Cisco Switch Fundamentals

iSIS System Manual Collection (Internal)

Copyright

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 Tables

1 What this document describes

This document is intended to provide information regarding the basic setup of a Cisco Catalyst switch / router.

The document describes the rolls in which a Cisco switch / router can be deployed and gives specific commands for a given roll. The four rolls are:

- Basic Control Network
- Redundant Control Network
- Basic Data Network (input and output)
- Advanced Data Network

It is strongly recommended that all of the settings described in chapter 3 of this document should be setup on any Cisco switch / router in an Ericsson Television system regardless of the roll in to which the switch / router is deployed (control network, or data network).

2 Overview

Ericsson Television supply different network switches / routers for 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 switches are used. These switches must be configured before being deployed to ensure correct operation – an un-configured Cisco 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 set up of the Cisco Catalyst switch

3.1 Serial control

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

Table 3.1: Default Cisco 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 C2960:

```
Switch>
```

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

Note: If the unit is new, you will be asked if you wish to enter the initial setup dialogue. Type ‘no’ and press return.

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 ‘#’.

```
Switch>enable

Switch#
```

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.

```
Switch#configure terminal

Switch(config)#
```

The ‘configure terminal’ command may be abbreviated to ‘conf t’.

3.4 Naming the Switch

All switches in a system should be named 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.

```
Switch(config)#hostname SwitchName

SwitchName(config)#
```

3.5 Entering an Enable Password

It is necessary to protect access to the terminal session. The password usually entered in Ericsson Television systems is ‘cisco’ and is shown below.

```
SwitchName(config)#enable password cisco
```

3.6 Entering a ‘secret’ Password

It is not standard practice for Ericsson Television to configure a ‘Secret’ password. Customer managed switches are often configured with an encrypted ‘Enable’ password which results in the ‘Enable’ password being not human readable when viewing a Cisco configuration. This ‘Secret’ password replaces the ‘Enable’ password. If both are entered, the Cisco will use only the ‘Secret’ password. The ‘Secret’ password must not be the same as the ‘Enable’ password and so where used, it is recommended that, only the ‘Secret’ password is used. The following command shows how to enter ‘cisco’ as the secret password.

```
SwitchName(config)#enable secret cisco
```

3.7 Creating a VLAN

Not all models of Cisco switches automatically create a VLAN if a port is added to one that does not already exist. An example of this type of switch is the 4948.

To ensure that a VLAN is created, it is recommended to enter the VLAN’s configuration. This is different to the VLAN’s interface configuration and the command is subtly different. The example below shows how to create VLAN 11.

```
SwitchName(config)#vlan 11

SwitchName(config-vlan)exit
```

3.8 Assigning ports to a VLAN

When new, out of the box, all ports on the switch are in VLAN 1. This default VLAN will not be explicitly displayed when viewing the configuration, it is easy to forget that the port has been placed into a VLAN. Therefore, it is helpful to put the required ports into a known, manually specified, VLAN that will be displayed when viewing the switch configuration. The example below shows all ports in the range 1 to 24 being put into VLAN 11, a commonly used VLAN number. The exit command is used exit from the interface configuration.

```
SwitchName(config)#interface range fastEthernet 0/1 – 24

SwitchName(config-if-range)#switchport

SwitchName(config-if-range)#switchport access VLAN 11

SwitchName(config-if-range)#exit
```

It is possible to abbreviate these commands such that the following may be entered:

```
SwitchName(config)#int ran fa0/1 -24

SwitchName(config-if-range)#swit

SwitchName(config-if-range)#swit acc vlan 11

SwitchName(config-if-range)#exit
```

Note: In the example fa0/1, the ‘fa’ refers to the Cisco abbreviation for ‘fast Ethernet’ (100BASE/T). (gi is the Cisco abbreviation for ‘Gigabit Ethernet’). The ‘0’ addresses the card in the first slot of the chassis (some bigger switches have more than one slot or ‘layer’ of ports). The ‘1’ addresses the first interface on this layer.

