H3C MACsec Technology White Paper

Contents

Overview

Technical background

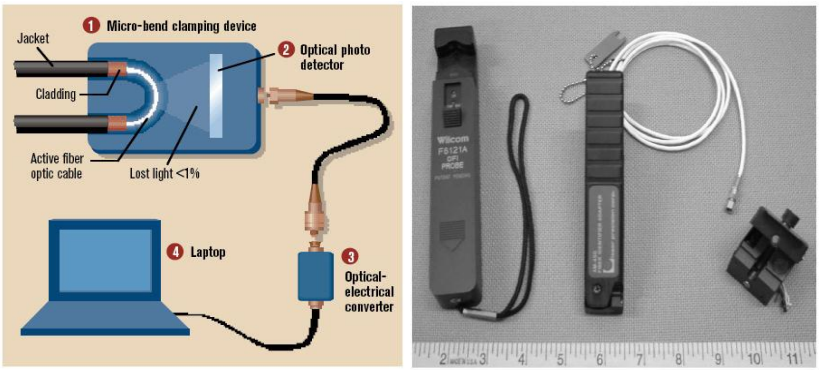
The PRISM incident raises unprecedented focus on network security. Securing network communication attracts wide attention from all walks of life.

Eavesdropping risks exist in Ethernet. Though 802.1X provides network access control for clients, it cannot encrypt data traffic to secure data transmission for these clients after they pass authentication.

The emergence of BYOD and the increasingly diverse access roles in the campus networks are breaking the traditional borders of campus networks, resulting in an increase in security risks.

For a campus network, cabling might inevitably traverse uncontrolled public areas. For example, two buildings at a long distance from each other in an enterprise campus network use fibers for network interconnection. The areas that the fibers traverse are public areas with a high risk of exposure. Currently, simple fiber sensing devices are already available for completely restoring and intercepting the content transmitted over a fiber. For example, a fiber eavesdropping apparatus was discovered on the network of Verizon in 2003, as shown in Figure 1. Such apparatuses are cheap and easy to use and operate.

Figure 1 Fiber eavesdropping apparatus



Cable sensing is another threat. Technologies are already available to sense electromagnetic field changes on a network cable when code streams are transmitted in the network cable. Based on electromagnetic induction principles, they can restore the content transmitted over the network cable. Using these technologies even can sense cables without destroying the original cabling.

Theoretically, the following methods are available to resolve the eavesdropping issue despite of the disadvantages:

- Traditional Layer 3 or Layer 4 encryption method such as IPsec.

  This method is not applicable to campus networks. It uses a point-to-point tunnel, and the intermediate devices receive packets in encrypted form and cannot perform policy-based control over the packets.

- External encryptors.

  The cost of an external encryptor is high and its performance barely suffices. The throughput capacity per port on a campus network already reaches 10 Gbps.

MACsec is thus introduced to secure data transmission on a campus network.

Benefits

MACsec is a hop-by-hop link layer security protocol suitable for the Ethernet. The protocol provides the following functions:

- **Data encryption**—Uses encryption algorithms and keys to change plain texts to garbled cipher texts. The cipher texts can hardly be decrypted even if they are intercepted.
- **Replay protection**—Prevents a hacker from capturing packets destined for a host and resending the packets to the host for the purpose of spoofing the host. For example, packet replay during identity authentication.
- **Anti-tampering**—Performs integrity check to prevent a hacker from altering the original content of a packet for malicious purposes.

MACsec has the following advantages:

- **Hardware-based**—Wire speed is attained for packet forwarding.
- **Coordination with 802.1X and easy deployment**—Suitable for campus networks.
- **Smooth compatibility**—An encrypted packet is decrypted into plain text after it arrives at a port. The original policy control for the packet can still be performed on the device. You do not need to change the original policy deployment.

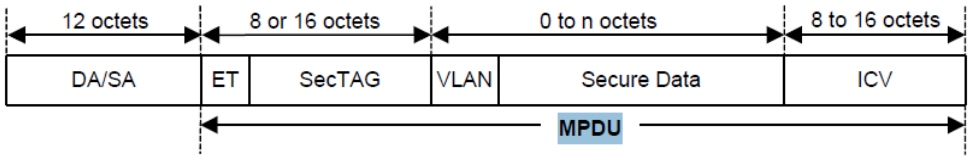
MACsec implementation

MACsec involves the 802.1AE and 802.1X-2010 standards. 802.1AE defines the data plane of MACsec, including the frame format and the mechanisms of encryption and replay protection. 802.1X-2010 defines the control plane of MACsec, including MACsec Key Agreement (MKA).

MACsec frame format

Figure 2 shows the MACsec frame format.

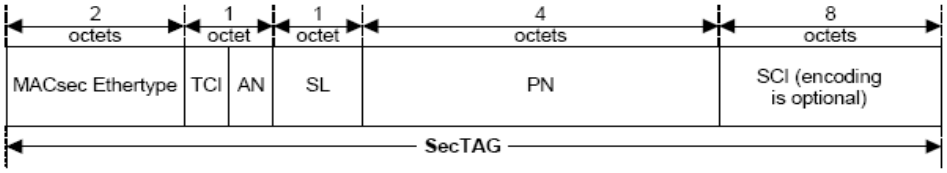
Figure 2 MACsec frame format



- **DA/SA**—Destination and source MAC addresses, each occupying 6 octets.
- **ET**—Ethernet type, which contains 2 octets. The value is **0x88E5**, which indicates the Ethernet type of the MACsec frame.
- **SecTAG**—Security tag, which contains 8 or 16 octets. For more information, see the description for Figure 3.
- **VLAN**—VLAN tag of the frame.
- **Secure Data**—Payload of the frame, which will be encrypted in cipher text. MACsec encrypts only the bytes after a confidentiality offset in the frame. A confidentiality offset can be 0, 30, or 50 bytes after the **ET** field.
- **ICV**—Integrity check value, which contains 8 to 16 octets. If the frame is altered, the ICV value will change. This field is used to protect the frame against malicious alteration.

Figure 3 shows the format of the **SecTAG** field.

Figure 3 Format of the SecTAG field



- **TCI**—TAG control information, which contains 6 bits to provide the following status information:
  - Version number.
  - Whether the frame is encrypted.
  - Whether the frame has experienced integrity check calculation.
  - Whether the ICV field is carried at the tail of the frame.
- **AN**—Association number. It contains 2 bits and indicates the secure association (SA) number of the secure channel (SC) on which the frame is sent. One SC can have four SAs.
- **SL**—Short length. The field value is the number of the octets in the **Secure Data** field if the number of octets in the **Secure Data** field is less than 48. Otherwise, the value of this field is zero.
- **PN**—Packet number, which contains 4 octets. The field value increments by 1 every time a frame is sent. This field is used to guard against the replay attack.
- **SCI (optional)**—Secure channel identifier, which contains 8 octets. It is a combination of a 6-octet MAC address and a 2-octet port number.

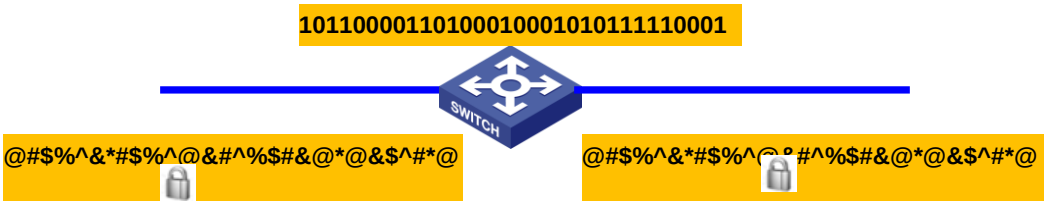
Packet encryption

MACsec performs packet encryption on a hop-by-hop basis. As shown in Figure 4, the MACsec packet encryption process is as follows:

1. After receiving an encrypted packet from the peer on the inbound port, the switch decrypts the packet. The switch will perform replay protection and integrity check on the packet if these features are configured on the switch.
2. The packet enters the switch in plain text mode.
3. The switch takes the predefined policy control actions on the packet content.
4. The switch uses another secure session established between the outbound port and its peer to re-encrypt the packet on the outbound port. After the encryption, the switch sends the packet out of the outbound port.

This encryption process highly improves data transmission security because data packets are always transmitted in ciphertext form over an exposed external cable. An encrypted packet can hardly be decrypted even if it is intercepted.

Figure 4 MACsec packet encryption



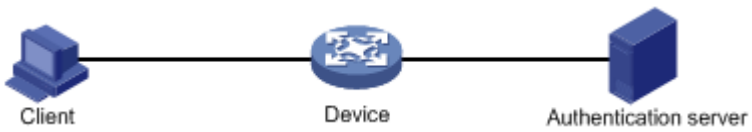
Mechanism

MACsec supports client-oriented and device-oriented modes.

Client-oriented MACsec

As shown in Figure 5, MACsec secures data transmission between the client and the access device. In this mode, MACsec must operate with 802.1X authentication.

Figure 5 Client-oriented MACsec

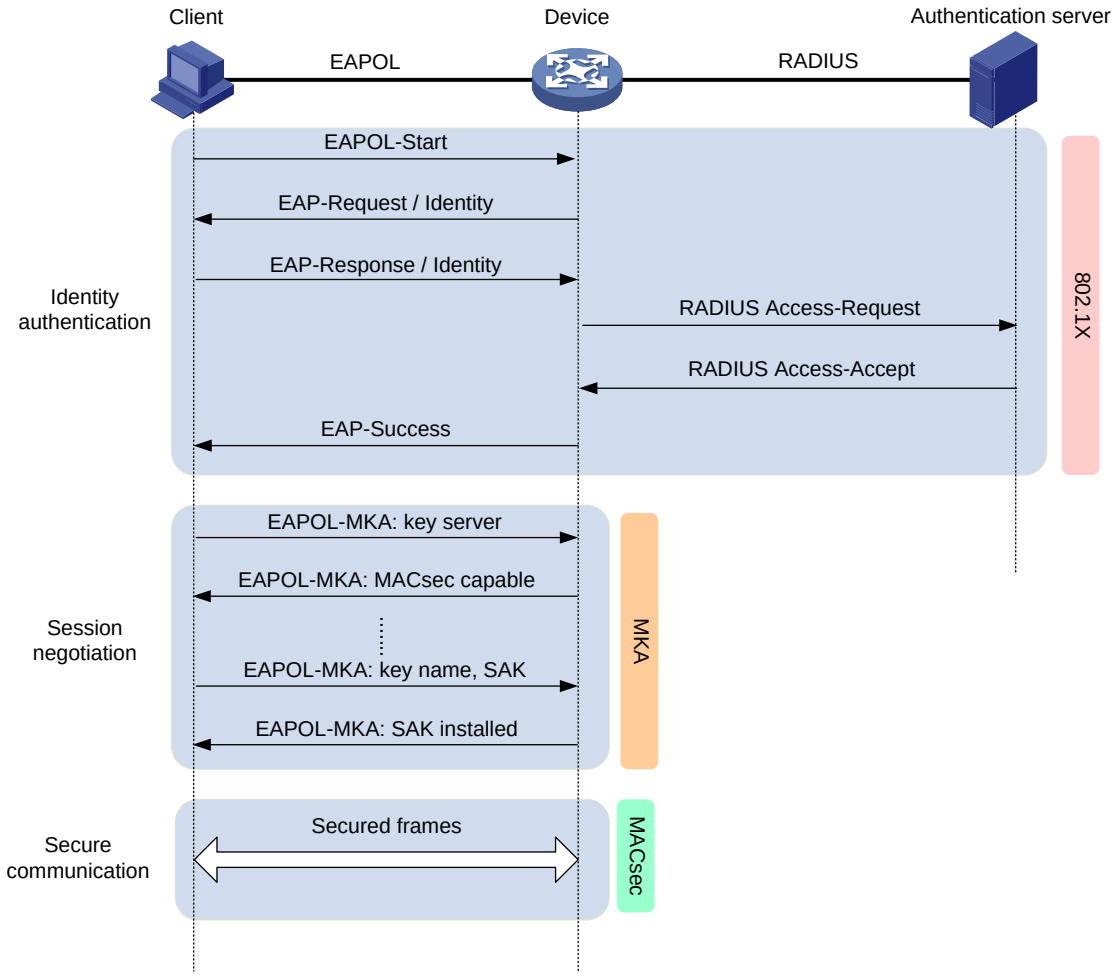


Client-oriented MACsec includes the following entities:

- **Client (supplicant)**—A software entity running on the client. It interacts with the authentication server and submits its own identity information to obtain the permission to access the network. To support MACsec, the client must support key negotiation and packet encryption. With key negotiation, the client can obtain keys securely. To have the packet encryption capability, the client can use either of the following methods:
  - Uses CPU soft encryption instead of having encryption capability by hardware. By using this method, the client can support MACsec but with limited performance.
  - Has the encryption capability embedded into the board of the client. The client can implement the encryption feature on hardware. This is the mainstream method. Currently, the board of an X86 client uses Intel Ethernet controller chips in most cases, and MACsec is embedded as a basic function in these chips.
- **Access device (authenticator)**—Acts as a control point or policy execution point during network access, usually a switch. Similar to the supplicant, the authenticator also must support key negotiation and packet encryption. Key negotiation can be easily supported through software, but packet encryption requires special hardware of the switch. Once packet encryption is supported, the packet encryption capability can attain wire speed such as 10 Gbps. This greatly outruns traditional encryption methods such as the encryptor and IPsec. In addition, hardware-based encryption saves costs.
- **Authentication server**—NMS software to implement AAA services for the client. Currently, the H3C implementation of MACsec does not have extra requirements for the authentication server. A traditional authentication server suffices.

Figure 6 illustrates how MACsec operates in client-oriented mode.

Figure 6 MACsec interactive process in client-oriented mode



The following shows the MACsec process:

1. After the client passes 802.1X authentication, the RADIUS server distributes the generated master session key (MSK) to the client and the access device through the 802.1X interactive process. After receiving the MSK, the client and the access device each calculate their own connectivity association key (CAK).

   The CAK is a basic key, from which MACsec derives all the other keys. The CAK has a long TTL and will not be frequently updated.

IMPORTANT:

The identity authentication process is the same as the 802.1X authentication process. To support MACsec deployment, 802.1X must use an authentication method that can generate MSKs, such as PEAP and EAP-TLS.

2. The client and the access device use the CAKs to exchange EAPOL-MKA packets.

   The client and the access device exchange the MACsec capability and required parameters for session establishment. The parameters include MKA key server priority and MACsec desire.

   During the negotiation process, the access device automatically becomes the key server. The key server generates a security association key (SAK) from the CAK for packet encryption. It then encrypts the SAK by using another key derived from the CAK and distributes the encrypted SAK to the client. SAK encryption prevents the SAK from being intercepted in plain text.

The client obtains the SAK after decryption. For the purpose of security, the data protected by each SAK is subject to an upper limit. When the upper limit is exceeded, the SAK will be refreshed. For example, if small-sized packets are sent on a 10-Gbps link, an SAK rekey occurs about every 5 minutes.

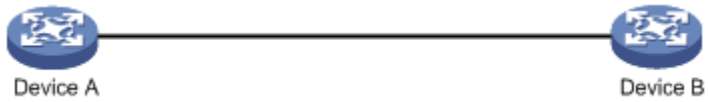
3. After the session negotiation is complete, the client and the access device use the SAK to encrypt packets and transmit the encrypted packets in secure channels. After receiving an encrypted packet, the client or the access device uses the same SAK to decrypt the packet.
4. When the access device receives a logoff request from the client, it immediately removes the associated secure session from the port. The remove operation prevents an unauthorized client from using the secure session established by the previous authorized client to access the network.

   The MKA protocol also defines a session keepalive timer. If one participant does not receive any MKA packets from the peer after the timer expires, the participant removes the established secure session. The keepalive time is 6 seconds.

Device-oriented MACsec

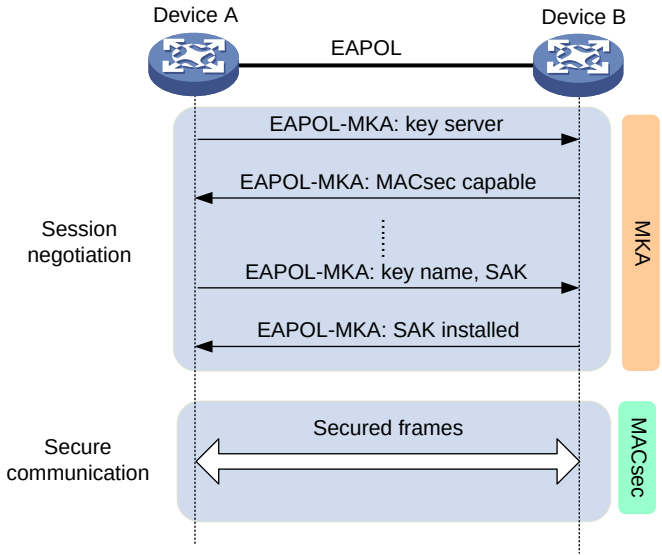
As shown in Figure 7, MACsec secures data transmission between devices. In this mode, the devices do not perform identity authentication, and the same preshared key must be configured on the MACsec ports that connect the devices for key negotiation and packet encryption.

Figure 7 Device-oriented mode



As shown in Figure 8, the devices use the configured preshared keys to start the session negotiation.

Figure 8 MACsec interactive process in device-oriented mode



The following shows the MACsec process:

1. The devices each use the configured preshared key to calculate a CAK to exchange EAPOL-MKA packets with each other.

   They exchange the MACsec capability and required parameters for session establishment. The parameters include MKA key server priority and MACsec desire.

During the negotiation process, the port with higher MKA key server priority becomes the key server. The key server derives an SAK from the CAK and distributes the SAK in encrypted form to the peer.

2. The devices use the same SAK to encrypt packets and send and receive the encrypted packets in secure channels.
3. When a device receives a logoff request from the peer, it immediately deletes the associated secure session.

   If one participant does not receive any MKA packets from the peer after the session keepalive timer expires, the participant removes the established secure session. The keepalive time is 6 seconds.

MACsec-capable H3C products

H3C offers a comprehensive portfolio of MACsec-capable products, from clients to switches that can be deployed at the access, distribution, or core layer. With these products, you can deploy an integrative MACsec solution that covers the network.

Table 1 MACsec-capable H3C products

Deployment location	Products
Core layer	S10500 switch series
Distribution layer	S7500E switch series S6800 switch series
Access layer	S5800EI switch series S5560S-EI switch series S5130S-HI switch series
Client	iNode client

Application scenarios

Deploy client-oriented MACsec, device-oriented MACsec, or both in a network depending on the network security condition and the service confidentiality requirements. For networks that require high confidentiality, deploy both client-oriented and device-oriented MACsec over the entire network.

As a best practice, use MACsec-capable clients that run up-to-date software and network devices that are built on MACsec-capable hardware. For devices that support removable cards, you can install MACsec-capable cards or replace the old cards with MACsec-capable new cards.

