

# Best practice per VLAN e suggerimenti per la sicurezza sui router Cisco Business

## Obiettivo

Obiettivo di questo articolo è illustrare le nozioni fondamentali, le procedure delle best practice e i suggerimenti sulla sicurezza per configurare le VLAN sulle apparecchiature Cisco Business.

## Sommario

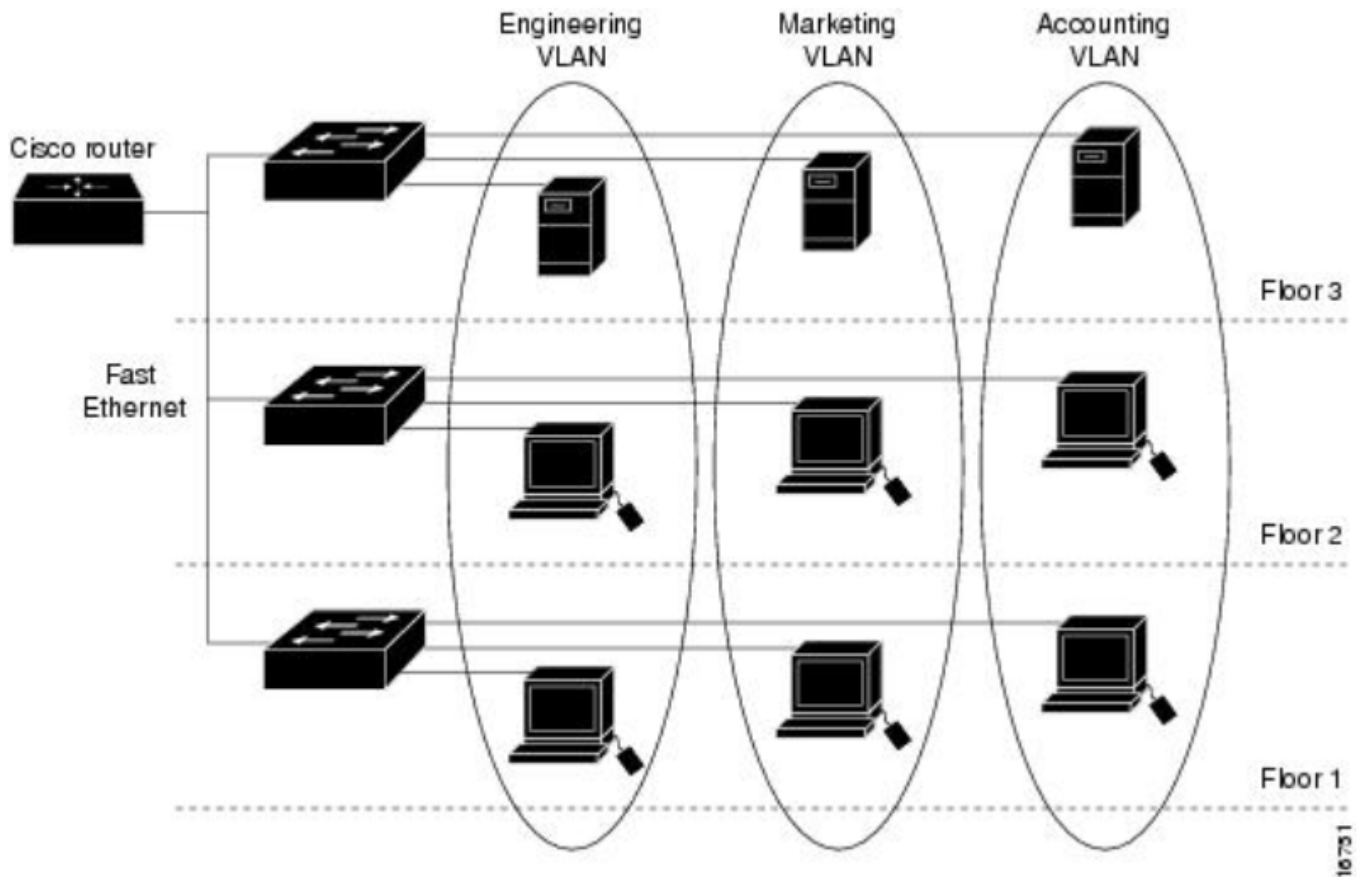
- [Un vocabolario veloce per i nuovi](#)
- [Best Practice 1: assegnazione delle porte VLAN](#) [Nozioni di base sull'assegnazione delle porte](#) [Configurazione delle porte di accesso](#) [Configurazione delle porte trunk](#) [Domande frequenti](#)
- [Best Practice #2 - VLAN predefinita 1 e porte inutilizzate](#) [Domande frequenti](#)
- [Best Practice n. 3 - Creazione di una VLAN "senza uscita" per le porte inutilizzate](#)
- [Best Practice #4 - Telefoni IP su una VLAN](#)
- [Best Practice n. 5 - Routing inter-VLAN](#)

