Reti Avanzate — Sicurezza dei Dati
A.A. 2017–2018, secondo semestre
Traccia delle lezioni

Mauro Brunato

Versione 2018-02-26

Caveat lector

Lo scopo principale di questi appunti è quello di ricostruire quanto detto a lezione. Queste note non sono complete, e la loro lettura non permette, da sola, di superare l'esame. Le fonti utili a ricostruire un discorso coerente e completo sono riportate alla pagina web del corso, dov'è disponibile anche la versione più recente di queste note:

`http://disi.unitn.it/~brunato/RetiAvanzate/`

Alcune fonti per approfondimenti sono indicate nelle note a pie' di pagina di questo documento.

Si suggerisce di confrontare la data riportata sul sito web con quella che appare nel frontespizio per verificare la presenza di aggiornamenti.

Alcune esercitazioni di laboratorio non sono riportate in questa dispensa perché descritte dal codice commentato disponibile alla pagina web del corso, oppure riportate in dettaglio in un documento a sé stante.

Changelog

2018-02-26

Versione iniziale

- Livello Data Link: protocollo Ethernet, hub, switch
- Reti locali virtuali (VLAN)
- Domande di comprensione sul livello Data Link
- Prima esercitazione

Indice

Parte I

Appunti di teoria

Capitolo 1

Livello 2: Data Link

1.1 Le reti locali (Local Area Networks, LAN), Ethernet

Una LAN[1] è una rete privata tra terminali "fisicamente" vicini (fino a qualche chilometro), connessi mediante schede di rete ed opportuno cablaggio (hub, switch, cavi rame o fibra, onde radio).

Ethernet[2] è ormai lo standard *de facto* nelle LAN. È nata come sistema broadcast su canale (bus) condiviso (trasmissione simultanea a più stazioni in banda base, ossia usando tutta la banda disponibile, su cavo coassiale), e si è sviluppata adottando man mano strategie più efficienti (collegamenti punto a punto, doppini intrecciati, fibra ottica).

L'indirizzamento Ethernet è "piatto", non riflette la topologia della rete: ogni scheda terminale ha un identificativo unico, fissato nel firmware (indirizzo MAC, MAC address)[3], da 48 bit (6 byte); l'intestazione Ethernet riporta, nell'ordine, il MAC address del destinatario, quello del mittente e un identificativo da 2 byte del protocollo usato nel payload.

1.1.1 Apparati di rete

Un *hub*[4] è un dispositivo di livello fisico che replica il segnale entrante in una porta su ogni altra porta, opportunamente ripulito e amplificato.

Uno *switch*[5] è un dispositivo di livello 2 che inoltra una trama Ethernet entrante esclusivamente sulle porte dove è possibile che il destinatario sia in ascolto. Per fare ciò, lo switch mantiene una tabella (dizionario) che associa a ogni indirizzo MAC già noto la porta a cui è collegato (vedi Fig. 1.1).

Un moderno cablaggio Ethernet prevede una gerarchia di switch ad albero, nella quale i terminali sono le foglie, con eventuali collegamenti ridondati per evitare che un singolo guasto porti alla partizione della rete.

Possiamo distinguere i dispositivi di una rete locale in *terminali* e *di comunicazione*:

- Dispositivi *terminali* (Data Terminal Equipment, **DTE**)— sono quegli apparati che fungono da mittenti o da destinatari delle trame Ethernet, e le cui porte hanno un indirizzo MAC: PC, stampanti, scanner, telefoni IP...
  Anche i router appartengono a questa categoria: infatti sono i destinatari finali delle trame contenenti un carico di livello rete da inoltrare all'esterno della LAN: anche le loro porte Ethernet hanno un MAC address, perché i PC debbono poter indirizzare le trame in uscita verso di loro.

[1] `https://en.wikipedia.org/wiki/Local_area_network`
[2] `https://en.wikipedia.org/wiki/Ethernet`
[3] `https://en.wikipedia.org/wiki/MAC_address`
[4] `https://en.wikipedia.org/wiki/Ethernet_hub`
[5] `https://en.wikipedia.org/wiki/Network_switch`

```
1.  inizializza tabella ← dizionario vuoto          Inizialmente nessun destinatario
2.  quando ricevi frame F dalla porta P
3.  ⌈ tabella[F.mittente] ← P                       Registra da dove arriva il mittente
4.  ⌊ accoda F, P                                   Metti il frame nella coda di invio
5.  quando estrai F, P dalla coda
6.  ⌈ se esiste tabella[F.destinatario]             Se il destinatario è registrato
7.  |    inoltra F alla porta F.destinatario        Inoltra direttamente
8.  | altrimenti                                    Altrimenti broadcast sulle altre porte
9.  | ⌈ per ogni porta R ≠ P
10. | ⌊    inoltra F alla porta R
```

Figura 1.1: Pseudocodice per il mantenimento di una MAC address table all'interno di uno switch

Figura 1.2: Collegamento DTE-DCE con cavo diretto e collegamento DTE-DTE (o DCE-DCE) con cavo incrociato. In tutti i casi, i piedini di uscita di un dispositivo sono collegati ai corrispondenti piedini di ingresso dell'altro. Nota bene: le pedinature sono esemplificative, non corrispondono a nessuno standard reale.

- Dispositivi *di comunicazione* (Data Communication Equipment, **DCE**) — non sono destinatari finali delle trame, e normalmente le loro porte Ethernet non hanno nemmeno un MAC address. Servono a inoltrare le trame da una porta all'altra.

La distinzione fra DTE e DCE è importante in quanto si riflette sul cablaggio della rete. In base allo standard Ethernet, le pedinature dei connettori DTE e DCE invertono le linee dati di ingresso con quelle di uscita. Di conseguenza (vedere Fig. 1.2):

- I cavi utilizzati per connettere un DTE e un DCE collegano semplicemente i piedini dei connettori aventi numerazione corrispondente (piedino 1 a piedino 1 e così via). In questo modo collegano gli ingressi di un dispositivo alle uscite dell'altro e viceversa. Sono detti cavi "diretti", "straight-through" (o "straight-thru"), o semplicemente "patch".
- I cavi utilizzati per connettere dispositivi della stessa categoria (DTE con DTE, oppure DCE con DCE) invertono coppie corrispondenti di piedini. Sono setti cavi "incrociati", "crosslink", "crossover" o semplicemente "cross"[6].

Domini di collisione e di broadcast

Due dispositivi connessi da un hub non possono trasmettere contemporaneamente: l'hub replicherebbe ciascuno dei due segnali corrompendoli. I due dispositivi appartengono allo stesso *dominio di collisione*[7].

Due dispositivi connessi da uno switch possono trasmettere contemporaneamente (lo switch partecipa al protocollo MAC di Ethernet), quindi uno switch separa i propri ingressi in domini di collisione distinti. Uno switch inoltra i pacchetti broadcast (MAC di destinazione `FF:FF:FF:FF:FF:FF`) su tutte

[6] `https://en.wikipedia.org/wiki/Crossover_cable`
[7] `https://en.wikipedia.org/wiki/Collision_domain`

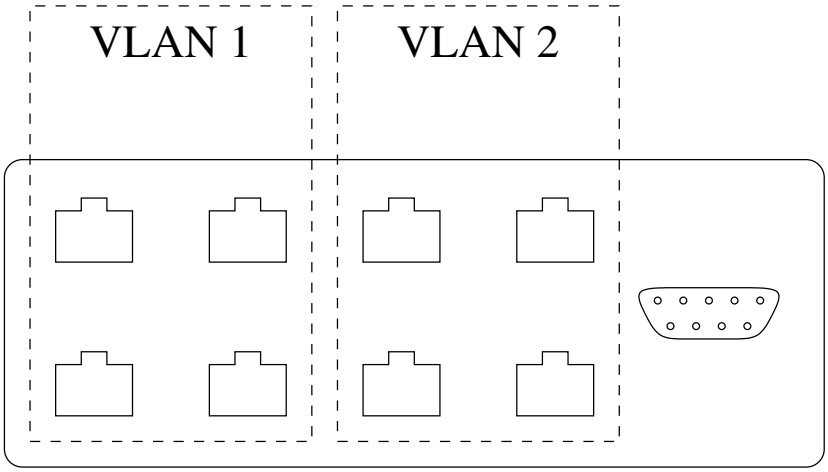

Figura 1.3: Partizione di uno switch in più VLAN.

le uscite. Una rete locale consiste normalmente in pochi domini di broadcast[8] e di molti domini di collisione.

