Maintaining your Optigo Connect network: Hardware and Software

Follow this guideline to help maintain your Optigo Connect network. Even if you cannot follow these suggestions to the letter, remember that it is better to check devices and update software sometimes than never.

Hardware

Check components | Quarterly

- Naturally over time as people work around, knock into device racks, and nudge or kink fiber, some device components can come loose. Check key parts, to ensure they are all fully seated.
  - Make sure that your universal power cord is well-seated, especially in the back. The cords can loosen, particularly as devices heat up.
  - Check that your RJ45 connections are seated tightly. When you press down on them, they should not come loose easily.
  - If you have redundant power supply sources, ensure they are both plugged in tightly. That way, if one loses power your redundancy will not be at risk because the other one is plugged in.
  - Replace any pieces that remain loose after you plug them back in. If that component is worn out, this is an easy, inexpensive way to prevent bigger problems in the future.

Check attenuation | Annually

- An optical power measurement tool is a handy device to measure the attenuation running through the fiber. This will help you keep tabs on whether your laser power is dipping too low or going too high.

Software

Update passwords | Annually, at minimum

- Ensure that your passwords are secure and difficult to guess (e.g. avoid "Password" or "1234").
- Consider who has access to passwords, and therefore the system. Match your or your customer's security policy, and update passwords annually, at minimum.

Upgrade firmware and software | Whenever updates are available

- Keep track of device firmware versions and warranty end dates. Some asset management programs will do this for you. Check everything before the warranty end date, and check annually to see if firmware is out of date.
- Know your software versions, and update to the latest versions as often as you can. It is best to make updates and upgrades on *your* schedule — rather than being taken by surprise when something breaks, or your network is hacked because of a software vulnerability.
- Software updates should be planned, and your customer should be informed before any big changes are made. If you are going to update software on a new controller, test it in your office *before* pushing it out to hundreds or thousands of devices.
- Take a top-down approach on updating your systems: if you have a supervisory controller with controllers underneath it, update at the top and then work your way down to the smallest edge devices. Keep your customer informed and test along the way.

Generate a report | Whenever you are on site

- Through Optigo OneView, generate and save a report. This gives you a periodic comparison so if something goes wrong on the network, you will have those reports to refer to.

Document device lists and configurations | Whenever you are on site

- After your initial setup, you will also want to back up your configurations in OneView. That way any changes that have been made since you originally configured your system will be preserved. Someone might have swapped a VLAN around, and if you forget that and a switch fails, you will lose the information.
- The same is true for any of your backend IP devices. Whenever you are on site, do a scan and make sure you have a copy of the latest scan with all your devices listed there.

Optigo Networks Inc.
1200 – 555 W Hastings St., Vancouver, BC, Canada
www.optigo.net | info@optigo.net | 1-888-629-6559