



Newer Cisco SBA for Government Guides Available

This guide is part of an older series of Cisco Smart Business Architecture for Government. To access the latest Cisco SBA for Government Guides, go to <http://www.cisco.com/go/govsba>

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.





SBA
FOR
GOVT

MIDSIZE

BORDERLESS
NETWORKS

Ipswitch Network Management Guide



● ● ● SBA FOR GOVERNMENT

The Purpose of This Guide

This guide is a concise reference on the Ipswitch WhatsUp Gold family of Network Management products.

The first section will introduce you to the products, including their features and benefits. Then, it will guide you through the deployment process.

Related Documents

Before reading this guide

- BN** Foundation Design Overview
- BN** Foundation Deployment Guide
- BN** Foundation Configuration Guide
- DC** Data Center Deployment Guide

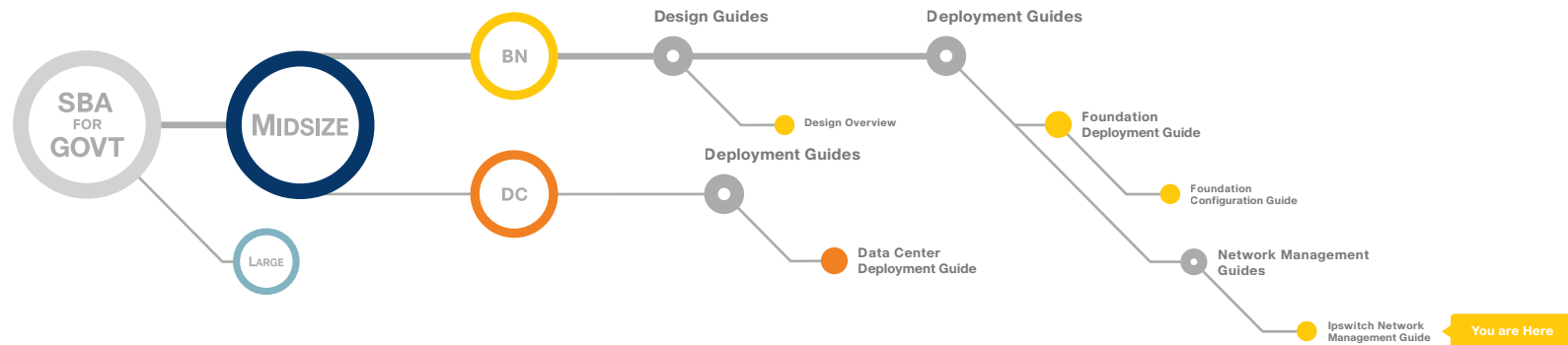


Table of Contents



- SBA Overview 1**
 - Guiding Principles 1
- Introduction..... 2**
- WhatsUp Gold Product Overview 4**
 - WhatsUp Gold Premium 4
 - WhatsUp Flow Monitor 4
 - WhatsConnected 5
 - WhatsConfigured 5
 - Additional Tools..... 5
- Deploying WhatsUp Gold 7**
- Appendix A: WhatsUp Gold Product Summary..... 15**
- Appendix B: SBA for Midsize Agencies Document System..... 16**

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental. Cisco Unified Communications SRND (Based on Cisco Unified Communications Manager 7.x)

© 2010 Cisco Systems, Inc. All rights reserved.

SBA Overview

The Cisco® Smart Business Architecture (SBA) for Government is a comprehensive design for networks with up to 1000 users. This out-of-the-box design is simple, fast, affordable, scalable, and flexible.

The Cisco SBA for Midsize Agencies incorporates LAN, WAN, wireless, security, WAN optimization, and unified communication technologies tested together as a solution. This solution-level approach simplifies the system integration normally associated with multiple technologies, allowing you to select the modules that solve your agency's problems rather than worrying about the technical details.

We have designed the Cisco SBA to be easy to configure, deploy, and manage. This architecture:

- Provides a solid network foundation
- Makes deployment fast and easy
- Accelerates ability to easily deploy additional services
- Avoids the need for re-engineering of the core network

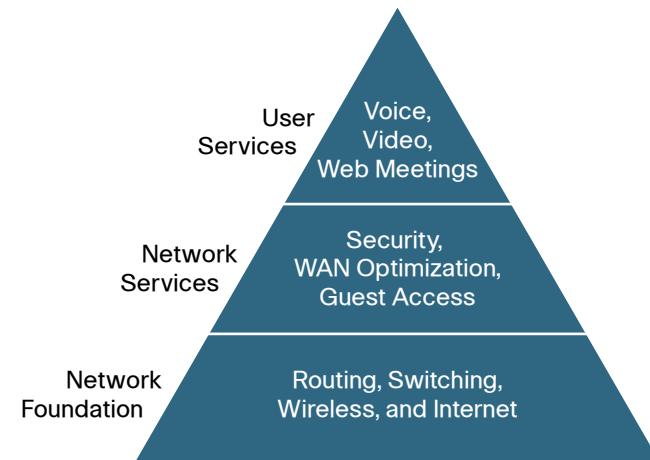
By deploying the Cisco SBA, your agency can gain:

- A standardized design, tested and supported by Cisco
- Optimized architecture for midsize agencies with up to 1000 users and up to 20 remote sites
- Flexible architecture to help ensure easy migration as the agency grows
- Seamless support for quick deployment of wired and wireless network access for data, voice, teleworker, and wireless guest
- Security and high availability for agency information resources, servers, and Internet-facing applications
- Improved WAN performance and cost reduction through the use of WAN optimization
- Simplified deployment and operation by IT workers with CCNA® certification or equivalent experience
- Cisco enterprise-class reliability in products designed for midsize agencies

Guiding Principles

We divided the deployment process into modules according to the following principles:

- **Ease of use:** A top requirement of Cisco SBA was to develop a design that could be deployed with the minimal amount of configuration and day-two management.
- **Cost-effective:** Another critical requirement as we selected products was to meet the budget guidelines for midsize agencies.
- **Flexibility and scalability:** As the agency grows, so too must its infrastructure. Products selected must have the ability to grow or be repurposed within the architecture.
- **Reuse:** We strived, when possible, to reuse the same products throughout the various modules to minimize the number of products required for spares.



The Cisco SBA can be broken down into the following three primary, modular yet interdependent components for the midsize agency.

- **Network Foundation:** A network that supports the architecture
- **Network Services:** Features that operate in the background to improve and enable the user experience without direct user awareness
- **User Services:** Applications with which a user interacts directly

Introduction

Network and application infrastructures have become some of the most critical elements in an agency's strategy. High reliance on network or application availability requires that all agencies, from small and medium agencies to large agencies, take a proactive approach to preventing or resolving outages with minimal impact to productivity and revenue. The Ipswitch WhatsUp Gold product family leverages a powerful, yet affordable, easy-to-deploy and use, network tools suite that ensures you always know the pulse of the network so you can respond quickly to changes.

