TECHNOLOGY SOLUTIONS

115 Enterprise Drive
Gretna, Louisiana 70056
Tel: 504.367.1650
www.ictcomputer.com

E-Rate Spin: 143019788

March 01, 2016

Prepared for**: ST. CHARLES PARISH PUBLIC SCHOOLS**
13855 River Road
Luling, Louisiana 70070

Reference: RFP: Network Infrastructure Upgrades
February 04, 2016

Dear Saint Charles Parish Public Schools,

Please find attached our proposal to provide equipment and professional services to Saint Charles Parish Public Schools.

Under contract arising from this solicitation, ICT understand the responsibilities to deliver the turn-key solution to Saint Charles Parish Public Schools. Scope of work will be installed, configured all proposed Network equipment contained in this proposal and ensure interoperability with existing Network infrastructure.

We would like to thank you for the opportunity to present this proposal and look forward to serving you in the near future.

Thank You,

Thuy Lam
Account Manager
ICT Technology Solutions
504.400.9060 mobile
thuylam@ictcomputer.com

Table of Contents

Letter of Transmittal

Contacts:

Dang Trinh
Operations Manager

115 Enterprise Dr.
Gretna, Louisiana 70056
Office: 504.367.1650
Mobile: 504.491.8523
dangtrinh@ictcomputer.com

Thuy “Tweetie” Lam
Account Manager

115 Enterprise Dr.
Gretna, Louisiana 70056
Office: 504.367.1650
Mobile: 504.400.9060
thuylam@ictcomputer.com

Through comprehensive, collaborative efforts, ICT offers optimized solutions for complex IT challenges. Our twenty-two year tenure supporting the Louisiana School System coupled with our continued commitment to superior customer service guarantees our client’s satisfaction and productivity.

As Manager of Operations, Dang Trinh will take the lead in responding to your technical needs quickly and effectively throughout the duration of this project. As Account Manager and primary Client Liaison, Thuy “Tweetie” Lam is always available to address any questions or concerns regarding your current or future projects with ICT.

Company Profile

ICT, Inc. is a **Louisiana Minority-Owned and self-certified SBA** business providing quality and innovative technology solutions. Founded in 1990 to address the emerging need for comprehensive support in Information Technology in Greater New Orleans Area schools, ICT, Inc. has been committed to providing superlative solutions to all of the technical challenges for small and large businesses, as well as educational and governmental institutions. Located in Gretna, Louisiana, our local presence affords our clients quick and timely response to their needs.

At ICT, meeting our clients' needs is our first priority. We evolve with technology's ever-changing landscape in order to provide only the most efficient, cost-effective and up-to-date sustainable solutions. Our veteran and seasoned team of IT professionals are committed to the highest level of service.

References

RECOVERY SCHOOL DISTRICT of LOUISIANA
Mrs. Kamala Jackson-Baker, Director of Technology Integration
SFMOP Capital Department
Office: 504.373.6200 x.20045
Cell: 504.232.1215
Kamala.Baker@rsdla.net

ICT currently manages the full Network Infrastructure installation and implementation under FEMA new school rebuilding.

ReNEW SCHOOLS
Sean Hudson, Executive Director of Information Technology
Office: 504.941.1185
sean@renewschools.org

ICT manages, supports, and maintains the Network Infrastructure of all schools within ReNEW Charter.

Ascension Parish Schoolboard
Mr. Carl Fontenot
Office: 225.391.7133

ICT provides Aruba wireless and help install a demo school.

KIPP NEW ORLEANS
Glen Walker, IT Director
Office: 504.565.6143
gwalker@kippneworleans.org

ICT manages, supports, and maintains the Network Infrastructure of all schools within KIPP New Orleans Charter.

InspireNOLA CHARTER SCHOOLS
De Rhonda Holmes, IT Director
Office: 504.302.7197
DeRhonda.Holmes@inspirenolaschools.org

ICT manages, supports, and maintains the Network Infrastructure of all schools within InspireNOLA Charter Schools as well as full desktop and notebook support for all schools within the charter.

Evaluation Prerequisites

Experience

ICT currently supports E-Rate Manage Internal Broadband Service (MIBS) and non-Erate Network Infrastructure Support for multiple schools and charter groups including, but not limited to:

- Audubon Charter School
- Einstein Charter School
- Edgar P. Harney Elementary School
- Morris Jeff Community School
- Fannie C. Williams Charter Schools
- Arise Academy
- New Beginning School Foundation
- KIPP New Orleans
- New Orleans Marine and Maritime Academy

ICT has a full complement of IT specialists to suit all of our clients' needs including:

- Cisco Engineers
- Microsoft Engineers
- A+ Certified Technicians
- Dell Certified Technicians
- Server Administrators
- Network Administrators
- Telecommunications Administrators
- Account Managers
- Helpdesk Technicians
- Network Technicians
- Printer Technicians
- Smartphone Technicians

ICT has installed, implemented, and maintained the entire IT infrastructure for multiple schools throughout the Louisiana School System for over twenty-two years.

Availability

Twenty-four hour Network Monitoring is available for all ICT clients seven days a week. Onsite service is available Monday through Friday, 7:00AM to 5:00PM. System upgrade services are scheduled for after school hours or on weekends to reduce possible network downtime for client school. Dates and times for such services are adjusted based on client preference. Helpdesk services for ICT clients are available for all hours of operation.

Minority Business Status

ICT is a SBA and Louisiana-minority owned small business.

In State Preference

ICT is a Greater New Orleans Area locally-owned business serving Louisiana since 1990.

Certified in Hudson Initiative and SEBD.

Project Management Experience

ICT has extensive Project Management experience within the Louisiana School System. Three recent examples:

1. Full integration of all schools within the Recovery School District Network including the wired and wireless networks, servers, call manager, and email services.

2. Full migration of Sophie B. Wright, Einstein, and Audubon Charter Schools from the OPSB network to independent domains for each.

3. Migration of Edgar P. Harney Elementary and Intercultural Charter School from the Recovery School District network to their own independent domains.

Statement of Work

ICT is submitting this proposal in response to the E-Rate Form 470 for Wireless Upgrade 2016-2017. This Statement of Work ("SOW") describes the Managed Deployment Services to be provided by ICT to International School of Louisiana.

Methodology

In order to successfully provide the clients with the expected results, the project will be divided into the following steps:

1. Network Assessment:

An assessment of the client's network will be done by ICT in order to correctly integrate new infrastructure:

- Network topology (Switches, Router, Wireless, VoIP
- Server infrastructure (DNS/DHCP, AD)
- Wiring Infrastructure (Fiber, Drops and Power requirement)

2. Network Design
   - Sample network configuration submitted to client for approval
   - Design customized to incorporate current configuration to minimize interruption
   - Design further tailored to optimize the functionality of new equipment
   - Complete design created to optimize client infrastructure to maximize synergy between current systems and new systems that are to be integrated.
3. Network Planning
   - Meet client face to face to get an assessment of their project vision
   - Make recommendations based on network assessment
   - Assign a project manager for each process
   - Work on timeline for each step of rollout
4. Network configuration and installation
   - Create an inventory of asset tags of all equipment according to client specification
   - Power up and burn in all equipment
   - Configure equipment based on design by Network Engineer
   - Test configuration based on design by Network Engineer
   - Label and inventory equipment according to location and design
5. Onsite installation and testing

6. Move equipment to school site
   - Remove old equipment from current site and document remove equipment
   - Install new equipment to current or new rack
   - Patched in all Fiber and Cat. Cables

- Power up and test for functionality of each piece of equipment
- Cleanup and removal of all debris incurred during installation process

7. Live testing and Documentation

   - A working environment testing will be done with presence of client
   - Documentation of install network will be provided to client with all IP address, configuration and Password to all install equipment

8. Network monitoring (basic maintenance)

   - ICT will install a monitoring server @ no cost to client to monitor client network infrastructure
   - Client appointed contact can be setup to receive network outage and change management
   - Response time for minor network problem will be 24 hrs. And major network problem will be 4 hrs.
   - ICT will also provide helpdesk to help with other networking issues.

