Indice generale

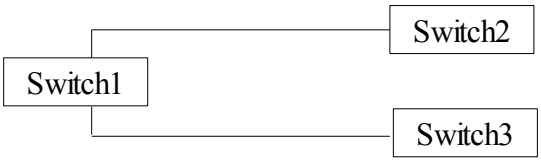
SWITCH

Inizialmente fu utilizzato il protocollo Ethernet 10-Base che prevede l' utilizzo di un cavo coassiale al quale sono connessi tutti gli utilizzatori. Questo protocollo prevede che un unico utente per volta invii i dati per evitare collisioni, quindi si deduce che la banda consentita per la trasmissione con questo protocollo è pari alla banda totale permessa diviso il numero di utenti della linea. Successivamente il protocollo Ethernet si è evoluto al protocollo 10-Base-T che prevede l' utilizzo di un cavo UTP e sopratutto l' utilizzo di un hub. Un hub come abbiamo già visto si comporta come un nodo pertanto non riduce il problema della collisione e quindi della riduzione di banda. Tramite l' utilizzo degli hub si è potuto pensare alla segmentazione della rete in più reti connesse tramite dei bridge. Il Bridge rappresenta la connessione tra un hub e un altro e rileva se la comunicazione richiede l'utilizzo di un ramo della rete già impegnato e in tal caso i dati sono memorizzati e inviati solo nel momento in cui il ramo di rete si libera. Con l' utilizzo dei bridge si è risolto il problema delle collisioni tra le reti connesse al bridge ma non quello delle collisioni delle linee connesse allo stesso hub permettendo di ampliare la banda disponibile ad ogni utente. Successivamente si introdussero gli Switch che trattano ogni utente come se fosse una rete indipendente così rendendo disponibile per ogni utente l'intera banda e risolvendo totalmente il problema delle connessioni.
Uno switch riceve un frame ethernet e esegue le azioni sotto riportate:

- decidere se inviare il frame o ignorarlo in funzione dell' indirizzo MAC. Il frame ricevuto è inviato ad una porta o ignorato in funzione della tabella degli indirizzi presente nello switch.
- memorizzare il nuovo indirizzo MAC. Lo switch determinando gli indirizzi MAC dei frame che giungono in ingresso può completare e aggiornare la tabella degli indirizzi.
- comunicare agli altri switch (in protocollo STP) il nuovo indirizzo. Se il frame ha un MAC di trasmissione che appartiene ad una subnet mask differente dal MAC del ricevente il frame è automaticamente lo switch invia una richiesta multicast dalle sue porte richiedendo informazioni su questo MAC sconosciuto. Se da una porta riceve informazioni sul MAC allora lo switch completa la tabella degli indirizzi altrimenti ignora il frame.

STP

Il protocollo STP evita che si creino dei loop tra gli switch in una rete Ethernet in cui esiste un anello.



In caso di rete Ethernet con un anello si può determinare un loop. Supponiamo che lo switch1 non riconosce un indirizzo MAC che gli giunge da un PC che in realtà si è sconnesso. Lo switch1 per determinare dove inviare il frame genererà un messaggio broadcast per aggiornare la sua tabella degli indirizzi. Alla richiesta inviata dallo switch1 gli altri switch risponderanno a loro volta con un messaggio broadcast dato che nessuno conosce la disposizione del MAC ricercato.
Mediante il protocollo STP lo switch blocca le porte da cui invia i frame così un solo ente è attivo.
Mediante il protocollo STP ogni interfaccia dello switch è in uno stato di blocco o attivo così in ogni LAN esiste un solo ente attivo.

Funzionamento degli Switch.

Ogni switch o bridge utilizza per la gestione del suo funzionamento un algoritmo di memorizzazione e successivamente, non appena le condizioni lo permettono, d' invio dei dati. Gli switch CISCO implementano anche un funzionamento cut-through and fragment-free che permette al dispositivo di decidere se inviare il frame non appena si ricevono i primi bit e d'iniziare la trasmissione senza attendere la completa ricezione del messaggio. Il funzionamento cut-through and fragment-free è reso possibile perché l'indirizzo MAC di destinazione è disposto all' inizio dei frame ricevuti. Dato che il bit di controllo FCS è situato alla fine del messaggio questo tipo di funzionamento non premette allo switch di verificare l' esattezza del frame prima di trasmetterlo.
Il funzionamento Fragment-free processing è analogo al funzionamento cut-through and fragment-free però la trasmissione inizia dopo avere ricevuto i primi 64 bit così consentendo di evitare di trasmettere i frame errati.

