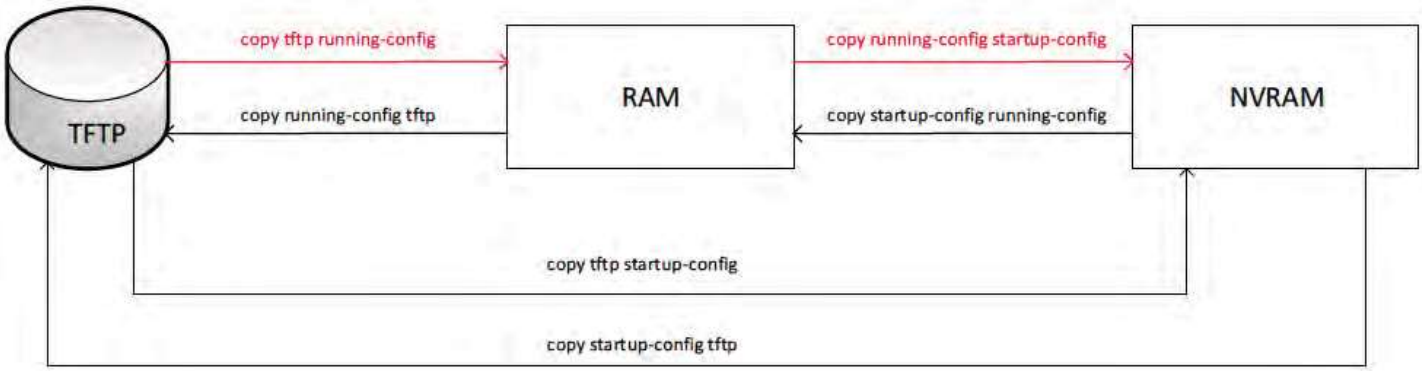
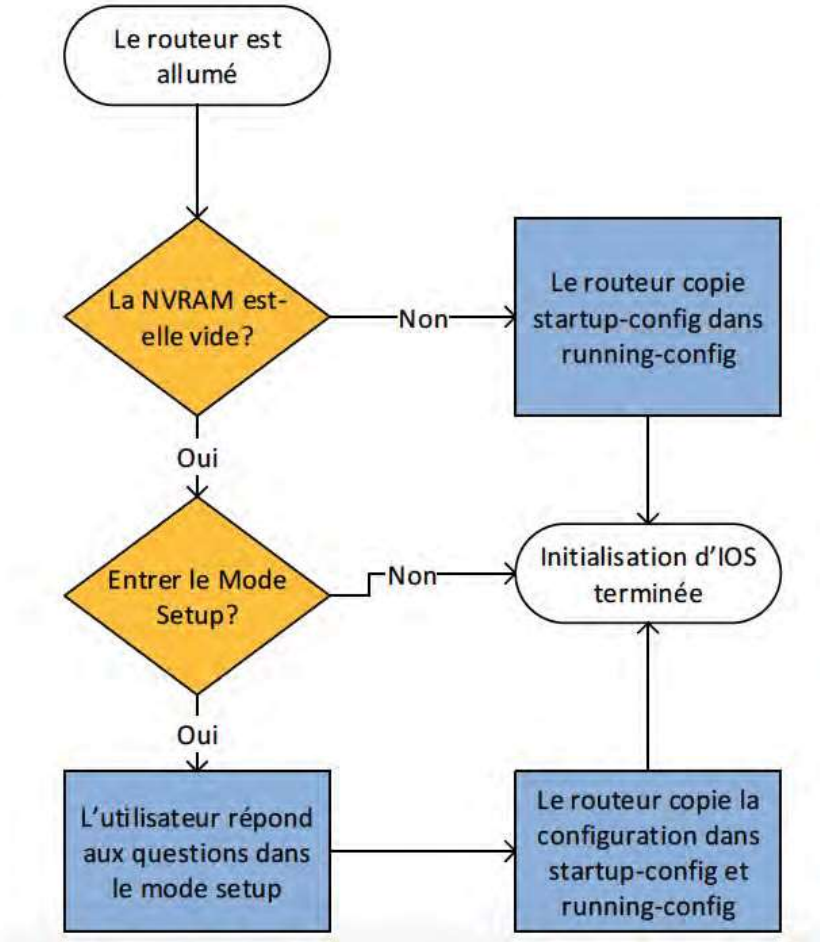
GESTION DES FICHIER IOS

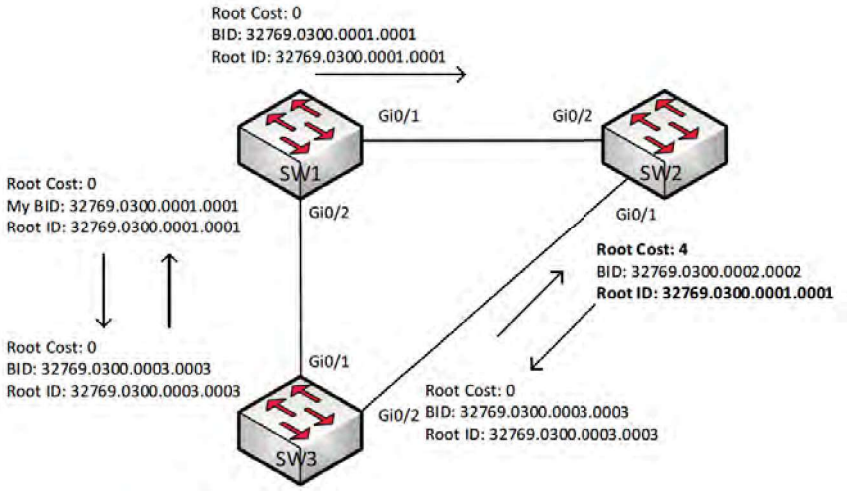
Les commandes Copy et leurs emplacements





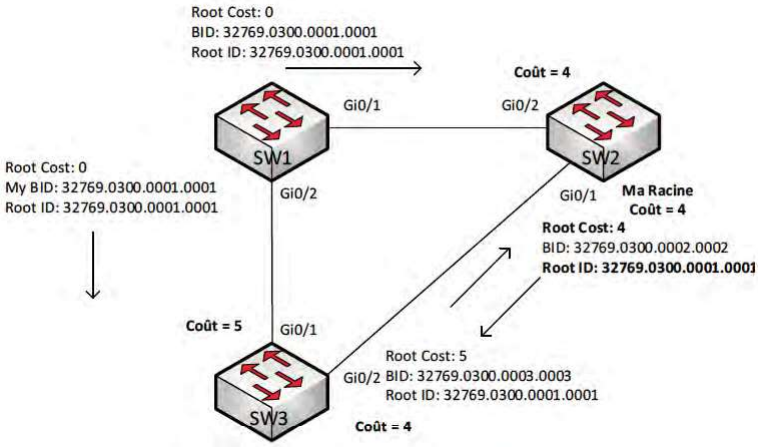
FLUX LOGIQUE POUR LE CHARGEMENT DE LA CONFIGURATION DANS LE ROUTEUR

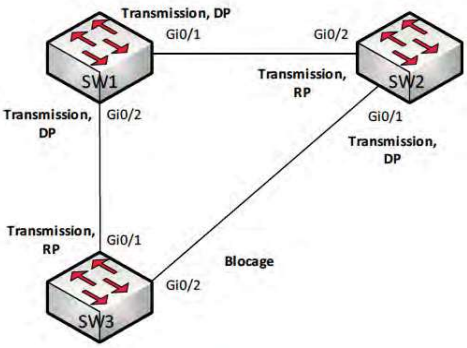
CONCEPTS DU PROTOCOLE SPANNING TREE



Au début du processus de sélection de la racine STP (Root Bridge), SW1 croit déjà qu'il est racine et envoie des BPDU avec son ID de pont (BID) comme le pont racine. SW2 a déjà décidé qu'il n'est pas le pont racine et annonce son BID plus le Root ID de SW1. SW3 pense qu'il est le pont racine mais puisque son BID est plus élevé que les deux autres, les BPDU de SW3 ne sont pas considérés par SW1 et SW2

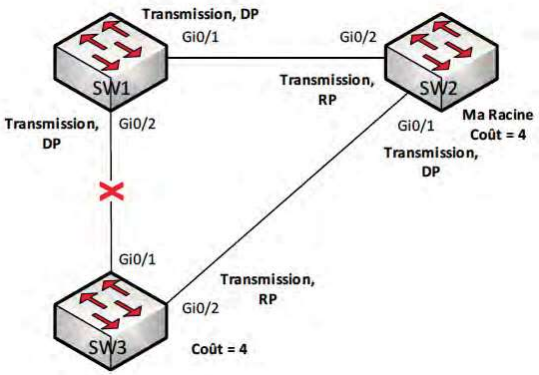
À ce stade, SW1 a gagné son élection. SW3 annonce que son coût racine à SW2 est 5. SW2 a un coût racine égal à 4. SW2 sait que le plus faible coût vers la racine est 4 en passant par GI0/2. SW3 sait que le coût racine par Gi0/1 vers SW1 est 5 et basé sur le hello de SW2, le coût racine par Gi0/2 est 8 (4 + 4).





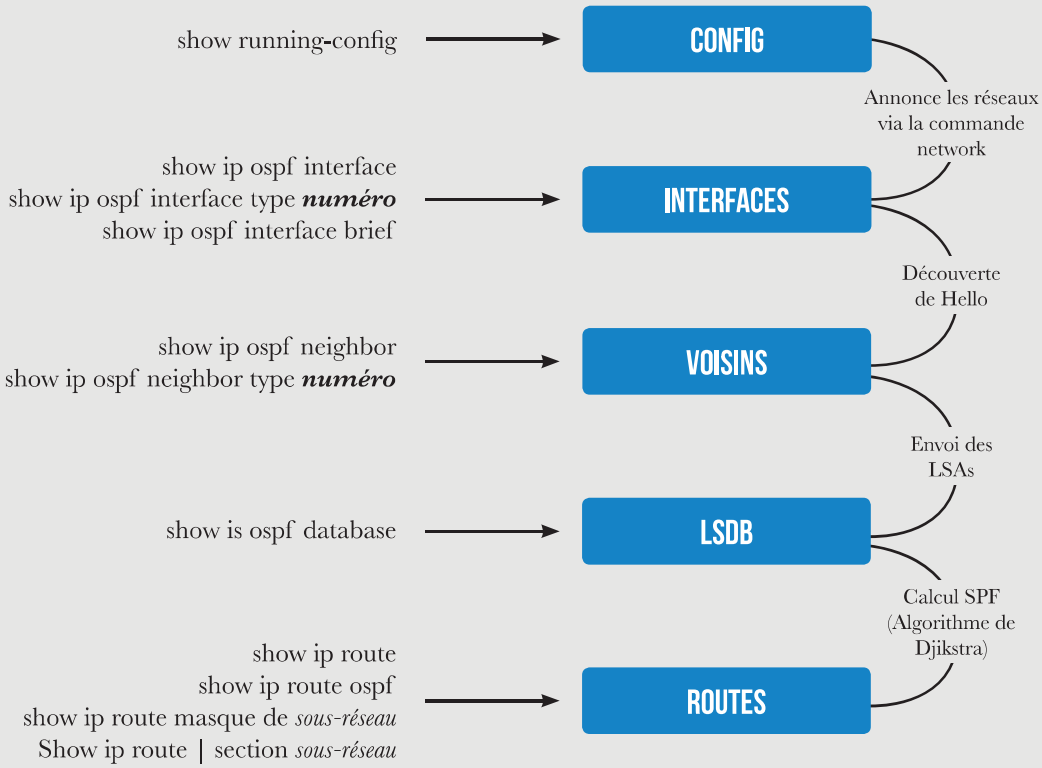
Après les calculs d'élection et de coût, STP prend ses décisions de transmission et de blocage sur chaque commutateur. SW1 est le commutateur racine, alors ses deux ports sont mis à transmission et port désigné (DP) sur leurs segments respectifs.
SW2 Gi0/2 et SW3 Gi0/1 sont des ports racines (RP) donc ils sont mis au statut de transmission. SW2 Gi0/1 est mis à transmission et est le DP sur sa connexion à SW3. SW3 Gi0/2
n'est ni un RP ni un DP, donc le port est mis à bloqué.

Ici, le lien entre SW1 et SW3 est tombé. Le recalcul de STP a été déclenché. À présent, SW2 annonce que son coût vers la racine est 4 et puisque SW3 n'a pas entendu d'autreS annonces de racine, son coût est 8 (4+4). SW3 change GI0/2 de Bloqué à Écoute, puis finalement, Transmission. Gi0/2 devient le RP pour SW3.



MISE EN OEUVRE DE OSPFV2 (IPV4)

COMMANDES DE VISUALISATION DU PROCESSUS OSPF ET LA PROGRESSION DE LA CONVERGENCE



CALCUL DE ROUTEUR-ID OSPF (RID)

1) Si le router-id rid est configuré sous router ospf, utilisez-le

2) Si OSPF RID n'est pas défini, choisissez l'adresse IP au numéro le plus élevé pour l'OSPF RID

3) Si le RID ne peut être fixé via une adresse IP loopback, utilisez l'adresse IP numérique la plus élevée sur une interface non-loopback

DÉFINITION D'ADJACENCE	ÉTAT DU VOISIN	DESCRIPTION
Adjacent (adjacency)	2-way	Les routeurs sont voisins sur la base des paquets hello. La relation d'adjacence est bonne
Complètement Adjacent (Fully adjacency)	Full	Les deux routeurs ont échangé les mêmes informations de base de données de l'état des liens

ÉTATS DES VOISINS OSPF

1) La couche physique est activée

2) Les paquets Hello sont échangés avec les IDs de routeur

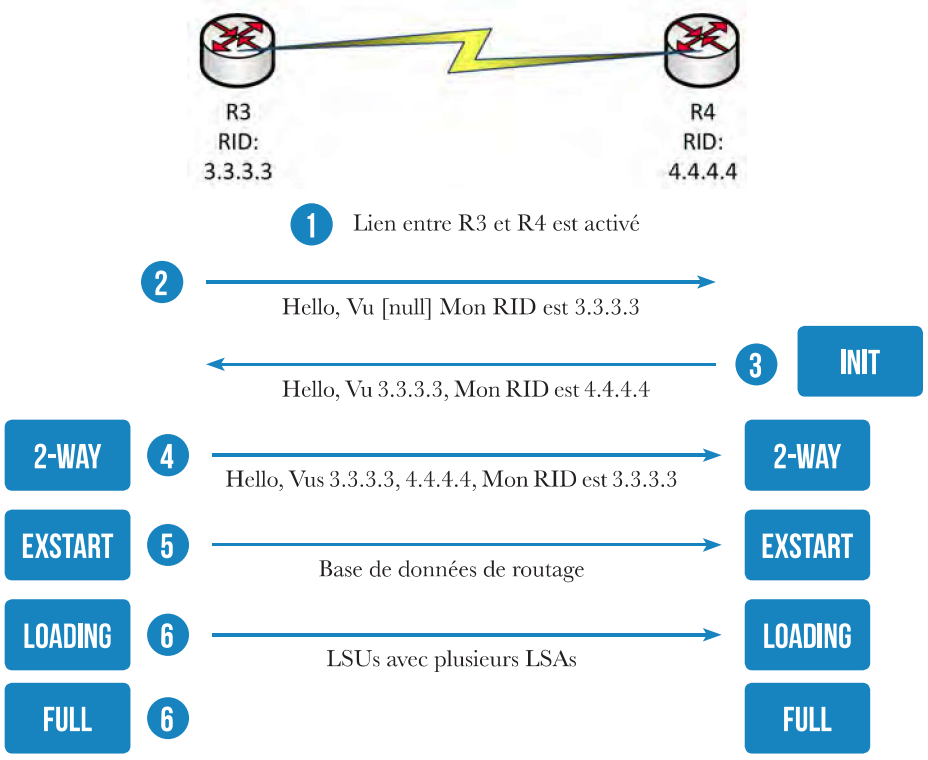
3) Le processus Init commence quand un routeur reconnaît l'autre routeur

4) **2-way** signifie que la communication bidirectionnelle est établie entre les deux routeurs

5) **ExStart** est le point où les routeurs échangent des informations de routage

6) **Loading** est l'état où les mises à jour d'état de liens sont échangées et les calculs SPF sont faits

7) Un état **Full** signifie que les routes sont échangées entre les deux routeurs



