HOEPLI
TECNICA
PER LA SCUOLA

LUIGI LO RUSSO
ELENA BIANCHI

SISTEMI E RETI

Per l'articolazione **INFORMATICA**
degli Istituti Tecnici
settore Tecnologico

3

RISORSE ONLINE

HOEPLI

PAOLO CAMAGNI RICCARDO NIKOLASSY

Sistemi e reti

Per l'articolazione informatica degli Istituti Tecnici settore Tecnologico

VOLUME 3

EDITORE ULRICO HOEPLI MILANO

Via Hoepli 5, 20121 Milano (Italy)
tel. +39 02 864871 – fax +39 02 8052886
e-mail hoepli@hoepli.it

www.hoepli.it

Indice

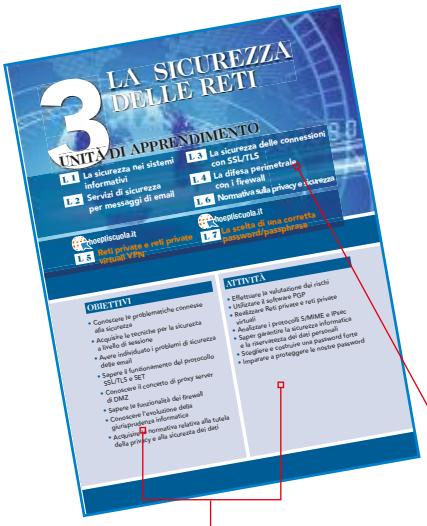
Presentazione

L'impostazione del presente corso in tre volumi è stata realizzata sulla base delle indicazioni ministeriali in merito a conoscenze ed abilità proposte per la nuova disciplina Sistemi e Reti. L'opera è in particolare adatta all'articolazione Informatica degli Istituti Tecnici settore Tecnologico, dove la materia è prevista nel secondo biennio e nel quinto anno del nuovo ordinamento.

Abbiamo ritenuto irrinunciabile fare tesoro della nostra esperienza maturata nel corso di numerosi anni di insegnamento che ci ha reso consapevoli della difficoltà di adeguare le metodologie didattiche alle dinamiche dell'apprendimento giovanile e ai continui cambiamenti tecnologici che implicano sempre nuove metodologie di comunicazione, per proporre un testo con una struttura innovativa, riducendo l'aspetto teorico e proponendo un approccio didattico di apprendimento operativo, privilegiando il "saper fare".

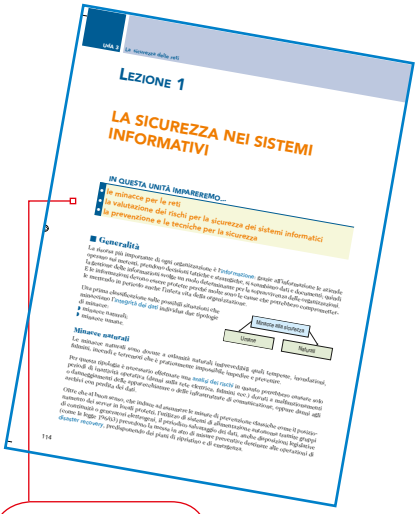
Il testo, arricchito di contenuti che lo rendono di facile lettura, grazie ai richiami a vocaboli nuovi, spesso in lingua inglese, e ad ampie sezioni di approfondimento, aiuta lo studente a una maggior comprensione degli argomenti, trattati fino ad oggi in modo assai nozionistico. Inoltre, le schede per il laboratorio rappresentano un valido strumento per il rafforzamento dei concetti assimilati attraverso esercitazioni operative.

Il terzo volume è strutturato in unità di apprendimento suddivise in lezioni che ricalcano le indicazioni dei programmi ministeriali per il quinto anno di studio: lo scopo di ciascuna unità di apprendimento è quello di presentare un intero argomento, mentre quello delle lezioni è di esporne un singolo aspetto.



Nella pagina iniziale di ogni unità di apprendimento è presente un indice delle lezioni trattate

Indice degli obiettivi che si intendono raggiungere e delle attività che si sarà in grado di svolgere

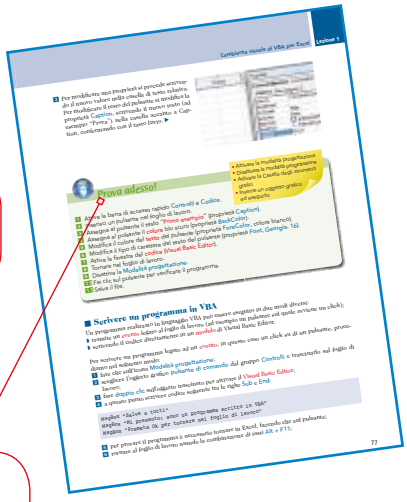


All'inizio di ogni lezione sono indicati in modo sintetico i contenuti

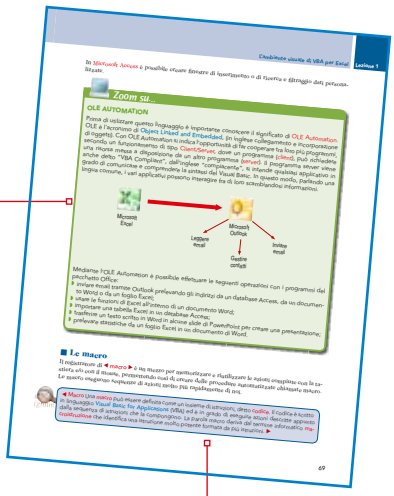
Le finalità e i contenuti dei diversi argomenti affrontati sono presentati all'inizio di ogni unità di apprendimento; in conclusione di ogni lezione sono presenti esercizi di valutazione delle conoscenze e delle competenze raggiunte, suddivisi in domande a risposta multipla, vero o falso, a completamento, e infine esercizi di progettazione da svolgere autonomamente.