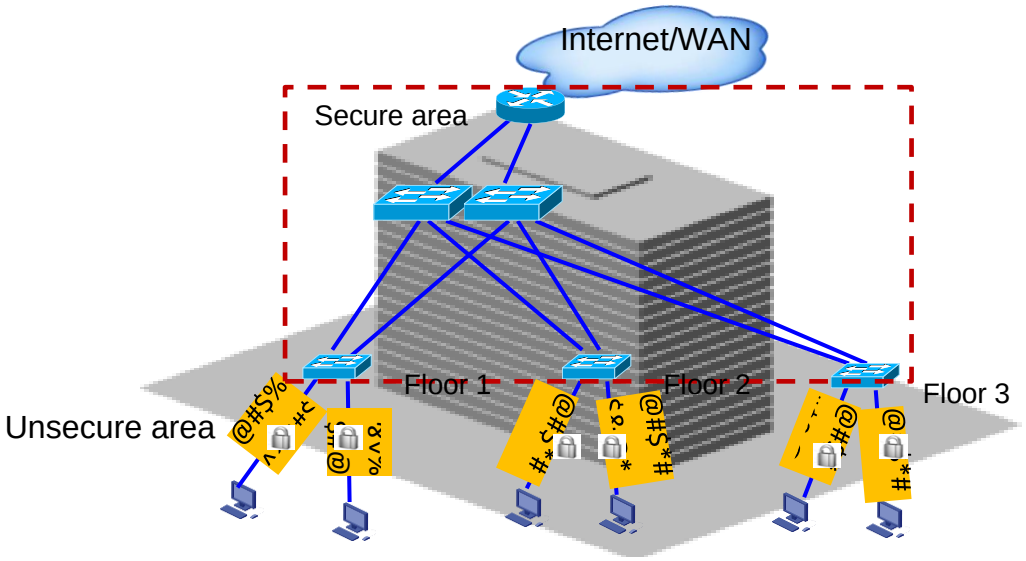
Client-oriented MACsec deployment

Client-oriented MACsec can be applied to networks where clients have to traverse unsecure public areas to access the network devices in the secure area. In such a network, even if the clients pass authentication, information might still be intercepted by unauthorized devices, causing information disclosure.

Client-oriented MACsec can secure communication between external clients and the internal network devices.

The iNode clients and S5130S-HI switches are applicable to client-oriented MACsec.

Figure 9 Network diagram



Device-oriented MACsec deployment

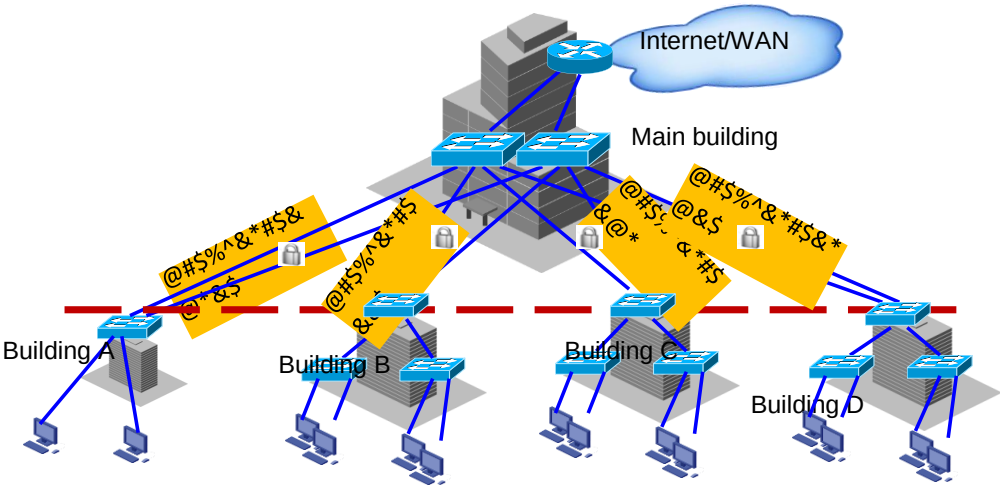
Device-oriented MACsec can be applied to campus or enterprise networks where multiple buildings are interconnected. The lines between the buildings are exposed in public areas and easy to be intercepted.