Proposal

Wireless

For wireless networking, ICT relies on Aruba Enterprise standard equipment to create a stable, secure wireless network centrally controlled by a Virtual WLC connected directly to the Main Distribution frame and controlling wireless access points throughout a client's school. This allows for maximum coverage and expandability as well as preventing connectivity outages in the case of any possible access point malfunction.

Wireless on Common Core:

With the onset of Common Core, a growing number of schools are adopting technology initiatives to deliver a rich learning experience by engaging students through the devices and applications they thrive on.
Textbooks are being swapped out for e-books that download content in real time. Transition to district-wide online testing is becoming critical. One-to-one and BYOD initiatives are becoming more popular than wired computer labs. Skype and Google Hangouts are fueling new study groups. And virtual field trips are creating new student development opportunities.
As a result, IT must look to the future and build a next-generation infrastructure that supports digital classroom learning and emerging technologies. Following are the critical steps that can help you build a next-generation classroom for Common Core and beyond. Start with a robust Wi-Fi infrastructure
Supporting digital learning, especially in one-to-one environments, means you'll need a Wi-Fi infrastructure that can support the influx of mobile devices along with the bandwidth-hungry applications running on them. There are several things you can do to prepare for this.
Plan to support 3-4 mobile devices per student, teacher devices, wireless printers, and other wireless equipment in the classroom. That means, in a classroom of 30 students, about 100 devices will connect to the network.
Assess classroom application needs by collaborating with teachers to support a rich multimedia curriculum. For example, HD-quality video streaming requires 4 Mbps and interactive learning games require 1 Mbps of bandwidth per user.
Don't let poor access point (AP) performance drag down the entire network. As students roam between APs, their devices can get stuck on an AP instead of associating with a closer one that has a stronger signal.

Aruba recommendation:

Migrate to an 802.11ac WLAN with advanced RF management capabilities. Most Aruba K-12 customers are deploying one AP per classroom for a richer Wi-Fi learning experience. As more users, devices and apps connect, 802.11ac can best handle the increased network traffic. It gives you faster gigabit throughput and greater client density. It even makes 802.11n devices go faster. Learn more about best practices for migrating to 802.11ac. WLANs with built-in RF management technology can get rid of sticky clients by gathering session performance metrics from devices and using this information to steer them to the best AP and radio. Learn more about Aruba's patented ClientMatch™ technology. Next-Gen Classrooms for Common Core & Beyond Executive Overview Ensure a stable academic testing environment. New student testing systems based on computer adaptive technology such as Smarter Balanced and PARCC required by the new Common Core curriculum have published bandwidth recommendations for testing readiness. For instance, PARCC recommends 5-50 Kbps bandwidth per user for testing, which adds up to 1.5 Mbps in a classroom of 30 students.However, the Common Core curriculum requirements of a rich digital classroom exceed these test requirements. The more important considerations for creating a reliable testing-ready Wi-Fi infrastructure are fair wireless access for all students and the ability for IT organizations to easily manage test traffic on the network. This can be done by ensuring that no test devices get preferential network access and that all students have a similar testing experience. Airtime fairness, an RF management feature that provides equal access for all Wi-Fi clients, must be present in all classroom WLANs. Most critical is creating a controlled academic assessment environment. The best way to do this is by making sure that test traffic gets priority treatment over other types of traffic on the network.

Deploy a smart WLAN that gives you application-layer visibility and control. Smart WLANs recognize different types of traffic on a network and let you assign the highest priority to more important testing traffic. This capability is essential to building a solid and reliable testing environment. In addition to testing, this application-awareness allows you to block the use of inappropriate apps and apply quality-of-service to delay-sensitive video instruction media. See how Aruba AppRF technology works. Empower teachers While technology enhances learning, it also creates new challenges for teachers in a digital classroom as students can get easily distracted on their mobile devices.To meet this challenge, give teachers greater visibility and control over how mobile devices are used in their classrooms. This is the best way to minimize distractions and ensure that students stay on task.

Choose a purpose-built classroom management system from a solution provider who specializes in classroom applications. Award-winning classroom management systems like LanSchool empower teachers by allowing them to observe and control student device screens, co-browse, block apps and keep everyone focused on learning. LanSchool uses efficient screen capture and transfer methods. For instance, if the entire teacher's screen is changing, LanSchool only uses about 24 Kbps to transfer that image to the students' screens. This is less than 1% of a 100 MB network. Next-Gen Classrooms for Common Core & Beyond Executive Overview Support BYOD with confidence Students, teachers, staff and guests connecting to the school network with a variety of personal devices creates a tough challenge for IT.
How to you give Wi-Fi access to these devices and keep the network secure with limited IT resources? Choose a device onboarding solution that best meets your needs. If you're strapped for resources like many K-12 IT organizations, you'll want a solution that automates and simplifies the onboarding process without sacrificing access security. Once onboarded, enforce differentiated network access based on contextual information like user roles, device types and location. This contextual granularity is vital to securely manage and enforce differentiated policies. Leverage low-cost technologies Schools everywhere are exploring network-shared devices like Apple TVs as low-cost alternatives to traditional projectors. However, it's important to consider how they can be securely deployed on your network. Consequently, you'll need to prevent students from hijacking Apple TVs to share inappropriate content or causing disruptions in class. At the same time, teachers must be able to grant access to groups of students who present their projects to the class.

Deploy a network access solution that simplifies device onboarding with self-enrollment and grants network access privileges based on user roles, device types and location. For onboarding, consider a simple captive portal that displays a web page, similar to a Wi-Fi hot spot. Here, students can simply accept the connection or sign in using their school credentials if you want to map traffic back to an individual user 802.1X authentication with AES encryption is even more secure. Users can simply enter a user name and password or they can self-enroll by automatically generating and installing device certificates through a web portal with no IT assistance. Let users onboard their own devices and control access based on contextual data – user roles (students, teachers, staff), device types (laptops, tablets, smartphones) and location (classrooms, common areas, district offices). Learn how Goddard Public Schools onboarded 5,500 students.

Choose an access management solution that securely enables network-based AV services over the air and allows you to enforce policy-controlled access. Look for a solution that lets you control which AirPlay and AirPrint devices are visible to teachers, students and staff. This visibility should be based on a user's role, location and what device they're using. See how Fraser Public Schools included Apple TVs in their 21st Century learning environment. Next-Gen Classrooms for Common Core & Beyond Executive Overview Simplify network management. Despite having limited IT resources, you can keep digital classrooms running by looking beyond traditional network management for a simpler and more cost-effective multivendor solution that meet your district needs. Opt for an integrated management solution rather than multiple, siloed point-products that solve only one or two management issue. This approach will enable you to better manage IT time and resources. Also be sure that your solution of choice can manage the application and device experience of users on multivendor networks that extend across geographically dispersed locations – from school campuses to district offices and maintenance yards. If IT resources are scarce, you should definitely consider a cloud-based management solution. Cloud-based management can reduce the cost and complexity of IT operations by eliminating the need to install and maintain lots of individual management appliances.

