Kyland Technology Co., Ltd.

White Paper

GOOSE-over-IP-Tunnel Technology

GOOSE-over-IP-Tunnel Technology

Key words: GOOSE, IP, GRE, Tunnel, Encapsulation, Decapsulation

Abstract: The GOOSE-over-IP-Tunnel technology capacitates GOOSE messages to travel through IP network and be transmitted (routing) to the other side of the IP network. This paper describes the basic mechanism and typical applications of GOOSE-over-IP-Tunnel technology.

Acronyms:

Acronym	Full Spelling
GOOSE	Generic Object Oriented Substation Event
GRE	Generic Routing Encapsulation
-	Tunnel/Tunneling
IP	Internet Protocol
PDU	Protocol Data Unit
LAN	Local Area Network
VLAN	Virtual LAN

Contents

1. Overview

GOOSE (Generic Object Oriented Substation Event) is defined in IEC61850, such as warning and tripping. It is a definition for the application layer. In the substation communication model, IEC61850 specifies the mappings of GOOSE to ISO/IEC8802.3. As IEC61850-8-1 defines, “The T-DATA destination address for a GOOSE message shall contain a multicast MAC address. The T-DATA source address for a GOOSE message shall contain a unicast MAC address.” (For details, see chapter 6.3.3 of IEC61850-8-1).

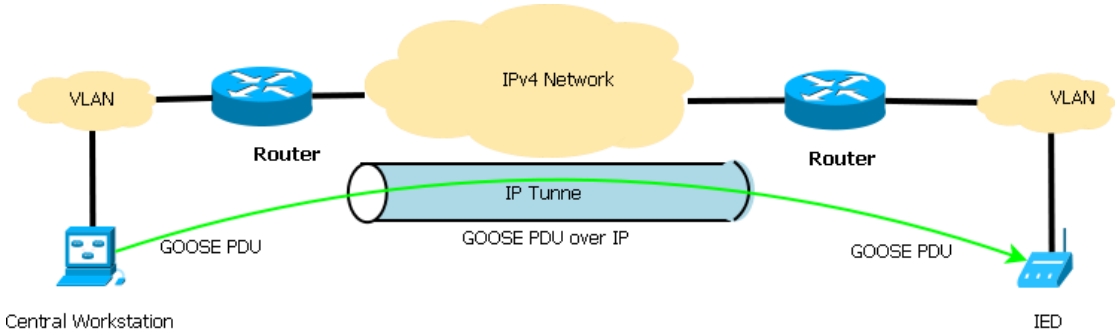
The mapping feature is that layer 2 multicast technologies are used to transmit GOOSE frames without passing through network layer. The maximum transmission domain is the source broadcast domain (LAN/VLAN) that a GOOSE frame belongs to.

IP tunneling technology can encapsulate a protocol message into an IP packet and forms routing-available format for forwarding in IP network.

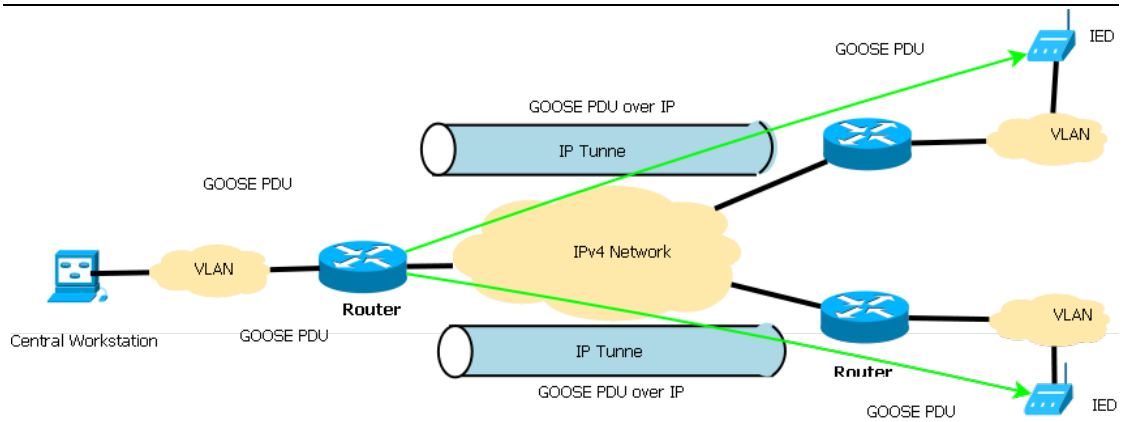
The combination of GOOSE PDU and IP tunneling technology breaks the restriction that GOOSE PDU can only be forwarded in LAN/VLAN, and delivers the designated GOOSE PDU via IP network to another LAN/VLAN that the GOOSE PDU cannot reach directly.

1.1 Background

In substation application, the central workstation may need to communicate with remote substation(s) through an IPv4 network. In such circumstances, the GOOSE messages from central workstation need to be carried by an IP network in a certain way and are transparently transmitted to remote substation(s), and then continue forwarding in LAN of remote substation(s), thus to achieve the purpose of controlling IEDs in remote substation(s).



(a) 1:1 Transmission



(b) 1:N Transmission

Figure 1: GOOSE-over-IP-Tunnel Application Network

(a) A GOOSE message from central workstation is delivered to one substation on the other side of IP network.

(b) A GOOSE message from central workstation is delivered to multiple substations across IP network.

1.2 Technology Advantages

1) You do not need to directly locate central workstation in substation, but connect central workstation to LAN/VLAN in the destination substation through IP network, so as to facilitate deployment and management
2) In multiple substations involved applications, the technology reduces the number of central workstations and achieves centralized management.
3) It offers a solution of sending one GOOSE PDU to multiple substations' LAN/VLANs through tunnels.
4) It supports VLAN remark when a VLAN message of GOOSE PDU from central workstation arrives at the substation on the other side of tunnel.

2. Technology Implementation

2.1Concepts

2.1.1 GOOSE

IEC61850 standard defines two types of abstract models: SAV (Sampled Analogue Value) transmission model and GOOSE (Generic Object Oriented Substation Event) model. SAV model is applied in SAV transmission and related services, but GOOSE model provides a fast transmission mechanism for substation events (such as command and warning) and it is used for tripping, fault recorder startup, and so on. The transmission of SAV and GOOSE messages both adopts publisher/subscriber communication structure. The mapping of SAV and GOOSE models to ISO/IEC8802.3 is as follows: application layer defines PDU (Protocol Data Unit); after encoded in presentation layer, they are directly mapped to data link layer and physical layer without passing through TCP/IP protocol stack. This paper focuses on the GOOSE model. IEC61850-8-1 presents and stipulates

GOOSE-ISO/IEC8802.3 mapping.

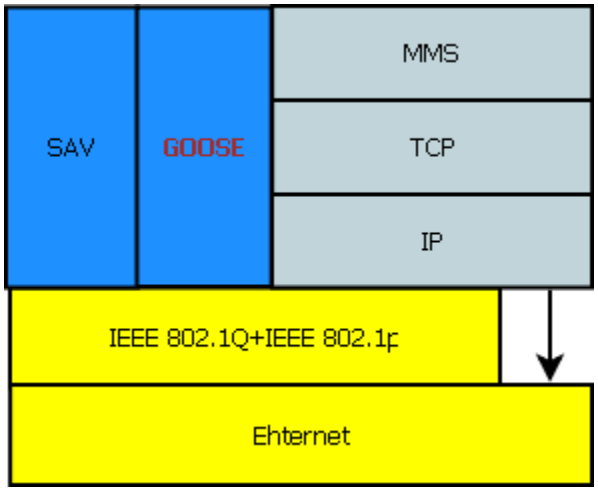


Figure 2: GOOSE-ISO/IEC8802.3 Mapping

2.1.2 Tunnel

Tunneling technology is a way of data transmission between networks by using network infrastructure. Data (or load) that is transmitted by tunnel can be different protocols' frames or packets. Tunneling protocol re-encapsulates other protocol's frames or packets, and then delivers them by tunnel. Both ends of the tunnel can perform data message encapsulation and decapsulation. Tunneling technology is the entire process of data encapsulation, delivery, and decapsulation.

Tunnel is a virtual connection with virtual interfaces at both ends of a connection. The interfaces are called Tunnel Interface. Tunnel interface provides parameters for data encapsulation and decapsulation, as well as tunnel identifiers (Tunnel ID) in tunnel application. The end for data encapsulation is called Tunnel Start and the other end that supports data decapsulation is called Tunnel End. Tunnel Start and Tunnel End are relative concepts and subject to data transmission direction. In a bi-directional transmission tunnel, both ends are Start and End to each other.

