

Test des performances sans fil sur les liaisons WAN

Contenu

[Introduction](#)

[Description détaillée](#)

[Contraintes](#)

[Capacité de liaison WAN](#)

[Sécurité](#)

[Tests de test](#)

[Débit](#)

[Retards d'itinérance](#)

[Conclusion](#)

[Informations connexes](#)

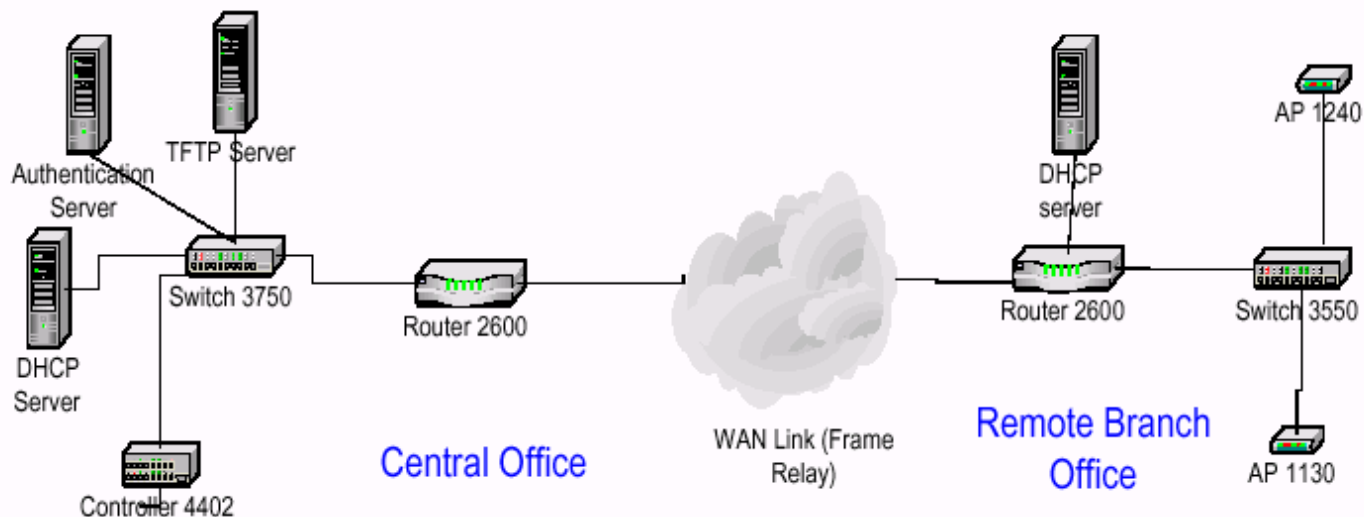
[Introduction](#)

Ce livre blanc présente les contraintes imposées par les liaisons WAN dans les systèmes sans fil des bureaux distants et met en évidence les deux tests de référence de base, le débit et la latence d'itinérance, pour de telles configurations.

[Description détaillée](#)

Les LAN sans fil (WLAN) sont devenus plus populaires dans les applications d'entreprise. Dans une situation où une entreprise ne souhaite pas installer de solution sans fil distincte pour une succursale, un point d'accès installé à distance, capable de gérer plusieurs utilisateurs et d'utiliser le réseau de l'entreprise pour d'autres besoins tels que la sécurité, la journalisation et la mise à niveau logicielle, est devenu plus populaire. Le réseau de la succursale est connecté au réseau du bureau central via les liaisons WAN. La [Figure 1 illustre](#) un scénario type dans lequel une liaison WAN série Frame Relay est utilisée.

Figure 1 : Configuration WLAN type pour une filiale distante



Les tests de performances impliquent une mesure des attributs qui montrent comment le système se comporte lorsqu'il est chargé à une capacité maximale. Les mesures standard des performances, telles que le débit, les délais d'itinérance et l'évolutivité, sont au coeur de chaque test de performances pour les équipements sans fil. Cependant, ces paramètres peuvent être gravement affectés par la topologie sous laquelle l'équipement est déployé. Ce document se concentre sur une topologie de ce type où la bande passante joue un rôle plus important qui affecte les mesures de performances standard.

Ce livre blanc présente plusieurs contraintes et techniques importantes utilisées pour résoudre ces problèmes et teste les performances sans fil sur les liaisons WAN dans une architecture basée sur contrôleur.

Contraintes

Cette section présente les principales contraintes d'une topologie de bureau distant.

Capacité de liaison WAN

Le point d'accès utilise un paquet Hello, également appelé pulsation, afin de communiquer avec le contrôleur. Dans un cas où cette pulsation est perdue, le point d'accès redécouvre le contrôleur. Au cours de ce processus, tous les clients existants sont déauthentiés. Cela entraîne une interruption des services sans fil dans la succursale. Par conséquent, l'un des objectifs du test sur la liaison WAN est non seulement de maintenir la pulsation dynamique, mais également de prendre en compte l'effet sur les performances globales du système.

L'intervalle de pulsation par défaut est de 30 secondes et ne peut pas être configuré manuellement. Lorsqu'un accusé de réception de pulsation du contrôleur est manqué, le point d'accès renvoie la pulsation jusqu'à 5 fois à des intervalles d'une seconde. Si un accusé de réception n'est pas reçu après 5 nouvelles tentatives, le point d'accès déclare le contrôleur inaccessible et recherche un nouveau contrôleur.

Une des techniques utilisées dans ces tests est la hiérarchisation du trafic. Cela permet de maintenir la pulsation afin d'éviter toute interruption de service. Le point d'accès utilise deux ports UDP afin de communiquer avec le contrôleur. L'AP utilise le port UDP 12223 pour tous les paquets de gestion et 12222 pour les paquets de données. Si la communication via le port 12223 peut être maintenue, la liaison entre le contrôleur et le point d'accès fonctionne même sous une

charge de trafic importante sur la liaison WAN. Ceci est généralement mis en oeuvre sur les ports du routeur WAN qui pointent vers les nuages WAN.

```
ip cef
!
frame-relay switching
!
class-map match-all 1
match access-group 199
!
policy-map mypolicy
class 1
bandwidth 64
!
interface Serial0/0
ip address 150.1.0.2 255.255.255.0
encapsulation frame-relay
clock rate 512000
frame-relay interface-dlci 101
frame-relay intf-type dce
service-policy output mypolicy
!
access-list 199 permit udp any any eq 12223
```

Sécurité

Dans un déploiement général, comme illustré à la [Figure 1](#), l'authentification est effectuée au bureau central où sont hébergés tous les serveurs d'authentification. Un serveur d'authentification local gardé au bureau distant n'est pas conseillé du point de vue du coût et de la maintenance. Si le contrôleur devient inaccessible pour une raison quelconque, le trafic peut être ponté localement. Cependant, comme il n'y a pas de serveur d'authentification local, seuls les types d'authentification ouverts et WPA (Wi-Fi Protected Access) sont pris en charge localement. Pour la plupart des clients, WPA forme le seul type d'authentification disponible. Cela devient une contrainte importante dans la conception des applications sans fil des bureaux distants.

Tests de test

Cette section analyse l'effet de ces contraintes sur les performances du système.

Débit

Comme indiqué précédemment dans ce document, le débit est gravement affecté par la bande passante disponible sur la liaison WAN, ainsi que par la hiérarchisation du trafic. Si vous supposez qu'une bande passante fixe sur la liaison WAN de 512 kbits/s est disponible avec un canal de hiérarchisation du trafic de 64 kbits/s, la bande passante de données disponible est de 448 kbits/s. Cependant, lorsque vous voyez le débit jusqu'à 501 kbits/s, vous pouvez croire que le débit de 64 kbits/s est préemptif au lieu d'un canal dédié.

La taille des trames ajoute une autre torsion. À partir de ce tableau, l'effet de la liaison WAN et de la taille des trames dans une topologie comme celle-ci est clair. Ce tableau présente également la comparaison avec les points d'accès connectés au bureau central. En outre, le débit est mesuré lorsque les clients de la succursale distante tentent d'envoyer des données à un client filaire du bureau central.

Tailles de trame (en octets)	Débit avec les points d'accès connectés au bureau central (bits/s)	Débit avec les points d'accès connectés au bureau distant (bits/s)
128	5,130,240	356,352
256	9,279,920	403,456
512	16,101,376	471,040
1024	24,576,000	483,328
1280	27,361,280	501,760
1450	28,756,400	498,800

Comme vous pouvez le voir dans ce tableau, le débit augmente avec la taille de trame jusqu'à ce que la taille de trame devienne 1280, puis retombe à 1450 octets. Ceci est dû à la fragmentation qui se produit pour les tailles de trames supérieures à 1418 octets dans les architectures basées sur des contrôleurs.

Retards d'itinérance

À partir de la discussion précédente, l'effet sur les délais d'itinérance est compris. Ce tableau affiche les données réelles. Il a été observé que les délais d'itinérance étaient beaucoup moins importants lorsque les points d'accès étaient connectés au commutateur via un concentrateur.

Authentification	Liaison WAN présente ?	Moyenne Délai d'itinérance (en ms)
Open (ouvert)	Non	36
Open (ouvert)	Oui	74
802.1x(LEAP)	Non	139
802.1x(LEAP)	Oui	230

Conclusion

Dans une configuration de filiale distante, la bande passante offerte par la liaison WAN joue un rôle crucial dans la décision des performances de l'équipement. Non seulement il est nécessaire d'établir des priorités de trafic, mais les effets sur le débit et l'itinérance sont un problème. La liaison WAN détermine l'étalonnage à effectuer. Ces essais diffèrent sensiblement des essais d'étalonnage standard. En outre, comme il n'y a pas de serveur d'authentification local, WPA est le type de sécurité préféré pour de telles applications. La capacité de liaison WAN et le type de sécurité sont des facteurs importants à prendre en compte lors du test de telles applications.

Informations connexes

- [Support et documentation techniques - Cisco Systems](#)