Device-oriented MACsec can secure communications between the access layer and the distribution layer or between the distribution layer and the core layer.

The following H3C products are applicable to this scenario:

- Access layer switches: S5130S-HI, S5560S-EI, and S5800EI.
- Distribution layer switches: S7500E and S6800.
- Core layer switches: S10500.

Figure 10 Network diagram

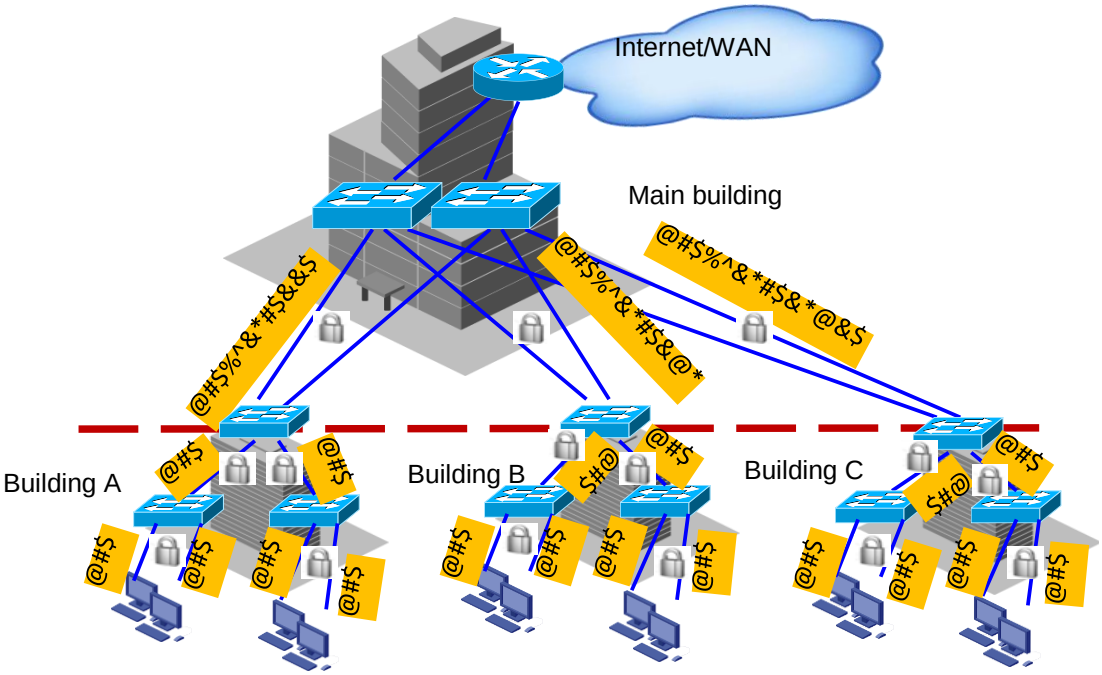


Network-wide integrative MACsec solution

The combination of client-oriented and device-oriented MACsec can be applied to enterprise networks that require high internal security or have security issues because cables traverse many public areas. The combination can secure communication from terminals till the core layer devices.

All MACsec-capable H3C products are applicable to this scenario.

Figure 11 Network diagram



New H3C Technologies Co., Limited

Beijing base
8 GuangShun South Street, Chaoyang District,Beijing
Zip: 100102

Hangzhou base
466 Changhe Road, Binjiang District, Hangzhou, Zhejiang Province 310052 P.R.China
Zip: 310052
Tel: +86-571-86760000
Fax: +86-571-86760001

http://www.h3c.com