Le osservazioni aiutano lo studente a comprendere e ad approfondire

Il significato di moltissimi termini informatici viene illustrato e approfondito



Lo studente può mettere in pratica in itinere quanto sta apprendendo nel corso della lezione

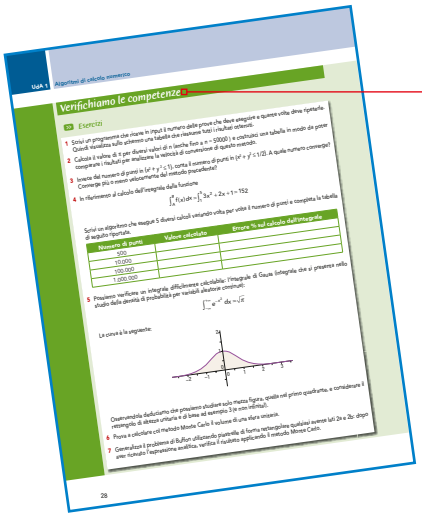


In questa sezione viene approfondito un argomento di particolare importanza

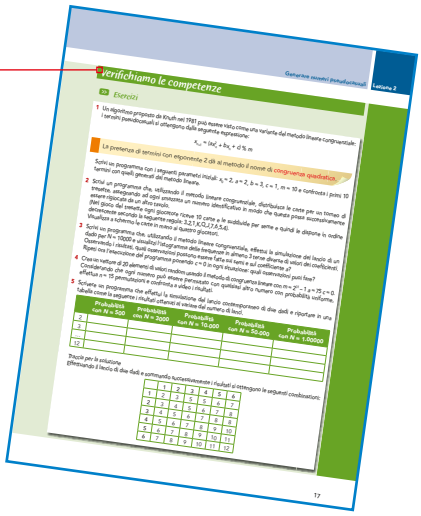
Le parole chiave vengono poste in evidenza e spiegate allo studente

hoepliscuola.it

Alla pagina web **http://www.hoepliscuola.it** sono disponibili le risorse online, tra cui lezioni integrative, numerosi esercizi aggiuntivi per il recupero e il rinforzo, nonché schede di valutazione di fine unità.



Per la verifica delle conoscenze e delle competenze è presente un'ampia sezione di esercizi



1 VLAN – VIRTUAL LOCAL AREA NETWORK

UNITÀ DI APPRENDIMENTO

L 1 Le Virtual LAN (VLAN)

L 2 Il protocollo VTP e l'Inter-VLAN Routing

OBIETTIVI

- Conoscere le caratteristiche delle VLAN
- Individuare pregi e difetti delle VLAN
- Acquisire le caratteristiche delle VLAN port based
- Acquisire le caratteristiche delle VLAN tagged
- Conoscere il protocollo VTP
- Conoscere l'Inter-VLAN routing

ATTIVITÀ

- Configurare gli switch singolarmente
- Saper configurare le VLAN
- Definire le VLAN in presenza di più switch
- Utilizzare il protocollo VTP per definire le VLAN

LEZIONE 1

LE VIRTUAL LAN (VLAN)

IN QUESTA LEZIONE IMPAREREMO...

- le caratteristiche delle VLAN
- la differenza tra VLAN port based e tagged

Generalità

Una Virtual LAN, meglio conosciuta come VLAN, è una LAN realizzata *logicamente* grazie allo standard 802.1Q che definisce le specifiche che permettono di definire più reti locali virtuali (VLAN) distinte, utilizzando e condividendo una stessa infrastruttura fisica.

> La struttura fisica di una VLAN non è quella di una normale rete di computer locale ma una astrazione che permette a computer anche collocati in luoghi non vicini fisicamente di comunicare come se fossero sullo stesso *dominio di collisione*.

Le VLAN non sono altro che un livello di astrazione in grado:
- di consentire a postazioni attestate su segmenti di rete fisicamente distinti, di apparire connessi alla stessa rete logica;
- di separare postazioni che sono sulla stessa rete fisica e quindi nello stesso dominio di broadcast in più reti logiche distinte, "scollegate" tra loro.

Ciascuna VLAN si comporta come se fosse una rete locale separata dalle altre dove i pacchetti broadcast sono confinati all'interno di essa, cioè la comunicazione a livello 2 è confinata all'interno della VLAN e la connettività tra diverse VLAN può essere realizzata solo a livello 3, attraverso routing.

I principali vantaggi che derivano dall'utilizzo delle VLAN sono:
- risparmio: sulle stesse strutture fisiche si realizzano nuove VLAN secondo i fabbisogni del momento, con notevole risparmio di tempo e di denaro;
- aumento di prestazioni: il frame non viene propagato verso le destinazioni che non hanno necessità di riceverlo grazie al confinamento del traffico broadcast alla singole VLAN;
- aumento della sicurezza: una utenza può vedere solo il traffico della propria VLAN e non delle altre, anche se condividono le stesso hardware di connessione;

- flessibilità: abbiamo due situazioni nelle quali il vantaggio è notevole:
  - se viene effettuato lo spostamento fisico di un utente all'interno dei locali raggiunti dalla infrastruttura di rete, questo può rimanere connesso alla VLAN senza modificare la topologia fisica della rete ma solo con una semplice riconfigurazione degli switch o dei bridge;
  - se viene effettuato lo spostamento fisico di un computer esso rimane comunque collegato alla stessa VLAN senza alcuna riconfigurazione dell'hardware.

Realizzazione di una VLAN

Per realizzare VLAN è necessario che gli switch e i bridge della infrastruttura di rete siano capaci di distinguere le diverse VLAN e per fare questo devono osservare lo standard 802.1Q.

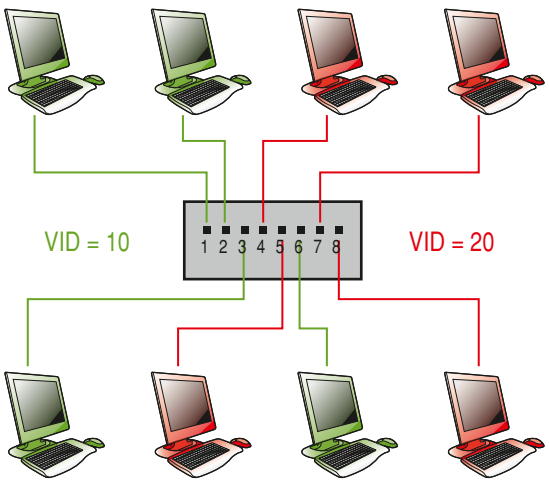
La realizzazione di VLAN può avvenire secondo due modalità:
- VLAN port based (untagged LAN o private VLAN);
- VLAN tagged (802.1Q).

