Brocade Switch Fundamentals

Ericsson Compression Systems Manual Collection
(Internal)

Copyright

Disclaimer

Contents

List of Tables

1 What this document describes

This document is intended to provide information regarding the basic set up of a Brocade Switch / Router.

There are four additional documents which describe the scenarios into which a Brocade switch / router can be deployed. Each document provides specific commands for a given scenario. The four scenarios are:

- Basic Control Network

- Redundant Control Network

- Basic Data Network (input and output)

- Advanced Data Network

2 Overview

Ericsson Television supply a range of network switches / routers applicable to different applications.

HP Procurve switches may be used in simple (non-redundant) control networks. The Procurve switches are typically taken out of the box and plugged into the system with little or no configuration. For larger, more complex control networks, or for customers who prefer more control, the Cisco Catalyst 2960, or Brocade FastIron WS (FWS) switches are used. These switches must be configured before being deployed to ensure correct operation; an un-configured Cisco or Brocade switch will cause operation issues.

Ericsson Television support only Cisco or Brocade switches / routers in the data networks within the Ericsson Television supplied system. The output of the Ericsson Television system often interfaces with a customer supplied switch / router of a different make, which is standard practice.

3 Basic Setup of the Brocade FastIron WS Switch

3.1 Serial control

When the switch is first removed from the box it will need configuring via an RS232 serial cable; HyperTerminal or TeraTerm should be used. The serial connection parameters are given below.

Table 3.1   Default Brocade serial connection parameters

Parameter	Setting
Baud rate	9600
Data	8 bit
Parity	None
Stop Bit	1 bit
Flow Control	None

The following prompt will be observed if the serial session is successfully established to a new, not yet configured FWS624G:

```
FWS624G Router>
```

At this level, any real-time logging will be displayed to the user. A restricted range of control commands may be entered.

3.2 Enabling access to the Serial session

It is necessary to 'enable' access to the 'terminal' session such that switch configuration related commands may be entered. The prompt will reflect the change, note the '**#**'.

```
FWS624G Router>enable
FWS624G Router#
```

The **enable** command may be abbreviated to **en**.

3.3 Entering configuration

It is necessary to enter the **configure terminal** prompt in order to enter switch configuration commands. The prompt will reflect the change.

```
FWS624G Router#configure terminal
FWS624G Router(config)#
```

The **configure terminal** command may be abbreviated to **conf t**.

3.4 Naming the Switch

It is helpful to name the switch as this helps to distinguish one switch from another. The prompt will change to reflect the new switch name once the name has been correctly entered. The name **SwitchName** is used in the example below.

```
FWS624G Router(config)#hostname SwitchName
SwitchName(config)#
```

3.5 Enabling IP Layer 3 software (FWS Only)

Brocade FWS switches have two versions of software, layer 2 and layer 3. This is not the equivalent to the Cisco IPBase (SMI) and IPServices (EMI) software. An FWS running layer 3 software will have the same functionality as an IPBase (SMI) Cisco. The layer 2 software does not have enough functionality to be able to be used in Ericsson Television systems.

Please see *section 5* for details on ensuring the correct version is in use.

```
SwitchName(config)#boot system flash secondary
SwitchName(Config)#end
SwitchName#wr mem
SwitchName#reload
```

This will reload the switch. It will boot up to the layer 3 code in the second bank containing the Layer 3 software.

3.6 Telnet

Telnet is enabled by default.

3.7 Entering a Telnet Password

By default, a device has no password assigned. It is necessary to protect access to the terminal session. The password usually entered in Ericsson Television systems is **brocade** and is shown below.

```
SwitchName(config)#enable telnet password brocade
```

3.8 Entering an Enable Password

It is common to restrict access to a super-user interface. The password usually entered in Ericsson Television systems is **brocade** and is shown below.

```
SwitchName(config)#enable super-user-password brocade
```

Note: By default Telnet and Enable passwords are not displayed in the running configuration screen.

3.9   SFP Ports on FWS Switches

The four SFP ports on an FWS switch are shared with the first four copper ports. They cannot be used to expand the switches port count to 24 ports. However, on a 10/100Base-T FastEthernet switch, the first four copper ports are 10/100/1000Base-T GigabitEthernet ports and can be used to feed equipment such as MX8400 in smaller ISIS8000 systems.