## Introduzione

Volete rendere la vostra rete aziendale più efficiente e al contempo sicura? A tale scopo, è possibile configurare correttamente le VLAN (Virtual Local Area Network).

Una VLAN è un gruppo logico di workstation, server e dispositivi di rete che si trovano sulla stessa LAN (Local Area Network), nonostante la loro distribuzione geografica. In poche parole, l'hardware installato sulle stesse VLAN permette di separare e proteggere il traffico tra le apparecchiature.

Ad esempio, è possibile avere un reparto di ingegneria, marketing e contabilità. Ogni reparto ha dipendenti su diversi piani dell'edificio, ma devono comunque accedere alle informazioni e comunicarle all'interno del proprio reparto. È essenziale per la condivisione di documenti e servizi Web.



Per garantire la sicurezza della rete, le VLAN devono essere configurate con best practice. Effettuare le seguenti scelte intelligenti durante la configurazione delle VLAN. Non te ne pentirai!

## Dispositivi interessati

- RV042
- RV110W
- RV130
- RV132
- RV134W
- RV160W
- RV215W
- RV260
- RV260P
- RV260W
- RV320
- RV325
- RV340
- RV340W
- RV345
- RV345P

In questo caso, i router della serie RV160 o RV260 possono trasportare fino a 16 VLAN, mentre i router della serie RV34x possono trasportare fino a 32 VLAN. RV320 supporta fino a 7 VLAN. Per conoscere il numero di VLAN che il router può trasportare, consultare il foglio dati del modello specifico sul [sito Web Cisco](http://www.cisco.com). Selezionare **Supporto** e immettere il numero di modello oppure cercare semplicemente il foglio dati e il numero di modello.



Questa immagine dell'interfaccia grafica è stata scattata da un router RV260W. Le opzioni potrebbero essere leggermente diverse. Ad esempio, nella serie RV34x, le etichette *Untagged*, *Excluded* e *Tagged* vengono abbreviate in base alla prima lettera. Il processo è lo stesso.

## VLANs to Port Table



VLAN ID	LAN1	LAN2	LAN3	LAN4
---------	------	------	------	------

1	U ▼	U ▼	U ▼	U ▼
---	-----	-----	-----	-----

U : Untagged, T : Tagged, E : Excluded

### Configurazione delle porte trunk

- Due o più VLAN condividono una porta LAN
- Una delle VLAN può essere etichettata come *Senza tag*.
- Le altre VLAN che fanno parte della porta trunk devono essere etichettate come *Tagged*.
- Le VLAN che non fanno parte della porta trunk devono essere contrassegnate con *Excluded* (Escluse) per tale porta.

Ecco un esempio di varie VLAN che si trovano tutte sulle porte trunk. Per impostare correttamente queste impostazioni, selezionare gli *ID VLAN* da modificare. **Fare clic** sull'icona *Modifica*.

