TP2 LAN

Consignes

Répartissez-vous en :
- 6 groupes de 3 postes de travail
- 2 groupes de 2 postes au niveau des baies bleues et rouges

Les groupes de 2 postes utiliseront une interface ethernet de l'un des postes pour simuler le 3ème poste. La commande *ping* sera alors utilisée avec l'option -I et les requête ICMP seront toujours envoyée de (et non vers) cette interface.

1 Commutation

Avant toute manipulation, désactivez le protocole spanning-tree (qui sera traité plus loin) sur les switches que vous utiliserez :
Switch(config)#no spanning-tree vlan 1

1) Connectez 3 postes A, B et C à un même commutateur. Consultez la table de commutation (*show mac-address-table*) et vérifiez qu'elle s'est dynamiquement alimentée.
Envoyez en continu des requêtes d'écho ICMP de A vers B.
Lancez une capture de trame sur C avec *wireshark*.
Changez rapidement le port sur lequel est connecté B tout en affichant la table d'acheminement du switch.
Analysez la capture de trames. Que s'est-t-il passé ?

2) Configurez une entrée statique dans le cache ARP de A, faisant correspondre une adresse MAC quelconque (par exemple 12:34:56:78:9A:BC) à une adresse IP non utilisée du même réseau que A.
Lancez une capture de trames sur tous les postes et envoyez une requête d'écho ICMP vers cette adresse, depuis A.
Analysez les capture et déduisez-en le comportement d'un commutateur lorsqu'il reçoit une trame destinée à une adresse inconnue.

3) Configurez le switch de manière à ce que la durée de rétention des entrées de la table de commutation soit minimale (10s au lieu de 5min par défaut).
Arrêtez l'émission des pings, patientez 10s et vérifiez que la table d'adresses MAC est vide.
Relancez la capture sur C et le ping de A vers B.
Analysez la capture de trames. Que s'est-t-il passé ?
Pourquoi ce phénomène ne se reproduit-il pas toutes les 10s ?
Quel problème peut poser une définition trop courte de cette durée ?
A l'inverse, imaginez les problèmes que peuvent poser un temps de rétention trop long.

4) Changez l'adresse MAC de C pour qu'elle soit identique à celle de B.
Lancez des échanges de pings entre A et B et entre A et C. Affichez la table de commutation (aussi appelée table CAM, pour Content Addressable Memory).
Tentez également de définir 2 entrées statiques pour cette adresse MAC.
Que constatez-vous ?

Reconfigurez l'ancienne adresse MAC de C.

5) Connectez B à un 2ème switch et interconnectez les 2 switches.
Lancez des pings entre A et B et entre B et C.
Affichez les tables de commutation des deux switches.
Que constatez-vous au niveau du port de 2ème switch connecté au 1er ?
Reconnectez de nouveau les postes sur le même switch.

2 Sécurisation des ports

Imaginez ce qui peut se produire si un poste envoie en permanence des trames dont l'adresse MAC source est à chaque fois différente.

1) Pour parer ce type de problème, il existe des mécanismes de sécurité.
Utilisez les options des commandes « mac-address-table », « port security » et/ou « switchport port-security » pour limiter à 2 le nombre maximum d'adresses MAC associées au port relié à B.
Lancez un ping sur A et affichez la table d'acheminement.
Aidez-vous des commandes « show port security » et « debug mac-address-table » pour les questions qui suivent.
Connectez A sur un autre port et tentez de le pinguer. Que se passe-t-il ?
Connectez B au port sécurisé et tentez de le pinguer. Que se passe-t-il ?
Reconnectez B sur son ancien port.
Connectez C au port sécurisé et tentez de le pinguer. Que se passe-t-il ?
Si vous disposez d'un switch 2950 et 2960, essayez également le mode *sticky* (collant).

2) Utilisez la commande *ifconfig* pour remplacer l'adresse MAC de C par celle de B. Tentez de nouveau de pinguer C. Qu'en déduisez-vous quant à la capacité de cette technique à sélectionner les postes autorisés à se connecter au réseau ?
Comparez avec les groupes voisins le comportement des switches selon qu'ils sont plus anciens (comme les 3500xl) ou plus récents (2560).

3) Connectez A et B sur un switch (S1), C sur un autre switch (S2), et inter-connectez les deux switches.
Sécurisez le port de S2 connecté à S1 et fixez le nombre maximum d'adresses MAC à 1.
Lancez un ping de C vers A.
Lancez un ping de B vers A. Que constatez-vous ?
Lancez de nouveau un ping de C vers A. Que constatez-vous ?

4)Faites en sorte que, en cas de violation de la sécurité (dépassement du quota d'adresses ou déplacement d'une adresse sur un autre port) les machines autorisées au préalable ne se voient pas bloquées.

5) Comment sécuriser une série (*range*) de ports sans relancer les commandes pour chaque port individuellement (uniquement sur switches 2550 ou supérieur).

3 Boucles de commutation

1) Connectez un poste A au switch S1.
Connectez le switch S1 au switch S2 par deux câbles.

Sur le poste A, lancez une capture de trames et envoyez une unique requête d'écho ICMP (option -c de ping) en diffusion générale.
Quel phénomène constatez-vous ? Quelle en est la cause.
Tentez de lancer une commande sur le terminal virtuel de configuration de l'un des switches.

2) Déconnectez et reconnectez l'une des interfaces de la boucle. Sur A, ajoutez au cache ARP une entrée statique pour une adresse IP inutilisée du même réseau que A et une adresse MAC unicast fictive. Lancez une capture de trames et envoyez une unique requête d'écho ICMP vers cette adresse. Que constatez-vous ?
Hormis le broadcast, quels autres types de trafic peuvent, selon vous, conduire à des boucles de commutation ?

3) Déconnectez l'une des interfaces, arrêtez la capture et affichez les statistiques pour noter le nombre de paquets/s capturés.
Configurez la fonctionnalité de contrôle de tempête (*storm control*) de manière à limiter le trafic de broadcast à 10 paquets/s.
Appliquez le filtre sur l'une des 4 interfaces impliquées dans la boucle suffit-il pour l'interrompre totalement ? Pourquoi ? Pour répondre, consultez la table de commutation.
Quelles sont, au minimum, les interfaces à filtrer pour interrompre la tempête ?

4) Quel problème peut poser le *storm control* sur un réseau de production ?

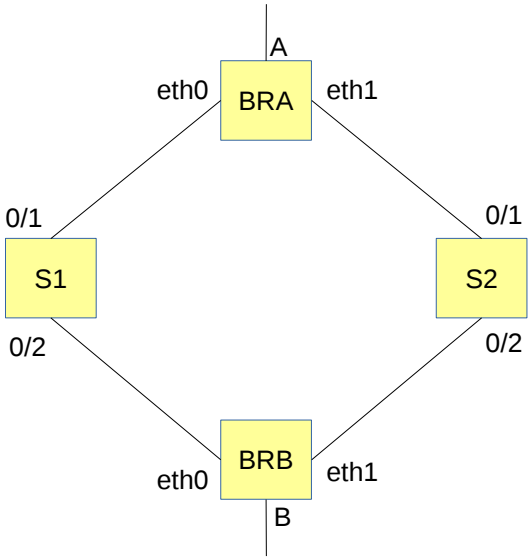
Désactivez les filtres et connectez les 2 switches par un unique lien.

4 Bridge Linux

Il sera utile par la suite de transformer un poste de travail en un commutateur (ou un pont, c'est-à-dire un commutateur à 2 ports).
Utilisez la commande *brctl* sur A pour :
- créer un bridge
- associer les interfaces ethernet de votre poste à ce bridge

Attribuez une adresse IP à l'interface A (qui est une interface virtuelle connectée au pont).
Connectez B et C sur A (attention au type de câble...) et vérifiez que A, B et C peuvent communiquer entre eux.
Déconnectez B et C et connectez S1 et S2 à A.

Transformez également B en pont et connectez-le à S1 et S2, comme sur la figure qui suit.



5 Arbre recouvrant

Il existe un moyen de résoudre intelligemment le problème de la tempête de diffusion (*broadcast storm*).

Si ce n'est pas déjà fait (*show spanning-tree*), désactivez STP sur S1 et S2 par la commande :
`Switch(config)#no spanning-tree`

Activez le mode debug sur S1 et S2 en lançant la commande :
`Switch#debug spantree events`

Lancez une capture de trames sur les interfaces eth0 et eth1 de A et B.
Lancez un ping en diffusion générale depuis A. Que constatez-vous ?
Déconnectez puis reconnectez l'une des interfaces de la boucle.

1) Activez STP sur A (*man brctl*). Analysez les captures de trames et affichez le résultat de la commande *brctl showstp A*. Envoyez de nouveau un ping en broadcast.
Que constatez-vous ? Pourquoi ?

2) Déconnectez le lien entre S1 et B. Observez pendant une vingtaine de secondes. Que se passe-t-il au niveau de A ? Pour quelle raison ?

3) Activez maintenant STP sur B, S1 et S2, captures actives, en lançant la commande suivante sur S1 et S2 :
`Switch(config)#spanning-tree`

Et la commande suivante sur C :
`brctl stp on`

Laissez tourner la capture un peu plus d'1 min avant de l'arrêter.

4) Les trames capturées sont appelées BPDU (*Bridge Protocol Data Unit*).
Les BPDU envoyées par un pont sont-elles reçues par le pont opposé du schéma ?

5) Comparez les BPDU envoyées par A, B, S1 et S2. Comment évolue le contenu des BPDU avec le temps ?

Quelle valeur permet aux switches d'élire le pont racine (*root bridge*) ?

Le bit de poids faible du 1er octet de l'adresse de destination des trames est à 1, ce qui signifie qu'il s'agit d'une adresse MAC de multicast. Les switches transmettent ce type de trames de la même manière que les trames de broadcast.

6) Sur S1 et S2, affichez le résultat de la commande *show spanning-tree brief*.
Quel est le nouveau pont racine ? Pourquoi et comment a-t-il été élu ?
Tentez à nouveau un ping en broadcast. A quel niveau la boucle a-t-elle été interrompue ? Pourquoi à ce niveau et pas ailleurs ?
Sur chaque pont non-racine, un et un seul port racine est choisit. Lequel et pourquoi ?
Sur chaque lien, un et un seul port désigné est choisit. Lequel et pourquoi ?

7) Quel problème peut poser la sélection automatique du pont racine ?
Faites en sorte que le nouveau pont racine soit de nouveau A.

8) Changez la vitesse du lien entre A et S1 pour que la bande passante soit de 10Mbit/s. Comment évolue le coût du chemin vers la racine (*root path cost*) des BPDU émis par A sur ce lien ? Quel chemin empruntent les données envoyées de B vers A (ping) ?
Pour forcer les données à prendre un chemin plutôt qu'un autre, inutile de changer la vitesse des liens. Remettez la vitesse du lien A-S1 sur auto et changer le coût associé à ce lien avec la commande *brctl*.

9) Désactivez les ports 1 et 2 de S2 (commande *shutdown*) pour simuler une panne de ce commutateur. B ne reçoit plus de BPDU de S2. Au bout de combien de temps et comment B réagit-il à la panne de S2 ? Par quels états successifs passent l'interface eth0 de B ? Quel chemin empruntent désormais les données envoyées de B vers A (ping) ?

Réactivez les ports 1 et 2 de S2 (commande *no shutdown*).

10) Quel est l'intérêt et/ou l'inconvénient d'activer STP sur les liens connectés à des postes de travail ?

11) Pour conclure sur STP, quels sont les 2 gros avantages qu'offre STP en bloquant automatiquement les boucles ?

6 Isolation des échanges

1) Connectez A au port 1, B au port 2 et C au port 3.
Appliquez la commande « port protected » ou « switchport protected » aux ports 1 et 2.
Envoyez une requête d'écho ICMP de A vers B, puis de A vers C. Que constatez-vous ?
Lancez une requête d'écho ICMP en diffusion générale (broadcast) à partir de A. Que constatez-vous ?
Quel est l'intérêt des ports « protégés » ?

2) Connectez maintenant B sur le port 2 d'un autre switch, « protégez » ce port et pinguez de nouveau B depuis A. Que constatez-vous ?

7 VLAN

A et B sont les postes de simples employés qui doivent être isolés des postes C et D, ceux du grand chef et de sa secrétaire.
A est connecté au port 1, B au port 2, C au port 3 et D au port 4.
Tous les postes ont des adresses du réseau 192.168.5.0/24

1) Utilisez la commande *switchport access* pour associer A et B au VLAN 2 et C et D au VLAN 3. Nommez le VLAN2 « atelier » et le VLAN3 « direction ».
Qui reçoit un ping en diffusion générale émis par A ?
Qui reçoit un ping en diffusion générale émis par C ?

2) Affichez la table de commutation. Quel est l'intérêt d'associer les entrées de cette table à des numéros de VLAN ?

3) Les bureaux de l'entreprise sont répartis de manière à ce que :
- A et C sont reliés sur les ports 1 et 2 du switch S1
- B et D sont reliés sur les ports 1 et 2 du switch S2

Proposez et mettez en place une solution basique (avec 2 câbles) pour que les employés puissent communiquer ensemble, et le patron avec sa secrétaire.

8 Trunk

1) Les deux switches de l'entreprise se trouvent dans deux bâtiments différents et sont reliés par un unique lien fibre optique. De plus, le service compta, le service commercial, le service après-vente, etc. souhaiteront eux aussi, par la suite, être dans leur propre réseau isolé.
Configurez un *trunk* entre les deux switches avec la commande *switchport mode*.

2) Intercalez un hub (concentrateur) entre S1 et S2 et connectez une sonde sur ce hub, c'est-à-dire un poste sur lequel vous lancez une capture de trames en mode *promiscuous*.
Echangez des messages ICMP entre A et B et entre C et D. Comparez les paquets capturés sur le trunk et les paquets envoyés ou reçus par les postes. Déduisez-en la manière dont les switches différencient les trames du VLAN 2 et les trames du VLAN 3 qui circulent sur le trunk.

3) Quelle est la taille du champ identifiant de VLAN ? Déduisez-en le nombre maximum de VLAN configurables sur un réseau.

4) Le protocole ISL est un protocole désuet et propriétaire Cisco. Remplacez le protocole ISL (utilisé par défaut sur le trunk des switches les moins récents) par le standard actuel (IEEE 802.1Q) en utilisant la commande *switchport trunk*.
Que se passe-t-il si les protocoles configurés aux extrêmités du trunk sont différents ?

5) Utilisez la commande *switchport trunk* pour indiquer aux switches S1 et S2 que le VLAN 2 est le VLAN *natif*. Capturez de nouveau quelques échanges entre A et B. Que constatez-vous ?
Lancez des pings en broadcast. Les VLAN 1 et 2 sont-ils toujours isolés l'un de l'autre ?
Peut-on en avoir plusieurs sur le même trunk ?
Le VLAN natif est utilisé par certains protocoles de signalisation, comme CDP (Cisco Discovery Protocol) ou DTP (Dynamic Trunking Protocol).

6) Le bureau de la secrétaire a changé de bâtiment. Déconnectez D de S2 et remettez le port 2 de S2 dans le VLAN par défaut (le VLAN 1).
Depuis C, lancez un ping en diffusion générale après avoir lancé une capture sur la sonde.
Que constatez-vous ? Le trunk transmet-il les trames transmises sur le VLAN 3 ? Pourquoi ?

7) Les switches récents (2550 et 2560) offrent la possibilité de négocier avec l'équipement distant le mode dans lequel se trouve un port (*trunk* ou *access*). Cette possibilité repose sur le protocole DTP (Dynamic Trunking Protocol), activé avec la commande *switchport mode dynamic*. Quel est l'intérêt de ce protocole ?
En matière de de sécurité informatique, et quelles que soient les circonstances, on ne peut pas faire confiance aux postes de travail des utilisateurs. Dans ces conditions, quel problème peut poser le protocole DTP ?

9 Surveillance de port

Les commutateurs Cisco offrent une fonctionnalité appelée Switch Port Analyzer (SPAN).
Utilisez la commande *port monitor* ou *monitor session* pour recopier tout le trafic circulant sur le trunk vers un port sur lequel vous connecterez votre sonde.