Configurazione

Per la configurazione degli switch CISCO si utilizza un interfaccia a linea di comando denominata CLI. Mediante il CLI l' amministratore della rete invia dei comandi allo switch il quale gli esegue ed eventualmente risponde con dei messaggi. Si tratteranno in questo capitolo i Cisco Catalyst che rappresentano la gamma di switch per uso domestico. Tra i Catalyst annoveriamo gli 2960 series (family) che rappresentano la gamma completa degli switch economici. Spesso la serie 2960 è utilizzata per connettere i vari utenti come uno access switch connesso a sua volta ad uno distribution switch che è di tipo superiore (i distribution switch e access switch sono trattai nei paragrafi successivi).
Lo switch è costituito da differenti moduli che possono realizzare anche comunicazioni con diversi protocolli Ethernet. Lo switch CISCO considera ogni connessione come una porta. Ogni porta è indicata con due numeri x/y di cui y è il numero incrementale che indica il numero di porta dell' interfaccia considerata mentre la x indica il modulo a cui appartiene la porta.
Gli switch CISCO supportano due sistemi operativi il Internetwork Operating System (IOS) e Catalyst Operating System (Cat OS) ma attualmente è utilizzato esclusivamente il IOS.
Gli switch CISCO sono provvisti di LED di stato dello switch e di LED dei stato per ogni porta.
Di seguito analizziamo i LED di stato:

- SYST: Indica lo stato complessivo dello switch. Se è spento lo switch è spento, se è verde fisso lo switch è acceso e il sistema operativo è funzionante, se è color ambra lo switch è in modalità di test
- RPS: Indica lo stato dell' alimentazione supplementare
- STAT: Indica lo stato delle porte e se è verde significa che le porte sono tutte in run
- DUPLX: Quando è verde indica che tutte le porte sono in configurazione duplex
- SPEED: Indica la velocità delle porte. Se è spenta le porte comunicano a 10 Mbps se è verde fissa le porte comunicano a 100 Mbps e se è verde lampeggiante le porte comunicano a 1 Gbps

I Led sulle porte indicano lo stato del singolo canale.

- off il canale non è utilizzato
- verde fisso il canale è utilizzato ma non ci sono comunicazioni in corso
- verde lampeggiante: il canale è utilizzato e c'è un comunicazione in corso
- arancione lampeggiante: il canale è disabilitato o non funzionante

Accesso al sistema IOS

L' IOS controlla e condiziona le funzionalità dello switch e definisce l' interfaccia CLI. Il CLI si comporta come un simulatore e solo dopo aver premuto il tasto enter trasmette le stringhe allo switch che le interpreta e le esegue.
Si può accedere all' interfaccia CLI in tre modi:

- Telnet
- SSH Secure Shell
- console

L' accesso in Telnet e SSH avviene tramite una porta Ethernet dell' interfaccia mentre l 'accesso in console avviene tramite una porta dedicata. La configurazione di uno switch può avvenire anche tramite un normale browser ma in questo caso non si utilizza l' interfaccia CLI ma dei tool detti Cisco Device Manager (CDM) o Cisco Security Device Manager (SDM).

CLI Access dalla Console

Per connettersi alla console si utilizza un cavo UTP con un connettore RJ-45 per la connessione con lo switch e una porta seriale o USB lato PC. Non appena ci connettiamo allo switch si avvia il programma Tera Term Pro software package (disponibile all' indirizzo www.ayera.com che installa il simulatore per poter configurare lo switch. Per consentire la comunicazione con lo switch la porta seriale del PC deve essere configurata con i seguenti parametri.:

- 9600 bits/second
- No hardware folw control
- 8-bit ASCII
- No stop bits
- 1 parity bit

CLI Access tramite Telnet o SSH

L' applicazione Telnet permette di utilizzare un terminale emulator. L' applicazione telnet usa una rete IP quindi per collegarsi in telnet allo switch è necessario che esso sia dotato d' indirizzo IP. Inoltre necessita che il PC che si collega allo switch abbia installato un Client Telnet.
L' applicazione Telnet Client richiama il simulatore del terminale e a tale richiesta l 'applicazione Telnet server risponde utilizzando la porta 23. Utilizzando la console in Telnet potremo collegarci

allo switch da remoto e variare i suoi parametri di configurazione oppure controllare il suo funzionamento.
Un ultima modalità di collegamento della console è Secure Shell (SSH). L' accesso alla console tramite protocollo SSH è analogo a quello Telnet però la comunicazione è più sicura perché avviene in modo criptato.

Password Security for CLI Access

Nello stato di default uno switch CISCO permette, mediante un collegamento diretto alla porta dedicata, l' accesso alla console con la quale si può eseguire ogni tipo di comando mentre per motivi di sicurezza l' accesso ai comandi dello switch in remoto mediante Telnet o SSH è protetto da password. E' possibile inserire la richiesta della password anche per la console utilizzando la stringa seguente:

line console 0 login password love

dopo aver utilizzato il comando sopra riportato per accedere alla console lo switch richiederà d' inserire la password “love” per accedere alla console
Per impostare come password d' accesso “love” alla virtual console tramite Telnet si utilizza il seguente comando:

line vty 0 16 login password love

Modalità di funzionamento

Per modificare la password d' accesso alla virtual console in SSH occorre commutare la modalità di collegamento SSH con lo switch in una modalità protetta e successivamente inserire il comando
L' accesso mediante console, Telnet e SSH rappresentano gli accessi EXEC mode. In EXEC mode l' utente può modificare i parametri fermare lo switch ma non causare guasti, inoltre l' EXEC mode è detto così perché è realizzato con dei comandi che sono eseguiti dalla switch.
Il sistemi CISCO supportano anche la modalità Enable. L' Enable mode è una modalità di funzionamento con maggiori privilegi della modalità EXEC, per esempio consente la reinizializzazione o il reboot dello switch. La modalità di funzionamento enable è protetta da password e non è accessibile in Telenet o SSH.
Un ulteriore modalità di funzionamento dei sistemi CISCO è la Configuration mode. Nella modalità di configurazione l' utente ha accesso a tutti quei comandi che definiscono e o modificano la configurazione dello switch.
Quando ci colleghiamo allo switch abbiamo accesso alla modalità di funzionamento EXEC dalla quale è possibile passare alla modalità di funzionamento con privilegi Enable mediane il comando:
enable
Se lo switch è in funzionamento enable può passare alla modalità di funzionamento di configurazione mediante il comando seguente:
config t
Se lo switch è in funzionamento di configurazione torna al funzionamento enable mediante il comando:
Ctrl-Z o exit
un altra modalità di funzionamento è quella setup che corrisponde alla modalità di funzionamento di configurazione ma presenta un interfaccia che aiuta gli utenti meno esperti a configurare lo switch.
Si attiva la modalità di funzionamento di setup dalla modalità enable con il comando seguente:
setup

HELP

La console CLI implementa uno strumento di help che aiuta a completare i parametri e rivedere la sintassi dei comandi. Di seguito riporto alcune sintassi di richiamo degli strumenti di help:

?	Ricapitola tutti i comandi eseguibili nella modalità in uso
Help	Descrive come richiamare gli strumenti di help
Command ?	descrive tutte le opzioni per il primo parametro del comando
Com?	Visualizza i comandi che iniziano con la strina com
Command param?	Visualizza tutti i parametri del comando che iniziano con la strina param
Command param<Tab>	Completa il comando terminandola con i caratteri mancanti se il comando è univocamente determinato
Command param ?	Visualizza la lista di tutti i prossimi parametri opzionali con una loro descrizione

L' output dello strumento di help dipende dalla modalità di funzionamento dato che visualizzerà solo i comandi e i parametri abilitati in quella modalità.
Gli switch CISCO hanno uno staeck per la memorizzazione dei comandi eseguiti così si può richiamare un comando già eseguito utilizzando una sequenza di tasti. Di seguito si riportano le sequenze di tasti che permettono di visualizzare l' historical dei comandi eseguiti.

Freccia alta o Ctrl-p	Visualizza gli ultimi comandi utilizzati. Ogni volta che è digitato il Ctrl-p è visualizzato un comando fino al termine dello steck di memorizzazione
Freccia bassa o Ctrl-n	Se stiamo visualizzando lo steck dei comandi precedenti con Ctrl-n si ritorna al comando più recente di quello visualizzato
Freccia sinistra o Ctrl-b	Torna un carattere indietro del comando con il cursore digitalizzato senza cancellare
Freccia destra o Ctrl-f	Muove il cursore in avanti senza cancellare nessun carattere
BackSpace	Muove il cursore indietro nella stringa corrente cancellando gli eventuali caratteri
Ctrl-a	Muove il cursore all' inizio della strina corrente
Ctrl-e	Muove il cursore alla fine della strina corrente
Ctrl-r	Visualizza nuovamente il comando digitato
Ctrl-d	Cancella il singolo carattere
Esc-b	Ritorna indietro con il cursore nella parola
Esc-f	Muove in avanti nella parola

Il comando **show** visualizza lo stato attuale dello switch in una lista d' informazioni
il comando **debug** richiede allo switch di controllare tutti i nuovi processi che sono eseguititi così lo switch invia un messaggio quando avviene un nuovo evento. I messaggi di debug sono memorizzati un una coda detta log message che può essere visualizzata dall' utente mediante un commando da terminale. Il riavvio dello switch disabilita tutti i debug in corso. Per disabilitare un comando di debug si utilizza la seguente sintassi:

no debug command

i comandi seguenti disabilitano tutte le funzioni di debug

no debug all
undebug all

il comando **show process** consente di visualizzare le attività dello switch. Per non determinare il cresh della macchina occorre non avviare nessun comando di debug dopo avere avviato lo show process

Configurazione del sistema IOS

La modalità di funzionamento di configurazione presenta molti insiemi di comandi divisi per argomento. Si analizzano di seguito i singoli insiemi di comandi esistenti per la configurazione di un apparecchio CISCO. Il sottoinsieme di funzioni più comunemente utilizzato è **interfacce** che permette di modificare i parametri dei singoli canali. Per modificare la velocità del canale 1 Fastethernet si utilizza la seguente sequenza di canali:
esempio:

Switch#**configure terminal**	questo comando permette di passare alla modalità di configurazione
Switch(config)**line console 0**	questo comando ci permette di utilizzare una console per inviare comandi allo switch
Switch(config-line)#**interfacce FastEthernet 0/1**	questo comando si porta a lavorare sul primo canale del modulo Fastethernet
Switch(config -if)#**speed 100**	Impostiamo la velocità del canale 100Mbps
Switch(config-if)#**exit**	
switch(config)#**end**	Ritorna alla modalità EXEC
Switch#	

I parametri di configurazione di uno switch sono memorizzati in una memoria RAM per il normale funzionamento dell' apparato , ma possono essere memorizzati , per motivi di sicurezza, anche in altri tipi di memorie:

- RAM è la memoria utilizzata durante il normale funzionamento dello switch
- ROM contiene un immagine del sistema IOS. Ad ogni bootstrap (insieme dei processi eseguiti all' avvio) del sistema l' immagine memorizzata nella ROM è copiata nella RAM e da quel punto lo switch inizi il normale funzionamento
- Flash Memori contiene un immagine del sistema IOS di altri files di backup e delle configurazioni. La Flash memory carica il sistema IOS e i parametri di configurazione dello switch nella RAM ad ogni avvio
- NVRAM memorizza la configurazione di startup utilizzata quando lo switch è spento o ricaricato.

Lo switch ha due file di configurazione uno per la memorizzazione della configurazione utilizzata durante la procedura di avvio dello switch “startup-configuratio” e uno per la memorizzazione della configurazione utilizzata durante il normale funzionamento “Running-config”
I due file possono essere visualizzati con i seguenti comandi:

show startup-config
show running-config

Per far utilizzare la configurazione normale anche durante lo startup occorre modificare il file startup-config mediante il comando copy:

copy running-config startup-config

il comando copy permette in generale di effettuare gli spostamenti di file negli switch CISCO ed ha la seguente sintassi:

copy {locazione di destinazione} { locazione di partenza}

Quando utilizziamo il comando copy per soprascrivere un file in realtà è eseguita una fusione (merge) tra i due file quindi non abbiamo la certezza che il secondo file sia come quello di provenienza. Per essere certi che mediante il comando copy otteniamo la copia del file di provenienza dobbiamo, se esiste, prima cancellare il file di destinazione.

Nella configurazione di default un utente non può collegarsi ad un router o switch in Telnet o SSH perché esso non è provvisto di indirizzo IP e non è configurata la vty password. Un utente connesso in Telnet o SSH non può avviare la modalità enable se non si esegue prima tramite console il comando in modalità di configurazione **enable secret mypassword**. Il comando enable secret aggiunge un 'istruzione al file running-config che permette ad un utente connesso mediante Telnet o SH di avviare la modalità di funzionamento enable

Esempio:
switch>**enable**
switch#**configure terminal**
switch(config)#**enable secret** love
switch(config)#**exit**
switch#

Per utilizzare la connessione SSH occorre abilitare l' utilizzo della password analogamente alle connessioni Telnet ma con la differenza che per la connessione SSH occorre definire una password e un nome utente. Per la connessione in SSH l' utente deve inserire un nome e una password configurati nello switch o un utente e una password configurati nel server esterno chiamato Authenticatio, Authorization and Accounting (AAA).
Sequenza di operazioni per il login con una connessione SSH.

- 1 **line vty 0 15** predispone la console per l' immissione della username e password
- 2 l**ogin local** predispone la console per l' immissione della password locale
- 3 **transport input telnet ssh** comunico allo switch di abilitare la comunicazione in ssh
- 4 **username** *name* **password** *pass-value* configura una coppia nome utente – password
- 5 **ip domain-name** *name* configura il dominio DNS
- **crypto key generate rsa** configura lo switch per la generazione di due coppie di utente – password uno pubblico e uno privato

Esempio:
Switch#**configure terminal**
Switch(config)#**line vty 0 15**
Switch(config-line)#**login local**
Switch(config-line)#**transport input telnet ssh**
Switch(config-line)#**exit**
Switch(config)#**username wendell password hope**

Switch(config)#**ip domain-name example.com**
Switch(config)#**crypto key generate rsa**

Se si vuole abilitare la sola connessione SSH si utilizza il comando **transport input ssh** al posto del comando **transport input telnet ssh**

Per evitare di memorizzare la password in chiaro nel file di configurazione si utilizza il comando **service password-encryption** con cui automaticamente lo switch convertirà in un formato codificato tutti gli esistenti comandi passwords presenti nei file di configurazione. Il comando **no service password-encryption** esegue la decodifica di tutti i comandi passwords presenti nei file di configurazione.

Configurazione delle proprietà LAN dello Switch

Si definisce configurazione Lan dello Switch la configurazione delle proprietà dell' interfacce dello switch ossia:

- Configurazione IP dello switch
- Configurazione dell' interfaccia (velocità e duplex)
- Port security
- configurazione di VLAN
- sicurezza dell' interfacce

Uno switch non necessita di un indirizzo IP per funzionare ma mediante esso un utente può connettersi per configurare o verificare lo switch tramite connessione ethernet. L' indirizzo IP di uno switch è costituto da un indirizzo IP, da una subnet mask che ne definisce la subnet e da un gateway che rappresenta il router più vicino. L' indirizzo IP dello switch può essere anche configurato automaticamente tramite DHCP. L' indirizzo IP dello switch rappresenta la VLAN di default utilizzata per tutte le porte. L' indirizzo IP dello switch è impostata tramite un interfaccia detta VLAN 1 interface. La VLAN 1 interface è avviata con il comando **interface vlan 1**.
L attribuzione dell' indirizzo IP allo switch è eseguita con i seguenti comadi.

- **interface vlan 1** avvia l' applicazione di configurazione
- **ip address ip-address mask** assegna l' indirizzo Ip e la subnet mask
- **no shutdown** abilita l'interfaccia VLAN
- **ip default-gatway ip-address** configura l' indirizzo del gateway

Per disabilitare la VLAN configurata si utilizza il comando **shutdown** nell' applicazione interface vlan 1. La configurazione dell' interfaccia può essere verificata visualizzando il file running-config
La configurazione dell' interfaccia dello switch tramite DHCP è eseguita con le seguenti istruzioni:

- **interface vlan 1** avvia l' applicazione di configurazione
- **ip address dhcp** assegna l' indirizzo Ip tramite DHCP
- **no shutdown** abilita l'interfaccia VLAN

La configurazione dell' indirizzo IP acquisito dallo switch tramite DHCP può essere verificata tramite il comando **show dhcp lease**
il comando **show interface vlan 1** permette di visualizzare la configurazione Ethernet dell 'interfaccia e lo stato di funzionamento del dispositivo.
Le singole porte possono essere configurate definendo la velocità di comunicazione e la modalità di comunicazione duplex sfruttando l' applicazione di configurazione interface come precedentemente descritto con i comandi speed e duples. E' possibile verificare la configurazione delle singole porte con il comando **show interfaces status** .Con il comando show interfaces status è visualizzato la

configurazione delle singole porte. Se la configurazione di una porta è frutto di un autonegoziazione nella lista dei parametri visualizzata con il comando show interface status è riportata una “a” vicino al parametro negoziato ad esempio a-100 o a-full.

Gli switch CISCO possono essere inseriti in particolari reti in cui le singole porte dell' interfaccia sono abilitate a colloquiare solo con interfacce NIC degli indirizzi specificati. Per abilitare le porte al colloquio con un numero ristretto di indirizzi Mac si utilizza l' utility Port Security. La configurazione di una Port securuty avviene come di seguito riportato:

- **switchport mode access** richiama il set di comandi per la configurazione della sicurezza
- **switchport port-security** abilita la sicurezza della porta
- **switchport port-security maximum** definisce il numero massimo d' indirizzi abilitati
- **switchport port-security violation {protect | restrict | shutdown}**definisce l' azione che compie lo switch in caso avvenga una violazione della sicurezza impostata ossia scartare il messaggio o disabilitare la porta
- **switchport port-security mac-address mac-address** specifica gli indirizzi abilitati
- **switchport port-security mac-address sticky** e in alternativa al comando precedente e definisce che il MAC del primo dispositivo collegato a quella porta è il MAC abilitato

Configurazione di una VLAN

Una potenzialità degli switch CISCO è di poter associare le diverse porte d' interfaccia a diverse VLAN. La configurazione delle VLAN è eseguita con i seguenti comandi:

- **configure** avvia la modalità di configurazione
- **vlan vlan-id** crea una VLAN con un Id di riferimento
- **name name** VLAN definisce un nome per la VLAN
- **interface range fastethernet 0/12 – 16** avvia la modalità di funzionamento interface e individuo dalla porta 0/12 alla porta 0/16
- **switchport access vlan id** identifica la vlan a cui voglio associare le porte precedentemente indicate
- **switchport mode access** disabilita il trunking

VTP, che sta per Virtual Trunking Protocol, ed è un protocollo di comunicazione in grado di mantenere, e aiutare a risolvere i problemi di, configurazioni VLAN di grandi dimensioni, rendendo più agevoli i compiti dell’ amministratore
Esso è un metodo per instradare il traffico di più VLAN su un unico link fisico sfruttando l' encapsulation al tagging, che permettono di identificare in modo univoco a qualeVLAN appartengono i frames ricevuti . Un trunk è una connessione fisica, ma anche logica, tra due switch, attraverso la quale circola il traffico di rete. Il Trnk rappresenta un canale di comunicazione tra due singoli punti, solitamente switch, detta anche connessione point to point. Con VTP le vlan vengono automaticamente mantenute attraverso un unico dominio amministrativo effettuando la configurazione su di un singolo switch.
Cisco è stata la prima a sviluppare un metodo che permettesse il trunking (ovviamente solo tra dispositivi di sua produzione), con l’Inter-Switch Link, protocollo proprietario che permette una corretta comunicazione tra i dispositivi impegnati nel trunk incapsulando i frames tra un header e un trailer rispettivamente di 26 e 4 bytes

VTP utilizza una gerarchia dove, a ogni switch della LAN, è possibile assegnare un “rango” che dice allo switch cosa è in grado di fare. In pratica lo switch può essere configurato in tre modi:

- Server
- Client
- Transparen

Gli switches vengono configurati come appartenenti a un VTP domain; uno switch appartiene sempre e solo a un dominio VTP, con un nome univoco. Gli switch che appartengono a uno stesso dominio possono comunicare tra di loro, e lo fanno tramite appositi VTP messages, ovvero dei layer 2 frames formattati a seconda del trunking protocol in uso (ISL, 802.1q ecc), scambiandosi informazioni che contengono eventuali ordini, cambiamenti che a seconda del rango a cui lo switch appartiene hanno un effetto sulla configurazione, vengono ignorati o inviati agli altri switches
I messaggi trasportano, quindi, tutte le informazioni che riguardano aggiunte, cancellazioni e modifiche alle VLAN e hanno effetto sulla configurazione dei singoli switches a seconda del rango (detto "mode").
Ecco come:

- Server switches: questi sono gli switches dove un 'amministratore andrà a configurare le VLAN. Aggiunte, rimozioni di Virtual LAN, ma anche la versione del protocollo usato all'interno del dominio. Salvate le informazioni in NVRAM, il layer2 invia VTP advertisement su tutte le porte configurate in trunk, verso gli altri switches, che siano essi settati come server o client.
- Client switches: i client non consentono nè la configurazione, nè il salvataggio delle informazioni in NVRAM. Essi ricevono i messaggi VTP , li processano, considerano eventuali cambiamenti e inoltrano i messaggi sulle porte in trunk. L'utilità del client sta nel poter utilizzare al meglio switches con scarse risorse hardware e nel fatto di poter configurare solo i servers per configurare automaticamente tutta la rete. Naturalmente, basta eseguire la configurazione su uno solo dei server, gli altri riceveranno gli advertisement, e come i clients si aggiorneranno.
- Transparent switches: non partecipi al dominio VTP (quindi non aderisce alle modifiche ricevute dai server), ma esegua il forward dei messaggi agli altri switches client e server. Nota: il forward viene eseguito solo se è configurata la versione 2 di VTP.

VTP permette di settare una password criptata con algoritmo Md5 Digest. Naturalemente, questa gestisce la possibilità o meno degli swichtes di interagire tra loro. La password va impostata, solitamente, su tutti gli switches del dominio VTP. All'interno degli advertisement c'è un campo preposto alla memorizzazione della password; questo field viene cosiderato da ogni membro e la password è utilizzata per vedere se il messaggio arriva da una fonte attendibile
Occorre quindi impostare da subito, prima di configurare le vlan, tutti gli switch come Transparent, in modo che non possano fare, inconsapevolmente, danno alla vostra configurazione per evitare che possano trasmettere una configurazione errata e danneggiare così la configurazione anche degli altri switch.
Il coordinamento degli switch di una LAN come unica entità VTP è assicurata dall'appartenenza allo stesso dominio, ma anche da una stessa versione del protocollo, e opzionale ma molto importante una password comune.
E' di seguito riportato come configurare un canale trunk:

Switch# vlan **database**	attivo la modalità di configurazione vlan
Switch (vlan)# vtp **domain nome_dominio**	setto il nome del dominio
Switch (vlan)# **vtp v2-mode**	setto la versione di vtp
Swicth (vlan)# vtp **password** vtp-*password*	imposta la password
Switch (vlan)# vtp **client**	imposta la modalità di Trunk

Il comando seguente permette di visualizzare la configurazione del trunk

Switch # show vtp **status**

Il comando seguente permette di visualizzare il funzionamento della configurazione trunk adottata

Switch # show vtp **statistics**

Per cancellare una configurazione di un Trunk occorrono utilizzare i comandi seguenti:
Switch # **delete flash:**vlan**.dat**
Switch # **erase startup-config**
Switch # **reload**

Tabella dei comandi e procedure

Comand	Azione
line console 0	Commuta alla modalità di configurazione della console
line vty 1st-vty 2nd-vty	Commuta alla modalità di configurazione la console vty nel range indicato
login	Indica all' IOS di predisporsi per una password
password pass-value	Imposta la password da inserire per un accesso se il login è abilitato
interface type port-number	Commuta alla modalità di funzionamento inteface
Shutdown no shutdown	Abilità o disabilità l' interfaccia
hostname name	Imposta il nome dello swicth
enable secret pass-value	Abilità la codifica della password
enable password pass-value	Abilita l' accesso con richiesta dell' inserimento della password
exit	Torna indietro nella modalità di funzionamento
End o Ctrl-Z	Esce dalla modalità di funzionamento per configurazione
no debug all undebug all	Disabilita ogni processo di debug
show process	Visualizza le attività della CPU
terminal monitor	Visualizza ogni messaggio di sistema o di debug agli utenti Telnet o SSH
Reload	Riavvia lo switch
copy from-location to-location	Copia il file dalla locazione d' origine a quella di destinazione indicata
copy running-config startup-config	Copia la configurazione attiva in quella d' inizializzazione

copy startup-config running-config	Esegue il merge della configurazione d' inizializzazione con quella attiva
show running-config	Visualizza il file di configurazione
write erase erase startup-config erase nvram:	Questi tre comandi cancellano il file di configurazione
setup	Commuta in modalità di setup
Quit	Disconnette l' utenet dal CLI
show system:running-config show startup-config show nvram:startup-config show nvram:	Visualizza il file di configurazione
enable	Commuta in modalità con privilegi enable
disable	Commuta dalla modalità Enable a quella Exec
configure terminal	Permette di commutare dalla modalità enable a quella di configurazione
hostname name	Configura il nome dello switch
enable secret pass-value	Imposta la password richiesta per attivare la modalità enalbe
history size length	Definisce il numero di comandi memorizzati nell' history
switchport port-security mac-address mac-address	Aggiunge un Mac alla lista dei Mac con cui la porta può colloquiare
switchport port-security mac-address sticky	Incica allo switch d' inserire tra i Mac abilitati alla porta quello attualmente connesso
switchport port-security maximum value	Imposta il numero massimo di Mac che può contenere lista dei Mac che possono colloquiare con la porta
witchport port-security violation {protect | restrict | shutdown}	Imposta l' azione che l' interfaccia intraprenderà in caso di violazione
Show maac-address-table	Visualizza la mac address table dello switch
Show mac address-table dynamic	Visualizza gli indirizzi della mac address table aquisiti dinamicamente
Switch # show vtp status	Visualizza la configurazione del canale Trunk
Switch # show vtp statistics	Visualizza le attività del canale trunk

Procedure	
enable Conf t enable secret *vecchia password* line console 0 password *nuova password* login exit	Configurazione Password da console
enable Conf t line vty 0 15 login local transport input telnet exit username *wendell* password *hope* ip domain-name *nome dominio* crypto key generate rsa	Configurazione password in Telnet
enable Conf t line vty 0 15 login local transport input telnet ssh exit username *wendell* password *hope* ip domain-name *nome dominio* crypto key generate rsa	Configurazione password in SSH
enable Conf t interface vlan number ip address ip-address subnet-mask ip address dhcp ip default-gateway address	Comandi per la configurazione dell' IP address
enable Conf t interface type port-number interface range type port-range shutdown no shutdown speed {10 | 100 | 1000 | auto} duplex {auto | full | half} description text	Comandi per la configurazione delle interfacce
enable	Configurazione di un canale Trunk

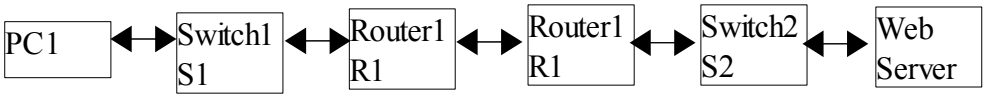
Switch# vlan database Switch (vlan)# vtp domain nome_dominio Switch (vlan)# vtp v2-mode Swicth (vlan)# vtp password vtp-password Switch (vlan)# vtp client	
enable Switch # delete flash:vlan.dat Switch # erase startup-config Switch # reload	Procedura di cancellazione di un canale Trunk
Enable config t int>Fa0/8> default switchport port-security	Procedura per la cancellazione della port security dell' interfaccia Fa0/8

Diagnosi del funzionamento di una rete LAN

Oltre a saper progettare e configurare una rete un amministratore di reti deve conoscere gli strumenti per verificare il funzionamento della rete e della sua configurazione e diagnosticare i problemi. Per diagnosticare un problema un 'amministratore deve:

- 1 Analizzare il funzionamento della rete interrogando gli switch
- 2 Isolare il problema
- 3 individuare la causa del problema in funziona dei risultati conseguiti dalle precedenti analisi.

L' analisi del funzionamento di una rete inizia con l' analisi del Layer 3 per poi passare allo studio dei Layer 2 e 1 e l' individuazione del problema. Con il termine “Layer 3” indichiamo lo studio qualitativo dei messaggi scambiati tra i partecipanti alla comunicazione. Supponiamo che l' utente PC1 abbia dei problemi a connettersi ad un sito web e si vuol diagnosticare il problema. L' analisi del problema inizia dalla definizione della topologia (disposizione e connessioni degli elementi) della rete. La rete utilizzata dall' utente PC1 è quella di seguito riportata:



Dallo studio del Lasyer3 si evidenziano le seguenti azioni:

- 1 L' utente PC1 invia un pacchetto allo switch 1
- Lo switch S1 rileva che l' utente di destinazione appartiene ad una subnet differente ed inia il messaggio al router R1
- Il router R1 mediante la sua routing table instrada il messaggio al router R2
- Il router R2 decide d' instradare il messaggio verso lo switch 2 utilizzando la sua routing table
- Lo switch S2 invia il messaggio al Web Server il quale risponde trasmettendo la pagina all' utente PC1
- Lo switch S2 riceve il messaggio inviato dal web Server e lo instrada verso il router R2
- Il router R2 ribalta il messaggio al router R1

- Il router R1 trasmette il messaggio allo switch S1 che lo trasmette all' utente PC1

Analizzando le attività descritte si può rilevare quale è il passaggio che genera il problema di comunicazione e analizzando il dettaglio del Layer 2 e 1 si determina il vero problema e la soluzione.

CDP

Il Cisco Discovery Protocol (CDP)è un protocollo proprietario della CISCO che permette ad uno switch di acquisire delle informazioni sulla rete interrogando i dispositivi di rete vicini. Tramite CDP ogni dispositivo può acquisire informazioni sulla topologia della rete acquisendo dei messaggio d' avviso inviati dagli altri dispositivi. Ogni dispositivo che supporta il protocollo CDP invia dei messaggi in broadcast così ogni altro dispositivo della rete può acquisire le informazioni. Le informazioni riportate in un messaggio CDT sono:

- Identificatore del dispositivo, solitamente l' hostname
- l' indirizzi del dispositivo
- Local inteface: I router e gli switch inviano la configurazione della loro interfaccia
- L' identificatore della porta che identifica la porta utilizzata per inviare il messaggio CDP
- lista delle capacità che è la lista dei tipi di dispositivi connessi alla rete
- Platform che identifica il sistema operativo utilizzato dai dispositivi connessi

comandi CDP:

- Il comando **show cdp** visualizza una lista sintetica dei parametri acquisiti mediante cdp.
- Il comando **show cdp neighbors** visualizza una lista sommaria di parametri dei dispositivi connessi
- Il comando **show cdp neighbors detail** visualizza una lista completa dei parametri dei dispositivi connessi.
- Il comando **show cdp entry** *name* visualizza la lista completa dei parametri del dispositivo che ha il nome indicato

1. Il comando **show cdp** visualizza lo stato del CDP globale dello switch

- il comando **show cdp interface** [*type number*] visualizza lo stato del CDP dell' interfaccia specificata
- il comando show **cdp traffic** visualizza le statistiche riguardanti i messaggi di cdp inviati

La CISCO consiglia di disabilitare il protocollo CDT quando non è necessario con i seguenti comandi:

- **no cdp enable** disabilita il cdp per un interfaccia
- **cdp enable** riabilita il cdp per un iterfaccia
- **no cdp run** disabilita il cdp per l' intero switch
- **cdp run** abilita il cdp per l' intero switch

Strumenti per l' analisi del funzionamento dell' interfacce

Analisi Layer 2

I comandi ***s*how interfaces** e **show interfaces** description permettono di verificare lo stato di funzionamento del Layer 1 e del Layer 2 dell' interfaccia di uno switch visualizzando i code line status e protocol status. Si riportano di seguito le indicazione visualizzate dai code *Protocol status* e *Interface staus* corrispondenti a differenti modalità di funzionamento dell 'interfaccia:

Funzionamento della	Protocol status	Interface status	Tipica Causa

Linea			
Shutdown della linea dall' amministratore	Down	Disable	Questo stato è generato con il comando shutdown
Down	Down	notconnect	Questo stato può essere causato: - cavo disconnesso - non supportata la velocità del dispositivo connesso - Il dispositivo connesso è spento o scollegato
Up	Down	notconnect	Lo stato dell' interfaccia non è ben definito
Down	Down (err-disable)	err-disable	La Port security ha disabilitato la porta
Up	Up	Connect	L' interfaccia funziona correttamente

Analisi Layer 1

Può accedere che un apparato CISCO riporti lo stato della connessione al valore Up ma in realtà si verifichino dei problemi di comunicazione determinati da anomalie sul Layer 1 ad esempio un cavo UTP danneggiato. Quando sono presenti problemi di Layer 1 durante la trasmissione alcuni bitpossono cambiare valore e il ricevitore rileva l' errore di ricezione. Il ricevitore rileva gli errori mediante i bit FCS, e richiede la ritrasmissione del dato. Gli errori di comunicazione rilevati dallo switch sono contati e memorizzati nel parametro CRC (cyclic redundancy check).
Un altro parametro che può dare delle indicazioni del corretto funzionamento della rete è il numero di collisioni. Le collisioni in una rete ethernet che utilizza uno switch superano l' 1% se:

- le interfacce connesse ad uno stesso dominio di collisione presentano dei cavi di collegamento troppo lunghi
- l' interfaccia utilizza una comunicazione half duplex mentre il dispositivo connesso utilizza una comunicazione full duplex