CHAPTER 2

System Configuration Group

System Configuration refers to the group of functions used to configure system interaction with peripheral equipment, storage devices, and host computers. These functions are accessed from the system configuration group and consist of the following types of objects:

- PasswdTable (a four column password table)—Controls user access to the system
- Master timing link selection—Selects time source
- Clock and calendar configuration—Changes clock/calendar settings
- Active to standby switch—Switches control from active to standby
- License configuration—Updates time-slot allocation license or displays current usage
- System features—Modifies system operation characteristics
- Firmware configuration—Displays version, revision, field software revision, and checksum information
- File system configuration—Specifies the storage devices and directories for system log and system trace files
- Peripheral configuration—Defines operating parameters for system peripheral equipment
- Host configuration—Configures host interfaces and software overlays
- System host configuration—Configures parameters for interaction between the system and the host
- System shutdown—Resets system controller from a remote management station

System configuration utilities enable you to do the following:

- Define operating parameters for system printers and local/remote administration consoles, including Ethernet Telnet connections (for systems equipped with the Ethernet Communications option)
- Specify devices and directories for file system storage/retrieval
- Configure host interfaces and software overlays
- Add system users and modify passwords/access levels
- Set system clock/calendar
- Display/change system features
- Assign access levels and map function keys to each system administration screen
- View the system software and firmware configuration
- Update the system’s Time-Slot Allocation License or view the system’s current usage of time-slots
- Configure system host parameters

For further information on the system configuration, refer to the *Cisco VCO/4K System Administrator's Guide.*

Password Configuration

Use the objects in this table to create or change system passwords and set access levels for up to 16 system users. Each system user is identified by a unique username, an alphanumeric password and an access level. The ability to update this configuration information is limited by a user's access level. Access levels determine the user's ability to modify screen information and update the system database. For further information on password configuration, refer to the *Cisco VCO/4K System Administrator's Guide.*

passwdTable

{config 1}

Description

Table of the authorized users and their password.

Object Identifier

1.3.6.1.4.1.886.1.1.1

Data Type

Sequence of PasswdEntry

Access Policy

Not accessible

Status

Mandatory

passwdEntry

{passwdTable 1}

Description

An index into the password (passwd) table.

Object Identifier

1.3.6.1.4.1.886.1.1.1.1

Data Type

PasswdEntry

Access Policy

Not accessible

Status

Mandatory

Index

{passwdIndex}

PasswdEntry

Sequence

passwdIndex	Integer
userName	DisplayString
accessLevel	Integer
passwdString	DisplayString
passwdErrorStatus	Integer
passwdOwnerString	OwnerString
passwdEntryStatus	EntryStatus

passwdIndex

{passwdEntry 1}

Description

Contains the user's password. You must add users to the password table sequentially.

Object Identifier

1.3.6.1.4.1.886.1.1.1.1.1

Data Type

Integer

Access Policy

Read only

Status

Mandatory

userName

{passwdEntry 2}

Description

The user's name (consists of 3 to 15 upper- and lowercase alphanumeric characters).

Object Identifier

1.3.6.1.4.1.886.1.1.1.1.2

Data Type

DisplayString

Access Policy

Read-write

Status

Mandatory

accessLevel

{passwdEntry 3}

Description

Specifies a user's access level to the information in the database.

Object Identifier

1.3.6.1.4.1.886.1.1.1.1.3

Data Type

Integer. The valid numerical values and their meanings are shown in the following table:

Value	Meaning
0	Read and database update access to all screens
1	Varies based on screen access configuration
2	Varies based on screen access configuration
3	Read access only to all objects

Access Policy

Read-write

Status

Mandatory

passwdString

{passwdEntry 4}

Description

Specifies the password associated with the username entered. Issuing an SNMP_GET command on this attribute returns the encoded password.

Object Identifier

1.3.6.1.4.1.886.1.1.1.1.4

Data Type

DisplayString. Length of the user's password is from 4 to 12 upper- and lowercase alphanumeric characters.

Access Policy

Read-write

Status

Mandatory

passwdErrorStatus

{passwdEntry 5}

Description

Registers the last error that occurred in this object.

Object Identifier

1.3.6.1.4.1.886.1.1.1.1.5

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String
4096	invalidPasswdId
4097	passwdNotEmpty
4098	invalidPosition
4099	passwdAlreadyExists

Access Policy

Read only

Status

Mandatory

passwdOwnerString

{passwdEntry 6}

Description

The entity that configured this object and is therefore using the resources assigned to it.

Object Identifier

1.3.6.1.4.1.886.1.1.1.1.6

Data Type

OwnerString

Access Policy

Read-write

Status

Mandatory

passwdEntryStatus

{passwdEntry 7}

Description

The status of the password object.

Object Identifier

1.3.6.1.4.1.886.1.1.1.1.7

Data Type

EntryStatus

Access Policy

Read-write

Status

Mandatory

passwdTableLastModified

{config 2}

Description

The time, displayed in hundredths of a second, since the password table was last modified. Helps NMS application developers determine the polling of the agent parameters.

Object Identifier

1.3.6.1.4.1.886.1.1.2

Data Type

TimeTicks

Access Policy

Read only

Status

Mandatory

FTP Configuration Group

Use the objects in this table to create or change system passwords and set access levels for up to 16 system users. Each system user is identified by a unique username, an alphanumeric password and an access level. The ability to update this configuration information is limited by a user's access level. Access levels determine the user's ability to modify screen information and update the system database. For further information on password configuration, refer to the *Cisco VCO/4K System Administrator's Guide.*

ftppwdTable

{config 29}

Description

Table of the authorized users and their password.

Data Type

Sequence of FtpPasswdEntry

Access Policy

Not accessible

Status

Mandatory

ftppwdEntry

{ftppwdTable 1}

Description

An entry into the ftp password (passwd) table.

Data Type

FtpPasswdEntry

Access Policy

Not accessible

Status

Mandatory

Index

{ftppwdIndex}

FtpPasswdEntry

Sequence

ftppwdIndex	INTEGER
ftpuserName	DisplayString
ftpaccessLevel	INTEGER
ftppwdString	DisplayString
ftppwdErrorStatus	INTEGER
ftppwdOwnerString	OwnerString
ftppwdEntryStatus	EntryStatus

ftppwdIndex

{ftppwdEntry 1}

Description

An index into the ftp passwd table. You must add users to the password table sequentially.

Data Type

INTEGER

Access Policy

Read only

Status

Mandatory

ftpuserName

{ftppwdEntry 2}

Description

The user's name consists of 3 to 15 upper- and lowercase alphanumeric characters.

Data Type

DisplayString (SIZE (3..15))

Access Policy

Read-write

Status

Mandatory

ftpaccessLevel

{ftppwdEntry 3}

Description

Possible values and their meanings are listed below.

Data Type

Integer. The valid numerical values and their meanings are shown in the following table:

Value	Meaning
0	Read and database update access to all screens
1	Varies based on screen access configuration
2	Varies based on screen access configuration
3	Read access only to all screens

Access Policy

Read-write

Status

Mandatory

ftppwdString

{ftppwdEntry 4}

Description

Specifies the ftp password associated with the username entered. Issuing an SNMP_GET command on this attribute returns the encoded password.

Data Type

DisplayString. Length of the user's password is from 4 to 12 upper- and lowercase alphanumeric characters.

Access Policy

Read-write

Status

Mandatory

ftppwdErrorStatus

{ftppwdEntry 5}

Description

Registers the last error that occurred on this entry.

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String
6912	invalidFtpPasswdId
6913	ftppwdNotEmpty
6914	invalidPosition
6915	ftppwdAlreadyExists

Access Policy

Read only

Status

Mandatory

ftppwdOwnerString

{ftppwdEntry 6}

Description

The entity that configured this entry.

Data Type

OwnerString

Access Policy

Read-write

Status

Mandatory

ftppwdEntryStatus

{ftppwdEntry 7}

Description

The status of this entry.

Data Type

EntryStatus

Access Policy

Read-write

Status

Mandatory

ftppwdTableLastModified

{config 30}

Description

The time, displayed in hundredths of a second, since the password table was last modified. Helps NMS application developers determine the polling of the agent parameters.

Data Type

TimeTicks

Access Policy

Read only

Status

Mandatory

Master Timing Link Configuration

The master timing link configuration is used to select the system T1 and PRI timing source. You can derive timing from VCO internal clocking or from an incoming T1 or PRI bit stream. If incoming timing is used, the incoming reference is lost and the system automatically tries to synchronize with the internal clock. For further information on the master timing link, refer to the *Cisco VCO/4K System Administrator's Guide.*

syncsource

{config 3}

Object Identifier

1.3.6.1.4.1.886.1.1.4

masTimingSource

{syncsource 1}

Description

Indicates the source of the reference signal currently used for T1 synchronization.

Object Identifier

1.3.6.1.4.1.886.1.1.4.1

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String	Meaning
1	internal	Use timing supplied by NBC3 for synchronization.
2	external	Use external network synchronization.
3	incoming	Use timing from an incoming digital stream.

Access Policy

Read-write

Status

Mandatory

masPrimaryTimingCard PhyAddr

{syncsource 2}

Description

Specifies the physical address of the card from which clocking is to be derived. The physical address must be that of an online digital trunk card (can be a T1, E1, MVDCT1, or PRI).

Setting the physical address of the primary timing source initializes the secondary timing source. It is not mandatory to set the secondary timing source.

To display the physical address, issue an SNMP_GET command on the card's physical address.

This object can only be set if masTimingSource is set to incoming.

Object Identifier

1.3.6.1.4.1.886.1.1.4.2

Data Type

Integer

Access Policy

Read-write

Status

Mandatory

masSecondaryTiming CardPhyAddr

{syncsource 3}

Description

Specifies the physical address of the card from which clocking is to be derived. The hardware address must be that of an on-line digital trunk card. The card can be a T1, E1, MVDCT1, or PRI.

To display the physical address, issue an SNMP_GET command on the card's physical address.

This object can only be set if masTimingSource is set to incoming and masPrimaryTimingCardPhyAddr is set to a valid value.

Object Identifier

1.3.6.1.4.1.886.1.1.4.3

Data Type

Integer

Access Policy

Read-write

Status

Mandatory

masTimingErrorStatus

{syncsource 4}

Description

Registers the last error that occurred in this object.

Object Identifier

1.3.6.1.4.1.886.1.1.4.4

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String
3328	invalidCardType
3329	cardDoesNotExist
3330	secondarySameAsPrimary
3331	illegalOperation

Access Policy

Read only

Status

Mandatory

masTimingOwnerString

{syncsource 5}

Description

The entity that configured this object and is therefore using the assigned resources.

Object Identifier

1.3.6.1.4.1.886.1.1.4.5

Data Type

OwnerString

Access Policy

Read-write

Status

Mandatory

masTimingEntryStatus

{syncsource 6}

Description

The status of this table object.