Le SPAN rend ainsi le hub inutile.

10 VTP

VTP (VLAN Trunking Protocol) est un protocole propriétaire Cisco qui permet de faciliter l'administration des VLAN.

1) Configurez S1 en mode serveur et S2 en mode client.
Affichez la liste des VLAN sur S1 et de nouveau, depuis D, lancez un ping en diffusion générale après avoir lancé une capture sur la sonde.
Que constatez-vous ? Le trunk transmet-il les trames envoyées sur le VLAN3 ? Pourquoi ?
Que transportent les paquets VTP ?
Tentez de créer un VLAN sur S2. Que se passe-t-il ? Est-ce normal ?

2) Ajoutez un VLAN sur S1 et observez la modification du numéro de séquence des annonces VTP.
Mettez maintenant S2 en mode *server* et ajoutez un autre VLAN. Que se passe-t-il ?
Réfléchissez au problème de sécurité que pose ce protocole.

3) Faites en sorte que seuls les VLAN utilisés sur S1 soit transmis à ce switch par VTP.

4) Quel problème pose le fait que VTP soit un protocole propriétaire ?

Lorsque VTP est actif (mode *client* ou *server*), seuls les VLAN 1 à 1005 peuvent être utilisés.
La base de données des VLAN se trouve dans le fichier flash:vlan.dat

11 Routage inter-vlan

Utilisez un routeur pour réaliser le routage entre les VLAN 2 et 3.
Pour cela, connectez un lien trunk entre l'un des deux switches et le routeur, et sur le routeur,

configurez des interfaces virtuelles associées aux VLAN.

Les trames 802.1Q peuvent-elles passer « à travers » les routeurs (d'un réseau à un autre) ?

12 Trunk et serveur

1) Un hyperviseur héberge des serveurs virtuels qui doivent être connectés à des réseaux différents. Aidez-vous de la commande vconfig pour configurer un trunk entre S2 et votre poste, sur lequel une interface virtuelle sera connectée au VLAN2 et une autre interface sera connectée au VLAN3.
Le module du noyau Linux qui gère le protocole 802.1q, nommé « vlan », est préchargé sur vos postes.
Vérifiez que vous pouvez joindre votre voisin, lui aussi connecté au VLAN2 et 3 via un trunk.

3) L'administrateur du réseau ne souhaite pas, pour des raisons évidentes de sécurité, que les serveurs puisent accéder à tous les VLAN du réseau.
Limitez leur accès au seul VLAN2 en utilisant la commande *switchport trunk*.

13 Agrégation de liens

13.1 Etherchannel

1) Le lien trunk entre S1 et S2 constitue un goulet d'étranglement, car son débit est identique au débit des liens utilisés par les postes (liens d'accès).
Réalisez une interface virtuelle (appelée *port-channel* ou *port group*) agrégeant 3 des interfaces de S1 et de S2. Mettez ensuite cette interface en mode *trunk*.

2) Utilisez iperf pour charger le lien entre A et B, connectés respectivement à S1 et S2, sur le VLAN2.
Affichez les statistiques des interfaces. La charge est-elle répartie sur les trois liens de l'Etherchannel ?
Lancez maintenant 2 transferts simultanés depuis un poste vers 2 postes différents. La charge est-elle répartie sur les trois liens de l'Etherchannel ?
Lancez maintenant 2 transferts simultanés vers le même poste. La charge est-elle répartie sur les trois liens de l'Etherchannel ?
Sur quel critère le switch se base-t-il pour répartir les trames sur les interfaces de l'Etherchannel ?

13.2 Bonding Linux

Sous Linux, l'agrégation de liens se nomme « bonding ». Le module du noyau Linux qui gère le bonding, nommé également « bonding », est préchargé sur vos postes.

1) La charge réseau vers un serveur peut parfois être importante. Pour augmenter la bande passante totale et la fiabilité de la liaison avec le serveur, agrégez 2 liens entre votre poste et le commutateur en utilisant la commande *ifenslave*.

2) Réitérez les transferts réalisés dans le chapitre précédent. Que constatez-vous ?