mxn corp

QUARTERLY NEWSLETTER

Updates from Bob

2920 Switch Replacement

Hewlett Packard Enterprise

Business Partner

For a long time, the 2920 switch has been Hewlett-Packard's high-end, managed, layer 2 stackable switch, but now it's been replaced by two new switches—the 2930M and 2930F. Both collect PoE and non-PoE gigabit end device connections and then forward them along over gigabit, 10 gigabit and (now) even 40 gigabit Ethernet uplinks. Both come in 24- and 48-port stackable switches models, but you need to consider your requirements and pick one or the other. They can't seamlessly interoperate in the same wiring closet, so you need to choose one or the other.

If you still need to connect lots of wired ports in any wiring closet to a backbone network—the traditional network architecture—the 2930M (Modular) switch line is the best choice. You can stack up to ten switches in a single stack that can be managed with a single IP address, and you can download and upgrade firmware to the entire stack. You can create redundant stacking links between each switch in the stack, using 2-port stacking modules in each switch, and then add proprietary 25 GBPS stacking cables. You can then install a variety of uplinks into one or more of the switches in the stack—10 gigabit Ethernet SFP+, SmartRate RJ-45, or 40 gigabit Ethernet QSFP. There's also now a switch with 24 SmartRate ports in the front, if you need to do high-capacity wireless connections to support highest-capacity wireless access points. The 2930M switches have a variety of power supplies, and you can install redundant power supplies in each one.

Downsides to the 2930M? They are more expensive, and the connections are in the back of the switches, which can cause problems in tight (shallow or crowded) racks.

The 2930F switch alternative is designed for wiring closets with more modest requirements for lots of copper PoE and non-PoE ports. Hewlett-Packard calls this their 'wireless first' alternative. You can still stack up to four switches and manage them with a single IP address, using the Virtual Switch Fabric (VSF), which is used to turn two 5400R switches into a single virtual switch. These switches have no module slots in the back; each switch comes with four SFP+ ports on the front. Any port can be a 10 gigabit uplink, or it can support a switch stack using a 10 gigabit DAC. DAC can also be configured in a 'ring' configuration of connected switches. You can't uplink switches at more than 10 gigabits/second, and the switches don't support SmartRate (so you can't support full bandwidth from an AP335 or an AP345). And—make a note here—the 2930F switches don't support LRM optics, which means that if you have older 62.5-micron fiber backbones, you won't be able to uplink switches at 10 gigabit Ethernet. But these switches are less complicated and less expensive, and they have all connections on the front.

New Security Product

Anyone reading about the hell that the City of Atlanta has fallen into lately? It has been over three weeks, and their hacked systems still are not up and running. The SamSam hacking team that hit Atlanta has made well over a million dollars in ransom income in 2018 by concentrating on local governments, hospitals and universities because these organizations can't afford to be down for extended periods of time and don't haven't the staff and the tools to prevent attacks. Organizations just quietly pay the ransom and hope that the hackers restore their services. We expect that the City of Atlanta will soon add $51,000 in BitCoins to that running haul, because after paying huge sums to consulting and disinfection companies, they'll realize that paying ransom and hoping their systems get unlocked is the most effective alternative. They seem to be having to completely re-create some of their systems from the ground up, and so far the consulting bills are more than $2.7 million. Yes, they have lost.

Atlanta will soon be joined by other potential victims that currently have ransomware quietly spreading through their networks and networked servers. This new ransomware is designed to spread quietly without immediate detonation and getting itself into multiple backups, so that it can't be defeated by wiping a server or workstation clean and restoring it from a backup. These new victims will shortly be facing significant disruption, embarrassment, and large unanticipated costs.

Running conventional anti-virus software on clients and firewalls won't solve the problem, because the polymorphic malware is designed to stay newer than any signatures used to identify and delete it. The Internet-of-Things also means that networks will more and more be home to devices that can't be controlled, like the salt-water fish tank in the lobby of the Las Vegas Casino that was used to loot it for $30 million.

We think that you have three options.

The first option is to do as you have so far: continue to whistle past the graveyard, hoping that you somehow will be spared. Small size no longer seems to be a defense, however: at about the same time as the City of Atlanta attack, the City of Loganville, a much smaller suburban Atlanta city, was also attacked, with citizen and employee personal information stolen. Pervasive networks mean that it's now easy to reach any victim with very little effort. So why not pick on smaller organizations, with much less well-developed defenses? Everyone will soon be a target.

The second option is to assume that you will be attacked and prepare for it. Arrange to get a BitCoin account so that you can meet the ransom demands quickly and hope that the hackers will unlock your resources after you pay it. Just to be safe, assume that they won't, and buy malware insurance to fund your future consulting and remediation expenses. This insurance is expensive and will get more expensive as the pace of attacks grows, but it'll still be less expensive than funding recovery out of your own pockets, and you can budget it now rather than having to scramble for funds later. Start interviewing remediation firms immediately, select one or more of these very soon, and guarantee a premium to have priority service delivered to you when the hack occurs. Priority service is important because the increase in attacks makes remediation and security consulting technical time hard to come by—reserve your place in line now with a payment premium! Make contingency plans to run your organization offline until you can restore electronic service by ransom or rebuild. Do as the City of Atlanta has done—lay in paper and pencil, and pre-printed forms and filing cabinets to hold the filled-in forms. Also, plan to top off your BitCoin account periodically, because after paying the next ransom you'll become known as an easy mark, and others will be in line to lock you up and blackmail you.

The third option is to work to do something about actual prevention and add products to your existing security systems to counter malware attacks. Yes, there are a few products out there, and they are inexpensive, easy to run, and effective.

Ask us about providing you with the least expensive and disruptive option.

Cloud Nine?

Establishing a ‘local cloud’ is now the least cost option if you want to implement a new voice over IP system. There’s an excellent chance that you already run some virtual servers to do local computing; voice over IP is then merely a set of three or four inexpensive controllers (less than $1,000 each) installed on your servers, plus the cost of IP phones and phone licenses. Additionally, if you already have IP phones, you can use those. The typical VoIP system can be installed and configured, and cut over, in about two weeks.

HPE Aruba Product Updates

ClearPass 6.7.1 Release

We are pleased to announce the immediate availability of ClearPass 6.7.1! In addition to bug fixes, this release also includes several new features that our Engineering and QA team have worked tirelessly to include:

- Improved TACACS+ license consumption model. TACACS+ is no longer consumed using the session-based model introduced in ClearPass 6.7.0. With only 100 Access licenses, a customer can now use TACACS+ for an unlimited number of network devices and/or administrators. Just add appliances to scale up based upon demands.
- Ability to Rollback a Cumulative Patch.
- ClearPass now supports downgrades from major (pre-6.7 feature) and minor (NEW) releases, e.g. 6.7.1 -> 6.7.2 -> 6.7.1.
- Support for SNMP IPv6 targets.
- ClearPass can now send SNMP traps to IPv6 enabled trap receivers.

AirWave 8.2.6 Released

The AirWave team is celebrating Aruba's 16th birthday by releasing our version 8.2.6, which the team has worked very hard on. In this release, we have continued our commitment to adding features to help with management of Aruba switches, added support for the latest Aruba devices, and added customer-requested features that enhance usability.

A few highlights:

- New device support:
    - 8320
    - 2930F
    - AP303

- New Firmware support:
  - AOS-S 16.05
  - AOS 8.2
- The feature formerly called AppRF is now **Traffic Analysis**. We renamed it because the feature supports both wired and wireless clients, and because Traffic Analysis is a more accurate description of what is provided.
- Configuration backup, diff and restore. For all Aruba switches, we save a history of configuration backups and provide workflows for a user to differentiate a config against backed up configs or another device's config, and an easy way for the user to restore a switch to a previous config.
- A user can now execute CLI commands on a device from the topology view.
- A report definition can now be duplicated, allowing a user to re-use report profiles.
- VisualRF now supports replacing a floorplan's background image.
- Third party support: Cisco 28xx APs, and added support for newer versions of WLC firmware

Mitel Product and MXN Mitel Service Update

Manufacturer Discontinuance Notice: Cordless Accessories for Mitel 5300 Series

Mitel announces the Manufacture Discontinuance (MD) of the Mitel 5300 Integrated DECT Headset / Handset / Module and Mitel 5300 Bluetooth Module / Handset. **Read on in our Mitel Notice bulletin…**

Inside Sales

Our Inside Sales department would like to remind our valued customers, that while our sales staff is often on the road seeing customers, we are in the office five days a week. You can reach us at insidesales@mxncorp.com to request quotes for new products or support renewals, submit purchase orders, or if you have any questions at all. Please let us know if there is anything you need!

Deborah, darnett@mxncorp.com, 770-926-6762
Tricia, twillman@mxncorp.com, 678-981-5310

Support

Please see our **MXN Professional Services and Support Brochure** for a description of all MXN support offerings. We are here to help!

MXN Professional Services and Support
Common-Sense Economical IT Service and Support Programs
support@mxncorp.com