Cisco Network Planning Solution 2.1 and Cisco Network Planning Solution - Service Provider 2.1

Cisco® Network Planning Solution (NPS) and Cisco Network Planning Solution: Service Provider (NPS-SP) help enterprises and network service providers optimize network capacity and performance, analyze network resiliency and service continuity, plan for new technology deployments, and validate planned configuration changes. Cisco NPS and Cisco NPS-SP help reduce the risks associated with network growth, migration, and consolidation.

Product Overview

The network has become a critical business resource, and organizations need strategies that strengthen business continuity through improved network and application resilience while reducing operational expense. This includes the ability to predict, avoid, and lessen the effects of costly network and application service disruptions and the confidence to quickly adapt the network to changing business opportunities.

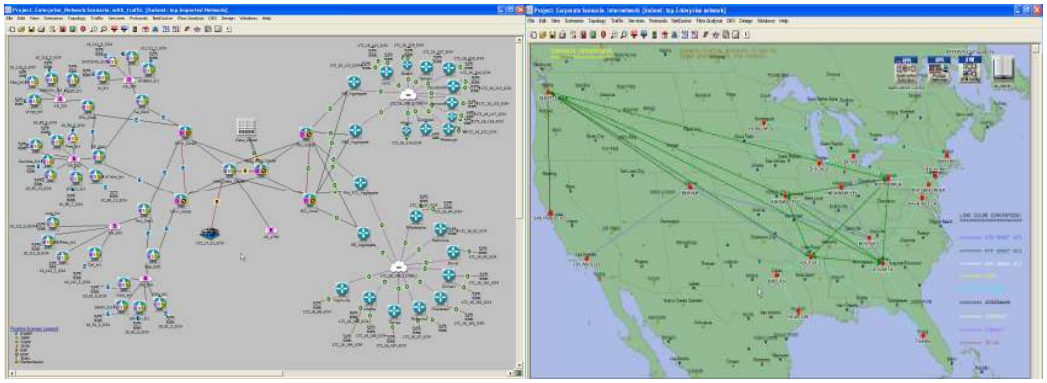
Cisco NPS and Cisco NPS-SP are key components of the Cisco Network Application Performance Analysis Solution, an innovative combination of sophisticated management tools and services from Cisco that provide users with a holistic view of the interaction between network resources and application/service performance. Cisco Network Application Performance Analysis Solution redefines how enterprises can monitor and analyze application performance while proactively planning for changing network requirements. Cisco NPS and Cisco NPS-SP provide powerful analysis tools for the planning and design phases of the network lifecycle.

Cisco NPS and Cisco NPS-SP are vital tools for improving network availability as well as the continuity of applications and services. It operates on a high-fidelity software model of the production network, accurately simulating the behavior of routers, switches, firewalls, and applications to facilitate a broad range of change impact (“what-if”) analyses. Actionable information derived from analysis is used to make automated or guided configuration changes in the network. Using Cisco NPS and Cisco NPS-SP removes the guesswork in the rollout of new applications and services, reduces costs by eliminating manual and time-consuming tasks, and can lower capital expenses. With Cisco NPS and Cisco NPS-SP you can:

- Plan for network and traffic growth, consolidation, and migration
- Automatically size links for network performance and resilience
- Plan for new technologies such as VPNs and voice over IP (VoIP)
- Forecast traffic based on trends
- Predict the impact of node and link failures on traffic flows and resource usage
- Optimize network topology for projected growth
- Plan for deployment of Multiprotocol Label Switching (MPLS)–based traffic engineering (with Cisco NPS-SP)

Cisco NPS and Cisco NPS-SP provide a graphical view of the network topology (Figure 1), with the ability to access detailed information about node and link attributes. The network model can be modified through the GUI to predict the impact of changes in topology, device configuration, and traffic. Configuration changes can also be introduced into the model through a Cisco IOS® Software command-line interface (CLI). Study results from Cisco NPS and Cisco NPS-SP are provided in Web (HTML), Microsoft Word (.rtf), or Extensible Markup Language (XML) reports.

Figure 1. Network Topology View from Cisco NPS



Key Features and Benefits

Advanced Network Planning and Analysis

Cisco NPS and Cisco NPS-SP accurately model a broad range of Layer 2 and Layer 3 technologies, Cisco devices, and third-party devices. Link utilization or end-to-end flow data can be introduced into the network model to perform accurate traffic-flow simulations. Multilayer survivability analysis determines which traffic flows will be most affected by outages and where resulting bottlenecks are likely to occur in a network. You can subject the entire network to an automated reachability analysis to identify potential connectivity problems. Cisco NPS and Cisco NPS-SP also help you predict the impact of deploying new technologies, protocols, or hosted applications, including VPNs, VLANs, and more. For example, a VoIP readiness assessment wizard guides you through a step-by-step analysis, scoring the network's readiness for VoIP deployment. Services analysis demonstrates the impact of change on end-to-end services.

Automated Network Design and Optimization

Cisco NPS and Cisco NPS-SP feature an integrated design framework with standard, configurable models for common design operations. Configurable design actions can be parameterized, sequenced, and saved for repeated execution as a compound task.

- Capacity planning analyzes trends in the current traffic patterns and projects future traffic loads.
- Resilient link dimensioning determines the optimum networkwide link capacity in an existing topology to support projected traffic flows under normal and failure conditions. A failure case can encompass selected links, nodes, and shared risk groups.
- Topology design determines link placement for a ring backbone, a spanning tree, or dual spanning trees. Topology design actions can be used to design new networks as well as perform incremental expansion of an existing network.

- Quality of service (QoS) planning automatically sets IP QoS parameters and sizes the queue bandwidths or weights on IP interfaces based on the queue load and queue configuration rules.
- MPLS traffic engineering automates planning for initial deployment of MPLS label-switched paths (LSPs) for traffic engineering through Cisco NPS-SP.

Optional Modules and Solutions

Cisco NPS – Network Validation Module

Proposed network changes can be validated before deploying them. The optional Cisco NPS – Network Validation Module (NPS-NVM) provides a powerful rules-based engine that systematically checks the entire network model, diagnosing device misconfigurations, errors, policy violations, and inefficiencies. Cisco NPS-NVM processes and interprets device configurations the same way that production network devices do during operation. Expert knowledge of network devices, protocols, and routing behavior facilitates networkwide analysis of connectivity and resiliency, unlike other analysis tools that are limited to simple syntax checks on a single device at a time. A port scan analysis of network security detects gaps in network defenses.

Customizable reports can demonstrate compliance with regulatory and IT governance requirements, such as:

- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- National Institute of Standards and Technology (NIST) Special Publication 800-53 and Federal Information Security Management Act (FISMA)
- Defense Information Systems Agency (DISA) Network Infrastructure Security Technical Implementation Guide (STIG)
- National Security Agency (NSA) Router and Swich Security Configuration Guides
- ITIL/BS15000, ISO 17799, and others

Cisco NPS-NVM is provided with hundreds of standard checks that reflect industry best practices published by Cisco, U.S. government agencies, and others. Rules are provided with source code, sample policy templates, and an integrated authoring environment to help incorporate your organization’s best practices. Standard checks encompass:

- Security configuration
- IP addressing and routing
- Protocol configurations, including Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP), and Border Gateway Protocol (BGP)
- Route maps and access control lists (ACLs)
- Hot Standby Router Protocol (HSRP)
- Simple Network Management Protocol (SNMP), system logging, and router administration
- Firewall configurations and security protocols including authentication, authorization, and accounting (AAA), Kerberos Protocol, Network Address Translation (NAT), RADIUS, and TACACS+
- VPNs, tunnels, and VLANs

- QoS and more

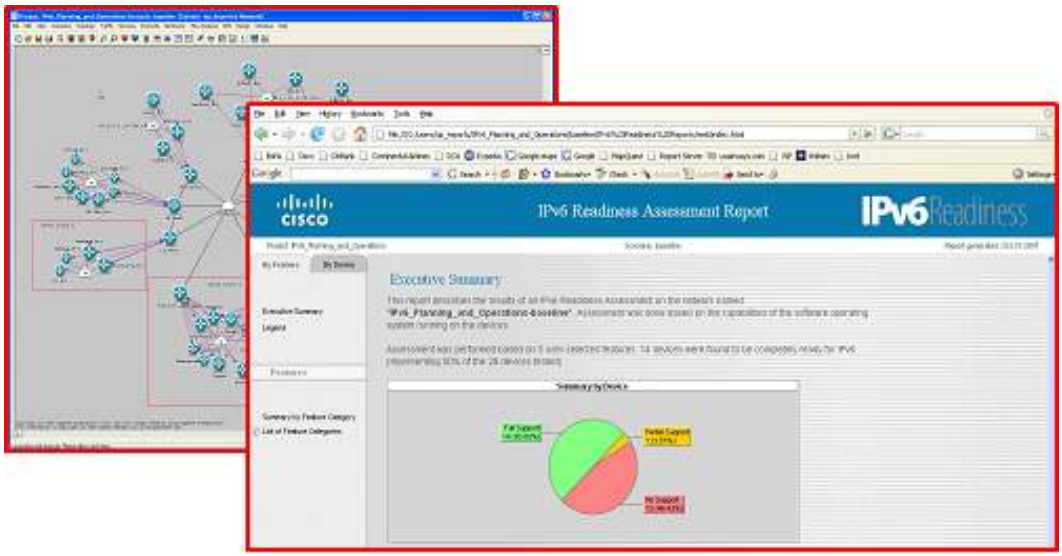
Cisco NPS-NVM is provided as an integrated component of Cisco NPS-SP.

