G00273656

Know When It's Time to Replace Enterprise Network Equipment

FOUNDATIONAL **Refreshed:** 21 June 2016 | **Published:** 4 March 2015

Analyst(s): Danilo Ciscato, Mark Fabbi

Network managers must find a balance between maximizing installed equipment lifetime and jeopardizing network availability. To prioritize investments and minimize outages, they must understand factors that affect product life and events that trigger a replacement, then set a strategy for support.

Gartner foundational research is reviewed periodically for accuracy. This document was last reviewed on 21 June 2016.

Key Challenges

- To minimize cost, enterprises seek to avoid prematurely replacing equipment, but must balance this against avoiding network failures.
- Because the anticipated useful lives of different types of network equipment vary, enterprises are constantly upgrading or replacing a portion of their network infrastructure.

Recommendations

- Set a policy for network equipment upgrades based on IT requirements, budget constraints, technical innovation and acceptable risk.
- Establish product-specific replacement plans and support levels for the various classes of equipment within the network.

Table of Contents

List of Tables

List of Figures

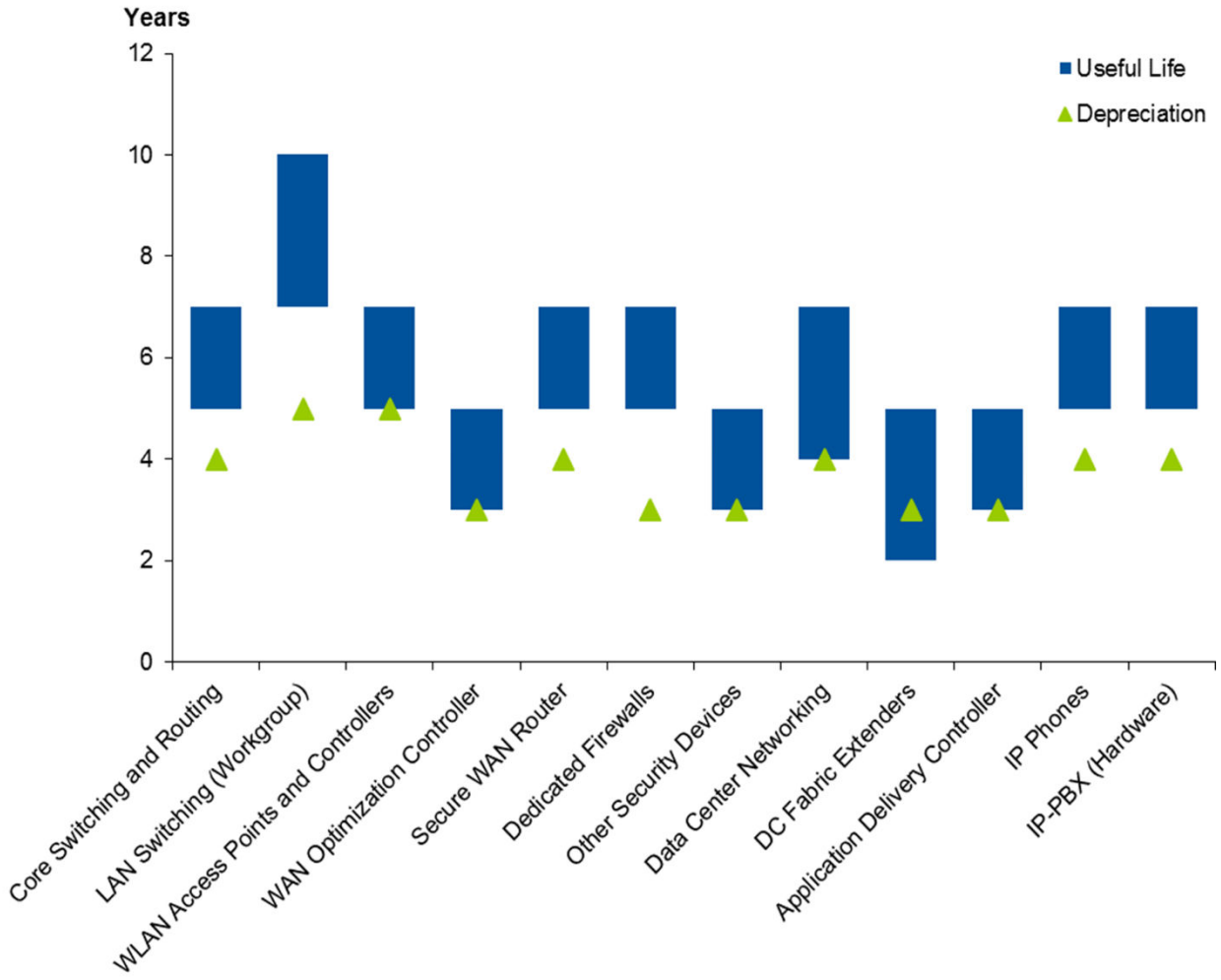
Introduction

This document was revised on 3 April 2015. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

Deployment of new applications and services can trigger the need to upgrade network equipment, but in their absence, most enterprises simply replace older assets based on the expiration of continuing vendor support. However, enterprises that routinely change out equipment based on vendor end of life (EOL) policies will find they are prematurely replacing network equipment and incurring unnecessary costs.

This research provides recommendations for a more holistic approach to the useful life of specific enterprise network equipment (see Figure 1), as well as methods enterprises can use to assess the risks associated with aging network technologies. Network managers must understand the unique dynamics of each network device category and focus yearly capital expenditure (capex) investments to avoid prematurely replacing equipment. They can better justify and prioritize necessary investments to their CIOs if they address each area in a differentiated fashion.

Figure 1. Recommended Useful Life for Networking Equipment



IPS = intrusion prevention system
DC = data center
IP = Internet Protocol

Source: Gartner (March 2015)

Analysis

Set a Policy for Network Equipment Upgrades

Replacement of network equipment does not need to follow a timed schedule. Upgrades should follow a consistent policy set by IT and not by the vendor. To assist in setting this policy, Figure 1 depicts Gartner's guidelines regarding the typical useful life of various pieces of enterprise network equipment.

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 economically advantageous.

Gartner's definition of useful life represents the normal time we expect a piece of equipment to be in place in a typical enterprise network. However, unanticipated changes to the operating environment can affect the equipment's useful life. For example, a significant business expansion will place increasing demands on a core switch, which will shrink its useful life. New applications can also require a new WAN architecture, negatively affecting the anticipated useful life of network equipment. On the other hand, a reasonably stable environment may allow organizations to push useful life beyond our recommendations.

Over the past 15 years, the useful life for data networking equipment has continually expanded, though the life of voice-related technologies contracted with the adoption of Internet Protocol (IP)-based collaboration systems. In general, enterprises should continue to drive toward longer life spans for most product areas, and avoid setting fixed replacement schedules for networking equipment.

This document covers the traditional enterprise acquisition model in which networking equipment is purchased (with capex) and is covered by a support contract. Some clients employ alternative acquisition models (see Notes 1 and 2). The evaluation criteria laid out in this research equally applies.

We strongly encourage organizations to perform risk assessment because each area of the network is associated with different risk levels and organizations treat risk differently. For example, failure of an access point in a school has a different impact than failure of a core switch in a financial stock exchange.

Each product category follows different dynamics (See Note 3 for a discussion of various technology areas), so establish a specific upgrade policy to comply with business requirements, prioritize investments within budget boundaries, and keep risk to an acceptable level.

Four Key Factors That Determine Useful Life

The four primary factors that determine a hardware product's useful life in an enterprise network are summarized in the following table.

Table 1. Factors That Determine Useful Life

Useful-Life Factor	Details
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 stabilize or elongate a product's useful life. Products with a smaller percentage of embedded software or with stable software features are also good candidates for extended life. Market innovations do not necessarily require or force an upgrade. See Note 4 for examples.
Vendor EOL Policies	Many vendors have similar EOL policies and the end of sales (EOS) announcement triggers a chain of events that influences useful life of a hardware product, although it doesn't have to dictate it. See Note 5 for more details. Certain products can include some form of hardware lifetime warranty, but may sometimes exclude power supplies and fans. Enterprises need to carefully assess the fine print of limited lifetime warranties.
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 mean time between failures (MTBF), which is calculated based on a curve that predicts a level of failure in the product line. Most network equipment is designed to have MTBF greater than 100,000 hours (roughly 11 years), with a general trend toward increasing MTBF due to simpler and standardized design elements. Hence, hardware failures are generally rare, but harsh environmental conditions (high temperature and humidity, power spikes, dust and so on) will diminish MTBF, so equipment operating in these conditions could show significantly higher failure rates than predicted by MTBF.
Operating Cost	These are the costs of maintaining equipment in operation: essentially energy consumption and the vendor's support contract. Operating costs of installed equipment usually remains constant, but the operating cost for equivalent new products available on the market might be lower. For example, new Ethernet switches not only have lower purchase price, but also have lower energy consumption and support costs. In this case, replacing equipment earlier can save money. We have seen situations where new products — especially those with lifetime warranties — reduce operating expenditure (opex) significantly, justifying a capex investment with a business case showing ROI of two years or less. Aggressive trade-ins and incentives are sometimes offered by vendors and should also be considered in this business case.

Source: Gartner (March 2015)

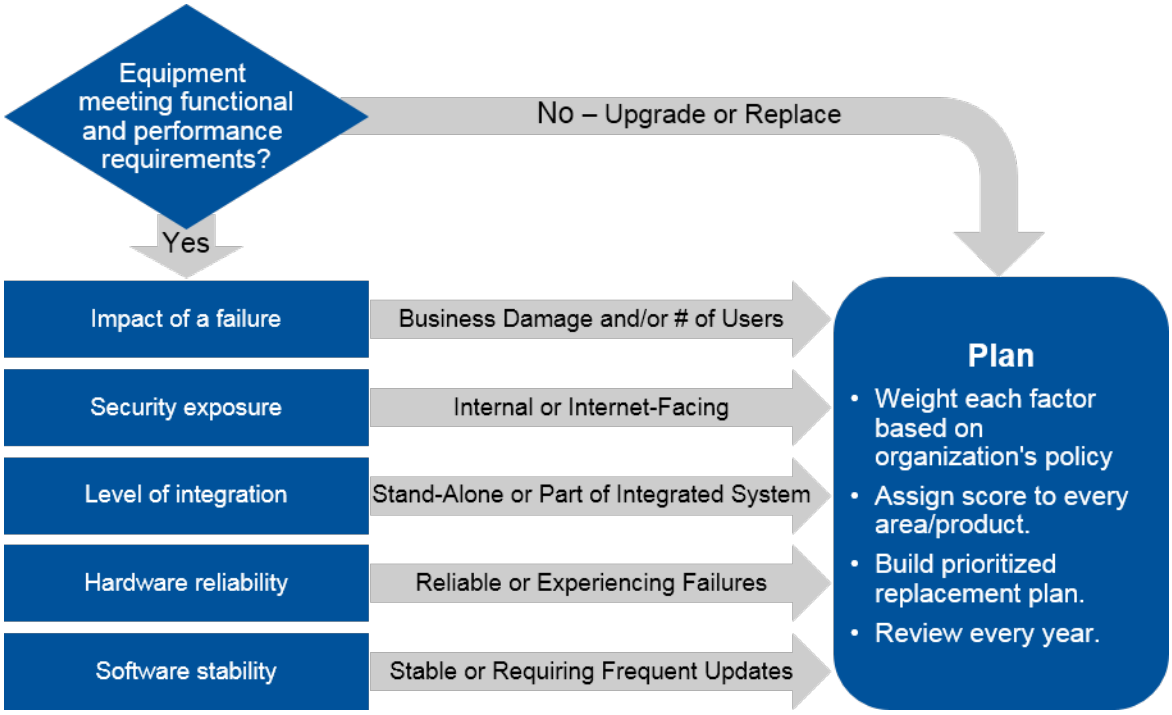
Establish Product-Specific Replacement Plans and Support-Level Requirements for the Different Classes of Equipment Within the Network

We recommend that enterprises create a consolidated plan on the likely timing of various upgrades based on current business demands and update it on a yearly basis. This approach yields greater budget flexibility; it adjusts timing of projects based on changing drivers and assist in prioritizing investments.