Choose a multivendor network management solution for a complex network infrastructure or a cloud-based solution for a simple and cost-effective deployment. Whichever you choose, be sure that your solution of choice allows you to manage multiple generations of wired and wireless networking equipment from multiple vendors through a single, centralized pane of glass. Cloud-based management is subscription based with network management services hosted in the public cloud. The great thing about cloud-managed Wi-Fi is that it reduces both capex and opex. Learn how Fairfax County Public Schools centrally manages Wi-Fi at 238 locations. Mobilize the wired network The wired networks that used to support teacher and staff devices and a handful of computer labs must be upgraded to meet the dynamic requirements of mobile learning. To mobilize your wired network, it’s important to avoid creating bottlenecks where traffic enters your access switches. For example, 802.11ac supports gigabit Wi-Fi speeds so your access switches should be equipped with 10 gigabit uplinks. It’s also important to anticipate how you’ll modernize and support network and IP services as hundreds more mobile devices wirelessly connect at every school. And with wireless outpacing wired, what should you do with all those unused wired ports? Next-Gen Classrooms for Common Core & Beyond Executive Overview

Mobilize your wired infrastructure to support the network and IP services you’ll need to handle the onrush of mobile devices. Wired networks that are designed for mobility apply policies to users and devices based on the same contextual data as wireless. So instead of creating and managing separate access policies for wired and wireless, you’ll have one consistent set of policies for both 802.11ac is designed to support digital learning in classrooms that have high concentrations of mobile devices. Get your wired network ready for 802.11ac by supporting the latest APs on every 802.3at PoE+ port and 10-gigabit uplinks to unleash the full potential of gigabit Wi-Fi. Rethink VLANs. Consider software-defined flow-based policies that optimize wired and wireless traffic paths without changing your existing network. Also consider how you’ll scale DHCP and AAA servers to handle the influx of mobile devices.

Rightsize your wired infrastructure by reducing the number of switch ports in your wiring closet. In doing so, you’ll reduce your capex and opex and be in a great position to redirect the savings to digital learning initiatives for the classroom.

Conclusion

With the right network infrastructure planning, you can not only be Common Core-Compliant, but also empower teachers and students to leverage the latest technology in devices and applications for a richer learning experience while streamlining IT operations across campus.

Summary of Aruba recommendations for a next-generation classroom:

- Deploy one 802.11ac AP per classroom to address device density and rich applications.
- Prioritize testing traffic on the network for a reliable and controlled test environment.
- Keep students focused on learning with purpose-built classroom management systems.
- Simplify the onboarding process by having users enroll their own mobile devices.
- Grant network access privileges based on user roles, device types and location.
- Strengthen the security Apple TVs in classrooms using policy-based access controls.
- Simplify network management and migrate toward a mobility-centric infrastructure.

Technical Response
Wireless
Our Bid comply to all the requirement below

2.1.2 The solution being proposed must satisfy all of the requirements listed below. Vendors must state compliance in their response. If there is an exception to the listed requirements, the vendor must provide a detailed explanation of the proposed alternate.

2.1.2.1 Access points must be based on 802.11ac and 802.11ac wave 2 radio technology.

2.1.2.2 Access points must be able to provide connectivity for at least 35 devices (35:1 ratio) simultaneously.

2.1.2.3 Access points must support multi-user MIMO with three spatial streams and/on SU-MIMO with four spatial streams.

2.1.2.4 Access points must support up to 16 BSSIDs per radio.

2.1.2.5 Access points must be backwards compatible to support 802.11 a/b/g/n.

2.1.2.6 Access points must include radios for both 2.4 GHz and 5 GHz.

2.1.2.7 If controller-based solution is proposed it must support high availability allowing a second controller to take over duties with minimal disruption.

2.1.2.8 If controller-based solution is proposed it must support client connectivity in the event that a WAN outage disrupts communication between the access point and the controller.

2.1.2.9 Solution must offer access points with internal and external antenna options.

2.1.2.10 Solution must offer the ability to manage all access points as one wireless network via a single management platform.

2.1.2.11 Solution must support QoS capabilities and policy enforcements.

2.1.2.12 Solution must support technology to automatically configure RF settings such as channel assignment and transmit power.

2.1.2.13 Solution must support technology that optimizes overall network capacity in mixed-client environments by helping ensure that 802.11 a/g/n and 802.11 ac clients operate at the best possible rate.

2.1.2.14 Solution must support technology to steer dual band capable clients from 2.4 GHz to 5 GHz.

2.1.2.15 Solution must provide the capability of client moving from one access point to another without noticeable loss of connectivity.

2.1.2.16 Solution must provide a guest portal on a separate Vlan to allow unauthenticated user access to the Internet, yet still utilize the District's web filter.

2.1.2.17 Access points must be able to be mounted to drop ceilings or walls without loss of coverage area.

6

2.1.2.18 Solution must minimize interference from 3G/4G cellular network and distributed antenna systems.

2.1.2.19 Solution must offer wireless intrusion protection, rogue detection, and containment.

2.1.2.20 Vendor must describe warranty included with each brand/model of equipment proposed.

2.1.3 Vendor must describe their installation and testing procedures for the proposed wireless solution, and must include/address all requirements below.

2.1.3.1 Vendor will be responsible for un-boxing, asset tagging, and logging each piece of equipment in an asset tracking spreadsheet provided by SCPPS, in an area designated by SCPPS.

2.1.3.2 Any trash resulting from the un-boxing process must be disposed of by the vendor.

2.1.3.3 Vendor will be responsible for installing any necessary software and firmware updates.

2.1.3.4 Vendor will be responsible for configuration of access points.

2.1.3.5 Vendor will be responsible for mounting access points in designated areas as specified in agreed upon network design, and connecting access point to the network drop provided for that area.

2.1.3.6 Vendor will be responsible for testing every access point installed. Wireless coverage must meet specifications in the network design.

2.1.3.7 The installation of any access point model which will require more than one

network drop must be clearly communicated as such to SCPPS in your
installation response.

Our Bid comply to all the requirement below

2.2 Network Switches

2.2.1 The solution being proposed must satisfy all of the requirements listed below. Vendors must state compliance in their response. If there is an exception to the listed requirements, the vendor must provide a detailed explanation of the proposed alternate. Anticipated quantities needed are designated in the **SCPPS 2.2 Network Switches Cost Sheet.** Vendor must complete and submit proposed brands and models, along with costs, on the **SCPPS 2.2 Network Switches Cost Sheet**. SCPPS reserves the right to adjust quantities based on needs assessed throughout the project.
2.2.1.1 Layer 3 and Layer 2 switches functionally equivalent to, or better than, Avaya ERS 3549GTS-PWR+
2.2.1.2 Solution must offer SFP+.
2.2.1.3 Must support both 1 Gb/ 10 Gb speeds on each SFP port.
2.2.1.4 Must support multiple Vlans.
2.2.1.5 Must provide at least 48 ports capable of auto-negotiating 100 Mbs or 1 Gbs.
2.2.1.6 Must support Spanning Tree Protocol.
2.2.1.7 Must support IPv4 routing protocols (static, RIPv2, OSPF,EIGRP).
2.2.1.8 Must support Internet Group Management Protocol (IGMP) Snooping for IPv4 for multicast forwarding.
2.2.1.9 Must support IGMP filtering.

2.2.1.10 Must support telnet and SSH for remote management.
2.2.1.11 Must support QoS capabilities.
2.2.1.12 Must support stacking capabilities.
2.2.1.13 Must support POE+ and non POE options.
2.2.1.14 Must offer solution for management of multiple switches.
2.2.1.15 Vendor must describe warranty included with each brand/model of equipment proposed.
2.2.2 Vendor must describe their installation and testing procedures for the proposed network switch solution, and must include/address all requirements below:
2.1.2.1 Vendor will be responsible for un-boxing, asset tagging, and logging each piece of equipment in an asset tracking spreadsheet provided by SCPPS, in an area designated by SCPPS.
2.1.2.2 Any trash resulting from the un-boxing process must be disposed of by the vendor.
2.1.2.3 Vendor will be responsible for configuration of network switches.
2.1.2.4 Vendor will be responsible for placing and securing network switches in the designated racks, and connecting cabling to the network switches. Cable management within rack must be agreed upon with SCPPS prior to installation of network switches.
2.1.2.5 Existing network switches being replaced must be removed by vendor and placed in an area designated by SCPPS.
2.1.2.6 Vendor will be responsible for testing every network switch installed.