Cisco NPS IPv6 Planning and Operations Module

This optional module includes the IPv6 readiness assessment, a systematic rules-based analysis of network device configurations to verify IPv6 readiness. The rules validate each device's compatibility with IPv6 features including operating system version, routing, QoS, multicast, and security. Users can use an integrated authoring environment to tailor the analyses to their own requirements. At the end of the assessment, a comprehensive report is created, identifying which devices are ill prepared and offering tips to help ensure their compatibility (Figure 2).

Another feature is an intuitive wizard that guides the user through a series of questions to determine an optimal migration strategy. A custom migration strategy is created on the fly by using the configuration information collected from the operational network. The strategy can recommend a combination of capacity and configuration changes, equipment enhancements, and use of tunnels and dual-stacked devices to make sure that network performance is preserved after migration. The user can also make manual adjustments to the proposed configuration in the virtual network environment to determine their impact prior to deployment. The new network configuration undergoes a comprehensive survivability analysis to verify that backup strategies are set up correctly such that no one device or link failure compromises the resiliency of the overall network.

Figure 2. IPv6 Readiness Assessment Report



Cisco Virtual Network Data Server

Cisco Virtual Network Data Server (VNDS) is a complementary solution that automatically maintains a detailed data model of the production network, including topology, configuration, and traffic. It collects and intelligently merges detailed network data from a broad range of sources, reconciling conflicts based on user-configurable priorities. Information can be obtained online from network devices including Cisco routers, Cisco CRS-1 Carrier Routing System, Cisco Catalyst® switches, the Cisco PIX® security appliance, and devices from many other vendors. Built-in software intelligence also allows data to be imported from CiscoWorks LAN Management Solution (LMS), CiscoWorks Network Compliance Manager, Cisco WAN Manager, Cisco CNS NetFlow Collection Engine, and numerous third-party sources.

An additional feature of VNDS is the device autodiscovery adapter. The adapter performs SNMP autodiscovery from a seed IP address or set of seed IP addresses. It attempts to discover all neighboring network devices through collection of MIB data and inference to contact neighboring devices. The adapter performs SNMP community string guessing from a provided set of community strings and can be configured with various filtering options. Filtering options include inclusion/exclusion of IP subnets and ranges, vendor enterprise IDs, and sysService capability. Options are provided for both fast and exhaustive operation to control speed and accuracy of the autodiscovery capability.

Service Providers

Cisco NPS-SP is designed to address the demands of service provider network environments. Cisco NPS-SP provides all the functionality of Cisco NPS in addition to Cisco NPS-NVM for network-aware configuration analysis, and it supports MPLS modeling and analysis, Intermediate System-to-Intermediate System (IS-IS), IPv6, and Cisco Carrier Routing System-1 Cisco IOS XR Software–based device modeling, planning, and analysis (requires Cisco VNDS).

System Requirements

Cisco NPS and Cisco NPS-SP are typically implemented on the user desktop. Cisco VNDS is generally implemented on a dual-processor platform with the prerequisite database environment. Table 1 lists the system requirements for Cisco NPS/Cisco NPS-SP and Cisco VNDS.

Table 1. System Requirements

	Cisco NPS/Cisco NPS-SP	Cisco VNDS
Disk space	20 GB	160 GB (or larger depending on network size and data-retention practices)
Hardware	Intel Pentium 3, 4, Xeon or equivalent 1.5+ GHz (Windows)	Dual 3.4+ GHz Intel Pentium D or Xeon with 1066 MHz front-side bus (FSB)
Memory	1 GB (minimum)	4 GB (minimum)
Software	Only English-language versions are supported: • Windows Server 2003, Windows Server 2003 x64 Edition, and Windows Server 2003 R2 x64 Edition • Windows 2000 Server and Windows Server 2003 R2 • Windows XP Professional and Windows XP Professional x64 Edition • Windows 2000 Professional • Red Hat Enterprise Linux 3 (V2.4 Kernel) • Red Hat Enterprise Linux 4 (V2.6 Kernel)	Only English-language versions are supported: • Windows Server 2003 • Windows 2000 Server • Windows XP Professional • Windows 2000 Professional • Red Hat Enterprise Linux 3 (V2.4 Kernel) • Red Hat Enterprise Linux 4 (V2.6 Kernel)

Ordering Information

Cisco Network Planning Solution 2.1 and Cisco Network Planning Solution – Service Provider 2.1 are available for purchase through regular Cisco sales and distribution channels worldwide. To place an order, contact your Cisco representative or visit http://www.cisco.com.

Cisco Network Planning Solution and Cisco Network Planning Solution – Service Provider licensing options are described in the Cisco Network Planning Solution 2.1/Cisco Network Planning Solution – Service Provider 2.1 product bulletin, viewed at http://www.cisco.com/en/US/products/ps6363/prod_bulletins_list.html.

Service and Support

Cisco delivers a wide range of services programs through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare the network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, contact your Cisco representative or visit http://www.cisco.com.

For More Information

For more information about Cisco Network Planning Solution and Cisco Network Planning Solution – Service Provider, contact your Cisco representative or visit http://www.cisco.com/go/nps.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.

Printed in USA C78-442971-00 11/07