G00235400

Know When It's Time to Replace Enterprise Network Equipment

Published: 15 August 2012

Analyst(s): Caio Misticone, Mark Fabbi

Four primary factors determine the useful life of network equipment: market innovation, vendor end-of-life policies, operating life and operating cost. Failing to properly assess the EOL of equipment will result in premature equipment replacement or increased risks for the organization.

Key Challenges

- The primary factors that determine the useful life of enterprise equipment are market innovation, vendor end of life (EOL) policies, operating life and operating cost.
- Limited lifetime warranties, higher mean time between failures (MTBF) design criterion for critical networking components and modular platforms are affecting enterprise useful life assumptions in a positive way.
- Two primary inhibitors to extending the useful life of older network equipment are the vendors' EOL support programs and the critical role of the equipment in the network.

Recommendations

- Upgrade or replace network equipment only when the risks become unacceptable or significant new technical requirements emerge.
- Analyze and understand each major product category and end of sale (EOS) announcements from different vendors to determine the associated risks and prepare a migration plan.
- Do not follow predetermined, regular upgrade cycles for network equipment, since business, application and technical requirements can impact useful life positively and negatively.

Analysis

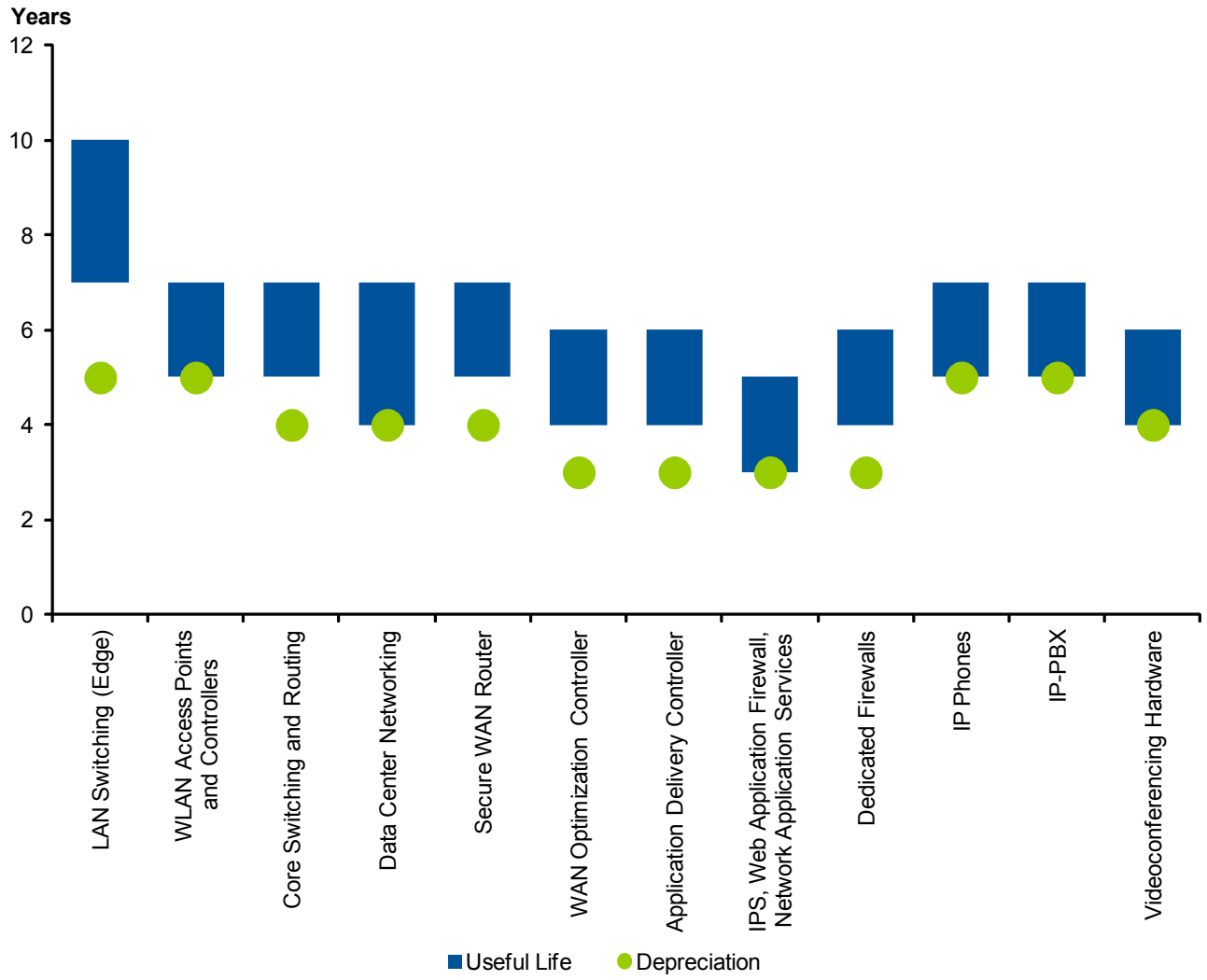
Enterprises increasingly consider replacing older assets based on the equipment's increased risk to breakage or lack of continuing vendor support. This research provides recommendations for

evaluating the useful life of enterprise network equipment, as well as methods that enterprises can use to assess the risks associated with aging network infrastructure technologies.

Understanding how to evaluate the network landscape will help enterprises focus investments in the proper areas and ensure that equipment is not replaced prematurely. Contrasting areas where organizations can save money with areas that demand greater attention and investment will also help IT managers justify new investments to their CIOs.

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 enterprise network equipment. We strongly encourage enterprises to perform risk assessments, because risk will be treated differently by different types of organizations or by the specific requirements in various parts of the network. For example, public sector organizations tend to replace equipment in a prescribed manner due to budget cycles and changes in governments, rather than making business-driven changes that are typical of the private sector. WAN routers facing the Internet are more exposed to security threats than workgroup edge switches when vendors announce end-of-software support.

Figure 1. Recommended Useful Life Schedule for New Equipment



Source: Gartner (August 2012)

Useful Life Guidelines

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 a new product an economic advantage. 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.

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, but these former norms have changed considerably.

Due to the increased standardization and stable requirements of edge switching, limited lifetime warranties offered by several vendors and increasing MTBF, the useful life of this type of equipment has increased to seven to 10 years.

As a result of better quality and reliability when compared with older wireless LAN (WLAN) standards, IEEE 802.11n equipment useful life stands in the five- to seven-year range. Enterprises continue to struggle to use the capacity that is available as part of 802.11n, even without using some of the scalability functionality that is already available. There will be a lot of early adopters for 802.11ac in the home market, but no traction in the enterprise.

In most cases, we recommend that IT organizations use core switches and routers for five to seven years. Replacement should not be done on a regular schedule, but should be based on:

- Analysis of new requirements
- The cost of operating the old equipment
- The level of risk associated with operating long-lived network assets

In some circumstances, it may be possible to extend the useful life beyond seven years. This type of equipment may be negatively impacted by capacity increases (for example, LAN backbone traffic or increasing WAN speeds), which may lower its useful life. Alternatively, these assets may be redeployed, for example, by moving the core switch to handling aggregated or even edge-traffic, medium office WAN routers to smaller branch offices.

Compared with core switches and routers, some of the newer data center technologies can have shorter useful lives. These include fabrics, fabric extenders and input/output (I/O) convergence, whose useful life ranges from four to seven years. Until these new technologies and products have a proven track record, we advise a slightly more conservative approach when setting useful life expectations.

We expect application delivery controllers (ADCs) and WAN optimization controllers (WOCs) to have a three- to five-year useful life. There remains significant innovation in these markets, which may lead to forced software or hardware upgrades and, consequently, reduced useful life. The useful life of WOCs is still limited by their use of hard disks. We find that new features, such as new Secure Sockets Layer (SSL) key size, in the ADC market can lead to upgrade requirements.

Security requirements can be split between threat-facing and nonthreat-facing equipment. Threat-facing devices will usually have a shorter life (three to five years). Unified threat management devices will reduce the overall life, because of the requirement to expand as one or more particular functions consume all the resources of the appliance. Longer life cycles (five to seven years) can be attained by using dedicated function appliances.

New IP telephony (IPT) equipment has a significantly shorter life cycle (five to seven years) than the traditional time division multiplexing (TDM) equipment (seven to 12 years), which IPT has largely replaced. 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 shorter useful life.

After two ways of innovation (move from Integrated Services Digital Network [ISDN] to Internet Protocol [IP], and standard-definition [SD] to high-definition [HD] video resolution), videoconferencing equipment's useful life has stabilized between four to six years. Although there are new features, such as 2K line video, 3D video and new codecs, which will be put into place for new installations, it is unlikely to prematurely retire existing installations. Most clients consider "good enough" video to be adequate for most purposes.

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 is key for determining the useful life of most products. Markets that are increasingly standardized or have progressed further down the 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 is no need to upgrade a workgroup LAN to 10GbE. However, a requirement for Power Over Ethernet (PoE or PoE +) for items like security cameras or some high-end WLAN access points (APs) may force a technology upgrade. Other new requirements — such as broad deployments of network access control or WOCs — may be better handled by overlays, while enabling the switch and router installation to remain in place to extend their useful lives.

Other parts of the network, such as network security and ADCs, have more innovation and critical demands for new capabilities. For example, the migration of 2048-bit or 4096-bit SSL keys has necessitated a move toward ADCs with higher overall performance.

Vendor EOL Policies

Vendor EOL 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. In some circumstances, it is perfectly fine to get support from a third-party vendor. It is important to understand what an EOS announcement means. Although it impacts and influences useful life of a product, it doesn't have to dictate it.

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, presented as three years for software 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 and HP support plans are similar to Cisco; however, Juniper is now offering five years of software support (though not necessarily for the current version of Junos). This can be a competitive differentiator, especially for products that are Internet-facing and require security patches to lower risk.

Most other vendors have some variations on these five-year, EOS support options. Some workgroup switches will include some form of lifetime warranty for the hardware, but may exclude power supplies and fans in other cases. Enterprises need to carefully understand the fine print on what is covered on these often-limited lifetime warranties.

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

Operating life 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 MTBF 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.

Looking at new hardware design, fixed form-factor switches are being designed with increasing MTBF — 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.

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 warranties and more energy-efficient 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 an ROI of two years or less.

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 LANs 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 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.

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 typical 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 vendor's support window expires.

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

The risk for routers (and other devices like unified communications equipment) is greater as product support for the software is no longer available, because these products are likely to run older OS 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 MTBF 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.

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, and where new configurations are often deployed and new features are required, older products will usually need to be replaced on a more-aggressive schedule. The biggest issue here is that changes can lead to environments with a mix of software releases and may introduce potential incompatibilities. Changes to an environment where few additional devices are being added will carry less risk.

Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"IT Market Clock for Enterprise Networking Infrastructure, 2012"

"Hype Cycle for Networking and Communications, 2012"

"The Disaggregation of the Enterprise Network"

GARTNER HEADQUARTERS

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

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp