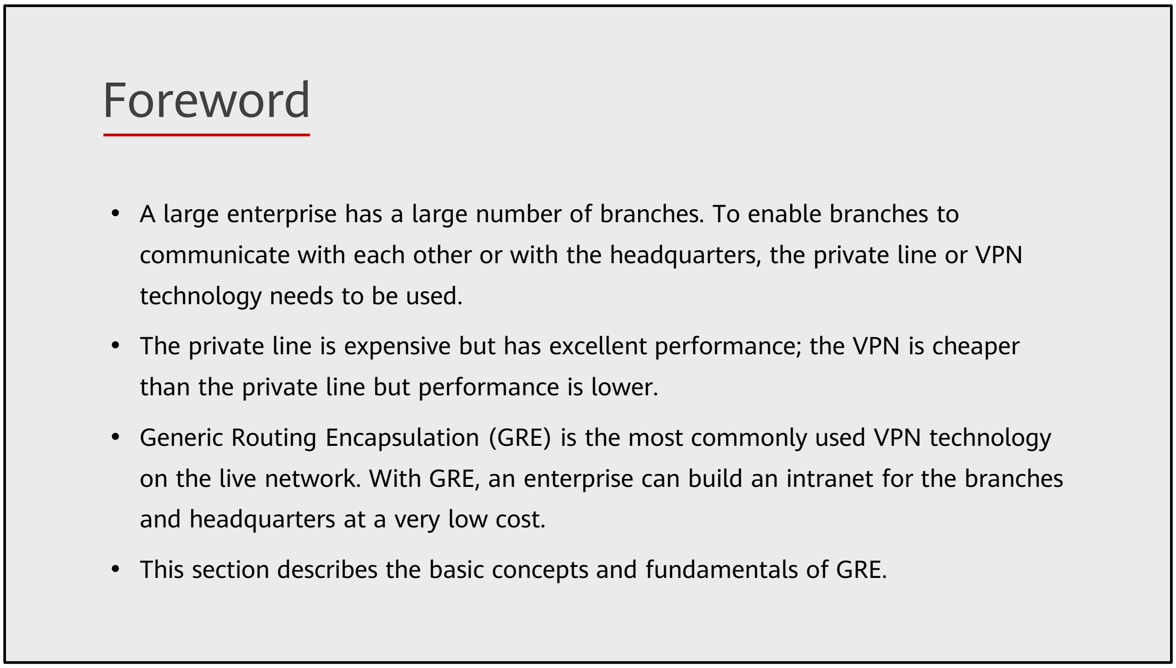
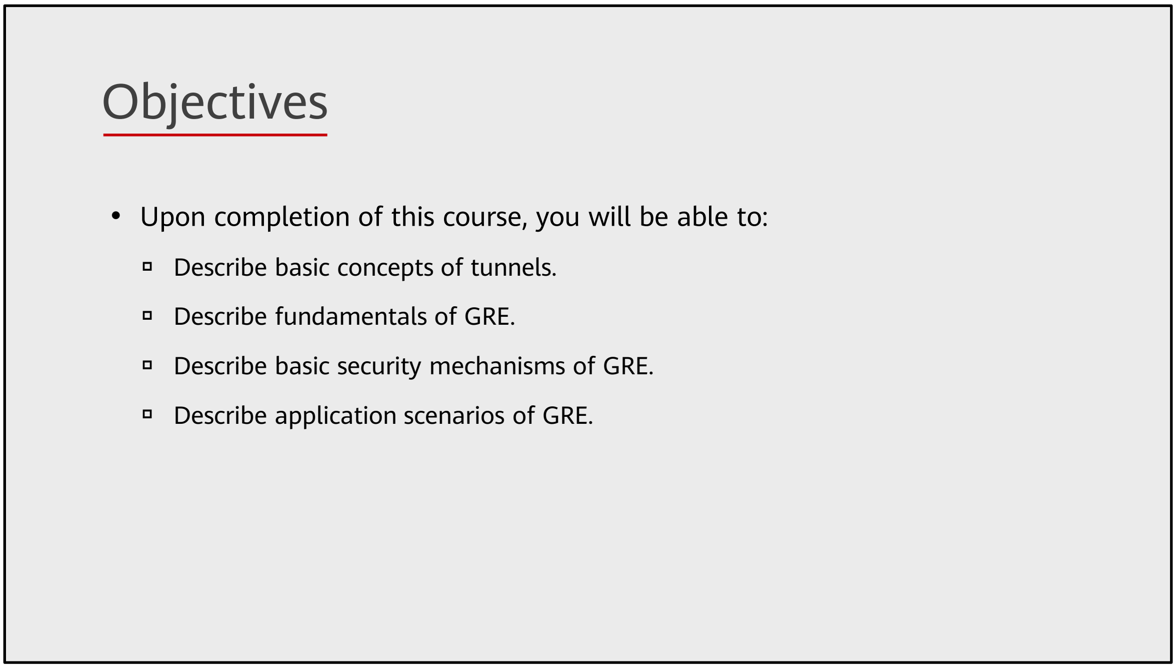
GRE Technology



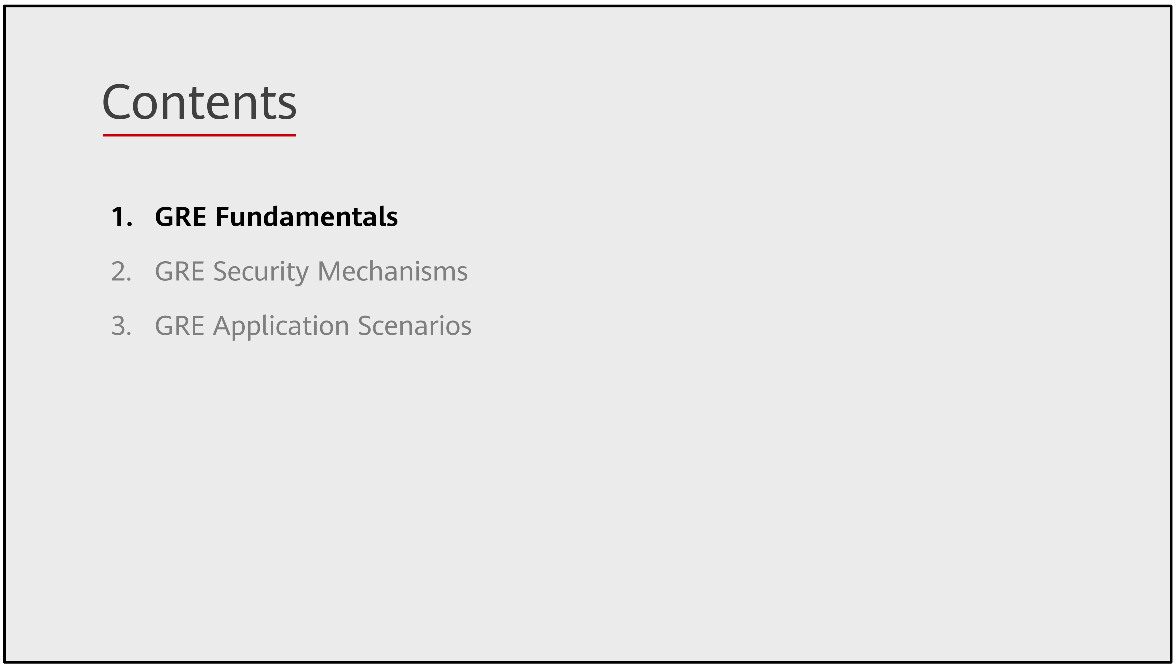
Foreword

- A large enterprise has a large number of branches. To enable branches to communicate with each other or with the headquarters, the private line or VPN technology needs to be used.
- The private line is expensive but has excellent performance; the VPN is cheaper than the private line but performance is lower.
- Generic Routing Encapsulation (GRE) is the most commonly used VPN technology on the live network. With GRE, an enterprise can build an intranet for the branches and headquarters at a very low cost.
- This section describes the basic concepts and fundamentals of GRE.



Objectives

- Upon completion of this course, you will be able to:
  - Describe basic concepts of tunnels.
  - Describe fundamentals of GRE.
  - Describe basic security mechanisms of GRE.
  - Describe application scenarios of GRE.

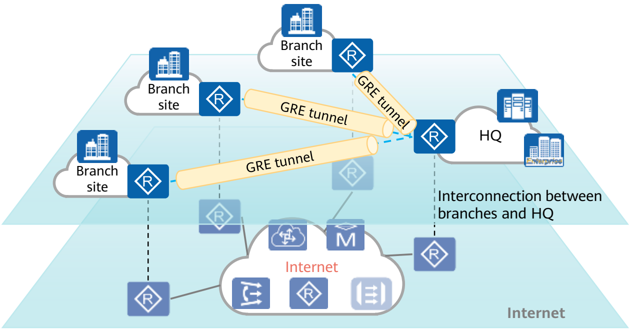


Contents

1. **GRE Fundamentals**
2. GRE Security Mechanisms
3. GRE Application Scenarios

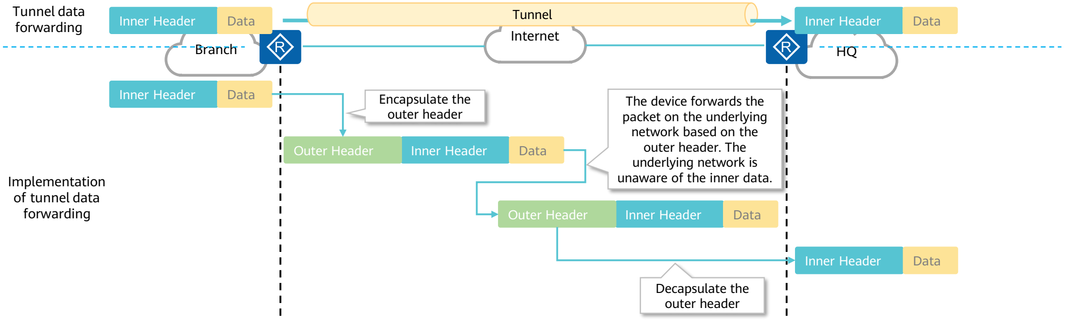
GRE Background

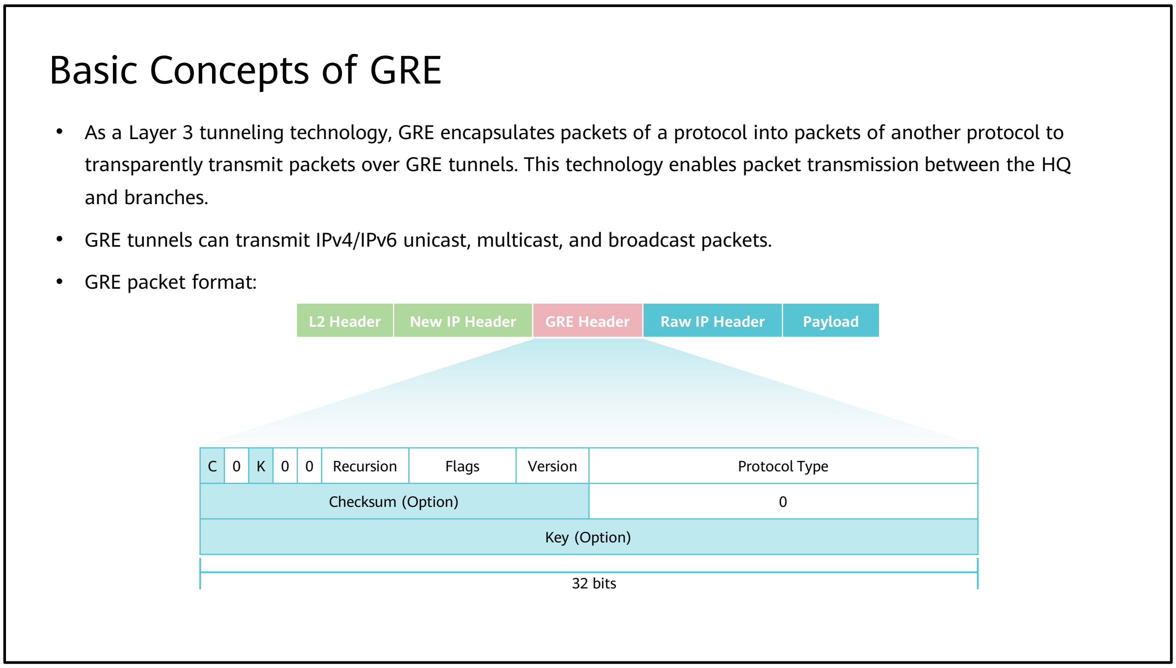
- With the development of enterprises, more and more enterprises need to communicate between branches and headquarters. Private lines (such as MPLS and SDH/MSTP private lines) need to be leased for communication between the headquarters and branches. However, private lines are expensive. For small- and medium-sized enterprises or cross-border companies, the cost is high.
- With the development of the Internet, the Internet has sufficient bandwidth and coverage. Therefore, it is more feasible to implement communication on the intranet between the headquarters and branches through the Internet. GRE is proposed in this background.
- Through GRE tunnels, the enterprise network can be established between the branch and headquarters based on the Internet.



Introduction to Tunneling Technologies

- GRE is one of tunneling technologies. A tunnel is similar to a bridge. Forwarding channels are established on the underlying network (for example, Internet). Users can establish a tunnel network by themselves without the intervention of the underlying network provider (for example, an ISP).
- There are many tunneling technologies, such as MPLS, GRE, Layer 2 Tunneling Protocol (L2TP), and Virtual Extensible LAN (VXLAN). The following figure shows the implementation of tunnel data forwarding.


Tunnel data forwarding
Inner Header
Data
Tunnel
Internet
Branch
HQ
Inner Header
Data
Implementation of tunnel data forwarding
Inner Header
Data
Encapsulate the outer header
Outer Header
Inner Header
Data
The device forwards the packet on the underlying network based on the outer header. The underlying network is unaware of the inner data.
Outer Header
Inner Header
Data
Inner Header
Data
Decapsulate the outer header



Basic Concepts of GRE

- As a Layer 3 tunneling technology, GRE encapsulates packets of a protocol into packets of another protocol to transparently transmit packets over GRE tunnels. This technology enables packet transmission between the HQ and branches.
- GRE tunnels can transmit IPv4/IPv6 unicast, multicast, and broadcast packets.
- GRE packet format:

L2 Header	New IP Header	GRE Header	Raw IP Header	Payload

C	0	K	0	0	Recursion	Flags	Version	Protocol Type
Checksum (Option)								0
Key (Option)								

