Test delle prestazioni wireless su collegamenti WAN

Sommario

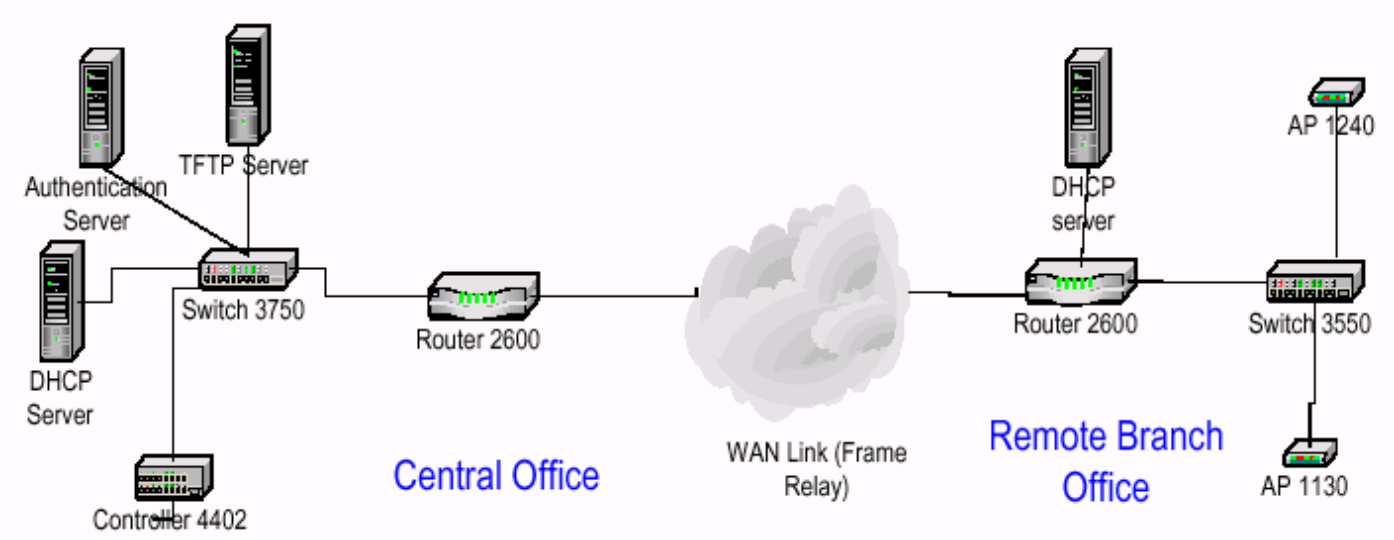
Introduzione

Questo white paper esamina i vincoli imposti dai collegamenti WAN nei sistemi wireless degli uffici remoti ed evidenzia i due test di benchmarking di base, throughput e latenza di roaming, per tali configurazioni.

Descrizione dettagliata

Le LAN wireless (WLAN) sono sempre più diffuse nelle applicazioni aziendali. In una situazione in cui un'azienda non desidera installare una soluzione wireless separata per una succursale, un punto di accesso (AP) installato in remoto in grado di gestire diversi utenti e di utilizzare la rete aziendale per altre esigenze, quali la sicurezza, la registrazione e l'aggiornamento del software, ha acquisito maggiore popolarità. La rete delle filiali è collegata alla rete degli uffici centrali tramite i collegamenti WAN. La Figura 1 mostra uno scenario tipico in cui viene utilizzato un collegamento WAN seriale Frame Relay.

Figura 1: Configurazione WLAN tipica per filiali remote



Il test delle prestazioni prevede la misurazione degli attributi che mostrano il comportamento del sistema quando viene caricato alla capacità massima. Le misure standard delle prestazioni, quali throughput, ritardi di roaming e scalabilità, sono alla base di ogni test delle prestazioni per le apparecchiature wireless. Tuttavia, questi parametri possono subire gravi conseguenze a causa della topologia utilizzata per la distribuzione dell'apparecchiatura. Questo documento si concentra su una di queste topologie in cui la larghezza di banda svolge un ruolo più importante che influisce sulle misure delle prestazioni standard.

Questo white paper evidenzia diversi importanti vincoli e tecniche utilizzati per risolverli e verifica le prestazioni wireless sui collegamenti WAN in un'architettura basata su controller.

Vincoli

In questa sezione vengono evidenziati i principali vincoli di una topologia di uffici remoti.

Capacità collegamento WAN

L'access point utilizza un pacchetto hello, noto anche come heartbeat, per comunicare con il controller. In caso di perdita di questo heartbeat, l'access point individua nuovamente il controller. Durante questo processo, tutti i client esistenti vengono deautenticati. Questo causa l'interruzione dei servizi wireless nelle filiali. Pertanto, uno degli obiettivi del test sul collegamento WAN è non solo mantenere attivo l'heartbeat, ma anche tenere in considerazione l'effetto sulle prestazioni complessive del sistema.

L'intervallo di heartbeat predefinito è di 30 secondi e non può essere configurato manualmente. Quando un riconoscimento di heartbeat dal controller non viene riconosciuto, l'access point invia il heartbeat fino a 5 volte a intervalli di 1 secondo. Se non viene ricevuta conferma dopo 5 tentativi, l'access point dichiara il controller non raggiungibile e cerca un nuovo controller.

Una delle tecniche utilizzate in questo test è l'assegnazione di priorità al traffico. In questo modo il battito cardiaco rimane attivo per evitare interruzioni del servizio. L'access point utilizza due porte UDP per comunicare con il controller. L'access point usa la porta UDP 1223 per tutti i pacchetti di gestione e la porta UDP 1222 per i pacchetti di dati. Se la comunicazione tramite la porta 1223 può essere mantenuta attiva, il collegamento tra il controller e l'access point funziona anche in caso di grave carico di traffico attraverso il collegamento WAN. Questa procedura viene generalmente implementata sulle porte del router WAN che puntano ai cloud 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
```

Sicurezza

In una distribuzione generale, come illustrato nella Figura 1, l'autenticazione viene eseguita presso l'ufficio centrale in cui sono ospitati tutti i server di autenticazione. Un server di autenticazione locale conservato presso la sede remota non è consigliabile dal punto di vista dei costi e della manutenzione. Se il controller diventa inaccessibile per qualsiasi motivo, il traffico può essere bloccato localmente. Tuttavia, poiché non esiste un server di autenticazione locale, solo i tipi di autenticazione aperta e WPA (Wi-Fi Protected Access) sono supportati localmente. Per la maggior parte dei clienti, WPA è l'unico tipo di autenticazione disponibile. Questo diventa un grave vincolo nella progettazione delle applicazioni wireless degli uffici remoti.

Test benchmark

Questa sezione analizza l'effetto di questi vincoli sulle prestazioni del sistema.

Velocità effettiva

Come accennato in precedenza in questo documento, la velocità di trasmissione è seriamente influenzata dalla larghezza di banda disponibile sul collegamento WAN, nonché dalla definizione delle priorità del traffico. Se si presume che sia disponibile una larghezza di banda fissa sul collegamento WAN di 512 kbps con un canale di prioritizzazione del traffico di 64 kbps, la larghezza di banda disponibile per i dati è di 448 kbps. Tuttavia, quando il throughput arriva fino a 501 kbps, si potrebbe pensare che il 64 kbps sia preventivo invece di un canale dedicato.

Le dimensioni dei fotogrammi aggiungono un'altra torsione a questo. Da questa tabella, l'effetto del collegamento WAN e le dimensioni dei frame in una topologia come questa sono chiare. La tabella mostra anche il confronto con i punti di accesso collegati all'ufficio centrale. La velocità di trasmissione viene inoltre misurata quando i client della succursale remota tentano di inviare dati a un client cablato della sede centrale.

Dimensioni frame	Throughput con gli access point collegati nell'ufficio centrale	Throughput con i punti di accesso collegati negli uffici remoti

(in byte)	(bit/sec.)	(bit/sec.)
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

Come si può vedere da questa tabella, il throughput aumenta con le dimensioni del frame fino a quando le dimensioni del frame diventano 1280 e poi scendono a 1450 byte. Ciò è dovuto alla frammentazione che si verifica per dimensioni di frame superiori a 1418 byte in architetture basate su controller.

Ritardi roaming

Dalla discussione precedente si comprende l'effetto sui ritardi del roaming. In questa tabella vengono visualizzati i dati effettivi. È stato osservato che i ritardi del roaming erano molto inferiori quando gli access point erano collegati allo switch tramite un hub.

Autenticazione	Collegamento WAN presente?	Media Ritardo roaming (in msec)
Open (Aperto)	No	36
Open (Aperto)	Sì	74
802.1x(LEAP)	No	139
802.1x(LEAP)	Sì	230

Conclusioni

In una configurazione di filiale remota, la larghezza di banda offerta dal collegamento WAN gioca un ruolo cruciale nella decisione delle prestazioni dell'apparecchiatura. Non solo è necessario definire le priorità del traffico, ma gli effetti sul throughput e sul roaming sono un problema. Il collegamento WAN determina il benchmark da eseguire. Tali test differiscono notevolmente dai test di benchmarking standard. Inoltre, poiché non esiste un server di autenticazione locale, WPA è il tipo di protezione preferito per tali applicazioni. La capacità del collegamento WAN e il tipo di sicurezza sono fattori importanti da prendere in considerazione quando si testano tali applicazioni.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems