Best practice per gli switch Catalyst serie 6500/6000 e Catalyst serie 4500/4000 con software Cisco IOS

Sommario

Introduzione

In questo documento vengono illustrate le best practice per gli switch Catalyst serie 6500/6000 e 4500/4000 con software Cisco IOS® su Supervisor Engine.

Gli switch Catalyst serie 6500/6000 e Catalyst serie 4500/4000 supportano uno di questi due sistemi operativi che vengono eseguiti sul Supervisor Engine:

- CatOS (Catalyst OS)
- Software Cisco IOS

Con CatOS, è possibile eseguire il software Cisco IOS su schede secondarie del router o moduli quali:

- Il modulo Multilayer Switch Feature Card (MSFC) negli switch Catalyst 6500/6000
- Modulo 4232 Layer 3 (L3) in Catalyst 4500/4000

In questa modalità, sono disponibili due righe di comando per la configurazione:

- Riga di comando CatOS per lo switching
- Riga di comando del software Cisco IOS per il routing

CatOS è il software di sistema, in esecuzione sul Supervisor Engine. Il software Cisco IOS in esecuzione sul modulo di routing è un'opzione che richiede il software di sistema CatOS.

Per il software Cisco IOS, è disponibile una sola riga di comando per la configurazione. In questa modalità, le funzionalità di CatOS sono state integrate nel software Cisco IOS. Il risultato dell'integrazione è una singola riga di comando per la configurazione di switching e routing. In questa modalità, il software Cisco IOS è il software di sistema e sostituisce CatOS.

I sistemi operativi CatOS e Cisco IOS Software vengono entrambi implementati nelle reti critiche. CatOS, con l'opzione software Cisco IOS per le schede secondarie e i moduli del router, è supportato nelle seguenti serie di switch:

- Catalyst 6500/6000
- Catalyst 5500/5000
- Catalyst 4500/4000

Il software di sistema Cisco IOS è supportato nelle seguenti serie di switch:

- Catalyst 6500/6000
- Catalyst 4500/4000

Per informazioni sul software di sistema CatOS, fare riferimento al documento Best Practices for Catalyst 4500/4000, 5500/5000 e 6500/6000 Series Running CatOS Configuration and Management.

Il software di sistema Cisco IOS offre agli utenti alcuni dei seguenti vantaggi:

- Un'unica interfaccia utente
- Una piattaforma di gestione unificata della rete
- Funzioni QoS avanzate
- Supporto switching distribuito

Questo documento offre linee guida per la configurazione modulare. Pertanto, potete leggere ogni

sezione in modo indipendente e apportare modifiche in un approccio a fasi. Per questo documento si presume che l'interfaccia utente del software Cisco IOS abbia una comprensione e una familiarità di base. Il documento non copre la progettazione generale della rete del campus.

Operazioni preliminari

Sfondo

Le soluzioni presentate in questo documento rappresentano anni di esperienza sul campo da parte di tecnici Cisco che lavorano con reti complesse e molti dei più grandi clienti. Di conseguenza, in questo documento vengono enfatizzate le configurazioni del mondo reale che rendono le reti efficienti. Questo documento offre le seguenti soluzioni:

- Soluzioni che, statisticamente, presentano la più ampia esposizione sul campo e, quindi, il rischio più basso
- Soluzioni semplici, che concedono una certa flessibilità per risultati deterministici
- Soluzioni facili da gestire e configurate dai team operativi di rete
- Soluzioni che promuovono alta disponibilità e alta stabilità

Riferimenti

Sono disponibili diversi siti di riferimento per le linee di prodotti Catalyst 6500/6000 e Catalyst 4500/4000 su Cisco.com. I riferimenti elencati in questa sezione forniscono ulteriori informazioni sugli argomenti trattati in questo documento.

Per ulteriori informazioni su uno degli argomenti trattati in questo documento, fare riferimento al supporto della tecnologia di switching LAN. La pagina di supporto fornisce la documentazione del prodotto, nonché i documenti di risoluzione dei problemi e di configurazione.

In questo documento vengono forniti riferimenti al materiale in linea pubblico in modo che sia possibile approfondire la lettura. Ma altri buoni riferimenti fondativi ed educativi sono:

- Cisco ISP Essentials
- Confronto tra i sistemi operativi Cisco Catalyst e Cisco IOS per gli switch Cisco Catalyst serie 6500
- Cisco LAN Switching (serie CCIE Professional Development)
- Creazione di reti commutate multilayer Cisco
- Gestione di prestazioni e errori
- SICURO: Un progetto di sicurezza per le reti aziendali
- Manuale per applicazioni Cisco: Configurazione degli switch Catalyst

Configurazione di base

In questa sezione vengono descritte le funzionalità distribuite quando si utilizza la maggior parte delle reti Catalyst.

Protocolli Catalyst Control Plane

In questa sezione vengono illustrati i protocolli in esecuzione tra gli switch in condizioni operative

normali. Una comprensione di base dei protocolli è utile quando si affronta ogni sezione.

Traffico Supervisor Engine

La maggior parte delle funzionalità abilitate in una rete Catalyst richiede la collaborazione di due o più switch. Pertanto, è necessario uno scambio controllato di messaggi keepalive, parametri di configurazione e modifiche di gestione. Che si tratti di protocolli di proprietà di Cisco, come Cisco Discovery Protocol (CDP), o basati su standard, come IEEE 802.1D (Spanning Tree Protocol [STP]), tutti hanno alcuni elementi in comune quando i protocolli vengono implementati sulla serie Catalyst.

Nell'inoltro di frame di base, i frame di dati utente hanno origine dai sistemi finali. L'indirizzo di origine (SA) e l'indirizzo di destinazione (DA) dei frame di dati non vengono modificati in tutti i domini a commutazione di livello 2 (L2). Le tabelle di ricerca CAM (Content-addressable memory) su ciascuno switch Supervisor Engine sono popolate da un processo di apprendimento SA. Le tabelle indicano la porta di uscita che inoltra ciascun frame ricevuto. Se la destinazione è sconosciuta o il frame è destinato a un indirizzo broadcast o multicast, il processo di apprendimento dell'indirizzo è incompleto. Quando il processo è incompleto, il frame viene inoltrato (esteso) a tutte le porte della VLAN. Lo switch deve inoltre riconoscere i frame da commutare attraverso il sistema e i frame da indirizzare alla CPU dello switch stessa. La CPU dello switch è nota anche come Network Management Processor (NMP).

Per creare il piano di controllo Catalyst vengono utilizzate voci speciali nella tabella CAM. Queste voci speciali sono denominate voci di sistema. Il control plane riceve e indirizza il traffico all'NMP su una porta dello switch interna. Pertanto, con l'uso di protocolli con indirizzi MAC di destinazione noti, il traffico del control plane può essere separato dal traffico di dati.

Cisco ha un intervallo riservato di indirizzi MAC e di protocollo Ethernet, come mostrato nella tabella in questa sezione. Questo documento descrive in dettaglio tutti gli indirizzi riservati, ma la tabella fornisce un riepilogo per comodità:

Funzionalità	Tipo di protocollo SNAP[1] HDLC[2]	MAC multicast di destinazione
PAgP[3]	0x0104	01-00-0c-cc-cc-cc
PVST+, RPVST+[4]	0x010b	01-00-0c-cc-cc-cd
Bridge VLAN	0x010c	01-00-0c-cd-cd-ce
UDLD[5]	0x0111	01-00-0c-cc-cc-cc
CDP	0x2000	01-00-0c-cc-cc-cc
DTP[6]	0x2004	01-00-0c-cc-cc-cc
STP UplinkFast	0x200a	01-00-0c-cd-cd-cd
Spanning Tree IEEE 802.1D	N/D—DSAP[7] 42 SSAP[8] 42	01-80-c2-00-00-00
ISL[9]	N/D	01-00-0c-00-00-00
VTP[10]	0x2003	01-00-0c-cc-cc-cc
Pausa IEEE	N/D: DSAP 81	01-80-C2-00-00-00>0F

802.3x	SAP 80	

[1] SNAP = Protocollo di accesso alla sottorete.

[2] HDLC = controllo di collegamento dati di alto livello.

[3] PAgP = Protocollo di aggregazione porte.

[4] PVST+ = Per VLAN Spanning Tree+ e RPVST+ = Rapid PVST+.

[5] UDLD = Rilevamento collegamenti unidirezionali.

[6] DTP = Dynamic Trunking Protocol.

[7] DSAP = punto di accesso al servizio di destinazione.

[8] SSAP = punto di accesso al servizio di origine.

[9] ISL = Collegamento tra switch.

[10] VTP = VLAN Trunk Protocol.

La maggior parte dei protocolli di controllo Cisco utilizza un incapsulamento SNAP IEEE 802.3, che include Logical Link Control (LLC) 0xAAAA03 e Organizational Unique Identifier (OUI) 0x00000C. Potete vederlo su una traccia di LAN Analyzer.

Questi protocolli presuppongono una connettività point-to-point. L'uso deliberato di indirizzi di destinazione multicast consente a due switch Catalyst di comunicare in modo trasparente su switch non Cisco. I dispositivi che non comprendono e intercettano i frame si limitano a inondarli. Tuttavia, le connessioni point-to-multipoint negli ambienti multifornitore possono causare comportamenti incoerenti. In generale, evitare connessioni point-to-multipoint in ambienti multifornitore. Questi protocolli terminano sui router di layer 3 e funzionano solo all'interno di un dominio di switch. Questi protocolli ricevono la priorità sui dati utente tramite l'elaborazione e la pianificazione ASIC (Application-Specific Integrated Circuit) in entrata.

Ora la discussione verte sull'associazione di protezione. I protocolli dello switch utilizzano un indirizzo MAC ricavato da un gruppo di indirizzi disponibili. Un EPROM sullo chassis fornisce la banca di indirizzi disponibili. Usare il comando **show module** per visualizzare gli intervalli di indirizzi disponibili per ciascun modulo per la sorgente del traffico, ad esempio BPDU (STP Bridge Protocol Data Unit) o frame ISL. Di seguito viene riportato un esempio di output del comando:

```
>show module
…

Mod MAC-Address(es)                         Hw     Fw          Sw
--- --------------------------------------- ------ ----------  -----------------
1   00-01-c9-da-0c-1e to 00-01-c9-da-0c-1f 2.2    6.1(3)      6.1(1d)
    00-01-c9-da-0c-1c to 00-01-c9-da-0c-1
    00-d0-ff-88-c8-00 to 00-d0-ff-88-cb-ff
!--- These are the MACs for sourcing traffic.
```

VLAN 1

La VLAN 1 ha un significato speciale nelle reti Catalyst.

Quando si esegue il trunking, Catalyst Supervisor Engine usa sempre la VLAN predefinita, la VLAN 1, per contrassegnare un numero di protocolli di controllo e gestione. Tali protocolli includono CDP, VTP e PAgP. Per impostazione predefinita, tutte le porte dello switch, compresa l'interfaccia sc0 interna, sono configurate in modo da essere membri della VLAN 1. Per impostazione predefinita, tutti i trunk trasportano la VLAN 1.

Queste definizioni sono necessarie per aiutare a chiarire alcuni termini ben utilizzati nelle reti Catalyst:

- La VLAN di gestione è la posizione in cui sc0 risiede sugli switch CatOS e low-end. La VLAN può essere modificata. Tenere presente questa condizione quando si interagiscono entrambi gli switch CatOS e Cisco IOS.
- La VLAN nativa è la VLAN a cui torna una porta quando non è in corso il trunking. Inoltre, la VLAN nativa è la VLAN senza tag su un trunk IEEE 802.1Q.

Esistono diversi buoni motivi per configurare una rete e modificare il comportamento delle porte nella VLAN 1:

- Quando il diametro della VLAN 1, come di qualsiasi altra VLAN, raggiunge dimensioni tali da costituire un rischio per la stabilità, in particolare nella prospettiva di un STP, è necessario riorganizzare la VLAN. Per ulteriori informazioni, vedere la sezione Switch Management Interface and Native VLAN.
- Per semplificare la risoluzione dei problemi e ottimizzare i cicli della CPU disponibili, è necessario mantenere separati i dati del control plane sulla VLAN 1 dai dati utente. Evitare i loop di layer 2 nella VLAN 1 quando si progettano reti campus multilivello senza STP. Per evitare loop di layer 2, cancellare manualmente la VLAN 1 dalle porte del trunk.

In sintesi, annotare le seguenti informazioni sui tronchi:

- Gli aggiornamenti CDP, VTP e PAgP vengono sempre inoltrati sui trunk con un tag VLAN 1. Ciò si verifica anche se la VLAN 1 è stata eliminata dai trunk e non è la VLAN nativa. Se si cancella la VLAN 1 per i dati utente, l'azione non ha alcun impatto sul traffico del control plane che viene ancora inviato con l'uso della VLAN 1.
- Su un trunk ISL, i pacchetti DTP vengono inviati sulla VLAN1. Ciò si verifica anche se la VLAN 1 è stata cancellata dal trunk e non è più la VLAN nativa. Su un trunk 802.1Q, i pacchetti DTP vengono inviati sulla VLAN nativa. In questo caso, anche se la VLAN nativa è stata cancellata dal trunk.
- Nella tecnologia PVST+, le BPDU IEEE 802.1Q vengono inoltrate senza tag sulla VLAN 1 dello Spanning Tree comune per consentire l'interoperabilità con altri fornitori, a meno che la VLAN 1 non sia stata cancellata dal trunk. Ciò avviene indipendentemente dalla configurazione VLAN nativa. Le PVST+ BPDU Cisco vengono inviate e contrassegnate per tutte le altre VLAN. Per ulteriori informazioni, vedere la sezione Spanning Tree Protocol.
- Le BPDU 802.1s Multiple Spanning Tree (MST) vengono sempre inviate sulla VLAN 1 sui trunk ISL e 802.1Q. Ciò si applica anche quando la VLAN 1 è stata eliminata dai trunk.
- Non cancellare o disabilitare la VLAN 1 sui trunk tra i bridge MST e i bridge PVST+. Tuttavia, se la VLAN 1 è disabilitata, il bridge MST deve diventare la radice per consentire a tutte le VLAN di evitare che il bridge MST collochi le proprie porte limite nello stato di incoerenza della radice. per ulteriori informazioni, fare riferimento a Descrizione di Multiple Spanning Tree Protocol (802.1s).

Caratteristiche standard

In questa sezione vengono illustrate le funzionalità di switching di base comuni a tutti gli ambienti. Configurare queste funzionalità su tutti i dispositivi di switching Cisco IOS Software Catalyst nella rete del cliente.

VLAN Trunk Protocol

Scopo

Un dominio VTP, detto anche dominio di gestione VLAN, è composto da uno o più switch interconnessi tramite un trunk che condividono lo stesso nome di dominio VTP. Il VTP è progettato per consentire agli utenti di apportare modifiche alla configurazione della VLAN a livello centrale su uno o più switch. Il VTP comunica automaticamente le modifiche a tutti gli altri switch del dominio VTP (rete). È possibile configurare uno switch in modo che si trovi in un solo dominio VTP. Prima di creare le VLAN, determinare la modalità VTP da usare nella rete.

Panoramica operativa

Il VTP è un protocollo di messaggistica di layer 2. Il VTP gestisce l'aggiunta, l'eliminazione e la ridenominazione delle VLAN su tutta la rete per mantenere la coerenza della configurazione VLAN. Il VTP riduce al minimo gli errori di configurazione e le incoerenze di configurazione che possono causare una serie di problemi. I problemi includono nomi di VLAN duplicati, specifiche del tipo di VLAN non corrette e violazioni della sicurezza.

Per impostazione predefinita, lo switch è in modalità server VTP ed è in stato no-management domain. Queste impostazioni predefinite cambiano quando lo switch riceve un annuncio per un dominio su un collegamento trunk o quando viene configurato un dominio di gestione.

Il protocollo VTP comunica tra gli switch tramite un MAC multicast di destinazione Ethernet conosciuto (01-00-0c-cc-cc-cc-cc) e un protocollo SNAP HDLC di tipo 0x2003. Analogamente ad altri protocolli intrinseci, il VTP utilizza anche un incapsulamento SNAP IEEE 802.3, che include LLC 0xAAAA03 e OUI 0x00000C. Potete vederlo su una traccia di LAN Analyzer. Il VTP non funziona sulle porte non trunk. Pertanto, i messaggi non possono essere inviati finché il DTP non ha attivato il trunk. In altre parole, il VTP è un payload di ISL o 802.1Q.

I tipi di messaggio includono:

- Annunci di riepilogo ogni 300 secondi (sec)
- Crea subset di annunci e richiedi annunci in caso di modifiche
- Join quando l'eliminazione VTP è abilitata

Il numero di revisione della configurazione VTP viene incrementato di uno a ogni modifica apportata a un server e la tabella viene propagata a tutto il dominio.

Quando si elimina una VLAN, le porte che una volta erano membri della VLAN passano allo stato `inactive`. Analogamente, se uno switch in modalità client non è in grado di ricevere la tabella VLAN VTP all'avvio, da un server VTP o da un altro client VTP, tutte le porte nelle VLAN diverse dalla VLAN predefinita 1 vengono disattivate.

Èpossibile configurare la maggior parte degli switch Catalyst in modo che funzionino in una di

queste modalità VTP:

- Server: in modalità server VTP, è possibile:Creazione di VLANModifica di VLANEliminazione di VLANSpecificare altri parametri di configurazione, ad esempio la versione VTP e l'eliminazione VTP, per l'intero dominio VTPI server VTP annunciano la configurazione VLAN su altri switch dello stesso dominio VTP. I server VTP sincronizzano anche la configurazione della VLAN con altri switch in base agli annunci ricevuti sui collegamenti trunk. Il server VTP è la modalità predefinita.
- Client: i client VTP si comportano come i server VTP. Tuttavia, non è possibile creare, modificare o eliminare le VLAN su un client VTP. Inoltre, il client non ricorda la VLAN dopo un riavvio perché nella NVRAM non sono state scritte informazioni sulla VLAN.
- Trasparente: gli switch VTP trasparenti non partecipano al VTP. Uno switch VTP trasparente non annuncia la propria configurazione VLAN e non sincronizza la configurazione VLAN in base agli annunci ricevuti. Tuttavia, nella versione 2 del VTP, gli switch trasparenti inoltrano gli annunci VTP in cui gli switch ricevono le loro interfacce trunk.

Funzionalità	Server	Cliente	Trasparente	Disattivato [1]
Messaggi VTP di origine	Sì	Sì	No	—
Ascolto dei messaggi VTP	Sì	Sì	No	—
Creazione di VLAN	Sì	No	Sì (solo significativi localmente)	—
Memorizza VLAN	Sì	No	Sì (solo significativi localmente)	—

[1] Il software Cisco IOS non ha l'opzione di disabilitare il VTP in modalità `off`.

La tabella seguente è un riepilogo della configurazione iniziale:

Funzionalità	Valore predefinito
Nome di dominio VTP	Null
Modalità VTP	Server
Versione VTP	Versione 1 abilitata
Eliminazione VTP	Disattivato

In modalità VTP trasparente, gli aggiornamenti VTP vengono semplicemente ignorati. L'indirizzo MAC multicast VTP conosciuto viene rimosso dalla CAM del sistema che normalmente viene utilizzata per prendere i frame di controllo e indirizzarli al Supervisor Engine. Poiché il protocollo utilizza un indirizzo multicast, lo switch in modalità trasparente o uno switch di un altro fornitore invia semplicemente il frame ad altri switch Cisco del dominio.

Il VTP versione 2 (VTPv2) include la flessibilità funzionale descritta in questo elenco. Tuttavia, il VTPv2 non è interscambiabile con il VTP versione 1 (VTPv1):

- Supporto Token Ring
- Supporto di informazioni VTP non riconosciute: gli switch propagano ora valori che non possono analizzare.
- Modalità trasparente dipendente dalla versione: la modalità trasparente non controlla più il nome di dominio. Ciò consente il supporto di più domini in un dominio trasparente.
- Propagazione del numero di versione: se il VTPv2 è possibile su tutti gli switch, tutti gli switch possono essere abilitati con la configurazione di un singolo switch.

per ulteriori informazioni, fare riferimento a Descrizione del VLAN Trunk Protocol (VTP).

Funzionamento VTP nel software Cisco IOS

Le modifiche alla configurazione in CatOS vengono scritte nella NVRAM subito dopo aver apportato una modifica. Al contrario, il software Cisco IOS non salva le modifiche della configurazione nella NVRAM a meno che non si esegua il comando **copy run start**. I sistemi client e server VTP richiedono che gli aggiornamenti VTP da altri server VTP vengano salvati immediatamente nella NVRAM senza l'intervento dell'utente. I requisiti per l'aggiornamento VTP sono soddisfatti dall'operazione CatOS predefinita, ma il modello di aggiornamento software Cisco IOS richiede un'operazione di aggiornamento alternativa.

Per questa modifica, è stato introdotto un database VLAN nel software Cisco IOS per Catalyst 6500 come metodo per salvare immediatamente gli aggiornamenti VTP per i client e i server VTP. In alcune versioni del software, questo database VLAN è sotto forma di file separato nella NVRAM, chiamato file vlan.dat. Controllare la versione del software in uso per determinare se è necessario un backup del database VLAN. Per visualizzare le informazioni VTP/VLAN memorizzate nel file vlan.dat per il client VTP o il server VTP, usare il comando **show vtp status**.

l'intera configurazione VTP/VLAN non viene salvata nel file della configurazione di avvio nella NVRAM quando si esegue il comando **copy run start** su questi sistemi. Ciò non si applica ai sistemi che eseguono come VTP trasparente. I sistemi VTP trasparenti salvano l'intera configurazione VTP/VLAN nel file della configurazione di avvio nella NVRAM quando si esegue il comando **copy run start**.

Nelle versioni software Cisco IOS precedenti al software Cisco IOS versione 12.1(11b)E, è possibile configurare le VTP e le VLAN solo tramite la modalità database VLAN. La modalità database VLAN è una modalità distinta dalla modalità di configurazione globale. La ragione di questo requisito di configurazione è che, quando si configura il dispositivo in modalità server o client VTP, i router adiacenti VTP possono aggiornare il database VLAN in modo dinamico tramite annunci VTP. Non si desidera che questi aggiornamenti vengano propagati automaticamente alla configurazione. Pertanto, il database VLAN e le informazioni VTP non vengono archiviati nella configurazione principale, ma nella NVRAM in un file con il nome vlan.dat.

Nell'esempio viene mostrato come creare una VLAN Ethernet in modalità database VLAN:

```
Switch#vlan database
Switch(vlan)#vlan 3
VLAN 3 added:
Name: VLAN0003
Switch(vlan)#exit
APPLY completed.
Exiting....
```

Nel software Cisco IOS versione 12.1(11b)E e successive, è possibile configurare il VTP e le

VLAN tramite la modalità database VLAN o la modalità di configurazione globale. In modalità server VTP o in modalità VTP trasparente, la configurazione delle VLAN aggiorna ancora il file vlan.dat nella NVRAM. Tuttavia, questi comandi non vengono salvati nella configurazione. Pertanto, i comandi non vengono visualizzati nella configurazione corrente.

Per ulteriori informazioni, consultare la sezione *Configurazione della VLAN in modalità di configurazione globale* nel documento sulla configurazione delle VLAN.

Nell'esempio viene mostrato come creare una VLAN Ethernet in modalità di configurazione globale e come verificare la configurazione:

```
Switch#configure terminal
Switch(config#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Switch(config#vlan 3
Switch(config-vlan)#end
Switch#
OR
Switch#vlan database
Switch(vlan#vtp server
Switch device to VTP SERVER mode.
Switch(vlan#vlan 3
Switch(vlan#exit
APPLY completed.
Exiting....
Switch#
```

Nota: la configurazione VLAN è memorizzata nel file vlan.dat e memorizzata nella memoria non volatile. Per eseguire un backup completo della configurazione, includere il file vlan.dat nel backup insieme alla configurazione. Quindi, se l'intero switch o modulo Supervisor Engine deve essere sostituito, l'amministratore di rete deve caricare entrambi i file per ripristinare la configurazione completa:

- Il file vlan.dat
- Il file di configurazione

VTP e VLAN estese

La funzione ID sistema esteso viene usata per abilitare l'identificazione della VLAN dell'intervallo esteso. Quando l'ID sistema esteso è abilitato, disabilita il pool di indirizzi MAC utilizzati per lo Spanning Tree VLAN e lascia un singolo indirizzo MAC che identifica lo switch. Le versioni software Catalyst IOS 12.1(11b)EX e 12.1(13)E introducono il supporto dell'ID di sistema esteso per Catalyst 6000/6500 in modo da supportare le VLAN 4096 in conformità allo standard IEEE 802.1Q. Questa funzione è stata introdotta nel software Cisco IOS versione 12.1(12c)EW per gli switch Catalyst 4000/4500. Le VLAN sono organizzate in diversi intervalli, ciascuno dei quali può essere utilizzato in modo diverso. Alcune di queste VLAN vengono propagate ad altri switch nella rete quando si usa il VTP. Poiché le VLAN dell'intervallo esteso non vengono propagate, è necessario configurare manualmente le VLAN dell'intervallo esteso su ciascun dispositivo di rete. Questa funzionalità ID sistema esteso equivale alla funzionalità di riduzione dell'indirizzo MAC nel sistema operativo Catalyst.

Nella tabella seguente vengono descritti gli intervalli di VLAN:

VLAN	Interv	Utilizzo	Propa

	allo		gata dal VTP?
0, 4095	Rese rved	Solo per uso di sistema. Queste VLAN non possono essere visualizzate o usate.	—
1	Norm ale	Impostazione predefinita di Cisco. La VLAN può essere utilizzata, ma non eliminata.	Sì
2–100 1	Norm ale	Per VLAN Ethernet. Le VLAN possono essere create, utilizzate ed eliminate.	Sì
1002–1005	Norm ale	Impostazioni predefinite di Cisco per FDDI e Token Ring. non è possibile eliminare le VLAN 1002-1005.	Sì
1006–4094	Rese rved	Solo per VLAN Ethernet.	No

I protocolli dello switch utilizzano un indirizzo MAC ricavato da un gruppo di indirizzi disponibili forniti da una EPROM sullo chassis come parte degli identificatori di bridge per le VLAN in esecuzione in PVST+ e RPVST+. Gli switch Catalyst 6000/6500 e Catalyst 4000/4500 supportano sia gli indirizzi MAC 1024 che 64, a seconda del tipo di chassis.

Gli switch Catalyst con indirizzi MAC 1024 non abilitano l'ID sistema esteso per impostazione predefinita. Gli indirizzi MAC sono allocati in sequenza, il primo nell'intervallo è assegnato alla VLAN 1, il secondo alla VLAN 2 e così via. Ciò consente agli switch di supportare 1024 VLAN e ciascuna VLAN utilizza un identificatore di bridge univoco.

Tipo di chassis	Indirizzo chassis
WS-C4003-S1, WS-C4006-S2	1024
WS-C4503, WS-C4506	641
WS-C6509-E,WS-C6509, WS-C6509-NEB, WS-C6506-E, WS-C6506, WS-C6009, WS-C6006, OSR-7609-AC, OSR-7609-DC	1024
WS-C6513, WS-C6509-NEB-A, WS-C6504-E, WS-C6503-E, WS-C6503, CISCO7603, CISCO7606, CISCO7609, CISCO7613	641

[1] Lo chassis con 64 indirizzi MAC abilita l'ID sistema esteso per impostazione predefinita e la funzione non può essere disabilitata.

Per ulteriori informazioni, consultare la sezione *Descrizione dell'ID bridge* in Configurazione di STP e MST IEEE 802.1s.

Per gli switch Catalyst serie 1024 indirizzi MAC, per abilitare l'ID sistema esteso è necessario supportare 4096 VLAN con istanze PVST+ o 16 MISTP, in modo da avere identificatori univoci

senza aumentare il numero di indirizzi MAC richiesti sullo switch. L'ID sistema esteso riduce il numero di indirizzi MAC richiesti dall'STP da uno per ciascuna VLAN o istanza MISTP a uno per ciascuno switch.

Nella figura viene illustrato l'identificatore del bridge quando l'ID sistema esteso non è abilitato. L'identificatore del bridge è costituito da una priorità del bridge di 2 byte e da un indirizzo MAC di 6 byte.

L'ID di sistema esteso modifica la parte relativa all'identificatore del bridge Stp (Spanning Tree Protocol) delle BDPU (Bridge Protocol Data Units). Il campo di priorità originale da 2 byte viene suddiviso in 2 campi; Un campo di priorità del bridge a 4 bit e un'estensione dell'ID di sistema a 12 bit che consente la numerazione delle VLAN da 0 a 4095.

Se l'ID sistema esteso è abilitato sugli switch Catalyst per usare le VLAN dell'intervallo esteso, deve essere abilitato su tutti gli switch dello stesso dominio STP. Ciò è necessario per mantenere coerenti i calcoli radice STP su tutti gli switch. Dopo aver abilitato l'ID sistema esteso, la priorità del bridge radice diventa un multiplo di 4096 più l'ID VLAN. È possibile che gli switch senza ID sistema esteso richiedano inavvertitamente l'autenticazione root, in quanto hanno una granularità più fine nella selezione del relativo ID bridge.

Sebbene sia consigliabile mantenere una configurazione coerente dell'ID di sistema esteso all'interno dello stesso dominio STP, non è pratico applicare l'ID di sistema esteso a tutti i dispositivi di rete quando si introduce un nuovo chassis con 64 indirizzi MAC nel dominio STP. Tuttavia, è importante capire quando due sistemi sono configurati con la stessa priorità Spanning-tree, il sistema senza ID di sistema esteso ha una priorità Spanning-tree migliore. Per abilitare la configurazione dell'ID di sistema esteso, usare questo comando:

spanning-tree extend system-id

Le VLAN interne vengono allocate in ordine crescente, a partire dalla VLAN 1006. Per evitare conflitti tra le VLAN utente e le VLAN interne, si consiglia di assegnare le VLAN utente il più vicino possibile alla VLAN 4094. Usare il comando **show vlan internal usage** su uno switch per visualizzare le VLAN assegnate internamente.

```
Switch#show vlan internal usage

VLAN Usage
---- --------------------
1006 online diag vlan0
1007 online diag vlan1
1008 online diag vlan2
1009 online diag vlan3
1010 online diag vlan4
1011 online diag vlan5
1012 PM vlan process (trunk tagging)
```

```
1013 Port-channel100
1014 Control Plane Protection
1015 L3 multicast partial shortcuts for VPN 0
1016 vrf_0_vlan0
1017 Egress internal vlan
1018 Multicast VPN 0 QOS vlan
1019 IPv6 Multicast Egress multicast
1020 GigabitEthernet5/1
1021 ATM7/0/0
1022 ATM7/0/0.1
1023 FastEthernet3/1
1024 FastEthernet3/2
------deleted------
```

Nel sistema operativo IOS nativo, è possibile configurare la **policy di allocazione interna delle vlan in ordine decrescente** in modo che le VLAN interne vengano allocate in ordine decrescente. l'equivalente CLI per il software CatOS non è ufficialmente supportato.

decrescente criterio di allocazione interna vlan

[Consiglio di configurazione Cisco]

Èpossibile creare le VLAN quando uno switch Catalyst 6500/6000 è in modalità server VTP, anche senza nome di dominio VTP. Configurare il nome di dominio VTP prima di configurare le VLAN sugli switch Catalyst 6500/6000 con software di sistema Cisco IOS. La configurazione in questo ordine mantiene la coerenza con altri switch Catalyst con CatOS.

Non è consigliabile utilizzare modalità client/server VTP o modalità VTP `trasparente`. Alcuni clienti preferiscono la facilità di gestione della modalità client/server VTP, nonostante alcune considerazioni riportate in questa sezione. Si consiglia di disporre di due switch in modalità server in ciascun dominio per la ridondanza, in genere i due switch a livello di distribuzione. Impostare gli altri switch del dominio sulla modalità client. Quando si implementa la modalità client/server con l'uso del VTPv2, tenere presente che un numero di revisione superiore viene sempre accettato nello stesso dominio VTP. Se uno switch configurato in modalità client VTP o server viene introdotto nel dominio VTP e ha un numero di revisione superiore a quello dei server VTP esistenti, il database VLAN all'interno del dominio VTP viene sovrascritto. Se la modifica della configurazione non è intenzionale e le VLAN vengono eliminate, la sovrascrittura può causare un'interruzione grave della rete. Per garantire che gli switch client o server abbiano sempre un numero di revisione della configurazione inferiore a quello del server, modificare il nome di dominio VTP del client in un nome diverso dal nome standard, quindi ripristinare lo standard. Questa azione imposta su 0 la revisione della configurazione nel client.

Il VTP può apportare facilmente delle modifiche in una rete in virtù di vantaggi e svantaggi. Molte aziende preferiscono un approccio cauto e utilizzano la modalità VTP `trasparente` per i seguenti motivi:

- Questa pratica incoraggia un buon controllo delle modifiche, in quanto la modifica obbligatoria di una VLAN su uno switch o su una porta trunk deve essere considerata come un unico switch alla volta.
- La modalità VTP trasparente limita il rischio di errori dell'amministratore, ad esempio l'eliminazione accidentale di una VLAN. Tali errori possono influire sull'intero dominio.
- Le VLAN possono essere eliminate dai trunk sugli switch che non hanno porte nella VLAN. Questo comporta un frame flooding più efficiente in termini di larghezza di banda. La potatura manuale ha anche un diametro ridotto di spanning-tree. Per ulteriori informazioni, vedere la

sezione Dynamic Trunking Protocol. Anche una configurazione VLAN per switch incoraggia questa pratica.
- Non vi è alcun rischio che venga introdotto nella rete un nuovo switch con un numero di revisione VTP superiore che sovrascrive l'intera configurazione VLAN di dominio.
- La modalità trasparente VTP del software Cisco IOS è supportata in Campus Manager 3.2, che fa parte di CiscoWorks 2000. La restrizione precedente che richiede di avere almeno un server in un dominio VTP è stata rimossa.

Comandi VTP	**Commenti**
nome di dominio vtp	Il CDP controlla il nome per evitare errori di cablaggio tra i domini. Nei nomi di dominio viene fatta distinzione tra maiuscole e minuscole.
vtp mode {server | client | trasparente}	Il VTP funziona in una delle tre modalità.
numero_vlan vlan	Verrà creata una VLAN con l'ID fornito.
switchport trunk consentito *intervallo_vlan*	Questo è un comando di interfaccia che permette ai trunk di trasportare le VLAN quando necessario. Il valore predefinito è tutte le VLAN.
switchport trunk eliminazione *intervallo_vlan*	Questo comando di interfaccia limita il diametro STP mediante eliminazione manuale, ad esempio sui trunk dal livello di distribuzione al livello di accesso, dove la VLAN non esiste. Per impostazione predefinita, tutte le VLAN sono idonee per l'eliminazione.

Altre opzioni

Il VTPv2 è un requisito fondamentale negli ambienti Token Ring, in cui si consiglia vivamente la modalità client/server.

La sezione Suggerimenti per la configurazione Cisco di questo documento illustra i vantaggi dell'eliminazione delle VLAN per ridurre inutili perdite di frame. Il comando **vtp pruning** elimina automaticamente le VLAN, arrestando l'inefficiente flooding di frame che non sono necessari.

Nota: a differenza dell'eliminazione manuale delle VLAN, l'eliminazione automatica non limita il diametro dello spanning-tree.

L'IEEE ha prodotto un'architettura basata su standard per ottenere risultati simili al VTP. Come membro del protocollo GARP (Generic Attribute Registration Protocol) 802.1Q, il protocollo GVRP (Generic VLAN Registration Protocol) consente l'interoperabilità della gestione VLAN tra i fornitori. Tuttavia, il GVRP esula dall'ambito di questo documento.

Nota: il software Cisco IOS non dispone di funzionalità VTP off mode e supporta solo VTPv1 e VTPv2 con eliminazione.

Negoziazione automatica Fast Ethernet

Scopo

La negoziazione automatica è una funzione opzionale dello standard Fast Ethernet (FE) IEEE 802.3u. La negoziazione automatica consente ai dispositivi di scambiare automaticamente le informazioni sulla velocità e sulle capacità duplex su un collegamento. La negoziazione automatica funziona sul layer 1 (L1). La funzione è destinata alle porte assegnate alle aree in cui utenti o dispositivi temporanei si connettono a una rete. Gli esempi includono switch e hub del livello di accesso.

Panoramica operativa

La negoziazione automatica utilizza una versione modificata del test di integrità del collegamento per i dispositivi 10BASE-T per negoziare la velocità e scambiare altri parametri di negoziazione automatica. Il test originale di integrità del collegamento 10BASE-T è noto come Normal Link Pulse (NLP). La versione modificata del test di integrità del collegamento per la negoziazione automatica a 10/100 Mbps è nota come FLP (Fast Link Pulse). I dispositivi 10BASE-T prevedono un impulso di burst ogni 16 (+/-8) millisecondi (ms) come parte del test di integrità del collegamento. Il protocollo FLP per la negoziazione automatica a 10/100 Mbps invia questi burst ogni 16 (+/-8) ms con gli impulsi aggiuntivi ogni 62,5 (+/-7) microsecondi. Gli impulsi all'interno della sequenza di frammentazione generano parole di codice utilizzate per gli scambi di compatibilità tra partner di collegamento.

In 10BASE-T, viene inviato un impulso di collegamento ogni volta che una stazione si avvicina. Questo è un singolo impulso che viene inviato ogni 16 ms. Anche i dispositivi 10BASE-T inviano un impulso di collegamento ogni 16 ms quando il collegamento è inattivo. Questi impulsi di collegamento sono anche chiamati heartbeat o NLP.

Un dispositivo 100BASE-T invia dati FLP. Questo impulso viene inviato come raffica invece che come impulso singolo. La frammentazione viene completata entro 2 ms e viene ripetuta nuovamente ogni 16 ms. Dopo l'inizializzazione, il dispositivo trasmette un messaggio FLP a 16 bit al partner di collegamento per la negoziazione del controllo della velocità, del duplex e del flusso. Questo messaggio a 16 bit viene inviato ripetutamente fino a quando il partner non lo riconosce.

Nota: in base alla specifica IEEE 802.3u, non è possibile configurare manualmente un partner di collegamento per la modalità full duplex a 100 Mbps e continuare la negoziazione automatica per la modalità full duplex con l'altro partner di collegamento. Il tentativo di configurare un partner di collegamento per la modalità full duplex a 100 Mbps e l'altro partner di collegamento per la negoziazione automatica determina una mancata corrispondenza del duplex. Risultati di mancata corrispondenza duplex perché un partner del collegamento esegue la negoziazione automatica e non visualizza alcun parametro di negoziazione automatica dell'altro partner del collegamento. Per impostazione predefinita, il primo partner del collegamento viene quindi impostato sulla modalità

half-duplex.

Tutti i moduli di switching Catalyst 6500 Ethernet supportano 10/100 Mbps e la modalità half-duplex o full-duplex. Usare il comando **show interface capabilities** per verificare questa funzionalità su altri switch Catalyst.

Una delle cause più comuni dei problemi di prestazioni dei collegamenti Ethernet a 10/100 Mbps si verifica quando una porta sul collegamento funziona in modalità half-duplex, mentre l'altra porta funziona in modalità full-duplex. Questa situazione si verifica occasionalmente quando si reimposta una o entrambe le porte in un collegamento e il processo di negoziazione automatica non genera la stessa configurazione per entrambi i partner del collegamento. La situazione si verifica anche quando si riconfigura un partner del collegamento ma non l'altro. È possibile evitare di effettuare chiamate di assistenza relative alle prestazioni se:

- Crea un criterio che richiede la configurazione delle porte per il comportamento richiesto per tutti i dispositivi non temporanei
- Applicare la politica con adeguate misure di controllo dei cambiamenti

I sintomi tipici della sequenza di controllo del frame (FCS) con problemi di prestazioni aumentano, il controllo di ridondanza ciclico (CRC), l'allineamento o i contatori runt sullo switch.

Nella modalità half-duplex, si dispone di una coppia di cavi di ricezione e di una coppia di cavi di trasmissione. Non è possibile utilizzare contemporaneamente entrambi i fili. Il dispositivo non può trasmettere quando è presente un pacchetto sul lato ricezione.

In modalità full duplex, si hanno la stessa coppia di cavi di ricezione e trasmissione. Tuttavia, entrambe le funzioni possono essere usate contemporaneamente perché le funzioni Sensore vettore e Rilevamento collisioni sono state disabilitate. Il dispositivo può trasmettere e ricevere contemporaneamente.

Pertanto, una connessione da half-duplex a full-duplex funziona, ma c'è un elevato numero di collisioni sul lato half-duplex che determinano prestazioni scadenti. Le collisioni si verificano perché il dispositivo configurato come full duplex può trasmettere contemporaneamente alla ricezione dei dati.

I documenti di questo elenco descrivono in dettaglio la negoziazione automatica. In questi documenti viene illustrato il funzionamento della negoziazione automatica e vengono descritte le diverse opzioni di configurazione.

- Configurazione e risoluzione dei problemi Ethernet 10/100/1000Mb Half/Full Duplex Auto-Negotiation
- Risoluzione dei problemi di compatibilità NIC degli switch Cisco Catalyst

Un'idea errata comune sulla negoziazione automatica è che è possibile configurare manualmente un partner di collegamento per la modalità full duplex 100 Mbps e la modalità di negoziazione automatica per la modalità full duplex con l'altro partner di collegamento. In realtà, un tentativo di eseguire questa operazione determina una mancata corrispondenza del duplex. Questa è una conseguenza del fatto che un partner del collegamento esegue la negoziazione automatica, non vede alcun parametro di negoziazione automatica dall'altro partner e per impostazione predefinita è half-duplex.

La maggior parte dei moduli Catalyst Ethernet supporta 10/100 Mbps e la modalità half/full duplex. Tuttavia, è possibile confermare questa condizione se si usa il comando **show interface *mod/porta* capabilities**.

FEFI

L'indicazione di guasto Far End (FEFI) protegge le interfacce 100BASE-FX (fibra) e Gigabit, mentre la negoziazione automatica protegge 100BASE-TX (rame) da errori fisici relativi a layer/segnalazione.

Un guasto all'estremità remota è un errore nel collegamento che una stazione può rilevare mentre l'altra non lo può rilevare. Un cavo di trasmissione disconnesso è un esempio. Nell'esempio, la stazione di invio riceve ancora dati validi e rileva che il collegamento è valido tramite il monitoraggio dell'integrità del collegamento. Tuttavia, la stazione di invio non è in grado di rilevare che l'altra stazione non riceve la trasmissione. Una stazione 100BASE-FX che rileva un errore remoto può modificare il flusso `IDLE` trasmesso in modo da inviare uno speciale modello di bit per informare il vicino del guasto remoto. Lo speciale modello di bit è noto come modello `FEFI-IDLE`. Il modello `FEFI-IDLE` attiva successivamente la disabilitazione della porta remota (`errDisable`). Per ulteriori informazioni sulla protezione dai guasti, vedere la sezione Rilevamento collegamento unidirezionale di questo documento.

Questi moduli/hardware supportano FEFI:

- Catalyst 6500/6000 e 4500/4000:Tutti i moduli 100BASE-FX e GE

Raccomandazione porta infrastruttura Cisco

La configurazione della negoziazione automatica su collegamenti a 10/100 Mbps o della velocità del codice rigido e del duplex dipende in ultima analisi dal tipo di partner di collegamento o di dispositivo finale connesso a una porta dello switch Catalyst. La negoziazione automatica tra dispositivi terminali e switch Catalyst in genere funziona correttamente e gli switch Catalyst sono conformi alla specifica IEEE 802.3u. Tuttavia, se la scheda di interfaccia di rete (NIC) o gli switch del fornitore non sono esattamente conformi, possono verificarsi problemi. Inoltre, le funzionalità avanzate specifiche del fornitore non descritte nella specifica IEEE 802.3u per la negoziazione automatica a 10/100 Mbps possono causare incompatibilità hardware e altri problemi. Questi tipi di funzioni avanzate includono la protezione automatica e l'integrità dei cavi. Questo documento offre un esempio:

- Avviso: Problemi di prestazioni con le schede di interfaccia di rete Intel Pro/1000T che si connettono a CAT4K/6K

In alcune situazioni, è necessario impostare host, velocità della porta e duplex. In generale, eseguire le seguenti operazioni di risoluzione dei problemi di base:

- Verificare che la negoziazione automatica sia configurata su entrambi i lati del collegamento o che il codice hardware sia configurato su entrambi i lati.
- Consultare le note sulla versione per le avvertenze comuni.
- Verificare la versione del driver della scheda NIC o del sistema operativo in uso. Spesso è necessario utilizzare il driver o la patch più recente.

Di regola, utilizzare innanzitutto la negoziazione automatica per qualsiasi tipo di partner del collegamento. La configurazione della negoziazione automatica per dispositivi temporanei quali i notebook offre evidenti vantaggi. La negoziazione automatica funziona bene anche con altri dispositivi, ad esempio:

- Con dispositivi non temporanei quali server e workstation fisse
- Da switch a switch

- Da switch a router

Ma, per alcune delle ragioni citate in questa sezione, possono sorgere problemi di negoziazione. Per le procedure di risoluzione dei problemi di base in questi casi, fare riferimento alla configurazione e risoluzione dei problemi di negoziazione automatica Ethernet 10/100/1000Mb Half/Full Duplex.

Disabilita negoziazione automatica per:

- Porte che supportano dispositivi dell'infrastruttura di rete quali switch e router
- Altri sistemi finali non transitori, quali server e stampanti

Definire sempre le impostazioni di velocità e duplex per queste porte.

Configurare manualmente queste configurazioni dei collegamenti 10/100 Mbps per la velocità e il duplex, che in genere sono full duplex a 100 Mbps:

- Switch-to-switch
- Switch-to-server
- Switch-to-router

Se la velocità della porta è impostata su auto su una porta Ethernet a 10/100 Mbps, sia la velocità che il duplex vengono negoziati automaticamente. Per impostare la porta su auto, usare questo comando di interfaccia:

```
Switch(config)#interface fastethernet slot/port
Switch(config-if)#speed auto
!--- This is the default.
```

Per configurare la velocità e la modalità duplex, eseguire questi comandi di interfaccia:

```
Switch(config)#interface fastethernet slot/port
Switch(config-if)#speed {10 | 100 | auto}
Switch(config-if)#duplex {full | half}
```

Suggerimenti per Cisco Access Port

Gli utenti finali, i lavoratori mobili e gli host temporanei devono eseguire la negoziazione automatica per ridurre al minimo la gestione di questi host. è possibile far funzionare la negoziazione automatica anche con gli switch Catalyst. Sono spesso necessari i driver NIC più recenti.

Per abilitare la negoziazione automatica della velocità della porta, eseguire questi comandi globali:

```
Switch(config)#interface fastethernet slot/port
Switch(config-if)#speed auto
```

Nota: se si imposta la velocità della porta su Auto su una porta Ethernet 10/100 Mbps, la negoziazione automatica viene eseguita sia per la velocità che per il duplex. Non è possibile modificare la modalità duplex delle porte di negoziazione automatica.

Quando le schede NIC o gli switch dei fornitori non sono conformi esattamente alla specifica IEEE 802.3u, possono verificarsi problemi. Inoltre, le funzionalità avanzate specifiche del fornitore non

descritte nella specifica IEEE 802.3u per la negoziazione automatica a 10/100 Mbps possono causare incompatibilità hardware e altri problemi. Tali caratteristiche avanzate includono protezione automatica e integrità dei cavi.

Altre opzioni

Quando la negoziazione automatica è disabilitata tra gli switch, l'indicazione di errore di layer 1 può anche essere persa per alcuni problemi. Utilizzare i protocolli di layer 2 per migliorare il rilevamento degli errori, ad esempio il protocollo UDLD aggressivo.

La funzione di negoziazione automatica non rileva queste situazioni, anche quando è abilitata:

- Le porte si bloccano e non ricevono né trasmettono
- Un lato della linea è su ma l'altro è giù
- I cavi in fibra non sono collegati correttamente

La negoziazione automatica non rileva questi problemi perché non si trovano al livello fisico. I problemi possono causare loop STP o buchi neri nel traffico.

UDLD è in grado di rilevare tutti questi casi e di disabilitare entrambe le porte sul collegamento, se il protocollo UDLD è configurato su entrambe le estremità. In questo modo, il protocollo UDLD impedisce i loop STP e i buchi neri nel traffico.

Negoziazione automatica Gigabit Ethernet

Scopo

Gigabit Ethernet (GE) dispone di una procedura di negoziazione automatica più estesa di quella utilizzata per Ethernet a 10/100 Mbps (IEEE 802.3z). Con le porte GE, la negoziazione automatica viene utilizzata per scambiare:

- Parametri di controllo del flusso
- Informazioni errore remoto
- Informazioni duplex**Nota:** le porte GE della serie Catalyst supportano solo la modalità full duplex.

IEEE 802.3z è stato sostituito da IEEE 802.3:2000. Per ulteriori informazioni, fare riferimento agli standard LAN/MAN 802s (Local and Metropolitan Area Networks + Drafts) .

Panoramica operativa

A differenza della negoziazione automatica con FE 10/100 Mbps, la negoziazione automatica GE non comporta la negoziazione della velocità della porta. Inoltre, non è possibile usare il comando **set port speed** per disabilitare la negoziazione automatica. La negoziazione delle porte GE è abilitata per impostazione predefinita e le porte su entrambe le estremità di un collegamento GE devono avere la stessa impostazione. Il collegamento non viene attivato se le porte a ciascuna estremità del collegamento sono impostate in modo incoerente, il che significa che i parametri scambiati sono diversi.

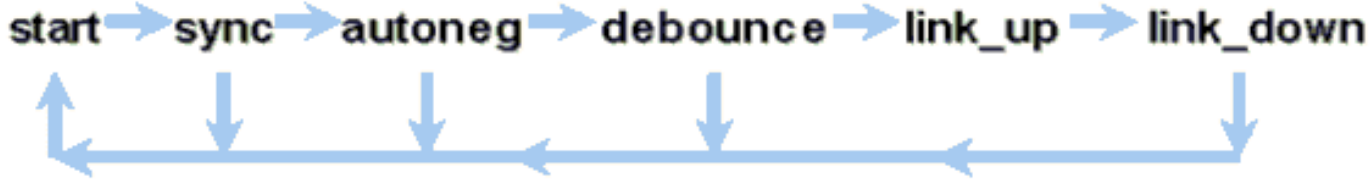
Si supponga, ad esempio, che vi siano due dispositivi, A e B. Ciascun dispositivo può avere la funzione di negoziazione automatica abilitata o disabilitata. Questa tabella contiene le possibili configurazioni e i rispettivi stati di collegamento:

Negoziazione	B abilitato	B Disattivato
A Attivato	su su entrambi i lati	A giù, B su
A Disabilitato	A su, B giù	su su entrambi i lati

In GE, la sincronizzazione e la negoziazione automatica (se abilitate) vengono eseguite all'avvio del collegamento tramite l'utilizzo di una sequenza speciale di parole di codice del collegamento riservate.

Nota: esiste un dizionario di parole valide e non tutte le parole possibili sono valide in GE.

La vita di una connessione GE può essere caratterizzata nel modo seguente:



Una perdita di sincronizzazione indica che l'indirizzo MAC rileva un collegamento non attivo. La perdita della sincronizzazione si verifica indipendentemente dal fatto che la negoziazione automatica sia abilitata o disabilitata. La sincronizzazione viene persa in determinate condizioni non riuscite, ad esempio la ricezione di tre parole non valide in successione. Se questa condizione persiste per 10 ms, viene asserita una condizione di errore di sincronizzazione e il collegamento viene impostato sullo stato `link_down`. Una volta persa la sincronizzazione, sono necessari altri tre periodi di inattività validi consecutivi per eseguire nuovamente la sincronizzazione. Altri eventi catastrofici, come la perdita del segnale di ricezione (Rx), provocano un evento di collegamento non attivo.

La negoziazione automatica fa parte del processo di collegamento. Quando il collegamento è attivo, la negoziazione automatica è terminata. Tuttavia, lo switch continua a monitorare lo stato del collegamento. Se la negoziazione automatica è disabilitata su una porta, la fase di negoziazione automatica non è più un'opzione.

La specifica GE in rame (1000BASE-T) supporta la negoziazione automatica tramite un sistema Next Page Exchange. Next Page Exchange consente la negoziazione automatica per velocità di 10/100/1000 Mbps su porte in rame.

Nota: tuttavia, la specifica della fibra GRE prevede solo la negoziazione del duplex, il controllo del flusso e il rilevamento degli errori remoti. Le porte Fibre Channel GE non negoziano la velocità delle porte. Per ulteriori informazioni sulla negoziazione automatica, fare riferimento alle sezioni 28 e 37 della specifica IEEE 802.3-2002 .

Il ritardo di riavvio della sincronizzazione è una funzionalità software che controlla il tempo totale di negoziazione automatica. Se la negoziazione automatica non ha esito positivo in questo periodo di tempo, il firmware riavvia la negoziazione automatica in caso di deadlock. Il comando **sync-restart-delay** ha effetto solo quando la negoziazione automatica è impostata su enable.

Raccomandazione porta infrastruttura Cisco

La configurazione della negoziazione automatica è molto più critica in un ambiente GE che in un ambiente a 10/100 Mbps. Disabilitare la negoziazione automatica solo nelle situazioni seguenti:

- Sulle porte degli switch collegate a dispositivi che non supportano la negoziazione
- Quando problemi di connettività derivano da problemi di interoperabilità

Abilitare la negoziazione Gigabit su tutti i collegamenti da switch a switch e, in genere, su tutti i dispositivi GE. Il valore predefinito sulle interfacce Gigabit è la negoziazione automatica. Tuttavia, per verificare che la negoziazione automatica sia abilitata, usare questo comando:

```
switch(config)#interface type slot/port
switch(config-If)#no speed
!--- This command sets the port to autonegotiate Gigabit parameters.
```

Un'eccezione nota si verifica quando si esegue la connessione a un Gigabit Switch Router (GSR) con software Cisco IOS versione precedente al software Cisco IOS versione 12.0(10)S, la versione che aggiunge il controllo del flusso e la negoziazione automatica. In questo caso, disattivare le due funzioni. Se queste funzionalità non vengono disattivate, la porta dello switch risulterà non connessa e il GSR segnalerà gli errori. Di seguito viene riportato un esempio di sequenza di comandi dell'interfaccia:

```
flowcontrol receive off
flowcontrol send off
speed nonegotiate
```

Suggerimenti per Cisco Access Port

Poiché i file FLP possono variare da fornitore a fornitore, è necessario considerare le connessioni da switch a server caso per caso. I clienti Cisco hanno riscontrato alcuni problemi con la negoziazione Gigabit su server Sun, HP e IBM. Chiedere a tutti i dispositivi di utilizzare la negoziazione automatica Gigabit, a meno che il fornitore della scheda NIC non indichi espressamente il contrario.

Altre opzioni

Il controllo del flusso è una parte opzionale della specifica 802.3x. Se si utilizza il controllo del flusso, è necessario negoziarlo. I dispositivi possono o non possono inviare e/o rispondere a un frame di pausa (MAC 01-80-C2-00-00-00 0F noto). Inoltre, i dispositivi possono anche non essere in grado di accettare la richiesta di controllo del flusso del router adiacente più lontano. Una porta con un buffer di input che inizia a riempire invia un frame di pausa al partner di collegamento. Il partner di collegamento interrompe la trasmissione e mantiene eventuali frame aggiuntivi nei buffer di output del partner di collegamento. Questa funzione non risolve alcun problema di oversubscription steady-state. Tuttavia, la funzione rende il buffer di input più grande di una frazione del buffer di output del partner durante i picchi.

La funzione PAUSE è progettata per prevenire l'inutile eliminazione dei frame ricevuti da parte dei dispositivi (switch, router o stazioni terminali) a causa di condizioni di overflow del buffer causate da un sovraccarico del traffico transitorio di breve durata. Un dispositivo in sovraccarico di traffico impedisce l'overflow del buffer interno quando il dispositivo invia un frame di pausa. Il frame di pausa contiene un parametro che indica il periodo di tempo che il partner full duplex deve attendere prima di inviare altri frame di dati. Il partner che riceve il frame di pausa cessa di inviare i

dati per il periodo specificato. Alla scadenza del timer, la stazione ricomincia a inviare i frame di dati dal punto in cui era stata interrotta.

Una stazione che emette una pausa può emettere un altro frame di pausa che contiene un parametro di tempo zero. Questa azione annulla il resto del periodo di pausa. Pertanto, un frame di pausa appena ricevuto ignora qualsiasi operazione di pausa attualmente in corso. Inoltre, la stazione che emette il frame di pausa può estendere il periodo di pausa. La stazione emette un altro frame di pausa che contiene un parametro di tempo diverso da zero prima della scadenza del primo periodo di pausa.

Questa operazione di pausa non è un controllo del flusso basato sulla velocità. L'operazione è un semplice meccanismo di start-stop che consente al dispositivo sotto traffico, quello che ha inviato il frame di pausa, di ridurre la congestione del buffer.

L'utilizzo ottimale di questa funzionalità è nei collegamenti tra porte di accesso e host finali, dove il buffer di output dell'host è potenzialmente grande quanto la memoria virtuale. L'uso da switch a switch offre vantaggi limitati.

Per controllare questa condizione sulle porte dello switch, usare questi comandi di interfaccia:

```
flowcontrol {receive | send} {off | on | desired}
```

```
>show port flowcontrol

 Port  Send FlowControl    Receive FlowControl   RxPause TxPause
       admin    oper       admin    oper
-----  -------- --------   -------- --------     ------- -------
 6/1   off      off        on       on           0       0
 6/2   off      off        on       on           0       0
 6/3   off      off        on       on           0       0
```

Nota: tutti i moduli Catalyst rispondono a un frame di `pausa` se negoziato. Alcuni moduli (ad esempio, WS-X5410 e WS-X4306) non inviano mai frame di pausa, anche se negoziano per farlo, perché non bloccano.

Dynamic Trunking Protocol

Scopo

Per estendere le VLAN tra i dispositivi, i trunk identificano temporaneamente e contrassegnano (collegamento locale) i frame Ethernet originali. Questa azione consente il multiplexing dei frame su un singolo collegamento. Inoltre, questa azione assicura che il broadcast della VLAN e i domini di sicurezza siano separati tra gli switch. Le tabelle CAM mantengono la mappatura tra frame e VLAN all'interno degli switch.

Panoramica operativa

Il DTP è la seconda generazione di ISL dinamico (DISL). ISL supportato solo da DISL. Il DTP supporta sia ISL che 802.1Q. Questo supporto assicura che gli switch a entrambe le estremità di un trunk concordino sui diversi parametri dei frame trunking. Tali parametri comprendono:

- Tipo di incapsulamento configurato
- VLAN nativa
- Funzionalità hardware

Il supporto DTP aiuta anche a proteggere contro il sovraccarico di frame con tag da parte delle porte non trunk, il che rappresenta un rischio di sicurezza potenzialmente grave. Il DTP protegge da tali inondazioni perché garantisce che i porti e i loro vicini si trovino in uno stato coerente.

Modalità trunking

Il DTP è un protocollo di layer 2 che negozia i parametri di configurazione tra una porta dello switch e la porta adiacente. DTP utilizza un altro indirizzo MAC multicast conosciuto di 01-00-0c-cc-cc-cc-cc e un tipo di protocollo SNAP 0x2004. In questa tabella viene descritta la funzione su ciascuna delle possibili modalità di negoziazione DTP:

Modalità	Funzione	Frame DTP trasmessi?	Stato finale (porta locale)
`Auto dinamico` (equivalente alla modalità `Auto` in CatOS)	Rende la porta disponibile a convertire il collegamento in trunk. La porta diventa una porta trunk se la porta adiacente è impostata `sulla` modalità `accesa` o `desiderata`.	Sì, periodico	`Trunking`
`Trunk` (equivalente alla modalità `ON` in CatOS)	Mette la porta in modalità di `trunking` permanente e negozia per convertire il collegamento in trunk. La porta diventa una porta trunk anche se la porta adiacente non accetta la modifica.	Sì, periodico	`Trunking` incondizionato
`Nonegotiate`	Porta in modalità `trunking` permanente ma non consente alla porta di generare frame DTP. Per stabilire un collegamento trunk, è necessario configurare manualmente la porta adiacente come porta trunk. Questa opzione è utile per i dispositivi che non supportano il DTP.	No	`Trunking` incondizionato
`Dinamica`	Fa in modo che la porta	Sì, periodico	Il `trunki`

desiderabile (è consigliabile un comando paragonabile a CatOS)	tenti attivamente di convertire il collegamento in un collegamento trunk. La porta diventa una porta trunk se la porta adiacente è impostata su on, desired o auto mode.		ng termina solo se la modalità remota è attivata, automatica o desiderata.
Accesso	Porta in modalità non trunking permanente e negozia per convertire il collegamento in un collegamento non trunk. La porta diventa una porta non trunk anche se la porta adiacente non accetta la modifica.	No, allo stato stazionario, ma trasmette le informazioni per accelerare il rilevamento dell'estremità remota dopo un passaggio da in avanti.	Non trunking

Nota: è possibile impostare o negoziare il tipo di incapsulamento ISL e 802.1Q.

Nella configurazione predefinita, il DTP presume le seguenti caratteristiche sul collegamento:

- Le connessioni point-to-point e i dispositivi Cisco supportano le porte trunk 802.1Q che sono solo point-to-point.
- Durante la negoziazione DTP, le porte non partecipano a STP. La porta viene aggiunta a STP solo dopo che il tipo di porta è diventato uno dei tre seguenti:AccessoISL802.1QPAgP è il processo successivo da eseguire prima che la porta partecipi a STP. PAgP viene utilizzato per la negoziazione automatica EtherChannel.
- La VLAN 1 è sempre presente sulla porta trunk. Se la porta è trunking in modalità ISL, i pacchetti DTP vengono inviati sulla VLAN 1. Se la porta non trunking in modalità ISL, i pacchetti DTP vengono inviati sulla VLAN nativa (per le porte trunking 802.1Q o non trunking).
- I pacchetti DTP trasferiscono il nome di dominio VTP, la configurazione del trunk e lo stato admin. Affinché venga generato un trunk negoziato, il nome di dominio VTP deve corrispondere. Questi pacchetti vengono inviati ogni secondo durante la negoziazione e ogni 30 secondi dopo la negoziazione. Se una porta in modalità auto o desiderabile non rileva un pacchetto DTP entro 5 minuti (min), la porta viene impostata come non trunk.

Attenzione: è necessario comprendere che le modalità trunk, nonegotiate e access specificano esplicitamente lo stato in cui la porta termina. Una configurazione errata può portare a uno stato pericoloso/incoerente in cui un lato è trunking e l'altro non è trunking.

Per ulteriori informazioni sull'ISL, fare riferimento a Configurazione del trunking ISL sugli switch

Catalyst serie 5500/5000 e 6500/6000. Per ulteriori informazioni sugli switch 802.1Q, fare riferimento al trunking tra gli switch Catalyst serie 4500/4000, 5500/5000 e 6500/6000 con incapsulamento 802.1Q con software Cisco CatOS.

Tipo di incapsulamento

Panoramica operativa ISL

ISL è un protocollo di trunking proprietario di Cisco (schema di tagging VLAN). ISL è in uso da molti anni. Al contrario, 802.1Q è molto più recente, ma 802.1Q è lo standard IEEE.

ISL incapsula completamente il frame originale in uno schema di tagging a due livelli. In questo modo, ISL è effettivamente un protocollo di tunneling e, come vantaggio aggiuntivo, trasporta frame non Ethernet. ISL aggiunge un'intestazione da 26 byte e un FCS da 4 byte al frame Ethernet standard. Le porte configurate come trunk prevedono e gestiscono i frame Ethernet di dimensioni maggiori. ISL supporta 1024 VLAN.

Formato frame - Tag ISL ombreggiato

40 Bits	4 Bits	4 Bits	48 Bits	16 Bits	24 Bits	24 Bits	15 Bits	1 Bit	16 Bits	16 Bits
DA	Type	USER	SA	LEN	SNAP LLC	HSA	VLAN	BPDU	INDEX	Reserve
01-00-0c-00-00					AAAA03	00000C				

Encapsulated Frame	FCS
Variable length	32 bits

Per ulteriori informazioni, fare riferimento a Collegamento tra switch e formato frame IEEE 802.1Q.

Panoramica operativa 802.1Q

Sebbene lo standard IEEE 802.1Q si riferisca solo a Ethernet, lo standard specifica molto di più dei tipi di incapsulamento. 802.1Q include, tra gli altri GARP (Generic Attribute Registration Protocol), miglioramenti spanning-tree e tag QoS 802.1p. Per ulteriori informazioni, fare riferimento a Standard IEEE online .

Il formato di frame 802.1Q conserva le schede Ethernet SA e DA originali. Tuttavia, gli switch devono ora aspettarsi di ricevere frame baby-giant, anche sulle porte di accesso dove gli host possono usare la funzione di tagging per esprimere la priorità degli utenti 802.1p per la

segnalazione QoS. Il tag è di 4 byte. I frame Ethernet v2 802.1Q sono da 1522 byte, un risultato ottenuto dal gruppo di lavoro IEEE 802.3ac. Inoltre, 802.1Q supporta la numerazione degli spazi per le VLAN 4096.

Tutti i frame dati trasmessi e ricevuti sono contrassegnati con tag 802.1Q, ad eccezione dei frame che si trovano sulla VLAN nativa. In questo caso, è presente un tag implicito basato sulla configurazione della porta dello switch in entrata. I frame sulla VLAN nativa vengono sempre trasmessi senza tag e normalmente ricevuti senza tag. Tuttavia, questi frame possono anche essere ricevuti con tag.

Per ulteriori informazioni, fare riferimento a questi documenti:

- Interoperabilità VLAN
- Trunking tra switch Catalyst serie 4500/4000, 5500/5000 e 6500/6000 con incapsulamento 802.1q con software Cisco CatOS

Formato frame 802.1Q/802.1p

		Tag Header						
		TPID	TCI					
48 bits	48 bits	16 bits	3 bits	1 bit	12 bits	16 bits	Variable length	32 bits
DA	SA	TPID	Priority	CFI	VLAN ID	Length/ Type	Data with PAD	FCS
		0x8100	0 – 7	0-1	0-4095			

Consiglio di configurazione Cisco

Uno dei principali obiettivi di Cisco è quello di ricercare la coerenza all'interno della rete, laddove sia possibile. Tutti i nuovi prodotti Catalyst supportano 802.1Q e alcuni supportano solo 802.1Q, ad esempio i moduli precedenti di Catalyst serie 4500/4000 e Catalyst serie 6500. Pertanto, tutte le nuove implementazioni devono seguire questo standard IEEE 802.1Q e le reti precedenti devono migrare gradualmente da ISL.

Per abilitare il trunking 802.1Q su una determinata porta, usare questo comando di interfaccia:

```
Switch(config)#interface type slot#/port#
Switch(config-if)#switchport
!--- Configure the interface as a Layer 2 port. Switch(config-if)#switchport trunk encapsulation
dot1q
```

Lo standard IEEE consente l'interoperabilità con i fornitori. L'interoperabilità con i fornitori è vantaggiosa in tutti gli ambienti Cisco in quanto sono disponibili nuove schede di interfaccia di rete e nuovi dispositivi compatibili con 802.1p. Sebbene le implementazioni ISL e 802.1Q siano solide, lo standard IEEE ha in ultima analisi una maggiore esposizione sul campo e un maggiore supporto di terze parti, che include il supporto per gli analizzatori di rete. Inoltre, una considerazione minore è che lo standard 802.1Q ha anche un sovraccarico di incapsulamento inferiore rispetto a ISL.

Per motivi di completezza, l'assegnazione implicita di tag sulle VLAN native costituisce un fattore di sicurezza. È possibile trasmettere i frame da una VLAN, VLAN X, a un'altra VLAN, VLAN Y, senza un router. La trasmissione può avvenire senza un router se la porta di origine (VLAN X) si trova sulla stessa VLAN della VLAN nativa di un trunk 802.1Q sullo stesso switch. Per risolvere il problema, è possibile usare una VLAN fittizia per la VLAN nativa del trunk.

Per stabilire una VLAN nativa (impostazione predefinita) per il trunking 802.1Q su una determinata porta, eseguire questi comandi di interfaccia:

```
Switch(config)#interface type slot#/port#
Switch(config-If)#switchport trunk native vlan 999
```

Poiché tutti i nuovi componenti hardware supportano 802.1Q, tutte le nuove implementazioni sono conformi allo standard IEEE 802.1Q e consentono la migrazione graduale delle reti precedenti da ISL. Fino a poco tempo fa, molti moduli Catalyst 4500/4000 non supportavano ISL. Pertanto, 802.1Q è l'unica opzione per il trunking Ethernet. Fare riferimento all'output del comando **show interface capabilities** o del comando **show port capabilities** per CatOS. Poiché il supporto per il trunking richiede l'hardware appropriato, un modulo che non supporta 802.1Q non può mai supportare 802.1Q. L'aggiornamento del software non supporta 802.1Q. La maggior parte del nuovo hardware degli switch Catalyst 6500/6000 e Catalyst 4500/4000 supporta sia ISL che 802.1Q.

Se la VLAN 1 viene eliminata da un trunk, come descritto nella sezione Switch Management Interface e Native VLAN, sebbene non vengano trasmessi o ricevuti dati utente, il protocollo NMP continua a passare i protocolli di controllo sulla VLAN 1. Esempi di protocolli di controllo sono CDP e VTP.

Inoltre, come descritto nella sezione VLAN 1, i pacchetti CDP, VTP e PAgP vengono sempre inviati sulla VLAN 1 durante il trunking. Con l'incapsulamento dot1q (802.1Q), questi frame di controllo sono contrassegnati con la VLAN 1 se viene modificata la VLAN nativa dello switch. Se il trunking dot1q su un router e la VLAN nativa viene modificata sullo switch, è necessaria una sottointerfaccia nella VLAN 1 per ricevere i frame CDP contrassegnati e fornire la visibilità dei router adiacenti CDP.

Nota: il dot1q è una potenziale considerazione di sicurezza che può essere causata dal tagging implicito della VLAN nativa. È possibile trasmettere i frame da una VLAN all'altra senza un router. Per ulteriori informazioni, consultare le domande frequenti sul rilevamento delle intrusioni . Per risolvere il problema, è possibile usare un ID VLAN per la VLAN nativa del trunk che non sia usato per l'accesso dell'utente finale. Per ottenere questo risultato, la maggior parte dei clienti Cisco lascia la VLAN 1 come VLAN nativa su un trunk e assegna le porte di accesso alle VLAN diverse dalla VLAN 1.

Cisco consiglia una configurazione esplicita della modalità trunk di `dynamic desiderabile` su

entrambe le estremità. Questa è la modalità predefinita. In questa modalità, gli operatori di rete possono considerare attendibili i messaggi di stato della riga di comando e del syslog per cui una porta è `attiva` e trunking. Questa modalità è diversa dalla modalità `on`, che consente di visualizzare una porta anche se il router adiacente non è configurato correttamente. Inoltre, i trunk in modalità `desiderabile` forniscono stabilità in situazioni in cui un lato del collegamento non può diventare un trunk o cede lo stato `trunk`.

Se il tipo di incapsulamento viene negoziato tra gli switch con l'uso del DTP e l'opzione ISL viene scelta come vincitore per impostazione predefinita, se entrambe le estremità lo supportano, è necessario usare questo comando di interfaccia per specificare dot1q[1]:

```
switchport trunk encapsulation dot1q
```

[1] Alcuni moduli che includono WS-X6548-GE-TX e WS-X6148-GE-TX non supportano il trunking ISL. Questi moduli non accettano il comando **switchport trunk encapsulation *dot1q***.

Nota: per disabilitare i trunk su una porta, usare il comando **switchport mode access**. Questa disabilitazione aiuta a eliminare lo spreco di tempo delle negoziazioni quando vengono aperte porte host.

```
Switch(config-if)#switchport host
```

Altre opzioni

Un'altra configurazione comune del cliente utilizza la modalità `desiderabile dinamica` a livello di distribuzione e la configurazione predefinita più semplice (modalità `automatica dinamica`) a livello di accesso. alcuni switch, come Catalyst 2900XL, i router Cisco IOS o altri dispositivi del fornitore, non supportano al momento la negoziazione trunk tramite DTP. È possibile utilizzare la modalità `non negoziazione` per impostare una porta in modo che venga trunk in modo incondizionato su questi dispositivi. Questa modalità consente di standardizzare un'impostazione comune in tutto il campus.

Cisco consiglia di `non negoziare` quando ci si connette a un router Cisco IOS. Durante il bridging, alcuni frame DTP ricevuti da una porta configurata con **switchport mode trunk** possono tornare alla porta trunk. Alla ricezione del frame DTP, la porta dello switch cerca di rinegoziare inutilmente. Per eseguire la rinegoziazione, la porta dello switch `abbassa` il trunk e lo `solleva`. Se l'opzione `non negoziazione` è abilitata, lo switch non invia frame DTP.

```
switch(config)#interface type slot#/port#
switch(config-if)#switchport mode dynamic desirable
!--- Configure the interface as trunking in desirable !--- mode for switch-to-switch links with
multiple VLANs. !--- And... switch(config-if)#switchport mode trunk
!--- Force the interface into trunk mode without negotiation of the trunk connection. !--- Or...
switch(config-if)#switchport nonegotiate
!--- Set trunking mode to not send DTP negotiation packets !--- for trunks to routers.
switch(config-if)#switchport access vlan vlan_number
!--- Configure a fallback VLAN for the interface. switch(config-if)#switchport trunk native vlan
999
!--- Set the native VLAN. switch(config-if)#switchport trunk allowed vlan vlan_number_or_range
!--- Configure the VLANs that are allowed on the trunk.
```

Spanning Tree Protocol

Scopo

Lo Spanning Tree mantiene un ambiente Layer 2 privo di loop in reti bridge e commutate ridondanti. Senza STP, i fotogrammi vengono ripetuti e/o moltiplicati per un tempo indefinito. Questa circostanza causa un blocco della rete in quanto un traffico elevato interrompe tutti i dispositivi nel dominio di trasmissione.

Per alcuni aspetti, STP è un protocollo che è stato inizialmente sviluppato per le specifiche bridge basate su software lento (IEEE 802.1D). Tuttavia, l'STP può essere complicato per la corretta implementazione in reti a commutazione di grandi dimensioni con:

- Molte VLAN
- Molti switch in un dominio
- Supporto multifornitore
- Nuovi miglioramenti IEEE

Il software di sistema Cisco IOS ha iniziato a sviluppare nuovi sistemi STP. I nuovi standard IEEE, che includono i protocolli 802.1w Rapid STP e 802.1s Multiple Spanning Tree, forniscono convergenza rapida, condivisione del carico e scalabilità del control plane. Inoltre, le funzionalità avanzate di STP come RootGuard, filtro BPDU, Portfast BPDU Guard e Loopguard forniscono una protezione aggiuntiva contro i loop di inoltro di layer 2.

Panoramica operativa di PVST+

La scelta del bridge radice per VLAN viene effettuata dallo switch con l'identificatore del bridge radice (BID) più basso. L'offerta è la priorità del bridge in combinazione con l'indirizzo MAC dello switch.

Inizialmente, le BPDU vengono inviate da tutti gli switch e contengono l'offerta di ciascuno switch e il costo del percorso per raggiungere lo switch. In questo modo è possibile determinare il bridge radice e il percorso più economico alla radice. I parametri di configurazione aggiuntivi contenuti nelle BPDU della directory principale sostituiscono quelli configurati localmente in modo che l'intera rete utilizzi timer coerenti. Per ogni BPDU ricevuto da uno switch dalla radice, il protocollo NMP centrale Catalyst elabora una nuova BPDU e la invia con le informazioni della radice.

La topologia converge attraverso i seguenti passaggi:

1. Viene selezionato un singolo bridge radice per l'intero dominio Spanning Tree.
2. Una porta radice (che si trova di fronte al bridge radice) viene selezionata su ogni bridge non radice.
3. Viene selezionata una porta designata per l'inoltro BPDU su ciascun segmento.
4. Le porte non designate diventano bloccanti.

Per ulteriori informazioni, fare riferimento a questi documenti:

- Configurazione di STP e IEEE 802.1s MST
- Informazioni sul protocollo Rapid Spanning Tree (802.1w)

Timer pred	Nome	Funzione

efiniti		
2 sec.	salve	Controlla la partenza delle BPDU.
15 sec.	ritardo in avanti (Fwd delay)	Controlla il tempo che una porta impiega nello stato di `ascolto` e nell'`apprendimento` dello stato e influenza il processo di modifica della topologia.
20 sec	massimo	Controlla per quanto tempo lo switch conserva la topologia corrente prima di cercare un percorso alternativo. Dopo il periodo di aging massimo (massimo), un BPDU viene considerato obsoleto e lo switch cerca una nuova porta radice nel pool delle porte bloccanti. Se non è disponibile alcuna porta bloccata, lo switch dichiara di essere la radice stessa sulle porte designate.

Cisco consiglia di non modificare i timer perché ciò potrebbe influire negativamente sulla stabilità. La maggior parte delle reti distribuite non vengono ottimizzate. I semplici timer STP accessibili tramite la riga di comando (ad esempio hello-interval, maxage e così via) sono a loro volta costituiti da un insieme complesso di altri timer presunti e intrinseci. Pertanto, è difficile regolare i timer e considerare tutte le ramificazioni. Inoltre, è possibile minacciare la protezione UDLD. Per ulteriori informazioni, vedere la sezione Rilevamento collegamento unidirezionale.

Nota sui timer STP:

I valori predefiniti del timer per il protocollo STP si basano su un calcolo che prende in considerazione il diametro di rete di sette switch (sette hop dalla radice al bordo della rete) e il tempo necessario affinché una BPDU viaggi dal bridge radice agli switch al bordo della rete, ossia sette hop di distanza. Questo presupposto calcola i valori del timer accettabili per la maggior parte delle reti. Tuttavia, è possibile modificare questi timer in valori ottimali per accelerare i tempi di convergenza durante le modifiche della topologia di rete.

Èpossibile configurare il bridge radice con il diametro di rete per una VLAN specifica e i valori del timer vengono calcolati di conseguenza. Cisco consiglia, se è necessario apportare modifiche, di configurare solo i parametri di diametro e di ora legale sul bridge radice per la VLAN.

```
spanning-tree vlan vlan-id [root {primary | secondary}] [diameter diameter-value [hello hello-time]]
!--- This command needs to be on one line.
```

Questa macro crea la radice dello switch per la VLAN specificata, calcola i nuovi valori del timer in base al diametro e al tempo di saluto specificati e propaga queste informazioni nella configurazione BPDU a tutti gli altri switch della topologia.

La sezione Nuovi stati e ruoli porta descrive il protocollo 802.1D STP e confronta e confronta il protocollo 802.1D STP con il protocollo RSTP (Rapid STP). per ulteriori informazioni sul protocollo

RSTP, fare riferimento a Descrizione del protocollo 802.1w (Rapid Spanning Tree Protocol).

Nuovi stati e ruoli porta

802.1D è definito in quattro diversi stati di porta:

- Ascolto
- Apprendimento
- Blocco
- Inoltro

Per ulteriori informazioni, vedere la tabella nella sezione Port States. Lo stato della porta è misto (blocco o inoltro del traffico), così come il ruolo che la porta svolge nella topologia attiva (porta radice, porta designata e così via). Ad esempio, da un punto di vista operativo, non vi è differenza tra una porta in stato di blocco e una porta in stato di ascolto. Entrambi scartano i frame e non imparano gli indirizzi MAC. La vera differenza sta nel ruolo assegnato dallo Spanning Tree alla porta. Si può tranquillamente supporre che una porta di ascolto sia designata o principale e sia in viaggio verso lo stato di inoltro. Purtroppo, una volta che la porta è in stato di inoltro, non è possibile dedurre dallo stato della porta se la porta è radice o designata. Questo dimostra il fallimento di questa terminologia basata sullo stato. RSTP risolve questo errore perché RSTP dissocia il ruolo e lo stato di una porta.

Stati porta

Stati delle porte in STP 802.1D

Stati porte	Mezzi	Intervalli predefiniti allo stato successivo
`Disattivato`	Amministrativamente inattivo.	
`Blocco`	Riceve BPDU e arresta i dati utente.	Controlla la ricezione delle BPDU. 20 secondi di attesa per la scadenza massima o la modifica immediata se viene rilevato un errore del collegamento diretto/locale.
`Ascolto`	Invia o riceve pacchetti BPDU per verificare se è necessario tornare al blocco.	Attendere 15 secondi Fwddelay.
`Apprendimento`	Crea una tabella di topologia/CAM.	Attendere 15 secondi Fwddelay.
`Inoltro`	Invia/riceve dati.	

Totale modifiche alla topologia di base:

- 20 + 2 (15) = 50 sec, in attesa della scadenza di maxage
- 30 secondi per errore collegamento diretto

In RSTP rimangono solo tre stati di porta, che corrispondono ai tre possibili stati operativi. Gli stati 802.1D disabilitati, di blocco e di ascolto sono stati uniti in uno stato di eliminazione 802.1w univoco.

Stato porta STP (802.1D)	RSTP (802.1w) - Stato porta	La porta è inclusa nella topologia attiva?	Indica gli indirizzi MAC di Port Learning.
Disattivato	Eliminazione	No	No
Blocco	Eliminazione	No	No
Ascolto	Eliminazione	Sì	No
Apprendimento	Apprendimento	Sì	Sì
Inoltro	Inoltro	Sì	Sì

Ruoli porta

Il ruolo è ora una variabile assegnata a una determinata porta. La porta radice e i ruoli della porta designati rimangono, ma il ruolo della porta bloccante è ora suddiviso nei ruoli della porta di backup e alternativa. Lo Spanning Tree Algorithm (STA) determina il ruolo di una porta sulla base di BPDU. Tenere presente quanto segue sulle BPDU per semplificare le procedure: esiste sempre un modo per confrontare due BPDU e decidere se una è più utile dell'altra. La base della decisione è il valore memorizzato nella BPDU e, occasionalmente, la porta su cui la BPDU viene ricevuta. Nella parte restante di questa sezione vengono illustrati alcuni approcci molto pratici ai ruoli delle porte.

Ruolo porta radice

La porta che riceve il miglior pacchetto BPDU su un bridge è la porta radice. Questa è la porta più vicina al bridge radice in termini di costo del percorso. La STA seleziona un singolo bridge radice nell'intera rete con bridging (per VLAN). Il bridge radice invia pacchetti BPDU più utili di quelli che possono essere inviati da qualsiasi altro bridge. Il bridge radice è l'unico bridge della rete che non dispone di una porta radice. Tutti gli altri bridge ricevono BPDU su almeno una porta.

Ruolo porta designata

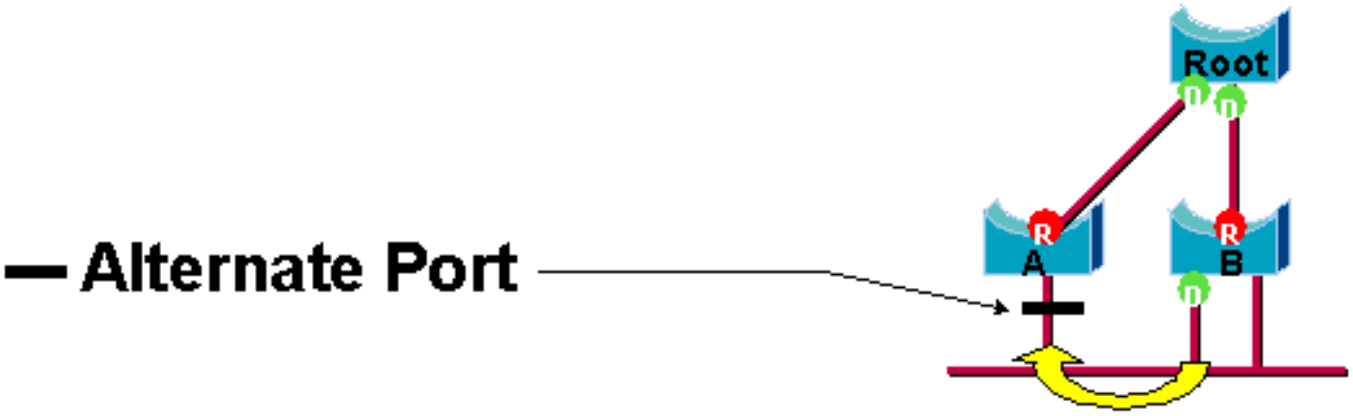
La porta è designata se può inviare il miglior pacchetto BPDU sul segmento a cui è collegata. I

bridge 802.1D collegano segmenti diversi (ad esempio, segmenti Ethernet) per creare un dominio con bridging. Su un determinato segmento, può esistere un solo percorso verso il ponte radice. Se sono presenti due percorsi, nella rete è presente un loop di bridging. Tutti i bridge connessi a un determinato segmento ascoltano le BPDU degli altri e concordano sul bridge che invia la BPDU migliore come bridge designato per il segmento. La porta corrispondente su tale ponte è designata.

Ruoli delle porte alternative e di backup

Questi due ruoli di porta corrispondono allo stato di blocco di 802.1D. La definizione di una porta bloccata è una porta che non è la porta designata o radice. Una porta bloccata riceve una BPDU più utile rispetto a quella che invia sul proprio segmento. Tenere presente che per mantenere il blocco, una porta deve assolutamente ricevere pacchetti BPDU. RSTP introduce questi due ruoli a questo scopo.

Una porta alternativa è una porta bloccata dalla ricezione di BPDU più utili da un altro bridge. Il diagramma mostra:



Una porta di backup è una porta bloccata dalla ricezione di BPDU più utili dallo stesso bridge su cui si trova la porta. Il diagramma mostra:

Questa distinzione è già stata fatta internamente all'interno di 802.1D. Questo è essenzialmente il modo in cui funziona Cisco UplinkFast. La logica alla base di questa operazione è che una porta alternativa fornisce un percorso alternativo al bridge radice. Pertanto, in caso di errore, questa porta può sostituire la porta radice. Naturalmente, una porta di backup fornisce connettività ridondante allo stesso segmento e non può garantire una connettività alternativa al bridge radice. La porta di backup è stata pertanto esclusa dal gruppo uplink.

Di conseguenza, RSTP calcola la topologia finale per lo Spanning Tree utilizzando esattamente gli stessi criteri di 802.1D. Non vi è alcun cambiamento nel modo in cui vengono utilizzate le diverse priorità dei ponti e dei porti. Il blocco dei nomi viene utilizzato per lo stato di eliminazione nell'implementazione di Cisco. CatOS versione 7.1 e successive visualizzano ancora gli stati di ascolto e apprendimento, che forniscono informazioni su una porta ancora maggiori di quelle richieste dallo standard IEEE. Tuttavia, la novità è che ora esiste una differenza tra il ruolo determinato dal protocollo per una porta e lo stato corrente. Ad esempio, ora è perfettamente valido per una porta da designare e bloccare contemporaneamente. Anche se in genere ciò accade per periodi di tempo molto brevi, significa semplicemente che questa porta si trova in uno stato transitorio verso l'inoltro designato.

Interazioni STP con VLAN

Per correlare le VLAN allo Spanning Tree, è possibile procedere in tre modi:

- uno Spanning Tree singolo per tutte le VLAN o un CST (Common Spanning Tree Protocol), ad esempio IEEE 802.1D
- uno Spanning Tree per VLAN o uno Spanning Tree condiviso, ad esempio Cisco PVST
- uno Spanning Tree per set di VLAN o un Multiple Spanning Tree (MST), ad esempio IEEE 802.1s

Da un punto di vista della configurazione, questi tre tipi di modalità Spanning Tree relative all'interazione con le VLAN possono essere configurati in uno dei tre tipi di modalità seguenti:

- **pvst**: Spanning Tree per VLAN. In questo modo viene implementato PVST+, ma nel software Cisco IOS viene indicato semplicemente come PVST.
- **rapid-pvst**: l'evoluzione dello standard 802.1D migliora i tempi di convergenza e incorpora le proprietà basate su standard (802.1w) di UplinkFast e BackboneFast.
- **mst** - È lo standard 802.1s per uno spanning tree su ciascun set di VLAN o MST. Questo incorpora anche il componente rapido 802.1w all'interno dello standard.

Uno Spanning Tree mono per tutte le VLAN consente solo una topologia attiva e quindi nessun bilanciamento del carico. Un STP blocca le porte per tutte le VLAN e non trasporta dati.

uno Spanning Tree per VLAN o PVST+ consente il bilanciamento del carico ma richiede una maggiore elaborazione della CPU BPDU all'aumentare del numero di VLAN.

Il nuovo standard 802.1s (MST) consente di definire fino a 16 istanze/topologie STP attive e di mappare tutte le VLAN a tali istanze. In un ambiente campus tipico, è necessario definire solo due istanze. Questa tecnica consente la scalabilità STP di molte migliaia di VLAN e, allo stesso tempo, il bilanciamento del carico.

Il supporto per Rapid-PVST e MST pre-standard è introdotto nel software Cisco IOS versione 12.1(11b)EX e 12.1(13)E per Catalyst 6500. Catalyst 4500 con software Cisco IOS versione 12.1(12c)EW e successive supporta MST pre-standard. Il supporto Rapid PVST è stato aggiunto nel software Cisco IOS versione 12.1(19)EW per la piattaforma Catalyst 4500. Il software MST conforme allo standard è supportato nel software Cisco IOS versione 12.2(18)SXF per Catalyst 6500 e nel software Cisco IOS versione 12.2(25)SG per gli switch Catalyst serie 4500.

per ulteriori informazioni, fare riferimento a Descrizione del protocollo Rapid Spanning-Tree Protocol (802.1w) e Descrizione del protocollo Multiple Spanning-Tree Protocol (802.1s).

Porte logiche dello Spanning Tree

Le note di rilascio di Catalyst 4500 e 6500 forniscono indicazioni sul numero di porte logiche nello Spanning Tree per switch. La somma di tutte le porte logiche è uguale al numero di trunk sullo switch moltiplicato per il numero di VLAN attive sui trunk, più il numero di interfacce non trunking sullo switch. Il software Cisco IOS genera un messaggio di registro del sistema se il numero massimo di interfacce logiche supera il limite. Si raccomanda di non superare gli orientamenti raccomandati.

In questa tabella viene confrontato il numero di porte logiche supportate con le diverse modalità STP e il tipo di supervisore:

Supervisor	PVST+	RPVST+	MST
Catalyst 6500 Supervisor 1	6.000[1] in totale 1.200 per modulo di switching	6.000 in totale 1.200 per modulo di switching	25.000 3.000[2] per modulo di switching
Catalyst 6500 Supervisor 2	13.000[1] totale 1.800[2] per modulo di switching	10.000 in totale 1.800[2] per modulo di switching	50.000 6.000[2] per modulo di switching
Catalyst 6500 Supervisor 720	13.000 in totale 1.800[2] per modulo di switching	10.000 in totale 1.800[2] per modulo di switching	50.003 6.000[2] per modulo di switching
Catalyst 4500 Supervisor II plus	1.500 in totale	1.500 in totale	25.000 in totale
Catalyst 4500 Supervisor	1.500 in totale	1.500 in totale	25.000 in totale

II plus-10GE			
Catalyst 4500 Supervisor IV	3.000 in totale	3.000 in totale	50.000 in totale
Catalyst 4500 Supervisor V	3.000 in totale	3.000 in totale	50.000 in totale
Catalyst 4500 Supervisor V 10GE	3.000 in totale	3.000 in totale	80.000 in totale

[1] Il numero massimo di porte logiche totali supportate in PVST+ con versione precedente al software Cisco IOS versione 12.1(13)E è 4.500.

[2] moduli di switching da 10 Mbps, 10/100 Mbps e 100 Mbps supportano un massimo di 1.200 interfacce logiche per modulo.

[3] Il numero massimo di porte logiche supportate in MST con software Cisco IOS versione 12.2(17b)SXA è 30.000.

Suggerimento

È difficile fornire una raccomandazione sulla modalità spanning-tree senza informazioni dettagliate quali hardware, software, numero di dispositivi e numero di VLAN. In generale, se il numero di porte logiche non supera le linee guida consigliate, per la distribuzione di una nuova rete è consigliabile utilizzare la modalità PVST rapida. La modalità PVST rapida fornisce una rapida convergenza di rete senza la necessità di ulteriori configurazioni, quali Backbone Fast e Uplink Fast. Per impostare lo spanning-tree in modalità Rapid-PVST, eseguire il comando seguente:

```
spanning-tree mode rapid-pvst
```

Altre opzioni

In una rete con una combinazione di hardware legacy e software precedente, è consigliata la modalità PVST+. Utilizzare questo comando per impostare lo spanning-tree in modalità PVST+:

```
spanning-tree mode pvst
----This is default and it shows in the configuration.
```

La modalità MST è consigliata per le VLAN in tutte le configurazioni di rete con un numero elevato di VLAN. Per questa rete, la somma delle porte logiche può superare le linee guida per PVST e Rapid-PVST. Utilizzare questo comando per impostare lo spanning-tree in modalità MST:

```
spanning-tree mode mst
```

Formati BPDU

Per supportare lo standard IEEE 802.1Q, Cisco ha esteso il protocollo PVST esistente in modo da fornire il protocollo PVST+. PVST+ aggiunge il supporto per i collegamenti nell'area dello spanning tree mono IEEE 802.1Q. PVST+ è compatibile sia con lo Spanning Tree mono IEEE 802.1Q sia con i protocolli Cisco PVST esistenti. Inoltre, PVST+ aggiunge meccanismi di controllo per garantire che non vi siano incoerenze di configurazione del trunking della porta e dell'ID della VLAN sugli switch. PVST+ è compatibile plug-and-play con PVST, senza la necessità di un nuovo comando o configurazione dell'interfaccia della riga di comando (CLI).

Di seguito sono riportati alcuni aspetti della teoria operativa del protocollo PVST+:

- PVST+ interagisce con lo spanning tree mono 802.1Q. PVST+ interagisce con switch conformi a 802.1Q su STP comune tramite trunking 802.1Q. Per impostazione predefinita, lo spanning tree comune è sulla VLAN 1, la VLAN nativa. Un BPDU Spanning Tree comune viene trasmesso o ricevuto con l'indirizzo MAC standard del gruppo di bridge IEEE (01-80-c2-00-00-00, tipo di protocollo 0x010c) sui collegamenti 802.1Q. Lo Spanning Tree comune può avere radici nella regione PVST o Mono Spanning Tree.
- PVST+ esegue il tunneling delle PVST BPDU sulla regione VLAN 802.1Q come dati multicast. Per ciascuna VLAN su un trunk, vengono trasmesse o ricevute BPDU con indirizzo MAC Cisco Shared STP (SSTP) (01-00-0c-cc-cd). Per le VLAN uguali all'identificatore della porta VLAN (PVID), il BPDU non ha tag. A tutte le altre VLAN, i BPDU hanno un tag.
- PVST+ è compatibile con le versioni precedenti dello switch Cisco su PVST tramite trunking ISL. I BPDU incapsulati dall'ISL vengono trasmessi o ricevuti tramite trunk ISL, analogamente al precedente protocollo Cisco PVST.
- PVST+ verifica le incoerenze tra porte e VLAN. PVST+ blocca le porte che ricevono BPDU incoerenti per impedire il verificarsi di loop di inoltro. PVST+ notifica inoltre agli utenti eventuali incoerenze tramite messaggi syslog.

Nota: nelle reti ISL, tutti i BPDU vengono inviati con l'indirizzo MAC IEEE.

Suggerimenti per la configurazione di Cisco

Per impostazione predefinita, su tutti gli switch Catalyst il protocollo STP è abilitato. Anche se si sceglie un progetto che non include loop di livello 2 e il protocollo STP non è abilitato per mantenere attiva una porta bloccata, lasciare la funzione abilitata per i seguenti motivi:

- In caso di loop, l'STP impedisce i problemi che possono essere aggravati dal multicast e dai dati trasmessi. Spesso la presenza di patch non corrette, la presenza di un cavo non valido o un'altra causa inducono a creare un loop.
- STP protegge da un guasto di EtherChannel.
- La maggior parte delle reti sono configurate con STP e pertanto ottengono la massima esposizione sul campo. Una maggiore esposizione equivale in genere a un codice più stabile.
- STP protegge da comportamenti errati delle schede NIC a doppio collegamento (o bridging abilitato sui server).
- Molti protocolli sono strettamente correlati a STP nel codice. Alcuni esempi:PAgPSnooping IGMP (Internet Group Message Protocol)TrunkingSe si esegue senza STP, è possibile ottenere risultati indesiderati.

- Durante un'interruzione di rete segnalata, i tecnici Cisco suggeriscono solitamente che il mancato utilizzo dell'STP è al centro del guasto, se non del tutto concepibile.

Per abilitare lo Spanning Tree su tutte le VLAN, usare questi comandi globali:

```
Switch(config)#spanning-tree vlan vlan_id
!--- Specify the VLAN that you want to modify. Switch(config)#default spanning-tree vlan vlan_id
!--- Set spanning-tree parameters to default values.
```

Non modificare i timer, il che può influire negativamente sulla stabilità. La maggior parte delle reti distribuite non vengono ottimizzate. I semplici timer STP accessibili tramite riga di comando, ad esempio hello-interval e maxage, dispongono di un insieme complesso di timer presupposti e intrinseci. Pertanto, si possono avere difficoltà se si tenta di regolare i timer e considerare tutte le ramificazioni. Inoltre, è possibile minacciare la protezione UDLD.

In teoria, evitare che il traffico degli utenti passi dalla VLAN di gestione. soluzione non applicabile agli switch Catalyst 6500/6000 Cisco IOS. Tuttavia, è necessario rispettare questa raccomandazione sugli switch Cisco IOS e CatOS di fascia più piccola che possono avere un'interfaccia di gestione separata e devono essere integrati con gli switch Cisco IOS. Specialmente con i processori switch Catalyst di vecchia generazione, tenere la VLAN di gestione separata dai dati dell'utente per evitare problemi con l'STP. Una stazione terminale che si comporta in modo errato può potenzialmente tenere il processore Supervisor Engine così occupato con i pacchetti di broadcast che il processore potrebbe perdere una o più BPDU. Tuttavia, gli switch più recenti con CPU più potenti e controlli di limitazione attenuano questa considerazione. Per ulteriori informazioni, vedere la sezione Interfaccia di gestione dello switch e VLAN nativa di questo documento.

Non sovraprogettare la ridondanza. Ciò può comportare il blocco di un numero eccessivo di porte e compromettere la stabilità a lungo termine. Mantenere il diametro totale di STP al di sotto di sette hop. Provare a progettare fino al modello multilayer di Cisco quando questo progetto è possibile. Le feature del modello:

- Domini a commutazione di dimensioni inferiori
- Triangoli STP
- Porte bloccate deterministiche

Influenza e conoscenza della posizione delle funzionalità principali e delle porte bloccate. Documentare queste informazioni nel diagramma della topologia. Conoscere la topologia Spanning Tree, essenziale per la risoluzione dei problemi. Le porte bloccate sono il punto in cui inizia la risoluzione dei problemi STP. La causa della modifica dal blocco all'inoltro è spesso la parte chiave dell'analisi della causa principale. Scegliete i livelli di distribuzione e core come posizione della radice principale/secondaria perché questi livelli sono considerati le parti più stabili della rete. Verificare la sovrapposizione ottimale di HSRP (Layer 3 and Hot Standby Router Protocol) con i percorsi di inoltro dati di Layer 2.

Questo comando è una macro che configura la priorità del bridge. La radice imposta la priorità in modo che sia molto più bassa di quella predefinita (32.768) e la secondaria imposta la priorità in modo che sia ragionevolmente più bassa di quella predefinita:

```
Switch(config)#interface type slot/port
Switch(config)#spanning-tree vlan vlan_id root primary
!--- Configure a switch as root for a particular VLAN.
```

Nota: questa macro imposta la priorità principale in uno dei modi seguenti:

- 8192 per impostazione predefinita
- Priorità radice corrente meno 1, se è noto un altro bridge radice
- Priorità radice corrente, se l'indirizzo MAC è inferiore alla radice corrente

Eliminare le VLAN non necessarie dalle porte trunk, operazione bidirezionale. L'azione limita il diametro del sovraccarico di elaborazione di STP e NMP su parti della rete in cui alcune VLAN non sono necessarie. L'eliminazione automatica VTP non rimuove il protocollo STP da un trunk. È possibile anche rimuovere la VLAN 1 predefinita dai trunk.

per ulteriori informazioni, fare riferimento a Problemi del protocollo Spanning Tree e considerazioni di progettazione correlate.

Altre opzioni

Cisco dispone di un altro protocollo STP, chiamato **VLAN-bridge**, che funziona con l'uso di un indirizzo MAC di destinazione conosciuto come **01-00-0c-cd-cd-ce** e un tipo di protocollo 0x010c.

Questo protocollo è particolarmente utile quando è necessario eseguire il bridge di protocolli non instradabili o legacy tra VLAN senza interferenze con le istanze dello Spanning Tree IEEE in esecuzione su tali VLAN. Se le interfacce VLAN per il traffico non bridge vengono bloccate per il traffico di layer 2, anche il traffico di layer 3 sovrastante viene inavvertitamente eliminato, creando un effetto collaterale indesiderato. Questo blocco di layer 2 può verificarsi facilmente se le interfacce VLAN per il traffico non bridge partecipano allo stesso STP delle VLAN IP. Il bridge VLAN è un'istanza separata di STP per i protocolli con bridging. Il protocollo fornisce una topologia separata che può essere manipolata senza alcun effetto sul traffico IP.

Eseguire il protocollo VLAN-bridge se è richiesto il bridging tra VLAN su router Cisco come l'MSFC.

Funzione STP PortFast

Èpossibile utilizzare PortFast per ignorare il normale funzionamento dello Spanning Tree sulle porte di accesso. PortFast accelera la connettività tra le unità terminali e i servizi a cui le unità terminali devono connettersi dopo l'inizializzazione del collegamento. Per l'implementazione di Microsoft DHCP, è necessario che la porta di accesso sia in modalità di `inoltro` subito dopo che lo stato del collegamento è `attivo` per poter richiedere e ricevere un indirizzo IP. Alcuni protocolli, ad esempio Internetwork Packet Exchange (IPX)/Sequenced Packet Exchange (SPX), devono visualizzare la porta di accesso in modalità di `inoltro` immediatamente dopo l'`attivazione` dello stato del collegamento in modo da evitare problemi di connessione al server più vicino (GNS).

Per ulteriori informazioni, fare riferimento a Utilizzo di PortFast e di altri comandi per correggere i ritardi della connettività di avvio della workstation.

Panoramica operativa di PortFast

PortFast ignora gli stati normali di `ascolto`, `apprendimento` e `inoltro` di STP. La funzione sposta una porta direttamente dalla modalità di `blocco` alla modalità di `inoltro` dopo che il collegamento è stato `visualizzato come attivo`. Se questa funzione non è abilitata, STP elimina tutti i dati utente finché non decide che la porta è pronta per essere spostata nella modalità di `inoltro`. Questo processo può richiedere (2 x ForwardDelay), ovvero 30 secondi per impostazione predefinita.

`La` modalità `Portfast` impedisce la generazione di una notifica TCN (Topology Change Notification)

STP ogni volta che lo stato di una porta cambia da `apprendimento` a `inoltro`. I TCN sono normali. Ma un'ondata di cittadini di paesi terzi che colpisce il ponte principale può prolungare inutilmente il tempo di convergenza. Un'ondata di cittadini di paesi terzi si verifica spesso la mattina, quando le persone accendono i loro PC.

Suggerimenti per la configurazione della porta di accesso Cisco

Impostare STP PortFast su `on` per tutte le porte host abilitate. Inoltre, impostare esplicitamente STP PortFast su `off` per i collegamenti e le porte dello switch che non sono in uso.

Per implementare la configurazione consigliata per le porte di accesso, usare il comando **switchport host** macro in modalità di configurazione interfaccia. La configurazione inoltre contribuisce in modo significativo alla negoziazione automatica e alle prestazioni della connessione:

```
switch(config)#interface type slot#/port#

switch(config-if)#switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
!--- This macro command modifies these functions.
```

Nota: PortFast non significa che lo Spanning Tree non venga eseguito sulle porte. Le BPDU vengono ancora inviate, ricevute ed elaborate. Lo Spanning Tree è essenziale per una LAN completamente funzionale. Senza il rilevamento e il blocco dei loop, un loop può causare la disattivazione involontaria dell'intera LAN in tempi rapidi.

Inoltre, disabilitare il trunking e il channeling per tutte le porte host. Per impostazione predefinita, ciascuna porta di accesso è abilitata per il trunking e il channeling, ma sulle porte host le porte adiacenti allo switch non sono progettate appositamente. Se si lascia la negoziazione di questi protocolli, il successivo ritardo nell'attivazione della porta può causare situazioni indesiderate. I pacchetti iniziali dalle workstation, come le richieste DHCP e IPX, non vengono inoltrati.

Un'opzione migliore è configurare PortFast per impostazione predefinita nella modalità di configurazione globale con questo comando:

```
Switch(config)#spanning-tree portfast enable
```

Quindi, su ciascuna porta di accesso con un hub o uno switch in una sola VLAN, disabilitare la funzione PortFast su ciascuna interfaccia con il comando **interface**:

```
Switch(config)#interface type slot_num/port_num
Switch(config-if)#spanning-tree portfast disable
```

Altre opzioni

La protezione BPDU PortFast fornisce un metodo per prevenire i loop. BPDU Guard sposta una porta non trunking in uno stato `errDisable` alla ricezione di una BPDU su tale porta.

In condizioni normali, non ricevere mai pacchetti BPDU su una porta di accesso configurata per

PortFast. Una BPDU in ingresso indica una configurazione non valida. L'azione migliore è chiudere la porta di accesso.

Il software di sistema Cisco IOS offre un utile comando globale che abilita automaticamente `BPDU-ROOT-GUARD` su qualsiasi porta abilitata per UplinkFast. Utilizzare *sempre* questo comando. Il comando funziona per switch e non per porta.

Utilizzare questo comando globale per abilitare `BPDU-ROOT-GUARD`:

```
Switch(config)#spanning-tree portfast bpduguard default
```

Un trap SNMP (Simple Network Management Protocol) o un messaggio syslog avvisa il gestore della rete se la porta non funziona. È inoltre possibile configurare un tempo di ripristino automatico per le porte `errDisabled`. Per ulteriori informazioni, vedere la sezione Rilevamento collegamenti unidirezionali di questo documento.

per ulteriori informazioni, fare riferimento ai miglioramenti della funzionalità Spanning Tree PortFast BPDU Guard.

Nota: PortFast per le porte trunk è stata introdotta nel software Cisco IOS versione 12.1(11b)E. PortFast per porte trunk è progettato per aumentare i tempi di convergenza per le reti di layer 3. Quando si utilizza questa funzione, accertarsi di disabilitare BPDU Guard e BPDU Filter sulla base dell'interfaccia.

UplinkFast

Scopo

UplinkFast fornisce una rapida convergenza STP dopo un errore di collegamento diretto nel livello di accesso alla rete. UplinkFast funziona senza modifiche di STP. Lo scopo è quello di accelerare il tempo di convergenza in una specifica circostanza a meno di tre secondi, invece del tipico ritardo di 30 secondi. Fare riferimento alla sezione sulla descrizione e configurazione della funzione Cisco UplinkFast.

Panoramica operativa

Con il modello di progettazione multilayer di Cisco sul livello di accesso, l'uplink di blocco viene immediatamente spostato su uno stato di `inoltro` se l'uplink di inoltro viene perso. La funzione non attende gli stati di `ascolto` e `apprendimento`.

Un gruppo uplink è un insieme di porte per VLAN che possono essere considerate una porta radice e una porta radice di backup. In condizioni normali, le porte radice assicurano la connettività dall'accesso alla radice. Se per qualsiasi motivo la connessione principale principale non riesce, il collegamento principale di backup viene attivato immediatamente, senza che sia necessario attendere i 30 secondi di ritardo della convergenza.

Poiché UplinkFast ignora in modo efficace il normale processo di gestione delle modifiche della topologia STP (`ascolto` e `apprendimento`), è necessario un meccanismo alternativo di correzione della topologia. Il meccanismo deve aggiornare gli switch nel dominio con le informazioni che le stazioni terminali locali sono raggiungibili tramite un percorso alternativo. Pertanto, lo switch del livello di accesso con UplinkFast genera anche frame per ciascun indirizzo MAC nella relativa

tabella CAM a un indirizzo MAC multicast conosciuto (protocollo 0x200a). Questo processo aggiorna la tabella CAM in tutti gli switch del dominio con la nuova topologia.

Consiglio Cisco

Cisco consiglia di abilitare UplinkFast per gli switch di accesso con porte bloccate se si esegue lo Spanning Tree 802.1D. Non utilizzare UplinkFast sugli switch senza la conoscenza della topologia implicita di un root link di backup, in genere switch di distribuzione e core in un design multilayer di Cisco. In generale, non abilitare UplinkFast su uno switch con più di due modalità di uscita dalla rete. Se lo switch si trova in un ambiente ad accesso complesso e si dispone di più blocchi dei collegamenti e inoltro di un collegamento, evitare di utilizzare questa funzione sullo switch o rivolgersi al tecnico dei servizi avanzati.

Utilizzare questo comando globale per abilitare UplinkFast:

```
Switch(config)#spanning-tree uplinkfast
```

Questo comando del software Cisco IOS non regola automaticamente tutti i valori di priorità del bridge su un valore alto. Al contrario, il comando modifica solo le VLAN con una priorità bridge che non è stata modificata manualmente in altri valori. Inoltre, a differenza di CatOS, quando si ripristina uno switch con UplinkFast abilitata, la forma no di questo comando (**no spanning-tree uplinkFast**) ripristina i valori predefiniti di tutti i valori modificati. Pertanto, quando si utilizza questo comando, è *necessario* controllare lo stato corrente delle priorità del bridge prima e dopo per assicurarsi che venga raggiunto il risultato desiderato.

Nota: quando la funzione di filtro dei protocolli è abilitata, è necessaria la parola chiave **all protocols** per il comando UplinkFast. Poiché il CAM registra il tipo di protocollo e le informazioni MAC e VLAN quando il filtro del protocollo è abilitato, è necessario generare un frame UplinkFast per ciascun protocollo su ciascun indirizzo MAC. La parola chiave **rate** indica i pacchetti al secondo dei frame di aggiornamento della topologia UplinkFast. L'impostazione predefinita è consigliata. Non è necessario configurare UplinkFast con RSTP in quanto il meccanismo è incluso in modo nativo e abilitato automaticamente in RSTP.

BackboneFast

Scopo

BackboneFast fornisce una rapida convergenza da errori di collegamento indiretti. BackboneFast riduce i tempi di convergenza dall'impostazione predefinita di 50 secondi a, in genere, 30 secondi e, in questo modo, aggiunge funzionalità a STP. Anche in questo caso, questa funzione è applicabile solo quando si esegue 802.1D. Non configurare la funzione quando si esegue Rapid PVST o MST (che include il componente rapido).

Panoramica operativa

BackboneFast viene avviata quando una porta radice o una porta bloccata su uno switch riceve BPDU inferiori dal bridge designato. La porta riceve in genere pacchetti BPDU inferiori quando uno switch a valle perde la connessione alla radice e inizia a inviare pacchetti BPDU per selezionare una nuova radice. Una BPDU inferiore identifica uno switch come bridge radice e bridge designato.

In base alle normali regole dello spanning tree, lo switch ricevente ignora i BPDU inferiori per il tempo massimo configurato. Per impostazione predefinita, il valore massimo è 20 secondi. Ma, con BackboneFast, lo switch vede la BPDU inferiore come un segnale di un possibile cambiamento nella topologia. Lo switch usa le BPDU Root Link Query (RLQ) per determinare se ha un percorso alternativo al bridge radice. Questa aggiunta di protocollo RLQ consente a uno switch di controllare se la radice è ancora disponibile. RLQ sposta una porta bloccata in una posizione precedente e notifica allo switch isolato che ha inviato il BPDU inferiore che la radice è ancora presente.

Di seguito sono riportati alcuni punti salienti del funzionamento del protocollo:

- Uno switch trasmette il pacchetto RLQ solo dalla porta principale (ossia il pacchetto va verso la porta principale).
- Uno switch che riceve un RLQ può rispondere se è lo switch radice o se lo switch sa di aver perso la connessione con la radice. Se lo switch non è a conoscenza di questi elementi, deve inoltrare la query alla porta radice.
- Se un commutatore ha perso la connessione alla radice, deve rispondere in negativo a questa query.
- La risposta deve essere inviata solo dalla porta da cui proviene la query.
- Il parametro radice deve sempre rispondere alla query con una risposta positiva.
- Se la risposta viene ricevuta su una porta non radice, ignorarla.

L'operazione può ridurre i tempi di convergenza STP fino a 20 secondi perché maxage non deve scadere. per ulteriori informazioni, fare riferimento a Comprensione e configurazione della backbone Fast sugli switch Catalyst.

Consiglio Cisco

Abilitare BackboneFast su tutti gli switch con STP solo se l'intero dominio con spanning-tree può supportare questa funzione. È possibile aggiungere la funzione senza interrompere la rete di produzione.

Utilizzare questo comando globale per abilitare BackboneFast:

```
Switch(config)#spanning-tree backbonefast
```

Nota: è necessario configurare questo comando a livello globale su tutti gli switch di un dominio. Il comando aggiunge a STP le funzionalità che tutti gli switch devono comprendere.

Altre opzioni

BackboneFast non è supportato sugli switch Catalyst 2900XL e 3500XL. In generale, è necessario abilitare BackboneFast se il dominio dello switch contiene questi switch oltre agli switch Catalyst 4500/4000, 5500/5000 e 6500/6000. Quando si implementa BackboneFast in ambienti con switch XL, in topologie rigide è possibile abilitare la funzione in cui lo switch XL è l'ultimo switch in linea ed è connesso al core solo in due punti. Non implementare questa funzione se l'architettura degli switch XL è concatenata a margherita.

Non è necessario configurare BackboneFast con RSTP o 802.1w perché il meccanismo è incluso in modo nativo e abilitato automaticamente in RSTP.

Spanning Tree Loop Guard

Loop Guard è un'ottimizzazione proprietaria di Cisco per STP. La protezione loop protegge le reti di layer 2 dai loop che si verificano a causa di un malfunzionamento dell'interfaccia di rete, di una CPU occupata o di qualsiasi altra cosa che impedisca il normale inoltro delle BPDU. Un loop STP viene creato quando una porta di blocco in una topologia ridondante passa erroneamente allo stato di inoltro. Questo in genere accade perché una delle porte in una topologia fisicamente ridondante (non necessariamente la porta bloccante) non riceve più BPDU.

La protezione loop è utile solo nelle reti commutate in cui gli switch sono connessi tramite collegamenti point-to-point, come è il caso nella maggior parte delle moderne reti di campus e centri dati. L'idea è che, su un collegamento point-to-point, un bridge designato non possa scomparire senza inviare una BPDU inferiore o interrompere il collegamento. La funzione STP loop guard è stata introdotta nel software Cisco IOS versione 12.1(13)E del software Catalyst Cisco IOS per Catalyst 6500 e nel software Cisco IOS versione 12.1(9)EA1 per gli switch Catalyst 4500.

per ulteriori informazioni sul controllo loop, fare riferimento a Miglioramenti del protocollo Spanning-Tree con le funzionalità Loop Guard e BPDU Skew Detection.

Panoramica operativa

Loop Guard controlla se una porta radice o una porta radice alternativa/di backup riceve BPDU. Se la porta non riceve BPDU, la protezione del loop mette la porta in uno stato incoerente (blocco) finché non ricomincia a ricevere BPDU. Una porta in stato incoerente non trasmette pacchetti BPDU. Se una porta di questo tipo riceve nuovamente i BPDU, la porta (e il collegamento) vengono considerati nuovamente validi. La condizione di incoerenza del loop viene rimossa dalla porta e STP determina lo stato della porta. In questo modo, il ripristino è automatico.

La protezione loop isola l'errore e consente allo spanning tree di convergere in una topologia stabile senza il collegamento o il bridge in errore. Protezione loop impedisce i loop STP con la velocità della versione STP in uso. Non vi è alcuna dipendenza da STP (802.1D o 802.1w) o quando si sintonizzano i timer STP. Per questi motivi, Cisco consiglia di implementare la protezione loop insieme al protocollo UDLD nelle topologie che si basano su STP e in cui il software supporta le funzionalità.

Quando il controllo loop blocca una porta incoerente, viene registrato questo messaggio:

```
%SPANTREE-SP-2-LOOPGUARD_BLOCK: Loop guard blocking port GigabitEthernet2/1 on VLAN0010
```

Dopo aver ricevuto la BPDU su una porta in uno stato STP con loop incoerente, la porta passa a un altro stato STP. Secondo la BPDU ricevuta, questo significa che il ripristino è automatico e non è necessario alcun intervento. Dopo il ripristino, viene registrato questo messaggio:

```
%SPANTREE-SP-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port GigabitEthernet2/1 on
VLAN0010
```

Interazione con altre funzioni STP

Protezione radice

La funzione Root Guard forza la designazione di una porta sempre. La protezione in loop è efficace solo se la porta è una porta radice o una porta alternativa, il che significa che le loro

funzioni si escludono a vicenda. Pertanto, non è possibile abilitare contemporaneamente loop guard e root guard su una porta.

UplinkFast

Loop Guard è compatibile con UplinkFast. Se la protezione loop mette una porta radice in uno stato di blocco, UplinkFast mette in stato di inoltro una nuova porta radice. Inoltre, UplinkFast non seleziona una *porta con loop incoerente* come porta radice.

BackboneFast

Loop Guard è compatibile con BackboneFast. BackboneFast viene attivata dalla ricezione di una BPDU inferiore proveniente da un ponte designato. Poiché le BPDU vengono ricevute da questo collegamento, la protezione loop non viene attivata. Pertanto, BackboneFast e loop guard sono compatibili.

PortFast

PortFast esegue il passaggio di una porta allo stato designato per l'inoltro subito dopo il collegamento. Poiché una porta abilitata per PortFast non è una porta radice/alternativa, la protezione loop e PortFast si escludono a vicenda.

PAgP

Loop Guard utilizza le porte conosciute per STP. Pertanto, la protezione loop può sfruttare l'astrazione delle porte logiche fornite da PAgP. Tuttavia, per formare un canale, tutte le porte fisiche raggruppate nel canale devono avere configurazioni compatibili. PAgP applica una configurazione uniforme della protezione loop su tutte le porte fisiche per formare un canale. Quando si configura la protezione loop su EtherChannel, tenere presenti le seguenti avvertenze:

- STP sceglie sempre la prima porta operativa del canale per inviare i BPDU. Se il collegamento diventa unidirezionale, la protezione del loop blocca il canale, anche se altri collegamenti nel canale funzionano correttamente.
- Se un set di porte che sono già bloccate da un controllo loop viene raggruppato per formare un canale, STP perde tutte le informazioni sullo stato per tali porte e la nuova porta del canale può raggiungere lo stato di inoltro con un ruolo designato.
- Se un canale è bloccato da una protezione in loop e il canale si interrompe, STP perde tutte le informazioni sullo stato. Le singole porte fisiche possono raggiungere lo stato di inoltro con un ruolo designato, anche se uno o più collegamenti che hanno formato il canale sono unidirezionali.

In questi ultimi due casi, è possibile che si verifichi un loop finché il protocollo UDLD non rileva il problema. Ma la protezione continua non riesce a rilevarla.

Confronto tra le funzionalità di Loop Guard e UDLD

La funzione Loop Guard e la funzionalità UDLD si sovrappongono parzialmente, in parte nel senso che entrambe proteggono dagli errori STP causati dai collegamenti unidirezionali. Queste due caratteristiche sono diverse nell'approccio al problema e anche nella funzionalità. In particolare, esistono errori unidirezionali specifici che UDLD non è in grado di rilevare, ad esempio errori causati da una CPU che non invia pacchetti BPDU. Inoltre, l'uso di timer STP aggressivi e della modalità RSTP può generare loop prima che il protocollo UDLD possa rilevare gli errori.

Loop Guard non funziona sui collegamenti condivisi o nelle situazioni in cui il collegamento è stato unidirezionale dopo il collegamento. Nel caso di un collegamento che è stato unidirezionale dal collegamento, la porta non riceve mai BPDU e viene designata. Questo può essere un comportamento normale, quindi la protezione loop non copre questo caso particolare. UDLD offre protezione contro uno scenario di questo tipo.

L'abilitazione del protocollo UDLD e della protezione loop offre il livello di protezione più alto. Per ulteriori informazioni sul confronto di caratteristiche tra loop guard e UDLD, consultare:

- Sezione *Loop Guard vs. Unidirectional Link Detection* dei miglioramenti dello Spanning-Tree Protocol che usano le funzionalità Loop Guard e BPDU Skew Detection
- Sezione UDLD di questo documento

Consiglio Cisco

Cisco consiglia di abilitare la protezione loop a livello globale su una rete di switch con loop fisici. È possibile abilitare la protezione loop a livello globale su tutte le porte. La funzione è effettivamente attivata su tutti i collegamenti point-to-point. Il collegamento point-to-point viene rilevato dallo stato duplex del collegamento. Se il duplex è pieno, il collegamento viene considerato point-to-point.

```
Switch(config)#spanning-tree loopguard default
```

Altre opzioni

Per gli switch che non supportano una configurazione global loop guard, si consiglia di abilitare la funzione su tutte le singole porte, incluse le porte del canale della porta. Sebbene non vi siano vantaggi se si abilita la protezione loop su una porta designata, non considerare l'abilitazione un problema. Inoltre, una riconvergenza valida dello Spanning Tree può trasformare una porta designata in una porta radice, rendendo la funzione utile su questa porta.

```
Switch(config)#interface type slot#/port#
Switch(config-if)#spanning-tree guard loop
```

Le reti con topologie prive di loop possono comunque beneficiare della protezione in loop nel caso in cui i loop vengano introdotti accidentalmente. L'abilitazione della protezione loop in questo tipo di topologia può tuttavia causare problemi di isolamento della rete. Se si crea una topologia senza loop e si desidera evitare problemi di isolamento della rete, è possibile disabilitare la protezione loop a livello globale o singolarmente. Non abilitare la protezione del loop sui collegamenti condivisi.

```
Switch(config)#no spanning-tree loopguard default
!--- This is the global configuration.
```

o

```
Switch(config)#interface type slot#/port#
Switch(config-if)#no spanning-tree guard loop
!--- This is the interface configuration.
```

Spanning Tree Root Guard

La funzionalità Root Guard offre un modo per applicare la posizione del root bridge nella rete. Root Guard assicura che la porta su cui root guard è abilitato sia la porta designata. In genere, tutte le porte del root bridge sono porte designate, a meno che due o più porte del root bridge non siano collegate tra loro. Se il bridge riceve pacchetti BPDU STP superiori su una porta abilitata per la protezione radice, sposta questa porta in uno stato STP non coerente per la radice. Lo stato di incoerenza root è l'equivalente dello stato di ascolto. Su questa porta il traffico non viene reindirizzato, così Root Guard applica la posizione del root bridge. Root Guard è disponibile nel primo software Cisco IOS versione 12.1E e successive.

Panoramica operativa

Root Guard è un meccanismo incorporato di STP. Root Guard non dispone di un proprio timer e si basa solo sulla ricezione di BPDU. Quando root guard viene applicato a una porta, questa non può diventare una porta radice. Se la ricezione di una BPDU attiva una convergenza dello Spanning Tree che rende una porta designata una porta radice, la porta viene messa in uno stato di incoerenza a livello di radice. In questo messaggio syslog viene illustrato:

```
%SPANTREE-SP-2-ROOTGUARD_BLOCK: Root guard blocking port GigabitEthernet2/1 on VLAN0010
```

Quando la porta non invia più BPDU superiori, viene nuovamente sbloccata. Tramite STP, la porta passa dallo stato di ascolto allo stato di apprendimento e alla fine allo stato di inoltro. Questo messaggio syslog mostra la transizione:

```
%SPANTREE-SP-2-ROOTGUARD_UNBLOCK: Root guard unblocking port GigabitEthernet2/1
on VLAN0010
```

Il ripristino è automatico. E non è necessario alcun intervento manuale.

Poiché root guard forza la designazione di una porta e loop guard è efficace solo se la porta è una porta radice o una porta alternativa, le funzioni si escludono a vicenda. Pertanto, non è possibile abilitare contemporaneamente la protezione loop e la protezione root su una porta.

per ulteriori informazioni, fare riferimento al miglioramento della root guard dello Spanning Tree Protocol.

Consiglio Cisco

Cisco consiglia di abilitare la funzione root guard sulle porte che si connettono a dispositivi di rete non sottoposti a controllo amministrativo diretto. Per configurare root guard, utilizzare questi comandi quando si è in modalità di configurazione interfaccia:

```
Switch(config)#interface type slot#/port#
Switch(config-if)#spanning-tree guard root
```

EtherChannel

Scopo

EtherChannel comprende un algoritmo di distribuzione dei frame che esegue un multiplexing efficiente dei frame nei collegamenti component 10/100-Mbps o Gigabit. L'algoritmo di distribuzione del frame consente il multiplexing inverso di più canali in un singolo collegamento

logico. Sebbene ogni piattaforma differisca da quella successiva nell'implementazione, è necessario comprendere le seguenti proprietà comuni:

- Deve esistere un algoritmo per il multiplex statistico dei frame su più canali. Negli switch Catalyst, si tratta di una funzionalità correlata all'hardware. Ecco alcuni esempi:Catalyst 5500/5000s: presenza o assenza di un EBC (Ethernet Bundling Chip) sul moduloCatalyst 6500/6000s: algoritmo in grado di leggere ulteriormente nel frame e in modalità multiplex tramite indirizzo IP.
- La creazione di un canale logico consente di eseguire una singola istanza di STP o di utilizzare un singolo peering di routing, a seconda che si tratti di un EtherChannel di layer 2 o 3.
- Esiste un protocollo di gestione per verificare la coerenza dei parametri a entrambe le estremità del collegamento e per facilitare la gestione del recupero del bundling in caso di guasto o aggiunta del collegamento. Questo protocollo può essere PAgP o LACP (Link Aggregation Control Protocol).

Panoramica operativa

EtherChannel comprende un algoritmo di distribuzione dei frame che esegue un multiplexing efficiente dei frame nei collegamenti component da 10/100 Mbps, Gigabit o 10 Gigabit. Le differenze negli algoritmi per piattaforma derivano dalla capacità di ciascun tipo di hardware di estrarre informazioni di frame header per prendere la decisione di distribuzione.

L'algoritmo di distribuzione del carico è un'opzione globale per entrambi i protocolli di controllo del canale. PAgP e LACP utilizzano l'algoritmo di distribuzione del frame perché lo standard IEEE non impone alcun algoritmo di distribuzione particolare. Tuttavia, qualsiasi algoritmo di distribuzione garantisce che, quando si ricevono i frame, l'algoritmo non causi un ordinamento errato dei frame che fanno parte di una determinata conversazione o duplicazione di frame.

Nella tabella seguente viene illustrato in dettaglio l'algoritmo di distribuzione dei frame per ciascuna piattaforma elencata:

Piattaforma	Algoritmo di bilanciamento del carico del canale
Catalyst serie 3750	Catalyst 3750 con algoritmo di bilanciamento del carico del software Cisco IOS che utilizza indirizzi MAC o IP e l'origine o la destinazione del messaggio, o entrambi.
Catalyst serie 4500	Catalyst 4500 con algoritmo di bilanciamento del carico del software Cisco IOS che utilizza indirizzi MAC, indirizzi IP o numeri di porta di livello 4 (L4) e l'origine o la destinazione del messaggio, o entrambi.
Catalyst serie 6500/6000	È possibile usare due algoritmi di hashing, che dipende dall'hardware del Supervisor Engine. L'hash è un polinomio a diciassette gradi che viene implementato nell'hardware. In tutti i casi, l'hash accetta l'indirizzo MAC, l'indirizzo IP o il numero di porta IP TCP/UDP e applica l'algoritmo

	per generare un valore a 3 bit. Questo processo viene eseguito separatamente sia per le associazioni di protezione che per gli agenti di protezione. L'operazione XOR viene quindi utilizzata con i risultati per generare un altro valore a 3 bit. Il valore determina la porta del canale da usare per inoltrare il pacchetto. I canali sullo switch Catalyst 6500/6000 possono essere formati tra le porte di qualsiasi modulo e possono essere fino a otto porte.

Questa tabella indica i metodi di distribuzione supportati sui vari modelli Catalyst 6500/6000 Supervisor Engine. Nella tabella viene inoltre illustrato il comportamento predefinito:

Hardware	Descrizione	Metodi di distribuzione
WS-F6020A (motore Layer 2) WS-F6K-PFC (motore Layer 3)	I Supervisor Engine successivo e IA Supervisor Engine IA/Policy Feature Card 1 (PFC1)	MAC layer 2: SA DA IP layer 3 SA e DA: SA DA SA e DA (impostazione predefinita)
WS-F6K-PFC 2	Supervisor Engine II/PFC2	MAC layer 2: SA DA IP layer 3 SA e DA: SA DA Sessione di livello 4 SA e DA (predefinita): porta S; porto D; Porta S e D
WS-F6K-PFC3A WS-F6K-PFC3B WS-F6K-PFC3BXL	Supervisor Engine 720/PFC3A Supervisor Engine 720/Supervisor Engine 32/PFC3B Supervisor Engine 720/PFC3BXL	MAC layer 2: SA DA IP layer 3 SA e DA: SA DA Sessione di livello 4 SA e DA (predefinita): porta S; porto D; Porta S e D

Nota: nella distribuzione di layer 4, il primo pacchetto frammentato usa la distribuzione di layer 4. Tutti i pacchetti successivi utilizzano la distribuzione di layer 3.

Nota: per ulteriori informazioni sul supporto di EtherChannel su altre piattaforme e su come configurare EtherChannel e risolvere i problemi, consultare i seguenti documenti:

- Informazioni sul bilanciamento del carico EtherChannel e sulla ridondanza negli switch Catalyst
- Configurazione di EtherChannel di layer 3 e layer 2 (Guida alla configurazione del software Cisco IOS Catalyst serie 6500, 12.2SX)
- Configurazione di EtherChannel di layer 3 e layer 2 (Guida alla configurazione del software Cisco IOS Catalyst serie 6500, 12.1E)
- Configurazione di EtherChannel (Guida alla configurazione del software Cisco IOS per gli

switch Catalyst serie 4500, 12.2(31)SG)
- Configurazione di EtherChannel (Guida alla configurazione del software degli switch Catalyst 3750, 12.2(25)SEE)
- Configurazione di EtherChannel tra gli switch Catalyst 4500/4000, 5500/5000 e 6500/6000 con CatOS System Software

Consiglio Cisco

Gli switch Catalyst 3750, Catalyst 4500 e Catalyst serie 6500/6000 eseguono il bilanciamento del carico eseguendo l'hashing degli indirizzi IP di origine e di destinazione per impostazione predefinita. Si consiglia di procedere in questo modo, partendo dal presupposto che IP sia il protocollo dominante. Per impostare il bilanciamento del carico, usare questo comando:

```
port-channel load-balance src-dst-ip
!--- This is the default.
```

Altre opzioni

A seconda dei flussi di traffico, è possibile usare la distribuzione di layer 4 per migliorare il bilanciamento del carico se la maggior parte del traffico è tra lo stesso indirizzo IP di origine e di destinazione. È necessario comprendere che, quando la distribuzione di layer 4 è configurata, l'hashing include solo le porte di origine e destinazione di layer 4. Non combina gli indirizzi IP di layer 3 nell'algoritmo di hash. Per impostare il bilanciamento del carico, usare questo comando:

```
port-channel load-balance src-dst-port
```

Nota: la distribuzione di layer 4 non è configurabile sugli switch Catalyst serie 3750.

Usare il comando **show etherchannel load-balance** per controllare la policy di distribuzione dei frame.

A seconda delle piattaforme hardware, è possibile usare i comandi CLI per determinare l'interfaccia di EtherChannel che inoltra il flusso del traffico specifico, a partire dalla policy di distribuzione dei frame.

Per gli switch Catalyst 6500, usare il comando **remote login switch** per accedere in remoto alla console dello Switch Processor (SP). Quindi, eseguire il **test etherchannel load-balance interface** ***port-channel number*** **{ip | l4porta | mac} [***ip_origine_aggiungi* | *mac_origine* | *source_l4_port***] [***dest_ip_add* | *dest_mac_add* | *dest_l4_port***]**.

Per gli switch Catalyst 3750, eseguire il **test dell'interfaccia di bilanciamento del carico etherchannel** ***numero di canale della porta*** **{ip | mac} [***ip_origine_aggiungi* | *source_mac_add***] [***dest_ip_add* | *dest_mac_add***]**.

Per Catalyst 4500, il comando equivalente non è ancora disponibile.

Linee guida e restrizioni alla configurazione di EtherChannel

EtherChannel verifica le proprietà delle porte su tutte le porte fisiche prima di aggregare le porte compatibili in un'unica porta logica. Le linee guida e le restrizioni alla configurazione variano a seconda della piattaforma dello switch. Completa queste linee guida e restrizioni per evitare

problemi di bundling. Ad esempio, se QoS è abilitato, EtherChannel non viene formato quando si includono i moduli di switching Catalyst serie 6500/6000 con funzionalità QoS diverse. Sugli switch Catalyst 6500 con software Cisco IOS, è possibile disabilitare il controllo degli attributi della porta QoS sul bundling EtherChannel con il comando **no mls qos channel-consistency** port-channel interface. Il comando **show interface capabilities** *mod/porta* consente la visualizzazione delle funzionalità della porta QoS e determina se le porte sono compatibili.

Per evitare problemi di configurazione, fare riferimento a queste linee guida per diverse piattaforme:

- Configurazione di EtherChannel di layer 3 e layer 2 (Guida alla configurazione del software Cisco IOS Catalyst serie 6500, 12.2SX)
- Configurazione di EtherChannel di layer 3 e layer 2 (Guida alla configurazione del software Cisco IOS Catalyst serie 6500, 12.1E)
- Configurazione di EtherChannel (Guida alla configurazione del software Cisco IOS per gli switch Catalyst serie 4500, 12.2(31)SG)
- Configurazione di EtherChannel (Guida alla configurazione del software degli switch Catalyst 3750, 12.2(25)SEE)

Il numero massimo di EtherChannel supportati dipende anche dalla piattaforma hardware e dalle versioni software. Gli switch Catalyst 6500 con software Cisco IOS versione 12.2(18)SXE e successive supportano un massimo di 128 interfacce canale porta. Le versioni software precedenti al software Cisco IOS versione 12.2(18)SXE supportano un massimo di 64 interfacce canale porta. Il numero di gruppo configurabile può essere compreso tra 1 e 256, indipendentemente dalla versione del software. Gli switch Catalyst serie 4500 supportano un massimo di 64 EtherChannel. Per gli switch Catalyst 3750, si consiglia di non configurare più di 48 EtherChannel sullo stack.

Calcolo del costo della porta Spanning Tree

Ènecessario comprendere il calcolo del costo della porta Spanning Tree per EtherChannels. È possibile calcolare il costo della porta Spanning Tree per EtherChannels con il metodo short o long. Per impostazione predefinita, il costo della porta viene calcolato in modalità breve.

Nella tabella viene mostrato il costo della porta Spanning Tree per un EtherChannel di layer 2 in base alla larghezza di banda:

Larghezza di banda	Valore STP precedente	Nuovo valore Long STP
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 Gbps	4	20,000
N X 1 Gbps	3	6660
10 Gbps	2	2,000
100 Gbps	N/D	200
1 Tbps	N/D	20
10 Tbps	N/D	2

Nota: in CatOS, il costo della porta Spanning Tree per EtherChannel rimane invariato dopo l'errore del collegamento del membro del canale della porta. Nel software Cisco IOS, il costo della porta per EtherChannel viene aggiornato immediatamente in modo da riflettere la nuova larghezza di

banda disponibile. Se si desidera evitare di apportare modifiche non necessarie alla topologia dello spanning tree, è possibile configurare in modo statico il costo della porta dello spanning tree con il comando **spanning-tree cost *cost***.

Protocollo PAgP (Port Aggregation Protocol)

Scopo

PAgP è un protocollo di gestione che verifica la coerenza dei parametri a entrambe le estremità del collegamento. PAgP assiste inoltre il canale con l'adattamento per il collegamento guasto o aggiunta. Ecco le caratteristiche della PAgP:

- PaGP richiede che tutte le porte nel canale appartengano alla stessa VLAN o siano configurate come porte trunk. Poiché le VLAN dinamiche possono forzare la modifica di una porta in una VLAN diversa, le VLAN dinamiche non sono incluse nella partecipazione a EtherChannel.
- Quando un bundle esiste già e la configurazione di una porta viene modificata, tutte le porte nel bundle vengono modificate in modo da corrispondere a tale configurazione. Un esempio di modifica di questo tipo è una modifica della VLAN o una modifica della modalità `trunking`.
- PAgP non raggruppa le porte che funzionano a velocità diverse o in modalità duplex. Se la velocità e la modalità duplex vengono modificate quando esiste un pacchetto, la modalità PAgP modifica la velocità della porta e la modalità duplex per tutte le porte del pacchetto.

Panoramica operativa

La porta PAgP controlla ogni singola porta fisica o logica da raggruppare. Per inviare i pacchetti PAgP, viene usato lo stesso indirizzo MAC del gruppo multicast usato per i pacchetti CDP. L'indirizzo MAC è 01-00-0c-cc-cc-cc. Tuttavia, il valore del protocollo è 0x0104. Questo è un riepilogo dell'operazione del protocollo:

- Finché la porta fisica è attiva, i pacchetti PAgP vengono trasmessi ogni secondo durante il rilevamento e ogni 30 secondi in stato stazionario.
- Se si ricevono pacchetti di dati ma non si ricevono pacchetti PAgP, si presume che la porta sia collegata a un dispositivo non compatibile con PAgP.
- Attendere i pacchetti PAgP che dimostrano che la porta fisica ha una connessione bidirezionale a un altro dispositivo compatibile con PAgP.
- Quando si ricevono due pacchetti di questo tipo su un gruppo di porte fisiche, provare a formare una porta aggregata.
- Se i pacchetti PAgP si arrestano per un certo periodo, lo stato `PAgP` viene disattivato.

Elaborazione normale

Questi concetti aiutano a dimostrare il comportamento del protocollo:

- Agport: porta logica composta da tutte le porte fisiche nella stessa aggregazione e che può essere identificata dal relativo ifIndex SNMP. Un agport non contiene porte non operative.
- Canale - Un'aggregazione che soddisfa i criteri di formazione. Un canale può contenere porte non operative ed è un superset di agport. I protocolli, che includono STP e VTP ma escludono CDP e DTP, vengono eseguiti sopra il protocollo PAgP sulle porte dell'agente. Nessuno di questi protocolli può inviare o ricevere pacchetti finché PAgP non collega le porte a una o più porte fisiche.

- Capacità gruppo - Ogni porta fisica e agport possiede un parametro di configurazione denominato `capacità gruppo`. Una porta fisica può essere aggregata a qualsiasi altra porta fisica che abbia la stessa `funzionalità di gruppo` e solo a tale porta fisica.
- Procedura di aggregazione: quando una porta fisica raggiunge lo stato `UpData` o `UpPAgP`, la porta viene collegata a un agport appropriato. Quando la porta lascia uno di questi stati per un altro stato, viene scollegata dall'agport.

Questa tabella fornisce ulteriori dettagli sugli stati:

State	Significato
`SuDati`	Nessun pacchetto PAgP ricevuto. I pacchetti PAgP vengono inviati. La porta fisica è l'unica porta collegata all'agport. I pacchetti non PAgP vengono trasmessi in entrata e in uscita tra la porta fisica e agport.
`Bidirezionale`	È stato ricevuto esattamente un pacchetto PAgP che dimostra l'esistenza di una connessione bidirezionale a un solo router adiacente. La porta fisica non è connessa ad alcuna porta porta secondaria. I pacchetti PAgP vengono inviati e possono essere ricevuti.
`UpPAgP`	Questa porta fisica, probabilmente in associazione con altre porte fisiche, è connessa a una porta di accesso. I pacchetti PAgP vengono inviati e ricevuti sulla porta fisica. I pacchetti non PAgP vengono trasmessi in entrata e in uscita tra la porta fisica e agport.

Entrambe le estremità di entrambe le connessioni devono concordare sul raggruppamento. Il raggruppamento è definito come il gruppo di porte più grande nell'agport consentito da entrambe le estremità della connessione.

Quando una porta fisica raggiunge lo stato `UpPAgP`, viene assegnata all'agport che dispone di porte fisiche membro corrispondenti alla `capacità di gruppo` della nuova porta fisica e che si trovano nello stato `BiDir` o `UpPAgP`. Tutte le porte `BiDir` di questo tipo vengono spostate contemporaneamente nello stato `UpPAgP`. Se non esiste un agport con parametri di porta fisica che siano compatibili con la porta fisica appena pronta, la porta viene assegnata a un agport con parametri appropriati a cui non sono associate porte fisiche.

Èpossibile che si verifichi un timeout PAgP sull'ultimo router adiacente noto sulla porta fisica. La porta in timeout viene rimossa da agport. Allo stesso tempo, vengono rimosse tutte le porte fisiche sulla stessa porta di aggregazione che hanno timer scaduti. In questo modo, un agport la cui altra estremità è morta viene eliminato in una sola volta, anziché una porta fisica alla volta.

Comportamento in caso di errore

Se si verifica un errore in un collegamento di un canale esistente, l'agport viene aggiornato e viene eseguito l'hashing del traffico sui collegamenti che rimangono senza perdita di dati. Esempi di errori includono:

- Porta scollegata
- Gigabit Interface Converter (GBIC) viene rimosso

- Fibra rotta

Nota: quando si interrompe un collegamento in un canale con un modulo spento o rimosso, il comportamento può essere diverso. Per definizione, un canale richiede due porte fisiche. Se una porta viene persa dal sistema in un canale a due porte, la porta logica viene eliminata e la porta fisica originale viene reinizializzata rispetto allo spanning tree. Il traffico può essere scartato finché l'STP non consente alla porta di essere di nuovo disponibile per i dati.

Questa differenza nelle due modalità di errore è importante quando si pianifica la manutenzione di una rete. È possibile che si verifichi una modifica della topologia STP di cui è necessario tenere conto quando si esegue una rimozione o un inserimento online di un modulo. È necessario gestire ogni collegamento fisico nel canale con il sistema di gestione della rete (NMS, Network Management System) perché l'agport può rimanere indisturbato in caso di guasto.

Completare uno dei seguenti suggerimenti per ridurre le modifiche indesiderate alla topologia sugli switch Catalyst 6500/6000:

- Se per formare un canale si utilizza una singola porta per modulo, utilizzare tre o più moduli (tre in totale).
- Se il canale si estende su due moduli, utilizzare due porte su ciascun modulo (quattro in totale).
- Se è necessario un canale a due porte su due schede, utilizzare solo le porte del Supervisor Engine.

Opzioni di configurazione

Èpossibile configurare EtherChannel in modalità diverse, come illustrato nella tabella seguente:

Modalità	Opzioni configurabili
`On`	PAgP non è in funzione. I canali della porta, indipendentemente dalla configurazione della porta adiacente. Se la modalità porta adiacente è `attivata`, viene formato un canale.
`Auto`	L'aggregazione è sotto il controllo dell'APgP. Una porta viene messa in uno stato di negoziazione passivo. Sull'interfaccia non vengono inviati pacchetti PAgP finché non viene ricevuto almeno un pacchetto PAgP che indica che il mittente funziona in modalità `desiderabile`.
`Desirable`	L'aggregazione è sotto il controllo dell'APgP. Un porto si trova in uno stato di negoziazione attivo, in cui il porto avvia le negoziazioni con altre porte tramite la trasmissione di pacchetti PAgP. Un canale viene formato con un altro gruppo di porte in modalità `desiderabile` o `automatica`.
`Non silenzioso` Questa è l'impost	Parola chiave `auto` o mode `desiderabile`. Se l'interfaccia non riceve pacchetti di dati, non viene mai collegata a un agport e non può essere utilizzata per i dati. Questo controllo della bidirezionalità è stato eseguito su hardware Catalyst 5500/5000 specifico perché

azione predefinita sulle porte Catalyst 5500/5000 Fiber FE e GE.	alcuni errori di collegamento provocano una divisione del canale. Quando si abilita la modalità `non invisibile all'utente`, non è mai consentito che una porta adiacente in fase di ripristino torni su e divida il canale inutilmente. I pacchetti più flessibili e i controlli di bidirezionalità migliorati sono presenti per impostazione predefinita nell'hardware Catalyst serie 4500/4000 e 6500/6000.
`Silenzioso` Questa è l'impostazione predefinita su tutte le porte Catalyst 6500/6000 e 4500/4000 e sulle porte 5500/5000 in rame.	Parola chiave `auto` o mode `desiderabile`. Se l'interfaccia non riceve pacchetti di dati, dopo un periodo di timeout di 15 secondi, l'interfaccia viene collegata da sola a un agport. Pertanto, l'interfaccia può essere utilizzata per la trasmissione dei dati. `La` modalità `silenziosa` consente anche il funzionamento del canale quando il partner può essere un analizzatore o un server che non invia mai PAgP.

Le impostazioni `per le connessioni invisibili all'utente/non invisibili all'utente` influiscono sul modo in cui le porte reagiscono alle situazioni che causano il traffico unidirezionale. Quando una porta non è in grado di trasmettere a causa di un errore dell'interfaccia fisica o di un cavo o fibra rotto, la porta adiacente può essere lasciata in stato operativo. Il partner continua a trasmettere i dati. Tuttavia, i dati vengono persi perché non è possibile ricevere il traffico di ritorno. Anche i loop Spanning-Tree possono formarsi a causa della natura unidirezionale del collegamento.

Alcune porte in fibra hanno la funzionalità desiderata per portare la porta in uno stato non operativo quando la porta perde il segnale di ricezione (FEFI). In questo modo, la porta del partner non è più operativa e le porte su entrambe le estremità del collegamento diventano inattive.

Quando si utilizzano dispositivi che trasmettono dati (BPDU) e non è possibile rilevare condizioni unidirezionali, utilizzare la modalità `non silenziosa` per fare in modo che le porte rimangano non operative finché non vengono ricevuti i dati e non viene verificato che il collegamento è bidirezionale. Il tempo necessario alla funzione PAgP per rilevare un collegamento unidirezionale è di circa 3,5 * 30 secondi = 105 secondi. Trenta secondi è l'intervallo di tempo tra due messaggi PAgP successivi. Usare il protocollo UDLD, che permette di rilevare più rapidamente i collegamenti unidirezionali.

Se si utilizzano dispositivi che non trasmettono alcun dato, utilizzare la modalità `in background`. L'uso della modalità `silenziosa` forza la porta a connettersi e a diventare operativa, indipendentemente dal fatto che i dati ricevuti siano presenti o meno. Inoltre, per le porte che possono rilevare la presenza di una condizione unidirezionale, viene utilizzata per impostazione

predefinita la modalità `silenziosa`. Esempi di queste porte sono le piattaforme più recenti che usano il layer 1 FEFI e UDLD.

Per disattivare il channeling su un'interfaccia, usare il comando **no channel-group** *number*:

```
Switch(config)#interface type slot#/port#
Switch(config-if)#no channel-group 1
```

Verifica

La tabella riportata in questa sezione fornisce un riepilogo di tutti i possibili scenari di modalità di channeling PAgP tra due switch connessi direttamente, lo switch A e lo switch B. In alcune di queste combinazioni, il protocollo STP può impostare le porte del lato del channeling sullo stato `errDisable`, ossia le porte del lato del channeling possono essere chiuse. La funzione di protezione dalla configurazione errata di EtherChannel è abilitata per impostazione predefinita.

Cambia modalità canale A	Modalità canale switch B	Cambia Stato Del Canale	Stato canale switch B
On	On	Canale (non PAgP)	Canale (non PAgP)
On	Non configurato	Non canale (errDisable)	Non canale
On	Auto	Non canale (errDisable)	Non canale
On	Desirable	Non canale (errDisable)	Non canale
Non configurato	On	Non canale	Non canale (errDisable)
Non configurato	Non configurato	Non canale	Non canale
Non configurato	Auto	Non canale	Non canale
Non configurato	Desirable	Non canale	Non canale
Auto	On	Non canale	Non canale (errDisable)
Auto	Non configurato	Non canale	Non canale
Auto	Auto	Non canale	Non canale
Auto	Desirable	Canale PAgP	Canale PAgP
Desirable	On	Non canale	Non canale
Desirable	Non configurato	Non canale	Non canale
Desirable	Auto	Canale PAgP	Canale PAgP
Desirable	Desirable	Canale PAgP	Canale PAgP

Consiglio di configurazione Cisco per canali L2

Abilitare PAgP e utilizzare un'impostazione `desiderabile-desiderabile` su tutti i collegamenti EtherChannel. Per ulteriori informazioni, vedere questo output:

```
Switch(config)#interface type slot#/port#
Switch(config-if)#no ip address
!--- This ensures that there is no IP !--- address that is assigned to the LAN port.
Switch(config-if)#channel-group number mode desirable
!--- Specify the channel number and the PAgP mode.
```

Verificare la configurazione nel modo seguente:

```
Switch#show run interface port-channel number
Switch#show running-config interface type slot#/port#
Switch#show interfaces type slot#/port# etherchannel
Switch#show etherchannel number port-channel
```

Prevenzione di errori di configurazione di EtherChannel

Èpossibile configurare in modo errato un EtherChannel e creare un loop nello spanning-tree. Questa configurazione errata può ostacolare il processo dello switch. Per prevenire il problema, il software di sistema Cisco IOS include la funzione di **configurazione errata** di **spanning-tree etherchannel guard**.

Eseguire questo comando di configurazione su tutti gli switch Catalyst con software Cisco IOS come software di sistema:

```
Switch(config)#spanning-tree etherchannel guard misconfig
```

Altre opzioni

Quando si collegano due dispositivi che non supportano PAgP ma supportano LACP, si consiglia di abilitare LACP con la configurazione di LACP attivo su entrambe le estremità dei dispositivi. Per ulteriori informazioni, vedere la sezione LACP (Link Aggregation Control Protocol) di questo documento.

Quando si effettua il channeling su dispositivi che non supportano PAgP o LACP, è necessario programmare il canale `su ON`. Questo requisito si applica a questi dispositivi di esempio:

- Server
- Direttore locale
- Switch Content
- Router
- Switch con software precedente
- Switch Catalyst 2900XL/3500XL
- Catalyst 8540s

Utilizzare i seguenti comandi:

```
Switch(config)#interface type slot#/port#
```

```
Switch(config-if)#channel-group number mode on
```

Protocollo LACP (Link Aggregation Control Protocol)

Il protocollo LACP è un protocollo che consente alle porte con caratteristiche simili di formare un canale tramite negoziazione dinamica con switch adiacenti. PAgP è un protocollo proprietario di Cisco che può essere eseguito solo sugli switch Cisco e sugli switch con licenza dei fornitori. Tuttavia, il protocollo LACP, definito in IEEE 802.3ad, consente agli switch Cisco di gestire il channeling Ethernet con dispositivi conformi alla specifica 802.3ad.

LACP è supportato con le seguenti piattaforme e versioni:

- Catalyst serie 6500/6000 con software Cisco IOS versione 12.1(11b)EX e successive
- Catalyst serie 4500 con software Cisco IOS versione 12.1(13)EW e successive
- Catalyst serie 3750 con software Cisco IOS versione 12.1(14)EA1 e successive

La differenza tra LACP e PAgP da un punto di vista funzionale è minima. Entrambi i protocolli supportano un massimo di otto porte in ogni canale e le stesse proprietà delle porte vengono controllate prima di formare il bundle. Queste proprietà delle porte includono:

- Speed
- Duplex
- VLAN nativa e tipo di trunking

Le differenze notevoli tra LACP e PAgP sono:

- Il protocollo LACP può essere eseguito solo su porte full-duplex e non supporta porte half-duplex.
- Il protocollo LACP supporta porte in standby a caldo. LACP tenta sempre di configurare il numero massimo di porte compatibili in un canale, fino al numero massimo consentito dall'hardware (otto porte). Se il protocollo LACP non è in grado di aggregare tutte le porte compatibili (ad esempio, se il sistema remoto ha limitazioni hardware più restrittive), tutte le porte che non possono essere incluse attivamente nel canale vengono messe in stato di hot standby e utilizzate solo se una delle porte utilizzate ha esito negativo.

Nota: per gli switch Catalyst serie 4500, il numero massimo di porte a cui è possibile assegnare la stessa chiave amministrativa è otto. Per gli switch Catalyst 6500 e 3750 con software Cisco IOS, LACP cerca di configurare il numero massimo di porte compatibili in un EtherChannel, fino al numero massimo consentito dall'hardware (otto porte). È possibile configurare otto porte aggiuntive come porte di standby a caldo.

Panoramica operativa

Il protocollo LACP controlla ogni singola porta fisica (o logica) da includere nel pacchetto. I pacchetti LACP vengono inviati con l'indirizzo MAC del gruppo multicast **01-80-c2-00-00-02**. Il valore del tipo/campo è 0x8809 con un sottotipo di 0x01. Di seguito viene riportato un riepilogo dell'operazione del protocollo:

- Il protocollo si basa sui dispositivi per annunciare le loro funzionalità di aggregazione e le informazioni sullo stato. Le trasmissioni sono inviate periodicamente su ciascun collegamento aggregabile.
- Finché la porta fisica è attiva, i pacchetti LACP vengono trasmessi ogni secondo durante il rilevamento e ogni 30 secondi in stato stazionario.

- I partner su un collegamento aggregabile ascoltano le informazioni inviate all'interno del protocollo e decidono quale azione o azioni intraprendere.
- Le porte compatibili sono configurate in un canale, fino al massimo consentito dall'hardware (otto porte).
- Le aggregazioni sono mantenute grazie allo scambio regolare e tempestivo di informazioni aggiornate sullo stato tra i partner di collegamento. Se la configurazione cambia (ad esempio a causa di un errore di collegamento), i partner del protocollo scadono ed eseguono l'azione appropriata in base al nuovo stato del sistema.
- Oltre alle trasmissioni periodiche LACP data unit (LACPDU), in caso di modifica delle informazioni sullo stato, il protocollo trasmette ai partner una LACPDU basata su eventi. I partner del protocollo intraprendono le azioni appropriate in base al nuovo stato del sistema.

Parametri LACP

Per consentire alla LACP di determinare se un insieme di collegamenti si connettono allo stesso sistema e se tali collegamenti sono compatibili dal punto di vista dell'aggregazione, è necessario essere in grado di stabilire:

- Identificatore univoco globale per ogni sistema che partecipa all'aggregazione dei collegamenti.A ogni sistema con LACP deve essere assegnata una priorità che può essere scelta automaticamente (con la priorità predefinita di 32768) o dall'amministratore. La priorità di sistema viene utilizzata principalmente in combinazione con l'indirizzo MAC del sistema per formare l'identificativo del sistema.
- Un mezzo per identificare l'insieme di funzionalità associate a ciascuna porta e a ciascun aggregatore, come compreso da un determinato sistema.A ciascuna porta del sistema deve essere assegnata automaticamente una priorità (con la priorità predefinita di 128) o dall'amministratore. La priorità viene utilizzata insieme al numero di porta per formare l'identificatore della porta.
- Un mezzo per identificare un gruppo di aggregazione link e il relativo aggregatore associato.La capacità di una porta di aggregarsi a un'altra porta è riepilogata da un semplice parametro intero a 16 bit rigorosamente maggiore di zero, denominato chiave. Ciascun codice è determinato sulla base di diversi fattori, quali:Le caratteristiche fisiche della porta, tra cui velocità dei dati, duplessità e supporto point-to-point o condivisoVincoli di configurazione stabiliti dall'amministratore di reteA ciascuna porta sono associate due chiavi:Chiave amministrativaUna chiave operativaLa chiave di amministrazione consente la manipolazione dei valori della chiave da parte della gestione e pertanto l'utente può scegliere questa chiave. La chiave operativa viene utilizzata dal sistema per formare le aggregazioni. L'utente non può scegliere o modificare direttamente questa chiave. Il set di porte in un determinato sistema che condividono lo stesso valore di chiave operativa è considerato membro dello stesso gruppo di chiavi.

Pertanto, dati due sistemi e un set di porte con la stessa chiave amministrativa, ogni sistema tenta di aggregare le porte, a partire dalla porta con la priorità più alta nel sistema con la priorità più alta. Questo comportamento è possibile perché ogni sistema conosce le seguenti priorità:

- La propria priorità, assegnata all'utente o al software
- Priorità del partner, individuata tramite pacchetti LACP

Comportamento in caso di errore

Il comportamento di errore per LACP è lo stesso di quello per PAgP. Se un collegamento in un canale esistente ha esito negativo (ad esempio, se una porta è scollegata, se un GBIC è rimosso

o se una fibra è interrotta), l'agport viene aggiornato e il traffico sui collegamenti rimanenti viene incapsulato entro 1 secondo. Tutto il traffico che non deve essere ripristinato dopo il guasto (ossia il traffico che continua a essere inviato sullo stesso collegamento) non subisce alcuna perdita. Il ripristino del collegamento non riuscito attiva un altro aggiornamento dell'agport e l'hashing del traffico viene eseguito di nuovo.

Opzioni di configurazione

Èpossibile configurare EtherChannel LACP in modalità diverse, come illustrato nella tabella seguente:

Modalità	Opzioni configurabili
On	L'aggregazione dei collegamenti deve essere formata senza alcuna negoziazione LACP. Lo switch non invia il pacchetto LACP né elabora alcun pacchetto LACP in arrivo. Se la modalità porta adiacente è attiva, viene formato un canale.
Off (o non configurato)	La porta non sta effettuando il channeling, a prescindere dalla configurazione della porta adiacente.
Passivo (predefinito)	È simile alla modalità **automatica** in PAgP. Lo switch non avvia il canale, ma riconosce i pacchetti LACP in arrivo. Il peer (in stato attivo) avvia la negoziazione (inviando un pacchetto LACP) che lo switch riceve e a cui lo switch risponde, formando eventualmente il canale di aggregazione con il peer.
Attive	Questa è simile alla modalità **desiderata** in PAgP. Lo switch avvia la negoziazione per formare un collegamento di aggregazione. L'aggregazione dei collegamenti viene creata se l'altra estremità viene eseguita in modalità attiva o passiva LACP.

LACP utilizza un timer a intervalli di 30 secondi (Slow_Periodic_Time) dopo che sono stati stabiliti i canali EtherLACP. Il numero di secondi prima dell'annullamento della convalida delle informazioni LACPDU ricevute quando si utilizzano timeout lunghi (3 volte il valore di Slow_Periodic_Time) è 90. Si consiglia UDLD come rilevatore più rapido di collegamenti unidirezionali. Non è possibile regolare i timer LACP e a questo punto non è possibile configurare gli switch in modo che utilizzino la trasmissione PDU (Fast Protocol Data Unit) (ogni secondo) per mantenere il canale dopo che è stato formato.

Verifica

La tabella riportata in questa sezione fornisce un riepilogo di tutti i possibili scenari di modalità di channeling LACP tra due switch connessi direttamente (switch A e switch B). In alcune di queste combinazioni, EtherChannel Guard può mettere le porte sul lato del canale in stato err-disabled. La funzione di protezione dalla configurazione errata di EtherChannel è abilitata per impostazione predefinita.

Cambia modalità canale A	Modalità canale switch B	Cambia Stato Del Canale	Stato canale switch B
On	On	Canale (non LACP)	Canale (non LACP)
On	Spento	Non canale (errDisable)	Non canale
On	Passivo	Non canale (errDisable)	Non canale
On	Active	Non canale (errDisable)	Non canale
Spento	Spento	Non canale	Non canale
Spento	Passivo	Non canale	Non canale
Spento	Active	Non canale	Non canale
Passivo	Passivo	Non canale	Non canale
Passivo	Active	Canale LACP	Canale LACP
Active	Active	Canale LACP	Canale LACP

Consigli di Cisco

Cisco consiglia di abilitare il protocollo PAgP sulle connessioni di canale tra gli switch Cisco. Quando si collegano due dispositivi che non supportano PAgP ma supportano LACP, si consiglia di abilitare LACP con la configurazione di LACP attivo su entrambe le estremità dei dispositivi.

Sugli switch con CatOS, tutte le porte di uno switch Catalyst 4500/4000 e di uno switch Catalyst 6500/6000 usano il protocollo di canale PAgP per impostazione predefinita. Per configurare le porte in modo da utilizzare LACP, è necessario impostare il protocollo di canale sui moduli su LACP. Non è possibile eseguire LACP e PAgP sullo stesso modulo sugli switch con CatOS. questa limitazione non si applica agli switch con software Cisco IOS. Gli switch con software Cisco IOS possono supportare PAgP e LACP sullo stesso modulo. Per impostare la modalità del canale LACP su attiva e assegnare un numero di chiave amministrativa, eseguire questi comandi:

```
Switch(config)#interface range type slot#/port#
Switch(config-if)#channel-group admin_key mode active
```

Il comando **show etherchannel summary** visualizza un riepilogo di una riga per gruppo di canali che include le seguenti informazioni:

- Raggruppa numeri
- Numeri dei canali porte
- Stato delle porte
- Le porte che fanno parte del canale

Il comando **show etherchannel port-channel** visualizza informazioni dettagliate sul canale della porta per tutti i gruppi di canali. L'output include le seguenti informazioni:

- Stato del canale
- Protocollo utilizzato
- Periodo di tempo trascorso dall'aggregazione delle porte

Per visualizzare informazioni dettagliate su un gruppo di canali specifico, visualizzando separatamente i dettagli di ciascuna porta, usare il **comando show etherchannel** ***numero_canale*** **detail**. L'output del comando include i dettagli del partner e del canale della porta. per ulteriori informazioni, fare riferimento a Configurazione del protocollo LACP (802.3ad) tra uno switch Catalyst 6500/6000 e uno switch Catalyst 4500/4000.

Altre opzioni

Se i dispositivi del canale non supportano PAgP o LACP, è necessario impostare il codice hardware del canale `su on`. Questo requisito si applica a questi dispositivi:

- Server
- Direttore locale
- Switch Content
- Router
- Switch con software precedente
- Switch Catalyst 2900XL/3500XL
- Catalyst 8540s

Utilizzare i seguenti comandi:

```
Switch(config)#interface range type slot#/port#
Switch(config-if)#channel-group admin_key mode on
```

Rilevamento collegamenti unidirezionali

Scopo

UDLD è un protocollo leggero e proprietario di Cisco sviluppato per rilevare le istanze di comunicazioni unidirezionali tra i dispositivi. Esistono altri metodi per rilevare lo stato bidirezionale dei supporti di trasmissione, ad esempio FEFI. In alcuni casi, tuttavia, i meccanismi di rilevamento del layer 1 non sono sufficienti. Questi scenari possono determinare:

- Il funzionamento imprevedibile di STP
- L'inondazione errata o eccessiva dei pacchetti
- Il buco nero del traffico

La funzione UDLD soddisfa le seguenti condizioni di errore sulle interfacce Ethernet in fibra e in rame:

- Monitoraggio delle configurazioni di cablaggio fisico: le porte cablate in modo non corretto `vengono` chiuse.
- Protezione dai collegamenti unidirezionali: quando viene rilevato un collegamento unidirezionale a causa di un malfunzionamento del supporto o della porta/interfaccia, la porta interessata viene chiusa come `errDisabled`. Viene generato un messaggio syslog corrispondente.
- Inoltre, la modalità aggressiva UDLD controlla che un collegamento bidirezionale

precedentemente considerato non perda la connettività nel caso in cui diventi inutilizzabile a causa di una congestione. La modalità aggressiva UDLD esegue test di connettività continui sul collegamento. Lo scopo principale della modalità aggressiva UDLD è quello di evitare il black holing del traffico in alcune condizioni di errore non gestite dal protocollo UDLD in modalità normale.

Per ulteriori informazioni, fare riferimento a Descrizione e configurazione della funzionalità UDLD (Unidirectional Link Detection Protocol).

Lo Spanning Tree ha un flusso BPDU unidirezionale in stato stazionario e può avere gli errori elencati in questa sezione. Una porta può improvvisamente non essere in grado di trasmettere i BPDU. In questo caso, lo stato di STP passa dal `blocco` all'`inoltro` sul router adiacente. Tuttavia, il loop esiste ancora perché la porta è ancora in grado di ricevere.

Panoramica operativa

UDLD è un protocollo di layer 2 che funziona al di sopra del layer LLC (destinazione MAC 01-00-0c-cc-cc-cc, tipo di protocollo SNAP HDLC 0x0111). Quando si esegue UDLD in combinazione con i meccanismi FEFI e di negoziazione automatica di livello 1, è possibile convalidare l'integrità fisica (L1) e logica (L2) di un collegamento.

UDLD dispone di disposizioni per le funzionalità e la protezione che FEFI e la funzione di negoziazione automatica non sono in grado di eseguire. Queste caratteristiche includono:

- Rilevamento e cache delle informazioni sui router adiacenti
- La disattivazione di tutte le porte non connesse
- Rilevamento di malfunzionamenti di porte/interfacce logiche o di errori su collegamenti non point-to-pointNota: quando i collegamenti non sono point-to-point, attraversano i convertitori di supporti o gli hub.

il protocollo UDLD utilizza questi due meccanismi di base.

1. UDLD viene a conoscenza dei router adiacenti e mantiene le informazioni aggiornate in una cache locale.
2. il protocollo UDLD invia una serie di messaggi echo/probe UDLD al rilevamento di un nuovo router adiacente o quando un router adiacente richiede una risincronizzazione della cache.

UDLD invia costantemente messaggi probe/echo su tutte le porte. Alla ricezione di un messaggio UDLD corrispondente su una porta, viene attivata una fase di rilevamento e un processo di convalida. La porta è abilitata se sono soddisfatte tutte le condizioni valide. Le condizioni sono soddisfatte se la porta è bidirezionale e collegata correttamente. Se le condizioni non sono soddisfatte, la porta è `errDisabled`, il che attiva questo messaggio syslog:

```
UDLD-3-AGGRDISABLE: Neighbor(s) of port disappeared on bidirectional link.
   Port disabled
UDLD-3-AGGRDISABLEFAIL: Neighbor(s) of port disappeared on bidirectional link.
   Failed to disable port
UDLD-3-DISABLE: Unidirectional link detected on port disabled.
UDLD-3-DISABLEFAIL: Unidirectional link detected on port, failed to disable port.
UDLD-3-SENDFAIL: Transmit failure on port.
UDLD-4-ONEWAYPATH: A unidirectional link from port to port of device [chars]
   was detected.
```

Per un elenco completo dei messaggi di sistema per struttura, inclusi gli eventi UDLD, fare riferimento ai messaggi UDLD (Cisco IOS System Messages, volume 2 di 2).

Dopo aver stabilito un collegamento e averlo classificato come bidirezionale, UDLD continua a pubblicizzare i messaggi echo/probe a un intervallo predefinito di 15 secondi.

Questa tabella fornisce informazioni sugli stati delle porte:

Stato porta	Commento
Indeterminato	Rilevamento in corso/UDLD adiacente disabilitato.
Non applicabile	UDLD disabilitato.
Shutdown	È stato rilevato un collegamento unidirezionale e la porta è stata disabilitata.
Bidirezionale	È stato rilevato un collegamento bidirezionale.

Gestione cache router adiacenti

UDLD invia periodicamente pacchetti hello probe/echo su ciascuna interfaccia attiva per mantenere l'integrità della cache dei nodi adiacenti UDLD. Alla ricezione di un messaggio hello, il messaggio viene memorizzato nella cache e mantenuto in memoria per un periodo massimo, definito come tempo di attesa. Alla scadenza del tempo di attesa, la voce della cache corrispondente viene esaurita. Se si riceve un nuovo messaggio di saluto entro il periodo di tempo di attesa, il nuovo messaggio sostituisce quello precedente e il timer di durata corrispondente viene reimpostato.

Ogni volta che un'interfaccia abilitata per il protocollo UDLD viene disabilitata o che un dispositivo viene reimpostato, tutte le voci della cache esistenti per le interfacce interessate dalla modifica alla configurazione vengono cancellate. Questa distanza mantiene l'integrità della cache UDLD. UDLD trasmette almeno un messaggio per informare i rispettivi vicini della necessità di svuotare le voci della cache corrispondenti.

Meccanismo di rilevamento dell'eco

Il meccanismo di eco costituisce la base dell'algoritmo di rilevamento. Ogni volta che un dispositivo UDLD viene a conoscenza di un nuovo router adiacente o riceve una richiesta di risincronizzazione da un router adiacente non sincronizzato, riavvia la finestra di rilevamento dal lato della connessione e invia una sequenza di messaggi echo in risposta. Poiché questo comportamento deve essere lo stesso per tutti i router adiacenti, il mittente dell'eco si aspetta di ricevere gli echi in risposta. Se la finestra di rilevamento termina senza ricevere alcun messaggio di risposta valido, il collegamento viene considerato unidirezionale. A partire da questo punto, è possibile avviare un processo di ripristino del collegamento o di arresto della porta. Altre, rare condizioni anomale per le quali il dispositivo verifica:

- Fibre Tx (Looped-back Transmit) al connettore Rx della stessa porta
- Errori di scrittura in caso di interconnessione di supporti condivisi (ad esempio, un hub o un dispositivo simile)

Tempo di convergenza

Per impedire la formazione di loop STP, il software Cisco IOS versione 12.1 e successive ha

ridotto l'intervallo dei messaggi predefinito UDLD da 60 secondi a 15 secondi. Questo intervallo è stato modificato in modo da arrestare un collegamento unidirezionale prima che una porta precedentemente bloccata nello Spanning Tree 802.1D possa passare a uno stato di inoltro. Il valore dell'intervallo tra i messaggi determina la frequenza con cui un router adiacente invia le richieste UDLD dopo la fase di collegamento o rilevamento. Non è necessario che l'intervallo tra i messaggi corrisponda su entrambe le estremità di un collegamento, anche se è preferibile una configurazione coerente quando possibile. Quando si stabiliscono i router adiacenti UDLD, l'intervallo dei messaggi configurato viene inviato al router adiacente e l'intervallo di timeout per il peer viene calcolato nel modo seguente:

```
3 * (message interval)
```

Di conseguenza, una relazione tra pari si interrompe dopo che tre hellos consecutivi (o sonde) sono mancanti. Poiché gli intervalli dei messaggi sono diversi su ciascun lato, questo valore di timeout è semplicemente diverso su ciascun lato e un lato riconosce un errore più rapidamente.

Il tempo approssimativo necessario per rilevare un errore unidirezionale di un collegamento precedentemente stabile è circa:

```
2.5 * (message interval) + 4 seconds
```

Questo valore è di circa 41 secondi con l'intervallo predefinito dei messaggi di 15 secondi. Questo periodo di tempo è molto più breve rispetto ai 50 secondi solitamente necessari per la riconversione di STP. Se la CPU NMP dispone di alcuni cicli di riserva e l'utente ne controlla attentamente il livello di utilizzo (una buona pratica), è accettabile una riduzione dell'intervallo dei messaggi (pari) al minimo di 7 secondi. Inoltre, la riduzione dell'intervallo tra i messaggi consente di velocizzare il rilevamento in base a un fattore significativo.

Nota: nel software Cisco IOS versione 12.2(25)SEC, il minimo è 1 secondo.

Di conseguenza, il protocollo UDLD dipende dai timer Spanning Tree predefiniti. Se la sintonizzazione di STP consente una convergenza più rapida rispetto a UDLD, prendere in considerazione un meccanismo alternativo, ad esempio la funzione di protezione del loop STP. In questo caso, prendere in considerazione un meccanismo alternativo anche quando si implementa RSTP (802.1w), in quanto RSTP ha caratteristiche di convergenza in ms, a seconda della topologia. In questi casi, per ottenere la massima protezione, usare la funzione di protezione in loop insieme al protocollo UDLD. Protezione loop impedisce i loop STP con la velocità della versione STP in uso. Inoltre, il protocollo UDLD si occupa del rilevamento delle connessioni unidirezionali sui singoli collegamenti EtherChannel o nei casi in cui i BPDU non fluiscono lungo la direzione interrotta.

Nota: il protocollo UDLD è indipendente dal protocollo STP. UDLD non rileva tutte le situazioni di errore STP, ad esempio gli errori causati da una CPU che non invia pacchetti BPDU per un periodo di tempo superiore a (2 * Fwddelay + maxage). Per questo motivo, Cisco consiglia di implementare il protocollo UDLD insieme alla protezione loop nelle topologie che si basano sul protocollo STP.

Attenzione: prestare attenzione alle versioni precedenti del protocollo UDLD sugli switch 2900XL/3500XL che usano un intervallo di messaggi predefinito non configurabile pari a 60 secondi. Sono suscettibili alle condizioni dello spanning-tree loop.

Modalità UDLD Aggressive

Il protocollo UDLD aggressivo è stato creato per risolvere quei pochi casi in cui è necessario un test continuo della connettività bidirezionale. Pertanto, la modalità aggressiva offre una protezione avanzata contro le condizioni di collegamento unidirezionale pericolose in queste situazioni:

- quando la perdita di PDU UDLD è simmetrica e si verifica il timeout di entrambe le unità. In questo caso, nessuna delle porte è disabilitata a causa di un errore.
- Un lato del collegamento ha una porta bloccata (sia Tx che Rx).
- Un lato del collegamento rimane attivo mentre l'altro lato è inattivo.
- La negoziazione automatica o un altro meccanismo di rilevamento degli errori di layer 1 è disabilitata.
- Èauspicabile ridurre il ricorso ai meccanismi FEFI di layer 1.
- Ènecessaria la massima protezione da errori di collegamento unidirezionale su collegamenti FE/GE point-to-point. In particolare, se non è ammesso alcun guasto tra due vicini, le sonde aggressive UDLD possono essere considerate un battito cardiaco, la cui presenza garantisce la salute del collegamento.

Il caso più comune di implementazione di un protocollo UDLD aggressivo è l'esecuzione del controllo della connettività su un membro di un bundle quando la negoziazione automatica o un altro meccanismo di rilevamento errori di layer 1 è disabilitato o inutilizzabile. È particolarmente utile con le connessioni EtherChannel perché PAgP e LACP, anche se abilitate, non utilizzano timer hello molto bassi allo stato stazionario. In questo caso, l'uso aggressivo del protocollo UDLD ha l'ulteriore vantaggio di prevenire possibili loop nello spanning-tree.

Èimportante ricordare che la modalità normale UDLD verifica la presenza di una condizione di collegamento unidirezionale, anche quando un collegamento raggiunge lo stato bidirezionale. Il protocollo UDLD ha lo scopo di rilevare i problemi di layer 2 che causano loop STP e tali problemi sono in genere unidirezionali (in quanto il flusso delle BPDU viene eseguito solo in una direzione allo stato stazionario). Pertanto, l'uso del protocollo UDLD normale in combinazione con la negoziazione automatica e la protezione in loop (per le reti che si basano sul protocollo STP) è quasi sempre sufficiente. Se la modalità aggressiva UDLD è abilitata, quando tutti i dispositivi adiacenti a una porta sono scaduti, sia nella fase di annuncio che in quella di rilevamento, la modalità aggressiva UDLD riavvia la sequenza di collegamento nel tentativo di eseguire una risincronizzazione con i dispositivi adiacenti potenzialmente non sincronizzati. Se dopo una trasmissione rapida dei messaggi (otto tentativi non riusciti) il collegamento viene ancora considerato indeterminato, la porta viene messa nello stato err-disabled.

Nota: alcuni switch non supportano il protocollo UDLD. Attualmente, Catalyst 2900XL e Catalyst 3500XL hanno intervalli di messaggi hardcoded di 60 secondi. Questa velocità non è considerata sufficiente per proteggere il sistema da potenziali loop STP (con i parametri STP predefiniti considerati).

Ripristino automatico dei collegamenti UDLD

Il ripristino della porta da una condizione di errore è disabilitato a livello globale per impostazione predefinita. Dopo essere stata abilitata a livello globale, se una porta viene messa nello stato err-disabled, viene riabilitata automaticamente dopo un intervallo di tempo selezionato. L'ora predefinita è 300 secondi, un timer globale che viene mantenuto per tutte le porte di uno switch. A seconda della versione del software, è possibile impedire manualmente la riattivazione di una porta se si imposta il timeout di errdisable per la porta in modo che venga disabilitato con il meccanismo di ripristino del timeout di errdisable per UDLD:

```
Switch(config)#errdisable recovery cause udld
```

Prendere in considerazione l'uso della funzione di timeout di errdisable quando si implementa la modalità aggressiva UDLD senza funzionalità di gestione della rete fuori banda, in particolare sul livello di accesso o su qualsiasi dispositivo che possa rimanere isolato dalla rete in caso di errore.

Per ulteriori informazioni su come configurare un periodo di timeout per le porte con stato err-disabled, consultare la guida di riferimento dei comandi di Cisco IOS serie 6500, versione 12.1 E.

Il ripristino da uno stato di errore può essere particolarmente importante per il protocollo UDLD nel livello di accesso quando gli switch di accesso sono distribuiti in un campus e la visita manuale di ciascuno switch per riattivare entrambi gli uplink richiede molto tempo.

Cisco sconsiglia di disabilitare il ripristino da uno stato di errore nel core della rete, in quanto un core dispone in genere di più punti di ingresso e il ripristino automatico nel core può causare problemi ricorrenti. Pertanto, se il protocollo UDLD disabilita la porta, è necessario riattivarla manualmente.

UDLD su collegamenti indirizzati

Ai fini di questa discussione, un link indirizzato è uno dei due tipi di connessione seguenti:

- Point-to-point tra due nodi di router (configurato con una subnet mask a 30 bit)
- VLAN con più porte, ma che supporta solo connessioni instradate, ad esempio in una topologia di base di layer 2 suddiviso

Ciascun protocollo IGRP (Interior Gateway Routing Protocol) ha caratteristiche univoche per quanto riguarda il modo in cui gestisce le relazioni tra nodi adiacenti e la convergenza dei percorsi. In questa sezione vengono descritte le caratteristiche rilevanti ai fini del presente documento, che contrasta due dei più diffusi protocolli di routing attualmente in uso, il protocollo OSPF (Open Shortest Path First) e il protocollo EIGRP (Enhanced IGRP).

Nota: un errore di layer 1 o layer 2 su una rete con routing point-to-point determina la disconnessione quasi immediata della connessione di layer 3. Poiché l'unica porta dello switch di tale VLAN passa a uno stato non connesso in seguito a un errore di layer 1/2, la funzione di stato automatico dell'interfaccia sincronizza gli stati delle porte di layer 2 e layer 3 in circa due secondi e attiva/disattiva l'interfaccia VLAN di layer 3 (protocollo di linea inattivo).

Se si presumono i valori predefiniti del timer, OSPF invia messaggi di saluto ogni 10 secondi e ha un intervallo inattivo di 40 secondi (4 * salve). Questi timer sono coerenti per le reti point-to-point e broadcast OSPF. Poiché OSPF richiede una comunicazione bidirezionale per formare un adiacente, il tempo di failover peggiore è di 40 secondi. Ciò è vero anche se il guasto di layer 1/layer 2 non è puro in una connessione point-to-point e lascia uno scenario a metà con cui il protocollo di layer 3 deve gestire. Poiché il tempo di rilevamento del protocollo UDLD è molto simile al tempo di rilevamento di un timer inattivo OSPF in scadenza (circa 40 secondi), i vantaggi della configurazione della modalità normale UDLD su un collegamento point-to-point del layer 3 OSPF sono limitati.

In molti casi, la convergenza EIGRP è più rapida rispetto a quella OSPF. Tuttavia, è importante notare che la comunicazione bidirezionale non è un requisito per lo scambio di informazioni di routing tra vicini. In scenari di guasto molto specifici, l'EIGRP è vulnerabile al blocco nero del traffico che dura fino a quando qualche altro evento attiva le rotte attraverso il vicino. La modalità normale UDLD può risolvere queste situazioni, in quanto rileva un errore nel collegamento unidirezionale e la porta viene disabilitata a causa di un errore.

Per le connessioni di routing di layer 3 che usano un protocollo di routing qualsiasi, UDLD normal offre ancora la protezione contro problemi presenti all'attivazione iniziale del collegamento, come cavi errati o hardware difettoso. Inoltre, la modalità aggressiva UDLD offre i seguenti vantaggi sulle connessioni di routing di layer 3:

- Impedisce inutili blocchi del traffico (con tempi minimi in alcuni casi)
- Attiva lo stato err-disabled per un collegamento intermittente
- Protezione da loop risultanti da configurazioni EtherChannel di layer 3

Comportamento predefinito del protocollo UDLD

Il protocollo UDLD è disabilitato a livello globale e abilitato per impostazione predefinita nelle porte Fibre Channel. Poiché il protocollo UDLD è un protocollo di infrastruttura necessario solo tra switch, per impostazione predefinita il protocollo UDLD è disabilitato sulle porte in rame, che generalmente vengono usate per l'accesso all'host. Affinché i router adiacenti possano raggiungere lo stato bidirezionale, è necessario abilitare il protocollo UDLD a livello globale e a livello di interfaccia. L'intervallo predefinito per i messaggi è 15 secondi. Tuttavia, in alcuni casi l'intervallo predefinito dei messaggi può essere pari a sette secondi. per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCea70679 (solo utenti registrati). L'intervallo predefinito dei messaggi può essere configurato tra sette e 90 secondi e la modalità aggressiva UDLD è disabilitata. Il software Cisco IOS versione 12.2(25)SEC riduce ulteriormente questo timer minimo a un secondo.

Consiglio di configurazione Cisco

Nella maggior parte dei casi, Cisco consiglia di abilitare la modalità normale UDLD su tutti i collegamenti FE/GE point-to-point tra gli switch Cisco e di impostare l'intervallo dei messaggi UDLD su 15 secondi quando si usano i timer Spanning Tree predefiniti 802.1D. Inoltre, se le reti si basano sul protocollo STP per la ridondanza e la convergenza (ossia se nella topologia sono presenti una o più porte in stato di blocco STP), utilizzare il protocollo UDLD insieme alle funzionalità e ai protocolli appropriati. Tali funzionalità includono FEFI, negoziazione automatica, protezione loop e così via. In genere, se la negoziazione automatica è abilitata, la modalità aggressiva non è necessaria perché la negoziazione automatica compensa il rilevamento degli errori sul layer 1.

Per abilitare il protocollo UDLD, usare una delle due opzioni seguenti:

Nota: la sintassi è cambiata in diverse piattaforme/versioni.

-
```
udld enable
!--- Once globally enabled, all FE and GE fiber !--- ports have UDLD enabled by default.
udld port
```

  o

-
```
udld enable
!--- The copper ports of some earlier Cisco IOS Software !--- releases can have UDLD enabled
by individual port command.
```

Ènecessario abilitare manualmente le porte che vengono chiuse a causa dei sintomi del collegamento unidirezionale. Utilizzare uno dei metodi seguenti:

```
udld reset
!--- Globally reset all interfaces that UDLD shut down. no udld port
udld port [aggressive]
!--- Per interface, reset and reenable interfaces that UDLD shut down.
```

I comandi di configurazione globale **errdisable recovery cause** udld e **errdisable recovery interval** consentono di ripristinare automaticamente il sistema dallo stato err-disabled.

Cisco consiglia di utilizzare il meccanismo di ripristino da uno stato di errore solo nel livello di accesso della rete, con timer di ripristino di 20 minuti o più, in caso di difficoltà di accesso fisico allo switch. La situazione migliore è quella di attendere il tempo necessario per la stabilizzazione e la risoluzione dei problemi della rete, prima che la porta venga rimessa in linea e causi instabilità della rete.

Cisco consiglia di *non* utilizzare i meccanismi di ripristino nel nucleo della rete perché ciò può causare instabilità e causare problemi di convergenza ogni volta che viene ripristinato un collegamento difettoso. La progettazione ridondante di una rete principale fornisce un percorso di backup per un collegamento guasto e consente di disporre del tempo necessario per un'analisi dei motivi di errore UDLD.

Usa UDLD senza protezione loop STP

Per i collegamenti di layer 3, point-to-point o layer 2 con topologia STP senza loop (senza blocco delle porte), Cisco consiglia di abilitare il protocollo UDLD sui collegamenti FE/GE point-to-point tra gli switch Cisco. In questo caso, l'intervallo tra i messaggi è impostato su sette secondi e 802.1D STP utilizza i timer predefiniti.

UDLD su EtherChannel

Indipendentemente dal fatto che STP loop guard sia distribuito o meno, la modalità aggressiva UDLD è consigliata per tutte le configurazioni EtherChannel, insieme alla modalità canale desiderabile. Nelle configurazioni EtherChannel, un errore nel collegamento del canale che trasporta le Spanning Tree BPDU e il traffico di controllo PAgP può causare loop immediati tra i partner di canale se i collegamenti di canale vengono disaggregati. La modalità aggressiva UDLD chiude una porta guasta. PAgP (modalità canale automatico/desiderabile) può quindi negoziare un nuovo collegamento di controllo ed eliminare efficacemente un collegamento guasto dal canale.

UDLD con Spanning Tree 802.1w

Per impedire i loop quando si usano versioni più recenti dello Spanning Tree, usare la modalità normale UDLD e la protezione loop STP con RSTP come 802.1w. UDLD può fornire protezione dai collegamenti unidirezionali durante una fase di collegamento e STP loop guard può impedire i loop STP nel caso in cui i collegamenti diventino unidirezionali *dopo che* UDLD ha stabilito i collegamenti come bidirezionali. Poiché non è possibile configurare il protocollo UDLD su un valore inferiore a quello dei timer 802.1w predefiniti, è necessario attivare la protezione STP loop per impedire completamente la formazione di loop nelle topologie ridondanti.

Per ulteriori informazioni, fare riferimento a Descrizione e configurazione della funzionalità UDLD (Unidirectional Link Detection Protocol).

Test e monitoraggio UDLD

Il protocollo UDLD non è facile da testare senza un componente realmente difettoso/unidirezionale presente in laboratorio, ad esempio un GBIC difettoso. Il protocollo è stato progettato per rilevare scenari di errore meno comuni rispetto agli scenari generalmente utilizzati in un laboratorio. Ad esempio, se si esegue un test semplice, come lo scollegamento di un trefolo di una fibra per verificare lo stato `err-disabled` desiderato, è necessario prima disattivare la negoziazione automatica di layer 1. In caso contrario, la porta fisica `si blocca` e la comunicazione del messaggio UDLD viene reimpostata. L'estremità remota passa allo stato `undefined` in modalità normale UDLD e allo stato err-disabled solo in modalità aggressiva UDLD.

Un metodo di test aggiuntivo simula la perdita della PDU del router adiacente per il protocollo UDLD. Il metodo consiste nell'utilizzare i filtri del livello MAC per bloccare l'indirizzo hardware UDLD/CDP e consentire il passaggio di altri indirizzi. alcuni switch non inviano frame UDLD quando la porta è configurata per essere una destinazione SPAN (Switched Port Analyzer), che simula una porta adiacente UDLD che non risponde.

Per monitorare il protocollo UDLD, usare questo comando:

```
show udld gigabitethernet1/1
Interface Gi1/1
---
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 7
Time out interval: 5
```

Inoltre, dalla modalità di abilitazione nel software Cisco IOS versione 12.2(18)SXD o successive, è possibile usare il comando **show udld neighbors** nascosto per controllare il contenuto della cache UDLD (allo stesso modo del CDP). Spesso è molto utile confrontare la cache UDLD con la cache CDP per verificare se esiste un'anomalia specifica del protocollo. Ogni volta che viene influenzato anche il CDP, in genere il problema si verifica in tutte le BPDU/PDU. Pertanto, controllare anche STP. Ad esempio, verificare se sono state apportate modifiche recenti all'identità principale o alla posizione della porta principale/designata.

Èpossibile monitorare lo stato UDLD e la coerenza della configurazione utilizzando le variabili MIB UDLD SNMP di Cisco.

Switching multilayer

Panoramica

Nel software di sistema Cisco IOS, lo switch multilayer (MLS) è supportato sui Catalyst serie 6500/6000 e solo internamente. Il router deve quindi essere installato nello switch. I Supervisor Engine Catalyst 6500/6000 più recenti supportano MLS CEF, in cui la tabella di routing viene scaricata su ciascuna scheda. Ciò richiede hardware aggiuntivo, che include la presenza di una DFC (Distributed Forwarding Card). Le DFC non sono supportate nel software CatOS, anche se si sceglie di utilizzare il software Cisco IOS sulla scheda del router. Le DFC sono supportate solo nei software di sistema Cisco IOS.

La cache MLS utilizzata per abilitare le statistiche NetFlow sugli switch Catalyst è la cache basata sul flusso usata dalla scheda Supervisor Engine I e dagli switch Catalyst precedenti per abilitare lo switching di layer 3. MLS è abilitato per impostazione predefinita sul Supervisor Engine 1 (o

Supervisor Engine 1A) con MSFC o MSFC2. Per la funzionalità MLS predefinita non è necessaria alcuna configurazione MLS aggiuntiva. È possibile configurare la cache MLS in una delle tre modalità seguenti:

- destinazione
- origine-destinazione
- porta origine-destinazione

La maschera di flusso viene usata per determinare la modalità MLS dello switch. Questi dati vengono successivamente utilizzati per abilitare i flussi di layer 3 negli switch Catalyst con provisioning IA di Supervisor Engine. I blade Supervisor Engine II non utilizzano la cache MLS per commutare i pacchetti perché questa scheda è abilitata per l'hardware CEF, una tecnologia molto più scalabile. La cache MLS viene mantenuta nella scheda Supervisor Engine II per abilitare solo l'esportazione statistica NetFlow. Pertanto, è possibile abilitare Supervisor Engine II per il flusso completo, se necessario, senza alcun impatto negativo sullo switch.

Configurazione

Il tempo di aging MLS si applica a tutte le voci della cache MLS. Il valore temporale di aging viene applicato direttamente alla misurazione durata in modalità di destinazione. Il valore del tempo di aging MLS viene diviso per due in modo da derivare il tempo di aging dalla modalità origine alla destinazione. Dividere il valore del tempo di aging MLS per otto per trovare il tempo di aging del flusso completo. Il valore predefinito del tempo di aging MLS è 256 sec.

Èpossibile configurare il tempo di aging normale in un intervallo compreso tra 32 e 4092 secondi con incrementi di otto secondi. Qualsiasi valore relativo al tempo di aging che non sia un multiplo di otto secondi viene regolato sul multiplo di 8 secondi più vicino. Ad esempio, il valore 65 viene portato a 64 e il valore 127 a 128.

Altri eventi possono causare l'eliminazione di voci MLS. Tali eventi comprendono:

- Modifiche routing
- Modifica dello stato del collegamentoAd esempio, il collegamento PFC non è attivo.

Per mantenere le dimensioni della cache MLS al di sotto delle 32.000 voci, abilitare questi parametri dopo aver eseguito il comando **mls aging**:

```
Normal: configures the wait before aging out and deleting shortcut entries in
the L3 table.

Fast aging: configures an efficient process to age out entries created for flows that
only switch a few packets and then are never used again. The fast aging parameter uses
the time keyword value to check if at least the threshold keyword value of packets has
been switched for each flow. If a flow has not switched the threshold number of packets
during the time interval, then the entry in the L3 table is aged out.

Long: configures entries for deletion that have been up for the specified value even if
the L3 entry is in use. Long aging is used to prevent counter wraparound, which could
cause inaccurate statistics.
```

Configurazione

Una voce tipica della cache che viene rimossa è la voce per i flussi verso e da un server DNS (Domain Name Server) o TFTP che non può più essere utilizzata dopo la creazione della voce. Il rilevamento e il timeout di queste voci consentono di risparmiare spazio nella cache MLS per il

traffico di altri dati.

Se è necessario abilitare il tempo di invecchiamento rapido MLS, impostare il valore iniziale su 128 secondi. Se le dimensioni della cache MLS continuano ad aumentare oltre 32.000 voci, diminuire l'impostazione fino a che le dimensioni della cache non rimangono inferiori a 32.000. Se le dimensioni della cache continuano ad aumentare oltre 32.000 voci, diminuire il tempo di aging MLS normale.

Configurazione MLS consigliata da Cisco

Lasciare MLS sul valore predefinito, solo destinazione, a meno che non sia richiesta l'esportazione NetFlow. Se è richiesto NetFlow, abilitare MLS full flow solo sui sistemi Supervisor Engine II.

Per abilitare la destinazione del flusso MLS, usare questo comando:

```
Switch(config)#mls flow ip destination
```

Frame jumbo

Unità massima di trasmissione

L'MTU (Maximum Transmission Unit) è il datagramma o la dimensione del pacchetto più grande in byte che un'interfaccia può inviare o ricevere senza frammentare il pacchetto.

In base allo standard IEEE 802.3, le dimensioni massime del frame Ethernet sono:

- **1518 byte** per frame normali (1500 byte più 18 byte aggiuntivi di intestazione Ethernet e sequenza terminale CRC)
- **1522 byte** per frame 802.1Q incapsulati (1518 più 4 byte di tagging)

Baby Giants: La funzione Baby Giants permette allo switch di passare attraverso/inoltrare pacchetti leggermente più grandi dell'MTU Ethernet dell'IEEE, invece di dichiarare i frame di dimensioni eccessive e di eliminarli.

Jumbo: La definizione delle dimensioni dei frame dipende dal fornitore, in quanto le dimensioni dei frame non fanno parte dello standard IEEE. I frame jumbo sono frame più grandi delle dimensioni standard Ethernet (pari a 1518 byte, che includono l'intestazione di layer 2 e la sequenza di controllo dei frame [FCS]).

La dimensione MTU predefinita è 9216 byte dopo che il supporto dei frame jumbo è stato abilitato sulla singola porta.

Quando prevedere pacchetti superiori a 1518 byte

Per trasportare il traffico tra le reti commutate, verificare che l'MTU del traffico trasmesso non superi quella supportata sulle piattaforme dello switch. Le dimensioni MTU di alcuni frame possono essere troncate per diversi motivi:

- **Requisiti specifici del fornitore**: le applicazioni e alcune schede NIC possono specificare una dimensione MTU non compresa nei 1500 byte standard. Questo cambiamento è avvenuto a causa di studi che provano che un aumento delle dimensioni di un frame Ethernet può

aumentare il throughput medio.

- **Trunking**: per trasportare le informazioni sull'ID VLAN tra gli switch o altri dispositivi di rete, il trunking è stato utilizzato per aumentare il frame Ethernet standard. Oggi, le due forme più comuni di trunking sono:Incapsulamento ISL proprietario Cisco802.1Q
- **Multiprotocol Label Switching (MPLS)**: dopo aver abilitato MPLS su un'interfaccia, MPLS può aumentare le dimensioni del frame di un pacchetto, che dipende dal numero di etichette nello stack di etichette di un pacchetto con tag MPLS. La dimensione totale di un'etichetta è di 4 byte. Le dimensioni totali di una pila di etichette sono:
  `n * 4 bytes`
  Se è formato uno stack di etichette, i frame possono superare l'MTU.
- **Tunneling 802.1Q**: i pacchetti di tunneling 802.1Q contengono due tag 802.1Q, di cui solo uno alla volta è in genere visibile all'hardware. Pertanto, il tag interno aggiunge 4 byte al valore MTU (dimensioni del payload).
- **Universal Transport Interface (UTI)/Layer 2 Tunneling Protocol versione 3 (Layer 2TPv3)**: UTI/Layer 2TPv3 incapsula i dati di Layer 2 da inoltrare sulla rete IP. UTI/Layer 2TPv3 può aumentare le dimensioni del frame originale fino a 50 byte. Il nuovo frame include una nuova intestazione IP (20 byte), un'intestazione Layer 2TPv3 (12 byte) e una nuova intestazione Layer 2. Il payload Layer 2TPv3 è costituito dal frame Layer 2 completo, che include l'intestazione Layer 2.

Scopo

La commutazione basata su hardware ad alta velocità (1 Gbps e 10 Gbps) ha reso i frame jumbo una soluzione molto concreta ai problemi di throughput non ottimale. Anche se non esiste uno standard ufficiale per le dimensioni dei frame jumbo, un valore piuttosto comune che viene spesso adottato nel campo è 9216 byte (9 KB).

Considerazioni sull'efficienza della rete

Èpossibile calcolare l'efficienza della rete per l'inoltro di un pacchetto dividendo le dimensioni del payload per la somma del valore del sovraccarico e le dimensioni del payload.

Anche se l'efficienza della rete aumenta con i frame jumbo, e va dal 94,9% (1500 byte) al 99,1% (9216 byte), il sovraccarico di elaborazione (utilizzo della CPU) dei dispositivi di rete e degli host terminali diminuisce in modo proporzionale alle dimensioni del pacchetto. Ecco perché le tecnologie di rete LAN e WAN ad alte prestazioni tendono a preferire dimensioni massime piuttosto grandi.

Il miglioramento delle prestazioni è possibile solo quando vengono eseguiti lunghi trasferimenti di dati. Esempi di applicazioni sono:

- Comunicazione back-to-back del server (ad esempio, transazioni NFS)
- Clustering dei server
- Backup dei dati ad alta velocità
- Interconnessione supercomputer ad alta velocità
- Trasferimento dei dati delle applicazioni grafiche

Considerazioni sulle prestazioni della rete

Le prestazioni di TCP su WAN (Internet) sono state studiate in modo approfondito. Questa equazione spiega come il throughput TCP abbia un limite superiore basato su:

- Le dimensioni massime del segmento (MSS), ossia la lunghezza dell'MTU meno la lunghezza delle intestazioni TCP/IP
- Tempo di andata e ritorno (RTT, Round Trip Time)
- La perdita di pacchetti

$$Throughput \leq\sim 0.7 \times MSS / \left(RTT \times \sqrt{packet\_loss}\right)$$

In base a questa formula, la velocità di trasmissione TCP massima raggiungibile è direttamente proporzionale al valore MSS. Ciò significa che, con il routing RTT costante e la perdita di pacchetti, è possibile raddoppiare la velocità di trasmissione TCP raddoppiando le dimensioni del pacchetto. Analogamente, quando si utilizzano frame jumbo anziché frame da 1518 byte, un aumento di dimensioni pari a sei volte può comportare un potenziale miglioramento di sei volte nella velocità TCP di una connessione Ethernet.

Panoramica operativa

La specifica dello standard IEEE 802.3 definisce una dimensione massima del frame Ethernet di **1518**. I frame 802.1Q incapsulati, con una lunghezza compresa tra 1519 e 1522 byte, sono stati aggiunti alla specifica 802.3 in una fase successiva attraverso l'addendum IEEE Std 802.3ac-1998. In letteratura si fa talvolta riferimento a loro come **giganti dei bambini**.

In generale, i pacchetti vengono classificati come **frame giant** quando superano la lunghezza massima Ethernet specificata per una connessione Ethernet specifica. I pacchetti giganti sono anche noti come **frame jumbo**.

Il principale punto di confusione riguardo ai frame jumbo è la configurazione: interfacce diverse supportano dimensioni massime di pacchetto diverse e, talvolta, trattano pacchetti di grandi dimensioni in modi leggermente diversi.

Catalyst serie 6500

La tabella seguente cerca di riepilogare le dimensioni MTU attualmente supportate dalle diverse schede sulla piattaforma Catalyst 6500:

Scheda di linea	Dimensioni MTU
Predefinito	9216 byte
WS-X6248-RJ-45, WS-X6248A-RJ-45, WS-X6248-TEL, WS-X6248A-TEL, WS-X6348-RJ-45, WS-X6348-RJ45V, WS-X6348-RJ-21 e WX-X6348-RJ21V	8092 byte (limitati dal chip PHY)
WS-X6148-RJ-45(V), WS-X6148-RJ-21(V), WS-X6148-45AF e WS-X6148-21AF	9100 byte (a 100 Mbps) 9216 byte (a 10 Mbps)
WS-X6516-GE-TX	8092 byte (a 100 Mbps) 9216 byte (a 10 o 1000 Mbps)
WS-X6148(V)-GE-TX, WS-X6148-GE-	1500 byte

45AF, WS-X6548(V)-GE-TX e WS-X6548-GE-45AF	
OSM ATM (OC12c)	9180 byte
OSM CHOC3, CHOC12, CHOC48 e CT3	9216 byte (OCx e DS3) 7673 byte (T1/E1)
FlexWAN	7673 byte (CT3 T1/DS0) 9216 byte (OC3c POS) 7673 byte (T1)
WS-X6148-GE-TX e WS-X6548-GE-TX	Nessun supporto

Per ulteriori informazioni, fare riferimento a Configurazione di Ethernet, Fast Ethernet, Gigabit Ethernet e switching 10 Gigabit Ethernet.

Supporto jumbo layer 2 e layer 3 nel software Catalyst 6500/6000 Cisco IOS

Èdisponibile il supporto jumbo di layer 2 e layer 3 con PFC/MSFC1, PFC/MSFC2 e PFC2/MSFC2 su tutte le porte GE configurate come interfacce fisiche di layer 2 e layer 3. il supporto esiste indipendentemente dal fatto che queste porte siano trunking o channeling. Questa funzione è disponibile a partire da Cisco IOS versione 12.1.1E.

- Le dimensioni MTU di tutte le porte fisiche abilitate per jumbo sono legate tra loro. Un cambiamento in uno di questi cambia tutto. Mantengono sempre le stesse dimensioni MTU jumbo frame dopo essere state abilitate.
- Durante la configurazione, abilitare tutte le porte nella stessa VLAN abilitata al jumbo o abilitare nessuna di esse al jumbo.
- Le dimensioni MTU dell'interfaccia virtuale commutata (SVI) (interfaccia VLAN) vengono impostate separatamente dall'MTU delle porte fisiche. Una modifica dell'MTU delle porte fisiche non modifica le dimensioni dell'MTU della SVI. Inoltre, una modifica dell'MTU SVI non influisce sull'MTU delle porte fisiche.
- Il supporto di frame jumbo di layer 2 e layer 3 sulle interfacce FE è iniziato nel software Cisco IOS versione 12.1(8a) EX01. Il comando **mtu 1500** disabilita i frame jumbo su FE e il comando **mtu 9216** abilita i frame jumbo su FE. Fare riferimento all'ID bug Cisco CSCdv90450 (solo utenti registrati).
- I frame jumbo di layer 3 sulle interfacce VLAN sono supportati solo su:PFC/MSFC2 (software Cisco IOS versione 12.1(7a)E e successive)PFC2/MSFC2 (software Cisco IOS versione 12.1(8a)E4 e successive)
- Non si consiglia di usare i frame jumbo con PFC/MSFC1 per le interfacce VLAN (SVI) perché MSFC1 potrebbe non essere in grado di gestire la frammentazione come desiderato.
- La frammentazione dei pacchetti all'interno della stessa VLAN (jumbo di layer 2) non è supportata.
- I pacchetti che devono essere frammentati sulle VLAN/subnet (jumbo di layer 3) vengono inviati al software per la frammentazione.

Informazioni sul supporto Jumbo Frame nel software Catalyst 6500/6000 Cisco IOS

Un frame jumbo è un frame più grande della dimensione predefinita del frame Ethernet. Per

abilitare il supporto dei jumbo frame, configurare una dimensione MTU superiore a quella predefinita su una porta o su un'interfaccia VLAN e, con il software Cisco IOS versione 12.1(13)E e successive, configurare la dimensione MTU della porta LAN globale.

Verifica delle dimensioni del traffico con bridging e routing nel software Cisco IOS

Scheda di linea	In ingresso	In uscita
Porte 10, 10/100, 100 Mbps	Controllo delle dimensioni MTU completato. Il supporto di frame jumbo confronta le dimensioni del traffico in entrata con le dimensioni MTU della porta LAN globale alle porte Ethernet 10, 10/100 e 100 Mbps in entrata e alle porte LAN 10-GE con dimensioni MTU non predefinite configurate. La porta scarta il traffico sovradimensionato.	Il controllo delle dimensioni MTU non è stato eseguito. Le porte configurate con una dimensione MTU non predefinita trasmettono frame che contengono pacchetti di qualsiasi dimensione superiore a 64 byte. Con una MTU configurata con dimensioni non predefinite, le porte LAN Ethernet a 10, 10/100 e 100 Mbps non verificano la presenza di frame in uscita di dimensioni eccessive.
Porte GE	Il controllo delle dimensioni MTU non è stato eseguito. Le porte configurate con una MTU non predefinita accettano frame che contengono pacchetti di qualsiasi dimensione superiore a 64 byte e non verificano la presenza di frame in ingresso di dimensioni eccessive.	Controllo delle dimensioni MTU completato. Il supporto di frame jumbo confronta le dimensioni del traffico in uscita con le dimensioni MTU della porta LAN in uscita globale sul GE in uscita e le porte LAN 10-GE con dimensioni MTU configurate non predefinite. La porta scarta il traffico sovradimensionato.
Porte 10-GE	Controllo delle dimensioni MTU completato. La porta scarta il traffico sovradimensionato.	Controllo delle dimensioni MTU completato. La porta scarta il traffico sovradimensionato.
SVI	Il controllo delle dimensioni MTU non è stato eseguito. La SVI non controlla le	Controllo delle dimensioni MTU completato. Le dimensioni MTU

	dimensioni del frame sul lato in entrata.	vengono controllate sul lato in uscita della SVI.
	PFC	
Tutto il traffico indirizzato	Per il traffico che deve essere instradato, il supporto jumbo frame sulla PFC confronta le dimensioni del traffico con le dimensioni MTU configurate e fornisce la commutazione di livello 3 per il traffico jumbo tra le interfacce configurate con dimensioni MTU sufficienti a supportare il traffico. Tra interfacce non configurate con MTU di dimensioni sufficienti: • Se il bit "non frammentare" (DF, Don't Fragment) non è impostato, il PFC invia il traffico all'MSFC per essere frammentato e instradato nel software. • Se il bit DF è impostato, il PFC scarta il traffico.	

Consigli di Cisco

Se implementati correttamente, i frame jumbo possono fornire un potenziale miglioramento di sei volte nella velocità di trasmissione TCP di una connessione Ethernet, con un sovraccarico di frammentazione ridotto (più un sovraccarico inferiore della CPU sui dispositivi terminali).

Ènecessario verificare che non vi siano dispositivi intermedi in grado di gestire le dimensioni MTU specificate. Se il dispositivo frammenta e inoltra i pacchetti, l'intero processo viene annullato. Ciò può causare un ulteriore sovraccarico sul dispositivo per la frammentazione e il riassemblaggio dei pacchetti.

In questi casi, il rilevamento dell'MTU del percorso IP aiuta i mittenti a trovare la lunghezza minima comune del pacchetto, adatta a trasmettere il traffico su ciascun percorso. In alternativa, è possibile configurare i dispositivi host con supporto dei frame jumbo con una MTU delle dimensioni minime supportate nella rete.

Ènecessario controllare attentamente ciascun dispositivo per verificare che possa supportare le dimensioni MTU. Vedere la tabella di supporto delle dimensioni MTU in questa sezione.

Il supporto di frame jumbo può essere abilitato su questi tipi di interfacce:

- Port-channel interface
- SVI
- Interfaccia fisica (layer 2/layer 3)

Èpossibile abilitare i frame jumbo sul canale della porta o sulle interfacce fisiche che partecipano al canale della porta. È molto importante verificare che l'MTU sia la stessa su tutte le interfacce fisiche. In caso contrario, è possibile che l'interfaccia venga sospesa. È necessario modificare l'MTU di un'interfaccia del canale della porta perché modifica l'MTU di tutte le porte del membro.

Nota: se non è possibile modificare l'MTU di una porta membro sul nuovo valore perché la porta membro è la porta che blocca, il canale della porta viene sospeso.

Prima di configurare il supporto dei frame jumbo su una SVI, accertarsi sempre che tutte le interfacce fisiche di una VLAN siano configurate per i frame jumbo. L'MTU di un pacchetto non

viene controllata sul lato in entrata di una SVI. Ma è controllato sul lato in uscita di una SVI. Se l'MTU del pacchetto è più grande dell'MTU SVI in uscita, il pacchetto viene frammentato dal software (se il bit DF non è impostato), il che si traduce in prestazioni scadenti. La frammentazione del software avviene solo per lo switching di livello 3. Quando un pacchetto viene inoltrato a una porta di layer 3 o a una SVI con MTU inferiore, il software viene frammentato.

L'MTU di una SVI deve essere sempre più piccola della MTU più piccola tra tutte le porte dello switch nella VLAN.

Catalyst serie 4500

I frame jumbo sono supportati principalmente sulle porte non bloccanti delle schede di linea Catalyst 4500. Queste porte GE non bloccanti hanno connessioni dirette al fabric di switching del Supervisor Engine e supportano i frame jumbo:

- Supervisor EngineWS-X4515, WS-X4516 - Due porte GBIC di uplink su Supervisor Engine IV o VWS-X4516-10GE - Due uplink 10-GE e quattro uplink 1-GE Small Form Factor Pluggable (SFP)WS-X4013+ - Due uplink 1 GEWS-X4013+10GE - Due uplink 10-GE e quattro uplink 1-GE SFPWS-X4013+TS—20 porte 1-GE
- Schede di lineaWS-X4306-GB - Modulo GE 1000BASE-X (GBIC) a sei porteWS-X4506-GB-T: 10/100/1000 Mbps a sei porte e SFPWS-X4302-GB - Modulo GE 1000BASE-X (GBIC) a due porteLe prime due porte GBIC di un modulo GE di switching per server a 18 porte (WS-X4418-GB) e le porte GBIC del modulo WS-X4232-GB-RJ
- Switch a configurazione fissaWS-C4948—Tutte le 48 porte 1-GEWS-C4948-10GE: tutte le 48 porte 1-GE e due porte 10-GE

Èpossibile usare queste porte GE non bloccanti per supportare i jumbo frame di 9 KB o la soppressione delle trasmissioni hardware (solo Supervisor Engine IV). Tutte le altre schede di linea supportano i frame giant per bambini. È possibile utilizzare i neonati giganti per il bridging di MPLS o per Q in Q passthrough con un payload massimo di 1552 byte.

Nota: le dimensioni del frame aumentano con i tag ISL/802.1Q.

I giant e i frame jumbo sono trasparenti per le altre funzionalità di Cisco IOS con Supervisor Engine IV e V.

Funzionalità di sicurezza software Cisco IOS

Funzioni di sicurezza di base

Un tempo, la sicurezza veniva spesso trascurata nei progetti dei campus. Ma la sicurezza è ormai una parte essenziale di ogni rete aziendale. Normalmente il client ha già stabilito una policy di sicurezza per aiutare a definire quali strumenti e tecnologie Cisco sono applicabili.

Protezione tramite password di base

La maggior parte dei dispositivi software Cisco IOS è configurata con due livelli di password. Il primo livello è per l'accesso Telnet al dispositivo, noto anche come accesso vty. Dopo aver concesso l'accesso vty, è necessario accedere in modalità abilitazione o in modalità di esecuzione privilegiata.

Proteggere la modalità di abilitazione dello switch

La password enable consente a un utente di ottenere l'accesso completo a un dispositivo. Assegnare la password enable solo a utenti attendibili.

```
Switch(config)#enable secret password
```

Assicurarsi che la password rispetti le seguenti regole:

- La password deve contenere da 1 a 25 caratteri alfanumerici maiuscoli e minuscoli.
- La password non deve contenere un numero come primo carattere.
- Èpossibile utilizzare spazi iniziali, ma vengono ignorati. Vengono riconosciuti gli spazi intermedi e finali.
- Il controllo della password fa distinzione tra maiuscole e minuscole. La password Secret, ad esempio, è diversa dalla password secret.

Nota: il comando **enable secret** utilizza una funzione di hashing MD5 (Message Digest 5) con crittografia unidirezionale. Se si usa il comando **show running-config**, è possibile visualizzare questa password crittografata. L'uso del comando **enable password** è un altro modo per impostare la password di abilitazione. Tuttavia, l'algoritmo di crittografia utilizzato con il comando **enable password** è debole e può essere facilmente invertito per ottenere la password. Pertanto, non utilizzare il comando **enable password**. Per una maggiore sicurezza, utilizzare il comando **enable secret**. Per ulteriori informazioni, fare riferimento a Cisco IOS Password Encryption Facts.

Accesso sicuro Telnet/VTY allo switch

Per impostazione predefinita, il software Cisco IOS supporta cinque sessioni Telnet attive. Queste sessioni sono note come vty da 0 a 4. È possibile abilitare queste linee per l'accesso. Ma per abilitare il login, è necessario anche impostare la password per queste linee.

```
Switch(config)#line vty 0 4
Switch(config-line)#login
Switch(config-line)#password password
```

Il comando **login** configura queste righe per l'accesso Telnet. Il comando **password** configura una password. Assicurarsi che la password rispetti le seguenti regole:

- Il primo carattere non può essere un numero.
- La stringa può contenere qualsiasi carattere alfanumerico, fino a un massimo di 80 caratteri. I caratteri includono spazi.
- Non è possibile specificare la password nel formato spazio-numero carattere. Lo spazio dopo il numero causa problemi. hello 21, ad esempio, è una password valida, mentre hello 21 non è una password valida.
- Il controllo della password fa distinzione tra maiuscole e minuscole. La password Secret, ad esempio, è diversa dalla password secret.

Nota: con questa configurazione della linea vty, lo switch memorizza la password in testo non crittografato. Se si usa il comando **show running-config**, la password è visibile. Per evitare questa situazione, usare il comando **service password-encryption**. Il comando crittografa la password in modo approssimativo. Il comando cripta solo la password della riga vty e la password enable configurata con il comando **enable password**. La password enable configurata con il comando

enable secret utilizza una crittografia più avanzata. La configurazione con il comando **enable secret** è il metodo consigliato.

Nota: per una maggiore flessibilità nella gestione della sicurezza, verificare che tutti i dispositivi software Cisco IOS implementino il modello di sicurezza autenticazione, autorizzazione e accounting (AAA). AAA può utilizzare database locali, RADIUS e TACACS+. Per ulteriori informazioni, vedere la sezione Configurazione autenticazione TACACS+.

Servizi di sicurezza AAA

Panoramica delle operazioni AAA

Il controllo dell'accesso controlla chi dispone dell'autorizzazione per accedere allo switch e quali servizi possono essere utilizzati dagli utenti. I servizi di sicurezza della rete AAA offrono la struttura principale per configurare il controllo dell'accesso sullo switch.

In questa sezione vengono descritti in dettaglio i vari aspetti del processo AAA:

- Autenticazione: questo processo convalida l'identità richiesta di un utente finale o di un dispositivo. In primo luogo, vengono specificati i vari metodi che possono essere utilizzati per autenticare l'utente. Questi metodi definiscono il tipo di autenticazione da eseguire (ad esempio, TACACS+ o RADIUS). Viene inoltre definita la sequenza in cui tentare di utilizzare questi metodi di autenticazione. I metodi vengono quindi applicati alle interfacce appropriate, attivando così l'autenticazione.
- Autorizzazione: questo processo concede i diritti di accesso a un utente, a gruppi di utenti, a un sistema o a un processo. Il processo AAA è in grado di eseguire un'autorizzazione singola per singola operazione. Il processo definisce gli attributi (sul server AAA) su ciò che l'utente è autorizzato a eseguire. Ogni volta che l'utente tenta di avviare un servizio, lo switch esegue una query sul server AAA e richiede l'autorizzazione dell'utente. Se il server AAA approva, l'utente è autorizzato. Se il server AAA non approva, l'utente non dispone dell'autorizzazione per eseguire il servizio. È possibile utilizzare questa procedura per specificare che alcuni utenti possono eseguire solo determinati comandi.
- Accounting: questo processo consente di tenere traccia dei servizi a cui gli utenti accedono e della quantità di risorse di rete che gli utenti utilizzano. Quando l'accounting è abilitato, lo switch segnala l'attività dell'utente al server AAA sotto forma di record di accounting. Tra gli esempi di attività dell'utente segnalati sono inclusi l'ora della sessione e l'ora di inizio e di fine. L'analisi di questa attività può quindi essere eseguita a scopo di gestione o di fatturazione.

Sebbene il metodo AAA sia il metodo principale e consigliato per il controllo degli accessi, il software Cisco IOS offre funzionalità aggiuntive per il controllo semplice degli accessi che non rientrano nell'ambito del metodo AAA. Le caratteristiche aggiuntive includono:

- Autenticazione nome utente locale
- Autenticazione password riga
- Abilita autenticazione password

Tuttavia, queste funzionalità non offrono lo stesso livello di controllo degli accessi possibile con AAA.

Per una migliore comprensione del processo AAA, consultare i seguenti documenti:

- Autenticazione, autorizzazione e accounting (AAA)
- Configurazione della funzionalità AAA di base su un server di accesso
- Confronto tra TACACS+ e RADIUS

Questi documenti non menzionano necessariamente i parametri. Tuttavia, i concetti AAA descritti nel documento sono validi per gli switch.

TACACS+

Scopo

Per impostazione predefinita, le password senza privilegi e in modalità privilegiata sono globali. Queste password si applicano a tutti gli utenti che accedono allo switch o al router, sia dalla porta console che tramite una sessione Telnet in rete. L'implementazione di queste password sui dispositivi di rete è un'operazione lunga e non centralizzata. Inoltre, l'implementazione delle restrizioni di accesso può presentare difficoltà dovute all'uso di elenchi di controllo di accesso (ACL) che possono essere soggetti a errori di configurazione. Per risolvere questi problemi, adottare un approccio centralizzato quando si configurano nomi utente, password e criteri di accesso su un server centrale. Questo server può essere Cisco Secure Access Control Server (ACS) o un server di terze parti. I dispositivi sono configurati in modo da utilizzare questi database centralizzati per le funzioni AAA. In questo caso, i dispositivi sono switch software Cisco IOS. Il protocollo utilizzato tra i dispositivi e il server centrale può essere:

- TACACS+
- RAGGIO
- Kerberos

TACACS+ è un'implementazione comune nelle reti Cisco ed è l'argomento principale di questa sezione. TACACS+ offre le seguenti funzionalità:

- Autenticazione: processo che identifica e verifica un utente. Per autenticare un utente è possibile utilizzare diversi metodi. Tuttavia, il metodo più comune include una combinazione di nome utente e password.
- Autorizzazione—Quando l'utente tenta di eseguire un comando, lo switch può controllare con il server TACACS+ se all'utente è stata concessa l'autorizzazione a usare quel particolare comando.
- Accounting: questo processo registra ciò che un utente fa o ha fatto sul dispositivo.

per un confronto tra TACACS+ e RADIUS, fare riferimento a Confronto tra TACACS+ e RADIUS.

Panoramica operativa

Il protocollo TACACS+ inoltra nomi utente e password al server centralizzato. Le informazioni vengono crittografate sulla rete con l'hashing unidirezionale MD5. Per ulteriori informazioni, fare riferimento alla RFC 1321 . TACACS+ utilizza la porta TCP 49 come protocollo di trasporto e offre i seguenti vantaggi rispetto a UDP:

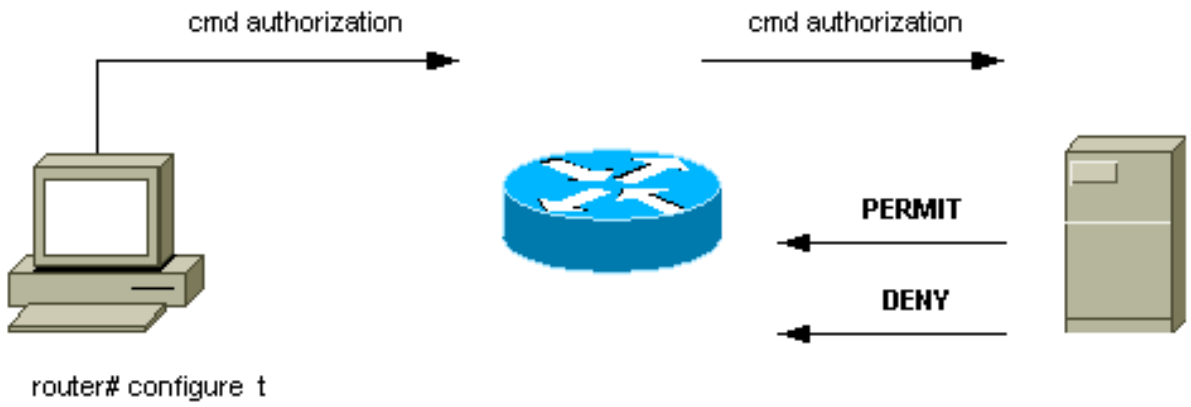
Nota: RADIUS utilizza UDP.

- Trasporto orientato alle connessioni
- Separata conferma della ricezione di una richiesta (riconoscimento TCP [ACK]), indipendentemente dal modo in cui è stato caricato il meccanismo di autenticazione back-end

- Indicazione immediata di un arresto anomalo del server (reimpostare i pacchetti [RST])

Se è necessario un ulteriore controllo delle autorizzazioni, durante una sessione lo switch controlla con TACACS+ per determinare se all'utente è stata concessa l'autorizzazione a utilizzare un particolare comando. Questo passaggio offre un maggiore controllo sui comandi che possono essere eseguiti sullo switch e consente di disaccoppiarsi dal meccanismo di autenticazione. L'accounting dei comandi consente di controllare i comandi eseguiti da un utente specifico mentre è collegato a un dispositivo di rete specifico.

Il diagramma mostra il processo di autorizzazione:



Quando un utente esegue l'autenticazione a un dispositivo di rete utilizzando TACACS+ in un semplice tentativo di accesso in modalità ASCII, questo processo si verifica in genere:

- Una volta stabilita la connessione, lo switch contatta il daemon TACACS+ per ottenere un prompt con il nome utente. Lo switch visualizza quindi il prompt per l'utente. L'utente immette un nome utente e lo switch contatta il daemon TACACS+ per ottenere una richiesta della password. Lo switch visualizza la richiesta della password per l'utente, che immette una password che viene inviata anche al daemon TACACS+.
- Il dispositivo di rete riceve infine una delle seguenti risposte dal daemon TACACS+:ACCEPT - L'utente viene autenticato e il servizio può iniziare. Se il dispositivo di rete è configurato per richiedere l'autorizzazione, l'autorizzazione inizia in questo momento.REJECT: l'utente non ha eseguito l'autenticazione. All'utente viene negato un ulteriore accesso o viene richiesto di riprovare la sequenza di accesso. Il risultato dipende dal daemon TACACS+.ERROR: si è verificato un errore durante l'autenticazione. L'errore può verificarsi sul daemon o nella connessione di rete tra il daemon e lo switch. Se viene ricevuta una risposta di ERRORE, il dispositivo di rete tenta in genere di utilizzare un metodo alternativo per autenticare l'utente.CONTINUE - All'utente vengono richieste informazioni di autenticazione aggiuntive.
- Prima di procedere all'autorizzazione TACACS+, gli utenti devono completare correttamente l'autenticazione TACACS+.
- Se è richiesta l'autorizzazione TACACS+, si contatta nuovamente il daemon TACACS+. Il daemon TACACS+ restituisce una risposta di autorizzazione ACCEPT o REJECT. Se viene restituita una risposta ACCEPT, la risposta contiene dati sotto forma di attributi utilizzati per indirizzare la sessione EXEC o NETWORK per l'utente. Determina i comandi a cui l'utente può accedere.

Procedura di configurazione base del server AAA

La configurazione del processo AAA è relativamente semplice dopo aver compreso le procedure di base. Per configurare la sicurezza su un router o un server di accesso Cisco con AAA, attenersi alla seguente procedura:

1. Per abilitare il server AAA, usare il comando di configurazione globale **aaa new-model**.
   ```
   Switch(config)#aaa new-model
   ```

   Suggerimento: salvare la configurazione prima di configurare i comandi AAA. Salvare nuovamente la configurazione solo dopo aver completato tutte le configurazioni AAA e aver verificato che funzioni correttamente. Quindi, se necessario, è possibile ricaricare lo switch per ripristinare lo stato precedente ai blocchi imprevisti (prima di salvare la configurazione).
2. Se si decide di utilizzare un server di sicurezza separato, configurare i parametri del protocollo di sicurezza, ad esempio RADIUS, TACACS+ o Kerberos.
3. Usare il comando **aaa authentication** per definire gli elenchi dei metodi di autenticazione.
4. Utilizzare il comando **login authentication** per applicare gli elenchi di metodi a una determinata interfaccia o riga.
5. Usare il comando opzionale **aaa authorization** per configurare l'autorizzazione.
6. Usare il comando opzionale **aaa accounting** per configurare l'accounting.
7. Configurare il server esterno AAA per elaborare le richieste di autenticazione e autorizzazione dallo switch.**Nota:** Per ulteriori informazioni, consultare la documentazione del server AAA in uso.

Configurazione autenticazione TACACS+

Per configurare l'autenticazione TACACS+, eseguire la procedura seguente:

1. Per abilitare il processo AAA sullo switch, usare il comando **aaa new-model** in modalità di configurazione globale.
2. Definire il server TACACS+ e la chiave associata.Questa chiave è utilizzata per crittografare il traffico tra il server TACACS+ e lo switch. Nel comando **tacacs-server host 1.1.1.1 key mysecretkey**, il server TACACS+ ha indirizzo IP 1.1.1.1 e la chiave di crittografia è mysecretkey. Per verificare che lo switch possa raggiungere il server TACACS+, avviare un ping Internet Control Message Protocol (ICMP) dallo switch.
3. Definire un elenco di metodi.Un elenco di metodi definisce la sequenza dei meccanismi di autenticazione da provare per vari servizi. I vari servizi possono essere, ad esempio:AttivaLogin (per accesso vty/Telnet)**Nota:** per informazioni sull'accesso vty/Telnet, vedere la sezione Funzioni di sicurezza di base di questo documento.ConsoleIn questo esempio viene preso in considerazione solo **l'accesso**. È necessario applicare l'elenco dei metodi alle interfacce/linee:
   ```
   Switch(config)#aaa authentication login METHOD-LIST-LOGIN group tacacs+ line
   Switch(config)#line vty 0 4
   Switch(config-line)#login authentication METHOD-LIST-LOGIN
   Switch(config-line)#password hard_to_guess
   ```

   In questa configurazione, il comando **aaa authentication login** utilizza il nome dell'elenco creato METHOD-LIST-LOGIN e il metodo tacacs+ prima della riga del metodo. Gli utenti vengono autenticati usando il server TACACS+ come primo metodo. Se il server TACACS+

non risponde o invia un messaggio di ERRORE, la password configurata sulla riga viene utilizzata come secondo metodo. Tuttavia, se il server TACACS+ rifiuta l'utente e risponde con un messaggio REJECT, il server AAA considera la transazione riuscita e non utilizza il secondo metodo.**Nota:** la configurazione non è completa finché non si applica l'elenco (METHOD-LIST-LOGIN) alla riga vty. Eseguire il comando **login authentication METHOD-LIST-LOGIN** in modalità di configurazione riga, come mostrato nell'esempio.**Nota:** nell'esempio viene creata una backdoor per i casi in cui il server TACACS+ non è disponibile. Gli amministratori della sicurezza possono o non possono accettare l'implementazione di una backdoor. Accertati che la decisione di implementare queste backdoor sia conforme alle politiche di sicurezza del sito.

Configurazione autenticazione RADIUS

La configurazione RADIUS è quasi identica alla configurazione TACACS+. Sostituire semplicemente la parola RADIUS con TACACS nella configurazione. Di seguito è riportato un esempio di configurazione RADIUS per l'accesso alla porta COM:

```
Switch(config)#aaa new-model
Switch(config)#radius-server host 1.1.1.1 key mysecretkey
Switch(config)#aaa authentication login METHOD-LIST-LOGIN group radius line
Switch(config)#line con 0
Switch(config-line)#login authentication METHOD-LIST-LOGIN
Switch(config-line)#password hard_to_guess
```

Banner di accesso

Creare appositi banner indicanti in modo specifico le azioni intraprese in caso di accesso non autorizzato. Non annunciare il nome del sito o le informazioni di rete a utenti non autorizzati. I banner offrono la possibilità di ricorrere in caso di danneggiamento di un dispositivo e di cattura del responsabile. Per creare i banner di accesso, usare questo comando:

```
Switch(config)#banner motd ^C
*** Unauthorized Access Prohibited ***
^C
```

Sicurezza fisica

Accertarsi che sia necessaria una corretta autorizzazione per accedere fisicamente ai dispositivi. Tenere l'apparecchiatura in uno spazio controllato (bloccato). Per garantire che la rete rimanga operativa e non venga danneggiata da manomissioni dannose o fattori ambientali, verificare che tutte le apparecchiature dispongano di:

- Un gruppo di continuità (UPS) adeguato, con fonti ridondanti ove possibile
- Controllo della temperatura (aria condizionata)

Ricorda che, se una persona con intenzioni maligne viola l'accesso fisico, è molto più probabile che si verifichino interruzioni tramite il recupero della password o altri mezzi.

Configurazione gestione

Diagrammi di rete

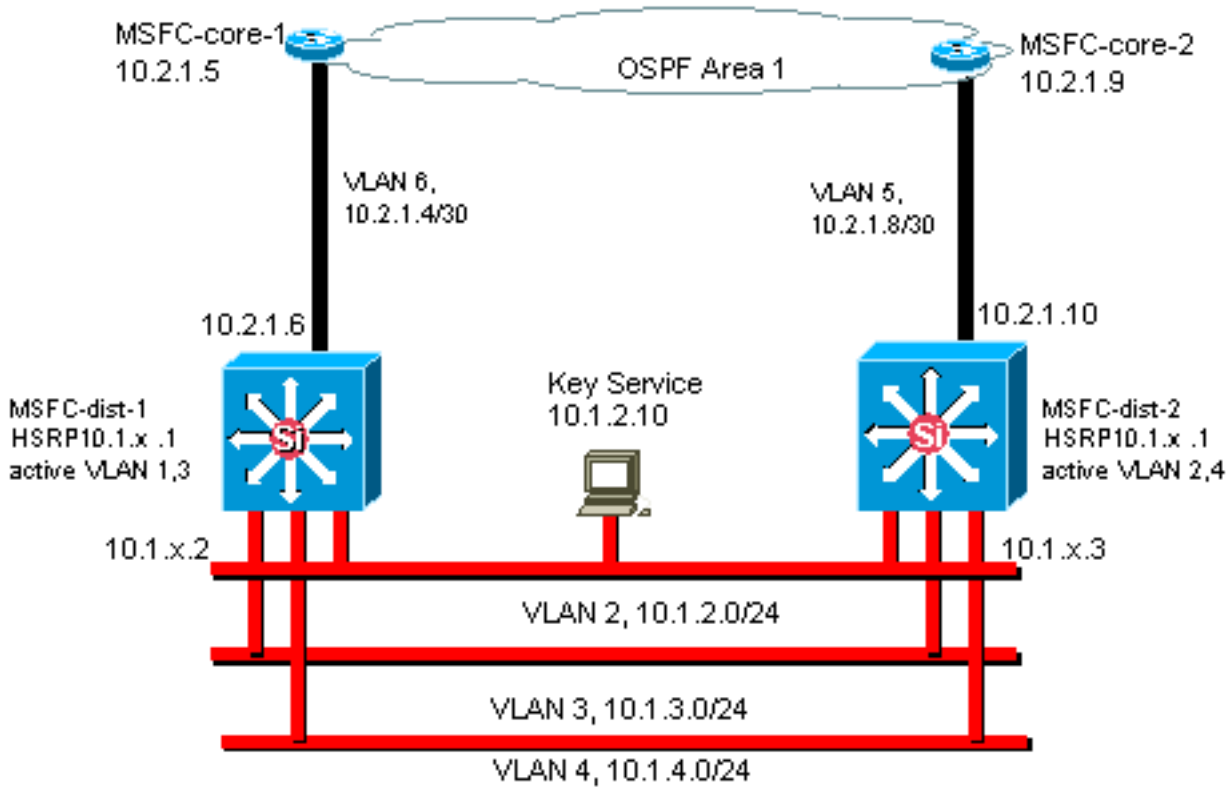
Scopo

I chiari diagrammi di rete sono una parte fondamentale delle operazioni di rete. I diagrammi diventano critici durante la risoluzione dei problemi e rappresentano il veicolo più importante per la comunicazione delle informazioni durante l'escalation a fornitori e partner durante un'interruzione delle attività. Non sottovalutare la preparazione, la prontezza e l'accessibilità fornite dai diagrammi di rete.

Suggerimento

Sono necessari i seguenti tre tipi di diagrammi:

- **Diagramma generale** - Anche per le reti più grandi è importante disporre di un diagramma che indichi la connettività fisica o logica end-to-end. Spesso, le aziende che hanno implementato un documento di progettazione gerarchico, ogni livello separatamente. Quando si pianificano e si risolvono i problemi, ciò che conta è una buona conoscenza di come i domini si collegano tra loro.
- **Diagramma fisico**: il diagramma mostra tutto l'hardware e i cavi dello switch e del router. Assicurarsi che il diagramma indichi ciascuno di questi aspetti:TrunkLinkVelocitàGruppi di canaliNumeri di portaSlotTipi di chassisSoftwareDomini VTPPonte radicePriorità bridge radice di backupIndirizzo MACPorte bloccate per VLANPer una maggiore chiarezza, rappresentare i dispositivi interni come il router MSFC Catalyst 6500/6000 come router su uno stick collegato tramite un trunk.
- **Diagramma logico**: questo diagramma mostra solo la funzionalità di layer 3, ossia mostra i router come oggetti e le VLAN come segmenti Ethernet. Verificare che nel diagramma siano presenti le etichette per i seguenti aspetti:indirizzi IPSubnetIndirizzamento secondarioHSRP attivo e in standbyAccesso ai livelli di distribuzione di baseInformazioni di routing



Interfaccia di gestione dello switch e VLAN nativa

Scopo

In questa sezione vengono descritti la significatività e i potenziali problemi di utilizzo della VLAN predefinita 1. Vengono inoltre descritti i potenziali problemi quando si esegue il traffico di gestione sullo switch nella stessa VLAN del traffico utente sugli switch serie 6500/6000.

I processori sui Supervisor Engine e gli MSFC per Catalyst serie 6500/6000 utilizzano la VLAN 1 per una serie di protocolli di controllo e gestione. Alcuni esempi:

- Protocolli di controllo switch:BPDU STPVTPDTPCDP
- Protocolli di gestione:SNMPTelnetSSH (Secure Shell Protocol)Syslog

Quando la VLAN viene utilizzata in questo modo, viene indicata come VLAN nativa. La configurazione predefinita dello switch imposta la VLAN 1 come VLAN nativa predefinita sulle porte del trunk Catalyst. È possibile lasciare la VLAN 1 come VLAN nativa. Tuttavia, occorre tenere presente che per impostazione predefinita, su tutti gli switch della rete con software di sistema Cisco IOS, tutte le interfacce configurate come porte degli switch di livello 2 hanno accesso alle porte della VLAN 1. Molto probabilmente, uno switch da qualche parte nella rete usa la VLAN 1 come VLAN per il traffico dell'utente.

La preoccupazione principale per l'uso della VLAN 1 è che, in generale, il protocollo NMP del Supervisor Engine non deve essere interrotto da gran parte del traffico broadcast e multicast generato dalle stazioni terminali. In particolare, le applicazioni multicast tendono a inviare una grande quantità di dati tra server e client. Il Supervisor Engine non ha bisogno di visualizzare questi dati. Se le risorse o i buffer del Supervisor Engine sono completamente occupati mentre il Supervisor Engine è in ascolto del traffico non necessario, il Supervisor Engine può non visualizzare i pacchetti di gestione che possono causare un loop nello spanning-tree o un errore di

EtherChannel (nello scenario peggiore).

Il comando **show interfaces** *interface_type slot*/*port* counters e il comando **show ip traffic** possono fornire alcune indicazioni su:

- Proporzione del traffico broadcast rispetto al traffico unicast
- La proporzione del traffico IP rispetto al traffico non IP (che in genere non si osserva nelle VLAN di gestione)

La VLAN 1 contrassegna e gestisce la maggior parte del traffico del control plane. La VLAN 1 è abilitata su tutti i trunk per impostazione predefinita. Con reti di campus più grandi, è necessario fare attenzione al diametro del dominio VLAN 1 STP. L'instabilità di una parte della rete può influire sulla VLAN 1 e sulla stabilità del control plane e sulla stabilità dell'STP di tutte le altre VLAN. È possibile limitare la trasmissione VLAN 1 dei dati utente e il funzionamento di STP su un'interfaccia. È sufficiente non configurare la VLAN sull'interfaccia trunk.

Questa configurazione non arresta la trasmissione dei pacchetti di controllo da uno switch all'altro nella VLAN 1, come con un analizzatore di rete. Tuttavia, non viene inoltrato alcun dato e STP non viene eseguito su questo collegamento. Pertanto, è possibile utilizzare questa tecnica per suddividere la VLAN 1 in domini di errore più piccoli.

Nota: non è possibile cancellare la VLAN 1 dai trunk sugli switch Catalyst 2900XL/3500XL.

Anche se si presta attenzione a vincolare le VLAN degli utenti a domini di switch relativamente piccoli e di conseguenza a piccoli errori/limiti di layer 3, alcuni clienti sono ancora tentati di trattare le VLAN di gestione in modo diverso. Questi clienti cercano di coprire l'intera rete con una singola subnet di gestione. Non vi è alcun motivo tecnico per cui un'applicazione NMS centrale debba essere adiacente al layer 2 dei dispositivi gestiti dall'applicazione, né si tratta di un argomento di sicurezza qualificato. Limitare il diametro delle VLAN di gestione alla stessa struttura di dominio routing delle VLAN utente. Considerare la gestione fuori banda e/o il supporto SSH come un modo per aumentare la sicurezza della gestione della rete.

Altre opzioni

Per queste raccomandazioni Cisco, per alcune topologie sono necessarie considerazioni di progettazione. Ad esempio, un progetto multilayer Cisco comune e desiderabile evita l'uso di uno spanning tree attivo. In questo modo, il progetto richiede il vincolo di ciascuna subnet IP/VLAN a un singolo switch di livello di accesso (o cluster di switch). In questi progetti, non è possibile configurare il trunking fino al livello di accesso.

Si crea una VLAN di gestione separata e si abilita il trunking per trasportarlo tra i livelli di accesso di layer 2 e distribuzione di layer 3? Non c'è una risposta facile a questa domanda. Per l'esame del progetto, considerare le seguenti due opzioni con il tecnico Cisco:

- **Opzione 1** - Trunk di due o tre VLAN univoche dal livello di distribuzione a ciascuno switch del livello di accesso. Questa configurazione consente una VLAN dati, una VLAN voce e una VLAN di gestione e ha il vantaggio che l'STP non è attivo. Per rimuovere la VLAN 1 dai trunk, è necessario un ulteriore passaggio di configurazione. In questa soluzione, è necessario considerare anche i punti di progettazione per evitare il traffico di routing del black holing temporaneo durante il ripristino in caso di errore. Usare STP PortFast per i trunk (in futuro) o per la sincronizzazione automatica della VLAN con inoltro STP.
- **Opzione 2**: una singola VLAN per i dati e la gestione può essere accettabile. Se si desidera

mantenere l'interfaccia sc0 separata dai dati dell'utente, l'hardware dello switch più recente rende questo scenario meno problematico di quanto lo fosse in precedenza. L'hardware più recente offre:CPU più potenti e controlli di limitazione della velocità del control planeUn design con domini broadcast relativamente piccoli, come richiesto dal design multilayerPer prendere una decisione finale, esaminare il profilo del traffico di broadcast per la VLAN e discutere con il tecnico Cisco le funzionalità dell'hardware dello switch. Se la VLAN di gestione contiene tutti gli utenti su tale switch del livello di accesso, usare i filtri di input IP per proteggere lo switch dagli utenti, come mostrato nella sezione Funzioni di sicurezza software di Cisco IOS.

Consiglio per l'interfaccia di gestione e la VLAN nativa Cisco

Interfaccia di gestione

Il software di sistema Cisco IOS consente di configurare le interfacce come interfacce di layer 3 o porte dello switch di layer 2 in una VLAN. Quando si usa il comando **switchport** nel software Cisco IOS, tutte le porte dello switch sono porte di accesso nella VLAN 1 per impostazione predefinita. Quindi, a meno che non si configuri diversamente, i dati utente possono esistere anche sulla VLAN 1 per impostazione predefinita.

Rendere la VLAN di gestione una VLAN diversa dalla VLAN 1. Tenere tutti i dati utente fuori dalla VLAN di gestione. Configurare invece un'interfaccia loopback0 come interfaccia di gestione su ciascuno switch.

Nota: se si utilizza il protocollo OSPF, anche questo diventa l'ID del router OSPF.

Verificare che l'interfaccia di loopback abbia una subnet mask a 32 bit e configurare l'interfaccia di loopback come un'interfaccia di solo livello 3 sullo switch. Questo è un esempio:

```
Switch(config)#interface loopback 0
Switch(config-if)#ip address 10.x.x.x 255.255.255.255
Switch(config-if)#end
Switch#
```

VLAN nativa

Configurare la VLAN nativa in modo che sia una VLAN fittizia ovvia che non è mai stata abilitata sul router. Cisco ha raccomandato la VLAN 999 in passato, ma la scelta è puramente arbitraria.

Per stabilire una VLAN come nativa (impostazione predefinita) per il trunking 802.1Q su una determinata porta, eseguire questi comandi di interfaccia:

```
Switch(config)#interface type slot/port
Switch(config-if)#switchport trunk native vlan 999
```

Per ulteriori suggerimenti sulla configurazione del trunking, vedere la sezione Protocollo di trunking dinamico in questo documento.

Gestione fuori banda

Scopo

Èpossibile aumentare la disponibilità della gestione di rete se si crea un'infrastruttura di gestione separata intorno alla rete di produzione. Questa configurazione consente ai dispositivi di essere raggiungibili in remoto, nonostante il traffico che viene indirizzato o gli eventi del control plane che si verificano. Questi due approcci sono tipici:

- Gestione fuori banda con una LAN esclusiva
- Gestione fuori banda con server terminal

Panoramica operativa

Èpossibile fornire a ogni router e switch della rete un'interfaccia di gestione Ethernet fuori banda su una VLAN di gestione. È possibile configurare una porta Ethernet su ciascun dispositivo della VLAN di gestione e collegarla all'esterno della rete di produzione a una rete di gestione commutata separata.

Nota: gli switch Catalyst 4500/4000 dispongono di un'interfaccia me1 speciale sul Supervisor Engine che deve essere utilizzata solo per la gestione fuori banda e non come porta dello switch.

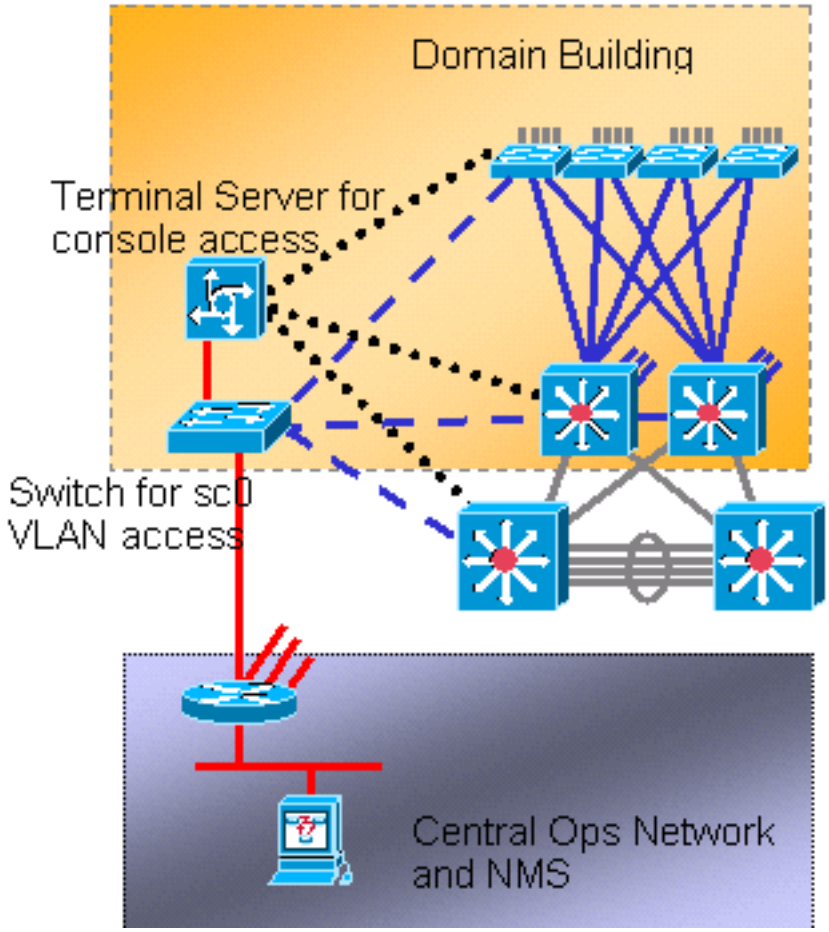
Inoltre, è possibile ottenere la connettività del server terminal configurando un router Cisco 2600 o 3600 con cavi seriali RJ-45 per accedere alla porta console di ogni router e switch del layout. L'utilizzo di un server terminal evita inoltre la necessità di configurare scenari di backup, ad esempio modem su porte ausiliarie per ogni dispositivo. È possibile configurare un singolo modem sulla porta ausiliaria del server terminal. Questa configurazione fornisce il servizio di connessione remota agli altri dispositivi durante un errore di connettività di rete. Per ulteriori informazioni, fare riferimento a Collegamento di un modem alla porta console sugli switch Catalyst.

Suggerimento

Con questa disposizione, sono possibili due percorsi fuori banda per ciascuno switch e router, oltre a numerosi percorsi in-band. La disposizione consente una gestione di rete ad alta disponibilità. I vantaggi sono:

- La disposizione separa il traffico di gestione dai dati utente.
- L'indirizzo IP di gestione si trova in una subnet, una VLAN e uno switch separati per motivi di sicurezza.
- Vi è una maggiore garanzia per il recapito dei dati di gestione durante gli errori di rete.
- Lo spanning tree non è attivo nella VLAN di gestione. La ridondanza in questo caso non è un fattore critico.

Il diagramma mostra la gestione fuori banda:



Log di sistema

Scopo

I messaggi syslog sono specifici di Cisco e possono fornire informazioni più precise e reattive rispetto al protocollo SNMP standardizzato. Ad esempio, le piattaforme di gestione come Cisco Resource Manager Essentials (RME) e Network Analysis Toolkit (NATKit) utilizzano in modo efficace le informazioni di syslog per raccogliere le modifiche all'inventario e alla configurazione.

Suggerimenti per la configurazione di Cisco Syslog

La registrazione del sistema è una pratica operativa comune e accettata. Un syslog UNIX può acquisire e analizzare informazioni/eventi sul router, quali:

- Stato interfaccia
- Avvisi di sicurezza
- Condizioni ambientali
- Hop di processo CPU
- Altri eventi

Il software Cisco IOS può eseguire il login UNIX a un server syslog UNIX. Il formato syslog di Cisco UNIX è compatibile con UNIX 4.3 Berkeley Standard Distribution (BSD). Usa queste impostazioni del registro software Cisco IOS:

- **no logging console**: per impostazione predefinita, tutti i messaggi di sistema vengono inviati alla console di sistema. La registrazione dalla console è un'attività ad alta priorità nel software

Cisco IOS. Questa funzione è stata principalmente progettata per fornire messaggi di errore all'operatore di sistema prima di un errore di sistema. Disabilitare la registrazione dalla console in tutte le configurazioni dei dispositivi per evitare che il router/switch si blocchi durante l'attesa di una risposta dal terminale. I messaggi della console possono tuttavia essere utili durante l'isolamento dei problemi. In questi casi, abilitare la registrazione della console. Per ottenere il livello desiderato di registrazione dei messaggi, usare il comando **logging console level**. I livelli di registrazione sono compresi tra 0 e 7.

- **no logging monitor**: questo comando disabilita la registrazione per le linee terminali diverse dalla console del sistema. La registrazione del monitoraggio può essere necessaria (con l'utilizzo della **registrazione** del **debug del monitoraggio** o di un'altra opzione di comando). In questo caso, abilitare la registrazione del monitoraggio al livello di registrazione specifico necessario per l'attività. Per ulteriori informazioni sui livelli di registrazione, vedere l'elemento **console** senza registrazione in questo elenco.
- **logging buffered 16384** - Il comando **logging buffered** deve essere aggiunto ai messaggi del sistema di log nel buffer di log interno. Il buffer di registrazione è circolare. Una volta riempito il buffer di registrazione, le voci meno recenti vengono sovrascritte da quelle più recenti. Le dimensioni del buffer di registrazione possono essere configurate dall'utente e sono specificate in byte. Le dimensioni del buffer di sistema variano a seconda della piattaforma in uso. 16384 è un buon valore predefinito che nella maggior parte dei casi fornisce una registrazione adeguata.
- **logging trap notification**: questo comando fornisce messaggi di livello di notifica (5) al server syslog specificato. Il livello di registrazione predefinito per tutti i dispositivi (console, monitor, buffer e trap) è il debug (livello 7). Se si lascia il livello di registrazione delle trap su 7, vengono generati molti messaggi estranei che non interessano affatto lo stato della rete. Impostare il livello di registrazione predefinito per i trap su 5.
- **logging facility local7**: questo comando imposta la funzione/il livello di logging predefinito per UNIX syslogging. Configurare il server syslog che riceve questi messaggi per la stessa struttura/lo stesso livello.
- **logging host** - Questo comando imposta l'indirizzo IP del server di logging UNIX.
- **logging source-interface loopback 0**: questo comando imposta l'associazione di sicurezza IP predefinita per i messaggi syslog. Codificare a livello di codice l'associazione di protezione che esegue la registrazione per semplificare l'identificazione dell'host che ha inviato il messaggio.
- **service timestamp debug datetime localtime show-timezone msec**: per impostazione predefinita, i messaggi del log non sono contrassegnati da un timestamp. È possibile utilizzare questo comando per abilitare l'indicatore orario dei messaggi di log e configurare l'indicatore orario dei messaggi di debug del sistema. L'opzione Timestamp (Data e ora) consente di definire l'ora relativa degli eventi registrati e migliora il debug in tempo reale. Queste informazioni sono particolarmente utili quando i clienti inviano output di debug al personale di supporto tecnico per assistenza. Per abilitare l'indicatore orario dei messaggi di debug del sistema, usare il comando in modalità di configurazione globale. Il comando ha effetto solo quando è attivato il debug.

Nota: abilitare inoltre la registrazione dello stato del collegamento e dello stato del bundle su tutte le interfacce Gigabit dell'infrastruttura.

Il software Cisco IOS fornisce un unico meccanismo per impostare la struttura e il livello di log per tutti i messaggi di sistema destinati a un server syslog. Impostare il livello di registrazione su notifica (livello 5). Se si imposta il livello dei messaggi trap su notifica, è possibile ridurre al minimo

il numero di messaggi informativi inoltrati al server syslog. Questa impostazione può ridurre in modo significativo la quantità di traffico syslog sulla rete e può ridurre l'impatto sulle risorse del server syslog.

Per abilitare i messaggi syslog, aggiungere questi comandi a ciascun router e switch con software Cisco IOS:

- Comandi di configurazione syslog globali:

```
no logging console
no logging monitor
logging buffered 16384
logging trap notifications
logging facility local7
logging host-ip
logging source-interface loopback 0
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
```

- Comandi di configurazione syslog interfaccia:

```
logging event link-status
logging event bundle-status
```

SNMP

Scopo

Èpossibile utilizzare il protocollo SNMP per recuperare statistiche, contatori e tabelle memorizzati nei MIB dei dispositivi di rete. Gli NMS come HP OpenView possono utilizzare queste informazioni per:

- Generazione di avvisi in tempo reale
- Misurare la disponibilità
- Produzione di informazioni sulla pianificazione della capacità
- Guida per l'esecuzione dei controlli di configurazione e risoluzione dei problemi

Funzionamento dell'interfaccia di gestione SNMP

SNMP è un protocollo a livello di applicazione che fornisce un formato di messaggio per la comunicazione tra i manager SNMP e gli agenti. L'SNMP fornisce un framework standardizzato e un linguaggio comune per il monitoraggio e la gestione dei dispositivi in una rete.

Il framework SNMP è costituito da tre parti:

- Un manager SNMP
- Un agente SNMP
- MIB

Il manager SNMP è il sistema che utilizza il protocollo SNMP per controllare e monitorare le attività degli host di rete. Il sistema di gestione più comune è denominato NMS. È possibile applicare il termine NMS a un dispositivo dedicato utilizzato per la gestione della rete o alle

applicazioni utilizzate in tale dispositivo. Con il protocollo SNMP è disponibile una vasta gamma di applicazioni per la gestione della rete. Queste applicazioni vanno da semplici applicazioni CLI a interfacce grafiche complete di funzionalità, come la linea di prodotti CiscoWorks.

L'agente SNMP è il componente software all'interno del dispositivo gestito che mantiene i dati per il dispositivo e li segnala, se necessario, alla gestione dei sistemi. L'agente e il MIB risiedono sul dispositivo di routing (il router, il server di accesso o lo switch). Per abilitare l'agente SNMP su un dispositivo di routing Cisco, è necessario definire la relazione tra il manager e l'agente.

Il MIB è un'area di storage virtuale per le informazioni sulla gestione della rete. Il MIB è costituito da insiemi di oggetti gestiti. All'interno del MIB, sono presenti insiemi di oggetti correlati definiti nei moduli MIB. I moduli MIB vengono scritti nel linguaggio del modulo MIB SNMP, come definito dalle specifiche STD 58, RFC 2578 , RFC 2579 e RFC 2580 .

Nota: i singoli moduli MIB vengono anche definiti MIB. Ad esempio, il gruppo di interfacce MIB (IF-MIB) è un modulo MIB nel MIB del sistema.

L'agente SNMP contiene variabili MIB, i cui valori possono essere richiesti o modificati dal programma di gestione SNMP tramite operazioni get o set. Un manager può ottenere un valore da un agente o memorizzarne uno in tale agente. L'agente raccoglie i dati dal MIB, che è il repository per le informazioni sui parametri dei dispositivi e i dati di rete. L'agente può inoltre rispondere alle richieste del manager di ottenere o impostare dati.

Un manager può inviare le richieste dell'agente per ottenere e impostare i valori MIB. L'agente può rispondere a queste richieste. Indipendentemente da questa interazione, l'agente può inviare notifiche non richieste (trap o informazioni) al gestore per notificare al gestore le condizioni della rete. Con alcuni meccanismi di sicurezza, un NMS può recuperare informazioni nei MIB con richieste `get` e `get next` e può usare il comando **set** per modificare i parametri. È inoltre possibile configurare un dispositivo di rete per generare un messaggio trap per l'NMS per gli allarmi in tempo reale. Le porte UDP IP 161 e 162 vengono utilizzate per le trap.

Panoramica operativa delle notifiche SNMP

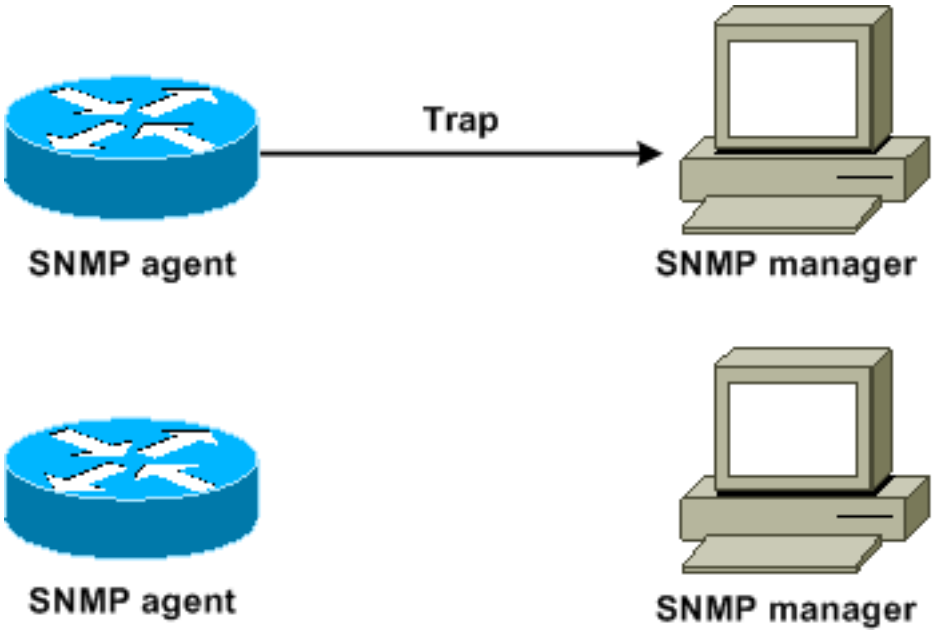
Una funzionalità chiave del protocollo SNMP è la capacità di generare notifiche da un agente SNMP. Queste notifiche non richiedono l'invio di richieste da SNMP Manager. Le notifiche non richieste (asincrone) possono essere generate come trap o richieste informative. I trap sono messaggi che avvisano il manager SNMP di una condizione sulla rete. Le richieste informative sono trap che includono una richiesta di conferma di ricezione da parte del manager SNMP. Le notifiche possono indicare eventi significativi quali:

- Autenticazione utente non corretta
- Riavvii
- Chiusura di una connessione
- La perdita della connessione a un router adiacente
- Altri eventi

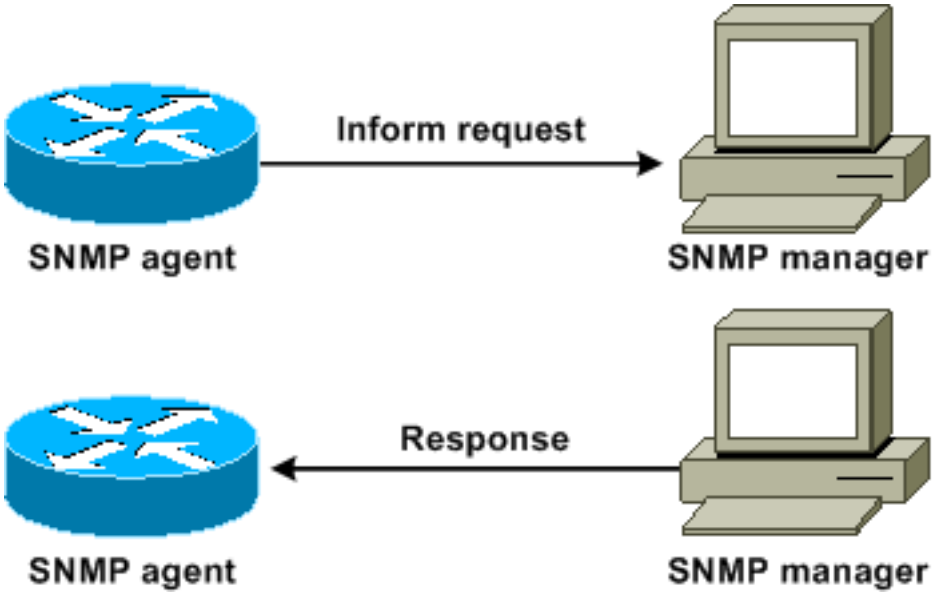
I trap sono meno affidabili di quelli informativi perché il ricevitore non invia alcuna conferma quando riceve una trap. Il mittente non può determinare se la trap è stata ricevuta. Un programma di gestione SNMP che riceve una richiesta di informazioni riconosce il messaggio con una unità PDU (Response Protocol Data Unit) SNMP. Se il responsabile non riceve una richiesta di informazioni, non invia una risposta. Se il mittente non riceve mai una risposta, può inviare di nuovo la richiesta di informazioni. È più probabile che gli informatori raggiungano la destinazione prevista.

Tuttavia, le trap sono spesso preferibili perché le informazioni consumano più risorse nel router e nella rete. Una trap viene scartata non appena viene inviata. Una richiesta di informazioni deve tuttavia essere mantenuta in memoria fino al ricevimento di una risposta o al timeout della richiesta. Inoltre, le trap vengono inviate una sola volta, mentre è possibile eseguire più volte un nuovo tentativo di invio di un'informazione. I tentativi aumentano il traffico e contribuiscono a un maggiore sovraccarico sulla rete. Pertanto, le trap e le richieste informative forniscono un compromesso tra affidabilità e risorse. Se è necessario che il manager SNMP riceva ogni notifica, utilizzare le richieste inform. Tuttavia, se si hanno dubbi sul traffico sulla rete o sulla memoria del router e non è necessario ricevere tutte le notifiche, utilizzare le trap.

Questi diagrammi illustrano le differenze tra le trap e le richieste informative:

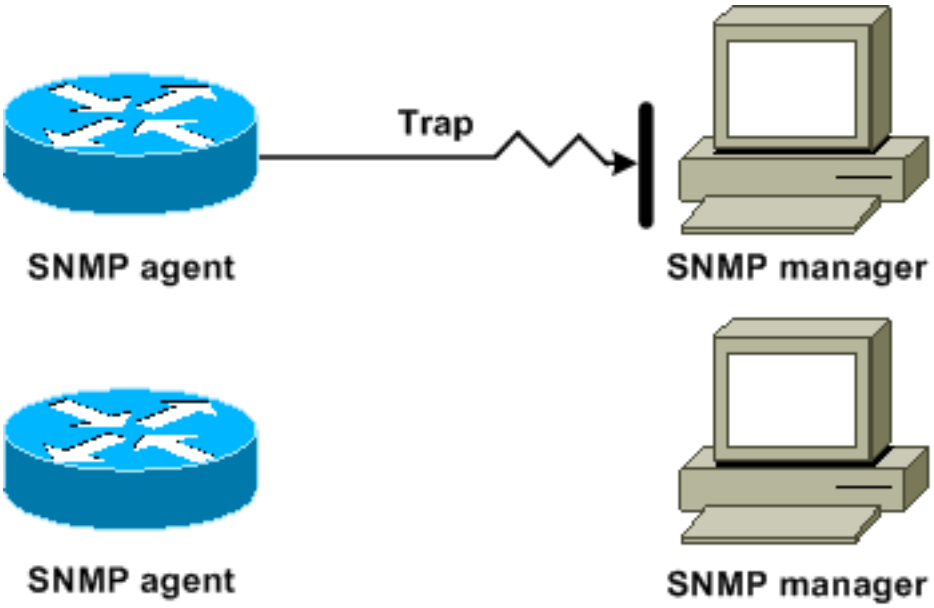


Questo diagramma mostra come il router dell'agente invia correttamente una trap al programma di gestione SNMP. Sebbene il responsabile riceva la trap, non invia alcuna conferma all'agente. L'agente non ha modo di sapere che la trappola ha raggiunto la destinazione.

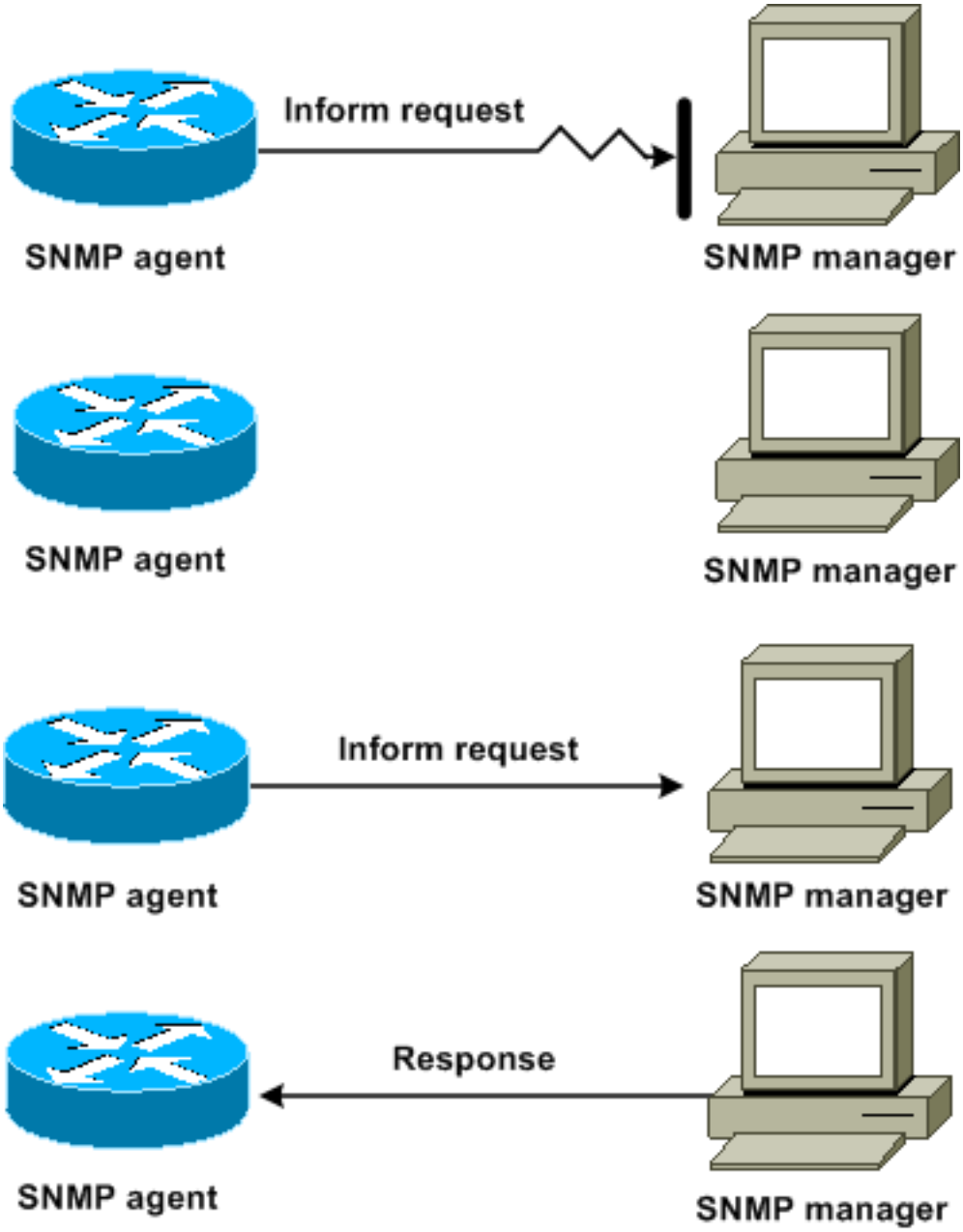


Questo diagramma mostra come il router dell'agente invia correttamente una richiesta di informazione al manager. Quando il responsabile riceve la richiesta di informazioni, invia una risposta all'agente. In questo modo, l'agente sa che la richiesta di informazioni ha raggiunto la destinazione. Si noti che nell'esempio il traffico è il doppio. Ma l'agente sa che il responsabile ha

ricevuto la notifica.



In questo diagramma, l'agente invia una trap al manager, ma la trap non raggiunge il manager. L'agente non ha modo di sapere che la trappola non ha raggiunto la destinazione, quindi la trappola non viene inviata di nuovo. Il manager non riceve mai la trappola.



In questo diagramma, l'agente invia una richiesta di informazioni al responsabile, ma la richiesta di informazioni non raggiunge il responsabile. Poiché il manager non ha ricevuto la richiesta di informazioni, non è disponibile alcuna risposta. Trascorso un determinato periodo di tempo, l'agente invia nuovamente la richiesta di informazioni. La seconda volta, il responsabile riceve la richiesta di informazioni e risponde con una risposta. Nell'esempio viene rilevato maggiore traffico. Ma la notifica raggiunge il programma di gestione SNMP.

Riferimenti MIB e RFC Cisco

I documenti RFC in genere definiscono i moduli MIB. I documenti RFC vengono inviati alla Internet Engineering Task Force (IETF), un organismo internazionale di normalizzazione. Individui o gruppi scrivono le RFC affinché siano prese in considerazione dalla società Internet (ISOC) e dalla comunità Internet nel suo complesso. Per ulteriori informazioni sul processo di standardizzazione e sulle attività dell'IETF, consultare la home page Internet Society . Fare riferimento alla home page dell'IETF per leggere il testo completo di tutte le RFC, le bozze Internet (I-D) e le unità SSD a cui fanno riferimento i documenti Cisco.

L'implementazione Cisco del protocollo SNMP utilizza:

- Le definizioni delle variabili MIB II descritte nella RFC 1213
- Le definizioni delle trap SNMP descritte nella RFC 1215

Cisco fornisce le proprie estensioni MIB private con ogni sistema. I MIB aziendali Cisco sono conformi alle linee guida descritte dalle RFC pertinenti, a meno che la documentazione non indichi diversamente. I file di definizione del modulo MIB e un elenco dei MIB supportati su ciascuna piattaforma Cisco sono disponibili nella home page dei MIB Cisco.

Versioni SNMP

Il software Cisco IOS supporta queste versioni di SNMP:

- SNMPv1: uno standard Internet completo definito dalla RFC 1157 . La RFC 1157 sostituisce le versioni precedenti pubblicate come RFC 1067 e RFC 1098 . La sicurezza è basata sulle stringhe della community.
- SNMPv2c: SNMPv2c è il framework amministrativo basato su stringhe della community per SNMPv2. SNMPv2c (la community c rappresenta) è un protocollo Internet sperimentale definito dalla RFC 1901 , RFC 1905 e RFC 1906 . SNMPv2c è un aggiornamento delle operazioni di protocollo e dei tipi di dati di SNMPv2p (SNMPv2 classico). SNMPv2c utilizza il modello di sicurezza basato sulla community di SNMPv1.
- SNMPv3: SNMPv3 è un protocollo interoperabile basato su standard definito dalla RFC 2273 , RFC 2274 e RFC 2275 . L'SNMPv3 fornisce un accesso sicuro ai dispositivi con una combinazione di autenticazione e crittografia dei pacchetti sulla rete.Le funzioni di sicurezza fornite da SNMPv3 sono:Integrità dei messaggi: assicura che un pacchetto non sia stato manomesso durante la trasmissione.Autenticazione (Authentication) - Determina che il messaggio proviene da un'origine valida.Crittografia: codifica il contenuto di un pacchetto, impedendo il rilevamento da parte di un'origine non autorizzata.

Sia SNMPv1 che SNMPv2c utilizzano una forma di sicurezza basata su community. Un ACL di indirizzo IP e una password definiscono la comunità di manager in grado di accedere al MIB dell'agente.

Il supporto di SNMPv2c include un meccanismo di recupero in blocco e la segnalazione dettagliata dei messaggi di errore alle stazioni di gestione. Il meccanismo di recupero in blocco supporta il recupero di tabelle e di grandi quantità di informazioni, riducendo al minimo il numero di round trip necessari. Il supporto migliorato di SNMPv2c per la gestione degli errori include codici di errore estesi che distinguono i diversi tipi di condizioni di errore. Queste condizioni vengono segnalate tramite un singolo codice di errore in SNMPv1. I codici di errore restituiti ora segnalano il tipo di errore.

L'SNMPv3 fornisce sia modelli di sicurezza che livelli di sicurezza. Un modello di protezione è una strategia di autenticazione impostata per un utente e il gruppo in cui risiede l'utente. Un livello di protezione è il livello di protezione consentito all'interno di un modello di protezione. La combinazione di un modello di sicurezza e di un livello di sicurezza determina il meccanismo di sicurezza da utilizzare quando viene gestito un pacchetto SNMP.

Configurazione generale di SNMP

Per abilitare la gestione SNMP, usare questi comandi su tutti gli switch del cliente:

- Comando per ACL SNMP:
  `Switch(config)#`**`access-list 98 permit`** *`ip_address`*

```
!--- This is the SNMP device ACL.
```

- Comandi SNMP globali:

```
!--- These are sample SNMP community strings. Switch(config)#snmp-server community RO-
community ro 98
snmp-server community RW-community rw 98
snmp-server contact Glen Rahn (Home Number)
snmp-server location text
```

Consigli sulle trap SNMP

L'SNMP è la base per la gestione della rete e viene abilitato e utilizzato su tutte le reti.

Un agente SNMP può comunicare con più manager. Per questo motivo, è possibile configurare il software in modo che supporti le comunicazioni con una stazione di gestione con SNMPv1 e un'altra stazione di gestione con SNMPv2. La maggior parte dei clienti e degli NMS utilizza ancora SNMPv1 e SNMPv2c perché il supporto dei dispositivi di rete SNMPv3 nelle piattaforme NMS è leggermente inferiore.

Abilitare le trap SNMP per tutte le funzionalità in uso. Se lo si desidera, è possibile disattivare altre funzionalità. Dopo aver abilitato una trap, è possibile usare il comando **test snmp** e impostare la gestione appropriata sul server NMS per l'errore. Esempi di tale gestione includono un avviso tramite cercapersone o un popup.

Per impostazione predefinita, tutte le trap sono disattivate. Abilitare tutti i trap sugli switch core, come mostrato nell'esempio:

```
Switch(config)#snmp trap enable
Switch(config)#snmp-server trap-source loopback0
```

Abilitare inoltre i trap delle porte per le porte chiave, ad esempio i collegamenti dell'infrastruttura a router e switch e le porte server chiave. L'abilitazione non è necessaria per altre porte, ad esempio le porte host. Per configurare la porta e abilitare la notifica di collegamento attivo/inattivo, eseguire questo comando:

```
Switch(config-if)#snmp trap link-status
```

Quindi, specificare i dispositivi a cui inviare le trap e agire sui trap in modo appropriato. È ora possibile configurare ciascuna destinazione di trap come destinatario SNMPv1, SNMPv2 o SNMPv3. Per i dispositivi SNMPv3, è possibile inviare informazioni affidabili anziché trap UDP. Questa è la configurazione:

```
Switch(config)#snmp-server host ip_address [traps | informs] [version {1 | 2c | 3}] community-
string
!--- This command needs to be on one line. !--- These are sample host destinations for SNMP
traps and informs. snmp-server host 172.16.1.27 version 2c public
snmp-server host 172.16.1.111 version 1 public
snmp-server host 172.16.1.111 informs version 3 public
snmp-server host 172.16.1.33 public
```

Consigli per il polling SNMP

Accertarsi che questi MIB siano i principali MIB sottoposti a polling o monitoraggio nelle reti del campus:

Nota: questa raccomandazione è del gruppo Cisco Network Management Consulting.

Object Name	Object Description	OID	Period	Max
MIB-II				
SysUpTime	system uptime in 1/100ths of seconds	1.3.6.1.2.1.1.3	5 min	< 30000
CISCO-STACK-MIB				
ChassisPs1status	Status of power supply 1	1.3.6.1.4.1.9.5.1.2.4	10 min	≠ 2
ChassisPs2Status	Status of power supply 2	1.3.6.1.4.1.9.5.1.2.7	10 min	≠ 2
ChassisFanStatus	Status of Chassis Fan	1.3.6.1.4.1.9.5.1.2.9	10 min	≠ 2
ChassisMinorAlarm	Chassis Minor Alarm Status	1.3.6.1.4.1.9.5.1.2.11	10 min	≠ 1
chassis MajorAlarm	Chassis Major Alarm Status	1.3.6.1.4.1.9.5.1.2.12	10 min	≠ 1

Object Name	Object Description	OID	Period	Max
ChassisTempAlarm	Chassis Temperature Alarm status	1.3.6.1.4.1.9.5.1.2.13	10 min	≠ 1
ModuleStatus	Operational Status of the module	1.3.6.1.4.1.9.5.1.3.1.1.10	30 min	≠ 2
CISCO-PROCESS-MIB				
CpmCPUTotal5min	The overall CPU busy percentage in the last 5 minute period. This object deprecates the avgBusy5 object from the OLD-CISCO-SYSTEM-MIB	1.3.6.1.4.1.9.9.109.1.1.1.5	5 min	
CISCO-STACK-MIB				
SysTraffic	% of bandwidth utilization for the previous polling interval	1.3.6.1.4.1.9.5.1.1.8	30 min	

Object Name	Object Description	OID	Period	Max
SysTrafficPeak	Peak traffic meter value since the last time the port counters were cleared or the system started	1.3.6.1.4.1.9.5.1.1.19	30 min	
BRIDGE-MIB				
CiscoEsStackSwitchBufferOverruns	Number of times the switch was out of buffers	1.3.6.1.4.1.9.5.14.2.1.1.17	30 min	

Protocollo orario di rete

Scopo

Il protocollo NTP (Network Time Protocol), RFC 1305 , sincronizza la gestione del tempo tra una serie di server e client distribuiti. L'NTP consente la correlazione degli eventi alla creazione dei registri di sistema e quando si verificano altri eventi specifici dell'ora.

Panoramica operativa

La RFC 958 ha documentato prima l'NTP. Tuttavia, il protocollo NTP si è evoluto attraverso la RFC 1119 (NTP versione 2). La RFC 1305 definisce ora il protocollo NTP, che è alla sua terza versione.

Il protocollo NTP sincronizza l'ora di un client o di un server su un altro server o su un'altra origine dell'ora di riferimento, come una radio, un ricevitore satellitare o un modem. L'NTP fornisce un'accuratezza del client che in genere si trova all'interno di ms sulle LAN e fino a poche decine di ms sulle WAN, rispetto a un server primario sincronizzato. Ad esempio, è possibile utilizzare il protocollo NTP per coordinare l'ora UTC (Coordinated Universal Time) tramite un ricevitore GPS (Global Positioning Service).

Le configurazioni NTP tipiche utilizzano più server ridondanti e percorsi di rete diversi per ottenere un alto livello di accuratezza e affidabilità. Alcune configurazioni includono l'autenticazione crittografica per impedire attacchi accidentali o dannosi al protocollo.

Il protocollo NTP viene eseguito sull'UDP, che a sua volta viene eseguito sull'IP. Tutte le comunicazioni NTP utilizzano l'ora UTC, che corrisponde all'ora di Greenwich.

Attualmente sono disponibili implementazioni NTP versione 3 (NTPv3) e NTP versione 4 (NTPv4).

L'ultima versione software su cui si sta lavorando è NTPv4, ma lo standard Internet ufficiale è ancora NTPv3. Inoltre, alcuni fornitori di sistemi operativi personalizzano l'implementazione del protocollo.

Salvaguardie NTP

L'implementazione NTP tenta anche di evitare la sincronizzazione con un computer in cui l'ora non può essere accurata. NTP esegue questa operazione in due modi:

- NTP non esegue la sincronizzazione con un computer non sincronizzato.
- L'NTP confronta sempre l'ora riportata da diverse macchine e non si sincronizza con una macchina su cui l'ora è significativamente diversa dalle altre, anche se quella macchina ha uno strato inferiore.

Associazioni

Le comunicazioni tra computer che eseguono NTP, note come associazioni, sono in genere configurate in modo statico. A ogni computer vengono assegnati gli indirizzi IP di tutti i computer con cui è necessario creare associazioni. L'accurata temporizzazione è possibile grazie allo scambio di messaggi NTP tra ogni coppia di macchine con un'associazione. Tuttavia, in un ambiente LAN, è possibile configurare il protocollo NTP in modo che utilizzi i messaggi broadcast IP. Con questa alternativa, è possibile configurare il computer per l'invio o la ricezione di messaggi broadcast, ma l'accuratezza della memorizzazione dei tempi viene ridotta marginalmente in quanto il flusso di informazioni è unidirezionale.

Se la rete è isolata da Internet, l'implementazione NTP di Cisco consente di configurare un computer in modo che agisca come se fosse sincronizzato con l'uso di NTP, quando in realtà ha determinato l'ora con l'uso di altri metodi. Altre macchine si sincronizzano con quella macchina con l'uso di NTP.

Un'associazione NTP può essere:

- Associazione peerQuesto significa che il sistema può eseguire la sincronizzazione con l'altro sistema o consentire all'altro sistema di eseguire la sincronizzazione con esso.
- Associazione serverCiò significa che solo questo sistema esegue la sincronizzazione con l'altro sistema. L'altro sistema non esegue la sincronizzazione con questo sistema.

Per formare un'associazione NTP con un altro sistema, utilizzare uno dei seguenti comandi in modalità di configurazione globale:

Comando	Scopo
indirizzo ip **peer ntp [normal-sync]** *[numero* **versione] [key** *key-id]* **[source** *interface]* **[preferisci]**	Crea un'associazione peer con un altro sistema
indirizzo-ip **server ntp [***numero* **versione]** *[id-chiave]* **[***interfaccia* **di origine] [preferisci]**	Crea un'associazione tra un server e un altro sistema

Nota: è necessario configurare una sola estremità di un'associazione. L'altro sistema stabilisce automaticamente l'associazione.

Accesso ai server di riferimento orario pubblico

La subnet NTP attualmente include oltre 50 server primari pubblici sincronizzati direttamente con UTC via radio, satellite o modem. In genere, le workstation client e i server con un numero relativamente ridotto di client non vengono sincronizzati con i server principali. Esistono circa 100 server secondari pubblici sincronizzati con i server primari. Questi server consentono la sincronizzazione di oltre 100.000 client e server su Internet. La pagina Server NTP pubblici gestisce gli elenchi correnti e viene aggiornata di frequente.

Inoltre, esistono numerosi server primari e secondari privati che normalmente non sono disponibili al pubblico. Per un elenco dei server NTP pubblici e informazioni su come utilizzarli, fare riferimento a The Network Time Protocol Project (Università del Delaware). Non vi è alcuna garanzia che questi server NTP Internet pubblici siano disponibili e producano l'ora corretta. Pertanto, è necessario considerare altre opzioni. Ad esempio, utilizzare vari dispositivi GPS autonomi collegati direttamente a un certo numero di router.

Un'altra opzione è l'uso di vari router, impostati come master Stratum 1. Tuttavia, non è consigliabile utilizzare un router di questo tipo.

Strato

NTP utilizza uno strato per descrivere il numero di hop NTP che si trovano lontano da una macchina da una fonte temporale autorevole. Un server di riferimento ora di strato 1 ha un orologio radio o atomico collegato direttamente. Un server di riferimento ora di strato 2 riceve l'ora da un server di riferimento ora di strato 1 e così via. Un computer che esegue NTP sceglie automaticamente come origine del tempo il computer con il numero di strato più basso con il quale è configurato per comunicare attraverso NTP. Questa strategia consente di creare in modo efficace una struttura auto-organizzante di altoparlanti NTP.

Il protocollo NTP evita la sincronizzazione con un dispositivo su cui l'ora potrebbe non essere precisa. Per ulteriori informazioni, vedere la sezione *Salvaguardie NTP* di Network Time Protocol.

