MACsec を使用した BPDU 透過性の設定

この章では、MACsec 機能での BPDU 透過性について説明します。この機能を使用すると、送信元カスタマー エッジ（CE）デバイスと宛先 CE デバイス間にトンネルを作成し、このトンネルをこれら 2 つの CE 間でのトラフィックの伝送に使用します。

MACsec でのレイヤ 2 コントロール プレーンのトンネリング

レイヤ 2 コントロール プレーン トンネリングのパントの判断は、MACsec で設定されているインターフェイスによって異なります。メイン インターフェイスが MACsec ポリシーで設定されている場合、すべての MACsec パケットがパントされるため、カスタマー エッジ（CE）デバイスとプロバイダー エッジ（PE）デバイス間に MACsec セッションが確立されます。メイン インターフェイスが MACsec で設定されていない場合は、すべての MACsec パケットがリモート CE へトンネリングされます。

MACsec および MKA の概要

MACsec は、IEEE 802.1AE 規格ベースのレイヤ 2 ホップバイホップ暗号化であり、これにより、メディア アクセス非依存プロトコルに対してデータの機密性と完全性を確保できます。

MACsec は、暗号化キーにアウトオブバンド方式を使用して、有線ネットワーク上で MAC レイヤの暗号化を提供します。MACsec Key Agreement（MKA）プロトコルでは、必要なセッション キーを提供し、必要な暗号化キーを管理します。ホスト側のリンク（ネットワーク アクセス デバイスと、PC や IP フォンなどのエンドポイント デバイス間のリンク）だけが MACsec を使用して保護できます。

MACsec Key Agreement（MKA）による 802.1AE 暗号化は、ホスト デバイス間の暗号化用に、ダウンリンク ポートでサポートされています。

MACsec は、イーサネット パケットの送信元および宛先 MAC アドレスを除くすべてのデータを暗号化します。

WAN またはメトロ イーサネット上に MACsec サービスを提供するために、サービス プロバイダーは、Ethernet over Multiprotocol Label Switching（EoMPLS）および L2TPv3 などのさまざまなトランスポート レイヤ プロトコルを使用して、E-Line や E-LAN などのレイヤ 2 透過サービスを提供しています。

EAP-over-LAN（EAPOL）プロトコル データ ユニット（PDU）のパケット本体は、MACSec Key Agreement PDU（MKPDU）と呼ばれます。3 回のハートビート後（各ハートビートは 2 秒）に参加者から MKPDU を受信しなかった場合、ピアはライブ ピア リストから削除されます。たとえば、クライアントが接続を解除した場合、スイッチ上の参加者はクライアントから最後の MKPDU を受信した後、3 回のハートビートが経過するまで MKA の動作を継続します。

MKA 機能のサポートにより、暗号化されていない VLAN タグ（802.1Q タグ）などのトンネリング情報を提供します。そのため、サービス プロバイダーは、複数のポイントツーポイント サービスが単一の物理インターフェイス上で共存でき、表示されるようになった VLAN ID に基づいて差別化できるように、サービス多重化を提供できます。

サービス多重化の他に、暗号化されていない VLAN タグもサービス プロバイダーが 802.1Q タグの一部として表示されている 802.1P（CoS）に基づいて SP ネットワーク全体にわたり Quality of Service（QoS）を提供できるようにします。

L2CP トンネリング

レイヤ 2 制御プロトコル トンネリング（L2PT）は、レイヤ 2 スイッチング ドメイン間でイーサネット プロトコル フレームをトンネリングするための、シスコ独自のプロトコルです。レイヤ 2 コントロール プレーンは、数多くのカスタマー コントロール プレーンとプロバイダー コントロール プレーンに分割されています。IEEE 規格 802.1Q-2011 で定義されているように、L2CP フレームはコントロール プレーン用に予約されている 32 個のアドレスのうちの 1 つである宛先 MAC アドレスを含んでいるフレームです。VPWS または VPLS のサービスを使用してトラフィックを転送できます。

MACsec での L2CP トンネリング

パントの判断は、MACsec で設定されているインターフェイスによって異なります。インターフェイスが MACsec ポリシーで設定されている場合は、すべての MACsec パケットがパントされるため、2つのカスタマーエッジ（CE）デバイス間で MACsec セッションが確立されます。インターフェイスが MACsec で設定されていない場合は、すべての MACsec パケットがリモート CE にトンネリングされます。MACsec はサブインターフェイスでは設定できません。

CE が MACsec で設定されていて、PE が L2VPN VPWS で設定されている場合、すべての MACsec パケットは VPWS を介してトンネリングされます。

PC のいずれかの CE 接続インターフェイスで MACsec が設定されている場合、このインターフェイス上のすべての MACsec パケットはパントされます。これらのパケットはリモート CE に転送されません。PE のインターフェイスで MACsec が設定されている場合、PE デバイスと CE デバイス間で MACsec セッションは確立されません。

設定

以降の項では、MACsec 機能を使用して BPDU 透過性を設定する手順について説明します。

- MPLS のコアの設定
- L2VPN クロス コネクトの設定
- CE デバイスでの MACsec の設定

L2VPN クロス コネクトの設定

コアに接続するインターフェイス上に IPv4 アドレスを設定します。

```
Router# configure
Router(config)# interface tengige 0/1/0/8/2.1
Router(config-subif)# no shut
Router(config-subif)# ipv4 address 192.0.2.1/24
```

IPv4 ループバック インターフェイスを設定します。

```
Router# configure
Router(config)#  interface loopback 0
Router(config)# ipv4 address 10.0.0.1/32
```

IGP として OSPF を設定します。

```
Router# configure
Router(config)# router ospf 100 area 0
Router(config-ospf-ar)# interface Tengige 0/1/0/8/3
Router(config-ospf-ar-if)# exit
Router(config-ospf-ar)# interface loopback 1
```

物理コア インターフェイスに MPLS LDP を設定します。

```
Router(config-ospf-ar)# mpls ldp
Router(config-ldp)# interface TenGigE 0/1/8/3
```

コアに接続するインターフェイス上に IPv4 アドレスを設定します。

```
Router# configure
Router(config)#  router bgp 100
Router(config-bgp)# bgp router-id 10.10.10.1
Router(config-bgp)# address-family ipv4 unicast
Router(config-bgp-af)# exit
Router(config-bgp)# address-family l2vpn vpls-vpws
Router(config-bgp-af)# exit
Router(config-bgp)# neighbor 172.16.0.1
Router(config-bgp-nbr)# remote-as 2002
```

```
Router(config-bgp-nbr)# update-source loopback 2
Router(config-bgp-nbr)# address-family l2vpn vpls-vpws
Router(config-bgp-nbr-af)# next-hop-self
```

レイヤ 2 転送として AC を設定し、リモートの疑似回線にパケットを転送します。

```
Router# configure
Router(config)# interface TenGigE 0/1/0/8/2.1 l2tranport
Router(config-if)# encap dot1q 1
```

疑似回線であるネイバーを使用して L2VPN クロスコネクトを設定します。

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group g1
Router(config-l2vpn-xc)# p2p g1
Router(config-l2vpn-xc-p2p)# interface TenGigE 0/1/0/2.1
Router(config-l2vpn-xc-p2p)# neighbor 172.16.0.1 pw-id 1
Router(config-l2vpn-xc-p2p-pw)#
```

CE デバイスでの MACsec の設定

```
Router# configure
Router(config)# key chain KC1 macsec
Router(config-kc1-MacSec)# key 5010
Router(config-kc1-MacSec-5010)# key-string password
04795B232C766A6C513A5C4E37582F220F087178116703312446552501 7A0C7101 cryptographic-algorithm
 aes-128-cmac
Router(config-kc1-MacSec-5010)# lifetime 11:08:00 Aug 08 2017 infinite
Router(config-kc1-MacSec-5010)# commit
!
Router# configure
Router(config)# interface HundredGigE 0/0/0/3
Router(config-if)# macsec psk-keychain KC1
Router(config-if)# commit
```

実行コンフィギュレーション

ここでは、MACsec を使用した BFD 透過性の実行コンフィギュレーションを示します。

```
/* Configuring MPLS core.*/

/* Configure an IPv4 address on an interface that connects to the MPLS core. */

interface tengige 0/1/0/8/3
 no shut
 ipv4 address 192.0.2.0/24
!

/* Configure an IPv4 loopback interface. */

 interface loop 0
 ipv4 address 10.0.0.1/32

/* Configure OSPF as IGP. */

 router ospf 100 area 0
  interface TenGige 0/1/0/8/3
   interface loop 0
!
```

```
/* Configure MPLS LDP for the physical core interface. */

 mpls ldp
  interface TenGige 0/1/0/8/3
  !
!

/* Configuring L2VPN Xconnect. */

/* Configure an IPv4 address on an interface that connects to the MPLS core. */

router bgp 100
 bgp router-id 192.1.2.22
 address-family ipv4 unicast
 exit
 address-family l2vpn vpls-vpws
 neighbor 172.16.0.1
  remote-as 100
  update-source Loopback2
  address-family l2vpn vpls-vpws
   next-hop-self

/* Configure L2VPN Xconnect with a neighbour which is a pseudowire. */

l2vpn
 xconnect group g1
  p2p g1
  interface tengige 0/1/0/8/2.1
  neighbor 172.16.0.1 pw-id 1

/* Configure MACSec on CE device */
configure
 key chain KC1 macsec
  key 5010
   key-string password 04795B232C766A6C513A5C4E37582F220F087178116703312446552501 7A0C7101
 cryptographic-algorithm aes-128-cmac
   lifetime 11:08:00 Aug 08 2017 infinite
commit
!
configure
 interface HundredGigE0/0/0/3
  macsec psk-keychain KC1
commit
end
```

確認

次の項に示す show 出力には、MACsec 機能を使用した BPDU 透過性設定の詳細と、それらの設定のステータスが表示されます。

```
/* Verify if IGP on the core is up. */
Router# show ospf neighbor
Group Wed Aug 16 20:32:33.665 UTC
Indicates MADJ interface
# Indicates Neighbor awaiting BFD session up
Neighbors for OSPF 100
Neighbor ID     Pri   State           Dead Time   Address     Interface
172.16.0.1      1     FULL/DR         00:00:30    10.1.1.2    TenGigE0/1/0/8/0
 Neighbor is up for 06:05:27Total neighbor count: 1
```

```
/* Verify if the MPLS core is up. */
Router# show mpls ldp neighbor
Wed Aug 16 20:32:38.851 UTC

Peer LDP Identifier: 172.16.0.1:0
  TCP connection: 172.16.0.1:64932 - 172.31.255.254:646
  Graceful Restart: No
  Session Holdtime: 180 sec
  State: Oper; Msgs sent/rcvd: 487/523; Downstream-Unsolicited
  Up time: 06:05:24
  LDP Discovery Sources:
    IPv4: (2)
      TenGigE0/1/0/8/0
      Targeted Hello (172.31.255.254 -> 172.16.0.1, active)
    IPv6: (0)
  Addresses bound to this peer:
    IPv4: (8)
      10.0.0.1       10.0.0.2         10.0.0.200       172.16.0.1
      192.168.0.1    172.31.255.255   172.16.0.2       10.255.255.254
    IPv6: (0)

/* Verify if the BGP neighbor is up. */
Router# show bgp neighbor 10.10.10.1

Wed Aug 16 20:32:52.578 UTC

BGP neighbor is 10.10.10.1
 Remote AS 15169, local AS 15169, internal link
 Remote router ID 172.31.255.255
  BGP state = Established, up for 06:03:40
  NSR State: None
  Last read 00:00:34, Last read before reset 00:00:00
  Hold time is 180, keepalive interval is 60 seconds
  Configured hold time: 180, keepalive: 60, min acceptable hold time: 3
  Last write 00:00:34, attempted 19, written 19
  Second last write 00:01:34, attempted 19, written 19
  Last write before reset 00:00:00, attempted 0, written 0
   ****************
Connections established 1; dropped 0

/* Verify if the BGP neighbor's next-hop information is valid. */
Router# show cef 10.10.10.1
Wed Aug 16 20:33:18.949 UTC
10.10.10.1/32, version 16, internal 0x1000001 0x0 (ptr 0x8e0ef628) [1], 0x0 (0x8e287bc0),

 0xa20 (0x8e9253e0)
 Updated Aug 16 14:27:15.149
 local adjacency 172.16.0.1
 Prefix Len 32, traffic index 0, precedence n/a, priority 3
   via 172.16.0.1/32, TenGigE0/1/0/8/0, 5 dependencies, weight 0, class 0 [flags 0x0]
    path-idx 0 NHID 0x0 [0x8eb60568 0x8eb60e70]
    next hop 172.16.0.1/32
    local adjacency
     local label 64001      labels imposed {ImplNull}

/* Verify if L2VPN Xconnect is up. */
Router# show l2vpn xconnect

Wed Aug 16 20:47:01.053 UTC
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
        SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect                  Segment 1                       Segment 2
```

```
Group       Name        ST   Description            ST       Description            ST

------------------------   ------------------------------   ------------------------------
b1          b1          UP   BE100                  UP       10.10.10.1      1      UP

-----------------------------------------------------------------------------------------

/* Note: If L2VPN is down even though the MPLS LDP neighbor is up, check if the AC is
down.
To do this, use the show l2vpn xconnect detail command. */


/* Verify if L2VPN Xconnect is up */
Router# show l2vpn xconnect detail

!
 !

AC: Bundle-Ether100, state is up      <<<< This indicates that the AC is up.
    Type Ethernet
    MTU 1500; XC ID 0xa0000002; interworking none
    Statistics:
      packets: received 761470, sent 0
      bytes: received 94326034, sent 0
  PW: neighbor 10.10.10.1, PW ID 1, state is up ( established )
    PW class not set, XC ID 0xc0000001
    Encapsulation MPLS, protocol LDP
    Source address 172.16.0.2
    PW type Ethernet, control word disabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set

!
 !
```