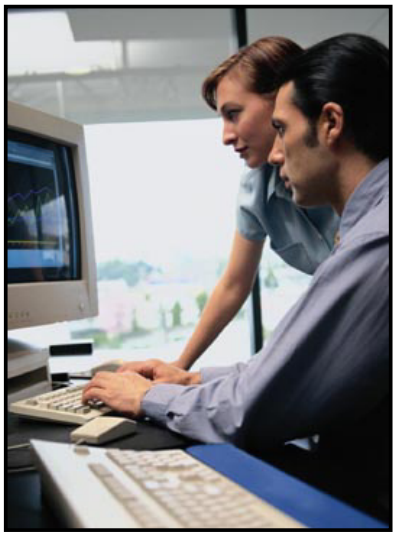
# CiscoWorks CiscoView

# CiscoView v6.1 Tutorial

# About This Tutorial

Cisco.com

- **Identify the need for easy to use, graphical network management tools**
- **Describe how to use CiscoView to configure and monitor Cisco devices**
- **Provide several scenarios for using CiscoView to configure and monitor Cisco devices**
- **Provide helpful install and maintenance guidelines for system administrators**
- **Provide links to helpful reference documents on CiscoWorks and CiscoView**



CiscoView v6.1 Tutorial



-2

## About This Tutorial

The CiscoWorks CiscoView tutorial provides self-paced training focused on using CiscoView for configuring and monitoring Cisco network devices using SNMP (Simple Network Management Protocol). This tutorial will focus on how to use and administer CiscoView to manage your Cisco network devices.

CiscoView is available with the purchase of the CiscoWorks LAN Management Solution (LMS) or the CiscoWorks Small Network Management Solution (SNMS) . CiscoWorks is a suite of network management applications used for configuring, administering, monitoring, and troubleshooting a Cisco-based network. It enables network administrators to effectively manage their small/medium/large enterprise networks.

The tutorial is structured as a series of self-paced modules, or chapters, that conclude with self-administered exercises. Also included as part of the tutorial is a helpful reference section containing links to technical documents on component products, concepts, and terminology. The tutorial material is presented through text, illustrations, hypertext links, and typical scenarios.

This tutorial is not intended to teach you how to manage your network, but rather it will help you to use the configuration and monitoring features of CiscoView, which in the end will help you to manage the individual devices in the network.

# How the Tutorial Is Organized

Cisco.com

| | |
|---|---|
| **Chapter 1**<br>Introduction to Network Management Using CiscoView | Review the importance of network management, the tools, and the data available |
| **Chapter 2**<br>Using CiscoView for Cisco Device Management | Learn how CiscoView can help a user to easily configure and monitor Cisco devices |
| **Chapter 3**<br>Scenarios | Using an example, learn how CiscoView can help manage Cisco network devices |
| **Chapter 4**<br>System Administration Guidelines | Review important system requirements, installation guidelines, and system troubleshooting tools |
| **Chapter 5**<br>Helpful Links to Reference Material | A comprehensive set of links to information on CiscoWorks and CiscoView |

CiscoView v6.1 Tutorial



-3

# How This Tutorial Is Organized

The tutorial is divided into five chapters. Each chapter outlines its specific learning objectives, and concludes with a series of self-assessment exercises based on the chapter objectives. The multiple-choice exercises provide a means for you to assess your understanding of the material presented in a given chapter. A summary of each chapter is listed below.

### *Chapter 1: Introduction to Network Management Using CiscoView*

This chapter identifies the need for using graphical network management tools for simplifying the management of network devices. This chapter will first identify the need for network management and various tools used to configure and monitor network devices. Finally, the chapter will introduce CiscoView as a graphical tool for performing common network management tasks.

### *Chapter 2: Using CiscoView for Cisco Device Management*

This chapter discusses the key features of CiscoView in a manner that allows you to understand not only the product as a whole, but any reason for the individual tasks necessary for using CiscoView. Before getting into the specifics on how to use the various functions of CiscoView, the chapter discusses its architecture,, to provide an understanding of how CiscoView is used to configure and monitor Cisco devices. A workflow for using CiscoView is presented in a logical manner showing how you would begin and continue to use its features.

### *Chapter 3: CiscoView Scenarios*

This chapter walks you through a step-by-step examples to provide hands-on experience using CiscoView. The scenarios begins with steps on how to get started, followed by device configuration and monitoring activities. The scenarios will help to reinforce the information learned in Chapter 2.

### *Chapter 4: System Administration Guidelines*

This chapter provides information about server requirements, software installation guidelines, and tips for troubleshooting and avoiding common problems when using CiscoView. Detailed instructions on installing the software can be found in the CiscoView Installation Guide. A link to these documents can be found in the References section of the tutorial (Chapter 5).

### *Chapter 5: References*

This chapter contains a comprehensive list of additional product information, such as links to related white papers and documentation.

### *Chapter Questions and Answers*

This section contains the answers to the questions that conclude each chapter.

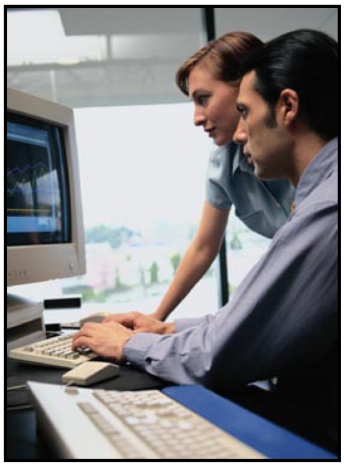
# Introduction to Network Management Using CiscoView

## Chapter 1

# Chapter 1 Outline

Cisco.com

- **Importance of Managing Network Devices**
  - *Configuration Management*
  - *Performance Management*
  - *Fault Management*
- **Common Ways to Analyze the Configuration, Performance, and Faults on a Cisco Device**
  - *CLI (Command Line Interface)*
  - *SNMP (Simple Network Management Protocol)*
  - *CiscoView*
- **A Closer Look At CiscoView**
  - *Where to Find CiscoView*
  - *Supported Devices*







## Chapter 1 Outline

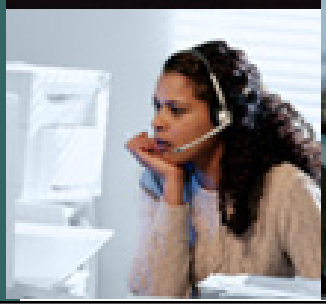
Welcome to the CiscoView tutorial! Before introducing CiscoView, let's first acknowledge the importance of managing the individual network devices. Management begins first with configuring the devices and continues with monitoring the performance of the devices as well as detecting, isolating, and diagnosing faults with a device.

Secondly, the chapter will look at different ways network administrators can manage network devices. Managing the devices begins with accessing the device, locally or remotely. And common methods for accessing the configuration or statistics of a device include, but are not limited to, the CLI (Command Line Interface) and SNMP (Simple Network Management Protocol) queries.

And finally, the chapter will introduce CiscoView as a way to access the configuration or status of a Cisco device. CiscoView is a graphical tool for managing supported Cisco devices. Find out how CiscoView can be obtained. And get a quick look at how CiscoView can be used for configuration, performance, and fault management.

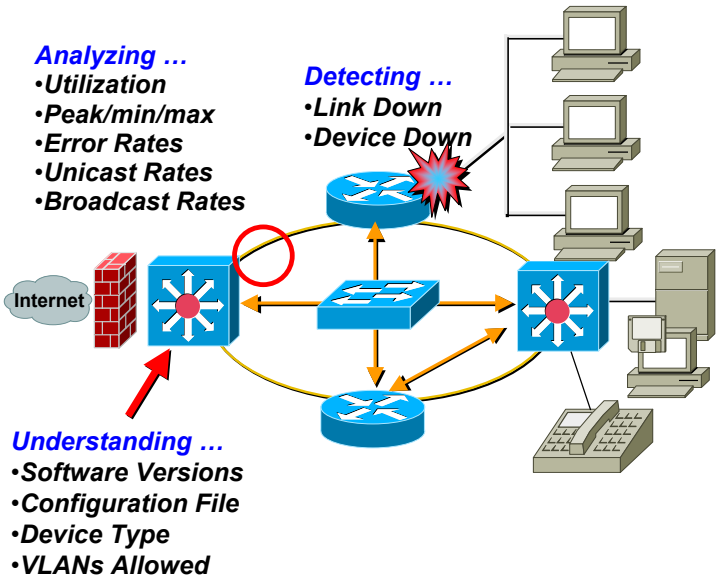
# The Importance of Managing Network Devices

- **The Importance of Managing Network Devices**
- Common Ways to Manage Devices
- A Closer Look at CiscoView



# Managing Your Network

Cisco.com




- **The operation of the network is crucial to most businesses**
- **The overall network performance is dependent upon the performance of *each* network device**
- **Important to manage each device for:**
  - *Faults*
  - *Performance*
  - *Configuration*





## Managing Your Network

There is no doubt that networks are the foundation that most organizations depend on for their day-to-day, mission critical operations. Businesses today rely on their networks to provide reliable and responsive communications and services for departments and business partners located in every corner of the globe, to enable device, file, and application sharing and to provide portals for e-commerce services.

With the network being such a crucial element in the operation of a business, the management of individual network devices is essential. Understanding how and when the network and shared systems and applications are being used is critical to the effective use and planning of networks. Also, tracking performance and faults of networks, systems and applications in real-time is also essential for minimizing downtime and maximizing availability, service levels and customer satisfaction.

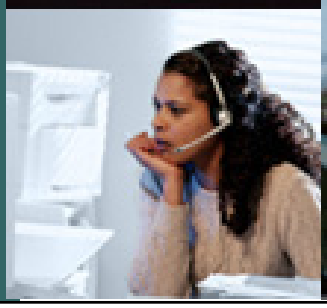
When determining cost of downtime or degradation, lost productivity and lost revenue must be taken into account. A study conducted by Infonetics, Inc., an international market research company, showed that network degradations result in an approximate 16 percent loss of networked worker productivity and a 10 percent loss in revenue, as a result of the decreased productivity of revenue-producing employees. If the network were to be down completely, these figures increase to 24 percent lost productivity from networked employees and revenue loss of as much as 60 percent. A company with 1000 employees and annual revenues of $200 million, as an example, could suffer losses that easily surpass $8,000 per hour. Tools, like CiscoView, help to discover problems before they occur and help to resolve the problem quickly.

Additionally, understanding the configuration of network devices will assist the network administrators with network planning, troubleshooting, and implementation. Managing the configuration of devices can be daunting; it includes every changeable aspect of the device, such as the individual modules, the different software versions, and each line the configuration file.

*Managing your network is not optional; it is essential to the business that it supports!*

# Common Ways to Manage Devices

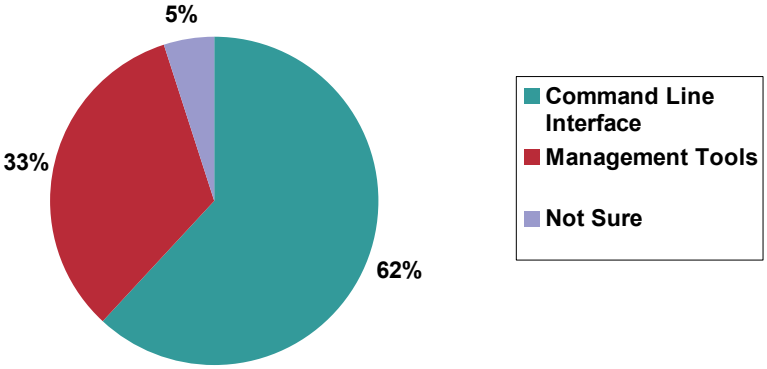
- The Importance of Managing Network Devices
- ➢ **Common Ways to Manage Devices**
- A Closer Look at CiscoView



# End-Users' Perspective

Cisco.com

**"What method do you prefer for configuring and managing network devices?"**




Source: Cisco Web Seminar 522 Viewers





## End-Users' Perspective

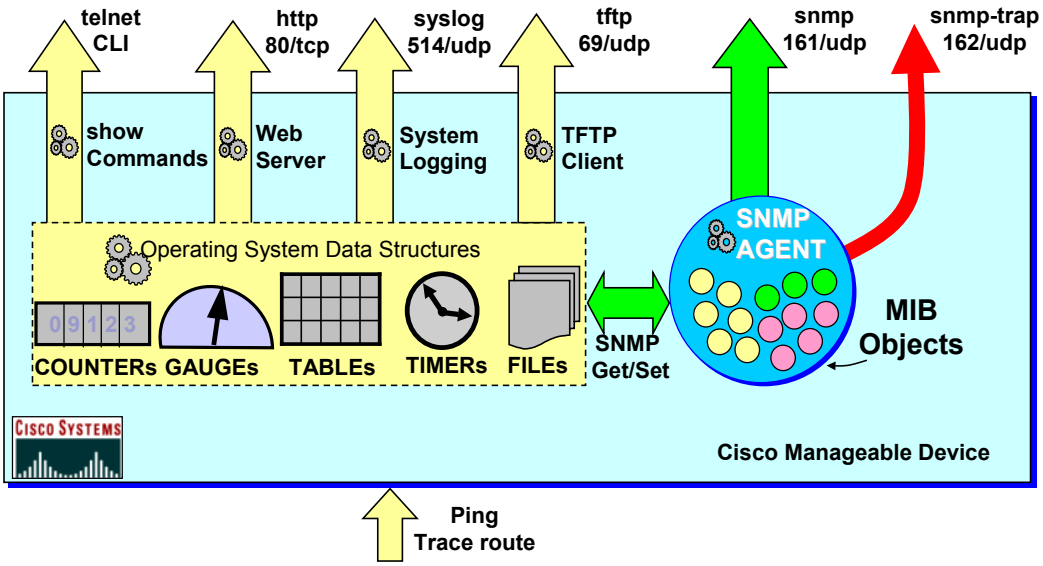
So how do network managers today, manage or configure their devices?

A decade ago, every network administrator would configure and manage their network devices directly from the command line interface (CLI) of the device. But times have changed since then. Network administrators are having to do more with less resources. The enterprise networks are much larger and configuration of the networks are much more complex by introducing IP telephony into data networks, and maintaining quality of service requirements.

Thus, many network administrators are using or considering network management tools to help with many of the redundant tasks associated with configuring and monitoring individual network devices. Network management tool vendors are continuously improving the ease of use and efficiency of their tools. But, when all else fails, the command line interface is always there for configuring and monitoring the device.

# Sources of Network Management Data

Cisco.com








## Sources of Network Management Data

So where does all the information come from to help manage the network devices?

Every Cisco device has internal mechanisms designed to report on its status and configuration. Access to the data provided by these internal data structures is essential for network management activities.

The data structures can consist of: counters, gauges, tables, timers, and files. The data or links to the data can be stored on the device in a Management Information Base or MIB.

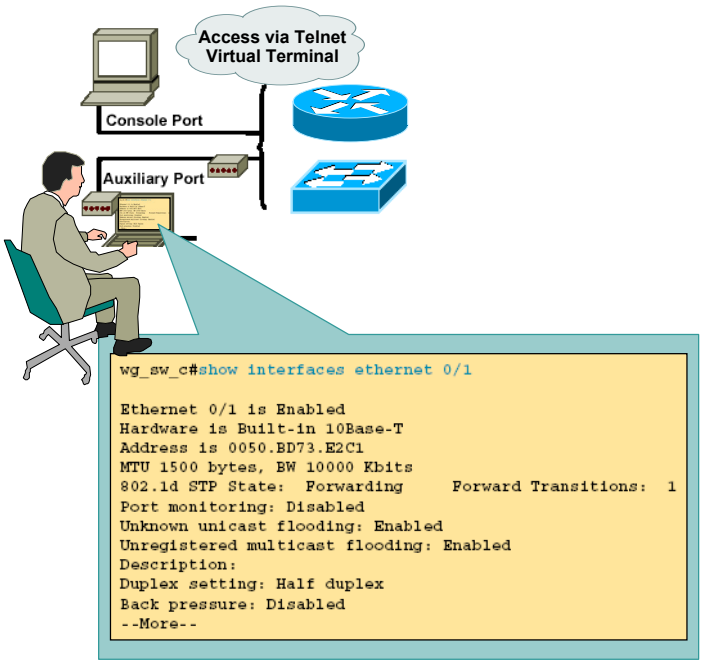
The retrieval and/or modification of the information in these data structures for network management purposes can be achieved through numerous communication protocols (depending on the device type) including the traditional Command-Line Interface (CLI), telnet, HTTP, syslog, and TFTP. Other simple applications can also provide network management information such as ping and trace route.

In an effort to standardize the mechanism used for device status information necessary for network management tasks, the Management Information Base (MIB) information model was created. Likewise the Simple Network Management Protocol (SNMP) was chosen as the standardized communication model or network protocol for retrieving information held by the MIB.

*Note: The mechanism implementations vary from one system to another. Factors that can be used to characterize the mechanisms include device type, make of device, operating system, version of operating system, and so on.*

# CLI – Command Line Interface

Cisco.com




- **Access the CLI of a network device using direct console port, auxiliary port, or Telnet**
- **Use the CLI to view statistics or the configuration of a device, card, or interface**
- **Use the CLI to modify the configuration of a device**





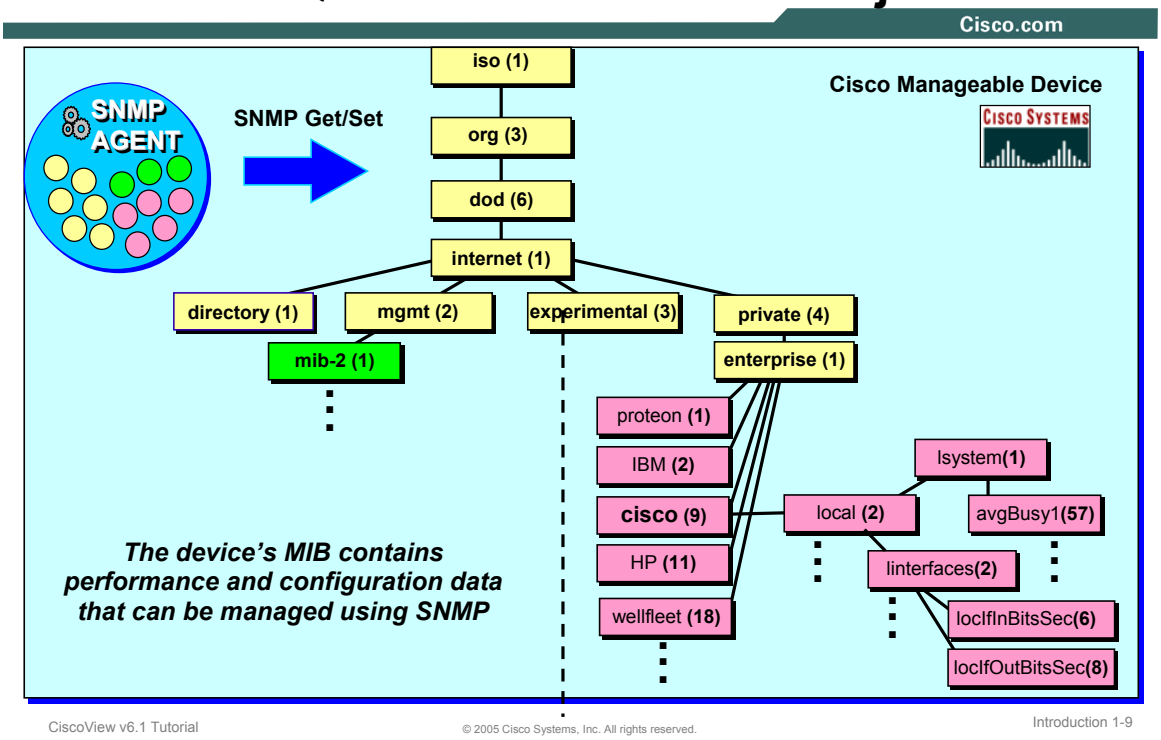
## Using the CLI to Manage Devices

The Command Line Interface (CLI) provides direct access to the set-up, configuration, and statistics of a device. The user must first get access to the device either through the network using Telnet or by directly connecting to the device through its console or auxiliary port.

Once the user has access to the device, the device may be configured to authenticate the user for access. And once authenticated, the user must be familiar with the commands and the command syntax to be entered.

Skilled users may prefer the CLI than a graphical user interface (GUI) because it may be faster to use for simple tasks or the command syntax can be entered in one line rather than a series of menus. But for the novice user, it can be challenging to remember all the commands and the command syntax.

# SNMP – Queries to Device MIB Objects




## Using SNMP to Manage Devices

SNMP tools and utilities provide an alternative to using the CLI to access the data structures in a device across the network. As previously mentioned, the performance statistics or configuration parameters are stored on the device in data structures, called a MIB. Using SNMP, the data in the MIB is network accessible by knowing the hierarchical tree structure's object ID.

As illustrated above, the MIB can be quite large and is easily extendible by the device manufacturers. Since the data structure is hierarchical, each one of the branches of the MIB tree can be added onto. Each vendor can add on to their data structure from the private>enterprise branch. Cisco's MIB contains the statistics and configuration for the device itself and every interface on each module.

To access the data in the MIB, SNMP managers (tools or utilities on a PC) send a message across the network to the SNMP agent enabled on a device. The SNMP managers and agents encapsulate messages and responses in UDP for transmission over IP. Each SNMP message contains a text string (community string) used to restrict access to managed devices. In order to read or write from/to the device MIB the community strings must match on the SNMP manager and agent (device). (*These SNMP community strings are what we call Device Credentials, discussed later in this tutorial.*)

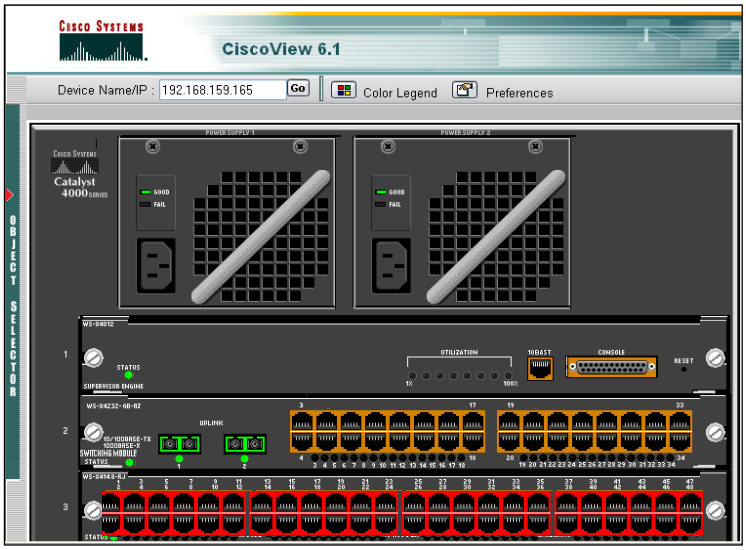
**Different Versions of SNMP (v1/v2/v3)**

Today, virtually all vendors of network-based equipment provide SNMP agents in their devices to provide management capability across the TCP/IP-based network. SNMP was first introduce in 1988. To enhance the basic functionality, a new version of SNMP was introduced in 1993 and revised in 1996. SNMPv2 added the retrieve of bulk data and other extensions. However, neither SNMPv1 nor SNMPv2 offered security features. SNMPv3 is SNMPv2 plus added administration and security features lacking in v2. SNMPv3 includes three important services: authentication, privacy, and access control through the following features:

- SNMP v3 messages may be encrypted to ensure privacy
- Agent may enforce access control policies to ensure limited access to its data
- Transmission from the SNMP manager to the agent may be authenticated

# CiscoView – A Cisco Graphical Alternative

Cisco.com




- **A graphical SNMP-based tool to manage Cisco devices**
- **Graphically view/modify the configuration of a Cisco device (No syntax knowledge required!)**
- **Graphically monitor real-time status or statistics of a Cisco device and its components**





## Using CiscoView to Manage Devices

CiscoView is a graphical device management tool that uses SNMP v2/v3 to retrieve or set performance and configuration data from networked Cisco devices. Using the performance data retrieved, CiscoView provides real-time views of Cisco devices. These views deliver a continuously updated physical/logical picture of device configuration and performance conditions. With the proper user authorization, the user can configure a Cisco device, its cards and interfaces. The user can also monitor real-time statistics for interfaces, resource utilization, and device performance.

CiscoView simply uses SNMP to queries the configuration and performance of the device and displays the information graphically. Given the proper user authorization privileges, CiscoView can also be used to change or modify the configuration of the device using SNMP.

There network managers can use CiscoView to:

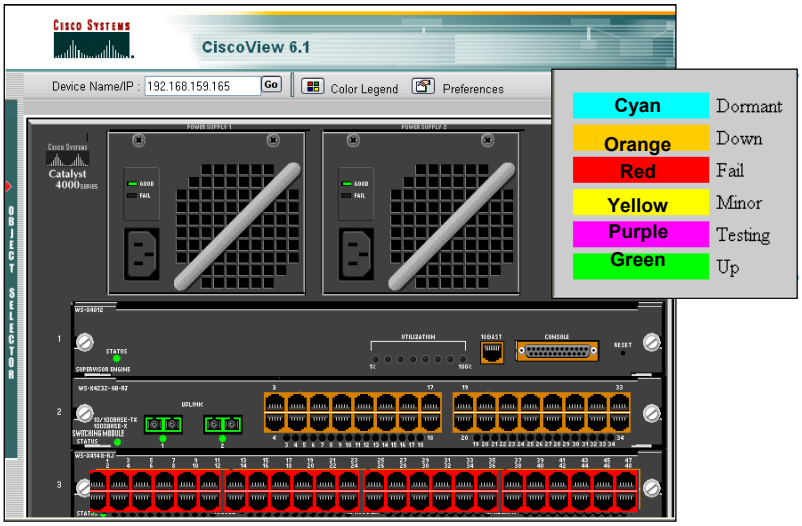
- View a graphical representation of the device, including component (interface, card, power supply, LED) status.
- Configure parameters for devices, cards, and interfaces.
- Monitor real-time statistics for interfaces, resource utilization, and device performance.
- Set user preferences.
- Perform device-specific operations as defined in each device package.
- Manage groups of stackable devices.

# A Closer Look at CiscoView

- The Importance of Managing Network Devices
- Common Ways to Manage Devices
- ➢ **A Closer Look at CiscoView**

# CiscoView for Fault Management

Cisco.com




**Graphical real-time status view of a Cisco device and its components**

**Status is color coded based on recently polled information from device MIB**





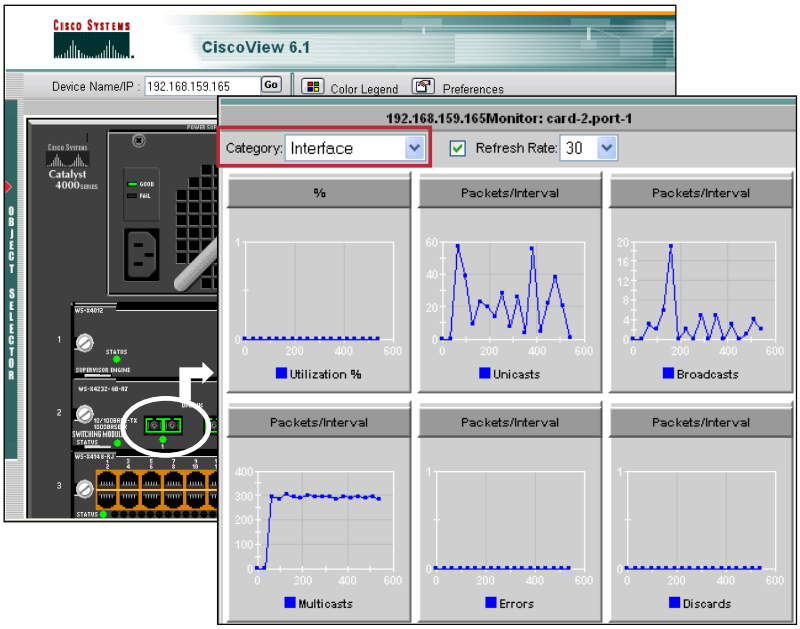
## CiscoView for Fault Management

The goal of any fault management strategy should be the detection, isolation, and correction of any condition that may lead to network service degradation, prior to it actually disrupting the normal behavior of the network. For many physical type faults (i.e. interface down) this may seem like a fairly straightforward exercise. However, many times these faults are a result of other more subtle conditions on a device (i.e. buffer utilization). For example, when an interface buffer reaches its thresholds, the packets may be throttled back, the buffer may overflow, the packets may get buffered elsewhere, or simply dropped. This subtle condition may have been the root cause of a service or device degradation or fault condition. Thus, the real trick to fault management is determining what conditions lead to faults, and what information to gather in order to detect the condition.

CiscoView presents an image of the device as if standing in front of it. A user could use this image to quickly ascertain physical faults by viewing the status of ports and cards on the device. The user could then use CiscoView to drill down into the device or interface and monitor real-time statistics for interfaces, resource utilization, and device performance.

# CiscoView for Performance Management

Cisco.com




- **Drill down to view real-time device, card, or interface statistics**
- **No command syntax is needed to get the data**
- **Types of categories and statistics may vary for each device based on the software type and version**





## CiscoView for Performance Management

One key to delivering a responsive and reliable network services is performance management. The performance of the network overall is a function of how well each individual network device is performing. Thus, monitoring the performance of core network devices is essential for minimizing downtime and maximizing availability, service levels and customer satisfaction.

CiscoView provides the user with real-time statistics graphically; no command syntax is needed. The user can quickly verify the integrity of an interface by looking at the interface color codes. Additionally, the user can then monitor real-time the resources of the device (CPU busy, memory, buffers) or polling real-time interface statistics from a network device. This is often the first step for troubleshooting performance related issues.

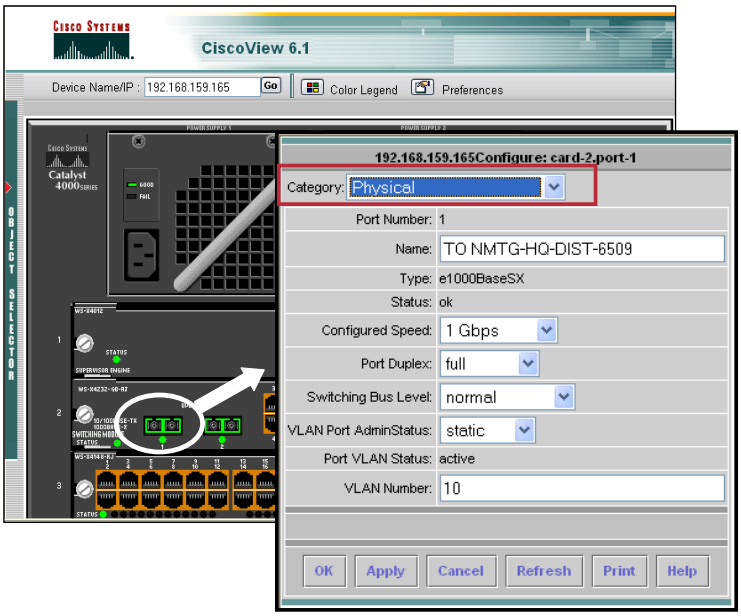
CiscoView provides a moving window of real-time data which is polled from the device and displayed. Note that the polling frequency can be configured and that the real-time data is only displayed and the data is not stored on the CiscoWorks server.

*Note(s):*

- *The maximum amount of data displayed is 25 data points. Thus, if the polling frequency is set to 30 seconds, then the moving window will display the last 12.5 minutes of data.*

# CiscoView for Configuration Management

Cisco.com




- **Graphically view/modify the configuration parameters of a Cisco device**
- **No command syntax is needed to get/set the values**
- **Types of configuration categories may vary for each device based on the device type and software version**





## CiscoView for Configuration Management

Understanding the configuration of a network device is at the very root of all network management tasks. If a clear picture of the connectivity and configuration of the device is known, then the network can be effectively maintained, and problems can be easily resolved.

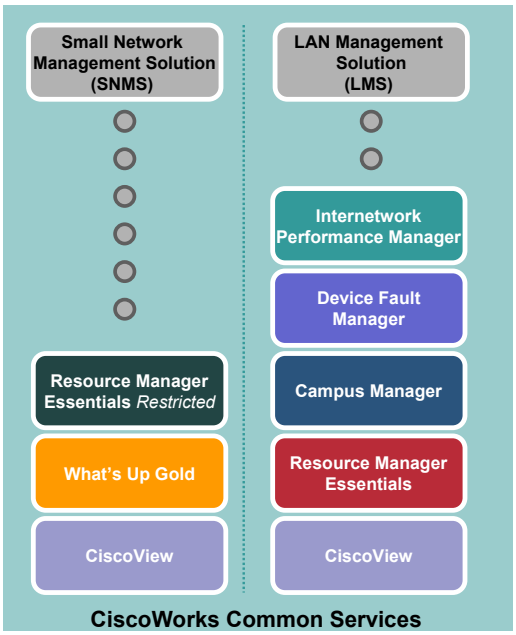
CiscoView provides the user with a graphical view of the device and an easy way for the user to access and/or modify the configuration of the device, card or interface graphically with **no** command syntax needed to be entered or known.

*Note(s):*

- *Not every configuration parameters on a device may be configurable with CiscoView, but the list of Configuration Categories and Parameters is growing. As long as the configuration parameter (feature) is accessible with SNMP, CiscoView can configure it! In the past, CiscoView only worked well with the CatOS switches. But as newer IOS software versions come out and with the advent of SNMPv3, more and more features will be configurable by SNMP (and CiscoView).*
- *Depending upon the device and OS version, CiscoView can also launch embedded addlets or applications (I.e. StackMaker, Cluster Management Suite, or Catalyst QoS Device Manager) on the device to support the configuration of features that can not be configured using SNMP. These addlets can be launched from the context menus that appear when configuring a device.*
- *Keep in mind that once the configuration of a device has been changed, the CiscoWorks Resource Manager Essentials (RME) application can be used to maintain a current archive of devices configurations as well as track the changes to them.*

# Where to Find CiscoView

Cisco.com




- **CiscoView is available in various CiscoWorks solution bundles**
  - **SNMS**
  - **LMS**
- **All applications within a CiscoWorks bundle require the CiscoWorks Common Services to be installed**





## Where to Find CiscoView

CiscoView is available in one of several CiscoWorks solution bundles such as: SNMS (Small Network Management Solution) and LMS (LAN Management Solution).

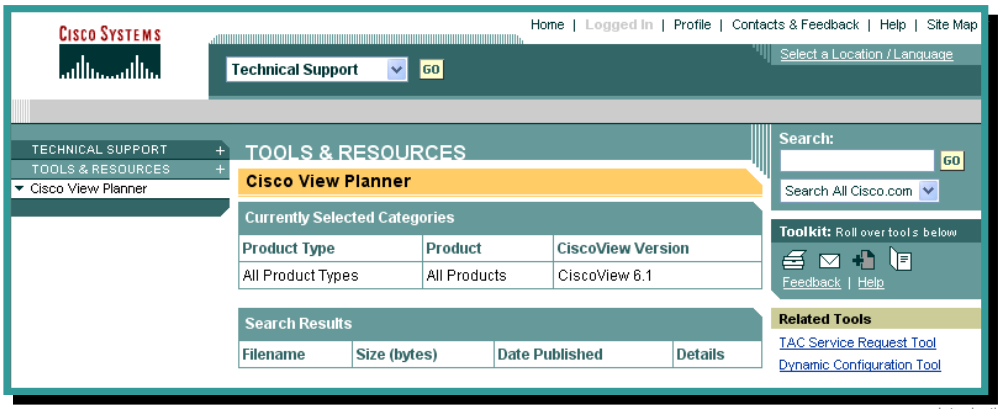
The applications within the CiscoWorks bundles all rely upon the CiscoWorks Common Services (CCS) software that is installed on the CiscoWorks server. These services provide the necessary background processes for accessing the database, web services, network discovery, process management, security, and more.

Now that the applications share the same database information, less information needs to be entered by the CiscoView user. Devices can be discovered by Campus Manager; SNMP community strings can be entered and managed by Resource Manager Essentials; and all this information can be stored in a common Device Credential Repository shared by all applications.

# Devices Supported By CiscoView

Cisco.com

- ***CiscoView supports numerous Cisco devices. Go to the CiscoView Planner web page to view the devices supported.***
- ***Depending upon the device type and software release, CiscoView may be able to configure or monitor different aspects of a device using SNMP.***








## Devices Supported by CiscoView

There are too many devices supported by CiscoView to list all of them here in this tutorial. To find out if a particular device is supported by CiscoView, refer to the CiscoView Planner page at the following URL. First, go to Cisco.com and log in. Then, go to the following URL:

http://www.cisco.com/cgi-bin/Software/CiscoView/cvresult.cgi?product_class=All+Product+Types&product=All+Products&application=CiscoView+6.1

Not every configuration parameter on a device may be configurable with CiscoView, but the list of Configuration Categories and Parameters is growing. As long as the configuration parameter (feature) is accessible with SNMP, CiscoView can configure it! In older software releases, CiscoView worked best with the CatOS switches. But as newer IOS software versions come out and with the advent of SNMPv3, more and more features will be configurable by SNMP (and CiscoView).

If the device is supported and CiscoView fails to display the device, then check one of the following:

- The SNMP server may not be set in the device.
- The SNMP credentials are incorrect. Verify that the device attributes are correct in the CiscoWorks Device and Credential Repository (DCR). See *User Guide for CiscoWorks Common Services* for more information.
- The management station cannot reach and successfully ping the device.
- The timeout value is too low in a busy network. Doubling the existing timeout value is a good starting point. Open the Device Preferences dialog box by either selecting *Administration > Device Preferences* from the CiscoView tab in the CiscoWorks homepage or clicking *Preferences* from the Options bar in the CiscoView desktop.
- The device package is not up-to-date. Check the CiscoView device packages and compare the date to the Cisco.com device package version. Upgrade the device package to the latest version, if required. Refer to Chapter 2 for more information on upgrading the device packages.

# Helpful Links to More Information

Cisco.com

**To learn more on SNMP v3:**

**www.cisco.com/warp/public/759/ipj_1-3/ipj_1-3_snmpv3.html**

**Use Cisco's SNMP Object Navigator and take advantage of this helpful online tool:**

**tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en**

**User Guide for CiscoWorks CiscoView v6.1:**

**http://www.cisco.com/en/US/partner/products/sw/cscowork/ps2406/products_user_guide_book09186a00800f6dd4.html**





## Helpful Links to More Information

The URLs above provide a wealth of information on SNMP, Cisco's SNMP Object Navigator, and CiscoView. Additional reference documents and URLs on CiscoView and related information can also be found in Chapter 5 of this tutorial.

18

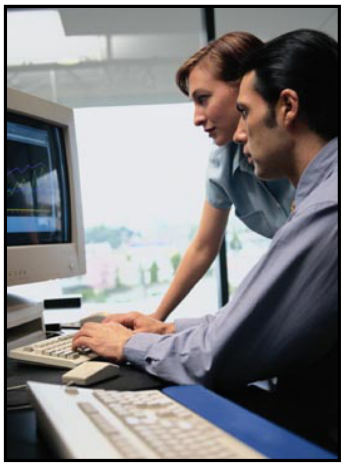
# Using CiscoView for Device Management

## Chapter 2

# Chapter 2 Outline

Cisco.com

- **How CiscoView Works**
- **Getting Ready to Use CiscoView**
  - *Managing CiscoView Software Updates*
  - *Managing Devices and Credentials*
- **Managing Cisco Devices Using CiscoView**
  - *Monitoring Cisco devices*
  - *Configuring Cisco devices*







## Chapter 2 Outline

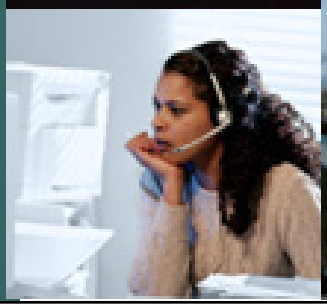
This chapter contains a quick overview of how CiscoView works – the functional architecture and its important underlying components and protocols.

Additionally, this chapter will assist the CiscoView user prepare the software for use by understanding the importance of updating of CiscoView software and device packages and managing devices, device groups, and their credentials.

And finally, this chapter will outline the procedures for using CiscoView to manage Cisco devices.

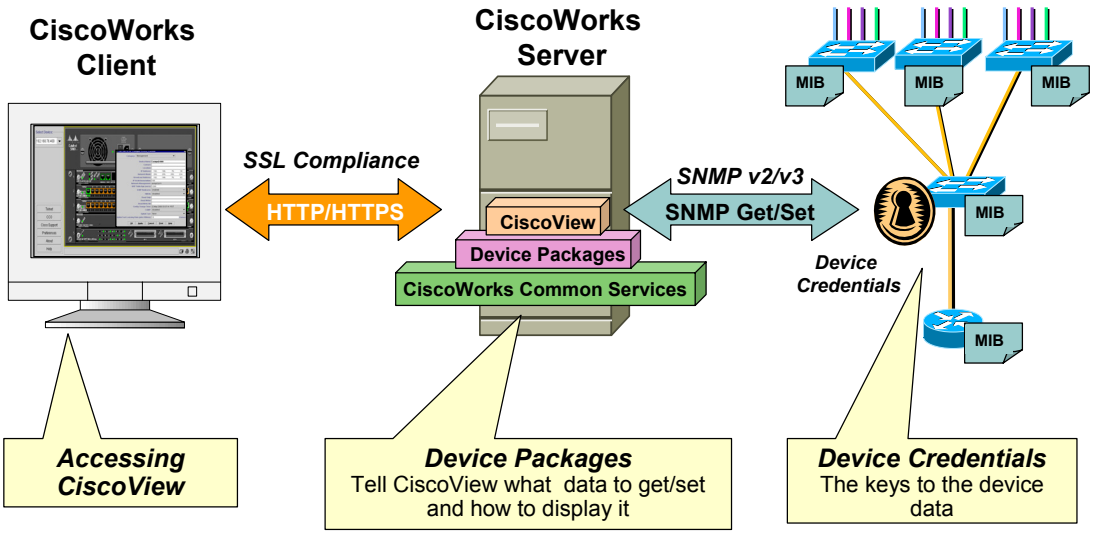
# How CiscoView Works

- ➢ **How CiscoView Works**
- Getting Ready to Use CiscoView
- Managing Cisco Devices Using CiscoView



# CiscoView Overview

Cisco.com








## CiscoView Overview

To understand how it all works, let's first look at a functional overview of CiscoView. (More information on these topics will be discussed on the next few pages in this section.)

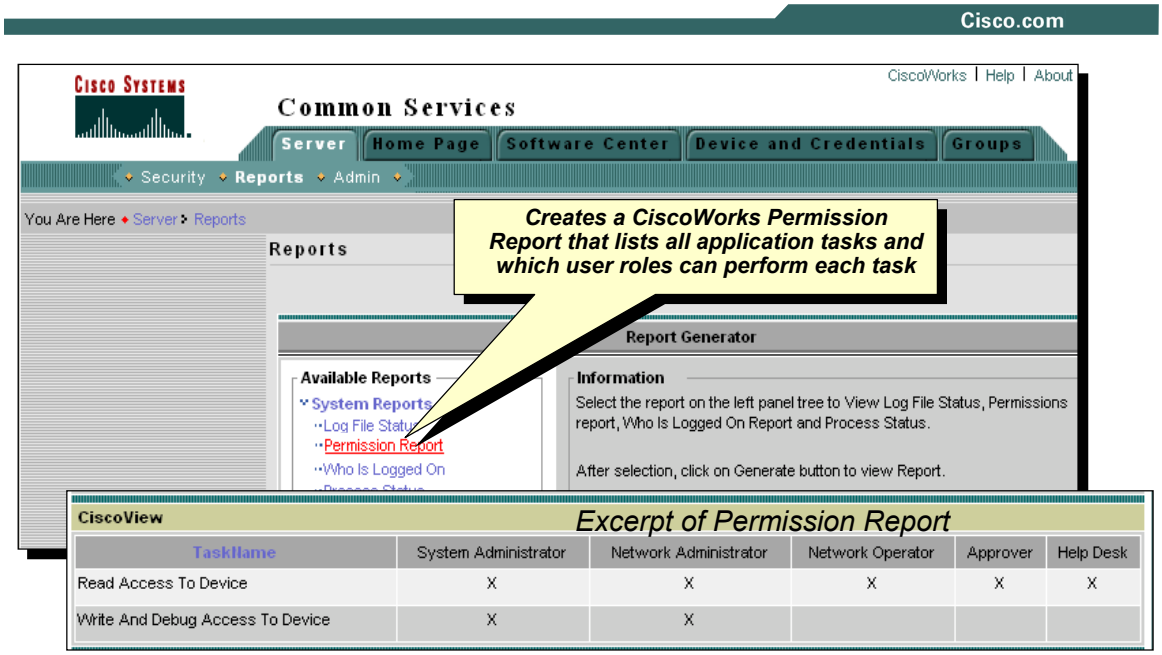
As previously mentioned, CiscoView is a graphical device management tool that provides real-time status views of networked devices. These views deliver a continuously updated physical picture of device configuration and performance conditions. The user can configure parameters for devices, cards, and interfaces. Additionally, the user can also monitor real-time statistics for interfaces, resource utilization, and device performance.

CiscoView is a CiscoWorks application that relies on the CiscoWorks Common Services (CCS). CCS provides the required background processes and database for all CiscoWorks applications. All the MIB definitions and physical layout descriptions are defined in a "*device package*". Each Cisco device type has a device package that can be installed on the CiscoWorks server. CiscoWorks applications like CiscoView and Resource Manager Essentials use the device packages to understand the MIB definitions and other features for each device type.

A user can access the CiscoWorks applications using a supported web browser. The communication between the client (web browser) and the CiscoWorks server can be secured by enabling SSL (Secure Socket Layer) on the server. The communication between the CiscoView application and a Cisco device is via SNMP v2 or v3. Knowledge of "*device credentials*" provides access to protected information on a device. CiscoView's knowledge of a device's SNMP community strings allows access to the device MIB. Additional security features, such as encryption and access control policies, are available by implementing the latest version of SNMP, v3.

Now, let's look closer at each of these areas.

# CiscoWorks User Roles








## CiscoWorks User Roles

Since CiscoView can be used to view and modify the configuration of a device, CiscoWorks has various user roles that can be assigned to users to limit access to this information.

CiscoView is subjected to the same user privilege security as all other CiscoWorks applications; only allowing users with certain user roles (System Administrator, Network Administrator, Network Operator, Approver, and Help Desk) assigned to perform certain tasks.

When new users are created within CiscoWorks, the system administrator assigns one or more user roles to the new user. Based on these roles, the user will be only allowed specific tasks within CiscoWorks.

To view which roles are allowed to perform which CiscoWorks tasks, generate a Permission Report from the *Common Services>Server>Reports* menu.

The permissions per user role can be tailored if the CiscoWorks AAA mode has been set to log in users using a Cisco ACS (Access Control Server). Thus, in ACS, the system administrator can create new roles or modify existing roles.

Even with the user-role based security, care should be taken on who is given access to which device, in order to control who is able to view and configure which devices.

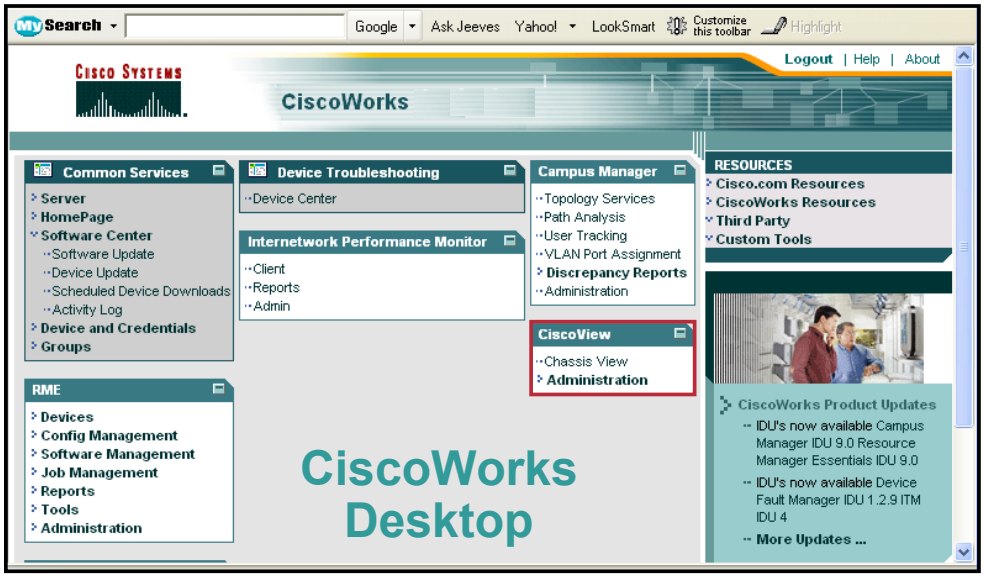
*Note(s):*

- *Refer to the Common Services Users Guide for information on "Logging in Using the ACS Login Module"*

# Accessing CiscoView

Cisco.com

**http://<CiscoWorksServer>:<port>**








## Accessing CiscoView

Access to the CiscoWorks desktop can be achieved from anywhere on the network as long as the client is capable of reaching the CiscoWorks server via HTTP (Hypertext Transfer Protocol). The client accesses the CiscoWorks desktop and its registered applications using one of the web-browsers supported by CiscoWorks, such as Netscape or Microsoft's Internet Explorer. For the desktop to properly display, the user must ensure that the browser has been properly configured.

During installation, the administrator can choose to set the HTTP port to be used for CiscoWorks access or can accept the default port – TCP 1741. If the default port is used, the user would then simply enter the following URL to access the CiscoWorks desktop

```
http://<server IP address or hostname>:1741
```

Optionally, the CiscoWorks desktop can be accessed securely using HTTPS (Hypertext Transfer Protocol Secure). Secure access *does* require additional setup steps by the system administrator.

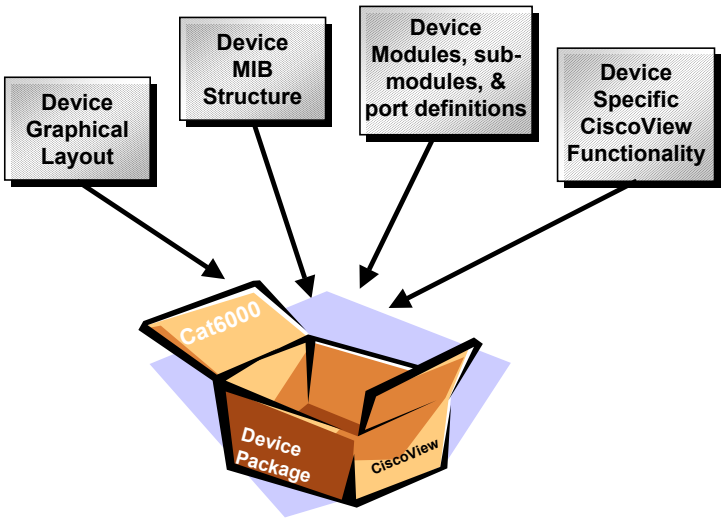
Once the user has accessed the CiscoWorks server, they are prompted to log in. The login ID is authenticated and the user can then view and access all registered CiscoWorks applications. The CiscoView launch point is illustrated above.

*Notes:*

- *A list of supported web browsers can be found Chapter 4 of this tutorial or the CiscoWorks Users Guide.*
- *Refer to the Common Services Users Guide for information on creating CiscoWorks users and enabling SSL.*
- *Various methods for authenticating users are available. Refer to the Common Services Users Guide for information*

# What are Device Packages?

Cisco.com




- **A Device Package is a software update for CiscoView**
- **Device Packages exist for each Cisco device type supported by CiscoView**
- **Device Packages provide CiscoView with information about the MIBs supported by the device and how to display the device**





## What are Device Packages?

CiscoView uses device packages to understand the physical layout of a device and the MIB data structure. CiscoView provides support for a considerable range of devices by installing a device package for each device type. A CiscoView device package is a software update for CiscoView that enables it to support new features for a particular device. CiscoView uses the device package to display a dynamic chassis view of the physical device and all its modules, sub-modules, and ports.

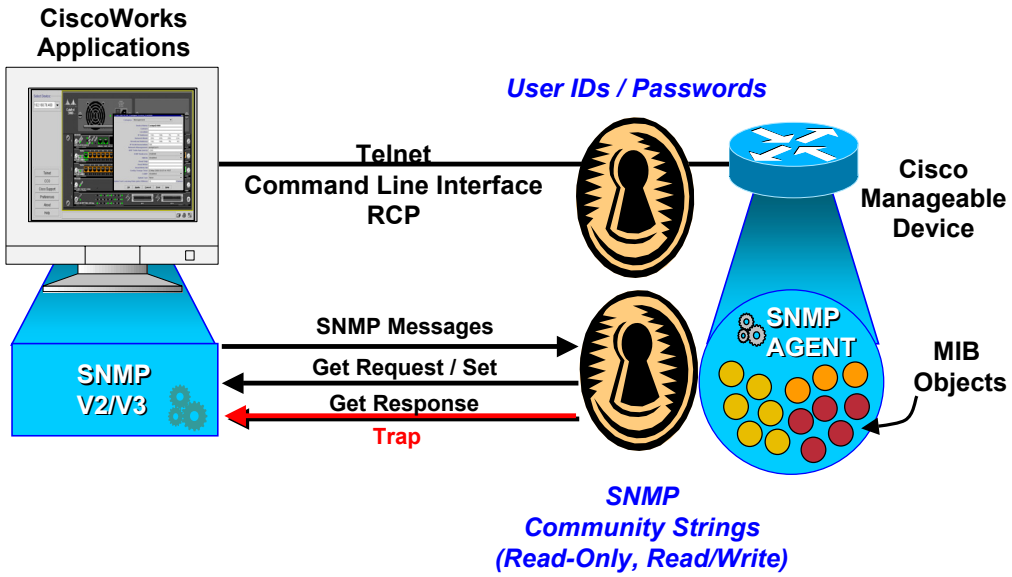
Because new devices are continuously being introduced, and capabilities of current devices are frequently enhanced, the device packages should be kept up-to-date to ensure that CiscoView is correctly displaying everything possible.

Remember, CiscoView can only be used to configure a device if the device's MIB structure supports it and SNMP is enabled for managing the MIB. New versions of the OS for devices are adding more and more configuration support via the MIB all the time. Therefore, it is critical to update the device packages on a regular basis.

The next section of this chapter will describe how to retrieve and install new Cisco Device Packages as they become available.

# What are Device Credentials?

Cisco.com








## What are Device Credentials?

Device credentials are the keys to getting started using CiscoView. They are values used to access a managed device such as a switch or router. For CiscoView, the device credentials are the IP addresses and their associated SNMP community strings for that managed device. Other applications may require the Telnet or enable password for the device in order to manage it.

The CiscoWorks device credentials are stored in a common location on the CiscoWorks server – the Device and Credential Repository (DCR). The DCR is a common repository of devices, their attributes, and the credentials required to manage devices in a common management domain. Individual CiscoWorks applications interact with the repository to get the device list, device attributes and device credentials. Applications can read or retrieve the information as well as update the information in the DCR so that it can be shared with other applications.

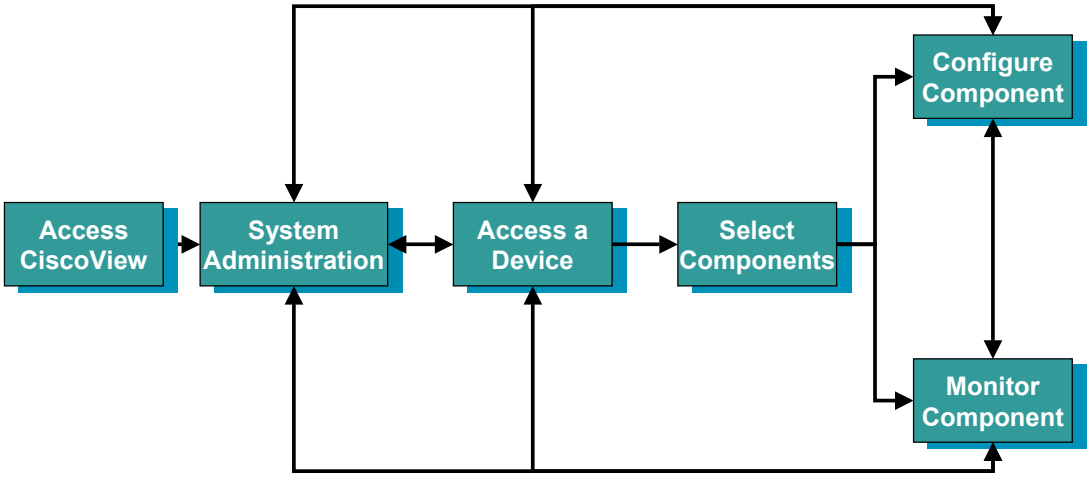
The next section of this chapter will describe how to manage the device credentials for use with CiscoView.

# Getting Ready to Use CiscoView

- How CiscoView Works
- ➢ **Getting Ready to Use CiscoView**
- Managing Cisco Devices Using CiscoView

# Getting Started Tasks

Cisco.com








## Getting Started Tasks

Now that you understand what CiscoView needs to run properly (i.e. device credentials, device packages, and CCS) and we know how to access the CiscoWorks desktop and CiscoView, let's get started!

As with most applications, they should be set-up and configured appropriately before using. With CiscoView, the initial configuration is minimal. Most device packages are installed when the application is installed. The device packages may need to be updated depending upon when the product was released. Optionally, all the devices to be managed and their credentials should be defined in DCR so that they can easily be managed in the future. However, not having the information in the DCR does not prevent the user from using CiscoView; they would simply need to manually enter the information in the CiscoView main window. And finally, and also optionally, the CiscoView preferences can be adjusted.

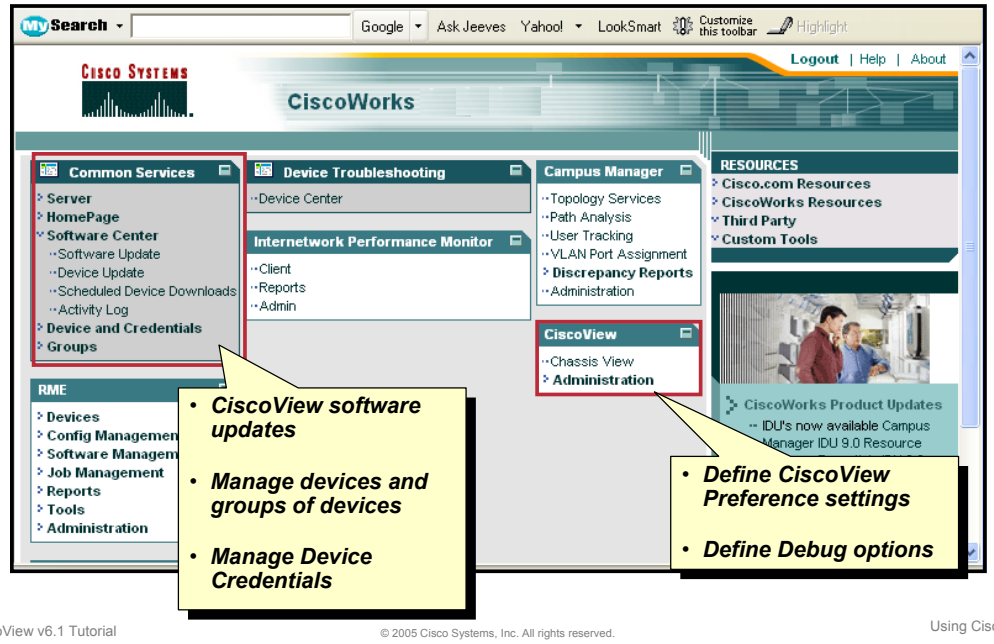
Now once the user has selected a device in the DCR or manually enter the device address/hostname and associated credentials, the user can access and view the physical layout of the device. When the device chassis is displayed, the user can select the component(s) on the device to be configured or monitored.

We will now use this workflow as the agenda for the remaining sections of this chapter.

# System Administration Tasks

Cisco.com

**http://<CiscoWorksServer>:1741**








## System Administration Tasks

A System Administration should login to the CiscoWorks server using the default CiscoWorks admin login ID or a user account that has System Administrator privileges. The System Administration tasks for CiscoView can be found on the CiscoWorks desktop. The System Administration tasks for CiscoView will be under the following two sections"

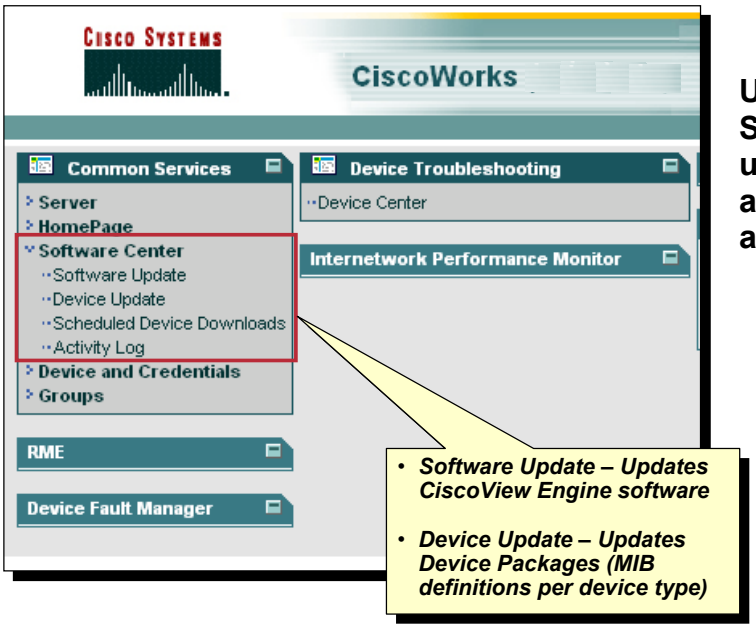
- ***Common Services*** – The system administrator can use the tasks in this section to update the CiscoView engine software, update or install new device packages, and manage/organize the devices and their credentials in the DCR.
- ***CiscoView>Administration*** **-** The system administrator can use the tasks in this section to adjust the CiscoView preferences (i.e. Polling frequency, SNMP timeouts, retries, etc.) and debug options.

*Notes:*

- *A list of supported web browsers can be found Chapter 4 of this tutorial or the CiscoWorks Users Guide.*
- *Refer to the Common Services Users Guide for information on creating CiscoWorks users with System Administrator privileges (CiscoWorks User Roles).*

# Managing CiscoView Software Updates

Cisco.com




**Use the CiscoWorks Software Center to update the CiscoView application software and Device Packages**

- **View installed software**
- **Check for software updates on Cisco.com or on the server's file system**
- **Install new updates**





## Managing CiscoView Software Updates

There are two types of software updates for CiscoView:

1. Update the CiscoView engine software. This software contains updates or bug fixes to the CiscoView software itself.
2. Update the device definitions (CiscoView Device Packages or CiscoWorks IDUs (Incremental Device Updates). This software update contains the information on how to manage different device types. Also, if a new software image or module has been released for a device, the device package may get updated to contain the new features. CiscoView would need the new device package to manage the new features.

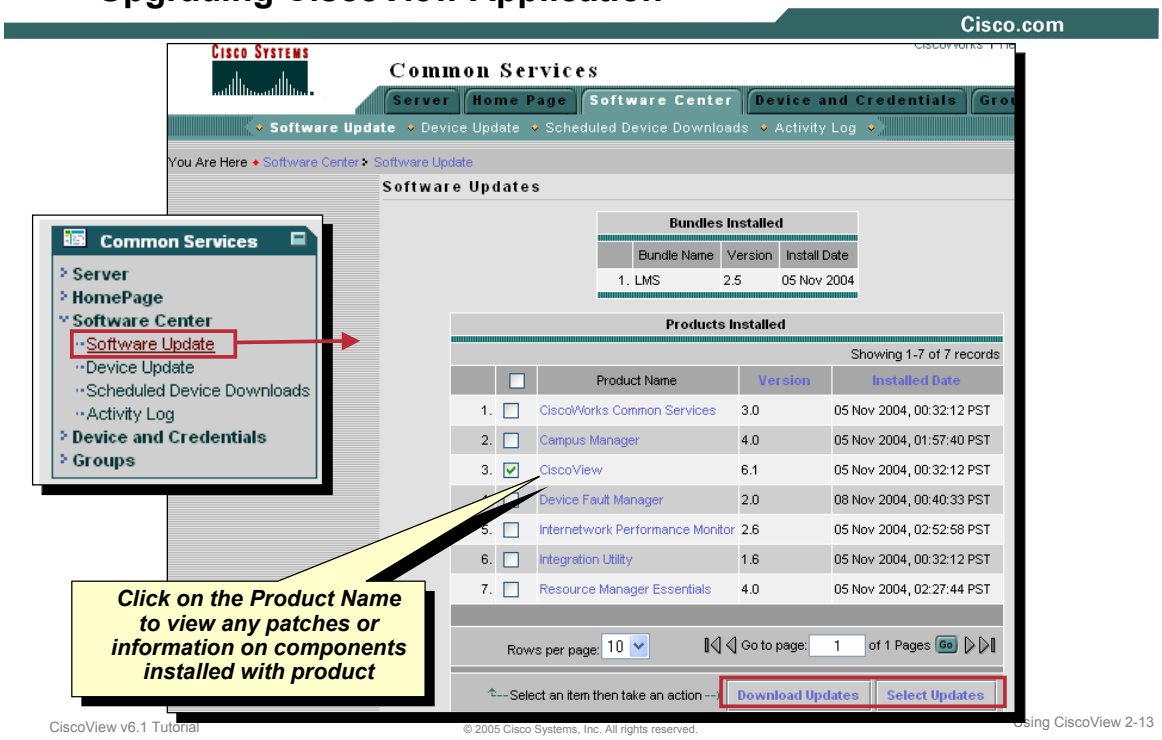
Software Center is a component of CiscoWorks Common Services and is used to manage these types of software updates. The Software Center allows the user to check for software and device support updates, download them to the server along with the related dependent packages, and install the updates. The Software Center looks for software updates from Cisco.com, and downloads them to a server location, from where you can install the updates.

Note(s):

- *A user can go to the **Software Center>Activity Log** to view Events (updates, downloads, o r scheduled jobs) that have occurred using the Software Center.*
- *An IDU is a software package that enables CiscoWorks to support new devices. An IDU might also contain patches. CiscoWorks IDUs are released cumulatively; that is, new IDUs include the contents of any previous IDUs.*
- *You can download IDUs and their Readme files as they become available by logging into Cisco.com at: http://www.cisco.com/en/US/partner/products/sw/cscowork/ps4565/prod_upgrades_and_downloads.html*

# Managing CiscoView Software Updates

## Upgrading CiscoView Application




## Upgrading CiscoView

Let's first look at how you would update the CiscoView engine software. Select ***Software Center>Software Update*** from Common Services. This features allows you to check for new releases, download, and install updates for all CiscoWorks applications installed on the server.

As illustrated, you can view a list of all CiscoWorks related bundles and products already installed on the server, along with their respective versions and the dates on which the software was installed. To sort the table by version or date of installation, click on the *Version / Installed Date* column heading.

In the *Products Installed* table, you can click on each product to view a table that lists any patches or sub-applications installed with the selected application, along with their respective versions and the dates on which the software was installed.

To download software updates from Cisco.com, if any exist, first check the box next to the product name, then select ***Download Updates***.

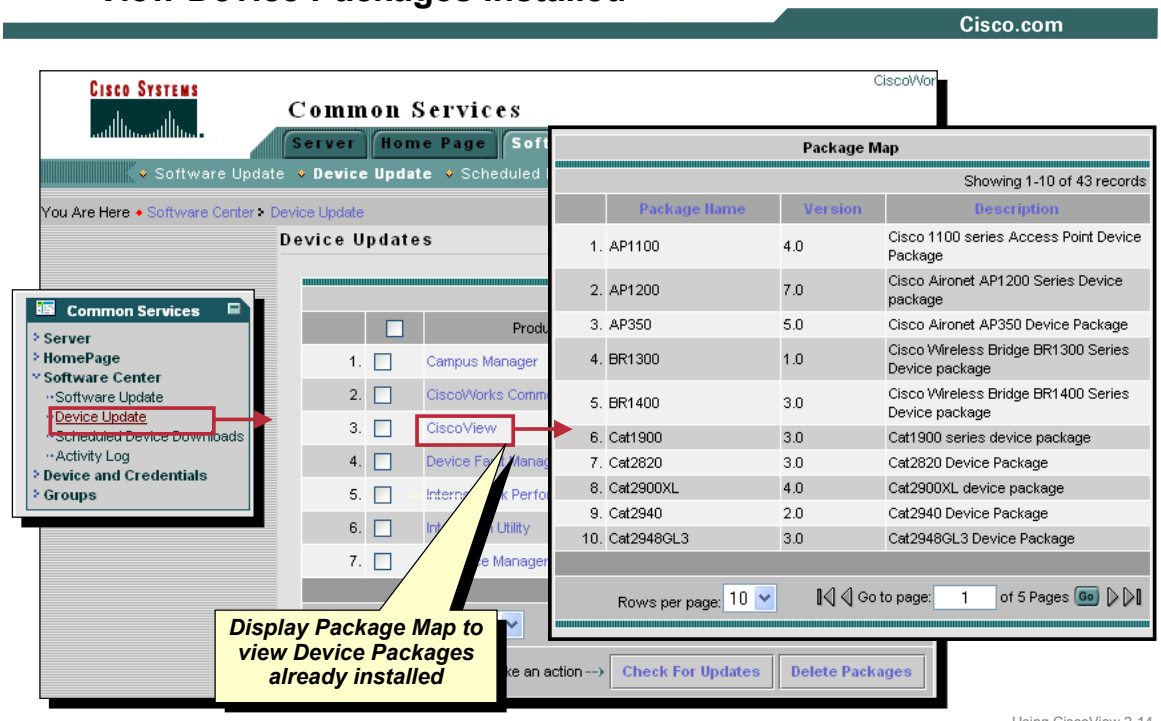
Or, to select specific software updates from a list prior to downloading, first check the box next to the product name, then select ***Select Updates***.

Note(s):

- *The software update feature looks to Cisco.com as the default site for updates.*

# Managing CiscoView Software Updates

## View Device Packages Installed




## View Device Packages Installed

Now, let's look at how to manage the second type of software updates for CiscoView, the Device Packages.

Device Packages can be added to CiscoWorks anytime after the initial product release or installation. When new device packages become available, they are placed on Cisco.com. The Software Center can be used to manage the Device Packages. Use the Software Center, ***Software Center>Device Update*** from Common Services to perform the following tasks:

- Check for which Device Packages are already installed (illustrated above)
- Check if new updates are available on Cisco.com; if so, install them or download them to your server's file system
- Install the Device Packages from your server's file system

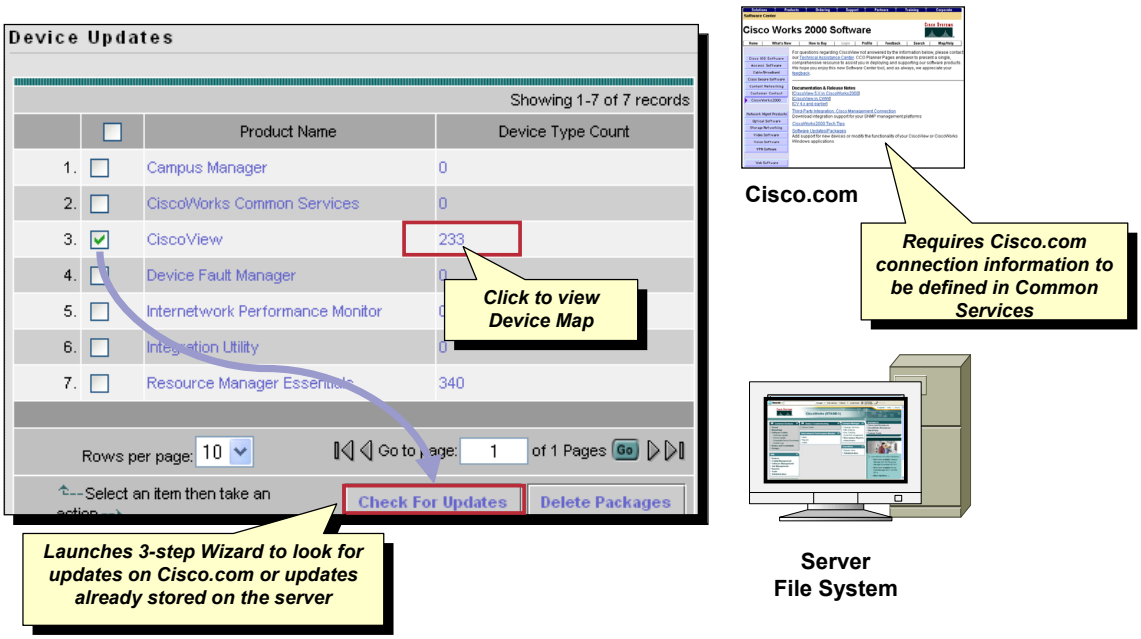
Note(s):

- *Software Center maintains two types of mappings in the installed packages directory of the respective applications :*
    - *The **Package Map** s a list of all device packages installed on the server. For example, the package name AP350 represents Cisco Aironet 350 Device Package. (Illustrated above.)*
    - *The **Device Map** is a list of all the different types of device types supported by the selected application and which Device Package supports it. To view, click the device type count link next to the product name. (Illustrated on next page.)*
- *Most of the device family based packages can be installed directly from the web interface. The device support packages such as IDU have to be installed based on the installation instructions documented in the respective readme files.*
- *The Software Center can also be used to uninstall a device support package.*
- *Make sure to review the CiscoView release notes for each device package because they supply critical information, notes, and cautions about usage.*

# Managing CiscoView Software Updates

## Manually Check for Device Package Updates

Cisco.com








## Manually Check for Device Updates

To manually check if updated device definitions are available, use the Software Center again.

Select ***Software Center>Device Update*** from Common Services; check the CiscoView application; and click **Check for Updates**. This will launch a 3-step wizard to help you update the device definitions for the selected application. The 3 steps consists of:

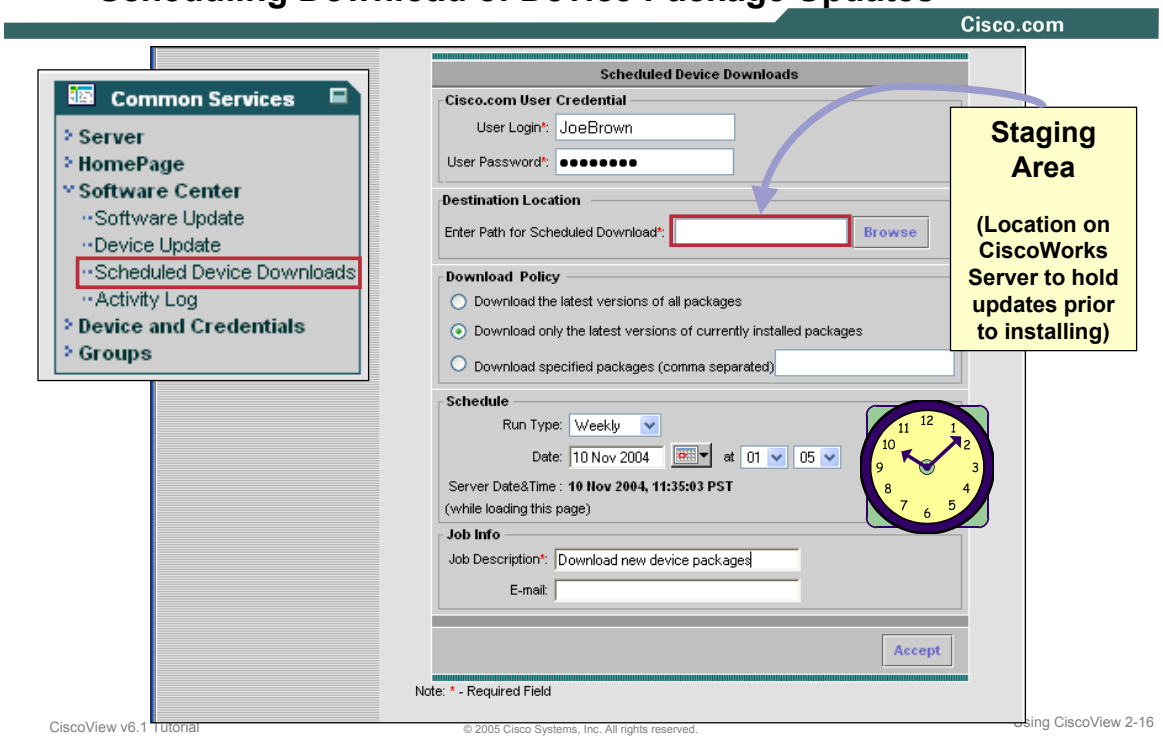
1. First, select source location for where you want to look for the device updates, either online at Cisco.com or updates that have already been downloaded and stored on your CiscoWorks server.
2. Next, select the updates (Device Packages) that are available. The list contains information on the package name, type of update (IDU or device package), version, readme details, size of update and more.
3. Finally, choose to install the updates or download the updates to the server to installation to the scheduled.

*Note(s):*

- *Access to information on Cisco.com requires the Cisco.com login information to be defined in the Common Services. To define the login information, select* ***Server>Security>Cisco.com Connection Management>Cisco.com User Account Setup*** *from the Common Services area.*

# Managing CiscoView Software Updates

## Scheduling Download of Device Package Updates




## Scheduling Download of Device Updates

On the previous page, you learned that the device updates can be stored on the CiscoWorks server and installed later on. To get the device updates stored on the server, you could have manually downloaded them from Cisco.com or, better yet, you could have CiscoWorks periodically retrieve them when they become available on Cisco.com.

To schedule device package downloads, select ***Software Center>Scheduled Device Downloads*** from Common Services to define a job to check for the latest device packages on Cisco.com. Simply specify the time and frequency (daily, weekly) of the downloads, the download location or "Staging area" on the server, Cisco.com user account login information, and the download policy. Software Center supports the following download policies:

- Download all latest device packages of products installed in the machine.
- Download newer versions of currently installed packages.
- Download the specified packages separated by commas.

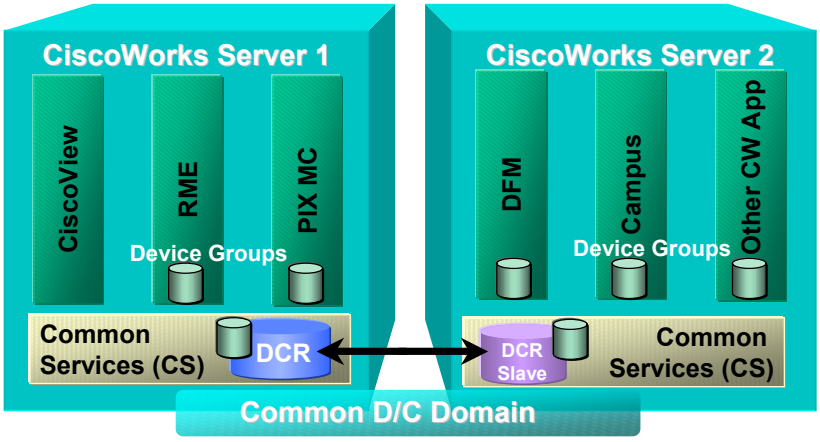
Note(s):

- *An e-mail message can be sent to the user once the job has been completed so that the user can check to see if there were new updates that have been download and now can be installed.*
- *Only one download can be scheduled at a time.*
- *A user can go to the* ***Software Center>Activity Log*** *to view scheduled jobs.*

# Managing Devices and Credentials

Cisco.com

- **CiscoView requires the Device IP Address/Name and SNMP credentials. This information can be manually entered or selected from the CiscoWorks DCR (Device & Credentials Repository).**
- **Other CiscoWorks applications have stored device information in the DCR and built Device Groups that can be shared between other CiscoWorks applications**








## Managing Devices and Credentials

As previously mentioned in the last section, the Device and Credential Repository (DCR) is a common repository of devices, their attributes, and the credentials required to manage devices in a management domain. CiscoView requires knowledge of the device's IP Address/Name and its SNMP credentials in order to manage the device. This information can be manually entered or ideally if another CiscoWorks application has already obtained this information it can store it in the CiscoWorks DCR. The CiscoView user can then browse the DCR to select and manage the device.

Individual CiscoWorks applications interact with the DCR to get a list of devices, their attributes and credentials. Applications can read or retrieve the information, organize the devices into Device Groups, as well as update the information in the DCR so that it can be shared with other applications. The CCS, RME, DFM, and Campus Manager applications automatically organize the devices into system-defined Device Groups that can be used by all other CiscoWorks applications. CiscoView does not automatically create new Device Groups, but a CiscoView user can use the Device Groups created by the other CiscoWorks applications or he/she can create user-defined Device Groups to better organize their devices.

Additionally, if CiscoWorks is deployed in a distributed environment on multiple servers, the DCRs can operate in a master/slave relationship and can be synchronized.

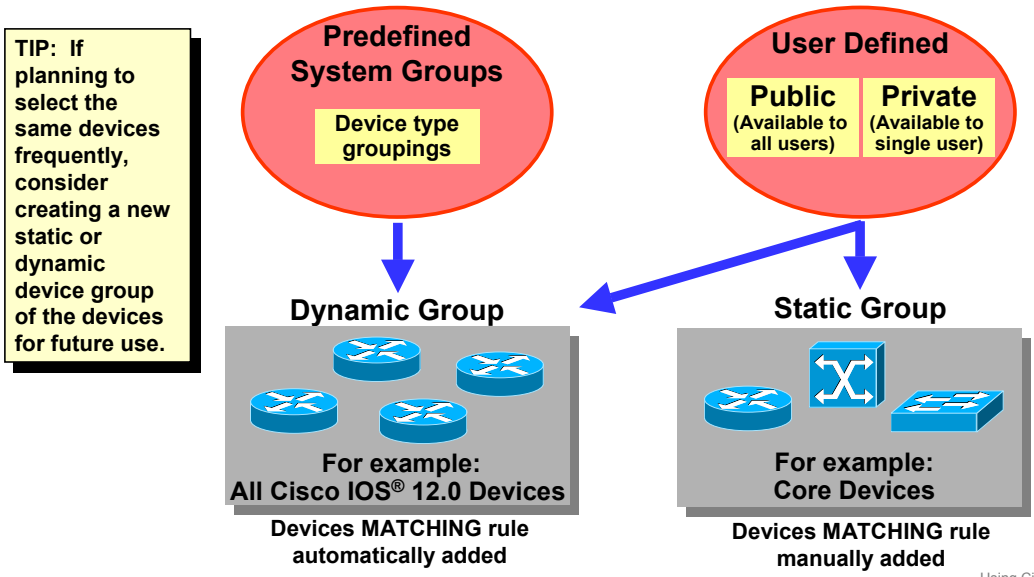
*Note(s):*

- *The DCR can be populated with devices in many ways including: discovery, import from third-party products like HP OpenView and Netview, or manual input.*
- *Management of the DCR and its contents is handled by the CCS and not the individual applications. Refer to the CiscoWorks Common Services Users Guide for information on populating the DCR, creating device groups, and synchronizing multiple CiscoWorks servers.*

# Managing Devices and Credentials
## Understanding Device Groups

Cisco.com

**Meaningful grouping of devices for task execution and reporting**




CiscoView v6.1 Tutorial © 2005 Cisco Systems, Inc. All rights reserved. Using CiscoView 2-18

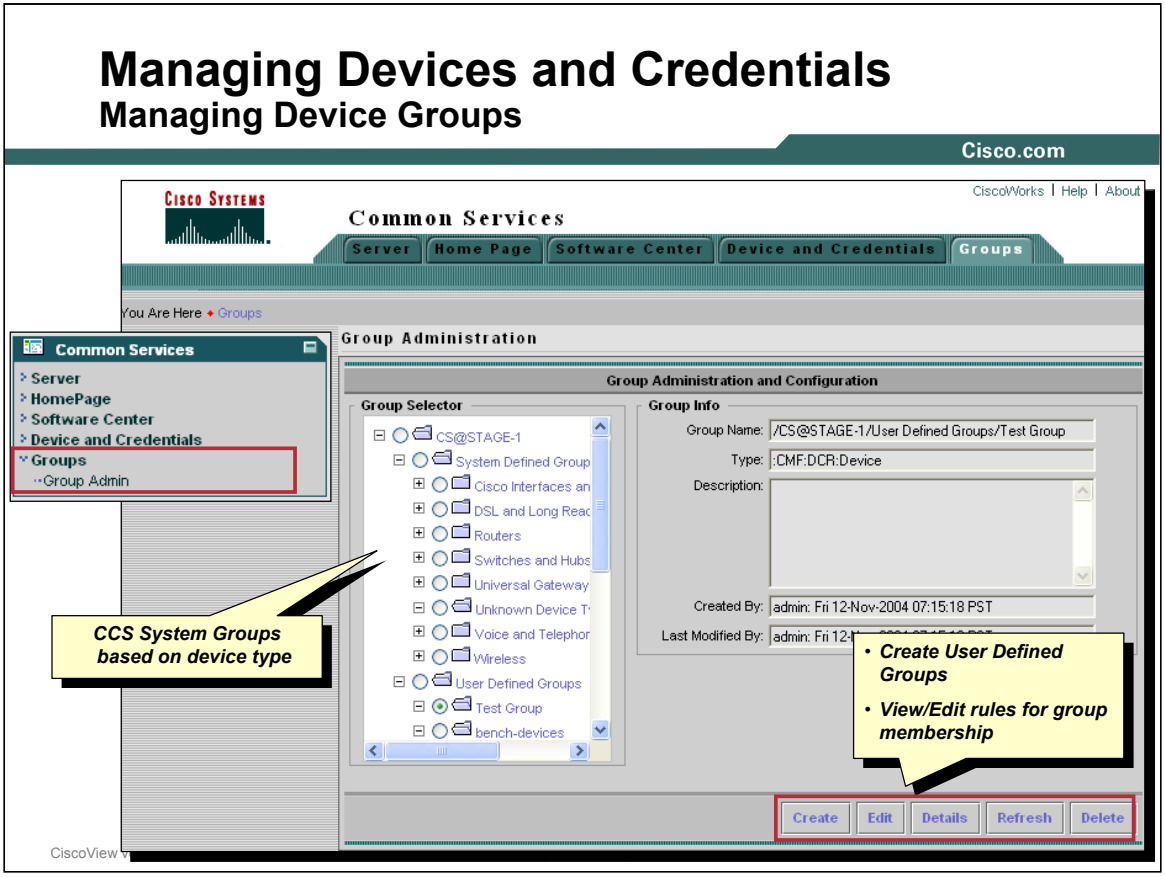
## Understanding Device Groups

A Device Group is a named set of devices in CiscoWorks that helps a user organize the many devices in the DCR by some logical or physical attribute. The group is characterized by a set of properties such as a name, description, type, access permission, etc., but, most important, an associated rule. The rule determines the membership of a group, which can change when the rule is evaluated. Groups are hierarchical and can be Dynamic or Static. They can also be Public or Private.

- Dynamic Groups – The members in a dynamic group are determined each time you view its members. Based on the group's rule, the members of the group may change. For example, if the rule is based on IOS software version, the members of the group may change as devices are upgraded to new software versions.
- Static Groups - The members in a static group are refreshed only when you explicitly request it.
- System Groups - When you add a device to DCR, the device is either added to an existing system group with the corresponding device type/attribute or if such a group does not exist, a new system is automatically created based on the device type.
- User-defined Groups - You can create groups here based on device attributes in the DCR.

# Managing Devices and Credentials

## Managing Device Groups




## Managing Device Groups

The **Groups** feature in CiscoWorks Common Services (CCS) allows you to group devices and manage device groups.

Device groups created using the Groups feature in CCS, can be used across all CiscoWorks applications. A nice feature is that CCS, Campus, RME, and DFM applications will automatically create System-Defined groups. For example:

- CCS creates System Groups based on device types (I.e. Routers, Switches, etc. ) and sub-system groups based on the type of router, switch, etc.
- Campus Manager creates System Groups based on Subnets or unreachable devices.
- Resource Manager Essentials creates System Groups based the management status of the device

CiscoView does not create new device groups, but you can use all the system-defined groups from all the other CiscoWorks applications! So, when you need to select a device for CiscoView to monitor or configure, you can use the groups automatically created by CCS or the other CiscoWorks applications to help locate and select the device.

And for flexibility, the Groups feature in CCS allows a user to create user-defined groups based on simple or complex rules that match or filter on the device attributes in the DCR.

*Note(s):*

- *Management of Device Groups and their memberships is handled by the CCS and not the individual applications. Refer to the Common Services Users Guide for information on creating and managing device groups.*

# Managing Cisco Devices Using CiscoView

- How CiscoView Works
- Getting Ready to Use CiscoView
- ➢ **Managing Cisco Devices Using CiscoView**

# Using CiscoView for Device Configuration

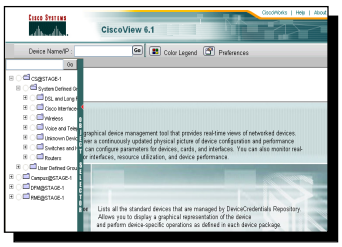
Cisco.com

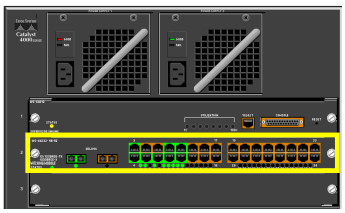
Access Device → Select Device Component → View/Modify Configuration Parameters

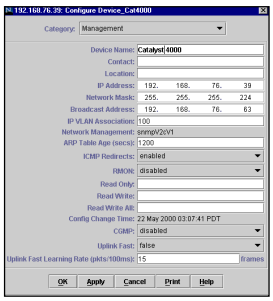
- **Choose device from device list in DCR**
- **Or manually enter device address and community strings**

- **Chassis**
- **Module / Sub-Module**
- **Port / Interface**

- **Right mouse click component to see configuration options**
- **Change Categories to view different configuration parameters**
- **Make changes and apply**







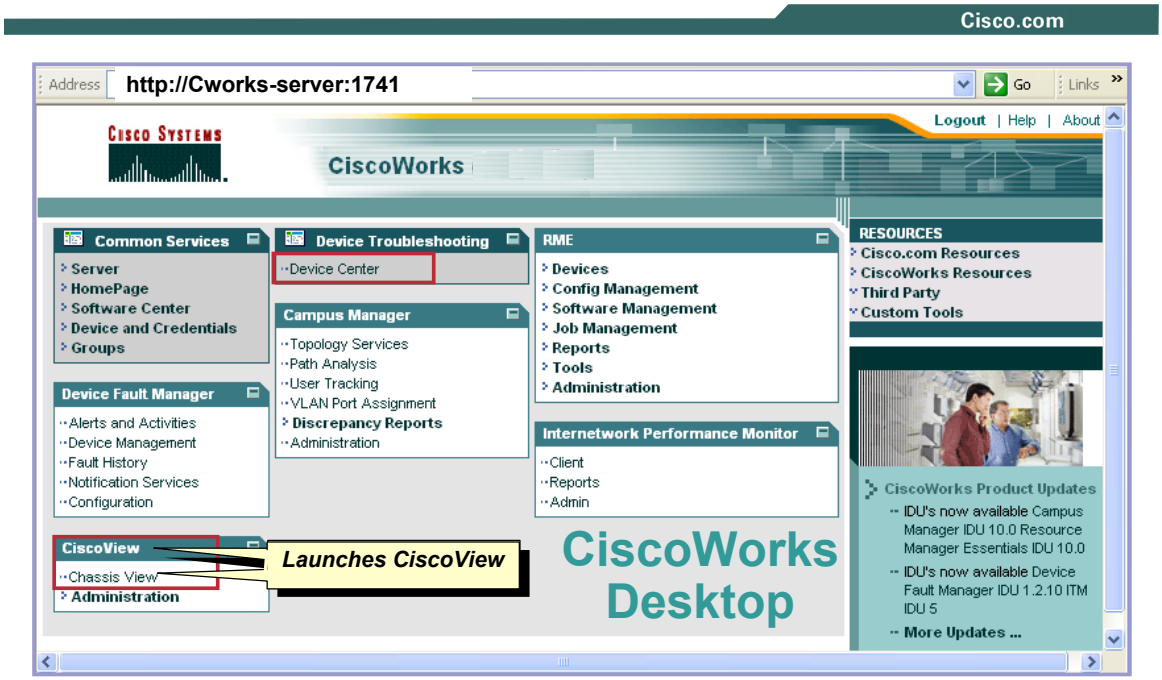



## Using CiscoView for Device Configuration

The upcoming pages will describe how to access a Cisco device using CiscoView, how to select a device component (such as an interface or chassis for global features) to configure, and then how to view or modify the device components parameters through a series of context menus using SNMP.

Since CiscoView is a CiscoWorks application, the device information can be shared for easy access. And using graphical tools to view device status and configure features, makes everything more intuitive.

# Access CiscoView








## Access CiscoView

Let's now begin to use CiscoView for monitoring or configuring a Cisco device!

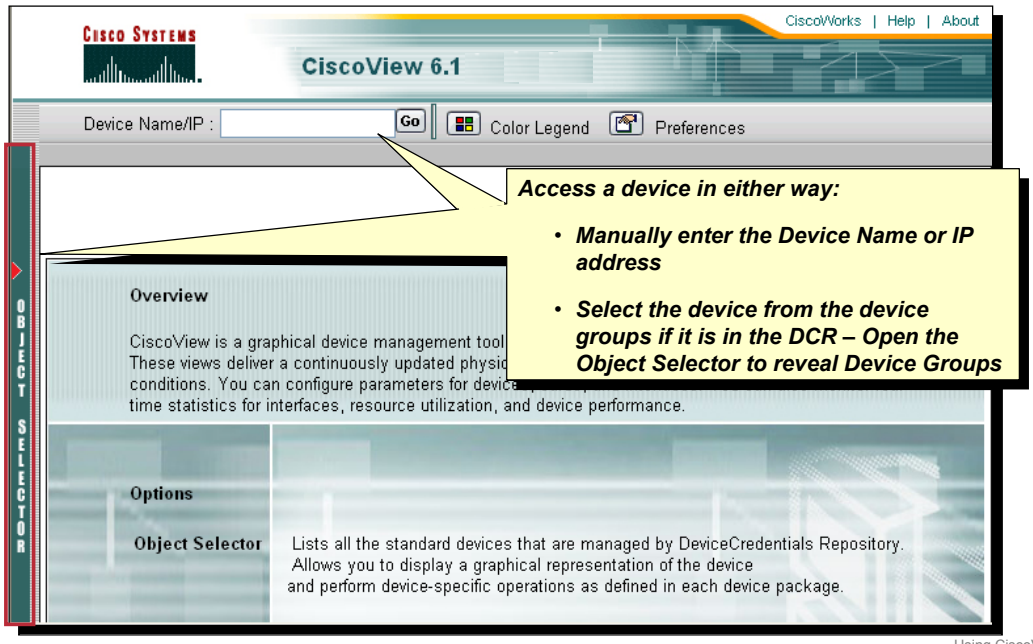
First, access the CiscoWorks desktop and login. As illustrated, the CiscoView application can be launched from the CiscoWorks desktop. Click on either the **CiscoView** application name in the title bar or **Chassis View** to launch CiscoView.

*Note(s):*

- *Management of CiscoWorks user accounts is handled by the CCS and not the individual applications. Refer to the Common Services Users Guide for information on creating and managing CiscoWorks user accounts.*
- *If other CiscoWorks applications are installed, CiscoView may also be launched from these applications (I.e. Campus Manager's Topology Services)*
- *Additionally, CiscoView can be integrated into the menus of other network management applications, such as HP OpenView, using the Integration Utility.*

# Access a Device Using CiscoView

Cisco.com





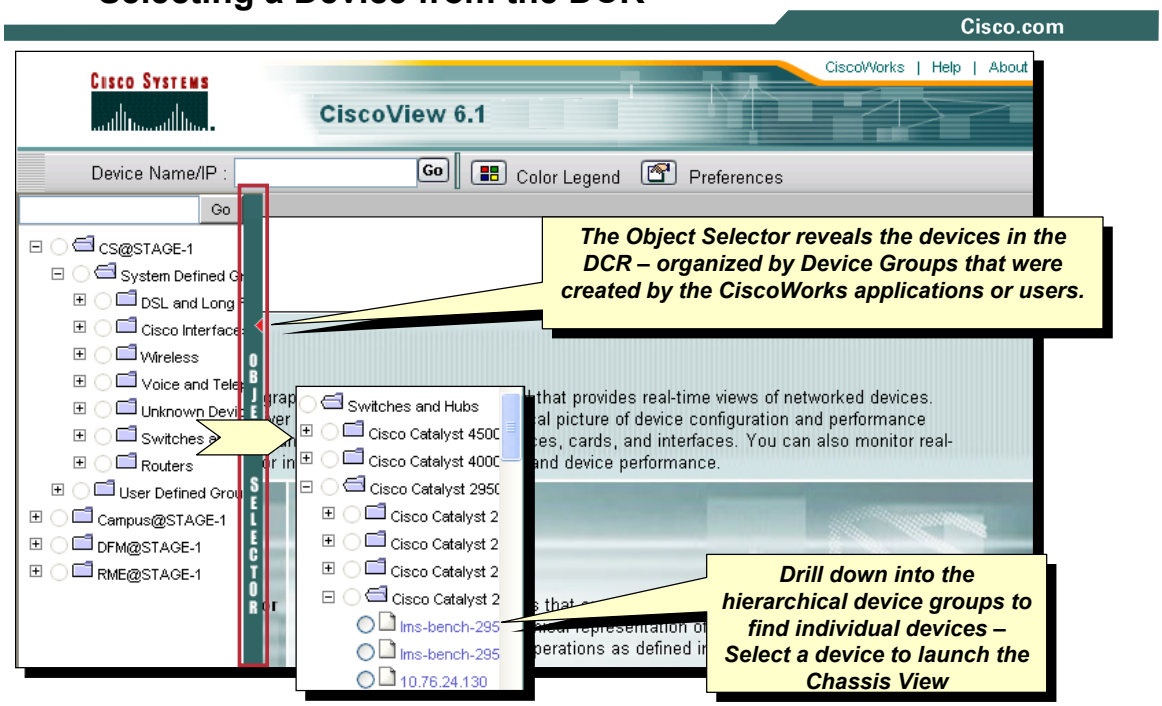



## Access a Device Using CiscoView

Once you select CiscoView (or Chassis View) from the CiscoWorks desktop, the CiscoView home page will be display, as illustrated above. From this window you can access a device by either manually entering the device name (or IP address of the device) or by selecting the device from the device groups already defined in the DCR. To view the device groups, click anywhere on the vertical OBJECT SELECTOR title bar.

# Access a Device Using CiscoView

## Selecting a Device from the DCR




## Selecting a Device from the DCR

When you open the OBJECT SELECTOR to display the devices already in the DCR, you will see a hierarchy of organized device groups. Simply click on the "+" sign to open the hierarchy of device groups.

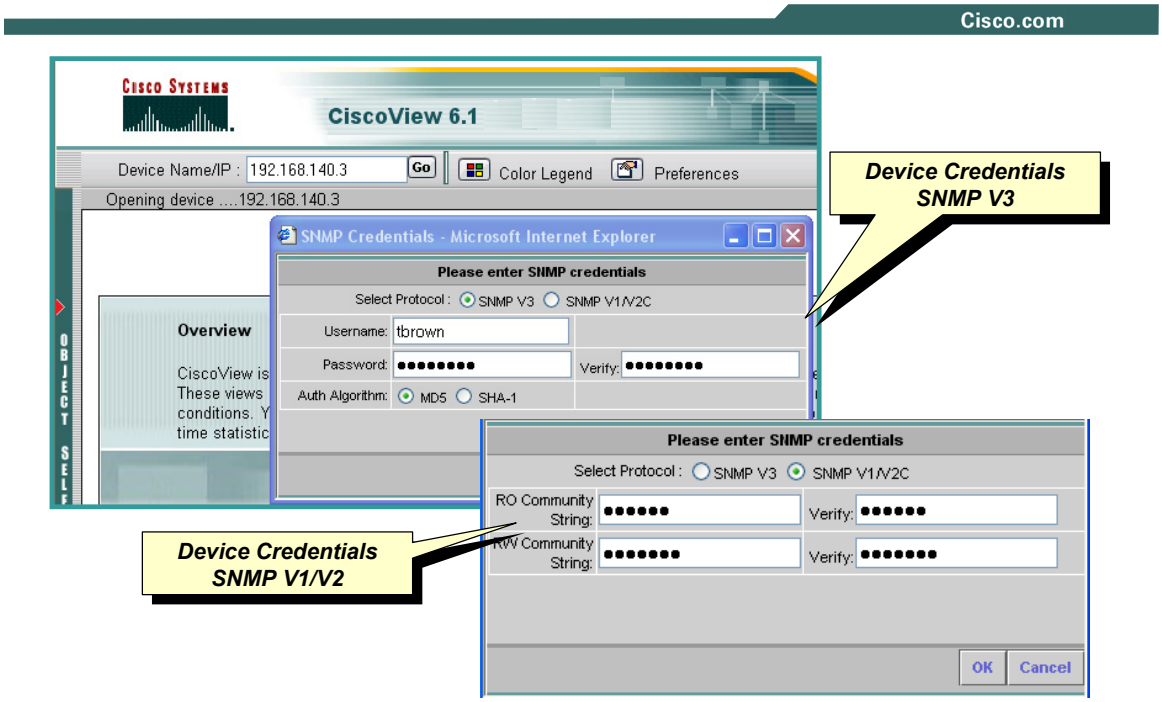
At the first level are the various CiscoWorks applications or services (i.e. CCS, Campus Manager, Device Fault Manager (DFM), and Resource Manager Essentials (RME)) that automatically create system-defined device groups.

At the second level, the device groups are organized by either System-Defined groups or User-Defined groups. The types of system-defined groups vary per application. For example, the CS system-defined groups are based on device types and model numbers; the Campus Manager system-defined groups are based on subnets; and the RME system-defined groups are based on all devices, normal devices, or devices that have been previously selected or managed with RME.

Continue to open the sub-levels to locate your individual device that you would like access using CiscoView. Then select the device to open the Chassis View of the device. CiscoView will attempt to access the device using the device credentials store in the DCR or manually entered.

# Access a Device Using CiscoView

## Credentials Verified








## Credentials Verified

If you enter the IP address or name of a device which has credentials configured in the CiscoWorks DCR, CiscoView displays the chassis view for that device without prompting you to enter its SNMP credentials. However, if the credentials are not in the DCR, or you simply entered the IP address or name of a device in the Device Name/IP field, then the SNMP Credentials dialog box appears and you must enter the SNMP version and credentials manually.

In the Select Protocol field, select either the SNMP V3 or SNMP V1/V2C radio button, depending on the type of credentials you want to use for the device. If you selected the SNMP V3 radio button, do the following:

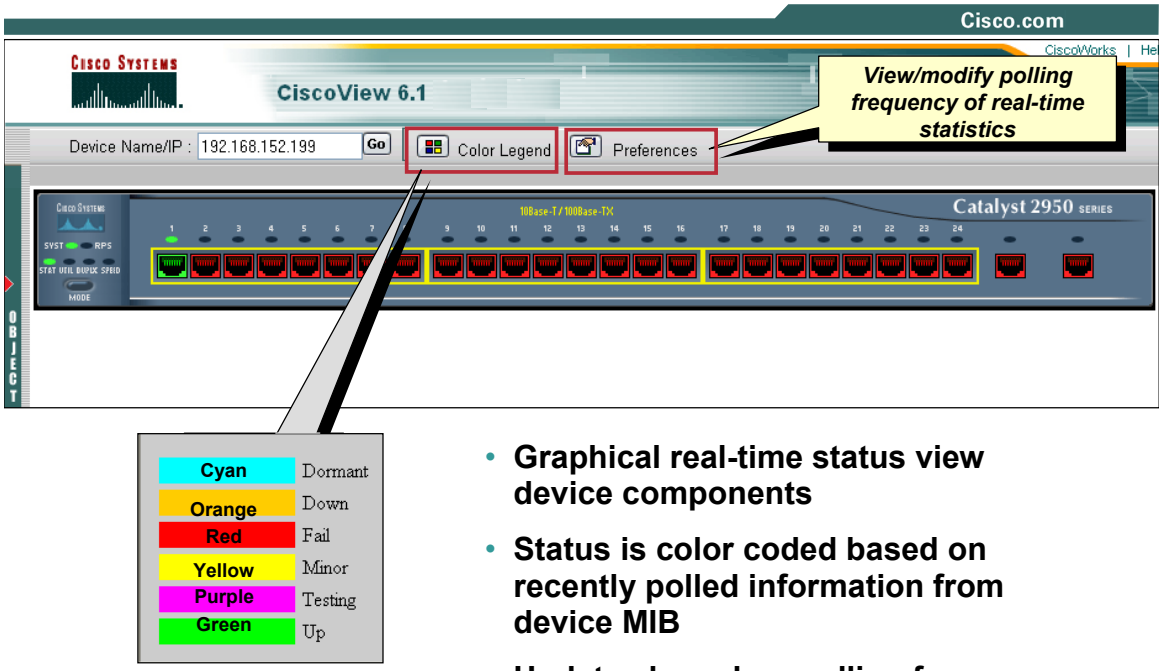
1. Enter the appropriate username and password.
2. Specify the authentication algorithm you want to use by selecting either the MD5 or SHA-1 radio button.

If you selected the SNMP V1/V2C radio button, enter the appropriate read-only and read-write community strings.

If the credentials are correct and the device is SNMP reachable, the device is displayed in the CiscoView Chassis View (as illustrated next). If the credentials are incorrect or the device can not be reached using SNMP, an error message is displayed.

# Access a Device Using CiscoView

## Chassis View – Real-Time Status




- **Graphical real-time status view device components**
- **Status is color coded based on recently polled information from device MIB**
- **Updates based on polling frequency**





## Chassis View – Real-Time Status

If the device is accessible and the credentials are valid, the device will be displayed in the Chassis View. CiscoView uses the device package information to graphically display the device and access the MIB variables that contain the device configuration and real-time status.

A graphical representation of the device will be displayed as though the user was standing in front of the device. CiscoView polls the status indicators of the power supplies, modules, and interfaces and then displays, in color, the real-time status in the Chassis View. The Color Legend can be viewed by clicking on the **Color Legend** icon. The polling frequency of the real-time statistics is defined and can be modified by clicking on the **Preferences** icon. (Refer to Chapter 4 for more information on setting CiscoView Preferences.)

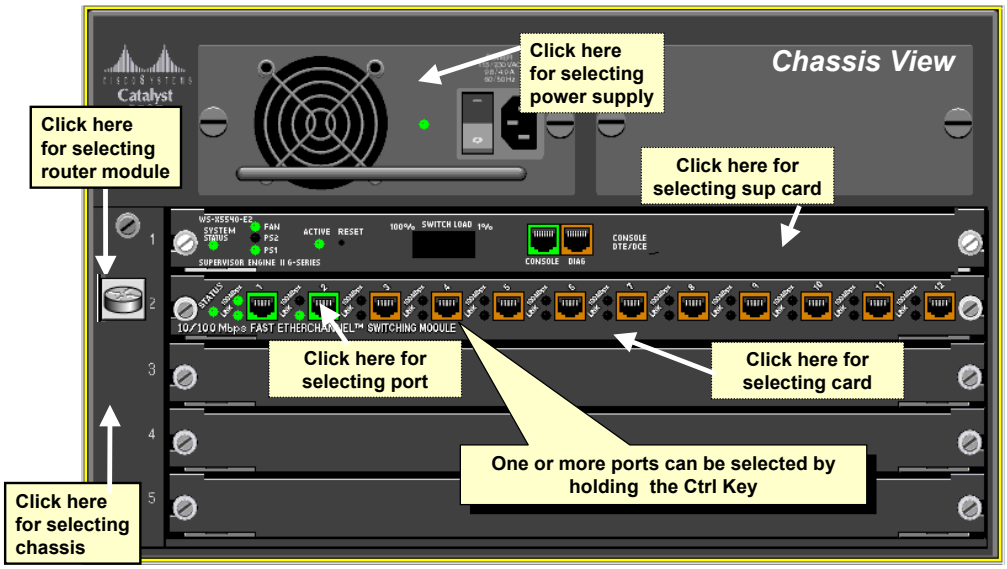
| | |
|---|---|
| Cyan (blue-green) | Port is dormant; Interface cannot pass packets, but is in a pending state, waiting for some external event to place it in the Up state. Interface could have packets to transmit before establishing a connection to a remote system or a remote system establishing a connection to the interface; for example, dialing up to a SLIP server. When the expected event occurs, the interface state changes to Up. |
| Orange/Light Brown | Port is down. Admin status is up and operational value is down. For Catalyst 4000, 5000, and 6000 devices, it can also indicate that the port is not connected. |
| Red | Port failed. Hardware failure in the port or the port is not connected. For Catalyst 4000, 5000, and 6000 devices, orange/light brown indicates that the port is not connected. |
| Yellow | Minor failure. Port or interface is down: both admin and operational status are down. This does not necessarily indicate a fault condition. Yellow can also indicate that the port is disabled. |
| Purple | Port is being tested. Admin status is up, but tests must be performed on the interface. After testing is completed, the interface state changes to Up, Dormant, or Down as appropriate. |
| Green | Port is active. Interface is able to send and receive packets. |

# Selecting Components

Cisco.com

**Click on component (Chassis, Module/Sub-module, Port)**

**Selected Component is Highlighted in Yellow**








## Selecting Components

When you select a device in CiscoView, a graphical representation of the device is displayed in the chassis view. Both device configuration and monitoring tasks are sensitive to the device component selected in the Chassis View. The user could select either the device chassis, a module, or one or more ports to monitor or configure. For example, if the user selected the chassis, then the parameters available for configuration or monitoring would be related to global device information.

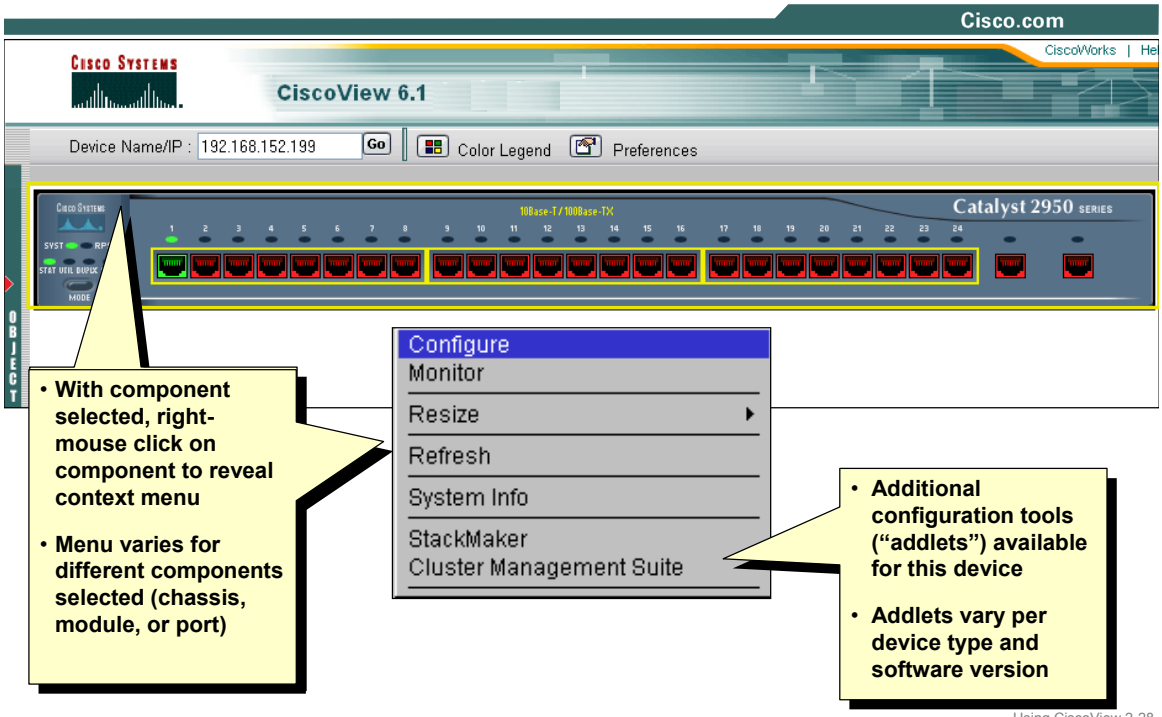
The picture above illustrates where the user should click to select the chassis, a module, or one or more ports. Once selected, the user can perform monitoring or view/modify configuration parameters.

The context menu, illustrated next, appears when you right-click a device or its components when it's selected. Its contents are context-sensitive and vary according to the device and your selection.

*Note(s):*

- *To select more than one port, hold the Ctrl key down while selecting the additional ports. Also, keep holding the Ctrl key when bringing up the Context Menus (discussed next).*

# Selecting Components
## Context Menus




CiscoView v6.1 Tutorial © 2005 Cisco Systems, Inc. All rights reserved. Using CiscoView 2-28

## Context Menus

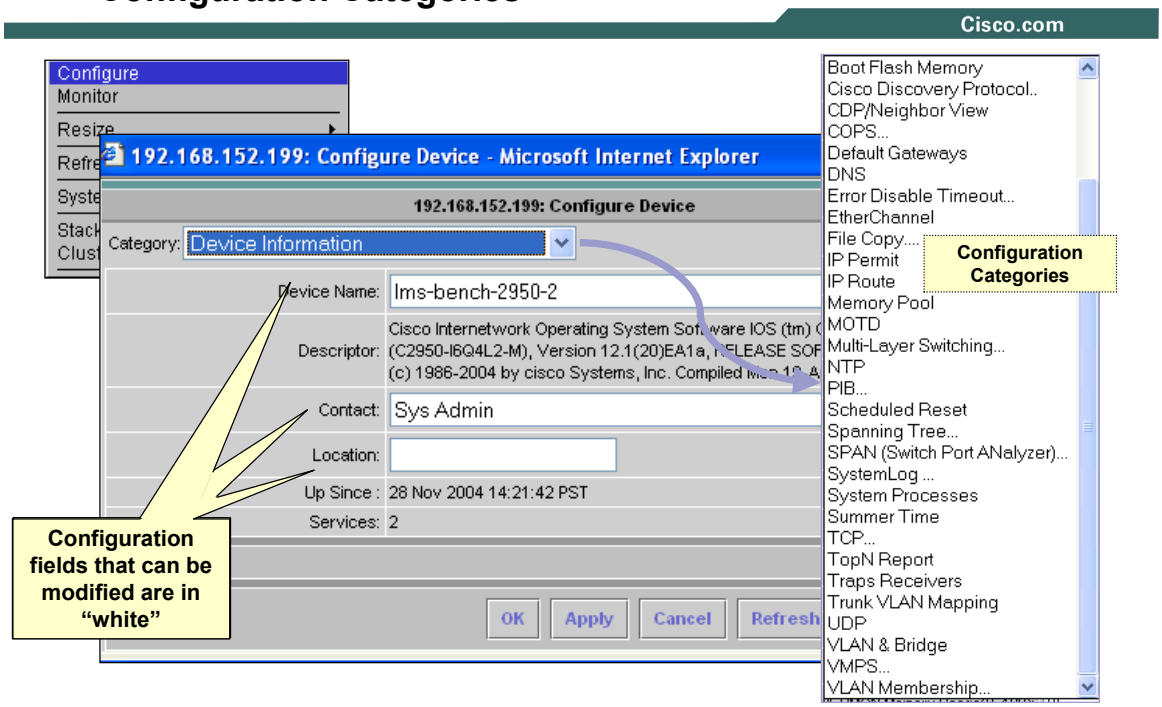
In the example above, the user clicked on the device chassis so that the global device configuration information could be viewed. To reveal the context menus for the selected component, right-mouse click on the selected area.

The context menu contents vary by device, but typically contains these options:

| Option | Description |
|---|---|
| Configure | Configures device categories, such as Management, Physical, ARP Table, TCP, and so on. |
| Monitor | Displays a set of dynamic charts for selected device categories. |
| Front or Rear | Displays either the front or back device panel. A logical view can also be displayed as defined by the device package. |
| Resize | Reduces the graphical display down to 75% or 50%. You can resize it back up to 100%. |
| Refresh | Triggers component polling and display update. |
| System Info | Displays system MIB information (name, description, location, contact, and up-time) for a displayed device. |
| Device-specific options | Options defined in the device package, such as "Clear All Counters." |

# Device Configuration Using CiscoView

## Configuration Categories




## Device Configuration Using CiscoView

Let's first look at configuring devices using CiscoView. After a component is selected, right-mouse click to reveal the context menu and then select *Configure*.

The Configuration Categories available are different for each device type and for each component (chassis, module, or port) selected on the device. In the example above, the device chassis was selected in order to configure global features. By default, the configuration category *Device Information* was displayed.

CiscoView can determine the different types of categories based on the Device Packages. (Another reason for having the latest Device Packages.)

The example above displays the Configuration Categories for a Catalyst device. All the configuration features that are configurable using SNMP and that CiscoView is aware of using the information in the Device Package is displayed.

Keep in mind that all features may not be configurable and some device types may not have any configuration categories. As new software images for the devices become available and Device Packages are updated, more features may become available for configuration using CiscoView.

# Using CiscoView for Device Monitoring

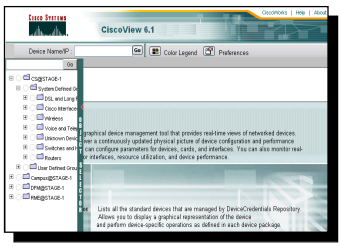
Cisco.com

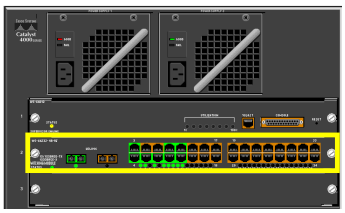
Access Device → Select Device Component → View Statistics

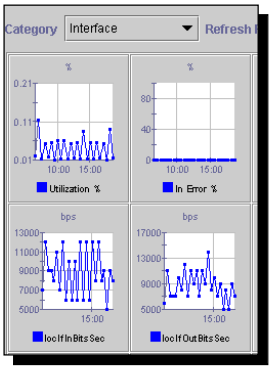
- **Choose device from device list in DCR**
- **Or manually enter device address and community strings**

- **Chassis**
- **Module / Sub-Module**
- **Port / Interface**

- **Right mouse click component and select Monitor**
- **Change Categories to different statistics**










## Using CiscoView for Device Monitoring

We will now switch gears and look at how CiscoView can be used for monitoring Cisco devices. To monitor a device, simply access a Cisco device and select a device component (such as an interface or chassis for CPU or memory statistics) the same way. And then view the device statistics through a series of context menus.

# Device Performance Monitoring Using CiscoView

Cisco.com

**Statistics collected for Cisco Catalyst OS devices include:**

- **Device Statistics**: Statistics include memory, CPU and process utilization statistics
- **Protocol Statistics**: IP, TCP, SNMP, ICMP, and Spanning Tree statistics
- **Interface Statistics:** Generic interface statistics as well as statistics specific to the interface type. This group includes such group statistics as bridge, interface, and Ethernet statistics.

**Statistics collected for Cisco IOS devices include:**

- **Device Statistics**: These statistics include memory, CPU and process usage statistics and more.
- **Layer 3 Interface Statistics**: These statistics include bandwidth utilization, errors, queue drops, collisions, internal interface resets and more.
- **Layer 2 Interface Statistics:** Serial interface include the number of checksum error packets, aborted packets, carrier signal transactions and overruns.

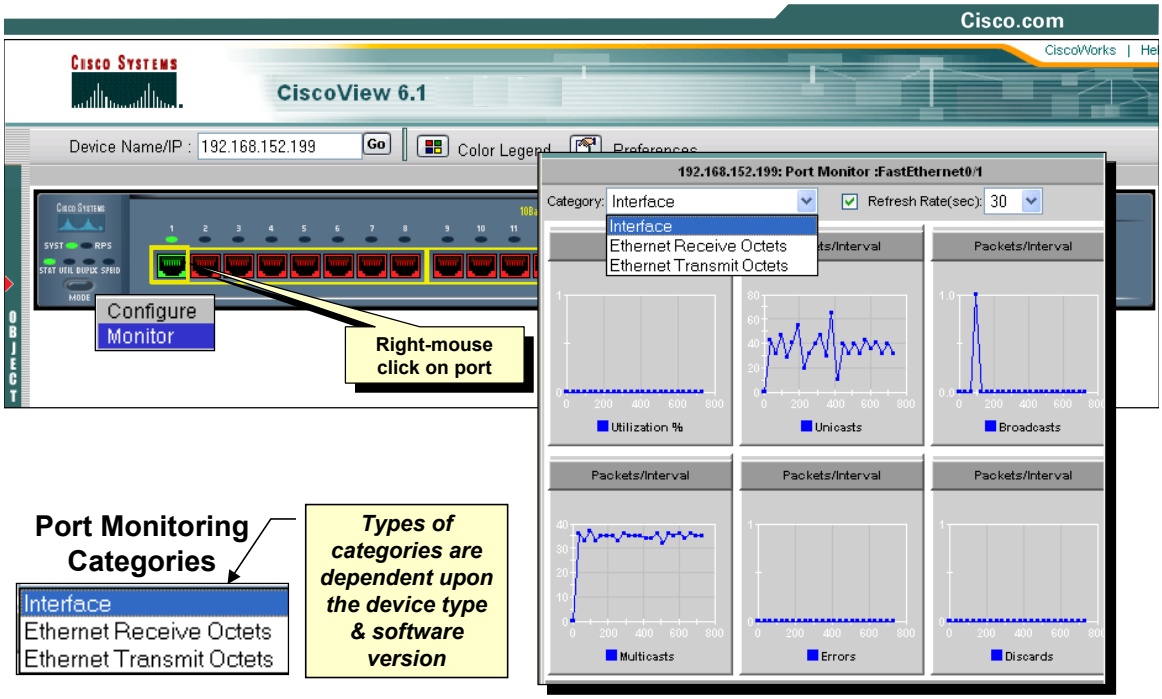




## Device Performance Monitoring Using CiscoView

The statistics collected by CiscoView are slightly different for different device types and software versions. CiscoView uses the device packages installed to determine the MIB variables available for monitoring. Generally, there are interface, protocol, and device (CPU and memory utilization) statistics. The context menus will guide you to the information that is available.

