

**cDOT 8.3.x Networking**

**Authors:** Ian Daniel

**Contributors:**

**Document Version:** V0.5

**Date:** January 2017

Status: Draft

**CONFIDENTIAL INFORMATION**

This document contains information proprietary to Thomson Reuters and may not be reproduced, disclosed or used in whole or part without express permission of Thomson Reuters.

© Thomson Reuters 2017

Contents

[1 Introduction 3](#_Toc471205908)

[1.1 Management Summary 3](#_Toc471205909)

[1.2 Change History 3](#_Toc471205910)

[1.3 Distribution List 4](#_Toc471205911)

[1.4 Glossary 4](#_Toc471205912)

[2 Network Configuration 5](#_Toc471205913)

[2.1 Description 5](#_Toc471205914)

[2.2 Network Interfaces 5](#_Toc471205915)

[2.3 VLANs 5](#_Toc471205916)

[2.4 Cluster IP Spaces 5](#_Toc471205917)

[2.5 Broadcast Domains 6](#_Toc471205918)

[2.6 Dual Homing Controllers 6](#_Toc471205919)

[3 Example Additional Network Configuration 7](#_Toc471205920)

[3.1.1 Description 7](#_Toc471205921)

[3.1.2 Backup Cluster Network Configuration (Example) 7](#_Toc471205922)

[3.1.3 Backup Cluster Port Allocation 7](#_Toc471205923)

[3.1.4 ICL Creation 8](#_Toc471205924)

[3.1.5 Cluster Peering 9](#_Toc471205925)

# Introduction

## Management Summary

This document details the process used to configure networks in cDOT.

## Change History

|  |  |  |  |
| --- | --- | --- | --- |
| **Ver** | **Date** | **Author** | **Key Changes** |
| 0.1 | October 2016 | Ian Daniel | Initial Version |
| 0.2 | December 2016 | Ian Daniel | Re-worked to take upgraded systems into account. |
| 0.3 | January 2017 | Ian Daniel | Updated to add broadcast domains and address other comments. |
| 0.4 | January 2017 | Ian Daniel | Updated to address other comments. |
| 0.5 | January 2017 | Ian Daniel | Updated to address other comments. |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Distribution List

|  |  |
| --- | --- |
| **Name** | **Role** |
| Storage Engineering | Reviewer |
| Storage Delivery | Reviewer |
| Storage Architecture | Reviewer |

## Glossary

|  |  |
| --- | --- |
| **Term** | **Definition** |
| cDOT | clustered Data ONTAP |
| Vserver | A logical storage virtual server, also known as a Storage Virtual Machine (SVM), which contains LIFs, Volumes, and configuration information such as access control details. |
| LIF | Logical Interface – a cDOT logical network interface with an IP address, assigned to a single Vserver. |
| CIFS | Short for Common Internet File System, a protocol that defines a standard for remote file access using millions of computers at a time. With CIFS, users with different platforms and computers can share files without having to install new software. |
| SMB | Short for Server Message Block, a message format used by DOS and Windows to share files, directories and devices. |
| NFS | A distributed file system protocol originally developed by Sun Microsystems in 1984, allowing a user on a client computer to access files over a computer network much like local storage is accessed. |

# Network Configuration

## Description

In certain cases, we connect primary and backup clusters to multiple networks. In order to ensure this doesn’t cause any issues with ICLs and to also provide a partition between management and data networks we use IP Spaces and Broadcast domains to segregate traffic on the cluster nodes.

**Note:** When upgrading from 8.2.3P5 any existing vservers will automatically be put into the default IP Space and there is no facility to move them afterwards. Moving volumes between vservers will only be possible after ONTAP 9.x is in use at TR.

## Network Interfaces

In order to dual home a controller you will need spare interfaces capable of being attached to the additional network you want to have access to. The diagram below shows a possible configuration.



## VLANs

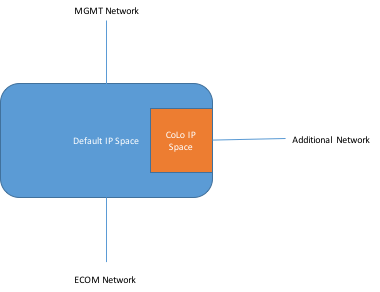
Part of our network design involves the use of VLANS. These are created on the physical interfaces (normally an ifgrp) and it is these interfaces that are added to the relevant Broadcast Domain and by association an IP Space. The actual physical ifgrp interface is **NOT** added to any IP Space we only use the tagged interfaces for data.

In addition VLANs can be moved between different broadcast domains should the need arise.

## ****Cluster IP Spaces****

In ensure network traffic in clusters only travels on the relevant networks (COLO and ECOM from the above example) you need to use IP Spaces and broadcast domains. Note that the FIRST network we attach to the controller will be put into the default IP Space. This ensures new builds match any upgraded systems and creates a standard configuration for TR.

The diagram below shows how this would work. In this case the first network is ECOM, that will not always be the case.



## ****Broadcast Domains****

Broadcast domains are used to limit traffic to LIFs as and when required. These are not a replacement for a failover group like we have in 8.2.x. When upgrading to 8.3.x broadcast domains are created but you will still have a corresponding failover group.

