PPE 3.1 Sécurisation & Optimisation de l'Infrastructure du Stade

I-) Contexte

a) Presentation de stadium company

Stadium Company est une société qui s'occupe de la gestion des stades , qui souhaite moderniser l'infrastructure réseau de son stade , la rendre scalable au fur et à mesure que ses ambitions augmentent . Elle emploie 170 personnes à plein temps et 80 à temps partiels . Elle projette ajouter des fonctions haute technologie afin de pouvoir prendre en charge l'organisation des concerts . La direction de Stadium Company n'étant pas compétente en matière d'Infrastructure réseau décide de faire appel à une entreprise de consultants réseaux qui s'en occupera de la conception à la mise en oeuvre en passant par la gestion du projet . Il sera mis en oeuvre en trois phases à savoir :

- La planification du projet et la préparation de la conception réseau haut niveau
- Le développement de la conception reseau détaillée
- La mise en oeuvre de la conception

b) Presentation NetworkingCompany

Le prestataire désigné pour l'exécution de ce projet est la société Networking Company, une firme locale spécialisée dans la conception d'infrastructure réseau et le conseil . C'est une société Cisco Premier Partner qui emploie 20 ingénieurs réseaux certifiés et expérimentée dans ce secteur.

Dans le but de concevoir le nouveau plan de l'infrastructure de haut niveau , Networking Company a décrit un profil de l'organisation et des installations sur la base des études menées par ses experts notamment en interrogeant le personnel.

II-) Cahier des charges :

a-) Mission 1

Vous intégrez le service informatique du centre administratif de stade. Sur ce site sont effectuées toutes les opérations concernant la gestion du personnel, et l'administration du stade. On y trouve 7 grands services :
- Service Administration (170 personnes)
-Service Equipes (164 personnes)
- Service WiFi (100 personnes)
- Service Caméra IP (80 caméras)
- Service VIP-Presse (80 personnes)
- Service Fournisseurs (44 personnes)
- Service Restaurant (14 personnes)
- Le réseau de StadiumCompany doit comporter plusieurs périmètres de sécurité
- Adressage réseau et attribution de noms faciles à mettre à niveau : 172.20.0.0/22
- Un système de cloisonnement du réseau devra être testé. Les commutateurs devront être facilement administrables afin de propager les configurations rapidement et aisément
- Solution permettant l'interconnexion des différents sites (stade, billetterie et magasin)
- Les différents commutateurs ainsi que le routeur doivent disposer de réglages de base homogènes. La solution doit se faire avec les équipements réseau CISCO.

Solutions:

1- Comparaison et choix de solution
a-) adressage statique et dynamique
b-) administration et gestion de VLAN (VTP et GVRP)
c-) Vlan statique (axée sur le port niveau 1) et dynamique (axée sur l'adresse mac niveau 2 , ip niveau 3)
d-) Routage statique et dynamique (InterVlan)

IV-) Mise en oeuvre

a) Adressage statique (VLSM)
b) Administration et gestion des VLANs (VTP) + ports TRUNK
c) Creation des VLANs et attributions des ports VLANs
d) Routage statique et routage InterVlan
e) Schema de reseaux visio.

V-) **Conclusion**
VI-) **Annexes**
VII-) **Activites**

PS: routage statique = site distant r-stade =>r-billetterie / r-stade=>r-magasin souvenirs

SOLUTION & Comparaison

I- Adressage

La division en sous réseau permet de créer plusieurs sous-réseaux logiques existant sur un seul réseau de Classe A, B ou C . Sans la division en sous-réseaux , il ne peut être utilisé qu'un réseau du réseau de classe A , B ou C ce qui est peu réaliste.
Chaque liaison de données sur un réseau doit avoir un et un seul ID réseau , chaque noeud sur cette liaison étant un membre du même réseau . La décomposition d'un réseau majeur (classe A,B ou C) en sous-réseaux plus petits , permet de créer un réseau de sous-réseaux d'interconnexion . Alors chaque liaison de données sur ce réseau aurait alors un seul ID réseau/sous-réseau . Ainsi tout périphériques , ou toute passerelle , qui se connecte a n réseaux / sous-réseau on a n adresses IP distinctes , une pour chaque réseau/sous-réseau d'interconnexion.

Avantage de la technique VLSM :

- Utilisation efficace de l'espace d'adressage
- Utilisation de plusieurs longueurs de masque de sous-réseau
- Division d'un bloc d'adresses en blocs plus petits
- Prise en charge des résumés du routage
- Plus grande souplesse de conception de réseau
- Prise en charge des réseaux d'entreprises hiérarchiques.

II- VTP - GVRP

II-1 - GVRP

Le protocole **GVRP** est directement incluse dans la norme 802.1P . Il facilite la diffusion des informations sur les VLANs declarer sur les ports d'un **switch** . Il permet de configurer dynamiquement les VLANs déclarés sur les **switch** et de mettre à jour la table d'association des VLANs .
Pour une diffusion efficace l'ensemble des switchs composants le réseau doivent avoir un agent GVRP active .
L'utilisation de ce protocole requiert quelques éléments :

- L'agent **GVRP Participant** qui gère les ports physiques de chaque switch. Il stocker des informations sur les **VLANs** déclarer pour les ports du switch
- La **BPDU GIP** (**GARP Information Propagation**) qui définit les messages diffusés entre les ports en interne au switch
- La **BPDU GIP** (**GARP Information Déclaration**) qui définit les messages diffusés entre les agents de deux switchs distincts.

Fonctionnement du GVRP

- Enregistrement statique d'un VLAN sur un port

- Transmission aux autres ports par GIP (GVRP Participant)
- Transmission aux autres commutateurs par GID
- Association du port avec avec les VLANs contenu dans le GID
- Répétition du processus avec transmission en GIP

II-2 - VTP

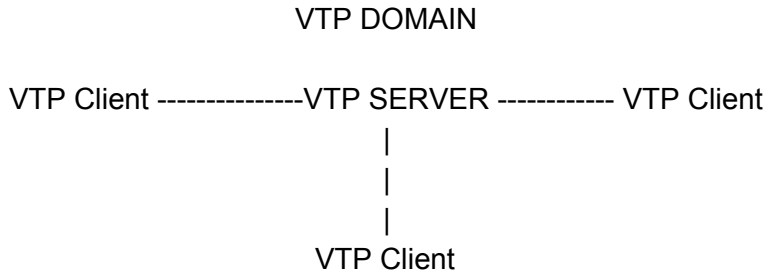
VTP (VLAN Trunking protocol)

Le VTP permet de diffuser la déclaration des **VLANs** pour les ports trunk sur l'ensemble du réseau en réalisant une administration centralisée de ceux ci . Il est propriétaire **CISCO**. Il fonctionne avec une architecture client serveur.

Fonctionnement VTP :

Le serveur tient à jour une table de VLANs déclarés . Cette table est diffusée à l'ensemble des clients sur le même domaine VTP . Ainsi chaque modification de la table se répercute sur l'ensemble des clients . Du coup tous les VLANs définis sur le serveur pourront transiter par l'ensemble des ports trunk des switchs clients (sauf configuration contraire des interfaces).
Les matériels peuvent être en mode :

- Server : Il est associee a un domaine VTP . La déclaration des VLANs s'effectue sur le serveur qui tient à jour la liste des VLANs déclarés et la diffuse à l'ensemble des clients .
- Client : Il est associee a un domaine VTP . Il reçoit la liste des VLANs , il la propage aux autres clients auxquels il est connecté et met à jour sa propre liste
- Transparent : il n'est associée à aucun domaine VTP . Sa liste de VLAN est locale et n'est pas mis à jour lorsqu'il reçoit une trame VTP . Cependant il propage les listes de VLAN qu'il reçoit .