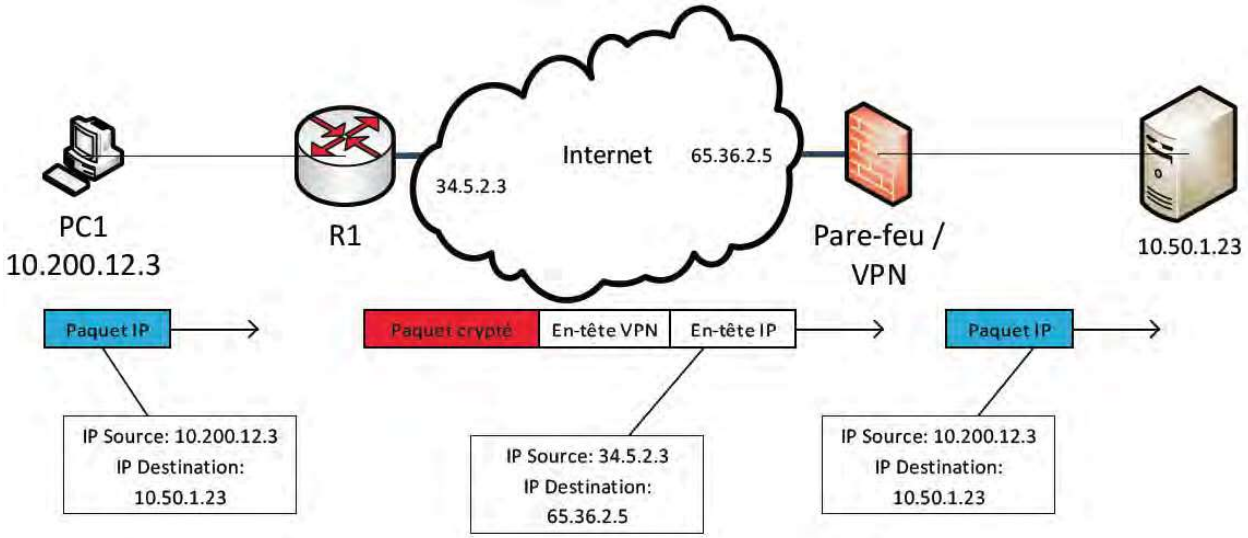
RÉSEAUX PRIVÉS VIRTUELS

POINTS CLÉS DES RÉSEAUX PRIVÉS VIRTUELS (VIRTUAL PRIVATE NETWORK):

Un Réseau Privé Virtuel (VPN) est un moyen d'avoir la sécurité d'une ligne louée sans les frais mensuels. Un VPN est établi entre deux points ou plus à travers un réseau non sécurisé tel que l'Internet et le trafic est crypté entre les points établis.
Un VPN est **privé** ce qui signifie que les données sont cryptées en transit et cela empêche les attaques du milieu appelée **man-in-the-middle.**
Un VPN fournit **l'authentification** parce que le récepteur peut vérifier que l'expéditeur du paquet est authentique
Un VPN fournit **l'intégrité** des données en s'assurant que le paquet n'a pas été modifié par un tiers alors qu'il était en transit vers la destination.
Un VPN empêche également les **attaques par rejeu** («replay»). Une attaque par rejeu prend un paquet, copie le paquet et envoie le paquet à la destination ce qui pourrait confondre l'hôte ou apparaître comme un utilisateur légitime.

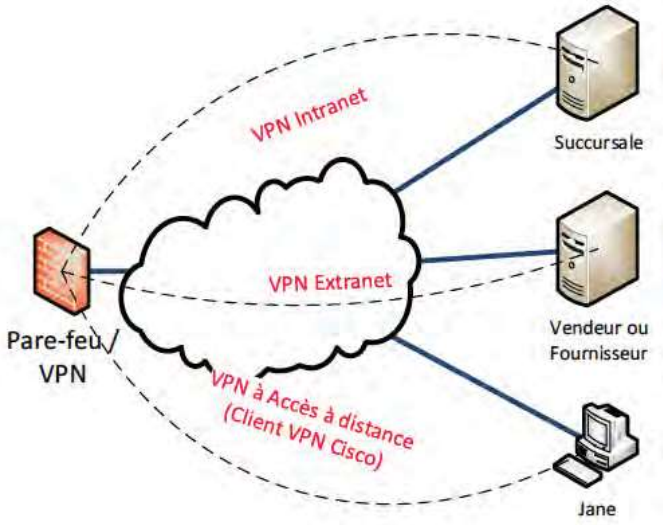
TYPES DE VPN ET UTILISATIONS TYPIQUES

TYPE DE VPN	UTILISATION TYPIQUE
Intranet	Utilisé pour connecter des sites distants appartenant à la même organisation
Extranet	Utilisé pour connecter des sites distants appartenant à différentes organisations
Accès à distance	Connecte les utilisateurs individuels à l'organisation d'attache via Internet



Envoi d'un paquet à travers un tunnel VPN de 10.200.12.3 au serveur 10.50.1.23:

1) L' hôte envoie les paquets de 10.200.12.3 à 10.50.1.23
2) Le routeur R1 crypte le paquet et ajoute un nouvel en-tête VPN. L'IP de destination 65.36.2.5 et l'IP source 34.5.2.3 sont ajoutés à un nouvel en-tête IP puis le paquet combiné est transmis.
3) Le pare-feu à 65.36.2.5 reçoit le paquet combiné, confirme l'authenticité du paquet, retire l'en-tête VPN et l'en-tête IP puis décrypte le paquet original de 10.200.12.3
4) Le pare-feu envoie le paquet d'origine vers le serveur 10.50.1.23



Comparaison entre différentes utilisations de VPN