- **IP tunnel**

When IP protocol serves as tunneling protocol to encapsulate other protocols, the tunnel formed is IP tunnel. By combining IP tunnel and other IP network technologies (such as routing and security), we have:

- Routing-unavailable protocol message travels through routing-available IP network, such as the transparent transmission of GOOSE PDU in IP network
- Private information passes through public network
- Private LAN communicates with another private network that is in the same organization across public network
- Connect protocol islands, such as IPv6-over-IPv4 tunnel

- **GRE tunnel**

GRE (Generic Routing Encapsulation) tunnel defines a generic encapsulation format for routing-available tunnel. It divides the entire tunnel encapsulation

into three layers: Delivery protocol, Encapsulation protocol, and Passenger protocol, as shown in Figure 3.

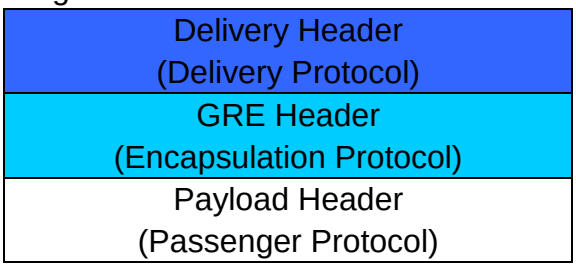


Figure 3: GRE Encapsulation

The relationship among them: Passenger protocol is encapsulated to a message according to the format of Encapsulation protocol, and then the message becomes the data of Delivery protocol, that is, a Delivery protocol message. Then the message is transmitted in tunnel. When arriving at the Tunnel End, the message is decapsulated according to the format of Encapsulation protocol, and then Passenger protocol is released.

- **GRE-IP tunnel**

When IP protocol serves as Delivery protocol and encapsulates Passenger protocol according to GRE encapsulation format. The tunnel for data delivery is called GRE-IP tunnel.

2.1.3 GOOSE-over-GRE-IP-Tunnel

In tunnel encapsulation, if GOOSE message is used as passenger protocol message, GRE encapsulation as encapsulation protocol, and IP protocol as delivery protocol, it can form a GRE-IP tunnel for GOOSE message transmission in IP network and the tunnel is called GOOSE-over-GRE-IP tunnel. In this paper, we shorten it to GOOSE-over-IP tunnel or GOOSE-Tunnel when no ambiguity occurs.

Figure 4: GOOSE-over-GRE-IP Encapsulation

In order to realize GOOSE message's 1:N tunnel mode, the destination IP address of GOOSE-Tunnel can be set to IP multicast address other than IP unicast address.

2.1.4 Binding of GOOSE Message and Tunnel Start Interface

On GOOSE Tunnel Start, in order to specify GOOSE stream for tunnel transmission and select the Tunnel start interface for GOOSE stream, it is needed to set the binding relation between GOOSE stream and Tunnel start interface and form a GOOSE-Tunnel-Binding-List. This list is configurable.

- **Binding mode**

The binding of GOOSE stream and Tunnel start interface can be in either of the following modes: Tunnel-only mode and Normal mode.

Tunnel-Only mode: The qualified GOOSE stream is only forwarded to the bound Tunnel start interface.

Normal mode: The qualified GOOSE stream is not only forwarded to the bound Tunnel start interface, but also continues normal forwarding in its source

VLAN.

- **Binding scope**

Global binding (global-based binding): When searching in GOOSE-Tunnel-Binding-List, only the GOOSE MAC address (excluding VLAN) is used to match the entries that do not contain VLAN information in the binding list.

VLAN-based binding: When searching in GOOSE-Tunnel-Binding-List, both GOOSE MAC address and VLAN information are used to conduct accurate matching. If no match is found, global binding is further performed.

2.1.5 VLAN Remark of GOOSE PDU

When GOOSE message reaches GOOSE tunnel termination and completes decapsulation, its VLAN can be remarked according to its IEEE802.1Q VID. VLAN remark is configurable.

If remark succeeds, GOOSE PDU is forwarded to a new VLAN.

If remark fails, it means no remark configuration for this VID. In this case, GOOSE PDU shall be forward to VLAN with the same VID.

2.1.6 Static GOOSE Entry

On GOOSE termination device, the static binding relation between GOOSE PDU and out interface in target VLAN can be configured.

2.1.7 Release Mode of Decapsulated GOOSE PDU

When GOOSE message reaches tunnel termination and the target VLAN is confirmed, the next step is to specify the out interface. There are two modes:

Strict mode: only the GOOSE PDU static binding list is searched. If no match is found, the message is discarded.