II-3 - VLAN

Un VLAN (Virtual Local Area Network) est un réseau local regroupant un ensemble de machines de façon logique et non physique.
Il peut coexister de nombreux VLANs sur un même switch . Dans un réseau local la communication entre les différentes machines est régie par l'architecture physique
Il existe trois types de VLAN :

- VLAN (niveau 1): qui définit un réseau en fonction des port de raccordement sur le commutateur
- VLAN (niveau 2): qui définit un réseau virtuel en fonction des adresses MAC . Il est beaucoup plus souple que le VLAN de niveau 1 car il est indépendant de la localisation de la station .
- VLAN (niveau 3): même principe que celui du VLAN de niveau 2 a l'exception que l'on indique les adresses IP (ou une plage d'IP) qui appartiendront à tel ou tel VLAN

Interets des VLANs :

- Gestion du réseau amélioré ,
- Amélioration de la bande passante
- Separation des flux
- Plus de sécurité : permet de créer un ensemble logique isolé pour ameliorer la securite
- Le seul moyen pour communiquer entre des machines appartenant à des VLAN différents est alors de passer par un routeur.

III- Trunking

Un trunk est le lien entre deux équipements , le plus souvent entre deux switchs , configuré de manière a y faire circuler des trames Ethernet modifiées contenant des informations relatives au VLAN sur lequel elles transitent. Plus précisément c'est la configuration d'une encapsulation des trames lorsqu'elles transitent sur le lien de sorte que le switch qui la reçoit peut ensuite la relayer dans le bon VLAN.
L'encapsulation fait appel à des protocoles . Chez CISCO il en existe deux pour l'encapsulation des données sur un trunk :

- ISL (Inter Switch Link) : c'est le protocole propriétaire CISCO tendant à disparaître , qui encapsule toute les trames quelque soit le VLAN
- dot1Q (IEEE 802.1Q) c'est le protocole standard defini par l'IEEE . On utilisera dot1Q dans notre cas. Il insère un **tag** (étiquette) dans l'entête de la trame **ethernet** et uniquement sur les VLANs autres que le VLAN natif. (VLAN natif : est celui utilisé par les protocoles comme CDP par exemple pour s'échanger les informations)

IV- Routage

Il existe 3 types de routage :

- **Routage statique :**
  Ajouter une route manuellement dans la table de routage par l'administrateur :
  Réseaux de destination → masque → prochain saut

- **Routage dynamique:**
  Il existe deux types de routage dynamique , l'ajout de routes se fait automatiquement .

  - **Vecteur de distance** : algorithme **RIPv1** (broadcast) et **RIPv2** (multicast) (224.0.0.9)
    RIPv1 est considere comme un protocole **IGP** par classes (classful).
    Un protocole à vecteur de distance qui diffuse intégralement sa table de routage à chaque routeur voisin , à intervalles prédéfinis . L'intervalle par défaut est de 30s . RIP utilise le nombre de sauts comme métrique , avec une limite de 15 sauts maximum.
    Capacité à gérer l'équilibrage de charge sur au plus six chemins de coût égal , avec quatre chemins par défaut .
    Si le routeur reçoit des informations concernant un réseau et que l'interface de réception appartient au même réseau mais se trouve sur un sous réseau différent , le routeur applique le masque de sous réseau configuré sur l'interface de réception.
    RIPv1 comporte des limitations suivantes :
    - Il n'envoie pas d'informations sur les masques de sous-réseau dans ses mises à jour
    - Il envoie des mises à jour sous forme de broadcasts sur 255.255.255.255
    - Il ne prend pas l'authentification en charge
    - Il ne prend en charge ni VLSM , ni le routage CIDR (Classless Interdomain Routing)

RIPv2 présente une fonctionnalité de routage CIDR lui permettant d'envoyer des informations sur les masques des sous réseaux avec la mise à jour des routes . RIPv2 permet l'authentification dans ses mises a jour . Il est possible d'utiliser une permet de choisir le type d'authentification à utiliser dans les paquets RIPv2 . Il peut s'agir de texte en clair ou d'un cryptage basé sur l'algorithme d'authentification MD5. Le type d'authentification par défaut est le texte en clair. L'algorithme . Pour une meilleure efficacité , RIPv2 utilise l'adresse de classe D 224.0.0.9 pour envoyer les mises à jour de routage en multicast.

