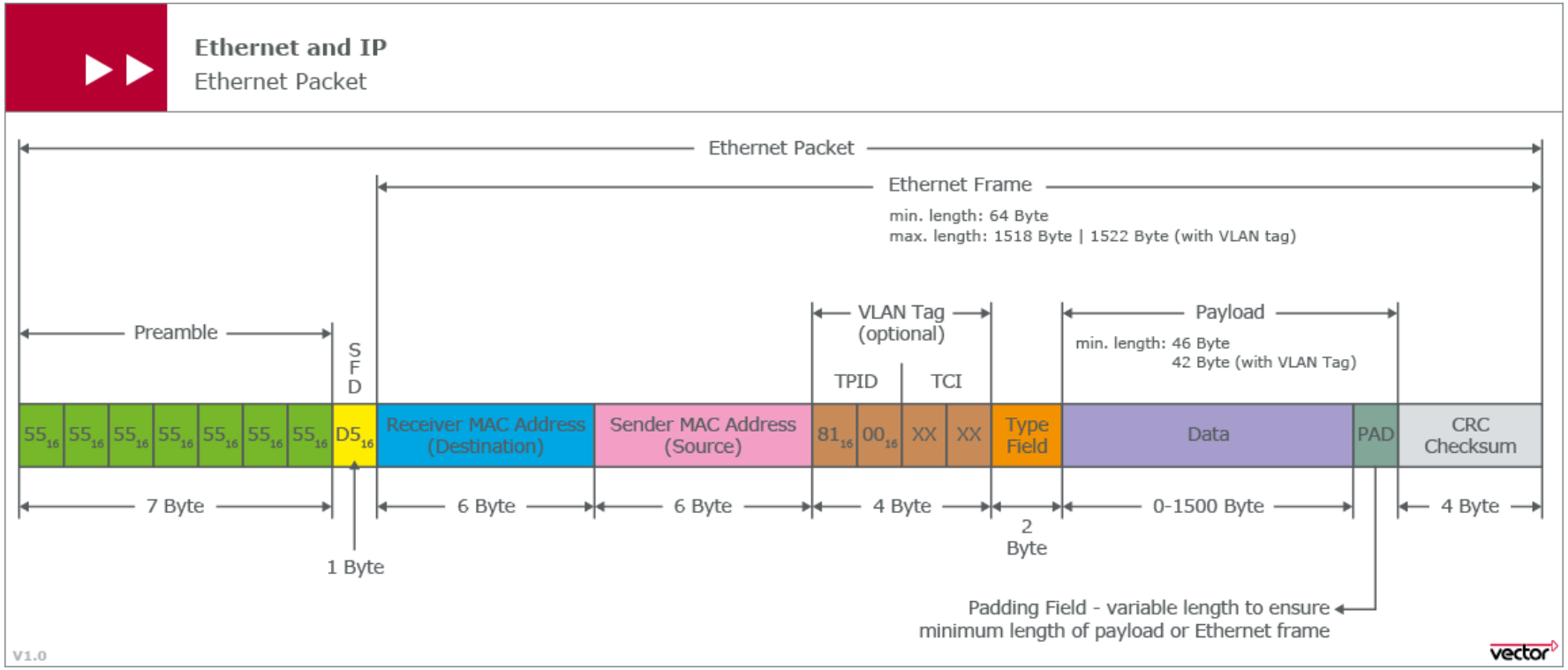
Le VLAN

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

- Una **LAN** 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** è ormai lo standard de facto nelle LAN. E` nata come sistema broadcast su canale (bus) condiviso (trasmissione simultanea a piu` stazioni in banda base, ossia usando tutta la banda disponibile, su cavo coassiale), e si `e sviluppata adottando man mano strategie piu` 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), 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.

Ethernet

Ethernet è una famiglia di tecnologie standardizzate per reti locali, sviluppato a livello sperimentale da Robert Metcalf e David Boggs (1980) allo Xerox PARC, che ne definisce le specifiche tecniche a livello fisico (connettori, cavi, tipo di trasmissione, etc.) e a livello MAC del modello architetturale di rete ISO/OSI.



https://it.wikipedia.org/wiki/Ethernet

Il formato del frame nella rete IEEE 802.3 è mostrato nella figura precedente, in cui sono evidenziati i diversi campi che lo compongono:

- Preambolo: questo campo ha una lunghezza di 7 byte, ognuno costituito dalla sequenza 10101010.
- Delimitatore di inizio del frame SFD: questo campo è formato dal byte 10101011 e serve ad indicare l'inizio del frame.
- Indirizzo della stazione di destinazione e sorgente: questo campo ha una lunghezza di 6 byte; se il bit più significativo del campo indirizzo della stazione di destinazione è uguale a 0, il campo contiene un indirizzo MAC ordinario mentre se tale bit è uguale a 1 allora si ha una trasmissione multicast. Al contrario, se l'indirizzo della stazione di destinazione è formato da bit uguali a 1, allora si ha una trasmissione broadcasting. Il bit 46 (accanto a quello più significativo) serve a distinguere indirizzi locali e globali.
- Type Field: valori <=1500per questo campo indicano che il campo è usato per indicare la lunghezza del payload in byte, mentre valori >= 1536 indicano che il campo è usato per rappresentare EtherType.
- Dati: questo campo ha una lunghezza variabile tra 0 e 1500 byte.
- PAD: questo campo ha una lunghezza variabile tra 0 e 46 byte e viene introdotto per garantire che la lunghezza minima del pacchetto non sia inferiore a 64 byte. Come vedremo, questo valore minimo del pacchetto è necessario per un corretto funzionamento del protocollo CSMA/CD.
- CRC: questo campo, formato da 2 byte, consente di effettuare il controllo degli errori sul pacchetto utilizzando un codice ciclico.

Esempi di EtherType >= 1536

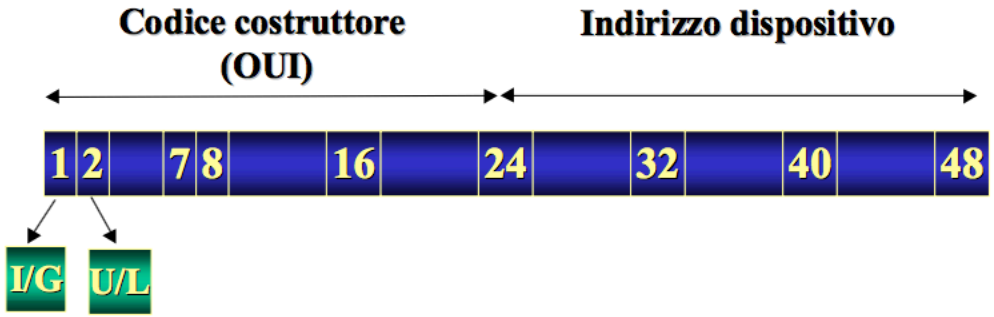
EtherType	Protocol
0x0800	Internet Protocol version 4 (IPv4)
0x0806	Address Resolution Protocol (ARP)
0x0842	Wake-on-LAN[7]
0x22F3	IETF TRILL Protocol
0x22EA	Stream Reservation Protocol
0x6003	DECnet Phase IV
0x8035	Reverse Address Resolution Protocol
0x809B	AppleTalk (Ethertalk)
0x80F3	AppleTalk Address Resolution Protocol (AARP)
0x8100	VLAN-tagged frame (IEEE 802.1Q) and Shortest Path Bridging IEEE 802.1aq with NNI compatibility[8]

Parentesi sui MAC

- L'uso degli indirizzi a livello MAC è stato standardizzato dal comitato IEEE 802. Questo comunicato consente di scegliere tra i seguenti valori di lunghezza: 16 bit o 48 bit
- Per le LAN IEEE 802.6 è possibile anche il valore di 60 bit.
- La scelta di 16 bit presenta il vantaggio di ridurre la lunghezza dell'header del frame e quindi aumenta l'efficienza della LAN. Esso richiede la presenza di un gestore degli indirizzi di ciascuna LAN che assegna l'indirizzo alle singole apparecchiature al momento in cui sono connesse in rete.
- Oggi si utilizzano indirizzi MAC a 48 bit. In questo caso si possono fornire indirizzi validi globalmente per ogni dispositivo, forniti direttamente dal costruttore ed quindi indipendenti dalla rete su cui viene inserito il dispositivo.

- L'indirizzo MAC di destinazione mostrato nella figura 3 può essere di tre tipi:
  - *singolo*, se è indirizzato ad un singolo dispositivo;
  - *multicast*, se è indirizzato ad un gruppo di dispositivi;
  - *broadcast*, se è indirizzato a tutti i dispositivi.
- L'indirizzo broadcast è FF-FF-FF-FF-FF-FF.

- L'uso di **indirizzi universali** richiede la presenza di un'autorità che distribuisca gli indirizzi. Quest'autorità, inizialmente Xerox, è oggi rappresentata da IEEE.
- Il costruttore richiede un blocco di indirizzi composto 2^{24} indirizzi, ciascuno composto da 6 byte (figura 4) con la seguente struttura:
  - i primi 3 byte identificano il costruttore;
  - i rimanenti 3 byte (2^{24} indirizzi) sono a disposizione del costruttore per identificare i singoli dispositivi.



- **I/G (Individual/Group)** serve a distinguere tra indirizzi individuali o di gruppo. (I/G= 0 : indirizzo di un singolo dispositivo, I/G=1 : indirizzo relativo ad un gruppo logico di dispositivi.
- **U/L (Universal/Local)** indica se l'indirizzo è globale (assegnato da IEEE) o deciso localmente.

Hub e Switch

- Un **hub** è un dispositivo di livello fisico che replica il segnale entrante in una porta su ogni altra porta, opportunamente ripulito e amplificato.
- Uno **switch** è un dispositivo di **livello 2** che inoltra un frame Ethernet entrante esclusivamente sulle porte dove `e 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

Apparati di rete

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:

- **DTC**
- **DCE**

DTE e DCE

- **Dispositivi terminali** (Data Terminal Equipment, DTE)— sono quegli apparati che fungono da mittenti o da destinatari dei frame 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 dei frame con- tenenti un carico di livello rete da inoltrare all'esterno della LAN: anche le loro porte Ethernet hanno un MAC address, perchè i PC debbono poter indirizzare i frame in uscita verso di loro.
- **Dispositivi di comunicazione** (Data Communication Equipment, DCE) — non sono destinatari finali dei frame, e normalmente le loro porte Ethernet non hanno nemmeno un MAC address. Servono a inoltrare i frame da una porta all'altra.

