Risoluzione dei problemi degli ambienti di switching LAN

Introduzione

In questo documento vengono descritte le funzionalità comuni degli switch LAN e viene spiegato come risolvere i problemi di switching LAN.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Le sezioni di questo capitolo descrivono le funzionalità comuni degli switch LAN e le soluzioni ad alcuni dei problemi più comuni di switching LAN. Gli argomenti trattati sono i seguenti:

- Introduzione allo switching LAN
- Suggerimenti per la risoluzione dei problemi generali dello switch
- Risoluzione dei problemi di connettività delle porte
- Risoluzione dei problemi di negoziazione automatica Ethernet 10/100 MB half/full duplex
- Trunking ISL su switch Catalyst serie 5000 e 6000
- Configurazione e risoluzione dei problemi dello switch EtherChannel sullo switch
- Usare Portfast e altri comandi per risolvere i problemi di connettività all'avvio della stazione terminale
- Configurazione e risoluzione dei problemi di switching multilayer

Introduzione allo switching LAN

Se non si ha familiarità con la commutazione LAN, in queste sezioni vengono esaminati alcuni dei concetti principali relativi agli switch. Uno dei prerequisiti per la risoluzione dei problemi di qualsiasi dispositivo è la conoscenza delle regole in base alle quali funziona. Gli switch sono diventati molto più complessi negli ultimi anni perché hanno acquisito popolarità e raffinatezza. Questi paragrafi descrivono alcuni dei concetti chiave da conoscere riguardo ai parametri.

Hub e switch

A causa della grande richiesta che viene posta sulle reti locali, si è passati da una rete a larghezza di banda condivisa, con hub e cavi coassiali, a una rete a larghezza di banda dedicata, con switch. Un hub consente il collegamento di più dispositivi allo stesso segmento di rete. I dispositivi su quel segmento condividono la larghezza di banda tra loro. Se si tratta di un hub a 10 MB e vi sono 6 dispositivi connessi a 6 porte diverse sull'hub, tutti e sei i dispositivi condividono i 10 MB di larghezza di banda tra loro. Un hub da 100 MB condivide 100 MB di larghezza di banda tra i dispositivi collegati. Per quanto riguarda il modello OSI, un hub è considerato un dispositivo di livello uno (livello fisico). Sente un segnale elettrico sul cavo e lo passa alle altre porte.

Uno switch può sostituire fisicamente un hub nella rete. Uno switch consente il collegamento di più dispositivi alla stessa rete, proprio come un hub, ma questa è l'area in cui termina la similarità. Uno switch consente a ciascun dispositivo connesso di avere una larghezza di banda dedicata anziché condivisa. La larghezza di banda tra lo switch e il dispositivo è riservata alla comunicazione da e verso il dispositivo. Sei dispositivi collegati a sei porte diverse su uno switch da 10 MB hanno ognuno 10 MB di larghezza di banda da utilizzare, anziché condividerla con gli altri dispositivi. Uno switch può aumentare notevolmente la larghezza di banda disponibile nella rete, migliorando le prestazioni della rete.

Bridge e switch

Uno switch di base è considerato un dispositivo di livello due. Quando si utilizza la parola layer, si fa riferimento al modello OSI a 7 livelli. Un commutatore non si limita a trasmettere i segnali elettrici, come fa un hub; al contrario, assembla i segnali in un fotogramma (livello due), quindi decide cosa fare con il fotogramma. Uno switch determina cosa fare con un frame quando prende in prestito un algoritmo da un altro dispositivo di rete comune: un bridge trasparente. Logicamente, uno switch agisce come un bridge trasparente, ma può gestire i frame molto più rapidamente di quanto potrebbe fare un bridge trasparente (a causa di hardware e architettura speciali). Una volta che lo switch decide dove inviare il frame, lo passa alla porta (o alle porte) appropriata. Uno switch può essere paragonato a un dispositivo che crea connessioni istantanee tra varie porte, fotogramma per fotogramma.

VLAN

Poiché lo switch decide, frame per frame, quali porte scambiano i dati, si tratta di un'estensione naturale che consente di inserire la logica nello switch e di scegliere le porte per gruppi speciali. Questo raggruppamento di porte è denominato VLAN (Virtual Local Area Network). Lo switch assicura che il traffico proveniente da un gruppo di porte non venga mai inviato ad altri gruppi di porte (routing). Ciascuno di questi gruppi di porte (VLAN) può essere considerato un singolo segmento LAN.

Le VLAN sono anche descritte come domini di broadcast. Ciò è dovuto all'algoritmo di bridging trasparente, in base al quale i pacchetti broadcast (pacchetti destinati all'indirizzo di *tutti i dispositivi*) devono essere inviati a tutte le porte dello stesso gruppo (ossia della stessa VLAN). Tutte le porte che si trovano nella stessa VLAN si trovano anche nello stesso dominio di broadcast.

Algoritmo Bridging Trasparente

L'algoritmo di bridging trasparente e lo Spanning Tree sono illustrati in dettaglio altrove (Capitolo 20: Risoluzione dei problemi relativi agli ambienti di bridging trasparenti). Quando uno switch riceve un frame, deve decidere cosa fare con quel frame. Potrebbe ignorare il frame; potrebbe passare il frame fuori da un'altra porta o potrebbe passare il frame fuori da molte altre porte.

Per sapere cosa fare con il frame, lo switch apprende la posizione di tutti i dispositivi sul segmento. Queste informazioni sulla posizione vengono inserite in una tabella di memoria indirizzabile al contenuto (CAM - denominata in base al tipo di memoria utilizzata per memorizzare queste tabelle). La tabella CAM mostra, per ciascun dispositivo, l'indirizzo MAC del dispositivo, la porta in uscita da cui è possibile trovare l'indirizzo MAC e la VLAN a cui è associata questa porta. Lo switch impara continuamente quando riceve dei frame. La tabella CAM dello switch viene continuamente aggiornata.

Queste informazioni nella tabella CAM vengono utilizzate per decidere come gestire un frame ricevuto. Per decidere dove inviare un frame, lo switch cerca l'indirizzo MAC di destinazione in un frame ricevuto e cerca l'indirizzo MAC di destinazione nella tabella CAM. La tabella CAM mostra la porta attraverso la quale il frame deve essere inviato per raggiungere l'indirizzo MAC di destinazione specificato. Di seguito sono riportate le regole di base utilizzate da uno switch per eseguire la responsabilità di inoltro del frame:

Se l'indirizzo MAC di destinazione è presente nella tabella CAM, lo switch invia il frame alla porta associata all'indirizzo MAC di destinazione nella tabella CAM. Questa operazione viene definita *inoltro*.

Se la porta associata per l'invio del frame è la stessa porta su cui originariamente il frame è arrivato, non è necessario inviare nuovamente il frame dalla stessa porta e il frame viene ignorato. Questo processo è denominato *filtraggio* .

Se l'indirizzo MAC di destinazione non è presente nella tabella CAM (l'indirizzo è *sconosciuto*), lo switch invia il frame a tutte le altre porte che si trovano nella stessa VLAN del frame ricevuto. Questo si chiama allagamento. Il frame non viene inondato dalla stessa porta su cui è stato ricevuto.

Se l'indirizzo MAC di destinazione del frame ricevuto è l'indirizzo di broadcast (FFFF.FFFF.FFFF), il frame viene inviato a tutte le porte che si trovano sulla stessa VLAN del frame ricevuto. Questo processo è noto anche come inondazione. Il frame non viene inviato dalla stessa porta su cui è stato ricevuto.

Spanning Tree Protocol

Come avete visto, l'algoritmo di bridging trasparente propaga i frame sconosciuti e broadcast di tutte le porte che si trovano sulla stessa VLAN del frame ricevuto. Questo causa un potenziale problema. Se i dispositivi di rete che eseguono questo algoritmo sono connessi tra loro in un loop fisico, i frame a scorrimento (come i broadcast) vengono trasmessi da uno switch all'altro, intorno al loop e così via, per sempre. A seconda delle connessioni fisiche coinvolte, i frame possono in realtà moltiplicarsi in modo esponenziale a causa dell'algoritmo di flooding, che può causare gravi problemi di rete.

Esiste un vantaggio per un loop fisico nella rete: può fornire ridondanza. Se un collegamento non riesce, c'è ancora un altro modo per il traffico di raggiungere la sua destinazione. Per consentire i vantaggi derivanti dalla ridondanza e non interrompere la rete a causa delle inondazioni, è stato creato un protocollo chiamato spanning tree. Spanning Tree è stato standardizzato nella specifica IEEE 802.1d.

Lo scopo del protocollo STP (Spanning Tree Protocol) è identificare e bloccare temporaneamente i loop in un segmento di rete o in una VLAN. Gli switch eseguono l'STP e selezionano un bridge radice o uno switch. Gli altri switch misurano la distanza dallo switch radice. Se esistono più modi per raggiungere il commutatore principale, si verifica un loop. Gli switch tracciano l'algoritmo per determinare le porte da bloccare per interrompere il loop. Il protocollo STP è dinamico. Se un collegamento nel segmento ha esito negativo, le porte che in origine erano bloccate possono essere passate alla modalità di inoltro.

Trunking

Il trunking è un meccanismo molto spesso utilizzato per consentire a più VLAN di funzionare in modo indipendente su più switch. Anche i router e i server possono utilizzare il trunking, che consente loro di risiedere simultaneamente su più VLAN. Se la rete dispone di una sola VLAN, non è necessario eseguire il trunking; tuttavia, se la rete dispone di più VLAN, è probabile che si desideri sfruttare i vantaggi del trunking.

Una porta di uno switch appartiene in genere a una sola VLAN. Si presume che il traffico ricevuto o inviato su questa porta appartenga alla VLAN configurata. Una porta trunk, d'altra parte, è una porta che può essere configurata per inviare e ricevere traffico per molte VLAN. A tal fine, vengono allegate le informazioni VLAN a ciascun frame, un processo denominato *tagging* del frame. Inoltre, il trunking deve essere attivo su entrambi i lati del collegamento; l'altro lato deve prevedere alcuni frame che includono le informazioni VLAN per consentire una corretta comunicazione.

Esistono diversi metodi di trunking che dipendono dal supporto utilizzato. I metodi di trunking per Fast Ethernet o Gigabit Ethernet sono ISL (Inter-Switch Link) o 802.1q. Il trunking su ATM utilizza LANE. Il trunking su FDDI utilizza 802.10.

EtherChannel

EtherChannel è una tecnica utilizzata quando si hanno più connessioni allo stesso dispositivo. Anziché ciascuna funzione di collegamento in modo indipendente, EtherChannel raggruppa le porte in modo che funzionino come un'unica unità. Distribuisce il traffico su tutti i collegamenti e fornisce ridondanza in caso di errore di uno o più collegamenti. Le impostazioni di EtherChannel devono essere le stesse su entrambi i lati dei collegamenti coinvolti nel canale. Normalmente, lo Spanning Tree blocca tutte le connessioni parallele tra i dispositivi perché sono loop, ma EtherChannel viene eseguito *sotto lo* Spanning Tree, in modo che lo Spanning Tree pensi che tutte le porte all'interno di un determinato EtherChannel siano solo una porta.

MLS (Multilayer Switching)

Lo switching multilivello (MLS) è la capacità di uno switch di inoltrare i fotogrammi in base alle informazioni contenute nell'intestazione di livello tre e talvolta di livello quattro. Questo si applica in genere ai pacchetti IP, ma ora può verificarsi anche per i pacchetti IPX. Lo switch impara a gestire questi pacchetti quando comunica con uno o più router. Con una spiegazione semplificata, lo switch monitora il modo in cui il router elabora un pacchetto, quindi lo switch elabora i pacchetti futuri nello stesso flusso. Tradizionalmente, gli switch sono stati più veloci nello switching dei

frame rispetto ai router, quindi la loro riduzione del traffico dal router può comportare miglioramenti significativi della velocità. Se qualcosa cambia nella rete, il router può dire allo switch di cancellare la cache di terzo livello e ricostruirla di nuovo con l'evolversi della situazione. Il protocollo utilizzato per comunicare con i router è denominato MLSP (Multilayer Switching Protocol).

Informazioni su queste funzionalità

Queste sono solo alcune delle funzionalità di base supportate dagli switch. Ogni giorno ne vengono aggiunti altri. È importante capire come funzionano gli switch, quali funzionalità si usano e come devono funzionare. Per ulteriori informazioni sugli switch Cisco, visitare il sito Web Cisco. Andare alla sezione *Assistenza e supporto*, quindi scegliere *Documenti tecnici*. Da qui, scegliere *Home page Documentazione*. La documentazione relativa a tutti i prodotti Cisco è disponibile qui. Il collegamento *Switch LAN multilivello* permette di accedere alla documentazione di tutti gli switch LAN Cisco. Per informazioni sulle funzionalità di uno switch, consultare la *guida alla configurazione software* della versione in uso. Le guide alla configurazione software forniscono informazioni di base sulla funzione e sui comandi da utilizzare per configurarla sullo switch. Tutte queste informazioni sono gratuite sul web. Non è nemmeno necessario avere un account per questa documentazione, in quanto è disponibile per chiunque. Alcune di queste guide alla configurazione possono essere lette in un pomeriggio e valgono il tempo speso.

Un'altra parte del sito Web Cisco è popolata dal sito Web Cisco Support and Documentation. Contiene informazioni progettate per semplificare l'implementazione, la manutenzione e la risoluzione dei problemi della rete. Visitare il sito Web Supporto e documentazione per ottenere informazioni dettagliate sul supporto in base a prodotti o tecnologie specifici.

Suggerimento per la risoluzione dei problemi generali dello switch

Per risolvere i problemi relativi a uno switch, procedere in diversi modi. Con la crescita delle caratteristiche degli switch, aumentano anche le possibilità di interruzione. Per risolvere i problemi in modo efficace, è consigliabile sviluppare un approccio o un piano di test anziché un approccio basato su riscontri positivi e negativi. Di seguito sono riportati alcuni suggerimenti generali:

Acquisire familiarità con il normale funzionamento dello switch. Come accennato nella sezione precedente, il sito Web Cisco contiene una quantità enorme di informazioni tecniche che descrivono il funzionamento degli switch. Le guide alla configurazione in particolare sono molto utili. Molti casi aperti vengono risolti con le informazioni delle guide alla configurazione del prodotto.

- Per le situazioni più complesse, disporre di una mappa fisica e logica accurata della rete. Una mappa fisica mostra come sono connessi i dispositivi e i cavi. Una mappa logica mostra i segmenti (VLAN) esistenti nella rete e i router che forniscono servizi di routing a questi segmenti. Una mappa Spanning Tree è molto utile per risolvere problemi complessi. A causa della capacità di uno switch di creare segmenti diversi con l'implementazione di VLAN, le sole connessioni fisiche non raccontano l'intera storia; è necessario sapere come gli switch sono configurati per determinare quali segmenti (VLAN) esistono e come sono connessi logicamente.

  Prenda un piano. Alcuni problemi e soluzioni sono ovvi, altri no. I sintomi rilevati nella rete possono essere il risultato di problemi in un'altra area o livello. Prima di saltare alle conclusioni, provare a verificare in modo strutturato cosa funziona e cosa non funziona. Poiché le reti possono essere complesse, è utile isolare i possibili domini con problemi. A tale

scopo, è possibile utilizzare il modello a sette livelli OSI. Ad esempio: controllare le connessioni fisiche interessate (livello 1), controllare i problemi di connettività nella VLAN (livello 2), controllare i problemi di connettività sulle diverse VLAN (livello 3) e così via. Se sullo switch è presente una configurazione corretta, molti dei problemi riscontrati sono correlati a problemi fisici (porte e cavi fisici). Oggi, gli switch sono coinvolti in problemi di livello tre e quattro, che incorporano funzionalità intelligenti per commutare i pacchetti in base alle informazioni derivate dai router, o hanno router che risiedono all'interno dello switch (switching di livello tre o quattro).

Non presumere che un componente funzioni, è necessario prima controllarlo. In questo modo è possibile risparmiare molto tempo sprecato. Se ad esempio un PC non è in grado di accedere a un server della rete, è possibile che si verifichino molti problemi. Non saltare le cose di base e pensare che qualcosa funzioni; qualcuno può aver cambiato qualcosa e non dirtelo. È sufficiente un minuto per verificare alcuni aspetti di base (ad esempio, che le porte coinvolte siano collegate al posto giusto e siano attive), il che potrebbe far risparmiare molte ore sprecate.

Risoluzione dei problemi di connettività delle porte

Se la porta non funziona, non funziona nulla. Le porte sono la base della rete di commutazione. Alcuni porti hanno un significato particolare a causa della loro posizione nella rete e della quantità di traffico che trasportano. Queste porte includono connessioni ad altri switch, router e server. Queste porte possono essere più complicate da risolvere perché spesso sfruttano funzionalità speciali, quali trunking ed EtherChannel. Anche le altre porte sono importanti, in quanto connettono gli utenti effettivi della rete.

Molte cose possono causare la non funzionalità di una porta: problemi hardware, problemi di configurazione e problemi di traffico. Queste categorie vengono analizzate un po' più a fondo.

Problemi hardware

Generale

La funzionalità delle porte richiede due porte attive collegate da un cavo attivo (del tipo corretto). Per impostazione predefinita, la maggior parte degli switch Cisco ha una porta nello stato *notconnect*, ossia non è attualmente connessa ad alcun dispositivo, ma desidera connettersi. Se si collega un cavo valido a due porte dello switch in stato *notconnect*, la spia di collegamento diventa verde per entrambe le porte e lo stato della porta è *connected*, ovvero la porta è attiva per il layer 1. In questi paragrafi vengono evidenziati gli elementi per i quali verificare se il livello 1 non è attivo.

Controllare lo stato di entrambe le porte coinvolte. Accertarsi che nessuna delle porte coinvolte nel collegamento sia chiusa. L'amministratore può aver chiuso una o entrambe le porte. Il software all'interno dello switch può aver spento la porta a causa di condizioni di errore di configurazione. Se un lato è spento e l'altro no, lo stato sul lato abilitato è *notconnect* (perché non rileva alcun vicino sull'altro lato del cavo). Lo stato visualizzato sul lato shutdown dice qualcosa come *disable* o *errDisable* (a seconda dell'arresto effettivo della porta). Il collegamento non viene attivato a meno che entrambe le porte non siano abilitate.

Quando si collega un cavo valido (di nuovo, se del tipo corretto) tra due porte abilitate, in pochi secondi viene visualizzata una spia verde per il collegamento. Inoltre, lo stato della porta indica

connected (connesso) nell'interfaccia della riga di comando (CLI). A questo punto, se il collegamento non è disponibile, il problema è limitato a tre elementi: la porta su un lato, la porta sull'altro lato o il cavo al centro. In alcuni casi sono interessati altri dispositivi: convertitori di supporti (da fibra a rame e così via) oppure sui collegamenti Gigabit è possibile avere connettori di interfaccia Gigabit (GBIC). Tuttavia, si tratta di un'area ragionevolmente limitata in cui effettuare la ricerca.

I convertitori di supporti possono aggiungere rumore a una connessione o indebolire il segnale se non funzionano correttamente. Aggiungono inoltre connettori aggiuntivi che possono causare problemi e sono un altro componente di cui eseguire il debug.

Controllare che non vi siano collegamenti allentati. A volte un cavo sembra essere inserito nel jack, ma in realtà non lo è; scollegare il cavo e reinserirlo. È inoltre necessario cercare sporcizia, spille perse o rotte. Eseguire questa operazione su entrambe le porte coinvolte nella connessione.

Il cavo può essere collegato alla porta sbagliata, cosa che normalmente accade. Accertarsi che entrambe le estremità del cavo siano collegate alle porte desiderate.

Èpossibile avere un collegamento da un lato e non dall'altro. Verificare che il collegamento sia presente su entrambi i lati. Un singolo filo rotto può causare questo tipo di problema.

La spia del collegamento non garantisce che il cavo sia perfettamente funzionante. Può essersi scontrato con uno stress fisico che lo rende funzionale a un livello marginale. In genere, ciò si verifica a causa della porta che contiene molti errori di pacchetto.

Per determinare se il problema è causato dal cavo, sostituirlo con un cavo sicuramente funzionante. Non sostituirlo semplicemente con un altro cavo; accertarsi di sostituirlo con un cavo che si sappia essere valido e del tipo corretto.

Se si tratta di un cavo molto lungo (sotterraneo, attraverso un grande campus, ad esempio), è bello avere un sofisticato tester di cavi. Se non si dispone di un tester per cavi, è possibile considerare quanto segue:

- Provare a utilizzare porte diverse per verificare se il cavo è lungo.
- Collegare la porta in questione a un'altra porta nello stesso switch per verificare se la porta è collegata localmente.
- Spostare temporaneamente gli switch l'uno vicino all'altro, in modo da poter provare a utilizzare un cavo sicuramente funzionante.

Rame

Assicurarsi di disporre del cavo corretto per il tipo di connessione che si esegue. Il cavo di categoria 3 può essere utilizzato per connessioni UTP da 10 MB, mentre il cavo di categoria 5 deve essere utilizzato per connessioni 10/100.

Per il collegamento di unità terminali, router o server a uno switch o a un hub, viene utilizzato un cavo RJ-45 straight-through. Un cavo crossover Ethernet viene utilizzato per collegare lo switch al dispositivo o per collegare l'hub al dispositivo. Questa è l'uscita per un cavo crossover Ethernet. Le distanze massime per i cavi in rame Ethernet o Fast Ethernet sono di 100 metri. Una buona regola generale consiste nell'utilizzare un cavo straight-through quando si collega un livello OSI,

come tra uno switch e un router; quando si collegano due dispositivi nello stesso livello OSI, come tra due router o due switch, utilizzare un cavo crossover. Solo ai fini di questa regola, trattare una workstation come un router.

Le due immagini mostrano i pin-out necessari per un cavo crossover da switch a switch.

Fibra ottica

Per le fibre ottiche, assicurarsi di disporre del cavo corretto per le distanze interessate e il tipo di porte in fibra utilizzate (modalità singola, modalità multipla). Verificare che le porte connesse siano entrambe in modalità singola e multi. La fibra monomodale in genere raggiunge i 10 chilometri e la fibra multimodale in genere raggiunge i 2 chilometri, ma esiste il caso speciale della modalità multipla 100BaseFX usata nella modalità half-duplex, che può andare solo a 400 metri.

Per le connessioni in fibra, verificare che il cavo di trasmissione di una porta sia collegato al cavo di ricezione dell'altra porta e viceversa; la trasmissione, la ricezione e la ricezione non funzionano.

