Redundant Control Networking (Cisco, Brocade, Juniper)

Ericsson Compression Systems Manual Collection (Internal)

Disclaimer

No part of this document may be reproduced in any form without the written permission of the copyright owner.

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.

Contents

List of Figures

List of Tables

1 What this document describes

This document details the setting up of a redundant control network. Although this document details Cisco switch configuration, it is possible to use other makes and models of layer 2 switches.

2 Overview

It is possible to implement a redundant control network such that a single failure on the control network will not affect the operation or availability of any of the devices in the iSiS 8000 system. In the case where a device is not equipped with dual Ethernet control ports, only failure of the device, the device's connection to the switch, or the failure of the switch into which the device is connected should affect the connectivity of this device.

There are five stages involved with the setup of a redundant control network:

1. Setting up Teaming on the Windows Server
2. Setting up the MX8400
3. Setting up the E57xx or EN80xx series Encoders (this step not required for VPC devices)
4. Setting up the switches in the network
5. Testing the network

3 Setting up HP Server Teaming

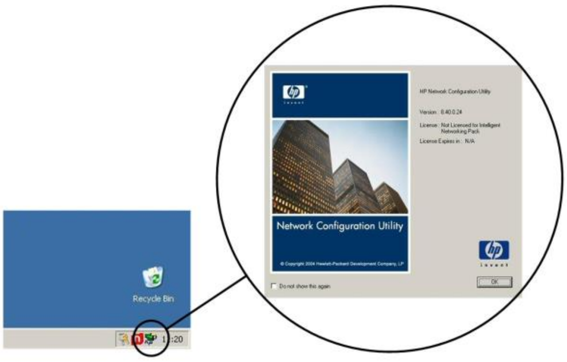
CAUTION…

It is required that the server is setup according to the Server/Client Machine Setup iSiS document (Part of the iSIS manual collection) before Teaming is setup.

iSiS 8000 nCC control platforms will be installed on HP servers running Windows Server 2003. The HP Network Configuration Utility software must be installed. None of the features detailed in this document require any additional licensing.

Note: The Broadcom Advanced Control Suite supplied with some older HP servers does not support redundant control networking in the manner perscribed within this document and is not supported by Ericsson Television. This application must be uninstalled. The HP Network Configuration Utility software is available for all currently supported Prolient HP servers (not for the DL140 G3).

1. The HP network configuration software will run as an application in the taskbar when Windows Server has fully booted (Figure 3.1). If the icon is not present ensure the ‘HP Teaming’ service is started and running.
2. Double-click on the Teaming icon to launch the **HP Network Configuration Utility**.



HP Network Configuration Utility

Version : 8.40.0.24

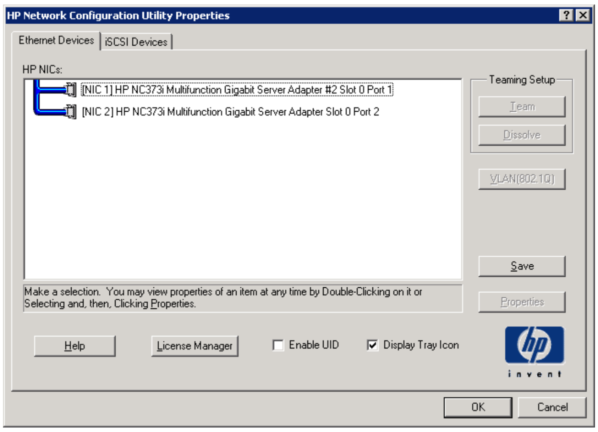
License : Not Licensed for Intelligent Networking Pack

License Expires in : N/A

Network Configuration Utility
© Copyright 2004 Hewlett-Packard Development Company, LP
Do not show this again
OK
Recycle Bin

Figure 3.1 HP Network Configuration Utility

3. The list of NICs installed in the server will be displayed. Select those which are to be used in the redundant ‘team’, then click **Team**.



HP Network Configuration Utility Properties

Ethernet Devices | iSCSI Devices

HP NICs:

[NIC 1] HP NC373i Multifunction Gigabit Server Adapter #2 Slot 0 Port 1

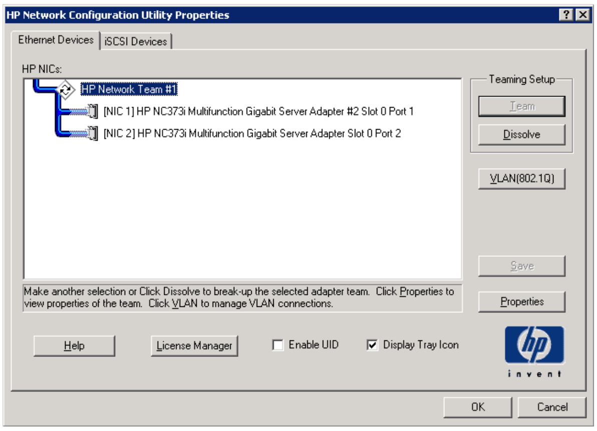
[NIC 2] HP NC373i Multifunction Gigabit Server Adapter Slot 0 Port 2

Make a selection. You may view properties of an item at any time by Double-Clicking on it or Selecting and, then, Clicking Properties.

□ Enable UID ☑ Display Tray Icon

Figure 3.2 Teaming available NICs

4. When the team is created, an icon at the ‘root’ level of the network adapter tree is created (see Figure 3.3):



HP Network Configuration Utility Properties

Ethernet Devices | iSCSI Devices

HP NICs:

HP Network Team #1

[NIC 1] HP NC373i Multifunction Gigabit Server Adapter #2 Slot 0 Port 1

[NIC 2] HP NC373i Multifunction Gigabit Server Adapter Slot 0 Port 2

Make another selection or Click Dissolve to break-up the selected adapter team. Click Properties to view properties of the team. Click VLAN to manage VLAN connections.

□ Enable UID ☑ Display Tray Icon

Figure 3.3 Showing the Teamed NICs

5. The Teaming of the nCC Server can be setup in one of two ways depending on the network topology in use. The possible two options are:

   a Small Networks
   For network topologies where a single failure could result in a loss of connection between Primary and Backup in Figure 3.4 (except for a failure of either of these two switches), the nCC server should be setup to behave in the same way as the Encoders with regard to a network preference. Select **Network Fault Tolerance <u>with Preference Order</u>**.