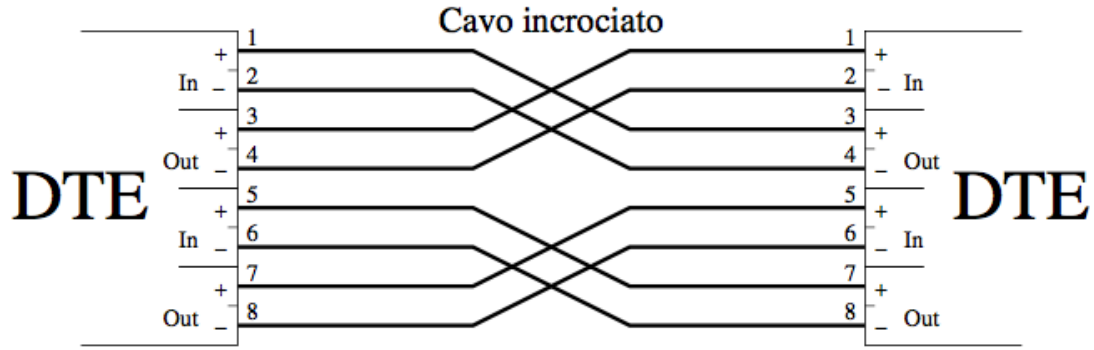
Cablaggio

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

- 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 cos`ı 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".**

Cavo diretto

Cavo incrociato



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**.

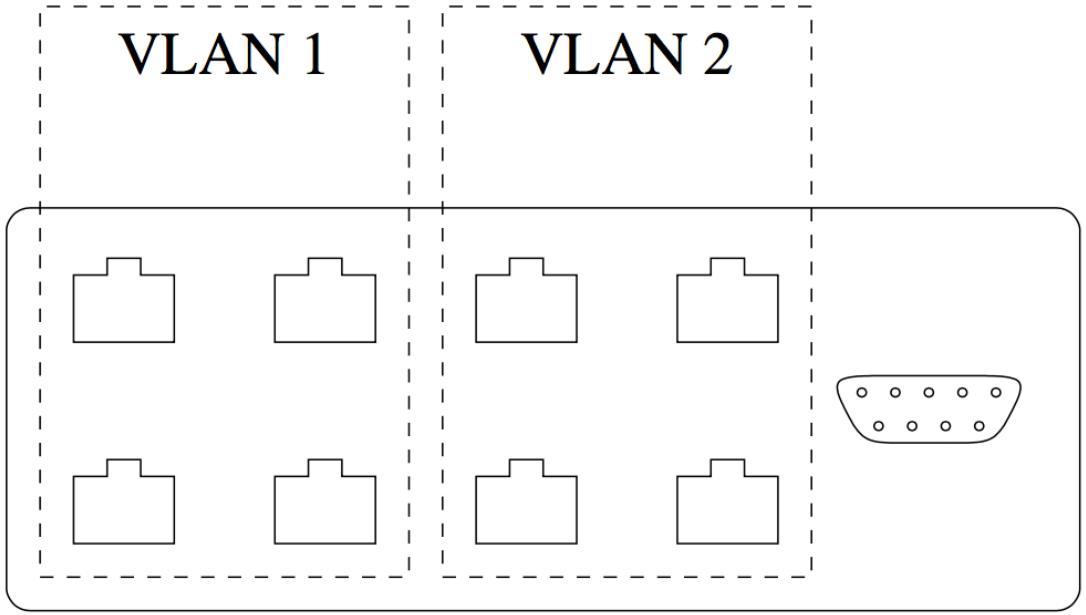
Due dispositivi connessi da uno switch possono trasmettere contemporaneamente (lo switch partecipa al protocollo MAC di Ethernet), quindi uno switch separa i propri ingressi in domini di collisione distinti. Uno switch inoltra i pacchetti broadcast (MAC di destinazione FF:FF:FF:FF:FF:FF) su tutte le uscite. Una rete locale consiste normalmente in pochi domini di **broadcast** e di molti domini di collisione.

https://en.wikipedia.org/wiki/Collision_domain

LAN virtuali (VLAN)

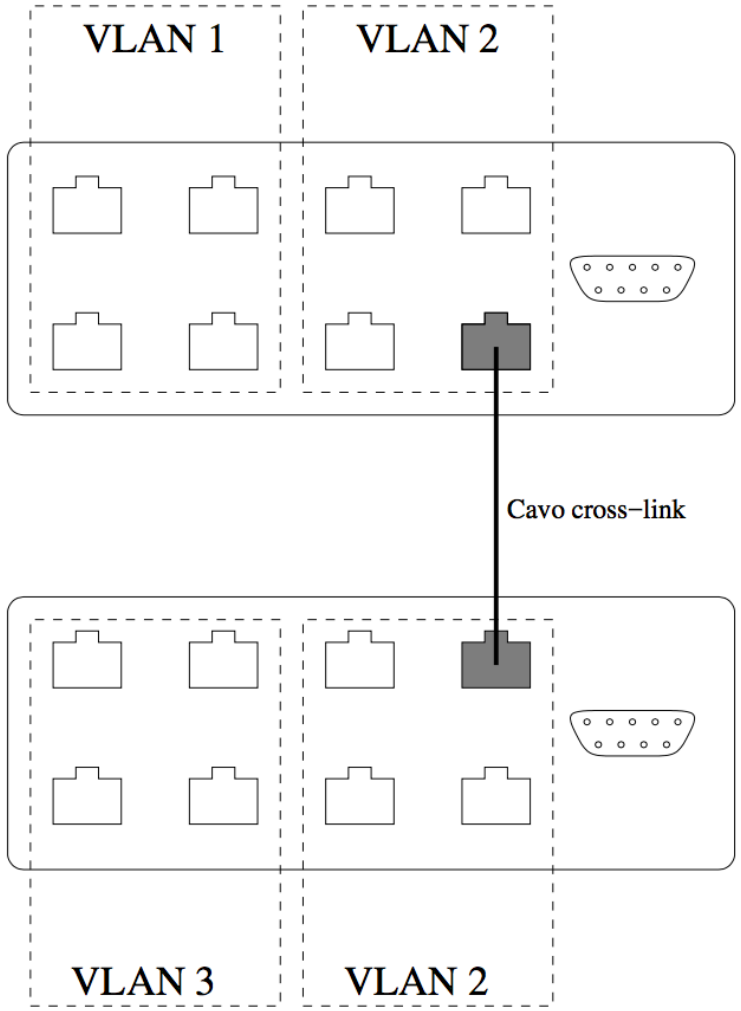
- In uno switch di livello 2 (=DataLink) è possibile raggruppare alcune delle porte che lo compongono (o alcuni dei MAC Address ad esso afferenti) a formare un **dominio di broadcasting autonomo** (VLAN: virtual LAN).
- Creando più VLAN si ottiene quindi un numero equivalente di domini di broadcasting del tutto indipendenti, come se avessimo suddiviso lo stesso switch fisico in piu` 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. Nel singolo switch si definiscono i nomi delle varie VLAN (es.: vlan1, vlan2...) e si associano a ciascuna le relative porte.

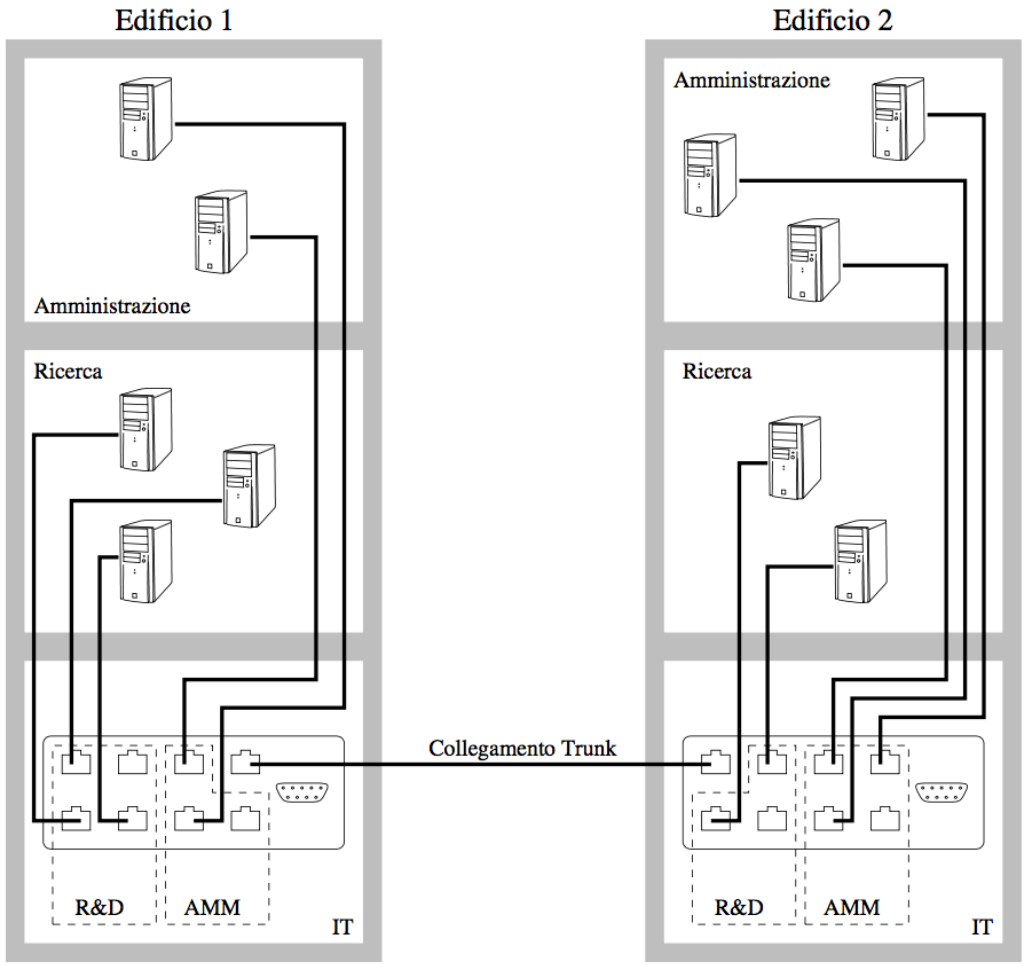


- Se un host viene spostato da una porta a un’altra occorre riconfigurare lo switch, ma questo offre un vantaggio in termini di sicurezza.

E’ possibile estendere una VLAN attraverso più switch, come si vede in figura.



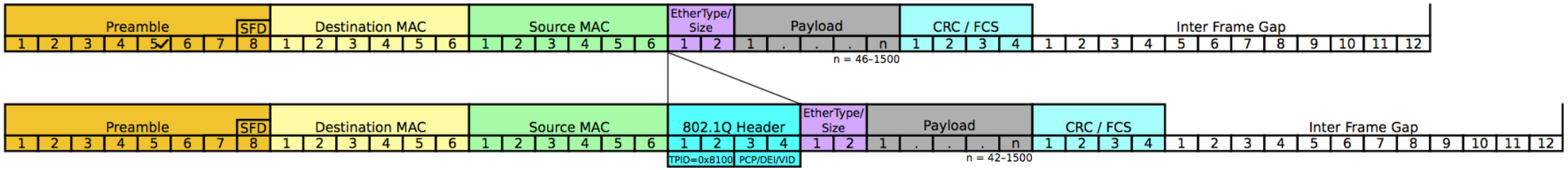
Due LAN possono anche essere completamente separate da un punto di vista logico, pur condividendo alcune connessioni



Un collegamento fra switch può essere infatti utilizzato per una sola VLAN, oppure per portare pacchetti di piu` VLAN diverse, ad esempio quando le stesse VLAN occupano edifici diversi:

- **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 (**VAN untagged**).
- **Trunk link** — E` il caso più interessante: lo stesso link porta frame appartenenti a varie VLAN. Esempio, il link fra edifici visto in precedenza **(VLAN tagged).**

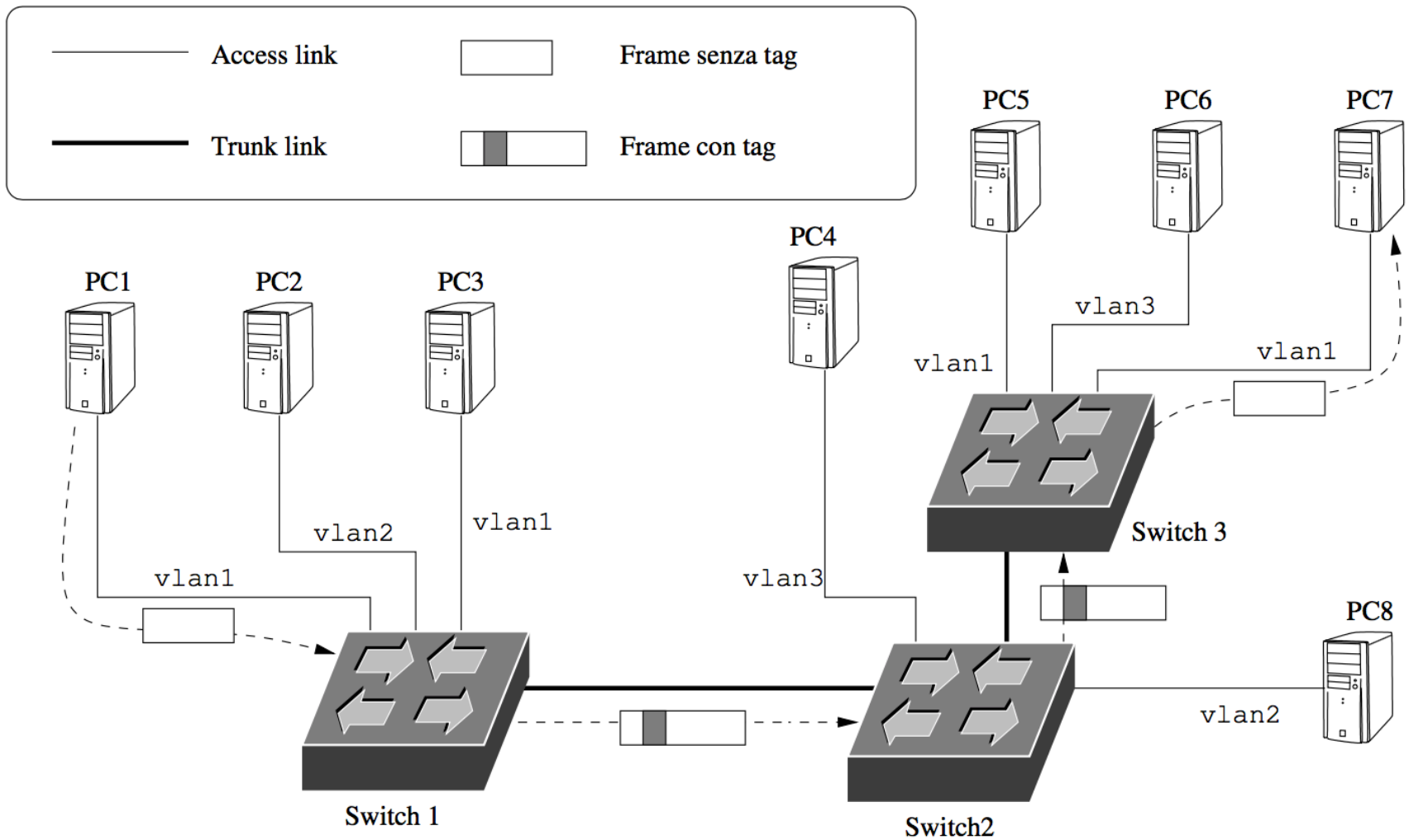
- Se più frame possono transitare per lo stesso link, devono contenere l’informazione della VLAN di appartenenza.
- La porta che immette il frame nel trunk link inserisce nel frame un campo di 4 byte che contiene il valore identificativo (12 bit) della VLAN. Tale campo `e detto tag. Lo standard che estende in tal senso la definizione dell’intestazione Ethernet è **IEEE 802.1Q**.



Come si vede in figura, 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.
Un frame che transita attraverso un trunk link è quindi detto “tagged” (“**taggato**”, etichettato) ad indicare che il frame contiene l’identificativo della VLAN di appartenenza.


Access link
Frame senza tag
Trunk link
Frame con tag
PC1
PC2
PC3
PC4
PC5
PC6
PC7
PC8
vlan1
vlan2
vlan1
vlan3
vlan1
vlan3
vlan1
vlan2
Switch 1
Switch2
Switch 3

- Lungo un trunk link possono anche passare frame senza tag (untagged); essi possono essere associati ad una ed una sola VLAN che viene detta nativa.
- La Figura presenta un esempio di trattamento di un frame 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).
  - Un frame da PC1 a PC7 viaggia in modo nativo da PC1 allo switch 1; viene munito di tag nei due segmenti trunk, poi torna in modo nativo nell'ultimo access link.

VTP

VTP sta per VLAN Trunking Protocol: si tratta di un protocollo proprietario di Cisco che propaga la definizione di una VLAN sulla intera rete LAN.

Per fare questo VTP trasmette le informazioni sulle VLAN a tutti gli switch presenti nel dominio VTP. VTP trasmette messaggi diretti agli switch chiamati VTP advertisements: essi possono essere inviati su 802.1Q, oppure su ISL.

Cisco Inter-Switch Link (**ISL**) è un protocollo proprietario di Cisco che trasmette le informazioni relative alla VLAN dentro frame Ethernet.

VTP può essere configurato su Switch Cisco in tre modalità:

- Client;
- Server;
- Transparent.

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.

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.

https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html

Parametri configurazione VTP

- **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”;
- **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.

Un esempio di configurazione IP per una LAN

Si supponga di dover gestire la rete 192.168.10.0/24 in modo da accomodare tre sottoreti da un massimo di 10 host l'una.

La più piccola rete in grado di indirizzare almeno 10 host è la /28, con 4 bit di host (quindi in grado di distinguere 14 indirizzi host). Le tre sottoreti di cui abbiamo bisogno sono dunque:

- 192.168.10.0/28, con indirizzi host da .1 a .14, e .15 come indirizzo di broadcast.
- 192.168.10.16/28, con indirizzi host da .17 a .30, e .31 come indirizzo di broadcast.
- 192.168.10.32/28, con indirizzi host da .33 a .46, e .47 come indirizzo di broadcast.

Ovviamente non `e possibile utilizzare gli indirizzi rimanenti (da .49 a .255) come se componessero un'unica sottorete. Infatti, il valore binario della rete successiva (.48, in binario 00110000) termina con soli quattro zeri, quindi non permette una rete più ampia di una /28.

L'intervallo più vasto disponibile subito in seguito alle tre sottoreti indicate sopra è dunque

• 192.168.10.48/28, con indirizzi host da .49 a .62, e .63 come indirizzo di broadcast.

La sottorete .64 (in binario 01000000) mette a disposizione 6 bit per indirizzare l'host, quindi la rete successiva è

• 192.168.10.64/26, con indirizzi host da .65 a .126, e .127 come indirizzo di broadcast. Infine, la sottorete che inizia da .128 (binario 10000000) permette di collocare il resto degli indirizzi disponibili:
• 192.168.10.128/25, con indirizzi host da .129 a .254, e .255 come indirizzo di broadcast.

Router R1

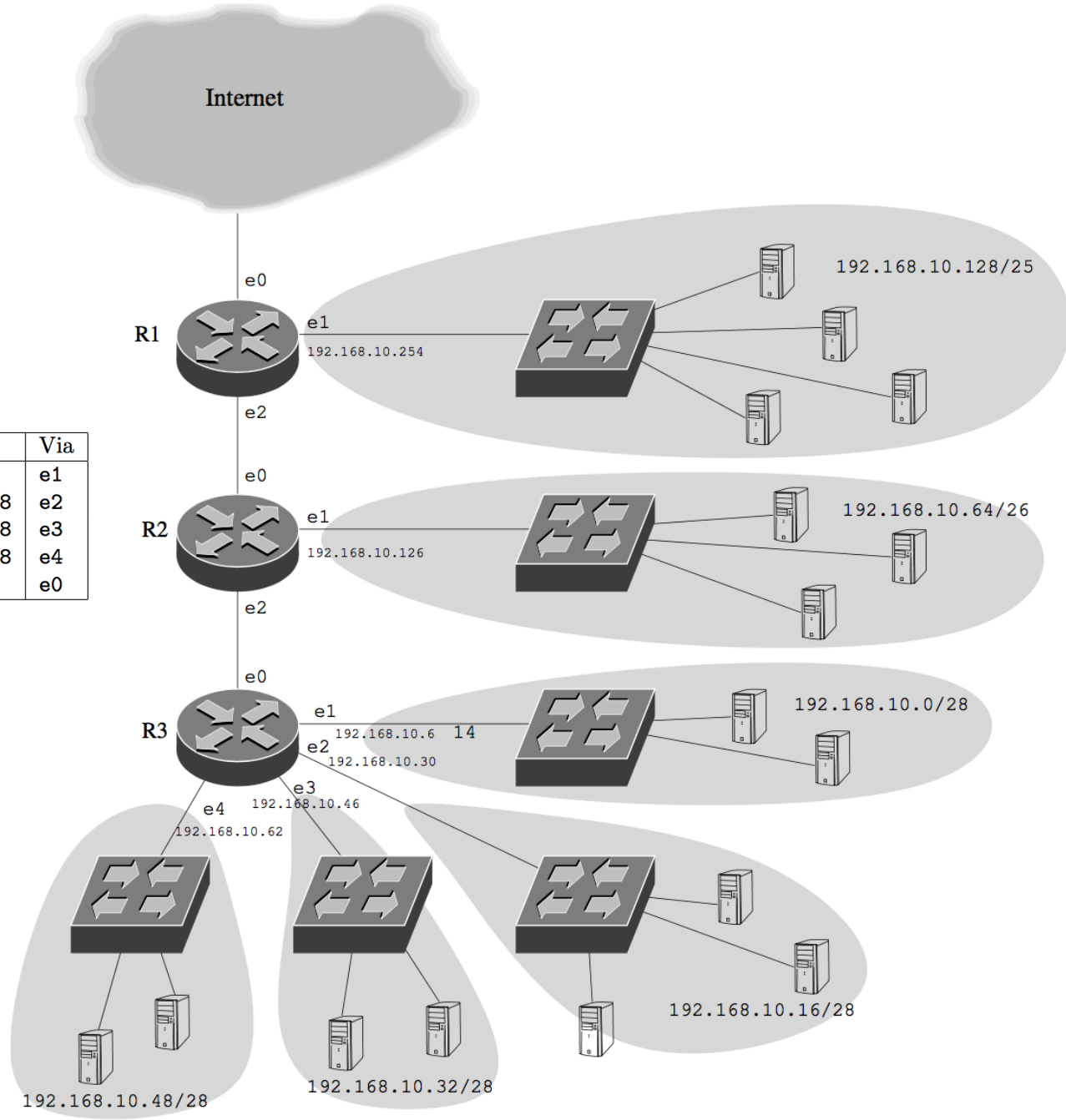
Subnet	Via
192.168.10.128/25	e1
192.168.10.0/25	e2
0.0.0.0/0	e0

Router R2

Subnet	Via
192.168.10.64/26	e1
192.168.10.0/26	e2
0.0.0.0/0	e0

Router R3

Subnet	Via
192.168.10.0/28	e1
192.168.10.16/28	e2
192.168.10.32/28	e3
192.168.10.48/28	e4
0.0.0.0/0	e0



- E` buona norma che la topologia della rete locale rispecchi il più possibile la struttura della suddivisione in sottoreti. Questo permette una maggior chiarezza nella progettazione e nel mantenimento, oltre a ridurre le informazioni necessarie a mantenere e a far operare la rete. Ad esempio, la struttura della suddivisione appena descritta potrebbe rispecchiarsi nella rete della figura precedente.
- Le tabelle di instradamento dei tre router potrebbero essere quelle rappresentate nella slide precedente. Si noti come, dal punto di vista di R1, le sottoreti gestite dai router R2 ed R3 non hanno motivo di essere distinte.

Default Gateway

Il **default gateway** è un router o altro dispositivo di routing che collega una rete locale solitamente ad Internet.

Quando un host richiede il collegamento ad un indirizzo IP esterno alla rete locale, la richiesta viene girata automaticamente ad un gateway incaricato. Quando non ne esiste uno appositamente configurato per la richiesta questa passa automaticamente al default gateway. Il parametro *Default Gateway* è proprio del sistema TCP/IP ed è una indicazione importante per la realizzazione del routing, ovvero l'instradamento dei pacchetti di dati nella rete Internet.

Ogni macchina (PC o altro) collegata ad Internet deve avere un default gateway di riferimento nelle sue impostazioni se deve avere la possibilità di inviare dati sulla rete

Inter-VLAN routing. → minaccia di rete

Abbiamo visto che host appartenenti a VLAN differenti non possono comunicare fra loro a livello 2 in quanto appartengono a LAN separate. E` dunque necessario operare a livello 3 della pila ISO/OSI.

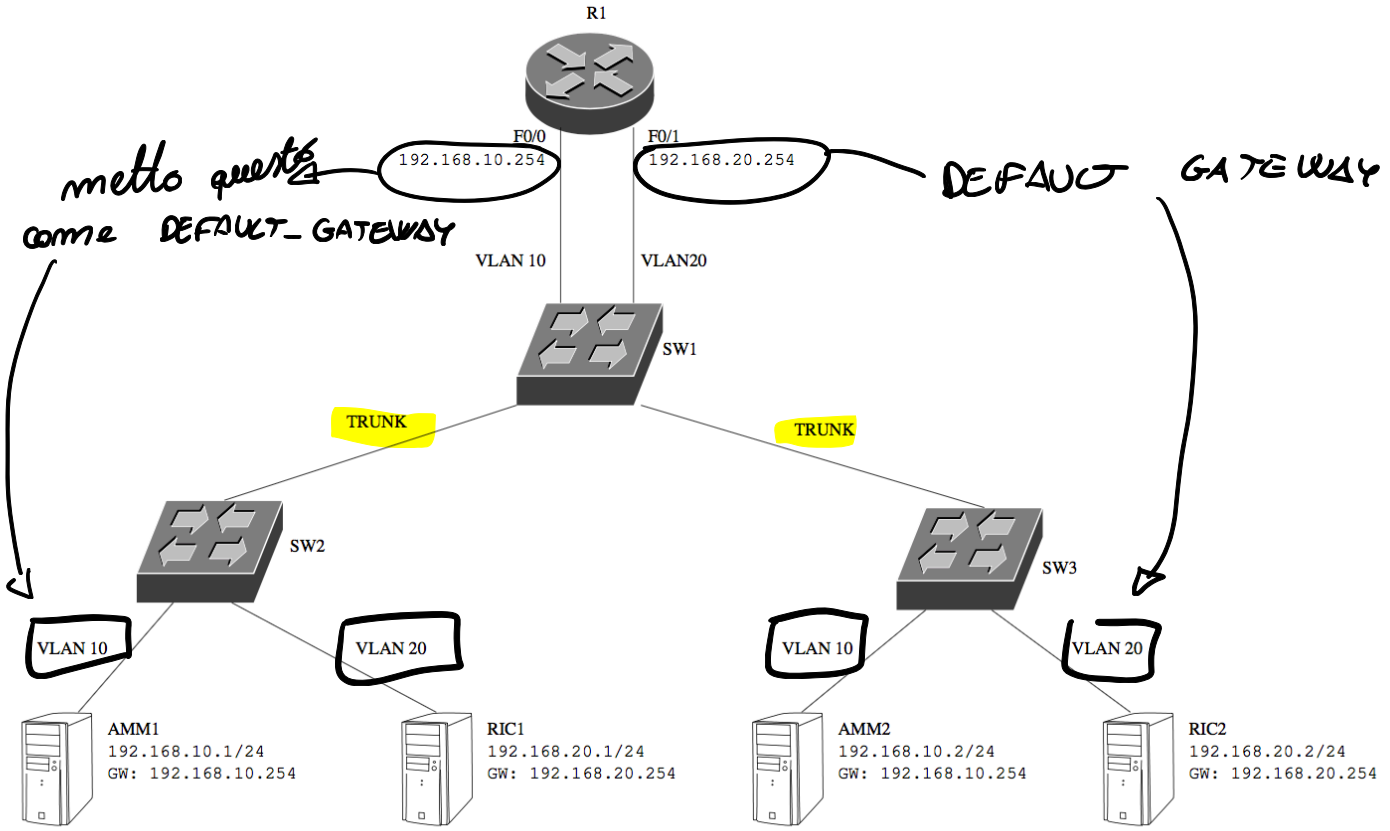
Soluzioni per routing tra VLAN:

1. Router a due porte
2. Router a una porta

Router a due porte

SFRUTTO IL LIVELLO SUPERIORE PER INFRANGERE LA PRIVATEZZA DELLA VLAN

La soluzione piu` ovvia e classica, ma normalmente poco efficace in termini di costo, è quella di figura sotto: trattare le due VLAN come reti fisicamente separate e frapporre un router fra esse. Le due interfacce separate del router, F0/0 e F0/1, agiscono da default gateway per le due VLAN.



Router a una porta

Altrimenti detta “router-on-a-stick” o “one-legged router”, prevede un router collegato a un’unica linea trunk accessibile a entrambe le VLAN. Il router preleva i pacchetti a lui destinati (a livello 2, in quanto default gateway), opera le sostituzioni previste dalla routing table, li reimmette sulla stessa linea con il tag dell’altra rete.

In figura si vede lo schema “logico” interno al router. L’unica interfaccia fisica F0/0, in modalità trunk, è separata internamente in due interfacce logiche F0/0.1 e F0/0.2, ciascuna assegnata a una diversa VLAN e configurata come gateway per le due sottoreti.