- **Etats de liens : algorithme OSPF**
  Le protocole **OSPF** est un protocole de routage à état de lien . Il a le même objectif que les algorithmes à vecteur distance :
  Obtenir une table de routage avec les meilleures routes
  Converger au plus vite vers une table de routage optimale
  Attention : les sens de meilleur et optimal dépendant de la métrique .

Le déroulement complet d'**OSPF** est le suivant :

- Chaque routeur découvre son voisinage et conserve une liste de tous les voisins
- Utilise un protocole fiable pour échanger les informations topologiques avec ses voisins
- Stocke les informations posologiques apprises dans leur base de données
- Exécute l'algorithme **OSPF** pour calculer les meilleures routes
- Place ensuite la meilleure route vers chaque sous-réseau dans sa table de routage

Chaque routeur possède :

- Une table de ses voisins , appele Neighbour Table
- Une base de données de la topologie du réseau , appelee Topology database
- Une table de routage, appelee routing table

Avantage d'un protocole à vecteur distance :

- Un routeur connaît ses voisins uniquement lors de la transmission de mise à jour de leur part
- Lors d'un envoi d'une mise à jour à un voisin , ce voisin ne retourne aucune confirmation de l'expéditeur .

Avantage d'un protocole à l'état de lien :

- Beaucoup d'informations sont transmises et nécessitent beaucoup de ressources
- Chaque routeur doit connaître ses voisins avant d'échanger des informations

c) Le routage hybride : **EIGRP** (224.0.0.10)

Basée sur l'algorithme Dual

AS : Autonomous System : domaine de routage

Un protocole de routage dynamique est dit être hybride quand celui-ci possede a la fois des fonctionnalités d'algorithmes de routage à vecteur distance et d'algorithmes de routage à états de liens .

EIGRP est une version avancee d'IGRP
Converge plus vite qu'IGRP

EIGRP envoie d’abord toutes ses informations de routage a un voisin et ensuite seulement des mises à jour
IGRP envoie régulièrement (toutes les 90s) la totalité de sa table de routage .
EIGRP fonctionne avec **Novell IPX** et **Apple AppleTalk** en plus d’**IP** , contrairement a IGRP

Choix de solutions

A- **Adressage :**
Pour profiter du découpage en sous réseaux logiques nous adoptons le découpage en différents VLANs ainsi l'administration et la sécurité seront les meilleurs.

B- **VTP - GVRP**
Pour une sécurité infaillible en cas de défaillance d'un des deux switchs nous optons pour le déploiement du mode VTP

C- **Routage**
On mettra en place un routage statique pour l'interconnexion des points distants , interVLAN .
Et on mettra le routage hybride (EIGRP) du fait de la petite structure reseau

A -) **Adressage + VLSM**

Reseau Principal : 172.20.0.0/22 [172.20.0.1 - 172.20.3.254] Broadcast : 172.20.3.255

Services	VLAN	Nombres de machine	Adresse reseau	1ere adresse	Derniere adresse	broadcast
Administration	VLAN10	254	172.20.0.0/24	172.20.0.1	172.20.0.254	172.20.0.255
Equipes	VLAN11	254	172.20.1.0/24	172.20.1.1	172.20.1.254	172.20.1.255
Wifi-stade	VLAN12	126	172.20.2.0/25	172.20.2.1	172.20.2.126	172.20.2.127
Camera IP	VLAN13	126	172.20.2.128/25	172.20.2.129	172.20.2.254	172.20.2.255
VIP-Presse	VLAN 14	126	172.20.3.0/25	172.20.3.1	172.20.3.126	172.20.3.127
Fournisseurs	VLAN15	62	172.20.3.128/26	172.20.3.129	172.20.3.191	172.20.3.192
Restaurant	VLAN16	14	172.20.3.192/28	172.20.3.193	172.20.3.206	172.20.3.207