2.3 Cabling ** NO BID **

2.3.1 The solution being proposed must satisfy all of the requirements listed below. Vendors must state compliance in their response. If there is an exception to the listed requirements, the vendor must provide a detailed explanation of the proposed alternate. Estimated quantities needed are designated in the **SCPPS 2.3 Cabling Cost Sheet**. Vendor should reference the **SCPPS_Site_Maps** for location of fiber placement. Vendor must complete and submit proposed costs on the **SCPPS 2.3 Cabling Cost Sheet**. SCPPS reserves the right to adjust quantities based on needs assessed throughout the project.

2.3.1.1 Vendor (or proposed subcontractor) must have all applicable state licensing and be able to provide any additional statutory requirements (such as bonds or permits) as applicable for installing wired telecommunication services. Provide the name and license number of the company providing the wiring.

2.3.1.2 The contractor must be certified to install and terminate both copper and fiber.

2.3.1.3 All cable must meet the requirements of the National Electrical Code (NEC) except where other authorities or codes impose a more stringent requirement or practice.

2.3.1.4 Cabling must meet all local building codes and nationally recognized cabling standards, including BICSI, ANSI/TIA/EIA, and IEEE 802.3.

2.3.1.5 Singlemode fiber should meet or exceed the loss characteristics defined by either ITU or TIA standards.

2.3.1.6 All fiber should be indoor/outdoor rated, distribution style, singlemode fiber cable.

2.3.1.7 Plenum rated cable is NOT required.

2.3.1.8 Fiber connections must include termination on both ends of all strands into a mounted, 12/24-port, fiber optic enclosure (LIU) at each end and two fiber patch cables (2 meter, LC to LC).

2.3.1.9 Fiber must be terminated so that it is compatible with devices at each end.

2.3.1.10 Underground cabling (fiber) shall include the cost of trenching or boring as needed, appropriate PVC pipe, transition from PVC to EMT (up to 8 feet EMT included), building entry, and interduct (orange flex tubing). Where existing conduit is a viable solution, vendor and SCPPS must agree on a final solution.

2.3.1.11 No outdoor cabling shall be exposed. All outside tubing shall be watertight. For outside conduit, EMT conduit should be used above ground and PVC conduit underground. All tubing shall meet building and recognized cabling specifications.

2.3.1.12 No indoor cabling shall be exposed except in attics, above ceiling tiles, as patch cords, or unless approved in advance by SCPPS. However, fiber in attics must be in orange flex tubing (interduct) or conduit.

2.3.1.13 The cable installer must provide clean and legible as-built cable drawings and records in both hard and soft copy as part of system installation. These drawings must, at a minimum, show the location and type of all communication rooms, communication closets, all distributing cable runs, and all outlets. Cable records must include information necessary to correlate cable runs and terminating locations. Vendor may utilize the **SCPPS_Site_Maps** to assist in final drawings.

2.3.1.14 Category 6 drops shall include all needed supplies (i.e. Cat6 cable, jacks, etc.) and termination into patch panel and into jack. In some instances, other supplies might be required on certain drops like wall caddy, wall box and raceway. No Cat 6 drop will exceed 300 feet. This should be accounted for in vendor responses.

2.3.1.15 Cable accessories (ie. Jacks, Connectors, etc.) must include at least a 3 year warranty. SCPPS currently uses Panduit cabling accessories.

2.3.1.16 Vendor proposals shall address cabling services and cabling materials.

2.3.1.17 All cables, patch panels, and faceplates must be labeled using a permanent marking system. Handwritten labels are not acceptable.

2.3.1.18 All cables must be installed at least one foot from any fluorescent lighting unless contained in separate conduit, and four feet from other sources of electrical interference such as motors and generators unless otherwise agreed upon by vendor and SCPPS.

2.3.1.19 Cat 6 cables for access points must be purple, all other drops must be blue. Corresponding patch cables must match the color of the run.

2.3.1.20 Cat 6 drops should be pulled to the closest data rack.
2.3.1.21 All cable runs must be continuous from end to end. Cable splicing to achieve greater cable length is not allowed.
2.3.1.22 All data drops must be tested and certified. Certification reports must be provided to SCPPS.
2.3.1.23 Vendor must supply 1ft – 3ft patch cables as needed to connect from patch panel to switch.
2.3.1.24 Vendor must include the cost of racks and patch panels in the proposal. However, SCPPS

Equipment Details:

Indoor Wireless Access Points

Instant 224/225

Instant 214/215

Instant 204/205

- **Instant 224/225**

  - Ideal for boosting speeds on 802.11n and 802.11ac mobile devices
  - 802.11ac, 3x3 MIMO, 3 spatial streams, 1.3 Gbps
  - 2.4 GHz and 5 GHz radios
  - Internal and external antenna options

Instant 204/205

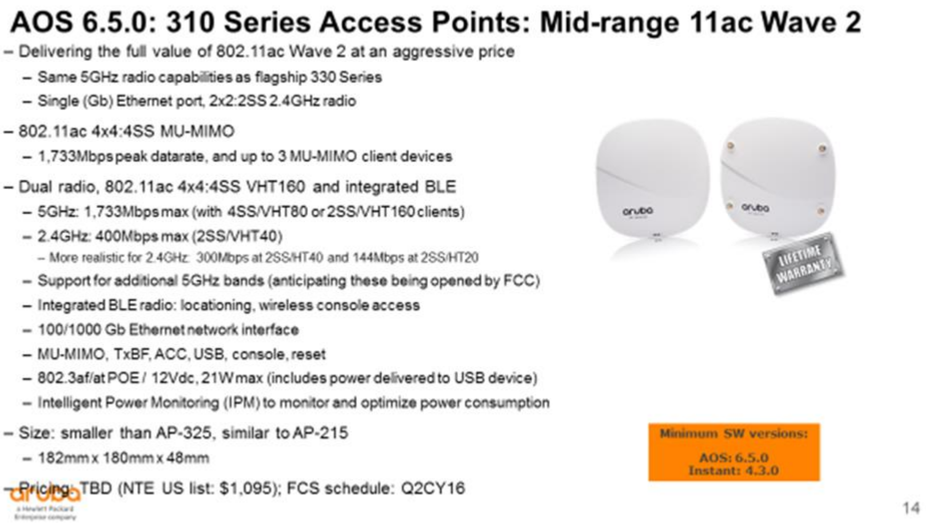
- AP-205 and IAP-205
  - 2.4-GHz (300 Mbps max rate) and 5-GHz (867 Mbps max rate) radios, each with 2×2 MIMO and four integrated omni-directional downtilt antennas.
- AP-204 and IAP-204
  - 2.4-GHz (300 Mbps max rate) and 5-GHz (867 Mbps max rate) radios, each with 2×2 MIMO and two combined, diplexed external RP-SMA antenna connectors.

Instant 274/275 outdoor

- AP type: Outdoor, dual radio, 5-GHz 802.11ac and 2.4-GHz 802.11n

  In addition to 802.11n data rates, the 2.4-GHz radio supports 802.11ac data rates using 256-QAM modulation. This gives TurboQAM-enabled clients a 33% boost above the maximum supported data rate to deliver up to 600 Mbps.