Object Identifier

1.3.6.1.4.1.886.1.1.4.6

Data Type

NonTabEntryStatus

Access Policy

Read-write

Status

Mandatory

Clock/Calendar Configuration

Use the clock/calendar configuration to change the system date, time, and day-of-week settings. The VCO clock should be set by the host on a regular basis to ensure that host time and VCO time are synchronized. For further information on the features in the clock/calendar configuration section, refer to the *Cisco VCO/4K System Administrator's Guide.*

calendar

{config 4}

Object Identifier

1.3.6.1.4.1.886.1.1.4

sysDay

{calendar 1}

Description

The day of the week. For example, Wednesday (4).

Object Identifier

1.3.6.1.4.1.886.1.1.4.1

Data Type

Integer. Valid values are from 1 to 7.

Access Policy

Read only

Status

Mandatory

sysMonth

{calendar 2}

Description

The month of the year. For example, October (10).

Object Identifier

1.3.6.1.4.1.886.1.1.4.2

Data Type

Integer. Valid values are from 1 to 12.

Access Policy

Read-write

Status

Mandatory

sysDate

{calendar 3}

Description

The date. For example, 19.

Object Identifier

1.3.6.1.4.1.886.1.1.4.3

Data Type

Integer. The months and the corresponding numerical values are shown in the following table:

Month	Valid Values
January	1 to 31
February	1 to 29
March	1 to 31
April	1 to 30
May	1 to 31
June	1 to 30
July	1 to 31
August	1 to 31
September	1 to 30
October	1 to 31
November	1 to 30
December	1 to 31

Access Policy

Read-write

Status

Mandatory

sysYear

{calendar 4}

Description

This object represents the number of the current year minus 1900. For example, the year 1999 is returned as 99.

This object will be deprecated for all software releases following version 5.1(3). When this occurs, the object calendarYear should be used to replace the object sysYear.

Object Identifier

1.3.6.1.4.1.886.1.1.4.4

Data Type

Integer. Valid values are from 91 to 219.

Access Policy

Read-write

Status

Deprecated

sysHour

{calendar 5}

Description

The hour. For example, the 11 in 11:12:22 (U.S. format).

Object Identifier

1.3.6.1.4.1.886.1.1.4.5

Data Type

Integer. Valid values are 0 to 23.

Access Policy

Read-write

Status

Mandatory

sysMin

{calendar 6}

Description

The minutes. The 12 in 11:12:22 (U.S. format).

Object Identifier

1.3.6.1.4.1.886.1.1.4.6

Data Type

Integer. Valid values are 0 to 59.

Access Policy

Read-write

Status

Mandatory

sysSec

{calendar 7}

Description

The seconds. The 22 in 11:12:22 (U.S. format).

Object Identifier

1.3.6.1.4.1.886.1.1.4.7

Data Type

Integer. Valid values are 0 to 59.

Access Policy

Read-write

Status

Mandatory

calendarErrorStatus

{calendar 8}

Description

Registers the last error that occurred in this entry.

Object Identifier

1.3.6.1.4.1.886.1.1.4.8

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String
4608	invalidYear
4609	invalidMonth
4610	invalidDate
4611	invalidHour
4612	invalidMinute
4613	invalidSecond

Access Policy

Read only

Status

Mandatory

calendarOwnerString

{calendar 9}

Description

The entity that configured the object and is therefore using the entry assigned to it.

Object Identifier

1.3.6.1.4.1.886.1.1.4.9

Data Type

OwnerString

Access Policy

Read-write

Status

Mandatory

calendarEntryStatus

{calendar 10}

Description

The status of the table entry.

Object Identifier

1.3.6.1.4.1.886.1.1.4.10

Data Type

NonTabEntryStatus

Access Policy

Read-write

Status

Mandatory

calendarYear

{calendar 11}

Description

This object represents an integer value for the current year. Valid values are 1991 through 2119. This object replaces sysYear which uses a different date format.

Note This object will only be available for system software releases subsequent to Version 5.1(3).

Object Identifier

1.3.6.1.4.1.886.1.1.4.11

Data Type

Integer

Access Policy

Read-write

Status

Mandatory

Hardware Configuration

busType

{hardware 1}

Description

The capacity of the switching bus. B-bus systems allow for 1776 timeslots, C-bus for 3968.

Object Identifier

1.3.6.1.4.1.886.1.1.5.1

Data Type

Integer: 1 for B-bus, 2 for C-bus

Access Policy

Read only

Status

Mandatory

Active To Standby

Use the active to standby table to switch the active system to standby status. For further information, refer to the *Cisco VCO/4K System Administrator's Guide.*

actsby

{config 15}

Object Identifier

1.3.6.1.4.1.886.1.1.15

actsbySwitch

{actsby 1}

Description

Enables you to switch the active system to standby status. This object is only set to standby from the active side. However, it returns the correct status on both standby (1) and active (2) sides.

Object Identifier

1.3.6.1.4.1.886.1.1.15.1

Data Type

Integer. The valid numerical values are 1 (standby) and 2 (active).

Access Policy

Read-write

Status

Mandatory

actsbyErrorStatus

{actsby 2}

Description

Registers the last error that occurred in this entry.

Object Identifier

1.3.6.1.4.1.886.1.1.15.2

Data Type

Integer. The possible numerical and string values are shown in the following table:

Value	String
3584	cannotSwitchStandby
3585	fileSyncNotDone
3586	notRedundantSystem
3587	invalidValue

Access Policy

Read only

Status

Mandatory

actsbyOwnerString

{actsby 3}

Description

The entity that configured this object and is therefore using the entry assigned to it.

Object Identifier

1.3.6.1.4.1.886.1.1.15.3

Data Type

OwnerString

Access Policy

Read-write

Status

Mandatory

System Shutdown

Use the system shutdown option to reset the system controller from the system administration console. When you select this option, the system closes all open system files, terminates host communication and resets the system controller.

In a nonredundant system, if you select this option, all calls being carried by the system are torn down. If the system is redundant, control is passed to the standby system controller and all stable calls are maintained. Calls that have not reached a stable state are torn down.

systemShutdown

{config 16}

Description

Resets the system controller. With this object set, the system closes all open system files, terminates host communication, and resets the system controller.

If you select this option in a nonredundant system, the system tears down all calls carried by the system. In a redundant system, control is passed to the standby system controller and stable calls are maintained. Unstable calls are torn down.

Object Identifier

1.3.6.1.4.1.886.1.1.16

Data Type

Integer. The only valid value is 19950426.

Access Policy

Read-write

Status

Mandatory

License Configuration

Use the entries in this section to update your Time-Slot Allocation License or display the system's information concerning the current usage of time-slots. For further information on license configuration, refer to the *Cisco VCO/4K System Administrator's Guide.*

sysLicenseTable

{config 17}

Description

The system license table.

Object Identifier

1.3.6.1.4.1.886.1.1.17

Data Type

Sequence of SysLicenseEntry

Access Policy

Not accessible

Status

Mandatory

sysLicenseEntry

{sysLicenseTable 1}

Description

Entry in the license table.

Object Identifier

1.3.6.1.4.1.886.1.1.17.1

Data Type

SysLicenseEntry

Access Policy

Not accessible

Status

Mandatory

Index

{sysLicenseIndex}

SysLicenseEntry

Sequence

sysLicenseIndex	Integer
sysTimeSlotAllotted	Integer
sysTimeSlotLicensed	Integer
sysTimeSlotRemaining	Integer
sysSerialNum	DisplayString
sysLicenseNum	DisplayString
sysLicenseOwnerString	OwnerString
sysLicenseEntryStatus	FixedTabEntryStatus

sysLicenseIndex

{sysLicenseEntry 1}

Description

The index into the system license table. One (1) is the active side, two (2) is the standby side (in a redundant system).

Object Identifier

1.3.6.1.4.1.886.1.1.17.1.1

Data Type

Integer

Access Policy

Read only

Status

Mandatory

sysTimeSlotAllotted

{sysLicenseEntry 2}

Description

Number of time-slots currently assigned in the system.

Object Identifier

1.3.6.1.4.1.886.1.1.17.1.2

Data Type

Integer

Access Policy

Read only

Status

Mandatory

sysTimeSlotLicensed

{sysLicenseEntry 3}

Description

Maximum number of licensed time-slots for the system.

Object Identifier

1.3.6.1.4.1.886.1.1.17.1.3

Data Type

Integer

Access Policy

Read only

Status

Mandatory

sysTimeSlotRemaining

{sysLicenseEntry 4}

Description

The number of available time-slots.

Object Identifier

1.3.6.1.4.1.886.1.1.17.1.4

Data Type

Integer

Access Policy

Read only

Status

Mandatory

sysSerialNum

{sysLicenseEntry 5}

Description

Displays the serial number of the system's CPU card. This number is encoded in the CPU card at the factory and cannot be altered. A unique license number is associated with this serial number.

Object Identifier

1.3.6.1.4.1.886.1.1.17.1.5

Data Type

DisplayString. The valid value is an octet string with a length from 1 to 12 characters.

Access Policy

Read only

Status

Mandatory

sysLicenseNum

{sysLicenseEntry 6}

Description

Gives the license number associated with the serial number of your CPU. You must enter a new license number when your Time-Slot Allocation License is updated or when you replace the CPU card.

Object Identifier

1.3.6.1.4.1.886.1.1.17.1.6

Data Type

DisplayString. The valid value is an octet string with a length from 1 to 12 characters.

Access Policy

Read-write

Status

Mandatory

sysLicenseOwnerString

{sysLicenseEntry 7}

Description

The entity that configured this object and is, therefore, using the assigned entry.

Object Identifier

1.3.6.1.4.1.886.1.1.17.1.7

Data Type

OwnerString

Access Policy

Read-write

Status

Mandatory

sysLicenseEntryStatus

{sysLicenseEntry 8}

Description

The status of this object.

Object Identifier

1.3.6.1.4.1.886.1.1.17.1.8

Data Type

FixedTabEntryStatus

Access Policy

Read-write

Status

Mandatory

sysLicenseErrorStatus

{sysLicenseEntry 9}

Description

Registers the last error that occurred on this entry.

Object Identifier

1.3.6.1.4.1.886.1.1.17.1.9

Data Type

Integer. Valid values are as follows:

Value	String
8704	notRedundantSystem
8705	invalidLength
8706	decryptionFailed

Access Policy

Read only

Status

Mandatory

sysLicenseTableLast Modified

{config 18}

Description

The time, displayed in hundredths of a second, since the feature table was last modified. Helps NMS application developers determine the polling of the agent parameters.

Object Identifier

1.3.6.1.4.1.886.1.1.18

Data Type

TimeTicks

Access Policy

Read-write

Status

Mandatory

System Feature Table

Use the entries in the system feature table section to see and if necessary, change, all the current system features. With system features you can modify system operating characteristics to meet specific application requirements. For further information on configuring the system features, refer to the *Cisco VCO/4K System Administrator's Guide.*

features

{config 19}

Object Identifier

1.3.6.1.4.1.886.1.1.19

featureRedundantSystem

{features 1}

Description

Informs the system-controller initialization software whether the system is redundant or nonredundant. Redundant systems have a second system controller and an NBC3 card. If the redundant hardware is present, the system does not function as a redundant system unless this feature is enabled.