1.2 LAN virtuali (VLAN)

- In uno switch di livello 2 è possibile raggruppare alcune delle porte che lo compongono (o alcuni dei MAC Address ad esso afferenti) a formare un dominio di broadcasting autonomo (VLAN: virtual LAN)[9].
- Creando più VLAN si ottiene quindi un numero equivalente di domini di broadcasting del tutto indipendenti, come se avessimo suddiviso lo stesso switch fisico in più switch logici fra loro separati.
- Il vantaggio sta quindi:
  - nel risparmio economico di acquisto e gestione;
  - nella riduzione del traffico di broadcasting;
  - nella possibilità di gestire con maggior granularità gli aspetti legati alla sicurezza

Nel caso più frequente e più semplice, ogni porta viene assegnata a una specifica VLAN (Fig. 1.3). Nel singolo switch si definiscono i nomi delle varie VLAN (es.: `vlan1`, `vlan2`...) e si associano a ciascuna le relative porte.

Se un host viene spostato da una porta a un'altra occorre riconfigurare lo switch, ma questo offre un vantaggio in termini di sicurezza.

È possibile estendere una VLAN attraverso più switch, come si vede in Fig. 1.4.

Due LAN possono anche essere completamente separate da un punto di vista logico, pur condividendo alcune connessioni. Un collegamento fra switch può essere infatti utilizzato per una sola VLAN, oppure per portare pacchetti di più VLAN diverse, ad esempio quando le stesse VLAN occupano edifici diversi (Fig. 1.5):

[8] `https://en.wikipedia.org/wiki/Broadcast_domain`
[9] `https://en.wikipedia.org/wiki/Virtual_LAN`

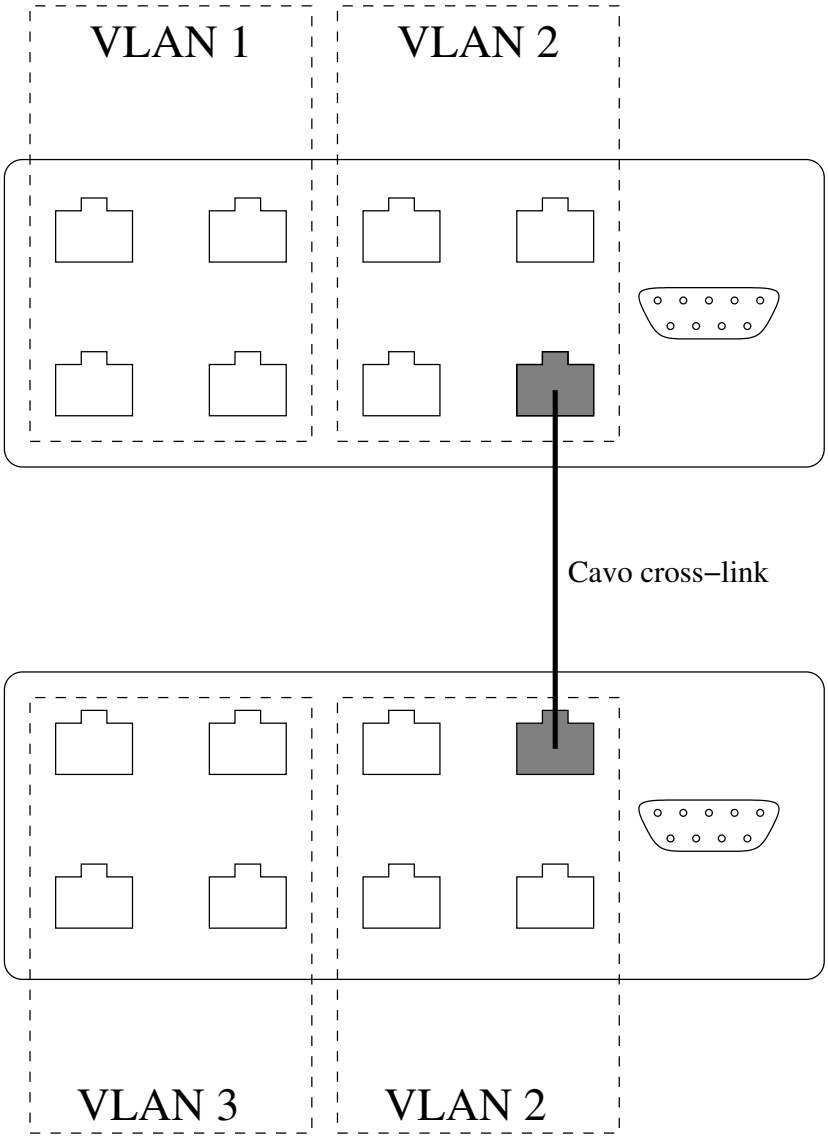

Figura 1.4: Estensione di una VLAN su più switch.

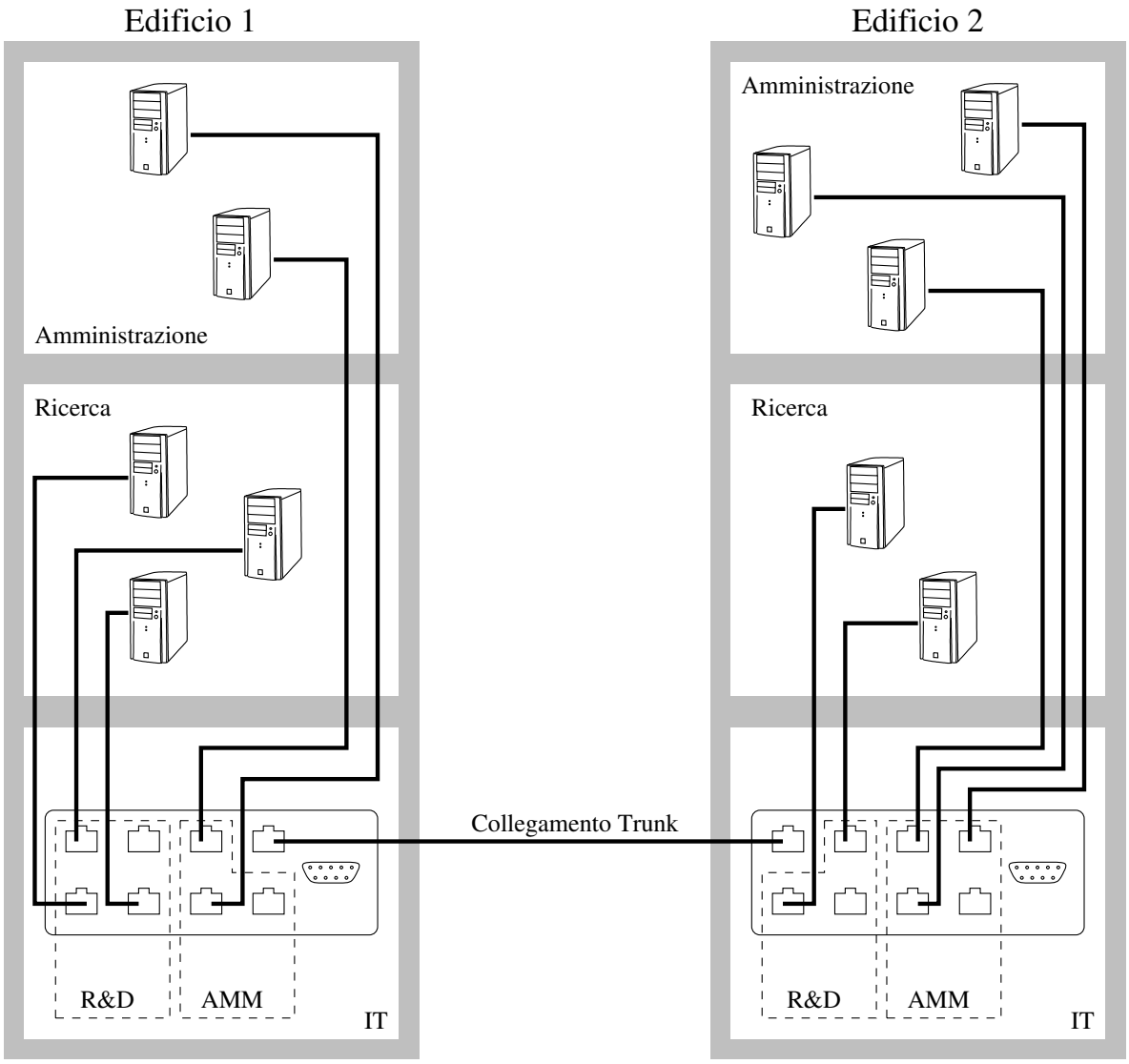

Figura 1.5: VLAN estese fra edifici, con un link condiviso (*trunk link*).

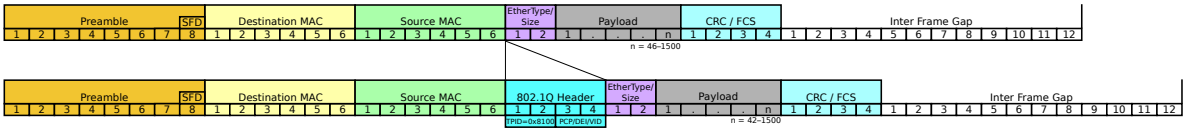

Figura 1.6: Inserimento del tag VLAN in una trama ethernet lungo un trunk link.

- Access link — Nel primo caso, le due porte appartenenti alla connessione sono associate a una VLAN specifica (si dice che sono configurate in modalità *access*). Tutti i pacchetti che transitano per quella linea sono implicitamente appartenenti alla stessa VLAN.
- Trunk link — È il caso più interessante: lo stesso link porta trame appartenenti a varie VLAN. Esempio, il link fra edifici visto in precedenza.

Se più trame possono transitare per lo stesso link, devono contenere l'informazione della VLAN di appartenenza.

La porta che immette la trama nel trunk link inserisce nella trama un campo di 4 byte che contiene il valore identificativo (12 bit) della VLAN. Tale campo è detto *tag*. Lo standard che estende in tal senso la definizione dell'intestazione Ethernet è IEEE 802.1Q.

Come si vede in Fig. 1.6, il campo viene inserito prima del campo Length / Protocol. Contiene:

- Il *Tag Protocol Identifier* (TPID, 2 byte), sempre `0x8100`.
- Il *Tag Control Identifier* (TCID, 2 byte), suddiviso in:
  - *Priority Code Point* (PCP, 3 bit), da 0 a 7;
  - *CanonicalFormat Indicator* (CFI, 1 bit), 0 in Ethernet;
  - *VLAN Identifier* (VID, 12 bit), numero della VLAN.

Il campo addizionale (tag) viene utilizzato dalla porta ricevente per indirizzare il pacchetto esclusivamente alle altre porte dello switch appartenenti alla stessa VLAN.

Una trama che transita attraverso un trunk link è quindi detta "tagged" ("taggata", etichettata) ad indicare che essa contiene l'identificativo della VLAN di appartenenza.

Eccezione

Lungo un trunk link possono anche passare trame senza tag (untagged); esse possono essere associate ad una ed una sola VLAN che viene detta *nativa*.

La Figura 1.7 presenta un esempio di trattamento di una trama mentre transita per i diversi link di tipo access e trunk che connettono la sorgente alla destinazione.

