Module 4
Network management

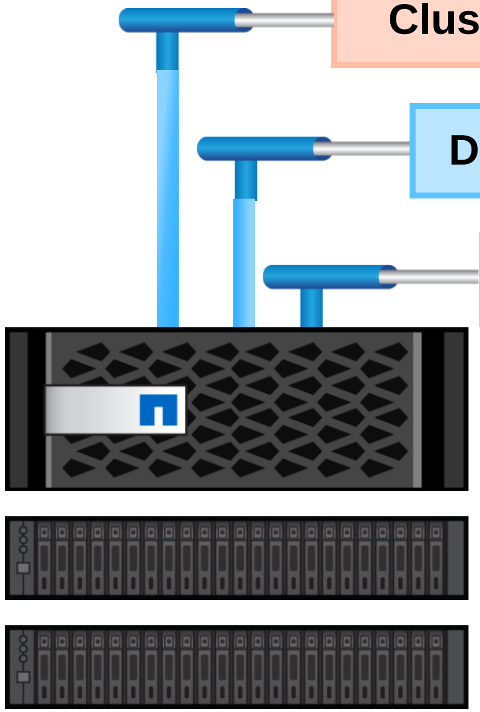
About this module

This module focuses on enabling you to do the following:

- Describe the interaction between physical and virtual network resources in a cluster
- Configure and manage physical and virtual networking resources

Lesson 1
NetApp ONTAP network review

Networks



Cluster Interconnect: Required

Data Network: Required

Management Network: Optional

Management network:

- Cluster administration
- FAS and AFF systems that include dedicated ports for management
- Recommended to use a dedicated network separate from the data network

Data network:

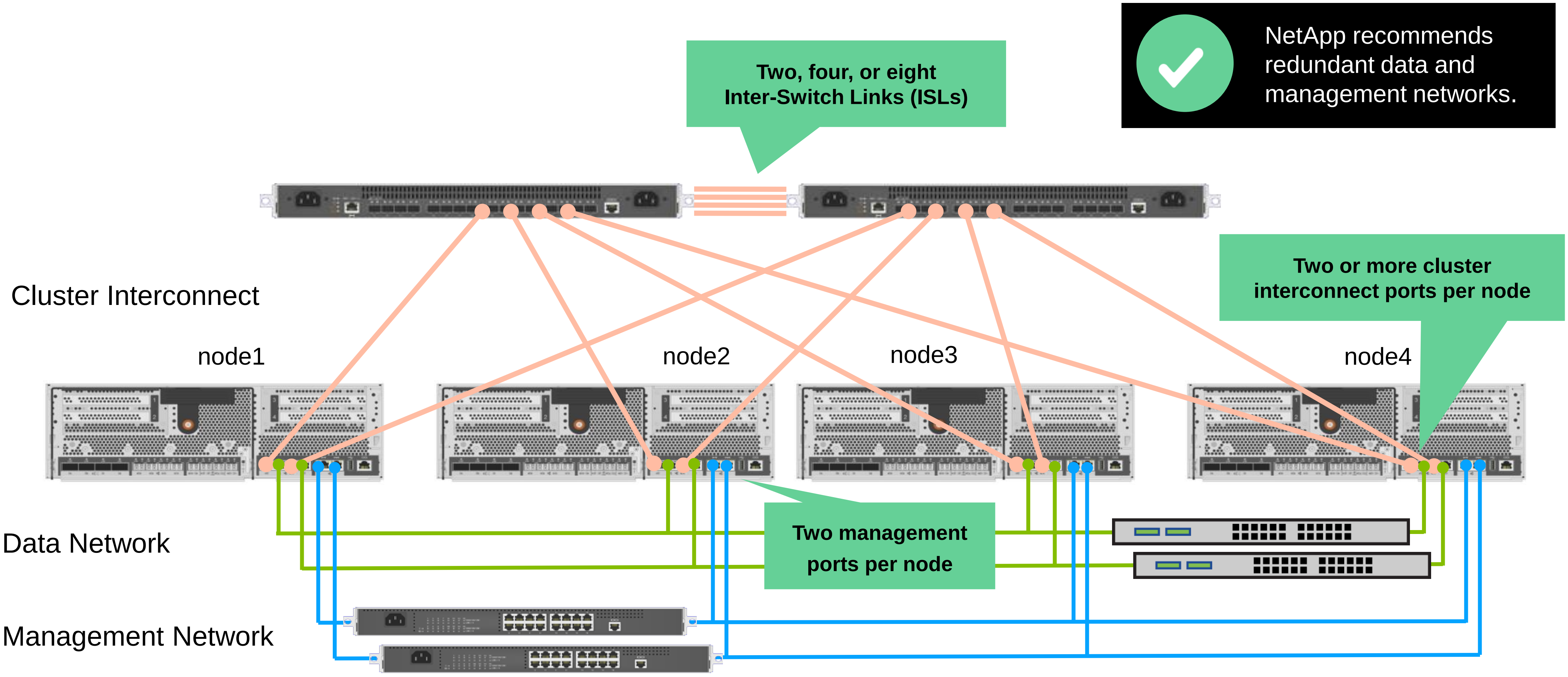
- One or more networks for data access from clients or hosts
- Ethernet, FC, or converged network

Cluster interconnect:

Private network for the following:

- Inter-node communications
- Indirect data access

Networks



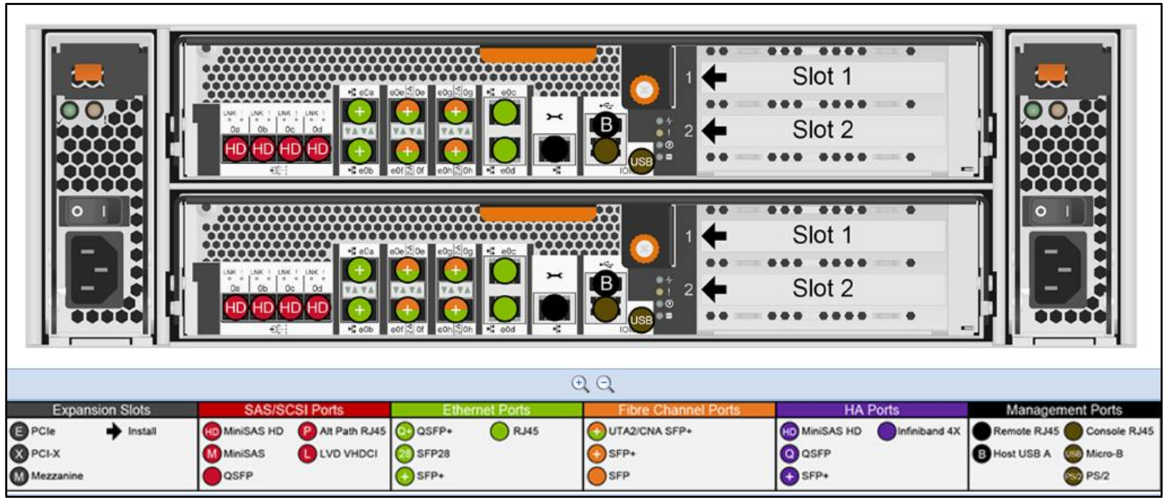
NetApp recommends redundant data and management networks.
Two, four, or eight Inter-Switch Links (ISLs)
Cluster Interconnect
Two or more cluster interconnect ports per node
node1
node2
node3
node4
Data Network
Two management ports per node
Management Network

Lesson 2
Network ports

Physical ports example

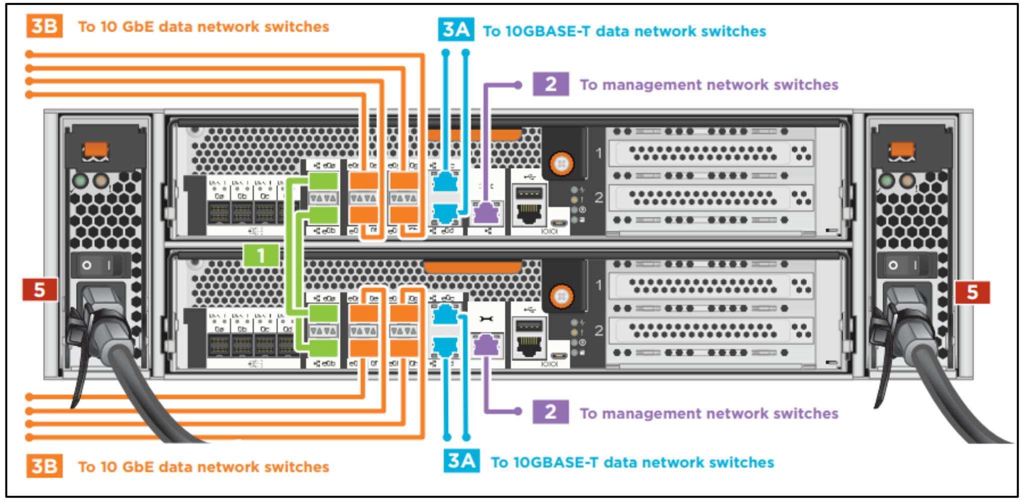
Hardware Universe

- Focused on port identification
- Downloadable Visio-template-based picture



Installation and Setup Instructions (ISI)

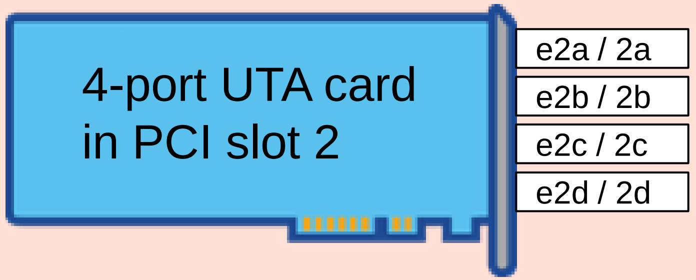
- Focused on cabling
- PDF on MySupport website



Cluster Interconnect   Data Network (FC/Ethernet)   Data Network (Ethernet)

Physical port identification

- Ethernet ports are named e<location><letter>:
  - e0a is the first port on the controller motherboard.
  - e3a is a port on a card in slot 3.
- FC ports are named <location><letter>:
  - 0a is the first port on the controller motherboard.
  - 3a is a port on a card in slot 3.
- Unified target adapter (UTA) ports have both an Ethernet name and an FC name,
  e <location><letter> / <location><letter>
  - e0a / 0a is the first port on the controller motherboard.
  - e3a / 3a is a port on a card in slot 3.
  - Use of show commands returns only FC label names (even in Ethernet mode).



Modifying network port attributes

Change the personality of a UTA port

Insert the proper optical module before changing modes.