Caution When you set or change this feature, reinitialize your system for the change to take effect.

Object Identifier

1.3.6.1.4.1.886.1.1.19.1

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	System is not redundant
2	yes	System is redundant

Access Policy

Read-write

Status

Mandatory

featureOutputPeriodicAlarmReports

{features 2}

Description

Controls the output of Major/Minor alarm reports to the system printer. If you anticipate heavy call traffic, disable this feature to reduce processing overhead on the system.

Caution When you set or change this feature, reinitialize your system for the change to take effect.

Object Identifier

1.3.6.1.4.1.886.1.1.19.2

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	No reports are sent to the system printer.
2	yes	The Major/Minor alarm reports are sent to the system printer 5 minutes after system initialization is completed and every 30 minutes thereafter.

Access Policy

Read-write

Status

Mandatory

featureNoCardAlarmStatusAtInit

{features 3}

Description

Blocks the printing of card restored and alarm messages for every card during the initial 10 minutes following system boot. These messages in large systems will slow the system boot and lead to performance problems. Therefore, this feature should be enabled in those systems.

Caution When you set or change this feature, reboot your system for the change to take effect.

Object Identifier

1.3.6.1.4.1.886.1.1.19.3

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	All alarm messages are printed.
2	yes	Blocks the printing of card restored and alarm messages during the first 10 minutes following system initialization.

Access Policy

Read-write

Status

Mandatory

featureManual InterventionForSLIPOOF

{features 4}

Description

Controls the system's response to return or not return a card to active service after an error condition. The system automatically takes a T1 card out of service when the SLIP or Out-of-Frame (OOF) limit is reached. The limits are:

OOFs 17

SLIPS 256

Both error threshold counters are reset to zero (0) at midnight.

Object Identifier

1.3.6.1.4.1.886.1.1.19.4

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	The system automatically returns the card to the Active state when the condition clears.
2	yes	The system takes the card out of service and does not try to reset it. You must manually reset the card. Use the Card Maintenance menu on the console or set the status object in the card table entry.

Access Policy

Read-write

Status

Mandatory

featureEnableGraceTimingOnNullRule

{features 5}

Description

Controls the system response to outgoing port detection. The Null Outpulse Rule performs an outward seizure (SEIZE token), a wait for final answer (FINAL SUP A token), and starts a 30-second grace timer.

Refer to Chapter 2 of the *Cisco VCO/4K Extended Programming Reference* or Chapter 2 of the *Cisco VCO/4K Standard Programming Reference* for further information on the Null Outpulse Rule.

Object Identifier

1.3.6.1.4.1.886.1.1.19.5

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	The system only accepts detection of true answer supervision as the final answer from an outgoing port.
2	yes	The outgoing port is considered answered if the system detects either a true answer or the grace timer expires.

Access Policy

Read-write

Status

Mandatory

featureDisableCardErrorReportReset

{features 6}

Description

Controls printing of card error reports.

Object Identifier

1.3.6.1.4.1.886.1.1.19.6

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	The system prints the card error report when the error occurs and when the threshold counters are reset at midnight.
2	yes	The system disables the printing of the card error report and prevents resetting of the card error threshold counters.

Access Policy

Read-write

Status

Mandatory

featureEnableDigitFieldReporting

{features 7}

Description

Controls the information on digit field reports.

Object Identifier

1.3.6.1.4.1.886.1.1.19.7

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	The Field Designator does not appear in reports.
2	yes	Causes the optional Field Designator byte to appear in MF Digit ($D0), DTMF Digit ($D1), and Spoken Digit ($D4) reports. This Optional Field Designator byte indicates the field where the system stores the digits reported. When enabled, this byte appears in the byte offset position (reserved for the digit string). The digit string shifts to the next byte offset.

Access Policy

Read-write

Status

Mandatory

featureSuppressPSCRuleAbort Messages

{features 8}

Description

Prevents log files from becoming filled with Inpulse Rule abort messages. Use this feature only with the optional TeleRouter software overlay.

Certain types of line equipment use the tones issued during permanent signal processing to determine disconnects. This feature suppresses the PSC messages generated by the normal occurrence with these line types. Also, certain situations might generate Inpulse Rule abort messages due to incoming call abandons before call routing.

Object Identifier

1.3.6.1.4.1.886.1.1.19.8

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	PSC/Rule Abort messages are sent to the system log.
2	yes	PSC and Inpulse Rule abort messages are not sent to the system log when TeleRouter is operating in an unhosted environment.

Access Policy

Read-write

Status

Mandatory

featureEnableHost PasswordCheck

{features 9}

Description

Enables or disables Ethernet password checking on the system. Use this feature with host-to-VCO communication on a small, closed network. Define Ethernet passwords with the Password hostPassword object (1.3.6.1.4.1.886.1.1.27.1.1.6) in the hostTable.

Object Identifier

1.3.6.1.4.1.886.1.1.19.9

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	Ethernet password checking disabled. Enables the system to establish a link without requiring the correct password on that link.
2	yes	Ethernet password checking enabled.

Access Policy

Read-write

Status

Mandatory

featureForceBearerLap Activation

{features 10}

Description

Forces the ISDN B channels to the Active state without the D-channel being in the Active state.

Note Use this feature under the direction of your Cisco Systems TAC.

Object Identifier

1.3.6.1.4.1.886.1.1.19.10

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	ISDN B- and D-channels are both in the same state.
2	yes	ISDN B-channel is forced into the Active state without the D-channel being in the Active state.

Access Policy

Read-write

Status

Mandatory

Default Value

1 {no}

featureEnableMFCR2SupervisedClear

{features 11}

Description

A system-wide feature that enables or disables automatic call release on outgoing ports in response to backward MFCR2 supervision tones.

The system performs disconnect processing appropriate for the port type involved and generates an Outgoing Port Change of State ($DA) report (indicates a supervision error and specifies a backward tone detected). Refer to your country supplement for information on backward supervision tones.

Object Identifier

1.3.6.1.4.1.886.1.1.19.11

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	When set to N (No), the outgoing port remains in setup state unless out-of-band supervision or a host command changes the port state.
2	yes	When set to Y (Yes), an outgoing port is released when a specified backward tone is detected during R2 signaling. Backward tones are country specific. See your country supplement for specific tones.

Access Policy

Read-write

Status

Mandatory

featureEnableSLICGuardedDisconnect

{features 12}

Description

Enables or disables the Guarded Disconnect option available for special SLIC cards.

Object Identifier

1.3.6.1.4.1.886.1.1.19.12

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	The Guarded Disconnect option is disabled.
2	yes	The special SLIC card sends an out-of-band Calling Party Disconnect signal to the two-wire devices connected to the card.

Access Policy

Read-write

Status

Mandatory

Default Value

1 {no}

featureEnableCPAMonitorDisconnect

{features 13}

Description

Enables the UTC devices that cannot pass out-of-band end-of-call signals to detect in-band tones when the call is abandoned. When received, the tone is treated as a positive disconnect.

Object Identifier

1.3.6.1.4.1.886.1.1.19.13

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	UTC devices, that cannot pass out-of-band end-of-call signals, cannot detect in-band tones when the call is abandoned.
2	yes	Enables this feature. To function the system must meet the following conditions: • A CPA port must be attached to the UTC throughout the call to monitor the in-band tone. Done automatically when the feature flag is enabled and the incoming UTC is answered using an answer token in the Inpulse rule. • The busy token in Supervision Template #24 must be specified as OK and the template must be downloaded to the CPA.

Access Policy

Read-write

Status

Mandatory

Default Value

1 {no}

featureRevertToBasicRedundancy

{features 14}

Description

Enables both VCO controllers to consistently track conference calls and ports in SETUP.

Object Identifier

1.3.6.1.4.1.886.1.1.19.14

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	Enables redundancy tracking.
2	yes	Disables redundancy tracking.

Access Policy

Read-write

Status

Mandatory

featureSendReportBeforeGuardTime

{features 15}

Description

Specifies whether to send the Incoming Port Change of State Report ($DB) before or after guard timing completes.

Object Identifier

1.3.6.1.4.1.886.1.1.19.15

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	$DB report is sent to the host system after guard timing completes.
2	yes	$DB report is sent to the host system before guard timing completes.

Access Policy

Read-write

Status

Mandatory

featureEnableISDNManualDisconnect

{features 16}

Description

Enables all the cards in the system to perform the same call processing procedure. This feature is independent of the switch type selected for the PRI card.

Object Identifier

1.3.6.1.4.1.886.1.1.19.16

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	Disabled (default)
2	yes	Enabled

Access Policy

Read-write

Status

Mandatory

Default Value

1 {no}

featureSendAIIISDNConnect Reports

{features 17}

Description

Specifies whether to send the ISDN Change of State Report ($EA) each time an ISDN Connect message event is received from an ISDN D-channel.

Object Identifier

1.3.6.1.4.1.886.1.1.19.17

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	$EA report sending controlled by the ISDN supervision template configuration or by an ISDN Port Control ($49) host command.
2	yes	$EA report sent to the host for every ISDN connect message received.

Access Policy

Read-write

Status

Mandatory

featureEnable66CmdHostChecking

{features 18}

Description

When you enable this feature, the system checks whether the host system can send the $66 command. If the host system setup timer is on when the feature is on, host setup timing is cancelled.

Object Identifier

1.3.6.1.4.1.886.1.1.19.18

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	The host cannot send the $66 command.
2	yes	The host can send the $66 command.

Access Policy

Read-write

Status

Mandatory

featureCutThruForNonISDNAlerting

{features 19}

Description

Controls the system's response when an alerting message is received in an ISDN to non-ISDN connection.

Object Identifier

1.3.6.1.4.1.886.1.1.19.19

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	Let the incoming port listen to the outgoing port.
2	yes	Send a ring-back tone to the incoming port.

Access Policy

Read-write

Status

Mandatory

featureEnable4thColumnDTMF

{features 20}

Description

Controls whether the system collects fourth column DTMF digits.

Object Identifier

1.3.6.1.4.1.886.1.1.19.20

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	All host and report commands function as in previous software versions.
2	yes	The system collects fourth column DTMF digits. Also $D1 segments attached to $DD or $ED reports follow the enhanced format.

Access Policy

Read-write

Status

Mandatory

featureSetSystemToALaw

{features 21}

Description

If this feature is set to yes, then the system is set to A Law.

Object Identifier

1.3.6.1.4.1.886.1.1.19.21

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	The system is not set to A-Law.
2	yes	The system is set to A-Law

Access Policy

Read-write

Status

Mandatory

featureSendAllISDN DisconnectReports

{features 22}

Description

The Send All ISDN Disconnect Reports feature flag specifies whether to send the ISDN Change of State Report ($EA) each time an ISDN DisConnect message event is received from an ISDN D-channel. If the feature flag is set to Y, the $EA report is sent to the host for every ISDN `DisConnect' message received. If the feature flag is set to N, the sending of $EA reports for `DisConnect' messages is controlled by the ISDN supervision template configuration or by an ISDN Port Control ($49) host command.

Object Identifier

1.3.6.1.4.1.886.1.1.19.22

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	Do not send all ISDN Disconnect reports.
2	yes	Send all ISDN Disconnect reports.

Access Policy

Read-write

Status

Mandatory

featureOperationMode Extended

{features 23}

Description

This flag is read only and is used to verify whether extended operational mode is activated. Extended mode is activated during the installation process by selecting the Set Extended Operational Mode option from the Installation Utilities screen. To configure the VCO system for 4,096 ports, both the Extended Operation Mode Set and Enable C-bus flags must be set to yes.

Object Identifier

1.3.6.1.4.1.886.1.1.19.23

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	Extended operational mode is not set.
2	yes	Extended operational mode is set.

Access Policy

Read only

Status

Mandatory

featureCbusMode

{features 24}

Description

This flag is read only and is used to verify whether the C-bus is enabled. If yes, C-bus is enabled, and the VCO system can take advantage of 4,096 ports. If no, C-bus is disabled, and the system is limited to 2,048 ports. To configure the VCO system for 4,096 ports, both the Enable C-bus and Extended Operation Mode Set flags must be set to yes.

Object Identifier

1.3.6.1.4.1.886.1.1.19.24

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	The C-bus is not enabled.
2	yes	The C-bus is enabled.

Access Policy

Read only

Status

Mandatory

featureEnableAllPortsDeactivatedAlarm

{features 25}

Description

If this feature is set to yes, a PRI/N card alarm is raised when all the ports on the card are deactivated. An Alarm Condition ($F0) report is sent to the host specifying which card caused the alarm. A minor system alarm is raised and the event is logged if the system alarm condition does not already exist. The new alarm is raised only when all the ports are deactivated from the Card Maintenance screen, the $90 command from the host, or through a far end port-state transition to out of service.

When at least one of the deactivated ports becomes available for use, the card alarm is cleared and the event is logged. An Alarm Condition ($F0) report is generated to the host, specifying the card in which the alarm condition is cleared. The minor system alarm is cleared and the event is logged if there are no other occurrences of the same alarm.

For the alarm to clear, a port which has been deactivated must be made available from the Card Maintenance screen, the $90 command from the host, or through a far end port-state transition to out of service.

When all the ports of a PRI/N card are deactivated, a card alarm is raised and this event is logged.

Object Identifier

1.3.6.1.4.1.886.1.1.19.25

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	A card alarm is not raised when all ports are deactivated.
2	yes	A card alarm is raised when all ports are deactivated.

Access Policy

Read-write

Status

Mandatory

featureEaReportsOnDchannelRestart

{features 26}

Description

If this feature is set to yes, an ISDN Port Change of State ($EA) report is generated for the D-channel and all associated B-channels when the system receives a RESTART. For more information about $EA reports, refer to the *Cisco VCO/4K ISDN Supplement.*

Object Identifier

1.3.6.1.4.1.886.1.1.19.26

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	Do not send $EA ISDN Port Change of State on D-channel restart.
2	yes	Send $EA ISDN Port Change of State on D-channel restart.

Access Policy

Read-write

Status

Mandatory

featureEnableNet5OverlapReceiving

{features 27}

Description

Operates in situations where there is a variable digit length for a called number. In these cases, only the host application can determine if information about the called number is complete and that the call can be routed to its destination. The Generic depends on the host application for an indication of Overlap Receiving occurrence. To do this, the host application sends SETUP_ACK down to the Generic through the $49 command with a specified inpulse rule.

Object Identifier

1.3.6.1.4.1.886.1.1.19.27

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	Do not enable Net 5 Overlap Receiving.
2	yes	Enable Net 5 Overlap Receiving.

Access Policy

Read-write

Status

Mandatory

featureConvertReorderToneToBusy

{features 28}

Description

For use with Japanese networks. Allows you to select an alternate busy tone for Japanese networks which use a normal busy tone instead of the reorder tone during PSC (Permanent Signaling Condition) processing on a port.

When set to no, the normal reorder tone is presented during PSC. When set to yes, the normal busy tone is presented.

Object Identifier

1.3.6.1.4.1.886.1.1.19.28

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	Do not convert reorder tone to busy.
2	yes	Convert reorder tone to busy.

Access Policy

Read-write

Status

Mandatory

featureEnableHostCallRef

{features 30}

Description

If this feature is set to yes, the system passes call reference up to the host, which enables the host application to support 2 B-channel transfer. The call reference is sent to the host in bytes 20 and 21 of the $EA report.

Object Identifier

1.3.6.1.4.1.886.1.1.19.30

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	Do not pass call references to the host.
2	yes	Pass call references to the host.

Access Policy

Read-write

Status

Mandatory

featureErrorStatus

{features 65)

Description

Registers the last error that occurred on this feature object.

Object Identifier

1.3.6.1.4.1.886.1.1.19.65

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String
5376	invalidFeature
5377	invalidValue

Access Policy

Read only

Status

Mandatory

featureOwnerString

{feature 66}

Description

The entity that last configured a feature.

Object Identifier

1.3.6.1.4.1.886.1.1.19.66

Data Type

OwnerString

Access Policy

Read-write

Status

Mandatory

featureEntryStatus

{features 67}

Description

The modification status of the configuration.

Object Identifier

1.3.6.1.4.1.886.1.1.19.67

Data Type

NonTabEntryStatus

Access Policy

Read-write

Status

Mandatory

systemAlarmAudible

{config 23}

Description

Enables or disables the AAC alarm contact to stop any external central office (CO) alarms tied to the switch.

Object Identifier

1.3.6.1.4.1.886.1.1.23

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	yes	Stop external CO alarms.
2	no	Do not stop external CO alarms.

Access Policy

Read-write

Status

Mandatory

Firmware Version Table

Use the objects in the firmware version table to display the version numbers of the software running on your system.

Note The objects that are returned when you do an SNMP “walk” of objects in the firmware table are dependent on the value of firmwareDevice. By default, the value of firmwareDevice is 0 ('none'). When firmwareDevice is 'none', there is no information to return for firmwareExeTable or firmwareDwnldTable. If you change firmwareDevice to, for example, 'c', then an SNMP “walk” will return all information on the objects in the firmware tables (if the switch uses boot and download files from 'c').

firmware

{config 24}

Object Identifier

1.3.6.1.4.1.886.1.1.24

firmwareVrtxVersion

{firmware 1}

Description

Version or revision number of VRTX.

Object Identifier

1.3.6.1.4.1.886.1.1.24.1

Data Type

DisplayString. Length of the display is from 1 to 4 characters.

Access Policy

Read only

Status

Mandatory

firmwareIfxVersion

{firmware 2}

Description

Version or revision number of IFX.

Object Identifier

1.3.6.1.4.1.886.1.1.24.2

Data Type

DisplayString. Length of the display string is from 1 to 4 characters.

Access Policy

Read only

Status

Mandatory

firmwareTnxVersion

{firmware 3}

Description

Version or revision number of TNX.

Object Identifier

1.3.6.1.4.1.886.1.1.24.3

Data Type

DisplayString. Length of the display string is from 1 to 4 characters.

Access Policy

Read only

Status

Mandatory

firmwareDevice

{firmware 4}

Description

Specifies the device to display configuration information.

Note The objects that are returned when you do an SNMP “walk” of objects in the firmware table are dependent on the value of firmwareDevice. By default, the value of firmwareDevice is 'none'. When firmwareDevice is 0 ('none'), there is no information to return for firmwareExeTable or firmwareDwnldTable. If you change firmwareDevice to, for example, 'c', then an SNMP “walk” will return all information on the objects in the firmware tables (if the switch uses boot and download files from 'c').

Object Identifier

1.3.6.1.4.1.886.1.1.24.4

Data Type

Integer. The possible values and their meanings are shown in the following table:

Value	String	Value
0	none	No information is displayed.
1	a	Display information is sent to drive A.
2	c	Display information is sent to drive C.
3	f	Display information is sent to the floppy drive.
4	memory	Display information is sent to memory.

Access Policy

Read-write

Status

Mandatory

firmwareGenericVersion

{firmware 5}

Description

Version, revision, or FSR (field support release) number of the generic software.

Object Identifier

1.3.6.1.4.1.886.1.1.24.5

Data Type

DisplayString. Length of the display string is from 0 to 8 characters.

Access Policy

Read only

Status

Mandatory

Firmware Executable Table

The objects in the firmware executable table enable you to display the attributes of the firmware executable files.

firmwareExeTable

{firmware 6}

Description

Table of executable files.

Object Identifier

1.3.6.1.4.1.886.1.1.24.6

Data Type

Sequence of FirmwareExeEntry

Access Policy

Not accessible

Status

Mandatory

firmwareExeEntry

{firmwareExeTable 1}

Description

An entry in the firmware executable table.

Object Identifier

1.3.6.1.4.1.886.1.1.24.6.1

Data Type

FirmwareExeEntry

Access Policy

Not accessible

Status

Mandatory

Index

firewareExtIndex

FirmwareExeEntry

Sequence

firmwareExeIndex	Integer
firmwareExeName	DisplayString
firmwareExeVersion	DisplayString
firmwareExeChecksum	Integer

firmwareExeIndex

{firmwareExeEntry 1}

Description

An index into the firmware executable table.

Object Identifier

1.3.6.1.4.1.886.1.1.24.6.1.1

Data Type

Integer

Access Policy

Read only

Status

Mandatory

firmwareExeName

{firmwareExeEntry 2}

Description

Name of the executable file.

Object Identifier

1.3.6.1.4.1.886.1.1.24.6.1.2

Data Type

DisplayString. Length of the display string is from 1 to 12 characters.

Access Policy

Read only

Status

Mandatory

firmwareExeVersion

{firmwareExeEntry 3}

Description

Version or revision number of the executable file.

Object Identifier

1.3.6.1.4.1.886.1.1.24.6.1.3

Data Type

DisplayString. Length of the display string is from 1 to 4 characters.

Access Policy

Read only

Status

Mandatory

firmwareExeChecksum

{firmwareExeEntry 4}

Description

Checksum of the executable file.

Object Identifier

1.3.6.1.4.1.886.1.1.24.6.1.4

Data Type

Integer

Access Policy

Read only

Status

Mandatory

Firmware Download Table

The objects in the firmware download table enable you to display the attributes of the firmware downloadable files.

firmwareDwnldTable

{firmware 7}

Description

Table of the card download files.

Object Identifier

1.3.6.1.4.1.886.1.1.24.7

Data Type

Sequence of FirmwareDwnldEntry

Access Policy

Not accessible

Status

Mandatory

firmwareVcoMibVersion

{firmware 8}

Description

Version of the vco MIB used by the SNMP agent software, in the form: x.y.z. See the beginning of the vco MIB text file for information on what the various parts of the version mean.

Object Identifier

1.3.6.1.4.1.886.1.1.24.8

Data Type

DisplayString (SIZE (5..8))

Access Policy

Read only

Status

Mandatory

firmwareDwnldEntry

{firmwareDwnldTable 1}

Description

An entry in the firmware card download table.