  3×3 MIMO with three spatial streams and up to 1.3 Gbps wireless data rate

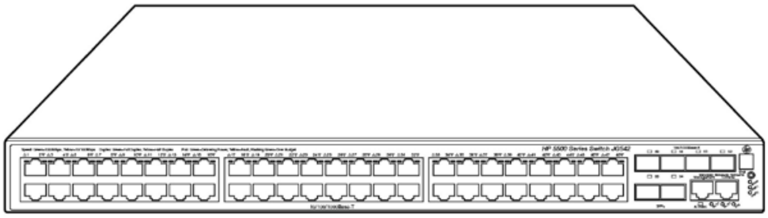


AOS 6.5.0: 310 Series Access Points: Mid-range 11ac Wave 2

- Delivering the full value of 802.11ac Wave 2 at an aggressive price
  - Same 5GHz radio capabilities as flagship 330 Series
  - Single (Gb) Ethernet port, 2x2:2SS 2.4GHz radio
- 802.11ac 4x4:4SS MU-MIMO
  - 1,733Mbps peak datarate, and up to 3 MU-MIMO client devices
- Dual radio, 802.11ac 4x4:4SS VHT160 and integrated BLE
  - 5GHz: 1,733Mbps max (with 4SS/VHT80 or 2SS/VHT160 clients)
  - 2.4GHz: 400Mbps max (2SS/VHT40)
    - More realistic for 2.4GHz: 300Mbps at 2SS/HT40 and 144Mbps at 2SS/HT20
  - Support for additional 5GHz bands (anticipating these being opened by FCC)
  - Integrated BLE radio: locationing, wireless console access
  - 100/1000 Gb Ethernet network interface
  - MU-MIMO, TxBF, ACC, USB, console, reset
  - 802.3af/at POE / 12Vdc, 21W max (includes power delivered to USB device)
  - Intelligent Power Monitoring (IPM) to monitor and optimize power consumption
- Size: smaller than AP-325, similar to AP-215
  - 182mm x 180mm x 48mm
- Pricing: TBD (NTE US list: $1,095); FCS schedule: Q2CY16

Minimum SW versions:

AOS: 6.5.0
Instant: 4.3.0



Overview

The HPE 5500 HI Switch Series comprises Gigabit Ethernet switches that deliver outstanding resiliency, security, and multiservice support capabilities at the edge layer of data center, large campus, and metro Ethernet networks. The switches can also be used in the core layer of SMB networks.

With Intelligent Resilient Fabric (IRF) support and available dual power supplies, the HPE 5500 HI Switch Series can deliver the highest levels of resiliency and manageability. In addition, the PoE+ models provide up to 1440 W of PoE+ power with the dual power supply configuration.

Designed with two fixed 10GbE ports and extension module flexibility, these switches can provide up to six 10GbE uplink or 70 GbE ports. With complete IPv4/IPv6, OpenFlow, and MPLS/VPLS features, the series provides investment protection with an easy transition from IPv4 to IPv6 networks.

Features and benefits

Software-defined networking

- **OpenFlow**
  supports OpenFlow 1.3 specification to enable SDN by allowing separation of the data (packet forwarding) and control (routing decision) paths

Quality of Service (QoS)

- **Advanced classifier-based QoS**
  classifies traffic using multiple match criteria based on Layer 2, 3, and 4 information; applies QoS policies such as setting priority level and rate limit to selected traffic on a per-port or per-VLAN basis
- **Traffic policing**
  supports Committed Access Rate (CAR) and line rate
- **Powerful QoS feature**
  creates traffic classes based on access control lists (ACLs), IEEE 802.1p precedence, IP, and DSCP or Type of Service (ToS) precedence; supports filter, redirect, mirror, or remark; supports the following congestion actions: strict priority (SP) queuing, weighted round robin (WRR), weighted fair queuing (WFQ), weighted random early discard (WRED), weighted deficit round robin (WDRR), SP+WDRR, and SP+WFQ.
- **Storm restraint**
  allows limitation of broadcast, multicast, and unknown unicast traffic rate to reduce unwanted broadcast traffic on the network

Management

- **Friendly port names**
  allow assignment of descriptive names to ports
- **sFlow** (RFC 3176)
  provides scalable ASIC-based wirespeed network monitoring and accounting with no impact on network performance; this allows network operators to gather a variety of sophisticated network statistics and information for capacity planning and real-time network monitoring purposes
- **Complete session logging**
  provides detailed information for problem identification and resolution
- **Remote configuration and management**
  enables configuration and management through a secure Web browser or a CLI located on a remote device
- **Manager and operator privilege levels**
  provides read-only (operator) and read/write (manager) access on CLI and Web browser management interfaces
- **Management VLAN**

segments traffic to and from management interfaces, including CLI/Telnet, a Web browser interface, and SNMP

- **Command authorization**
  leverages RADIUS to link a custom list of CLI commands to an individual network administrator's login; an audit trail documents activity
- **Secure web GUI**
  provides a secure, easy-to-use graphical interface for configuring the module via HTTPS
- **SNMPv1, v2c, and v3**
  facilitate centralized discovery, monitoring, and secure management of networking devices
- **Remote monitoring (RMON)**
  uses standard SNMP to monitor essential network functions; supports events, alarm, history, and statistics group plus a private alarm extension group
- **Remote intelligent mirroring**
  mirrors ingress/egress ACL-selected traffic from a switch port or VLAN to a local or remote switch port anywhere on the network
- **In-service software upgrade (ISSU)**
  enables operators to perform upgrades in the shortest possible amount of time with minimal risk to network operations or traffic disruptions

Connectivity

- **Auto-MDIX**
  provides automatic adjustments for straight-through or crossover cables on all 10/100 and 10/100/1000 ports
- **Packet storm protection**
  protects against broadcast, multicast, or unicast storms with user-defined thresholds
- **Ethernet operations, administration and maintenance (OAM)**
  detects data link layer problems that occurred in the "last mile" using the IEEE 802.3ah OAM standard; monitors the status of the link between two devices
- **Flow control**
  provides back pressure using standard IEEE 802.3x, reducing congestion in heavy traffic situations
- **Fixed 10GbE ports**
  provides two fixed SFP+ ports for a 20 GbE connection to the network without the need for additional extension interface modules
- **Optional 10GbE ports**
  deliver, through the use of optional modules, additional 10GbE connections, which are available for uplinks or high-bandwidth server connections; flexibly support copper, XFP, SFP+, or CX4 local connections
- **Optional 8-port SFP module**
  adds up to eight additional wirespeed Gigabit Ethernet ports for unprecedented Gigabit density in a single 1U enclosure
- **Jumbo packet support**
  supports up to 12288-byte frame size to improve the performance of large data transfers
- **High-bandwidth CX4 local stacking**
  achieves 12 Gbps per connection when using local CX4 stacking, allowing for up to 96 Gbps total stacking bandwidth (full duplex) in a resilient stacking configuration
- **IEEE 802.3at Power over Ethernet (PoE+)**
  provides up to 30 W per port that allows support of the latest PoE+-capable devices such as IP phones, wireless access points, and security cameras, as well as any IEEE 802.3af-compliant end device; eliminates the cost of additional electrical cabling and circuits that would otherwise be necessary in IP phone and WLAN deployments

Performance

- **Hardware-based wirespeed access control lists (ACLs)** help provide high levels of security and ease of administration without impacting network performance with a feature-rich TCAM-based ACL implementation

- **Nonblocking architecture**
  delivers up to 224 Gb/s of wire-speed switching with a nonblocking switching fabric and up to 167 million pps throughput

Resiliency and high availability

- **Separate data and control paths**
  separates control from services and keeps service processing isolated; increases security and performance
- **Device Link Detection Protocol (DLDP)**
  monitors link connectivity and shuts down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks
- **Intelligent Resilient Fabric (IRF)**
  creates virtual resilient switching fabrics, where two or more switches perform as a single L2 switch and L3 router; switches do not have to be co-located and can be part of a disaster-recovery system; servers or switches can be attached using standard LACP for automatic load balancing and high availability; can eliminate the need for complex protocols like Spanning Tree Protocol, Equal-Cost Multipath (ECMP), or VRRP, thereby simplifying network operation
- **Rapid Ring Protection Protocol (RRPP)**
  connects multiple switches in a high-performance ring using standard Ethernet technology; traffic can be rerouted around the ring in less than 50 ms, reducing the impact on traffic and applications
- **Smart link**
  allows 50 ms failover between links
- **Virtual Router Redundancy Protocol (VRRP)**
  allows groups of two routers to dynamically back each other up to create highly available routed environments