3.9 Assigning an IP address to a VLAN

It is often necessary to contact the switch via an IP address. The switch must be given a known IP address. This is often assigned to the VLAN. It will then be possible to contact the switch on the given IP address from any port in that VLAN. 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 vlan 11

SwitchName(config-if)#ip address 192.168.1.253 255.255.255.0

SwitchName(config-if)#exit
```

3.10 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.

All control and data networks require an IGMP Querier to be enabled on all switches. The examples below show how to turn on IGMP snooping and enable the Querier . This command is the same for layer 2 (SMI / IP Base) and layer 3 (EMI / IP Services) Cisco Catalyst switches:

```
SwitchName(config)#ip igmp snooping

SwitchName(config)#ip igmp snooping querier
```

3.11 nCC SNMP Configuration

The control and data switches 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 Cisco by using the following commands:

```
SwitchName(config)#snmp-server community public RO

SwitchName(config)#snmp-server community private RW
```

3.12 Telnet

It is desirable to assess the switch and alter the configuration remotely without using the blue serial cable. Telnet can be used to achieve this. The Cisco C2960 and C3560 switches / routers support up to 16 Virtual Terminal Interfaces (VTY), these are known to the switch as ‘lines’ and are numbered 0 to 15. In the example below, all of these are configured to allow Telnet access. As a security measure, a Telnet password should set in addition to the mandatory ‘Enable’ password (see Entering an Enable Password), the password in the example (and in all systems Ericsson Television deliver) is set to ‘cisco’. The required commands are shown below:

```
SwitchName(config)#line vty 0 15

SwitchName(config-line)#password cisco

SwitchName(config-line)#login

SwitchName(config-line)#exit
```

It should now be possible to connect to the switch using any port in VLAN 11 and Telnet into the switch.

3.13 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)#spanning-tree mode rapid-pvst
```

Configuring the priority of each VLAN in a control network is essential where a redundant network is used (redundant control networking is covered in-depth in a different document in the iSiS collection). Priority is a Spanning Tree parameter. Each switch may have a different priority. The switch with the lowest number has the highest priority. VLAN 11 is used in the example below and is give a priority of 20480 (the switch will list valid priority values).

```
SwitchName(config)#spanning-tree vlan 11 priority 20480
```

3.14 Switchport mode access

By default, a switchport will be placed into the ‘dynamic’ mode. That means that it could be dynamically turned into a trunk port by an external controller. This functionality is never required in Ericsson Television systems. The role of each port is static - a trunk port is always a trunk port and a port which is not a trunk port never will be. The behaviour of the front panel status light is affected with regard to spanning-tree and switchport mode. For example: If a port is blocked and is ‘switchport mode dynamic’ it will remain green. Whereas, if the port is blocked and is ‘switchport mode access’ the front panel light will change to orange. Thus, to aid diagnostics, all ports should be set to switchport mode access unless there is a compelling reason to do otherwise.

```
SwitchName(config)#int ran fa0/1 - 24

SwitchName(config-if-range)switchport mode access
```

3.15 Portfast

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. ‘Portfast’ can be used to disable this checking and avoid the delay.

Portfast 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 or an iPlex (in some cases this can also be setup for these devices). In the example below, Portfast is enabled on ports in the range 1 to 24.

```
SwitchName(config)#int ran fa0/1 - 24
SwitchName(config-if-range)#spanning-tree portfast

SwitchName(config-if-range)#exit
```

3.16 Spanning Tree root guard

Spanning tree root guard is intended to prevent problems caused when an unknown cable is connected to a switch in the control or data network. Spanning tree root guard should be enabled on all ports where the root bridge should not appear.

Do not enable root guard on ports/links between switches/routers where spanning tree is used. In the example, spanning tree root guard is configured for ports 1 to 20.

```
SwitchName(config)#int ran fa0/1 – 20

SwitchName(config)#spanning-tree guard root
```

3.17 Port speed and duplex

Manually setting speed and duplex is only recommended when connecting a Cisco switch / router to another Cisco switch /router. In this case, the speed and duplex be manually set on both ends of the connection. Auto MDIX is disabled when speed and duplex are manually defined and so a twisted, or ‘crossover’ cable must be used in this case.

