1. Configuration de base

```
enable ( en )                       # Passe en mode privilégié
configure terminal ( conf t )       # Mode configuration globale
hostname SW1                        # Définit le nom du switch
enable secret MonMotDePasse         # Définit un mot de passe chiffré pour le mode privilégié
service password-encryption         # Chiffre tous les mots de passe en clair
banner motd                         # Affiche un message lors de la connexion
```

Ces commandes établissent les paramètres de base du switch, incluant le nom d'hôte, les mots de passe sécurisés et un message d'avertissement.

---

2. Configuration de l'interface de gestion

```
interface vlan1
        ip address 192.168.1.2 255.255.255.0    # Attribue une IP à l'interface VLAN 1
        no shutdown                             # Active l'interface
exit
ip default-gateway 192.168.1.1                  # Définit la passerelle par défaut
```

L'interface VLAN 1 est souvent utilisée pour la gestion du switch. Assurez-vous que l'interface est active et que la passerelle est correctement définie pour permettre l'accès à distance.

---

3. Gestion des interfaces

```
interface FastEthernet0/1
        description “Description”       # Ajoute une description à l'interface
        shutdown                        # Désactive l'interface
        no shutdown                     # Active l'interface
exit
default interface FastEthernet0/1       # Réinitialise l'interface à sa configuration par défaut
```

Ces commandes permettent de gérer l'état des interfaces, d'ajouter des descriptions utiles pour l'administration et de réinitialiser les interfaces si nécessaire.

---

4. VLANs

```
vlan 10
        name Clients                    # Crée le VLAN 10 nommé 'Clients'
exit
interface FastEthernet0/2
        switchport mode access          # Définit le port en mode accès
        switchport access vlan 10       # Associe le port au VLAN 10
```

La création de VLANs permet de segmenter le réseau pour une meilleure organisation et sécurité. Assurez-vous d'assigner les ports aux VLANs appropriés.

---

5. Trunking

```
interface GigabitEthernet0/1
  switchport trunk encapsulation dot1q      # Définit l'encapsulation 802.1Q
  switchport mode trunk                     # Définit le port en mode trunk
  switchport trunk allowed vlan 10,20       # Autorise les VLANs 10 et 20 sur le trunk
```

Les ports trunk permettent de transporter plusieurs VLANs entre les switches. Assurez-vous que les VLANs nécessaires sont autorisés sur le trunk.

---

6. Sécurité des ports

```
interface FastEthernet0/3
  switchport mode access                    # Définit le port en mode accès
  switchport port-security                  # Active la sécurité du port
  switchport port-security maximum 1        # Limite à une seule adresse MAC
  switchport port-security violation shutdown  # Désactive le port en cas de violation
  switchport port-security mac-address sticky  # Apprend automatiquement l'adresse MAC
```

La sécurité des ports empêche les accès non autorisés en limitant le nombre d'adresses MAC autorisées sur un port.

---

7. Spanning Tree Protocol (STP)

```
spanning-tree mode rapid-pvst          # Active le mode Rapid PVST+
interface FastEthernet0/4
   spanning-tree portfast              # Active PortFast pour accélérer la convergence
   spanning-tree bpduguard enable      # Désactive le port si des BPDUs sont reçus
```

Le STP prévient les boucles réseau. PortFast est utilisé sur les ports connectés à des hôtes pour accélérer la mise en service.

---

8. Protocole de découverte (CDP/LLDP)

```
cdp run                    # Active le Cisco Discovery Protocol
show cdp neighbors         # Affiche les voisins CDP
lldp run                   # Active le Link Layer Discovery Protocol
show lldp neighbors        # Affiche les voisins LLDP
```

CDP et LLDP permettent de découvrir les périphériques voisins sur le réseau, facilitant le dépannage et la documentation.

---

9. Configuration NTP

```
ntp server 192.168.1.100       # Définit le serveur NTP
ntp update-calendar            # Met à jour l'horloge matérielle avec NTP
```

La synchronisation de l'heure est essentielle pour la cohérence des logs et des événements réseau.

---

10. Commandes de vérification

```
show running-config            # Affiche la configuration en cours
show vlan brief                # Affiche les VLANs configurés
show interfaces status         # Affiche l'état des interfaces
show mac address-table         # Affiche la table des adresses MAC
show port-security             # Affiche l'état de la sécurité des ports
```

Ces commandes permettent de vérifier la configuration et l'état du switch pour le dépannage et la maintenance.

---

11. Sauvegarde de la configuration

```
copy running-config startup-config      # Sauvegarde la configuration en cours
copy startup-config tftp:               # Sauvegarde la configuration vers un serveur TFTP
```

Il est important de sauvegarder régulièrement la configuration pour éviter toute perte en cas de redémarrage ou de panne.

12. Listes de Contrôle d'Accès (ACL)

Les ACL permettent de filtrer le trafic réseau en autorisant ou en bloquant des paquets en fonction de critères définis. Elles sont essentielles pour renforcer la sécurité et contrôler l'accès aux ressources du réseau.

12.1 ACL Standard

Les ACL standard filtrent le trafic en se basant uniquement sur l'adresse IP source.

```
access-list 10 permit 192.168.1.0 0.0.0.255  # Autorise le trafic provenant du réseau 192.168.1.0/24
access-list 10 deny any                      # Bloque tout autre trafic
interface FastEthernet0/1
        ip access-group 10 in                # Applique l'ACL en entrée sur l'interface
```

Remarque : L'ACL standard est généralement appliquée près de la destination.

12.2 ACL Étendue

Les ACL étendues offrent un filtrage plus précis en considérant l'adresse IP source et destination, le protocole, et les ports.

```
access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 80  # Autorise le trafic HTTP depuis 192.168.1.0/24 vers n'importe quelle destination
access-list 100 deny ip any any                             # Bloque tout autre trafic
interface FastEthernet0/1
 ip access-group 100 in                                     # Applique l'ACL en entrée sur l'interface
```

Remarque : L'ACL étendue est généralement appliquée près de la source.

12.3 ACL Nominale

Les ACL nominales permettent une gestion plus flexible en utilisant des noms au lieu de numéros.

```
ip access-list extended WEB_ACCESS
 permit tcp 192.168.1.0 0.0.0.255 any eq 80
 deny ip any any
interface FastEthernet0/1
 ip access-group WEB_ACCESS in
```

Remarque : Les ACL nominales facilitent l'ajout, la suppression et la modification des règles.

13. Configuration SNMP (Simple Network Management Protocol)

SNMP permet la surveillance et la gestion à distance des équipements réseau via des outils comme PRTG, Zabbix ou SolarWinds.

13.1 Activer SNMP avec une communauté en lecture seule

```
snmp-server community public RO          # Crée une communauté SNMP nommée 'public' en lecture seule
```

Cette commande définit une communauté SNMP avec des droits de lecture seule, permettant aux outils de supervision de collecter des informations sans modifier la configuration du switch.

13.2 Définir l'emplacement et le contact

```
snmp-server location "Salle Serveurs R1"          # Spécifie l'emplacement physique du switch
snmp-server contact admin@example.com             # Indique l'adresse e-mail de l'administrateur responsable
```

Ces informations facilitent l'identification et la gestion des équipements dans les outils de supervision.

13.3 Configurer l'envoi de traps SNMP

```
snmp-server enable traps                                  # Active l'envoi de traps SNMP
snmp-server host 192.168.1.100 version 2c public          # Définit le serveur de supervision recevant les traps
```

Les traps SNMP sont des alertes envoyées par le switch pour signaler des événements importants (ex. : redémarrage, lien en panne).

13.4 Vérifier la configuration SNMP

```
show snmp                    # Affiche la configuration SNMP actuelle
```

Cette commande permet de vérifier les paramètres SNMP configurés sur le switch.

14. Sécurité des Ports (Port Security)

La sécurité des ports limite l'accès aux ports du switch en autorisant uniquement des adresses MAC spécifiques, renforçant ainsi la sécurité du réseau.

14.1 Activer la sécurité sur un port

```
interface FastEthernet0/1
 switchport mode access          # Définit le port en mode accès
 switchport port-security        # Active la sécurité du port
```

Ces commandes activent la sécurité sur le port spécifié, permettant de restreindre l'accès basé sur les adresses MAC.

14.2 Définir le nombre maximum d'adresses MAC autorisées

```
switchport port-security maximum 2          # Autorise jusqu'à 2 adresses MAC sur le port
```

Cette commande limite le nombre d'adresses MAC pouvant être apprises sur le port, empêchant ainsi les connexions non autorisées.

14.3 Configurer le mode de violation

```
switchport port-security violation restrict    # Bloque les paquets non autorisés et envoie une alerte
```

Le mode 'restrict' bloque le trafic non autorisé et génère une alerte sans désactiver le port.

14.4 Activer l'apprentissage des adresses MAC (Sticky)

```
switchport port-security mac-address sticky          # Apprend automatiquement les adresses MAC et les conserve
```

Cette commande permet au switch d'apprendre dynamiquement les adresses MAC et de les enregistrer dans la configuration en cours.

14.5 Vérifier la configuration de la sécurité des ports

```
show port-security interface FastEthernet0/1          # Affiche l'état de la sécurité sur le port spécifié
```

Cette commande fournit des informations sur la configuration de la sécurité des ports, y compris les adresses MAC sécurisées et les violations.