The following six questions can help identify and rank the different network elements as they approach their expected life span, or as the equipment nears its end-of-support date. Figure 2 summarizes the process. Equipment with higher risk levels in more dynamic environments are a higher priority for replacement and will need to be covered by support agreements. Equipment at

the other end of the spectrum should remain in the network, likely even when vendor support has expired. Always evaluate for both hardware and software support.

Figure 2. Building a Network Equipment Upgrade Plan



Source: Gartner (March 2015)

Is the Network Equipment Still Meeting Functional and Performance Requirements?

The most important point is to assess whether the product is still meeting your functional and performance requirements. Assuming no other compelling factor discussed below applies, the equipment is a good candidate to remain in the infrastructure, regardless of age.

What Impact Will a Failure Have on This Network Element?

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 can impair major portions of the network, or with a device such as an application delivery controller (ADC) that can 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 a lower risk. For example, routers that are exposed to the Internet are at a higher risk once after the vendor 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) escalates with the expiration of product support for the software because these products would run older OS releases, but need to interoperate with newer releases. As time progresses, the likelihood of new-vs.-old OS incompatibility increases because vendors often do not exhaustively test these older releases with the same rigor they use to perform interoperability tests on current versions of software and hardware.

Is There Increasing Risk of Hardware Component Failure?

As products move toward their operational life spans, we have observed increasing failure rates. LAN switches and branch routers typically have MTBF that are in the 10-year-or-longer range. Similarly, all network equipment have increasingly long operational life expectancies, so hardware 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 risk here is that changes can lead to environments with a mix of software releases and may introduce potential incompatibilities. Conversely, changes to an environment where few additional devices are being added will carry less risk.

Gartner Recommended Reading

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

"IT Market Clock for Enterprise Networking Infrastructure, 2014"

"Predicts 2014: Unified Communications Accelerators Will Be Software- and Cloud-Oriented, but Less Interoperable"

"How to Reduce Network Equipment Support Costs"

Note 1 Alternative Equipment Consumption Models

Purchasing networking hardware is not the only way for an enterprise to get capabilities. Alternative consumption models are emerging and should be considered when replacing equipment. For more

information, see "New 'Cloudlike' Utility Network Consumption Models Can Improve Enterprise Network Agility."

Note 2 Web-Scale IT: The Contrarian View

For organizations that have implemented a Web-scale IT approach, the support strategy is completely different. These organizations utilize a disposable fit-for-purpose approach to hardware. When the switch breaks, just throw it away and replace it with a spare on the shelf. While this trend is growing and worth investigating, the vast majority of Gartner clients have not yet adopted this culture in their data center. For more information, see "Cultural Issues Are the Primary Barrier to Web-Scale IT Adoption."

Note 3 Technology-Specific Implications

Workgroup Switching

Useful life of workgroup switching has increased to seven to 10 years due to limited lifetime warranties offered by several vendors, increasing MTBF and largely stable access layer requirements.

Wireless LAN Equipment

WLAN equipment compliant to the IEEE 802.11n WLAN standard fulfills the need of most enterprise customers, and its useful life stands in the five- to seven-year range as a result of better quality and reliability when compared with older WLAN standards.

The next-generation standard IEEE 802.11ac was ratified in January 2014 and is being implemented in two waves of increasing performance. Considering the limited benefits of Wave 1 and the small number of end-user devices (like tablets, smartphones and laptops) ready for 802.11ac, enterprises should wait until Wave 2 products are widely available before considering the migration.

