Make your mobile cost effective

PUBLICATION

Shared Data Clusters, by Dilip Ranade, delivers an examination of how cluster software works, as well as a discussion of essential clustering services, such as locking and messaging. Real-world applications are studied, including the difficulties in deploying them and best practices. www.wiley.com/compbooks

Computer Networks, A Systems Approach, by Larry Peterson and Bruce Davie, is a third edition that treats the network as a system composed of interrelated building blocks, as opposed to strict layers, to give a conceptual foundation to understand networking technologies. It now includes information on MPLS, switching, IPv6, wireless and peer-to-peer networks. www.mkp.com

Enterprises need to have a clear strategy for deploying and managing mobile devices, according to Ken Smiley, director and mobile enterprise analyst for Forrester Research. An organization's bottom line can suffer, he says, especially in organizations that emphasize employee convenience over organization benefits.

"Organizations that do not have an effective business strategy for mobility," says Smiley, "are more likely to find themselves attempting to support a myriad of platforms and devices for various reasons, thus resulting in increased costs."

A Gartner report on mobile device deployment and management estimates that, from 2001 to 2004, enterprises without an IT asset management program to track and manage mobile devices will incur a 30% to 40% increased total cost of ownership when compared with organizations that provide mobile asset tracking and service accountability.

IDC estimates the mobile device management market will grow from $121.3 million in revenue in 2001 to a projected $715.1 million by 2006. The proliferation of mobile and wireless devices within the enterprise, which vary in operating system, connectivity, form factor and purpose in both horizontal and vertical markets, is a primary IT challenge, the research firm says. Providing an integrated mobile device management solution as part of an overall systems management environment is critical, IDC adds, as customers do not want to manage solutions with separate consoles but prefer one consolidated view to manage all devices across multiple environments.

"Mobile device management software continues to gain market acceptance and expand its reach from what once was a niche laptop play to a critical requirement to manage the variety of mobile and wireless devices within an organization," says Stephen Drake, program manager for IDC's mobile infrastructure software service. "The heightened adoption of enterprise mobile-enablement projects and increased product development addressing broader mobile and wireless connectivity options, mobile work scenarios, and critical IT management issues are driving the growth within this market."

According to Smiley, one option for simplification of management and reduced support costs is to limit the number of different platforms for an intended solution. He suggests aligning device selection and acquisition with the organization's business strategy for mobility.

Smiley points out that implementing only one mobile platform company-wide makes little sense if that platform is not capable of meeting the business needs of the organization, despite the upfront cost savings. The needs of a 200-member sales team, for example, are different from a field-service fleet.

"If the organization can do it all on one platform, then additional cost savings can be had," he says. "However, in our experience, this is a very rare occurrence in today's market. In most cases, needs are simply too diverse to limit an organization to a single platform today."

When multiple platforms are required, Smiley suggests that individual platforms should be chosen to accomplish specific tasks or to satisfy specific business needs that can be quantified in terms of a positive return on investment. When deciding between nearly equal devices or nearly equal platforms, he recommends an organization should choose the platform with more flexibility.

Smiley warns, though, that flexibility often comes at a higher price point and organizations will have to weigh whether or not that flexibility is likely to be used during the lifetime of the platform or device chosen.

Continued on page 10

EVENTS

- ✔ **WebSec 2003**, July 28-30, San Francisco, provides security professionals with sessions on secure instant messaging, Web security architecture, hacking Web applications and wireless authentication, as well as a vendor exposition. www.misti.com/websec
- ✔ **BICSI Fall 2003**, Aug. 18-21, Nashville, offers educational seminars on cabling installation, wireless, LAN and outside plant technologies, as well as technical demonstrations and exhibits. www.bicsi.org
- ✔ **Fall 2003 VON**, Sept. 22-25, Boston, focuses on the convergence of the telecom and Internet industries. The tradeshow and exposition tackles issues affecting IP communications, including both voice and data. www.von.com

Another factor is how recent the platform is to market. Sometimes, Smiley advises, it pays not to buy early. "For almost the last 18 months, a pattern has emerged among mobile device vendors and, in particular, among PDA vendors," he says. "Within three to six months of release, the price of the device will have fallen 20% to 25% compared to its introductory price. Unless there is a compelling feature of a new platform that the organization cannot do without, simply waiting three months to purchase may save substantially on upfront costs."

Buying in quantity, as well as seeking device and service combination discounts, will also save money. "Devices sourced from an operator or carrier are more likely to be subsidized to some degree, thereby lowering the initial acquisition costs," says Smiley. "In some cases, the devices are free if the purchaser will simply sign an agreement for a certain period of time."

Yet, equipment choices vary greatly from one provider to the next, and companies may have to choose between a discounted platform that is less than ideal, or purchasing devices and service plans separately at a higher cost. According to Smiley, "The latter is more often the better approach in terms of cost savings over the life of the solution, since supplemental costs to enhance a less optimal solution will likely outweigh the initial cost savings."

Worms are getting faster!

SHORT TAKE

"When it comes to voice-data convergence, the applications that reach 'killer' status will be those that are easy for the user to understand, purchase and use."

—Mike Durance, vice president and general manager of Toshiba's telecommunication systems division, as quoted in Deloitte and Touche's 2003 annual report.

Computer worms and viruses have become increasingly easy to distribute and significantly more threatening to the security of global communication networks, according to analyst firm Probe Group of Cedar Knolls, N.J. An attack can be launched by virtually anyone, from anywhere in the world, explains Probe analyst Tony Marson, with a future potential spread time of mere seconds.

"The increasing level of sophistication is clearly exemplified when comparing the Slammer and Code Red attacks," says Marson. "Although Slammer was just one-tenth the size of Code Red, the former took only 10 minutes to spread globally, while the latter required three days." The bottom line, he says, is that in the last 18 months the time required for the infection of global targets has shrunk from days to minutes.

Marson suggests that for those seeking to maintain the integrity of their infrastructures during a worm attack, multilayered security should be implemented, blanketing all aspects of infrastructure.

Although the worm attacks to date have looked to exploit the vulnerabilities in operating systems such as Windows and Linux, these are the same operating systems that network operators use to run network-management systems, services/applications servers, switches and routers. "One can envision a future worm attack that could completely disable a network-operating system just by exploiting a particular vulnerability," states Marson. "Therefore, a sense of urgency persists for all network operators and enterprises to incorporate common-sense network security measures that can be easily implemented."

Marson also contends that service providers have a responsibility to ensure the continuation of service and availability of their networks during a worm attack. He says the benefits of prevention as opposed to recovery are clear–not only is it cheaper, but it also allows network operators to do the following:

- maintain service-level agreements, thus avoiding penalties;
- maintain reliability of connectivity;
- reduce personnel costs (by not needing to retain significant numbers of personnel to deal with continuous breaches of the network and the recovery from an attack);
- maintain a consistency in customer service and delivery;
- increase customer satisfaction; and
- reduce support costs.

While no network is 100% secure from a worm or virus attack, Marson says, the alternative (as with Cloud Nine) is that the service operator can go out of business. ❑