When combining the reliability of Cisco hardware with the value of WhatsUp Gold, you can be confident that you have the tools to manage your network easily and reliably.

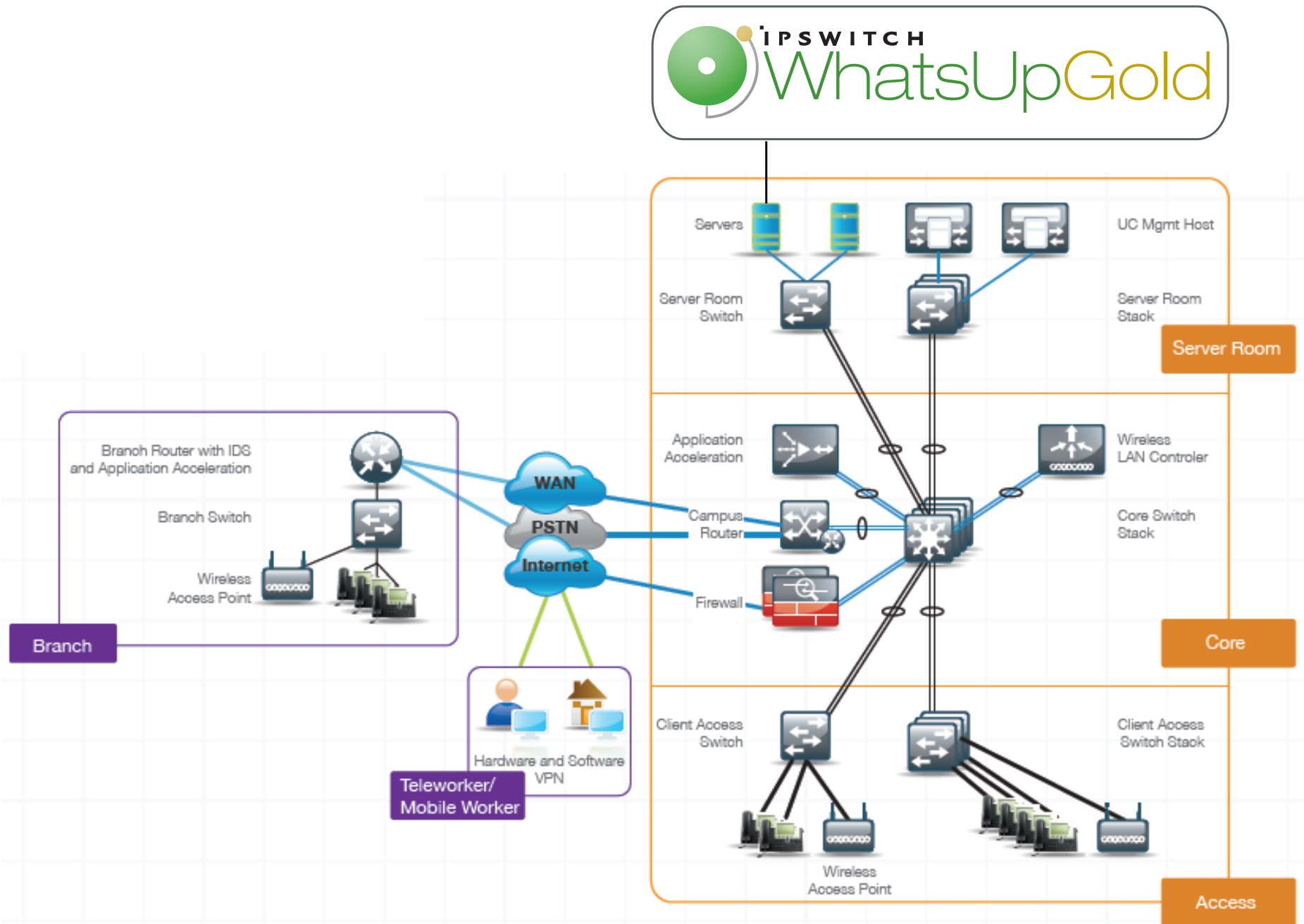
With the Cisco SBA for Midsize Agencies—Borderless Networks, you can increase your profits and reduce the time you spend selling to customers in the 250-1,000 user market segment. The Cisco SBA for Midsize Agencies—Borderless Networks offers Partners valuable network design and deployment best practices, helping you grow a profitable Cisco practice and deliver a superior end-user experience that includes switching, routing, wireless, WAN optimization, and security technologies, combined with comprehensive management capabilities for the entire system. It also includes modular components that allow you to build in unified communications and data center components for advanced customer requirements.

The modular design of the architecture means that you can add technologies when the customer is ready to deploy them. It also provides Cisco-tested configurations and topologies which CCNA-level engineers can use for design and installation, and to support customer needs.

Cisco offers a number of options to provide Network Management capabilities. This guide is focused on our partnership with Ipswitch and the WhatsUp Gold line of products that meet Cisco's goal to deliver affordable, easy-to-use network management.

Notes

Figure 1. Ipswitch WhatsUp Gold Integration in the SBA



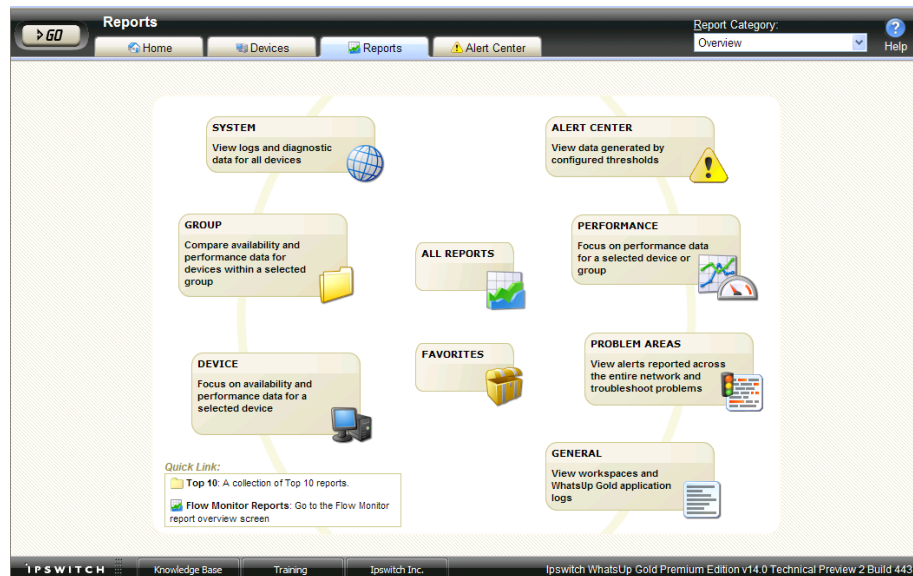
WhatsUp Gold Product Overview

This network management module deploys the following four primary WhatsUp Gold products.

WhatsUp Gold Premium

WhatsUp Gold Premium monitors, reports, alerts, and takes action on the status of network devices, the system, and services. WhatsUp Gold installs, discovers, and maps network connected assets in minutes. Leveraging SNMP v1/2/3 and WMI, it enables predictive monitoring in combination with powerful alerting and notification capabilities to keep you informed when issues arise and to keep the network infrastructure running smoothly. Intuitive Web-enabled workspace reports and dashboards provide quick navigation to over 200 reports, documenting all device, bandwidth and application-related activity. WhatsUp Gold ensures network managers have 360° visibility, actionable intelligence and complete control to make smarter decisions faster.

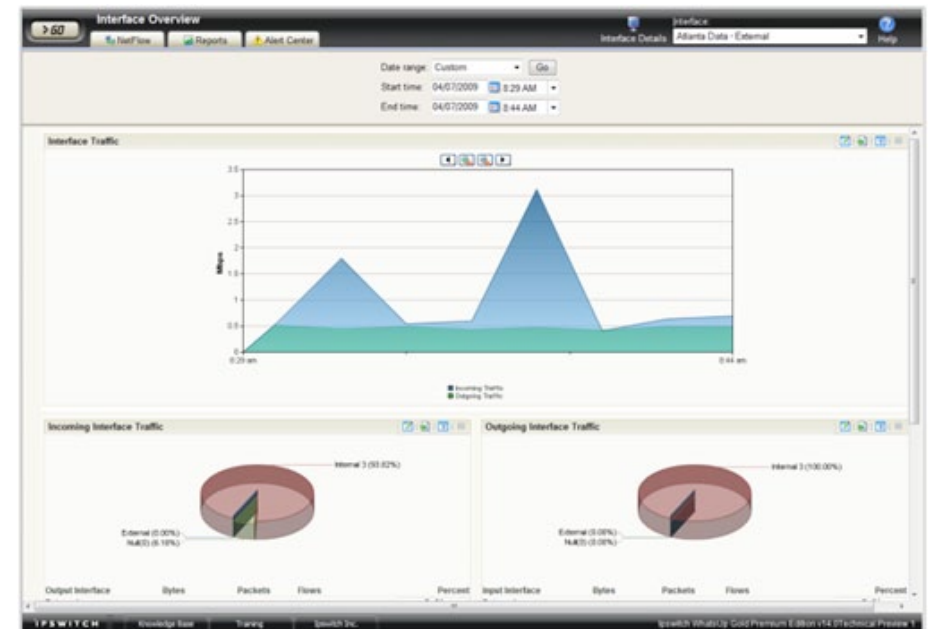
Figure 2. WhatsUp Gold Premium



WhatsUp Flow Monitor

This plug-in for WhatsUp Gold leverages Cisco NetFlow enabled switches, routers, and Adaptive Security Appliances (ASA) to gather, analyze, report, and alert on LAN/WAN network traffic patterns and bandwidth utilization in real-time. It highlights not only overall utilization for the LAN/WAN, specific devices, or interfaces; it also indicates users, applications, and protocols that are consuming abnormal amounts of bandwidth. WhatsUp Flow Monitor protects network security by detecting virus and worm activity on the network. Comprehensive reporting takes the raw real-time network traffic data from routers and switches and presents you with useful information to understand trends, utilization, and where network bandwidth is consumed.

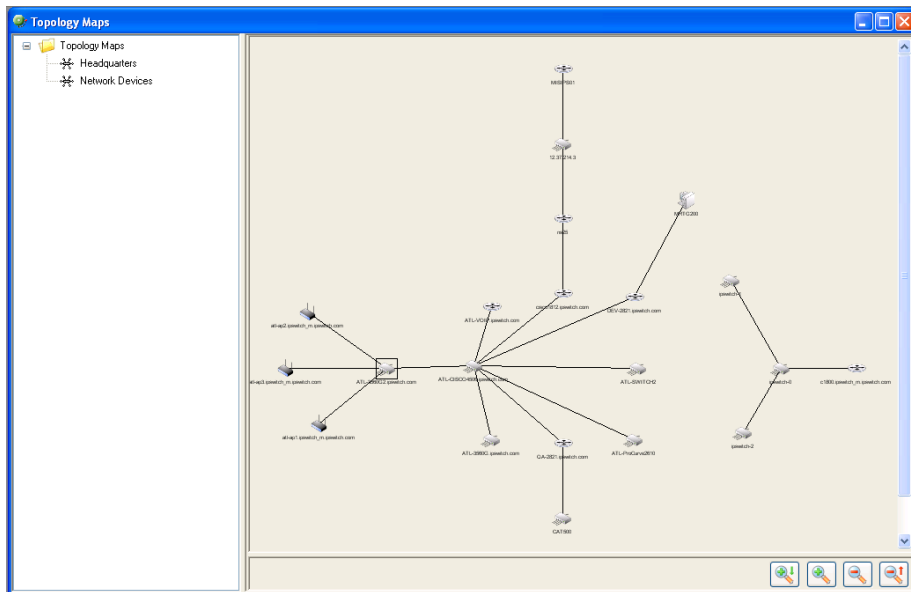
Figure 3. WhatsUp Flow Monitor



WhatsConnected

WhatsConnected is a plug-in for WhatsUp Gold that provides layer 2/3 network discovery and topology mapping to visually depict device connectivity down to the individual port. It also employs deep device scanning that provides detailed information about discovered devices in a simple device list view, a device category view, and a detailed topology view. You can publish any of the network maps as a network diagram in Microsoft® Visio™ or export detailed device information to WhatsUp Gold to automate the creation of detailed network topology map views. WhatsConnected also includes Layer 2 Trace and IP/MAC Finder tools to validate connection paths and report real-time availability data on devices.

Figure 4. What'sConnected



WhatsConfigured

As a fully integrated plug-in for WhatsUp Gold, WhatsConfigured automates the key configuration and change management tasks required to maintain and control configuration files for networking devices, reducing the risk of network outages caused by misconfigured devices. You can leverage automated configuration to reduce the time you spend ensuring network devices are configured correctly, freeing valuable time.

Additional Tools

WhatsVirtual

This plug-in provides additional capabilities to discover, map, monitor, alert, and report on virtual environments in WhatsUp Gold. One discovery scan can discover both virtual and physical devices. In Device View, virtual devices are displayed alongside physical devices. For each virtual host discovered, a group is created for the virtual host and all of its associated virtual machines. Leveraging the VMWare API, WhatsVirtual enables the same predictive monitoring and powerful alerting and notification capabilities of WhatsUp Gold to keep you informed when issues arise and to keep the network infrastructure running smoothly.

VoIP Monitor

This is a plug-in for WhatsUp Gold that measures your network's ability to provide the quality of service (QoS) necessary for VoIP calls on your LAN and WAN links. After a simple setup, the VoIP Monitor accesses Cisco IP SLA (Service Level Agreement) enabled devices to monitor VoIP performance and quality parameters including jitter, packet loss, and latency. The plug-in's full integration with WhatsUp Gold allows you to easily view graphs and metrics for bandwidth and interface utilization and troubleshoot network issues that affect VoIP performance.

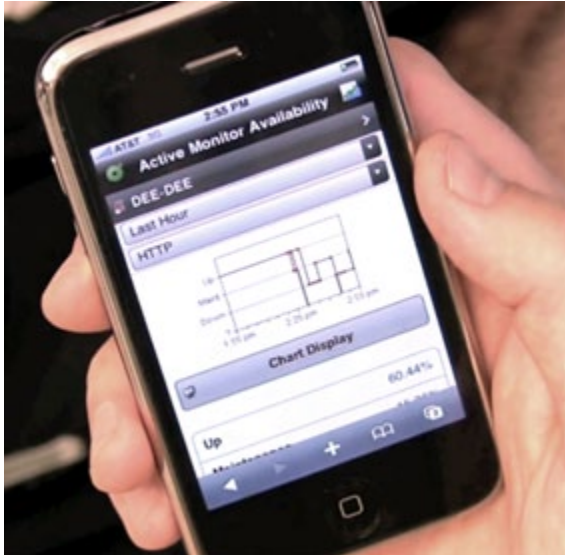
Dashboard

Dashboard is included free with WhatsUp Gold Premium and is a stand-alone application designed to complement WhatsUp Gold with increased visibility into network status. Dashboard runs on either single or multiple display panels and cycles through report pages on the WhatsUp Gold Web interface. This capability provides network administrators a dynamic, self-updating means with which to display and view their important network information. Additionally, Dashboard provides the capability to display data for multiple networks, allowing administrators to view data for multiple networks simultaneously.

Mobile Interface

This feature is included free with WhatsUp Gold Premium and Distributed editions to provide mobile access to the WhatsUp Gold network management application. You can conveniently view your network status from a mobile device at anytime. This WhatsUp Gold feature ensures that you are informed about network issues so that you can maintain critical network performance. The Mobile Interface supports mobile devices such as the iPhone, Blackberry, and other popular mobile devices.

Figure 5. Mobile Interface

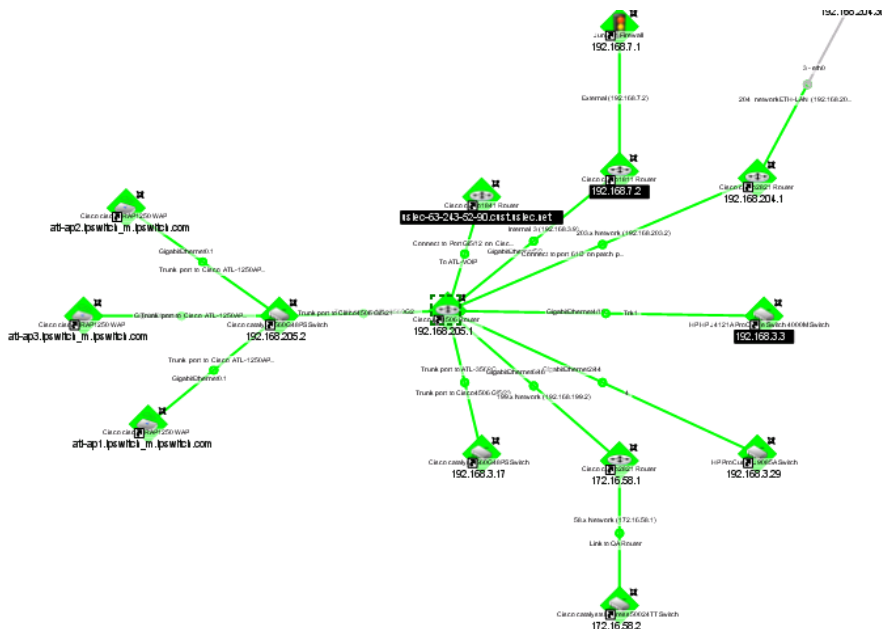


Notes

Deploying WhatsUp Gold

This document organizes the tasks necessary to deploy WhatsUp Gold to manage Cisco SBA for Midsize Agencies—Borderless Networks into four stages. The time required to execute each stage is less than an hour. It is feasible to complete all four stages on a single day.

Figure 6. Topology Map



Process

Preparing the Network

1. Download and Install WhatsUp Gold
2. Enable SNMP on Key Cisco Devices
3. Configure NetFlow on Key Cisco Devices

Procedure 1

Download and Install WhatsUp Gold

The installation program includes the evaluation license and activates automatically.

The installation program for WhatsUp Gold bundles and delivers all of the prerequisites of the application, including Microsoft .NET Framework 3.5, Microsoft SQL Server 2005 Express Edition, and Ipswitch Web Server.

Step 1: Download an evaluation copy of WhatsUp Gold and all available plug-ins from WhatsUpGold.com.



Tech Tip

You don't have to use the bundled Microsoft SQL Server 2005 Express Edition or Ipswitch Web Server with WhatsUp Gold. You can also install WhatsUp Gold to use an existing installation of Microsoft SQL Server 2005 or Microsoft SQL Server 2008 as its data store, and you can use Microsoft Internet Information Services (IIS) as its Web server.

For more information on specific installation steps, consult the WhatsUp Gold release notes, which you can access from the first screen of the installation program.

Procedure 2 Enable SNMP on Key Cisco Devices

WhatsUp Gold uses SNMP to determine the manufacturer and model, components (such as fans, CPUs, and hard disks), operating system, and specific services (such as HTTP or DNS) of each device.

Step 1: We recommend configuring important devices to respond to SNMP requests.

Tech Tip

For information about how to enable SNMP on Cisco devices, see the *Cisco SBA for Midsize Agencies—Borderless Networks Foundation Deployment Guide*.

Procedure 3 Configure NetFlow on Key Cisco Devices

To monitor network bandwidth utilization, WhatsUp Gold Flow Monitor collects NetFlow data exported from network devices. Flow Monitor accepts NetFlow version 1, 5, and 9.

Step 1: Apply the following example, which shows the command line interface commands required to enable NetFlow exports for devices on which you want to enable network bandwidth monitoring.

```
ip flow-export version 9
ip flow-export destination 192.168.28.4 9999
```

Tech Tip

Instead of 192.168.28.4, use the IP address of the WhatsUp Gold server.

Step 2: In addition, configure each interface to export data to WhatsUp Gold Flow Monitor. Enter the following at the command line:

```
ip flow ingress
OR
ip flow egress
```

Step 3: If the device exporting Flow data is also performing network address translation (NAT), we recommend exporting egress data from the internal interface so that private network addresses are displayed in Flow Monitor reports. Any other configuration results in all private addresses reporting as the public addresses of the device performing the network address translation. WhatsUp Gold Flow Monitor automatically begins tracking network bandwidth utilization when it receives NetFlow data.