In ogni caso devono essere definite le VLAN all'interno del bridge, con nome e numero identificativo per distinguerle una dall'altra: per prima cosa è necessario identificare ogni VLAN mediante un numero, il VID (Virtual Identificator), che ha range 1-1005 e un proprio blocco di indirizzi.

Per poter gestire più reti virtuali sulla stessa struttura fisica i bridge devono saper svolgere tre funzioni:
- ingress: il bridge deve essere in grado di capire a quale VLAN appartenga un frame in ingresso da una porta;
- forwarding: il bridge deve conoscere verso quale porta deve essere inoltrato il frame verso destinazione in base alla VLAN di appartenenza;
- egress: il bridge deve poter trasmettere il frame in uscita in modo che la sua appartenenza alla VLAN venga correttamente interpretata da altri bridge a valle.

Individuazione delle VLAN da parte degli switch

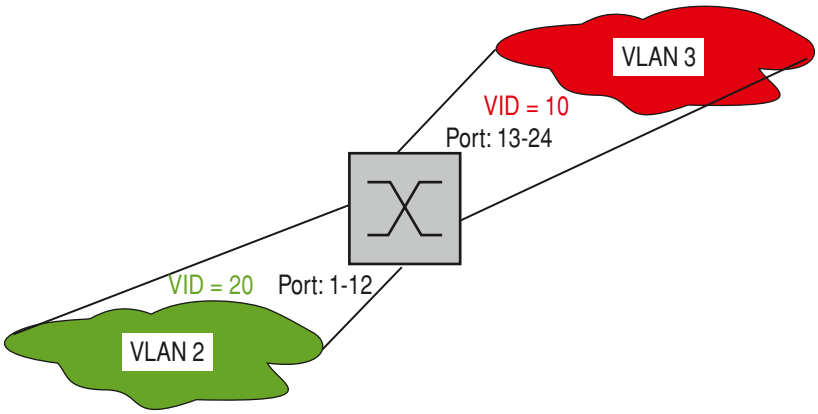
Una delle applicazioni più semplici realizzate tramite una VLAN è quella di "tagliare" un unico switch fisico in due o più reti diverse.
Potremmo ad esempio realizzare come in figura due reti isolate utilizzando un unico switch:
- A la rete rossa è una VLAN con VID 20 e collega i 4 host (porta 4,5,7,8);
- B la rete verde è una VLAN con VID 10 e collega i 4 host (porta 1,2,3,6).



Gli host "verdi" vedranno solo gli host "verdi", e analogo discorso vale per quelli rossi: senza le VLAN sarebbe necessario utilizzare *due switch* diversi, uno per ogni VLAN.

Una volta definita una VLAN, ci sono sostanzialmente due tecniche per associarvi degli host:

- utilizzando i numeri di "porta" dello switch: potremmo decidere che la prima metà delle porte è riservata agli host della VLAN 20 e le rimanenti per quelli della VLAN 10; questo è il sistema più semplice ma ha grossi limiti di sicurezza in quanto il concentratore associa una sua porta alla VLAN e non a un host: qualunque "dispositivo" venga connesso alla porta diviene parte della VLAN;



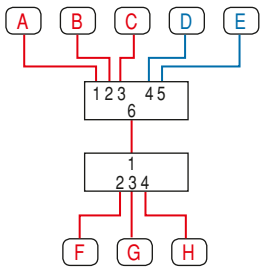
- utilizzando degli indirizzi delle interfacce di rete degli host: se si associano alla VLAN i singoli indirizzi degli host si realizza un sistema più sicuro; in questo caso un host viene collegato a una qualunque porta dello switch dato che viene riconosciuta la sua appartenenza alla VLAN o per mezzo del suo indirizzo IP, che sappiamo però poter essere modificabile in qualsiasi momento, oppure l'indirizzo MAC, che è unico e immutabile per ogni interfaccia.

Port based VLAN (untagged)

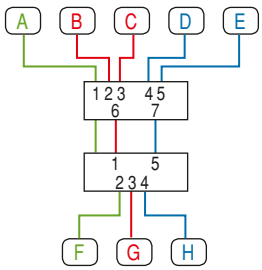
Le VLAN che utilizzano i numeri di "porta" dello switch, cioè l'assegnazione statica di ciascuna porta del bridge a una VLAN, prendono il nome di Port based LAN.
Le porte possono essere assegnate a VLAN differenti e in questo modo si realizza un partizionamento del bridge in due o più bridge logici.

ESEMPIO

In questo esempio abbiamo due VLAN, una delle quali è limitata a un singolo switch.



In questo secondo esempio abbiamo tre VLAN e ciascuna crea una connessione "virtuale" tra i due switch.



Le operazioni che devono svolgere i bridge sono particolarmente semplici:

- ingress: un frame in ingresso appartiene alla VLAN a cui è assegnata la porta, quindi non è richiesto nessun altro "meccanismo "di riconoscimento di appartenenza sul frame;
- forwarding: il frame può essere inoltrato solo verso porte appartenenti alla stessa VLAN a cui appartiene la porta di ingresso che è mappato in un forwarding database, distinto per ogni VLAN;
- egress: una volta determinata la porta (o le porte) attraverso cui deve essere trasmesso il frame, questo può essere trasmesso così come è stato ricevuto, senza che venga modificato.

Non è quindi necessario che le VLAN untagged richiedano l'osservanza dello standard 802.1Q dato che tutta la gestione è fatta all'interno dello switch che deve essere opportunamente configurato (e configurabile).