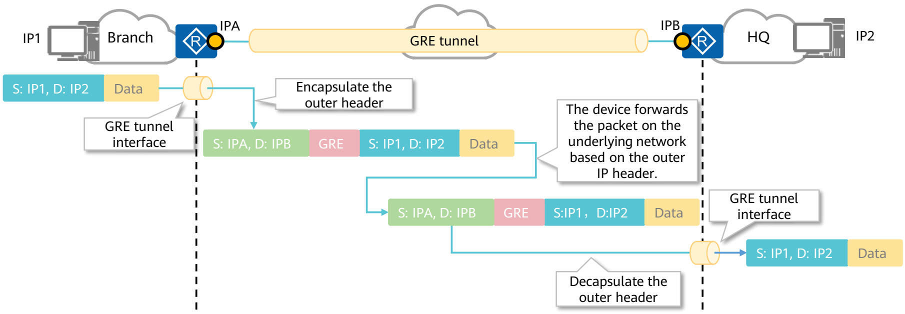
32 bits

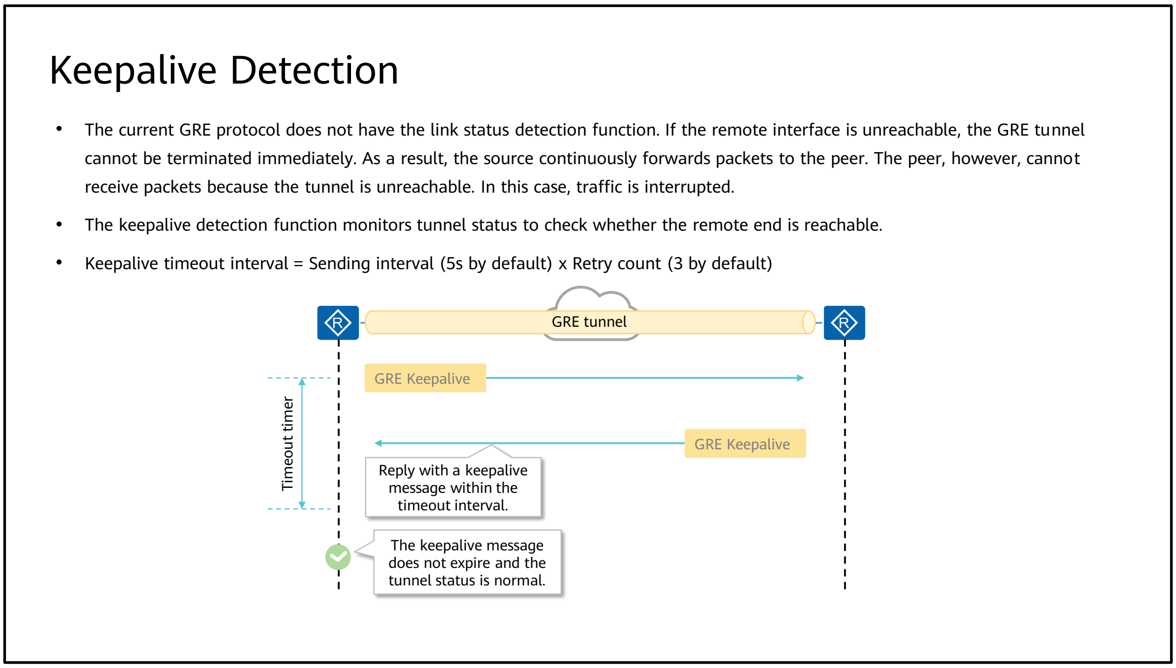
- Description of fields in a GRE header:

Field	Description
C	Checksum verification bit. The value 1 indicates that the Checksum field is inserted into the GRE header. The value 0 indicates that the GRE header does not contain the checksum field.
K	Key bit. The value 1 indicates that the Key field is inserted into the GRE header. The value 0 indicates that the GRE header does not contain the keyword field.
Recursion	Number of layers where GRE packets are encapsulated. The value of this field is increased by 1 after one GRE encapsulation is complete. If the number of encapsulation layers is greater than 3, the packet is discarded. This field is used to prevent packets from being encapsulated continuously.
Flags	Reserved field. The value must be 0.
Version	Version. The value must be 0.
Protocol Type	Type of the passenger protocol. A common passenger protocol is the IPv4 protocol, with the value of 0800. The protocol number of Ethernet over GRE is 0x6558.
Checksum	Checksum of the GRE header and the payload.
Key	Key used to authenticate the packet at the receive end.

GRE Fundamentals

- The GRE tunnel is a Layer 3 tunnel and mainly carries IPv4/IPv6 packets. GRE encapsulates the outer IP header so that data can be transmitted on the public network. In this way, enterprise branches and the headquarters can communicate with each other.
- The following figure shows the process of forwarding packets over a GRE tunnel.



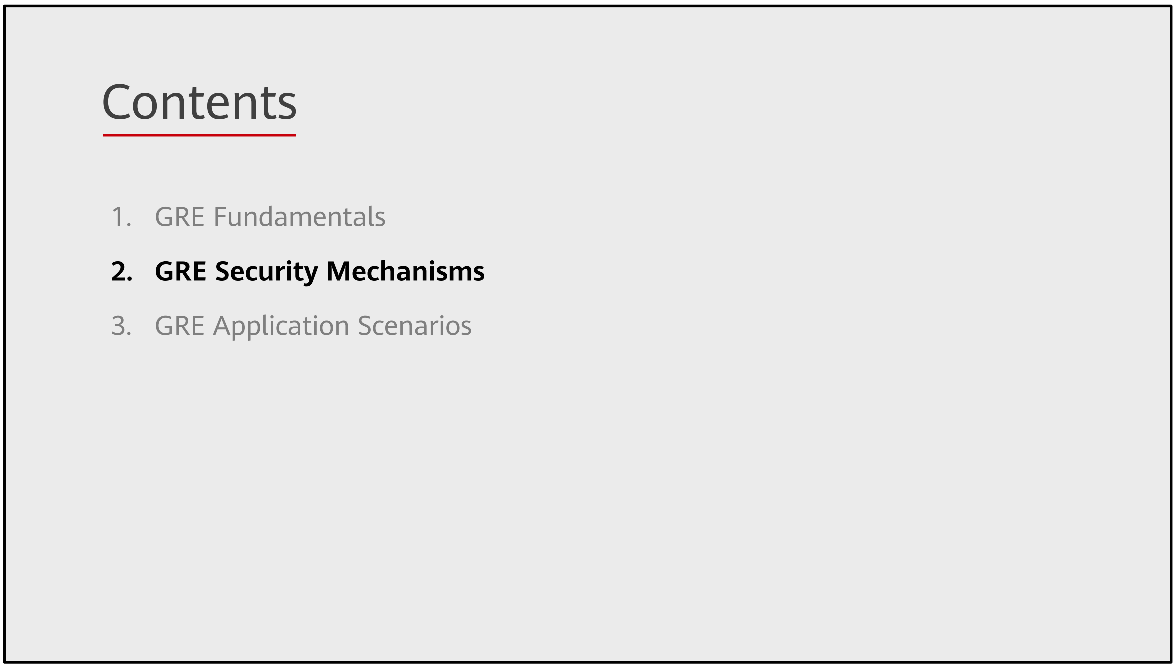


Keepalive Detection

- The current GRE protocol does not have the link status detection function. If the remote interface is unreachable, the GRE tunnel cannot be terminated immediately. As a result, the source continuously forwards packets to the peer. The peer, however, cannot receive packets because the tunnel is unreachable. In this case, traffic is interrupted.
- The keepalive detection function monitors tunnel status to check whether the remote end is reachable.
- Keepalive timeout interval = Sending interval (5s by default) x Retry count (3 by default)

GRE tunnel
GRE Keepalive
GRE Keepalive
Timeout timer
Reply with a keepalive message within the timeout interval.
The keepalive message does not expire and the tunnel status is normal.

- Keepalive detection functions as follows:
  - After being enabled on the source end of a GRE tunnel, the source end starts a timer to periodically send and count keepalive messages. The number of sent keepalive messages increases by one each time a keepalive message is sent.
  - The destination end sends a response message to the source end each time it receives a keepalive message from the source end.
  - If the source end receives a reply packet before the counter value reaches the preset value, it considers the remote end reachable. If the source end does not receive any response message before the counter reaches the preset value, specifically, the retry count, the source end considers the peer end unreachable and resets the counter. Then, the source end terminates the tunnel connection. In this case, the source interface still sends Keepalive messages to the remote interface. When the remote interface becomes Up, the source interface becomes Up and sets up a tunnel with the remote interface.



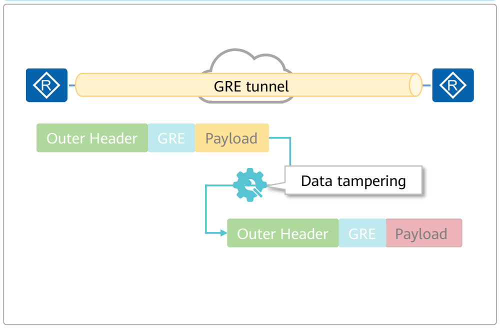
Contents

1. GRE Fundamentals
2. **GRE Security Mechanisms**
3. GRE Application Scenarios

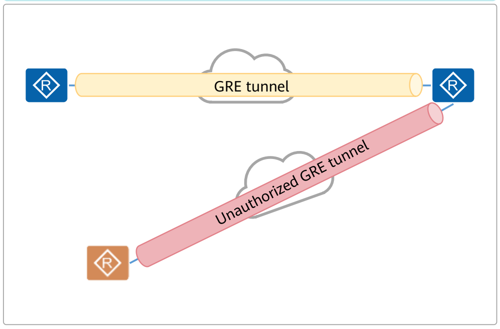
Security Threats to GRE Tunnels

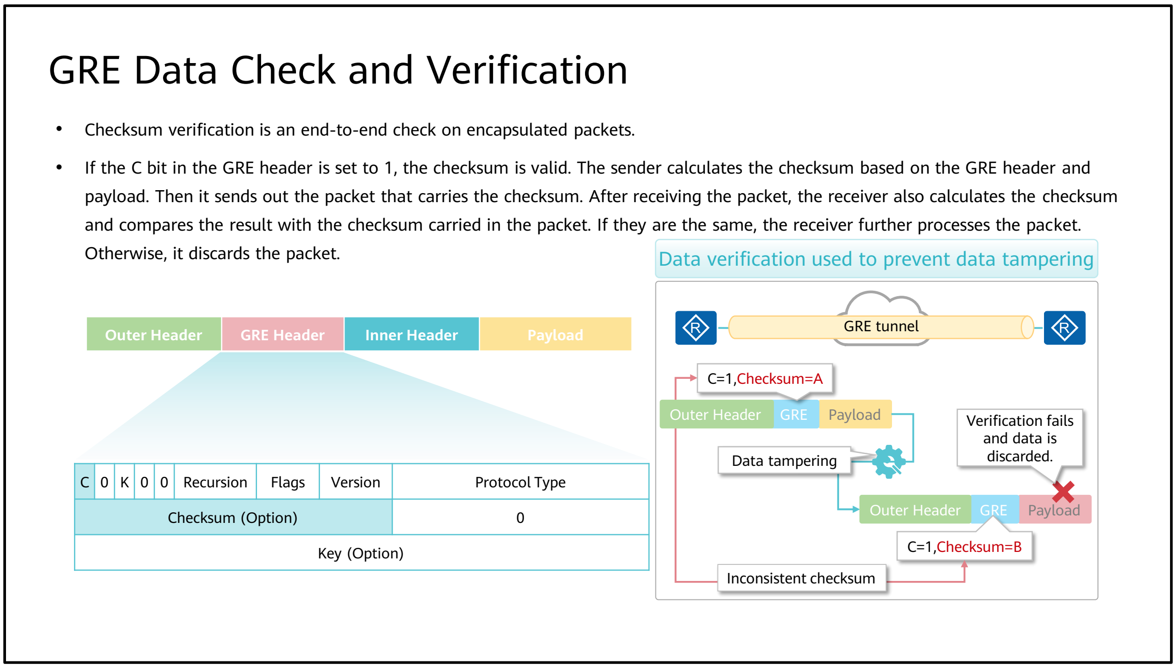
- GRE tunnels are used to transmit data between branches and the HQ. Data is not encrypted and may be tampered with.
- There are potential risks in GRE tunnel establishment. Attackers can forge IP addresses to establish GRE tunnels between authorized and unauthorized devices.

GRE data tampering



Unauthorized GRE tunnel setup





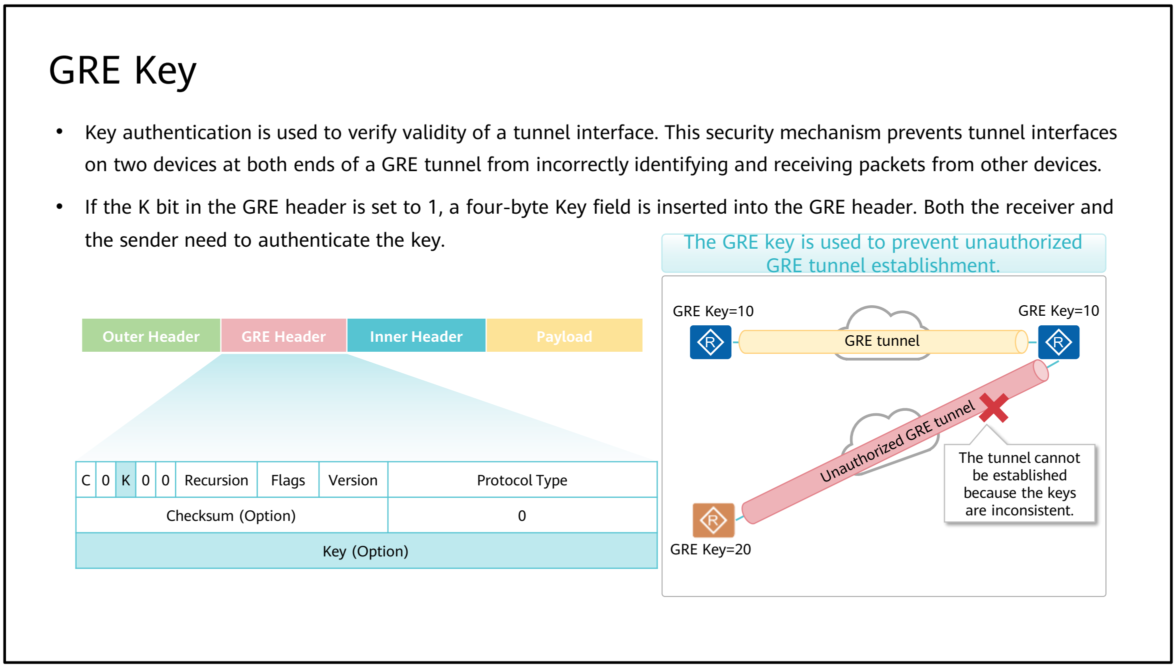
GRE Data Check and Verification

- Checksum verification is an end-to-end check on encapsulated packets.
- If the C bit in the GRE header is set to 1, the checksum is valid. The sender calculates the checksum based on the GRE header and payload. Then it sends out the packet that carries the checksum. After receiving the packet, the receiver also calculates the checksum and compares the result with the checksum carried in the packet. If they are the same, the receiver further processes the packet. Otherwise, it discards the packet.

C	0	K	0	0	Recursion	Flags	Version	Protocol Type
Checksum (Option)								0
Key (Option)								

Data verification used to prevent data tampering

- You can enable or disable checksum verification on both ends of a tunnel in actual applications. If checksum verification is enabled on the local end and disabled on the remote end, the local end does not check checksum values of received packets, but checks checksum values of packets to be sent. If checksum verification is disabled on the local end and enabled on the remote end, the local end checks checksum values of received packets, but does not check checksum values of packets to be sent.



GRE Key

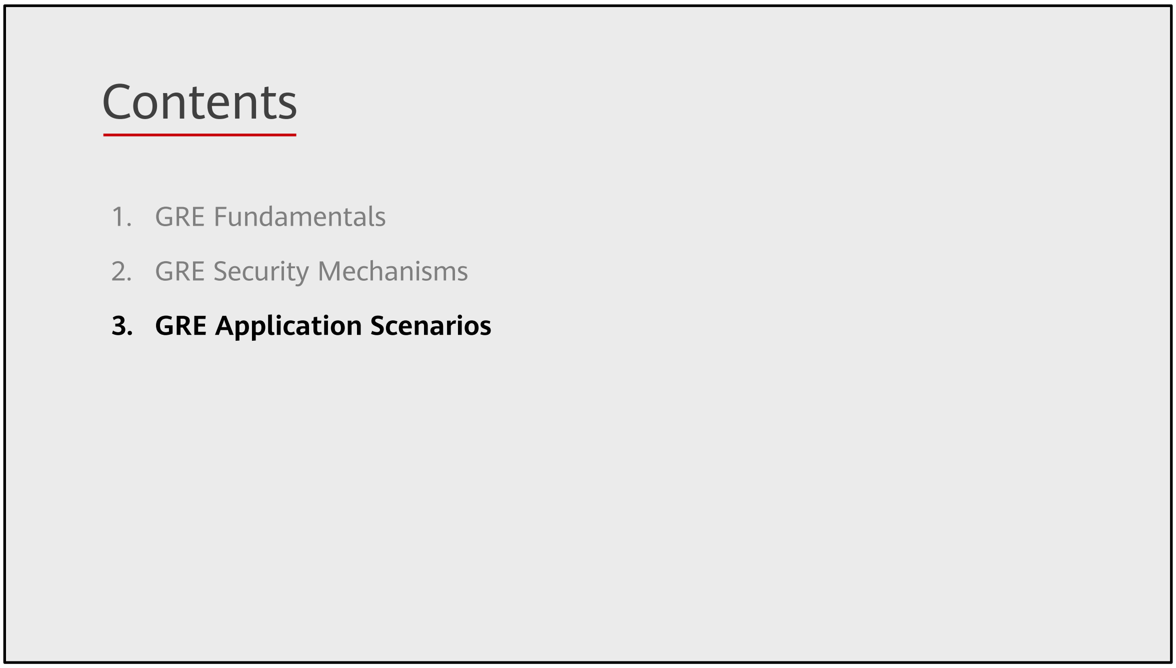
- Key authentication is used to verify validity of a tunnel interface. This security mechanism prevents tunnel interfaces on two devices at both ends of a GRE tunnel from incorrectly identifying and receiving packets from other devices.
- If the K bit in the GRE header is set to 1, a four-byte Key field is inserted into the GRE header. Both the receiver and the sender need to authenticate the key.

C	0	K	0	0	Recursion	Flags	Version	Protocol Type
Checksum (Option)								0
Key (Option)								

The GRE key is used to prevent unauthorized GRE tunnel establishment.

GRE Key=10
GRE Key=10
GRE tunnel
Unauthorized GRE tunnel
GRE Key=20
The tunnel cannot be established because the keys are inconsistent.

- This field identifies traffic in a tunnel. Packets of the same traffic use the same key. During packet decapsulation, GRE identifies data packets of the same traffic based on the key. Packets will pass verification only when the two ends of the tunnel use the same Key field. If packets fail the verification, they will be discarded. Successful authentication requires that both ends are either configured with the same Key field or not configured with the Key field.

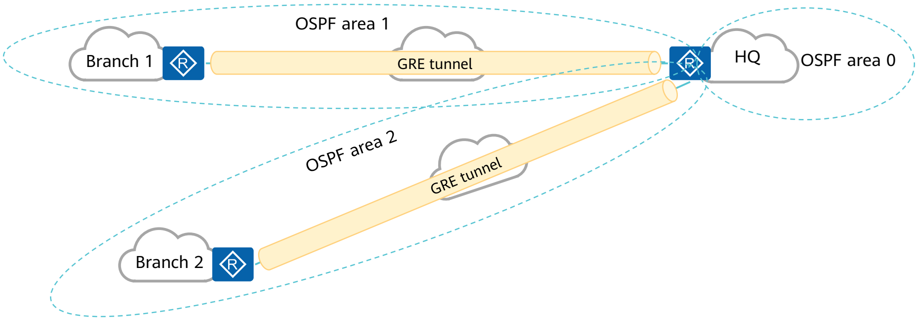


Contents

1. GRE Fundamentals
2. GRE Security Mechanisms
3. **GRE Application Scenarios**

Using GRE to Build an Intranet Between the HQ and Branches

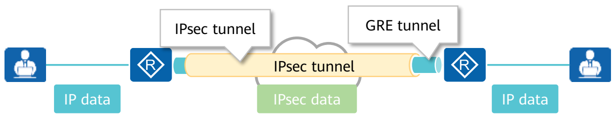
- GRE tunnels can transmit IPv4/IPv6 unicast, multicast, and broadcast packets. Dynamic routing neighbor relationships can be configured between branches and the HQ through GRE tunnels, facilitating intranet interconnection between branches and the HQ.

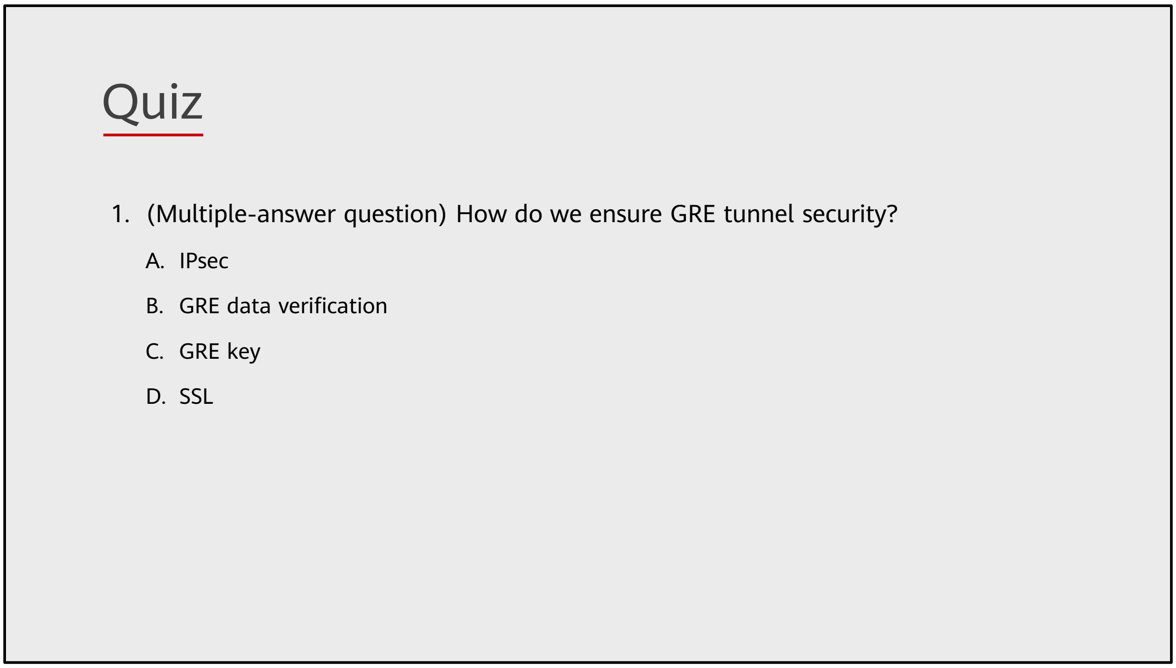


GRE Over IPsec

- GRE is simple. However, data is transmitted over a GRE tunnel in cleartext and can be easily obtained. On the live network, GRE is usually used together with IPsec. The GRE technology is used to establish the internal network connection between the branch and headquarters, and the IPsec technology is used to encrypt GRE tunnel packets.

GRE over IPsec data encapsulation

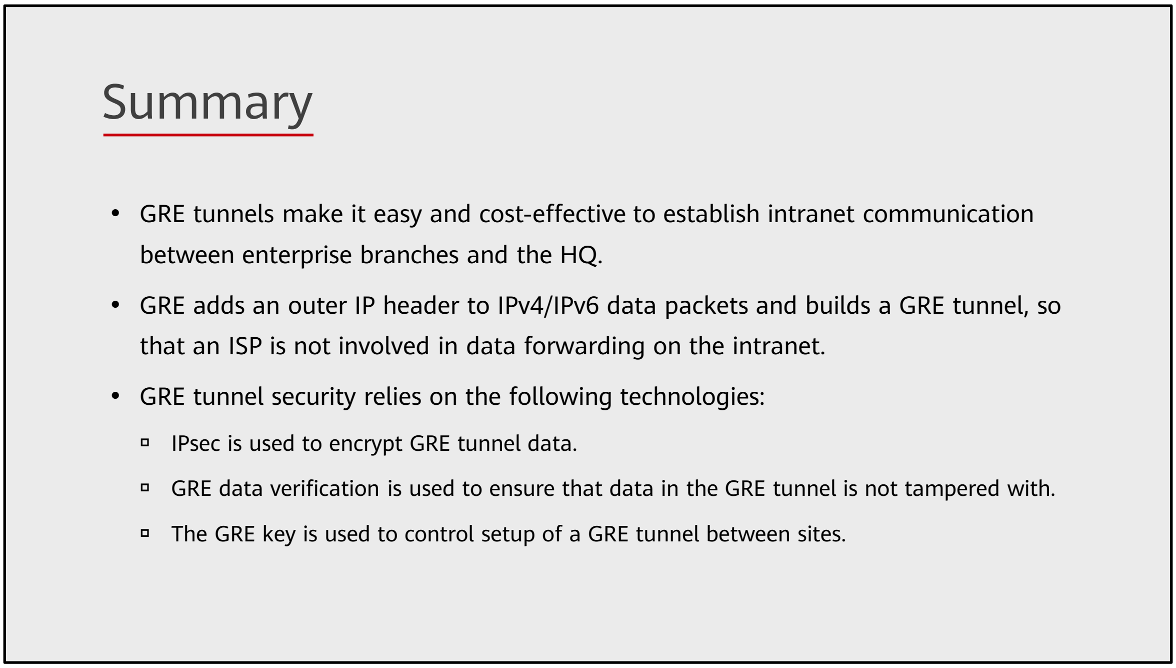




Quiz

1. (Multiple-answer question) How do we ensure GRE tunnel security?
   A. IPsec
   B. GRE data verification
   C. GRE key
   D. SSL

- 1. ABC



Summary

- GRE tunnels make it easy and cost-effective to establish intranet communication between enterprise branches and the HQ.
- GRE adds an outer IP header to IPv4/IPv6 data packets and builds a GRE tunnel, so that an ISP is not involved in data forwarding on the intranet.
- GRE tunnel security relies on the following technologies:
  - IPsec is used to encrypt GRE tunnel data.
  - GRE data verification is used to ensure that data in the GRE tunnel is not tampered with.
  - The GRE key is used to control setup of a GRE tunnel between sites.