Process

Discovering and Mapping the Network

1. Run the Quick Setup Assistant
2. Configure Action Policies
3. Customize Device Roles
4. Discover the Network
5. Map the Network

Procedure 1 Run the Quick Setup Assistant

The Quick Setup Assistant guides you through the initial configuration that is necessary for WhatsUp Gold to discover network devices. You can use the Quick Setup Assistant to configure the connection to your mail server and set up the default email address for email notifications.

Most importantly, the Quick Setup Assistant collects information about your SNMP communities and other credential types, such as VMware for the WhatsVirtual plug-in, and TFTP and SSH credentials for the WhatsConfigured plug-in.

Step 1: Run the Quick Setup Assistant.

Step 2: Enter each community that you configured during the Global Configuration module. The Quick Setup Assistant automatically generates SNMPv1 and SNMPv2 credentials for each community entered.

Procedure 2 Configure Action Policies

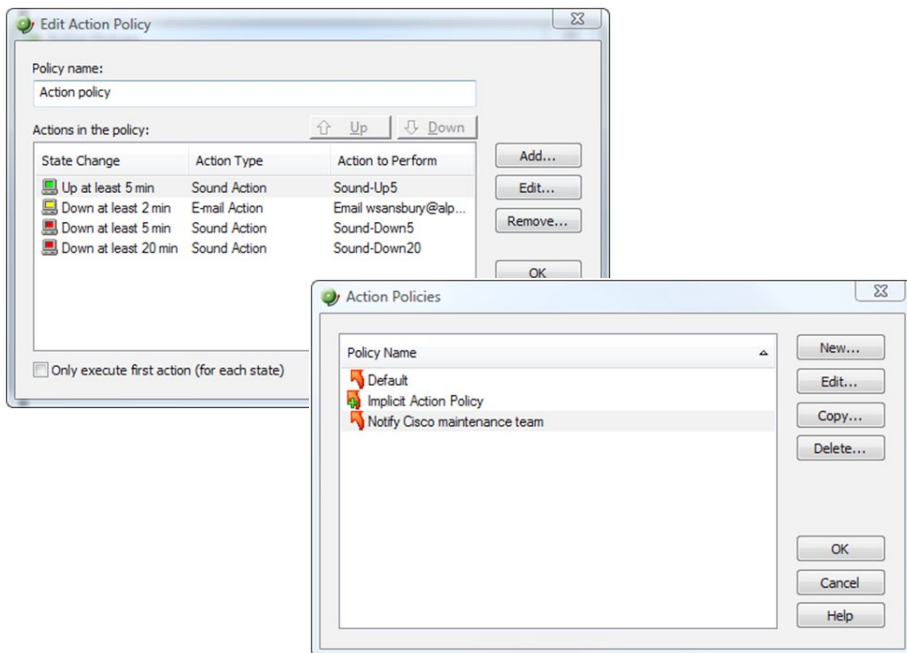
Action policies are sets of rules WhatsUp Gold uses to determine what actions it takes when it detects network issues. By default, WhatsUp Gold creates an action policy that sends email notifications to the address you specified in the Quick Setup Assistant and applies it to all discovered devices.

Action policies are primarily used to send notifications via email, SMS, and pager, but actions can also be used to write events to common logs, restart Windows services, set SNMP values, and run custom programs and scripts.

Step 1: If you want WhatsUp Gold to take other actions when issues are detected on devices, configure additional action policies.

Action policies can be applied to specific devices automatically when they match a device role (such as an action policy that is applied automatically to all routers).

Figure 7. Action Policies



Procedure 3 Customize Device Roles

When WhatsUp Gold discovers devices, it tries to determine the type of device so that it can monitor devices appropriately by comparing the discovered attributes of the device to a set of criteria called a device role.

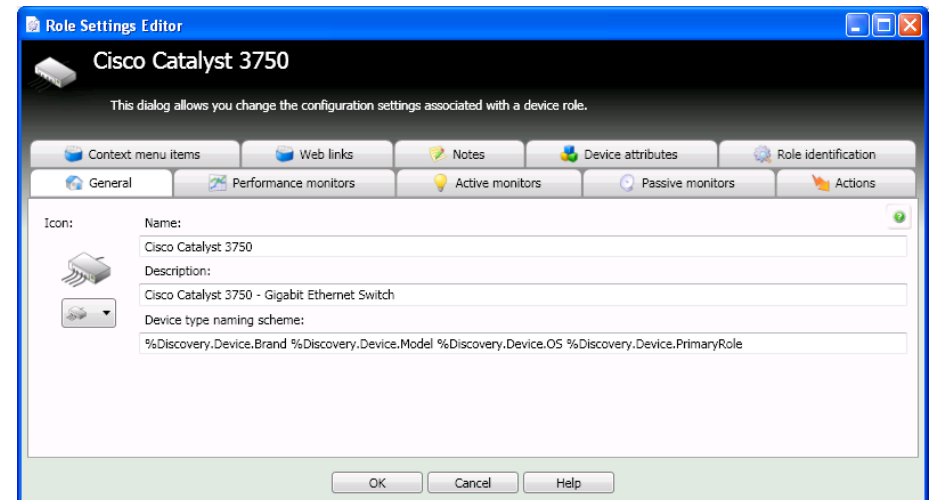
Device roles do two things:

- Specify the criteria that a device must match to be identified as the device role
- Specify the monitoring configuration that is applied to the device when it is added to WhatsUp Gold

WhatsUp Gold provides several default device roles that are used to identify most common network devices. These default roles correctly identify the majority of the devices in the Cisco SBA for Midsize Agencies—Borderless Networks, but you can modify the device roles to customize what is monitored on each device and what action policy is applied. In addition, you can create new device roles to specify how WhatsUp Gold monitors and reports on devices it does not natively recognize.

Step 1: At a minimum, we recommend creating a device role for any IP telephony device on your network.

Figure 8. Role Settings Editor



Tech Tip

When you create a device role for IP telephony devices, you can automatically assign the VoIP Monitor, which gauges IP telephony performance using Cisco's IP SLA. If you use this option, additional configuration is needed on the IP SLA responder and source devices.

Procedure 4 Discover the Network

After you have configured the network devices and the customized device roles, you can discover the network using WhatsUp Gold.

Step 1: We recommend using the SNMP Smart Scan option to discover the network. Enter an IP address of the Core router and an IP address of each Branch router as seed addresses, and specify a Scan Depth of 2.

When you start the discovery session, WhatsUp Gold begins scanning the network and identifying physical devices and virtual devices (if WhatsVirtual is installed). Discovered devices are added to the list in the Devices Discovered pane. As each device is scanned, additional information about it becomes available, such as the device brand, model, and operating system. Based on what is discovered about each device, WhatsUp Gold designates a device role.

Step 2: After all devices are discovered, click "Add completed devices to WhatsUp Gold" to add the discovered devices to a device group and map.

Figure 9. Devices Discovered

The screenshot shows the 'WhatsUp Gold Discovery Console' window. It features a 'Progress Summary' pane on the left and a 'Devices Discovered' table on the right. The 'Progress Summary' pane includes sections for 'Device Summary', 'Network Traffic', 'Session Metrics', and 'Session Settings'. The 'Devices Discovered' table lists various devices with columns for Host Name, Address, Brand, Model, Operating System, Role, Status, and Progress. A progress bar at the bottom indicates 100.00% completion. Below the table, there is a 'Device Information' section for a selected device, showing details like Name, Location, Contact, Description, and CPUs.

Device Summary	
Device Limit	Unlimited
Existing Devices	211
Discovered Devices	224

Network Traffic	
SNMP Bytes (in/out)	4630906 / 3726400
PDU (in/out)	53493 / 54843

Session Metrics	
Scan Start	6/2/2009 5:59:26 AM
Scan End	6/2/2009 6:07:20 AM
Elapsed Time	00:07:53

Session Settings	
Scan Type	Smart
SNMP Credentials	(4 / 4)
Windows Credentials	(0 / 0)

Devices Discovered							
Host Name	Address	Brand	Model	Operating System	Role	Status	Progress
192.168.3.18	192.168.3.18	Cisco	catalyst3560G4PS	IOS	Switch	complete	Saved/Updated
atl-disco4506.ipswitch_m...	192.168.3.1	Cisco	cat4506	IOS	Router	complete	Saved/Updated
192.168.203.1	192.168.203.1	Cisco	cat4506	IOS	Router	complete	Saved/Updated
192.168.199.1	192.168.199.1	Cisco	cat4506	IOS	Router	complete	Saved/Updated
192.168.2.1	192.168.2.1	Cisco	cat4506	IOS	Router	complete	Saved/Updated
192.168.205.1	192.168.205.1	Cisco	cat4506	IOS	Router	complete	Saved/Updated
atl-esxi.ipswitch_m.ipswit...	192.168.3.178			Windows Vista	Web server	complete	Saved/Updated
192.168.3.176	192.168.3.176			Windows Vista	FTP server	complete	Saved/Updated
atl-wsantbury.ipswitch_m...	192.168.3.179			Windows Vista	Web server	complete	Saved/Updated
DELPHI	192.168.3.182			Windows Vista	Web server	complete	Saved/Updated
BACOHUS	192.168.3.180			Windows Vista	Web server	complete	Saved/Updated
192.168.3.177	192.168.3.177			Windows 7	Web server	complete	Saved/Updated
atl-rdp1.ipswitch_m.ipswit...	192.168.3.168			Windows XP	Email server	complete	Saved/Updated
JI-TEST	192.168.3.164			Windows Vista	FTP server	complete	Saved/Updated
atl-rdp2.ipswitch_m.ipswit...	192.168.3.169			Windows XP	Email server	complete	Saved/Updated
ATL175	192.168.3.175			Windows XP	Email server	complete	Saved/Updated
ATL-RDP3	192.168.3.173			Windows XP	Email server	complete	Saved/Updated
atl-jslaRozsky.ipswitch_m...	192.168.3.184			Windows Vista	Web server	complete	Saved/Updated

Progress: 100.00 %

Device Information

Name: ATL-3560G2.ipswitch.com
 Location: Atlanta-Server Room
 Contact: Shawn Ayton
 Description: Cisco IOS Software, C3560 Software (C3560-IPBASE-M), Version 12.2(50)SE, RELEASE SOFTWARE (fc1)
 Copyright (c) 1986-2009 by Cisco Systems, Inc.
 Compiled Fri 27-Feb-09 22:41 by wellu
 CPUs: 1

When VMWare hosts are discovered with the WhatsVirtual plug-in, after you click "Add completed devices to WhatsUp Gold", the VMWare hosts are listed in the Device View, VMWare Hosts folder in the Dynamic Group Examples. Double-click a VMWare Host to view the associated virtual machines.

Tech Tip

The default username and password are admin/ironport.

Procedure 5 Map the Network

After devices are added to WhatsUp Gold, you can alternately configure a topology map with WhatsConnected. These network topology maps provide an easy and fast way to browse the network infrastructure and display physical connections between devices. It simplifies the day-to-day complexities of managing and quickly resolving network issues.

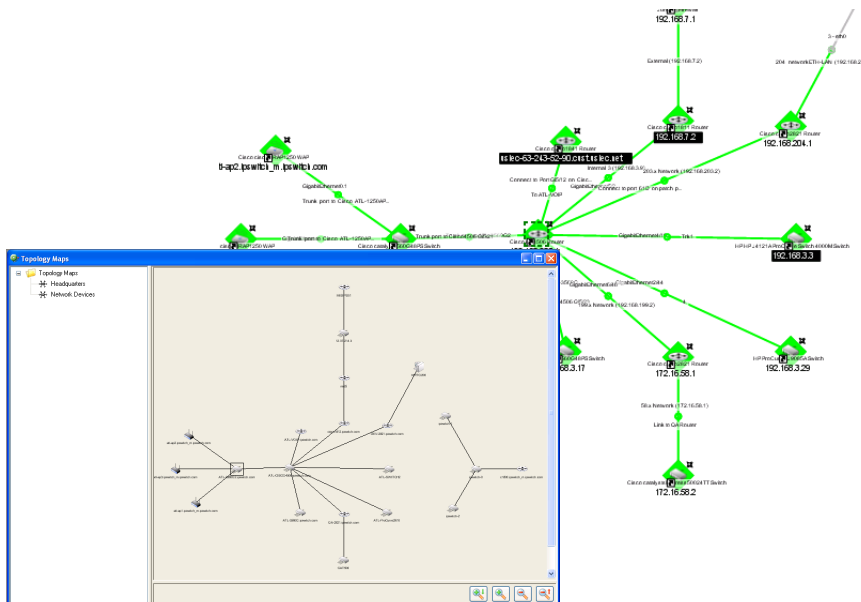
Unlike other topology mapping solutions that simply overlay devices on a topology bitmap or Visio drawing, WhatsConnected scans your network using industry-standard protocols (such as ICMP, SNMP and LLDP) to automatically create Layer 2 topology maps of your network segments. WhatsConnected provides a simple solution to actively monitor network devices from a topology map view.

When combined with WhatsUp Gold, WhatsConnected provides a complete solution for monitoring the devices on your network and their topology, both physical and virtual.

Step 1: After the map has been created, export it from WhatsConnected to WhatsUp Gold.

You can also export the topology maps to Microsoft Visio, making documenting your network topology nearly effortless.

Figure 10. Topology Map



Process

Customizing Reports

1. Set Up Workspace Views
2. Customize Device Status Reports
3. Configure Alert Center Thresholds

Procedure 1 Set up Workspace Views

You can group collections of reports into pages called Workspace Views. You can create Workspace Views to give you quick and personalized dashboard-style overviews of the health of portions of your network.

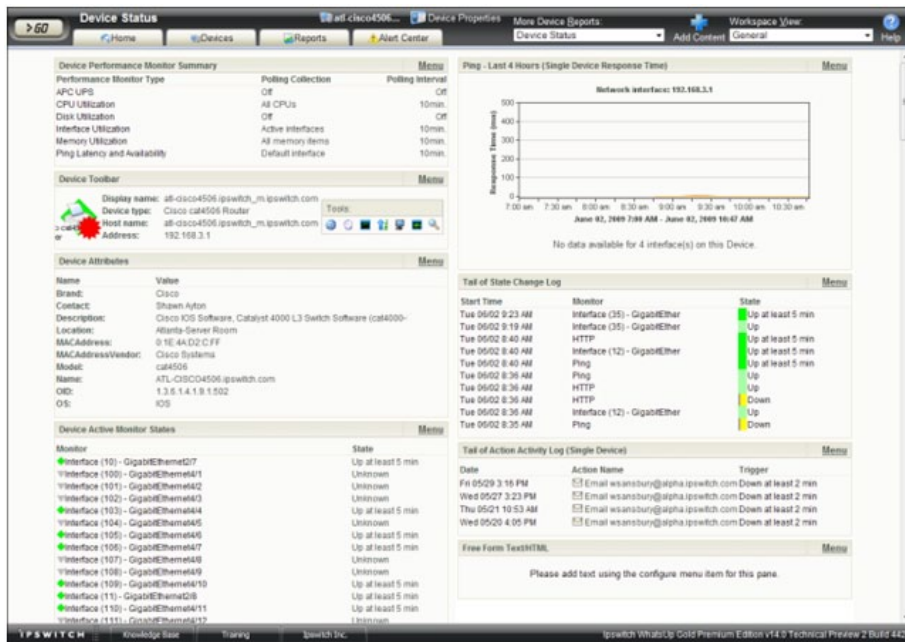
Figure 11. Workspace View



Step 1: Creating a Workspace View to show the health of the Server Room, Core, Access, and Branch portions of the Cisco Smart Architecture for Midsized Networks.

Step 2: You may also want to create Workspace Views that show the statuses of different types of devices, such as a Routers, Switches, Virtual Machines, or VoIP devices Workspace View.

Figure 12. Workspace View



Procedure 3 Configure Alert Center Thresholds

As soon as WhatsUp Gold is installed and your network is discovered, Alert Center begins monitoring and alerting on a variety of thresholds for devices across the network. Disk, CPU, interface, and memory utilization are tracked for all devices and virtual devices (with the optional WhatsVirtual plug-in), as are ping response time and availability. Additional thresholds are keyed to Flow Monitor data, exposing and alerting on network traffic that could indicate a problem.

Step 1: You can create a myriad of other thresholds to monitor other types of performance, passive and Flow Monitor data, which can be applied to all devices collecting that type of data or to a select group of devices.

Figure 13. New Ping Response Time Threshold

The screenshot shows the 'New Ping Response Time Threshold' configuration window. It includes fields for 'Name' (set to 'Ping response avg > 2 ms') and 'Threshold' (set to 'Ping Response Time average exceeds 2 ms for more than 30 minutes'). There is a 'Devices to Monitor' section with a 'Select...' button. The 'Notification' section shows 'Email Bob and Sue' as the chosen method. The 'Threshold Check' section is set to 'Check threshold every 3 minutes'. At the bottom, there is an option to 'Automatically resolve items no longer out of threshold' and 'OK'/'Cancel' buttons.

Procedure 2 Customize Device Status Reports

The Device Status Report gives you a detailed look at the health of a single device by aggregating multiple reports that apply to that device. You can view the Device Status Report for any Cisco or other device you are managing using WhatsUp Gold.

The Device Status Report is automatically configured to display the most commonly viewed information about a device, but you can customize it to your specific requirements.

Process

Managing the Network

1. Configure WhatsConfigured
2. Configure a NOC Display
3. View Reports on the Go
4. Assess Issues with Real-Time Tool

Procedure 1 Configure WhatsConfigured

If you have deployed the WhatsConfigured configuration management plug-in with WhatsUp Gold, then you can setup the devices you want to manage.

Step 1: Assign credentials for each device that you plan to manage through WhatsConfigured.

Step 2: Configure Task scripts that login to devices via SSH or Telnet to run command-line interface (CLI) commands on managed devices. Tasks can use pre-configured task scripts or you can configure your own custom task scripts with the WhatsConfigured Custom Script Language.

Task scripts can perform a number of operations, such as restoring or backing up a running or startup configuration, or changing an application password. After tasks are configured and assigned, they either run on the schedule you configure, or can be run as needed from the WhatsConfigured Task Library and the WhatsUp Gold Device Properties Tasks dialog. Task scripts are stored and managed in the Task Script Library and associated to WhatsConfigured in the WhatsConfigured Task dialog.

Procedure 2 Configure a NOC Display

After you have discovered your network and configured WhatsUp Gold, you can extend the visibility WhatsUp Gold provides to your Network Operations Centers (NOC) using Dashboard.

Dashboard is a standalone utilitarian application included with WhatsUp Gold Premium and Distributed editions that cycles through report pages on the WhatsUp Gold Web interface, providing network administrators with constant insight and views into network health.

Figure 14. NOC





Tech Tip

If your network contains more than a couple of branch offices, consider using WhatsUp Gold Distributed Edition. WhatsUp Gold Distributed Edition extends the full functionality of WhatsUp Gold Premium Edition to each branch office, sharing network health information between a central NOC and any number of remote sites, no matter where they're located or how they're connected.