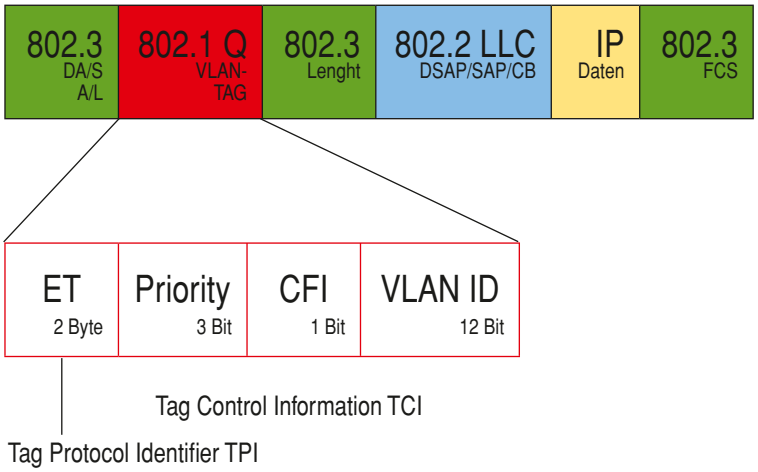
VLAN 802.1Q (tagged VLAN)

La tecnologia che permette di far condividere una VLAN a due o più switch mediante una modifica del formato del frame ethernet è quella che utilizza lo standard 802.1Q, la quale aggiunge 4 byte (TAG) che trasportano le informazioni sulla VLAN e altre aggiuntive.

Questa tecnologia prende il nome di tagged VLAN, anche chiamata VLAN trunking.

I primi 2 byte sono chiamati Tag Protocol Identifier (TPI) e contengono il tag EtherType (valore 0x8100), numero che evidenzia il nuovo formato del frame. I successivi 2 byte sono chiamati Tag Control Information TCI (o VLAN Tag), così strutturati:

- user_priority: campo a 3 bit che può essere utilizzato per indicare un livello di priorità per il frame;
- CFI: campo di 1 bit che indica se i MAC address nel frame sono in forma canonica;
- VID: campo di 12 bit che indica l'ID delle VLAN; con 12 bit possono essere definite 4096 VLAN: la prima (VLAN 0) e l'ultima (VLAN 4095) sono riservate, quindi gli ID realmente usabili sono 4094.

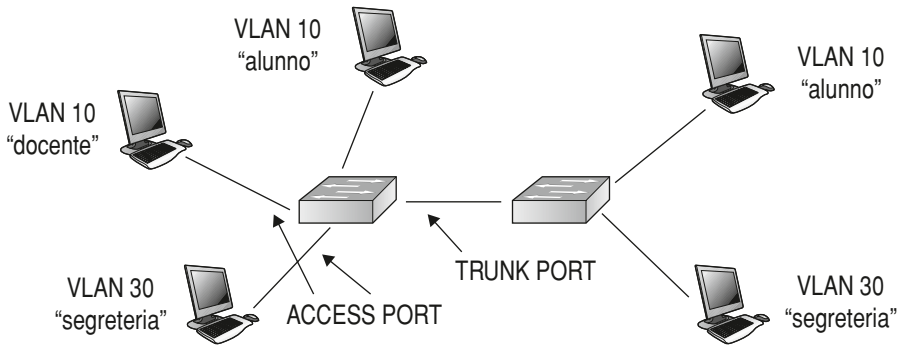


Con queste "aggiunte" è possibile che il frame possa superare la lunghezza di 1518 byte, limite massimo dello standard Ethernet: i bridge che ammettono standard 802.1Q devono poter accettare frame con 2 byte in più.

I pacchetti con questo formato non possono arrivare su qualsiasi porta dello switch in quanto questo deve essere in grado di interpretarli: è necessario avere una classificazione anche delle porte, che possono essere distinte in porte trunk/tagged e porte untagged:

- se la porta è associata a una VLAN "port based" (untagged) i frame ricevuti da quella porta non necessitano (e non trasportano) tag TPI e TCI, né dovranno trasportarla i frame in uscita; queste porte sono chiamate porte d'accesso (access port) e il link attestato su tali porte si dice access link;
- se la porta è associata a una o più VLAN in modalità tagged, i frame trasporteranno le informazioni di TAG e la VLAN di appartenenza del frame è definita dal valore inserito nel TAG: queste porte sono chiamate porte Trunk e il link associato a tali porte si dice trunk link.

Osservando la rete rappresentata nella figura possiamo sicuramente affermare che le porte che connettono i due dispositivi devono essere trunk in quanto in esse circoleranno frame di più VLAN.



Porte ibride

Lo standard VLAN 802.1Q richiede che una porta deve poter essere utilizzata in entrambe le modalità cioè deve poter essere associata a una VLAN in modalità untagged oppure ad altre VLAN in modalità tagged: in questo caso si parla di hybrid port.
Questa porta, come primo passo, riconosce se nel frame vi sono i tag TGI e TCI: se questi non sono presenti, il frame è del tipo untugged e quindi la porta funzionerà in tale modalità, se invece sono presenti, questi vengono analizzati e la VLAN di appartenenza viene individuata dal valore del VID.

> La VLAN a cui la porta è associata in modalità untagged viene anche detta PVID (Private Vlan ID).

Le operazioni che devono svolgere i bridge in questi casi sono diverse da quelle descritte per le VLAN untagged:

- ingress: per prima cosa il bridge deve riconoscere il tipo di frame e identificare la VLAN di appartenenza e quindi:
  - se il frame è untagged, la VLAN di appartenenza è identificata con la VLAN a cui la porta è associata in modalità untagged;
  - se il frame è tagged, la VLAN di appartenenza viene identificata dai TAG;
- forwarding: una volta identificata la VLAN di appartenenza vengono applicate le regole di forwarding e viene identificata la porta di uscita:

- egress: in questo caso può essere necessario effettuare l'inserimento e la rimozione dei TAG:
  - se il frame in ingresso è di tipo 802.1Q e la porta in uscita è associata alla VLAN di appartenenza in modalità tagged, il frame viene inoltrato senza modifiche;
  - se il frame in ingresso è untagged e la porta in uscita è associata alla VLAN di appartenenza in modalità untagged, il frame viene inoltrato senza modifiche;
  - se il frame in ingresso è di tipo 802.1Q e la porta di uscita è in modalità untagged è necessario rimuovere la TPI e TCI prima di effettuare l'inoltro;
  - se il frame in ingresso è di tipo 802.3 e la porta di uscita è associata alla VLAN di appartenenza in modalità tagged è necessario inserire TPI e TCI prima di effettuare l'inoltro.

