

1 **Q. Re: Network Infrastructure, Schedule B, Pages 88 and 89 of 93**

2
3 **Newfoundland Power states that “...the equipment which facilitates communication**
4 **between the Company’s shared servers and related application...” is eight (8) years**
5 **old and requires replacing. What is the industry standard for replacing such**
6 **equipment?**

7
8 A. The industry standard for replacing such equipment is seven (7) years according to
9 Gartner, Inc.¹

10
11 A copy of a 2010 report from Gartner, Inc. titled *Updating Enterprise Network Useful*
12 *Life Recommendations* is provided in Attachment A. Figure 1 on page 7 of the Gartner
13 article states that the expected useful life of LAN Switching (Edge and Core) equipment,
14 the type of equipment to be replaced in 2013 as part of the Network Infrastructure
15 project, is seven (7) years.

¹ Gartner, Inc. is the world's leading information technology research and advisory company with over 12,000 clients worldwide. Founded in 1979, Gartner is headquartered in Stamford, Connecticut, U.S.A., and has 5,200 associates, including 1,280 research analysts and consultants.

Updating Enterprise Network Useful Life Recommendations

Gartner, Inc.

Updating Enterprise Network Useful Life Recommendations

Published: 4 June 2010

Analyst(s): Mark Fabbi, Tim Zimmerman

Organizations increasingly face replacing older assets based on the perception of the equipment's increased risk. This research provides new recommendations for the useful life of network equipment, as well as ways to assess the risks associated with aging network infrastructure technologies.

Key Findings

- Limited lifetime warranties and higher mean-time-between-failure (MTBF) design criterion for critical networking components are affecting enterprise useful life assumptions. Switches and routers are expected to remain in most enterprise networks for a minimum of seven years.
- As a result of better quality and reliability, which has been driven by ratification of 802.11n, wireless LAN (WLAN) access points and network application service appliances — where guest access, network management or client forensic applications reside — will have a useful life of five to seven years. This is equivalent to switches at the edge of the network.
- Two primary inhibitors extending the useful life of older network equipment are the vendors' end-of-life support programs and the critical role of the equipment in the network.

Recommendations

- Do not follow predetermined, regular upgrade cycles for network equipment, because changes in application architectures and deployments can still affect the useful life of network equipment.
- Analyze each major product category to determine the associated risks, and prepare a migration plan.
- Only upgrade or replace network equipment when the risks become unacceptable or significant new technical requirements emerge.

What You Need to Know

The useful life of WLAN, switching and routing equipment is increasing to a minimum of seven years. However, rather than relying on predetermined replacement schedules, network managers need to make upgrade decisions based on the risk profiles and the operating costs of various types of equipment. Enterprises should avoid premature upgrades, while maintaining an acceptable level of risk.

Strategic Planning Assumption

By 2014, the useful life guidelines for networking equipment will increase by 50%.

Analysis

During periods of rapid innovation, network infrastructure components tend to be replaced on a regular and short cycle. Historically, data-networking equipment was replaced every three or four years, and it was a fairly common practice to lease equipment for three years and then "rip and replace" the equipment for a new solution. Traditional voice equipment was at the other end of the spectrum, remaining in the infrastructure for seven to 12 years or more, with few or no hardware upgrades.

WLAN equipment has had unpredictable life cycles. In the 1990s, it was managed by operations and only replaced every seven to 10 years. However, when the responsibility moved to IT in the early 2000s, it was integrated into the data equipment life cycle of three to four years, but now it has been extended to match other data networking equipment, with a life cycle of five to seven years. Understanding how to evaluate the network landscape will help enterprises focus investments in the proper areas and ensure that equipment is not replaced prematurely, which is an issue Gartner sees too often in client inquiries.

We recommend that switches and routers, as well as access points and network application service appliances, be used for five to seven years in most cases. Replacement should not be done on a regular schedule, but should be based on an analysis of new requirements, the cost of operating the old equipment and the level of risk associated with operating long-lived network assets.

Terminology

The following related, but separate, terms and concepts are used to describe how to think about an asset's life in the network.

Useful Life

Sometimes referred to as the technological life of an asset, the useful life reflects how long the equipment can be used before the product becomes functionally obsolete — that is, when the risk associated with the product becomes too great or when the operational costs make a transition to new products an economic advantage.

Economic Life

The economic life of an asset is the period of time in which the asset has some economic value (residual value or fair market value). The useful life of an asset will often exceed its economic life. The useful life and economic life are important for financial reasons, because they will dictate the maximum length of an operating lease. An important element that also needs to be part of the economic life consideration is that new equipment has been designed to consume less power. This means that total cost of ownership calculations for new equipment may speed the replacement of older components, as operational savings can be realized that justify a shorter life cycle of existing equipment.

Depreciation

Depreciation relates to how the asset is written down financially over time, and should be closely related to the minimum expected useful life, rather than the economic life of an asset. Enterprises need to understand and account for installations in countries that have specific depreciation periods that are mandated by accounting rules or fiscal rules.

Operating Life

Hardware design and expected MTBF will determine operating life, which basically measures how long a piece of hardware is expected to last while performing its specific function.

Useful Life

Useful life represents the normal time a piece of equipment is expected to be in place in an average enterprise network. Unanticipated changes to the operating environment can affect the equipment's useful life — for example, a significant expansion to the business that puts increasing demands on a core switch or new application architectures that change the WAN infrastructure could negatively affect the anticipated useful life.

Factors That Determine Useful Life

Four primary factors determine a product's useful life in an enterprise network.

Market Innovation

The relative stability of a product or market area is key for determining the useful life of most products. Markets that are increasingly standardized or have progressed further down the commoditization curve (see "Exploiting the Enterprise Networking Commoditization Curve") provide the impetus to increase or stabilize the useful life of products. Products with a smaller percentage of software or stable software features are also good candidates for extended life.

Market innovations do not necessarily require or force an upgrade. For example, there's no need to upgrade a workgroup LAN to Gigabit Ethernet. However, a requirement for Power Over Ethernet (PoE), because of a large IP telephony (IPT) deployment or WLAN, is likely to force a technology upgrade. Other new requirements — such as broad deployments of network access control or WAN

optimization controllers — may be better handled by overlays, while enabling the switch and router installation to remain in place to extend their useful lives.

Vendor End-of-Life Announcements

Such announcements trigger a series of events that lead to the end of support for a product. Although the lack of a support contract is an issue for network operations, it does not result in a mandatory requirement to replace the equipment. It is important to understand what an end-of-sale (EOS) announcement means.

In the case of Cisco, an EOS announcement causes a specific chain of events. The final date that Cisco will accept orders for new networking equipment is approximately six months after an EOS announcement. Starting with this EOS date, Cisco will provide full software and hardware support for the product for a total of five years — three years of software support and five years for hardware. Software support generally means that bugs will be fixed and security vulnerabilities will be closed. There may be some feature upgrades (especially if the product is part of a family where active developments are still being performed). After the third year, Cisco will only provide hardware support (basically replacement for failed components).

Juniper Networks' router support model is similar; however, software phone support extends to 42 months — primarily to assist with the migration to newer software releases. Most other vendors have some variations on these five-year, EOS support options; however, some workgroup switches will offer some form of lifetime warranty for the hardware. Enterprises need to carefully understand the "fine print" on what is covered on these often-limited lifetime warranties (see "Network Equipment Lifetime Warranties: Enterprise Savings or Vendor Marketing?").

A final vendor issue in determining the useful life of a product may come down to luck and careful buying. Buying a product near the end of its time in a product portfolio can reduce its useful life in the network. Although organizations should be aware of where a product fits in a vendor's life cycle, it's not always easy to predict when a vendor will update its product portfolio.

Operating Life

This affects useful life and is specifically tied to the hardware design of the product. It is related to, but not the same as, the product's MTBF, which is calculated based on a curve that predicts a level of failure in the product line. Historically, most network equipment was designed to have MTBFs of approximately 100,000 hours (roughly 11 years). Failures often occur in power supplies and fans, although environmental issues can also affect the longevity of semiconductor components.