Manageability

- **Dual flash images**
  provides independent primary and secondary operating system files for backup while upgrading
- **Multiple configuration files**
  allow multiple configuration files to be stored to a flash image
- **IEEE 802.1AB Link Layer Discovery Protocol (LLDP)**
  facilitates easy mapping using network management applications with LLDP automated device discovery protocol
- **Troubleshooting**
  allows ingress and egress port monitoring enabling network problem solving; virtual cable tests provide visibility into cable problems
- **IPv6 management**
  future-proofs networking, as the switch is capable of being managed whether the attached network is running IPv4 or IPv6; supports pingv6, tracertv6, Telnetv6, TFTPv6, DNSv6, and ARPv6

Layer 2 switching

- **GARP VLAN Registration Protocol**
  allows automatic learning and dynamic assignment of VLANs
- **IP multicast snooping and data-driven IGMP**
  automatically prevents flooding of IP multicast traffic
- **Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) protocol snooping**
  controls and manages the flooding of multicast packets in a Layer 2 network
- **32K MAC addresses**
  provide access to many Layer 2 devices

Overview

- **IEEE 802.1ad QinQ and selective QinQ**
  increase the scalability of an Ethernet network by providing a hierarchical structure; connect multiple LANs on a high-speed campus or metro network
- **10GbE port aggregation**
  allows grouping of ports to increase overall data throughput to a remote device
- **Spanning Tree/MSTP, RSTP, and STP root guard**
  prevent network loops
- **32 MSTP instances**
  allow multiple configurations of STP per VLAN group

Layer 3 services

- **Loopback interface address**
  defines an address in Routing Information Protocol (RIP) and Open Standard Path First (OSPF), improving diagnostic capability
- **Address Resolution Protocol (ARP)**
  determines the MAC address of another IP host in the same subnet; supports static ARPs; gratuitous ARP allows detection of duplicate IP addresses; proxy ARP allows normal ARP operation between subnets or when subnets are separated by a Layer 2 network
- **Dynamic Host Configuration Protocol (DHCP)**
  simplifies the management of large IP networks and supports client and server; DHCP Relay enables DHCP operation across subnets
- **User Datagram Protocol (UDP) helper function**
  allows UDP broadcasts to be directed across router interfaces to specific IP unicast or subnet broadcast addresses and prevents server spoofing for UDP services such as DHCP

Layer 3 routing

- **IPv4 routing protocols**
  support static routes, RIP, OSPF, ISIS, and BGP
- **IPv6 routing protocols**
  provide routing of IPv6 at wire speed; support static routes, RIPng, OSPFv3, IS-ISv6, and BGP4+ for IPv6
- **PIM-SSM, PIM-DM, and PIM-SM (for IPv4 and IPv6)**
  support IP Multicast address management and inhibition of DoS attacks
- **MPLS support**
  provides extended support of MPLS, including MPLS VPNs and MPLS Traffic Engineering (MPLS TE)
- **Virtual Private LAN Service (VPLS)**
  establishes point-to-multipoint Layer 2 VPNs across a provider network
- **Bidirectional Forwarding Detection (BFD)**
  enables link connectivity monitoring and reduces network convergence time for RIP, OSPF, BGP, IS-IS, VRRP, MPLS, and IRF
- **Policy-based routing**
  makes routing decisions based on policies set by the network administrator
- **Equal-Cost Multipath (ECMP)**
  enables multiple equal-cost links in a routing environment to increase link redundancy and scale bandwidth
- **IPv6 tunneling**
  allows a smooth transition from IPv4 to IPv6 by encapsulating IPv6 traffic over an existing IPv4 infrastructure

Security

Overview

- **Access control lists (ACLs)**
  provide IP Layer 2 to Layer 4 traffic filtering; support global ACL, VLAN ACL, port ACL, and IPv6 ACL; up to 6144 ingress ACLs and 1024 egress ACLs are supported
- **IEEE 802.1X**
  defines an industry-standard method of user authentication using an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server
- **MAC-based authentication**
  authenticates the client with the RADIUS server based on the client's MAC address
- **Identity-driven security and access control**
  - **Per-user ACLs**
    permit or deny user access to specific network resources based on user identity and time of day, allowing multiple types of users on the same network to access specific network services without risking network security or providing unauthorized access to sensitive data
  - **Automatic VLAN assignment**
    assigns users automatically to the appropriate VLAN based on their identities
- **Port security**
  allows access only to specified MAC addresses, which can be learned or specified by the administrator
- **Secure FTP**
  allows secure file transfer to and from the switch; protects against unwanted file downloads or unauthorized copying of a switch configuration file
- **STP BPDU port protection**
  blocks Bridge Protocol Data Units (BPDUs) on ports that do not require BPDUs, preventing forged BPDU attacks
- **DHCP protection**
  blocks DHCP packets from unauthorized DHCP servers, preventing denial-of-service attacks
- **DHCP snooping**
  helps ensure that DHCP clients receive IP addresses from authorized DHCP servers and maintain a list of DHCP entries for trusted ports; prevents reception of fake IP addresses and reduces ARP attacks, improving security
- **DHCPv6 snooping**
  ensures that DHCPv6 clients obtain IPv6 addresses from authorized DHCPv6 servers and record IP-to-MAC mappings of DHCPv6 clients
- **Dynamic ARP protection**
  blocks ARP broadcasts from unauthorized hosts, preventing eavesdropping or theft of network data
- **STP root guard**
  protects the root bridge from malicious attacks or configuration mistakes
- **Guest VLAN**
  provides a browser-based environment to authenticated clients that is similar to IEEE 802.1X
- **Port isolation**
  secures and adds privacy, and prevents malicious attackers from obtaining user information
- **IP source guard**
  helps prevent IP spoofing attacks
- **IPv6 source guard**
  help prevent IPv6 spoofing attacks using ND Snooping as well as DHCPv6 Snooping
- **ND Snooping**
  allows only packets with a legally obtained IPv6 address to pass
- **Endpoint Admission Defense (EAD)**
  provides security policies to users accessing a network
- **RADIUS/HWTACACS**
  eases switch management security administration by using a password authentication server
- **Secure management access**
  delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2 and SNMPv3

- **Unicast Reverse Path Forwarding (URPF)**
  allows normal packets to be forwarded correctly, but discards the attaching packet due to lack of reverse path route or incorrect inbound interface; prevents source spoofing and distributed attacks; supports distributed UFPF

Convergence

- **LLDP-MED (Media Endpoint Discovery)**
  defines a standard extension of LLDP that stores values for parameters such as QoS and VLAN to automatically configure network devices such as IP phones
- **Internet Group Management Protocol (IGMP)**
  utilizes Any-Source Multicast (ASM) or Source-Specific Multicast (SSM) to manage IPv4 multicast networks; supports IGMPv1, v2, and v3
- **Multicast Source Discovery Protocol (MSDP)**
  allows multiple PIM-SM domains to interoperate; is used for inter-domain multicast applications
- **Multicast Border Gateway Protocol (MBGP)**
  allows multicast traffic to be forwarded across BGP networks and kept separate from unicast traffic
- **Multicast VLAN**
  allows multiple VLANs to receive the same IPv4 or IPv6 multicast traffic, lessening network bandwidth demand by reducing or eliminating multiple streams to each VLAN
- **LLDP-CDP compatibility**
  receives and recognizes CDP packets from Cisco's IP phones for seamless interoperation

Additional information

- **Green initiative support**
  provides support for RoHS and WEEE regulations
- **Green IT and power**
  improves energy efficiency through the use of the latest advances in silicon development; shuts off unused ports and utilizes variable-speed fans, reducing energy costs

Warranty and support

- **Limited Lifetime Warranty**
  see **http://www.hpe.com/networking/warrantysummary** for warranty and support information included with your product purchase.
- **Software releases**
  to find software for your product, refer to **http://www.hpe.com/networking/support**; for details on the software releases available with your product purchase, refer to **http://www.hpe.com/networking/warrantysummary**

Overview

Aruba 2530 Switch Series

Models

HP 2530-48G-PoE+ Switch	J9772A HP
2530-24G-PoE+ Switch	J9773A HP
2530-8G-PoE+ Switch	J9774A HP
2530-48-PoE+ Switch	J9778A HP
2530-24-PoE+ Switch	J9779A HP
2530-8-PoE+ Switch	J9780A HP
2530-48G Switch	J9775A HP 2530-
24G Switch	J9776A HP 2530-
8G Switch	J9777A HP 2530-
48 Switch	J9781A HP 2530-
24 Switch	J9782A HP 2530-8
Switch	J9783A HP 2530-
48G-PoE+-2SFP+ Switch	J9853A HP 2530-
24G-PoE+-2SFP+ Switch	J9854A HP 2530-
48G-2SFP+ Switch	J9855A HP 2530-
24G-2SFP+ Switch	J9856A
HP 2530-8-PoE+ Internal Power Supply Switch	JL070A

Key features

Overview

- Cost-effective, reliable and secure Aruba Layer 2 switch series.
- ACLs, EEE, traffic prioritization and models with 10 Gigabit uplinks.
- 8-, 24-, and 48-port Gigabit or Fast Ethernet models
- PoE+ models for voice, video and wireless.
- Supports ClearPass Policy Manager and Airwave Network Management.

Introduction

The Aruba 2530 Switch Series provides security, reliability, and ease of use for enterprises, branch offices, and SMBs. This series of fully managed switches delivers full Layer 2 capabilities with enhanced access security, ACLs, traffic prioritization, sFlow, and IPv6 host support. Right size deployment is simple with choice of 8-, 24-, and 48-port models available with Gigabit or Fast Ethernet ports, optional PoE+, and optional 10GbE uplinks. The 2530 delivers power savings with fanless models, Energy Efficient Ethernet, and ability to disable LEDs and enable port low power mode. These switches provide consistent wired/wireless user experience with unified management tools such as ClearPass Policy Manager and Airwave Network Management.

The Aruba 2530 Switch Series offers uplink flexibility with either four Gigabit or two 10 Gigabit Ethernet uplinks on some 24- and 48-port models. The Gigabit 24- and 48-port models have either two small form-factor pluggable plus (SFP+) or four small form-factor pluggable (SFP) slots for fiber connectivity. The Fast Ethernet 24- and 48-port models have two SFPs and two RJ-45 Gigabit uplinks. The compact and fan-less 8-port switches offer additional flexibility with two dual-personality ports that can be used as either RJ-45 Gigabit Ethernet or SFP ports. The Aruba 2530 Switch Series PoE+ Switches are IEEE 802.3af- and IEEE 802.3at-compliant with up to 30 W per port, making them suitable for voice, video, or wireless deployments with PoE+.

Features and Benefits

Quality of Service (QoS)

- **Traffic prioritization (IEEE 802.1p)**
  allows real-time traffic classification with support for eight priority levels mapped to either two or four queues, and uses weighted deficit round robin (WDRR) or strict priority
- **Simplified QoS configuration**
  - **Port-based**
    prioritizes traffic by specifying a port and priority level
  - **VLAN-based**
    prioritizes traffic by specifying a VLAN and priority level
- **Class of Service (CoS)**
  sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ
- **Rate limiting**
  establishes per-port ingress-enforced maximums for all ingressed traffic or for broadcast, multicast, or unknown destination traffic
- **Layer 4 prioritization**
  enables prioritization based on TCP/UDP port numbers
- **Flow control**
  helps deliver reliable communication during full-duplex operation

Management

- **Choice of management interfaces**
  - **HTML-based easy-to-use Web GUI**

Overview

allows configuration of the switch from any Web browser

- **Robust CLI**
  provides advanced configuration and diagnostics
- **Simple network management protocol (SNMPv1/v2c/v3)**
  allows the switch to be managed with a variety of third-party network management applications

- **Virtual stacking**
  provides single IP address management for up to 16 switches
- **sFlow (RFC 3176)**
  delivers wire-speed traffic accounting and monitoring, configured by SNMP and CLI with three terminal encrypted receivers
- **IEEE 802.1AB Link Layer Discovery Protocol (LLDP)**
  automates device discovery protocol for easy mapping by network management applications
- **Logging**
  provides local and remote logging of events via SNMP (v2c and v3) and syslog; provides log throttling and log filtering to reduce the number of log events generated
- **Port mirroring**
  allows traffic to be mirrored on any port or a network analyzer to assist with diagnostics or detecting network attacks
- **Remote monitoring (RMON)**
  provides advanced monitoring and reporting capabilities for statistics, history, alarms, and events
- **Find, fix, and inform**
  finds and fixes common network problems automatically, and then informs the administrator
- **Friendly port names**
  allows assignment of descriptive names to ports
- **Dual flash images**
  provides independent primary and secondary operating system files for backup while upgrading
- **Multiple configuration files**
  are easily stored with a flash image
- **Front-panel LEDs**
  - **Locator LEDs**
    allows users to set the locator LED on a specific switch to turn on, blink, or turn off; and simplifies troubleshooting by making it easy to locate a particular switch within a rack of similar switches
  - **Per-port LEDs**
    provides an at-a-glance view of the status, activity, speed, and full-duplex operation
  - **Power and fault LEDs**
    display issues, if any
- **Comware CLI**
  - **Comware-compatible CLI**
    bridges the experience of Hewlett Packard Enterprise Comware CLI users who are using the ProVision CLI
  - **Display and fundamental Comware CLI commands**
    are natively embedded in the switch CLI; display output is formatted as on Comware-based switches; fundamental commands provide Comware-familiar initial switch setup
  - **Configuration Comware CLI commands**
    when Comware commands are entered, CLI help is elicited to formulate the correct ProVision software CLI command
- **Download Software via DHCP**
  adds the option to specify the location of switch software via DHCP
- **TR-069 support**
  enables zero-touch configuration for switches
- **Zero-Touch ProVisioning (ZTP)**

Overview

uses settings in DHCP to enable ZTP with Aruba AirWave Network Management

Connectivity

- **IPv6**
  - **IPv6 host**
    allows the switch to be deployed and managed at the edge of an IPv6 network
  - **Dual stack (IPv4/IPv6)**
    supports connectivity for both protocols; provides a transition mechanism from IPv4 to IPv6
  - **MLD snooping**
    forwards IPv6 multicast traffic to appropriate interface; prevents IPv6 multicast traffic from flooding the network
  - **IPv6 ACL/QoS**
    supports ACL & QoS for IPv6 network traffic on Gigabit & 48 port 10/100 models
  - **Security**
    RA Guard, DHCPv6 Protection, Dynamic IPv6 Lockdown (YA only)
- **IEEE 802.3af Power over Ethernet (PoE)**
  provides up to 15.4 W per port to IEEE 802.3af-compliant PoE-powered devices such as IP phones, wireless access points, and security cameras
- **IEEE 802.3at PoE+**
  provides up to 30 W per port to IEEE 802.3 for PoE/PoE+-powered devices such as video IP phones, IEEE 802.11n wireless access points, and advanced pan/tilt/zoom security cameras (refer to the product specifications for the total PoE power availability)
- **Auto-MDIX**
  adjusts automatically for straight-through or crossover cables on all ports
- **Pre-standard PoE support**
  detects and provides power to pre-standard PoE devices (refer to the list of supported devices in the product FAQs, which can be accessed at hpe.com/networking)
- **SFP slots**
  provides fiber connectivity such as Gigabit-SX, -LX, -LH, and -BX with four SFP slots on all 24- and 48-port Gigabit Ethernet models. Fast Ethernet 24- and 48-port models have two SFP slots and two RJ-45 Gigabit uplinks; 8-port models have two dual-personality ports supporting either SFP or RJ-45 Gigabit uplinks
- **Dual-personality (RJ-45 or USB micro-B) serial console port**
  gives easy access to switch CLI with front-of-switch location and the flexibility of using either an RJ-45 or USB micro-B serial console port

Layer 2 switching

- **VLANs**
  provides support for 512 VLANs and 4,094 VLAN IDs
- **Jumbo packet support**
  supports up to 9,220-byte frame size to improve the performance of large data transfers; 8- and 24-port Fast Ethernet models automatically support up to 2,000-byte frames with no configuration needed
- **16K MAC address table**
  provides access to many Layer 2 devices
- **GARP VLAN Registration Protocol**
  allows automatic learning and dynamic assignment of VLANs
- **Rapid Per-VLAN Spanning Tree (RPVST+)**
  allows each VLAN to build a separate spanning tree to improve link bandwidth usage; is compatible with PVST+

Overview

Security

- **ACLs**
  accommodates IPv4/IPv6 port and VLAN-based ACLs (IPv6 ACL is supported only on Gigabit Ethernet and 48-port models.)
- **Source-port filtering**
  allows only specified ports to communicate with each other
- **RADIUS/TACACS+**
  eases switch management security administration by using a password authentication server
- **Secure Sockets Layer (SSL)**
  encrypts all HTTP traffic, allowing secure access to the browser-based management GUI in the switch
- **Port security**
  allows access only to specified MAC addresses, which can be learned or specified by the administrator
- **MAC address lockout**
  prevents particular configured MAC addresses from connecting to the network
- **Multiple user authentication methods**
  - **IEEE 802.1X**
    uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards
  - **Web-based authentication**
    provides a browser-based environment, similar to IEEE 802.1X, to authenticate clients that do not support the IEEE 802.1X supplicant
  - **MAC-based authentication**
    authenticates the client with the RADIUS server based on the client's MAC address
- **Secure shell (SSH) v2**
  encrypts all transmitted data for secure remote CLI access over IP networks
- **Secure shell**
  encrypts all transmitted data for secure remote CLI access over IP networks
- **STP BPDU port protection**
  blocks Bridge Protocol Data Units (BPDUs) on ports that do not require BPDUs, preventing forged BPDU attacks
- **STP root guard**
  protects the root bridge from malicious attacks or configuration mistakes
- **Secure management access**
  delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2 and SNMPv3
- **Custom banner**
  displays security policy when users log in to the switch
- **Secure FTP**
  allows secure file transfer to and from the switch; protects against unwanted file downloads or unauthorized copying of a switch configuration file
- **Protected ports CLI**
  offers intuitive CLI to configure the source-port filter feature, by allowing specified ports to be isolated from all other ports on the switch; the protected port or ports can communicate only with the uplink or shared resources
- **Authentication flexibility**
  - **Multiple IEEE 802.1X users per port**
    provides authentication for up to eight IEEE 802.1X users per port; prevents a user from "piggybacking" on another user's IEEE 802.1X authentication
  - **Concurrent IEEE 802.1X and Web or MAC authentication schemes per port**
    allows a switch port to accept any IEEE 802.1X and either Web or MAC authentications
- **Switch management logon security**

Overview

helps secure switch CLI logon by optionally requiring either RADIUS or TACACS+ authentication

- **DHCP protection**
  blocks DHCP packets from unauthorized DHCP servers, preventing denial-of-service attacks
- **Dynamic ARP protection:**
  blocks ARP broadcasts from unauthorized hosts, preventing eavesdropping or theft of network data
- **Dynamic IP lockdown**
  works with DHCP protection to block traffic from unauthorized hosts, preventing IP source address spoofing

Convergence

- **LLDP-MED (Media Endpoint Discovery)**
  defines a standard extension of LLDP that stores values for parameters such as QoS and VLAN to automatically configure network devices such as IP phones
- **IP multicast (data-driven IGMP)**
  prevents flooding of IP multicast traffic
- **IEEE 802.1AB Link Layer Discovery Protocol (LLDP)**
  facilitates easy mapping using network management applications with LLDP automated device discovery protocol
- **PoE and PoE+ allocations**
  support multiple methods—automatic, IEEE 802.3at dynamic, LLDP-MED fine grain, IEEE 802.3af device class, or user specified—to allocate and manage PoE/PoE+ power for more efficient energy use
- **Voice VLAN**
  uses LLDP-MED to automatically configure a VLAN for IP phones
- **IP multicast (data-driven IGMPv3)**
  prevents flooding of IP multicast traffic
- **LLDP-CDP compatibility**
  receives and recognizes CDP packets from Cisco's IP phones for seamless interoperation
- **Local MAC Authentication**
  assigns attributes such as VLAN and QoS using locally configured profile that can be a list of MAC prefixes

Unified Wired and Wireless

- **ClearPass Policy Manager support**
  unified wired and wireless policies using Aruba ClearPass Policy Manager
- **HTTP redirect function**
  supports HPE Intelligent Management Center (IMC) bring your own device (BYOD) solution
- **Switch auto-configuration**
  automatically configures switch for rogue AP detection, add VLAN, and set PoE priority when Aruba AP is detected

Resiliency and high availability

- **Port trunking and link aggregation**
  - **Trunking**
    supports up to eight links per trunk to increase bandwidth and create redundant connections; and supports L2, L3, and L4 trunk load-balancing algorithm (L4 trunk load balancing is supported only on Gigabit Ethernet and 48-port models.)
  - **IEEE 802.3ad Link Aggregation Control Protocol (LACP)**
    eases configuration of trunks through automatic configuration
- **IEEE 802.1s Multiple Spanning Tree**

Overview

provides high link availability in multiple VLAN environments by allowing multiple spanning trees; provides legacy support for IEEE 802.1d and IEEE 802.1w

- **SmartLink**
  provides easy-to-configure link redundancy of active and standby links

Product Architecture

- **Energy-efficient design**
  - **IEEE 802.3az**
    reduces power consumption during periods of low data activity on Gigabit Ethernet switches
  - **Port low power mode**
    enables the port to automatically go into low-power mode to conserve energy when no link is detected
  - **Fanless and variable-speed fans**
    decreases power consumption in fanless (all 8-port, 2530-24, and 2530-48 PoE+ switches) as well as variable-speed fan switches
  - **Port LEDs**
    conserves energy by optionally turning off port link and activity LEDs
- **Switch on a chip**
  provides a highly integrated, high-performance switch design with a non-blocking architecture

Flexibility

- **Flexible mounting**
  - **Rack mountable**
    allows the switch to be mounted on a standard 19-inch rack, with the hardware included
  - **Wall mountable**
    allows the switch to be mounted on a wall, using the hardware included
  - **Surface mountable**
    allows the switch to be mounted above or below a surface (such as a desk or table), using the hardware included
- **Quiet operation**
  lowers noise, making it suitable for deployments in acoustically sensitive environments such as conference rooms and office spaces
- **Compact size**
  reduces space requirements (refer to the product specifications for the exact dimensions)

Warranty and support

- **Limited Lifetime Warranty**
  see **http://www.hpe.com/networking/warrantysummary** for warranty and support information included with your product purchase.
- **Software releases**
  to find software for your product, refer to **http://www.hpe.com/networking/support**; for details on the software releases available with your product purchase, refer to **http://www.hpe.com/networking/warrantysummary**