Generic UDP Encapsulation (update)

draft-ietf-nvo3-gue-01

Tom Herbert therbert@google.com
Lucy Yong lucy.yong@huawei.com
Osama Zia osamaz@microsoft.com

July 2015 Prague Czech

Changes in 01 version

- Removed GUE preamble bit. First two bits of GUE header are the version number and the rest of the header format is defined based on version.
- Added description of “No-next-hdr” and control type number zero. Allows payload types that are described by other means.
- Removed most of the text in the security section, which is covered by the GUE security draft.
- Added procedures for multicast of GUE packets.
- Description of request for IANA registry for GUE flags and GUE optional fields.

Proposed Extensions

- VNID option (draft-hy-nvo3-gue-4-nvo-02**)**
- Security option (draft-hy-gue-4-secure-transport-02)
- Payload transform option (draft-hy-gue-4-secure-transport-02)
- GUE header checksum (draft-herbert-guecsum-00)
- Remote checksum offload (draft-herbert-remotecsumoffload-00)
- GUE fragmentation (draft-herbert-gue-fragmentation-00)
- Session identifier (draft-herbert-gue-session-id-00)

Implementation & deployment

- Software implementation
  - GUE introduced in Linux 3.17
    - Basic tunneling support
    - Planning to add support in OVS and LWT (light weight tunnels)
- Hardware support
  - Basic GUE adopts protocol generic mechanisms and works well with most deployed HW
  - More advanced features might benefit from HW support, some vendors are adding this
- Deployment
  - Being deployed as generic tunnel mechanism
  - Good replacement for IPIP in particular (that does not work well with ECMP)

Next Steps

- Request the registries from IANA
  - make GUE extension proposals easier to specify
- Address comments/suggestions
- WG crosscheck, e.g. TSV WG
- Get more implementation and deployment

Generic UDP Encapsulation (GUE) for Network Virtualization Overlay (NVO)

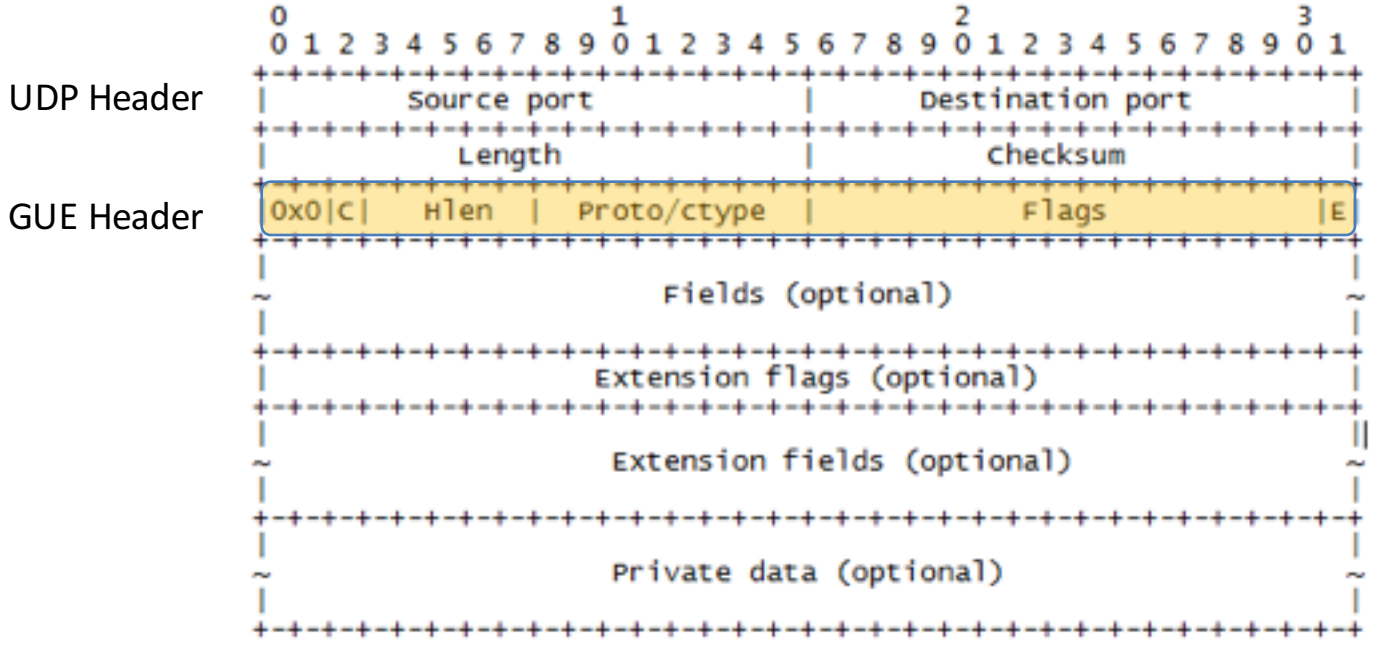
draft-hy-nvo3-gue-4-nvo-02

Lucy Yong lucy.yong@huawei.com
Tom Herbert therbert@google.com
Osama Zia osamaz@microsoft.com

July 2015 Prague Czech

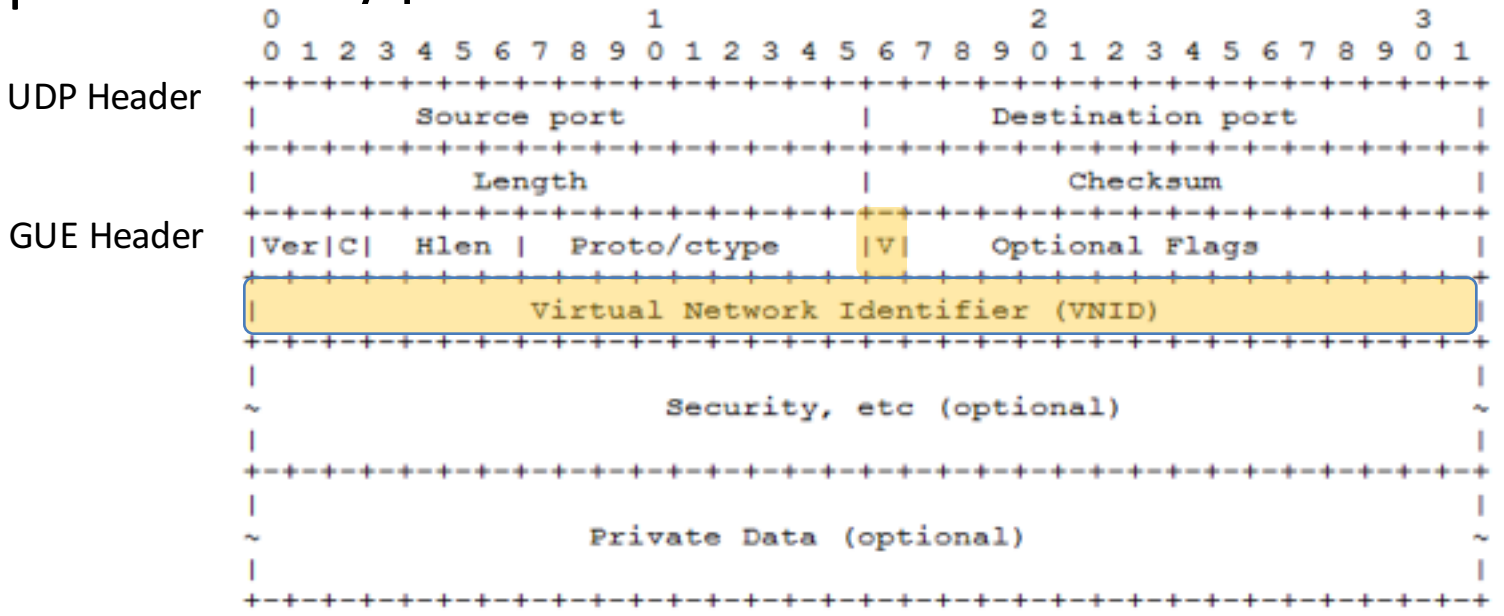
Generic UDP Encapsulation (GUE)

- A UDP encapsulation for network tunnel encapsulation
- The format has a GUE header after UDP header
- GUE header has:
  - 32 bits base header for 5 key fields
  - extensible structure for tunnel transport and tunnel applications



GUE for NVO3 Encapsulation

- Allocates one flag bit, 'V', from GUE flag field for NVO3 encap.
  - MUST set the flag for NVO3 encapsulation
- Defines a Virtual Network Identifier (VNID) field (32 bits) that associates with 'V' flag
  - MUST present when flag 'V' is set, MUST NOT present when clear
- Uses other GUE options such as GUE security in NVO3 encap.
- Option to carry private data in GUE header



GUE for NVO3 Encapsulation Merits

- Use of a unified tunnel encapsulation in DCs
  - With rich a set of tunnel transport features, e.g. security, offload
- VN ID is in GUE option field, extensible in future, e.g.
  - Define a new option to supersede it or
  - New flag to add more bits, e.g. 64
- No requirement on VN ID structure, local site matter
- Fully compliant with NVO3 architecture
  - with extensibility in future
- Ability to carry private data

Read draft-ietf-nvo3-gue-02 for more information

Changes in 02 version

- Added new co-author
- Expended Section 4 of Encapsulation/Decapsulation Operation

- Allow the proto/ctype in GUE header to be NULL
  - Useful when NVO3 encap. uses encryption option
- Use GUE security and encryption options
- IANA Request:
  - Allocate the first bit in the registry of GUE optional flag field for NVO3
  - Register a 32 bit field on GUE option field registry for VN ID

Next Steps

- Welcome comments
- Authors request WG adoption
  - GUE draft (WG draft) only specifies GUE protocol structure and key fields, VNID for NVO3 is in GUE optional field and described in this draft.
  - This draft also specifies additions for GUE to be used for NVO3 encapsulation

Generic UDP Encapsulation (GUE) For Secure Transport

draft-hy-gue-4-secure-transport-02

Lucy Yong lucy.yong@huawei.com
Tom Herbert therbert@google.com

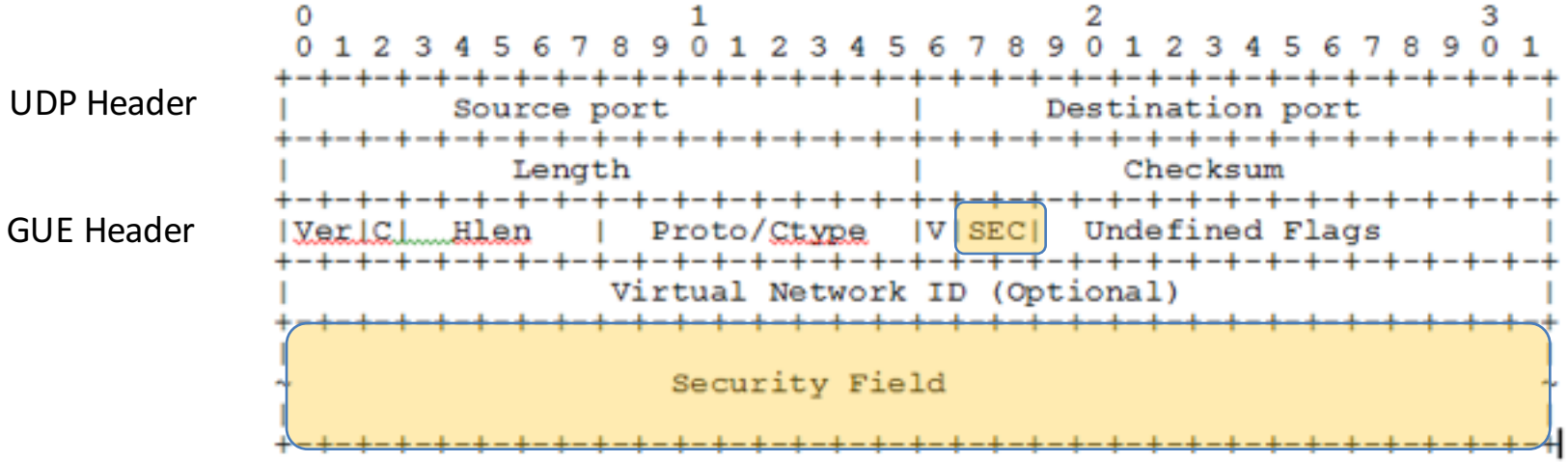
July 2015 Prague Czech

GUE Secure Transport Capability

- GUE has two security related options for GUE applications to use such as NOV3,
  A. GUE header authentication and integrity validation
  B. GUE payload encryption
- Two options can be used independently or together
- GUE secure transport options apply to both IPv4 and IPv6 delivery networks

A: Header Authentication & Integrity

- Use two flag bits ‘SEC’ in GUE flag field, specify ‘SEC’ flags as of:
  - 00 - No security field
  - 01 - 64 bit security field
  - 10 - 128 bit security field
  - 11 - 256 bit security field
- The corresponding security field MUST be present when the value of ‘SEC’ is set
- The value in the security field is used for GUE header authentication and integrity validation
  - The negotiation of the value is done out of band b/w GUE tunnel endpoints
  - Examples for the value produce method: Cookies or GUE header hash



B: GUE Payload Encryption

- Apply Datagram Transport Layer Security (DTLS) [RFC6347] to GUE payload, which results,
  - GUE payload is encrypted but GUE header remains in plaintext
- Use one bit 'T' in GUE flag field to indicate payload encryption
  - When the flag 'T' is set, a payload transform field MUST be present in GUE optional fields and the format as follows:

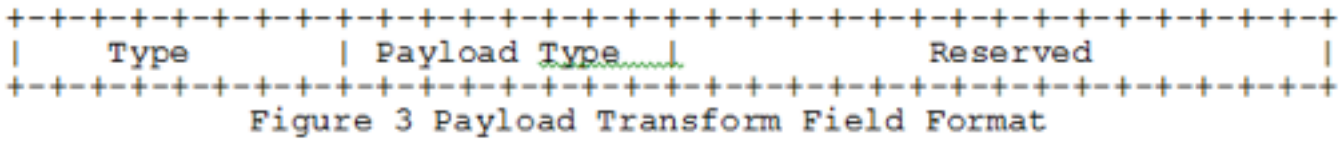


Figure 3 Payload Transform Field Format

Type: Payload Transform Type, i.e., Code Point (allow other encryp.)

Payload Type: Indicate encrypted payload type

Note: When encryption is used, proto/ctype in GUE header MUST set to NULL

- UDP dst. port uses GUE UDP port and UDP src port for entropy

Read draft-hy-gue-secure-transport-02 for detail

Changes in 02 version

- Clarified GUE security capabilities
- Added GUE payload transform option
  - Protocol for GUE payload encryption
  - GUE encapsulator/decapsulator operations
  - Discuss other security mechanisms

GUE Secure Transport for NVO3

- Secure Transport over IP networks is important for NVO3.
- NVO3 encapsulation can use GUE security options to authenticate header and/or encrypt tenant payload.
- VNID is encoded in GUE header and can be protected by header authentication option.
- NVA may facilitate NVEs for the negotiation of the value in security field.
- NVE may use other encryption mechanism for the payload encryption and encode the type in the payload transform field.
- To secure the payload type when use of payload encryption, proto/ctype in GUE header MUST set to NULL, the payload type SHOULD be encoded in the payload transform field.

Next Steps

- Solicit comments and suggestions
- Discuss this in SAAG
- Authors request WG adoption
  - NVO3 needs secure transport capability
  - NVO3 encapsulation can use GUE secure transport options to achieve the goal

Comment and Question?