# Monitoring Using CiscoView
## Interface Statistics








## Monitoring Using CiscoView – Interface Statistics

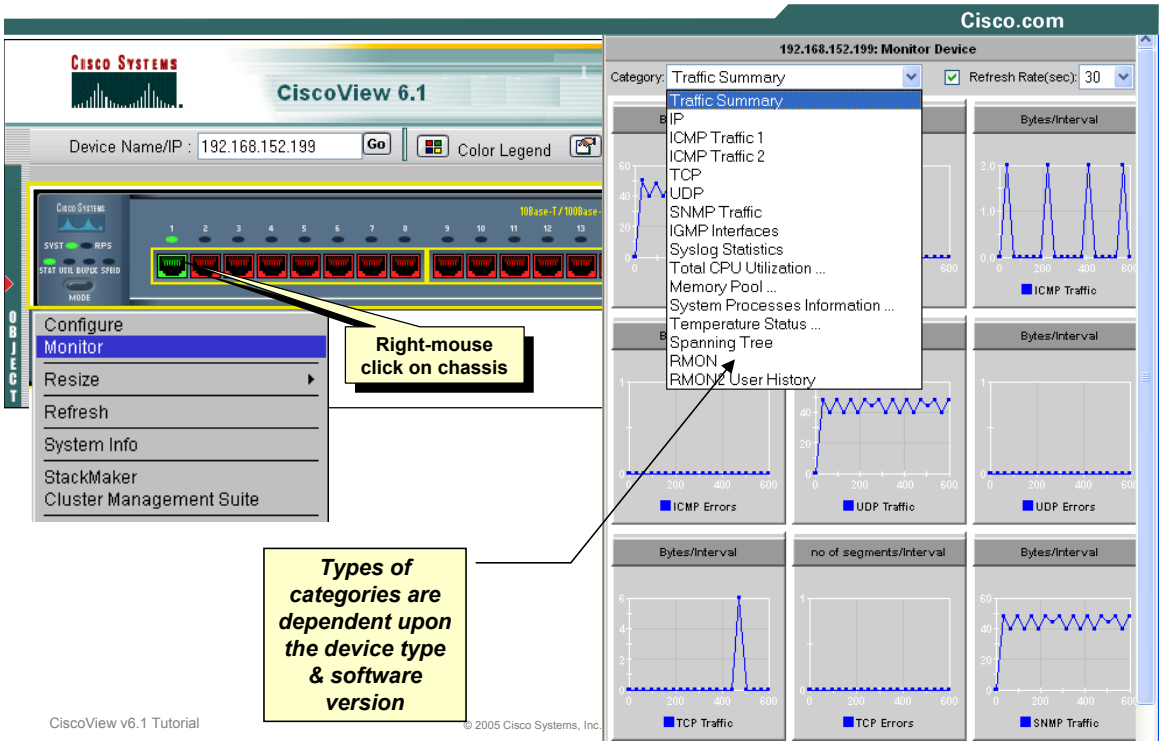
For example, to monitor the interface statistics of a device, select the interface to monitor, right-mouse click on the selected interface, and then choose *Monitor*.

In the example above, the Interface Statistics (% utilization and packet rates for Unicast, Multicast, Broadcast, Errors, and Discards) are displayed by default. The user can easily change the type of statistics displayed by changing the Category. The types of categories are dependent upon the device type and software version.

*Note(s):*

- *Remember, the statistics are not stored in a database; thus, once the window is closed, the historical statistics can not be retrieved.*
- *The polling interval or data points can be varied by changing the Refresh Rate.*
- *The amount of data that is viewable in the display is based on the number of data points. Currently, CiscoView supports 25 points on each chart. When a graph fills up with 25 data points, it scrolls to the left as polling continues.*

# Monitoring Using CiscoView
## Device-Level Statistics




## Monitoring Using CiscoView – Device-Level Statistics

Device level statistics can also be monitored using CiscoView. Select the device chassis, right-mouse click on an area of the selected chassis, and then choose *Monitor*.

In the example above, the Traffic Summary Statistics (Byte rate for various protocols) are displayed by default. The user can easily change the type of statistics displayed by changing the Category. Information on CPU and memory usage can be polled by simply changing the category. The types of categories are dependent upon the device type and software version.

*Note(s):*

- *Some devices and components have no categories*
- *Remember, the statistics are not stored in a database; thus, once the window is closed, the historical statistics can not be retrieved.*
- *The polling interval or data points can be varied by changing the Refresh Rate.*
- *The amount of data that is viewable in the display is based on the number of data points. Currently, CiscoView supports 25 points on each chart. When a graph fills up with 25 data points, it scrolls to the left as polling continues.*

34

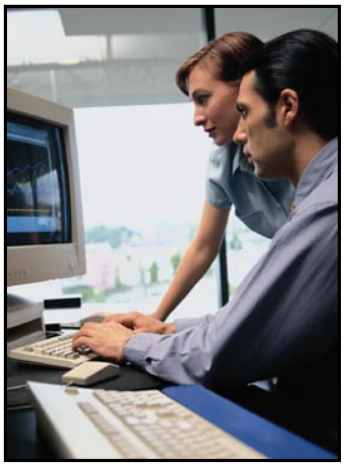
# Scenarios Using CiscoView

## Chapter 3

# Chapter 3 Outline

Cisco.com

- **Scenario 1**
  - *Using CiscoView to configure Syslog messaging on a Cisco CatOS device*
- **Scenario 2**
  - *Using CiscoView to configure VLANs on a Cisco switch*
- **Scenario 3**
  - *Using CiscoView to monitor interface statistics on Cisco switch*







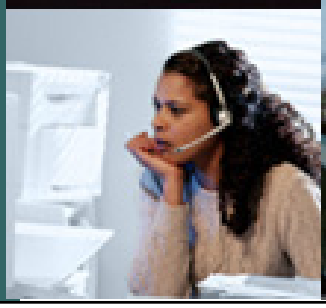
## Chapter 3 Outline

This chapter contains several common scenarios for using CiscoView to manage Cisco devices. The scenarios will provide step-by-step examples of how to use CiscoView to configure Syslog messaging and VLANs on a switch, and monitor interface statistics on a Cisco device.

So let's get started.

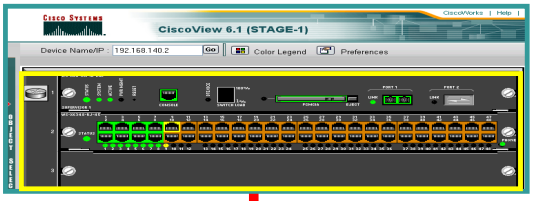
# Scenario #1

## Using CiscoView to Configure Syslog Messaging on Cisco CatOS Device



# Scenario 1 Overview

Cisco.com




**Use CiscoView to easily:**

1. **Identify the Syslog server that will be collecting the device system messages (CiscoWorks server)**
2. **Define the syslog messages to collect based on severity levels**
3. **Enable syslog messaging**

**Severity Level**

0 - emergency
1 - alert
2 - critical
3 - error
4 - warning
5 - notification
6 - informational
7 - debugging

**Catalyst 6009 CatOS v6.3**

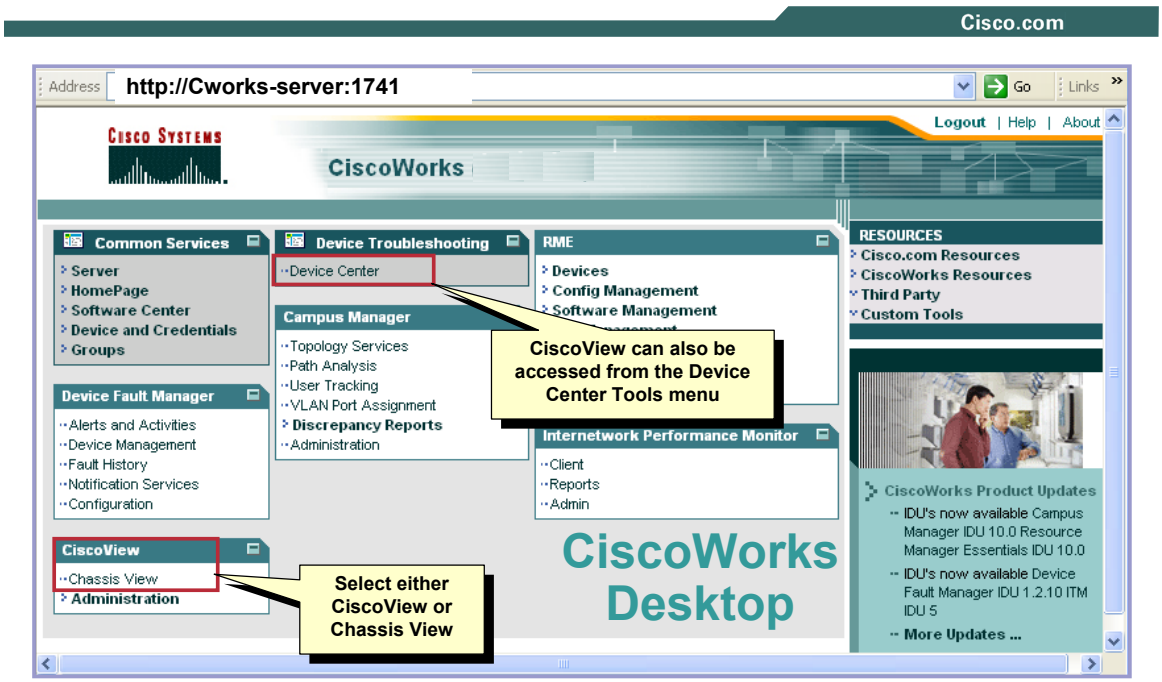
CiscoView v6.1 Tutorial © 2005 Cisco Systems, Inc. All rights reserved. Scenarios 3-4

## Scenario 1 Overview

Sometimes it can be difficult to remember all the commands to configure features on a device. CiscoView makes life easy by simplifying the configuration. Simply access the device and use the graphical user interface to select the parameters. CiscoView will change the device configuration for you using SNMP. There are no jobs to schedule; the configuration changes occur when you make the changes on the screen.

In this scenario, we will illustrate and show the steps for configuring Syslog messaging on a Catalyst 6000 switch. Syslog messages with severity levels 0-6 will be forwarded to the CiscoWorks server for analysis using Resource Manager Essentials (RME).

# Access CiscoWorks







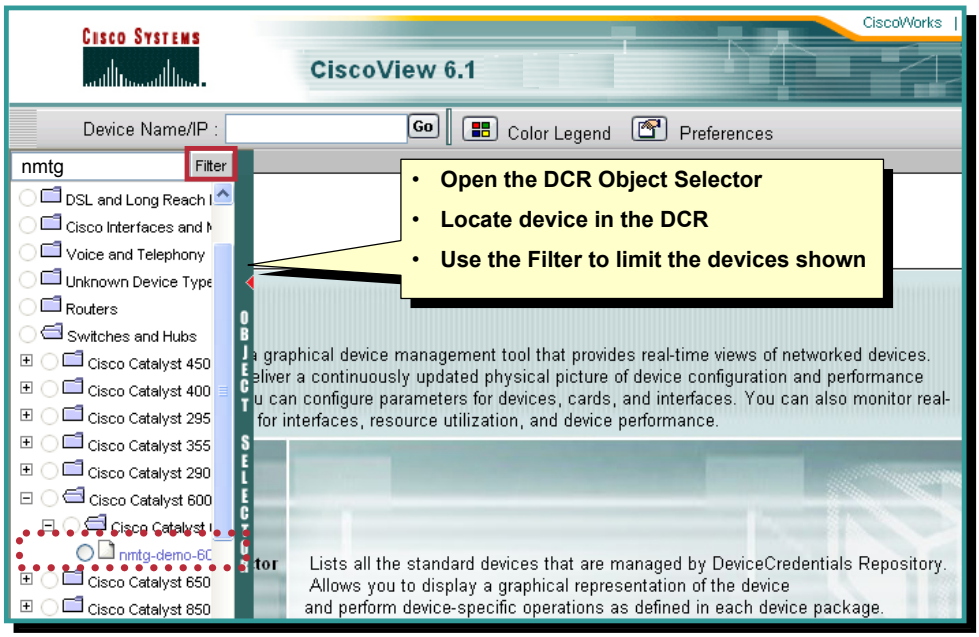

## Access CiscoWorks

Step 1. First, access CiscoWorks. Using a supported web browser, enter the CiscoWorks URL and login to the CiscoWorks server using a user account that has the CiscoWorks Network Administrator user role. (This user role is required for configuring devices.)

One way to access CiscoView is to launch the application from the CiscoWorks desktop. CiscoView can also be accessed from other application menus, such as the Device Center. Let's try launching CiscoWorks both ways. First, let's launch CiscoView from the link on the CiscoWorks desktop; and secondly, launch CiscoView from the CiscoWorks Device Center.

Step 2. From the CiscoWorks desktop, the user can see all the CiscoWorks applications installed or registered with the server. To launch CiscoView from the CiscoWorks desktop link, click either the *CiscoView* header or click *Chassis View to launch CiscoView directly*.

# Access the Device from the DCR








## Access the Device from the DCR

When launching CiscoView from the CiscoWorks desktop, you will now need to tell CiscoView which device to access. You can either enter the device IP address or hostname or select the device from the CiscoWorks Device and Credentials Repository, known as the DCR. Follow these steps to have CiscoView access your device.

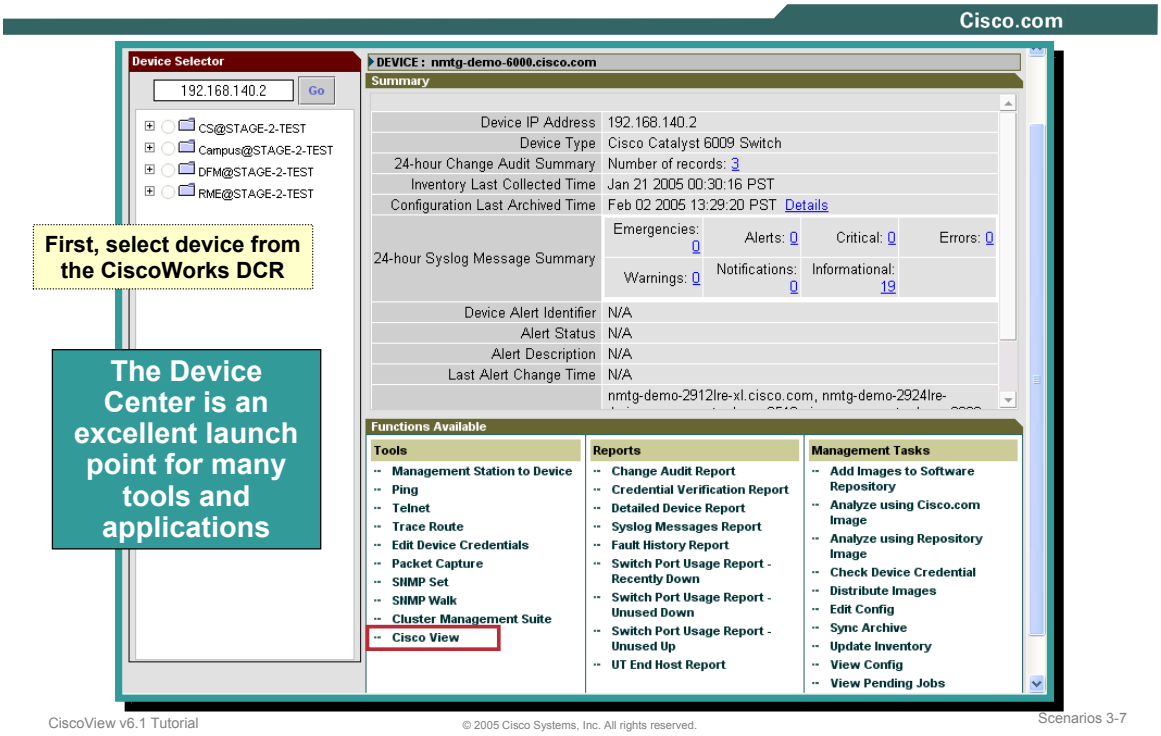
Step 1. If you know the device name or its IP address, great! Simply enter it in the field next to the *Go* button and click *Go*. Otherwise, locate the device in the CiscoWorks DCR. The DCR is populated from other CiscoWorks services or applications, but the information (device IP addresses and SNMP community strings) can be shared by all CiscoWorks applications.

Step 2. In the illustration above, we used the DCR to pick the Catalyst switch. To open the DCR, select the vertical OBJECT SELECTOR bar.

Step 3. A portion of the device name was known; thus, the user typed a part of the name into the Filter field and clicked *Filter*. This will limit the devices shown in the DCR to just those device names that match the filter string.

Step 4. Once the device is located, the user can click on the device to open CiscoView and the Chassis View of the device.

# Access CiscoView from the Device Center




## Access CiscoView from the Device Center

Alternatively, you can access CiscoView from the application menus of other CiscoWorks applications, like Device Center. We like the Device Center because it provides quick access to many network management tools and reports for the device selected.

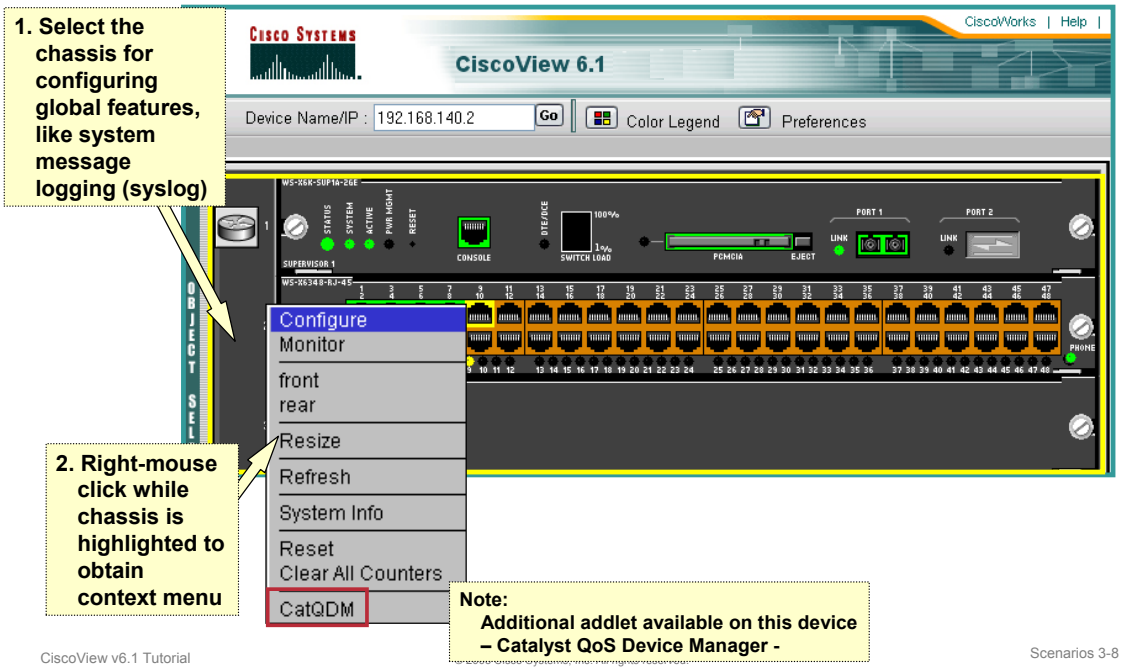
To launch the Device Center and CiscoView, follow these steps.

Step 1. From the CiscoWorks desktop, locate and select *Device Center*.

Step 2. Select the device you want to manage using the CiscoWorks DCR in the left window pane.

Step 3. Once the Device Center has successfully accessed the device, go to the *Tools* menu at the bottom of the page of the Device Center. Select *CiscoView*.

# Access the Context Menus




## Access the Context Menus

If the device is SNMP reachable and the SNMP community strings configured on the device match that in CiscoWorks, the Chassis View of the device will be displayed. Let's use the following steps to get ready to configure the device for System Messaging (Syslog).

Step 1. System Messaging (Syslog) is a global feature on the device. Therefore, select the *chassis* component or the outside casing of the device displayed. Once selected, the component to configure or monitor (in this case, the chassis), it is highlighted in yellow.

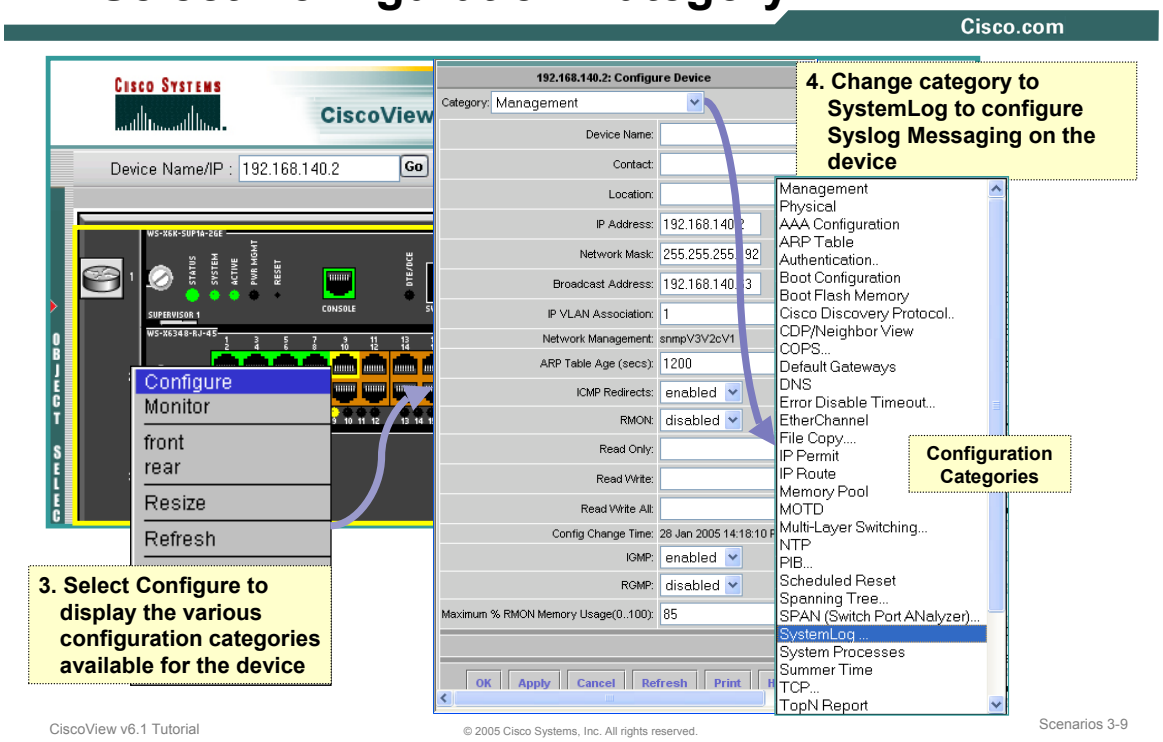
Step 2. Once the chassis is selected (for global device configuration), right-mouse click on it to obtain the context menu. The context menu for the chassis of the Catalyst 6000 is illustrated above.

Step 3. To configure System Logging (Syslog), select *Configure*.

*Note(s):*

- *In this illustration, the device has an embedded addlet on the device, CatQDM. This is the Catalyst QoS Device Manager. The QoS features may not be configurable using SNMP and CiscoView; thus, this addlet will allow the user to still use CiscoView and an easy to use GUI to configure these features.*

# Select Configuration Category




## Select Configuration Category

Step 1. Once you have selected *Configure* on the component selected, the Configure Device window will be displayed.

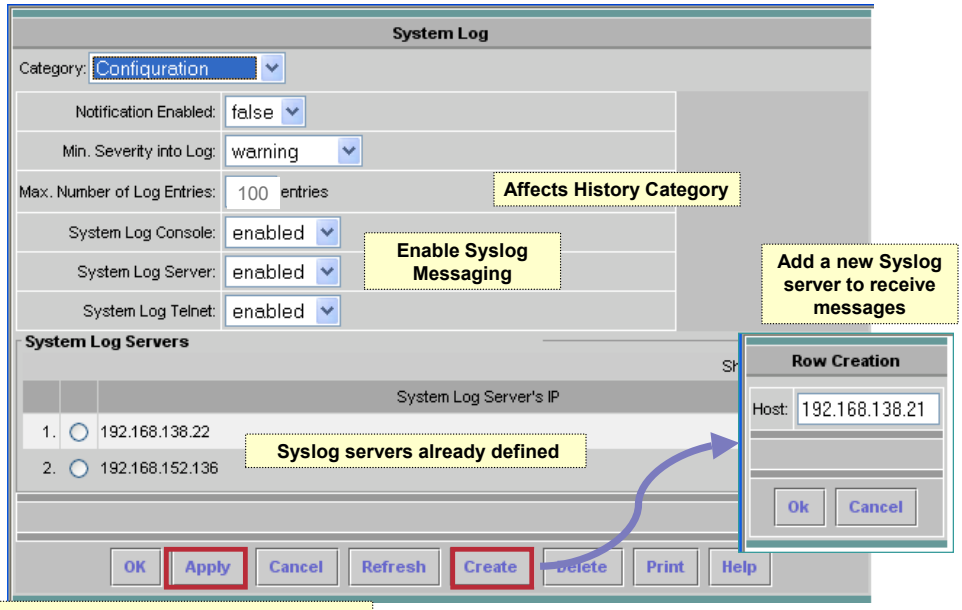
Step 2. Click the *down-arrow* on the Category field at the top of the window. This will display all the different configuration categories.

Step 3. To configure Syslog, locate and select *SystemLog* in the list of configuration categories.

# Configure Syslog Messaging

## Adding a New Syslog Server

Cisco.com




Click **Apply** to save changes immediately to device config





## Configure Syslog Messaging

Step 1. Once you've selected *SystemLog* as the configuration category, a new dialog window will be displayed with all the parameters related to this category. In this case, System Log has sub-categories to view.

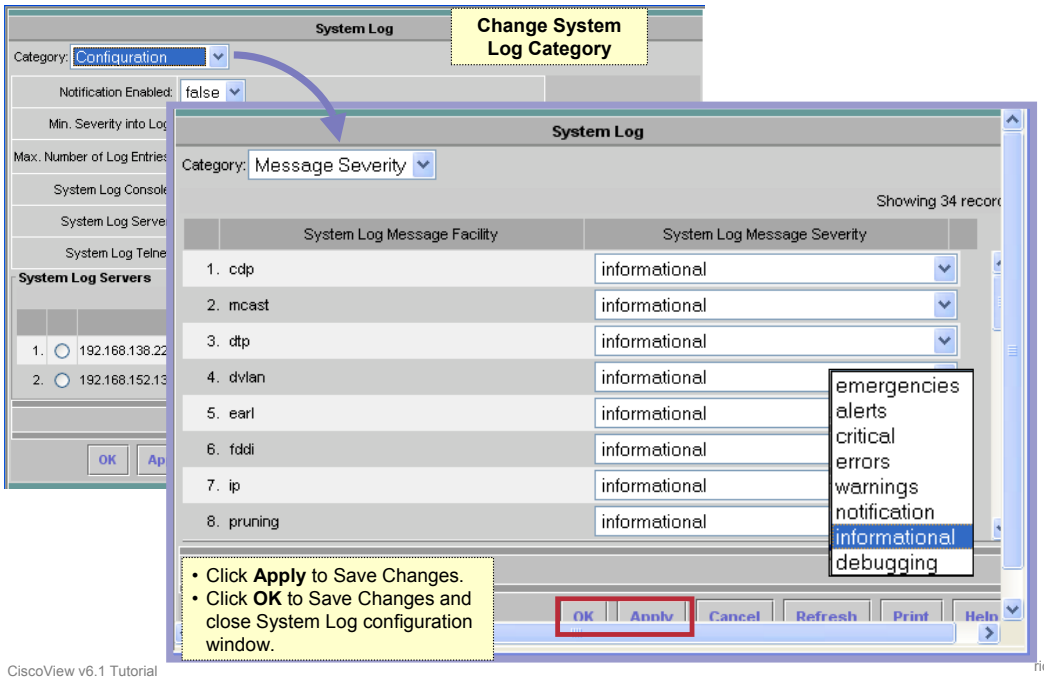
Step 2. With the sub-category Configuration selected, review the following:

- System log is enabled
- Configure the system log preferences. You can set the number of entries in the log to display and the minimum severity level to view in the log. The illustration above changed the number of entries to view in the log to 100 with a minimum level of warning messages.
- Add the CiscoWorks server as a server to receive syslog messages. To add a new server, click the *Create* button and enter its IP address.

Step 3. Click *Apply* to Save the changes to the Configuration sub-category.

# Configure Syslog Messaging
## Setting the Severity Levels

Cisco.com




CiscoView v6.1 Tutorial

Scenarios 3-11

## Setting the Severity Levels

Step 1. Now change the System Log sub-category from *Configuration* to *Message Severity* by selecting the down-arrow next to the sub-category.

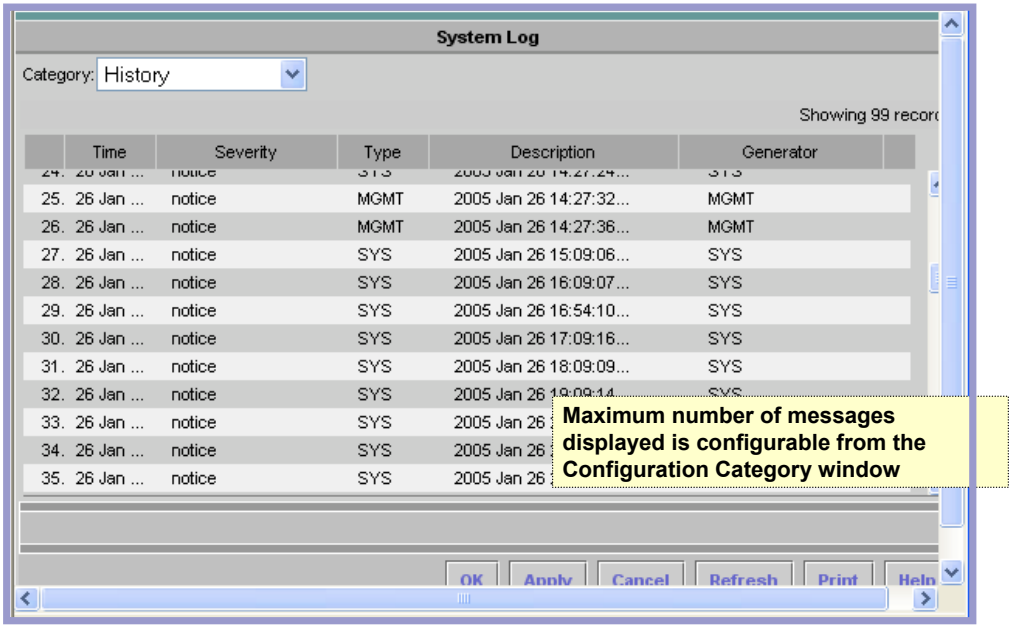
Step 2. With the sub-category changed to *Message Severity*, scroll down and view all the device facilities that generate system messages.

Step 3. Verify the levels for all the facilities. Remember that the levels are cumulative. So, if you set the level to debugging, all messages would be logged for that facility.

Step 4. Click *Apply* to Save the changes to the Message Severity sub-category.

# Configure Syslog Messaging
## View System Log on Device

Cisco.com








## View the System Log on the Device

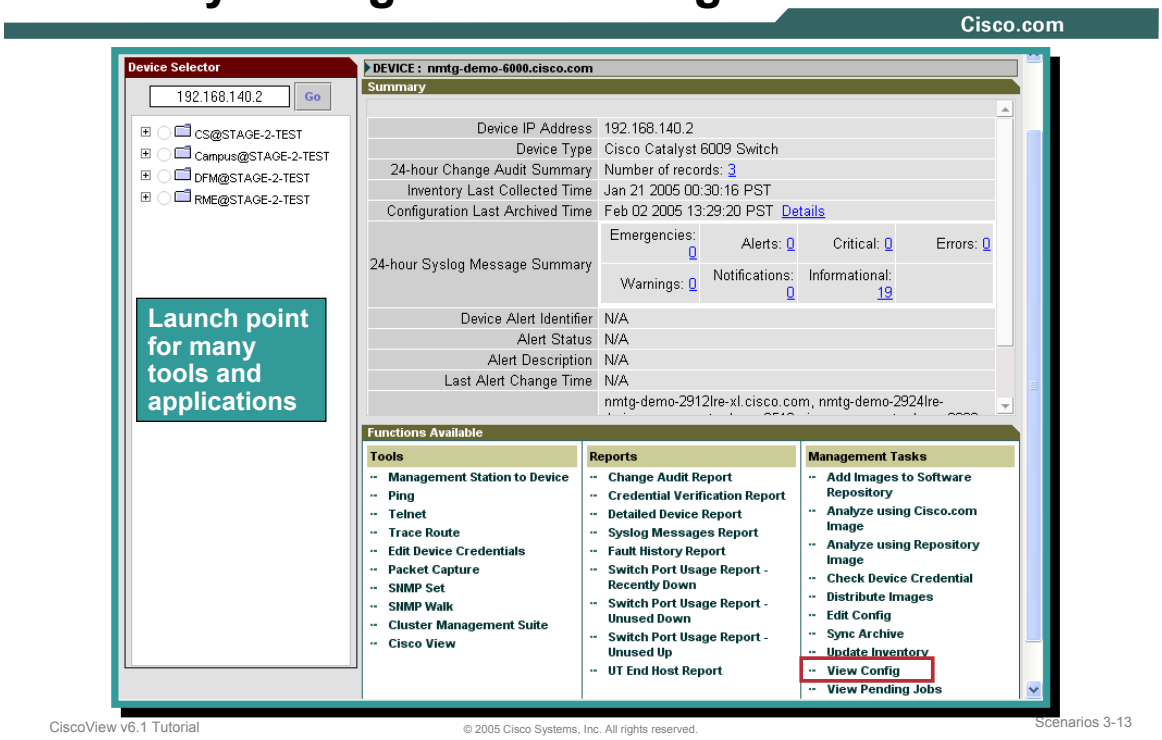
Step 1. Now change the System Log sub-category from *Message Severity* to *History* by selecting the down-arrow next to the sub-category.

Step 2. This feature allows the user to view when syslog messages have been generated and sent to the configured syslog servers defined earlier.

Remember that the number and types of messages viewed here is dependent on the settings in the System Log Configuration sub-category.

Step 3. Click *OK*. The changes to the device configuration file will take place immediately.

# Verify Configuration Changes







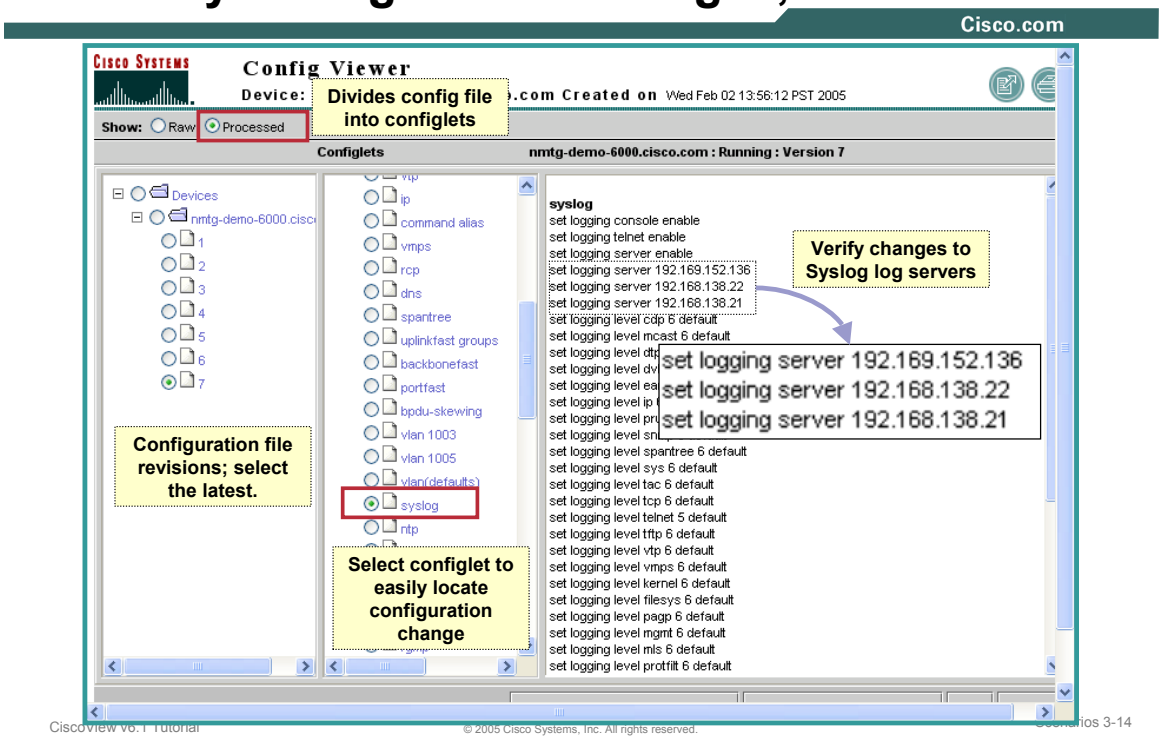

## Verify Configuration Changes

The Device Center is a great place to launch other tools as well, such as the Config Viewer. (The Device Center is available as apart of the LMS bundle. The Resource Manager Essentials (RME) application provides the services that collects and archives device configuration files.)

Step 1. Launch the *Device Center* from the CiscoWorks desktop. Select the device from the DCR.

Step 2. Let's use the View Config task to view the configuration file for the device. Click *View Config* from the Device Center's Management Tasks.

# Verify Configuration Changes, continue …




## Verify Configuration Changes, continue …

Step 3. When *View Config* is selected in the Device Center, the Config Viewer from RME is launched.

Step 4. To easily locate configuration features in a config file, Config Viewer can process the config file into Configlets. Select the *Processed* radio button.

Step 5. Open the device tree to view all the archived configuration files for the device. Select the latest one.

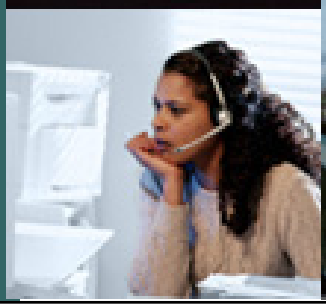
Step 6. Locate the Configlet *syslog* and select the radio button for it.

Step 7. The right-side of the screen will display the portion of the config file related to syslog.

Step 8. Verify the configuration file for correctness.

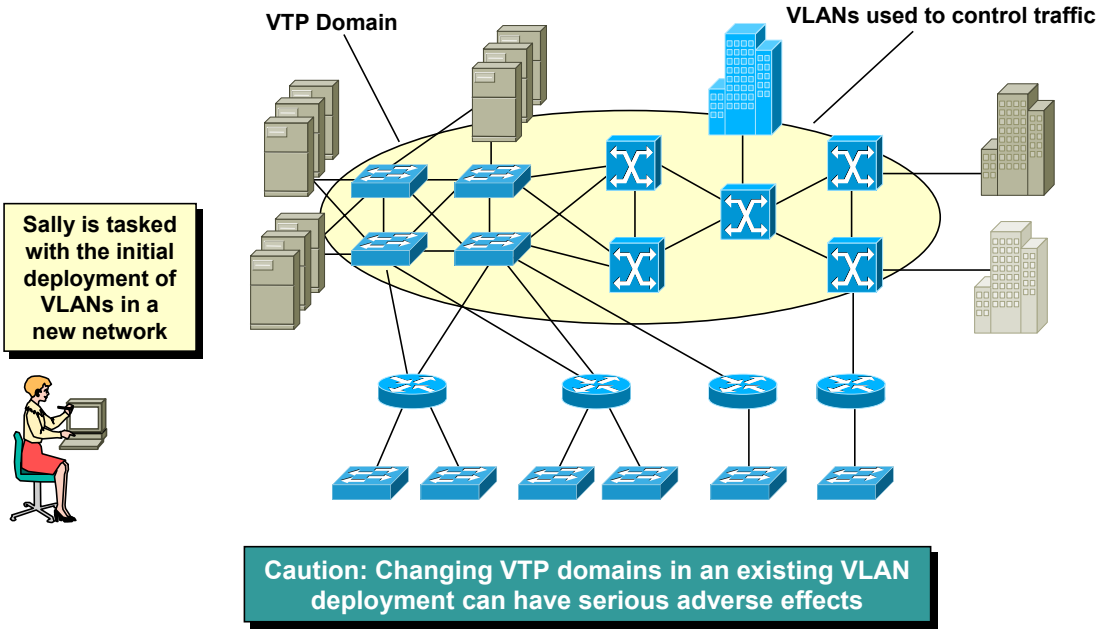
# Scenario #2

## Using CiscoView to Configure VLANs on Cisco Devices



# Scenario 2 Overview

Cisco.com








## Scenario 2 Overview

In this scenario, we will use CiscoView to create new VLANs in an existing VTP (VLAN Trunking Protocol) domain and use CiscoView to easily assign various ports to the new VLANs.

The new VLANs will be created to support the new Engineering and Administration departments.

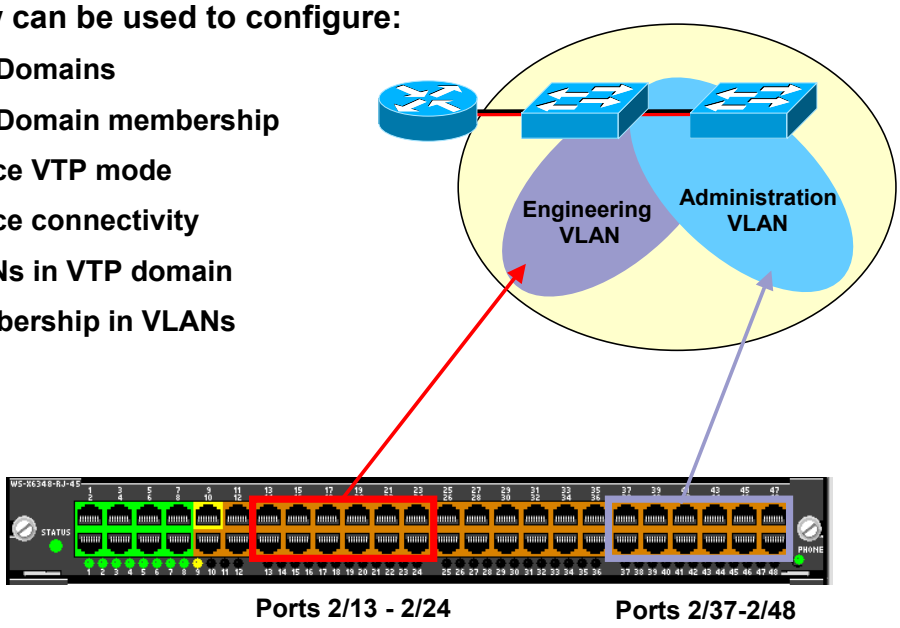
(This scenario is not meant to teach you how to implement VLANs and VTP domains in your network. This scenario will illustrate the features within CiscoView to support the configuration of VLANs and VTP domains on a Cisco device.)

# CiscoView Features to Support VLANs

Cisco.com

**CiscoView can be used to configure:**

- **VTP Domains**
- **VTP Domain membership**
- **Device VTP mode**
- **Device connectivity**
- **VLANs in VTP domain**
- **Membership in VLANs**








## CiscoView Features to Support VLANs

Using SNMP and CiscoView, a user can define a VTP domain, configure devices as VTP servers, clients, or transparent devices in the domain, create VLANs within the domain, assign ports to a VLAN, and view the ports assigned to a VLAN.

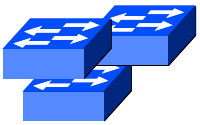
In this scenario, two VLANs will be created (Engineering and Administration) and selected ports on a device will be assigned to the newly created VLANs.

# VLAN Configuration Overview

Cisco.com

- **Enable protocols on devices**
  - SNMP (Simple Network Management Protocol)
  - ➢ STP (Spanning Tree Protocol)
  - CDP/ILMI (Cisco Discovery Protocol)
  - ➢ VTP (VLAN Trunking Protocol)
- ➢ **For each device, configure its VTP domain name and mode (VTP server, client, or transparent)**
- ➢ **Set up at least one device as a VTP server in every VTP domain to advertise the VLAN configuration for the devices in the domain**
- **Enable trunking for links between devices supporting multiple VLANs**
- **Router configured to route between VLANs**

**This scenario will illustrate how to configure/view many of these VLAN features:**
- ➢ **VTP Domain**
- ➢ **VTP Mode**
- ➢ **STP settings per VLAN**



CiscoView v6.1 Tutorial © 2005 Cisco Systems, Inc. All rights reserved. Scenarios 3-18

## VLAN Configuration Overview

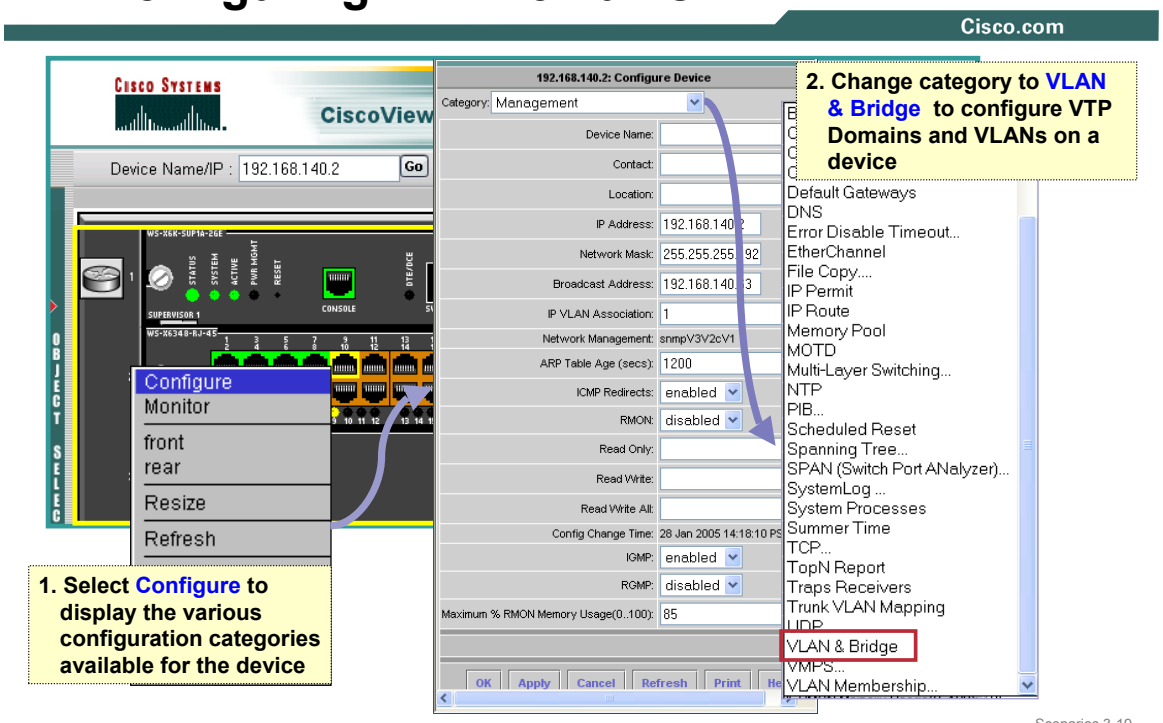
If you are not familiar with configuring VLANs in a network, it can be a daunting task. The list above identifies important VLAN features that need to be configured in the network devices in order for VLAN to work properly.

In this scenario, we will illustrate how to configure many of these features using CiscoView; however, SNMP must be enabled first prior to using CiscoView. Remember, CiscoView uses SNMP to configure and monitor the devices that it is managing. (The tasks highlighted above with an arrow as a bullet will be illustrated in this scenario.)

*Note(s):*

- *Although, not illustrated in this scenario, CiscoView can also be used to enable CDP, define default gateways, and more.*

# Configuring VTP Domains




## Configuring VTP Domains

The VLAN Trunking Protocol (VTP) is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs for all devices within a VTP domain. A VTP domain (also called a VLAN management domain) is made up of one or more network devices that share the same VTP domain name and that are interconnected with trunks. VTP minimizes configuration inconsistencies that can result in a number of problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

With VTP, you can make configuration changes centrally on one or more network devices (the VTP server device) and have those changes automatically communicated to all the other network devices in the network.

So let's get started by first defining a VTP domain on a device. The following steps bring you to the configuration category for configuring VLAN features.

Step 1. Following the same steps as in the first scenario to open the Chassis View of the device to be configured.

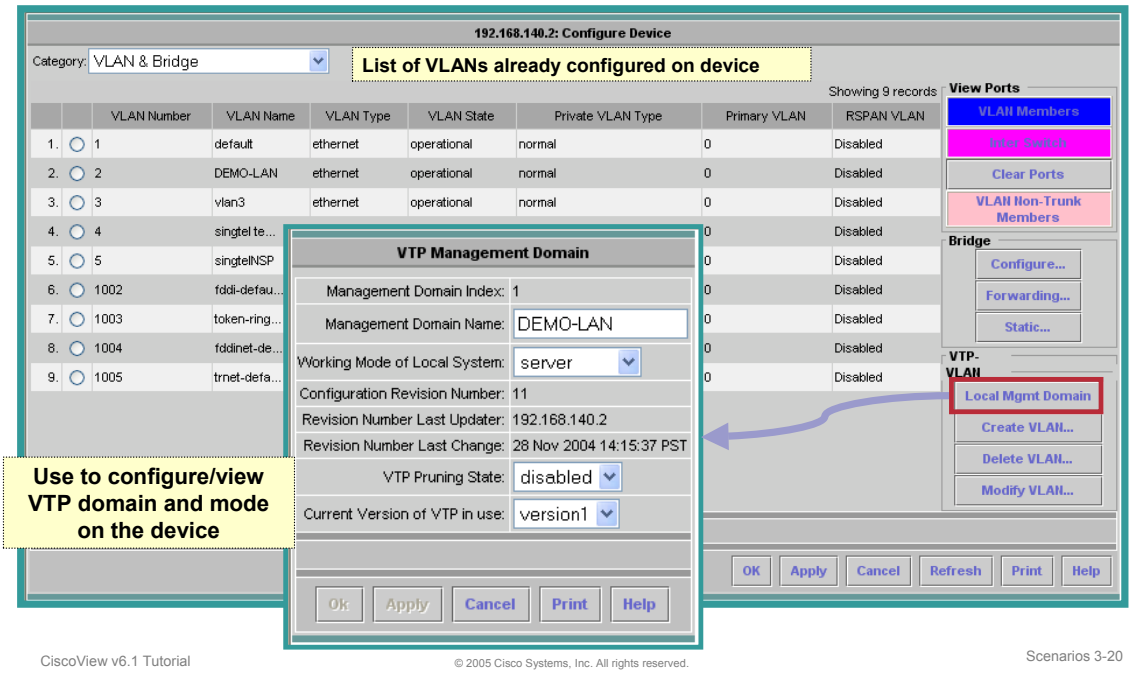
Step 2. The VTP Domain information is also a global feature on the device. Therefore, select the chassis component. Once selected, it is highlighted in yellow.

Step 3. Once the chassis is selected (for global device configuration), right-mouse click on it to obtain the context menu. The context menu for the chassis of the Catalyst 6000 is illustrated above.

Step 4. To configure or View the VTP Domain, select *Configure*.

Step 5. Change the Category to *VLAN & Bridge*. You can use the VLAN & Bridge option to configure VTP Domains, view VLANs and their members.

# Configuring VTP Domains




## Configuring VTP Domains

In our example above, the VTP management domain is called “DEMO-LAN”. Thus, all devices configured for VTP and in the DEMO-LAN VTP domain, will be knowledgeable about the VLANs configured in that domain.

The device will also be configured with the VTP mode of “server”. In VTP server mode, you can create, modify, and delete VLANs and specify other configuration parameters (such as VTP version and VTP pruning) for the entire VTP domain. VTP servers advertise their VLAN configuration to other network devices in the same VTP domain and synchronize their VLAN configuration with other network devices based on advertisements received over trunk links. VTP server is the default mode.

In the steps below, we will see how to use CiscoView to perform these CLI commands.

```
Cat-6509# configure terminal
Cat-6509(config)# vtp mode server
Setting device to VTP SERVER mode.
Cat-6509(config)# vtp domain DEMO-LAN
Setting VTP domain name to DEMO-LAN
Cat-6509(config)# end
Cat-6509# show vtp status
```

To making these VTP configuration changes using CiscoView, follow these steps:

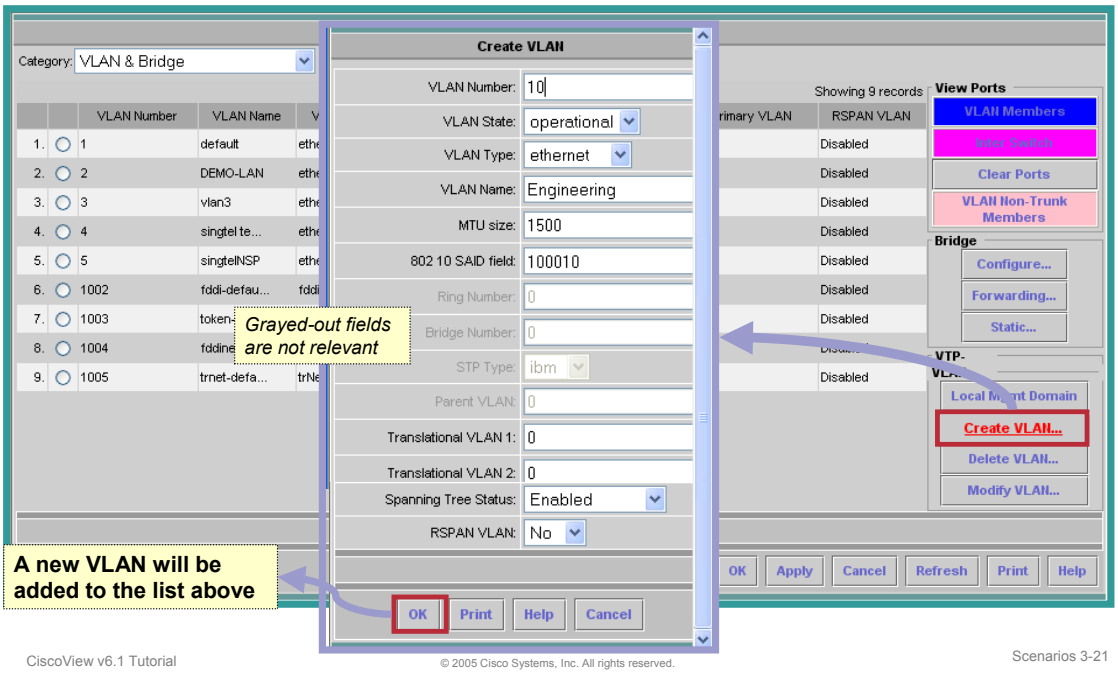
Step 6. With the Category changed to *VLAN & Bridge*, select *Local Mgmt Domain*. The VTP Management Domain window will appear.

Step 7. In the *Management Domain Name* field, enter the VTP Domain name “DEMO-LAN”.

Step 8. In the *Working Mode of Local System* field, enter server. This will make the device a VTP server.

Step 9. Click *OK* to save and close the window.

# Creating New VLANs in the VTP Domain




## Creating New VLANs in the VTP Domain

Virtual LANs (VLANs) allow you to logically group resources independent of their physical location. This arrangement of resources, and the ports to which they are attached, is called a logical grouping. A logical group of ports is called a VLAN. Ports or groups of ports in a VLAN are called members. VLANs isolate all traffic, including broadcasts and multicasts, from being propagated to members of other VLANs.

There are many guidelines and restrictions when creating and modifying VLANs in a network and using CiscoView can help to avoid misconfigurations.

To define new VLANs in the device's VTP domain using CiscoView, follow these steps:

Step 1. With the Category set to *VLAN & Bridge*, select the *Create VLAN* button. The Create VLAN window will appear.

Step 2. Set the attributes of the VLAN: VLAN number, name, MTU size, 802.10 SAID, and STP. Select OK to save and close window. Setting these fields is equivalent to the following CLI commands.

Cat-6509# **configure terminal**

Cat-6509(config)# **vlan 10**

Cat-6509(config-vlan)# **name Engineering**

Cat-6509(config-vlan)# **mtu 1500**

Cat-6509(config-vlan)# **exit**

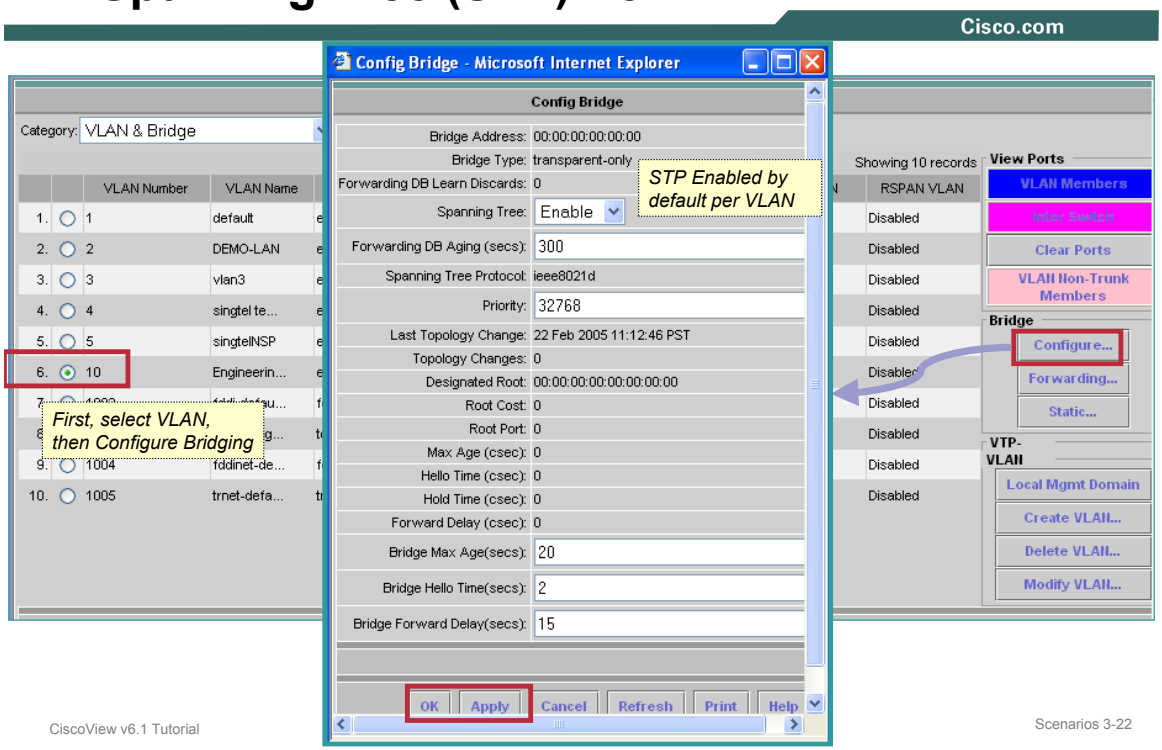
Cat-6509(config)# **vlan 11**

Cat-6509(config-vlan)# **name Administration**

Cat-6509(config-vlan)# **exit**

Cat-6509# **show vlan id 10**

# Spanning Tree (STP) Per VLAN



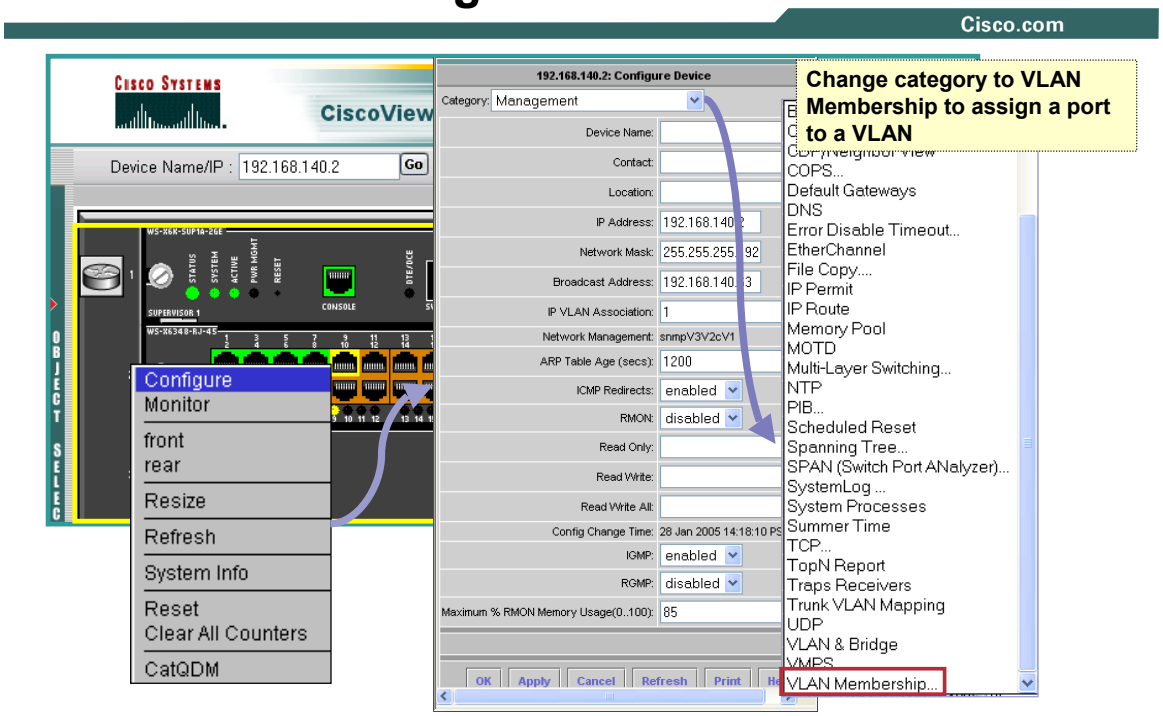

## Spanning Tree (STP) Per VLAN

As seen on the previous screen, the spanning tree protocol, can be enabled when the VLAN is created. Additionally, the STP can be enabled/disabled and its attributes can be viewed or customized using the *Bridge>Configure button*, also found under the VLAN & Bridge category, after the VLAN has been created.

*Note(s):*

- *Most of the configuration required in bridging is related to the Spanning Tree Algorithm. The Spanning Tree Algorithm allows the connected network topology to contain multiple physical paths between two stations, but constrains the active topology to be a single-span tree. If a port on one bridge fails, the other bridges can reconfigure the topology and switch traffic over to new paths.*
- *If the Spanning Tree feature is not enabled, no backup path exists to maintain bridge connectivity.*

# VLAN Port Assignments



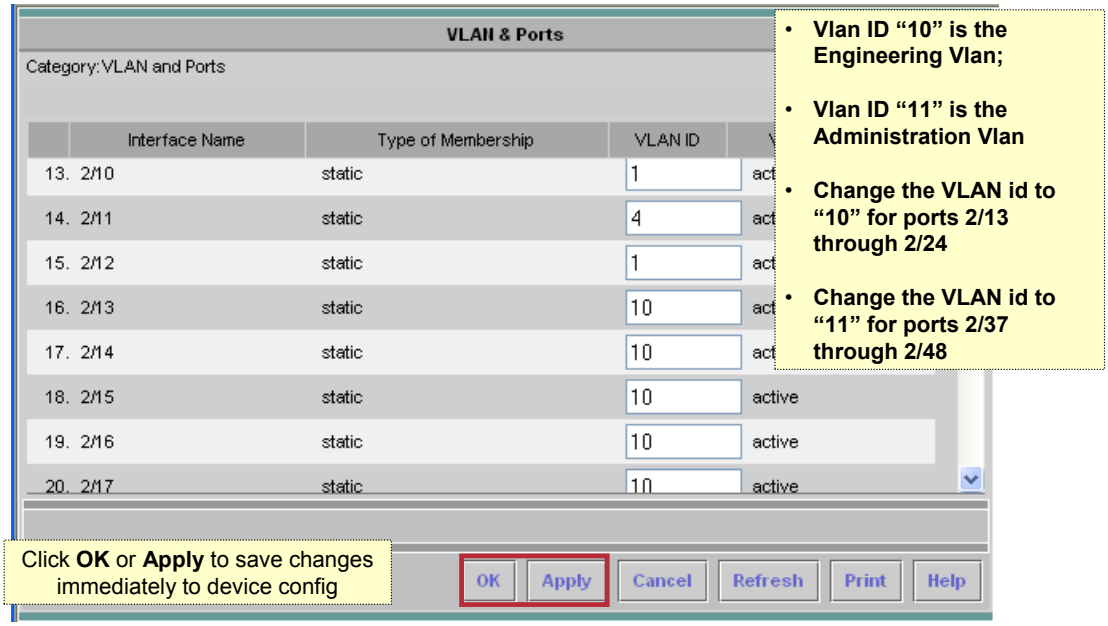

## VLAN Port Assignments

In this scenario, we have already defined the VTP domain and VTP mode on the device. Additionally, two VLANs (Engineering and Administration) have been created in the domain. Now it's time to assign ports to the VLANs just created.

To assign ports on the device, using CiscoView, to a VLAN that has been already defined, follow the steps on this page and next:

Step 1. With the chassis component still selected, and the configuration categories still shown, change the Category to *VLAN Membership*. The VLAN & Ports window will appear, as illustrated on the next page.

# VLAN Port Assignments, continue







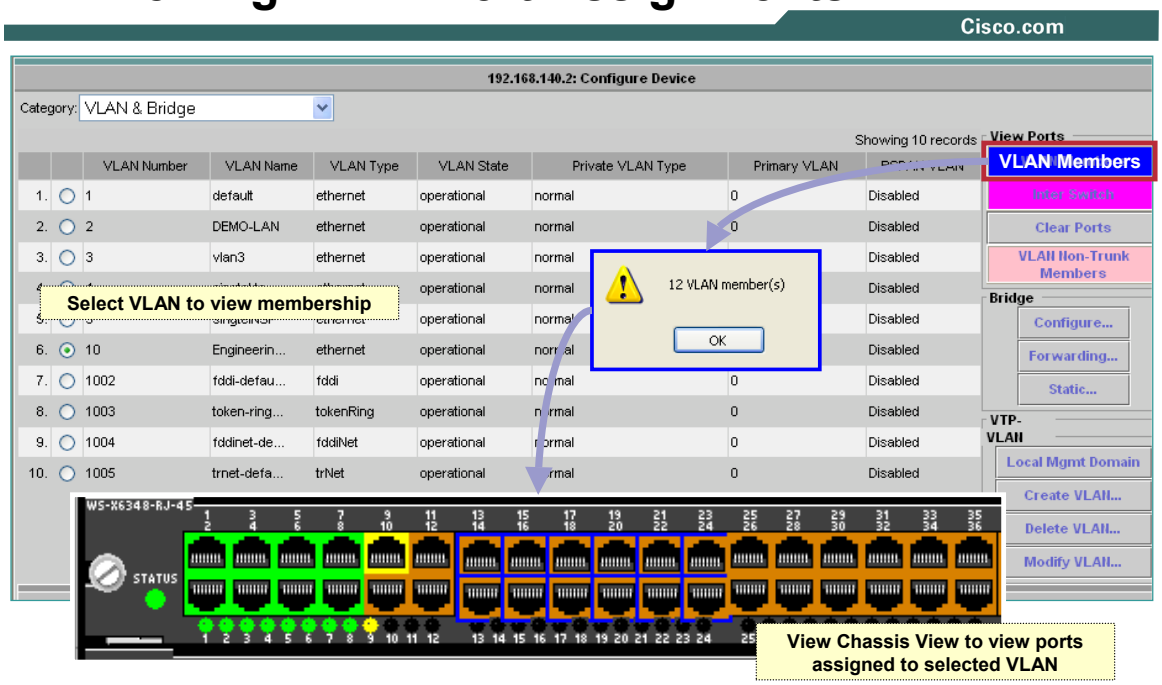

## VLAN Port Assignments, continue …

Step 2. In the VLAN & Ports window, locate the ports that should belong to the Engineering and Administration VLANs.

Step 3. Change the VLAN ID field to the ID that reflects the Engineering and Administration VLANs. For example, ports 2/13 through 2/24 have been assigned to the Engineering VLAN.

Step 4. When finished, click *Apply* or *OK* to have CiscoView make the changes on the device using SNMP. OK will also close the VLAN & Ports window.

# Viewing VLAN Port Assignments








## Viewing VLAN Port Assignments

The Chassis View in CiscoView can highlight which physical ports are members of a particular VLAN.

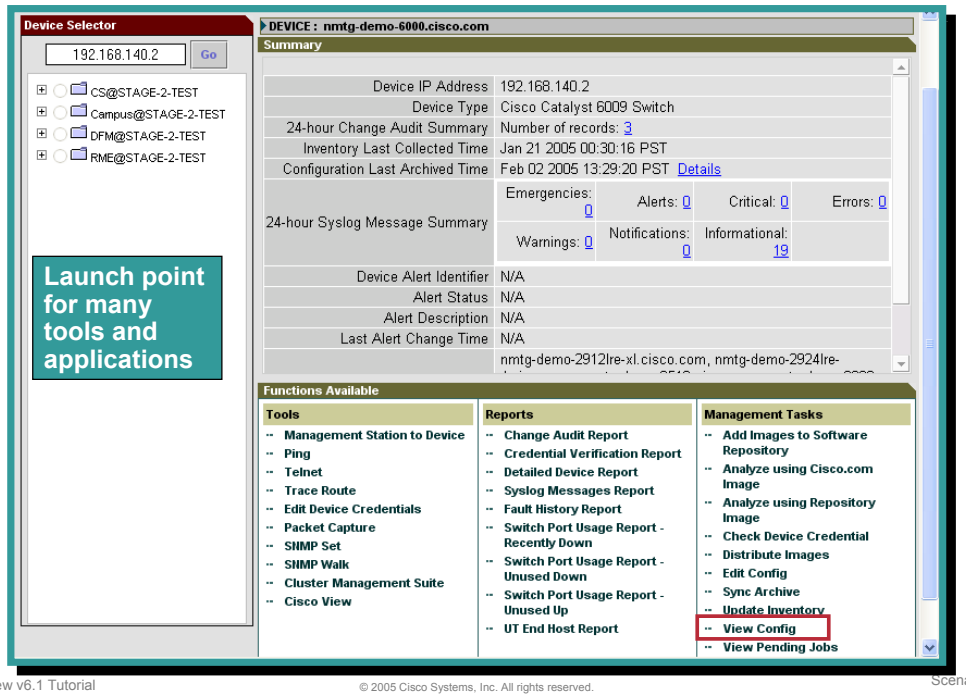
To view which VLANs are in the Engineering VLAN, follow these steps.

Step 1. With the VLAN & Bridge category open, select the Engineering VLAN by clicking on its radio button in the window.

Step 2. Select the *VLAN Members* button, as illustrated. A pop-up dialog window opens and the ports that belong to the VLAN are highlighted on the device display. The count includes both logical and physical ports, but CiscoView does not highlight the logical ports.

Step 3. To un-highlight the Engineering VLANs in the Chassis View, click the *Clear Ports* button.

# Verify Configuration Changes








## Verify Configuration Changes

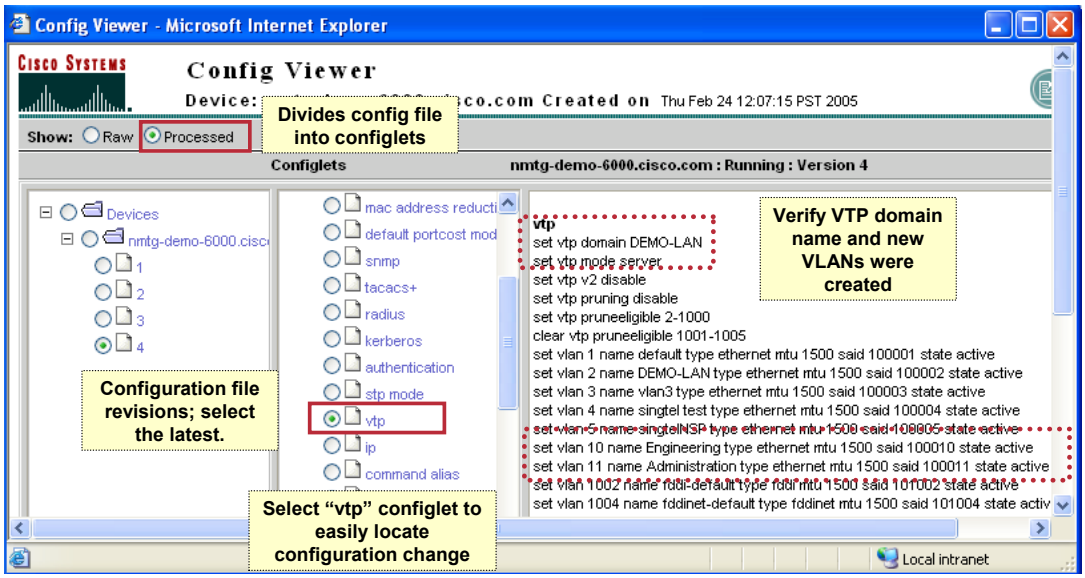
As illustrated in the first scenario, the Device Center is a great place to launch other tools as well. Let's use the *View Config* task to view the configuration file for the device just configured using CiscoView. (The Device Center is available as apart of the LMS bundle. The Resource Manager Essentials (RME) application provides the services that collects and archives device configuration files.)

Step 1. If not already displayed, launch the Device Center from the CiscoWorks home page. Select the device just configured using CiscoView.

Step 2. Click *View Config*, as illustrated above.

# Verify Configuration Changes, continue …

Cisco.com








## Verify Configuration Changes, continue …

Step 3. When *View Config* is selected in the Device Center, the Config Viewer from RME is launched, as illustrated above.

Step 4. To easily locate configuration features in a config file, Config Viewer can process the config file into Configlets. Select the *Processed* radio button.

Step 5. Open the device tree to view all the archived configuration files for the device. Select the latest one.

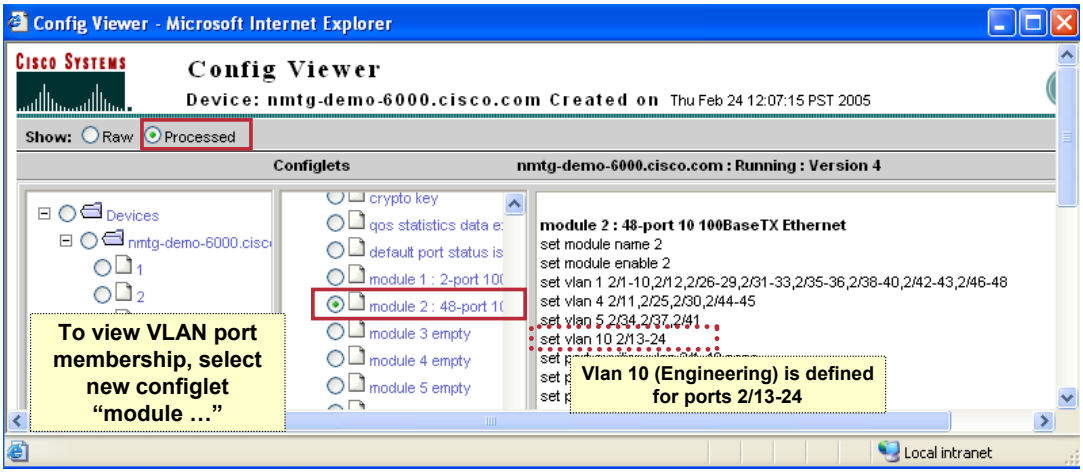
Step 6. Locate the Configlet vtp and select the radio button for it. The vtp configlet contains lines in the configuration file that show the VTP domain, mode, and VLANs defined in the domain.

Step 7. The right-side of the screen will display the portion of the config file related to vtp.

Step 8. Review the configuration file lines for the VTP changes just made to the device using CiscoView.

# Verify Configuration Changes, continue …

Cisco.com








## Verify Configuration Changes, continue …

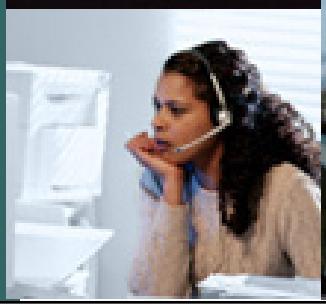
Step 9. To view the VLAN port membership, locate the Configlet "module …" and select the radio button for it.

Step 10. The right-side of the screen will display the portion of the config file related to the module.

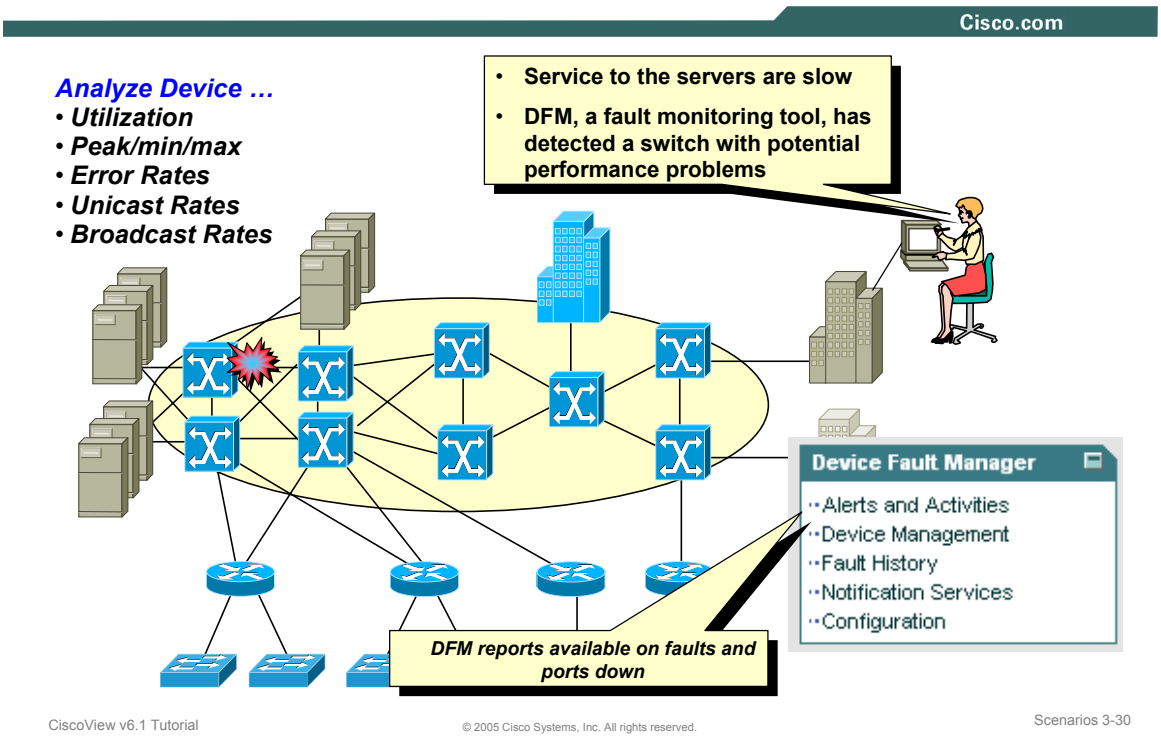
Step 11. Review the configuration file lines for the VLAN port membership changes just made to the device using CiscoView.

# Scenario #3

## Using CiscoView to Monitor Interface Statistics on a Cisco Switch



# Scenario 3 Overview




## Scenario 3 Overview

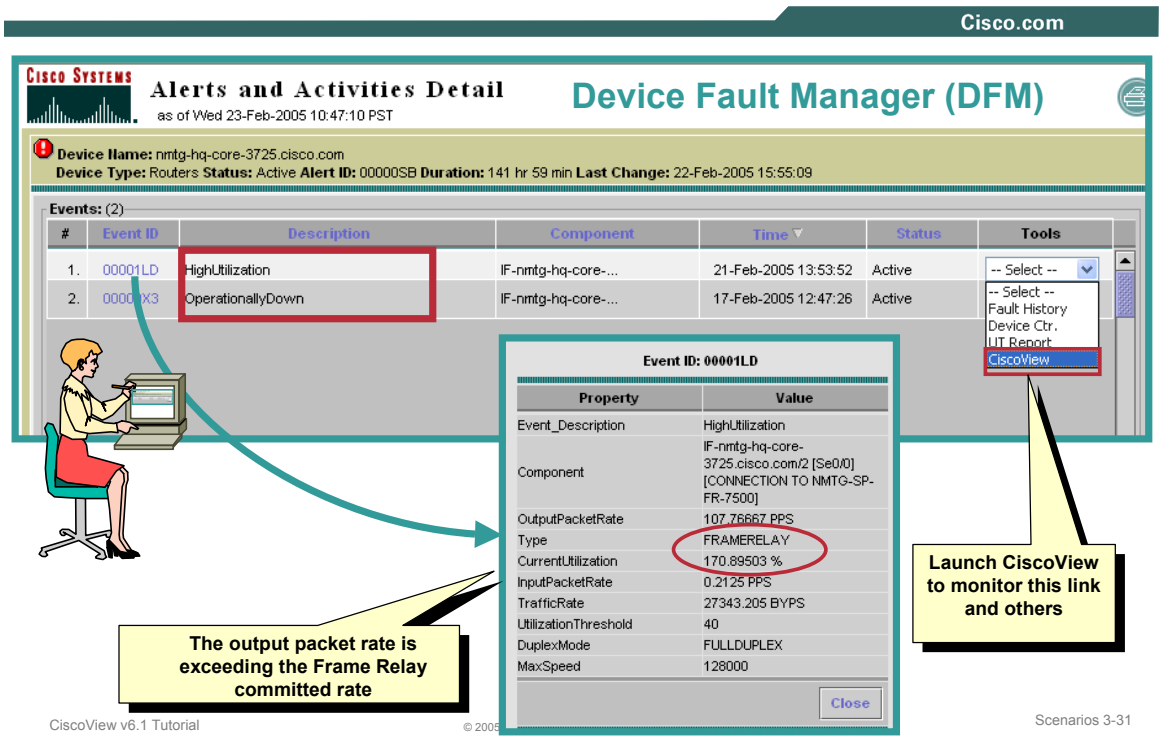
In this scenario, Sally in the network operations center is monitoring events (high port utilization) being logged by the CiscoWorks Device Fault Manager (DFM). And now, phone calls are coming into the network operations center indicating that service to the human resource servers are slow.

In this scenario, we will use CiscoView to monitor the device reported by DFM as having high port utilization.

*Note(s):*

- *DFM is designed to give early warnings of potential problems in the managed environment. DFM monitors the Cisco network devices and uses a codebook to pinpoint exceptions before devices fail. It automatically polls for relevant data maintained by each network element and applies intelligent analysis to distill the polled data into actionable information.*
- *DFM is a part of the CiscoWorks LMS bundle.*

# Alerts to Device Performance & Faults




## Alerts to Device Performance & Faults

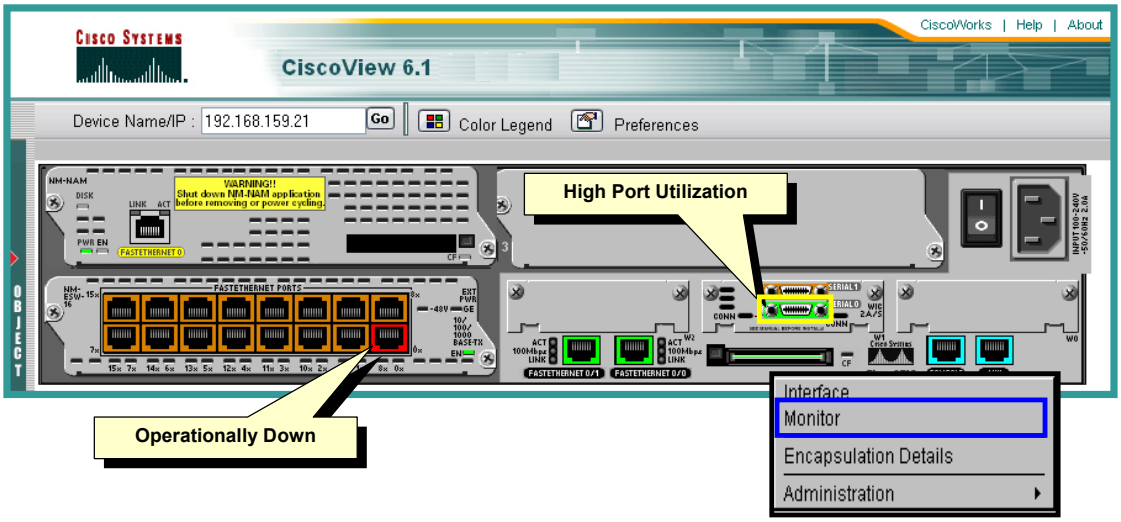
Sally in the network operations center periodically monitoring the CiscoWorks Alerts and Activities window updated by DFM. Sally notices that one of the core routers is experiencing high utilization on one of its Frame Relay links. Additionally, one of the Fast Ethernet interfaces is operationally down.

Sally clicks on the Event Id to obtain more information. From the event details, it is clear that the output packet rate far exceeds the maximum defined rate for the Frame Relay link.

Sally quickly launches CiscoView to monitor this link and other links on the device to get a clearer picture of the activity on the device.

# Using CiscoView to Monitor Interfaces

Cisco.com








## Using CiscoView to Monitor Interfaces

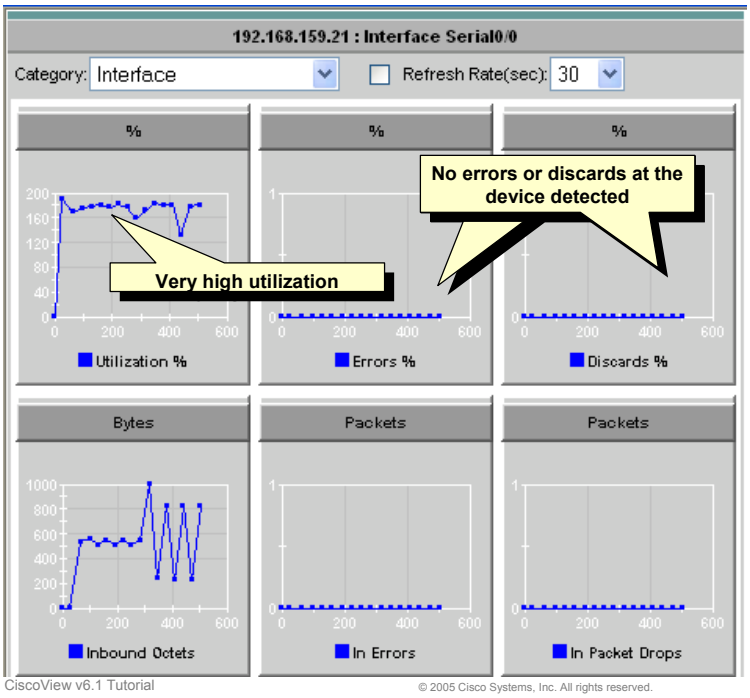
CiscoView is launched from the DFM Alerts and Activities window for the device experiencing the event. The color coded ports clearly illustrate the following:

- Ports that are active (green)
- Ports that are operationally down (red)
- Ports that are not connected (orange / light brown)
- Ports (Console/Aux) that are dormant (cyan)

To monitor, in real-time, the serial port that indicated high utilization, select the serial port and then right-mouse click on the selected port. The context menu will appear as illustrated above. Select *Monitor*.

# Using CiscoView to Monitor an Interface

Cisco.com




- Real-time statistics
- CiscoView polls the interface statistics based on the refresh rate chosen
- Up to 25 data points can be displayed on the graphs





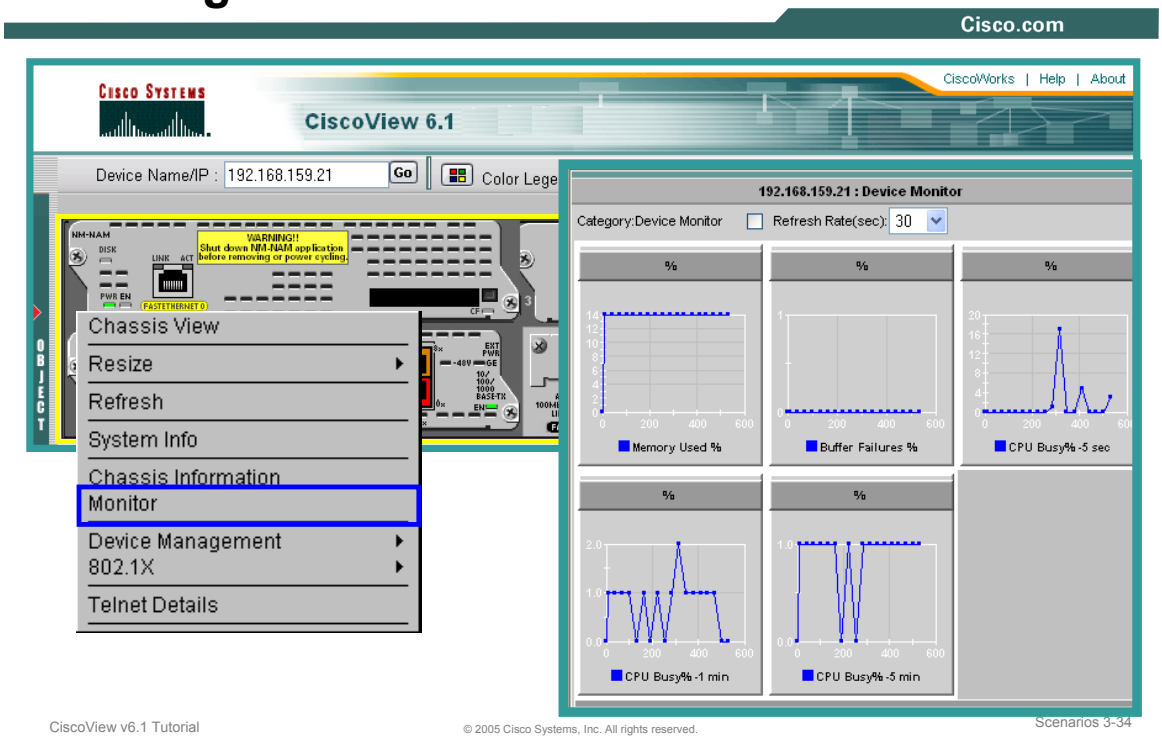
## Using CiscoView to Monitor an Interface

Sally monitored the serial link for a short period of time. The data in the CiscoView graphs are real-time and not saved to a database. Once 25 data points have been reached, the data is aged off the graph. With the refresh rate set to 30 seconds, Sally could view about 12 minutes of data. During that time the utilization remained consistently high (170%) with zero errors and discards.

Sally decides to increase the refresh rate (maximum 100 seconds) and monitor the interface for a longer period of time (about 40 minutes of data). But in the meantime, Sally now has information to send to the network engineers to determine if the high packet rate is affecting the throughput of the device and resulting in a buffering of packets, hence a slow response time to the servers.

But before Sally sends this information to the network engineers, she also gathered additional information on the device (CPU utilization, memory utilization, and buffer failures). (Refer to the next page.)

# Using CiscoView to Monitor a Device








## Using CiscoView to Monitor a Device

To monitor the device statistics, simply select the chassis instead of the interface and then right-mouse click to get the context menu. Then select *Monitor*. CiscoView will poll, based on the refresh rate, the memory and CPU utilization, and in this case, buffer failures.

Everything looks healthy from the device standpoint. So Sally sends the information off to the network engineers to determine if the attributes of the Frame Relay link (speed, CIR, etc.) need to be adjusted to improve the overall network performance.

*Note(s):*

- *The types of statistics and tasks available in the context menu is device and OS dependent.*

35

36

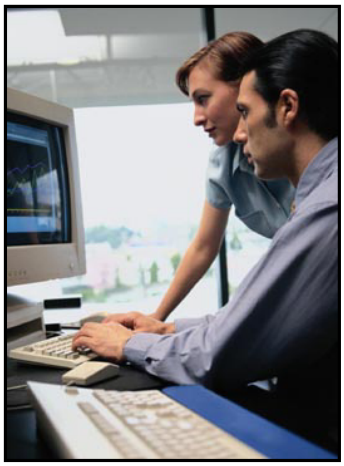
# CiscoView System Administration

## Chapter 4

# Chapter 4 Outline

Cisco.com

- **System Requirements**
  - *CiscoWorks Server*
  - *CiscoWorks Client*
  - *Cisco Devices*
- **Installation Guidelines**
  - *New install*
  - *Upgrade existing system*
- **System Maintenance, Troubleshooting & Preference Settings**







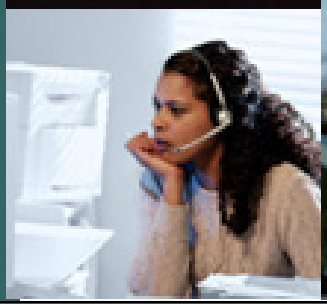
## Chapter 4 Outline

This chapter provides key information and important facts for system administrators when installing, troubleshooting, and maintaining CiscoView. It also highlights Cisco device requirements for using CiscoView to manage the device.

For detailed installation steps or information on upgrading from previous versions of CiscoView, refer to the CiscoView User Guide. A link to the user guide can be found in Chapter 5.

# System Requirements

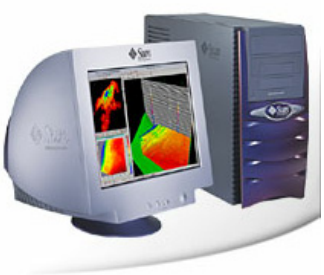
- **System Requirements**
- Installation Guidelines
- System Maintenance, Troubleshooting, & Preferences



# Hardware Requirements
## CiscoWorks Server (CCS, CiscoView)

Cisco.com

- **System Hardware*:**
  - **Sun Ultra I0 or better**
  - **Pentium 4 processor, 1 GHz or better**
- **RAM Memory*: 1GB or more; Swap: double the RAM**
- **Disk space*: 2 GB**
- **CDROM drive**
- **Network Interface Card (NIC)**
- **Color Monitor**



**** These specifications are for the CiscoWorks Common Services and CiscoView software only and need to be increased if additional applications co-exist.***





## Hardware Requirements – CiscoWorks Server

If your CiscoWorks server platform does not host other applications, the following are the minimum hardware requirements to run the CiscoWorks Common Services and CiscoView application:

- System hardware—Sun Ultra I0 or Pentium 4 1GHz or better. (CiscoWorks Common Services also supports Ultra SPARC III machines such as Sun-Fire-280R, Netra-T4, Sun Blade 1000)
- A CD-ROM drive on the server or, if on Solaris, on a remote host system that can be accessed by the Network File System (NFS)
- Memory—1 GB of RAM or more
  - Minimum requirements vary, depending on which components you choose to install: CiscoWorks Common Services alone requires 512 MB RAM
  - Integration Utility alone requires 128 MB RAM and 50 MB disk space
  - CiscoView alone requires 128 MB RAM and 96 MB disk space
- Swap Space – Double the amount of RAM
- Hard disk space—2 GB for application data
- Color monitor
- Printer—optional PostScript-compatible printer for printing graphs and charts

# System Requirements
## CiscoWorks Server (CCS, CiscoView)

Cisco.com

- **System Software**
  - Solaris 2.8 or Solaris 2.9 with the required patches from Sun Microsystems
  - Windows 2000 Professional and Server (with SP3 and SP4)
  - Windows 2000 Advanced Server (with SP3 and SP4)
  - Windows 2000 Advanced Server Terminal Services (Remote Administration mode with SP3 and SP4)
  - Windows 2003 (WS2K3) Server (Standard Edition and Enterprise Edition)
- **CiscoWorks Common Services 3.0 (CCS)**
  - CCS must be installed prior to installing CiscoView
- **A CiscoWorks license supports 1 instance of the CiscoView software installed**





## System Requirements – CiscoWorks Server

The CiscoWorks Common Services and applications can be installed on the following operating system platforms:

- Solaris 2.8 or Solaris 2.9 with the latest recommended and required patches from Sun Microsystems, Inc. Refer to the link in Chapter 5 to view the User Guide and obtain a list of Solaris patches.
- Windows 2000 Professional and Server (with SP3 and SP4)
- Windows 2000 Advanced Server (with SP3 and SP4)
- Windows 2000 Advanced Server Terminal Services (Remote Administration mode with SP3 and SP4)
- Windows 2003 (WS2K3) Server (Standard Edition and Enterprise Edition)

Once the operating system software and patches have been installed and/or verified, install the CiscoWorks Common Services software (CCS) v3.0. Then, install CiscoView.

# System Requirements
## CiscoWorks Client (CCS, CiscoView)

Cisco.com

- **CiscoWorks Client**
  - A Web browser
    - Windows: Microsoft Internet Explorer 6.0 SP1, Netscape 7.0,7.1, Mozilla 1.7.1
    - Solaris: Netscape 7.0 and Mozilla 1.7; set CLASSPATH variable to null
- **Client Platforms**
  - Solaris 2.8 or Solaris 2.9 with the recommended patches from Sun
  - Windows 2000 Professional and Server (with SP3 and SP4)
  - Windows 2000 Advanced Server (with SP3 and SP4)
  - Windows 2000 Advanced Server Terminal Services (Remote Administration mode with SP3 and SP4)
  - Windows 2003 (WS2K3) Server (Standard Edition and Enterprise Edition)
  - Windows XP Professional





## System Requirements – CiscoWorks Client

A web browser is required to access the CiscoWorks server. The web browser provides a flexible environment to access the CiscoWorks server and its tools and reports from anywhere.

To access the CiscoWorks server using a web browser, use one of the following platform types.

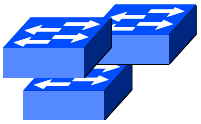
- Solaris 2.8 or Solaris 2.9 with the latest recommended and required patches from Sun Microsystems, Inc. Refer to the link in Chapter 5 to view the User Guide and obtain a list of Solaris patches.
- Windows 2000 Professional and Server (with SP3 and SP4)
- Windows 2000 Advanced Server (with SP3 and SP4)
- Windows 2000 Advanced Server Terminal Services (Remote Administration mode with SP3 and SP4)
- Windows 2003 (WS2K3) Server (Standard Edition and Enterprise Edition)
- Windows XP Professional (Client platform only)

*Note(s):*

- *CiscoView does not require Java since it is entirely HTML on the client side.*

# System Requirements
## Cisco Devices

Cisco.com



- **Reachability**
  - Ping the device from the CiscoWorks server
- **SNMP Server enabled**
  - Read-only community string configured
  - Read-write community string configured
  - SNMP v3 optional – username/password/authorization algorithm configured
  - Credentials on device must match those used in CiscoView
- **Latest device package(s) installed on CiscoWorks server**





## System Requirements – Cisco Devices

CiscoView manages only Cisco devices. To find out if a particular device is supported by CiscoView, refer to the CiscoView Planner page at the following URL. First, go to Cisco.com and log in. Then, go to the following URL:

http://www.cisco.com/cgi-bin/Software/CiscoView/cvresult.cgi?product_class=All+Product+Types&product=All+Products&application=CiscoView+6.1

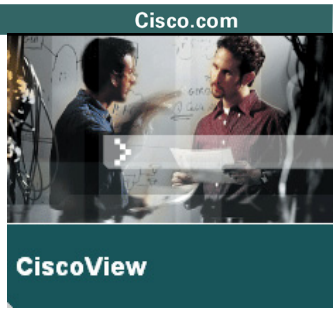
The following requirements must be met to successfully use CiscoView to manage the device:

- The management station cannot reach and successfully ping the device.
- The SNMP server may not be set in the device.
- The SNMP credentials are incorrect. Verify that the device attributes are correct in the CiscoWorks Device and Credential Repository (DCR). See *User Guide for CiscoWorks Common Services* for more information.
- The timeout value is too low in a busy network. Doubling the existing timeout value is a good starting point. Open the Device Preferences dialog box by either selecting *Administration > Device Preferences* from the CiscoView tab in the CiscoWorks homepage or clicking *Preferences* from the Options bar in the CiscoView desktop.
- The device package is not up-to-date. Check the CiscoView device packages and compare the date to the Cisco.com device package version. Upgrade the device package to the latest version, if required. Refer to Chapter 2 for more information on upgrading the device packages.

# Installation Guidelines

- System Requirements
- ➢ **Installation Guidelines**
- System Maintenance, Troubleshooting, & Preferences

# Installation Guidelines




## Simple Procedure

- ✓ Meet or exceed all CiscoWorks Common Services (CCS) v3.0 system requirements
- ✓ Successfully install the CCS prior to installing CiscoView

## Upgrading from Previous Releases

- ✓ CiscoView requires CiscoWorks Common Services (CCS) to be upgraded to the appropriate level
- ✓ Backup critical files before upgrading
- ✓ When upgrading from previous versions, ensure:
  - Current operating system (OS) is supported; if not, upgrade OS
  - OS patches or service packs are installed
- ✓ When upgrading, CiscoView does not save old preference setting and old device packages





# Installation Guidelines

### Simple Procedure

Installing CiscoView is straight forward. But before you install CiscoView, ensure that the system is ready and meets or exceeds all CiscoWorks Common Services (CCS) requirements. The required version of CCS must be installed first. All CiscoWorks applications in the LMS 2.5 release, including CiscoView v6.1, requires CCS v3.0.

### Upgrading From Previous Releases

Keep in mind that when upgrading that the CCS must be upgraded as well.

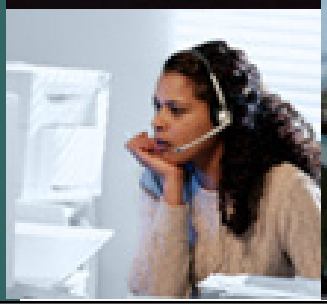
It is always a good idea to backup important files before upgrading. If there is a failure in the upgrade process or if you terminate the upgrade process, you cannot restore the old database.

Additionally, older versions of CiscoView may have been installed on older operating systems which may not be currently supported. Please reverify the hardware and system requirements prior to installing CiscoView.

When upgrading CiscoView, the preference settings and device packages from the previous version will not be saved.

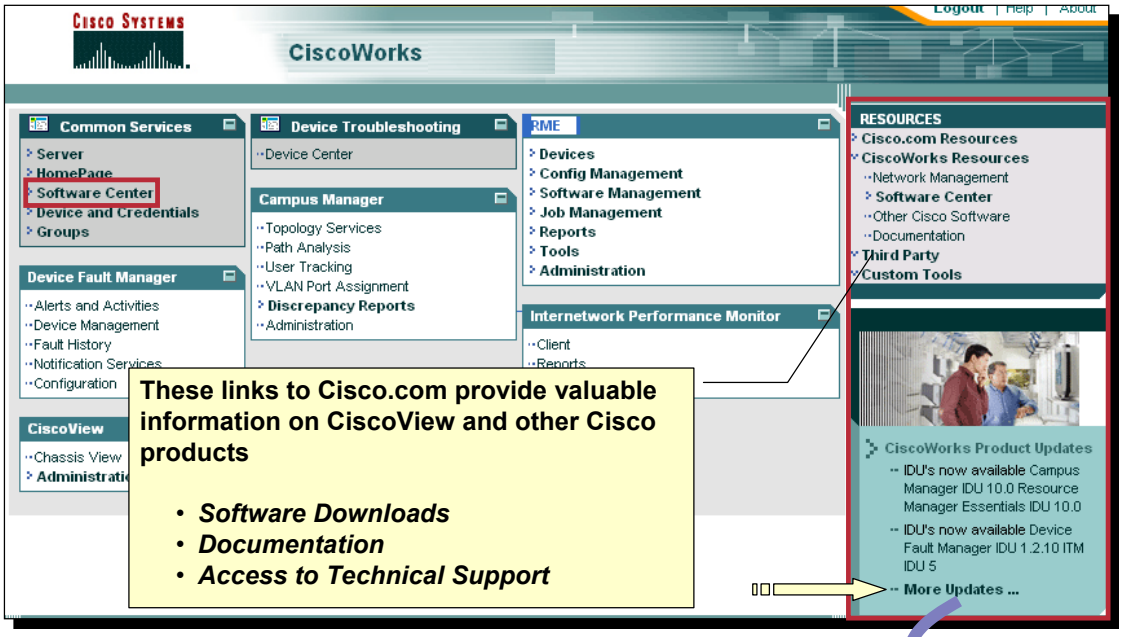
# System Maintenance, Troubleshooting & Preferences

- System Requirements
- Installation Guidelines
- ➢ **System Maintenance, Troubleshooting & Preferences**



# System Maintenance
## Server Updates

Cisco.com





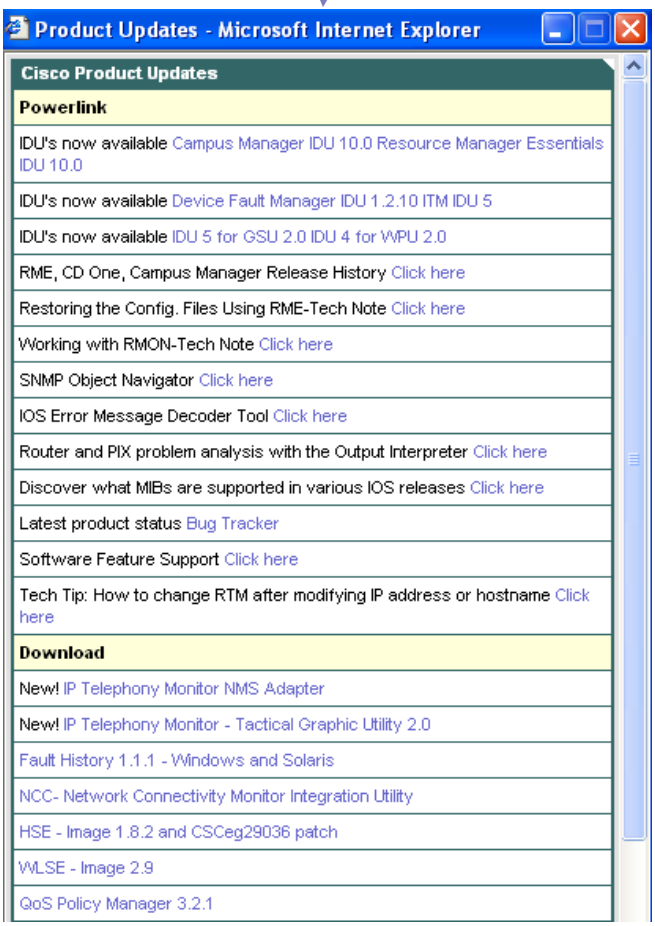



## Server Updates

The Resources section on the CiscoWorks desktop provides links for accessing additional information on CiscoView, other Cisco products, and other customized third party links and reference points.

By clicking on *More Updates*, you can obtain links to recently updated products, as illustrated in the upper figure, lower right corner.

Additionally, information about CiscoView software updates are available on Cisco's Website, by selecting *Common Services > Software Center Software Update* from the CiscoWorks homepage.



# Troubleshooting CiscoView

Cisco.com

## Test Connectivity & Credentials

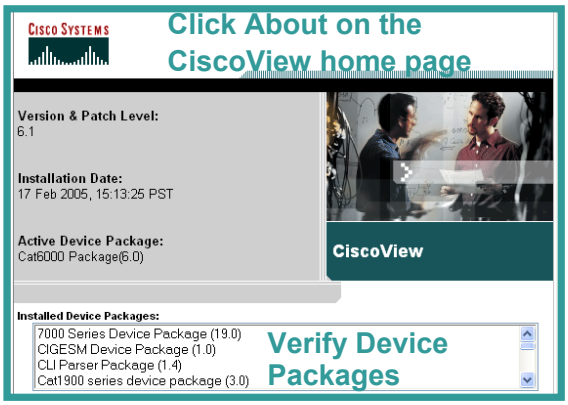
- ✓ Can you ping the device from the CiscoWorks server?
- ✓ Telnet to the server; verify SNMP credentials on the device with that used in CiscoView
- ✓ Modify SNMP timeout settings (see CiscoView preferences)

## Verify Device Packages

- ✓ Are the appropriate device packages installed?
- ✓ Are the devices packages out of date?

## View Debug and Trace Files

- ✓ Change the debug options to view every SNMP get/set command sent to the device







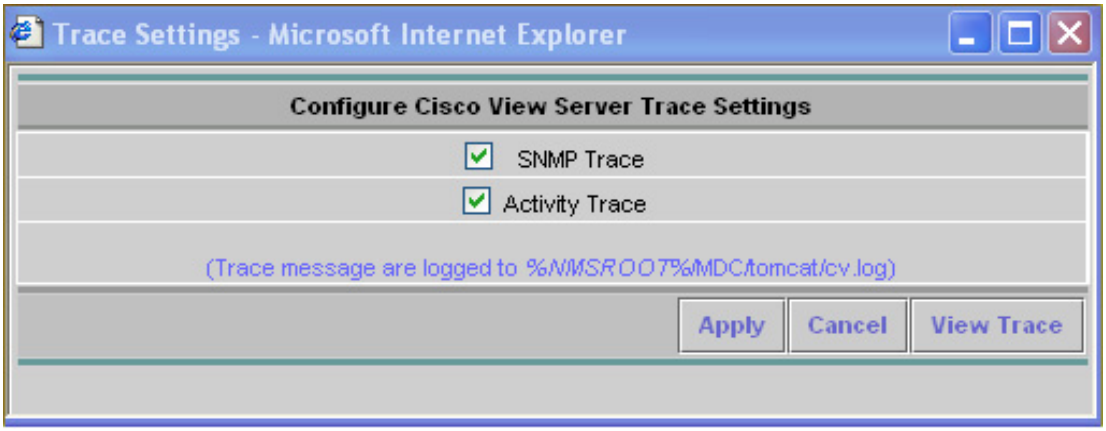


## Troubleshooting CiscoView

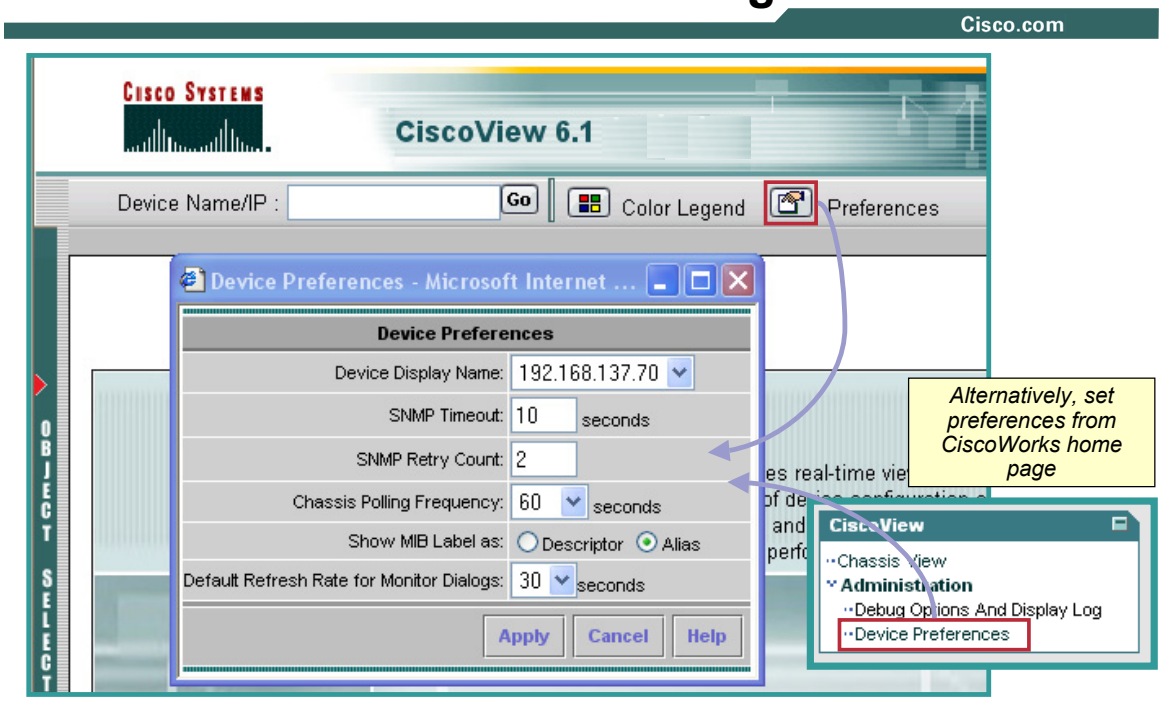
If you are having troubles with managing a supported Cisco device with CiscoView, start with the fundamentals. CiscoView is based on having IP connectivity to a Cisco device and using SNMP to get or set the various MIB variables defined in the device packages loaded on to the CiscoWorks server.

Verify the SNMP settings on the device and in CiscoWorks. Additionally, the CiscoView User Guide has an entire chapter on troubleshooting. A URL link to the User Guide can be found in Chapter 5 of this tutorial.

Additionally, a user could enable the debug options, and start a trace. Trace message are logged to *%NMSROOT%*/MDC/tomcat/cv.log. The trace file can be viewed from the GUI. Every SNMP get/set and activity using CiscoView can be logged and viewed.



# CiscoView Preference Settings








## CiscoView Preference Settings

There are two methods to change the system preferences for CiscoView:

- Click **Preferences** from the CiscoView main window, as illustrated above
- From the CiscoView area on the CiscoWorks homepage. Select **Administration > Device Preferences**, as illustrated above.

The following settings are available for changing:

- *Device Display Name* - Select the IP address of the device you want to set the preferences for
- *SNMP Timeout* - Enter a value (in seconds) in the field. This value represents the length of time that elapses before an SNMP request times out.
- *SNMP Retry Count* - Enter a value in the field. This value is the amount of times an SNMP request will be sent before the request times out.
- *Chassis Polling Frequency* - Select a value from the list. The default value varies by device. A typical value is every 60 seconds. CiscoView real-time status is based on periodic SNMP queries sent to the managed device. Reducing polling frequency (for example, from 10 seconds to 120 seconds) reduces SNMP-based traffic on the network and the workstation overhead required for processing.
- *Show MIB Label as* (defaults to Alias) - Click **Descriptor** to display MIB descriptors, for example, sysName. Click **Alias** to display textual labels, for example, System Name.
- *Default Refresh Rate for Monitor Dialogs* - Select a value from the list. The monitoring dialog is updated at the selected refresh rate.

14

Cisco.com

# Chapter 5

# References

**CiscoView v6.1**

# Reference Materials

Many Cisco reference documents have been created to help users understand the use of the CiscoWorks application, CiscoView. However, finding help and documentation can often be a challenge. This reference chapter has been created to assist you in your pursuit of additional product information. Below are links to documents and Web pages that provide further details on the CiscoView product.

- **CiscoView v6.1 Product Information**
  - **Data Sheet (URL)**

    www.cisco.com/en/US/products/sw/cscowork/ps4565/products_data_sheet0900aecd8021cced.html

  - **Documentation (URL)**

    www.cisco.com/en/US/partner/products/sw/cscowork/ps2406/products_user_guide_book09186a00800f6dd4.html

    - **User Guide**
    - **Installation Guide**
    - **Release Notes**
  - **Software Updates and Packages (URL)**

    www.cisco.com/cgi-bin/Software/CiscoView/cvplanner.cgi

- **Related Material**
  - **CiscoWorks LAN Management Solution (LMS) (URL)**

    Learn more about CiscoWorks solutions bundled in LMS:
    www.cisco.com/go/lms/

  - **CiscoWorks Common Service (CCS) v3.0 (URL)**

    Required for all CiscoWorks applications:
    http://www.cisco.com/en/US/products/sw/cscowork/ps3996/ps5672/index.html

  - **SNMP V3 (URL)**

    www.cisco.com/warp/public/759/ipj_1-3/ipj_1-3_snmpv3.html

  - **Cisco's SNMP Object Navigator (URL)**

    http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

- **Solaris Patches (URL)**

  To obtain the patches, contact your Sun Microsystems representative or download them from the Sun web site:
  sunsolve.sun.com/

- **LMS Documentation (URL)**
  www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_technical_documentation.html

  - **Quick Start Guide**
  - **Release Notes**

- **CiscoView Frequently Asked Questions (URL)**

  www.cisco.com/en/US/products/sw/cscowork/ps4565/products_qanda_item0900aecd8021ccfc.shtml

- **Online Bug Tracker (On Line URL)**

  Search for known problems on the Cisco bug tracking system tool, called Bug Toolkit. To access Bug Toolkit, perform the following steps:
  - Click on the link above (www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl)
  - Login to Cisco.com
  - Click ***Launch Bug Toolkit***.
  - Locate CiscoWorks Device Fault Manager from the list of Cisco Software Products
  - Then click ***Next***.

## Technical Notes / White Papers

- **Network Management Systems: Best Practices White Paper (URL)**

  http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a00800aea9c.shtml

  The objective of this paper is to provide some deployment guidelines for all areas of network management: Fault, Configuration, Accounting, Performance, and Security (FCAPS).

- **CiscoWorks LAN Management Solution White Papers (URL)**
  www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_white_papers_list.html

  - **LMS Deployment Guide**

    The objective of this paper is to review the steps to properly deploying the LMS suite of applications.

  - **Cost Analysis Using CiscoWorks LAN Management Solution**

    The CiscoWorks product family can provide a quantifiable financial and IT benefit to an organization, through the automation of routine labor, as well as helping to mitigate network degradation due to device failures. While it is difficult to derive an exact figure of the true and potential cost savings for every customer situation, the Cost Analysis Tool can provide an understanding of the scale of savings involved. At this point, the question that needs to be asked is not "What is the cost of the product?" but "What is the cost of NOT using CiscoWorks?"

# CiscoView v6.1 Tutorial

## Assessment Questions

Based on the information in the CiscoView product tutorial, please answer the following questions.

Q1) Cisco has bundled the CiscoView application into CiscoWorks management solutions. Which of the following bundles contain CiscoView? Choose two.

A) The LAN Management Solution (LMS)

B) The Enterprise Management Solution (EMS)

C) The Small Network Management Solution (SNMS)

D) The CiscoWorks Management Solution (CMS)

E) The WAN Management Solution (WMS)

Q2) All applications in a CiscoWorks management solution bundle require the CiscoWorks Common Services (CCS) software for runtime background processes, database access, and security services. Choose one.

A) True

B) False

Q3) CiscoView uses which protocol to retrieve real-time statistics from a Cisco device? Choose one.

A) MIB (Management Information Base)

B) CLI (Command Line Interface)

C) Telnet

D) SNMP (Simple Network Management Protocol)

E) CDP (Cisco Discovery Protocol)

Q4) CiscoView requires the Java Plug-in to be installed in the client's web browser. Choose one.

A) True

B) False

Q5) Which of the following provides CiscoView with knowledge of what features can be configured using CiscoView, what statistics are available for polling, and how to display the device in CiscoView? Choose one.

A) Device credentials

B) CiscoView preferences

C) CiscoView config.dat file

D) Device packages

E) A text file that the system administrator loads during install

Q6) Which of the following CiscoWorks user roles allow the CiscoView user to change the configuration of a device? Choose all that apply.

A) System Administrator

B) Network Administrator

C) Network Operator

D) Approver

E) Help Desk

Q7) CiscoView v6.1 supports which of the following versions of SNMP. Choose one.

A) SNMP v1

B) SNMP v2

C) SNMP v3

D) SNMP v1 and v2

E) All of the above

Q8) CiscoView can be used to monitor interfaces and device statistics. Which of the following statements are true? Choose all that apply.

A) The statistics are polled real-time and not stored in a database

B) The polling interval can be varied from 5 to 100 seconds

C) Once the monitoring window is closed the statistics polled are lost

D) Up to 25 data points can be displayed in the polling graph

E) All of the above are true

Q9) Which of the following are components that can be selected in the Chassis View for configuration and monitoring by CiscoView? Choose all that apply.

A) Single interface

B) Multiple interfaces

C) Supervisor card

D) Network modules

E) Device chassis

F) Power Supply

G) All of the above

Q10) Which of the following colors reflect that a port is dormant, meaning that the interface cannot pass packets, but is in a pending state, waiting for some external event to place it in the Up state, for example, a remote system establishing a connection to the interface or dialing up to a SLIP server? Choose one.

A) Cyan

B) Orange

C) Red

D) Purple

E) Green

# CiscoView v6.1 Tutorial

## Assessment Answers

Based on the information in the CiscoView product tutorial, please answer the following questions.

Q1) Cisco has bundled the CiscoView application into CiscoWorks management solutions. Which of the following bundles contain CiscoView? Choose two.

A) The LAN Management Solution (LMS)

B) The Enterprise Management Solution (EMS)

C) The Small Network Management Solution (SNMS)

D) The CiscoWorks Management Solution (CMS)

E) The WAN Management Solution (WMS)

Q2) All applications in a CiscoWorks management solution bundle require the CiscoWorks Common Services (CCS) software for runtime background processes, database access, and security services. Choose one.

A) True

B) False

Q3) CiscoView uses which protocol to retrieve real-time statistics from a Cisco device? Choose one.

A) MIB (Management Information Base)

B) CLI (Command Line Interface)

C) Telnet

D) SNMP (Simple Network Management Protocol)

E) CDP (Cisco Discovery Protocol)

Q4) CiscoView requires the Java Plug-in to be installed in the client's web browser. Choose one.

A) True

B) False

Q5) Which of the following provides CiscoView with knowledge of what features can be configured using CiscoView, what statistics are available for polling, and how to display the device in CiscoView? Choose one.

A) Device credentials

B) CiscoView preferences

C) CiscoView config.dat file

D) Device packages

E) A text file that the system administrator loads during install

Q6) Which of the following CiscoWorks user roles allow the CiscoView user to change the configuration of a device? Choose all that apply.

A) System Administrator

B) Network Administrator

C) Network Operator

D) Approver

E) Help Desk

Q7) CiscoView v6.1 supports which of the following versions of SNMP. Choose one.

A) SNMP v1

B) SNMP v2

C) SNMP v3

D) SNMP v1 and v2

E) All of the above

Q8) CiscoView can be used to monitor interfaces and device statistics. Which of the following statements are true? Choose all that apply.

A) The statistics are polled real-time and not stored in a database

B) The polling interval can be varied from 5 to 100 seconds

C) Once the monitoring window is closed the statistics polled are lost

D) Up to 25 data points can be displayed in the polling graph

E) All of the above are true

Q9) Which of the following are components that can be selected in the Chassis View for configuration and monitoring by CiscoView? Choose all that apply.

A) Single interface

B) Multiple interfaces

C) Supervisor card

D) Network modules

E) Device chassis

F) Power Supply

G) All of the above

Q10) Which of the following colors reflect that a port is dormant, meaning that the interface cannot pass packets, but is in a pending state, waiting for some external event to place it in the Up state, for example, a remote system establishing a connection to the interface or dialing up to a SLIP server? Choose one.

A) Cyan

B) Orange

C) Red

D) Purple

E) Green