Per le connessioni Gigabit, i GBIC devono essere abbinati su ciascun lato della connessione. Ci sono diversi tipi di GBIC a seconda del cavo e delle distanze coinvolte: lunghezza d'onda corta (SX), lunghezza d'onda lunga (LX/LH) e distanza estesa (ZX).

Un GBIC SX deve essere collegato a un GBIC SX; un GBIC SX non è collegato a un GBIC LX. Inoltre, alcune connessioni Gigabit richiedono cavi di condizionamento in base alla lunghezza. Consultare le note sull'installazione di GBIC.

Se il collegamento Gigabit non viene visualizzato, verificare che le impostazioni di controllo del flusso e di negoziazione delle porte siano coerenti su entrambi i lati del collegamento. L'implementazione di queste funzionalità può presentare incompatibilità se gli switch connessi provengono da fornitori diversi. In caso di dubbio, disattivare queste funzioni su entrambi gli switch.

Problemi di configurazione

Un'altra causa dei problemi di connettività delle porte è la configurazione software errata dello switch. Se una porta è illuminata da una luce arancione fissa, il software all'interno dello switch la arresta tramite l'interfaccia utente o tramite processi interni.

Accertarsi che l'amministratore non abbia chiuso le porte coinvolte (come accennato). La porta può essere chiusa manualmente dall'amministratore su un lato del collegamento o sull'altro. Il collegamento non viene attivato finché la porta non viene riattivata; verificare lo stato della porta.

alcuni switch, come Catalyst 4000/5000/6000, possono arrestare la porta se i processi software all'interno dello switch rilevano un errore. Se si controlla lo stato della porta, il messaggio *sarà errDisable*. È necessario risolvere il problema di configurazione e quindi rimuovere manualmente la porta dallo stato errDisable. In alcune versioni software più recenti (CatOS 5.4(1) e versioni successive), la porta può essere riattivata automaticamente dopo un periodo di tempo configurabile in stato errDisable. Di seguito sono riportate alcune delle cause dello stato errDisable:

- **Configurazione errata di EtherChannel**: se un lato è configurato per EtherChannel e l'altro no, il processo Spanning Tree può disattivare la porta sul lato configurato per EtherChannel. Se si tenta di configurare EtherChannel ma le porte interessate non hanno le stesse impostazioni (velocità, duplex, modalità trunking e così via) delle porte adiacenti sul collegamento, potrebbe verificarsi lo stato errDisable. Se si desidera utilizzare EtherChannel, è preferibile

impostare ciascun lato della modalità *desiderata* per EtherChannel. Nelle sezioni seguenti vengono fornite informazioni dettagliate su come configurare EtherChannel.

Mancata corrispondenza del duplex: se la porta dello switch riceve molte collisioni ritardate, ciò in genere indica un problema di mancata corrispondenza del duplex. Ci sono altre cause per le collisioni ritardate: una scheda NIC corrotta, segmenti di cavo troppo lunghi, ma la causa più comune al momento è una mancata corrispondenza del duplex. Il dispositivo full-duplex ritiene di poter inviare in qualsiasi momento. Il dispositivo half-duplex si aspetta solo pacchetti in determinati momenti - non in "qualsiasi" momento.

BPDU Port-guard: alcune versioni più recenti del software dello switch possono monitorare se portfast è abilitato su una porta. Le porte che usano portfast devono essere collegate a una unità terminale, non a dispositivi che generano pacchetti Spanning Tree chiamati BPDU. Se lo switch rileva una BPDU su una porta con portfast abilitata, la porta viene messa in modalità errDisable.

UDLD: Unidirectional Link Detection è un protocollo di alcune nuove versioni del software che rileva se la comunicazione su un collegamento è unidirezionale. La comunicazione unidirezionale può essere causata da un cavo in fibra rotto o da altri problemi di cavo/porta. Questi collegamenti parzialmente funzionanti possono causare problemi quando gli switch interessati non sanno che il collegamento è parzialmente interrotto. Questo problema può causare loop nello spanning tree. È possibile configurare il protocollo UDLD in modo che una porta venga messa in stato errDisable quando viene rilevato un collegamento unidirezionale.

Mancata corrispondenza della VLAN nativa: prima di attivare il trunking di una porta, questa appartiene a una singola VLAN. Quando il trunking è attivato, la porta può trasmettere il traffico di molte VLAN. La porta ricorda ancora la VLAN in cui si trovava prima dell'attivazione del trunking, ossia la VLAN nativa. La VLAN nativa è fondamentale per il trunking 802.1q. Se la VLAN nativa su entrambe le estremità del collegamento non corrisponde, una porta viene messa nello stato errDisable.

Altro: tutti i processi dello switch che riconoscono un problema sulla porta possono *attivarlo* lo stato *errDisable*.

Un'altra causa delle porte inattive è la scomparsa della VLAN a cui appartengono. Ogni porta di uno switch appartiene a una VLAN. Se la VLAN viene eliminata, la porta diventa inattiva. alcuni switch mostrano una luce arancione fissa su ciascuna porta su cui si è verificato questo problema. Se un giorno si entra in ufficio e si accendono centinaia di luci arancioni, non si verificherà alcun problema; è possibile che tutte le porte appartengano alla stessa VLAN e che qualcuno abbia accidentalmente eliminato la VLAN a cui appartenevano le porte. Quando si aggiunge nuovamente la VLAN alla tabella VLAN, le porte tornano ad essere attive. Una porta ricorda la VLAN assegnata.

Se il collegamento è attivo e le porte sono connesse, ma non è possibile comunicare con un altro dispositivo, ciò può essere particolarmente problematico. Di solito indica un problema più alto del livello fisico: livello 2 o livello 3. Prova queste cose.

Controllare che su entrambi i lati del collegamento Accertarsi che entrambi i lati siano nella

stessa modalità. Se si attiva la modalità trunking (anziché "auto" o "desiderabile") su una porta e l'altra porta ha il trunking

impostata su "off", non sono in grado di comunicare. Il trunking modifica il formato del pacchetto; le porte devono accettare il formato da utilizzare sul collegamento, o non si capiscono a vicenda.

Verificare che tutti i dispositivi si trovino nella stessa VLAN. Se non sono sulla stessa VLAN, occorre configurare un router per consentire le comunicazioni dei dispositivi.

Verificare che l'indirizzamento di livello tre sia configurato correttamente.

Problemi relativi al traffico

In questa sezione vengono descritte alcune delle informazioni che è possibile apprendere quando si esaminano le informazioni sul traffico di una porta. La maggior parte degli switch ha un modo per tenere traccia dei pacchetti quando entrano ed escono da una porta. I comandi che generano questo tipo di output sugli switch Catalyst 4000/5000/6000 **sono show portandshow mac**. L'output di questi comandi sugli switch 4000/5000/6000 è descritto nelle guide di riferimento dei comandi dello switch.

Alcuni di questi campi del traffico della porta mostrano la quantità di dati trasmessi e ricevuti sulla porta. In altri campi viene visualizzato il numero di frame di errore rilevati sulla porta. Se si verificano molti errori di allineamento, errori FCS o collisioni ritardate, è possibile che il duplex non corrisponda sul cavo. Altre cause di questi tipi di errori possono essere schede di interfaccia di rete non corrette o problemi di cavi. Se il numero di frame posticipati è elevato, il segmento è sovraccarico di traffico e lo switch non è in grado di inviare sufficiente traffico sul cavo per svuotare i relativi buffer. Considerate la possibilità di rimuovere alcuni dispositivi da un altro segmento.

Errore hardware dello switch

Se sono stati eseguiti tutti i tentativi possibili e la porta non funziona, è possibile che l'hardware sia difettoso.

A volte le porte sono danneggiate dalle scariche elettrostatiche (ESD). È possibile o non è possibile visualizzare alcuna indicazione in merito.

Esaminare i risultati del POST (Power-On Self-Test) restituiti dallo switch per verificare la presenza di eventuali guasti indicati per una parte qualsiasi dello switch.

Se vedi un comportamento che può solo essere considerato "strano", questo può indicare problemi hardware, ma anche problemi software. In genere è più facile ricaricare il software che acquistare nuovo hardware. Provare a utilizzare prima il software dello switch.

Il sistema operativo può avere un bug. Se si carica un sistema operativo più recente, è possibile risolvere il problema. Per individuare i bug noti, consultare le note sulla versione del codice in uso o usare Cisco Bug ToolKit.

Il sistema operativo avrebbe potuto essere in qualche modo danneggiato. Se si ricarica la stessa versione del sistema operativo, è possibile risolvere il problema.

Se la spia di stato sullo switch lampeggia in arancione, in genere significa che si è verificato un problema hardware con la porta, il modulo o lo switch. Lo stesso vale se lo stato della porta o del modulo indica *un errore*.

Prima di sostituire l'hardware dello switch, è possibile provare a eseguire le seguenti operazioni:

Ricollocare il modulo nello switch. Se si esegue questa operazione all'accensione, assicurarsi che il modulo sia sostituibile a caldo. In caso di dubbio, spegnere l'interruttore prima di ricollegare il modulo o consultare la guida all'installazione dell'hardware. Se la porta è integrata nello switch, ignorare questo passaggio.

Riavviare lo switch. A volte questo causa la scomparsa del problema; si tratta di una soluzione, non di una correzione.

Controllare il software dello switch. Se si tratta di una nuova installazione, tenere presente che alcuni componenti possono funzionare solo con determinate versioni del software. Consultare le note sulla versione o la guida all'installazione e alla configurazione dell'hardware per il componente da installare.

Se si è ragionevolmente certi di avere un problema hardware, sostituire il componente difettoso.

Risoluzione Dei Problemi Di Negoziazione Automatica Half/Full Duplex Ethernet 10/100 Mb

Obiettivi

In questa sezione vengono presentate le informazioni generali utilizzate per la risoluzione dei problemi e una descrizione delle tecniche per la risoluzione dei problemi di negoziazione automatica Ethernet.

Questa sezione illustra come determinare il comportamento corrente di un link. nonché spiegare le situazioni in cui la negoziazione automatica non ha esito positivo.

Molti switch Cisco Catalyst e router Cisco diversi supportano la negoziazione automatica. In questa sezione viene descritta la negoziazione automatica tra gli switch Catalyst 5000. I concetti qui illustrati possono essere applicati anche ad altri tipi di dispositivi.

Introduzione

La negoziazione automatica è una funzione opzionale dello standard Fast Ethernet IEEE 802.3u che consente ai dispositivi di scambiare automaticamente le informazioni sulla velocità e sulle capacità duplex tramite un collegamento.

La negoziazione automatica è destinata alle porte, assegnate alle aree in cui utenti o dispositivi temporanei si connettono a una rete. Molte aziende, ad esempio, forniscono uffici o cubi condivisi

che possono essere utilizzati dagli account manager e dai System Engineer quando si trovano in ufficio anziché in viaggio. Ogni ufficio o postazione dispone di una porta Ethernet connessa in modo permanente alla rete dell'ufficio. Poiché non è possibile garantire che ogni utente disponga di 10 MB, una rete Ethernet da 100 MB o una scheda 10/100 MB sul proprio pc, le porte degli switch che gestiscono queste connessioni devono essere in grado di negoziare la velocità e la modalità duplex. L'alternativa è in grado di fornire sia una porta da 10 MB che una porta da 100 MB in ogni ufficio o postazione e di etichettarli di conseguenza.

La negoziazione automatica non deve essere utilizzata per le porte che supportano dispositivi dell'infrastruttura di rete, quali switch e router, o altri sistemi terminali non transitori, quali server e stampanti. Sebbene la negoziazione automatica per la velocità e il duplex sia in genere il comportamento predefinito sulle porte dello switch che ne sono compatibili, le porte connesse a dispositivi fissi devono sempre essere configurate per il comportamento corretto, anziché essere autorizzate a negoziarlo. In questo modo vengono eliminati potenziali problemi di negoziazione e viene assicurato che l'utente sappia sempre esattamente come le porte devono funzionare. Ad esempio, un collegamento da switch a switch Ethernet 10/100BaseTX configurato per 100 MB Full Duplex funziona solo a quella velocità e modalità. Non è possibile per le porte effettuare il downgrade del collegamento a una velocità inferiore all'interno di un reset della porta o di un reset dello switch. Nel caso in cui le porte non possano funzionare come configurate, non devono superare alcun traffico. D'altra parte, un collegamento da switch a switch a cui è stato consentito di negoziare il proprio comportamento può funzionare nella modalità half-duplex a 10 MB. Un collegamento non funzionante è in genere più facile da individuare rispetto a un collegamento funzionante ma non funzionante alla velocità o alla modalità previste.

Una delle cause più comuni dei problemi di prestazioni dei collegamenti Ethernet a 10/100 MB è quando una porta sul collegamento funziona in modalità half-duplex, mentre l'altra porta funziona in modalità full-duplex. Questo si verifica occasionalmente quando una o entrambe le porte in un collegamento vengono resettate e il processo di negoziazione automatica non genera la stessa configurazione per entrambi i partner del collegamento. Questa condizione si verifica anche quando gli utenti riconfigurano un partner del collegamento ma non l'altro. Molte delle chiamate in assistenza relative a problemi di prestazioni possono essere evitate se si crea un criterio che richiede la configurazione delle porte di tutti i dispositivi non transitori per il comportamento richiesto e l'applicazione del criterio con misure di controllo delle modifiche adeguate.

Risoluzione Dei Problemi Di Negoziazione Automatica Ethernet Tra Dispositivi Dell'Infrastruttura Di Rete

Procedure e/o scenari

Scenario 1. Cat 5K con Fast Ethernet

Tabella 22-2: Problemi di connettività della negoziazione automatica

Possibile problema	Soluzione
Il comportamento corrente del collegamento è stato negoziato automaticamente?	1. Utilizzare il comando **show port num_mod/**num_**porta** per determinare il comportamento corrente del collegamento. Se entrambi i partner di collegamento (interfacce a una delle estremità del collegamento) indicano un prefisso "a-" nei campi di stato duplex e velocità, è probabile che la negoziazione automatica abbia avuto esito positivo.
negoziazione	2. Eseguire il comando **show port capabilities**

automatica non supportata.	**num_mod/**num**_porta** per verificare che i moduli supportino la negoziazione automatica. 3. Utilizzare **il comando set port speed**
la negoziazione automatica non funziona sugli switch Catalyst.	**num_mod/num_porta** su Catalyst per configurare la negoziazione automatica. 4. Provare con porte o moduli diversi. 5. Provare a ripristinare le porte. 6. Provare a utilizzare cavi patch diversi. 7. Spegnere e riaccendere i dispositivi.
la negoziazione automatica non funziona sui router Cisco.	8. Eseguire il comando Cisco IOS corretto per abilitare la negoziazione automatica (se disponibile) 9. Provare con interfacce diverse. 10. Provare a ripristinare le interfacce. 11. Provare a utilizzare cavi patch diversi. 12. Spegnere e riaccendere i dispositivi.

Esempio di configurazione e risoluzione dei problemi di negoziazione automatica Ethernet 10/100 MB

In questa sezione viene esaminato il comportamento di una porta Ethernet 10/100 MB che supporta la negoziazione automatica. Viene inoltre illustrato come apportare modifiche al comportamento predefinito e come ripristinarne il comportamento predefinito.

Attività da eseguire

Esaminare le funzionalità delle porte.

Configurare la negoziazione automatica per la porta 1/1 su entrambi gli switch.

Determinare se la velocità e la modalità duplex sono impostate per la negoziazione automatica.

Modificare la velocità sulla porta 1/1 nello switch A a 10MB.

Comprendere il significato di un prefisso "a-" sui campi di stato velocità e duplex.

Visualizzare lo stato duplex della porta 1/1 sullo switch B.

Comprendere l'errore di corrispondenza duplex.

Comprendere i messaggi di errore Spanning Tree.

Modificare la modalità duplex su half sulla porta 1/1 dello switch A.

Impostare la modalità duplex e la velocità della porta 1/1 sullo switch B.

Ripristinare la modalità duplex predefinita e la velocità sulle porte 1/1 su entrambi gli switch.

Visualizzare le modifiche dello stato della porta su entrambi gli switch.

Procedura dettagliata

Attenersi alla procedura seguente:

Il comando **show port capabilities 1/1** consente la visualizzazione di una porta Ethernet 10/100BaseTX 1/1 sullo switch A.

Immettere questo comando per entrambe le porte per le quali si desidera risolvere il problema. Entrambe le porte devono supportare le funzionalità duplex e di velocità mostrate se si prevede che utilizzino la negoziazione automatica.

```
Switch-A> (enable) show port capabilities 1/1
Model WS-X5530
Port 1/1
Type 10/100BaseTX
Speed auto,10,100
Duplex half, full
```

La negoziazione automatica è configurata per entrambe le funzionalità di velocità e modalità duplex sulla porta 1/1 di entrambi gli switch se si immette il comando **set port speed 1/1 auto** (l'impostazione predefinita per le porte che supportano la negoziazione automatica).

```
Switch-A> (enable) set port speed 1/1 auto
Port(s) 1/1 speed set to auto detect.
Switch-A (enable)
```

Nota: il comando **set port speed {num_mod/num_porta} auto** imposta anche la modalità duplex su Auto. Il comando set port duplex {num_mod/num_porta} auto non è disponibile.

Il comando **show port 1/1** visualizza lo stato delle porte 1/1 sugli switch A e B.

```
Switch-A> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- -----
 1/1               connected  1          normal a-full a-100 10/100BaseTX

Switch-B> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- -----
 1/1               connected  1          normal a-full a-100 10/100BaseTX
```

Notare che la maggior parte dell'output normale del comando **show port {num_mod/num_porta}** è stata omessa.

I prefissi "a-" di "full" e "100" indicano che questa porta non è stata hardcoded (configurata) per una modalità duplex o una velocità specifica. Pertanto, può negoziare automaticamente la modalità duplex e la velocità se anche il dispositivo a cui è connesso (partner del collegamento) può negoziare automaticamente la modalità duplex e la velocità. Notare anche che lo stato è "connected" (connesso) su entrambe le porte, ossia è stato rilevato un impulso di collegamento dall'altra porta. Lo stato può essere "connected" (connesso) anche se il duplex è stato negoziato in modo errato o non configurato correttamente.

Per dimostrare che cosa succede quando un partner del collegamento esegue la negoziazione automatica e l'altro no, la velocità sulla porta 1/1 nello switch A è impostata su 10 MB con il comando **set port speed 1/1 10**.

```
Switch-A> (enable) set port speed 1/1 10
Port(s) 1/1 speed set to 10Mbps.
Switch-A> (enable)
```

Nota: se si specifica la velocità su una porta, tutte le funzionalità di negoziazione automatica vengono disabilitate sulla porta per la velocità e il duplex.

Quando una porta è stata configurata per una velocità, la relativa modalità duplex viene configurata automaticamente per la modalità negoziata in precedenza. In questo caso, la modalità full duplex. Quando si immette il comando **set port speed 1/1 10**, la modalità duplex sulla porta 1/1 è configurata come se sia stato immesso anche il comando **set port duplex 1/1 full**. Questo viene spiegato di seguito.

Comprendere il significato di un prefisso "a-" nei campi di stato duplex e velocità.

L'assenza del prefisso "a-" nei campi di stato dell'output del comando **show port 1/1** sullo switch A indica che la modalità duplex è ora configurata per "full" e la velocità è ora configurata per "10".

```
Switch-A> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal  full  10    10/100BaseTX
```

Il comando **show port 1/1** sullo switch B indica che la porta ora funziona nella modalità half-duplex e 10 MB.

```
Switch-B> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal a-half a-10  10/100BaseTX
```

Questa procedura mostra che è possibile per un partner del collegamento rilevare la velocità a cui opera l'altro partner, anche se quest'ultimo non è configurato per la negoziazione automatica. Rilevando il tipo di segnale elettrico che arriva a scoprire se è 10Mb o 100Mb fa

questo. In questo modo lo switch B ha determinato che la porta 1/1 deve funzionare a 10 MB.

Non è possibile rilevare la modalità duplex corretta nello stesso modo in cui è possibile rilevare la velocità corretta. In questo caso, se la porta 1/1 dello switch B è configurata per la negoziazione automatica e la porta dello switch A no, la porta 1/1 dello switch B è stata costretta a selezionare la modalità duplex predefinita. Nelle porte Catalyst Ethernet, la modalità predefinita è la negoziazione automatica e, se la negoziazione automatica non ha esito positivo, la modalità half-duplex.

Questo esempio mostra anche che è possibile connettere un collegamento in caso di mancata corrispondenza nelle modalità duplex. La porta 1/1 sullo switch A è configurata per full duplex mentre l'impostazione predefinita per la porta 1/1 sullo switch B è half-duplex. Per evitare questo problema, configurare sempre entrambi i partner di collegamento.

Il prefisso "a-" nei campi di stato duplex e velocità non sempre indica che il comportamento corrente è stato negoziato. A volte significa solo che la porta non è stata configurata per una velocità o una modalità duplex. L'output precedente dello switch B mostra il duplex come "a-half" e la velocità come "a-10", a indicare che la porta funziona a 10 MB in modalità half-duplex. In questo esempio, il partner di collegamento su questa porta (porta 1/1 sullo switch A) è configurato per "full" e "10MB". Non è stato possibile eseguire la negoziazione automatica del comportamento corrente della porta 1/1 sullo switch B. Ciò dimostra che il prefisso "a-" indica esclusivamente la possibilità di eseguire la negoziazione automatica, ma non che questa sia stata effettivamente eseguita.

Comprendere il messaggio di errore Mancata corrispondenza duplex.

Questo messaggio relativo a una mancata corrispondenza della modalità duplex viene visualizzato sullo switch A dopo che la velocità sulla porta 1/1 è stata modificata a 10MB. La mancata corrispondenza è stata causata dalla porta 1/1 dello switch B, che per impostazione predefinita è half-duplex perché ha rilevato che il relativo partner di collegamento non può più eseguire la negoziazione automatica.

```
%CDP-4-DUPLEXMISMATCH:Full/half-duplex mismatch detected o1
```

Èimportante notare che questo messaggio viene creato dal Cisco Discovery Protocol (CDP), non dal protocollo di negoziazione automatica 802.3. Il protocollo CDP può segnalare i problemi individuati ma in genere non li corregge automaticamente. Una mancata corrispondenza duplex può causare o non può generare un messaggio di errore. Un'altra indicazione di una mancata corrispondenza duplex è il rapido aumento di errori di allineamento e FCS sul lato half-duplex e "runt" sulla porta full-duplex (come mostrato in una **porta sh {num_mod/num_porta}**).

Comprendere i messaggi Spanning Tree.

Oltre al messaggio di errore di mancata corrispondenza duplex, è possibile visualizzare questi messaggi Spanning Tree quando si modifica la velocità su un collegamento. La trattazione di Spanning Tree esula tuttavia dalle finalità di questo documento. Per ulteriori informazioni sullo Spanning Tree, fare riferimento al capitolo relativo.

```
%PAGP-5-PORTFROMSTP:Port 1/1 left bridge port 1/1
%PAGP-5-PORTTOSTP:Port 1/1 joined bridge port 1/1
```

Per dimostrare che cosa succede quando è stata configurata la modalità duplex, la modalità sulla porta 1/1 nello switch A è impostata su half con il comando **set port duplex 1/1 half**.

```
Switch-A> (enable) set port duplex 1/1 half
Port(s) 1/1 set to half-duplex.
Switch-A> (enable)
```

Il comando **show port 1/1** mostra la modifica nella modalità duplex su questa porta.

```
Switch-A> (enable) sh port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal half   10    10/100BaseTX
```

A questo punto, le porte 1/1 su entrambi gli switch funzionano in modalità half-duplex. La porta 1/1 sullo switch B è ancora configurata per la negoziazione automatica, come mostrato in questo output del comando **show port 1/1**.

```
Switch-B> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal a-half a-10  10/100BaseTX
```

Questo passaggio mostra come configurare la modalità duplex sulla porta 1/1 nello switch B su half. Questa impostazione è coerente con la policy consigliata per configurare entrambi i partner di collegamento allo stesso modo.

Per implementare la policy in modo da configurare entrambi i partner di collegamento con lo stesso comportamento, questa procedura ora imposta la modalità duplex su half e la velocità a 10 sulla porta 1/1 nello switch B.

Di seguito viene riportato l'output del comando **set port duplex 1/1 half** sullo switch B:

```
Switch-B> (enable) set port duplex 1/1 half
Port 1/1 is in auto-sensing mode.
Switch-B> (enable)
```

Il comando **set port duplex 1/1 half** non è riuscito perché non è valido se è abilitata la negoziazione automatica. Ciò significa anche che questo comando non disabilita la negoziazione automatica. La negoziazione automatica può essere disabilitata solo con il comando **set port speed {num_mod/num_porta {10 | 100} }**.

Di seguito viene riportato l'output del comando **set port speed 1/1 10** sullo switch B:

```
Switch-B> (enable) set port speed 1/1 10
Port(s) 1/1 speed set to 10Mbps.
Switch-B> (enable)
```

A questo punto, il comando **set port duplex 1/1 half** sullo switch B funziona:

```
Switch-A> (enable) set port duplex 1/1 half
Port(s) 1/1 set to half-duplex.
Switch-A> (enable)
```

Il comando **show port 1/1** sullo switch B mostra che le porte sono ora configurate per half-duplex e 10 MB.

```
Switch-B> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal half   10    10/100BaseTX
```

> **Nota**: **set port duplex {num_mod/num_porta {half | full }}** dipende dal comando **set port speed {num_mod/num_porta {10 | 100 }}**. In altre parole, è necessario impostare la velocità prima di poter impostare la modalità duplex.

Configurare le porte 1/1 su entrambi gli switch per la negoziazione automatica con il comando **set speed 1/1 auto**.

```
Switch-A> (enable) set port speed 1/1 auto
Port(s) 1/1 speed set to auto detect.
Switch-A> (enable)
```

> **Nota**: se la modalità duplex di una porta è stata configurata in modo diverso da auto, l'unico modo per configurare la porta in modo che venga rilevata automaticamente la modalità duplex è tramite il comando **set port speed { num_mod/num_porta}**. Il comando set port duplex {num_mod/num_porta} auto non è disponibile. In altre parole, se si esegue **il comando set port speed {num_mod/num_porta} auto**, vengono reimpostati il rilevamento velocità e modalità duplex delle porte su auto.

Esaminare lo stato delle porte 1/1 su entrambi gli switch con il comando **show port 1/1**.

```
Switch-A> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal a-full a-100 10/100BaseTX
Switch-B> (enable) show port 1/1
```

```
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal a-full a-100 10/100BaseTX
```

Entrambe le porte sono ora impostate sul comportamento predefinito della negoziazione automatica. Entrambe le porte hanno negoziato la modalità full duplex e 100 MB.

Prima di chiamare il team di supporto tecnico di Cisco Systems

Prima di chiamare il sito Web del supporto tecnico dei sistemi Cisco, accertarsi di aver letto questo articolo e di aver completato le azioni suggerite per i problemi del sistema. Inoltre, documenta i risultati in modo che Cisco possa assisterti meglio:

Acquisire l'output **di show** version da tutti i dispositivi interessati.

Acquisire l'output di **show port num_mod/num_porta** da tutte le porte interessate.

Acquisire l'output delle funzionalità **show port num_mod/num_porta** da tutte le porte interessate.

Configurazione delle connessioni tra switch e switch EtherChannel sugli switch Catalyst 4000/5000/6000

EtherChannel permette di associare più collegamenti Fast Ethernet o Gigabit Ethernet fisici in un unico canale logico. Questo consente al traffico tra i collegamenti di caricare la condivisione nel canale, nonché la ridondanza in caso di errore di uno o più collegamenti nel canale. EtherChannel può essere utilizzato per interconnettere switch LAN, router, server e client tramite cablaggio UTP (Unshielded Twisted-Pair) o fibra monomodale e multimodale.

EtherChannel è un modo semplice per aggregare la larghezza di banda tra dispositivi di rete critici. Su Catalyst 5000, è possibile creare un canale da due porte che lo rendono un collegamento a 200 Mbps (full-duplex 400 Mbps) o da quattro porte che lo rendono un collegamento a 400 Mbps (full-duplex 800 Mbps). Alcune schede e piattaforme supportano anche Gigabit EtherChannel e possono utilizzare da due a otto porte in un EtherChannel. Il concetto è lo stesso indipendentemente dalla velocità o dal numero di collegamenti coinvolti. Normalmente il protocollo STP (Spanning Tree Protocol) considera questi collegamenti ridondanti tra due dispositivi come loop e imposta i collegamenti ridondanti sulla modalità di blocco. In questo modo, questi collegamenti diventano effettivamente inattivi (in quanto forniscono solo funzionalità di backup se il collegamento principale non riesce). Quando si usa Cisco IOS 3.1.1 o versione successiva, lo Spanning Tree tratta il canale come un unico grande collegamento, quindi tutte le porte nel canale possono essere attive contemporaneamente.

In questa sezione vengono illustrati i passaggi per configurare EtherChannel tra due switch Catalyst 5000 e vengono mostrati i risultati dei comandi quando vengono eseguiti. Negli scenari presentati in questo documento, è possibile usare gli switch Catalyst 4000 e 6000 per ottenere gli stessi risultati. Per Catalyst 2900XL e 1900/2820, la sintassi del comando è diversa, ma i concetti di EtherChannel sono gli stessi.

EtherChannel può essere configurato manualmente se si immettono i comandi appropriati o automaticamente se lo switch negozia il canale con l'altro lato con il protocollo PAgP (Port Aggregation Protocol). Si consiglia di utilizzare la modalità PAgP desiderabile per configurare EtherChannel quando possibile, in quanto la configurazione manuale di EtherChannel può creare alcune complicazioni. Questo documento offre esempi su come configurare EtherChannel manualmente e esempi su come configurare EtherChannel con PAgP. Sono inoltre incluse la risoluzione dei problemi relativi a EtherChannel e l'utilizzo del trunking con EtherChannel. In questo documento, i termini EtherChannel, Fast EtherChannel, Gigabit EtherChannel o channel si riferiscono tutti a EtherChannel.

Sommario

Nella figura viene illustrato l'ambiente di test. La configurazione degli switch è stata cancellata con il comando **clear config all**. Quindi, il prompt è stato modificato con il **nome di sistema impostato**. Allo switch sono stati assegnati un indirizzo IP e una maschera a scopo di gestione con **int sc0 172.16.84.6 255.255.255.0** per lo switch A e **int sc0 172.16.84.17 255.255.255.0< /strong>per lo switch B. Un gateway predefinito è stato assegnato a entrambi gli switch con il valore predefinito della route ip 172.16.84.1 .**

Le configurazioni dello switch sono state cancellate in modo che partissero dalle condizioni predefinite. Agli switch sono stati assegnati nomi per identificarli dal prompt sulla riga di comando. Gli indirizzi IP sono stati assegnati in modo da poter eseguire il ping tra gli switch per verificarli. Il gateway predefinito non è stato utilizzato.Molti comandi visualizzano più output del necessario. L'output estraneo viene eliminato da questo documento.

Attività per la configurazione manuale di EtherChannel

Questa è una sintesi delle istruzioni per configurare manualmente EtherChannel:

- Mostra la versione e i moduli Cisco IOS utilizzati in questo documento.
- Verificare che EtherChannel sia supportato sulle porte.
- Verificare che le porte siano connesse e operative.

Verificare che le porte da raggruppare abbiano le stesse impostazioni.

Identificare I Gruppi Di Porte Validi.

Creare il canale.

Procedura dettagliataDi seguito viene riportata la procedura per configurare manualmente EtherChannel.

Per visualizzare la versione software in esecuzione sullo switch, usare il comando show version. Il comando show moduleelenca i moduli installati nello switch.

```
Switch-A show version
WS-C5505 Software, Version McpSW: 4.5(1) NmpSW: 4.5(1)
Copyright (c) 1995-1999 by Cisco Systems
?

Switch-A show module
Mod Module-Name          Ports Module-Type            Model    Serial-Num Status
--- -------------------- ----- ---------------------- --------- --------- -------
1                        0     Supervisor III         WS-X5530  006841805 ok
2                        24    10/100BaseTX Ethernet  WS-X5225R 012785227 ok
?
```

Verificare che EtherChannel sia supportato sulle porte. Le funzionalità show port sono disponibili nelle versioni 4.x e successive. Se la versione di Cisco IOS in uso è precedente alla 4.x, ignorare questo passaggio. Non tutti i moduli Fast Ethernet supportano EtherChannel. Alcuni dei moduli EtherChannel originali hanno la scritta "Fast EtherChannel" nell'angolo in basso a sinistra del modulo (rivolto verso lo switch), a indicare che la funzione è supportata. Questa convenzione è stata abbandonata nei moduli successivi. I moduli di questo test non dicono "Fast EtherChannel" su di loro, ma supportano la funzione.

```
Switch-A show port capabilities
Model                    WS-X5225R
Port                     2/1
Type                     10/100BaseTX
Speed                    auto,10,100
Duplex                   half,full
Trunk encap type         802.1Q,ISL
Trunk mode               on,off,desirable,auto,nonegotiate
Channel                  2/1-2,2/1-4
Broadcast suppression    percentage(0-100)
Flow control             receive-(off,on),send-(off,on)
Security                 yes
```

```
Membership               static,dynamic
Fast start               yes
Rewrite                  yes
Switch-B show port capabilities
Model                    WS-X5234
Port                     2/1
Type                     10/100BaseTX
Speed                    auto,10,100
Duplex                   half,full
Trunk encap type         802.1Q,ISL
Trunk mode               on,off,desirable,auto,nonegotiate
Channel                  2/1-2,2/1-4
Broadcast suppression    percentage(0-100)
Flow control             receive-(off,on),send-(off,on)
Security                 yes
Membership               static,dynamic
Fast start               yes
Rewrite                  no
```

Una porta che non supporta EtherChannel è simile alla seguente:

```
Switch show port capabilities
Model                    WS-X5213A
Port                     2/1
Type                     10/100BaseTX
Speed                    10,100,auto
Duplex                   half,full
Trunk encap type         ISL
Trunk mode               on,off,desirable,auto,nonegotiate
Channel                  no
Broadcast suppression    pps(0-150000)
Flow control             no
Security                 yes
Membership               static,dynamic
Fast start               yes
```

Verificare che le porte siano connesse e operative. Prima di collegare i cavi, questo è lo stato della porta.

```
Switch-A show port
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                     notconnect 1          normal   auto  auto 10/100BaseTX
 2/2                     notconnect 1          normal   auto  auto 10/100BaseTX
 2/3                     notconnect 1          normal   auto  auto 10/100BaseTX
 2/4                     notconnect 1          normal   auto  auto 10/100BaseTX
```

Dopo aver collegato i cavi tra i due switch, questo è lo stato.

```
1999 Dec 14 20:32:44 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
1999 Dec 14 20:32:44 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/2
1999 Dec 14 20:32:44 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/3
1999 Dec 14 20:32:44 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/4

Switch-A show port
Port  Name                 Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                      connected  1          normal a-full a-100 10/100BaseTX
 2/2                      connected  1          normal a-full a-100 10/100BaseTX
 2/3                      connected  1          normal a-full a-100 10/100BaseTX
 2/4                      connected  1          normal a-full a-100 10/100BaseTX
Switch-B show port
Port  Name                 Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                      connected  1          normal a-full a-100 10/100BaseTX
 2/2                      connected  1          normal a-full a-100 10/100BaseTX
 2/3                      connected  1          normal a-full a-100 10/100BaseTX
 2/4                      connected  1          normal a-full a-100 10/100BaseTX
```

Poiché le configurazioni dello switch sono state cancellate prima dell'inizio del test, le porte sono nelle condizioni predefinite. Si trovano tutti nella vlan1 e la velocità e la modalità duplex sono impostate su auto. Dopo la connessione dei cavi, vengono negoziati a una velocità di 100 Mbps e full duplex. Lo stato è connected (connesso), quindi è possibile eseguire il ping sull'altro switch.

```
Switch-A ping 172.16.84.17
172.16.84.17 is alive
```

In una rete, è possibile impostare manualmente le velocità a 100 Mbps e full duplex anziché ricorrere alla negoziazione automatica, in quanto probabilmente si desidera che le porte funzionino sempre alla velocità più elevata. Per una discussione sulla negoziazione automatica, vedere la sezione Risoluzione dei problemi di negoziazione automatica Ethernet 10/100 MB Half/Half/Full Duplex.

Verificare che le porte da raggruppare abbiano le stesse impostazioni. Si tratta di un punto importante che viene trattato in modo più dettagliato nella sezione relativa alla risoluzione dei problemi. Se il comando per configurare EtherChannel non funziona, in genere è perché le porte coinvolte nel canale hanno configurazioni diverse. incluse le porte dall'altro lato del collegamento e le porte locali. In questo caso, poiché le configurazioni dello switch sono state cancellate prima dell'avvio del test, le porte sono nelle condizioni predefinite. si trovano tutti nella vlan1; la velocità e la modalità duplex sono impostate su auto e tutti i parametri dello spanning tree per ciascuna porta sono impostati sullo stesso valore. Come si può notare dall'output, dopo la connessione dei cavi le porte eseguono la negoziazione a una velocità di 100 Mbps e full duplex. Poiché lo Spanning Tree viene eseguito su ciascuna

VLAN, è più facile configurare il canale e rispondere ai messaggi di errore piuttosto che cercare di controllare ogni campo dello Spanning Tree per verificare la coerenza su ciascuna porta e VLAN nel canale.

Identificare gruppi di porte validi. Su Catalyst 5000, solo alcune porte possono essere unite in un canale. Queste dipendenze restrittive non si applicano a tutte le piattaforme. Le porte di un canale su Catalyst 5000 devono essere contigue. Il comando show port capabilities restituisce le possibili combinazioni della porta 2/1:

```
Switch-A show port capabilities
Model                     WS-X5225R
Port                      2/1
Channel                   2/1-2,2/1-4
```

Si noti che questa porta può essere parte di un gruppo di due (2/1-2) o parte di un gruppo di quattro (2/1-4). Nel modulo è presente un componente denominato Ethernet Bundling Controller (EBC) che causa queste limitazioni di configurazione. Guardate un'altra porta.

```
Switch-A show port capabilities 2/3
Model                     WS-X5225R
Port                      2/3
Channel                   2/3-4,2/1-4
```

Questa porta può essere raggruppata in un gruppo di due porte (2/3-4) o in un gruppo di quattro (2/1-4).

Nota: a seconda dell'hardware, possono esistere ulteriori restrizioni. Su alcuni moduli (WS-X5201 e WS-X5203), non è possibile formare un EtherChannel con le ultime due porte in un "gruppo di porte" a meno che le prime due porte del gruppo non formino già un EtherChannel. Un "gruppo di porte" è un gruppo di porte a cui è consentito formare un EtherChannel (in questo esempio 2/1-4 è un gruppo di porte). Ad esempio, se si creano EtherChannel separati con solo due porte in un canale, non sarà possibile assegnare le porte 2/3-4 a un canale fino a quando le porte 2/1-2 non sono state configurate per un canale, per i moduli con questa restrizione. Analogamente, prima di configurare le porte 2/6-7, è necessario configurare le porte 2/5-6. Questa restrizione non si verifica sui moduli utilizzati per questo documento (WS-X5225R, WS-X5234).

Poiché si configura un gruppo di quattro porte (2/1-4), questo rientra nel raggruppamento approvato. non è possibile assegnare un gruppo di quattro alle porte 2/3-6. Questo è un gruppo di porte contigue, ma non iniziano sul limite approvato, come mostrato dal comando show port capabilities (i gruppi validi sono le porte 1-4, 5-8, 9-12, 13-16, 17-20, 21-24).

Creare il canale. Per creare il canale, usare il comando set port channel <mod/porta on per ciascuno switch. si consiglia di disattivare le porte su un lato del canale o sull'altro lato con il comando set port disable prima di attivare EtherChannel manualmente. In questo modo si evitano possibili problemi con lo Spanning Tree all'interno del processo di configurazione. Lo Spanning Tree può disattivare alcune porte (con stato "errdisable") se un lato è configurato come canale prima che l'altro lato possa essere configurato come canale. A causa di questa possibilità, è molto più facile creare EtherChannels con PAgP, come spiegato più avanti in

questo documento. Per evitare questa situazione quando EtherChannel viene configurato manualmente, disabilitare le porte sullo switch A, configurare il canale sullo switch A, configurare il canale sullo switch B e quindi riabilitare le porte sullo switch A.

Verificare innanzitutto che il channeling *sia disattivato*.

```
Switch-A (enable) show port channel
No ports channelling
Switch-B (enable) show port channel
No ports channelling
```

A questo punto, disabilitare le porte sullo switch A finché entrambi gli switch non sono stati configurati per EtherChannel in modo che lo Spanning Tree non generi errori e arresti le porte.

```
Switch-A (enable) set port disable 2/1-4
Ports 2/1-4 disabled.
[output from SwitchA upon disabling ports]
1999 Dec 15 00:06:40 %PAGP-5-PORTFROMSTP:Port 2/1 left bridg1
1999 Dec 15 00:06:40 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
1999 Dec 15 00:06:40 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 15 00:06:40 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
```

Attivare la modalità canale per lo switch A.

```
Switch-A (enable) set port channel 2/1-4 on
Port(s) 2/1-4 channel mode set to on.
```

Controllare lo stato del canale. Si noti che la modalità canale è stata impostata *su*, ma lo stato delle porte è disabilitato (perché la modalità è stata disabilitata in precedenza). A questo punto, il canale non è operativo, ma diventa operativo quando le porte sono abilitate.

```
Switch-A (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  disabled   on        channel
 2/2  disabled   on        channel
 2/3  disabled   on        channel
 2/4  disabled   on        channel
----- ---------- --------- ----------- ------------------------- ----------
```

Poiché le porte dello switch A sono state (temporaneamente) disabilitate, le porte dello switch B non sono più collegate. Questo messaggio viene visualizzato sulla console dello switch B quando le porte dello switch A sono state disabilitate.

```
Switch-B (enable)
2000 Jan 13 22:30:03 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
2000 Jan 13 22:30:04 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
2000 Jan 13 22:30:04 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
2000 Jan 13 22:30:04 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
```

Accendere il canale dello switch B.

```
Switch-B (enable) set port channel 2/1-4 on
Port(s) 2/1-4 channel mode set to on.
```

Verificare che la modalità canale sia attiva per lo switch B.

```
Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  notconnect on        channel
 2/2  notconnect on        channel
 2/3  notconnect on        channel
 2/4  notconnect on        channel
----- ---------- --------- ----------- ------------------------- ----------
```

Si noti che la modalità del canale per lo switch B è attiva, ma lo stato delle porte *non è connect*. Infatti, le porte dello switch A sono ancora disabilitate.

Infine, l'ultimo passaggio consiste nell'abilitare le porte sullo switch A.

```
Switch-A (enable) set port enable 2/1-4
Ports 2/1-4 enabled.
1999 Dec 15 00:08:40 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
1999 Dec 15 00:08:40 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
1999 Dec 15 00:08:40 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
1999 Dec 15 00:08:40 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4
```

Verifica della configurazionePer verificare che il canale sia impostato correttamente, eseguire il comando show port channel.

```
Switch-A (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  on        channel     WS-C5505    066509957(Sw  2/1
 2/2  connected  on        channel     WS-C5505    066509957(Sw  2/2
```

```
 2/3  connected  on        channel     WS-C5505    066509957(Sw  2/3
 2/4  connected  on        channel     WS-C5505    066509957(Sw  2/4
----- ---------- --------- ----------- ------------------------ ----------

Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                 Neighbor
                 mode      status      device                   port
----- ---------- --------- ----------- ------------------------ ----------
 2/1  connected  on        channel     WS-C5505    066507453(Sw  2/1
 2/2  connected  on        channel     WS-C5505    066507453(Sw  2/2
 2/3  connected  on        channel     WS-C5505    066507453(Sw  2/3
 2/4  connected  on        channel     WS-C5505    066507453(Sw  2/4
----- ---------- --------- ----------- ------------------------ ----------
```

In questo comando, lo Spanning Tree considera le porte come una porta logica. Quando la porta è elencata come*2/1-4*, lo spanning tree gestisce le porte 2/1, 2/2, 2/3 e 2/4 *come una porta*.

```
Switch-A (enable) show spantree
VLAN 1
Spanning tree enabled
Spanning tree type          ieee

Designated Root             00-10-0d-b2-8c-00
Designated Root Priority    32768
Designated Root Cost        8
Designated Root Port        2/1-4
Root Max Age   20 sec    Hello Time 2  sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-90-92-b0-84-00
Bridge ID Priority          32768
Bridge Max Age 20 sec    Hello Time 2  sec   Forward Delay 15 sec

Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-Method
--------- ----  -------------  -----  --------  ----------  ------------
 2/1-4    1     forwarding         8        32   disabled       channel
```

EtherChannel può essere implementato con diversi modi di distribuzione del traffico sulle porte di un canale. La specifica EtherChannel non determina la modalità di distribuzione del traffico sui collegamenti di un canale. Catalyst 5000 usa l'ultimo bit o gli ultimi due bit (a seconda del numero di collegamenti presenti nel canale) degli indirizzi MAC di origine e destinazione nel frame per determinare la porta nel canale da usare. È possibile vedere quantità di traffico simili su ciascuna delle porte del canale se il traffico è generato da una normale distribuzione di indirizzi MAC su un lato del canale o sull'altro. Per verificare che il traffico attraversi tutte le porte del canale, è possibile utilizzare il comando show macro. Se le porte erano attive prima di configurare EtherChannel, è possibile ripristinare i contatori del traffico a zero con il comando clear counterscommand e quindi i valori del traffico rappresentano la modalità con cui EtherChannel ha distribuito il traffico.In questo ambiente di test non è stata ottenuta una distribuzione reale perché non esistono workstation, server o router che generano traffico. Gli unici dispositivi che generano traffico sono gli switch stessi. Sono stati emessi alcuni ping tra lo switch A e lo switch B ed è possibile verificare che il traffico unicast utilizza la prima porta del canale. In questo caso, le informazioni di ricezione (RCV-Unicast) mostrano come lo switch B ha distribuito il traffico sullo switch A attraverso il canale. Un po' più in basso nell'output, le informazioni di trasmissione (Xmit-Unicast) mostrano come lo switch A ha distribuito il traffico attraverso il canale allo switch B. Si nota anche che una piccola quantità di traffico multicast generato dallo switch (ISL dinamico, CDP) si spegne su tutte e quattro le porte. I pacchetti broadcast sono query ARP (per il gateway predefinito che non esiste qui). Se le postazioni di lavoro inviano i pacchetti tramite lo switch a una destinazione sull'altro lato del canale, il traffico dovrebbe attraversare ciascuno dei quattro collegamenti del canale. È possibile monitorare la distribuzione dei pacchetti nella propria rete con il comando show macc.

```
Switch-A (enable) clear counters

This command will reset all MAC and port counters reported in CLI and SNMP.

Do you want to continue (y/n) [n]? y

MAC and Port counters cleared.

Switch-A (enable) show mac


Port      Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast

-------- -------------------- -------------------- --------------------

 2/1                        9                  320                  183

 2/2                        0                   51                    0

 2/3                        0                   47                    0

 2/4                        0                   47                    0
```

```
(...)

Port      Xmit-Unicast         Xmit-Multicast       Xmit-Broadcast
--------  -------------------- -------------------- --------------------
 2/1                        8                   47                  184
 2/2                        0                   47                    0
 2/3                        0                   47                    0
 2/4                        0                   47                    0
(...)

Port      Rcv-Octet            Xmit-Octet
--------  -------------------- --------------------
 2/1                    35176                17443
 2/2                     5304                 4851
 2/3                     5048                 4851
 2/4                     5048                 4851
(...)

Last-Time-Cleared
-------------------------
Wed Dec 15 1999, 01:05:33
```

Uso di PAgP per configurare EtherChannel (metodo preferito)

Il protocollo PAgP (Port Aggregation Protocol) semplifica la creazione automatica di collegamenti EtherChannel con lo scambio di pacchetti tra porte che supportano il canale. Il protocollo apprende le funzionalità dei gruppi di porte in modo dinamico e informa le porte vicine.Una volta che PAgP identifica i collegamenti con capacità di canale accoppiati correttamente, raggruppa le porte in un canale. Il canale viene quindi aggiunto allo Spanning Tree come una singola porta bridge. Un determinato pacchetto multicast o broadcast in uscita viene trasmesso su una sola porta del canale, non su tutte le porte del canale. Inoltre, i pacchetti broadcast e multicast in uscita trasmessi su una porta di un canale non possono essere restituiti su altre porte del canale.Sono disponibili quattro modalità di canale configurabili dall'utente: on, off, auto e desired. I pacchetti PAgP vengono scambiati solo tra le porte in modalità automatica e desiderabile. Le porte configurate in modalità inonoroffmode non scambiano pacchetti PAgP. Per configurare gli switch che si desidera creare

ed EtherChannel, è necessario impostare entrambi gli switch su desiderablemode. Questo fornisce il comportamento più affidabile quando una delle due parti incontra situazioni di errore o viene reimpostata. La modalità predefinita del canale è auto.Entrambe le modalità, automatiche e auspicabili, consentono alle porte di negoziare con le porte connesse per determinare se possono formare un canale in base a criteri quali velocità della porta, stato di trunking, VLAN nativa e così via.Le porte possono formare un EtherChannel quando si trovano in modalità canali diverse, a condizione che le modalità siano compatibili:

Una modalità di indicizzazione della porta può formare EtherChannel in modo corretto con un'altra porta indicizzabile o automatizzata.

Una porta in modalità automatica può formare un EtherChannel con un'altra modalità di porta non accessibile.

Una porta inautomode non può formare EtherChannel con un'altra porta anch'essa inautomode poiché nessuna porta avvia la negoziazione.

Una porta in modalità inon può formare un canale solo con una porta in modalità inon perché le porte in modalità inon non scambiano pacchetti PAgP.

Una porta in modalità offline non forma un canale con nessuna porta.

Quando si utilizza EtherChannel, se viene visualizzato un messaggio "SPANTREE-2: Channel misconfig - x/x-x will be disabled" o un messaggio syslog simile, indica una mancata corrispondenza delle modalità EtherChannel sulle porte connesse. È consigliabile correggere la configurazione e riattivare le porte con il comando set port enable. Le configurazioni EtherChannel valide includono:Tabella 22-5: configurazioni EtherChannel valide

Modalità Port-channel	Modalità canali porte adiacenti valide
desirable	desiderabile o automatico
auto (predefinito)	desiderabile o automatico[1]
on	on
Disattivato	Disattivato

[1]Se le porte locale e adiacente sono in modalità automatica, non viene creato un bundle EtherChannel.Di seguito è riportato un riepilogo di tutti i possibili scenari della modalità di channeling. Alcune di queste combinazioni possono causare lo spanning tree in modo che le porte sul lato del channeling vengano disabilitate (ovvero arrestate).Tabella 22-6: scenari della modalità channeling

Modalità canale switch A	Modalità canale switch-B	Stato canale
On	On	Canale

On	Spento	Non canale (errdisable)
On	Auto	Non canale (errdisable)
On	Desirable	Non canale (errdisable)
Spento	On	Non canale (errdisable)
Spento	Spento	Non canale
Spento	Auto	Non canale
Spento	Desirable	Non canale
Auto	On	Non canale (errdisable)
Auto	Spento	Non canale
Auto	Auto	Non canale
Auto	Desirable	Canale
Desirable	On	Non canale (errdisable)
Desirable	Spento	Non canale
Desirable	Auto	Canale
Desirable	Desirable	Canale

Il canale è stato disattivato dall'esempio precedente con questo comando sullo switch A e sullo switch B.

```
Switch-A (enable) set port channel 2/1-4 auto

Port(s) 2/1-4 channel mode set to auto.
```

La modalità del canale predefinita per una porta che può canalizzare è auto. Per verificare questa condizione, immettere questo comando:

```
Switch-A (enable) show port channel 2/1

Port  Status     Channel   Channel     Neighbor                 Neighbor
                 mode      status      device                   port
----- ---------- --------- ----------- ------------------------ ----------
 2/1  connected  auto      not channel
```

Il comando precedente mostra anche che al momento le porte non funzionano. Un altro modo per verificare lo stato del canale è questo.

```
Switch-A (enable) show port channel

No ports channelling

Switch-B (enable) show port channel
```

```
No ports channelling
```

Èmolto semplice far funzionare il canale con PAgP. A questo punto, entrambi gli switch sono impostati sulla modalità automatica, ossia si incanalano se una porta collegata invia una richiesta PAgP al canale. Se lo switch A è impostato su desiderato, lo switch A invia i pacchetti PAgP all'altro switch e chiede a quest'ultimo di inviare il canale.

```
Switch-A (enable) set port channel 2/1-4 desirable
Port(s) 2/1-4 channel mode set to desirable.
1999 Dec 15 22:03:18 %PAGP-5-PORTFROMSTP:Port 2/1 left bridg1
1999 Dec 15 22:03:18 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
1999 Dec 15 22:03:18 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 15 22:03:18 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
1999 Dec 15 22:03:19 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
1999 Dec 15 22:03:19 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 15 22:03:20 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
1999 Dec 15 22:03:23 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
1999 Dec 15 22:03:23 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
1999 Dec 15 22:03:23 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
1999 Dec 15 22:03:24 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4
```

Per visualizzare il canale, procedere come segue.

```
Switch-A (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------ ----------
 2/1  connected  desirable channel     WS-C5505    066509957(Sw  2/1
 2/2  connected  desirable channel     WS-C5505    066509957(Sw  2/2
 2/3  connected  desirable channel     WS-C5505    066509957(Sw  2/3
 2/4  connected  desirable channel     WS-C5505    066509957(Sw  2/4
----- ---------- --------- ----------- ------------------------ ----------
```

Poiché lo switch B era in modalità automatica, ha risposto ai pacchetti PAgP e ha creato un canale con lo switch A.

```
Switch-B (enable)
2000 Jan 14 20:26:41 %PAGP-5-PORTFROMSTP:Port 2/1 left bridg1
```

```
2000 Jan 14 20:26:41 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
2000 Jan 14 20:26:41 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
2000 Jan 14 20:26:41 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
2000 Jan 14 20:26:45 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
2000 Jan 14 20:26:45 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
2000 Jan 14 20:26:45 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
2000 Jan 14 20:26:47 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
2000 Jan 14 20:26:47 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
2000 Jan 14 20:26:47 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
2000 Jan 14 20:26:48 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4

Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  auto      channel     WS-C5505    066507453(Sw  2/1
 2/2  connected  auto      channel     WS-C5505    066507453(Sw  2/2
 2/3  connected  auto      channel     WS-C5505    066507453(Sw  2/3
 2/4  connected  auto      channel     WS-C5505    066507453(Sw  2/4
----- ---------- --------- ----------- ------------------------- ----------
```

Nota: si consiglia di impostare entrambi i lati del canale su desiderablabel in modo che entrambi provino ad avviare il canale se un lato si allontana. Se le porte EtherChannel sullo switch B vengono impostate su desiablemode, anche se il canale è attualmente attivo e in modalità automatica, non vi sono problemi. Questo è il comando.

```
Switch-B (enable) set port channel 2/1-4 desirable
Port(s) 2/1-4 channel mode set to desirable.

Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  desirable channel     WS-C5505    066507453(Sw  2/1
 2/2  connected  desirable channel     WS-C5505    066507453(Sw  2/2
```

```
 2/3  connected  desirable channel     WS-C5505    066507453(Sw  2/3
 2/4  connected  desirable channel     WS-C5505    066507453(Sw  2/4
----- ---------- --------- ---------- ------------------------ ----------
```

Ora, se lo switch A si interrompe per qualche motivo o se un nuovo hardware sostituisce lo switch A, lo switch B tenta di ristabilire il canale. Se la nuova apparecchiatura non è in grado di effettuare il canale, lo switch B tratta le proprie porte 2/1-4 come porte normali non raggruppate in un canale. Questo è uno dei vantaggi dell'utilizzo della modalità desiderabile. Se il canale è stato configurato con PAgP in modalità accesa e un lato della connessione presenta un errore o un reset, potrebbe verificarsi uno stato err-disabled (shutdown) sull'altro lato. Quando il protocollo PAgP è impostato sulla modalità desiderata su ciascun lato, il canale stabilizza e rinegozia la connessione EtherChannel.Trunking ed EtherChannelEtherChannel è indipendente dal trunking. È possibile attivare o disattivare il trunking. È inoltre possibile attivare il trunking per tutte le porte prima di creare il canale oppure dopo aver creato il canale (come si fa qui). Per quanto riguarda EtherChannel, non importa; trunking ed EtherChannel sono funzionalità completamente separate. Ciò che conta è che tutte le porte coinvolte si trovino nella stessa modalità: o sono tutte trunking prima di configurare il canale, o non sono trunking prima di configurare il canale. Tutte le porte devono essere nello stesso stato di trunking prima di creare il canale. Una volta formato un canale, qualsiasi modifica apportata a una porta viene estesa anche alle altre porte del canale. I moduli utilizzati in questo banco di prova possono eseguire il trunking ISL o 802.1q. Per impostazione predefinita, i moduli sono impostati sulla modalità di trunking automatico e di negoziazione, ovvero vengono trunk se l'altro lato richiede di eseguire il trunk e negoziano se utilizzare il metodo ISL o 802.1q per il trunking. Se non viene richiesto di eseguire il trunk, funzionano come porte normali non trunking.

```
Switch-A (enable) show trunk 2
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/1      auto         negotiate      not-trunking  1
 2/2      auto         negotiate      not-trunking  1
 2/3      auto         negotiate      not-trunking  1
 2/4      auto         negotiate      not-trunking  1
```

Esistono diversi modi per attivare il trunking. In questo esempio, lo switch A viene impostato su desiderabile. Lo switch A è già impostato per la negoziazione. La combinazione di opzioni desiderabili e negoziazione fa sì che lo switch A chieda allo switch B di eseguire il trunk e di

negoziare il tipo di trunking da eseguire (ISL o 802.1q). Poiché per impostazione predefinita lo switch B esegue la negoziazione automatica, lo switch B risponde alla richiesta dello switch A. Si verificano i seguenti risultati:

```
Switch-A (enable) set trunk 2/1 desirable

Port(s) 2/1-4 trunk mode set to desirable.

Switch-A (enable)

1999 Dec 18 20:46:25 %DTP-5-TRUNKPORTON:Port 2/1 has become isl trunk

1999 Dec 18 20:46:25 %DTP-5-TRUNKPORTON:Port 2/2 has become isl trunk

1999 Dec 18 20:46:25 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-4

1999 Dec 18 20:46:25 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/1-4

1999 Dec 18 20:46:25 %DTP-5-TRUNKPORTON:Port 2/3 has become isl trunk

1999 Dec 18 20:46:26 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/1-4

1999 Dec 18 20:46:26 %DTP-5-TRUNKPORTON:Port 2/4 has become isl trunk

1999 Dec 18 20:46:26 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/1-4

1999 Dec 18 20:46:28 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4

1999 Dec 18 20:46:29 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4

1999 Dec 18 20:46:29 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4

1999 Dec 18 20:46:29 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4


Switch-A (enable) show trunk 2

Port      Mode         Encapsulation  Status        Native vlan

--------  -----------  -------------  ------------  -----------

 2/1      desirable    n-isl          trunking      1

 2/2      desirable    n-isl          trunking      1

 2/3      desirable    n-isl          trunking      1

 2/4      desirable    n-isl          trunking      1
```

La modalità trunk è stata impostata su desiderabile. Di conseguenza, la modalità di trunking è stata negoziata con lo switch adiacente, che ha scelto ISL (n-isl). Lo stato corrente è in disuso. Questo è quello che è successo sullo switch B grazie al comando eseguito sullo switch A.

```
Switch-B (enable)

2000 Jan 17 19:09:52 %DTP-5-TRUNKPORTON:Port 2/1 has become isl trunk

2000 Jan 17 19:09:52 %DTP-5-TRUNKPORTON:Port 2/2 has become isl trunk

2000 Jan 17 19:09:52 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-4

2000 Jan 17 19:09:52 %DTP-5-TRUNKPORTON:Port 2/3 has become isl trunk
```

```
2000 Jan 17 19:09:52 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/1-4

2000 Jan 17 19:09:53 %DTP-5-TRUNKPORTON:Port 2/4 has become isl trunk

2000 Jan 17 19:09:53 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/1-4

2000 Jan 17 19:09:53 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/1-4

2000 Jan 17 19:09:55 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4

2000 Jan 17 19:09:55 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4

2000 Jan 17 19:09:55 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4

2000 Jan 17 19:09:55 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4


Switch-B (enable) show trunk 2

Port      Mode         Encapsulation  Status        Native vlan

--------  -----------  -------------  ------------  -----------

 2/1      auto         n-isl          trunking      1

 2/2      auto         n-isl          trunking      1

 2/3      auto         n-isl          trunking      1

 2/4      auto         n-isl          trunking      1
```

Si noti che tutte e quattro le porte (2/1-4) sono diventate trunk, anche se una sola porta (2/1) è stata modificata in modo specifico in desiderabile. Questo è un esempio di come la modifica di una porta nel canale influisca su tutte le porte.Risoluzione dei problemi di EtherChannelLe problematiche relative a EtherChannel possono essere suddivise in due aree principali: risolvere il problema nella fase di configurazione e risolvere il problema nella fase di esecuzione. Gli errori di configurazione in genere si verificano a causa di una mancata corrispondenza dei parametri sulle porte coinvolte (velocità diverse, duplex diverso, valori di porte Spanning Tree diversi e così via). Inoltre, è possibile generare errori all'interno della configurazione se si imposta il canale su un lato e si attende troppo tempo prima di configurare il canale sull'altro lato. In questo modo, lo spanning tree esegue loop che generano un errore e la porta viene chiusa.In caso di errore durante la configurazione di EtherChannel, verificare lo stato delle porte dopo aver corretto la situazione di errore di EtherChannel. Se lo stato della porta *è errdisable*, le porte sono state chiuse dal software e non possono essere riattivate finché non si immette il comando set port enable.Nota: se lo stato della porta *diventa errdisable*, è necessario abilitare specificamente le porte con il comando set port enable affinché diventino attive. Al momento, è possibile risolvere tutti i problemi di EtherChannel, ma le porte non vengono visualizzate o formano un canale finché non vengono riattivate! Nelle versioni future del sistema operativo è possibile verificare periodicamente se è necessario abilitare le porte disabilitate in errore.Per eseguire questi test, è necessario disattivare

il trunking e EtherChannel: parametri non corrispondenti, attendere troppo tempo prima di configurare l'altro lato, correggere lo stato err-disabled e visualizzare le conseguenze dell'interruzione e del ripristino di un collegamento.Parametri non corrispondentiDi seguito è riportato un esempio di parametri non corrispondenti. la porta 2/4 è stata impostata nella VLAN 2 mentre le altre porte sono ancora nella VLAN 1. Per creare una nuova VLAN, è necessario assegnare un dominio VTP per lo switch e creare la VLAN.

```
Switch-A (enable) show port channel

No ports channelling


Switch-A (enable) show port

Port  Name                 Status     Vlan       Level  Duplex Speed Type

----- ------------------ ---------- ---------- ------ ------ ----- ------------

 2/1                      connected  1          normal a-full a-100 10/100BaseTX

 2/2                      connected  1          normal a-full a-100 10/100BaseTX

 2/3                      connected  1          normal a-full a-100 10/100BaseTX

 2/4                      connected  1          normal a-full a-100 10/100BaseTX


Switch-A (enable) set vlan 2

Cannot add/modify VLANs on a VTP server without a domain name.


Switch-A (enable) set vtp domain testDomain

VTP domain testDomain modified


Switch-A (enable) set vlan 2 name vlan2

Vlan 2 configuration successful


Switch-A (enable) set vlan 2 2/4

VLAN 2 modified.

VLAN 1 modified.

VLAN  Mod/Ports

---- ----------------------

2     2/4


Switch-A (enable)

1999 Dec 19 00:19:34 %PAGP-5-PORTFROMSTP:Port 2/4 left bridg4
```

```
Switch-A (enable) show port
Port  Name                 Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                      connected  1          normal a-full a-100 10/100BaseTX
 2/2                      connected  1          normal a-full a-100 10/100BaseTX
 2/3                      connected  1          normal a-full a-100 10/100BaseTX
 2/4                      connected  2          normal a-full a-100 10/100BaseTX

Switch-A (enable) set port channel 2/1-4 desirable
Port(s) 2/1-4 channel mode set to desirable.

Switch-A (enable)
1999 Dec 19 00:20:19 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
1999 Dec 19 00:20:19 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
1999 Dec 19 00:20:19 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 19 00:20:20 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
1999 Dec 19 00:20:20 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
1999 Dec 19 00:20:22 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 19 00:20:22 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
1999 Dec 19 00:20:24 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-2
1999 Dec 19 00:20:25 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-2
1999 Dec 19 00:20:25 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/3
1999 Dec 19 00:20:25 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/4

Switch-A (enable) show port channel
Port  Status     Channel    Channel     Neighbor                  Neighbor
                 mode       status      device                    port
----- ---------- ---------- ----------- ------------------------- ----------
 2/1  connected  desirable channel     WS-C5505    066509957(Sw  2/1
 2/2  connected  desirable channel     WS-C5505    066509957(Sw  2/2
----- ---------- ---------- ----------- ------------------------- ----------
```

Si noti che il canale è formato solo tra le porte 2/1-2. Le porte 2/3-4 sono state escluse perché la porta 2/4 si trovava su una VLAN diversa. Non c'è stato alcun messaggio di errore; PAgP ha semplicemente fatto il possibile per far funzionare il canale. Quando si crea il canale, è necessario

visualizzare i risultati per verificare che abbia eseguito le operazioni desiderate.A questo punto, impostare manualmente il canale su "on" con la porta 2/4 su una VLAN diversa e verificare cosa succede. Impostare di nuovo la modalità canale su auto per abbattere il canale corrente, quindi impostare manualmente il canale su "on".

```
Switch-A (enable) set port channel 2/1-4 auto

Port(s) 2/1-4 channel mode set to auto.

Switch-A (enable)

1999 Dec 19 00:26:08 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-2

1999 Dec 19 00:26:08 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/1-2

1999 Dec 19 00:26:08 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3

1999 Dec 19 00:26:08 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4

1999 Dec 19 00:26:18 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1

1999 Dec 19 00:26:19 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/2

1999 Dec 19 00:26:19 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/3

1999 Dec 19 00:26:19 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/4


Switch-A (enable) show port channel

No ports channelling


Switch-A (enable) set port channel 2/1-4 on

Mismatch in vlan number.

Failed to set port(s) 2/1-4 channel mode to on.


Switch-A (enable) show port channel

No ports channelling
```

Sullo switch B è possibile accendere il canale e notare che il messaggio sul canale delle porte è corretto, ma lo switch A non è configurato correttamente.

```
Switch-B (enable) show port channel

No ports channelling


Switch-B (enable) show port

Port  Name                 Status     Vlan       Level  Duplex Speed Type

----- ------------------ ---------- ---------- ------ ------ ----- ------------

 2/1                      connected  1          normal a-full a-100 10/100BaseTX
```

```
 2/2                      connected  1          normal a-full a-100 10/100BaseTX
 2/3                      connected  1          normal a-full a-100 10/100BaseTX
 2/4                      connected  1          normal a-full a-100 10/100BaseTX

Switch-B (enable) set port channel 2/1-4 on
Port(s) 2/1-4 channel mode set to on.

Switch-B (enable)
2000 Jan 17 22:54:59 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
2000 Jan 17 22:54:59 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
2000 Jan 17 22:54:59 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
2000 Jan 17 22:54:59 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
2000 Jan 17 22:55:00 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
2000 Jan 17 22:55:00 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
2000 Jan 17 22:55:00 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
2000 Jan 17 22:55:00 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4

Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  on        channel     WS-C5505    066507453(Sw  2/1
 2/2  connected  on        channel     WS-C5505    066507453(Sw  2/2
 2/3  connected  on        channel     WS-C5505    066507453(Sw  2/3
 2/4  connected  on        channel     WS-C5505    066507453(Sw  2/4
----- ---------- --------- ----------- ------------------------- ----------
```

Èevidente che è necessario controllare entrambi i lati del canale quando si configura manualmente il canale per assicurarsi che entrambi i lati siano attivi, non solo uno. Questo output mostra che lo switch B è impostato per un canale, ma lo switch A non lo canalizza, in quanto ha una porta sulla VLAN errata.Attendere troppo tempo prima di configurare l'altro latoIn questo caso, EtherChannel è attivato sullo switch B, ma lo switch A no a causa di un errore di configurazione VLAN (le porte 2/1-3 si trovano nella vlan1, la porta 2/4 nella vlan2). Di seguito viene riportato ciò che accade quando un lato di EtherChannel è impostato su on mentre l'altro è ancora in modalità automatica. Dopo alcuni minuti, lo switch B chiude le porte a causa di uno spanning loop

detection. Infatti le porte 2/1-4 dello switch B funzionano tutte come una porta grande, mentre le porte 2/1-4 dello switch A sono tutte porte totalmente indipendenti. Una trasmissione inviata dallo switch B allo switch A sulla porta 2/1 viene rinviata allo switch B sulle porte 2/2, 2/3 e 2/4 perché lo switch A tratta queste porte come porte indipendenti. Ecco perché lo switch B segnala la presenza di un loop nello spanning tree. Si noti che le porte sullo switch B sono ora disabilitate e lo stato è *opridisable*.

```
Switch-B (enable)
2000 Jan 17 22:55:48 %SPANTREE-2-CHNMISCFG: STP loop - channel 2/1-4 is disabled in vlan 1.
2000 Jan 17 22:55:49 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-4
2000 Jan 17 22:56:01 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/1-4
2000 Jan 17 22:56:13 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/1-4
2000 Jan 17 22:56:36 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/1-4

Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  errdisable on        channel
 2/2  errdisable on        channel
 2/3  errdisable on        channel
 2/4  errdisable on        channel
----- ---------- --------- ----------- ------------------------- ----------
Switch-B (enable) show port
Port  Name                Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                      errdisable 1          normal   auto  auto 10/100BaseTX
 2/2                      errdisable 1          normal   auto  auto 10/100BaseTX
 2/3                      errdisable 1          normal   auto  auto 10/100BaseTX
 2/4                      errdisable 1          normal   auto  auto 10/100BaseTX
```

Correggi stato err-disabledA volte, quando si cerca di configurare EtherChannel, ma le porte non sono configurate allo stesso modo, le porte su un lato del canale o sull'altro vengono chiuse. Le luci di collegamento sono gialle sulla porta. È possibile verificare questa condizione dalla console se si digita show port. Le porte sono elencate *come disabilitate a causa di un errore*. Per risolvere questo problema, occorre correggere i parametri con mancata corrispondenza sulle porte

coinvolte, quindi riattivare le porte. Si noti che per riattivare le porte è necessario eseguire un'operazione separata perché le porte tornino a funzionare.Nell'esempio, si sa che la vlan dello switch A non corrisponde. Andare allo switch A e reinserire la porta 2/4 nella vlan1. Quindi, si accende il canale per le porte 2/1-4. Lo switch A non viene visualizzato connesso fino a quando le porte dello switch B non vengono riattivate. Quindi, dopo aver corretto lo switch A e averlo messo in modalità channeling, tornare allo switch B e riattivare le porte.

```
Switch-A (enable) set vlan 1 2/4

VLAN 1 modified.

VLAN 2 modified.

VLAN  Mod/Ports

---- ----------------------

1     2/1-24


Switch-A (enable) set port channel 2/1-4 on

Port(s) 2/1-4 channel mode set to on.

Switch-A (enable) sh port channel

Port  Status     Channel   Channel     Neighbor                  Neighbor

                 mode      status      device                    port

----- ---------- --------- ----------- ------------------------- ----------

 2/1  notconnect on        channel

 2/2  notconnect on        channel

 2/3  notconnect on        channel

 2/4  notconnect on        channel

----- ---------- --------- ----------- ------------------------- ----------


Switch-B (enable) show port channel

Port  Status     Channel   Channel     Neighbor                  Neighbor

                 mode      status      device                    port

----- ---------- --------- ----------- ------------------------- ----------

 2/1  errdisable on        channel

 2/2  errdisable on        channel

 2/3  errdisable on        channel

 2/4  errdisable on        channel

----- ---------- --------- ----------- ------------------------- ----------
```

```
Switch-B (enable) set port enable 2/1-4
Ports 2/1-4 enabled.
Switch-B (enable) 2000 Jan 17 23:15:22 %PAGP-5-PORTTOSTP:Port 2/1 joined bridg4
2000 Jan 17 23:15:22 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
2000 Jan 17 23:15:22 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
2000 Jan 17 23:15:22 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4

Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------ ----------
 2/1  connected  on        channel
 2/2  connected  on        channel
 2/3  connected  on        channel
 2/4  connected  on        channel
----- ---------- --------- ----------- ------------------------ ----------
```

Mostra cosa succede quando un collegamento si interrompe e viene ripristinatoQuando una porta del canale diventa inattiva, i pacchetti che normalmente vengono inviati su quella porta vengono spostati sulla porta successiva del canale. Per verificare questa condizione, utilizzare il comando show maccommand. In questo banco di prova, lo switch A invia pacchetti ping allo switch B per verificare quale collegamento viene utilizzato dal traffico. Cancellare prima i contatori, quindi visualizzare mac, inviare tre ping e infine visualizzare nuovamente mac per verificare su quale canale sono state ricevute le risposte ping.

```
Switch-A (enable) clear counters
This command will reset all MAC and port counters reported in CLI and SNMP.
Do you want to continue (y/n) [n]? y
MAC and Port counters cleared.

Switch-A (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------ ----------
 2/1  connected  on        channel     WS-C5505    066509957(Sw  2/1
```

```
 2/2  connected  on        channel     WS-C5505    066509957(Sw  2/2
 2/3  connected  on        channel     WS-C5505    066509957(Sw  2/3
 2/4  connected  on        channel     WS-C5505    066509957(Sw  2/4
----- ---------- --------- ----------- ------------------------ ----------

Switch-A (enable) show mac

Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
 2/1                        0                   18                    0
 2/2                        0                    2                    0
 2/3                        0                    2                    0
 2/4                        0                    2                    0
Switch-A (enable) ping 172.16.84.17
172.16.84.17 is alive
Switch-A (enable) ping 172.16.84.17
172.16.84.17 is alive
Switch-A (enable) ping 172.16.84.17
172.16.84.17 is alive
Switch-A (enable) show mac

Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
 2/1                        3                   24                    0
 2/2                        0                    2                    0
 2/3                        0                    2                    0
 2/4                        0                    2                    0
```

A questo punto, sono state ricevute le risposte ping sulla porta 3/1. Quando la console dello switch B invia una risposta allo switch A, EtherChannel usa la porta 2/1. A questo punto, la porta 2/1 viene chiusa sullo switch B. Dallo switch A, si esegue un altro ping e si controlla il canale su cui viene riattivata la risposta. (Lo switch A invia la stessa porta a cui è connesso lo switch B. È sufficiente visualizzare i pacchetti ricevuti dallo switch B perché i pacchetti di trasmissione si trovano più in basso nella visualizzazione della macro show).

```
1999 Dec 19 01:30:23 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-4
```

```
Switch-A (enable) ping 172.16.84.17

172.16.84.17 is alive

Switch-A (enable) show mac


Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast

-------- -------------------- -------------------- --------------------

 2/1                        3                   37                    0

 2/2                        1                   27                    0

 2/3                        0                    7                    0

 2/4                        0                    7                    0
```

Ora che la porta 2/1 è disabilitata, EtherChannel usa automaticamente la porta successiva, 2/2. A questo punto, è possibile riabilitare la porta 2/1 e attendere che si unisca al gruppo di bridge. Quindi, eseguire altri due ping.

```
1999 Dec 19 01:31:33 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4


Switch-A (enable) ping 172.16.84.17

172.16.84.17 is alive

Switch-A (enable) ping 172.16.84.17

172.16.84.17 is alive

Switch-A (enable) show mac


Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast

-------- -------------------- -------------------- --------------------

 2/1                        5                   50                    0

 2/2                        1                   49                    0

 2/3                        0                   12                    0

 2/4                        0                   12                    0
```

I ping vengono inviati dalla porta 2/1. Quando il collegamento torna attivo, EtherChannel lo aggiunge di nuovo al bundle e lo utilizza. Tutto questo viene fatto in modo trasparente per l'utente.

Comandi utilizzati in questa sezione

Questi sono i comandi utilizzati in questa sezione.Comandi da utilizzare per impostare la configurazione

impostare port channel on- per attivare la funzione EtherChannel.

set port channel auto: per ripristinare le porte alla modalità predefinita auto.

set port channel desired: consente di inviare pacchetti PAgP all'altro lato della porta per richiedere la creazione di un canale.

set port enable: consente di abilitare le porte dopo aver impostato la porta su disable o dopo uno stato err-disabled.

set port disable: per disabilitare una porta mentre vengono eseguite altre impostazioni di configurazione.

set trunk desiderable: per attivare il trunking e fare in modo che questa porta invii una richiesta all'altro switch per indicare che si tratta di un collegamento trunk. Se la porta è impostata su NEGOTIate (impostazione predefinita) per negoziare il tipo di trunking da utilizzare sul collegamento (ISL o 802.1q).

Comandi da utilizzare per verificare la configurazione

show version: per visualizzare la versione del software in esecuzione sullo switch.

show module: per visualizzare i moduli installati nello switch.

show port capabilities: per determinare se le porte che si desidera utilizzare possono eseguire EtherChannel.

show port: per determinare lo stato della porta (non connessa, connessa) e le impostazioni di velocità e duplex.

ping: per verificare la connettività con l'altro switch.

show port channel: visualizza lo stato corrente del bundle EtherChannel.

show port channel mod/porta: per una visualizzazione più dettagliata dello stato del canale di una singola porta.

show spantree: per verificare che spanning tree abbia visualizzato il canale come un unico collegamento.

show trunk: visualizza lo stato di trunking delle porte.

Comandi da utilizzare per risolvere i problemi relativi alla configurazione

show port channel: visualizza lo stato corrente del bundle EtherChannel.

show port: per determinare lo stato della porta (non connessa, connessa) e le impostazioni di velocità e duplex.

clear counters - per azzerare i contatori del pacchetto dello switch. I contatori sono visibili con il comando show maccommand.

show mac: per visualizzare i pacchetti ricevuti e inviati dallo switch.

ping: per verificare la connettività con l'altro switch e generare il traffico mostrato con il comando show maccommand.

Uso di Portfast e altri comandi per risolvere i problemi di connettività di avvio della stazione terminale

Se alcune workstation sono collegate a switch che non sono in grado di accedere al dominio di rete (NT o Novell) o di ottenere un indirizzo DHCP, è possibile provare i suggerimenti riportati in questo documento prima di esplorare altre possibilità. I suggerimenti sono relativamente semplici da implementare e molto spesso sono la causa dei problemi di connettività della workstation riscontrati durante la fase di inizializzazione/avvio della workstation.Con un numero sempre maggiore di utenti che installano il passaggio al desktop e sostituiscono gli hub condivisi con switch, spesso si verificano problemi negli ambienti client/server a causa di questo ritardo iniziale. Il problema più grande è che Windows 95/98/NT, Novell, VINES, IBM NetworkStation/IBM Thin Client e i client AppleTalk non sono in grado di connettersi ai loro server. Se il software su questi dispositivi non è persistente nella procedura di avvio, non tentano più di connettersi al server prima che lo switch abbia consentito il passaggio del traffico.Nota: questo ritardo di connettività iniziale spesso si manifesta come errori che compaiono quando si avvia una workstation per la prima volta. Di seguito sono riportati diversi esempi di messaggi di errore ed errori che è possibile visualizzare:

Viene visualizzato un client di rete Microsoft, "No Domain Controller Available" (Nessun controller di dominio disponibile).

Il messaggio inviato da DHCP è "No DHCP Servers Available" (Nessun server DHCP disponibile).

Una workstation di rete Novell IPX non dispone della "Schermata di accesso Novell" all'avvio.

Un client di rete AppleTalk visualizza, "L'accesso alla rete AppleTalk è stato interrotto. Per ristabilire la connessione, apri e chiudi il pannello di controllo di AppleTalk." È inoltre possibile che l'applicazione AppleTalk Client Chooser non visualizzi un elenco delle zone o un elenco delle zone incompleto.

Il ritardo iniziale della connettività è inoltre frequente in un ambiente commutato in cui un

amministratore di rete aggiorna software o driver. In questo caso, un fornitore può ottimizzare i driver in modo che le procedure di inizializzazione della rete vengano eseguite in anticipo nel processo di avvio del client (prima che lo switch sia pronto a elaborare i pacchetti).Con le varie funzioni ora incluse in alcuni switch, può essere necessario attendere quasi un minuto prima che uno switch inizi a servire una workstation appena connessa. Questo ritardo può influire sulla workstation a ogni accensione o riavvio. Queste sono le quattro principali caratteristiche che causano il ritardo:

- STP (Spanning-Tree Protocol)
- Negoziazione EtherChannel
- Negoziazione trunking
- Negoziazione velocità/duplex del collegamento tra lo switch e la workstation

Le quattro funzionalità sono elencate in ordine di tempo e causano il ritardo maggiore (Spanning-Tree Protocol) a cui causa il ritardo minore (negoziazione velocità/duplex). Una workstation connessa a uno switch in genere non causa loop nello spanning tree, non ha bisogno di EtherChannel e non ha bisogno di negoziare un metodo di trunking. (Se si disabilita la negoziazione della velocità/rilevamento del collegamento, è possibile ridurre il ritardo della porta se è necessario ottimizzare il più possibile il tempo di avvio).Questa sezione illustra come implementare i comandi di ottimizzazione della velocità di avvio su tre piattaforme dello switch Catalyst. Nelle sezioni relative agli intervalli, viene mostrato come ridurre il ritardo della porta dello switch e di quanto.Sommario

Ulteriori vantaggi per Portfast

In questa sezione, i termini "stazione di lavoro", "stazione terminale" e "server" sono utilizzati indifferentemente. Ciò a cui ci si riferisce è qualsiasi dispositivo collegato direttamente a uno switch da una singola scheda NIC. Può inoltre riferirsi a dispositivi con più schede NIC in cui la scheda NIC viene utilizzata solo per la ridondanza, in altre parole la workstation o il server non è configurato per fungere da bridge, ma dispone solo di più schede NIC per la ridondanza.Nota: alcune schede NIC per server supportano il trunking e/o EtherChannel. In alcuni casi, il server deve funzionare su più VLAN contemporaneamente (trunking) o ha bisogno di una maggiore larghezza di banda sul collegamento che lo connette allo switch (EtherChannel). In questi casi, non disattivare PAgP e non disattivare trunking. Inoltre, questi dispositivi vengono spenti o reimpostati di rado. Le istruzioni riportate nel presente documento non si applicano a questi tipi di dispositivi.SfondoIn questa sezione vengono illustrate quattro funzionalità di alcuni switch che causano ritardi iniziali quando un dispositivo è collegato a uno switch. In genere, una workstation non causa il problema dello Spanning Tree (loop) o non ha bisogno della funzionalità (PAgP, DTP), quindi il ritardo non è necessario.Spanning TreeSe di recente si è iniziato a passare da un ambiente hub a uno switch, questi problemi di connettività possono presentarsi perché uno switch funziona in modo molto diverso rispetto a un hub. Uno switch fornisce la connettività al livello di collegamento dati, non al livello fisico. Lo switch deve utilizzare un algoritmo di bridging per decidere se i pacchetti ricevuti su una porta devono essere trasmessi su altre porte. L'algoritmo di bridging è sensibile ai loop fisici nella topologia di rete. A causa di questa suscettibilità ai loop, gli switch eseguono un protocollo chiamato Spanning Tree Protocol (STP) che determina l'eliminazione dei loop nella topologia. Quando il protocollo STP viene eseguito, tutte le porte incluse nel processo Spanning Tree diventano attive molto più lentamente di quanto non sarebbero altrimenti, poiché rileva e blocca i loop. Una rete con bridge che dispone di loop fisici, senza Spanning Tree, si interrompe. Nonostante il tempo richiesto, l'STP è una buona cosa. Lo Spanning Tree eseguito sugli switch Catalyst è una specifica standard del settore (IEEE 802.1d).Dopo che una porta sullo switch è collegata e si unisce al gruppo di bridge, esegue Spanning Tree su tale porta. Una porta con Spanning Tree può avere uno di 5 stati: Blocking, Listening, Learning, Forwarding e Disabled. Lo Spanning Tree determina che la porta inizi il blocco, quindi si sposta immediatamente attraverso le fasi di ascolto e apprendimento. Per impostazione predefinita, impiega circa 15 secondi per l'ascolto e 15 per l'apprendimento.In stato di ascolto, lo switch cerca di determinare la posizione dello switch nella topologia dello Spanning Tree. In particolare, desidera sapere se questa porta fa parte di un loop fisico. Se fa parte di un loop, è possibile scegliere questa porta per accedere alla modalità di blocco. Il blocco significa che non invia o riceve dati utente al fine di eliminare i loop. Se la porta non fa parte di un loop, passa

allo stato di apprendimento che implica l'apprendimento degli indirizzi MAC attivi su questa porta. L'intero processo di inizializzazione dello Spanning Tree richiede circa 30 secondi.Se si collega una workstation o un server con una singola scheda NIC a una porta dello switch, questa connessione non può creare un loop fisico. Queste connessioni sono considerate nodi foglia. Non è necessario attendere 30 secondi che lo switch verifichi la presenza di loop quando la workstation non può causare un loop. Cisco ha quindi aggiunto una funzione chiamata "Portfast" o "Fast-Start", ossia lo Spanning Tree di questa porta può presupporre che la porta non faccia parte di un loop e possa passare immediatamente allo stato di inoltro, ignorando gli stati di blocco, ascolto o apprendimento. Ciò può risparmiare molto tempo. Questo comando non disattiva lo Spanning Tree. Lo Spanning Tree sulla porta selezionata ignora alcuni passaggi (non necessari in questo caso) all'inizio.Nota: la funzione Portfast non deve mai essere utilizzata sulle porte degli switch che si connettono ad altri switch, hub o router. Queste connessioni possono causare loop fisici ed è molto importante che lo Spanning Tree esegua l'intera procedura di inizializzazione in queste situazioni. Un loop nello spanning tree può compromettere la rete. Se portfast è attivata per una porta che fa parte di un loop fisico, può causare una finestra di tempo in cui i pacchetti potrebbero essere inoltrati continuamente (e anche moltiplicati) in modo tale che la rete non possa recuperare. Nel successivo software del sistema operativo Catalyst (5.4(1)), è disponibile una funzione chiamata Portfast BPDU-Guard che rileva la ricezione di BPDU sulle porte con Portfast abilitata. Poiché questa condizione non deve mai verificarsi, BPDU-Guard mette la porta in stato "errDisable".EtherChannelUn'altra caratteristica che uno switch può avere è chiamata EtherChannel (o Fast EtherChannel, o Gigabit EtherChannel). Questa funzione consente a più collegamenti tra gli stessi due dispositivi di funzionare come se si trattasse di un unico collegamento rapido, con il carico del traffico bilanciato tra i collegamenti. Uno switch può formare questi bundle automaticamente con un router adiacente con un protocollo chiamato Port Aggregation Protocol (PAgP). Le porte degli switch che possono eseguire PAgP in genere utilizzano per impostazione predefinita una modalità passiva denominata "auto", che indica che possono formare un bundle se il dispositivo adiacente sul collegamento lo richiede. Se il protocollo viene eseguito in modalità automatica, una porta potrebbe ritardare fino a 15 secondi prima di passare il controllo allo spanning tree algorithm (il protocollo PAgP viene eseguito su una porta prima dello spanning tree). Non vi è alcun motivo per cui PAgP debba essere eseguito su una porta collegata a una workstation. Se si imposta la porta dello switch in modalità PAgP su "off", il ritardo viene eliminato.TrunkingUn'altra funzionalità dello switch è la capacità di una porta di formare un trunk. Un trunk è configurato tra due dispositivi quando questi devono trasportare il traffico da più VLAN (Virtual Local Area Network). Una VLAN è qualcosa che gli switch creano per far apparire un gruppo di workstation come posizionato su un proprio "segmento" o "dominio di

broadcast". Le porte trunk permettono di estendere le VLAN su più switch, in modo che una singola VLAN possa coprire un intero campus. A tal fine, è necessario aggiungere dei tag ai pacchetti per indicare la VLAN a cui appartiene il pacchetto.Esistono diversi tipi di protocolli di trunking. Se una porta può diventare un trunk, può anche essere in grado di trunk automaticamente e in alcuni casi persino di negoziare il tipo di trunking da utilizzare sulla porta. Questa possibilità di negoziare il metodo di trunking con l'altro dispositivo è detta DTP (Dynamic Trunking Protocol), il precursore del DTP è un protocollo chiamato DISL (Dynamic ISL). Se questi protocolli sono in esecuzione, può ritardare l'attivazione di una porta sullo switch.In genere, una porta collegata a una workstation appartiene a una sola VLAN e quindi non deve essere trunk. Se una porta è in grado di negoziare la formazione di un trunk, per impostazione predefinita viene utilizzata la modalità "auto". Se la porta viene impostata sulla modalità trunking "off", riduce ulteriormente il ritardo di una porta dello switch che diventa attiva.Negoziazione velocità e duplexPer risolvere il problema, è sufficiente attivare Portfast e disattivare PAgP (se presente). Tuttavia, se si desidera eliminare tutti i secondi possibili, è possibile impostare manualmente la velocità della porta e la modalità duplex sullo switch, se si tratta di una porta a più velocità (10/100). La negoziazione automatica è una buona funzione, ma se viene disattivata si potrebbero risparmiare 2 secondi su Catalyst 5000 (non è di grande aiuto sui modelli 2800 o 2900XL).Tuttavia, ci possono essere delle complicazioni se si disattiva la negoziazione automatica sullo switch ma la si lascia attiva sulla workstation. Poiché lo switch non negozia con il client, il client può scegliere la stessa impostazione duplex utilizzata dallo switch o meno. Per ulteriori informazioni sulle avvertenze relative alla negoziazione automatica, vedere la sezione "Risoluzione dei problemi di negoziazione automatica Ethernet 10/100 MB Half/Half/Full Duplex".

Come ridurre il ritardo di avvio sugli switch Catalyst 4000/5000/6000

Questi cinque comandi mostrano come attivare Portfast, come disattivare la negoziazione PAgP, disattivare la negoziazione trunking (DISL, DTP) e disattivare la negoziazione velocità/duplex. il comando set spantree portfast viene eseguito su un intervallo di porte contemporaneamente (impostare spantree portfast 2/1-12 enable). In genere, il canale della porta impostata deve essere disattivato con un gruppo valido di porte che supportano il canale. In questo caso, il modulo 2 ha la capacità di effettuare il canale con le porte 2/1-2 o con le porte 2/1-4, quindi uno di questi gruppi di porte sarebbe stato valido per l'uso.Nota: la versione 5.2 di Cat OS per Catalyst 4000/5000 include un nuovo comando denominato set port host, una macro che combina questi comandi in un unico comando di facile utilizzo (a eccezione del fatto che non modifica le impostazioni di velocità e duplex).Configurazione

```
Switch-A (enable) set spantree portfast 2/1 enable
```

```
Warning: Spantree port fast start should only be enabled on ports connected
to a single host. Connecting hubs, concentrators, switches, bridges, and so on to
a fast start port can cause temporary spanning tree loops.  Use with caution.

Spantree port 2/1 fast start enabled.
Switch-A (enable) set port channel 2/1-2 off
Port(s) 2/1-2 channel mode set to off.

Switch-A (enable) set trunk 2/1 off
Port(s) 2/1 trunk mode set to off.
```

Le modifiche apportate alla configurazione vengono salvate automaticamente nella NVRAM.VerificaLa versione del software dello switch utilizzata in questo documento è la 4.5(1). Per l'output completo di show version e show module, fare riferimento a questa sezione del test sugli intervalli.

```
Switch-A (enable) show version
WS-C5505 Software,
Version McpSW: 4.5(1) NmpSW: 4.5(1)
```

Questo comando mostra come visualizzare lo stato corrente di una porta rispetto allo spanning tree. La porta è attualmente nello stato di inoltro dello Spanning Tree (invio e ricezione di pacchetti) e la colonna Fast-Start indica che portfast è attualmente disabilitata. In altre parole, la porta può impiegare almeno 30 secondi per passare allo stato di inoltro ogni volta che viene inizializzata.

```
Switch-A (enable) show port spantree 2/1

Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-Method
--------  ----  -------------  -----  --------  ----------  ------------
 2/1      1     forwarding        19        32
disabled
```

A questo punto, è possibile abilitare portfast su questa porta dello switch. Lo switch ci avverte che questo comando deve essere usato solo sulle porte connesse a un singolo host (una postazione di lavoro, un server e così via) e non deve mai essere usato sulle porte connesse ad altri hub o switch. Il motivo per cui si abilita portfast è che la porta inizia immediatamente a inoltrare. Questa

operazione può essere eseguita perché una workstation o un server non provoca un loop di rete. Questo può sprecare tempo. Ma un altro hub o switch può causare un loop e si desidera passare sempre attraverso le normali fasi di ascolto e apprendimento quando ci si connette a questi tipi di dispositivi.

```
Switch-A (enable) set spantree portfast 2/1 enable

Warning: Spantree port fast start should only be enabled on ports connected
to a single host.  Connecting hubs, concentrators, switches, bridges, and so on to
a fast start port can cause temporary spanning tree loops.  Use with caution.

Spantree port 2/1 fast start enabled.
```

Per verificare che Portfast sia abilitato per questa porta, eseguire questo comando.

```
Switch-A (enable) show port spantree 2/1

Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-Method
--------  ----  -------------  -----  --------  ----------  ------------
 2/1      1     forwarding        19        32
enabled
```

Per visualizzare le impostazioni di Portfast per una o più porte, è possibile anche visualizzare le informazioni dello Spanning Tree di una VLAN specifica. Più avanti, nella sezione temporizzazione di questo documento, verrà spiegato come impostare lo switch in modo che riporti in tempo reale ciascuna fase dello Spanning Tree attraversata. Questo output mostra anche il ritardo in avanti (15 secondi). In questo esempio, viene indicato per quanto tempo lo spanning tree può essere in stato di ascolto e per quanto tempo può essere in stato di apprendimento per ciascuna porta della VLAN.

```
Switch-A (enable) show spantree 1
VLAN 1
Spanning tree enabled
Spanning tree type          ieee

Designated Root             00-e0-4f-94-b5-00
Designated Root Priority    8189
Designated Root Cost        19
```

```
Designated Root Port        2/24
Root Max Age   20 sec    Hello Time 2  sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-90-92-b0-84-00
Bridge ID Priority          32768
Bridge Max Age 20 sec    Hello Time 2  sec   Forward Delay 15 sec

Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-Method
--------- ----  -------------  -----  --------  ----------  ------------

 2/1      1     forwarding        19        32   enabled
...
```

Per verificare che il protocollo PAgP sia disattivato, usare il comando show port channel. Accertarsi di specificare il numero del modulo (in questo caso 2) in modo che il comando mostri la modalità del canale anche se non è stato formato alcun canale. Se si omette il comando show port channeling senza che vi siano canali formati, significa che non vi è alcun canale per le porte. Per ulteriori informazioni, vedere la modalità corrente del canale.

```
Switch-A (enable) show port channel
No ports channeling

Switch-A (enable) show port channel 2
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------ ----------
 2/1  notconnect auto      not channel
 2/2  notconnect auto      not channel
...
Switch-A (enable) set port channel 2/1-2 off
Port(s) 2/1-2 channel mode set to off.

Switch-A (enable) show port channel 2
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------ ----------
```

```
 2/1  connected  off       not channel
 2/2  connected  off       not channel
...
```

Per verificare che la negoziazione Trunking sia disattivata, utilizzare il comando set trunk off. Viene visualizzato lo stato predefinito. Quindi si disattiva il trunking e si visualizza il risultato. Specificare il modulo numero 2 in modo da poter visualizzare la modalità del canale corrente per le porte in questo modulo.

```
Switch-A (enable) show trunk 2
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/1      auto         negotiate      not-trunking  1
 2/2      auto         negotiate      not-trunking  1
...

Switch-A (enable) set trunk 2/1-2 off
Port(s) 2/1-2 trunk mode set to off.

Switch-A (enable) show trunk 2
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/1      off          negotiate      not-trunking  1
 2/2      off          negotiate      not-trunking  1
```

Non è necessario, ad eccezione del caso più raro, disattivare la negoziazione automatica velocità/duplex o impostare manualmente la velocità e la modalità duplex sullo switch. Per informazioni su questa operazione, vedere la sezione Test di temporizzazione con e senza DTP, PAgP e Portfast su Catalyst 5000 se lo si ritiene necessario in base alla propria situazione.Test di temporizzazione con e senza DTP, PAgP e Portfast su Catalyst 5000Questo test mostra ciò che accade con i tempi di inizializzazione delle porte dello switch quando vengono applicati i vari comandi. Le impostazioni predefinite della porta vengono usate per prime per fornire un benchmark. Hanno la funzione portfast disabilitata, la modalità PAgP (EtherChannel) è impostata su auto (i canali IT sono attivati sul canale) e la modalità trunking (DTP) è impostata su auto (il trunking viene attivato se viene attivato il trunk). Il test prosegue quindi con l'attivazione di portfast e la misurazione del tempo, poi la disattivazione di PAgP e la misurazione del tempo,

quindi la disattivazione di trunking e la misurazione del tempo. Infine, è possibile disattivare la negoziazione automatica e misurare il tempo. Tutti i test vengono eseguiti su un Catalyst 5000 con una scheda Fast Ethernet 10/100 che supporta DTP e PAgP.Nota: quando portfast è attivato, non è come disattivare Spanning Tree (come indicato nel documento). Quando portfast è attivo, lo Spanning Tree continua a funzionare sulla porta; semplicemente non blocca, ascolta o apprende e passa immediatamente allo stato di inoltro. La disattivazione dello Spanning Tree non è consigliata perché influisce sull'intera VLAN e può lasciare la rete vulnerabile a loop della topologia fisica, che possono causare seri problemi di rete.

Visualizzare la versione e la configurazione dello switch Cisco IOS (show version, show module).

```
Switch-A (enable) show version
WS-C5505 Software, Version McpSW: 4.5(1) NmpSW: 4.5(1)
Copyright (c) 1995-1999 by Cisco Systems
NMP S/W compiled on Mar 29 1999, 16:09:01
MCP S/W compiled on Mar 29 1999, 16:06:50

System Bootstrap Version: 3.1.2

Hardware Version: 1.0  Model: WS-C5505  Serial #: 066507453

Mod Port Model      Serial #  Versions
--- ---- ---------- --------- ---------------------------------------
1   0    WS-X5530   006841805 Hw : 1.3
                               Fw : 3.1.2

                               Fw1: 3.1(2)
                               Sw : 4.5(1)
2   24   WS-X5225R  012785227 Hw : 3.2
                               Fw : 4.3(1)
                               Sw : 4.5(1)

       DRAM                    FLASH                   NVRAM
Module Total   Used    Free    Total   Used    Free    Total Used  Free
------ ------- ------- ------- ------- ------- ------- ----- ----- -----
1       32640K  13648K  18992K   8192K   4118K   4074K  512K  119K  393K

Uptime is 28 days, 18 hours, 54 minutes

Switch-A (enable) show module
Mod Module-Name         Ports Module-Type           Model    Serial-Num Status
--- ------------------- ----- --------------------- -------- --------- -------
1                       0     Supervisor III        WS-X5530  006841805 ok
2                       24    10/100BaseTX Ethernet WS-X5225R 012785227 ok
```

```
Mod MAC-Address(es)                        Hw     Fw          Sw
--- ---------------------------------------- ------ ---------- -----------------
1   00-90-92-b0-84-00 to 00-90-92-b0-87-ff 1.3    3.1.2      4.5(1)
2   00-50-0f-b2-e2-60 to 00-50-0f-b2-e2-77 3.2    4.3(1)     4.5(1)

Mod Sub-Type Sub-Model Sub-Serial Sub-Hw
--- -------- --------- ---------- ------
1   NFFC     WS-F5521  0008728786 1.0
```

Impostare la registrazione per Spanning Tree sul livello di registrazione più dettagliato (Impostare Spanning Tree 7). Questo è il livello di registrazione predefinito (2) per lo spanning tree, ossia vengono segnalate solo le situazioni critiche.

```
Switch-A (enable) show logging

Logging buffer size:          500
        timestamp option:     enabled
Logging history size:         1
Logging console:              enabled
Logging server:               disabled
        server facility:      LOCAL7
        server severity:      warnings(4)

Facility            Default Severity         Current Session Severity
-------------       ------------------------  ------------------------
...
spantree            2                         2
...
0(emergencies)        1(alerts)              2(critical)
3(errors)             4(warnings)            5(notifications)
6(information)        7(debugging)
```

il livello per lo Spanning Tree viene modificato in 7 (debug), in modo che sia possibile vedere come gli stati dello Spanning Tree vengono modificati sulla porta. La modifica della configurazione dura solo per la sessione del terminale, quindi torna alla configurazione normale.

```
Switch-A (enable) set logging level spantree 7
System logging facility <spantree for this session set to severity 7(debugging)

Switch-A (enable) show logging
...

Facility            Default Severity         Current Session Severity
-------------       ------------------------  ------------------------
```

```
...
spantree            2                       7
...
```

Iniziare con la porta del Catalyst spento.

```
Switch-A (enable) set port disable 2/1
Port 2/1 disabled.
```

Specificare ora l'ora e abilitare la porta. Si desidera verificare per quanto tempo la porta rimane in ciascuno stato.

```
Switch-A (enable) show time
Fri Feb 25 2000, 12:20:17
Switch-A (enable) set port enable 2/1
Port 2/1 enabled.
Switch-A (enable)
2000 Feb 25 12:20:39 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
2000 Feb 25 12:20:39 %SPANTREE-6-PORTBLK: port 2/1 state in vlan 1 changed to blocking.
2000 Feb 25 12:20:39 %SPANTREE-6-PORTLISTEN: port 2/1 state in vlane 1 changed to Listening
.
2000 Feb 25 12:20:53 %SPANTREE-6-PORTLEARN: port 2/1 state in vlan 1 changed to Learning.
2000 Feb 25 12:21:08 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 changed to forwarding.
```

Notare dall'output che la porta ha impiegato circa 22 secondi (da 20:17 a 20:39) per iniziare la fase di blocco dello Spanning Tree. Questo era il tempo necessario per negoziare il collegamento ed eseguire le operazioni DTP e PAgP. Quando il blocco ha inizio, si è nel regno Spanning Tree. Dal blocco della porta, è passato immediatamente all'ascolto (dalle 20:39 alle 20:39). Dall'ascolto all'apprendimento impiegò circa 14 secondi (20:39 a 20:53).

Dall'apprendimento all'inoltro ci sono voluti 15 secondi (dalle 20:53 alle 21:08). Il tempo totale prima che la porta diventasse effettivamente funzionale al traffico era di circa 51 secondi (20:17-21:08).

Nota: da un punto di vista tecnico, la fase di ascolto e apprendimento è entrambe di 15 secondi, ossia la modalità di impostazione del parametro del ritardo di inoltro per questa VLAN. La fase di apprendimento probabilmente è più vicina a 15 secondi che a 14 secondi se si dispone di misurazioni più accurate. Nessuna delle misurazioni qui è perfettamente accurata. Avete solo cercato di dare un'idea di quanto tempo ci vuole per le cose.

dall'output e dal comando show spantre si può sapere che spanning tree è attivo su questa porta. Esaminiamo altri elementi che potrebbero rallentare la porta quando raggiunge lo stato di inoltro. Il comando show port capabilities mostra che questa porta è in grado di eseguire il trunk e di creare un EtherChannel. Il comando show trunking indica che la porta è in modalità automatica e che è impostata per negoziare il tipo di trunking da utilizzare (ISL o 802.1q, negoziato tramite DTP (Dynamic Trunking Protocol)).

```
Switch-A (enable) show port capabilities 2/1
Model                     WS-X5225R
Port                      2/1
Type                      10/100BaseTX

Speed                     auto,10,100
Duplex                    half,full
Trunk encap type          802.1Q,ISL
Trunk mode                on,off,desirable,auto,nonegotiate
Channel                   2/1-2,2/1-4
Broadcast suppression     percentage(0-100)
Flow control              receive-(off,on),send-(off,on)
Security                  yes
Membership                static,dynamic
Fast start                yes
Rewrite                   yes
Switch-A (enable) show trunk 2/1
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/1      auto         negotiate      not-trunking  1
```

Innanzitutto, è possibile abilitare Portfast sulla porta. La negoziazione trunking (DTP) è ancora in modalità automatica e EtherChannel (PAgP) è ancora in modalità automatica.

```
Switch-A (enable) set port disable 2/1
Port 2/1 disabled.

Switch-A (enable) set spantree portfast 2/1 enable

Warning: Spantree port fast start should only be enabled on ports connected
to a single host.  Connecting hubs, concentrators, switches, bridges, and so on to
a fast start port can cause temporary spanning tree loops.  Use with caution.

Spantree port 2/1 fast start enabled.

Switch-A (enable) show time
Fri Feb 25 2000, 13:45:23
Switch-A (enable) set port enable 2/1
Port 2/1 enabled.
Switch-A (enable)
Switch-A (enable)
2000 Feb 25 13:45:43 %PAGP-5-PORTTOSTP:Port 2/1 joined bridgeport 2/1
2000 Feb 25 13:45:44 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 change to forwarding.
```

Ora hai un tempo totale di 21 secondi!Ci vogliono 20 secondi prima che si unisca al gruppo di bridge (da 45:23 a 45:43). Tuttavia, poiché Portfast è abilitata, l'avvio dell'inoltro richiede

solo un secondo (anziché 30 secondi). L'abilitazione di Portfast ha consentito di risparmiare 29 secondi. Verificare se è possibile ridurre ulteriormente il ritardo.

A questo punto, la modalità PAgP viene impostata su "off". Dal comando show port channel è possibile vedere che la modalità PAgP è impostata *su auto*, il che significa che viene incanalata se richiesto da un vicino che parla PAgP. È necessario disattivare il channeling per almeno un gruppo di due porte. Non è possibile eseguire questa operazione solo su una singola porta.

```
Switch-A (enable) show port channel 2/1
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  auto      not channel

Switch-A (enable) set port channel 2/1-2 off
Port(s) 2/1-2 channel mode set to off.
```

Spegnere la porta e ripetere il test.

```
Switch-A (enable) set port disable 2/1
Port 2/1 disabled.

Switch-A (enable) show time
Fri Feb 25 2000, 13:56:23
Switch-A (enable) set port enable 2/1
Port 2/1 enabled.
Switch-A (enable)
2000 Feb 25 13:56:32 %PAGP-5-PORTTOSTP:Port 2/1 joined bridgeport 2/1
2000 Feb 25 13:56:32 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 changed to forwarding.
```

Notare che ora sono necessari solo 9 secondi per raggiungere lo stato di inoltro (da 56:23 a 56:32) anziché 21 secondi come nel test precedente. L'attivazione di PAgP fromautotooffin questo test ha consentito di risparmiare circa 12 secondi.

Disabilitare il trunking (anziché impostarlo automaticamente) e verificare l'effetto sul tempo impiegato dalla porta per raggiungere lo stato di inoltro. Spegnere e riaccendere la porta e registrare l'ora.

```
Switch-A (enable) set trunk 2/1 off
Port(s) 2/1 trunk mode set to off.
Switch-A (enable) set port disable 2/1
Port 2/1 disabled.
```

Avviare il test con trunking impostato su off (anziché su auto).

```
Switch-A (enable) show time
Fri Feb 25 2000, 14:00:19
Switch-A (enable) set port enable 2/1
Port 2/1 enabled.
Switch-A (enable)
2000 Feb 25 14:00:22 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
2000 Feb 25 14:00:23 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 change for forwarding.
```

sono stati risparmiati alcuni secondi all'inizio, poiché sono bastati 4 secondi per raggiungere lo stato di inoltro dello spanning tree (da 00:19 a 00:22). Sono stati salvati circa 5 secondi quando si modifica la modalità di trunking *da disattivazione*.

(Facoltativo) Se il problema era causato dal tempo di inizializzazione della porta dello switch, deve essere risolto. Se è necessario ridurre ulteriormente di qualche secondo il tempo, è possibile impostare manualmente la velocità e la modalità duplex sulla porta e non utilizzare la negoziazione automatica.

Se si impostano manualmente la velocità e la modalità duplex su questo lato, è necessario impostare anche la velocità e la modalità duplex sull'altro lato. Infatti, se si imposta la velocità della porta e la modalità duplex, la negoziazione automatica viene disabilitata sulla porta e il dispositivo che si connette non visualizza i parametri di negoziazione automatica. Il dispositivo di connessione si connette solo nella modalità half-duplex e la mancata corrispondenza del duplex risultante risulta in prestazioni scadenti e errori di porta. Tenere presente che se si imposta la velocità e la modalità duplex su un lato, è necessario impostare anche la velocità e la modalità duplex sul dispositivo di connessione per evitare questi problemi.

Per visualizzare lo stato della porta dopo aver impostato la velocità e la porta doshow duplex.

```
Switch-A (enable) set port speed 2/1 100
Port(s) 2/1 speed set to 100Mbps.
Switch-A (enable) set port duplex 2/1 full
Port(s) 2/1 set to full-duplex.
Switch-A (enable) show port
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                     connected  1          normal   full   100 10/100BaseTX
...
```

Di seguito sono riportati i risultati relativi alla tempistica:

```
Switch-A (enable) show time
Fri Feb 25 2000, 140528 Eastern
Switch-A (enable) set port enable 2/1
Port 2/1 enabled.
Switch-A (enable)
```

```
2000 Feb 25 140529 Eastern -0500 %PAGP-5-PORTTOSTP:Port 2/1 joined bridgeport 2/1
2000 Feb 25 140530 Eastern -0500 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 changed to
forwarding.
```

Il risultato finale dà un tempo di 2 secondi (da 0528 a 0530).

Èstato eseguito un altro test visivamente programmato avviando un ping continuo (ping -t) diretto allo switch su un PC collegato allo switch. Il cavo è stato quindi scollegato dallo switch. I ping iniziarono a fallire. Quindi, ricollegare il cavo allo switch e controllare gli orologi per verificare il tempo impiegato dallo switch per rispondere ai ping dal PC. Sono occorsi circa 5-6 secondi con la negoziazione automatica per la velocità e il duplex attivate e circa 4 secondi con la negoziazione automatica per la velocità e il duplex disattivate.

Ci sono molte variabili in questo test (inizializzazione PC, software PC, risposte alle richieste della porta della console dello switch e così via), ma volevi solo capire quanto tempo ci sarebbe voluto per ottenere una risposta dal punto di vista del PC. Tutti i test sono stati eseguiti dal punto di vista del messaggio di debug interno degli switch.

Come ridurre il ritardo di avvio sullo switch Catalyst 2900XL/3500XL

I modelli 2900XL e 3500XL possono essere configurati da un browser Web, o da SNMP, o dall'interfaccia della riga di comando (CLI). si utilizza la CLI. In questo esempio viene visualizzato lo stato dello spanning tree di una porta, si attiva portfast e quindi si verifica che sia attiva. Gli switch 2900XL/3500XL supportano EtherChannel e il trunking, ma non la creazione dinamica di EtherChannel (PAgP) o la negoziazione dinamica del trunk (DTP) nella versione testata (11.2(8.2)SA6), pertanto non è necessario disattivarli in questo test. Inoltre, dopo l'attivazione di portfast, il tempo trascorso per l'accensione della porta è già inferiore a 1 secondo, quindi non c'è molto da provare a modificare le impostazioni di negoziazione velocità/duplex per velocizzare il processo. Si spera che un secondo sia sufficientemente veloce! Per impostazione predefinita, portfast è disattivato sulle porte dello switch. Di seguito sono riportati i comandi per attivare portfast:Configurazione

```
2900XL#conf t
2900XL(config)#interface fastEthernet 0/1
2900XL(config-if)#spanning-tree portfast
2900XL(config-if)#exit
2900XL(config)#exit
2900XL#copy run start
```

Questa piattaforma è simile al router Cisco IOS; se si desidera salvarla in modo permanente, è necessario salvare la configurazione (avvio esecuzione copia).VerificaPer verificare che Portfast sia abilitato, eseguire questo comando:

```
2900XL#show spanning-tree interface fastEthernet 0/1
Interface Fa0/1 (port 13) in Spanning tree 1 is FORWARDING
```

```
   Port path cost 19, Port priority 128
   Designated root has priority 8192, address 0010.0db1.7800
   Designated bridge has priority 32768, address 0050.8039.ec40
   Designated port is 13, path cost 19
   Timers: message age 0, forward delay 0, hold 0
   BPDU: sent 2105, received 1
   The port is in the portfast mode
```

Controllare la configurazione dello switch.

```
2900XL#show running-config
Building configuration...

Current configuration:
!
version 11.2
...
!
interface VLAN1
 ip address 172.16.84.5 255.255.255.0
 no ip route-cache
!
interface FastEthernet0/1
 spanning-tree portfast
!
interface FastEthernet0/2
!
...
```

Test di temporizzazione su Catalyst 2900XLQuesti sono i test di temporizzazione eseguiti su Catalyst 2900XL.

La versione 11.2(8.2)SA6 del software è stata utilizzata sulla 2900XL per questi test.

```
Switch#show version
Cisco Internetwork Operating System Software
Cisco IOS (tm) C2900XL Software (C2900XL-C3H2S-M), Version 11.2(8.2)SA6, MAINTENANCE
INTERIM SOFTWARE
```

```
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 23-Jun-99 16:25 by boba
Image text-base: 0x00003000, data-base: 0x00259AEC

ROM: Bootstrap program is C2900XL boot loader

Switch uptime is 1 week, 4 days, 22 hours, 5 minutes
System restarted by power-on
System image file is "flash:c2900XL-c3h2s-mz-112.8.2-SA6.bin", booted via console

cisco WS-C2924-XL (PowerPC403GA) processor (revision 0x11) with 8192K/1024K bytes of
memory.
Processor board ID 0x0E, with hardware revision 0x01
Last reset from power-on

Processor is running Enterprise Edition Software
Cluster command switch capable
Cluster member switch capable
24 Ethernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:50:80:39:EC:40
Motherboard assembly number: 73-3382-04
Power supply part number: 34-0834-01
Motherboard serial number: FAA02499G7X
Model number: WS-C2924-XL-EN
System serial number: FAA0250U03P
Configuration register is 0xF
```

se si desidera che lo switch ci dica cosa succede e quando accade, è necessario immettere i seguenti comandi:

```
2900XL(config)#service timestamps debug uptime
2900XL(config)#service timestamps log uptime
2900XL#debug spantree events
Spanning Tree event debugging is on
2900XL#show debug
General spanning tree:
  Spanning Tree event debugging is on
```

Quindi, la porta in questione viene chiusa.

```
2900XL#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
2900XL(config)#interface fastEthernet 0/1
```

```
2900XL(config-if)#shut
2900XL(config-if)#
00:31:28: ST: sent Topology Change Notice on FastEthernet0/6
00:31:28: ST: FastEthernet0/1 - blocking
00:31:28: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively
down
00:31:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
down
2900XL(config-if)#exit
2900XL(config)#exit
2900XL#
```

A questo punto, i comandi vengono incollati dagli appunti nello switch. Questi comandi mostrano l'ora sul router 2900XL e riaccendono la porta:

```
show clock
conf t
int f0/1
no shut
```

Per impostazione predefinita, Portfast è disattivato. Potete confermarlo in due modi. Il primo modo è che il comando show spanning-tree interface non menziona Portfast. Il secondo modo è verificare questa configurazione in esecuzione e in cui il comando thespanning-tree portfastcommand non viene visualizzato nell'interfaccia.

```
2900XL#show spanning-tree interface fastEthernet 0/1
Interface Fa0/1 (port 13) in Spanning tree 1 is FORWARDING
   Port path cost 19, Port priority 128
   Designated root has priority 8192, address 0010.0db1.7800
   Designated bridge has priority 32768, address 0050.8039.ec40
   Designated port is 13, path cost 19
   Timers: message age 0, forward delay 0, hold 0
   BPDU: sent 887, received 1
[Note: there is no message about being in portfast mode is in this spot...]

2900XL#show running-config
Building configuration...
...
!
interface FastEthernet0/1
[Note: there is no spanning-tree portfast command under this interface...]
!
```

Ecco il primo test temporale con Portfast disattivato.

```
2900XL#show clock
*00:27:27.632 UTC Mon Mar 1 1993
2900XL#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
2900XL(config)#int f0/1
2900XL(config-if)#no shut
2900XL(config-if)#
00:27:27: ST: FastEthernet0/1 - listening
00:27:27: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
00:27:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up
00:27:42: ST: FastEthernet0/1 - learning
00:27:57: ST: sent Topology Change Notice on FastEthernet0/6
00:27:57: ST: FastEthernet0/1 - forwarding
```

Il tempo totale tra lo spegnimento e l'inizio dell'inoltro della porta è stato di 30 secondi (dalle 27.27 alle 27.57)

Per attivare Portfast, procedere come segue:

```
2900XL#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
2900XL(config)#interface fastEthernet 0/1
2900XL(config-if)#spanning-tree portfast
2900XL(config-if)#exit
2900XL(config)#exit
2900XL#
```

Per verificare che Portfast sia abilitato, usare il comando show spanning-tree interface. Si noti che l'output del comando (vicino alla fine) indica che Portfast è abilitato.

```
2900XL#show spanning-tree interface fastEthernet 0/1
Interface Fa0/1 (port 13) in Spanning tree 1 is FORWARDING
   Port path cost 19, Port priority 128
   Designated root has priority 8192, address 0010.0db1.7800
   Designated bridge has priority 32768, address 0050.8039.ec40
   Designated port is 13, path cost 19
   Timers: message age 0, forward delay 0, hold 0
   BPDU: sent 1001, received 1

The port is in the portfast mode
```

Èinoltre possibile verificare che Portfast è abilitato nell'output di configurazione.

```
2900XL#sh  ru
Building configuration...
...
interface FastEthernet0/1
 spanning-tree portfast

...
```

Eseguire ora il test di temporizzazione con Portfast abilitato

```
2900XL#show clock
*00:23:45.139 UTC Mon Mar 1 1993
2900XL#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
2900XL(config)#int f0/1
2900XL(config-if)#no shut
2900XL(config-if)#
00:23:45: ST: FastEthernet0/1 -jump to forwarding from blocking
00:23:45: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
00:23:45: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
```

In questo caso il tempo totale è stato inferiore a 1 secondo. Se il problema era causato dal ritardo di inizializzazione della porta sullo switch, portfast deve risolverlo.

Tenere presente che lo switch non supporta attualmente la negoziazione trunk, quindi non è necessario disattivarla. Né supporta PAgP per il trunking, quindi non è necessario disattivarlo. Lo switch supporta la negoziazione automatica della velocità e del duplex, ma poiché il ritardo è così ridotto, non sarebbe necessario disabilitarlo.

èstato inoltre eseguito il ping tra una workstation e lo switch. La risposta dallo switch ha impiegato circa 5-6 secondi, sia che la negoziazione automatica per la velocità e il duplex sia attivata o disattivata.

Come ridurre il ritardo di avvio sullo switch Catalyst 1900/2800

I numeri 1900/2820 si riferiscono a Portfast con un altro nome: Spantree Start-Forwarding. Per la versione del software in uso, eseguire (V8.01.05). L'impostazione predefinita è questa: Portfast è abilitato sulle porte Ethernet (10 Mbps) e Portfast è disabilitato sulle porte Fast Ethernet (uplink). Quindi, quando si mostra runto per visualizzare la configurazione, se una porta Ethernet non dice nulla su Portfast, Portfast è abilitato. Se nella configurazione viene visualizzato il messaggio "no spantree start-forwarding" (nessun inoltro spanttree in fase di avvio), Portfast è disabilitato. Su una porta

FastEthernet (100 Mbps), è vero il contrario: per una porta FastEthernet, Portfast è attiva solo se la porta mostra "spantree start-forwarding" nella configurazione.Di seguito è riportato un esempio di impostazione di Portfast su una porta FastEthernet. In questi esempi viene utilizzato il software Enterprise Edition versione 8. Dopo aver apportato le modifiche, la configurazione viene salvata automaticamente sullo switch 1900. Tenere presente che non si desidera abilitare Portfast sulle porte che si connettono a un altro switch o hub, ma solo se la porta è collegata a una unità terminale. La configurazione viene salvata automaticamente nella NVRAM.Configurazione

```
1900#show version
Cisco Catalyst 1900/2820 Enterprise Edition Software
Version V8.01.05
Copyright (c) Cisco Systems, Inc.  1993-1998
1900 uptime is 0day(s) 01hour(s) 10minute(s) 42second(s)
cisco Catalyst 1900 (486sxl) processor with 2048K/1024K bytes of memory
Hardware board revision is 5
Upgrade Status: No upgrade currently in progress.
Config File Status: No configuration upload/download is in progress
27 Fixed Ethernet/IEEE 802.3 interface(s)
Base Ethernet Address: 00-50-50-E1-A4-80
1900#conf t
Enter configuration commands, one per line.  End with CNTL/Z
1900(config)#interface FastEthernet 0/26
1900(config-if)#spantree start-forwarding
1900(config-if)#exit
1900(config)#exit
1900#
```

VerificaPer verificare che portfast sia attivo, occorre esaminare la configurazione. Tenere presente che una porta FastEthernet deve indicare che è accesa. Una porta Ethernet è accesa a meno che la configurazione non indichi che è spenta. In questa configurazione, l'interfaccia Ethernet 0/1 ha portfast disattivato (è possibile vedere il comando per spegnerlo), l'interfaccia Ethernet 0/2 ha portfast attivato (non si vede niente - il che significa che è attivato) e l'interfaccia Fast Ethernet 0/26 (porta A nel sistema di menu) ha portfast attivato (è possibile vedere il comando per attivarlo).

```
1900#show running-config
Building configuration...
```

```
...
!
interface Ethernet 0/1

  no spantree start-forwarding
!
interface Ethernet 0/2


!
...
!
interface FastEthernet 0/26
  spantree start-forwarding
```

Il modo più semplice per visualizzare lo stato di portfast è tramite il sistema di menu. Se si sceglie (P) per Port Configuration (Configurazione porta) dal menu principale, quindi si sceglie port, l'output indica se la modalità veloce porta è abilitata. Questo output viene generato per la porta FastEthernet 0/26, ossia la porta "A" sullo switch.

```
        Catalyst 1900 - Port A Configuration


        Built-in 100Base-FX
        802.1d STP State:  Blocking     Forward Transitions:  0


    ---------------------- Settings ------------------------------------
     [D] Description/name of port
     [S] Status of port                              Suspended-no-linkbeat
     [I] Port priority (spanning tree)               128 (80 hex)
     [C] Path cost (spanning tree)                   10
     [H] Port fast mode (spanning tree)              Enabled
     [E] Enhanced congestion control                 Disabled
     [F] Full duplex / Flow control                  Half-Duplex


    ---------------------- Related Menus -------------------------------
     [A] Port addressing           [V] View port statistics
     [N] Next port                 [G] Goto port
```

```
[P] Previous port              [X] Exit to Main Menu

Enter Selection:
```

Test di temporizzazione su Catalyst 1900

I valori di temporizzazione sono più difficili da verificare su uno switch 1900/2820 a causa della mancanza di strumenti di debug, quindi è stato appena avviato un ping da un PC collegato allo switch diretto allo switch stesso. Il cavo è stato scollegato e quindi ricollegato e è stato registrato il tempo impiegato dallo switch per rispondere al ping con Portfast acceso e con Portfast spento. Per una porta Ethernet con Portfast attivo (stato predefinito), il PC ha ricevuto una risposta entro 5-6 secondi. Con Portfast spento, il PC ha ricevuto una risposta in 34-35 secondi.

Ulteriori vantaggi per Portfast

L'utilizzo di Portfast nella rete offre inoltre un ulteriore vantaggio allo Spanning Tree. Ogni volta che un collegamento diventa attivo e passa allo stato di inoltro nello spanning tree, lo switch invia un pacchetto speciale dello spanning tree chiamato Topology Change Notification (TCN). La notifica TCN viene passata alla radice dello spanning tree, dove viene propagata a tutti gli switch della VLAN. In questo modo, tutti gli switch scadono la tabella di indirizzi MAC con il parametro forward delay. Il parametro di ritardo in avanti è in genere impostato su 15 secondi. Ogni volta che una workstation si unisce al gruppo bridge, gli indirizzi MAC di tutti gli switch vengono usati dopo 15 secondi anziché dopo i 300 secondi normali.Poiché quando una workstation diventa attiva non modifica realmente la topologia in misura significativa per quanto riguarda tutti gli switch della VLAN, non è necessario che passino attraverso il periodo di invecchiamento rapido del TCN. Se si attiva portfast, lo switch non invia pacchetti TCN quando una porta diventa attiva.

Comandi da utilizzare per verificare il funzionamento della configurazione

Questo è un elenco di comandi da usare quando si verifica se la configurazione funziona.4000/5000/6000

show port spantree 2/1: verificare se "Fast-Start" (Portfast) è abilitato o disabilitato

show spanttree 1: visualizza tutte le porte della VLAN 1 e se "Fast-Start" è abilitato

show port channel: verifica della presenza di canali attivi

show port channel 2: vedere la modalità canale (auto, off e così via) per ciascuna porta sul modulo 2

show trunk 2: vedere la modalità trunk (auto, off e così via) per ciascuna porta sul modulo 2

show port: visualizza lo stato (connected, notconnect e così via), la velocità e il duplex di tutte le porte dello switch

2900XL/3500XL

show spanning-tree interface Fast Ethernet 0/1- per verificare se Portfast è abilitata su questa porta (se si omette Portfast, la porta non è abilitata)

show running-config: se una porta visualizza il comando spanning-tree portfast, portfast è abilitata

1900/2800

show running-config: visualizza le impostazioni correnti (alcuni comandi non sono visibili quando rappresentano le impostazioni predefinite dello switch)

Utilizzare il sistema di menu per visualizzare la schermata di stato della porta

Comandi da utilizzare per risolvere i problemi relativi alla configurazione

Questo è un elenco di comandi da usare per risolvere i problemi relativi alla configurazione.4000/5000/6000

show port spantree 2/1: verificare se "Fast-Start" (Portfast) è abilitato o disabilitato

show spanttree 1: visualizza tutte le porte della VLAN 1 e se "Fast-Start" è abilitato

show port channel: verifica della presenza di canali attivi

show port channel 2: vedere la modalità canale (auto, off e così via) per ciascuna porta sul modulo 2

show trunk 2: vedere la modalità trunk (auto, off e così via) per ciascuna porta sul modulo 2

show port: visualizza lo stato (connected, notconnect e do on), la velocità e il duplex di tutte le porte dello switch

show logging: visualizza il tipo di messaggi che generano l'output di logging

set logging level spantree 7: imposta lo switch in modo che registri la porta spanning tree in tempo reale sulla console

set port disable 2/1: disattiva la porta nel software (come "shutdown" sul router)

set port enable 2/1: attiva la porta nel software (come "no shutdown" sul router)

show time: visualizza l'ora corrente in secondi (utilizzata all'inizio di un test di temporizzazione)

show port capabilities: verifica delle funzionalità implementate sulla porta

set trunk 2/1 off- imposta la modalità di trunking su off (per accelerare il tempo di inizializzazione della porta)

set port channel 2/1-2 off- imposta la modalità EtherChannel (PAgP) su off (per accelerare il tempo di inizializzazione della porta)

set port speed 2/1 100- imposta la porta a 100 Mbps e disattiva la negoziazione automatica

set port duplex 2/1 full- imposta la porta duplex su full

2900XL/3500XL

timestamp del servizio: tempo di attività del debug: visualizza l'ora con i messaggi di debug

tempo di attività del log dei timestamp del servizio: visualizza l'ora con i messaggi di log

debug spanttree events: visualizza gli eventi dello spanning tree quando la porta si sposta

show clock- per visualizzare l'ora corrente (per i test di temporizzazione)

show spanning-tree interface Fast Ethernet 0/1- per verificare se Portfast è abilitata su questa porta (se si omette Portfast, la porta non è abilitata)

chiudi- per disattivare una porta dal software

nessuna chiusura: per accendere una porta dal software

1900/2800

show running-config: visualizza le impostazioni correnti (alcuni comandi non sono visibili quando rappresentano le impostazioni predefinite dello switch)

Configurazione e risoluzione dei problemi di MLS (IP Multilayer Switching)Obiettivi

In questo documento viene descritto come risolvere i problemi di MLS (Multilayer Switching) per IP. Questa funzione è diventata un metodo altamente desiderato per accelerare le prestazioni di routing tramite l'uso di ASIC (Application Specific Integrated Circuits) dedicati. Il routing tradizionale viene eseguito tramite una CPU e un software centralizzati; MLS scarica una parte significativa del routing (riscrittura dei pacchetti) sull'hardware ed è anche noto come switching. MLS e lo switching di livello tre sono termini equivalenti. La funzionalità NetFlow di Cisco IOS è distinta e non è descritta nel presente documento. MLS include anche il supporto

per IPX (IPX MLS) e multicasting (MPLS), ma questo documento si concentra esclusivamente sulla risoluzione dei problemi relativi all'IP MLS di base.IntroduzioneCon l'aumento delle richieste sulle reti, aumenta anche la necessità di prestazioni più elevate. Un numero sempre maggiore di PC è connesso a LAN, WAN e Internet e i loro utenti richiedono un accesso rapido a database, file/pagine Web, applicazioni di rete, altri PC e streaming video. Per mantenere le connessioni rapide e affidabili, le reti devono essere in grado di adattarsi rapidamente alle modifiche e agli errori e di trovare il percorso migliore, il tutto senza compromettere l'invisibilità nei confronti degli utenti finali. Gli utenti finali che sperimentano un rapido flusso di informazioni tra il proprio PC e il server con un minimo rallentamento della rete sono soddisfatti. La determinazione del percorso migliore è la funzione principale dei protocolli di routing e può essere un processo ad uso intensivo della CPU; un aumento significativo delle prestazioni si ottiene scaricando una parte di questa funzione sull'hardware di switching. Questo è il punto della funzione MLS.I componenti principali di MLS sono tre: due di questi sono MLS-RP e MLS-SE. Il MLS-RP è il router abilitato per MLS, che svolge la tradizionale funzione di routing tra subnet/VLAN. MLS-SE è uno switch abilitato per MLS, che normalmente richiede un router per il routing tra le subnet/VLAN, ma con hardware e software speciali può gestire la riscrittura del pacchetto. Quando un pacchetto attraversa un'interfaccia di routing, le parti non riguardanti i dati vengono modificate (riscritte) durante il trasporto verso la destinazione, hop dopo hop. In questo caso, si potrebbe creare confusione, poiché sembra che un dispositivo di livello due svolga un'attività di livello tre. In realtà, lo switch sta solo riscrivendo le informazioni di livello tre e sta commutando tra subnet/VLAN. Il router è ancora responsabile dei calcoli del percorso basati su standard e della determinazione del miglior percorso. Gran parte di questa confusione può essere evitata se si mantengono le funzioni di routing e switching separate a livello mentale, soprattutto quando, come accade comunemente, sono contenute nello stesso chassis (come con un MLS-RP interno). Considerare MLS come un modo molto più avanzato per memorizzare il router nella cache, mantenendo la cache separata dal router su uno switch. Per MLS sono richiesti sia MLS-RP che MLS-SE, insieme ai rispettivi valori minimi di hardware e software.L'MLS-RP può essere interno (installato in uno chassis di switch) o esterno (collegato tramite un cavo a una porta trunk sullo switch). Esempi di MLS-RP interni sono il Route-Switch Module (RSM) e la Route-Switch Feature Card (RSFC), installati rispettivamente in uno slot o nel supervisore di un Catalyst 5xxx; lo stesso vale per il Multilayer Switch Feature Card (MSFC) per la famiglia Catalyst 6xxx. Esempi di MLS-RP esterni includono i membri dei router Cisco serie 7500, 7200, 4700, 4500 o 3600. In generale, per supportare la funzione MLS IP, tutti gli MLS-RP richiedono una versione minima di Cisco IOS nei treni 11.3WA o 12.0WA; consultare la documentazione della release per le specifiche. Affinché il router sia un MLS-RP, deve essere abilitato anche il protocollo MLS.MLS-SE è uno switch dotato di hardware

speciale. Per i prodotti Catalyst 5xxx, MLS richiede che sul supervisore sia installata una NetFlow Feature Card (NFFC); le IIG e IIG del supervisore ne hanno una per impostazione predefinita. Inoltre, è richiesto almeno il software Catalyst OS 4.1.1. Il treno 4.x è "passato alla General Deployment (GD)" o ha superato i rigorosi criteri dell'utente finale e gli obiettivi di esperienza sul campo per la stabilità, quindi controlla il sito Web di Cisco per le ultime versioni. Il protocollo IP MLS è supportato e abilitato automaticamente per l'hardware e il software Catalyst 6xxx con MSFC/PFC (per impostazione predefinita, sugli altri router il protocollo MLS è disabilitato). Notare che MLS IPX e MLS per multicasting possono avere requisiti hardware e software diversi (Cisco IOS e Catalyst OS). Più piattaforme Cisco supportano/possono supportare la funzione MLS. Affinché uno switch sia un MLS-SE, deve essere abilitato anche il protocollo MLS.Il terzo componente principale di MLS è il protocollo MLSP (Multilayer Switching Protocol). Questo perché, una volta comprese le nozioni di base dell'MLSP, si arriva al cuore dell'MLS, e questo è essenziale per risolvere efficacemente i problemi dell'MLS. MLSP viene utilizzato da MLS-RP e MLS-SE per comunicare tra loro; attività che abilitano MLS e che installano, aggiornano o eliminano flussi (informazioni della cache), e la gestione e l'esportazione delle statistiche di flusso (l'esportazione dei dati NetFlow è illustrata in altra documentazione). MLSP consente inoltre all'MLS-SE di conoscere gli indirizzi MAC (Media Access Control) delle interfacce del router abilitate per MLS, controllare la maschera di flusso dell'MLS-RP (illustrata più avanti in questo documento) e verificare che l'MLS-RP sia operativo. Il protocollo MLS-RP invia pacchetti multicast "hello" ogni 15 secondi con il protocollo MLSP; se tre di questi intervalli non vengono ricevuti, il protocollo MLS-SE riconosce che il protocollo MLS-RP non è riuscito o che la connettività ad esso è stata persa.