Reseau Libre : 172.20.3.224 [172.20.3.225 - 172.20.3.254]

b) **VTP - GVRP**

VTP Server :

switch(config)# hostname Com1-srv
Com1-srv (config)#VTP mode server
VTP domain stadiumcompany.com
VTP version 2
exit

```
com1-srv#show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : stadiumcompany.com
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x74 0xF5 0x9F 0x4A 0xC5 0x10 0x7E 0x48
Configuration last modified by 0.0.0.0 at 3-1-93 00:05:16
Local updater ID is 0.0.0.0 (no valid interface found)
```

Trunk

Com1-srv(config)# interface range fa 0/22 - 24
switchport mode trunk
no shutdown
exit

VTP Client :

switch(config)#hostname com2-client
com2-client(config)# VTP mode client
#vtp domain stadiumcompany.com
vtp version 2
exit

```
com2-client#sh vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : stadiumcompany.com
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x03 0x39 0x96 0xD6 0x9C 0x4D 0xCF 0xD5
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Trunk

com2-client(config)# interface range fa 0/22 - 24
switchport mode trunk
no shutdown
exit

c-) **VLANs et Attributions de ports**

com1-srv(config) #vlan10
#name Administration
#exit
Com1-srv(config)#interface range fa 0/1 - 6
#switchport access vlan 10
no shutdown
exit

```
com1-srv(config) #vlan11
                  #name Equipes
                  #exit
Com1-srv(config)#interface range fa 0/7 - 12
                  #switchport access vlan 11
                  #no shutdown
                  # exit

com1-srv(config)#vlan12
                 #name Wifi-stade
                 #exit

com1-srv(config)#vlan13
                 #name CameraIP
                 #exit
Com1-srv(config)#interface range fa 0/13 -14
                  #switchport access vlan 12
                  #no shut down
                  #exit


com1-srv(config)#vlan14
                 #name VIP-Presse
                 #exit
com1-srv(config)#vlan15
                #name Fournisseurs
                #exit
com1-srv(config)#vlan16
                 #name Restaurant
                 #exit
```

```
com1-srv#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   administration                    active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6
11   equipes                           active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12
12   wifi-stade                        active    Fa0/13, Fa0/14
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
11   enet  100011     1500  -      -      -        -    -        0      0
12   enet  100012     1500  -      -      -        -    -        0      0
 --More-- |
```

Commutateur client

```
Com2-client(config)#interface range fa 0/1 - 6
                    #switchport access vlan 10
                    # no shutdown
                    # exit

Com2-client(config)#interface range fa 0/7 - 12
                    #switchport access vlan 11
                    #no shutdown
                    # exit

Com2-client(config)#interface range fa 0/13 -14
                    #switchport access vlan 12
                    #no shut down
                    #exit
```

d) **Routage Inter-Vlan**

```
router(config) # hostname r-stade

R-stade (config)# interface fa 0/0
                  #  no shutdown
                  # exit

R-stade (config)# interface fa0/0 10
                  # description vlan10
                  # encapsulation dot1Q 10
                  # ip address 172.20.0.1  255.255.255.0
                  # no shutdown
                  # exit

