

知 某局点S6520X-30QC-EI 无法建立MACSec会话问题

MACsec 刘雨 2022-03-28 发表

组网及说明

两台设备Ten1/1/1做MACSec对接

问题描述

两台设备Ten1/1/1做MACSec对接，如果不配置MacSec业务正常，配置后MACSec无法建立，端口mac-sec down

过程分析

现场使用的是支持mac-sec的子卡，两台设备之间裸光纤直连，debug看两端都有发报文，但是都没有收到对端的，直接就超时了：

```
<Line-Core>%Dec 25 18:13:45:312 2021 Line-Core IFNET/3/PHY_UPDOWN: Physical state on the interface Ten-GigabitEthernet1/1/1 changed to down.
```

```
*Dec 25 18:13:45:311 2021 Line-Core MACSEC/7/EVENT: -Slot=2; Received DOWN event on interface Ten-GigabitEthernet1/1/1.
```

```
*Dec 25 18:13:45:327 2021 Line-Core MACSEC/7/EVENT: Received DOWN event on interface Ten-GigabitEthernet1/1/1.
```

```
*Dec 25 18:13:47:531 2021 Line-Core MACSEC/7/EVENT: Connection status changed to Pending because of CP initialization on interface Ten-GigabitEthernet1/1/1.
```

```
*Dec 25 18:13:47:532 2021 Line-Core MACSEC/7/EVENT: Received UP event on interface Ten-GigabitEthernet1/1/1.
```

```
%Dec 25 18:13:47:532 2021 Line-Core IFNET/3/PHY_UPDOWN: Physical state on the interface Ten-GigabitEthernet1/1/1 changed to up.
```

```
*Dec 25 18:13:47:531 2021 Line-Core MACSEC/7/EVENT: -Slot=2; Received UP event on interface Ten-GigabitEthernet1/1/1.
```

```
*Dec 25 18:13:50:011 2021 Line-Core MACSEC/7/PKT:
```

```
Sent a MACsec Packet (length: 60) on interface Ten-GigabitEthernet1/1/1.
```

```
Basic Parameters
```

```
Tx priority      : 5
```

```
MACsec desire   : Yes
```

```
Key Server      : Yes
```

```
MACsec capability : 3
```

```
MI              : 94EF0B83FB1987C01B7ED995
```

```
MN              : 1
```

```
CKN             : E9AC
```

```
*Dec 25 18:13:51:997 2021 Line-Core MACSEC/7/PKT:
```

```
Sent a MACsec Packet (length: 60) on interface Ten-GigabitEthernet1/1/1.
```

```
Basic Parameters
```

```
Tx priority      : 5
```

```
MACsec desire   : Yes
```

```
Key Server      : Yes
```

```
MACsec capability : 3
```

```
MI              : 94EF0B83FB1987C01B7ED995
```

```
MN              : 2
```

```
CKN             : E9AC
```

```
*Dec 25 18:13:53:997 2021 Line-Core MACSEC/7/PKT:
```

```
Sent a MACsec Packet (length: 60) on interface Ten-GigabitEthernet1/1/1.
```

```
Basic Parameters
```

```
Tx priority      : 5
```

```
MACsec desire   : Yes
```

```
Key Server      : Yes
```

```
MACsec capability : 3
```

```
MI              : 94EF0B83FB1987C01B7ED995
```

```
MN              : 3
```

```
CKN             : E9AC
```

```
*Dec 25 18:13:53:997 2021 Line-Core MACSEC/7/EVENT: The MKA participant with CKN E9AC aged out on interface Ten-GigabitEthernet1/1/1.
```

后检查现场配置，发现端口没有允许vlan 1通过，但端口PVID缺省是1：

```
#
```

```
interface Ten-GigabitEthernet1/1/1
```

```
port link-mode bridge
```

```
port link-type trunk
```

```
undo port trunk permit vlan 1
```

```
port trunk permit vlan 42
```

```
macsec desire
```

macsec confidentiality-offset 30

macsec replay-protection window-size 100

macsec validation mode strict

修改端口放通vlan 1后协商正常。

macsec协商报文发出时会携带vlan tag，需要放通PVID对应的vlan。

mka psk ckn E9AC cak cipher \$c\$3\$zcE75HBnvGh7/D4QzSE+Wbln4G7xfXh/HqZP

#

mac-secc协商报文发出时会携带vlan tag，需要放通PVID对应的vlan。