With 11-year MTBFs, enterprises are experiencing an increase of failures in networking equipment that was installed prior to 2003 (with equipment that has passed its eighth in-service anniversary), which is consistent with MTBF failure curves. We anticipate an increasing number of failures for this equipment in the future. Depending on their location in the network, this will clearly increase the risks of using older equipment.

Looking at hardware design, fixed form-factor switches are being designed with increasing MTBFs — in many cases, 200,000 hours or more. Thus, for some equipment, the operating life will no

longer be part of the equation to determine the useful life. Switches equipped for PoE are likely to have a shorter operating life than those without PoE, because of larger power supplies, more heat and increased air cooling requirements. However, even PoE switches are being designed with MTBFs of 15 years or more, which brings this equipment beyond its intended life in an enterprise network.

Operating Cost

This is the final consideration when determining useful life. The price of some equipment — particularly Ethernet workgroup switches — has declined significantly in the past five to 10 years. In most cases, software and hardware service contracts are related to the original equipment costs. When you add in the arrival of new lifetime warranty products that are available on the market, we have seen cases in which replacing older LAN switches with new ones — especially those that offer lifetime warranties — can have a return on investment of two years or less. Armed with this background information, the key question remains, "When do I have to upgrade various network components?" Assuming that there are no overwhelming technological or cost reasons, the answer lies in performing a risk assessment of equipment and its role in the network.

Questions to Consider

What impact will a failure have on the network?

If the equipment is a workgroup switch or a WLAN access point that affects a few dozen users at most, the risk is fairly minimal, especially if there are local spares available or if the location is served by both wired and WLANs. On the other hand, risk escalates rapidly if you are dealing with a core switch or a router, where failure could affect major portions of the network, or with a device such as an application delivery controller (ADC) that could cause a key application failure. For more mission-critical areas of the network, assess whether the architecture can deal with a single device failure. Overlapping coverage for WLANs, dual-homing wired and wireless connections with redundant core switches, or ADCs deployed in redundant pairs will lessen the impact and risk, and enable core products to extend their useful lives.

Is the device restricted to internal networks or is it exposed to the Internet?

Products that are inside the corporate firewall are generally at low risk. For example, routers that are exposed to the Internet are at a higher risk once the three-year software support window runs out. Because of the risks associated with routers exposed to the Internet, they should be moved internally or replaced once the three-year support window expires.

Is it part of a system or does it operate stand-alone?

Again, the risk for routers (and other Layer 3 devices) is greater as product support for the software is no longer available, because these products are likely to run older operating system releases. As time progresses, the likelihood of incompatibility increases, because vendors will not test these

older releases with the same rigor they use to perform interoperability tests on software and hardware.

Is there increasing risk of component failure?

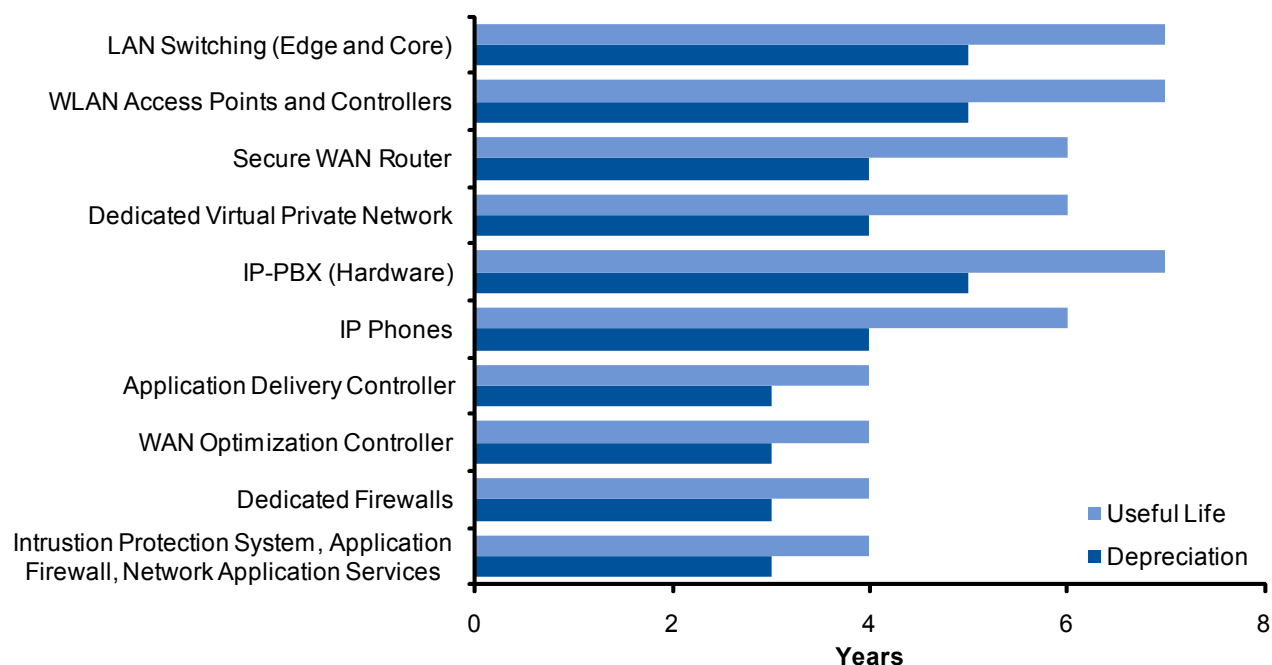
As products move toward their operational life span, we have observed increasing failure rates. LAN switches and branch routers typically have MTBFs that are in the 10-year or more range. Newer LAN switches have increasingly long operational life expectancies, so failure will be less of a consideration in the future. With the ratification of 802.11n, products such as WLAN access points are increasingly being used to provide connectivity at the edge of the network and their useful life expectation should be viewed as other edge network components. Although these components don't necessarily need to be replaced right away, unless they are affecting the functionality of the infrastructure, organizations need to begin migration planning.

How stable is the deployment?

For products with minimal software features or in an environment that is not subject to major change, the useful life can run well beyond the software support window. However, in environments where there are significant changes, new configurations are often deployed and new features are required, older products will tend to need replacement on a more-aggressive schedule. The biggest issue here is that changes can lead to environments with a mix of software releases and introduce potential incompatibilities. Changes to an environment where few additional devices are being added will carry less risk.

Although upgrades should be dealt with on a case-by-case basis, there are some generalizations based on the type of equipment under review. Figure 1 represents Gartner's guidelines regarding the typical useful life of various pieces of network equipment. However, the suggested risk assessment should still be performed because risk will be treated differently by different types of organizations or by the specific requirements in various parts of the network.

Figure 1. Recommended Useful Life Schedule



Source: Gartner (June 2010)

New IPT equipment is expected to have a significantly shorter life cycle than the traditional time division multiplex (TDM) equipment it is replacing. We expect the call setup hardware to have a life span similar to general-purpose servers, although the software is likely to be covered through software support contracts and have a longer useful life. A detailed analysis of IPT hardware and software is found in "IPT vs. TDM Life Cycle Purchase and Operations Costs."

Security requirements can be split between threat-facing and non-threat-facing equipment. Threat-facing devices will have a shorter life. Unified threat management devices will reduce the overall life span by as much as 50%, because of the requirement to expand as one or more particular functions consume all the resources of the appliance. Longer life cycles can be attained by using dedicated function appliances.

Tactical Guideline

Most WLAN, switching and routing technology will be replaced by end-of-life factors, rather than feature requirements.

Recommended Reading

"IPT vs. TDM Life Cycle Purchase and Operations Costs"

"Exploiting the Enterprise Networking Commoditization Curve"

"Network Equipment Lifetime Warranties: Enterprise Savings or Vendor Marketing?"

This research is part of a set of related research pieces. See [Why a Network Plan Is the Best Way to Control Your Network Cost](#) for an overview.

Regional Headquarters

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

© 2010 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity" on its website, http://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp.