Subject: [PATCH][BRIDGE] Lost call to br_fdb_fini() in br_init() error path
Posted by Pavel Emelianov on Tue, 27 Nov 2007 14:39:42 GMT
View Forum Message <> Reply to Message

In case the br_netfilter_init() (or any subsequent call)
fails, the br_fdb_fini() must be called to free the allocated
in br_fdb_init() br_fdb_cache kmem cache.

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

```
diff --git a/net/bridge/br.c b/net/bridge/br.c
index 93867bb..a901828 100644
--- a/net/bridge/br.c
+++ b/net/bridge/br.c
@@ -39,7 +39,7 @@ static int __init br_init(void)

  err = br_fdb_init();
  if (err)
-  goto err_out1;
+  goto err_out;

  err = br_netfilter_init();
  if (err)
@@ -65,6 +65,8 @@ err_out3:
 err_out2:
  br_netfilter_fini();
 err_out1:
+ br_fdb_fini();
+err_out:
  llc_sap_put(br_stp_sap);
  return err;
 }
```

Subject: Re: [PATCH][BRIDGE] Lost call to br_fdb_fini() in br_init() error path
Posted by Stephen Hemminger on Tue, 27 Nov 2007 16:19:56 GMT
View Forum Message <> Reply to Message

On Tue, 27 Nov 2007 17:39:42 +0300
Pavel Emelyanov <xemul@openvz.org> wrote:

> In case the br_netfilter_init() (or any subsequent call)
> fails, the br_fdb_fini() must be called to free the allocated
> in br_fdb_init() br_fdb_cache kmem cache.
>
> Signed-off-by: Pavel Emelyanov <xemul@openvz.org>

>
> ---
>
> diff --git a/net/bridge/br.c b/net/bridge/br.c
> index 93867bb..a901828 100644
> --- a/net/bridge/br.c
> +++ b/net/bridge/br.c
> @@ -39,7 +39,7 @@ static int __init br_init(void)
>
> err = br_fdb_init();
> if (err)
> - goto err_out1;
> + goto err_out;
>
> err = br_netfilter_init();
> if (err)
> @@ -65,6 +65,8 @@ err_out3:
> err_out2:
> br_netfilter_fini();
> err_out1:
> + br_fdb_fini();
> +err_out:
> llc_sap_put(br_stp_sap);
> return err;
> }

Good catch, thanks I hope you didn't find this in live system.

--
Stephen Hemminger <shemminger@linux-foundation.org>

Subject: Re: [PATCH][BRIDGE] Lost call to br_fdb_fini() in br_init() error path
Posted by Herbert Xu on Thu, 29 Nov 2007 12:45:22 GMT
View Forum Message <> Reply to Message

On Tue, Nov 27, 2007 at 05:39:42PM +0300, Pavel Emelyanov wrote:
> In case the br_netfilter_init() (or any subsequent call)
> fails, the br_fdb_fini() must be called to free the allocated
> in br_fdb_init() br_fdb_cache kmem cache.
>
> Signed-off-by: Pavel Emelyanov <xemul@openvz.org>

Patch applied to net-2.6. Thanks Pavel!
--
Visit Openswan at http://www.openswan.org/
Email: Herbert Xu ~{PmV>HI~} <herbert@gondor.apana.org.au>
Home Page: http://gondor.apana.org.au/~herbert/

PGP Key: http://gondor.apana.org.au/~herbert/pubkey.txt