

Virtual IP Routing

DESCRIPTION

Copyright

© Ericsson AB 2018–2019. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Understanding Virtual IP Routing	1
1.1	Key Virtual IP Routing Concepts	1
1.2	Gateway Routers	2
1.3	Front-end Elements	3
1.4	Static Routing	3
1.5	Dynamic Routing	3
1.6	Next-hop Supervision	4
1.7	Interlinking Networks	4
1.8	Supervised Remote Gateway	4
1.9	Resiliency Protection	5
2	Virtual IP Addressing-related Alarms and Events	6
3	Security Management	6





1 Understanding Virtual IP Routing

1.1 Key Virtual IP Routing Concepts

The Virtual IP Routing Management here described concerns the change of internetworking related parameters between Network Element (NE) and gateway routes for a NE deployed with the eVIP system framework component for embedded Virtual IP addressing. This Virtual IP system framework is used by several applications across different NEs provided by Ericsson.

The following key concepts are used for connectivity in a NE deployed with Virtual IP routing:

- Gateway routers
- Front-end elements
- Static routing
- Dynamic routing
- Interlinking networks
- Next-hop supervision
- Supervised gateway
- Resiliency protection

After a brief contextual overview the key concepts listed above will be described.

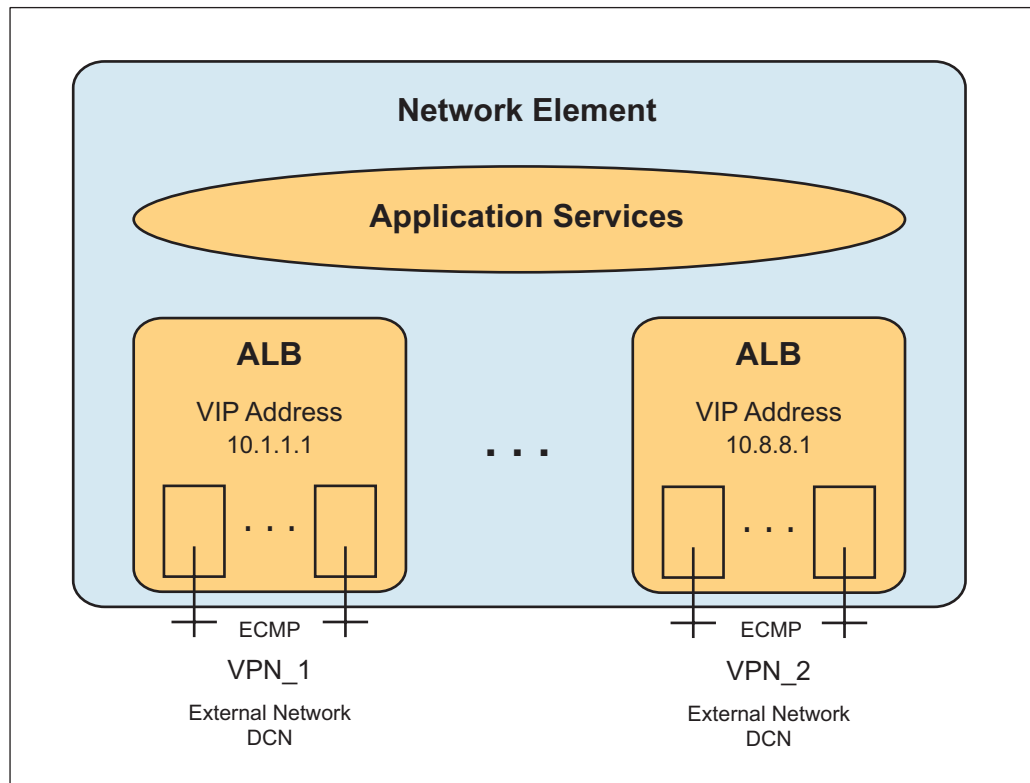


Figure 1 Shows ALBs with Front-end Elements

In a NE using this embedded Virtual IP framework the Virtual IP (VIP) addresses are within the system framework configured to Abstract Load Balancers (ALBs). The ALBs are logical software entities embedded in the NE. The external interfaces of an ALB are called the front-end element interfaces and are deployed through the Front End Elements (FEEs) of the ALB. Embedded in the NE, the FEEs which are software entities and acts functionally as IP routers. Furthermore, the front-end interfaces of the FEEs are externally connected to gateway routers for communication with the external world through the connected DCN.

1.2 Gateway Routers

The NE is connected to DCN through one or more gateway routers. In typical deployments two gateway routers are used for redundancy. From the gateway router towards the DCN, a variety of routing methods can be used and the choice is here only limited by DCN network arrangements in the specific deployment scenario and the capabilities of the type of gateway router used. In many typical deployments the gateway routers used are so called Virtual Routers configured in the networking infrastructure or on the Customer Premises Equipment (CPE).



1.3 Front-end Elements

The Front End Elements (FEEs) are logical entities in the NE which acts as embedded IP routers used for external connectivity through gateway routers that are connected to DCN. The FEEs in the NE are organized per Abstract Load Balancer (ALB) which delineates handling and resource allocation in the NE and also delineates connectivity to a Virtual Private Network (VPN) present in the DCN. Each VPN requires an own ALB which has an own set of FEEs. For example, a DCN with two VPNs requires two ALBs which each have their own set of FEEs that are connected to gateway routers of the corresponding VPN.

The external interfaces of an ALB, that is, the front-end interfaces which are configured in the Front End Elements (FEEs) of the ALB are also called external FEE interfaces. Each FEE has a single configured primary layer-3 address for the external interface which is used for the external connectivity over the interlinking network between the FEEs a next-hop gateway router.

1.4 Static Routing

The use of static routing between gateway routers and FEEs requires that at least one static route is configured in the gateway router for each VIP address pointing to at least one FEE's external interface IP address. However, usually several static routes are configured for a VIP address to point to several FEEs for Equal Cost Multi Paths (ECMP) traffic load sharing. Adding a new Virtual IP address in the NE usually requires the configuration of new static routes in the NE. Static routing is supported for both IPv4 and IPv6.

1.5 Dynamic Routing

In a Virtual IP routing context the use of dynamic routing means that VIP addresses are announced automatically to the gateway routers. For example, when adding a new VIP address to the NE, this new VIP address is on-the-fly announced to gateway routers. An advantage with dynamic routing is that there is no need to configure routes in the gateway router as new VIP addresses are added or removed in the NE.

Dynamic routing is a prerequisite for NEs using Any-cast routing with VIP addresses for Geographical Redundancy.

Dynamic routing is supported by the Open Shortest Path First (OSPF) routing protocol. For routing IPv4 traffic OSPFv2 is used and for routing IPv6 traffic OSPFv3 is used. The NEs that do use IPv6 for Virtual IP routing are always deployed as dual stack NEs. That is, both OSPFv2 and OSPFv3 are operational when IPv6 is used.

The OSPF protocols support Equal Cost Multi Paths load sharing of traffic and the protocols also takes care of resiliency failover in the event of a gateway router failure or an FEE failure situation.



Note:

- For connectivity between gateway routers and FEEs, the configured OSPFv2 area type must be of the Stub Area type or of the so called NSSA type. For OSPFv3 the configured area must be of type Stub Area. The configured area type must be the same for gateway routers and corresponding FEEs.
- All FEEs must be configured with OSPF Priority value set to 0. But gateway routers must be configured with an OSPF Priority value higher than 0.

1.6 Next-hop Supervision

Next-hop supervision here concerns the bi-directional supervision between gateway routers and FEEs. Next-hop supervision is done either by means of the Bi-directional Forwarding Detection (BFD) protocol or by the OSPF routing protocol or by a combination of both protocols.

BFD can be used in conjunction with both IPv4 and IPv6 static routing and with the OSPFv2 and OSPFv3 routing protocols.

When BFD is used in conjunction with OSPF the next-hops supervision and failover typically becomes much faster.

1.7 Interlinking Networks

The NE is connected to gateway routers over interlinking IP networks. Interlinking networks spans across intermediary Ethernet switches. Typically, several FEEs are connected to gateway routers over a common subnet. But in special configuration setups the use of separate small address range subnets per FEE is permissible.

1.8 Supervised Remote Gateway

The term Supervised Remote Gateway here concerns an optional feature whereby an FEE is configured to detect the unavailability of a specific gateway router IP address and thereafter raise an “eVIP Gateway Unavailable” alarm.

The Supervised Remote Gateway feature must be used in conjunction with one of the forms of next-hop supervision outlined in Section 1.6 Next-hop Supervision on page 4.

For example, if two gateway routers per ALB are used then each gateway router would be supervised by at least one FEE belonging to that ALB. To clarify, per ALB two FEEs would be used to supervise a pair of gateway routers in a one-to-one mapping.

**Note:**

- Optimally one gateway router is supervised by an individual FEE, however, more than one FEE may be configured to supervise the same gateway router.
- The configured Supervised Remote Gateway IP address should always correspond to one of the available next-hop gateway router addresses which is used by the default route on the FEE. For example, with OSPF there could be more than one available next-hop router advertised within the same area, however, it may not be desired to supervise more than one of these gateways from the same FEE.

WARNING: Multiple gateway addresses can be configured as supervised remote gateways under a single FEE, however, this means that the "Gateway Unavailable" alarm will NOT be raised until all configured gateways become unavailable.

1.9 Resiliency Protection

OSPF: In the case of dynamic routing between gateway routers and FEEs, resiliency failover is handled by the routing protocols OSPFv2 or OSPFv3 which both automatically takes advantage of ECMP and BFD when supported in deployed configurations. Hence, gateway routers and FEEs are thereby resiliency protected.

Static Routing with BFD: In the case of static routing with BFD between gateway routers the FEEs of an ALB may be divided into two sets where the first set uses one gateway router as next-hop and the second set uses the other router as next-hop. Conversely, each gateway router configures static routes (ECMP) to its corresponding set of external FEE interface IP addresses. This resiliency protection scheme can be used for both IPv4 and IPv6.

Static Routing: In the case where static routing (without BFD) is configured between gateway routers and the FEEs, the gateway routers can typically be configured with the Virtual Router Redundancy Protocol (VRRP) for redundancy. On the FEE side of the connection, configuring unsupervised static routes automatically enables a proprietary resilience mechanism known as "Resilient FEE IP Address". With this resiliency scheme the external IP address of an FEE can be relocated to any available FEE under the same ALB, should the FEE that the External IP was provisioned on go away for some reason. Multiple FEE External IP addresses can be temporarily relocated (hosted) on a single FEE, if needed, with this resiliency scheme.

Note: The Resilient FEE IP address mode of operation must only be used with unsupervised static routing. BFD supervision MUST not be used in this mode of operation.



2 Virtual IP Addressing-related Alarms and Events

Table 1 Virtual IP Addressing Related Alarms

Alarm	Description
eVIP, Gateway Unavailable	Raised when instability is detected on the connection between the FEE and external gateway.
eVIP, IPSEC Tunnel Fault	Raised when an IPsec tunnel goes down ungracefully between a VIP-enabled cluster and a peer.

Table 2 Virtual IP Addressing Related Events

Event	Description
eVIP, Configuration Fault	Reported when Virtual IP Addressing detects a faulty configuration.

3 Security Management

One Virtual IP Addressing role is defined, named System Administrator.

Once authenticated as a System Administrator, full access is granted to the Transport MO, its attributes, and actions.

For more information, refer to [User Management](#).