Negli ultimi due casi il bridge deve ricalcolare il valore del CRC del frame prima di ritrasmetterlo.

Naturalmente in una rete possono coesistere apparati che non supportano il protocollo 802.1Q: questi saranno connessi su porte del bridge associate esclusivamente a una VLAN in modalità untagged in modo che ogni frame ricevuto sarà associato a una VLAN e nessun frame di tipo 802.1Q sarà inoltrato verso l'apparato a valle, in quanto prima di arrivare al frame vengono rimossi i TAG.
In questo modo non è necessario sostituire tutto l'hardware esistente nel caso si voglia realizzare una VLAN: basta inserire in modo opportuno solo alcuni apparati 802.1Q e integrarli con l'hardware esistente, senza doverlo sostituire.
Anche le schede di rete presenti sugli host devono essere compatibili, e generalmente non lo sono: deve inoltre essere installato l'apposito driver e, infine, è necessario che il sistema operativo fornisca la possibilità di utilizzare le VLAN.

È buona norma non utilizzare le VLAN per isolare le diverse zone della rete, ad esempio per ospitare una DMZ, perché il traffico tra le VLAN è spoofabile, cioè facilmente falsificabile: è quindi sempre meglio affidarsi a un firewall per isolare le zone tra le quali la sicurezza del traffico è un fattore critico.

Verifichiamo le conoscenze

Esercizi a scelta multipla

1 Quale standard definisce le virtual LAN?

a) lo standard 802.1L
b) lo standard 802.1P
c) lo standard 802.1Q
d) lo standard 802.1V

2 Le VLAN sono in grado di:

a) consentire a postazioni attestate su segmenti di rete fisicamente distinti, di apparire connessi alla stessa rete logica
b) consentire a postazioni attestate su segmenti di rete fisicamente distinti, di apparire connessi alla stessa rete fisica
c) separare postazioni che sono sulla stessa rete fisica in più reti logiche distinte
d) separare postazioni che sono sulla stessa rete logica in più reti fisiche distinte

3 I principali vantaggi che derivano dall'utilizzo delle VLAN sono (indicare quelli errati):

a) risparmio
b) aumento di prestazioni
c) riduzione di occupazione di memoria
d) aumento della sicurezza
e) aumento della velocità di trasmissione
f) flessibilità

4 Il VID ha range:

a) 0-105
b) 1-105
c) 5-105
d) 0-1005
e) 1-1005
f) 5-1005

5 Per poter gestire più VLAN sulla stessa struttura fisica i bridge devono svolgere le funzioni di:

a) ingress
b) forwarding
c) wireless
d) espress
e) egress

6 I primi byte aggiunti nelle tagged VLAN sono chiamati:

a) Tag Protocol Identifier (TPI)
b) Tag Control Information TCI (o VLAN Tag)
c) Tag VLAN Definition (o VLAN Tag)
d) Tag Data Information TDI

Test vero/falso

1 La VLAN permette a computer anche collocati in luoghi non vicini fisicamente di comunicare come se fossero sulla stesso *dominio di collisione*. V F
2 La connettività tra diverse VLAN può essere realizzata a livello 2. V F
3 Una utenza può vedere solo il traffico della propria VLAN e non delle altre. V F
4 Il VID distingue le VLAN port based da quelle VLAN tagged. V F
5 Nelle VLAN è preferibile utilizzare l'indirizzo IP piuttosto che il MAC per riconoscere un host. V F
6 Le VLAN che utilizzano i numeri di "porta" dello switch prendono il nome di Port based LAN. V F
7 Nelle VLAN untagged tutta la gestione è fatta all'interno dello switch. V F
8 Nelle VLAN trunking vengono aggiunti 4 byte al frame ethernet. V F
9 Il frame VLAN non deve comunque superare la lunghezza massima del frame ethernet. V F
10 La VLAN a cui la porta è associata in modalità untagged viene anche detta PVID. V F
11 Sono presenti quattro casi nei quali il bridge deve ricalcolare il valore del CRC del frame. V F

Lezione 2

IL PROTOCOLLO VTP E L'INTER-VLAN ROUTING

IN QUESTA UNITÀ IMPAREREMO...

- il protocollo VTP
- la configurazione delle VLAN
- l'Inter-VLAN Routing

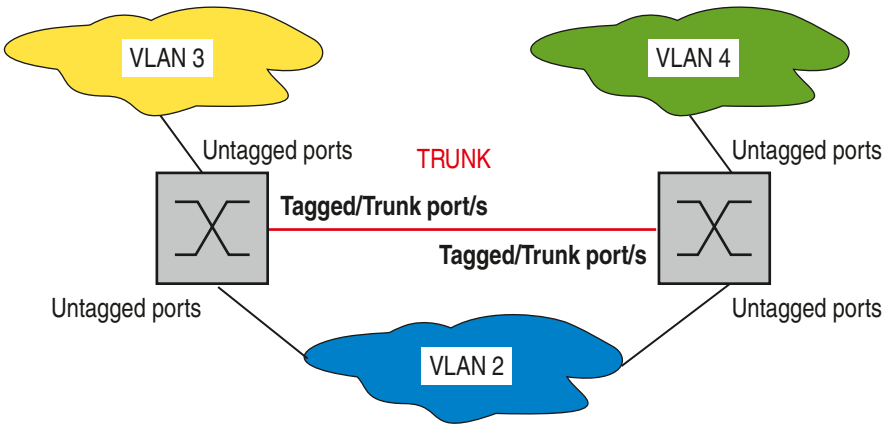
VLAN condivise su più di un switch

La suddivisione di una rete in VLAN risponde da una parte a motivi di sicurezza, poiché diminuisce le possibilità di accesso indebito, dall'altra a motivi di prestazioni della rete, in quanto riduce il numero degli hops per il router, aumenta l'ampiezza di banda per il singolo utente e riduce il traffico broadcast.

