

WHAT IS CLAIMED IS:

1. A method, comprising:
in response to an interface record creation request, generating an interface record
comprising an IP address and a subnet identifier of a first subnet containing the
first IP address, and storing the interface record in a persistent repository;
5 in response to a first attachment request to attach the interface record to a first resource
instance of a plurality of resource instances, enabling the first resource instance to
receive traffic targeted at the first IP address; and
in response to a detachment request to detach the interface record from the first resource
10 instance, preventing the first resource instance from receiving traffic targeted at
the first IP address, and retaining the interface record in the persistent repository.
2. The method as recited in claim 1, further comprising:
in response to a second interface record creation request, generating a second interface
15 record comprising a second IP address; and
in response to a second attachment request to attach the second interface record to the
first resource instance, enabling the first resource instance to receive
traffic targeted at the second IP address.
- 20 3. The method as recited in claim 2, wherein the second IP address is part of a
second subnet, and wherein the second interface record comprises a subnet identifier of the
second subnet.
4. The method as recited in claim 3, further comprising:
25 receiving, at the first resource instance, a network packet from a source IP address,
wherein the source IP address is reachable from the first resource instance via the
first subnet, and wherein the network packet has a destination IP address
reachable from the first resource instance via the second subnet; and
routing the network packet to the destination IP address via the second subnet.
30
5. The method as recited in claim 3, further comprising:
in response to an IP address modification request comprising a new IP address,
modifying the interface record to include the new IP address;

identifying a currently-attached resource instance of the plurality of resource instances to which the interface record is attached; and
enabling the currently-attached resource instance to receive traffic directed at the new IP address.

5

6. The method as recited in claim 3, wherein the first subnet is part of a first logical partition of a network with a first Common Internet Domain Routing (CIDR) address prefix, and the second subnet is part of a second logical partition of the network with a second CIDR address prefix.

10

7. The method as recited in claim 1, wherein the interface record comprises a set of security properties including a first authorization entry identifying one or more entities authorized to submit an attachment request.

15

8. The method as recited in claim 7, wherein the set of security properties includes a second authorization entry identifying one or more entities authorized to modify the first authorization entry.

20

9. A system, comprising:
a processor coupled to a non-transitory computer-accessible storage medium storing program instructions computer-executable to:
in response to an interface record creation request, generate an interface record comprising an IP address and a subnet identifier of a first subnet containing the first IP address, and storing the interface record in a persistent repository; and
in response to a first attachment request to attach the interface record to a first resource instance of a plurality of resource instances, wherein the first resource instance is in a running state subsequent to its booting up, enable traffic targeted at the first IP address to be received at the first resource instance.

30

10. The system of claim 9, wherein the program instructions are further computer-executable to:
in response to a second interface record creation request, generate a second interface record comprising a second IP address; and

in response to a second attachment request to attach the second interface record to the first resource instance, enable the first resource instance to receive traffic targeted at the second IP address.

5 11. The system of claim 10, wherein the program instructions are further computer-executable to:

receive, at the first resource instance, a network packet from a source IP address, wherein the source IP address is accessible from the first resource instance via the first subnet, and wherein the network packet has a destination IP address accessible
10 from the first resource instance via a second subnet associated with the second IP address; and

route the network packet to the destination IP address via the second subnet.

12. The system of claim 9, wherein the interface record comprises a set of security
15 properties including an authorization entry identifying one or more entities authorized to modify the IP address.

13. The system of claim 9, wherein the interface record comprises a set of security properties including an authorization entry identifying at least one of: a port restriction for
20 incoming traffic, a protocol restriction for incoming traffic, a protocol restriction for outgoing traffic, or a protocol restriction for outgoing traffic.

14. The system of claim 10, wherein the second IP address is part of a second subnet, and wherein the first subnet is a data subnet designated for transmission of client application
25 data, and the second subnet is a management subnet designated for transmission of network administration data.

15. The system of claim 10, wherein the first IP address is part of a first network logical partition maintained on behalf of a first customer, and wherein the second IP address is
30 part of a second network logical partition maintained on behalf of a second customer.

WHAT IS CLAIMED IS:

1. A system, comprising:

a plurality of resource instances implemented by one or more computers including a first resource instance and a second resource instance; and

a network interface virtualization coordinator implemented by one or more computers;

wherein the network interface virtualization coordinator is operable to:

in response to an interface record creation request, generate an interface record comprising a first Internet Protocol (IP) address, a subnet identifier of a first subnet containing the first IP address, and a first set of security properties, and store the interface record in a repository;

in response to a first attachment request to attach the interface record to the first resource instance, enable the first resource instance to receive traffic targeted at the first IP address through a first network interface card in accordance with the first set of security properties;

in response to a detachment request to detach the interface record from the first resource instance, prevent the first resource instance from receiving traffic targeted at the first IP address; and

in response to a second attachment request to attach the interface record to the second resource instance, enable the second resource instance to receive traffic targeted at the first IP address through a second network interface card in accordance with the first set of security properties.

2. The system as recited in claim 1, wherein the network interface virtualization coordinator is further operable to:

in response to a second interface record creation request, generate a second interface record comprising a second IP address, and store the second interface record in the repository; and

in response to a new attachment request to attach the second interface record to the first resource instance, enable the first resource instance to receive traffic targeted at the second IP address.

3. The system as recited in claim 2, wherein the second IP address is part of a second subnet, and wherein the second interface record comprises a subnet identifier of the second subnet.

4. The system as recited in claim 3, wherein the network interface virtualization coordinator is further operable to:

receive, at the first resource instance, a network packet from a source IP address, wherein the source IP address is reachable from the first resource instance via the first subnet, and wherein the network packet has a destination IP address reachable from the first resource instance via the second subnet; and

route the network packet to the destination IP address via the second subnet.

5. The system as recited in claim 1, wherein the interface record comprises one or more additional IP addresses, and wherein, in response to the first attachment request to attach the interface record to the first resource instance, the network interface virtualization coordinator is further operable to enable the first resource instance to receive traffic targeted at the one or more additional IP addresses.

6. The system as recited in claim 1, wherein the network interface virtualization coordinator is further operable to:

in response to an IP address modification request comprising a new IP address,

modify the interface record to include the new IP address;

identify a currently-attached resource instance of the plurality of resource instances to which the interface record is attached; and

enable the currently-attached resource instance to receive traffic directed at the new IP address.

7. A method, comprising:

in response to an interface record creation request, generating an interface record comprising a first IP address and a subnet identifier of a first subnet containing the first IP address, and storing the interface record in a persistent repository;

in response to a first attachment request to attach the interface record to a first resource instance of a plurality of resource instances, enabling the first resource instance to receive traffic targeted at the first IP address;

in response to a detachment request to detach the interface record from the first resource instance, preventing the first resource instance from receiving traffic targeted at the first IP address, and retaining the interface record in the persistent repository; and

in response to a second attachment request to attach the interface record to a second resource instance, enabling the second resource instance to receive traffic targeted at the first IP address.

8. The method as recited in claim 7, further comprising:

in response to a second interface record creation request, generating a second interface record comprising a second IP address; and

in response to a second attachment request to attach the second interface record to the first resource instance, enabling the first resource instance to receive traffic targeted at the second IP address.

9. The method as recited in claim 8, wherein the second IP address is part of a second subnet, and wherein the second interface record comprises a subnet identifier of the second subnet.

10. The method as recited in claim 9, further comprising:

receiving, at the first resource instance, a network packet from a source IP address, wherein the source IP address is reachable from the first resource instance via the first subnet, and wherein the network packet has a destination IP address reachable from the first resource instance via the second subnet; and

routing the network packet to the destination IP address via the second subnet.

11. The method as recited in claim 9, further comprising:

in response to an IP address modification request comprising a new IP address, modifying the interface record to include the new IP address;

identifying a currently-attached resource instance of the plurality of resource instances to which the interface record is attached; and

enabling the currently-attached resource instance to receive traffic directed at the new IP address.

12. The method as recited in claim 9, wherein the first subnet is part of a first logical partition of a network with a first Common Internet Domain Routing (CIDR) address prefix, and the second subnet is part of a second logical partition of the network with a second CIDR address prefix.

13. The method as recited in claim 7, wherein the interface record comprises a set of security properties including a first authorization entry identifying one or more entities authorized to submit an attachment request.

14. The method as recited in claim 13, wherein the set of security properties includes a second authorization entry identifying one or more entities authorized to modify the first authorization entry.

15. A non-transitory computer-accessible storage medium storing program instructions computer-executable to implement:

in response to an interface record creation request, generating an interface record comprising an IP address and a subnet identifier of a first subnet containing the first IP address, and storing the interface record in a persistent repository;

in response to a first attachment request to attach the interface record to a first resource instance of a plurality of resource instances, wherein the first resource instance is in a running state subsequent to its booting up, enabling traffic targeted at the first IP address to be received at the first resource instance;

in response to a detachment request to detach the interface record from the first resource instance, preventing the first resource instance from receiving traffic targeted at the first IP address; and

in response to a second attachment request to attach the interface record to a second resource instance of the plurality of resource instances, enabling traffic targeted at the first IP address to be received at the second resource instance.

16. The non-transitory computer-accessible storage medium as recited in claim 15, wherein the program instructions are computer-executable to implement:

in response to a second interface record creation request, generating a second interface record comprising a second IP address; and

in response to a second attachment request to attach the second interface record to the first resource instance, enabling the first resource instance to receive traffic targeted at the second IP address.

17. The non-transitory computer-accessible storage medium as recited in claim 16, wherein the second IP address is part of a second subnet, and wherein the second interface record comprises a subnet identifier of the second subnet.

18. The non-transitory computer-accessible storage medium as recited in claim 17, wherein the program instructions are computer-executable to implement:

receiving, at the first resource instance, a network packet from a source IP address, wherein the source IP address is accessible from the first resource instance via the first subnet, and wherein the network packet has a destination IP address accessible from the first resource instance via the second subnet; and

routing the network packet to the destination IP address via the second subnet.

19. The non-transitory computer-accessible storage medium as recited in claim 15, wherein the interface record comprises a set of security properties including an authorization entry identifying one or more entities authorized to modify the IP address.

20. The non-transitory computer-accessible storage medium as recited in claim 15, wherein the interface record comprises a set of security properties including an authorization entry identifying

at least one of: a port restriction for incoming traffic, a protocol restriction for incoming traffic, a port restriction for outgoing traffic, or a protocol restriction for outgoing traffic.

21. The non-transitory computer-accessible storage medium as recited in claim 15, wherein the program instructions are computer-executable to implement:

in response to an IP address modification request comprising a new IP address,
modifying the interface record to include the new IP address;
identifying a currently-attached resource instance of the plurality of resource instances to which the interface record is attached; and
enabling the currently-attached resource instance to receive traffic directed at the new IP address.

22. The non-transitory computer-accessible storage medium as recited in claim 17, wherein the first subnet is a data subnet designated for transmission of client application data, and the second subnet is a management subnet designated for transmission of network administration data.

23. The non-transitory computer-accessible storage medium as recited in claim 16, wherein the first IP address is part of a first network logical partition maintained on behalf of a first customer, and wherein the second IP address is part of a second network logical partition maintained on behalf of a second customer.