

Informazioni sullo pseudonimo MPLS L2VPN

Sommario

[Introduzione](#)

[Premesse](#)

[Panoramica di L2VPN](#)

[Perché L2VPN è necessario](#)

[Modelli MPLSL2VPN](#)

[Opzioni tecnologiche](#)

[1. Servizi VPWS](#)

[2. Servizi VPLS](#)

[3. EVPN](#)

[4. PBB-EVPN](#)

[VPWS - Pseudo modello di riferimento per fili](#)

[Layer 2 VPN Enabler: lo pseudofilo](#)

[Architettura AToM](#)

[L2Transport over MPLS](#)

[VPWS Traffic Encapsulation](#)

[Segnalazione dello pseudoforo](#)

[Parola di controllo](#)

[Elaborazione piano di inoltr](#)

[Funzionamento](#)

[Segnalazione dello stato di PW](#)

[Configurazione AToM di base](#)

[Analisi Pacchetti Pseudowire](#)

[Topologia](#)

[Interoperabilità L2VPN](#)

[Possibilità di interworking](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto il protocollo MPLS (Multiprotocol Label Switching) basato sugli pseudowire VPN (Virtual Private Network) di layer 2 (L2VPN).

Premesse

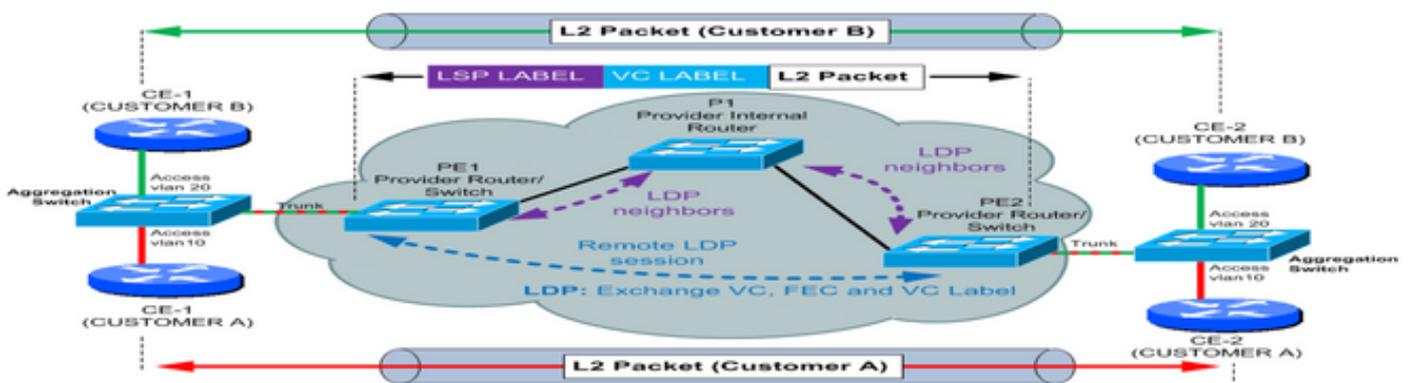
La segnalazione dello pseudofilo e l'analisi dei pacchetti in Cisco IOS®, IOS®-XE per illustrare il comportamento sono descritte.

Panoramica di L2VPN

Il trasporto Layer 2 (L2) su MPLS e IP esiste già per circuiti di collegamento simili, come Ethernet-Ethernet, PPP-to-PPP, High-Level Data Link Control (HDLC), e così via

Le VPN da sito a sito utilizzano i servizi L2 su MPLS per creare una topologia di connessioni point-to-point che connettono i siti terminali in una VPN. Queste VPN da sito a sito forniscono un'alternativa alle reti private fornite tramite linee dedicate in leasing o tramite circuiti virtuali L2 che utilizzano ATM o Frame Relay. Il servizio fornito con queste L2VPN è noto come VPWS (Virtual Private Wire Service).