R-stade (config)#interface fa 0/0 11
                   # description vlan 11
                   # encapsulation dot1Q 11
                   # ip address 172.20.1.1  255.255.255.0
                   # no shutdown
                   #exit
R-stade (config)#interface fa0/0 12
                  # description vlan12
                  # encapsulation dot1Q 12
                  # ip address 172.20.2.1 255.255.255.128
                  # no shutdown
                  # exit
R-stade(config) # interface fa0/1
```

ip address 200.200.200.1 255.255.255.252
no shutdown
exit

Routage statique :

R-stade (config)# IP route 192.168.1.0 255.255.255.0 200.200.200.2

```
r-stade>
r-stade>en
r-stade#sh ip int brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  up                    up
FastEthernet0/0.10     172.20.0.1      YES manual up                    up
FastEthernet0/0.11     172.20.1.1      YES manual up                    up
FastEthernet0/0.12     172.20.2.1      YES manual up                    up
FastEthernet0/1        200.200.200.1   YES manual up                    down
Vlan1                  unassigned      YES unset  administratively down down
r-stade#
```

---

router(config)#hostname billeterie
R-billeterie(config)#interface fa 0/1
IP address 200.200.200.2 255.255.255.252
no shutdown
#exit

R-billeterie (config)# interface fa 0/0
IP address 192.168.1.1 255.255.255.0
no shutdown
exit

R-billeterie(config)# ip route 172.20.0.0 255.255.252.0 200.200.200.2

```
r-billeterie>
r-billeterie>en
r-billeterie#sh ip int brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        198.162.1.1     YES manual up                    up
FastEthernet0/1        200.200.200.2   YES manual up                    down
Vlan1                  unassigned      YES unset  administratively down down
r-billeterie#
```

R-stade(config)# Router RIP
version 2
network 172.20.0.0
network 172.20.1.0
network 172.20.2.0
network 200.200.200.0
network 200.200.200.4
R-billeterie(config)# Router RIP
version 2
network 192.168.1.0
network 200.200.200.0

R-stade(config)# router EIGRP 100
#network 172.20.0.0 0.0.0.255
#network 172.20.1.0 0.0.0.255
#network 172.20.2.0 0.0.0.127
#network 200.200.200.0 0.0.0.3
#network 200.200.200.4

R-billeterie(config)# router EIGRP 100
#network 192.168.1.0 0.0.0.255
#network 200.200.200.0 0.0.0.3
#exit

R-stade(config)#Router OSPF 100
#network 172.20.0.0
#network 172.20.1.0
#network 172.20.2.0
#network 200.200.200.0
#network 200.200.200.4
R-billeterie(config)# Router OSPF 100
#network 192.168.1.0
#network 200.200.200.0

Pour les routeurs sans accès internet direct par défaut :
ip route 0.0.0.0 | 0.0.0.0

e-) **Trunking**

Com1-srv(config)#interface range fastethernet 0/19-20
Com1-srv(config)#switchport mode trunk

Com2-client(config)#interface range fastethernet 0/19-20
Com2-client(config)#switchport mode trunk

Conclusion :
L’interconnexion des équipements a été bien effectuée ainsi la sécurisation et la base du réseau sont en place. Il a ete mis en place l’usage du VTP , du routage InterVLAN , le decoupage en VLAN

Les activites

A1.1.1 Analyse du cahier des charges d’un service à produire
A1.1.2 Etude de l’impact de l'intégration d’un service sur le système informatique
A1.2.1 Élaboration et présentation d’un dossier de choix de solution technique
A1.2.4 Determination des tests necessaires a la validation d’un service
A1.2.5 Définition des niveaux d’habilitation associés à un service
A1.3.1 Test d'intégration et d’acceptation d’un service
A1.4.1 Participation a un projet
A2.3.2 Proposition d'amélioration d’un service
A3.1.1 Proposition d’une solution d’infrastructure
A3.1.2 Maquettage et prototypage d’une solution d’infrastructure
A3.2.1 Installation et configuration d'éléments d’infrastructure
A3.3.1 Administration sur site ou à distance des éléments d’un réseau , de serveurs , de services et d'équipements terminaux
A4.1.9 Rédaction d’une documentation technique .