Core Routing and Switching

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 aggregation or access layers or by migrating midsize-branch-office WAN routers to smaller branch locations.

Data Center Networking

Compared with core switches and routers, some of the newer data center technologies can have shorter useful lives. These include DC fabrics, DC fabric extenders and input/output (I/O) convergence.
DC equipment useful life ranges mostly from four to seven years, but products like DC Ethernet fabric extenders with 1 Gigabit Ethernet (GbE) interfaces are expected to have a shorter life (from two to five years) because 10GbE interfaces are becoming mainstream for servers.

Until these technologies and products have a proven track of record, we advise a slightly more conservative approach when setting useful-life expectations.

Application Delivery Controllers

We expect 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 Equipment

Security requirements can be split between threat-facing and non-threat-facing equipment. Threat-facing devices will usually have a shorter life (three to five years). Multifunction security devices (unified threat management devices, for example) 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, although firewall and IPS refresh can be driven earlier by increases in required throughput.

IP Telephony Equipment

IP telephony equipment has a shorter life cycle than traditional time division multiplexing (TDM) equipment (seven to 12 years), but we expect to see a difference emerge between hardware terminals (IP phones), software clients and call control functions. While hardware terminals such as desktop phones and video devices will continue to have a life span of between five and seven years, by 2016, we expect the average product development cycles for software will have dropped to three years (see "Predicts 2014: Unified Communications Accelerators Will Be Software- and Cloud-Oriented, but Less Interoperable").

Enterprise class IP phones are reliable and stable in terms of functionality, while software-based clients for laptops, tablets and smartphones follow the same dynamics as other enterprise client software. Upgrades for hardware IP telephony (IPT) terminals bring limited benefits, therefore extending their useful life. Increased adoption of IPT software clients and smartphones in the enterprise reduces the need for upgrading hardware terminals or might even lead to a reduction in their number.

Call control functions are increasingly becoming virtualized and cloud-based as call setup hardware migrates away from the enterprise premises and as hosted and cloud collaboration services gain traction.

Videoconferencing Equipment

Enterprises have slowed refresh rates of large room systems as group videoconferencing requirements have become more focused on personal endpoints and commodity appliances for "huddle rooms." In addition, supporting infrastructure for videoconferencing is rapidly transitioning to "virtual meeting room" services that do not require a local multipoint control unit (MCU). A limited number of enterprises will replace board room systems to take advantage of higher resolution, greater codec efficiency or improved content sharing. As a result, the useful life of mainstream room systems remains at four to six years, while modular small group systems will be replaced more frequently.

Note 4 Market Innovations Don't Always Force Immediate Upgrades

Vendors are constantly introducing new products and technologies, but buying the latest version is not always necessary. For example, the move to 802.11ac Wave 2 does not require a rip-and-replace of wired switching infrastructure (see "Don't Let the New WLAN Standard Break the Bank or Your Wired Network"). 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 that operate further up the stack, such as network security and ADCs, have more innovation and critical demands for new capabilities. For example, the migration of 2,048-bit or 4,096-bit SSL keys has necessitated a move toward ADCs with higher overall performance. Firewalls and IPS can also drive earlier upgrades for increased throughput.

Note 5 Vendor EOL Policies

Vendors will generally accept orders for the product for six months after the announcement, until the EOS date. After EOS, they will generally provide software and hardware support for the product for a total of five years.

At the end of this five-year period, support contracts will not be renewed by the OEM or resold by its authorized channel partners. Although the lack of a support contract is an issue for network operations, it should not result in a mandatory requirement to replace the equipment. Support needs must be assessed for both hardware and software. Some hardware (replacement parts or complete product) may be supported via a sparing strategy, or by a support contract from a third-party maintainer (TPM), such as Curvature, CXtec, Park Place Technologies or SMS (Systems Maintenance Services). Some hardware replacements might require relicensing for software.

More on This Topic

This is part of an in-depth collection of research. See the collection:

- How to Optimize Your Network Spending

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