance de premier saut (FHRP) sont des mécanismes qui fournissent des passerelles alternatives par défaut**
*** Il fournit une connexion réseau continue en cas d'échec d'un routeur.**
*** utilisé pour assurer la disponibilité**

SYSLOG:

Syslog utilise le port UDP 514 pour envoyer des messages de notification d'événements sur les réseaux IP aux collecteurs de messages d'événements, comme le montre la figure.

trois fonctions principales

+ La capacité à collecter les informations de journalisation pour la surveillance et le dépannage
+ La capacité de sélectionner le type d'information de journalisation capturée
+ La capacité à spécifier les destinations des messages Syslog capturés

Router

Est un équipement réseau informatique assurant le routage des paquets.

Le Rôle un router

+ Il assure l'interconnexion des réseaux
+ Il assure le routage des paquets vers la bonne destination

les composants les router

Processeur - Stockage et mémoire (RAM, ROM, NVRAM, flash, disque dur) - Système d'exploitation (OS)

Méthodes de transmission des paquets (router)

Permutation de processus - Commutation rapide - Cisco Express FORWARDING (CEF)

Présenter le processus de démarrage d'un routeur

Post – BOOTSTRAP - Chargement de IOS à partir de la mémoire flash - Chargement du fichier de configuration à partir de la NVRAM

Les types de connexion de base d'un router

Connexion des ports de gestion – connexion des interfaces LAN – connexion des interfaces WAN- en mode console

Les éléments nécessaires pour se connecter a un routeur par console :

+ Câble de console + Pc portable + Logiciel putt + Logiciel TERA-TERME

Caractéristiques d'un réseau

Vitesse – sécurité –fiabilité –cout

Li Définition

Interface de bouclage : est une interface logique interne du routeur

Un port routé : Est un port physique qui se comporte comme une interface sur un routeur.

Meilleur chemin : est sélectionné par un protocole de routage en fonction d'une valeur ou d'une métrique qu'il utilise pour déterminer la distance à parcourir pour atteindre un réseau.

Une métrique : est la valeur utilisée pour mesurer la distance par rapport à un réseau donné

DTP : est un protocole qui gérer la négociation du TRUNK

SSH : est un protocole de communication sécurisée message chiffré

ARP : est un protocole résolution adresse IP en adresse MAC.

RARP : est un protocole de résolution adresse MAC en adresse IP.

TELNET : est un protocole de communication no sécurisé

FHRP : est un acronyme cisco pour désigner les protocols de redondance du premier saut

MONODIFFUSION : est une adresse en utilise pour envoyer un paquet vers une seul destination

MULTIDIFFUSION : est une adresse en utilise pour envoyer un paquet vers un groupe de destination spécifier

DIFFUSION : utilise pour envoyer un paquet vers plusieurs destinations

Câble croisé : en utilisé entre des équipements de même type sachant un routeur à un ordinateur

Câbles droits : en utilisé entre des équipements de type déférent

Auto-MDIX : est une fonction en utilise pour détecter automatiquement les types des câbles.

Auto-speed : est une fonction en utilise pour la négociation des Paramètres vitesse.

HALF-DEBLEX : no simultanée qui permet l'envoi ou recevoir des donnés.

Full-DEBLEX : est une communication bidirectionnelle simultanée qui permit l'envoi et recevoir de donnés

FCS/CRC : c'est un code pour détection des erreurs et en ajoute à la fin de trame.

CSMA/CD : est un mécanisme en utilise pour détecter et évité des collisions

Une adresse link-local IPv6 : permet à un appareil de communiquer avec d'autres appareils IPv6 sur la même liaison et uniquement sur cette liaison (sous-réseau)

VPN

Réseaux privés virtuels (VPN) pour créer des connexions de réseau privé de bout en bout.

Un VPN est virtuel en ce sens qu'il transporte des

Informations au sein d'un réseau privé, mais que ces informations sont effectivement transférées via un réseau public.

Les principaux avantages des VPN

Réductions des coûts / Sécurité / Extensibilité /

Compatibilité

Types de VPN

VPN d'accès à distance / SSL VPNs
GRE sur Ipsec

Technologies VPN

+ VPN de site à site et d'accès distant

. Un VPN de site à site se termine sur les passerelles VPN

Le trafic VPN n'est crypté qu'entre les passerelles. Les hôtes internes ne savent pas qu'un VPN est utilisé

. VPN d'accès à distance est créé dynamiquement lorsque cela est nécessaire pour établir une connexion sécurisée entre un client et un périphérique de terminaison VPN.

+ VPN d'entreprise et de prestataire de service

VPN d'entreprise : des solutions similaires pour sécuriser le trafic d'entreprise sur l'internet

VPN des prestataires de services : sont créés et gérés sur le réseau du fournisseur

VOIP

Permet de passer ou de recevoir des appels via l'internet au lieu des lignes fixes traditionnelles

Max-dn: max number of phone lines

Max-ephone: max number of telephones

Auto assign: enregistrer automatiquement les téléphones 1 a 5

Le téléphone VoIP Est un commutateur à trois ports:

- **Le commutateur utilisera CDP pour informer le téléphone du VLAN voix.**
- **Le téléphone marquera son propre trafic (Voix) et peut définir le coût du service (CoS). CoS est QoS pour la couche 2.**
- **Le téléphone peut ou non étiqueter les trames du PC.**

Services intégrés (IntServ)

IntServ offre la qualité de service de bout en bout dont les applications en temps réel ont besoin.

LES AVANTAGES Services intégrés (IntServ)

- Contrôle d'admission des ressources explicite, de bout en bout.
- Contrôle d'admission de la stratégie par demande.
- Signalisation des numéros de port dynamiques.

Les inconvénient Services intégrés (IntServ)

Consommation importante de ressources due aux exigences de signalisation continue de l'architecture dynamique.

Services différenciés (DiffServ

Services différenciés (DiffServ) propose un mécanisme simple et évolutif pour classer et gérer le trafic réseau.

Les avantages Services différenciés (DiffServ:

- Haute évolutivité
- Large choix de niveaux de qualité

Les inconvénient Services différenciés (DiffServ

Aucune garantie stricte de la qualité de service