Enterprise Network Testing

The Role and Applications of Testing in
Pre-Deployment, Migration, and
Post-Deployment Network Operations

ciscopress.com

Andy Sholomon
Tom Kunath

Enterprise Network Testing

Andy Sholomon

Tom Kunath

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

Chapter 7

Network Readiness Testing Case Study

This chapter covers the following topics:

- Background for the Network Readiness Testing Case Study
- Network Readiness Assessment Approach and Findings

Network readiness testing can be an extremely worthwhile exercise when you are attempting to gauge how well a new application or solution will perform on an existing network infrastructure. This type of testing often occurs during the planning phase of a new project, either as a prequalification for a proposed solution, or as part of a network audit to identify gaps in the infrastructure that will need to be remediated prior to deployment. Because the performance requirements for VoIP are well defined in terms of loss, delay, and jitter, organizations planning to deploy IP Telephony or Unified Communications (UC) solutions often conduct testing on their live network to help gauge its readiness. Industry experts agree that assessing the network prior to deployment makes VoIP rollouts faster, more successful, and less costly by reducing post-implementation troubleshooting.

The following case study shares the details of how a software development company was able to successfully leverage network readiness testing as part of the overall certification of a Unified Communications design.

Background for the Network Readiness Testing Case Study

MilSpec Software Solutions is a U.S.-based software development company with major campus offices in Boston, Massachusetts, and Research Triangle Park (RTP), North Carolina. The company develops smartphone applications with a focus on enterprise feature integration. In line with the success of an industry that has boomed in recent times, MilSpec Software Solutions has grown at a rate of 15 percent year over year. The company has a 19 percent market share of the U.S. mobile enterprise application solutions segment, and is in the process of taking over another startup company located in San Francisco, California. The management is keen to acquire additional companies as part of a strategy to generate new business growth by opening up new markets. Around 30 percent of the company's workforce is composed of teleworkers, based out of home offices when not traveling to customers' and partners' sites. Teleworkers connect to the office using a software VPN solution.

Legacy Network Infrastructure Overview

MilSpec Software Solutions has been a Cisco Systems customer since its inception in 2001. Following the best practices guidelines for a hierarchical network design, its network has been deployed with clearly defined core, distribution, and access layers. The company operates two major data centers in its campus locations; one in the Headquarters site in Boston, and the other in a recently acquired company's main site located in RTP, North Carolina. The two locations are interconnected with a pair of OC12 circuits, forming the backbone of the network core. In addition to the Boston and RTP campus sites, MilSpec has 20 remote locations, where a distributed sales force, development group, and support teams maintain offices. These remote locations gain access to the corporate IT (data only) systems over a WAN built on a service provider Layer 3 MPLS service. Remote locations typically connect to the MPLS WAN by means of fractional T1 links, ranging from 512 Kbps to 768 Kbps depending on individual needs. The enterprise voice environment includes legacy PBXs at the campus sites and key telephone systems (KTS) obtained from various manufacturers at the remote locations. As part of the RTP campus site acquisition, the company inherited a legacy PBX from a different manufacturer than the one that was in place at its parent site in Boston, limiting the voice features that could be offered between the two major campuses. Figure 7-1 shows a high-level view of the MilSpec Software Solutions campus and remote office WAN connectivity.

Cisco Unified Communications Proposed Solution

MilSpec Software Solutions decided to invest in a Cisco Unified Communications infrastructure to improve workforce productivity, reduce operational costs, and ease the integration associated with company acquisitions. The first phase of UC deployment included a complete retrofit of legacy phone systems to Cisco VoIP, followed by the introduction of Cisco Contact Center Enterprise for streamlined call center operations. The primary drivers to justify this investment included the following:

- Reduced OPEX due to centralized management and control.
- Reduced time to offer unified voice capabilities to new companies that are acquired and integrated.
- Mobile workforces can have Single Number Reach (SNR) feature functionality.
- Reduced travel expenses as the UC solutions provide easier and more direct collaboration between coworkers, suppliers, and clients at different sites.

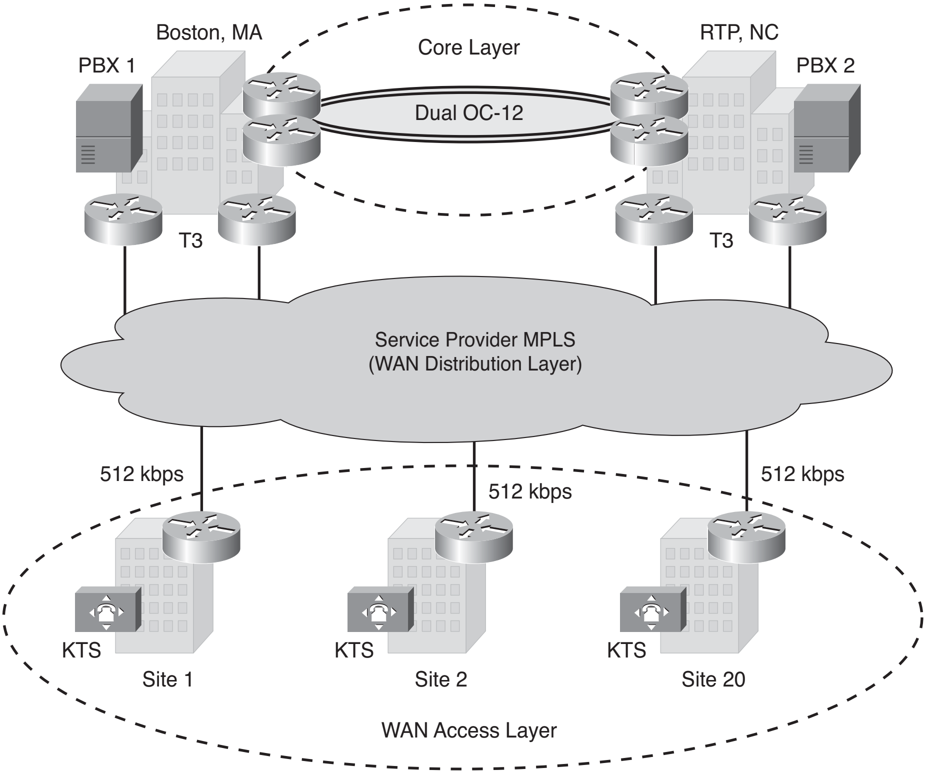

Figure 7-1 *Existing MilSpec Software Solutions Network Design*

Risks Associated with Implementing the Proposed Solution

Although the CIO was eager to realize the benefits of Unified Communications, he recognized that rushing the deployment could risk failure of the UC project and potentially impact data network stability. A primary concern for the CIO and his engineering team was whether the existing data network was capable of handling the unique demands of real-time VoIP traffic, and whether the performance of business data applications would be degraded under the additional strain. It was determined that a formal analysis would need to be completed to determine what gaps, if any, needed to be remediated prior to deploying the solution. To seek guidance with this analysis, the CIO hired a Cisco Advanced Services consultant specializing in VoIP and UC deployments. Having dealt with several clients with similar projects and concerns, the consultant recommended that a thorough assessment be carried out, involving the following activities:

- **Network Readiness Assessment (NRA):** Involves an audit of the network devices to determine operational health and compliance with standards and best practices for VoIP deployments. Information gained during the network audit would be used as a baseline to identify gaps in the device hardware, software, provisioning, and configuration standards that would need to be remediated.

- **Network Path Analysis (NPA):** Involves injection of synthetic VoIP traffic between various endpoints on the live production network. Results from the NPA would provide a good indicator of the voice quality that could be expected once the UC solution was deployed. Information from the NPA would be used to help guide decisions on whether circuit upgrades, QoS, or routing changes might be needed prior to deployment.
- **Summary of Recommendations:** Includes any predeployment actions that would need to be resolved prior to deployment (for example, hardware upgrades, enabling QoS features) and post-deployment processes and procedures for day-2 operations.

Network Readiness Assessment Approach and Findings

The following sections provide details on how the Network Readiness Assessment (NRA) and testing was accomplished, and how the associated findings were used to help MilSpec Software Solutions to prepare, deploy, and operate the new UC infrastructure.

The audit reports and recommendations delivered by the Cisco Advanced Services consultant are included after each section.

Network Readiness Assessment

The goal of the NRA is to identify the gaps, if any, that must be remediated on the network to support the additional requirements of real-time applications. An audit of design documentation, physical topology, running configurations, and operational performance statistics from network management system (NMS) reports is conducted during this exercise.

The NRA report is organized into several subsections that address different aspects of the core design.

Hierarchy and Modularity

This assessment evaluates whether an existing network infrastructure follows the Cisco best practice of hierarchical and modular design. This model offers many advantages over an unstructured, organically grown design, as it has proven to be easier to troubleshoot, upgrade, operate, and maintain. Network modularity helps to scale the design and simplify implementation and management because it is constructed from uniform building blocks and template configurations.

A manual review of the network topology and device hardware and software features and functionality is conducted.

Audit Report

- The network topology has been deployed in a hierarchical and modular fashion. Network routers and switches have been deployed in core, distribution, and access roles, each optimized for the specific functions that they entail. MilSpec has deployed standardized equipment models, Cisco IOS versions, and configurations across the network elements in each level of the hierarchy. The equipment models are all currently supported under a Cisco SMARTnet contract and their Cisco IOS versions will support the required QoS features needed for converged traffic.

- New Catalyst 6500 access layer switch lines cards are recommended for both campus sites to support power requirements and Ethernet connectivity of the Cisco IP Phones. The existing line cards do not support 802.1af (Power over Ethernet [PoE]) or the conditional endpoint QoS trust model.
- The remote office switches are Catalyst 3760s, which are PoE capable. It is recommended that a UPS be installed in each of the wiring closets to provide continuous service to the IP Phones in the event of a power outage.

Utilization and Redundancy

This assessment evaluates critical network resource utilization of production devices and circuits during peak usage hours. This includes short- and long-term sampling of link, CPU, and memory utilization of relevant routers and switches. A review of the circuit provisioning ratios throughout each layer of the hierarchy is also conducted to determine the oversubscription ratios that have been put in place. These ratios are compared against Cisco campus provisioning best practices to determine the likely congestion points that may cause problems when additional VoIP traffic is added to the network.

> **Note** Current best practices suggest distribution to access oversubscription ratio of 1:20, and core to distribution oversubscription ratio of 1:4.

The redundancy aspect of the verification includes checking for any single points of failure (SPOF) in the network. This includes a check for redundant supervisors, line cards, power supplies, and links at the critical paths of the infrastructure. The right level of network redundancy allows faster network convergence, which is an important consideration for real-time traffic like voice.

Audit Report

- The existing network has been provisioned within the guidelines of Cisco best practices for bandwidth oversubscription ratios. No more than ten access switches have been connected via 1-Gbps uplinks to any distribution level switch, reflecting a 1:10 distribution to access ratio, and the core to distribution ratio is less than 1:2.
- The peak utilization on all access layer uplinks is less than 20 percent. The OC-12 links between the data centers are underutilized (less than 25 percent) during office hours, but rise to 60 percent utilization during off-hours due to extensive backups and server mirroring. The WAN links to remote offices have been measured at relatively high utilization (above 60 percent) during office hours, spiking to over 80 percent in some cases. This is an area of concern for the planned IP telephony deployment because these circuits will require additional bandwidth for “on-net” interoffice

calls. It is recommended that the WAN bandwidth at all remote locations be increased to at least a full T1.

- The NMS historical report does not indicate any device crash or resource depletion (CPU or memory high utilization) for the past 12 months. A 12-month review was conducted to take into account any seasonal peak utilization variation (for example, MilSpec has a new software release cycle every 6 months, and hence there is a heavier workload expected during that time).
- MilSpec has implemented an Active/Active redundancy methodology on its production IT/IS systems and servers. A high degree of device redundancy (node, route processor, line card, circuit, power supply) has been enforced accordingly in critical places in the network. No SPOFs have been noted outside of user PCs that are single-homed to access switches.

Access Layer Links

This assessment examines the connectivity between the access and distribution layers of the network infrastructure for conformance with Cisco best practices and recommendations. Some of the most important include the following:

- Redundant, Layer 3 connections between access and distribution switches.
- When Layer 3 is not possible, Layer 2 devices and links should be enabled with Rapid Spanning Tree Protocol (RSTP) to provide convergence times consistent with a typical Layer 3 topology.
- Other Layer 2 optimizations should be enabled to improve convergence, including port-fast, manual duplex and trunk negotiations settings, lowered Hot Standby Router Protocol (HSRP) timers, BPDU Guard, Root Guard, and UniDirectional Link Detection (UDLD) configurations.
- The number of hosts in a broadcast domain should be limited to 512 or fewer.

Audit Report

- MilSpec has Layer 2 links from access to distribution switches and relies on default STP timers for network convergence. It is recommended that MilSpec reconfigure the Layer 2 links between access and distribution to Layer 3 links if possible so that convergence can be optimized.
- If a conversion to Layer 3 links is not possible, it is recommended that access to distribution links be enabled with RSTP to provide faster convergence. HSRP timers should also be reduced to 250 ms on the distribution layer switches to improve first hop redundancy convergence.
- A few of the access VLANs have grown exceptionally large, in some cases reaching nearly 1000 hosts. These VLANs should be repartitioned to limit the impact of the broadcast domains. A recommendation is made to change the current /21 VLAN allocation to /23, so that the site administrators will be less tempted to exceed the recommended number of 512 hosts/VLAN.