NETWORK INFRASTRUCTURE

A Guide to Maintenance, Repairs, Upgrades, and Replacements

Brought to You by:

WORLDLINK
INTEGRATION GROUP

Table of Contents

Hardware Maintenance

Servicing and Updating Network Infrastructure Equipment

Keeping cables, access points, routers, switches, patch panels, and hardware housing units clean and running efficiently is a necessary component in ensuring a safe, reliable network connection for any business with connectivity needs. The following information will provide general guidelines for maintenance needs, average timelines of services, and the most common equipment problems that call for repairs or replacements.

Preventative Care, Maintenance, and Upgrades of Equipment

Is it necessary to upgrade from Cat5 cabling to Cat6?

In most cases: no. In fact, it is pretty rare for most businesses to undergo a cabling infrastructure upgrade –not only because of its disruptive, costly nature –but also due to the lack of necessity for greater bandwidth capacity.

Instances in which an upgrade to Cat6 would be likely and/or necessary:

- A need to push massive amounts of data over the network
  - Examples: CAD or Video
- End of life and/or damage to the wiring
  - See **Average Lifespan of Equipment**

When should access point coverage be evaluated?

It is necessary to re-evaluate the airwave environment from time to time to determine how it has changed since an access point's initial installation.

- When neighboring businesses move, add, or eliminate access points, it can affect the strength and clarity of your access points that run over the same frequency
- When furniture has been moved or there has been reconstruction of office spaces (i.e. added walls or cubicles and/or the demolition of dividers, etc.)

Changes in the above-mentioned elements can affect the range of coverage and the parts of a building that receive adequate connectivity from a specific –or several –access points. If individuals, or your businesses as a whole, notice changes in connectivity clarity and reliability after remodeling or a change in nearby tenants, it is advisable to conduct a site survey and move or add access points. It is also recommended that you evaluate your coverage at least once a year to ensure that your network users are receiving efficient coverage.

How often will access points need to be replaced? Does this equipment require cleaning and/or repairs on a regular basis?

- The frequency of access point replacement depends on how long the equipment lasts (see **Average Lifespan of Equipment**) and the rate at which technology progresses.
- It is a rare occurrence for access points to be in need of repairs (especially component replacement) and/or basic cleaning. If an access point stops working, a full replacement is usually necessary.

Average Lifespan of Equipment

What is the average lifespan of cabling?

Wires have a life of approximately 25 years, but can require an earlier replacement due to erosion from:

- The environment (i.e. leaks in the building or exposure to sunlight
- Damage (i.e. from human interaction and/or pests such as mice or rats)

What is the average lifespan of an access point?

Generally, an access point lasts 3-5 years,[1] though businesses usually outgrow the technology before the technology wears out. The client will have a need for better coverage, more bandwidth, or have more people accessing Wi-Fi, which their current access point(s) may not be able to handle.

What is the average lifespan of routers?

Routers tend to last 4-5 years, but the technology may become outdated or unable to match the needs of your growing business before the device itself fails due to age.

How long do hardware housing units (i.e. cabinets and data racks) last?

Given that the housing units are more for protection and organization, the cases only need replacing if severely dented or otherwise damaged, or if the amount of routers, switches, and patch panels exceeds the capacity of the data rack or cabinet.

For a more comprehensive list of average equipment lifespan see:

Table of Life Expectancy for Network Equipment

[1] http://www.networkworld.com/article/2316063/network-security/when-to-upgrade.html

Software Updates

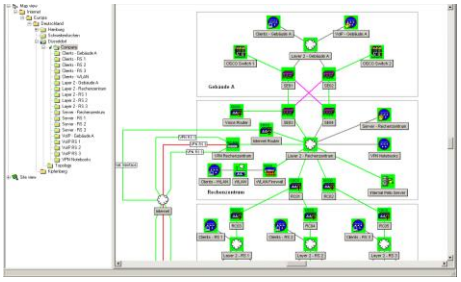
Network operating systems (OS) require a little more attention and more frequent updates than network hardware, due to their role in security and system efficiency. Minor improvements and adjustments are constantly made to networking software and require almost continual updates to maintain optimal operation. The longer a network goes without upgrades and attention, the longer the list of accumulated exploits to which it may be vulnerable.[2] This being said, it is important to set up your system to automatically monitor security threats, system errors, and possible upgrades. Whether this is done by an external source or your own IT department, the system should be programmed to provide alerts to key players in your business to ensure any problems that arise are dealt with immediately.

More frequent updates and continual maintenance of operating systems can reduce the need for large-scale upgrades of major software components.[3] Large-scale upgrades can:

- Be extremely costly
- Require time-consuming testing
- Lead to additional staff training
- Result in a significant amount of time installing and deploying the software

How often should updates be run?

A general guideline is to run internet-based or cloud-based updates on a daily basis, with manual updates completed as is necessary for your particular software. This depends on the frequency in which your operating system requires such updates. Monitor this on a consistent basis and set up your system to alert you of any new and/or urgent software upgrades.



When should I upgrade my networking software?

There is no standard timeframe as to how long a network should run on a specific software platform, but with the rapid rate at which technology advances, it is good practice to evaluate your current systems on an annual, if not semi-annual basis. The most common reasons a company would revamp their software is if its current application

[2] https://www.cisco.com/web/about/security/cspo/docs/perspective_silent_risk.pdf

[3] https://www.techsoupforlibraries.org/cookbook-3/maintaining-and-sustaining-technology/replacing-and-upgrading-technology

no longer meets the needs of the organization, the security has been compromised or lacks optimal effectiveness, or the software reaches end-of-life and thus no longer receives support from the provider (ex. Windows XP).

Most Common Problems

What are typical issues that arise with network connections and how can they be resolved?

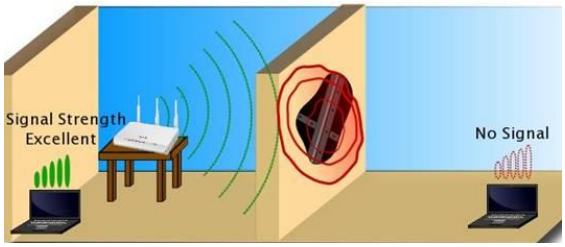
- Slow network speeds
  - Bandwidth overload
  - Need for more robust cabling infrastructure
  - Wireless access point (WAP) location and/or number of access points
- Loss of connection
- Server access errors
- Degraded cabling
- Outdated or malfunctioning equipment
- Compromised or out-of-date software

Equipment Malfunctions

If one or more of your employees are experiencing slow network connections, there are several culprits that could be at fault. Some of the issues can be resolved by replacing a damaged patch cable in your server room, adding access points, or upgrading from Cat5 cables to Cat6 or fiber optics (see **Preventative Care, Maintenance, and Upgrades of Equipment**).

There are several steps to take before considering major overhauls of your hardware and/or network operating system:

1. If using a wireless connection, plug into a hardline to determine if the issue is coming from a weak signal and/or a damaged access point. If connecting a device directly to a router resolves the network speed issue, then an analysis of your access point functionality is in order. If the access point is not damaged or malfunctioning, the problem may be in the location or the number of devices connected to a particular WAP. The best option at this point is to complete a site survey (see *When should access point coverage be evaluated?* under **Preventative Care, Maintenance, and Upgrades of Equipment**).



2. If the device is not accessing the system when hard-wired, swap out the patch cable from the device to the wall jack to determine if the issue stems from a damaged cable. If this does not work, connect the device directly to the router in order to evaluate whether another patch cable to switches or routers may be

to blame. If connectivity issues are resolved by connecting to the router, then you will need to backtrack through the system to determine if there is a faulty patch cable or horizontal cabling along the network path.

3. If a direct connection to the router does not restore your network speed to a desired pace, the problem could be an overload of your bandwidth, limited cabling capabilities (i.e. need for Cat6 or fiber optics rather than Cat5), or a problem with the telecommunication company. Swapping out network infrastructure cabling can be an expensive and timely process, so it is best to exhaust the other options first. Contact your service provider to ensure that they are not experiencing internal errors and find out if your company can upgrade your service plan to receive greater bandwidth.

Continual monitoring and maintenance of all hardware can mitigate the majority of the above-mentioned risks and prevent time-consuming and often costly restructuring and/or overhauls of network systems.

Security Dilemmas

A major concern in setting up and maintaining network systems is the potential for viruses, malware, and hackers invading your system and causing damage to your devices and/or exposing sensitive information to unauthorized viewers. To mitigate the risk of these threats it is important to run scans on all network-attached devices on a regular basis and educate your employees on the importance of avoiding and reporting suspicious sites and emails. All networks should be password protected and only key players should have access to the most sensitive information on your servers. The best approach to network security is a proactive preventative maintenance plan rather than a reactive one, but it is important to have a plan in place in case your system does fall victim to a breach.

Tips for Preventative Maintenance:

- Change passwords once a month
- Make sure anti-virus software is up-to-date
- Run full network scans weekly
- Maintain the most sensitive data on a separate server
- Backup new files on a daily basis and run a complete backup weekly
- Protect every connection with passwords
- Use data encryption

Steps to Take if an Attack Occurs:[4]

1. Identify the attack
2. Quarantine the infected servers, computers, and devices
3. Disinfect the network
4. Disclose the attack to proper channels (seek advice of legal and PR teams)
5. Re-secure network with new passwords and training of employees on security best practices

Average Cost of Service

Between actual equipment costs and the fees for service, network maintenance and repairs range from as little as $100 or less to upwards of $10,000.

- Router and the wiring: **$238 to $674** on average.[5]
- Contractors average from **$65 to $85 per hour** (excluding travel expenses) and IT specialists even more[6]
- Cat6 cabling is **$250** for every **one thousand feet**. [5]
- Wireless Access Points: **≤$20 to upwards of $10,000**
- Network Security Platforms: Average from **$5,000 up to $20,000+** depending on size of network to be protected and features required
- Anti-virus software: Generally falls in the **$1000-$3000** range for software compatible for business security

Average Time Needed

The amount of time it takes to install a single access point does not vary much and is not very time-consuming (assuming the wiring is already in place). However, running cable through an office (especially one that is *not* under construction) can be very time-consuming and the time it takes to complete a cabling project varies greatly. This discrepancy in timeframe is based on the cable run length, the current infrastructure of the building, the number of contractors hired to complete the job, and the hours at which the contractors actually have access to your network equipment (i.e. before, during, or after business hours).

Cabling, Access Points, and Routers

The average timeframes needed to complete networking projects are as follows:

---

[4] http://www.seculert.com/blog/2013/07/network-compromised-5-critical-steps-to-handling-a-security-breach.html

[5] http://www.redbeacon.com/hg/computer-network-wire-installation-cost/

[6] http://www.fixr.com/costs/upgrading-to-cat6-cabling

1. Replacing a wireless access point:

   If your access point is just being swapped out, the process will generally take about 15 minutes. However, configuration/programming may be needed which will require additional time. Keep in mind that most technicians will charge for minimum visit duration, which is typically 1 hour.

2. Replacing, adding, or removing routers/switches:

   The amount of time required for work will be vastly different between routers and switches, as routers are typically only a few connections and a switch (depending on size) could be from 24 - 100+ connections. It also depends on if the technician is doing a live cut (while people are working) or if they are doing an 'off-hours' cut (these go quicker due to no users on the network). There may also be a need to do configuring/programming, which adds time to the project. Some level of testing with a client's network support or help desk personnel will be of necessity, so again the timeframe is extended.

3. Running cable through a building (currently under construction):

   The size of a building won't have too much of an impact on running a cable if the building is under construction. Regardless of the size of the building, the furthest a cable can be ran is 100 meters (328 feet), so the question then becomes:
   What is the average cable run length and time to install each?

   -Short runs (up to 100 feet or so): Typically 1 hour
   -Mid runs (up to about 200 feet): Typically 1.5 hours
   -Long runs (up to 300 feet): Typically 2 hours

   Note: all of the average timeframes above depends on the assumption that there is a relatively clear pathway with no obstructions.

4. Replacing/upgrading network cabling in a completed infrastructure:

   Again, this has very little to do with the size of the building and more to do with the quantity of cables and average length of the cable runs. There's no average for the quantity of cables needed, as every business will have a varying number of cables installed. So, it is best to define how many cables constitute a 'small', 'medium' or 'large' office building and define the average cable run lengths of those cables. For a completed infrastructure, additional time may be needed for abatement (removal of old infrastructure), but on average a completed building will require slightly longer installation time.
   Time to install cable runs in a completed building:

   -Short runs (up to 100 feet or so): Typically 1.5 hour
   -Mid runs (up to about 200 feet): Typically 2 hours
   -Long runs (up to 300 feet): Typically 2.5 hours

Cleaning and Repairs

Equipment should be regularly wiped down and/or air-dusted to ensure unwanted debris does not interfere with the copper connections and other sensitive equipment. From time to time it is necessary to do a more thorough cleaning, which may require unplugging cables and ensuring the network is re-connected properly. This may require

hiring an outside resource if an internal IT team is not available. The amount of time it takes to wipe down equipment and blow out any micro-debris will depend on how extensive your server room is. Generally this will take less than an hour for businesses with small-scale network housing, but could take a day or more for businesses with a large room –or rooms –of network equipment.

As for repairs, these should be done as soon as an issue arises and can vary based on the equipment that needs to be replaced. The timeframe is also dependent on whether it is just a component of the system that needs replacement (often requires less time) or if a full swap-out is required. *See Most Common Problems for situations that may arise.*

Conclusion

Key Takeaways:

1. Think proactively: regularly service your equipment, update your operating systems, and scan your network for potential threats.
2. Find technicians and/or IT partners that are reliable, skilled, and trustworthy to handle maintenance and security of your network.
3. Set aside a budget for routine maintenance as well as worst-case scenarios (i.e. complete system failure, network-wide data breach, etc.).
4. Limit access to sensitive files and regularly change passwords, but have a plan in place to re-secure your network and manage publicity if a security breach should take place.

Keeping networks up and running at their optimal levels in regards to efficiency and security requires planning, diligence, and proactive thinking. Failing to monitor your system continually and engage in preventative maintenance may lead to costly failures.

For assistance, questions, or concerns regarding this manual or your network infrastructure, visit www.worldlinkintegration.com **or contact us at** 949-861-2830**.**