- Tre LAN virtuali: PC1/PC3/PC5/PC7 (`vlan1`), PC2/PC8 (`vlan2`), PC4/PC6 (`vlan3`).
- Una trama da PC1 a PC7 viaggia in modo nativo da PC1 allo switch 1; viene munita di tag nei due segmenti trunk, poi torna in modo nativo nell'ultimo access link.

Una porta di tipo trunk viene utilizzata non solo nei link fra gli switch ma anche nel caso in cui a una porta afferiscano dispositivi diversi (es. un PC ed un telefono VoIP), che inviano/ricevono rispettivamente trame senza tag 802.1Q (PC) e trame con tag (telefono VoIP).

- Il PC invia di solito alla porta trame prive di tag 802.1Q, e non è consapevole dell'esistenza di una LAN virtuale; il telefono invia trame con tag appartenenti ad una VLAN specifica.
- Se lo switch riceve dati da entrambi attraverso una stessa porta, questa viene definita di tipo trunk, ma ad essa viene associata anche una VLAN nativa, in modo che essa possa ricevere le trame prive di tag del PC.

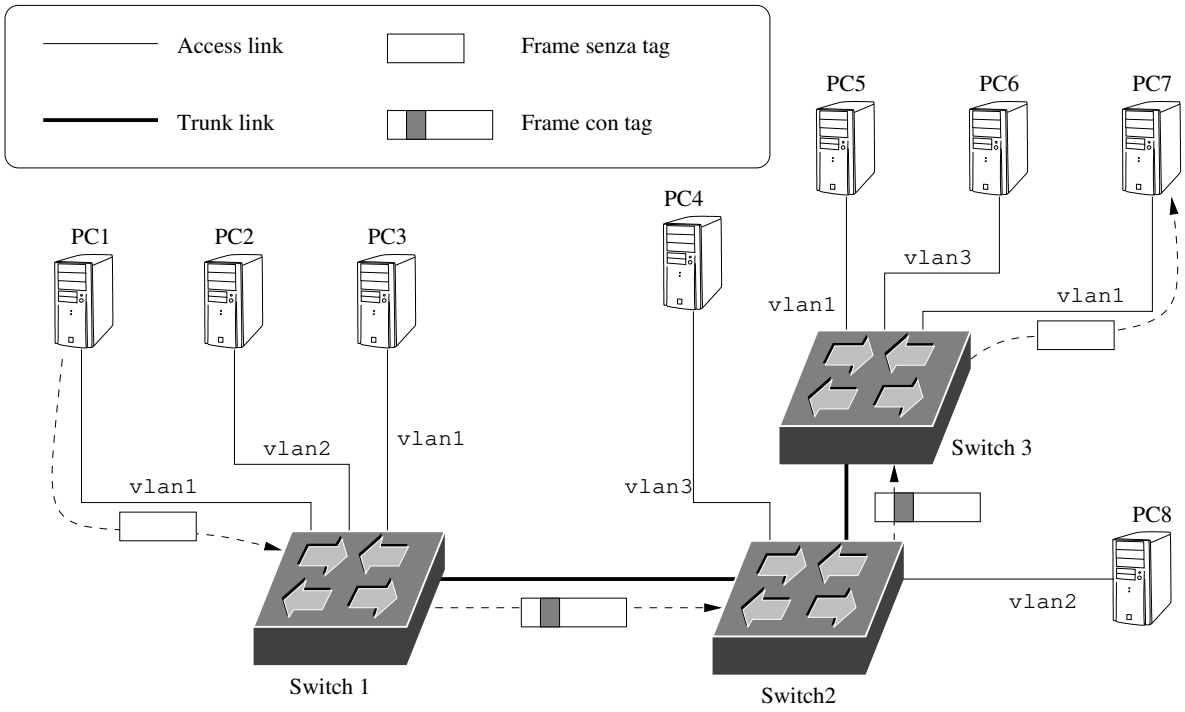

Figura 1.7: Transito di un pacchetto atraverso vari link.