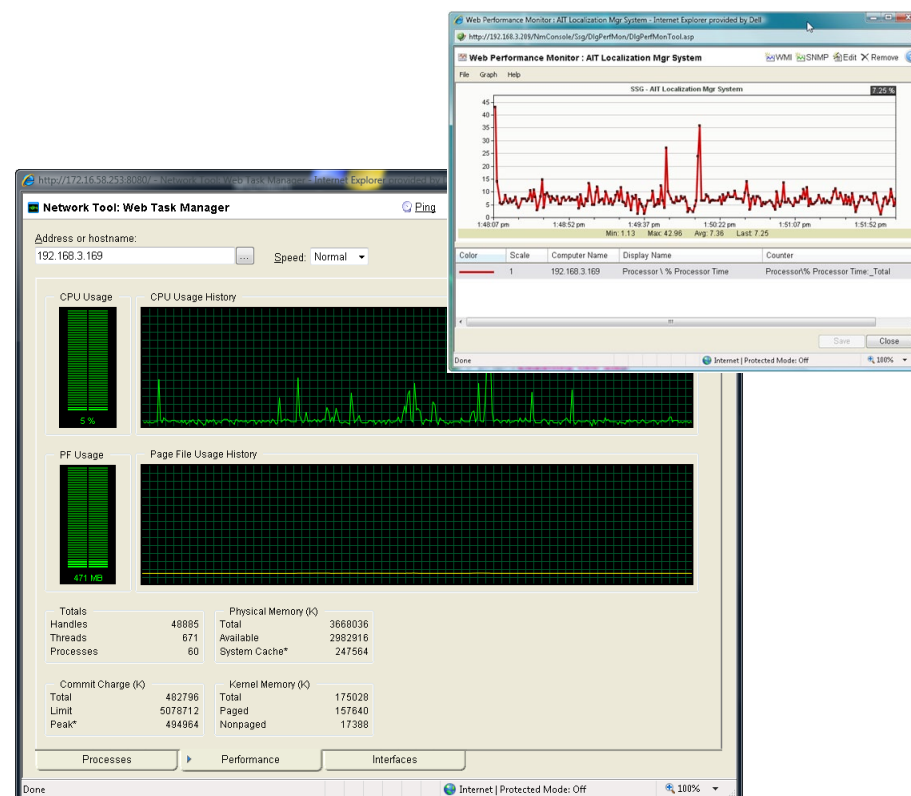
Procedure 3 View Reports on the Go

With many network management solutions, the most information you can get from your cell phone is a notification of an issue. With WhatsUp Gold's mobile interface, you don't have to run to the computer every time you get a message about network health. The mobile Web interface lets you view thirty-five WhatsUp Gold and Flow Monitor reports from virtually any modern mobile device, so you can troubleshoot issues as soon as you find out about them.

Procedure 4 Assess Issues with Real-Time Tool

Throughout reports in WhatsUp Gold, you can view InstantInfo pop-ups, which let you see, in real-time, how the metric shown on a report is performing. For example: If you're viewing an interface utilization report for a device, InstantInfo pop-ups allow you to see the real time interface utilization. This helps you to quickly evaluate the health of the device. Similarly, you can use two network tools to view real-time data on network devices: The Web Task Manager and Web Performance Manager. Bringing the power of the Microsoft Windows Task Manager and Microsoft Windows Performance Monitor tools to the Web, these tools let you view real-time device data directly from the Web interface.

Figure 15. Performance Management



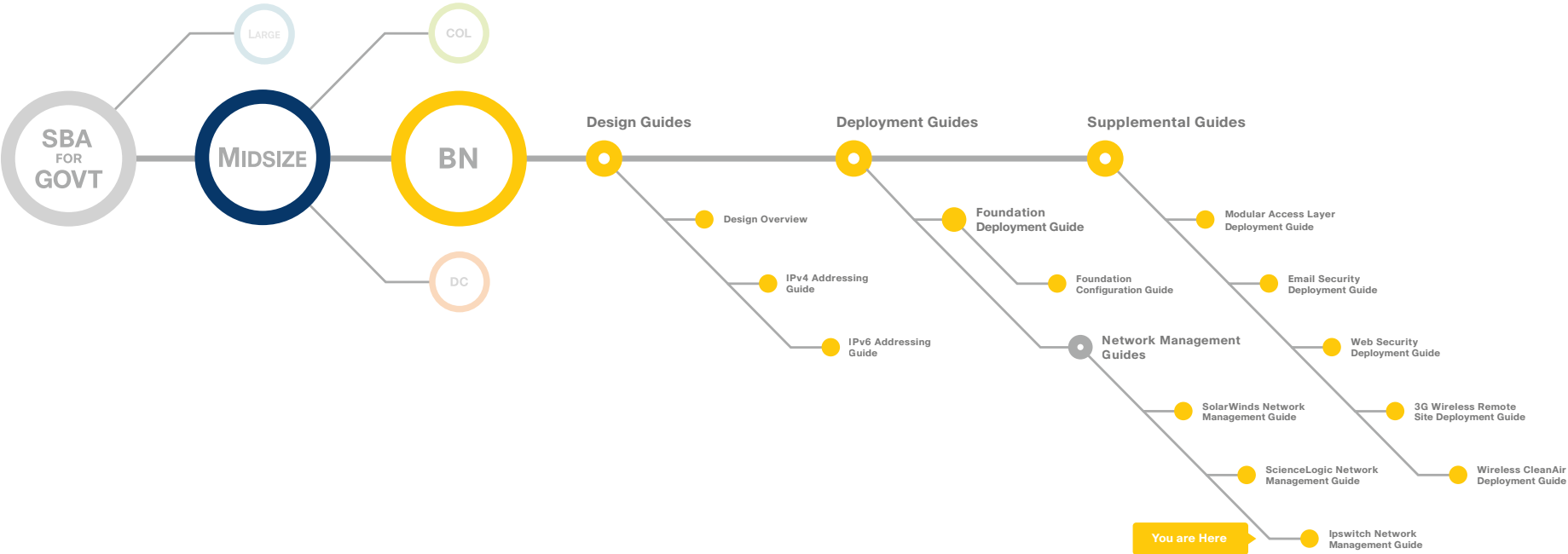
Reader Tip

With the Cisco SBA for Midsize Agencies—Borderless Networks and the WhatsUp Gold family of network management products, you can profitably deploy end-to-end network solutions to an expanded client base. To find out more about these WhatsUp Gold network management solutions, visit WhatsUpGold.com, where you can also download a 30-day free trial.

Appendix A: WhatsUp Gold Product Summary

WhatsUp Gold Premium Edition Comprehensive real-time network management and Windows application monitoring for single networks of all sizes.	WhatsUp Gold Distributed Edition Delivers far-reaching network management and Windows application monitoring for distributed multi-site enterprises.	WhatsUp Gold Standard Edition Presents essential network infrastructure monitoring priced right for small and midsize agencies.	WhatsVirtual Provides capabilities to discover, map, monitor, alert, and report on virtual environments in WhatsUp Gold.
WhatsConnected Layer 2/3 network mapping tool that discovers, maps and documents your network down to the individual port, making it simple to visualize the physical topology and understand device interconnections.	WhatsConfigured Manages critical device configurations for your network devices and automates key configuration and change management tasks required to maintain and control network device configuration files.	Flow Monitor Leverages Cisco NetFlow, J-Flow and sFlow data to provide insight into how efficiently your network is performing and how bandwidth is utilized, so that you can monitor network quality of service and quickly resolve traffic bottlenecks.	VoIP Monitoring Integrates Cisco IP SLA technology into WhatsUp Gold to monitor and report on your network's capacity to support and maintain acceptable performance for VoIP call quality.

Appendix B: SBA for Midsize Agencies Document System





SMART BUSINESS ARCHITECTURE



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

C07-641121-00 12/10