Modificarli in base alle proprie esigenze, seguendo i consigli riportati sopra. A proposito, avete notato che la VLAN 1 è esclusa da ciascuna porta LAN? Questa condizione viene spiegata nella sezione [Best Practice for Default VLAN 1](#).

### Assign VLANs to ports



<input type="checkbox"/>	VLAN ID	LAN1	LAN2	LAN3	LAN4
--------------------------	---------	------	------	------	------

<input checked="" type="checkbox"/>	1	Excluded ▼	Excluded ▼	Excluded ▼	Excluded ▼
-------------------------------------	---	------------	------------	------------	------------

<input checked="" type="checkbox"/>	30	Tagged ▼	Tagged ▼	Untaggec ▼	Untaggec ▼
-------------------------------------	----	----------	----------	------------	------------

<input checked="" type="checkbox"/>	40	Tagged ▼	Untaggec ▼	Tagged ▼	Tagged ▼
-------------------------------------	----	----------	------------	----------	----------

<input checked="" type="checkbox"/>	50	Untaggec ▼	Tagged ▼	Tagged ▼	Tagged ▼
-------------------------------------	----	------------	----------	----------	----------

3

Untagged  
Tagged  
Excluded

## Domande frequenti

### Perché una VLAN non ha tag quando è l'unica VLAN su quella porta?

Poiché a una porta di accesso è assegnata una sola VLAN, il traffico in uscita dalla porta viene inviato senza alcun tag VLAN sui frame. Quando il frame raggiunge la porta dello switch (traffico in entrata), lo switch aggiunge il tag VLAN.

### Perché le VLAN sono contrassegnate quando fanno parte di un trunk?

In questo modo, il traffico che passa non viene inviato alla VLAN sbagliata su quella porta. La porta è condivisa dalle VLAN. Simile ai numeri degli appartamenti aggiunti a un indirizzo per assicurarsi che la posta vada all'appartamento corretto all'interno di quell'edificio condiviso.

### Perché il traffico viene lasciato senza tag quando fa parte della VLAN nativa?

Una VLAN nativa è un modo per trasportare il traffico senza tag su uno o più switch. Lo switch assegna alla VLAN nativa tutti i frame non contrassegnati che arrivano su una porta contrassegnata. Se un frame della VLAN nativa lascia una porta trunk (con tag), lo switch elimina il tag VLAN.

### Perché le VLAN sono escluse quando non sono su quella porta?

In questo modo, il traffico su quel trunk viene mantenuto solo per le VLAN che l'utente desidera specificamente. È considerata una buona pratica.

## Best Practice #2 - VLAN predefinita 1 e porte inutilizzate

Tutte le porte devono essere assegnate a una o più VLAN, inclusa la VLAN nativa. I router aziendali Cisco vengono forniti con la VLAN 1 assegnata a tutte le porte per impostazione predefinita.

Una VLAN di gestione è la VLAN utilizzata per gestire, controllare e monitorare in remoto i dispositivi della rete tramite Telnet, SSH, SNMP, syslog o FindIT di Cisco. Per impostazione predefinita, questa è anche la VLAN 1. Una buona pratica in materia di sicurezza è separare il traffico dei dati di gestione da quello degli utenti. Pertanto, è consigliabile utilizzare la VLAN 1 solo a scopo di gestione quando si configurano le VLAN.

Per comunicare in remoto con uno switch Cisco a scopo di gestione, lo switch deve avere un indirizzo IP configurato sulla VLAN di gestione. Gli utenti di altre VLAN non sarebbero in grado di stabilire sessioni di accesso remoto allo switch a meno che non siano stati instradati alla VLAN di gestione, fornendo un ulteriore livello di sicurezza. Inoltre, lo switch deve essere configurato in modo da accettare solo sessioni SSH crittografate per la gestione remota. Per leggere alcune discussioni su questo argomento, fare clic sui seguenti link sul sito Web della Cisco Community:

- [Discussione sulla VLAN di gestione 1](#)
- [Discussione n. 2 sulla VLAN di gestione](#)

## Domande frequenti

### Perché non si consiglia la VLAN 1 predefinita per segmentare virtualmente la rete?

La ragione principale è che gli attori ostili sanno che la VLAN 1 è l'impostazione predefinita e spesso viene utilizzata. che possono utilizzare per accedere ad altre VLAN tramite "salto VLAN".

Come suggerisce il nome, l'attore ostile può inviare il traffico oggetto di spoofing che si presenta come VLAN 1 e che consente l'accesso alle porte trunk e quindi ad altre VLAN.

### È possibile lasciare una porta inutilizzata assegnata alla VLAN predefinita 1?

Per garantire la protezione della rete, non è necessario. Si consiglia di configurare tutte le porte in modo che siano associate a VLAN diverse dalla VLAN predefinita 1.

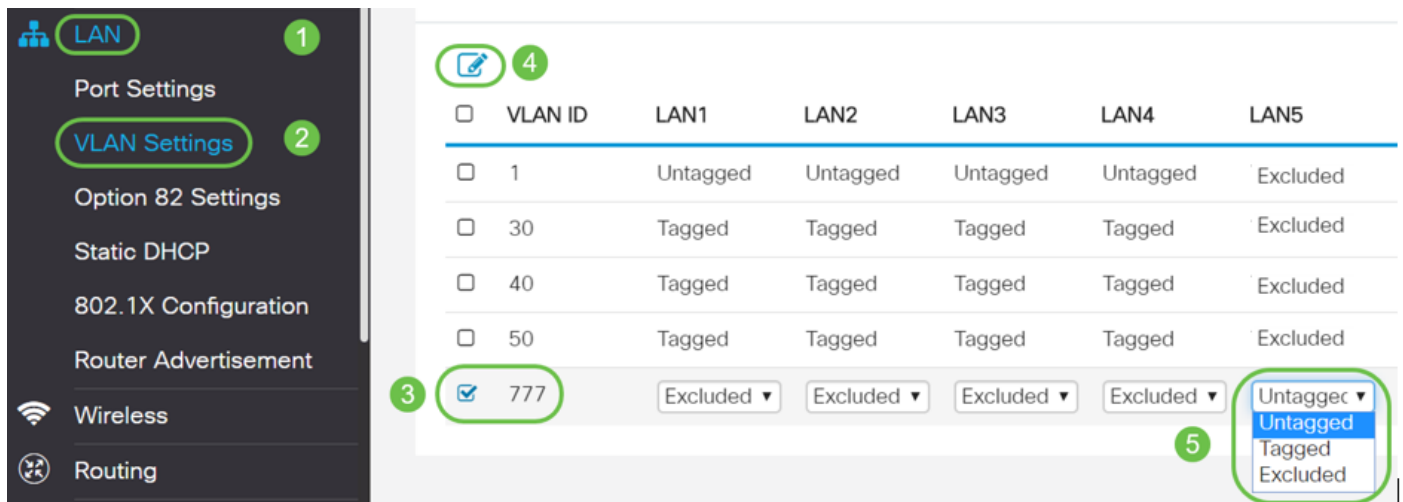
### Non assegnare alcuna VLAN di produzione a una porta non utilizzata. Cosa posso fare?

Si consiglia di creare una VLAN "morta" seguendo le istruzioni nella sezione successiva di questo articolo.

## Best Practice n. 3 - Creazione di una VLAN "senza uscita" per le porte inutilizzate

Passaggio 1. Passare a LAN > Impostazioni VLAN.

Selezionare un numero casuale per la VLAN. Verificare che la VLAN non abbia DHCP, routing tra VLAN o gestione dispositivi abilitata. In questo modo, le altre VLAN sono più sicure. Inserire eventuali porte LAN non utilizzate in questa VLAN. Nell'esempio seguente, la VLAN 777 è stata creata e assegnata alla LAN5. Questa operazione deve essere eseguita su tutte le porte LAN non utilizzate.