Object Identifier

1.3.6.1.4.1.886.1.1.24.7.1

Data Type

FirmwareDwnldEntry

Access Policy

Not accessible

Status

Mandatory

FirmwareDwnldEntry

Sequence

firmwareDwnldIndex	Integer
firmwareDwnldName	DisplayString
firmwareDwnldVersion	DisplayString
firmwareDwnldChecksum	Integer

firmwareDwnldIndex

{firmwareDwnldEntry 1}

Description

An index into the firmwareDwnldTable.

Object Identifier

1.3.6.1.4.1.886.1.1.24.7.1.1

Data Type

Integer

Access Policy

Read only

Status

Mandatory

firmwareDwnldName

{firmwareDwnldEntry 2}

Description

Name of the card download file.

Object Identifier

1.3.6.1.4.1.886.1.1.24.7.1.2

Data Type

DisplayString. Length of the display string is from 1 to 12 characters.

Access Policy

Read only

Status

Mandatory

firmwareDwnldVersion

{firmwareDwnldEntry 3}

Description

Version or revision number of the card download file.

Object Identifier

1.3.6.1.4.1.886.1.1.24.7.1.3

Data Type

DisplayString. Length of the display string is from 1 to 4 characters.

Access Policy

Read only

Status

Mandatory

firmwareDwnldChecksum

{firmwareDwnldEntry 4}

Description

Checksum of the card download file.

Object Identifier

1.3.6.1.4.1.886.1.1.24.7.1.4

Data Type

Integer

Access Policy

Read only

Status

Mandatory

File System Table

Use the file system table to display the attributes of the system files and to specify where you want to store system directories and log files.

filesystem

{config 25}

Object Identifier

1.3.6.1.4.1.886.1.1.25

fsBootDevice

{filesystem 1}

Description

Storage device for the boot or download file.

Object Identifier

1.3.6.1.4.1.886.1.1.25.1

Data Type

Integer. The possible values and their meanings are shown in the following table:

Value	String	Meaning
1	a	Boot from drive A
2	c	Boot from drive C
3	f	Boot from a floppy diskette

Access Policy

Read only

Status

Mandatory

fsBootDirectory

{filesystem 2}

Description

Directory for the boot or download file.

Object Identifier

1.3.6.1.4.1.886.1.1.25.2

Data Type

DisplayString. Length of the display string is from 1 to 36 characters.

Access Policy

Read only

Status

Mandatory

fsDatabaseDevice

{filesystem 3}

Description

The storage device for the system database files.

Object Identifier

1.3.6.1.4.1.886.1.1.25.3

Data Type

Integer. The possible values and their meanings are shown in the following table:

Value	String	Meaning
1	a	Store files on drive A
2	c	Store files on drive C
3	f	Store files on a floppy diskette

Access Policy

Read only

Status

Mandatory

fsDatabaseDirectory

{filesystem 4}

Description

Directory for the system database files.

Object Identifier

1.3.6.1.4.1.886.1.1.25.4

Data Type

DisplayString. Length of the display string is from 1 to 36 characters.

Access Policy

Read only

Status

Mandatory

fsLogDevice

{filesystem 5}

Description

Storage device for the system log files.

Object Identifier

1.3.6.1.4.1.886.1.1.25.5

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String	Meaning
1	a	Store files on drive A
2	c	Store files on drive C
3	f	Store files on a floppy diskette

Access Policy

Read-write

Status

Mandatory

fsLogDirectory

{filesystem 6}

Description

Directory for the system log files.

Object Identifier

1.3.6.1.4.1.886.1.1.25.6

Data Type

DisplayString. Length is from 1 to 36 characters.

Access Policy

Read-write

Status

Mandatory

fsTraceDevice

{filesystem 7}

Description

Storage device for system trace files.

Object Identifier

1.3.6.1.4.1.886.1.1.25.7

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String	MeaningValue
1	a	Store trace files on drive A
2	c	Store trace files on drive C
3	f	Store trace files on a floppy diskette

Access Policy

Read-write

Status

Mandatory

fsTraceDirectory

{filesystem 8}

Description

The directory for system trace files.

Object Identifier

1.3.6.1.4.1.886.1.1.25.8

Data Type

DisplayString. Length is from 1 to 36 characters.

Access Policy

Read-write

Status

Mandatory

fsErrorStatus

{filesystem 9}

Description

Registers the last error that occurred on this file system object.

Object Identifier

1.3.6.1.4.1.886.1.1.25.9

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String
5632	invalidFilesystem
5633	invalidValue

Access Policy

Read only

Status

Mandatory

fsOwnerString

{filesystem 10}

Description

Entity that configured the entry and is using the assigned resources.

Object Identifier

1.3.6.1.4.1.886.1.1.25.10

Data Type

OwnerString

Access Policy

Read-write

Status

Mandatory

fsEntryStatus

{filesystem 11}

Description

Modification status of this entry.

Object Identifier

1.3.6.1.4.1.886.1.1.25.11

Data Type

NonTabEntryStatus

Access Policy

Read-write

Status

Mandatory

Peripheral Configuration Table

Use the objects in the peripheral configuration table to define operating parameters for peripheral equipment. System peripherals can include local system consoles, remote system consoles connected to your system by a modem, and printers.

peripheral

{config 26}

Object Identifier

1.3.6.1.4.1.886.1.1.26

periphLocalKBType

{peripheral 1}

Description

Keyboard for the local TTY. For further information, refer to the *Cisco VCO/4K System Administrator's Guide.*

Object Identifier

1.3.6.1.4.1.886.1.1.26.1

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String
1	vt220
2	sunview
3	xview
4	universal

Access Policy

Read-write

Status

Mandatory

periphLocalBaud

{peripheral 2}

Description

Baud rate for the local TTY.

Object Identifier

1.3.6.1.4.1.886.1.1.26.2

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String
1	baud300
2	baud1200
3	baud2400
4	baud4800
5	baud9600
6	baud19200
7	baud38400

Access Policy

Read-write

Status

Mandatory

periphLocalStop

{peripheral 3}

Description

Stop bits for the local TTY.

Object Identifier

1.3.6.1.4.1.886.1.1.26.3

Data Type

Integer. Valid values are 1 and 2.

Access Policy

Read-write

Status

Mandatory

periphLocalBits

{peripheral 4}

Description

Bits per character for the local TTY.

Object Identifier

1.3.6.1.4.1.886.1.1.26.4

Data Type

Integer. Valid values or 7 or 8.

Access Policy

Read-write

Status

Mandatory

periphLocalParity

{peripheral 5}

Description

Parity for the local TTY.

Object Identifier

1.3.6.1.4.1.886.1.1.26.5

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	none	No parity is used.
2	odd	Parity is odd.
3	even	Parity is even.

Access Policy

Read-write

Status

Mandatory

periphRemoteKBType

{peripheral 6}

Description

Keyboard for the remote TTY. For further information, see the *Cisco VCO/4K System Administrator's Guide.*

Object Identifier

1.3.6.1.4.1.886.1.1.26.6

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String
1	vt220
2	sunview
3	xview
4	universal

Access Policy

Read-write

Status

Mandatory

periphRemoteBaud

{peripheral 7}

Description

The baud rate for the remote TTY.

Object Identifier

1.3.6.1.4.1.886.1.1.26.7

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String
1	baud300
2	baud1200
3	baud2400
4	baud4800
5	baud9600
6	baud19200
7	baud38400

Access Policy

Read-write

Status

Mandatory

periphRemoteStop

{peripheral 8}

Description

The stop bits for the remote TTY.

Object Identifier

1.3.6.1.4.1.886.1.1.26.8

Data Type

Integer. Valid values are 1 and 2.

Access Policy

Read-write

Status

Mandatory

periphRemoteBits

{peripheral 9}

Description

The bits per character for the remote TTY.

Object Identifier

1.3.6.1.4.1.886.1.1.26.9

Data Type

Integer. Valid values are 7 and 8.

Access Policy

Read-write

Status

Mandatory

periphRemoteParity

{peripheral 10}

Description

Parity for the remote TTY.

Object Identifier

1.3.6.1.4.1.886.1.1.26.10

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String	Meaning
1	none	No parity
2	even	Parity is even
3	odd	Parity is odd

Access Policy

Read-write

Status

Mandatory

periphTelnetKBType

{peripheral 11}

Description

Keyboard type for the Telnet TTY. For further information, see the *Cisco VCO/4K System Administrator's Guide.*

Object Identifier

1.3.6.1.4.1.886.1.1.26.11

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String
1	vt220
2	sunview
3	xview
4	universal

Access Policy

Read-write

Status

Mandatory

periphPrinterEOL

{peripheral 12}

Description

The printer end of line (EOL) control character.

Object Identifier

1.3.6.1.4.1.886.1.1.26.12

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String	Meaning
1	cr-lf	Carriage return and line feed
2	cr	Carriage return
3	lf	Line feed

Access Policy

Read-write

Status

Mandatory

periphErrorStatus

{peripheral 13}

Description

Registers the last error that occurred in this entry.

Object Identifier

1.3.6.1.4.1.886.1.1.26.13

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String
5888	notApplicable
5889	invalidValue

Access Policy

Read only

Status

Mandatory

periphOwnerString

{peripheral 14}

Description

The entity that configured this object and is using the attached resources.

Object Identifier

1.3.6.1.4.1.886.1.1.26.14

Data Type

OwnerString

Access Policy

Read-write

Status

Mandatory

periphEntryStatus

{peripheral 15}

Description

Modification status of this entry.

Object Identifier

1.3.6.1.4.1.886.1.1.26.15

Data Type

NonTabEntryStatus

Access Policy

Read-write

Status

Mandatory

periphLocalXonXoff

{peripheral 16}

Description

Flow-control for the Local TTY.

Object Identifier

1.3.6.1.4.1.886.1.1.26.16

Data Type

Integer (1=disabled;2=enabled)

Access Policy

Read-write

Status

Mandatory

periphRemoteXonXoff

{peripheral 17}

Description

Flow-control for the Remote TTY.

Object Identifier

1.3.6.1.4.1.886.1.1.26.17

Data Type

Integer (1=disabled;2=enabled)

Access Policy

Read-write

Status

Mandatory

Host Configuration Table

Use the objects in the host configuration table to configure host interfaces and to indicate the status of the alarm conditions for host interfaces.

host

{config 27}

Object Identifier

1.3.6.1.4.1.886.1.1.27

hostTable

{host 1}

Description

Table of the host interfaces.

Object Identifier

1.3.6.1.4.1.886.1.1.27.1

Data Type

Sequence of HostEntry

Access Policy

Not accessible

Status

Mandatory

hostEntry

{hostTable 1}

Description

Entry in the host table. An entry exports objects for all types of hosts, but certain fields are only meaningful for certain types of hosts.

Object Identifier

1.3.6.1.4.1.886.1.1.27.1.1

Data Type

HostEntry

Access Policy

Not accessible

Status

Mandatory

Index

{hostIndex}

HostEntry

Sequence

hostIndex	Integer
hostType	Integer
hostName	DisplayString
hostPassword	DisplayString
hostLocalPort	Integer
hostAddress	IpAddress
hostRemotePort	Integer
hostAlarm	Integer
hostProtocol	Integer
hostResetTime	Integer
hostSioPort	Integer
hostPollTimeout	Integer
hostBaud	Integer
hostRetryCount	Integer
hostParity	Integer
hostBlockFactor	Integer

hostModem	Integer
hostFormat	Integer
hostErrorStatus	Integer
hostOwnerString	OwnerString
hostEntryStatus	FixedTabEntryStatus
hostFailureAction	Integer

hostIndex

{hostEntry 1}

Description

An index into the host table. This object applies to all host types.

Object Identifier

1.3.6.1.4.1.886.1.1.27.1.1.1

Data Type

Integer. Valid values are 1 to 9.

Access Policy

Read only

Status

Mandatory

hostType

{hostEntry 2}

Description

Determines the type of host specified.The first entry is always reserved for type internal. If the TeleRouter is supported, an SNMP_GET command on the first entry returns type internal (2). Otherwise, it returns type unused (1)

Object Identifier

1.3.6.1.4.1.886.1.1.27.1.1.2

Data Type

Integer. Valid numerical and string values are shown in the following table:

Value	String	Meaning
1	unused	The TeleRouter is not installed.
2	internal	Internal software overlay. Optional TeleRouter software currently supported. You can specify only one Internal interface (must be first entry).

Value	String	Meaning
3	ethernet	Ethernet TCP/IP communication using the Ethernet port on the CPU-TM. You can specify up to eight Ethernet interfaces (cannot use first entry).
4	sio	ADLC asynchronous communication using ports on the CPU-TM. You can specify only two SIO port interfaces (cannot use first entry).

Access Policy

Read-write

Status

Mandatory

Default Value

1 (unused)

hostName

{hostEntry 3}

Description

Determines the name of the host. This object accepts up to ten alphanumeric characters, either upper- or lowercase. This object applies to all hosts.

This object is valid for all host types except unused (no host).

Object Identifier

1.3.6.1.4.1.886.1.1.27.1.1.3

Data Type

DisplayString. Length of the display string is from 1 to 12 characters.

Access Policy

Read-write

Status

Mandatory

hostPassword

{hostEntry 6}

Description

Specifies the password required before accepting data from the network (applies only to Ethernet hosts). Password checking is disabled through the System Feature configuration. See the featureTable object featureEnableHostPasswordCheck (Object Identifier 1.3.6.1.4.1.886.1.1.19.9).

Object Identifier

1.3.6.1.4.1.886.1.1.27.1.1.6

Data Type

DisplayString. The valid value is a string with a length of from 1 to 16 ASCII characters.

Access Policy

Read-write

Status

Mandatory

hostLocalPort

{hostEntry 7}

Description

Specifies the local port number from which the system accepts data (applies only to Ethernet hosts).

Object Identifier

1.3.6.1.4.1.886.1.1.27.1.1.7

Data Type

Integer. Valid values are 0 or a valid Ethernet port number.

Access Policy

Read-write

Status

Mandatory

Default Value

1024

hostAddress

{hostEntry 8}

Description

Specifies the Internet stations from which the system controller accepts data. This object applies only to Ethernet hosts.

Object Identifier

1.3.6.1.4.1.886.1.1.27.1.1.8

Data Type

IpAddress. INADDR_ANY (any Internet address == 0.0.0.0) or a valid Internet address.

Access Policy

Read-write

Status

Mandatory

hostRemotePort

{hostEntry 9}

Description

Specifies the TCP/IP port from which the system controller accepts data. This object applies only to Ethernet hosts.

Object Identifier

1.3.6.1.4.1.886.1.1.27.1.1.9

Data Type

Integer. Valid values are zero (0) or a valid port number. The port number must be greater than 1023.

Access Policy

Read-write

Status

Mandatory

Default Value

1024

hostAlarm

{hostEntry 10}

Description

Indicates current alarm state for host interface (applies only to Ethernet and SIO hosts).

Object Identifier

1.3.6.1.4.1.886.1.1.27.1.1.10

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String	Meaning
1	off	No alarm condition exits.
2	on	An alarm condition exists for this host interface link. The presence of an alarm state for an interface indicates that the link is currently out of service due to an error condition on either the system or the host end. You can use logfile messages to determine the cause of the link failure.

Access Policy

Read only

Status

Mandatory

hostProtocol

{hostEntry 11}

Description

Defines data transfer protocol used on host link (applies only to Ethernet and SIO hosts).

Object Identifier

1.3.6.1.4.1.886.1.1.27.1.1.11

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String	Meaning
1	tcp	TCP protocol. Required for Ethernet.
2	adlc	ADLC protocol. Required for SIO.
3	none	No protocol used.

Access Policy

Read only

Status

Mandatory

hostResetTime

{hostEntry 12}

Description

Specifies the time, in seconds, the VCO waits after a link failure/reset before re-establishing the link (applies to Ethernet and SIO hosts).

Object Identifier

1.3.6.1.4.1.886.1.1.27.1.1.12

Data Type

Integer. Valid value are from 0 to 999 seconds (cannot be set to 0).

Access Policy

Read-write

Status

Mandatory

hostSioPort

{hostEntry 13}

Description

The physical port number of the SIO link (applies only to SIO hosts).

Object Identifier

1.3.6.1.4.1.886.1.1.27.1.1.13

Data Type

Integer. Valid values are 3 for SIO3, 4 for SIO4, 0 otherwise.

Access Policy

Read-write

Status

Mandatory

hostPollTimeout

{hostEntry 14}

Description

Specifies the amount of time, in seconds, the system waits to be polled by the host before the system assumes an error exists on the link (applies only to SIO hosts).

Object Identifier

1.3.6.1.4.1.886.1.1.27.1.1.14

Data Type

Integer. Valid values are from 0 to 300 in increments of 1. Each increment is a 1 second interval. A setting of 15 seconds is recommended.

A zero (0) value equals an infinite wait. This is not recommended because the system uses this timeout to determine when a link failure has occurred.

Access Policy

Read-write

Status

Mandatory

Default Value

15 {seconds}

hostBaud

{hostEntry 15}

Description

Specifies the data transmission speed, in bits per second, over the link (applies only to SIO hosts).

Object Identifier

1.3.6.1.4.1.886.1.1.27.1.1.15

Data Type

Integer. The valid numerical and string values are shown in the following table. Default value is 5 (9600).

Value	String
1	baud300
2	baud1200
3	baud2400
4	baud4800
5	baud9600
6	baud19200
7	baud38400

Access Policy

Read-write

Status

Mandatory

hostRetryCount

{hostEntry 16}

Description

Specifies the number of times the system retransmits a message before assuming an error condition exists on the link. This object applies only to SIO hosts.

Object Identifier

1.3.6.1.4.1.886.1.1.27.1.1.16

Data Type

Integer. The valid values are from 0 to 255. Recommended value is 5.

Access Policy

Read-write

Status

Mandatory

Default Value

{5}

hostParity

{hostEntry 17}

Description

Specifies if the system performs error checking using a parity bit (applies only to SIO hosts).

Object Identifier

1.3.6.1.4.1.886.1.1.27.1.1.17

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String	Meaning
1	none	No parity
2	even	Parity is even
3	odd	Parity is odd

Access Policy

Read-write

Status

Mandatory

Default Value

1 {none}

hostBlockFactor

{hostEntry 18}

Description

Specifies the number of messages allowed in a multiblocked transmission. Transmit blocks can be constructed with a message count up to this number. This object applies only to SIO hosts.

Object Identifier

1.3.6.1.4.1.886.1.1.27.1.1.18

Data Type

Integer. Valid values are from 1 to 32. Recommended value is 5.

Access Policy

Read-write

Status

Mandatory

Default Value

5 {Messages in transmission}

hostModem

{hostEntry 19}

Description

Specifies whether you are using a modem between this port and the host computer (applies only to SIO hosts).

Object Identifier

1.3.6.1.4.1.886.1.1.27.1.1.19

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String	Meaning
1	no	You are not using a modem.
2	yes	You are using a modem. System uses full modem control signaling.

Access Policy

Read-write

Status

Mandatory

Default Value

1 (no modem)

hostFormat

{hostEntry 20}

Description

Specifies the number of stop bits used with the 8-bit data character (applies only to SIO hosts).

Object Identifier

1.3.6.1.4.1.886.1.1.27.1.1.20

Data Type

Integer. Valid values are 1 or 2.

Access Policy

Read-write

Status

Mandatory

hostErrorStatus

{hostEntry 21}

Description

Registers the last error that occurred on this entry (applies to all host types).

Object Identifier

1.3.6.1.4.1.886.1.1.27.1.1.21

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String
4864	invalidHost
4865	invalidSlot
4866	notApplicable
4867	invalidValue
4868	noTelerouter
4869	duplicate
4870	notSupported

Access Policy

Read only

Status

Mandatory

hostOwnerString

{hostEntry 22}

Description

The entity that configured the object (applies to all host types).

Object Identifier

1.3.6.1.4.1.886.1.1.27.1.1.22

Data Type

OwnerString

Access Policy

Read-write

Status

Mandatory

hostEntryStatus

{hostEntry 23}

Description

Modification status of the entry (applies to all host types).

Object Identifier

1.3.6.1.4.1.886.1.1.27.1.1.23

Data Type

FixedTabEntryStatus

Access Policy

Read-write

Status

Mandatory

hostFailureAction

{hostEntry 24}

Description

Defines the action taken on failure of the host (applies to Etherenet and SIO).

Object Identifier

1.3.6.1.4.1.886.1.1.27.1.1.24

Data Type

Integer

Access Policy

Read-write

Status

Mandatory

hostTableLastModified

{host 2}

Description

The time, displayed in hundredths of a second, since the host table was last modified. Helps NMS application developers determine the polling of the agent parameters.

Object Identifier

1.3.6.1.4.1.886.1.1.27.2

Data Type

TimeTicks

Access Policy

Read only

Status

Mandatory

System Host Configuration

Use the objects in the system host configuration table to configure the parameters that apply to the interactions between your system and the host.

sysHost

{config 28}

Object Identifier

1.3.6.1.4.1.886.1.1.28

sysHostSetupTimerEnabled

{sysHost 1}

Description

Enables or disables the host setup timer function.

Object Identifier

1.3.6.1.4.1.886.1.1.28.1

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String	Meaning
1	no	Host setup timer processing is not performed.
2	yes	Host setup timer processing performed based on the specified host setup timer value.

Access Policy

Read-write

Status

Mandatory

Default Value

2 {Yes}

sysHostSetupTimer

{sysHost 2}

Description

Configures the duration of the setup timer. The setup timer is the length of time a host has to respond to a new call report.

Object Identifier

1.3.6.1.4.1.886.1.1.28.2

Data Type

Integer. Valid values are from 0 to 60 seconds.