Speed and duplex **MUST** be set to automatic where it is not possible to set both ends of the connection.

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	
C2960	100	Full	
Result	100	MX8400 negotiates to Half duplex	Duplex mismatch!
MX8400	Auto	Auto	
C2960	Auto	Auto	

Device	Speed	Duplex	
Result	100	Full	Correct operation

Table 3.3 shows the control Ethernet top speed and duplex of several devices commonly found in Ericsson Television systems, this 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 Cisco
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 Setup chapter for further details.

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

```
SwitchName(config)#int fa0/24

SwitchName(config-if)#speed 100
SwitchName(config-if)#duplex full

SwitchName(config-if)#exit
```

3.18 Naming ports and VLANs

It is possible to give each port and VLAN 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 (description can be abbreviated to ‘desc’) ‘EN8130_01’. The same principle can be applied to naming VLANs.

```
SwitchName(config)#int fa0/2

SwitchName(config-if)#desc EN8130_01

SwitchName(config-if)#exit
```

3.19 Adding a Gateway

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

```
SwitchName(config)#ip default-gateway 192.168.1.254
```

The ‘default gateway’ command has no effect if ‘IP routing’ is enabled (enabling IP routing is only possible if the switch / router supports, and is licensed for, Layer 3 functionality. In this case, a static route should be used. This will be the ‘gateway of last resort’ to be used if the router has traffic which it otherwise would not know where to route, it does not route everything to this address!

```
SwitchName(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.254
```

3.20 DHCP

DHCP is used to dynamically assign IP addresses, the Cisco switches can also use this to send their config files across a network to an un-configured switch. In some cases, it has been observed that this traffic is processed by, and may cause poor performance of, Ericsson Television equipment and so the DHCP service should be disabled on Ericsson Television supplied switches / routers. The command to disable this service is shown below:

```
SwitchName(config)#no service dhcp
```

3.21 Domain Lookup

It is possible for the Cisco switch to search for a Domain Name Server (DNS) if the switch receives a command it does not understand. It will attempt to find a DNS in an attempt to resolve this command/name with an IP address. This feature should be manually turned off thus:

```
SwitchName(config)#no ip domain-lookup
```

3.22 Cisco Discovery Protocol (CDP)

Cisco Discovery Protocol (CDP) is a very useful Cisco proprietary protocol used by Cisco switches to discover other Cisco devices on a network. CDP is enabled by default and is very helpful when working out which ports are connected to which Cisco switches. Previous versions of the iSIS manual recommended that CDP be disabled. This was bad advice! CDP should not be turned off.

To globally enable CDP

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

To globally disable CDP

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

3.23 VTP

VLAN Trunking Protocol (VTP) enables a VTY controller to assign VLANs on switches in a network. The control switch should have this feature turned off as the VLAN configuration must not be accidentally manipulated by a rogue VTP controller. The command is shown below.

```
SwitchName(config)#vtp mode transparent
```

3.24 Encrypting all passwords

Although not standard practice at Ericsson Television, it is possible to encrypt all passwords such all passwords are not human readable when viewing the Cisco configuration. It is then possible to safely archive and distribute the configs without the fear that a third party could gain access to a customer’s switch. It remains possible to upload a config that has encrypted passwords, the Cisco will understand the encryption!

```
SwitchName(config)#service password-encryption
```

3.25 4948 interfaces 45-48

A 4948 switch is not the same as C3560s when it comes to the SFPs. The 4 SFPs on a 4948 are shared with the last 4 copper RJ45 interfaces on the switch. So the maximum number of interfaces that can be used at once is 48. By default, the switch is configured to use the SFPs for interfaces 45-48. A command is needed to configure the switch to use the RJ45s:

```
SwitchName(config)#interface range gi1/45-48

SwitchName(config-if-range)#media-type rj45
```

If there is a need to go back to using the SFPs then the command is:

```
SwitchName(config-if-range)#media-type fibre
```

3.26 Saving a configuration

The Cisco switch will action any configuration changes immediately. However, these changes will not be saved and if the switch is rebooted the changes will be lost. Use the following command to save the configuration:

```
SwitchName#write
```

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 all ports or VLAN

The following command can be used to display the current status of a port or VLAN. Port 1 has been selected for the example below.

```
SwitchName#show interface status
```

4.3 Port Monitoring

It is sometimes useful to monitor data sent and received from a device attached to a particular port. All Cisco 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. Cisco switches can run up to two monitor sessions at the same time. Any configuration applied to the destination port will be ignored whilst it is used as a monitoring port. Traffic can be filtered so the RX, TX or BOTH directions can be observed. In order to setup monitoring the following commands are used:

Setup the monitoring session source port:

```
SwitchName(config)#monitor session 1 source int fa0/1 both
```

Setup the monitoring session destination port:

```
SwitchName(config)#monitor session 1 destination int fa0/2
```

To remove the monitor function, the following can be entered:

```
SwitchName(config)#no monitor session 1
```

4.4 Clearing an Existing Switch Configuration

It is possible to delete the configuration and reboot (or ‘reload’) the Cisco switch such that it boots up as if new ‘out of the box’:

```
SwitchName#delete flash:config.text

(press enter to confirm)

y

SwitchName#delete flash:vlan.dat

(press enter to confirm)

y

SwitchName#reload
```

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

5 Upgrading, downgrading software and uploading and downloading configurations from a Cisco switch

5.1 What is possible

Retrieving the current configuration from a Cisco switch is nearly always required. Uploading a configuration to a Cisco switch is also a common requirement.

Cisco switches installed into systems may require upgrading or downgrading when new switches are installed into an existing system, or if switches need upgrading.

It is possible to extract the software currently installed on a Cisco switch and upload it to a computer. It is also possible to download software from a computer to a Cisco switch.

In the cases a tftp server will need to be installed and running on the computer.

When obtained from a Cisco switch, the Cisco software is compressed as a .tar (compressed) file form. It is usual to load the Cisco software from a computer to the Cisco as a .tar file.

5.2 Setting up the TFTP server

Note: Ensure that the TANDBERG or Ericsson TFTP server service (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 config from a Cisco switch

In this example, the currently running configuration is to be downloaded from the switch and saved as ‘config.text’ on the computer with IP address 192.168.1.50 running the TFTP server.

```
SwitchName#copy flash:config.text
tftp://192.168.1.50/config.text
```

The VLAN database is an important file which the Cisco IOS automatically maintains which remains hidden from the user. This file should also be retrieved and stored with the config.text file.

The following example shows how to retrieve the VLAN database and save it on the computer with IP address 192.168.1.50 running the TFTP server.

```
SwitchName#copy flash:vlan.dat tftp://192.168.1.50/vlan.dat
```

Note: The storage medium on each Cisco model may differ. For example, the C4948 stores files on nvram, not flash. The above commands should be changed with nvram replacing flash. For example:
`copy nvram:vlan.dat`

5.4 Uploading a config to a Cisco switch

It is possible to upload a config to a Cisco switch via null modem or serial. However, these instructions assume that the Cisco is configured with an IP address and there is network connectivity with the switch.

Uploading a saved config to a switch will add to any parameters already entered, it will not replace the existing config. The config.text file and VLAN.dat should be deleted from the switch before uploading a config.

In this example, the currently running configuration is removed from the switch, the config.text and VLAN.dat stored on the computer with IP address 192.168.1.50 running a TFTP server are uploaded to the switch and the switch is rebooted.

```
SwitchName#delete flash:config.text

SwitchName#delete flash:vlan.dat

SwitchName#copy tftp://192.168.1.50/config.text
flash:config.text

SwitchName#copy tftp://192.168.1.50/vlan.dat flash:vlan.dat

reload
```

Select ‘no’ if prompted to save changes. The switch should reboot. When booted check that the running config is as expected.

Note: The storage medium on each Cisco model may differ. For example, the C4948 stores files on nvram, not flash. The above commands should be changed with nvram replacing flash. For example: `copy://tftp:192.168.1.50/vlan.dat nvram:vlan.dat`

5.5 Loading software onto a Cisco switch (not C4948)

In this example, the file ‘Cisco_upgrade.tar’, stored in the c:\tftp-root directory on the TFTP server with IP address 192.168.1.50 will be loaded onto the Cisco. The Cisco will extract this software, reboot and use this new software.

```
SwitchName#archive download-sw /overwrite /reload
tftp://192.168.1.50/Cisco_upgrade.tar
```

Check that the switch is using the new software when it has finished rebooting.

5.6 Loading software onto a Cisco C4948 router

5.6.1 Remove unused software from router

Before upgrading, there must be enough space for the new code version. There normally is, but to make sure, check the currently running version and remove unused code versions from the router.

```
SwitchName#show version
```

Make a note of the Version information.

```
SwitchName#cd bootflash:
```

```
SwitchName#dir
```

This will list all files in the bootflash. This will include the currently running software. Make a note of other software images, these should be deleted thus: (Do not delete the currently running software image!)

```
SwitchName#delete bootflash:/<filename>
```

5.6.2 Upload New version

In this example, the file ‘cat4500-entservicesk9-mz.122-54.SG.bin’, stored in the c:\tftp-root directory on the TFTP server with IP address 192.168.1.50 will be uploaded to the Cisco.

```
SwitchName#copy tftp://192.168.1.50/cat4500-entservicesk9-
mz.122-54.SG.bin bootflash:
```

5.6.3 Verify new version

It is strongly recommended that the new code is verified by the router before attempting to use it. In the following example, the C4948 will verify the file ‘cat4500-entservicesk9-mz.122-54.SG.bin’.

```
SwitchName#verify bootflash:cat4500-entservicesk9-mz.122-
54.SG.bin
```

The output from this command will be reported differently depending on software version that is currently running. Some versions will report ‘success’ or ‘verified’ some versions will not report anything other than a long run of ‘C’s. Some versions will report three lines of debug, one of which will suggest an issue with a missing checksum but the final line will report ‘completed successfully’. These are all OK.

5.6.4 Set the Configuration Register

When the ‘show ver’ is performed, the router will report ‘Configuration register is 0x,<some numbers>. The configuration register should be set to 0x2101. This can be set thus (note; you must be in ‘conf t’):

```
SwitchName(config)#config-register 0x2101
```

5.6.5 Set the boot variable

Issue the following command:

```
SwitchName#show bootvar
```

The output should resemble the following example:

```
BOOT variable = bootflash:<filename>,1;r

CONFIG_FILE variable does not exist

BOOTLDR variable does not exist

Configuration register is 0x2102
```

The boot variable should be removed and re-added to use the newly uploaded software thus:

```
SwitchName(config)#no boot system flash
bootflash:<old_software_filename>

SwitchName(config)#boot system flash
bootflash:<new_software_filename>
```

5.6.6 Remove the previous (currently running) software version

The router will boot up using the first software image in the bootflash directory. Therefore, remove the existing software version from the bootflash directory such that only one version remains.

```
SwitchName#SwitchName#delete
bootflash:/<old_software_filename>
```

5.6.7 Reboot the router and check the software version

Save the currently running configuration and then reboot the switch thus.

```
SwitchName#wr
```

```
SwitchName#reload
```

Confirm the reload. Check the software version in use once the switch has booted.

5.7 Downloading software from a Cisco switch

In this example, the currently running software will be downloaded from the Cisco. The software will be saved in the TFTP root directory with the filename ‘Cisco_software.tar’

```
SwitchName#archive upload-sw
tftp://192.168.1.50/Cisco_upgrade.tar
```