FRRouting / frr Public

Code Issues 369 Pull requests 367 Discussions Actions Projects

Commit 7676cad

Mark Stapp committed 3 weeks ago · 20 / 21

```
bgpd: improve packet parsing for EVPN and ENCAP/VNC

Improve packet validation for EVPN NLRIs and for ENCAP/VNC.

Signed-off-by: Mark Stapp <mjs@cisco.com>
```

master (#21098)

1 parent 5c4ca88 commit 7676cad

3 files changed +35 -1 lines changed

Top

Filter files…

- bgpd
  - bgp_evpn.c
  - bgp_evpn_mh.c
  - rfapi
    - rfapi_rib.c

3 files changed +35 -1 lines changed

Search within code

bgpd/bgp_evpn.c

```
@@ -5023,6 +5023,14 @@ static int process_type2_route(struct peer *peer,
afi_t afi, safi_t safi,
5023 5023            goto fail;
5024 5024        }
5025 5025
     5026 +     /* Validate ipaddr_len against the NLRI length */
```

```
                5027 +      if ((psize != 33 + (ipaddr_len / 8)) && (psize != 36 + (ipaddr_len / 8)))
                       {
                5028 +          flog_err(EC_BGP_EVPN_ROUTE_INVALID,
                5029 +               "%u:%s - Rx EVPN Type-2 NLRI with invalid IP address length %d",
                5030 +               peer->bgp->vrf_id, peer->host, ipaddr_len);
                5031 +          goto fail;
                5032 +      }
                5033 +
5026            5034        if (ipaddr_len) {
5027            5035            ipaddr_len /= 8; /* Convert to bytes. */
5028            5036            p.prefix.macip_addr.ip.ipa_type = (ipaddr_len == IPV4_MAX_BYTELEN)
                       @@ -5120,6 +5128,15 @@ static int process_type3_route(struct peer *peer,
                       afi_t afi, safi_t safi,
5120            5128
5121            5129        /* Get the IP. */
5122            5130        ipaddr_len = *pfx++;
                5131 +
                5132 +      /* Validate */
                5133 +      if (psize != 13 + (ipaddr_len / 8)) {
                5134 +          flog_err(EC_BGP_EVPN_ROUTE_INVALID,
                5135 +               "%u:%s - Rx EVPN Type-3 NLRI with invalid IP address length %d",
                5136 +               peer->bgp->vrf_id, peer->host, ipaddr_len);
                5137 +          return -1;
                5138 +      }
                5139 +
5123            5140        if (ipaddr_len == IPV4_MAX_BITLEN) {
5124            5141            SET_IPADDR_V4(&p.prefix.imet_addr.ip);
5125            5142            memcpy(&p.prefix.imet_addr.ip.ip.addr, pfx, IPV4_MAX_BYTELEN);
```

bgpd/bgp_evpn_mh.c

```
                       @@ -845,9 +845,17 @@ int bgp_evpn_type4_route_process(struct peer *peer,
                       afi_t afi, safi_t safi,
845             845         memcpy(&esi, pfx, ESI_BYTES);
846             846         pfx += ESI_BYTES;
847             847
848             -
849             848         /* Get the IP. */
850             849         ipaddr_len = *pfx++;
                850 +
```

```
+     /* Validate */
+     if (psize != 19 + (ipaddr_len / 8)) {
+         flog_err(EC_BGP_EVPN_ROUTE_INVALID,
+              "%u:%s - Rx EVPN Type-4 NLRI with invalid IP address length %d",
+              peer->bgp->vrf_id, peer->host, ipaddr_len);
+         return -1;
+     }
+
      if (ipaddr_len == IPV4_MAX_BITLEN) {
          SET_IPADDR_V4(&vtep_ip);
          memcpy(&vtep_ip.ipaddr_v4, pfx, IPV4_MAX_BYTELEN);
```

bgpd/rfapi/rfapi_rib.c

```
@@ -668,11 +668,20 @@ static void rfapiRibBi2Ri(struct bgp_path_info *bpi,
struct rfapi_info *ri,
              break;

          case BGP_VNC_SUBTLV_TYPE_RFPOPTION:
+             /* Check for short subtlv: drop */
+             if (pEncap->length < 3)
+                 break;
+
+             /* Length of zero not valid */
+             if (pEncap->value[1] == 0)
+                 break;
+
              hop = XCALLOC(MTYPE_BGP_TEA_OPTIONS,
                            sizeof(struct bgp_tea_options));
              assert(hop);
              hop->type = pEncap->value[0];
              hop->length = pEncap->value[1];
+
              hop->value = XCALLOC(MTYPE_BGP_TEA_OPTIONS_VALUE,
                                   pEncap->length - 2);
              assert(hop->value);
```

Comments 0

Please sign in to comment.