TRUNK

Con il termine trunk si intende la connessione punto-punto tra due porte trunk di uno switch.

Una VLAN può essere estesa a due o più switch proprio come una normale LAN e ogni switch presente nella rete LAN deve essere configurato; se la LAN ha dimensioni elevate è evidente come la gestione risulta complessa e inoltre possono facilmente essere introdotti degli errori.



I frame che attraversano un trunk sono tutti "tagged" a eccezione di quelli appartenenti alla Native VLAN, che viene usata solo per il traffico di controllo.

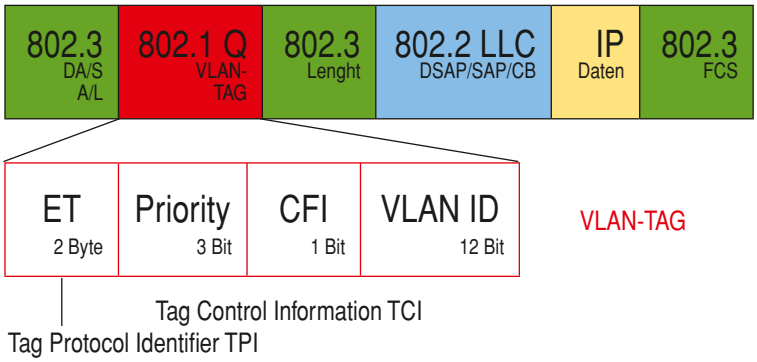
La configurazione della Native VLAN è la seguente:

```
Router (config)# interface FastEthernet o/x
Router (config-if)# switchport mode trunk
Router (config-if)# switchport trunk native vlan 99
```

Di default la porta trunk accetta tutte le VLAN ma è anche possibile configurare solo un sottoinsieme di VLAN consentite su un trunk con il comando:

```
Router (config-if)# switchport trunk allowed vlan y
```

La tecnologia che permette di far condividere una VLAN a due o più switch è detta VLAN trunking e sappiamo che si avvale di un preambolo di 2 byte, il VLAN-TAG, aggiunto al pacchetto prima della "parte" 802.3.



Quindi due switch si connettono tra loro con una porta trunk di tipo tagged in modo da condividere e gestire più VLAN in comune: ogni switch deve essere opportunamente configurato.

Cisco VTP-VLAN Trunking Protocol

Il protocollo Virtual Trunking Protocol (VTP), proprietario della CISCO, consente di configurare le VLAN su un solo switch, che si occupa poi di distribuire le VLAN a tutti gli switch della rete: quindi riduce drasticamente la configurazione manuale degli switch.

VTP può essere configurato su Switch Cisco in tre modalità:
- Client;
- Server;
- Transparent.

Solo sugli Switch in modalità "Server" l'amministratore di rete può modificare la configurazione delle VLAN: quando viene fatta una modifica questa automaticamente viene distribuita a tutti gli Switch del trunk VLAN:
- gli apparati in modalità "Transparent" reinviano le modifiche a tutti gli altri apparati a esso collegati;
- gli apparati in modalità "Client" prima applicano la modifica a se stessi e quindi la reinviano.

L'informazione viene propagata in base a mappe di raggiungibilità che l'algoritmo Spanning Tree (ST) ha costruito in maniera automatica.
Ogni modifica viene numerata con un *"version number"* e ogni apparato in modalità "Client" applica la modifica a se stesso solo se risulta avere un *"version number"* maggiore di quello attuale: se si aggiunge un nuovo componente alla VLAN si deve ripartire da zero per evitare conflitti e quindi tutti i *"version number"* vengono resettati.

Il comando che consente di valutare la configurazione VTP di uno switch è

```
Switch# show vtp status
```

```
Switch0>show vtp status
VTP Version                     : 2
Configuration Revision          : 4
Maximum VLANs supported locally : 255
Number of existing VLANs        : 7
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xFC 0xCA 0xC6 0x4B 0x09 0x14 0x7E 0x79
Configuration last modified by 0.0.0.0 at 3-1-93 00:22:37
Local updater ID is 0.0.0.0 (no valid interface found)
Switch0>
```

I parametri da configurare sono:

VTP version: esistono tre versioni del protocollo VTP (1, 2 e 3): di default la versione 1 e, solo nei dispositivi più recenti, la 2;

VTP mode: sono le tre modalità prima descritte (Client, Server, Transparent): di default uno switch si trova in modalità Server;

VTP Domain Name: un VTP Domain è un insieme di switch che si scambiano VTP advertisement per la distribuzione delle VLAN e uno switch può appartenere a un solo dominio VTP alla volta; il valore di default per il VTP Domain Name è "null";

Zoom su...

VTP ADVERTISEMENT

Un messaggio VTP è inviato ogni volta che bisogna propagare informazioni sulle VLAN: esistono tre tipi di VTP Advertisement:

- summary: contengono il VTP Domain Name e il Config Revision: sono inviate ogni 5 minuti e hanno lo scopo di informare i vicini del corrente VTP Config Revision;
- subset: contengono informazioni sulle VLAN (inserimento, cancellazione, modifica);
- request: inviate a un VTP server per richiedere l'invio di un messaggio Summary e di eventuali messaggi subset.

Config Revision (version number): è un contatore inizialmente impostato a zero che viene incrementato di uno ogni qual volta si verifica una modifica, cioè se viene aggiunta o rimossa una VLAN, in modo che gli switch sono in grado di valutare se le informazioni VTP memorizzate sono o meno aggiornate.

I comandi per modificarne i valori iniziano con vtp seguito semplicemente dal nome dell'opzione e dal valore alla quale deve essere settato:

```
Switch0(config)#vtp ?
  domain    Set the name of the VTP administrative domain.
  mode      Configure VTP device mode
  password  Set the password for the VTP administrative domain
  version   Set the adminstrative domain to VTP version
Switch0(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch0(config)#
```

Configurazione delle VLAN

Per creare una VLAN si procede son le seguenti operazioni:
a) ci si collega via Telnet allo switch;
b) si accede mediante il comando "Configure terminal";
c) il prompt diventerà *nomeswitch (config)#*;
d) con il comando vlan *{id_vlan}* si assegna un numero identificativo alla nuova VLAN diverso da 1, dato che la vlan 1 è quella cui per default sono assegnate tutte le porte dello switch.

ESEMPIO

Definiamo la VLAN con VID 10 e configuriamo un host con nome docente, come in figura:


```
Switch (config)# VLAN 10
```

È utile ai fini pratici assegnare anche un nome con il comando:

```
Switch (config)# name docente
```

Terminata la creazione, si esce dal Global configuration mode con exit.

Per verificare le operazioni effettuate si utilizza il comando:

```
Switch (config)# show vlan
```

Per salvare la configurazione si utilizza il comando:

```
Switch# copy running-config startup-config
```

Riepiloghiamo la sequenza di operazioni che ci permette di creare la VLAN 20, assegnarle il nome alunni e aggiungerla al database delle VLAN.

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name alunni
Switch(config-vlan)# end
Switch# show vlan
Switch# copy running-config startup-config
```

È possibile portare rettifiche ai parametri di una VLAN sempre utilizzando i sopra elencati comandi; è inoltre possibile eliminare una VLAN tramite il comando:

```
Switch(config)# no vlan 20
```

sempre digitandolo nel Global configuration mode.

> Naturalmente, a cancellazione avvenuta, la configurazione deve essere salvata con il solito copy running-config startup-config. In modo analogo si procede nel vlan configuration mode.

Per assegnare una porta a una VLAN si definisce prima l'interfaccia che si vuole assegnare alla VLAN, si precisa la modalità per la porta e quindi si assegna la porta.

I seguenti comandi ci permettono di assegnare alla vlan 20 la porta 0/1:

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1     // scelta dell'interfaccia
Switch(config-if)# switchport mode access     // modalità per la porta
Switch(config-if)# switchport access vlan 20 // assegnazione della porta
Switch(config-if)# end
```

Per verificare la corretta configurazione della porta si utilizza il comando:

```
Switch# show running-config interface fastethernet0/1
```

mentre per verificare l'assegnazione della porta si utilizza:

```
Switch# show interface fastethernet0/1
```

Per salvare la configurazione si utilizza il comando:

```
Switch# copy running-config startup-config
```

Inter-VLAN Routing

Le VLAN possono estendersi al di là dei limiti fisici dei singoli switch, tramite il VLAN tagging: la VLAN coinvolge quindi dei router, che devono essere appositamente configurati.

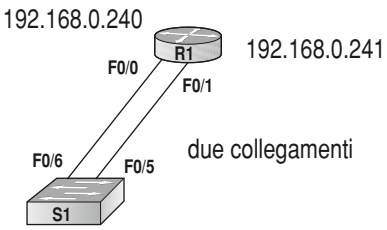
> Anche per consentire la comunicazione tra VLAN diverse è necessario introdurre nella LAN un router o uno switch di livello 3.
> In questo caso si parla di inter-VLAN Routing.

Il protocollo 802.1Q, che regola le VLAN, prevede che ciascun frame ethernet venga "etichettato" con le informazioni relative alla VLAN di appartenenza.

Sono disponibili tre soluzioni:
- Inter-VLAN tradizionale;
- "Router-on-a-stick" Inter-VLAN;
- Switch-based Inter-VLAN.

Inter-VLAN tradizionale

Per far cominciare due VLAN il modo più semplice è quello di inserire un router e connetterlo a uno degli switch della LAN: la connessione tra il router e lo switch deve essere fatta con un numero di interfacce fisiche pari al numero delle VLAN che devono poter comunicare tra di loro. ▶



Dato che a ogni interfaccia fisica del router è associata a una VLAN, questa deve avere un indirizzo IP appartenente a tale VLAN.

> Le porte dello switch connesse al router devono essere impostate in modalità access.

Vediamo come deve essere la corretta configurazione delle interfacce del Router con la corretta assegnazione degli indirizzo IP:

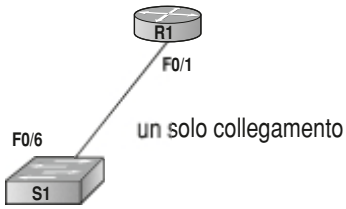
```
R1(config)# interface Fa 0/0
R1(config-if)#ip address 192.168.0.240 255.255.255.0
R1(config-if)# no shutdown
R1(config)# interface Fa 0/1
R1(config-if)#ip address 192.168.0.241 255.255.255.0
R1(config-if)# no shutdown
```

Sullo switch configuriamo le interfacce delle porte connesse al router in modalità access seguita dalla indicazione del nome della VLAN:

```
S1(config)# vlan 10
S1(config)# interface Fa 0/6
S1(config-if)# switchport access vlan 10
S1(config)# vlan 30
S1(config)# interface Fa 0/5
S1(config-if)# switchport access vlan 30
```

"Router-on-a-stick" Inter-VLAN

In questo caso il router viene connesso a uno degli switch della LAN con una sola interfaccia fisica. ▶



Opereremo una "suddivisione" dell'interfaccia fisica in tante interfacce virtuali quante sono le VLAN che possono comunicare tra di loro: ogni interfaccia virtuale (subinterface) del router è associata a una VLAN e deve quindi avere un indirizzo IP appartenente a tale VLAN.

> La porta dello switch connessa al router deve essere impostata in modalità trunk.