Normal mode: The GOOSE PDU static binding list is searched first. If no match is found, the FDB table is searched. If still no match is found, broadcast in target VLAN. In this mode, it can work with the GMRP function.

2.2Message Structure

- **GOOSE-GRE-IP-Tunnel Encapsulated Packet**

In this figure, IP protocol is used as Delivery protocol, GRE as Encapsulation protocol, and GOOSE PDU as Passenger protocol that is encapsulated in GRE. That is the payload of GRE-IP-Tunnel.

- **GOOSE PDU**

The following figure shows the PDU structure in GOOSE-ISO/IEC8802.3 mapping.

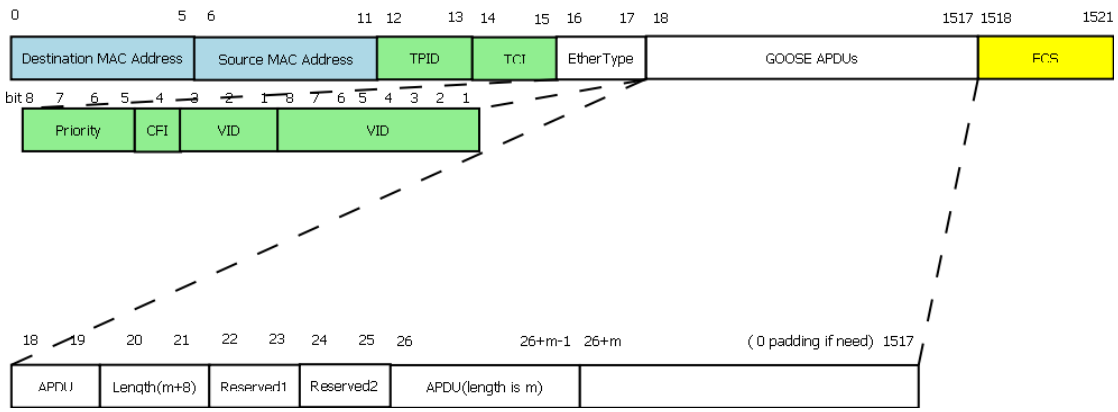


Figure 5: GOOSE PDU Encapsulation

Table 1 lists the descriptions of the fields.

Table 1 Field Explanation

Field		Explanation	Value
Destination MAC address		Destination MAC address	01-0C-CD-01-00-00~ 01-0C-CD-01-01-FF
Source MAC address		Source MAC address	It is set by the manufacturer.
802.1Q	TPID	Indicates the Ethertype assigned to 802.1Q Ethernet encoded frames	0x8100
	Priority	Priority tagging is used to separate time critical and high priority traffic for protection relevant applications from low priority busload.	If priority is not configured, the default value 4 shall be used.
	CFI	If it is set to 1, an Embedded Resource Identification Filed (E-RIF) follows the Length/Type field in the ISO/IEC8802-3 tagged frame. The value shall be 0.	0
	VID (VLAN Identifier)	The use of Virtual LAN support is optional. If this mechanism is used, the VLAN Identifier (VID) shall be set by configuration. If it is not used, it shall be set to 0.	[0,4094]
EtherType		GOOSE PDU Ethertype	0x88B8
APPID		Application Identifier. It is	

	used to select ISO/IEC8802-3 frames containing GOOSE messages and to distinguish the application association.	
Length	Number of octets including the Ethertype PDU header starting at APPID, and the length of the APDU (Application Protocol Data Unit). Therefore, the value of Length shall be 8+m, where m is the length of the APDU and m is less than 1492.	m+8
Reserved1 & Reserved2	They are reserved for future standardized applications.	It shall be set to 0, the default value.
APDU	Application Protocol Data Unit Octets	It is defined in IEC61850-8-1 Annex A.

- **GRE Header**

The format of GRE header is as follows (refer to REC2784 and RFC2890).

```
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|C| |K|S| Reserved0       | Ver |         Protocol Type         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Checksum (optional)      |       Reserved1 (Optional)    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Key (optional)                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Sequence Number (Optional)                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 6: GRE Header Encapsulation

Table 2 lists the descriptions of the fields.

Table 2 Field Explanation

Field	Definition	Value
C	The Checksum field is present and contains valid information if set.	0

Field	Definition	Value
K	The Key field contains a four octet number which was inserted by the encapsulator. The actual method by which this Key is obtained is beyond the scope of the document. The Key field is intended to be used for identifying an individual traffic flow within a tunnel. For example, packets may need to be routed based on context information not present in the encapsulated data. The Key field provides this context and defines a logical traffic flow between encapsulator and decapsulator. Packets belonging to a traffic flow are encapsulated using the same Key value and the decapsulating tunnel endpoint identifies packets belonging to a traffic flow based on the Key Field value.	0
S	The Sequence Number field contains an unsigned 32 bit integer which is inserted by the encapsulator. It may be used by the receiver to establish the order in which packets have been transmitted from the encapsulator to the receiver. The exact algorithms for the generation of the sequence number and the semantics of their reception are outside of the scope of this document.	configurable
Reserved0		0
Ver	Version of GRE	0
Protocol Type	Contains the protocol type of the payload packet. In general, the value will be the Ethernet protocol type field for the packet.	0x88B8
Checksum	Contains the IP (one's complement) checksum of the GRE header and the payload packet.	
Reserved1		0
Key	The Key field contains a four octet number which was inserted by the encapsulator.	
Sequence Number	Contains a number which is inserted by the encapsulator. It may be used by the receiver to establish the order in which packets have been transmitted from the encapsulator to the receiver.	Refer to the extension suggestions on RFC2890.

- **IP Header**

For details about IP header, please refer to RFC791.

In GRE-IP tunnel, the protocol field of the IP header protocol is equal to 47 (decimal).

2.3Working Process

- **Tunnel start binding**

When a GOOSE message arrives at the start device, the system searches for the binding between the GOOSE stream and Tunnel start interface in the GOOSE-Tunnel-Binding-List. If a match is found, the system processes the message according to the mode setting in the matched entry:

In Tunnel-only mode, the system only forwards GOOSE message to Tunnel start interface.

In Normal mode, the system not only forwards GOOSE message to Tunnel start interface, but also forwards the message in source VLAN according to FDB entries.

- **Encapsulation**

When a GOOSE message enters the tunnel, the tunnel start interface generates an IP header for the message according to message's destination IP address (IP unicast or IP multicast), and IP address of source interface. After encapsulating GOOSE PDU with GRE header, the system encapsulates it with IP header.

- **Delivery**

The IP message formed after encapsulation searches for the out interface in the routing table by device IP protocol stack, and then is delivered to the next-hop router, realizing routing and forwarding in IP network.

- **Decapsulation**

As soon as the encapsulated message reaches the destination device and the device confirms that the destination is the local address, the device will conduct message decapsulation and release passenger protocol message. This is the GOOSE PDU.

- **VLAN remark**

After GOOSE PDU decapsulation is completed, the VID of its IEEE802.1Q field is used to obtain its source VLAN, and then the GOOSE PDU VLAN remark list on device is searched for the target VLAN.

- **Forwarding in Target (V)LAN**

After the confirmation of target VLAN, the next step is to get the actual out interface in target VLAN.

The static GOOSE table is searched first. If a match is found, the message is forwarded to the bound out interface. If no match is found, the process moves to the next step according to the release mode of decapsulated GOOSE PDU:

If the release mode is Strict mode, the message is discarded.

If the release mode is Normal mode, the message is forwarded according to the FDB table. If no match is found in the FDB table, the system forwards it to all ports in target VLAN.

2.4Application Restrictions

- Because of routing transmission in IP network, it might cause additional network latency and the additional latency is hard to estimate.
- Due to the differences of routing paths in IP network, it might cause the disorder of the encapsulated messages when they reach tunnel termination. Because of the low latency requirements of GOOSE message, even if Sequence Number function of GRE tunnel is used, it is still hard for extended time cache and not easy to request re-transmission, so the messages in disorder will be discarded.
- In IP network transmission, when the encapsulated messages are lost due to network issues, the tunnel cannot provide re-transmission mechanism.
- When multicast IP address is used as the destination address of IP header to realize the application of 1:N copies and distribution, the IP network should be equipped with suitable IP multicast routing protocols, and there is no packet loss in the copy and forwarding of IP multicast data messages.

3. Typical Networking Application

3.1 IP Unicast GOOSE-GRE-IP-Tunnel Application

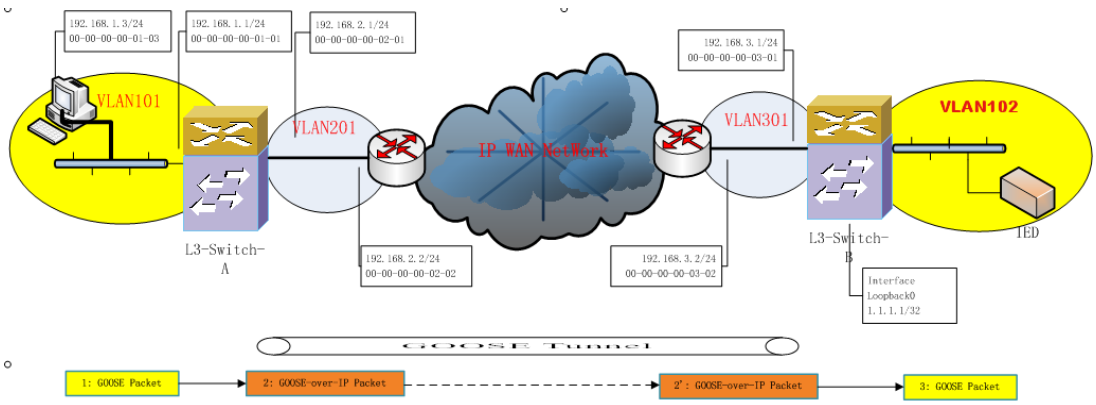


Figure 7: Typical Networking Application

As shown in Figure 7,

1) The central workstation (on the left) is connected to public IP network by Layer-3 Switch A that supports GOOSE-over-GRE-IP-Tunnel.
2) The IP address of central controller is 192.168.1.3/4.
3) The IP address of Interface VLAN101 of L3-Switch-A is 192.168.1.1/24.
4) The IP address of Interface VLAN201 of L3-Switch-A is 192.168.2.1/24, connected to public IP network.
5) The substation (on the right) is connected to the public IP network by Layer-3 switch B that supports GOOSE-over-GRE-IP-Tunnel.

6) The IP address of Interface VLAN301 of L3-Switch-A is 192.168.3.1/24, connected to public IP network.

Requirement: GOOSE (01-0C-CD-01-00-01) PDU sent from VLAN101 of the central controller in the central workstation can be transmitted to VLAN102 on the other side of IP network.

Configuration steps:

- L3-SWITCH-A configuration

  a) Create Tunnel interface 1.

  Switch-A(Config)#interface tunnel 1

  b) Set the type of Tunnel interface 1 to GRE-IP.

  Switch-A(Config-Tunnel-1)#mode gre-ip

  c) Configure the destination IP address of Tunnel interface 1 (unicast address).

  Switch-A(Config-Tunnel-1)#destination ip address 192.168.3.1

  d) Configure the source interface of Tunnel interface 1.

  Switch-A(Config-Tunnel-1)#source interface vlan 101

  e) Configure the start binding between GOOSE and Tunnel interface 1 (Tunnel-Only mode).

  Switch-A(Config)#goose tunnel-binding mac-address 01-0C-CD-01-00-01 vlan 101 interface tunnel 1 tunnel-only

  f) Configure a static route.

  Switch-A(Config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2

- L3-SWITCH-B configuration

  a) Create Tunnel interface 1.

  Switch-B(Config)#interface tunnel 1

  b) Set the type of Tunnel interface 1 to GRE-IP.

  Switch-B(Config-Tunnel-1)#mode gre-ip

  c) Configure the source port of Tunnel interface 1.

  Switch-B(Config-Tunnel-1)#source interface vlan 301

  d) Configure VLAN remark.

  Switch-B(Config)#goose vlan-remark mac-address 01-0C-CD-01-00-01 vlan 101 target-vlan 102

  e) Set the release mode of decapsulated GOOSE PDU to normal.

  Switch-B(Config)#goose forwarding-policy tunnel-end normal

4. Prospect

With GOOSE-over-GRE-IP tunnel, GOOSE PDU can pass through IP network. It extends the transmission range of GOOSE PDU and facilitates the network communication between central workstation and substations. With the development of network reliability, network speed and router performance, GOOSE transmission through IP tunnel across IP network can be a beneficial attempt for the combination of GOOSE application and IP network communication.

5. References

- IEC61850-8-1
- RFC1701 Generic Routing Encapsulation (GRE) (INFORMATIONAL)
- RFC1702 Generic Routing Encapsulation over IPv4 networks (INFORMATIONAL)
- RFC2784 Generic Routing Encapsulation (GRE) (PROPOSED STANDARD -Updated by RFC 2890)
- RFC2890 Key and Sequence Number Extensions to GRE (PROPOSED STANDARD)