VLAN ID	LAN1	LAN2	LAN3	LAN4	LAN5
1	Untagged	Untagged	Untagged	Untagged	Excluded
30	Tagged	Tagged	Tagged	Tagged	Excluded
40	Tagged	Tagged	Tagged	Tagged	Excluded
50	Tagged	Tagged	Tagged	Tagged	Excluded
777	Excluded	Excluded	Excluded	Excluded	Untagged

Si noti che le altre VLAN sono escluse da questa porta LAN.

Passaggio 2. Fare clic sul pulsante *Applica* per salvare le modifiche apportate alla configurazione.

## Best Practice #4 - Telefoni IP su una VLAN

Il traffico vocale è soggetto a rigorosi requisiti QoS (Quality of Service). Se la società dispone di computer e telefoni IP sulla stessa VLAN, ciascuno tenta di utilizzare la larghezza di banda disponibile senza considerare l'altro dispositivo. Per evitare questo conflitto, è buona norma usare VLAN separate per il traffico voce e il traffico dati della telefonia IP. Per ulteriori informazioni su questa configurazione, vedere i seguenti articoli e video:

- [Cisco Tech Talk: Configurazione e configurazione di VLAN voce con i prodotti Cisco Small Business](#) (video)
- [Configurazione di Auto Voice VLAN con QoS sugli switch serie SG500](#)

- [Configurazione della VLAN voce sugli switch gestiti serie 200/300](#)
- [Cisco Tech Talk: Configurazione della VLAN Auto-Voice sugli switch serie SG350 e SG550 \(video\)](#)

## Best Practice n. 5 - Routing inter-VLAN

Le VLAN sono configurate in modo da poter separare il traffico, ma a volte è necessario che le VLAN siano in grado di indirizzarsi tra loro. Questo è il routing tra VLAN e in genere non è consigliato. Se è necessario per la tua azienda, configuralo nel modo più sicuro possibile. Quando si utilizza il routing tra VLAN, assicurarsi di limitare il traffico utilizzando gli Access Control Lists (ACL) ai server che contengono informazioni riservate.

Gli ACL eseguono il filtro dei pacchetti per controllare lo spostamento dei pacchetti attraverso la rete. Il filtro dei pacchetti garantisce la sicurezza limitando l'accesso del traffico a una rete, limitando l'accesso di utenti e dispositivi a una rete e impedendo al traffico di uscire dalla rete. Gli elenchi degli accessi IP riducono la possibilità di attacchi di tipo spoofing e di tipo "denial of service" e consentono agli utenti di accedere in modo dinamico e temporaneo tramite un firewall.

- [Routing inter-VLAN su un router RV34x con restrizioni ACL di destinazione](#)
- [Cisco Tech Talk: Configurazione del routing tra VLAN sugli switch serie SG250 \(video\)](#)
- [Cisco Tech Talk: Configurazione tra VLAN su RV180 e RV180W \(video\)](#)
- [RV34x Inter-VLAN Access Limitation \(correzione dei bug di CSCvo92300\)](#)

## Conclusioni

Ecco a voi alcune best practice per configurare VLAN sicure. Tenere presenti questi suggerimenti quando si configurano le VLAN per la rete. Di seguito sono elencati alcuni articoli con istruzioni dettagliate. In questo modo si potrà passare a una rete produttiva ed efficiente, la più adatta per la propria azienda.

- [Configurazione delle impostazioni VLAN sugli switch RV160 e RV260](#)
- [Configurazione delle impostazioni della VLAN \(Virtual Local Area Network\) su un router serie RV34x](#)
- [Configurazione dell'appartenenza della VLAN sui router VPN RV320 e RV325](#)
- [Configurazione dell'appartenenza della VLAN \(Virtual Local Area Network\) su un router serie RV](#)
- [Configurazione dell'indirizzo IPv4 dell'interfaccia VLAN su uno switch Sx350 o SG350X dalla CLI](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).