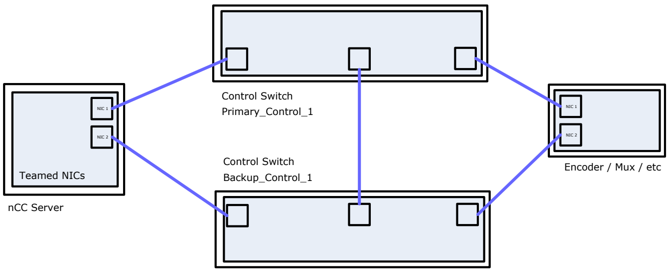


Figure 3.4 Example Small Network

b Larger Networks

The nCC server should be setup using **Network Fault Tolerance Only** for network topologies where a single failure should not result in a loss of connection between Primary 1 and Backup 1 in Figure 3.5 (except for a failure of either of these two switches). An example of a larger network is shown below:

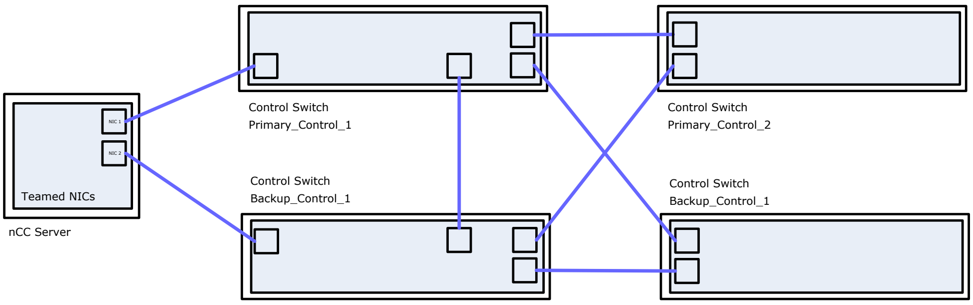
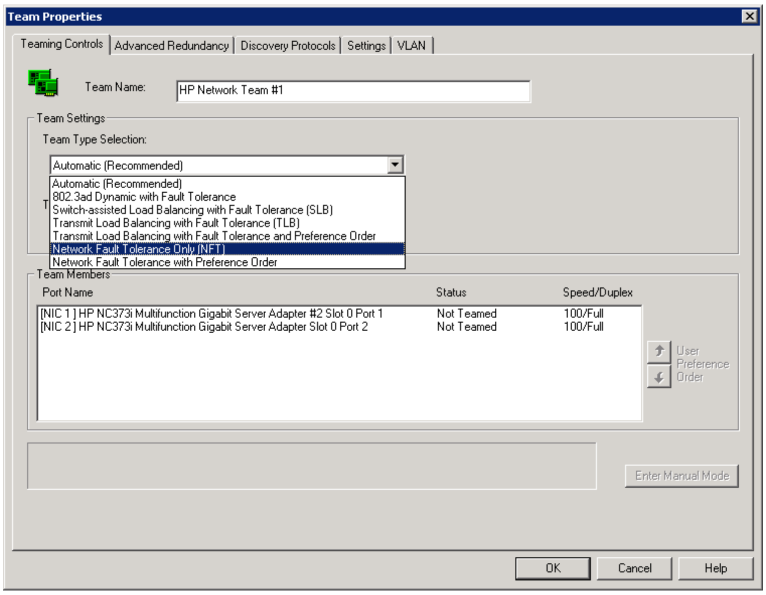


Figure 3.5 Larger Network

CAUTION…

It is very important that **Network Fault Tolerance <u>with Preference Order</u>** should ***<u>not</u>*** be used with larger networks.


Team Properties

Team Name: HP Network Team #1

Team Settings

Team Type Selection: Network Fault Tolerance Only (NFT)

Teaming Controls
Advanced Redundancy
Discovery Protocols
Settings
VLAN
Automatic (Recommended)
Automatic (Recommended)
802.3ad Dynamic with Fault Tolerance
Switch-assisted Load Balancing with Fault Tolerance (SLB)
Transmit Load Balancing with Fault Tolerance (TLB)
Transmit Load Balancing with Fault Tolerance and Preference Order
Network Fault Tolerance Only (NFT)
Network Fault Tolerance with Preference Order
User Preference Order
Enter Manual Mode
OK
Cancel
Help

Team Members

Port Name	Status	Speed/Duplex
[NIC 1] HP NC373i Multifunction Gigabit Server Adapter #2 Slot 0 Port 1	Not Teamed	100/Full
[NIC 2] HP NC373i Multifunction Gigabit Server Adapter Slot 0 Port 2	Not Teamed	100/Full

Figure 3.6 Setting up Network Fault Tolerance

Note: If Preference Order is used, ensure that **User Preference Order** is setup. Ensure that the NIC at the rear of the server labelled ‘NIC 1’ corresponds to NIC 1 on this list. This is <u>very important</u> as it quickly becomes confusing if this label is incorrect. Ensure that the preferred NIC is connected the same switch / router as the primary NIC of both the encoders and multiplex.

6. Under the **Settings** tab, ensure the following settings are set:

Table 3.1 Team adapter settings

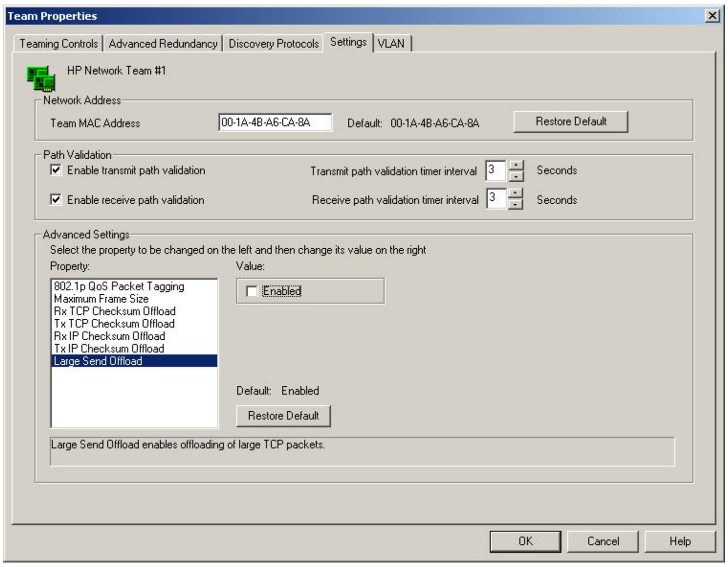
	Server Model			
Property	**G5**	**G6**	**G7**	**Desired setting**
802.1 QOS	☑	☑	☑	Disable
Ethernet@Wirespeed	☑	☑	☑	Disable
Flow Control	☑	☑	☑	Auto
IPv4 Checksum Offload	☑	☑	☑	None
IPv4 Large Send Offload	☑	☑	☑	Disable
Locally Administered Address	☑	☑	☑	Not Present
Receive Side Scaling	☑	☑	☑	Enable
Speed & Duplex	☑	☑	☑	Auto
Transmit Buffers	☑	☑	☑	Auto (or leave as default)
Interrupt moderation		☑	☑	Disabled
Priority and VLAN			☑	Priority & VLAN Disabled
VLAN ID			☑	Irrelevant

Note: It is possible to manually set the speed and duplex of the server NICs. However, this setting MUST be set to automatic. Ericsson Television testing has shown problems when manually setting the speed and duplex and it seems that HP acknowledge an issue with manually setting the speed and duplex of the NC373i NICs in the HP G5 servers. More information can be found here:

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?lang=en&cc=ie&taskId=120&prodSeriesId=1121486&prodTypeId=15351&objectID=c01604880

Note: The speed and duplex of the switch in to which the server is connected must also be set to automatic. Any other combination of settings must be avoided.

If **Preference Order** is used, ensure that **User Preference Order** is setup. Ensure that the NIC at the rear of the server labelled ‘NIC 1’ corresponds to NIC 1 on this list. This is very important, as it quickly becomes confusing if this label is incorrect. Ensure that the preferred NIC is connected to the same switch



HP Network Team #1

Network Address

Team MAC Address: 00-1A-4B-A6-CA-8A Default: 00-1A-4B-A6-CA-8A

Path Validation

☑ Enable transmit path validation — Transmit path validation timer interval: 3 Seconds

☑ Enable receive path validation — Receive path validation timer interval: 3 Seconds

Advanced Settings

Select the property to be changed on the left and then change its value on the right

Property:

- 802.1p QoS Packet Tagging
- Maximum Frame Size
- Rx TCP Checksum Offload
- Tx TCP Checksum Offload
- Rx IP Checksum Offload
- Tx IP Checksum Offload
- Large Send Offload

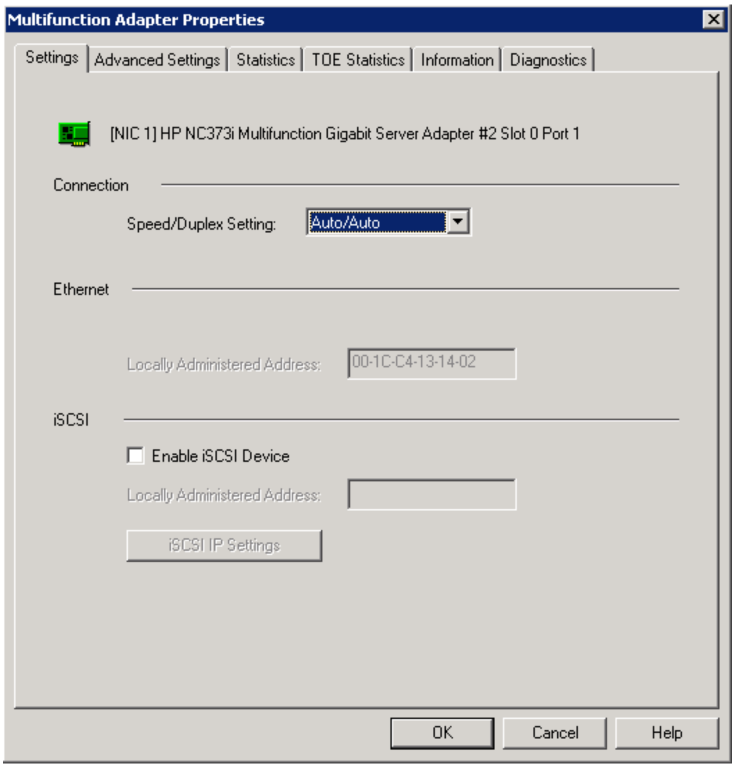
Value: □ Enabled

Default: Enabled

Large Send Offload enables offloading of large TCP packets.

Figure 3.7 Team Adapter settings

7. Return to the menu shown in Figure 3.3. Click on NIC 1 and select **Properties**. Ensure the Speed/Duplex Setting is set to **Auto**. Repeat for NIC 2. This is very important. Do not manually set the speed or duplex of the NIC, or the port on the Cisco into which the server is connected. Please see the document on Server/Client Machine Setup for further details.



[NIC 1] HP NC373i Multifunction Gigabit Server Adapter #2 Slot 0 Port 1

Connection

Speed/Duplex Setting: Auto/Auto

Ethernet

Locally Administered Address: 00-1C-C4-13-14-02

iSCSI

□ Enable iSCSI Device

Locally Administered Address:

Figure 3.8 Speed and Duplex set to Auto

8. Finally, ensure that the MAC address used as the Teams MAC address is the same as the MAC address used in the nCC license. This is located in:

…\Tandberg Television\nCompass Control Server\bin\license.xml

Once teaming is setup, if Windows Server 2003 detects a NIC has been disconnected, the user is alerted and the icon in the Windows Network Properties shows a disconnected state; this is also shown in the task bar.

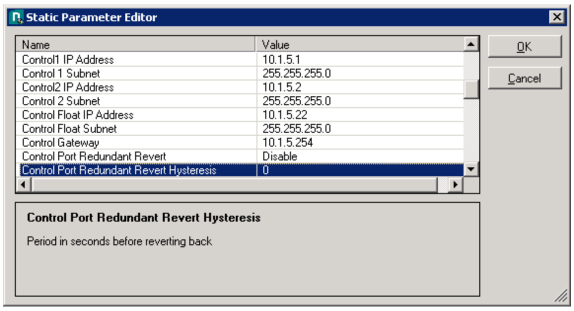
When the connection is re-established, neither icons revert to ‘connected’ until the user refreshes the Windows Networking Properties window (**press F5**).

If both NICs are connected, the team is still fully redundant and both NICs can be used despite the possible appearance of the icons indicating otherwise. Remember that these icons <u>may not represent</u> the current state of the system.

4 MX8400 Setup

4.1 Static Parameters

The MX8400 setup is performed through the manipulation of static parameters accessible through the nCC Equipment Setup physical map.



Name	Value
Control1 IP Address	10.1.5.1
Control 1 Subnet	255.255.255.0
Control2 IP Address	10.1.5.2
Control 2 Subnet	255.255.255.0
Control Float IP Address	10.1.5.22
Control Float Subnet	255.255.255.0
Control Gateway	10.1.5.254
Control Port Redundant Revert	Disable
Control Port Redundant Revert Hysteresis	0

Control Port Redundant Revert Hysteresis

Period in seconds before reverting back

Figure 4.1 MX8400 control port static parameters

Upload the physical map once the static parameters have been correctly completed.

Reboot the MX8400 following any change to the MX8400 control network settings.

4.2 Control Port Redundant Revert

It is advisable that **Control Port Redundant Revert** is used only for ‘small networks’ (see Figure 3.4 Example Small Network). In which case, **Redundant Revert Hysteresis** should be set to **90 sec**. This is sufficient time for the network to settle down and for nCC to have finished performing any configuration actions following a network switch power up. Setting shorter times can result in ‘race’ conditions, where packets can be lost when multiple devices are reverting to the Primary switch at not quite the same time.

It is advised that **Revert** is not used for larger networks and any toggling should be the result of a redundancy or manual switch. This should simplify system operation, testing and debugging.

4.3 Control Port IP Addresses

Set the IP addresses of both physical control ports.

It is possible to set all of the control port IP addresses the same i.e., Port 1 = Port 2 = Floating.

Whilst this has the benefit of minimising the number of required IP addresses in a system, it can be confusing when attempting to debug a system. It is often more simple to use a unique IP address for control port 1, control port 2, and the floating control IP address.

5 E57xx, EN59xx and EN80xx Setup

Because of the NIC implementation in the E57xx, EN59xx and EN80xx it is important to setup SNTP where a redundant control network is to be used.

The E57xx, EN59xx and EN80xx redundant control port connected to the switch may have electrical connectivity at all times. When not in use the redundant control port will be reported by the Cisco as having a MAC address of 00-00-00-00-00-00. When the Encoder switches to this redundant port it will use the MAC address previously associated with the primary NIC. The Encoder will not issue any indication of this condition to the network and until there is an ARP refresh; and the Encoder ‘reveals’ itself, it will be reported as ‘loss of contact’ by nCC.

5.1 Forcing Encoder to ‘talk’

It is possible to force the Encoder to ‘talk’ regularly through the network if it is setup to use an SNTP server. If the Encoder is setup to use SNTP server, it will open and maintain a socket session using the SNTP port. When the Encoder switches ports it will attempt to re-establish a connection to the SNTP server as quickly as it can using its other NIC. As a result, the switches will be able to update their tables and reflect the change of NIC. This method is currently the only way to ensure that the switch is notified of this change of MAC address and to avoid loss of contact.

6 VPC Setup

The VPC will behave correctly in a redundant control network if an Ethernet connection is present on control port 2 at boot time. In this situation, an alarm will be raised if control port 2 is disconnected.

- The VPC will not use control port 2 if the VPC is booted without an Ethernet connection on control port 2.
- VPC will not raise an alarm if control port 2 is subsequently reconnected then disconnected.

6.1 Determine if a VPC is working

Disconnecting control port 2 and checking if an alarm has been raised (either in the VPC web browser or nCC Equipment Status) is the only safe way for a user to determine if a VPC is working in a redundant control network.

7 Small Network Setup

Please refer to Figure 7.1 below for a conceptual overview of a ‘small’ network. This figure assumes that there is a redundant data network, which is represented by the two C3560G Cisco switches. It is suggested that for each switch, including the data switches, the control VLAN is given a unique IP address. These IP addresses can be used to gain Telnet access to each individual switch or to allow monitoring of each switch.

Note: In a small network setup it may be possible to use HP Procurve switches; though testing has been carried out only with Cisco Catalyst switches and Brocade switches. In systems with cascaded control switches (more than one primary switch or more than one secondary control switch) HP Procurve switches should not be used.

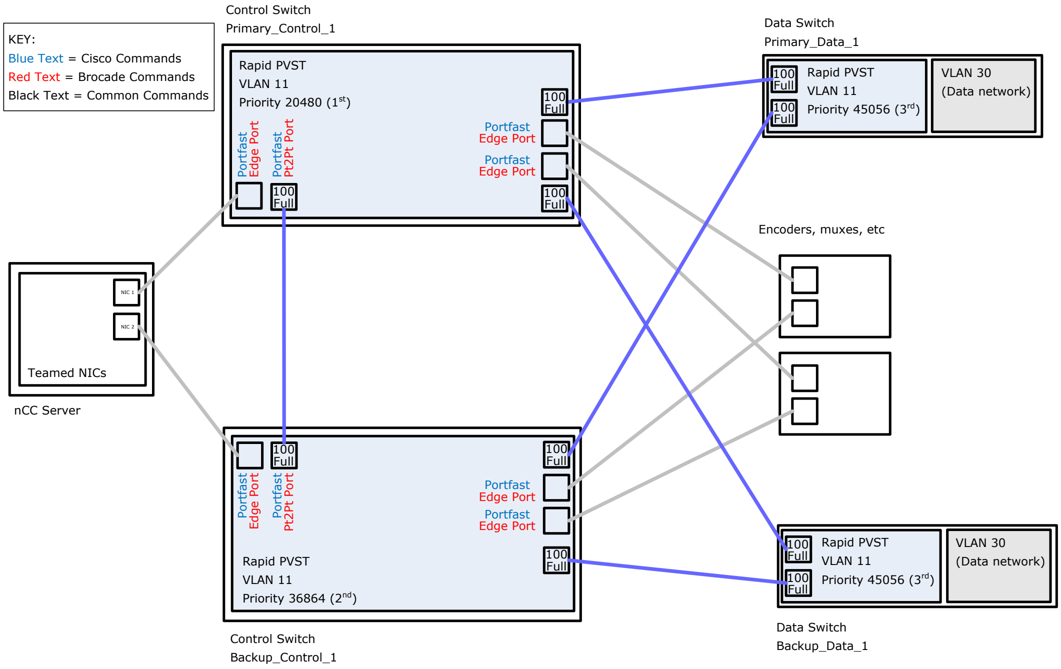


Figure 7.1 Redundant Control Network using two control switches.

7.1 Configuration Key Features

There are a number of key features which must be set up in order for the system to operate correctly, these are shown in the diagram and are listed below. More switch command related information can be found in Cisco Switch Fundamentals manual, part of the iSiS manual collection.

1. All switches are configured with Rapid Per VLAN Spanning Tree (Rapid PVST).
2. The Spanning Tree priorities are manually set; the data switches have the same priority.
3. Speed and duplex are manually configured between switches.
4. Crossover cables are used between switches (shown in blue).

5. PortFast is setup on the link between the two control switches but not the links to the other (data) switches.
6. PortFast is setup on every port not connected to a switch.
7. There are two ports in the control VLAN on each of the data switches.

8 Larger Network Setup

CAUTION…

Redundant Control Networking for larger networks has been extensively tested can deployed using Cisco Catalyst and Brocade switches. HP Procurve switches have been shown not to be at all suitable in this application.

Please refer to Figure 8.1 for a conceptual overview of a larger control network.

As with smaller networks, the setup given here relies on Spanning Tree to select the best path through the network. In a larger network, the Spanning Tree priority is very important, this is a major factor in the way the network elects a root through the network, and unlike the other settings, is not common to all switches in the network.

It is necessary to connect all additional switches; including any switches which are part of the data network, to the ‘Primary_1’ and ‘Backup_1’ switches. Using this approach enables these additional switches to recognise that there are two routes back to the 1st Priority switch. As soon as the first port fails, it will instantly use the alternative port, and achieve the fastest possible ‘network convergence’ time.

It is suggested that where possible, Multiplexers are connected to the Primary and Backup control switch 1 to minimise the number of switches through which Reflex traffic must pass.

The example in *Figure 8.1* has been thoroughly tested and behaves well.

8.1 Configuration Key Features

There are a number of key features which are shown in Figure 8.1and are listed below

1. All switches are configured with Rapid Per VLAN Spanning Tree (Rapid PVST)
2. The Spanning Tree priorities are manually set, the data switches have the same priority.
3. Speed and duplex are manually configured between switches.
4. Crossover cables are used between switches
5. PortFast is setup on the interconnecting ports that link the two control switches.
6. PortFast is NOT setup on the interconnecting ports that link the two control switches with any other switches (I.e.; No PortFast between Primary and Backup control switch 1 and Primary and Backup control switch 2).
7. PortFast is setup on every port not connected to a switch.
8. There are two ports in the control VLAN on each of the data switches.

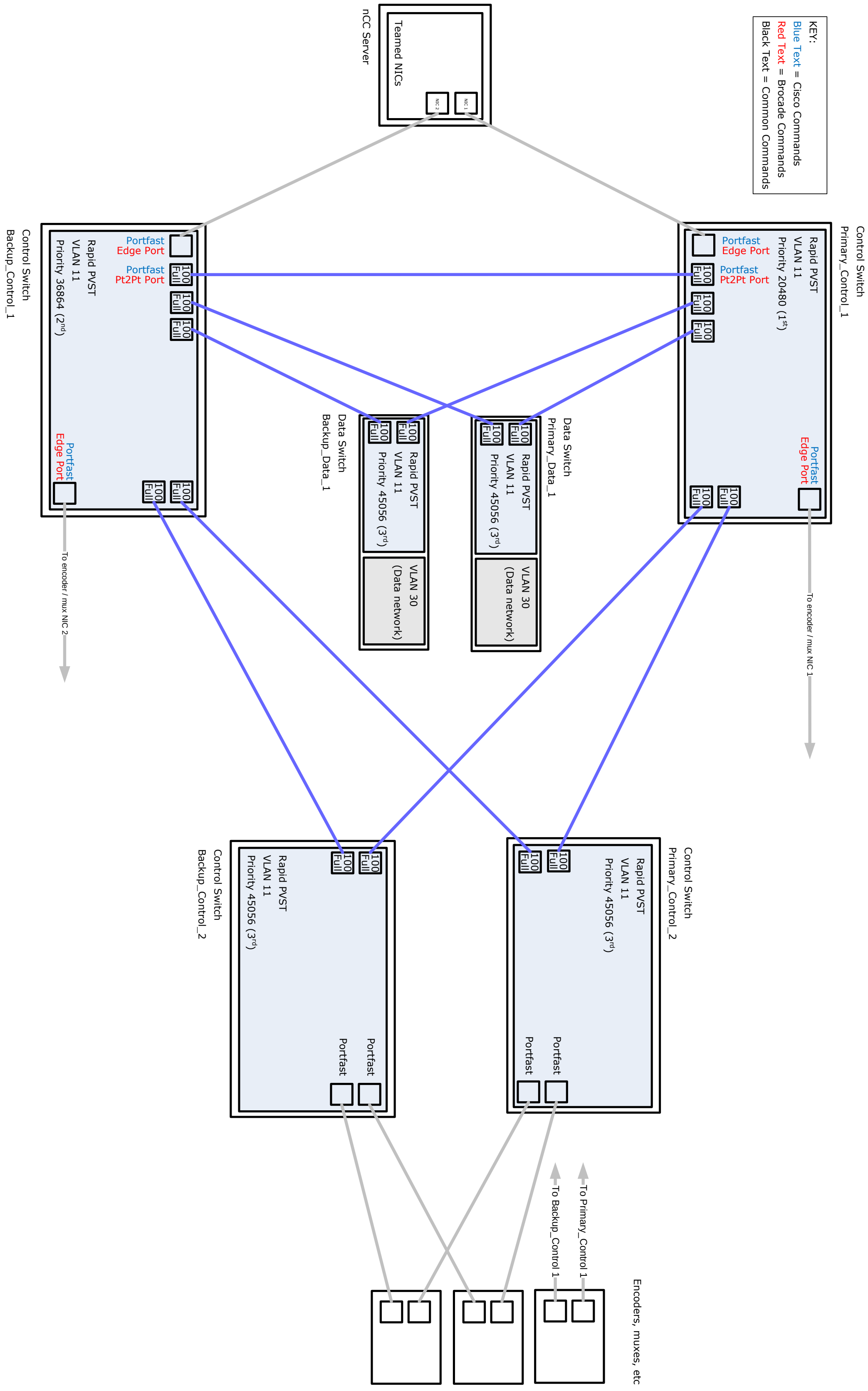


Figure 8.1 Redundant Control Network for a larger network.

9 Control of Remote Sites through Data Switches

The increased use of remote encoding leads to the use of redundant control networking across multiple sites. Figure 9.1 shows the correct way to approach this.

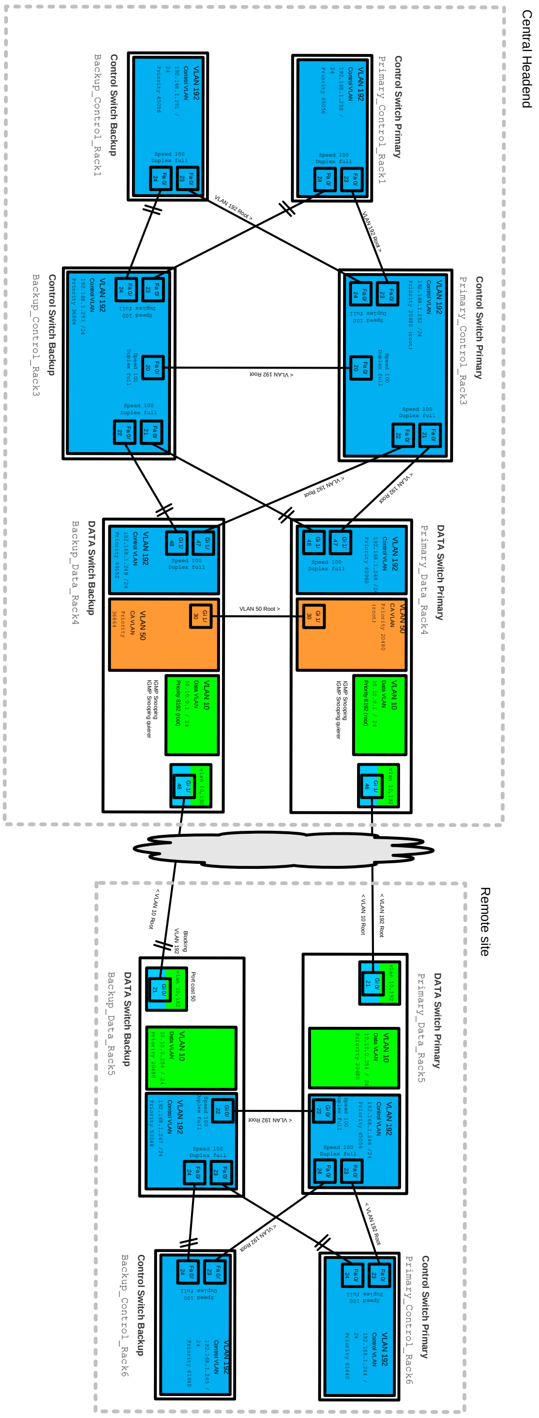


Figure 9.1 Redundant Control Network for a Network Over Remote Site.

9.1 Configuration Key Features

In addition to the setup steps described in Chapter 8 Larger Network Setup, there are a number of key features which must be setup in order for the network to operate correctly where the network includes remote sites.

1. The remote site connects to the central site through a layer 3 router.
2. The port cost command is in place to ensure that, where possible the control network traffic will use the primary route through the cloud. In normal operation all traffic should be carried by the primary link.
3. The star topology is continued on the remote site. Any additional control or data switches will connect to the 'Primary _Data_Rack5' and 'Primary _Data_Rack5'.

10 Expected behaviour for given failure modes

10.1 Overview

This chapter provides a pictorial overview of the expected operation when a section of the network fails. The scenarios have been tested in a real system, the observations from these tests are recorded in this chapter.

In order to ensure that the worst case behaviour was recorded during testing, the following settings for all devices were used in nCC. This is probably a more 'aggressive' setup than a typical customer system.

Table 10.1 Typical and Test Settings

	Test settings	Typical settings
Consecutive	2	2
Retries	1	1
Timeout	100ms	1000ms
Poll	3 sec	5 sec

The illustrations show a larger network, the principles are the same with a smaller network, which is simpler while network convergence time should be lower in a small network. Note that Redundant Revert is not used in the larger network.

Each scenario presumes that the system is starting in the 'normal' state, as shown in Figure 10.1. The diagrams given for each set of scenarios show the route that the network traffic takes (in green). Connected sections of the network that are not in use (from an nCC point of view) are shown in grey. Failed sections of the network are shown in red.

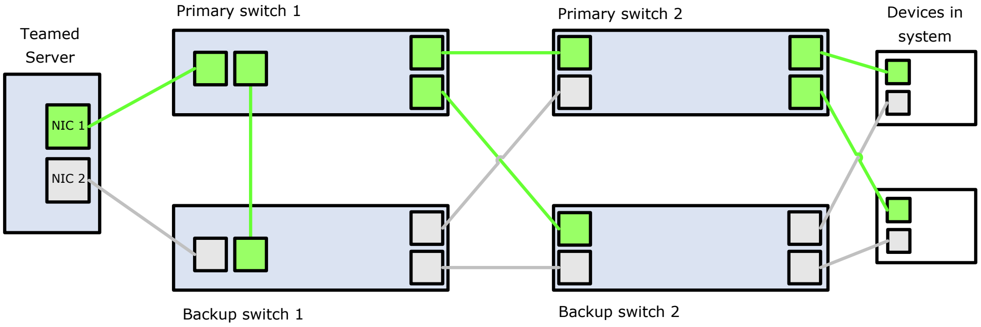


Figure 10.1 Normal Operation Showing Traffic Route

10.2 Failure Between Server and Control Switch 1

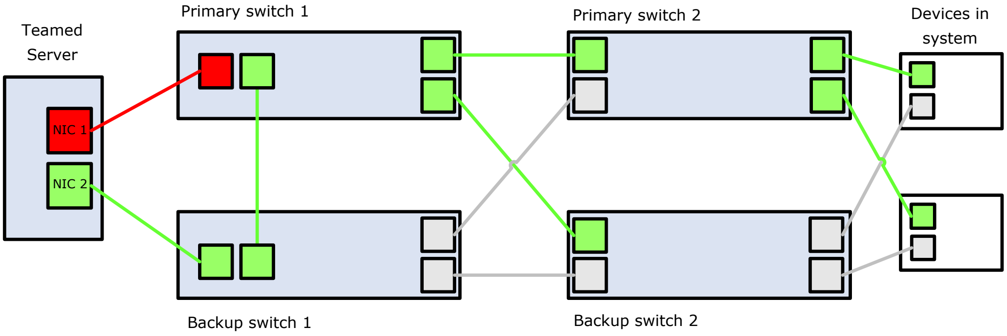


Figure 10.2 Failure Between Primary Switch 1 and the nCC Server

Table 10.2 Observations

	Failure occurs	**Failed condition rectified**
Action performed by server	Failover from NIC 1 to 2	None in large network Reverts to NIC 1 after revert delay in small network
Spanning – tree Action performed by Switch	None	None
Action performed by ‘Devices in system’	None	None
Windows Server observations	NIC 1 disconnected alert via taskbar	None, user must refresh Network Connections to clear alert
nCC observations	None	None

10.3 Failure Between Control Switch and Ericsson Device

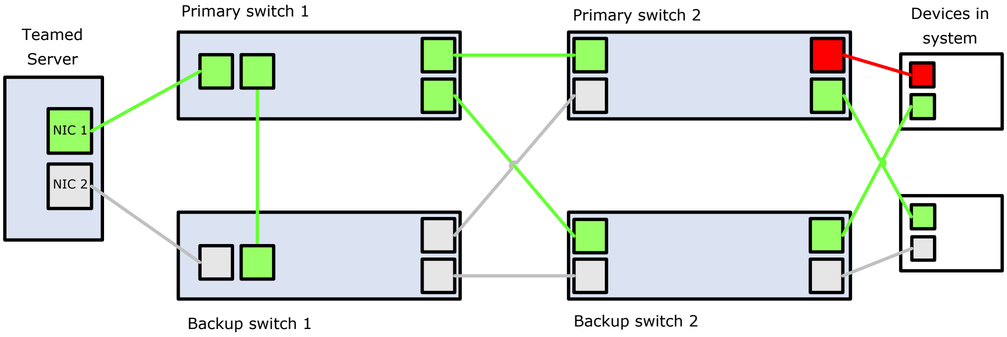


Figure 10.3 Failure Between Primary Control Network and Ericsson Television Device

Table 10.3 Observations

	Failure occurs	Failed condition rectified
Action performed by server	None	None
Spanning – tree Action performed by Switch	None	None
Action performed by ‘Devices in system’	Device fails over to NIC 2	Device either remains on NIC 2 or, depending on the device, reverts to NIC 1
Windows Server observations	None	None
nCC observations	Depending on device, an alarm is raised informing of device’s control port link down. No other actions should be performed or reported.	Alarm clears

10.4 Failure of Primary Control Switch 1

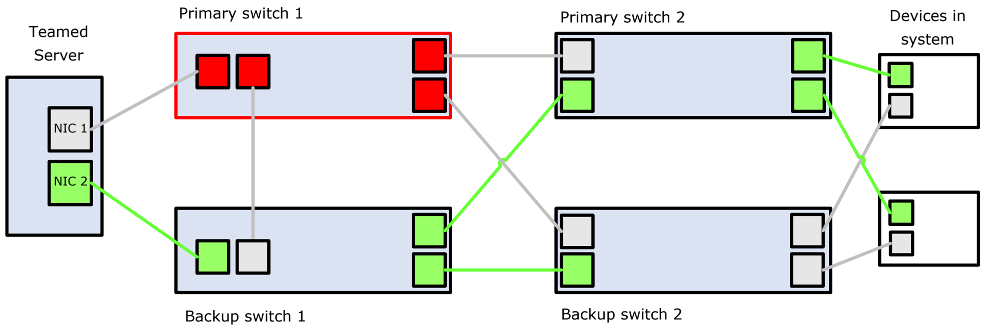


Figure 10.4 Failure of Primary Switch 1

Table 10.4 Observations

	Failure occurs	**Failed condition rectified**
Action performed by server	Failover from NIC 1 to 2	None in large network Reverts to NIC 1 after revert delay in small network
Spanning – tree Action performed by Switch	Primary and Backup 2 switches instantly detect failure and forward traffic to Backup Cisco 1.	Primary and Backup 2 switches detect the port is up. Spanning tree occurs. Primary and Backup 2 switches forward traffic to Primary Cisco 1 rather than Backup Cisco 1.
Action performed by 'Devices in system'	None	None
Windows Server observations	NIC 1 disconnected alert via taskbar	None, user must refresh Network Connections to clear alert
nCC observations	None (Primary Cisco 1 reported out of contact)	See note in section 10.5 below with regard to any Evolution Encoders connected to Primary Cisco 1 (Primary Cisco 1 back in contact)

10.5 Failure of Primary Control Switch 2

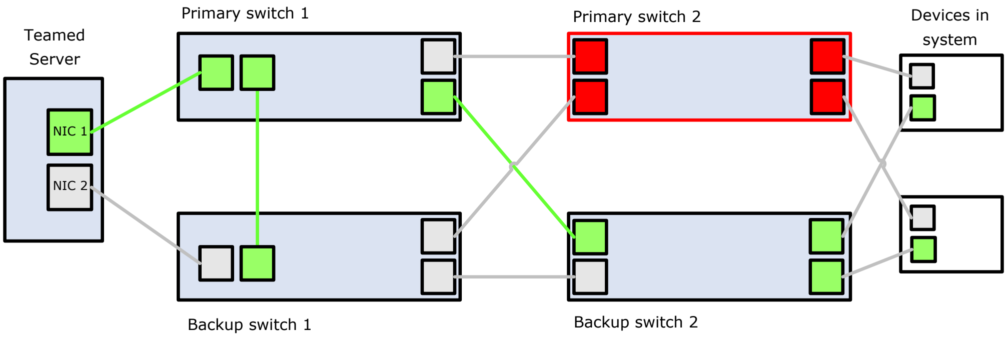


Figure 10.5 Failure of Primary Switch 2

Table 10.5 Observations

	Failure occurs	**Failed condition rectified**
Action performed by server	None	None
Spanning – tree Action performed by Switch	None	None
Action performed by 'Devices in system'	Devices fail over to NIC 2	Devices either remain on NIC 2 or, depending on the device, reverts to NIC 1
Windows Server observations	None	None
nCC observations	None (Primary Cisco 2 reported out of contact)	See note below (Primary Cisco 2 back in contact)

Note: A Cisco or Brocade switch performs diagnostic tests on its ports during its boot cycle. This causes the ports to become electrically active (at this point, the Cisco is not booted and will not perform any switch functions). If the Piglet (Evolution Encoder) Encoder senses electrical activity on its primary NIC it will switch to this NIC, regardless of the ability of the link to handle Ethernet frames. This is a limitation of the Encoder hardware at this time. It is possible that keen poll settings may result in nCC briefly losing contact with an unused Encoder

11 Restoring Normal Operation

Chapter 9 details the operation of the system under various failure modes and the operation of the system when the failure mode is corrected. It should be observed that some of these recovery scenarios may cause undesirable system performance (described in Chapter 10).

If the primary network has failed, it will be necessary to ensure that no switching can be actioned by nCC when the primary network switch is re-powered/repaired. This can be achieved by setting all spare devices to **Unavailable** in nCC Equipment Status.

We suggest that this precaution is undertaken if work or maintenance is carried out on either of the control network switches.

12 Example Cisco 2960 Configuration

The following example shows how a Cisco 2960 will look after a successful configuration following the instructions in this chapter.

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
no service dhcp

hostname Primary_Ctrl_1

enable secret 5 $1$fYKE$tgoxoOAAK/LHYG8PieLAo/

ip subnet-zero

no ip domain-lookup
vtp mode transparent

spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 11 priority 20480

interface FastEthernet0/1
 description E5770 1
 switchport access vlan 11
 switchport mode access
 spanning-tree PortFast

 interface FastEthernet0/2
 description E5770 2
 switchport access vlan 11
 switchport mode access
 spanning-tree PortFast

*** lots more interfaces, each correctly setup, not shown for
clarity***

interface FastEthernet0/22
 description Connected to Backup_Ctrl_1
 switchport access vlan 11
 switchport mode access
 duplex full
 speed 100
 spanning-tree PortFast

interface FastEthernet0/23
```

```
 description Connected to Primary_Ctrl_2
 switchport access vlan 11
 switchport mode access
 duplex full
 speed 100

interface FastEthernet0/24
 description Connected to Backup_Ctrl_2
 switchport access vlan 11
 switchport mode access
 duplex full
 speed 100

interface GigabitEthernet0/1
 switchport mode dynamic desirable

interface GigabitEthernet0/2
 switchport mode dynamic desirable

interface Vlan1

interface Vlan11
 description Control_VLAN
 ip address 192.168.1.253 255.255.255.0

ip default-gateway 192.168.1.254
ip classless
no ip http server

no cdp run
snmp-server community private RW
snmp-server community public RO

line con 0
line vty 0 4
 password 7 00071A150754
 login
line vty 5 15
 password 7 045802150C2E
 login
```

13 Example Brocade FWS Configuration

The following example shows how a Brocade FWS will look after a successful configuration following the instructions in this chapter.

```
ver 04.3.03T7e1
!
module 1 fws1g-24-port-copper-base-module
!
global-stp
!
!
!
vlan 1 name DEFAULT-VLAN by port
!
vlan 11 name Control_VLAN_11 by port
 untagged ethe 0/1/1 to 0/1/24
 router-interface ve 11
 spanning-tree 802-1w
 spanning-tree 802-1w priority 20480
!
!
!
boot sys fl sec
enable telnet password .....
enable super-user-password .....
hostname Primary_Control_1
ip route 0.0.0.0 0.0.0.0 192.168.1.254
!
snmp-server community public ro
snmp-server community private rw
interface ethernet 0/1/1
 port-name VPC_01
 spanning-tree 802-1w admin-edge-port
!
interface ethernet 0/1/2
 port-name VPC_02
 spanning-tree 802-1w admin-edge-port
!

*** lots more interfaces, each correctly setup, not shown for
clarity ***

!
interface ethernet 0/1/22
 port-name Connected_to_Backup_Ctrl_1
 spanning-tree 802-1w admin-pt2pt-mac
!
interface ethernet 0/1/23
 port-name Connected_to_Primary_Ctrl_2
 speed-duplex 100-full
 spanning-tree 802-1w admin-pt2pt-mac
!
interface ethernet 0/1/24
 port-name Connected_to_Backup_Ctrl_2
 speed-duplex 100-full
 spanning-tree 802-1w admin-pt2pt-mac
!
interface ve 11
 port-name Control_Interface_11
 ip address 192.168.1.253 255.255.255.0
!
end
```

14 Example Juniper Configuration

The following example shows how a Juniper EX series switch will look after a successful configuration following the instructions in this chapter.

<<<TO DO>>>