Relazione peer server

- Un server risponde alle richieste del client ma non tenta di incorporare informazioni sulla data da un'origine ora del client.
- Un peer risponde alle richieste del client e tenta di utilizzare la richiesta del client come potenziale candidato per una fonte di tempo migliore e per aiutare a stabilizzare la sua frequenza di clock.
- Per essere veri peer, entrambi i lati della connessione devono entrare in una relazione peer, anziché in una situazione in cui un utente funge da peer e l'altro da server. Chiedere ai peer di scambiare le chiavi in modo che solo gli host attendibili possano comunicare con altri come peer.
- In una richiesta client a un server, il server risponde al client e dimentica che il client ha posto una domanda.
- In una richiesta client a un peer, il server risponde al client. Il server conserva le informazioni sullo stato relative al client in modo da tenere traccia delle prestazioni del client durante la gestione dei tempi e dello strato server in cui viene eseguito il client.

Un server NTP può gestire migliaia di client senza alcun problema. Ma quando un server NTP gestisce più di pochi client (fino a poche centinaia), la capacità del server di conservare le informazioni sullo stato ha un impatto sulla memoria. Quando un server NTP gestisce una quantità

di risorse superiore a quella consigliata, vengono utilizzate più risorse CPU e larghezza di banda.

Modalità di comunicazione con il server NTP

Per comunicare con il server, è possibile utilizzare due modalità distinte:

- Modalità di trasmissione
- Modalità client/server

In modalità di trasmissione, i client sono in ascolto. In modalità client/server, i client eseguono il polling del server. È possibile utilizzare la trasmissione NTP se non è coinvolto alcun collegamento WAN a causa della sua velocità. Per attraversare un collegamento WAN, usare la modalità client/server (tramite polling). La modalità di trasmissione è progettata per una rete LAN, in cui molti client possono avere la necessità di eseguire il polling del server. Senza la modalità di trasmissione, tale polling può generare un numero elevato di pacchetti sulla rete. Il multicast NTP non è ancora disponibile in NTPv3, ma è disponibile in NTPv4.

Per impostazione predefinita, il software Cisco IOS comunica con l'utilizzo di NTPv3. Tuttavia, il software è compatibile con le versioni precedenti di NTP.

Sondaggio

Il protocollo NTP consente a un client di eseguire query su un server in qualsiasi momento.

Quando si configura NTP per la prima volta in una scatola Cisco, NTP invia otto query in rapida successione a intervalli `NTP_MINPOLL` (2^4=16 sec). `NTP_MAXPOLL` è di 2^14 secondi (16.384 sec o 4 ore, 33 min, 4 sec). Questo periodo di tempo è il più lungo prima che l'NTP esegua un nuovo sondaggio per ottenere una risposta. Al momento, Cisco non dispone di un metodo per consentire all'utente di forzare manualmente il tempo `POLL`.

Il contatore di polling NTP inizia a 2^6 (64) sec, o 1 min, 4 sec. Questo intervallo di tempo viene incrementato di 2 unità, man mano che i due server si sincronizzano tra loro, a 2^10. È possibile prevedere che i messaggi di sincronizzazione vengano inviati a un intervallo di 64, 128, 256, 512 o 1024 secondi, in base alla configurazione del server o del peer. Il tempo maggiore tra i sondaggi si verifica quando l'orologio corrente diventa più stabile a causa dei loop bloccati per fase. I loop bloccati a fasi tagliano il cristallo dell'orologio locale, fino a 1024 secondi (17 min).

Il tempo varia tra 64 secondi e 1024 secondi come potenza di 2 (che equivale a una volta ogni 64, 128, 256, 512 o 1024 secondi). Il tempo si basa sul loop a blocco di fase che invia e riceve i pacchetti. Se nel tempo c'è molta confusione, il sondaggio si verifica più spesso. Se l'orologio di riferimento è preciso e la connettività di rete è costante, i tempi di polling convergono su 1024 secondi tra ogni polling.

L'intervallo di polling NTP cambia quando cambia la connessione tra il client e il server. Con una connessione migliore, l'intervallo di polling è più lungo. In questo caso, una connessione migliore significa che il client NTP ha ricevuto otto risposte per le ultime otto richieste. L'intervallo di polling viene quindi raddoppiato. In caso di mancata risposta singola, l'intervallo di polling viene dimezzato. L'intervallo di polling inizia a 64 secondi e arriva a un massimo di 1024 secondi. Nelle migliori circostanze, il tempo necessario per passare da 64 secondi a 1024 secondi per l'intervallo di polling è leggermente superiore a 2 ore.

Trasmissioni

Le trasmissioni NTP non vengono mai inoltrate. Se si usa il comando **ntp broadcast**, il router inizia a generare i broadcast NTP sull'interfaccia su cui è configurato.

In genere, si usa il comando **ntp broadcast** per inviare i broadcast NTP su una LAN in modo da servire le stazioni terminali client e i server.

Sincronizzazione ora

La sincronizzazione di un client con un server prevede diversi scambi di pacchetti. Ogni scambio è una coppia richiesta/risposta. Quando un client invia una richiesta, la sua ora locale viene memorizzata nel pacchetto inviato. Quando un server riceve il pacchetto, memorizza la propria stima dell'ora corrente nel pacchetto e il pacchetto viene restituito. Quando riceve la risposta, il destinatario registra nuovamente il proprio tempo di ricezione per stimare il tempo di viaggio del pacchetto.

Queste differenze di tempo possono essere utilizzate per stimare il tempo necessario per la trasmissione del pacchetto dal server al richiedente. Il tempo di ritorno è preso in considerazione per una stima del tempo corrente. Più breve è il tempo di ritorno, più accurata è la stima del tempo corrente.

L'ora viene accettata solo dopo che si sono verificati diversi scambi di pacchetti. Alcuni valori essenziali vengono inseriti nei filtri multistadio per valutare la qualità dei campioni. In genere, sono necessari circa 5 minuti per la sincronizzazione di un client NTP con un server. È interessante notare che questo vale anche per gli orologi di riferimento locali che non hanno alcun ritardo per definizione.

Inoltre, la qualità della connessione di rete influenza anche la precisione finale. Reti lente e imprevedibili con ritardi variabili hanno un effetto negativo sulla sincronizzazione dell'ora.

Per la sincronizzazione NTP è necessario uno scarto temporale inferiore a 128 ms. La precisione tipica su Internet varia da circa 5 ms a 100 ms, che può variare con i ritardi di rete.

Livelli di traffico NTP

La larghezza di banda utilizzata dall'NTP è minima. L'intervallo tra i messaggi di polling scambiati dai peer viene in genere riconvertito a non più di un messaggio ogni 17 minuti (1024 secondi). Con un'attenta pianificazione, è possibile gestire questo problema all'interno delle reti di router sui collegamenti WAN. Avere i client NTP in corrispondenza dei server NTP locali e non in tutta la WAN fino ai router centrali del sito, che sono i server Stratum 2.

Un client NTP convergente utilizza medie di circa 0,6 bit al secondo (bps) per server.

Raccomandazione Cisco NTP

- Cisco consiglia di utilizzare più server di riferimento ora e percorsi di rete diversi per ottenere un alto livello di accuratezza e affidabilità. Alcune configurazioni includono l'autenticazione crittografica per impedire attacchi accidentali o dannosi al protocollo.
- In base all'RFC, l'NTP è stato progettato per consentire il polling di diversi server di riferimento orario e l'utilizzo di complesse analisi statistiche per ottenere un periodo di tempo valido, anche se non si è certi che tutti i server sottoposti a polling siano autorevoli. NTP stima gli errori di tutti gli orologi. Pertanto, tutti i server NTP restituiscono il tempo insieme a una stima

dell'errore corrente. Quando si utilizzano più server di riferimento orario, NTP desidera anche che questi server concordino un certo tempo.

- L'implementazione Cisco di NTP non supporta il servizio di strato 1. Non è possibile connettersi a una radio o a un orologio atomico. Cisco consiglia di derivare il servizio Ora per la rete dai server NTP pubblici disponibili su Internet IP.
- Consente a tutti gli switch client di inviare regolarmente richieste relative all'ora del giorno a un server NTP. È possibile configurare fino a 10 indirizzi server/peer per client in modo da ottenere una sincronizzazione rapida.
- Per ridurre il sovraccarico del protocollo, i server secondari distribuiscono il tempo tramite NTP agli host di rete locale rimanenti. Per garantire affidabilità, è possibile dotare gli host selezionati di orologi meno precisi ma meno costosi da utilizzare per il backup in caso di guasto dei server principale e/o secondario o dei percorsi di comunicazione tra di essi.
- **ntp update-calendar**: NTP in genere modifica solo l'orologio di sistema. Questo comando consente a NTP di aggiornare le informazioni di data e ora nel calendario. L'aggiornamento viene eseguito solo se l'ora NTP è sincronizzata. In caso contrario, il calendario mantiene la propria ora e non è influenzato dall'ora NTP o dall'orologio di sistema. Utilizzare sempre questa opzione sui router di fascia alta.
- **clock calendar-valid**: questo comando dichiara che le informazioni del calendario sono valide e sincronizzate. Utilizzare questa opzione sul master NTP. Se non è configurata, il router di fascia alta con il calendario continua a ritenere che l'ora sia non autorevole, anche se dispone della linea master NTP.
- Qualsiasi numero di strato superiore a 15 è considerato non sincronizzato. Per questo motivo, lo strato 16 viene visualizzato nell'output del comando **show ntp status** sui router per cui gli orologi non sono sincronizzati. Se il dispositivo master è sincronizzato con un server NTP pubblico, verificare che il numero di strato sulla linea master NTP sia superiore di uno o due al numero di strato più alto sui server pubblici su cui si esegue il polling.
- Molti clienti hanno configurato il protocollo NTP in modalità server sulle piattaforme software Cisco IOS, sincronizzato da diversi feed affidabili provenienti da Internet o da un orologio radio. Internamente, un'alternativa più semplice alla modalità server quando si aziona un gran numero di switch è abilitare il protocollo NTP in modalità broadcast sulla VLAN di gestione in un dominio commutato. Questo meccanismo consente a Catalyst di ricevere un orologio da singoli messaggi broadcast. Tuttavia, l'accuratezza del controllo dei tempi è marginalmente ridotta perché il flusso di informazioni è unidirezionale.
- Anche l'utilizzo degli indirizzi di loopback come origine degli aggiornamenti può contribuire alla coerenza. È possibile risolvere i problemi di sicurezza in due modi:Con il controllo degli aggiornamenti del server, come consigliato da CiscoPer autenticazione

Comandi di configurazione globale NTP

```
!--- For the client: clock timezone EST  -5  ????
ntp source loopback 0 ?????
ntp server ip_address key 1
ntp peer ip_address
!--- This is for a peer association. ntp authenticate
ntp authentication-key 1 md5 xxxx
ntp trusted-key 1

!--- For the server: clock timezone EST -5
clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00
clock calendar-valid
```

```
ntp source loopback0
ntp update-calendar

!--- This is optional: interface vlan_id ntp broadcast
!--- This sends NTP broadcast packets. ntp broadcast client
!--- This receives NTP broadcast packets. ntp authenticate
ntp authentication-key 1 md5 xxxxx
ntp trusted-key 1
ntp access-group access-list
!--- This provides further security, if needed.
```

Comando di stato NTP

```
show ntp status

Clock is synchronized, stratum 8, reference is 127.127.7.1
nominal freq is 250.0000 Hz, actual freq is 249.9974 Hz, precision is 2**18
reference time is C6CF0C30.980CCA9D (01:34:00.593 IST Mon Sep 12 2005)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.02 msec, peer dispersion is 0.02 msec
```

Questo è l'indirizzo dell'orologio di riferimento per il router Cisco quando il router funge da master NTP. Se il router non è stato sincronizzato con alcun server NTP, utilizza questo indirizzo come ID di riferimento. Per ulteriori informazioni sulla configurazione e sui comandi, consultare la sezione *Configurazione del protocollo NTP* in Esecuzione della gestione di base del sistema.

Protocollo Cisco Discovery

Scopo

Il CDP è eseguito sul layer 2 (livello di collegamento dati) su tutti i router, i bridge, i server di accesso e gli switch Cisco. Il CDP consente alle applicazioni di gestione della rete di individuare i dispositivi Cisco adiacenti a dispositivi già noti. In particolare, le applicazioni di gestione della rete possono rilevare i router adiacenti che eseguono protocolli trasparenti di livello inferiore. Con il CDP, le applicazioni di gestione della rete possono imparare il tipo di dispositivo e l'indirizzo dell'agente SNMP dei dispositivi adiacenti. Questa funzionalità consente alle applicazioni di inviare query SNMP a dispositivi adiacenti.

I comandi **show** associati alla funzione CDP consentono al tecnico di rete di determinare le seguenti informazioni:

- Numero di modulo/porta di altri dispositivi abilitati per CDP adiacenti
- Questi indirizzi del dispositivo adiacente:Indirizzo MACIndirizzo IPIndirizzo del canale della porta
- La versione software del dispositivo adiacente
- Queste informazioni sul dispositivo adiacente:SpeedDuplexDominio VTPImpostazione VLAN nativa

La sezione Panoramica operativa evidenzia alcuni dei miglioramenti apportati a CDP versione 2 (CDPv2) rispetto a CDP versione 1 (CDPv1).

Panoramica operativa

Il CDP viene eseguito su tutti i supporti LAN e WAN che supportano SNAP.

Ogni dispositivo configurato per CDP invia messaggi periodici a un indirizzo multicast. Ogni dispositivo annuncia almeno un indirizzo al quale può ricevere messaggi SNMP. Gli annunci contengono anche informazioni sul tempo di riproduzione. Queste informazioni indicano il periodo di tempo che un dispositivo ricevente impiega per conservare le informazioni CDP prima di eliminarle.

Il CDP utilizza l'incapsulamento SNAP con codice di tipo 2000. Su Ethernet, ATM e FDDI, viene utilizzato l'indirizzo multicast di destinazione 01-00-0c-cc-cc-cc. Sui Token Ring, viene utilizzato l'indirizzo funzionale c000.0800.0000. I frame CDP vengono inviati periodicamente ogni minuto.

I messaggi CDP contengono uno o più messaggi che consentono al dispositivo di destinazione di raccogliere e archiviare informazioni su ogni dispositivo adiacente.

Questa tabella fornisce i parametri supportati da CDPv1:

Parametro	Tipo	Descrizione
1	ID dispositivo	Nome host del dispositivo o numero di serie hardware in ASCII
2	Indirizzo	Indirizzo di layer 3 dell'interfaccia che invia l'aggiornamento
3	ID porta	Porta a cui viene inviato l'aggiornamento CDP
4	Funzionalità	Descrive le funzionalità del dispositivo nel modo seguente: • Router: 0x01 • Ponte SR[1]: 0x04 • Interruttore: 0x08 (fornisce switching di livello 2 e/o 3) • Host: 0x10 • Filtro condizionale IGMP: 0x20 • Il bridge o lo switch non inoltrano pacchetti di report IGMP su porte non router.
5	Version	Stringa di caratteri contenente la versione del software **Nota:** l'output del comando **show version** mostra le stesse informazioni.
6	Piattaforma	La piattaforma hardware, ad esempio WS-C5000, WS-C6009 e Cisco RSP[2]

[1] SR = source-route.

[2] RSP = Route Switch Processor.

In CDPv2 sono stati introdotti ulteriori valori TLV (Type, Length, Value) per il tipo e la lunghezza.

CDPv2 supporta qualsiasi TLV. Tuttavia, questa tabella fornisce i parametri che possono essere particolarmente utili negli ambienti a commutazione e che vengono utilizzati dal software Catalyst.

Quando uno switch esegue CDPv1, perde i frame CDPv2. Quando uno switch esegue CDPv2 e riceve un frame CDPv1 su un'interfaccia, inizia a inviare i frame CDPv1 fuori dall'interfaccia, oltre ai frame CDPv2.

Parametro	Tipo	Descrizione
9	Dominio VTP	Il dominio VTP, se configurato sul dispositivo
10	VLAN nativa	In dot1q, i frame della VLAN in cui si trova la porta se non è in corso il trunking, rimangono senza tag. Questa VLAN è in genere chiamata VLAN nativa.
11	Full/Half Duplex	Questo TLV contiene l'impostazione duplex della porta di invio.
14	Appliance VLAN-ID	Consente di distinguere il traffico VoIP da altro traffico tramite un ID VLAN separato (VLAN ausiliaria).
16	Consumo	Quantità massima di energia che si prevede verrà consumata, in mW, dal dispositivo connesso.
17	MTU	L'MTU dell'interfaccia con cui viene trasmesso il frame CDP.
18	Trust esteso	Indica che la porta è in modalità di attendibilità estesa.
19	COS per porte non attendibili	Valore CoS (Class of Service) da utilizzare per contrassegnare tutti i pacchetti ricevuti sulla porta non attendibile di un dispositivo di commutazione connesso.
20	NomeSistema	Nome di dominio completo del dispositivo (0, se sconosciuto).
25	Alimentazione richiesta	Trasmesso da un dispositivo di alimentazione per negoziare un livello di alimentazione adeguato.
26	Alimentazione disponibile	Trasmesso da un commutatore. Consente a un dispositivo alimentato di negoziare e selezionare un'impostazione di risparmio energia appropriata.

CDPv2/Power over Ethernet

Alcuni switch, come Catalyst 6500/6000 e 4500/4000, sono in grado di fornire alimentazione

tramite cavi UTP (unshielded twisted pair) a dispositivi alimentabili. Le informazioni ricevute tramite CDP (parametri 16, 25, 26) aiutano a ottimizzare la gestione dell'alimentazione dello switch.

Interazione CDPv2/Cisco IP Phone

I telefoni IP Cisco forniscono connettività per un dispositivo Ethernet 10/100-Mbps collegato esternamente. La connettività è resa possibile dall'integrazione di uno switch interno di layer 2 a tre porte nel telefono IP. Le porte dello switch interno sono indicate come:

- P0 (dispositivo telefonico IP interno)
- P1 (porta esterna 10/100 Mbps)
- P2 (porta esterna 10/100 Mbps che si connette allo switch)

Se si configurano le porte trunk di accesso dot1q, è possibile trasferire il traffico vocale su una VLAN separata sulla porta dello switch. Questa VLAN aggiuntiva è nota come VLAN ausiliaria (CatOS) o vocale (software Cisco IOS). Di conseguenza, il traffico contrassegnato con il punto1q proveniente dal telefono IP può essere inviato sulla VLAN ausiliaria/vocale e il traffico non contrassegnato può essere inviato tramite la porta esterna 10/100 Mbps del telefono tramite la VLAN di accesso.

Gli switch Catalyst possono informare un telefono IP dell'ID della VLAN vocale tramite CDP (parametro 14: Appliance VLAN-ID (TLV). Di conseguenza, il telefono IP contrassegna tutti i pacchetti relativi al VoIP con l'ID VLAN appropriato e con priorità 802.1p. Questo TLV CDP viene utilizzato anche per identificare se un telefono IP è collegato tramite il parametro ID accessorio.

Questo concetto può essere utilizzato quando si sviluppa una policy QoS. È possibile configurare lo switch Catalyst in modo che interagisca con il telefono IP in tre modi:

- Considera attendibile dispositivo Cisco IP PhoneConsidera attendibile il CoS solo quando viene rilevato un telefono IP tramite CDP. Quando viene rilevato un telefono IP tramite il parametro CDP-14, lo stato di attendibilità della porta viene impostato su Trust COS. Se non viene rilevato alcun telefono IP, la porta è non attendibile.
- Trust estesoLo switch può informare il telefono IP tramite CDP (parametro 18) in modo da considerare attendibili tutti i frame ricevuti sulla porta del dispositivo esterno a 10/100 Mbps.
- Riscrittura COS per porte non attendibiliLo switch può informare il telefono IP tramite CDP (parametro 19) per riscrivere i valori CoS 802.1p ricevuti sulla porta del dispositivo esterno da 10/100 Mbps.**Nota:** per impostazione predefinita, tutto il traffico ricevuto sulle porte 10/100-Mbps esterne del telefono IP è considerato non attendibile.

Nota: Questa è una configurazione di esempio per connettere un telefono IP non Cisco a uno switch.

Nota: Ad esempio,

```
Switch(config)#interface gigabitEthernet 2/1
Switch(config-if)#switchport mode trunk

!--- For example use VLAN 30 for voice VLAN, and VLAN 10 for access VLAN. Switch(config-
if)#switchport trunk native vlan 10
Switch(config-if)#switchport trunk allow vlan 10,30
Switch(config-if)#switchport voice vlan 30
Switch(config-if)#spanning-tree portfast trunk
```

```
!--- And besides that enable LLDP as Non Cisco IP Phone do not use CDP. Switch(config)#lldp run
```

Consiglio di configurazione Cisco

Le informazioni fornite dal CDP possono essere estremamente utili per la risoluzione dei problemi di connettività di layer 2. Abilitare CDP su tutti i dispositivi che supportano il funzionamento. Utilizzare i seguenti comandi:

- Per abilitare il CDP a livello globale sullo switch:
  ```
  Switch(config)#cdp run
  ```
- Per abilitare il CDP per ciascuna porta:
  ```
  Switch(config)#interface type slot#/port#
  Switch(config-if)#cdp enable
  ```

Elenco di controllo della configurazione

Comandi globali

Accedere, abilitare e accedere alla modalità di configurazione globale per avviare il processo di configurazione dello switch.

```
Switch>enable
Switch#
Switch#configure terminal
Switch(Config)#
```

Comandi globali generici (a livello aziendale)

In questa sezione Comandi globali vengono elencati i comandi globali da applicare a tutti gli switch della rete aziendale del cliente.

Questa configurazione contiene i comandi globali consigliati da aggiungere alla configurazione iniziale. È necessario modificare i valori nell'output prima di copiare e incollare il testo nella CLI. Per applicare la configurazione globale, eseguire questi comandi:

```
vtp domain domain_name
vtp mode transparent
spanning-tree portfast bpduguard
spanning-tree etherchannel guard misconfig
cdp run
no service pad
service password-encryption
enable secret password
clock timezone EST -5
clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00
clock calendar-valid
ip subnet-zero
ip host tftpserver your_tftp_server
ip domain-name domain_name
ip name-server name_server_ip_address
```

```
ip name-server name_server_ip_address
ip classless
no ip domain-lookup
no ip http server
no logging console
no logging monitor
logging buffered 16384
logging trap notifications
logging facility local7
logging syslog_server_ip_address
logging syslog_server_ip_address
logging source-interface loopback0
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
access-list 98 permit host_ip_address_of_primary_snmp_server
access-list 98 permit host_ip_address_of_secondary_snmp_server
snmp-server community public ro 98
snmp-server community laneng rw 98
snmp-server enable traps entity
snmp-server host host_address traps public
snmp-server host host_address traps public
banner motd ^CCCCC

This is a proprietary system, NOT for public or personal use.  All work products,
communications, files, data or information directly or indirectly created, input
or accessed on this system are and shall become the sole property of the company.
This system is actively monitored and accessed by the company.  By logging onto
this system, the user consents to such monitoring and access.

USE OF THIS SYSTEM WITHOUT OR IN EXCESS OF THE PROPER AUTHORIZATION MAY SUBJECT
THE USER TO DISCIPLINE AND/OR CIVIL AND CRIMINAL PENALTIES

^C
line console 0
exec-timeout 0 0
password cisco
login
transport input none
line vty 0 4
exec-timeout 0 0
password cisco
login
length 25
clock calendar-valid
ntp server ntp_server_ip_address
ntp server ntp_server_ip_address
ntp update-calendar
```

Comandi globali specifici per ogni chassis dello switch

I comandi globali illustrati in questa sezione sono specifici per ogni chassis di switch installato nella rete.

Variabili di configurazione specifiche dello chassis

Per impostare la data e l'ora, utilizzare questo comando:

```
Switch#clock set hh:mm:ss day month year
```

Per impostare il nome host del dispositivo, utilizzare i seguenti comandi:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Cat6500
```

Per configurare l'interfaccia di loopback per la gestione, eseguire questi comandi:

```
CbrCat6500(config)#interface loopback 0
Cat6500(config-if)#description Cat6000 - Loopback address and Router ID
Cat6500(config-if)#ip address ip_address subnet_mask
Cat6500(config-if)#exit
```

Per visualizzare la revisione del software Cisco IOS Supervisor Engine, eseguire questi comandi:

```
Cbrcat6500#show version | include IOS
IOS (tm) MSFC Software (C6MSFC-DSV-M), Version 12.1(13)E9, EARLY DEPLOYMENT RELE
ASE SOFTWARE (fc1)
cat6500#
```

Per visualizzare la revisione del file di avvio dell'MSFC, eseguire questo comando:

```
Cat6500#dir bootflash:
Directory of bootflash:/
 1 -rw- 1879040 Aug 19 2003 19:03:29 c6msfc-boot-mz.121-19.E1a

15990784 bytes total (14111616 bytes free
```

Per specificare le informazioni di contatto e il percorso del server SNMP, eseguire questi comandi:

```
Cat6500(config)#snmp-server contact contact_information
Cat6500(config)#snmp-server location location_of_device
```

Per copiare la configurazione di avvio da un Supervisor Engine esistente a un nuovo Supervisor Engine, potrebbe verificarsi una perdita di configurazione, ad esempio la configurazione sulle interfacce del Supervisor Engine esistente. Cisco consiglia di copiare la configurazione in un file di testo e incollarla in segmenti nella console per verificare se si sono verificati problemi di configurazione.

Comandi di interfaccia

Tipi di porte funzionali Cisco

Nel software Cisco IOS, le porte degli switch sono definite interfacce. Il software Cisco IOS dispone di due tipi di modalità di interfaccia:

- Interfaccia di routing di layer 3
- Interfaccia switch di livello 2

La funzione di interfaccia fa riferimento alla configurazione della porta. La configurazione della porta può essere:

- Interfaccia di routing
- Interfaccia virtuale commutata (SVI)
- Porta di accesso
- Trunk
- EtherChannel
- Una combinazione di questi

Il tipo di interfaccia fa riferimento a un tipo di porta. Il tipo di porta può essere uno dei seguenti:

- FE
- GE
- Port-channel

Di seguito vengono descritte brevemente le diverse funzioni dell'interfaccia del software Cisco IOS:

- Interfaccia fisica di routing (predefinita) - Per impostazione predefinita, ogni interfaccia dello switch è un'interfaccia di routing di layer 3, simile a qualsiasi router Cisco. L'interfaccia instradata deve trovarsi su una subnet IP univoca.
- Access switch port interface: questa funzione viene utilizzata per posizionare le interfacce nella stessa VLAN. Le porte devono essere convertite da un'interfaccia di routing a un'interfaccia di commutazione.
- SVI: è possibile associare una SVI a una VLAN che contiene le porte dello switch di accesso per il routing tra VLAN. Configurare la SVI in modo che sia associata a una VLAN quando si desidera un percorso o un bridge tra le porte dello switch di accesso su VLAN diverse.
- Interfaccia porta switch trunk: questa funzione viene utilizzata per trasportare più VLAN su un altro dispositivo. Le porte devono essere convertite da un'interfaccia di routing a una porta dello switch trunk.
- EtherChannel: EtherChannel viene utilizzato per raggruppare le singole porte in un'unica porta logica per la ridondanza e il bilanciamento del carico.

Suggerimenti per il tipo di porta funzionale Cisco

Utilizzare le informazioni di questa sezione per determinare i parametri da applicare alle interfacce.

Nota: ove possibile, vengono incorporati alcuni comandi specifici dell'interfaccia.

Negoziazione automatica

Non utilizzare la negoziazione automatica in una di queste situazioni:

- Per porte che supportano dispositivi dell'infrastruttura di rete quali switch e router
- Per altri sistemi finali non transitori, quali server e stampanti

Configurare manualmente la velocità e la modalità duplex in base alle configurazioni dei collegamenti a 10/100 Mbps. Le configurazioni sono in genere full-duplex a 100 Mbps:

- Collegamento switch-to-switch da 100 MB
- Collegamento switch-server da 100 MB
- Collegamento da switch a router da 100 MB

Èpossibile configurare queste impostazioni nel modo seguente:

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#speed 100
Cat6500(config-if)#duplex full
```

Cisco consiglia configurazioni di collegamento a 10/100 Mbps per gli utenti finali. I lavoratori mobili e gli host temporanei devono eseguire la negoziazione automatica, come mostrato nell'esempio seguente:

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#speed auto
```

Il valore predefinito sulle interfacce Gigabit è la `negoziazione automatica`. Tuttavia, eseguire questi comandi per verificare che la negoziazione automatica sia abilitata. Cisco consiglia di abilitare la negoziazione Gigabit:

```
Cat6500(config-if)#interface gigabitethernet mod#/port#
Cat6500(config-if)#no speed
```

Spanning Tree Root

In considerazione della progettazione della rete, identificare lo switch che meglio si adatta a fungere da root per ciascuna VLAN. In genere, è possibile scegliere uno switch potente al centro della rete. Posizionare il bridge radice al centro della rete e collegarlo direttamente ai server e ai router. Questa configurazione in genere riduce la distanza media tra i client, i server e i router. Per ulteriori informazioni, vedere Considerazioni sul protocollo Spanning Tree e sulla progettazione correlata.

Per fare in modo che uno switch sia la radice di una VLAN designata, eseguire questo comando:

```
Cat6500(config)#spanning-tree vlan vlan_id root primary
```

Spanning Tree PortFast

PortFast ignora il normale funzionamento dello Spanning Tree sulle porte di accesso per accelerare i ritardi di connettività iniziali che si verificano quando le stazioni terminali sono collegate a uno switch. Per ulteriori informazioni su PortFast, fare riferimento a Uso di PortFast e di altri comandi per risolvere i ritardi della connettività di avvio della workstation.

Impostare STP PortFast su on per tutte le porte di accesso abilitate connesse a un singolo host. Questo è un esempio:

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
```

```
 Use with CAUTION
%Portfast has been configured on FastEthernet3/1 but will only have effect
when the interface is in a non-trunking mode.
```

UDLD

Abilitare il protocollo UDLD solo sulle porte dell'infrastruttura connesse in fibra ottica o sui cavi Ethernet in rame per monitorare la configurazione fisica dei cavi. Per abilitare il protocollo UDLD, eseguire questi comandi:

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#udld enable
```

Informazioni sulla configurazione della VLAN

Configurare le VLAN con questi comandi:

```
Cat6500(config)#vlan vlan_number
Cat6500(config-vlan)#name vlan_name
Cat6500(config-vlan)#exit
Cat6500(config)#spanning-tree vlan vlan_id
Cat6500(config)#default spanning-tree vlan vlan_id
```

Ripetere i comandi per ciascuna VLAN, quindi uscire. Immettere questo comando

```
Cat6500(config)#exit
```

Per verificare tutte le VLAN, usare questo comando:

```
Cat6500#show vlan
```

SVI con routing

Configurare le SVI per il routing tra VLAN. Utilizzare i seguenti comandi:

```
Cat6500(config)#interface vlan vlan_id
Cat6500(config-if)#ip address svi_ip_address subnet_mask
Cat6500(config-if)#description interface_description
Cat6500(config-if)#no shutdown
```

Ripetere questi comandi per ciascuna funzione di interfaccia che contiene una SVI indirizzata, quindi uscire. Immettere questo comando

```
Cat6500(config-if)#^Z
```

Interfaccia fisica singola con routing

Per configurare l'interfaccia di layer 3 con routing predefinito, eseguire questi comandi:

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#ip address ip_address subnet_mask
Cat6500(config-if)#description interface_description
```

Ripetere questi comandi per ogni funzione di interfaccia che contiene un'interfaccia fisica di routing, quindi uscire. Immettere questo comando

```
Cat6500(config-if)#^Z
```

L3 (Routed EtherChannel)

Per configurare EtherChannel sulle interfacce di layer 3, eseguire i comandi descritti in questa sezione.

Configurare un'interfaccia canale porta logica nel modo seguente:

```
Cat6500(config)#interface port-channel port_channel_interface_#
Cat6500(config-if)#description port_channel_description
Cat6500(config-if)#ip address port_channel_ip_address subnet_mask
Cat6500(config-if)#no shutdown
```

Eseguire la procedura descritta in questa sezione per le porte che formano quel particolare canale. Applicare le informazioni rimanenti al canale della porta, come mostrato nell'esempio:

```
Cat6500(config)#interface range [type] mod/port_range
Cat6500(config-if)#channel-group 1-64 mode [active | auto | desirable | on | passive]
Cat6500(config-if)#no shutdown
Cat6500(config-if)#^Z
```

Nota: dopo aver configurato EtherChannel, la configurazione applicata all'interfaccia del canale della porta influisce su EtherChannel. La configurazione applicata alle porte LAN ha effetto solo sulla porta LAN a cui si applica la configurazione.

EtherChannel (L2) con trunking

Configurare EtherChannel di layer 2 per il trunking nel modo seguente:

```
Cat6500(config)#interface port-channel port_channel_interface_#
Cat6500(config-if)#switchport
Cat6500(config-if)#switchport encapsulation encapsulation_type
Cat6500(config-if)#switchport trunk native vlan vlan_id
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

Eseguire la procedura descritta in questa sezione solo per le porte che formano quel particolare canale.

```
Cat6500(config)#interface range [type] mod/port_range
```

```
Cat6500(config-if)#channel-group 1-64 mode [active | auto | desirable | on | passive]
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

Nota: dopo aver configurato EtherChannel, la configurazione applicata all'interfaccia del canale della porta influisce su EtherChannel. La configurazione applicata alle porte LAN ha effetto solo sulla porta LAN a cui si applica la configurazione.

Verificate la creazione di tutti gli EtherChannel e i trunk. Questo è un esempio:

```
Cat6500#show etherchannel summary
Cat6500#show interface trunk
```

Porte di accesso

Se la funzione di interfaccia è una porta di accesso configurata come interfaccia singola, eseguire i seguenti comandi:

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#switchport mode access
Cat6500(config-if)#switchport access vlan vlan_id
Cat6500(config-if)#exit
```

Ripetere questi comandi per ciascuna interfaccia che deve essere configurata come porta dello switch di layer 2.

Se la porta dello switch deve essere collegata a unità terminali, eseguire questo comando:

```
Cat6500(config-if)#spanning-tree portfast
```

Porta trunk (interfaccia fisica singola)

Se la funzione di interfaccia è una porta trunk configurata come interfaccia singola, eseguire questi comandi:

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#switchport
Cat6500(config-if)#switchport trunk encapsulation dot1q
Cat6500(config-if)#switchport trunk native vlan vlan_id
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

Ripetere questi comandi per ciascuna funzione di interfaccia che deve essere configurata come porta trunk.

Informazioni password

Utilizzare i seguenti comandi per le informazioni sulla password:

```
Cat6500(config)#service password-encryption
Cat6500(config)#enable secret password

CbrCat6500(config)#line con 0
Cat6500(config-line)#password password

CbrCat6500(config-line)#line vty 0 4
Cat6500(config-line)#password password
Cat6500(config-line)#^Z
```

Salvare la configurazione

Per salvare la configurazione, usare questo comando:

```
Cat6500#copy running-config startup-config
```

Nuove funzionalità software nel software Cisco IOS versione 12.1(13)E

Per ulteriori informazioni sul supporto telefonico IP, fare riferimento a Configurazione del supporto telefonico IP di Cisco.

Per ulteriori informazioni su NBAR (Network-Based Application Recognition) per le porte LAN, fare riferimento a Riconoscimento applicazioni basato sulla rete e Riconoscimento applicazioni basato sulla rete distribuita.

Note:

- NBAR per le porte LAN è supportato nel software dell'MSFC2.
- Il PFC2 fornisce il supporto hardware per gli ACL di input sulle porte LAN in cui è possibile configurare NBAR.
- Quando QoS PFC è abilitato, il traffico attraverso le porte LAN in cui si configura NBAR passa attraverso le code di ingresso e di uscita e le soglie di rilascio.
- Quando QoS PFC è abilitato, MSFC2 imposta la classe di servizio (CoS) in uscita come precedenza IP in uscita.
- Dopo che il traffico passa attraverso una coda in entrata, viene elaborato tutto nel software sulle porte MSFC2 on LAN in cui si configura NBAR.
- Distributed NBAR è disponibile sulle interfacce FlexWAN con software Cisco IOS versione 12.1(6)E e successive.

I miglioramenti NDE (NetFlow Data Export) includono:

- Maschere di flusso dell'interfaccia di destinazione-origine e dell'interfaccia completa
- NDE versione 5 da PFC2
- Esempio di NetFlow
- Opzione per popolare questi campi aggiuntivi nei record NDE:Indirizzo IP del router dell'hop successivoInterfaccia in ingresso SNMP ifIndexEsci interfaccia SNMP ifIndexNumero sistema autonomo di origine

Per ulteriori informazioni su questi miglioramenti, fare riferimento a Configurazione di NDE.

Altre caratteristiche avanzate includono:

- Configurazione di UDLD
- Configurazione del VTP
- Configurazione dei servizi Web Cache tramite WCCP

Questi comandi sono nuovi:

- **ritardo standby minimo ricaricamento**
- **debounce collegamento**
- **criteri di allocazione interna vlan {ascending} | decrescente}**
- **jumbomtu di sistema**
- **cancella misuratore di traffico catalyst6000**

Questi sono comandi avanzati:

- **show vlan internal usage**: questo comando è stato migliorato per includere le VLAN usate dalle interfacce WAN.
- **show vlan id**: questo comando è stato migliorato per supportare l'immissione di un intervallo di VLAN.
- **show l2protocol-tunnel**: questo comando è stato migliorato per supportare la voce di un ID VLAN.

Il software Cisco IOS versione 12.1(13)E supporta queste funzionalità software, precedentemente supportate nelle versioni 12.1 EX del software Cisco IOS:

- Configurazione di EtherChannel di layer 2 che includono interfacce su diversi moduli di switching dotati di DFCFare riferimento alla sezione Osservazioni generali risolte nella versione 12.1(13)E dell'ID bug Cisco CSCdt27074 (solo utenti registrati).
- Ridondanza del processore di routing Plus (RPR+)Fare riferimento alla sezione Configurazione della ridondanza del Supervisor Engine di RPR o RPR+.**Nota:** nel software Cisco IOS versione 12.1(13)E e successive, le funzionalità di ridondanza RPR e RPR+ sostituiscono la ridondanza EHSA (High System Availability) avanzata.
- 4.096 VLAN layer 2Fare riferimento alla sezione sulla configurazione delle VLAN.**Nota: il** software Cisco IOS versione 12.1(13)E e successive supporta la configurazione delle interfacce VLAN di layer 3 4096. Configurare un totale combinato di non più di 2.000 interfacce VLAN di layer 3 e porte di layer 3 su un MSFC2 con un Supervisor Engine II o un Supervisor Engine I. Configurare un totale combinato di non più di 1.000 interfacce VLAN di layer 3 e porte di layer 3 su un MSFC.
- Tunneling IEEE 802.1QFare riferimento alla sezione Configurazione del tunneling IEEE 802.1Q e del tunneling del protocollo di layer 2.
- Tunneling del protocollo IEEE 802.1QFare riferimento alla sezione Configurazione del tunneling IEEE 802.1Q e del tunneling del protocollo di layer 2.
- MST (Multiple Spanning Tree) IEEE 802.1sFare riferimento alla sezione sulla configurazione di STP e IEEE 802.1s MST.
- RSTP (Rapid STP) IEEE 802.1wFare riferimento alla sezione sulla configurazione di STP e IEEE 802.1s MST.
- LACP IEEE 802.3adFare riferimento alla configurazione di EtherChannel layer 3 e layer 2.
- Filtraggio BPDU PortFastFare riferimento alla sezione Configurazione delle feature STP.
- Creazione automatica di interfacce VLAN di layer 3 per supportare ACL VLAN (VACL)Fare riferimento alla sezione Configurazione della sicurezza di rete.
- Porte di acquisizione VACL che possono essere qualsiasi porta Ethernet di layer 2 in qualsiasi VLANFare riferimento alla sezione Configurazione della sicurezza di rete.

- Dimensioni MTU configurabili su singole porte fisiche di layer 3Fare riferimento alla panoramica della configurazione interfaccia.
- Configurazione delle porte di destinazione SPAN come trunk in modo che tutto il traffico SPAN sia contrassegnatoFare riferimento alla sezione sulla configurazione dello SPAN locale e remoto.

Informazioni correlate

- Strumenti e risorse - Cisco Systems
- Switch - Supporto dei prodotti
- Supporto della tecnologia di switching LAN
- Documentazione e supporto tecnico – Cisco Systems