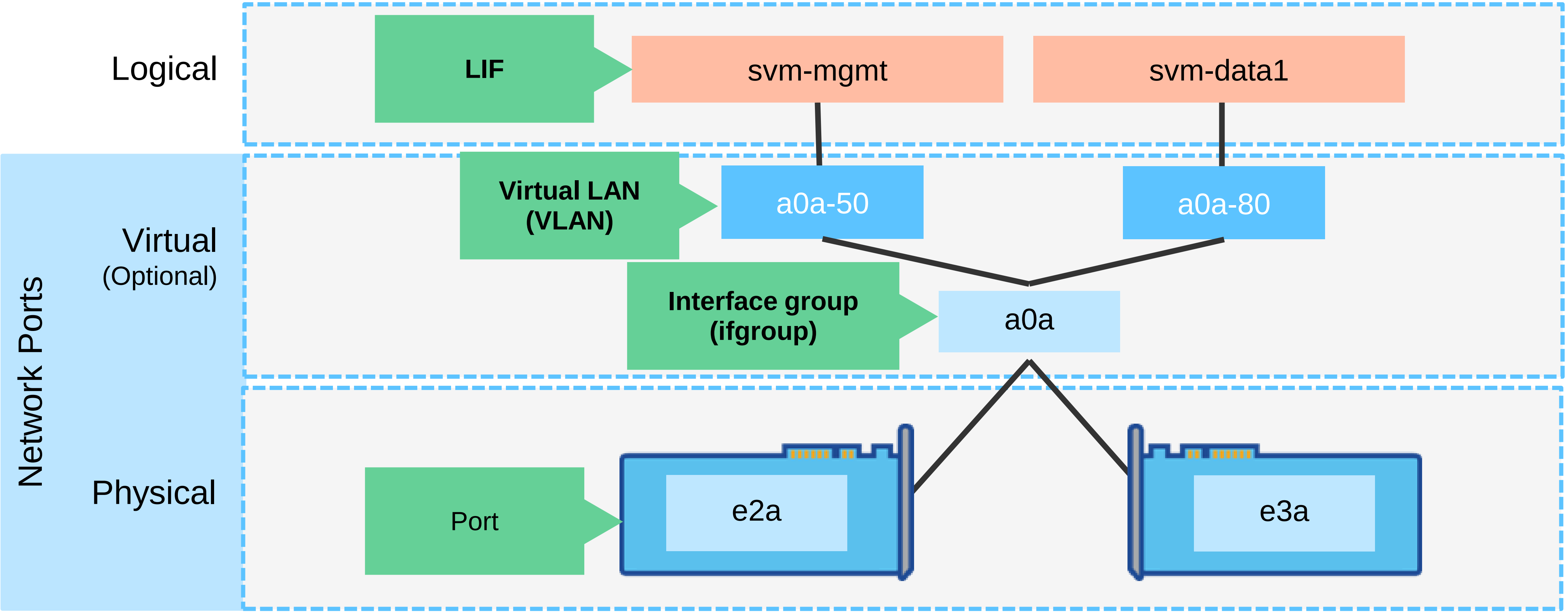
1. Remove LIFs or migrate LIFs to other ports.
2. Take the port offline.
3. Change the personality of the UTA port.

```
cluster2::> system node hardware unified-connect modify -node cluster2-01 -adapter 0e
            -mode fc|cna
```

4. Reboot the cluster node.

```
cluster2::> system node reboot –node cluster2-01
```

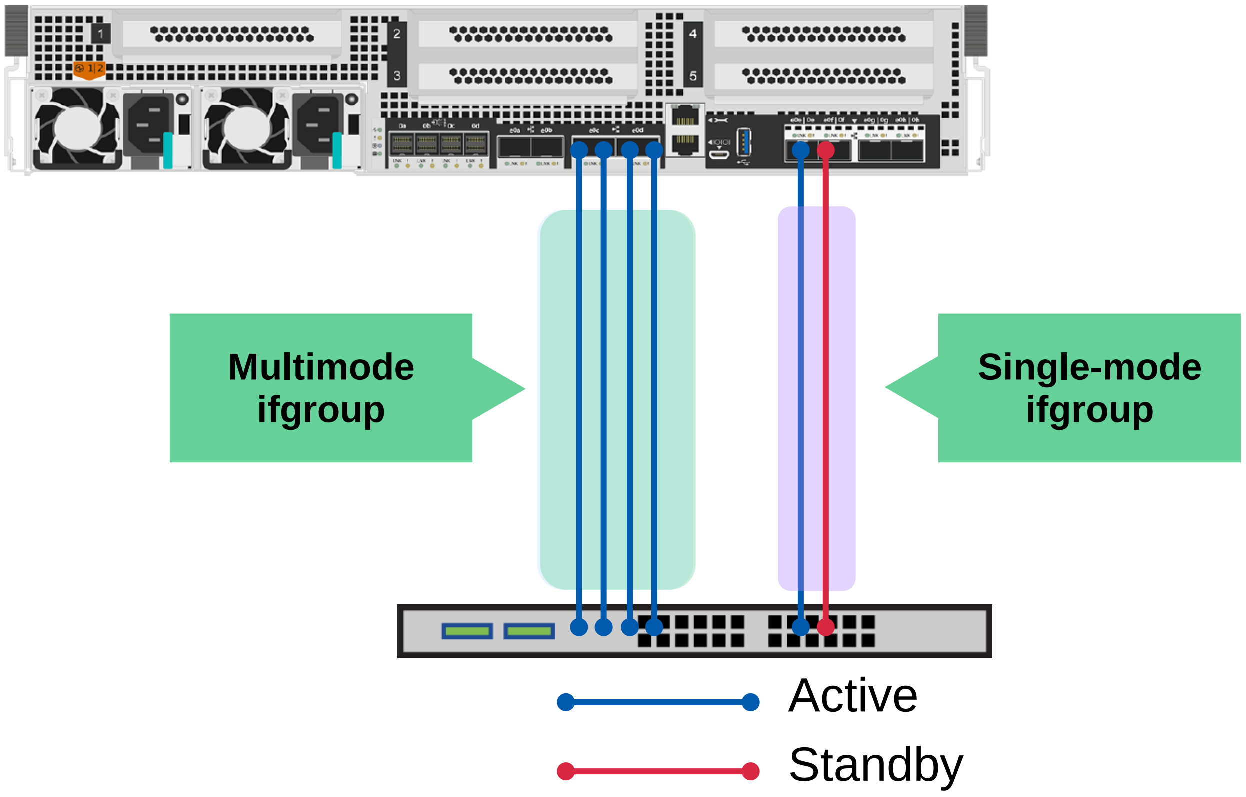

Virtual network ports



Interface groups

- Combination of one or more Ethernet interfaces
- Three ifgroup modes:
  - Single mode (active-standby)
  - Static multimode (active-active)
  - Dynamic multimode with
    Link Aggregation Control Protocol (LACP)
- Naming syntax:
  a <number> <letter>
  (for example, a0a)

NOTE: Vendors might use other terms for combining Ethernet interfaces (for example, Cisco EtherChannel).



Creating interface groups

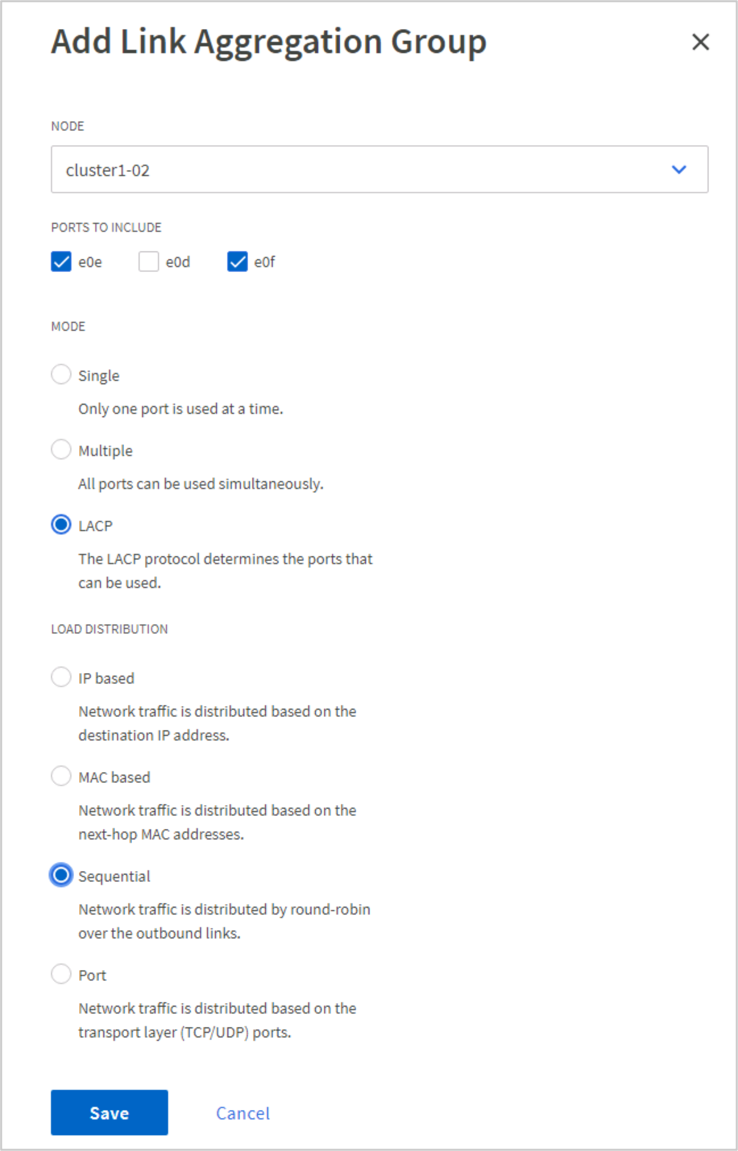
- Create a link aggregation group.

```
cluster2::> network port ifgrp create
-node cluster2-01 -ifgrp a0a
-distr-func ip -mode multimode
```

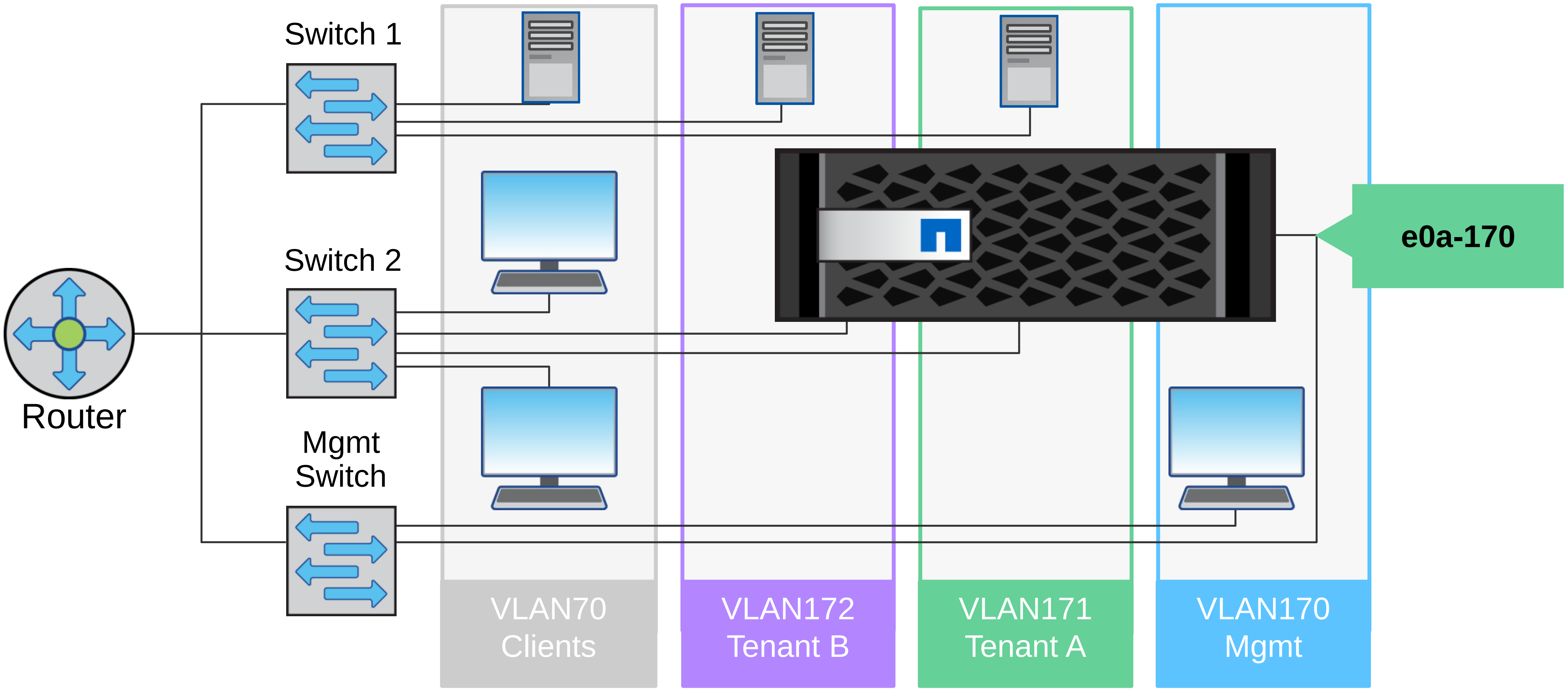
- Assign network ports to the link aggregation group.

```
cluster2::> network port ifgrp add-port
-node cluster2-01 -ifgrp a0a -port e0f
```

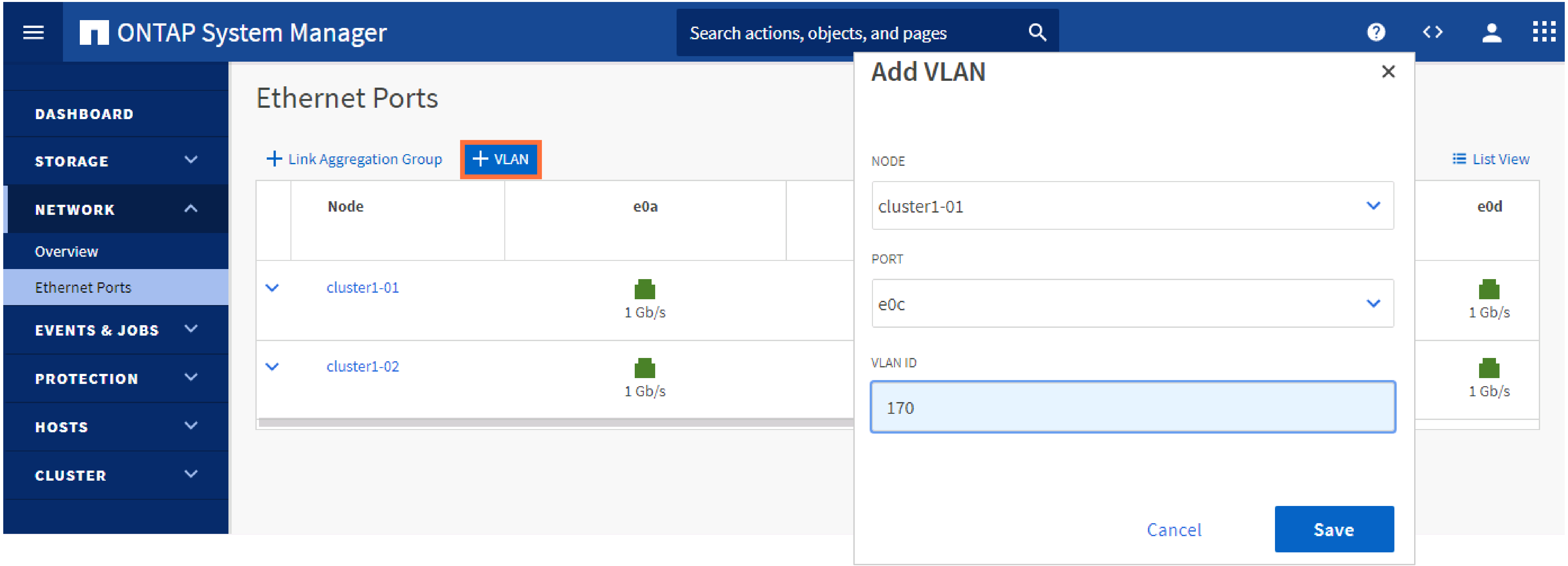
The name of the ifgroup must be in a<*number*><*letter*> format.



VLANs

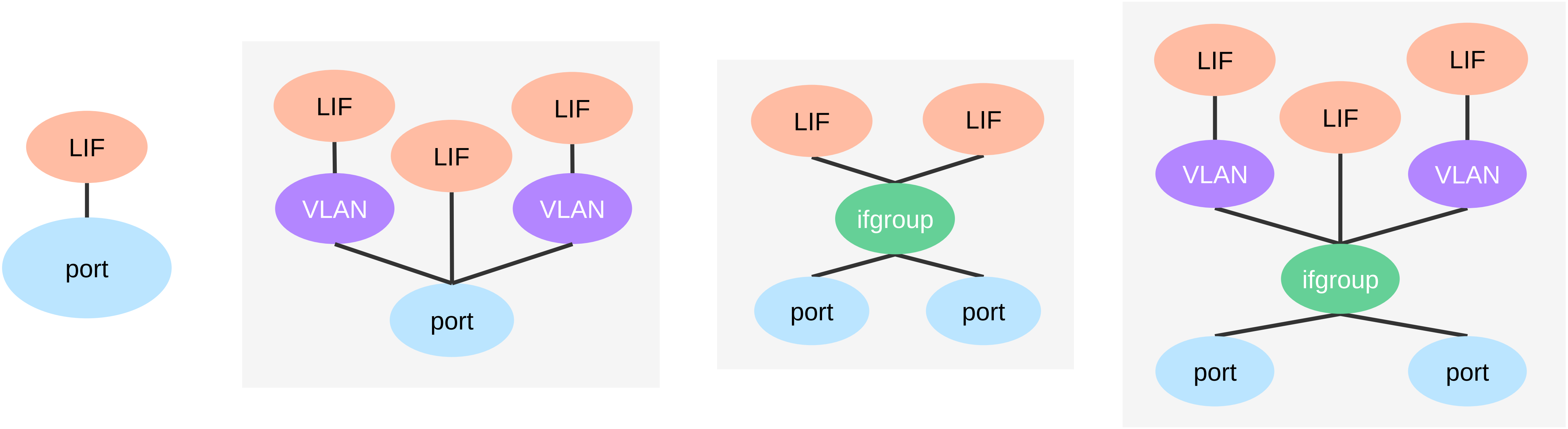

Switch 1
Switch 2
Router
Mgmt Switch
e0a-170
VLAN70 Clients
VLAN172 Tenant B
VLAN171 Tenant A
VLAN170 Mgmt

Creating VLANs



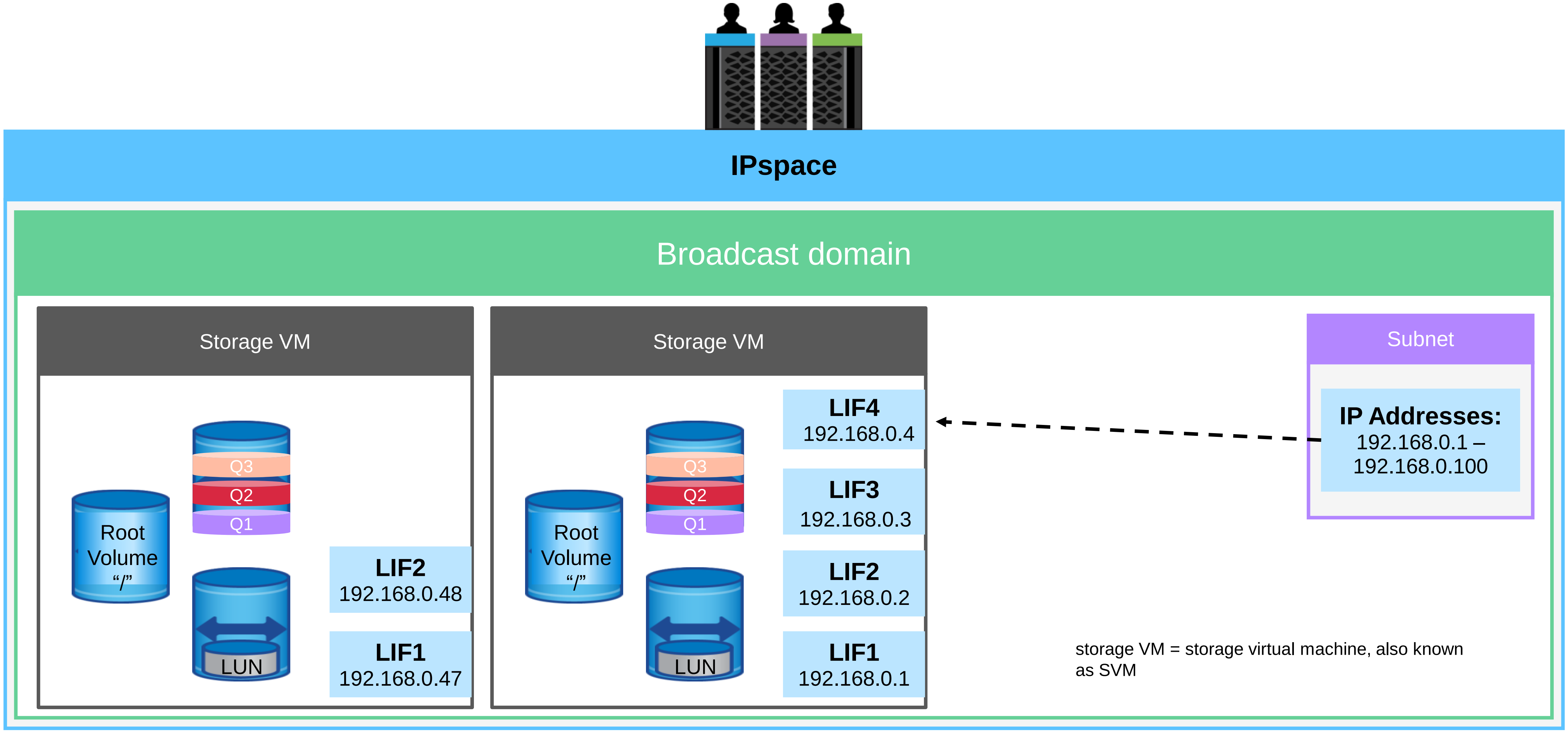

```
cluster2::> network port vlan create -node cluster2-01 -vlan-name a0a-11
```


Ports, ifgroups, and VLAN combinations



Lesson 3
Network traffic segregation

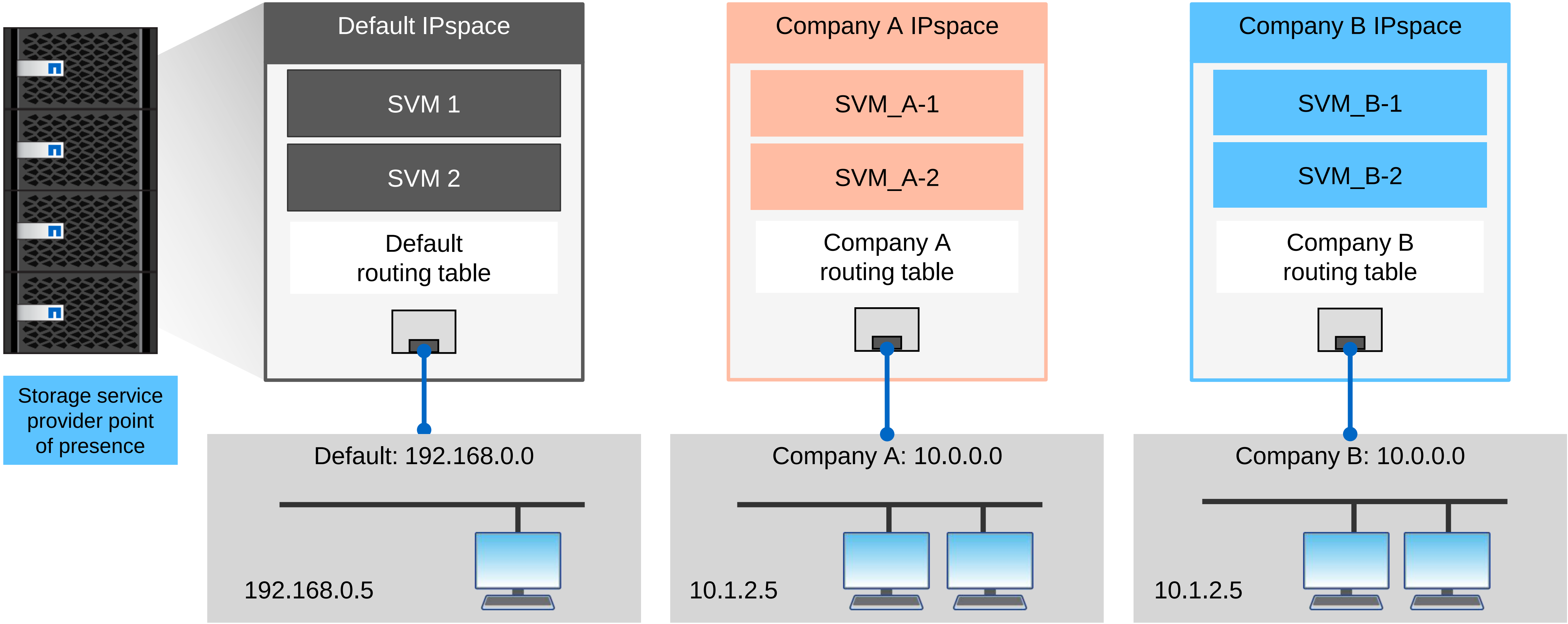
IPspace review



storage VM = storage virtual machine, also known as SVM

IPspace

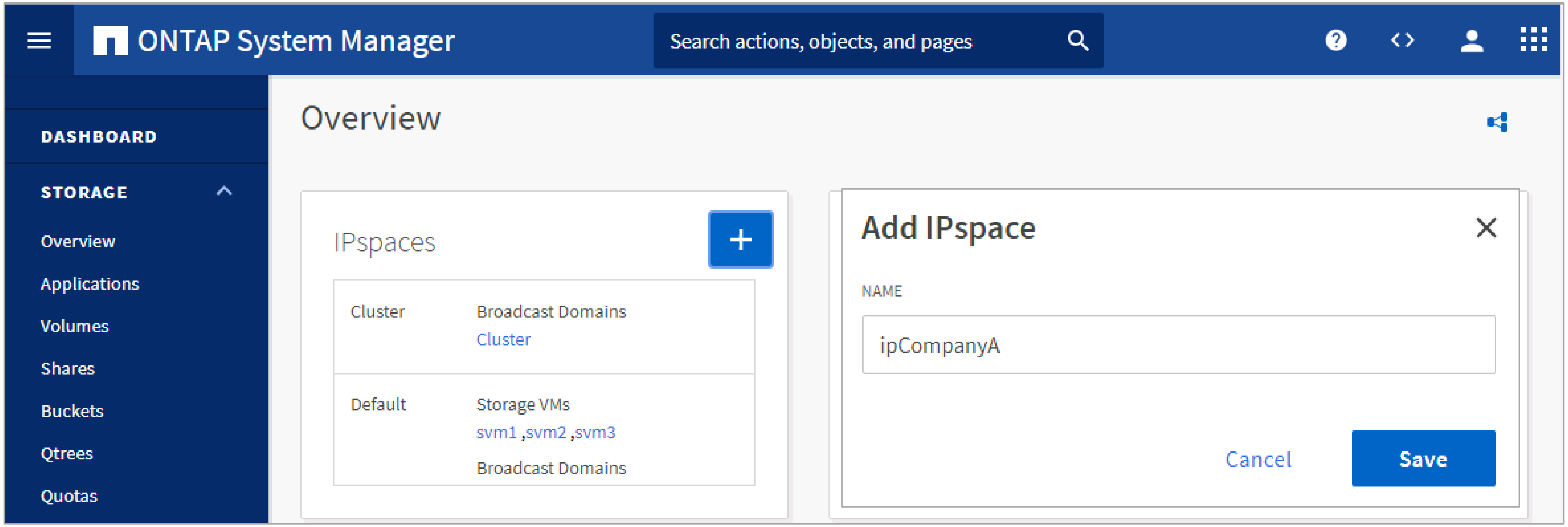
Segregating networks



Managing IPspaces

Create

You can create IPspaces when you need your SVMs to have distinct and secure storage, administration, and routing.

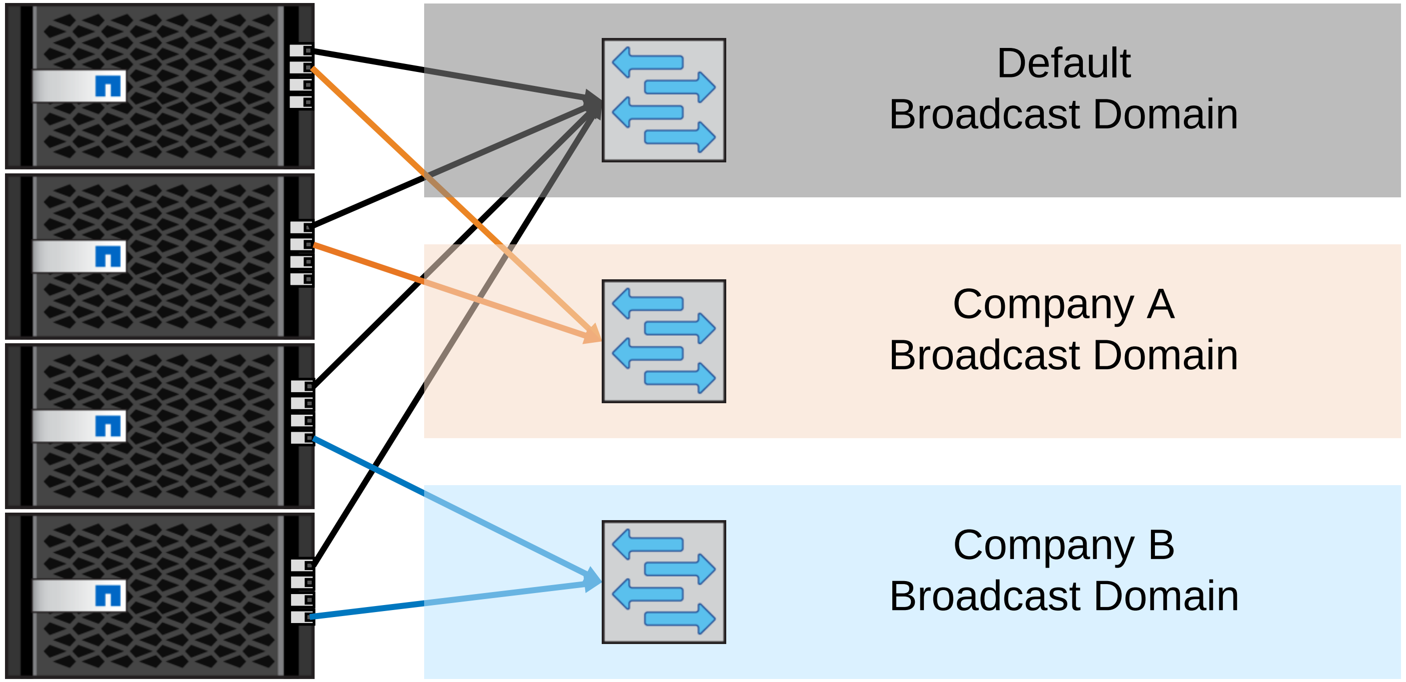



```
cluster1::> network ipspace create -ipspace ipCompanyB
```


Broadcast domains

Overview

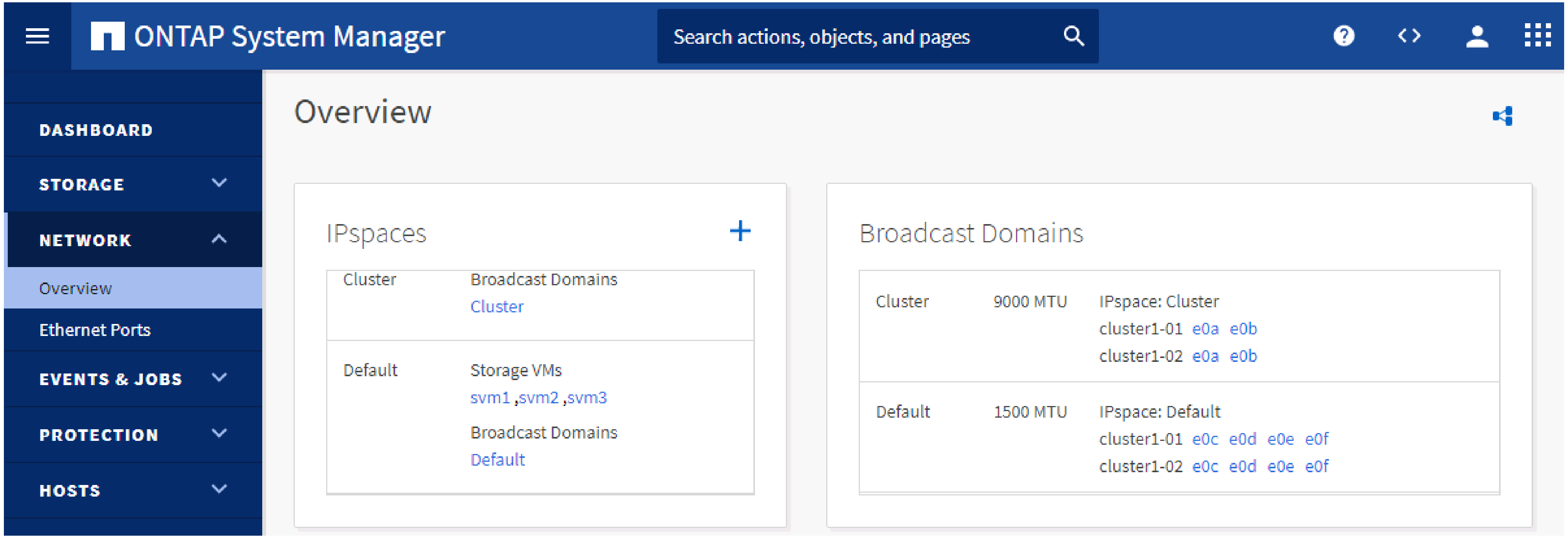
- Broadcast domains enable you to group network ports that belong to the same Layer 2 network.
- An SVM can then use the ports in the group for data or management traffic.



Broadcast domains can contain physical ports, ifgroups, and VLANs.

Broadcast domains

Managing broadcast domains

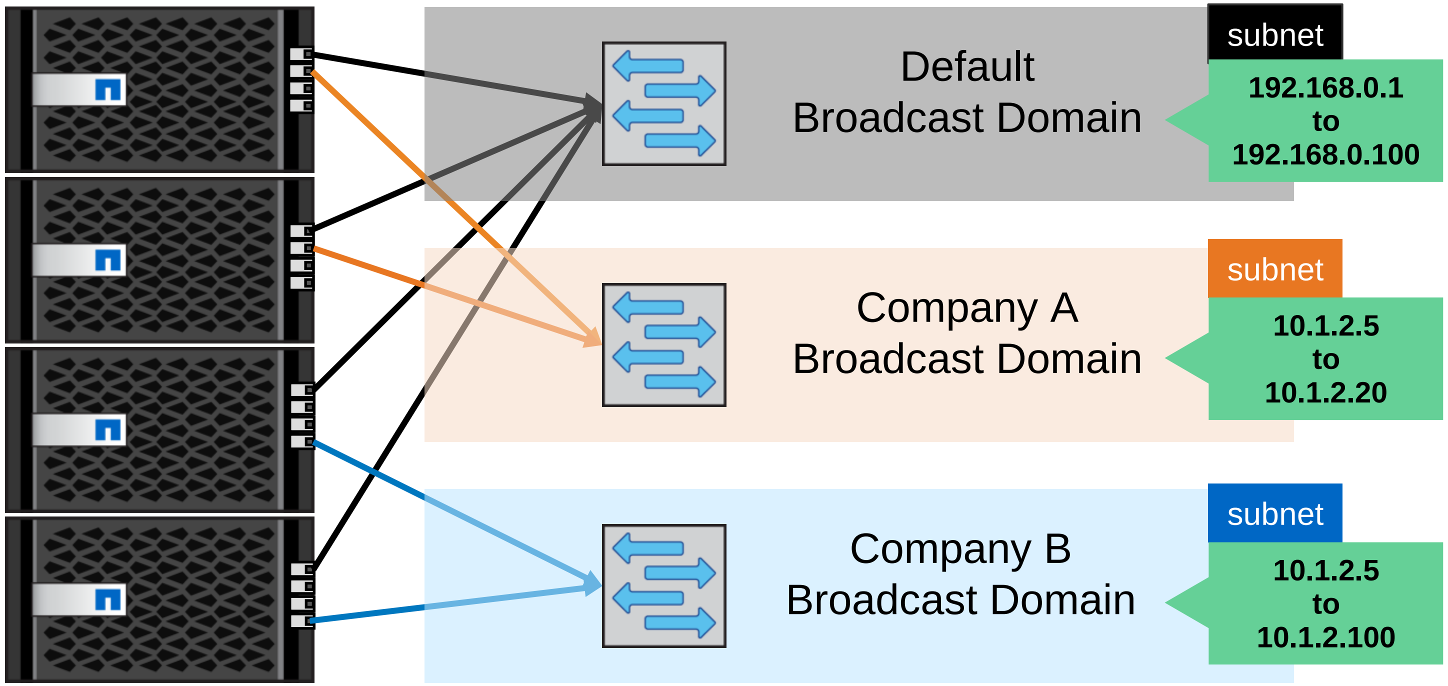


You create broadcast domains to group ports for an IPspace.

```
cluster1::> network port broadcast-domain create -broadcast-domain bdCompanyB -ipspace ipCompanyB
-mtu 1500 -ports cluster1-01:a0a,cluster1-02:a0a
```


Subnets

- Subnets enable the allocation of specific blocks, or pools, of IP addresses for easier LIF creation.
- A subnet is created within a broadcast domain and contains a pool of IP addresses that belong to the same Layer 3 subnet.



Subnets are recommended for easier LIF creation.

Creating subnets

- The broadcast domain and IPspace where you plan to add the subnet must exist.
- Subnet names must be unique within an IPspace.
- IP addresses in the specified range must not be in use by a LIF.
  Use the `–force-update-lif-associations` option to override the rule.

```
cluster1::> network subnet create –subnet-name subnet_A –broadcast-domain bdCompanyB
–ipspace ipCompanyB –subnet 10.1.2.0/24 –gateway 10.1.2.1
-ip-ranges “10.1.2.90-10.1.2.120,10.1.2.155-192.1.2.205” -force-update-lif-associations true
```


Subnets

Verifying subnets

To view subnet details:

```
::> network subnet show
Subnet                       Broadcast           Avail/
Name         Subnet          Domain    Gateway     Total  Ranges
----------- --------------- --------- ------------ ------ ------
subnet_def  192.168.0.0/24  Default   192.168.0.1  10/50  192.168.0.101-192.168.0.150
subnet_A    10.1.2.0/24     bd_A      10.1.2.1     4/51   10.1.2.90-10.1.2.140
subnet_B    10.1.2.0/24     bd_B      10.1.2.1     4/51   10.1.2.90-10.1.2.140
```

Subnets A and B have the same subnet address and gateway but different domains.

Notice how subnets A and B use overlapping IP ranges.

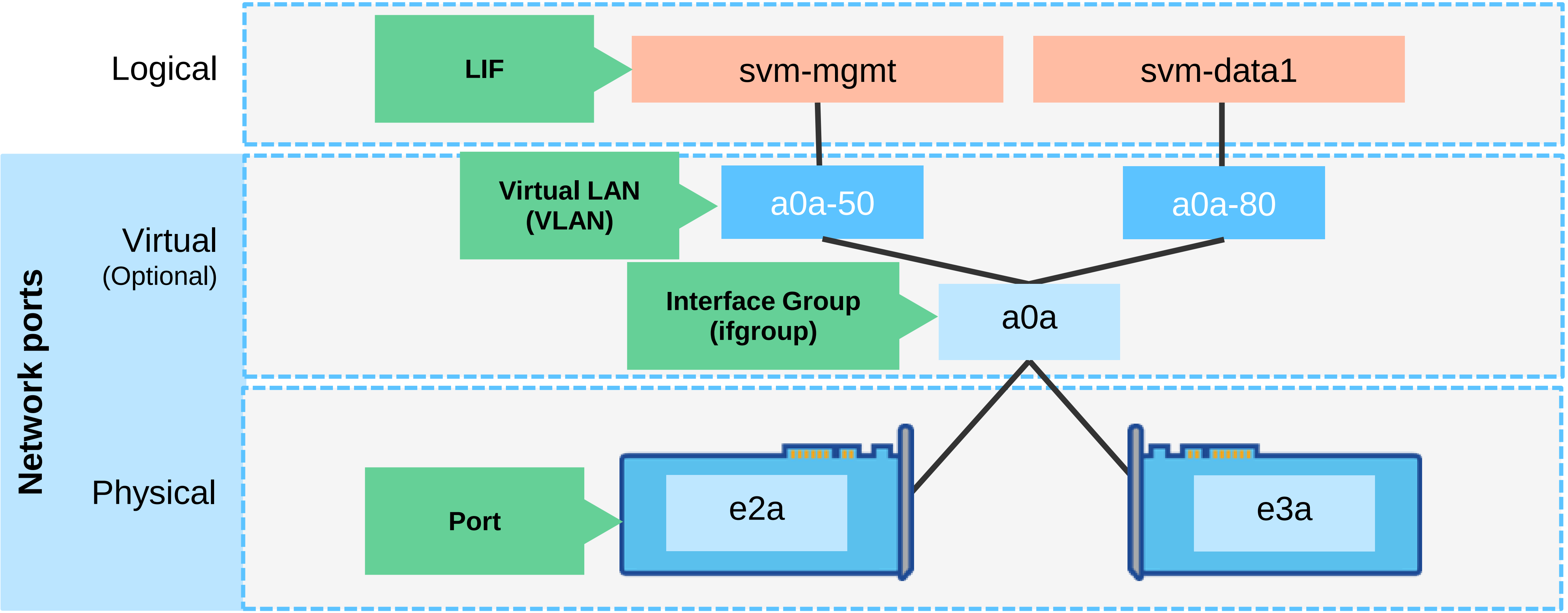
Topic for discussion

When do you need to create IPspaces, broadcast domains, or subnets?

Lesson 4
LIFs

Network interfaces

Review



Logical network interfaces

- An IP address or worldwide port name (WWPN) is associated with a LIF:
  - If subnets are configured (recommended), an IP address is automatically assigned when a LIF is created. Otherwise, IP addresses must be manually assigned.
  - When an FC LIF is created, WWPNs are automatically assigned.
- One node-management LIF exists per node.
- One cluster-management LIF exists per cluster.
- Cluster LIFs depend on the cluster configuration.
- Multiple data LIFs can be enabled per port (client-facing for NFS, CIFS, S3, iSCSI, and FC access).
- For intercluster peering, intercluster LIFs must be created on each node.

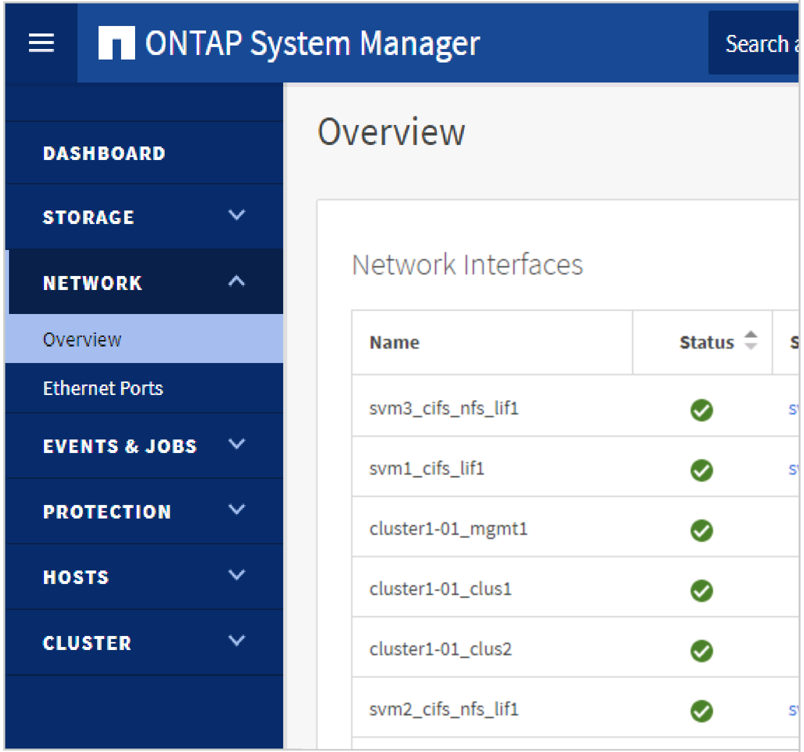
Creating data LIFs

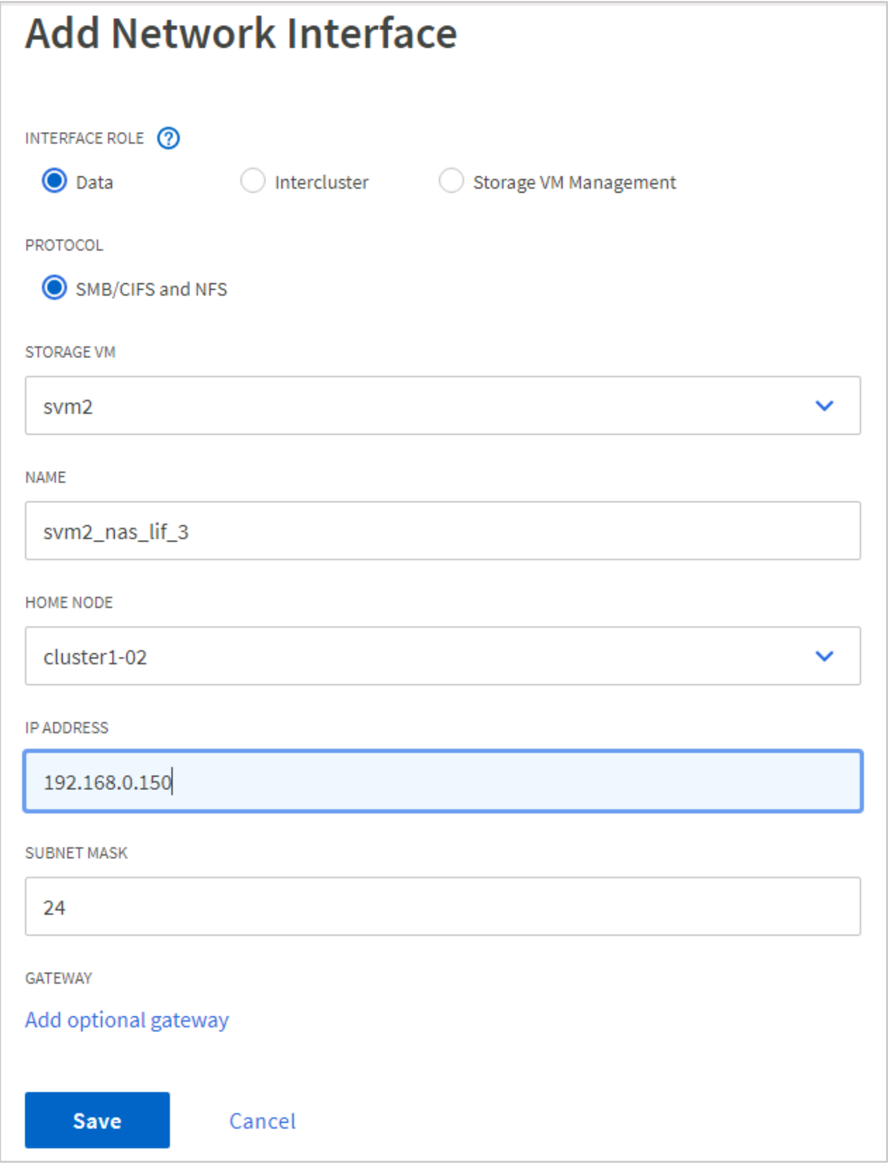
- Manually assign an IP address when creating a NAS LIF by using ONTAP System Manager.

  The subnet mask is determined automatically.

- Specify the subnet name to automatically assign an IP address when creating a NAS LIF by using the CLI.

  You must specify the IP address when subnets are not configured.





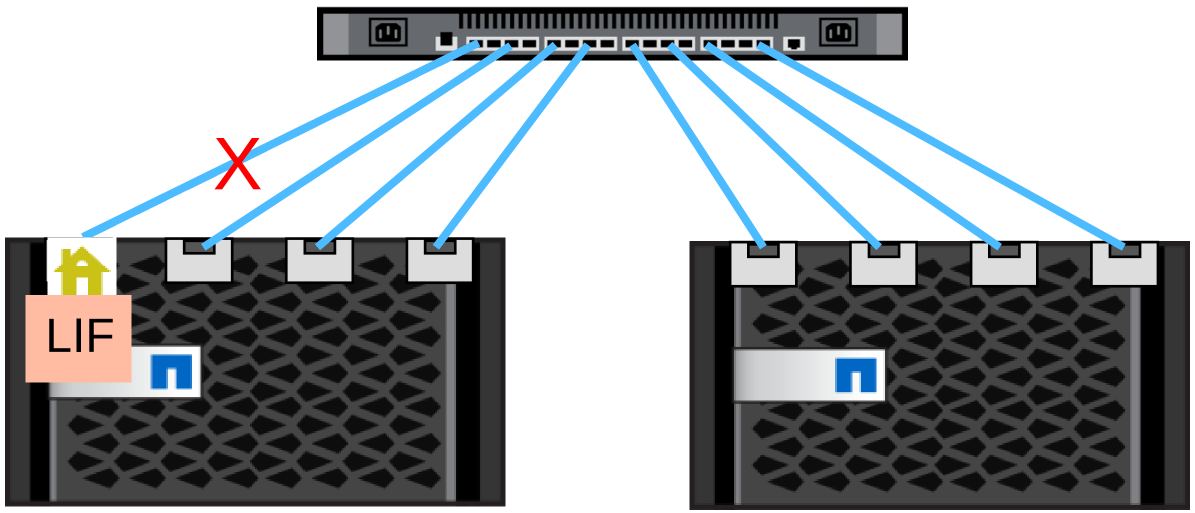

```
cluster1::> network interface create -vserver svm3
-lif svm3_nfs_lif2 -data-protocol nfs
-home-node cluster1-01 -home-port e0f -subnet-name sn_svm3
```


Lesson 5
Nondisruptive LIF configuration

Nondisruptive LIF features

LIF failover

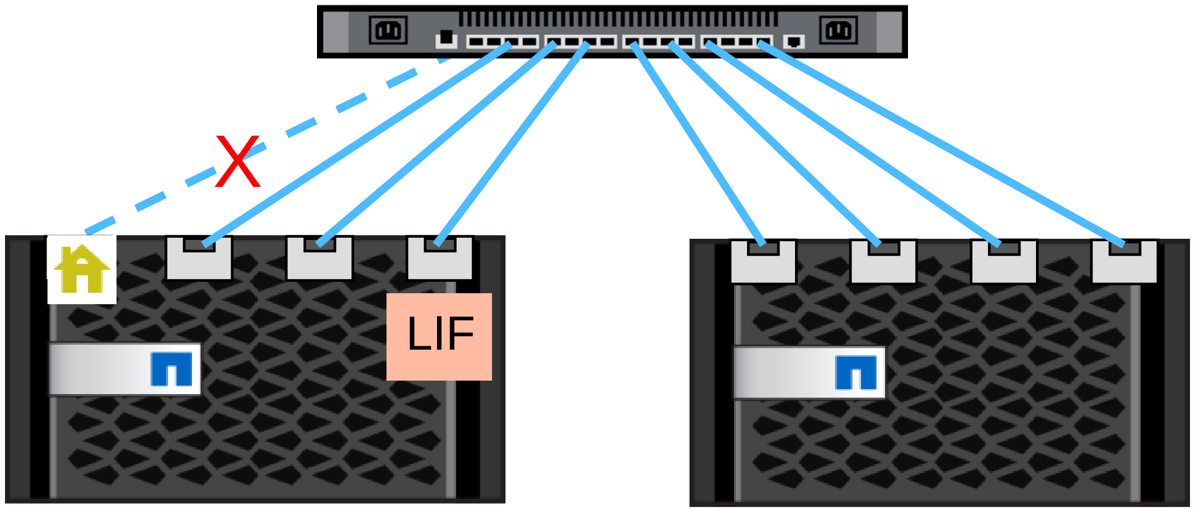
- **LIF failover**: Automatic migration that occurs because of a link failure or reboot



Nondisruptive LIF features

LIF migrate

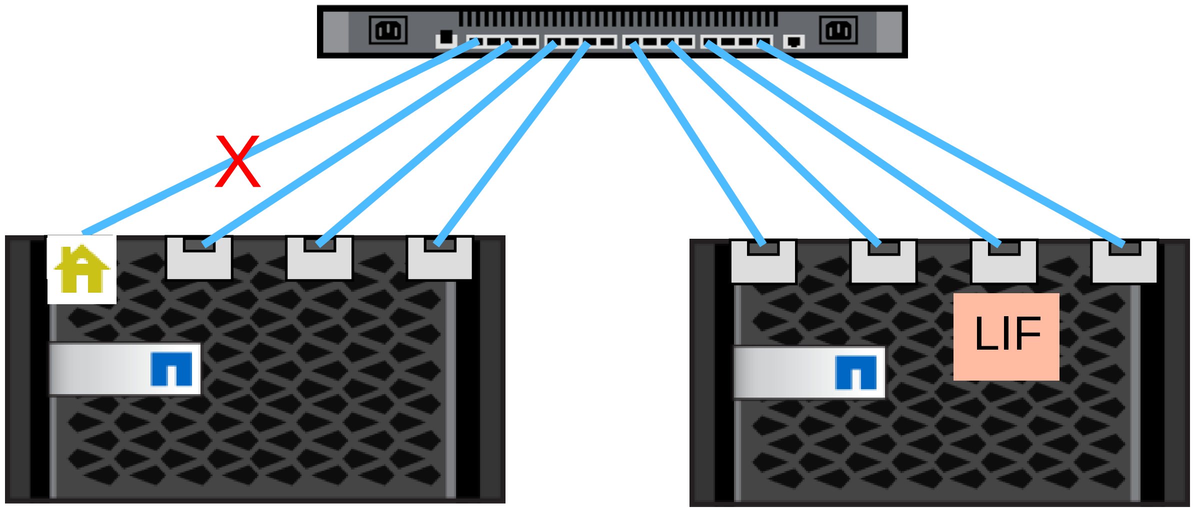
- **LIF failover**: Automatic migration that occurs because of a link failure or reboot
- **LIF migrate**: Manual movement of a LIF to another port



Nondisruptive LIF features

LIF revert

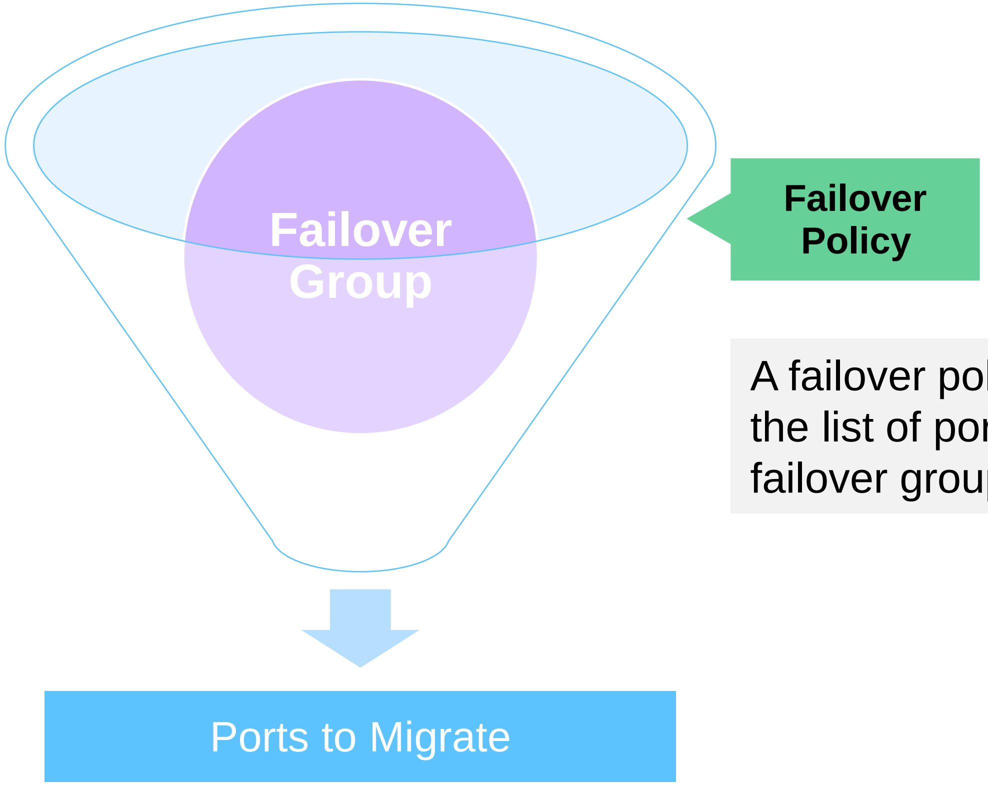
- **LIF failover**: Automatic migration that occurs because of a link failure or reboot
- **LIF migrate**: Manual movement of a LIF to another port
- **LIF revert**: Manual or automatic sending of a LIF back to the home node and home port



Failover groups versus failover policies

A failover group is a list of ports (physical or virtual):

- Defines the targets for the LIF
- Is automatically created when you create a broadcast domain
- Does not apply to iSCSI or FC SAN LIFs



A failover policy restricts the list of ports within a failover group.

Failover groups

Failover groups are created automatically, based on the network ports in the broadcast domain:

1

A **Cluster failover** group contains all the ports in the Cluster broadcast domain.

2

A **Default failover** group contains all the ports in the Default broadcast domain.

3

Additional **failover groups** are created for each broadcast domain that you create.

Custom failover groups

You create custom failover groups for specific LIF failover functionality
in one or more of the following circumstances:

- The automatic failover groups do not meet your requirements.
- You require only a subset of the ports that are available in the broadcast domain.
- You require consistent performance.

  For example, you have configured SnapMirror replication to use high-bandwidth ports.
  You might create a failover group that consists of only 25-GbE ports to ensure that the LIFs fail over to only high-bandwidth ports.

? More info in Addendum

Failover policies

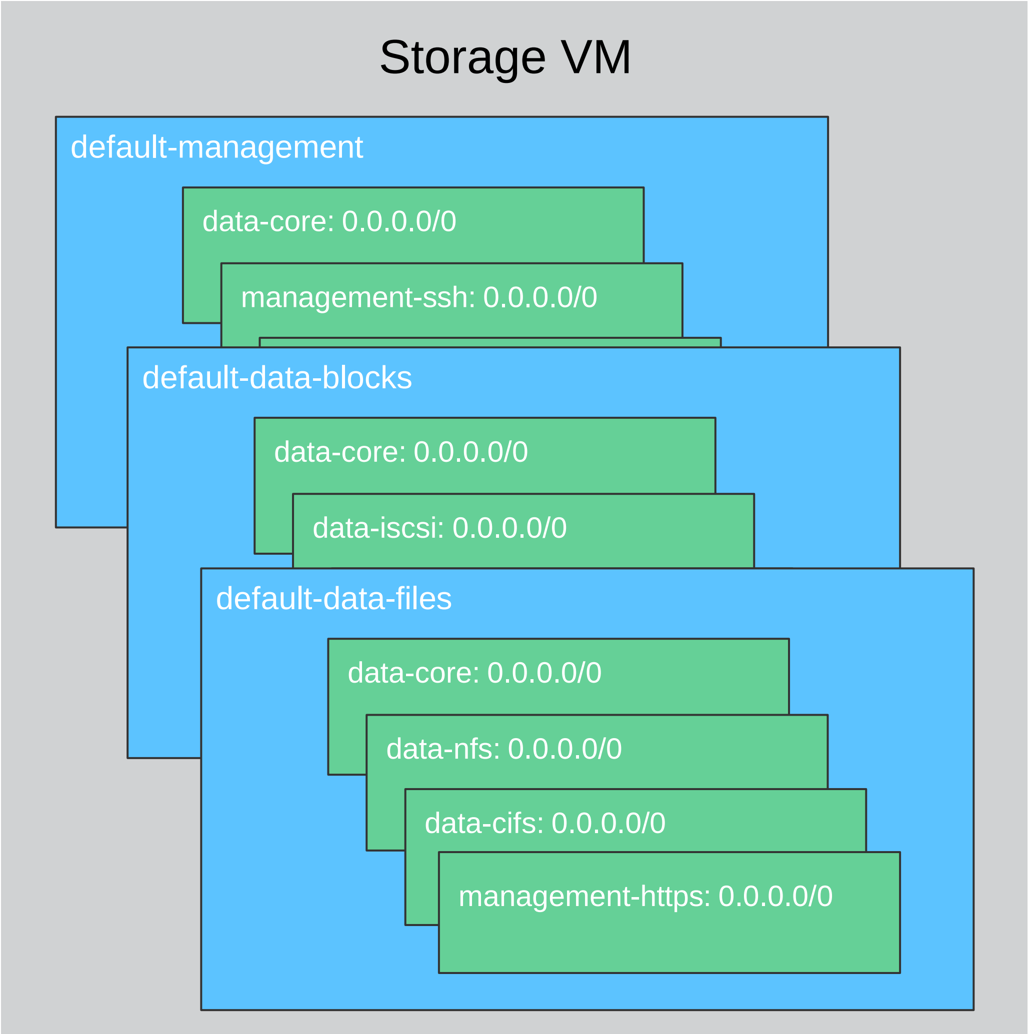
Failover policy	Available target ports	Details
broadcast-domain-wide	The LIF fails over to any port from any node in the failover group.	Default for cluster-management LIF
system-defined	The LIF fails over to only a port on the home node or a non-storage failover (SFO) partner.	Default for data LIFs *Recommended for nondisruptive software updates*
local-only	The LIF fails over to only a port on the home node of the LIF.	Default for cluster LIFs, node management LIFs, and intercluster LIFs
disabled	Failover is disabled for the LIF.	LIF that is not configured for failover

Failover policies and groups

LIF name	LIF type	LIF service policy	Default failover group	Default failover policy
Clus1	cluster	default-cluster	Cluster	local-only
cluster1-01_mgmt1	node management	default-management	Default	local-only
cluster_mgmt	cluster management	default-management	Default	broadcast-domain-wide
svm1_nas_lif01	data	default-data-files	Default	system-defined

Network service policies

- Many ONTAP network services are accessible through logical network interfaces.
- The network service policy defines which network services to provide and from which network addresses to accept requests.
- Each storage VM has its own set of network service policies.
- The network service policy is assigned to a LIF when the LIF is created.



Topic for discussion

- What are the benefits of each type of failover group and failover policy type?
- When should you use ifgroups or failover groups? Do you need both?

Lesson 6
Routing management

Routing management

Overview

You control the outbound traffic of LIFs by configuring route tables and static routes.

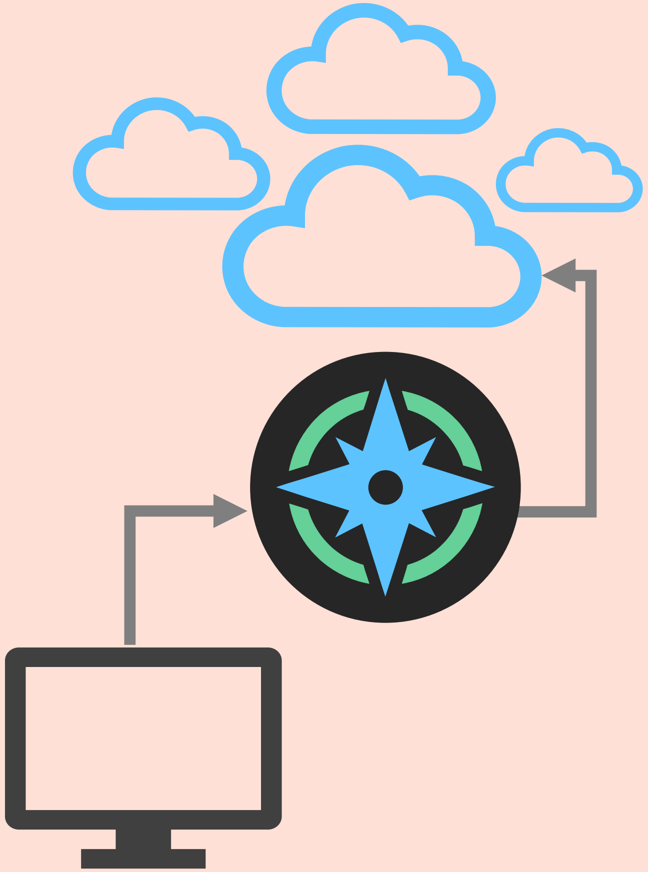
The following is true of route tables:

- Route tables are routes that are automatically created in an SVM when a service or application is configured for the SVM.
- Routes are configured for each SVM, identifying the SVM, subnet, and destination.
- Route tables are per SVM, so routing changes to one SVM do not pose a risk of corrupting another SVM route table.
- The system SVM of each IPspace has its own route table.

Routing management

Static routes

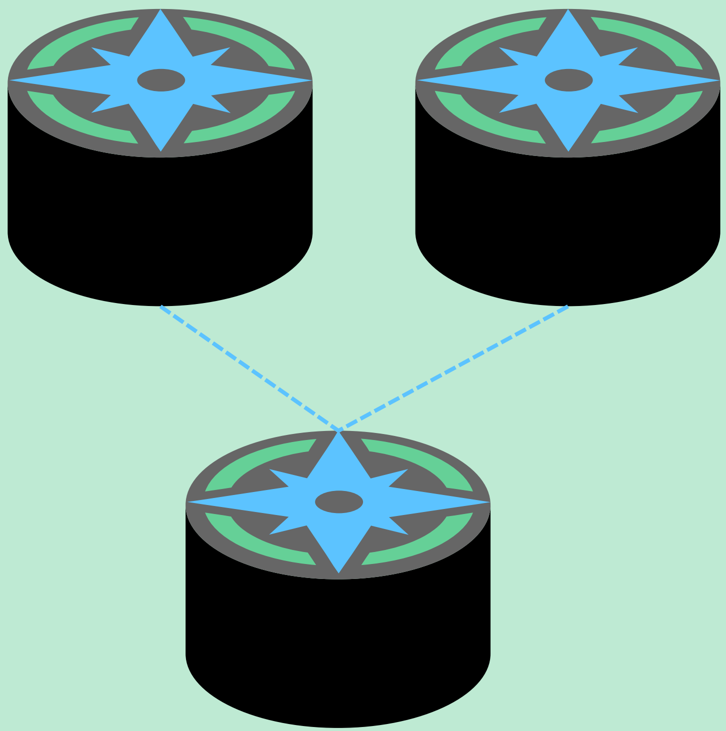
- A static route is a defined route between a LIF and a specific destination IP address.
- The route can use a gateway IP address.
- A static default route to the destination gateway is automatically added to the routing table of the SVM if the following is true:
  1. A default gateway is defined when you create the subnet.
  2. A LIF from the subnet is assigned to an SVM.



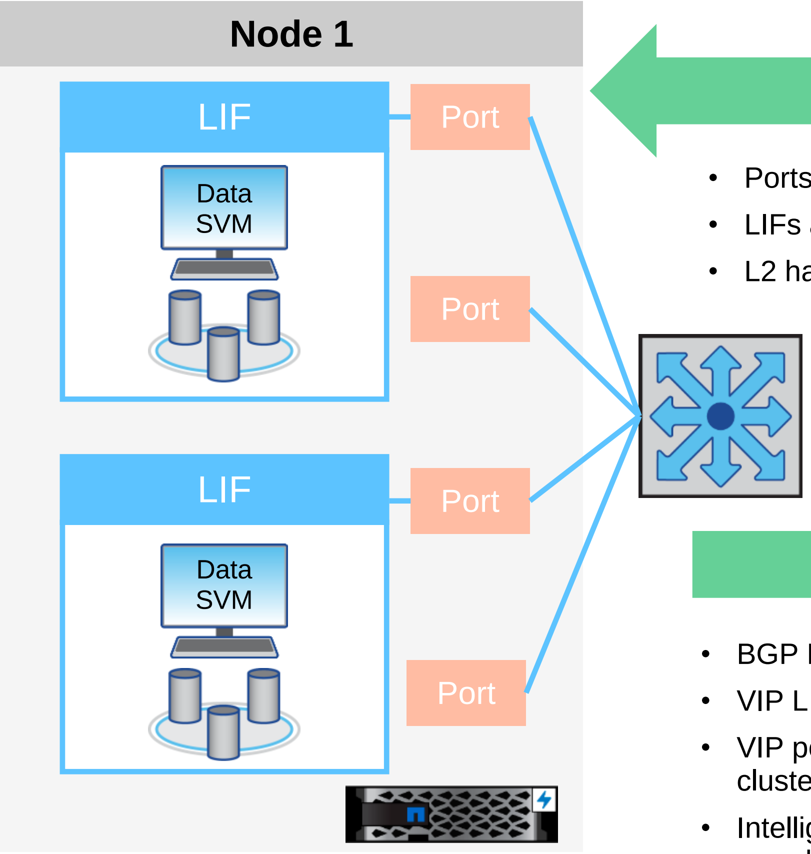
? More info in Addendum

Border Gateway Protocol routing

- ONTAP 9.5 and later software supports Layer 3 (L3) routing through Border Gateway Protocol (BGP).
- Previous ONTAP versions used Layer 2 (L2) routing, which creates hash tables of routes based on “distance.” The fewest hops between two points is assumed to be the preferred route.
- Layer 3 routing with BGP uses metrics to pick routes based on measurements like latency and bandwidth availability.
- Support for BGP also enables the separation of LIFs from the physical hardware and makes them entities of the network that are called virtual IPs (VIPs).



BGP and VIP LIFs

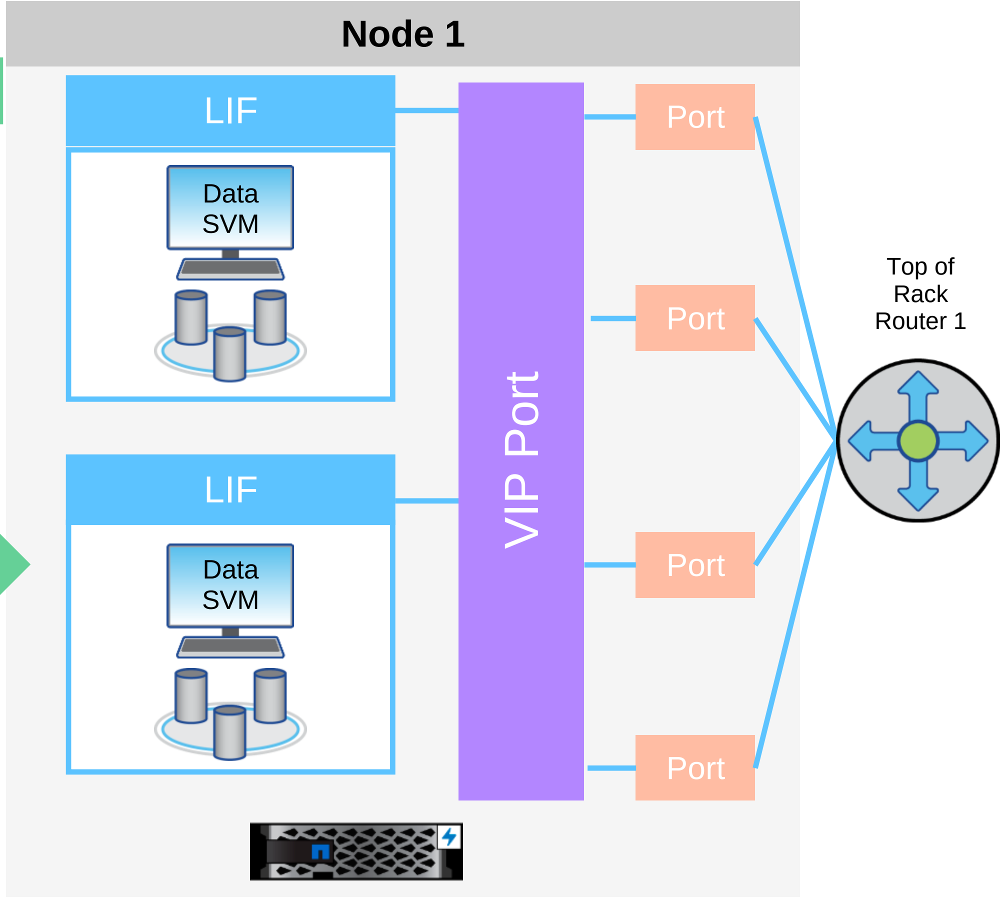


Traditional Data LIFS

- Ports belong to a specific node.
- LIFs are hosted on a single port.
- L2 hashing is used to load balance.

BGP VIP LIFs

- BGP LIFs act as another network layer.
- VIP LIFs live on VIP ports.
- VIP ports are not limited to physical ports or cluster nodes.
- Intelligent L3 routing uses metric-based round robin.



? More info in Addendum

Host-name resolution

Two methods support host-name resolution: DNS and hosts tables.

- You configure DNS and the hosts table in the admin SVM.
  - When you set up the cluster, you should configure DNS.
  - As nodes join the cluster, configurations are propagated to each node.
  - By default, the order of lookup is hosts table and then DNS.
- Cluster and SVM administrators can configure DNS in a data SVM.
- Each SVM has its own DNS and hosts table configuration.

? More info in Addendum

References

- NetApp Hardware Universe
  http://hwu.netapp.com

- ONTAP 9 Documentation Center
  http://docs.netapp.com/ontap-9/index.jsp
  - *Network Management Guide*
  - *ONTAP 9 Concepts*
  - *System Administration Reference*

- ONTAP System Manager Documentation Center
  https://docs.netapp.com/us-en/ontap/index.html

- TR-4182: Ethernet Storage Best Practices for ONTAP Configurations
  https://www.netapp.com/us/media/tr-4182.pdf

Knowledge check

Module 4: Network management

Knowledge check

Which statement about LIFs is true?

a. One cluster-management LIF exists per node.

b. One port can host multiple data LIFs.

c. Cluster LIFs and data LIFs can share a port.

d. A data LIF can be associated with multiple SVMs.

Knowledge check

Which statement about LIFs is true?

a. One cluster-management LIF exists per node.

b. One port can host multiple data LIFs.

c. Cluster LIFs and data LIFs can share a port.

d. A data LIF can be associated with multiple SVMs.

Knowledge check

Which statement about LIF failover policies is true?

a. Failover policies are assigned to failover groups.

b. Failover policies can be created to control LIF failover behavior.

c. Failover policies define how ports are selected during LIF failover.

d. Failover policies define how LIFs are assigned to failover groups.

Knowledge check

Which statement about LIF failover policies is true?

a. Failover policies are assigned to failover groups.

b. Failover policies can be created to control LIF failover behavior.

c. Failover policies define how ports are selected during LIF failover.

d. Failover policies define how LIFs are assigned to failover groups.

Module summary

This module focused on enabling you to do the following:

- Describe the interaction between physical and virtual network resources in a cluster
- Configure and manage physical and virtual networking resources

Complete an exercise

Module 4
Network management

Managing physical and logical network resources

Managing virtual network resources

- Access your lab equipment.
- Open your Exercise Guide, Module 4.
- Complete Exercises 1 and 2.
- Share your results.

This exercise requires approximately
35 minutes.

Addendum
Failover group commands

Failover

Managing failover groups and LIFs

Create a failover group:

```
::> net int failover-groups create –vserver svm4 –failover-group fg_svm4
-targets cluster1-01:e0f,cluster1-02:e0f
```

Add or remove targets from a failover group:

```
::> network interface failover-groups add-targets
::> network interface failover-groups remove-targets
```

Configure failover for an existing LIF:

```
::> net int modify –vserver svm4 –lif svm4_nfs_lif1
–failover-group fg_svm4 –failover-policy broadcast-wide-domain
```


Addendum
Routing management commands

Routing management

Managing routes

Create a static route:

```
::> network route create -vserver svm4 -destination 0.0.0.0/0
-gateway 192.168.0.1
```

Delete a static route:

```
::> network route delete -vserver svm4 -destination 0.0.0.0/0
-gateway 192.168.1.1
```

Display static routes:

```
::> network route show
Vserver  Destination    Gateway      Metric
-------- ------------   -----------  -------
svm4     0.0.0.0/0      192.168.0.1  20 ...
```


Host-name resolution

Configuring data storage VMs

Create a hosts table entry:

```
::> vserver services name-service dns hosts create -vserver svm4
-address 192.168.0.11 -hostname test.example.com -alias test
```

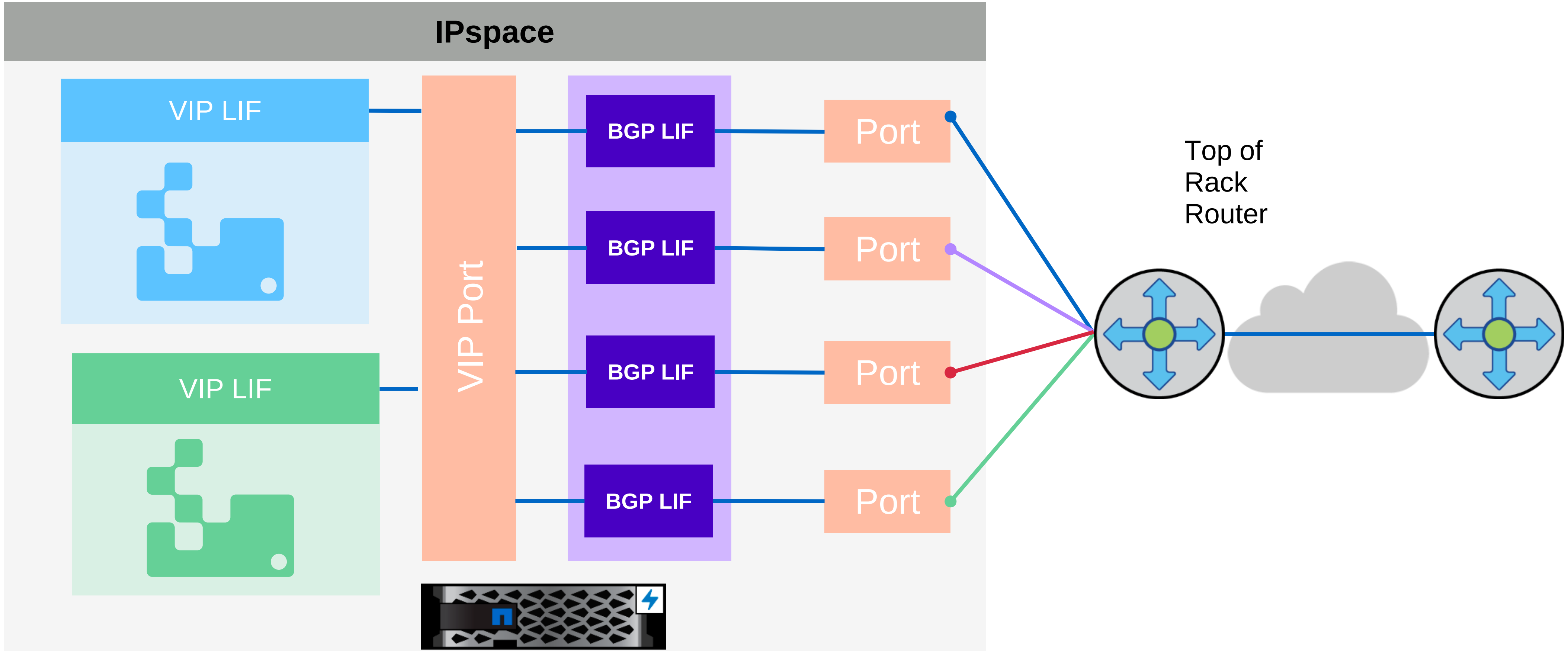
Configure DNS:

```
::> vserver services name-service dns create -vserver svm4
-domains example.com -name-servers 192.168.0.11
```


Addendum
BGP and VIP LIFs

BGP virtual IP

Full link use, direct cross-data-center traffic, and failure resiliency with a routed topology, including BGP support



Configuring BGP and VIP LIF

Setting up BGP

1. Create a BGP configuration.
2. Create a BGP LIF.
3. Create a BGP peer group.

Creating a VIP LIF

1. Create a VIP data LIF.
2. Verify the BGP session.

Setting up BGP

Example workflow

Create a BGP configuration (advanced command):

```
cluster1::*> network bgp config create -node node1 -asn 65502
-holdtime 180 -routerid 1.1.1.1
```

Create a BGP LIF:

```
cluster1::> network interface create -vserver cluster1 -lif bgp1
-service-policy net-route-announce -home-node cluster1-01 -home-port e0c
-address 10.10.10.100 -netmask 255.255.255.0
```

Create a BGP peer group (advanced command):

```
cluster1::*> network bgp peer-group create -peer-group group1
-ipspace Default -local-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65502 -route-preference
100
```


Create VIPs

Example workflow

Enable multipath routing (advanced command):

```
::*> network options multipath-routing modify -is-enabled true
```

Create a VIP data LIF:

```
::> network interface create -vserver vs34 -lif vip1 -is-vip true
-data-protocol cifs,nfs,fcache -service-policy default-data-files
-home-node gw-node1 -address 3.3.3.3
```

Verify that the BGP session is in `up` status:

```
::> network bgp vserver-status show

            Node        Vserver  bgp status
            ----------  -------- ---------
            node1       vs1      up
```

