

ケーブル ネットワークによる透過 LAN サービス

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[ケーブルを介した 802.1Q TLS とは何ですか](#)

[市場を牽引している要素](#)

[802.1Q TLS の操作はどのように機能しますか](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[ケーブル モデムの初期化](#)

[トラフィックの通過](#)

[トラブルシューティング](#)

[設計上の考慮事項](#)

[ケーブル側 \(DOCSIS \)](#)

[一般的な問題](#)

[付録 A : L2 スイッチと集約ルータ間のパケットトレース](#)

[関連情報](#)

概要

従来、ホーム ユーザ、および IP ベースのレイヤ 3 バーチャル プライベート ネットワーク (VPN) に、高速データ サービスを提供するために Cisco ケーブル モデム ターミネーション システム (CMTS) が使用されています。

ただし、ビジネスを行うためにレイヤ 2 接続を必要とするお客様もいます。

レイヤ 2 バーチャル プライベート ネットワーク (L2VPN) の展開を正当化する理由の一部は次のとおりです。

- 非 IPv4 プロトコルのサポート
- エンドツーエンド暗号化
- より多くのネットワーク機能
- プライベート IP アドレス空間の使用

通常、レイヤ 2 サービスは電話会社 (Telco) によって提供され、専用回線、フレームリレー、ISDN、ATM など、さまざまなテクノロジーが採用されています。

802.1Q 透過型 LAN サービス (TLS) 機能の導入によって、マルチプル サービス オペレータ (MSO) は L2VPN サービスを提供するために、その DOCSIS 展開を利用することによって、商用製品を強化できます。

前提条件

要件

このドキュメントの読者は次のトピックについて理解する必要があります。

- Cisco IOS® ソフトウェア リリース 12.2(15)BC2
- uBR7200VXR プラットフォーム

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco uBR7246 VXR ユニバーサル ブロードバンド ルータ
- Cisco Catalyst 2924-XL (サポート終了)
- Cisco 7206 VXR ルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

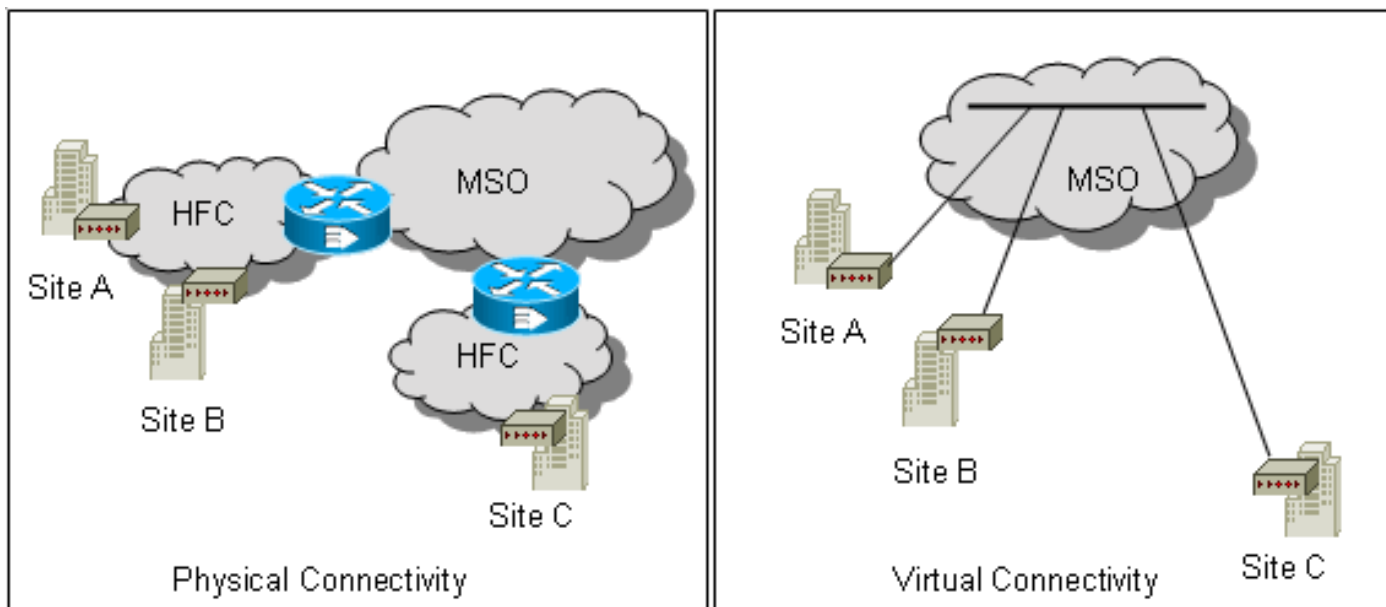
ケーブルを介した 802.1Q TLS とは何ですか

802.1Q TLS 機能は、プライベートな専用回線、フレームリレー、ISDN、ATM、SMDS、および電話会社の提供するものと同じように、複数のサイト間で L2VPN を作成する方法を提供します。

多くの場合、TLS は「フレームリレーのようなもの」と見なすことができます。ポイントツーポイント、ポイントツーマルチポイント、フルメッシュなど、多数のトラフィックパターンに対応できます。

図 1 に、802.1Q TLS の展開が概念的にはどのように VLAN に似ているかを示します。

図 1



市場を牽引している要素

この機能の導入の主要なドライバは、収益を増やす可能性です。

802.1Q TLS 機能は、より経済的な L2VPN サービスをエンド ユーザに提供することにより MSO が電話会社と競合できるようにします。

MSO のフットプリントは、すでに展開全体で多くの商用領域と接触しています。これらのビジネスの多くは、ケーブル TV サービスや電話会社の提供する既存のレイヤ 2 サービスにすでにサブスクリブします。

これらの電話会社の L2 サービスには、ローカル ループ アクセス、スイッチ ポート アクセスなどの繰り返し発生するコストが存在する傾向があります。

ほとんどの場合、802.1Q TLS サービスは次のように簡単に導入できます。

1. カスタマー サイトにケーブル モデムを届けます。
2. MSO のネットワーク機器を正しくプロビジョニングします。

サービスをさらに魅力的で市場向きにするため、MSO はケーブル TV と TLS をバンドルすることも選択できます。

802.1Q TLS の操作はどのように機能しますか

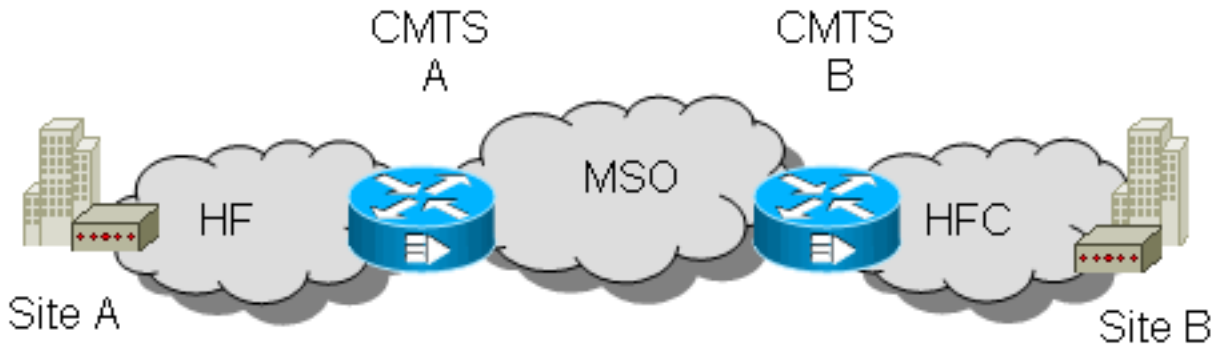
802.1Q TLS セットアップでは、特定の顧客のケーブル モデムは DOCSIS で説明されている標準のプロビジョニング方法でプロビジョニングされます。

プロビジョニングに加えて、CMTS は dot1q マップとして知られている定義で設定されます。dot1q マップには、ケーブル モデムの MAC アドレス、VLAN ID、発信インターフェイスなどが含まれます。これらの定義 (またはバインディング) は、サービス ID (SID) のデータベースに伝播されます。

特定のケーブル モデムから着信するトラフィックは VLAN ID でタグ付けされ、同じ顧客の別の VLAN とブリッジングできるネットワークに送信されます。VLAN のブリッジングは、いくつかの方法で実行できます。

図 2 に、TLS の仕組みを図解するために L2VPN のポイントツーポイント トポロジを示します。

図 2



各 CMTS には、ケーブル モデムの MAC アドレスを VLAN ID と発信インターフェイスとバインドする dot1q マップ定義があります。

サイト A からサイト B のパケットをトレースするとします。次のイベントは CMTS A がサイト A からのトラフィックを処理する方法を説明しています。

1. ケーブル モデムはイーサネット フレームを取得し、ケーブル モデムの SID (または SFID) を含む DOCSIS ヘッダーを追加します。
2. トラフィックを受信すると、CMTS は SID のルックアップを実行します。
3. CMTS は、SID に基づいてトラフィックが TLS かどうかを判断します。
4. トラフィックが TLS の場合、CMTS はパケットを調べて送信元の MAC アドレスを確認します。MAC アドレスがケーブル モデムの MAC アドレスに一致すると、トラフィックはレイヤ 3 スイッチング コードに送信されます。MAC アドレスがケーブル モデムの MAC アドレスに一致しない場合、トラフィックには適切な VLAN タグが付けられて、対応する発信インターフェイスに送信されます。

CMTS B では、サイト A から着信するパケットは次のように処理されます。

1. CMTS が VLAN タグ付きのフレームを受信すると、VLAN がケーブル モデムにマッピングされているかどうかを確認するためにデータベースのルックアップを実行します。
2. 一致がある場合、CMTS は VLAN のタグを削除して、DOCSIS ヘッダーを追加されます。
3. CMTS は適切な CoS または QoS パラメータに準拠するように、新しい DOCSIS パケットを処理します。
4. その後、パケットはケーブル インターフェイスで送信されます。

設定

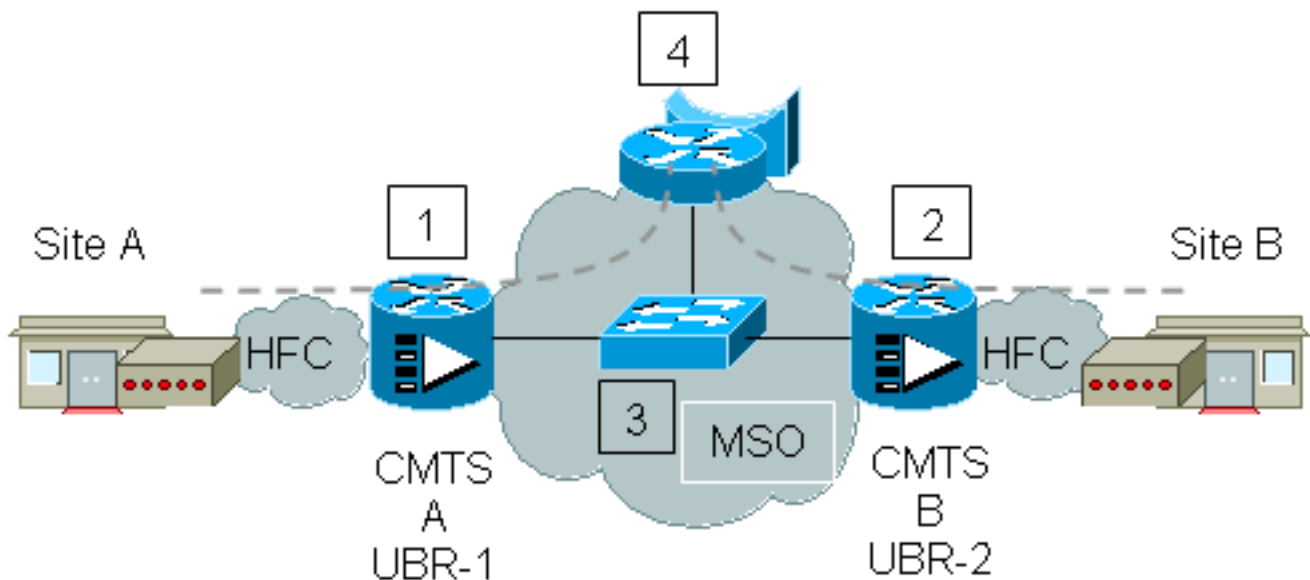
この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ([登録ユーザ専用](#)) を使用してください。

ネットワーク図

図 3 は、「[設定](#)」および「[確認](#)」の項で使用されるネットワーク トポロジを示します。

図3



設定

このドキュメントでは、次の設定を使用します。

1. [CMTS A](#)
2. [CMTS B](#)
3. [スイッチ](#)
4. [集約ルータ](#)

CMTS A

```
UBR-1:
↓
cable l2-vpn-service dot1q
cable dot1q-vc-map 0000.3973.be53 FastEthernet0/1 12
↓
```

CMTS B

```
UBR-2:
!
cable l2-vpn-service dot1q
cable dot1q-vc-map 0000.39a7.8a67FastEthernet0/0 21
!
```

スイッチ

```
!
interface FastEthernet0/1
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface FastEthernet0/2
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface FastEthernet0/3
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
```

```
SW# show vlan id 12 00:44:03: %SYS-5-CONFIG_I:
Configured from console by console VLAN Name Status
Ports ---- -
```

```

----- 12 VLAN0012 active VLAN
Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Transl
Trans2 -----
- - - - - 12 enet 100012 1500 - - -
- - 0 0 SW# show vlan id 21 VLAN Name Status Ports ----
-----
----- 21 VLAN0021 active VLAN Type SAID MTU
Parent RingNo BridgeNo Stp BrdgMode Transl Trans2 -----
-----
----- 21 enet 100021 1500 - - - - - 0 0

```

集約ルータ

```

↓
bridge irb
↓
↓
interface FastEthernet0/1
  no ip address
  duplex auto
  speed auto
↓
interface FastEthernet0/1.12
  encapsulation dot1Q 12
  bridge-group 1
↓
interface FastEthernet0/1.21
  encapsulation dot1Q 21
  bridge-group 1
↓
bridge 1 protocol ieee
↓

```

確認

このセクションでは、設定が正しく動作していることを確認するための情報が提供されています。

特定の **show** コマンドは、[Output Interpreter Tool](#) ([登録](#) ユーザ専用) によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

ケーブル モデムの初期化

802.1Q TLS のためにプロビジョニングされたモデムがオンラインになると、モデムを VLAN ID と出カインターフェイスにバインドするマップが作成されます。

次の debug コマンドを発行して、マッピングを確認します。

- [debug cable mac-address](#)
- [debug cable l2-vpn](#)

この出力はケーブル モデムがオンラインになるときに、CMTS が VLAN と発信インターフェイスがどのようにマッピングされるかを示します。また、VLAN と関連付けられたダウンストリームおよびアップストリームのサービス フロー ID も示します。

```

!--- Logs from CMTS A (UBR-1): UBR-1# show debug CMTS: CMTS L2 VPN debugging is on CMTS
specific: Debugging is on for Address 0000.3973.be53, Mask ffff.ffff.ffff UBR-1#
cmts_l2vpn_init_cm: cm 0000.3973.be53 on Cable3/0, sid 0xA map to FastEthernet0/1 VLAN id 12

```

Mapped DS srv flow 22 on Cable3/0 to FastEthernet0/1 VLAN 12 Mapped US srv flow 21 sid 10 on Cable3/0 to FastEthernet0/1 VLAN 12

トラフィックの通過

トラフィックがケーブル モデムから着信したもののか、またはケーブル モデムに発信されたものかどうかを確認するには、トラフィックをデバッグするか、カウンタを表示できます。

デバッグするには、次のデバッグをオンにします。

- [debug cable mac-address](#)
- [debug cable l2-vpn conditional](#)

注: 次のデバッグは、uBR7200 プラットフォームでのみ使用できます。

次の出力例は、**debug cable mac-address mac-address verbose** と **debug cable l2-vpn conditional** をアクティブにしたときのサイト A からサイト B へのパケットのデバッグを示します。

デバッグの最初の行は、サイト A から受信したパケットです。パケットが ping パケットであるため、次のデバッグの行は ping の応答です。どのようにパケットがケーブル モデムに送信されるかを示します。

```
UBR-1#
```

```
Pkt (size 114) from CM 0000.3973.be53 sid 10 src 0008.a3b6.d371  
dst 0008.a3b6.d74b fwd to FastEthernet0/1 vlan 12
```

```
Send pkt size 118 from 0008.a3b6.d74b on FastEthernet0/1:vlan 12  
to 0008.a3b6.d371 on Cable3/0:0xA CM 0000.3973.be53
```

バイトまたはパケット カウンタを表示するには、[show cable l2-vpn dot1q-vc-map mac-address verbose](#) コマンドを発行します。

```
UBR-1# show cable l2-vpn dot1q-vc-map 0000.3973.be53 verbose MAC Address : 0000.3973.be53  
Customer Name : Prim Sid : 5 Cable Interface : Cable3/0 Ethernet Interface : FastEthernet0/1  
DOT1Q VLAN ID : 12 Total US pkts : 0 Total US bytes : 0 Total DS pkts : 12 Total DS bytes : 816
```

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

設計上の考慮事項

DOCSIS ネットワークでサービスを展開する場合は、考慮する必要があるいくつかの設計要素があります。一部はケーブル側に固有のもので、その他はより一般的な問題です。

ケーブル側 (DOCSIS)

パイプのサイズまたはスループット

通常、主な制限はアップストリームの帯域幅を対象とします。表 1 に、異なるスループット値におけるおおよその数値を示します。

表 1

DOCSISバージョン	チャンネル幅 (MHz)	変調	おおよそのスループット (Mbps)
1.x	1.6	QPSK	2.2
1.x	1.6	16-QAM	4.4
1.x	3.2	16-QAM	8.9
2.0	3.2	64-QAM	13
2.0	6.4	64-QAM	26

DOCSIS バージョン 1.1 では、アップストリーム チャンネルを最適化する多くの機能が加わりました。これらの機能の一部には次のものが含まれています。

- 連結
- フラグメンテーション
- ペイロードヘッダー抑制

[DOCSIS QoS](#)

認定とベスト エフォート : DOCSIS バージョン 1.0 では、アップストリームのみで保証レートが許可されます。バージョン 1.1 および 2.0 では、両方向の保証レートが許可されます。認定情報レート (CIR) を保証するため、CMTS スケジューラはアップストリームのアドミッション制御を行い、オーバーサブスクリプションを防ぎます。

制御された遅延とジッター : DOCSIS のバージョン 1.1 の Unsolicited Grants (UGS) は、固定ビットレート (CBR) と同様のサービスを提供します。遅延とジッターを効果的に制御することによって、固定インターバルで認可を必要とするトラフィックに保証された最小データ レートを提供できます。

[セキュリティ](#)

ケーブル プラントを通過するトラフィックは、DOCSIS バージョン 1.0 または BPI+、DOCSIS の新しいバージョンで DOCSIS のベースライン プライバシー インターフェイス (BPI) を使用してセキュリティで保護できます。それからは、誰かがケーブル側のデータのスヌーピングや盗聴できなくなります。

たとえば、金融機関などの高いセキュリティを必要とするお客様には、エンドツーエンド IPsec 戦略が推奨されます。詳細については、[シスコのセキュリティ](#)を参照してください。

[一般的な問題](#)

[QoS](#)

802.1Q 環境では、3 つの主要な QoS 分野があります。

- CPE 側：CPE でトラフィックのポリシングとマーキングがどのように行われているか。これは、お客様によって制御され、その内部 QoS ポリシーに関連しています。
- ケーブル側：DOCSIS のプロトコルとケーブル モデムのプロビジョニングに準拠します。
- バックボーン：MSO はサービス レベル契約に基づいて QoS ポリシーを適用できます。

パフォーマンスと拡張性

CMTS では、データ構造と dot1q マップ (データベース) を保持するためメモリ量が少しだけ増えます。TLS パケットの交換は、他のパケットと同じです。

サポートされている VLAN の数は、プラットフォームによって異なります。

ブリッジング グループは、プラットフォームによって異なります。

イーサネットの境界を超えて 802.1Q TLS を拡張する方法

お客様がイーサネットの物理制限を超えているサイトへの接続を必要とする場合があります。たとえば、異なる町、市、または県にあるサイトなどです。

このような場合、MSO はいくつかの Metro Ethernet Relay Service ソリューションのいずれかを使用できます。

この中でラボでテスト済みの 2 つのソリューションは、次のとおりです。

- レイヤ 2 トンネル プロトコル (L2TP) バージョン 3 経由の IP コア ネットワークを介した TLS
- Ethernet over MPLS (EoMPLS) 経由のマルチプロトコル ラベル スイッチング (MPLS) コアを介した TLS