ESEMPIO

Supponiamo di avere tre VLAN, (vlan10, vlan20 e vlan30): l'interfaccia del router che lo connette allo switch deve essere suddivisa in 3 subinterfaces e a ogni subinterface deve essere associata una VLAN.

```
R1(config)# interface Fa 0/0.10
R1(config-if)# encapsulation dot1q 10
R1(config-if)#ip address 192.168.0.240 255.255.255.0
R1(config)# interface Fa 0/0.20
R1(config-if)# encapsulation dot1q 20
R1(config-if)# ip address 192.168.0.240 255.255.255.0
R1(config)# interface Fa 0/0.30
R1(config-if)# encapsulation dot1q 30
R1(config-if)# ip address 192.168.0.240 255.255.255.0
R1(config)# interface Fa 0/0
R1(config-if)# no shutdown
```

Sullo switch configuriamo le interfacce delle porte connesse al router in modalità trunk:

```
S1(config)# vlan 10
S1(config)# vlan 20
S1(config)# vlan 30
S1(config)# interface Fa 0/1
S1(config-if)# switchport mode trunk
```

Verifichiamo le conoscenze

Esercizi a scelta multipla

1 La suddivisione di una rete in VLAN (indica la motivazione errata):

a) diminuisce le possibilità di accesso indebito
b) riduce il numero degli hops per il router
c) aumenta l'ampiezza di banda per il singolo utente
d) riduce le possibilità di errore di indirizzamento
e) riduce il traffico broadcast

2 VTP può essere configurato su Switch Cisco in tre modalità:

a) Client
b) Server
c) Hybrid
d) Transparent

3 I parametri VTP da configurare sono (indica quello errato):

a) VTP version
b) VTP configuration revision
c) VTP mode
d) VTP Domain

4 Esistono tre tipi di VTP Advertisement:

a) summary
b) subset
c) request
d) responce

5 Quale tra i seguenti parametri non è messaggio contenuto nel subset?

a) Inserimento
b) Cancellazione
c) Modifica
d) Configurazione

6 Ordina la sequenza di operazioni necessarie per assegnare una porta a una VLAN:

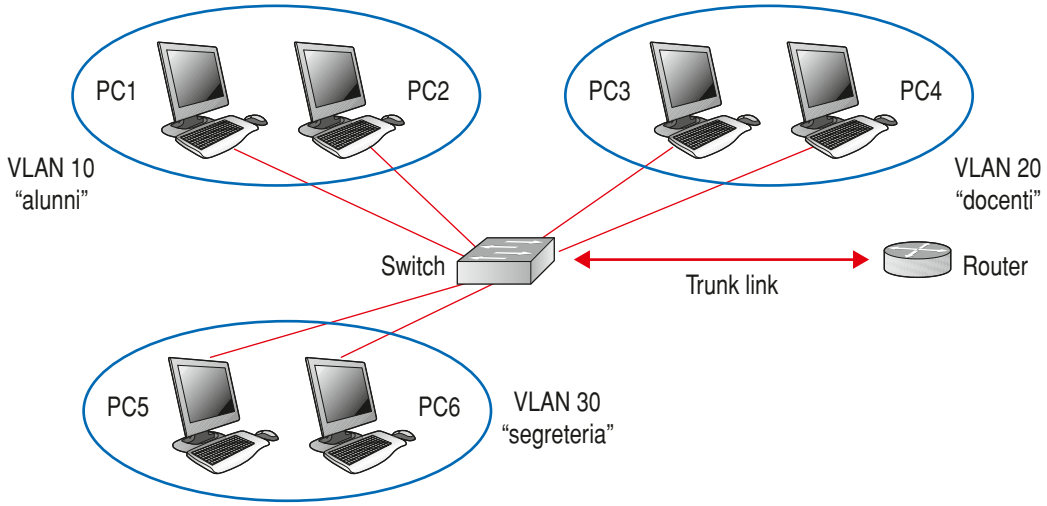
a) ..... si assegna la porta.
b) ..... si definisce l'interfaccia
c) ..... si precisa la modalità per la porta

Test vero/falso

1 Con il termine trunk si intende la connessione punto-punto tra due porte trunk di un router. V F
2 I frame che attraversano un trunk sono tutti "tagged". V F
3 Solo sugli switch in modalità "Server" si può modificare la configurazione delle VLAN. V F
4 Il "version number" indica la versione del VTP negli switch Cisco. V F
5 Esistono tre versioni del protocollo VTP; di default è configurato a 2. V F
6 Uno switch può appartenere a un solo dominio VTP alla volta. V F
7 Il comando "copy running-config startup-config" serve per fare una copia di backup. V F
8 Il VLAN tagging permette di estendersi al di là dei limiti fisici dei singoli switch. V F
9 Nell'Inter-VLAN tradizionale le porte dello switch sono connesse al router. V F
10 Nella "Router-on-a-stick" la porta dello switch connessa al router deve essere trunk. V F

Verifichiamo le competenze

1 Data la topografia di rete di figura si configuri lo switch seguendo le indicazioni dei commenti:



Soluzione

Prima di procedere alla configurazione dello switch assegniamo le porte alle funzioni preposte, come segue:

Porta 16	VLAN 1
Porta 17	
Porta 18	VLAN 2
Porta 19	
Porta 22	VLAN 3
Porta 23	
Porta 20	Porta TRUNK

```
configure terminal
.......................................
.......................................        crea ID VLAN1 e assegna il nome
end

.......................................
.......................................        crea ID VLAN2 e assegna il nome
end

.......................................
.......................................
.......................................        crea ID VLAN3 e assegna il nome
end
.......................................        salva la configurazione
.......................................        verifica la configurazione
```

```
.....
.....          0/16 configurazione VLAN1 sulla porta 16
.....
.....
end
.....          salva configurazione VLAN1 porta 16

.....
.....          0/17 configurazione VLAN1 sulla porta 17
.....
.....
end
.....          salva configurazione VLAN1 porta 17

.....
.....          configurazione VLAN2 sulla porta 18
.....
.....
end
.....          salva configurazione VLAN2 porta 18

.....
.....          configurazione VLAN2 sulla porta 19
.....
.....
end
.....          salva configurazione VLAN2 porta 19

.....
.....          configurazione VLAN3 sulla porta 22
.....
.....
end
.....          salva configurazione VLAN3 porta 22

.....
.....          configurazione VLAN3 sulla porta 23
.....
.....
end
.....          salva configurazione VLAN3 porta 23

.....
.....
.....          assegnazione della porta 20 all'acces-
               so di tipo trunk
end
.....          salva configurazione
```