Nel diagramma sono illustrati tre elementi essenziali da completare (con MLSP) per la creazione di un collegamento: i passaggi candidati, attivatori e cache. MLS-SE verifica la presenza di una voce MLS nella cache. Se la voce della cache MLS e le informazioni sul pacchetto corrispondono (una richiesta di accesso), l'intestazione del pacchetto viene riscritta localmente sullo switch (un collegamento o un bypass del router) anziché essere inviata al router, come succede normalmente. I pacchetti che non corrispondono e che vengono inviati al MLS-RP sono potenziali pacchetti; ovvero, esiste la possibilità di commutarli localmente. Dopo aver passato il pacchetto candidato attraverso la maschera di flusso MLS (descritta in una sezione più avanti) e aver riscritto le informazioni contenute nell'intestazione del pacchetto (la parte dati non viene toccata), il router lo invia all'hop successivo sul percorso di destinazione. Il pacchetto viene ora denominato pacchetto di attivazione. Se il pacchetto ritorna allo stesso MLS-SE da cui è stato lasciato, viene creato un collegamento MLS che viene inserito nella cache MLS. La riscrittura del pacchetto e di

tutti i pacchetti simili che lo tracciano (detto flusso) viene ora eseguita localmente dall'hardware dello switch anziché dal software del router. Lo stesso MLS-SE deve vedere sia i pacchetti candidati che quelli abilitanti per un particolare flusso per poter creare un collegamento MLS(ecco perché la topologia di rete è importante per MLS). Tenere presente che lo scopo di MLS è quello di consentire il percorso di comunicazione tra due dispositivi su VLAN diverse, connessi tramite lo stesso switch, in modo da ignorare il router e migliorare le prestazioni della rete.Utilizzando la maschera di flusso (essenzialmente un elenco degli accessi), l'amministratore può regolare il grado di somiglianza di questi pacchetti e l'ambito dei flussi: indirizzo di destinazione, indirizzo di destinazione e indirizzo di origine oppure informazioni su destinazione, origine e livello quattro. Notare che il primo pacchetto di un flusso passa sempre attraverso il router; da quel momento in poi, viene commutato localmente. Ogni flusso è unidirezionale; la comunicazione tra PC, ad esempio, richiede la configurazione e l'utilizzo di due collegamenti. Lo scopo principale di MLSP è l'impostazione, la creazione e la gestione di queste scelte rapide.Questi tre componenti (l'MLS-RP, l'MLS-SE e l'MLSP) liberano le risorse vitali del router quando permettono ad altri componenti della rete di assumere alcune delle sue funzioni. A seconda della topologia e della configurazione, MLS fornisce un metodo semplice ed estremamente efficace che migliora le prestazioni della rete LAN.Risoluzione dei problemi relativi alla tecnologia MLS IPIn questo documento viene illustrato un diagramma di flusso da utilizzare per risolvere i problemi relativi ai servizi MLS IP di base. Deriva dai tipi più comuni di richieste MLS-IP aperte con il sito Web del supporto tecnico Cisco e affrontate da utenti e tecnici del supporto tecnico fino al momento della creazione del presente documento. La funzionalità MLS è affidabile e non deve presentare problemi. In caso di problemi, è possibile risolvere i tipi di problemi MLS IP più probabili. Vengono fatte alcune ipotesi essenziali:

Dopo aver familiarizzato con i passaggi di configurazione di base necessari per abilitare il protocollo MLS IP sul router e sugli switch, i clienti hanno completato i seguenti passaggi: per un materiale eccellente, consultare le risorse elencate alla fine di questo documento.

Il routing IP è abilitato sul protocollo MLS-RP (è attivo per impostazione predefinita): se il comando no ip routing è presente nella configurazione globale di asshow run, è stato disattivato e IP MLS non funziona.

Esiste una connettività IP tra il protocollo MLS-RP e il protocollo MLS-SE:eseguire il ping degli indirizzi IP del router dallo switch e cercare i punti esclamativi (chiamati 'bang') da visualizzare in cambio.

Le interfacce MLS-RP sono in stato 'up/up' sul router: digitare show ip interface brief sul router per confermare questa condizione.

Avviso: ogni volta che si apportano modifiche alla configurazione di un router che deve essere permanente, ricordarsi di salvare le modifiche con copy running-config Starting-config (le versioni abbreviate di questo comando includono copy run startandwr mem). Le modifiche apportate alla configurazione vengono perse se il router viene ricaricato o reimpostato. L'RSM, l'RSFC e l'MSFC sono router, non switch. Al contrario, le modifiche apportate al prompt dello switch di un membro della famiglia Catalyst 5xxx o 6xxx vengono salvate automaticamente.

In questa sezione vengono descritti i problemi relativi alla tecnologia MLS IP.

I requisiti hardware e software minimi sono soddisfatti?

Aggiornare MLS-RP e SE per soddisfare i requisiti hardware e software minimi. Per il modello MLS-RP non è richiesto hardware aggiuntivo. Anche se MLS può essere configurato su interfacce non trunking, la connessione a MLS-SE generalmente avviene tramite interfacce VLAN (come con un RSM) o supporta il trunking (può essere configurato in modo da trasportare più informazioni VLAN configurando ISL o 802.1q). Inoltre, tenere presente che, al momento della pubblicazione, solo i membri delle famiglie di router 7500, 7200, 4700, 4500 e 3600 supportano MLS esternamente. Al momento, solo questi router esterni e i router che appartengono alle famiglie di switch Catalyst 5xxx o 6xxx (come l'RSM e l'RSFC per la famiglia Catalyst 5xxx e l'MSFC per la famiglia Catalyst 6xxx) possono essere MLS-RP. L'MSFC richiede anche la Policy Feature Card (PFC), entrambe installate sul Supervisor Catalyst 6xx. Il protocollo IP MLS è ora una funzionalità standard del software Cisco IOS versione 12.0 e successive. Per i software Cisco IOS versione inferiore a Cisco IOS 12.0 è in genere necessario un treno speciale; per il supporto di MLS IP di questo tipo, installare le immagini più recenti in Cisco IOS 11.3 con le lettere 'WA' nei nomi dei file.

Per il modello MLS-SE, è richiesta una scheda NFC (NetFlow Feature Card) per un dispositivo della famiglia Catalyst 5xxx; la scheda viene installata nel modulo Supervisor dello switch Catalyst e inclusa come hardware standard nei nuovi Supervisor Catalyst serie 5xxx (ossia dal 1999). La NFFC non è supportata sui Supervisor I o II ed è un'opzione dei primi Supervisor III. Inoltre, per il protocollo MLS IP, è richiesto almeno il protocollo CatOS 4.1.1. Per la famiglia Catalyst 6xxx, invece, l'hardware richiesto è fornito come apparecchiatura standard e il protocollo IP MLS è supportato dalla prima versione del software CatOS, la 5.1.1 (infatti, il protocollo IP MLS è un componente essenziale e predefinito per le sue prestazioni elevate). Con le nuove piattaforme e il nuovo software che supportano il protocollo IP MLS, è importante consultare la documentazione e le note sulla versione e, in generale, installare l'ultima versione nella versione più bassa che soddisfi i requisiti della vostra funzione. Consulta sempre le note sulla versione e consulta l'ufficio vendite Cisco locale per ottenere nuovo supporto MLS e per gli sviluppi delle funzionalità.

I comandi fusi per controllare le versioni hardware e software installate sul router e visualizzare il modulo sullo switch

Nota: al momento la famiglia di switch Catalyst 6xxx NON supporta MLS-RP esterni. Il valore MLS-RP deve essere un MSFC.

I dispositivi di origine e di destinazione si trovano su VLAN diverse dello stesso MLS-SE, e condividono un unico MLS-RP?

Il router deve disporre di un percorso a ciascuna VLAN. Tenere presente che lo scopo della licenza MLS è creare un collegamento tra due VLAN, in modo che il routing tra i due dispositivi terminali possa essere eseguito dallo switch, e in questo modo il router viene liberato per altre attività. Lo switch non effettua realmente il routing; riscrive i frame in modo che appaia ai dispositivi terminali che comunicano attraverso il router. Se i due dispositivi si trovano sulla stessa VLAN, MLS-SE commuta il frame localmente senza usare MLS, come fanno gli switch in un ambiente con bridging trasparente, e non viene creato alcun collegamento MLS. È possibile avere più switch e router nella rete e anche più switch lungo il percorso di flusso, ma il percorso tra i due dispositivi terminali per i quali si desidera un collegamento MLS deve includere un singolo MLS-RP in quella VLAN per quel percorso. In altre parole, il flusso tra l'origine e la destinazione deve attraversare un limite VLAN sullo stesso MLS-RP e una coppia di pacchetti candidato e attivatore deve essere vista dallo stesso MLS-SE per poter creare il collegamento MLS. Se questi criteri non vengono soddisfatti, il pacchetto viene indirizzato normalmente senza l'uso di MLS. Per i diagrammi e le discussioni relative alle topologie di rete supportate e non supportate, fare riferimento ai documenti suggeriti alla fine di questo documento.

L'MLS-RP contiene anmls rp ipstatement sia nella configurazione globale che in quella dell'interfaccia?

Se non ne è presente una, addmls rp esegue le istruzioni in modo appropriato su MLS-RP. Questo passaggio di configurazione è obbligatorio, ad eccezione dei router per cui il protocollo MLS IP è abilitato automaticamente (come l'MSFC Catalyst 6xxx). Per la maggior parte dei MLS-RP (router configurati per MLS IP), questa istruzione deve essere visualizzata sia nella configurazione globale sia nella configurazione interfaccia.

Nota: quando si configura il protocollo MLS-RP, ricordare anche di posizionare il comando rp management-interface sotto una delle relative interfacce IP MLS. Questo passaggio obbligatorio indica all'MLS-RP da quale interfaccia deve inviare i messaggi MLSP per comunicare con l'MLS-SE. Anche in questo caso, è necessario usare questo comando su una sola interfaccia.

Nell'interfaccia MLS-RP sono configurate funzionalità che disabilitano automaticamente MLS?

Il router offre diverse opzioni di configurazione che non sono compatibili con MLS. tra cui accounting IP, crittografia, compressione, protezione IP, NAT (Network Address Translation) e CAR (Committed Access Rate). Per ulteriori informazioni, fare riferimento ai collegamenti nella configurazione IP MLS inclusa alla fine di questo documento. I pacchetti che attraversano un'interfaccia router configurata con una di queste funzionalità devono essere indirizzati normalmente; non viene creato alcun collegamento MLS. Affinché MLS funzioni correttamente, disattivare queste funzioni sull'interfaccia MLS-RP.

Un'altra importante caratteristica che influisce su MLS sono gli elenchi degli accessi, sia in entrata che in uscita. Per ulteriori informazioni su questa opzione, vedere 'flowmask'.

MLS-SE riconosce l'indirizzo MLS-RP?

Affinché MLS funzioni, lo switch deve riconoscere il router come MLS-RP. Gli MLS-RP interni (di nuovo l'RSM o l'RSFC in un Catalyst 5xxx e l'MSFC in un Catalyst 6xxx) vengono riconosciuti automaticamente da MLS-SE sul quale sono installati. Per i moduli MLS-RP esterni, è necessario informare esplicitamente lo switch dell'indirizzo del router. Questo

indirizzo non è in realtà un indirizzo IP, anche se su MLS-RP esterni viene scelto dall'elenco di indirizzi IP configurati sulle interfacce del router; è semplicemente un ID router. Infatti, per gli MLS-RP interni, l'MLS-ID normalmente non è nemmeno un indirizzo IP configurato sul router; poiché gli MLS-RP interni vengono inclusi automaticamente, in genere si tratta di un indirizzo di loopback (127.0.0.x). Affinché MLS funzioni, includere su MLS-SE l'MLS-ID trovato su MLS-RP.

Usare il comando mls sul router per trovare l'MLS-ID. Quindi, configurare l'ID sullo switch con il comando mls include <MLS-ID>. Questa operazione di configurazione è obbligatoria quando si utilizzano moduli MLS-RP esterni.

Nota: se si modifica l'indirizzo IP delle interfacce MLS-RP e poi si ricarica il router, è possibile che il processo MLS sul router scelga un nuovo MLS-ID. Questo nuovo MLS-ID può essere diverso da quello incluso manualmente in MLS-SE, che può causare l'arresto di MLS. Non si tratta di un problema software, ma di un effetto dello switch che tenta di comunicare con un MLS-ID non più valido. Accertarsi di includere questo nuovo MLS-ID sullo switch per far sì che MLS funzioni nuovamente. Può essere inoltre necessario disabilitare/abilitare il protocollo MLS IP.

Nota: quando MLS-SE non è direttamente connesso a MLS-RP, come per questa topologia, l'indirizzo che deve essere incluso in MLS-SE può essere visualizzato come indirizzo di loopback indicato: uno switch collegato tra MLS-SE e MLS-RP. È necessario includere l'MLS-ID anche se l'MLS-RP è interno. Sul secondo switch, l'MLS-RP appare come router esterno poiché l'MLS-RP e l'MLS-SE non sono contenuti nello stesso chassis.

L'interfaccia MLS-RP e MLS-SE si trovano nello stesso dominio VTP abilitato?

MLS richiede che i componenti MLS, insieme alle stazioni terminali, si trovino nello stesso dominio VTP (Virtual Trunking Protocol). Il VTP è un protocollo di layer due utilizzato per gestire le VLAN su diversi switch Catalyst da uno switch centrale. Consente agli amministratori di creare o eliminare una VLAN su tutti gli switch di un dominio, ma non su tutti gli switch del dominio. Il protocollo MLSP (Multilayer Switching Protocol), utilizzato da MLS-SE e MLS-RP per comunicare tra loro, non supera un limite di dominio VTP. Se l'amministratore di rete ha abilitato il VTP sugli switch (il VTP è abilitato sui membri della famiglia Catalyst 5xxx e 6xxx per impostazione predefinita), usare il comando show vtp domain sullo switch per sapere in quale dominio VTP è stato posizionato MLS-SE. Ad eccezione dell'MSFC Catalyst 6xxx, su cui MLS è essenzialmente *plug-and*-play, è necessario aggiungere successivamente il dominio VTP a ciascuna delle interfacce MLS del router. Ciò consente ai multicast MLSP di spostarsi tra MLS-RP e MLS-SE e permette al MLS di funzionare.

In modalità di configurazione interfaccia di MLS-RP, immettere i seguenti comandi:

nessun MLS mls rp ipDisable sull'interfaccia MLS-RP interessata prima di modificare il dominio VTP.

mls rp vtp-domain < nome dominio VTP>Il nome di dominio VTP su ciascuna interfaccia abilitata per MLS deve corrispondere a quello dello switch.

mls rp vlan-id <VLAN #>Richiesto solo per interfacce MLS-RP esterne e non di trunking ISL.

mls rp management-interfaceEseguire questa operazione su una sola interfaccia del server MLS-RP. Questo passaggio obbligatorio indica al protocollo MLS-RP da quale interfaccia deve inviare i messaggi MLSP.

mls rp ipEnable MLS ancora una volta sull'interfaccia di MLS-RP.

Per modificare il nome di dominio VTP dell'MLS-SE, usare questo comando al prompt di abilitazione CatOS dello switch:

set vtp domain name <nome dominio VTP>

Affinché MLS funzioni, verificare che il VTP sia abilitato sullo switch:

set vtp enable

Le maschere di flusso concordano su MLS-RP e MLS-SE?

Una maschera di flusso è un filtro configurato da un amministratore di rete e utilizzato da MLS per determinare se è necessario creare un collegamento. Proprio come un elenco degli accessi, più dettagliati sono i criteri impostati, più a fondo il pacchetto deve essere esaminato dal processo MLS per verificare se il pacchetto soddisfa tali criteri. Per regolare l'ambito dei collegamenti creati da MLS, la maschera di flusso può essere resa più o meno specifica; la maschera di flusso è essenzialmente un dispositivo. I tipi di modalità MLS IP sono tre: IP destinazione, IP origine destinazione e IP flusso completo. La modalità IP di destinazione, predefinita, è in uso quando all'interfaccia del router abilitata per MLS non viene applicato alcun elenco degli accessi. La modalità origine-destinazione-IP è in uso quando si applica un elenco degli accessi standard. Full-flow-IP è attivo per un elenco degli accessi esteso. La modalità MLS sul MLS-RP è determinata implicitamente dal tipo di elenco degli accessi applicato all'interfaccia. Al contrario, la modalità MLS su MLS-SE è configurata esplicitamente. Se viene scelta la modalità appropriata, l'utente può quindi configurare MLS in modo che solo l'indirizzo di destinazione corrisponda per poter creare un collegamento MLS, o sia l'origine che la destinazione, o anche informazioni di livello quattro come i numeri di porta TCP/UDP.

La modalità MLS è configurabile sia su MLS-RP che su MLS-SE e, in generale, devono corrispondere. SE si ritiene che sia necessaria la modalità IP di origine e destinazione o la modalità MLS IP a flusso completo, è consigliabile configurarla sul router e applicare l'elenco degli accessi appropriato. MLS sceglie sempre la maschera più specifica. La maschera di flusso configurata sul MLS-RP ha la precedenza su quella trovata sul MLS-SE. PRESTARE ATTENZIONE se si cambia la modalità MLS dello switch dall'indirizzo IP di destinazione predefinito: per far funzionare il protocollo MLS, è necessario verificare che corrisponda alla modalità MLS sul router. Per le modalità origine-destinazione-ip e flusso-ip completo, ricordarsi di applicare l'elenco degli accessi all'interfaccia del router appropriata; senza applicare alcun elenco degli accessi, anche se configurata, la modalità MLS è semplicemente ip destinazione, che è l'impostazione predefinita.

Avviso: ogni volta che viene modificata la maschera di flusso, sia su MLS-RP che su MLS-SE, tutti i flussi MLS memorizzati nella cache vengono eliminati e il processo MLS viene riavviato. L'eliminazione può verificarsi anche quando si applica il comando clear ip route-cache sul router. Se si applica il comando di configurazione globale del router su ip routing, che disabilita il routing IP e essenzialmente trasforma il router in un bridge trasparente, il router viene eliminato e disabilitato dal protocollo MLS (ricordate che il routing è un prerequisito di MLS). Ognuna di queste caratteristiche può influire temporaneamente, ma in modo significativo, sulle prestazioni del router in una rete di produzione. Il router subisce un sovraccarico finché non vengono creati i nuovi collegamenti in quanto deve ora gestire tutti i flussi precedentemente elaborati dallo switch.

Nota: soprattutto se si considera un prodotto della famiglia Catalyst 5000 come MLS-SE, è

necessario evitare l'uso molto esteso di maschere di flusso configurate con informazioni di livello quattro. Se il router è obbligato a eseguire il peer in modo così approfondito in ogni pacchetto sull'interfaccia, molti dei vantaggi previsti del protocollo MLS vengono ignorati. Questo non è un problema quando si usa un dispositivo della famiglia Catalyst 6xxx come MLS-SE in quanto le porte dello switch possono riconoscere le informazioni di livello quattro.

Nota: fino a poco tempo fa, MLS non supportava le maschere di flusso configurate in entrata su un'interfaccia MLS-RP, ma solo in uscita. Se si utilizza il comando mls rp ip input-acl in aggiunta ai normali comandi di configurazione MLS-RP su un'interfaccia del router, viene supportata una maschera di flusso in ingresso.

Sono più di un paio di *MLST troppi* messaggi di errore moveserror continuamente visualizzati sullo switch?

Come indicato nella nota, per modificare una maschera di flusso, cancellare la cache route o disattivare globalmente il routing IP provoca un'eliminazione della cache. Altre circostanze possono inoltre causare epurazioni complete o di più singole voci e causare il lamentarsi *di troppe mosse da parte di* MLS. Questo messaggio ha varie forme, ma ognuna contiene queste tre parole. A parte quanto già detto, la causa più comune di questo errore è quando lo switch apprende più indirizzi MAC (Media Access Control) Ethernet identici all'interno della stessa VLAN. Gli standard Ethernet non consentono indirizzi MAC identici all'interno della stessa VLAN. Se il messaggio viene visualizzato di rado o solo qualche volta di seguito, non c'è motivo di preoccuparsi; MLS è una funzionalità affidabile e il messaggio può essere causato semplicemente da eventi di rete normali, ad esempio una connessione PC spostata tra le porte. Se osservato continuamente per diversi minuti, è probabile che sia un sintomo di un problema più grave.

In questo caso, la causa principale è in genere la presenza di due dispositivi con lo stesso indirizzo MAC effettivamente collegati a una VLAN, o di un loop fisico all'interno della VLAN (o di più VLAN se si crea un bridge su questi domini di broadcast). Risoluzione dei problemi con spanning-tree (illustrati in altri documenti) e suggerimento per trovare il loop ed eliminarlo. Inoltre, eventuali modifiche rapide della topologia possono causare instabilità temporanea della rete (e di MLS) (interfacce del router con flapping, una scheda di interfaccia di rete (NIC) difettosa e così via).

Suggerimento: utilizzare i comandi show mls notificationand show looktablesullo switch per indirizzare l'utente nella direzione del duplicato dell'indirizzo MAC o del loop fisico. Il primo fornisce un valore TA. Il comando show looktable <TA value>restituisce un possibile indirizzo MAC che può essere tracciato alla radice del problema.## Informazioni correlate

Sommario

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).