

---

Subject: [PATCH][BRIDGE] Properly dereference the br\_should\_route\_hook  
Posted by Pavel Emelianov on Tue, 27 Nov 2007 16:12:11 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

This hook is protected with the RCU, so simple

```
if (br_should_route_hook)
    br_should_route_hook(...)
```

is not enough on some architectures.

Use the rcu\_dereference/rcu\_assign\_pointer in this case.

Signed-off-by: Pavel Emelyanov <xemul@openvz.org>

---

```
diff --git a/net/bridge/br_input.c b/net/bridge/br_input.c
index 3cedd4e..b42b192 100644
--- a/net/bridge/br_input.c
+++ b/net/bridge/br_input.c
@@ -122,6 +122,7 @@ static inline int is_link_local(const unsigned char *dest)
struct sk_buff *br_handle_frame(struct net_bridge_port *p, struct sk_buff *skb)
{
    const unsigned char *dest = eth_hdr(skb)->h_dest;
+    typeof(br_should_route_hook) rhook;

    if (!is_valid_ether_addr(eth_hdr(skb)->h_source))
        goto drop;
@@ -147,9 +148,9 @@ struct sk_buff *br_handle_frame(struct net_bridge_port *p, struct sk_buff
*skb)

switch (p->state) {
case BR_STATE_FORWARDING:
-
-    if (br_should_route_hook) {
-        if (br_should_route_hook(skb))
+    rhook = rcu_dereference(br_should_route_hook);
+    if (rhook != NULL) {
+        if (rhook(skb))
            return skb;
        dest = eth_hdr(skb)->h_dest;
    }
}
diff --git a/net/bridge/netfilter/ehtable_broute.c b/net/bridge/netfilter/ehtable_broute.c
index e44519e..be6f186 100644
--- a/net/bridge/netfilter/ehtable_broute.c
+++ b/net/bridge/netfilter/ehtable_broute.c
@@ -70,13 +70,13 @@ static int __init ehtable_broute_init(void)
```

```
if (ret < 0)
    return ret;
/* see br_input.c */
- br_should_route_hook = ebt_broute;
+ rcu_assign_pointer(br_should_route_hook, ebt_broute);
    return ret;
}

static void __exit ebtable_broute_fini(void)
{
- br_should_route_hook = NULL;
+ rcu_assign_pointer(br_should_route_hook, NULL);
    synchronize_net();
    ebt_unregister_table(&broute_table);
}
```

---