- Le VPN da sito a sito sono basate sulla tecnologia Pseudowire (PW).
- I PW forniscono un formato intermedio comune per il trasporto di più tipi di servizi di rete su una rete PSN (Packet Switched Network) - una rete che inoltra pacchetti - IPv4, IPv6, MPLS, Ethernet.
- La tecnologia PW offre trasporto Like-to-Like e anche Interworking (IW).
- I frame ricevuti sul router PE sull'adattatore CA vengono incapsulati e inviati tramite il PSW al router PE remoto.
- Il router PE in uscita riceve il pacchetto dal PSW e rimuove il relativo incapsulamento.
- L'uscita PE estrae e inoltra il frame all'alimentazione CA.

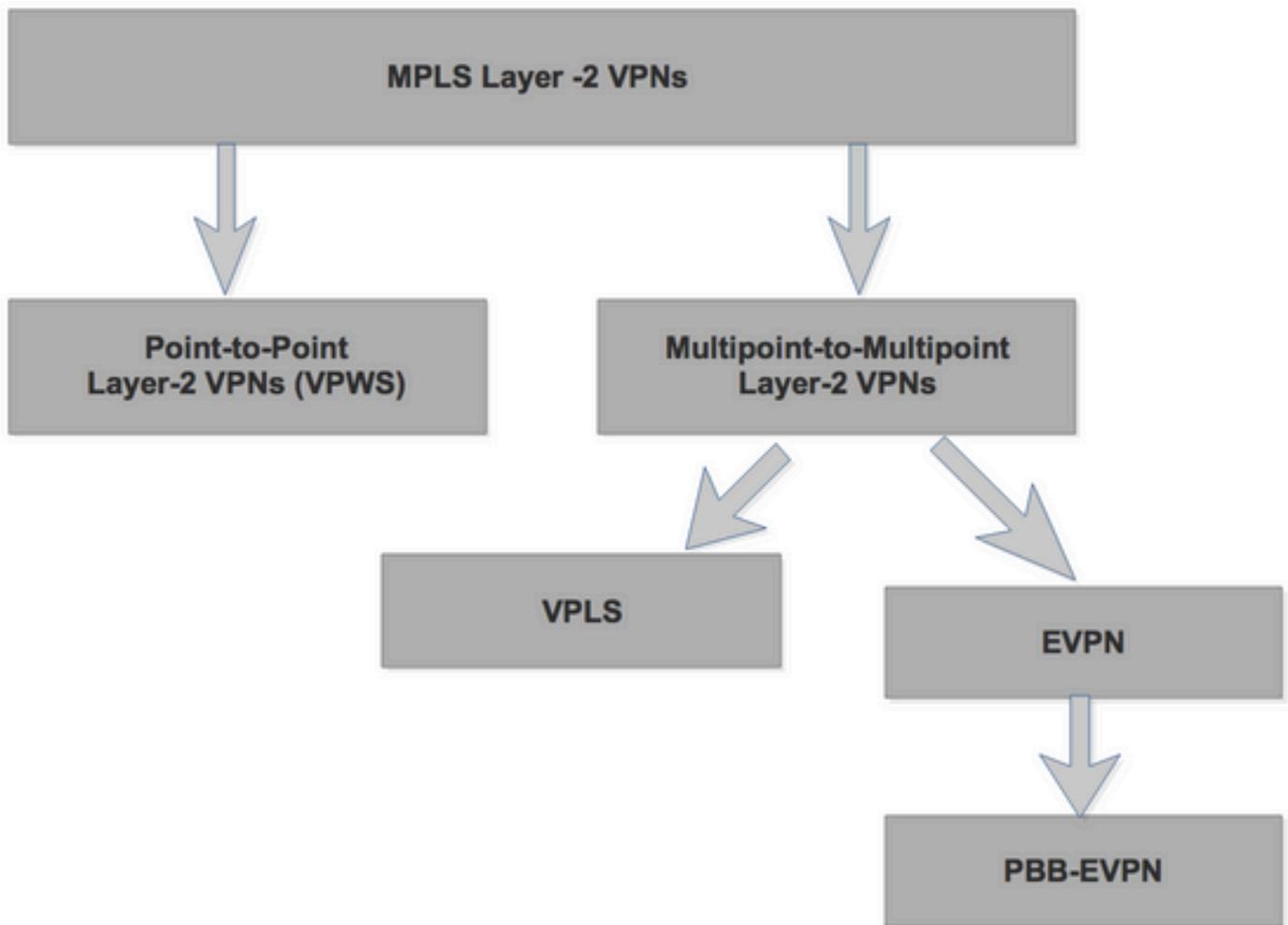


Perché L2VPN è necessario

- Consente agli SP di disporre di un'unica infrastruttura per i servizi IP e legacy.
- Migrazione dei servizi ATM e Frame Relay legacy al core MPLS/IP senza interruzione ai servizi esistenti.
- Il provisioning dei nuovi servizi L2VPN è incrementale (non da zero) nel core MPLS/IP esistente.
- Risparmio sui costi in conto capitale e operativi grazie alla convergenza della rete IP/MPLS.
- SP fornisce nuovi servizi point-2-point o point-2-multipoint. È possibile disporre di un proprio routing, criteri QoS, meccanismi di sicurezza e così via.

Modelli VPN MPLS L2

Opzioni tecnologiche



1. Servizi VPWS

- Point-to-point · Denominato Pseudowires (PW)

2. Servizi VPLS

Multipoint

3. EVPN

- La famiglia xEVPN introduce soluzioni di nuova generazione per i servizi Ethernet

a. Control-plane BGP per la distribuzione e l'apprendimento dei segmenti Ethernet e MAC sul core MPLS

b. Stessi principi ed esperienza operativa delle VPN IP

- Nessun utilizzo di pseudofili

a. Utilizza tunnel MP2P per unicast

b. Distribuzione di frame a più destinazioni tramite replica in entrata (tramite tunnel MP2P) o LSM

- Soluzioni multi-vendor con standardizzazione IETF

4. PBB-EVPN

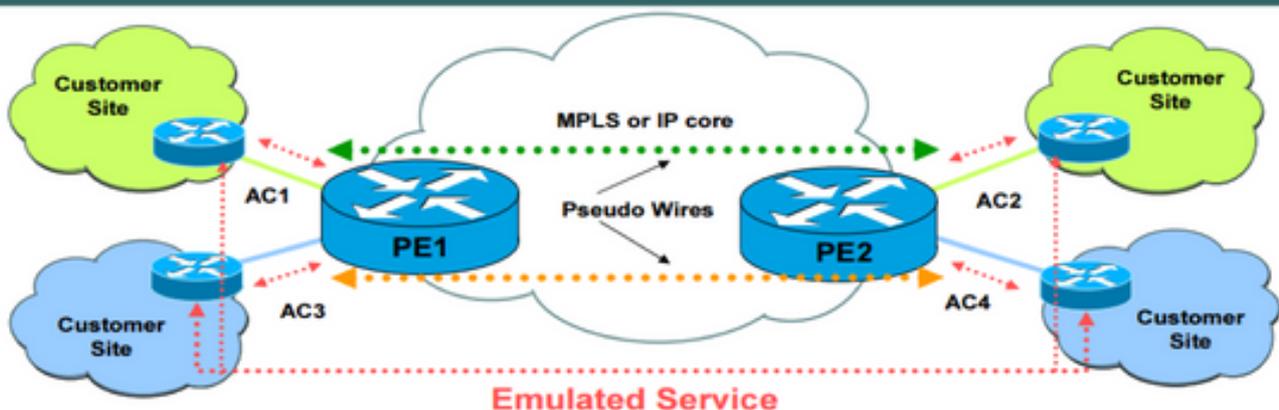
- Combina gli strumenti di scalabilità di PBB (alias MAC-in-MAC) con l'apprendimento MAC basato su BGP da EVPN

EVPN e Provider Backbone Bridging EVPN (PBB-EVPN) sono soluzioni L2VPN di nuova generazione basate sul control plane BGP per la distribuzione/apprendimento MAC sul core, progettate per soddisfare questi requisiti:

- Ridondanza per flusso e bilanciamento del carico
- Provisioning e funzionamento semplificati
- Inoltro ottimale
- Convergenza rapida
- Scalabilità degli indirizzi MAC

VPWS - Pseudo modello di riferimento per fili

1. PW è una connessione tra due dispositivi PE che connette due CA, che trasportano frame L2.
2. Any Transport Over MPLS (AToM) è l'implementazione di VPWS per le reti IP/MPLS da parte di Cisco.
3. Il circuito di collegamento (CA) è il circuito fisico o virtuale che collega un CE a un PE, che può essere ATM, Frame Relay, HDLC, PPP e così via.
4. L'apparecchiatura You Edge (CE) percepisce un PW come un collegamento o un circuito non condiviso.



Layer 2 VPN Enabler: lo pseudofilo

Le VPN da sito a sito sono basate sulla tecnologia Pseudowire (PW)

- I PW forniscono un formato intermedio comune per il trasporto di più tipi di servizi di rete su una rete PSN (Packet Switched Network) - una rete che inoltra pacchetti - IPv4, IPv6, MPLS, Ethernet.

- La tecnologia PW offre trasporto Like-to-Like e anche Interworking (IW).
- I frame ricevuti sul router PE sull'adattatore CA vengono incapsulati e inviati tramite il PSW al router PE remoto.
- Il router PE in uscita riceve il pacchetto dallo Pseudowire e ne rimuove l'incapsulamento.
- L'uscita PE estrae e inoltra il frame all'alimentazione CA.

Architettura AToM

- Nella rete AToM, tutti i router nell'SP eseguono MPLS e il router PE dispongono di un CA verso il router CE.
- Nel caso di AToM, il tunnel PSN non è altro che un LSP con percorso a commutazione di etichetta tra i due router PE.
- Di conseguenza, l'etichetta associata a tale provider di servizi di traduzione viene chiamata etichetta tunnel nel contesto di AToM.
- In primo luogo, il LDP segnala hop dopo hop tra il PE.
- In secondo luogo, l'LSP può essere un tunnel MPLS TE segnalato dall'RSVP con le estensioni necessarie per TE.
- Con questa etichetta del tunnel, è possibile identificare a quale tunnel PSN appartiene il frame trasportato.
- Questa etichetta del tunnel consente inoltre di ottenere i frame dal sistema PE locale o in entrata al sistema PE remoto o in uscita attraverso la backbone MPLS.
- Per eseguire il multiplexing di più Pseudowire su un tunnel PSN, il router PE utilizza un'altra etichetta per identificare lo Pseudowire.
- Questa etichetta viene chiamata etichetta VC o PW in quanto identifica la VC o PW in cui viene eseguito il multiplexing del frame.

Trasporto L2 su MPLS

Control Connection

- Targeted LDP session / BGP session / Static
 - Used for VC-label negotiation, withdrawal, error notification

The “emulated circuit” has **three (3) layers of encapsulation**

Tunnelling Component

- **Tunnel header (Tunnel Label)**
 - To get PDU from ingress to egress PE
 - MPLS LSP derived through static configuration (MPLS-TP) or dynamic (LDP or RSVP-TE)

Demultiplexing Component

- **Demultiplexer field (VC Label)**
 - To identify individual circuits within a tunnel
 - Could be an MPLS label, L2TPv3 header, GRE key, etc.

Layer 2 Encapsulation

- **Emulated VC encapsulation (Control Word)**
 - Information on enclosed Layer 2 PDU
 - Implemented as a 32-bit control word

VPWS Traffic Encapsulation



1. Incapsulamento a tre livelli
2. Pacchetti scambiati tra PE tramite etichetta tunnel
3. L'etichetta VC identifica PW
4. Etichetta VC segnalata tra file PE
5. La parola di controllo opzionale (CW) trasporta i bit di controllo di layer 2 e consente la sequenza

Control Word	
Encap.	Required
ATM N:1 Cell Relay	No
ATM AAL5	Yes
Ethernet	No
Frame Relay	Yes
HDLC	No
PPP	No
SAToP	Yes
CESoPS N	Yes

Segnalazione Pseudowire

- Una sessione TLDP tra il router PE invia un segnale allo pseudofilo.
- Una sessione T-LDP tra i router PE è quella di annunciare l'etichetta VC associata al PSW.
- Questa etichetta viene annunciata in un messaggio di mappatura delle etichette che utilizza la modalità di annuncio delle etichette non sollecitate a valle.
- Etichetta VC annunciata dal PE in uscita per il PE in entrata per l'AC durante la sessione

TLDP. # Etichetta VC di TLDP

- Etichetta del tunnel annunciata per il router PE in uscita sul router PE in entrata da LDP. # Etichetta del tunnel da LDP

Notare che in uscita PE pubblicizza l'etichetta 3, che indica che viene utilizzato PHP.

Il messaggio di mapping delle etichette annunciato nella sessione TLDP contiene alcuni TLV:

LDP Label Mapping message:

IP Header

TCP Header (Port 646)

LDP PDU

LDP Header

LDP Message: Label Mapping

FEC TLV

PW ID FEC Element 128: Interface Parameters

Generic Label TLV

Il router PE in ingresso inserisce innanzitutto l'etichetta VC nel frame. E poi spinge l'etichetta del tunnel.

Passaggio 2. L'etichetta del tunnel è l'etichetta associata al prefisso IGP che identifica il file PE remoto. Il prefisso è un bit specificato nella configurazione AToM.

Passaggio 3. Il pacchetto MPLS viene quindi inoltrato in base all'etichetta del tunnel, hop dopo hop fino a quando il pacchetto non raggiunge l'uscita PE2.

Passaggio 4. Quando il pacchetto raggiunge l'uscita PE, l'etichetta del tunnel è già stata rimossa. Ciò è dovuto al comportamento PHPbehavior tra l'ultimo router IP e il server PE in uscita.

Passaggio 5.

Il PE in uscita cerca quindi il Videoconferenza etichetta nella base delle informazioni di inoltro striscia disattiva Videoconferenza e inoltra il frame sull'alimentatore CA corretto.

Segnalazione dello stato di PW

Dopo che i router PE hanno impostato lo pseudowire, il sistema PE può segnalare lo stato dello pseudowire al sistema PE remoto. Esistono due metodi:

1. Ritiro dell'etichetta (più vecchio di 2)

- Un router PE può ritirare il mapping di etichette inviando il messaggio di ritiro dell'etichetta o inviando i messaggi di rilascio del mapping di etichette.
- Se l'alimentazione CA non è attiva, il router PE segnala questo problema inviando un messaggio Label Withdraw al computer remoto
- Se un'interfaccia fisica non funziona, l'etichetta ritira il messaggio che contiene l'ID gruppo per segnalare che l'alimentazione CA dell'interfaccia non è attiva

2. TLV stato PW

- Il TLV di stato PW segue il TLV di mapping delle etichette LDP quando lo pseudowire viene individuato. Ciò indica che il router PE desidera utilizzare il secondo metodo.
- Se l'altro router PE non supporta il metodo TLV di stato PW, entrambi i router PE torneranno al metodo di ritiro dell'etichetta.
- Dopo la selezione dello pseudowire, il TLV di stato PW viene trasmesso in un messaggio di notifica LDP. Il TLV di stato PW contiene il campo del codice di stato a 32 bit.

Configurazione AToM di base

Passaggio 1. Selezionate il tipo di incapsulamento.

Passaggio 2. Abilitare la specifica del comando connect sull'interfaccia di CE.

```
mpls xconnect peer-router-id vcid encapsulation
```

Peer-router-id: ID router LDP per il router PE remoto.

VCID: identificatore assegnato al PW.

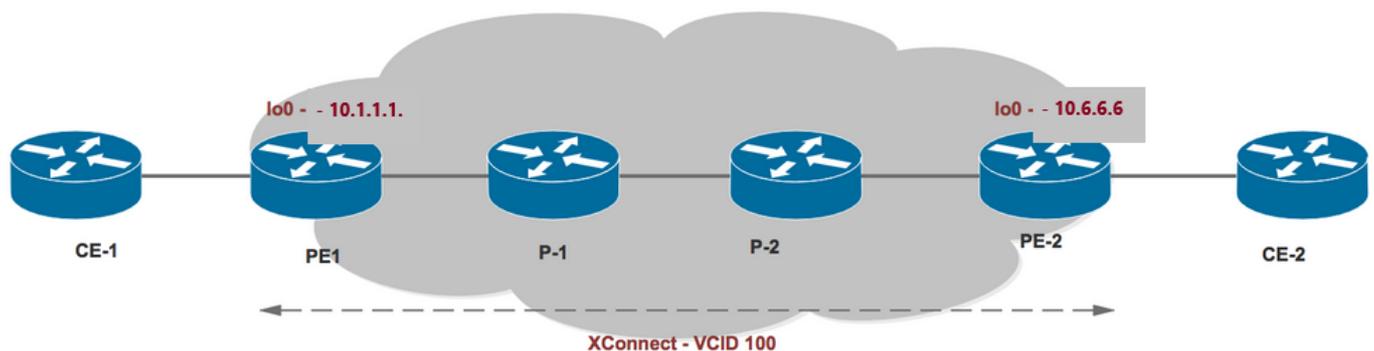
Passaggio 3. Non appena xconnect viene configurato in entrambi i router PE, viene stabilita la sessione LDP di destinazione tra il router PE.

Analisi Pacchetti Pseudowire

Iniziamo un ping tra Pseudowire e PE in ingresso.

Pacchetti MPLS Echo Request and Reply inviati su Pseudowire point-to-point.

Topologia



Eeguire il ping da PE1 a PE2:

```
R1#ping mpls pseudowire 10.6.6.6 100
```

```
Sending 5, 100-byte MPLS Echos to 10.6.6.6,
```

```
timeout is 2 seconds, send interval is 0 msec:
```

```
Type escape sequence to abort.
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/61/80 ms
```

Osservazioni formulate:

1. Richiesta ECHO:

Carries 2 Labels - VPN e trasporto

Inviato come pacchetto etichettato con ETICHETTA PW. Etichetta commutabile (con etichetta di trasporto)

ETICHETTE : 2

SRC IP : IP DI LOOPBACK (UTILIZZATO NELLE VICINANZE LDP DI DESTINAZIONE)

IP DST: 127.0.0.1

TIPO L4 : UDP

PORTA SRC : 3503

PORTA DST : 3505

BYTE TOS : DISATTIVATO

MPLS EXP : DISATTIVATO

BIT DF : ATTIVATO

Il campo IPv4 OPTIONS (OPZIONI IPv4) è in USE: CAMPO ROUTER ALERT OPTIONS (OPZIONI AVVISO ROUTER) (Punta alla CPU)

IL PAYLOAD UDP PUÒ ESSERE UNA RICHIESTA ECHO DI LABEL SWITCHING MPLS

Panoramica:

4 0.203148 10.1.1.1 10.0.0.1 MPLS E... 130 MPLS Echo Request

```
Frame 2: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface 0
Ethernet II, Src: ca:01:1b:c0:00:06 (ca:01:1b:c0:00:06), Dst: ca:04:13:5c:00:06 (ca:04:13:5c:00:06)
MultiProtocol Label Switching Header, Label: 24, Exp: 0, S: 0, TTL: 255 Transport label
MultiProtocol Label Switching Header, Label: 28, Exp: 0, S: 1, TTL: 1 VPN label
PW Associated Channel Header
Internet Protocol Version 4, Src: 10.1.1.1 Dst: 10.0.0.1
User Datagram Protocol, Src Port: 3503 (3503), Dst Port: 3503 (3503)
Multiprotocol Label Switching Echo
```

Etichette Layer 2:

```

> Frame 4: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface 0
v Ethernet II, Src: ca:01:1b:c0:00:06 (ca:01:1b:c0:00:06), Dst: ca:04:13:5c:00:06 (ca:04:13:5c:00:06)
  > Destination: ca:04:13:5c:00:06 (ca:04:13:5c:00:06)
  > Source: ca:01:1b:c0:00:06 (ca:01:1b:c0:00:06)
  Type: MPLS Label switched packet (0x8847)
v MultiProtocol Label Switching Header, Label: 24, Exp: 0, S: 0, TTL: 255
  0000 0000 0000 0001 1000 .... = MPLS Label: 24
  .... 000. .... = MPLS Experimental Bits: 0
  .... 0 .... = MPLS Bottom Of Label Stack: 0
  .... 1111 1111 = MPLS TTL: 255
v MultiProtocol Label Switching Header, Label: 28, Exp: 0, S: 1, TTL: 1
  0000 0000 0000 0001 1100 .... = MPLS Label: 28
  .... 000. .... = MPLS Experimental Bits: 0
  .... 1 .... = MPLS Bottom Of Label Stack: 1
  .... 0000 0001 = MPLS TTL: 1
v PW Associated Channel Header
  .... 0000 = Channel Version: 0
  Reserved: 0x00
  Channel Type: IPv4 packet (0x0021)
> Internet Protocol Version 4, Src: 10.1.1.1, Dst: 10.0.0.1
> User Datagram Protocol, Src Port: 3503 (3503), Dst Port: 3503 (3503)
> Multiprotocol Label Switching Echo

```

L3/L4:

```

v PW Associated Channel Header
  .... 0000 = Channel Version: 0
  Reserved: 0x00
  Channel Type: IPv4 packet (0x0021)
v Internet Protocol Version 4, Src: 10.1.1.1, Dst: 10.0.0.1
  0100 .... = Version: 4
  .... 0110 = Header Length: 24 bytes
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 104
  Identification: 0xfd8f (64911)
  v Flags: 0x02 (Don't Fragment)
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  > Time to live: 1
  Protocol: UDP (17)
  > Header checksum: 0x65ee [validation disabled]
  Source: 10.1.1.1
  Destination: 10.0.0.1
  [Source GeoIP: unknown]
  [Destination GeoIP: Unknown]
  v Options: (4 bytes), Router Alert
    v Router Alert (4 bytes): Router shall examine packet (0)
      > Type: 148
      Length: 4
      Router Alert: Router shall examine packet (0)
v User Datagram Protocol, Src Port: 3503 (3503), Dst Port: 3503 (3503)
  Source Port: 3503
  Destination Port: 3503
  Length: 80
  > Checksum: 0x029f [validation disabled]
  [Stream index: 0]
> Multiprotocol Label Switching Echo

```

Il payload MPLS effettivo:

```

  Multiprotocol Label Switching Echo
  Version: 1
  > Global Flags: 0x0000
  Message Type: MPLS Echo Request (1)
  Reply Mode: Reply via an IPv4/IPv6 UDP packet (2)
  Return Code: No return code (0)
  Return Subcode: 0
  Sender's Handle: 0xc7735d85
  Sequence Number: 284
  Timestamp Sent: Feb  3, 2017 10:41:23.998999000 UTC
  Timestamp Received: Jan  1, 1970 00:00:00.000000000 UTC
  Vendor Private
  Type: Vendor Private (64512)
  Length: 12
  Vendor Id: ciscoSystems (9)
  Value: 0001000400000004
  Target FEC Stack
  Type: Target FEC Stack (1)
  Length: 20
  FEC Element 1: FEC 128 Pseudowire (new)
  Type: FEC 128 Pseudowire (new) (10)
  Length: 14
  Sender's PE Address: 10.1.1.1
  Remote PE Address: 10.6.6.6
  VC ID: 100
  Encapsulation: Ethernet (5)
  MBZ: 0x0000
  Padding: 0000

```

2. Risposta Di Echo:

può trasportare 1 etichetta - Trasporto

Inviato come PACCHETTO UNICAST. Questa può essere commutata con etichetta (con etichetta di trasporto) a causa di LDP in un core.

ETICHETTE:1

SRC IP: INDIRIZZO IP DELL'INTERFACCIA EXIT (10.1.6.2 nel nostro caso)

DST IP: IP DI ORIGINE RILEVATO NELLA RICHIESTA ECHO - LOOPBACK DEL ROUTER DI ORIGINE

TIPO L4: UDP

PORTA SRC:3503

PORTA DST: 3505

BYTE TOS: OFF

MPLS EXP: DISATTIVATO

BIT DF: ON

IL PAYLOAD UDP PUÒ ESSERE UNA RISPOSTA ECHO DI LABEL SWITCHING MPLS

MPLS EXP è ON e IMPOSTATO su 6

Il bit DF è ON

Dettagli VC da consultare:

<#root>

```
R1#sh mpls l2transport vc detail
```

```
Local interface: Fa2/0 up, line protocol up, Ethernet up
```

```
Destination address: 10.6.6.6
```

```
,
```

```
VC ID: 100, VC status: up
```

```
Output interface: Fa0/1, imposed label stack {24 28}
```

```
Preferred path: not configured
```

```
Default path: active
```

```
Next hop: 10.1.1.2
```

```
Create time: 2d17h, last status change time: 2d17h
```

```
Last label FSM state change time: 2d17h
```

```
Signaling protocol: LDP, peer 10.6.6.6:0 up
```

```
Targeted Hello: 10.1.1.1(LDP Id) -> 10.6.6.6, LDP is UP
```

```
Status TLV support (local/remote) : enabled/supported
```

```
LDP route watch : enabled
```

```
Label/status state machine : established, LruRru
```

```
Last local dataplane status rcvd: No fault
```

```
Last BFD dataplane status rcvd: Not sent
```

```
Last BFD peer monitor status rcvd: No fault
```

```
Last local AC circuit status rcvd: No fault
```

```
Last local AC circuit status sent: No fault
```

```
Last local PW i/f circ status rcvd: No fault
```

```
Last local LDP TLV status sent: No fault
```

```
Last remote LDP TLV status rcvd: No fault
```

```
Last remote LDP ADJ status rcvd: No fault
```

MPLS VC labels: local 28, remote 28

Group ID: local 0, remote 0

MTU: local 1500, remote 1500

Remote interface description:

Sequencing: receive enabled, send enabled

Sequencing resync disabled

Control Word: On (configured: autosense)

Dataplane:

SSM segment/switch IDs: 4097/4096 (used), PWID: 1

VC statistics:

transit packet totals: receive 1027360, send 1027358

transit byte totals: receive 121032028, send 147740215

transit packet drops: receive 0, seq error 0, send 0

Interoperabilità L2VPN

L'interworking L2VPN si basa su questa funzionalità consentendo la connessione di circuiti di collegamento diversi. Una funzione di interworking facilita la traduzione tra diversi incapsulamenti di layer 2. Nelle versioni precedenti, i router della serie Cisco supportavano solo l'interworking con bridging, noto anche come interworking Ethernet.

Fino a questo punto, l'ACL su entrambi i lati è stato dello stesso tipo di incapsulamento, noto anche come funzionalità "like-to-like".

L2VPN Interworking è funzionalità AToM che consente un diverso tipo di incapsulamento su entrambi i lati della rete AToM

- È necessario interconnettere due circuiti di collegamento eterogenei (CA).
- Le due funzioni principali di L2VPN Interworking (IW) supportate nel software Cisco IOS sono:

1. IP/Routed: L'intestazione MAC viene rimossa (e sostituita con etichette MPLS) su un'estremità del cloud MPLS e viene costruita una nuova intestazione MAC sull'altra PE. L'intestazione IP rimane invariata.

2. Ethernet/Bridged: l'intestazione MAC non viene rimossa affatto. Le etichette MPLS vengono applicate sull'intestazione MAC e l'intestazione MAC viene consegnata così come è all'altra estremità del cloud MPLS.

Possibilità di interworking

- a. Da FR a Ethernet
- b. Da FR a PPP
- c. Da FR ad ATM
- d. Da Ethernet a VLAN
- e. Da Ethernet a PPP

Informazioni correlate

- [RFC Editor 4664](#)
- [RFC Editor 4667](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

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).