So, for the Default IP Space you will end up with 3 main broadcast domains which are:

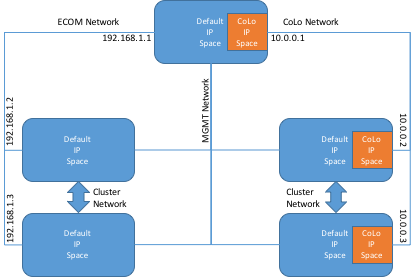
* Management – Node and cluster mgmt interfaces
* Cluster – Interconnect interfaces.
* Data Network – The first network to which the controller is attached.

## ****Dual Homing Controllers****

By default, we get a IP Space when the systems are built which is the default IP Space and this has an associated Broadcast Domain. We use this IP Space for management traffic as shown above. Management traffic will be contained within its own broadcast domain.

All data traffic for the first network attached will be in the same Default IP Space but again in its own broadcast domain. The next network we attach gets its own IP Space and is separate to the first network. This is how we enable dual homed backups.

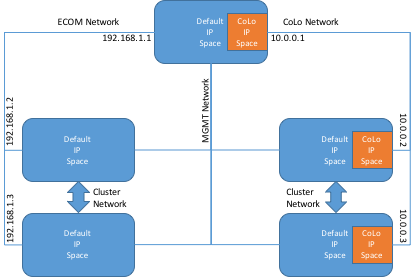
The following diagram shows an example of a dual homed backup controller and the primary clusters connecting to it.



# Example Additional Network Configuration

### Description

Taking this example, we would create the IP Spaces and Broadcast Domains as follows when adding CoLo.



### Backup Cluster Network Configuration (Example)

Create 1 x IP Space:

ipspace create colo-ipspace-01

Create 1 x Broadcast Domains:

broadcast-domain create -broadcast-domain colo -mtu 1500 -ipspace colo-ipspace-01

You then have this configuration:

cdot-832-bkp-01::> ipspace show

(network ipspace show)

IPspace Vserver List Broadcast Domains

------------------- ----------------------------- ----------------------------

Cluster

Cluster Cluster

Default

cdot-832-bkp-01 mgmt

colo-ipspace-01

colo-ipspace-01 colo

3 entries were displayed.

**Note**: There are vservers added which have the same names as the IP Spaces you created, you will need these for ICL creation.

### Backup Cluster Port Allocation

You will need to allocate the ports connected to the relevant network to the correct broadcast domain. By default, all the ports are in the Default broadcast domain. You need to remove them from this domain and add them to the correct broadcast domain for your requirements. The example below uses physical ports.

broadcast-domain remove-ports -broadcast-domain Default -ports node01:e0c

broadcast-domain remove-ports -broadcast-domain Default -ports node02:e0c

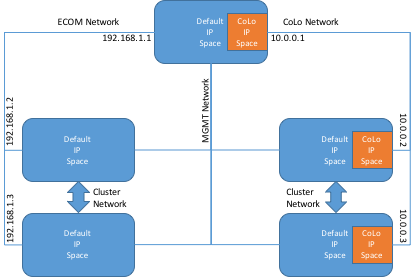
broadcast-domain add-ports -broadcast-domain colo -ports node01:e0c

broadcast-domain add-ports -broadcast-domain colo -ports node02:e0c

Once the ports are all assigned to the correct broadcast domains you can then create ICLs in each IP Space.

### ICL Creation

Now we need to create ICLs in the correct IP Spaces to ensure that peering works and can only see the intended interfaces. The Diagram below shows the IP Addresses used in this test configuration so you can see how the peering would work.



**COLO Primary Cluster**

You would create an ICL on each primary COLO node as follows:

net int create -vserver colo-ipspace-01 -lif cdot-832-colo-01-icl01 -role intercluster -home-node cdot-832-colo-01-01 -home-port e0d -address 10.0.0.2 -netmask 255.255.255.0 -status-admin up -failover-policy local-only -firewall-policy intercluster -auto-revert false -failover-group colo

net int create -vserver colo-ipspace-01 -lif cdot-832-colo-01-icl02 -role intercluster -home-node cdot-832-colo-01-02 -home-port e0d -address 10.0.0.3 -netmask 255.255.255.0 -status-admin up -failover-policy local-only -firewall-policy intercluster -auto-revert false -failover-group colo

**Backup Cluster**

You would create an ICL in each IP Space on the backup cluster node as follows:

net int create -vserver colo-ipspace-01 -lif cdot-832-bkp-01-colo-icl01 -role intercluster -home-node Node02 -home-port e0c -address 10.0.0.1 -netmask 255.255.255.0 -status-admin up -failover-policy local-only -firewall-policy intercluster -auto-revert false -failover-group colo

### Cluster Peering

The following commands would be used on the backup cluster to initiate peering.

clus peer create -peer-addrs 10.0.0.2 -address-family ipv4 -ipspace colo-ipspace-01

(cluster peer create)

Notice: Choose a passphrase of 8 or more characters. To ensure the authenticity of the peering relationship, use a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:

Confirm the passphrase:

Notice: Now use the same passphrase in the "cluster peer create" command in the other cluster.

You then run the following command on the COLO Cluster

clus peer create -peer-addrs 10.0.0.1 -address-family ipv4 -ipspace colo-ipspace-01

(cluster peer create)

Notice: Choose a passphrase of 8 or more characters. To ensure the authenticity of the peering relationship, use a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:

Confirm the passphrase:

Once peering is completed you can check the status.

clus peer show -fields ipspace ,ip-addrs

You can also ping all the nodes in the peer relationship as shown:

clus peer ping

Now create vservers in the relevant IP Space, they will be able to peer and SnapMirror/SnapVault can be configured.