付録 A : L2 スイッチと集約ルータ間のパケット トレース

ここでは、スイッチと集約ルータ間の ping パケットのパケット トレースを示します。2 つの ping 要求パケットがあることに注意してください。1 つはサイト A から集約ルータへの、1 つは集約ルータからサイト B への ping 要求パケットです。ping 応答についても同様です。

```

Frame 1 (118 bytes on wire, 118 bytes captured)
Ethernet II, Src: 00:08:a3:b6:d3:71, Dst: 00:08:a3:b6:d7:4b
802.1q Virtual LAN
  000. .... .. = Priority: 0
  ...0 .... .. = CFI: 0
  .... 0000 0000 1100 = ID: 12 Type: IP (0x0800) Internet Protocol, Src Addr: 192.168.50.1
(192.168.50.1), Dst Addr: 192.168.50.2 (192.168.50.2) Internet Control Message Protocol Type: 8
(Echo (ping) request) Code: 0 Checksum: 0x3fb9 (correct) Identifier: 0x0008 Sequence number:
0x0000 Data (72 bytes) 0000 00 00 00 00 00 3d 3e 4c ab cd ab cd ab cd .....=>L.....
0010 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ..... 0020 ab cd ab cd ab cd ab
cd ab cd ab cd ab cd ..... 0030 ab cd ab cd ab cd ab cd ab cd ab cd ab cd
..... 0040 ab cd ab cd ab cd ab cd ..... Frame 2 (118 bytes on wire, 118 bytes
captured) Ethernet II, Src: 00:08:a3:b6:d3:71, Dst: 00:08:a3:b6:d7:4b 802.1q Virtual LAN 000.
.... .. = Priority: 0 ...0 .... .. = CFI: 0 .... 0000 0001 0101 = ID: 21 Type: IP
(0x0800) Internet Protocol, Src Addr: 192.168.50.1 (192.168.50.1), Dst Addr: 192.168.50.2
(192.168.50.2) Internet Control Message Protocol Type: 8 (Echo (ping) request) Code: 0 Checksum:
0x3fb9 (correct) Identifier: 0x0008 Sequence number: 0x0000 Data (72 bytes) 0000 00 00 00 00 00
3d 3e 4c ab cd ab cd ab cd .....=>L..... 0010 ab cd ab cd ab cd ab cd ab cd ab cd

```

ab cd 0020 ab cd ab cd ab cd ab cd ab cd ab cd ab cd
0030 ab cd ab cd ab cd ab cd ab cd ab cd ab cd 0040 ab cd ab cd ab cd ab
cd Frame 3 (118 bytes on wire, 118 bytes captured) Ethernet II, Src: 00:08:a3:b6:d7:4b,
Dst: 00:08:a3:b6:d3:71 802.1q Virtual LAN 000. = Priority: 0 ...0 =
= CFI: 0 0000 0001 0101 = **ID: 21** Type: IP (0x0800) Internet Protocol, Src Addr:
192.168.50.2 (192.168.50.2), Dst Addr: 192.168.50.1 (192.168.50.1) Internet Control Message
Protocol Type: 0 (**Echo (ping) reply**) Code: 0 Checksum: 0x47b9 (correct) Identifier: 0x0008
Sequence number: 0x0000 Data (72 bytes) 0000 00 00 00 00 00 3d 3e 4c ab cd ab cd ab cd
.....=>L..... 0010 ab cd ab cd ab cd ab cd ab cd ab cd ab cd 0020 ab
cd ab cd ab cd ab cd ab cd ab cd ab cd 0030 ab cd ab cd ab cd ab cd ab cd
ab cd ab cd ab cd 0040 ab cd ab cd ab cd ab cd Frame 4 (118 bytes on
wire, 118 bytes captured) Ethernet II, Src: 00:08:a3:b6:d7:4b, Dst: 00:08:a3:b6:d3:71 802.1q
Virtual LAN 000. = Priority: 0 ...0 = CFI: 0 0000 0000 1100 =
ID: 12 Type: IP (0x0800) Internet Protocol, Src Addr: 192.168.50.2 (192.168.50.2), Dst Addr:
192.168.50.1 (192.168.50.1) Internet Control Message Protocol Type: 0 (**Echo (ping) reply**) Code:
0 Checksum: 0x47b9 (correct) Identifier: 0x0008 Sequence number: 0x0000 Data (72 bytes) 0000 00
00 00 00 00 3d 3e 4c ab cd ab cd ab cd=>L..... 0010 ab cd ab cd ab cd ab cd ab cd
ab cd ab cd ab cd 0020 ab cd ab cd ab cd ab cd ab cd ab cd ab cd
..... 0030 ab cd ab cd ab cd ab cd ab cd ab cd ab cd 0040 ab
cd ab cd ab cd ab cd

[関連情報](#)

- [ブロードバンド ケーブルに関するサポート ページ](#)
- [テクニカルサポート - Cisco Systems](#)