Access Policy

Read-write

Status

Mandatory

sysHostAllHostLinkFailureAction

{sysHost 3}

Description

Specifies the action taken if all host links fail.

Object Identifier

1.3.6.1.4.1.886.1.1.28.3

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String	Meaning
1	major-alarm	A major alarm is generated when all host links fail.
2	fatal-alarm	A fatal alarm is generated when all host links fail. The system controller shuts down and reboots. If the system is redundant, then a system switchover is initiated.
3	conditional-switchover	A major alarm is generated when all host links fail. A system switchover is initiated if the standby controller is on-line (file synchronization completed) and the system has active host links. No reboot is performed after a conditional switchover.

Access Policy

Read-write

Status

Mandatory

sysHostControlCallLoad

{sysHost 4}

Description

Enables or disables the host control of call load feature. This applies when the host links are marked as ready to process calls. No call reports are issued to a host link until it is marked as available to process calls.

Object Identifier

1.3.6.1.4.1.886.1.1.28.4

Data Type

Integer. The valid values and their meanings are shown in the following table:

Value	String	Meaning
1	no	Host links marked as available when link is established.
2	yes	Host links not marked as available until the system receives a $C0 04 command from the host.

Access Policy

Read-write

Status

Mandatory

Default Value

no {1}

sysHostControlChecking

{sysHost 5}

Description

Enables or disables host control verification.

Object Identifier

1.3.6.1.4.1.886.1.1.28.5

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String	Meaning
1	no	No host control verification is performed. The system accepts commands from any host link regardless of the host link assigned as controlling host.
2	yes	The system accepts commands only from the host link assigned to the call. Controlling host assignment is made based on the Incoming Call Distribution field configuration.

Access Policy

Read-write

Status

Mandatory

Default Value

no {1}

sysHostIncomingCallDistribution

{sysHost 6}

Description

Specifies how new incoming calls are distributed to available host links.

Object Identifier

1.3.6.1.4.1.886.1.1.28.6

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String	Meaning
1	broadcast	Reports for new calls are sent to all available host links. The first host to respond to the report is assigned as the controlling host.
2	cyclic	Reports for new calls are uniformly distributed among all available host links. One host link is assigned to the call by the system and all reports for that call are sent only to the assigned host link. If you enable Host Control Checking then resource commands for the call are only accepted from the assigned host link.

Access Policy

Read-write

Status

Mandatory

Default Value

1 {broadcast}

sysHostNoAlarmReportAtInit

{sysHost 7}

Description

Enables or disables the suppression of alarm reports during the first five minutes following system initialization. During system initialization several alarm conditions are set and cleared as part of normal processing.

An Alarm Condition ($F0) report is normally issued to all active host links whenever an alarm condition is set or cleared. Enabling this feature suppresses these reports until the system is beyond the initialization period.

Object Identifier

1.3.6.1.4.1.886.1.1.28.7

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String	Meaning
1	no	The $F0 alarm reports are issued to all active host links during initialization.
2	yes	The $F0 alarm reports are suppressed for the first five minutes following system initialization.

Access Policy

Read-write

Status

Mandatory

Default Value

1 {no}

sysHostReportInitToAll

{sysHost 8}

Description

Enables or Disables the sending of Active/Standby Mode ($DC) reports to indicate that the system has completed initialization and is ready to process calls.

Object Identifier

1.3.6.1.4.1.886.1.1.28.8

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String	Meaning
1	no	No Active/Standby Mode ($DC) report is issued when Phase 3 system initialization has completed.
2	yes	Active/Standby Mode ($DC) report is issued when Phase 3 system initialization has completed.

Access Policy

Read-write

Status

Mandatory

Default Value

1 {no}

sysHostErrorStatus

{sysHost 9}

Description

Registers the last error that occurred in this entry.

Object Identifier

1.3.6.1.4.1.886.1.1.28.9

Data Type

Integer. The valid numerical and string values are shown in the following table:

Value	String
5120	invalidFlag
5121	invalidValue

Access Policy

Read only

Status

Mandatory

sysHostOwnerString

{sysHost 10}

Description

The entity that last configured a feature.

Object Identifier

1.3.6.1.4.1.886.1.1.28.10

Data Type

OwnerString

Access Policy

Read-write

Status

Mandatory

sysHostEntryStatus

{sysHost 11}

Description

The modification status of the configuration.

Object Identifier

1.3.6.1.4.1.886.1.1.28.11

Data Type

NonTabEntryStatus

Access Policy

Read-write

Status

Mandatory

Live Upgrade

The software Live Upgrade option gives you the ability to update software on a redundant VCO system without loss of calls, and with a minimum reduction in capacity. The procedure consists of:

- Installing the new software
- Updating the system controller (CPU card) and/or NBC3 card and/or DTG-2 card (if needed)
- Switching over to the new release
- Updating certain network and service circuit cards (if needed)

Details concerning the live upgrade process can be found in the system Generic Release Notes for the latest release.

This chapter provides information pertaining only to live upgrade data which can be accessed from the VCO MIB.

Caution The MIB software is not backward compatible. If you are using SNMP, and you upgrade to the latest software release, you must recompile the MIB.

liveUOperState

{liveU 1}

Description

The current operational state of the live upgrade process. The above includes both internal and external states. Internal states indicate some event in progress on the local side or a wait in progress for an event to occur on the other side and end with the suffix InProgress or OnOther, respectively. While the live upgrade process is in an internal state, the only user-initiated event or action that is possible is abort. External states indicate the completion of some event or activity and end with the suffix Complete. The user can initiate another event at this point by setting liveUAdminEvent. The valid next possible events at any given time is indicated by the object liveUValidNextEvents.

Object Identifier

1.3.6.1.4.1.886.1.1.31.1.1.1

Data Type

Integer. Possible values are:

Value	State
1	idle
2	prepareInProgress
3	prepareComplete
4	installInProgress
5	waitingForInstallOnOther
6	bothInstallsComplete
7	upgradeInProgress
8	upgradeComplete
9	configInProgress
10	configComplete
11	updateInProgress
12	waitingForUpdateOnOther
13	bothUpdatesComplete
14	switchoverInProgress
15	switchoverComplete
16	cutoverInProgress
17	cutoverComplete
18	backupInProgress
19	backupComplete
20	cleanupInProgress
21	abortInProgress

Access Policy

Read only

Status

Mandatory

liveUAdminEvent

{liveU 2}

Description

The desired event that the user wants to generate.

All events, other than installComplete, configOptSoftComplete, cutoverComplete, and backupDBComplete generate some activity on the switch. The four events above indicate to the switch the completion of some activity carried out by the user. The user performs these activities using other MIB groups or other facilities. Installation may be performed via FTP or some other means. Configuration of optional software is performed using the groups optSoft and etherCfg. Cutting over cards is performed using the Status objects of the cards being cut over. Backup may be performed via FTP or some other means.

Object Identifier

1.3.6.1.4.1.886.1.1.31.1.1.2

Data Type

Integer. Possible values are:

Value	State
1	prepareForInstall
2	installComplete
3	upgrade
4	configOptSoftComplete
5	update
6	switchover
7	cutoverComplete
8	backupDBComplete
9	cleanup
10	abort
11	none

Access Policy

Read-write

Status

Mandatory

liveUValidNextEvents

{liveU 3}

Description

This is a bit mask that indicates the valid 'next possible events' as follows:

bit #	Meaning
1	prepareForInstall
2	installComplete
3	upgrade
4	configOptSoftComplete
5	update
6	switchover
7	cutoverComplete
8	backupDBComplete

bit #	Meaning
9	cleanup
10	abort

Bits are numbered according to Motorola format (LSB is bit 0).

Object Identifier

1.3.6.1.4.1.886.1.1.31.1.1.3

Data Type

Integer. (0..'7ff'h)

Access Policy

Read only

Status

Mandatory

liveUProgress

{liveU 4}

Description

This object indicates whether a liveU operation (started by setting liveUAdminEvent) is pending or not. The meanings of the various values are as follows:

Value	Meaning
notPending	No operation has been started since the system was last booted
pending	An operation that was previously started is currently pending completion
completedWithSuccess	An operation that was previously started has completed with success
completedWithFailure	An operation that was previously started has completed with failure

Object Identifier

1.3.6.1.4.1.886.1.1.31.1.1.4

Data Type

Integer. Possible values are as follows:

Value	String
1	notPending
2	pending
3	completedWithSuccess
4	completedWithFailure

Access Policy

Read only

Status

Mandatory

liveUErrorStatus

{liveU 5}

Description

The reason for failure if liveUAdminEvent cannot be set or if there is any other failure.

Object Identifier

1.3.6.1.4.1.886.1.1.31.1.1.5

Data Type

Integer. Possible values are as follows:

Value	String
7424	unknownFailure
7425	illegalEvent
7426	standbyNotOnline
7427	notRedundant
7428	notAllowedOnActive
7429	intErrQueue
7430	intErrInvalidState
7431	intErrInvalidEvent
7432	intErrProcessing

Access Policy

Read only

Status

Mandatory

liveUOwnerString

{liveU 6}

Description

The entity that configured the liveU group.

Object Identifier

1.3.6.1.4.1.886.1.1.31.1.1.6

Data Type

OwnerString

Access Policy

Read-write

Status

Mandatory

liveUEntryStatus

{liveU 7}

Description

The status of the liveU group.

Object Identifier

1.3.6.1.4.1.886.1.1.31.1.1.7

Data Type

NonTabEntryStatus

Access Policy

Read-write

Status

Mandatory

liveULastModified

{liveUGroup 2}

Description

The time (in hundredths of a second) since the epoch that the liveU group was last modified.

Object Identifier

1.3.6.1.4.1.886.1.1.31.1.2

Data Type

TimeTicks

Access Policy

Read only

Status

Mandatory

liveUlogTable

{liveUGroup 2}

Description

The list of logs.

Object Identifier

1.3.6.1.4.1.886.1.1.31.2.1

Data Type

Sequence of LiveUlogEntry

Access Policy

Not accessible

Status

Mandatory

liveUlogEntry

{liveUlogTable 1}

Description

A log entry.

Object Identifier

1.3.6.1.4.1.886.1.1.31.2.1.1

Data Type

LiveUlogEntry

Access Policy

Not accessible

Status

Mandatory

liveUlogYear

{liveUlogEntry 1}

Description

The year of the log time-stamp.

Object Identifier

1.3.6.1.4.1.886.1.1.31.2.1.1.1

Data Type

Integer (1991..2119)

Access Policy

Read only

Status

Mandatory

liveUlogMonth

{liveUlogEntry 2}

Description

The month of the log time-stamp.

Object Identifier

1.3.6.1.4.1.886.1.1.31.2.1.1.2

Data Type

Integer. Possible values are as follows:

Value	String
1	january
2	february
3	march
4	april
5	may
6	june
7	july
8	august
9	september
10	october
11	november
12	december

Access Policy

Read only

Status

Mandatory

liveUlogDate

{liveUlogEntry 3}

Description

The date of the log time-stamp.

Object Identifier

1.3.6.1.4.1.886.1.1.31.2.1.1.3

Data Type

Integer (1...31)

Access Policy

Read only

Status

Mandatory

liveUlogHour

{liveUlogEntry 4}

Description

The hour of the log time-stamp.

Object Identifier

1.3.6.1.4.1.886.1.1.31.2.1.1.4

Data Type

Integer (0...23)

Access Policy

Read only

Status

Mandatory

liveUlogMin

{liveUlogEntry 5}

Description

The minute of the log time-stamp.

Object Identifier

1.3.6.1.4.1.886.1.1.31.2.1.1.5

Data Type

Integer (0...59)

Access Policy

Read only

Status

Mandatory

liveUlogSec

{liveUlogEntry 6}

Description

The second of the log time-stamp.

Object Identifier

1.3.6.1.4.1.886.1.1.31.2.1.1.6

Data Type

Integer (1...59)

Access Policy

Read only

Status

Mandatory

liveUlogSequence

{liveUlogEntry 7}

Description

The sequence number of this log entry for this time-stamp, starting with one (1). If there are multiple log entries with the same time-stamp, this value starts incrementing by 1 for each entry with the same time-stamp. When the time-stamp changes, this value starts again from one (1).

Object Identifier

1.3.6.1.4.1.886.1.1.31.2.1.1.7

Data Type

Integer

Access Policy

Read only

Status

Mandatory

liveUlogDay

{liveUlogEntry 8}

Description

The day of the week.

Object Identifier

1.3.6.1.4.1.886.1.1.31.2.1.1.8

Data Type

Integer. Possible values are:

Value	String
1	sunday
2	monday
3	tuesday
4	wednesday
5	thursday
6	friday
7	saturday

Access Policy

Read only

Status

Mandatory

liveUlogActSby

{liveUlogEntry 9}

Description

For nonredundant systems, the value of this object is always 'active'. For redundant systems, this object identifies whether the side of the switch issuing this message was active or standby.

Object Identifier

1.3.6.1.4.1.886.1.1.31.2.1.1.9

Data Type

Integer. Possible values are:

Value	String
1	active
2	standby
3	unknown

Access Policy

Read only

Status

Mandatory

liveUlogMessage

{liveUlogEntry 10}

Description

The log message itself.

Object Identifier

1.3.6.1.4.1.886.1.1.31.2.1.1.10

Data Type

DisplayString (size 1...80)

Access Policy

Read only

Status

Mandatory

liveUlogErrorStatus

{liveUlogEntry 11}

Description

The error that was encountered in the last log operation.

Object Identifier

1.3.6.1.4.1.886.1.1.31.2.1.1.11

Data Type

Integer. Possible values are as follows:

Value	String
7680	fileOpenErr
7681	fileSeekErr
7682	devAndDirUnknown
7683	dirListErr
7684	expectedRecNotFnd
7685	expectedEorNotFnd
7686	unexpectedEofOrErr

Access Policy

Read only

Status

Mandatory

Optional Software Group

The optional software group provides SNMP access to optional software components running on the VCO system, including TeleRouter, ISDN/NFAS, and the Ethernet communications package.

The following object listings provide access to generic configuration functions related to optional software products. Specific information relating to Ethernet configuration follows in the “Ethernet Communciations Group” section on page 2-101. Information pertaining to ISDN/NFAS can be found in Chapter 6, “Single-Span ISDN Card Group”. Information pertaining to TeleRouter can be found in the “Routing Table Group” section on page 10-55.

optSoftTable

{optSoft 1}

Description

The list of optional software entries.

Object Identifier

1.3.6.1.4.1.886.1.1.32.1.1

Data Type

Sequence of OptSoftEntry

Access Policy

Not accessible

Status

Mandatory

optSoftEntry

{optSoftTable 1}

Description

An optional software entry.

Object Identifier

1.3.6.1.4.1.886.1.1.32.1.1.1

Data Type

OptSoftEntry

Access Policy

Not accessible

Status

Mandatory

optSoftName

{optSoftEntry 1}

Description

The optional software to be enabled or disabled.

Possible values include:

Value	String
1	Telerouter
2	Ethernet
3	ISDN
4	NFAS

Object Identifier

1.3.6.1.4.1.886.1.1.32.1.1.1.1

Data Type

Integer

Access Policy

Read only

Status

Mandatory

optSoftOperState

{optSoftEntry 2}

Description

Contains the status of the optional software. Possible values are:

Value	String
1	enabled
2	disabled
3	notLoaded

Object Identifier

1.3.6.1.4.1.886.1.1.32.1.1.1.2

Data Type

Integer

Access Policy

Read only

Status

Mandatory

optSoftAdminState

{optSoftEntry 3}

Description

Determines if the optional software should be enabled or disabled. If the optional software is not loaded, the value returned is 'disable'. Possible values are:

Value	String
1	enable
2	disable

Object Identifier

1.3.6.1.4.1.886.1.1.32.1.1.1.3

Data Type

Integer

Access Policy

Read-write

Status

Mandatory

optSoftErrorStatus

{optSoftEntry 4}

Description

The reason for failure if optSoftState cannot be set to the desired state or if there is some other error. Possible values are:

Value	String
7936	unknownFailure
7937	softwareNotLoaded

Object Identifier

1.3.6.1.4.1.886.1.1.32.1.1.1.4

Data Type

Integer

Access Policy

Read only

Status

Mandatory

optSoftOwnerString

{optSoftEntry 5}

Description

The entity that configured this entry and is therefore using the entry assigned to it.

Object Identifier

1.3.6.1.4.1.886.1.1.32.1.1.1.5

Data Type

OwnerString

Access Policy

Read-write

Status

Mandatory

optSoftEntryStatus

{optSoftEntry 6}

Description

The status of the optional software group.

Object Identifier

1.3.6.1.4.1.886.1.1.32.1.1.1.6

Data Type

FixedTabEntryStatus

Access Policy

Read-write

Status

Mandatory

optSoftTableLastModified

{optSoftEntry 2}

Description

The time (in hundredths of a second) since the epoch that the optional software table was last modified.

Object Identifier

1.3.6.1.4.1.886.1.1.32.1.2

Data Type

TimeTicks

Access Policy

Read only

Status

Mandatory

Ethernet Communciations Group

The Ethernet Communications Package supports Ethernet TCP/IP communications between the VCO system and one or more host computers. It is an optional package that consists of software and documentation.

TCP error handling includes checksum verification of messages, sequential message delivery, and protection against message duplication.

The Ethernet package supports a single physical link with multiple logical connections (i.e., sockets, which are the interface between the Ethernet communications protocol, and the application). The VCO system supports up to eight simultaneous sockets, using the BSD 4.3 Internet Domain sockets interface.

The VCO MIB provides access to system Ethernet configuration functions, including:

- Setting and changing IP addresses and subnet masks
- Configuring NFS access, IP addresses, names, IDs, and mount points
- Setting system names, IDs, and umasks
- Checking error status

The following object listings provide further details concerning Ethernet configuration through SNMP queries to the VCO MIB.

etherCfgOperSysInetAddr

{etherCfg 1}

Description

The current IP address of this switch.

Object Identifier

1.3.6.1.4.1.886.1.1.32.2.1.1

Data Type

IpAddress

Access Policy

Read only

Status

Mandatory

etherCfgAdminSysInetAddr

{etherCfg 2}

Description

The desired IP address of this switch.

Object Identifier

1.3.6.1.4.1.886.1.1.32.2.1.2

Data Type

IpAddress

Access Policy

Read-write

Status

Mandatory

etherCfgNFSFileAccess

{etherCfg 3}

Description

Enables or disables NFS file access.

Object Identifier

1.3.6.1.4.1.886.1.1.32.2.1.3

Data Type

Integer

Access Policy

Read-write

Status

Mandatory

etherCfgNFSServerInetAddr

{etherCfg 4}

Description

The IP address of the NFS server.

Object Identifier

1.3.6.1.4.1.886.1.1.32.2.1.4

Data Type

IpAddress

Access Policy

Read-write

Status

Mandatory

etherCfgNFSServerName

{etherCfg 5}

Description

The NFS server name.

Object Identifier

1.3.6.1.4.1.886.1.1.32.2.1.5

Data Type

DisplayString (SIZE (0..15))

Access Policy

Read-write

Status

Mandatory

etherCfgNFSMountDirPt

{etherCfg 6}

Description

The NFS Server Mount Directory Point.

Object Identifier

1.3.6.1.4.1.886.1.1.32.2.1.6

Data Type

DisplayString (SIZE (0..47))

Access Policy

Read-write

Status

Mandatory

etherCfgTargetSysName

{etherCfg 7}

Description

The system name of this switch.

Object Identifier

1.3.6.1.4.1.886.1.1.32.2.1.7

Data Type

DisplayString (SIZE (0..15))

Access Policy

Read-write

Status

Mandatory

etherCfgTargetSysUID

{etherCfg 8}

Description

The user id assigned to this switch.

Object Identifier

1.3.6.1.4.1.886.1.1.32.2.1.8

Data Type

Integer (0..65535)

Access Policy

Read-write

Status

Mandatory

etherCfgTargetSysGID

{etherCfg 9}

Description

The group id assigned to this switch.

Object Identifier

1.3.6.1.4.1.886.1.1.32.2.1.9

Data Type

Integer (0..65535)

Access Policy

Read-write

Status

Mandatory

etherCfgTargetSysUMask

{etherCfg 10}

Description

The Umask assigned to this switch. This should consist of no more than 3 numerals with no numeral exceeding the number 7 (i.e., octal values).

Object Identifier

1.3.6.1.4.1.886.1.1.32.2.1.10

Data Type

Integer

Access Policy

Read-write

Status

Mandatory

etherCfgErrorStatus

{etherCfg 11}

Description

Registers the last error that occurred in this group. Possible values are:

Value	String
8192	invalidValue
8193	unacceptableIpAddr

Object Identifier

1.3.6.1.4.1.886.1.1.32.2.1.11

Data Type

Integer

Access Policy

Read only

Status

Mandatory

etherCfgOwnerString

{etherCfg 12}

Description

The entity that configured this entry and is therefore using the entry assigned to it.

Object Identifier

1.3.6.1.4.1.886.1.1.32.2.1.12

Data Type

OwnerString

Access Policy

Read-write

Status

Mandatory

etherCfgEntryStatus

{etherCfg 13}

Description

The status of this table entry.

Object Identifier

1.3.6.1.4.1.886.1.1.32.2.1.13

Data Type

NonTabEntryStatus

Access Policy

Read-write

Status

Mandatory

etherCfgSysSubnetMask

{etherCfg 14}

Description

The subnet mask of this system.

Object Identifier

1.3.6.1.4.1.886.1.1.32.2.1.14

Data Type

IpAddress

Access Policy

Read-write

Status

Mandatory

etherCfgLastModified

{etherCfgGroup 2}

Description

The time (in hundredths of a second) since the epoch that the etherCfg group was last modified.

Object Identifier

1.3.6.1.4.1.886.1.1.32.2.2

Data Type

TimeTicks

Access Policy

Read only

Status

Mandatory