3.10   Port Nomenclature

Ports on an FWS switch are referred to by Stack ID \ Slot Number \ Port number. Ericsson Television systems will never use the FWS switches in a stacked configuration, so the stack ID will always be **0**. The FWS switches are single slot devices so the slot number is always **1**.

On Brocade switches, there is no distinction between FastEthernet and GigabitEthernet ports. For example port 10 on either a FastEthernet switch or GigabitEthernet switch is referred to as ethernet 0/1/10.

3.11   Tagged and Untagged Ports

The term 'tagged' and 'untagged' ports refer to 802.1Q VLAN tagging. On a Cisco this is referred to as a 'trunk port'. 802.1Q VLAN tagging is when a port is part of two or more VLANs, each packet that leaves the port is tagged with the originating VLAN. Incoming tagged packets are forwarded to the destined VLAN.

A port in a single VLAN on a Cisco is termed a 'switchport'. The equivalent port on a Brocade switch is termed an 'untagged' port. Packets leaving these ports are not tagged with VLAN information.

A port in multiple VLANs on a Cisco is termed a 'trunk' port. The equivalent port on a Brocade is termed a 'tagged' port. Packets leaving these ports are tagged with VLAN information.

Note: Untagged port can only be added to one VLAN. Tagged ports can be added to multiple VLANs.

3.12 Creating a VLAN/Modifying a VLAN

When new, out of the box, all ports on the switch are in untagged and in VLAN 1. This default VLAN will not display ports when viewing configuration. When a VLAN is created it needs to have a name associated with it. VLANs used in Ericsson Television systems are always port based VLANs. The following example shows how to create VLAN 10 named Control-Vlan.

```
SwitchName(config)#vlan 10 name Control-Vlan by port
SwitchName(config-vlan-10)#exit
SwitchName#
```

Once a VLAN has been created, it is then referred to by its number.

```
SwitchName(config)#vlan 10
SwitchName(config-vlan-10)#
```

3.13 Adding ports to a VLAN

The following examples show how to add a single untagged port and multiple untagged ports to a VLAN:

```
SwitchName(config)#vlan 10
SwitchName(config-vlan-10)#untagged ethernet 0/1/1
SwitchName(config-vlan-10)#untagged ethernet 0/1/10 to 0/1/20
```

The following example shows how to add a tagged port to two VLANs:

```
SwitchName(config)#vlan 10
SwitchName(config-vlan-10)#tagged ethernet 0/1/5
SwitchName(config-vlan-10)#exit
SwitchName(config)#vlan 20
SwitchName(config-vlan-20)#tagged ethernet 0/1/5
```

3.14 Moving ports between VLANs

Untagged ports only belong to one VLAN and only those ports belonging to the default VLAN can be assigned to another VLAN. If you wish to move untagged ports from one VLAN to another, they must first be removed from the 'old' VLAN and placed into the default VLAN by using the following command:

```
SwitchName(config-vlan-10)no untagged ethernet <port number>
```

The port can then be assigned to the new VLAN.

3.15 Adding an IP Address to a VLAN

On a Cisco switch there are two elements relating to a VLAN. There is the VLAN itself, which ports are placed into, and then there is the VLAN interface. The VLAN interface is a virtual interface attached to the VLAN. It is referred to as **Interface VLAN x**. It is this interface that can have an ip address attached to it. This is what is done when giving an IP address to a VLAN on a Cisco.

The Brocades have the same concept of a virtual interface that is attached to a VLAN and can have an IP address assigned. However, on a Brocade the virtual interface is not automatically linked to the VLAN by using the same number as the VLAN, the linking has to be done manually.

The first step is to link the VLAN to the virtual interface; it is known as a Virtual Ethernet (VE) interface. It is recommended to give the VE the same number as the VLAN. The following example shows how to create a VE numbered 10 and assigned to VLAN 10.

```
SwitchName(config)#vlan 10
SwitchName(config-vlan-10)#router-interface ve 10
```

Once the VE has been created, it can then have an IP address assigned. The IP address 192.168.1.253 with a subnet mask of 255.255.255.0 has been used in the example below.

```
SwitchName(config)#interface ve 10
SwitchName(config-vif-10)#port-name Control-VE
SwitchName(config-vif-10)#ip address 192.168.1.253 255.255.255.0
SwitchName(config-vif-10)#exit
```

Note...You can only access the VE when ports are in the VLAN it is assigned to. If the VLAN has no ports (tagged or untagged) then you will not be able to use the above command.

Brocade switches also support the use of "slash" notation with regard to entering subnets. In the above example the command:

```
SwitchName(config-vif-10)#ip address 192.168.1.253 255.255.255.0
```

Can be replaced with:

```
SwitchName(config-vif-10)#ip address 192.168.1.253/24
```

The running configuration will always show the subnet in the "dot" notation independent on how the subnet was entered during the configuration.

3.16 IGMP Snooping Querier

IGMP Snooping Querier must be used on all control switches and all data switches in an Ericsson system. IGMP snooping querier must be configured in order for IGMP Snooping to work.

IGMP Querier must be enabled on all switches in a control or data network. A Brocade specific 'funny'; to have a IGMP querier emit and IGMP message from interfaces that are part of a VLAN, there must be a ve, with an IP address configured, somewhere in the VLAN (either locally or connected to the VLAN via a physical interface. The ve IP address can be either an address within the VLAN, or an address unrelated to the VLAN (though it is most useful to have the ve address within the network the VLAN encompasses).

The examples below show how to turn on IGMP snooping and enable the Querier. The following command is for Brocade FastIron WS (FWS) switches:

```
SwitchName(config)#ip multicast active
```

3.17   nCC SNMP Configuration

The switch will need to be configured to respond to SNMP polls in order to be health polled by nCompass or nCompass Monitoring. If SNMP is not set up, the switch will appear to be out of contact in nCC.

The 'community names' used by the nCC and the switch are configurable. It is important that they match. The nCC default is **public/private**. This can be set in the Brocade by using the following commands:

```
SwitchName(config)#snmp-server community public ro
SwitchName(config)#snmp-server community private rw
```

3.18   Spanning Tree

It is important to set up Spanning Tree even if the switch is being used as a stand-alone switch. Poor system behaviour is often observed if this has not been setup. Rapid Per-VLAN Spanning (Rapid PVST) tree **must** be enabled.

```
SwitchName(config)#vlan 10
SwitchName(config-vlan-10)#spanning-tree 802-1w
```

Configuring the priority of each VLAN in a control network is essential where a redundant network is used (redundant control networking is covered in a different document in the iSiS series of manuals); it is not required for standalone switches. **Priority** is a Spanning Tree parameter. Each switch may have a different priority. The switch with the lowest number has the highest priority. VLAN 10 is used in the example below and is give a priority of 20480 (the switch will list valid priority values).

```
SwitchName(config)#vlan 10
SwitchName(config-vlan-10)#spanning-tree 802-1w priority 20480
```

3.19　Edge Ports

By default, Spanning Tree will cause a delay in the period between a port being physically connected and the switch receiving or forwarding traffic to this port. This behaviour can also be observed when a port is put into a VLAN (VLAN management by nCC for example). During this uplink delay the switch is working out if using this port will cause a loop in the network. **Edge-port** can be used to disable this checking and avoid the delay.

Edge-port should be used wherever it is known that the port will not be part of a network loop i.e., set this up on all ports connected to any device that is not another switch. In the example below, Edge-port is enabled on ports in the range of 1 to 24.

```
SwitchName(config)#interface ethernet 0/1/1 to 0/1/24
SwitchName(config-mif-0/1/1-0/1/24)#spanning-tree 802-1w admin-edge-
port
SwitchName(config-if-range)#exit
```

Note:　This command is the equivalent of the Cisco spanning-tree **portfast** command.

3.20　Point to Point Ports

When connecting two Brocade switches together, spanning-tree recovery after a switch failure is quicker if the interconnecting ports are configured to be point to point links. In the example below, point to point is configured on port 14.

```
SwitchName(config)#interface ethernet 0/1/13
SwitchName(config-mif-0/1/13#spanning-tree 802-1w admin-pt2pt-mac
SwitchName(config-if-range)#exit
```

3.21　Spanning Tree Root Guard

Spanning tree root guard must be enabled on all ports where the root bridge should not appear (see the document on Redundant Control Networking). This prevents the spanning-tree topology changing unexpectedly. This is particularly useful to prevent problems when an unknown cable is connected to the switch. In the example spanning tree root guard is configured for ports 1 to 20.

```
SwitchName(config)#interface ethernet 0/1/1 to 0/1/20
SwitchName(config-mif-0/1/1-0/1/20)#spanning-tree root-protected
SwitchName(config-if-range)#exit
```

3.22 Port speed and duplex

Speed and duplex **<u>MUST</u>** be set to automatic where it is not possible to set both ends of the connection. Manually setting speed and duplex is only valid where it is possible to manually set both ends of the connections.

Auto-negotiation will fail if the other device has manually set speed and duplex. In this situation, Auto-negotiation must assume half duplex (defined in the spec). Very poor network performance will result if one end of a connection is half duplex and the other is full duplex. Packets will be lost. This can be difficult to diagnose as simple tests such as PING will appear to work correctly.

Consider the following examples:

Table 3.2   Showing the effects of incorrectly manually set speed and duplex

Device	Speed	Duplex	
MX8400	Auto	Auto	
FWS624G	100	Full	
Result	100	Half	Duplex mismatch!

Device	Speed	Duplex	
MX8400	Auto	Auto	
FWS624G	Auto	Auto	
Result	100	Full	Correct operation

Table 3.3 shows the top speed and duplex of several devices commonly found in Ericsson Television systems. This table is included as reference such that the speed and duplex could be checked on a switch to confirm auto-negotiation has selected the optimum setting.

Table 3.3   Control port speed and duplex of devices commonly found in Ericsson Television systems

Device	Top Speed	Best Duplex	Required setting on Device	Required setting on Brocade

MX8400	100	Full	Auto	Auto
MX56xx	10	Half	n/a	Auto
MX52xx	10	Half	n/a	Auto
E57xx	10	Half	n/a	Auto
EN80xx	10	Half	n/a	Auto
EN71xx	100	Full	n/a	Auto
EN81xx	100	Full	Auto	Auto
TT12xx	100	Full	n/a	Auto
RX1290	100	Full	n/a	Auto
RX8xxx	100	Full	n/a	Auto
iPlex	100	Full	n/a	Auto
DEV 1951	100	Full	n/a	Auto
Leitch Panacea	10	Half	n/a	Auto
Leitch Integrator	10	Half	n/a	Auto
Leitch Integrator Gold	10	Half	n/a	Auto
Leitch Platinum	100	Full	n/a	Auto
Moxa nPort	100	Full	n/a	Auto
HP Server*	100	Full	Auto	Auto

* Note: Although it is possible to manually set the server's speed and duplex, it must remain at Auto/Auto. Please see the Server/Client Machine Setup document for further details.

The example below shows how to configure port 24 to be 100Mbit/s at full duplex:

```
SwitchName(config)#interface ethernet 0/1/24
SwitchName(config-if-e1000-0/1/24)#speed-duplex 100-full
SwitchName(config-if-e1000-0/1/24)#exit
```

3.23 Naming ports

It is possible to give each port a name / label /description. This is extremely useful and saves a lot of time when troubleshooting and configuring a system. The example below shows how to give port 2 the description 'EN8190–02'.

```
SwitchName(config)# interface ethernet 0/1/2
SwitchName(config-if-e1000-0/1/2)#port-name EN8190-02
SwitchName(config-if-e1000-0/1/2)#exit
```

3.24 Adding a Gateway

If the Brocade switch is to be connected to a gateway, it can be useful to explicitly define this as the default network.

```
SwitchName(config)#ip default-network 192.168.1.254 255.255.255.0
```

3.25 Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is a Cisco proprietary protocol used by Cisco switches to discover other CDP enabled devices on a network. Brocade support listening to CDP messages from Cisco switches; it is disabled by default. CDP is very helpful when working out which ports are connected to which Cisco switches.

To enable CDP

```
SwitchName(config)#cdp run
```

To disable CDP

```
SwitchName(config)#no cdp run
```

3.26 Disabling passwords encryption

By default all passwords are encrypted and therefore are not human readable when viewing Brocade configuration. This makes it possible to safely archive and distribute the configs without concern that a third party could gain access to a customer's switch. It is possible to disable password encryption, using the following command:

```
SwitchName(config)#no service password-encryption
```

3.27   Saving a configuration

The Brocade switch will execute any configuration changes immediately[this is known as the 'running' configuration. However, these changes will not be saved and if the switch is rebooted the changes will be lost. The running configuration needs to be saved to the startup configuration. Use the following command to save the running config to the startup config:

```
SwitchName#write memory
```

4　Useful Features and Commands

4.1　Viewing the running configuration

The following command can be used to display the currently running configuration:

```
SwitchName#show run
```

4.2　Viewing the current status of a port or VLAN

The following command can be used to display the current status of a port or brief description of all ports. Port 1 has been chosen in an example below:

```
SwitchName#show interface ethernet 0/1/1
SwitchName#show interface brief
```

4.3　Port Monitoring

It is sometimes useful to monitor data sent and received from a device attached to a particular port. All Brocade switches have a port monitoring function that enables the user to duplicate traffic travelling through one port and have it stream out of another. The duplicate traffic can then be analysed on a network analyzer or captured and analysed using a tool such as WireShark. Please see Table 4 below for a number of supported ports on Brocade FWS series switches.

To configure port monitoring, first specify the **mirror port**, then enable monitoring on the **monitored port**, as illustrated below, where port 23 is mirror and port 1 monitored:

```
SwitchName(config)#mirror-port ethernet 0/1/23
SwitchName(config)#interface ethernet 0/1/1
SwitchName(config-if-e1000-0/1/1)#monitor [both | input | output]
Where both | input | output represents all, input or output
monitored packets respectively.
```

Table 4　Number of mirror and monitored ports supported

Port type	Supported number
Ingress mirror ports	1 mirror port
Egress mirror ports	1
Ingress monitored ports	No limit
Egress monitored ports	8

Note:　The *mirror port* is the port to which the monitored traffic is copied. Attach your protocol analyzer to the mirror port. The *monitored port* is the port whose traffic you want to monitor.

4.4   Clearing an existing switch configuration

It is possible to delete the configuration and reboot (or 'reload') the Brocade switch so that it boots-up as if new 'out of the box'.

```
SwitchName#erase startup-config
SwitchName#reload
```

Select **no** if prompted to save changes. The switch should reboot in the default 'fresh-from-the-factory' configuration.

5 Software & Configuration Changes from a Brocade switch

5.1 What is possible

5.1.1 Configurations

Retrieving configurations from a switch is a vital activity. Uploading configurations to a switch can save time when configuring multiple switches or replicating customer issues.

It is recommended that when uploading and downloading configurations, always use the start-up configuration.

Configurations can be downloaded to or uploaded from a switch via TFTP server running on a machine that the switch can access on the network.

5.1.2 Software

Brocade FWS and FCX switches have two flash banks for the code (Primary and Secondary). When a Brocade FWS is first out of the box, it has a layer 2 version of software in the primary bank and what is termed 'base layer 3' code in the secondary bank. The base layer 3 code is the one that will need to be running when the switches are configured in Ericsson Television systems. The code for the Brocade switches is part of the system release. The correct version will need to be used and loaded onto both flash banks of the Brocade switch.

Software can be uploaded/download via a TFTP server; it can also be transferred directly between flash banks if necessary.

5.2 Setting up the TFTP server

Note: Ensure that the TANDBERG or Ericsson TFTP server (which was historically installed as part of the standard nCC installation) is not running on the computer.

A TFTP server can be downloaded from the following: http://tftpd32.jounin.net/

The Tftpd32.exe is standalone and does not require installation. The TFTP server is running when the GUI is open. Any files received will arrive in the **TFTP Root** or **Current Directory**.

5.3 Retrieving the current configuration from a Brocade switch

This example shows how to retrieve the start-up configuration from the switch and save it as a file called **config.text** on the computer, with IP address 192.168.1.50 running the TFTP server.

```
SwitchName#copy startup-config tftp 192.168.1.50 config.txt
```

5.4 Uploading a configuration to a Brocade switch

This example shows how to send the configuration file **config.txt** to a Brocade switch from the computer with IP address 192.168.1.50 running the TFTP server. It is saved as the startup-config and the switch is then reloaded to activate the configuration.

```
SwitchName#copy tftp startup-config 192.168.1.50 config.txt
SwitchName#reload
```

NOTE: Select **no** if prompted to save changes, selecting **yes** will overwrite the recently uploaded file with the current running-config.

5.5 Uploading Software to a Brocade switch

The following example shows uploading the software 'FGL04303.bin' from a computer with IP address 192.168.1.50 running the TFTP server. The software is saved in the primary flash bank. The switch is then reloaded to activate the software.

```
SwitchName#copy tftp flash 192.168.1.50 FGL4303.bin primary
SwitchName#reload
```

5.6 Copying Software between Flash Banks

The following example shows copying the code from the primary flash bank to the secondary.

```
SwitchName#copy flash flash secondary
```

The following example shows copying the code from the secondary flash bank to the primary.

```
SwitchName#copy flash flash primary
```

BLANK