

# Solution Data Sheet



## Product Overview

Uplevel's products are an infrastructure-as-a-service solution designed for Managed Service Providers (MSPs) serving small and medium sized businesses. The Uplevel platform enables MSPs to profitably deploy and scale connectivity and security. This all-in-one system provides a single hardware deployment customized via software and cloud services to fit customer needs, adapting as their environment changes. The monthly subscription pricing model simplifies sales by reducing upfront deployment expenses and eliminating support, maintenance, or warranty fees. The Uplevel model allows partners to rapidly expand and efficiently manage their clientele by reducing deployment time and simplifying configuration through a centralized management portal.

### Integrated network platform

Uplevel delivers all IT infrastructure services:

- High performance routing and switching with high throughput, supporting offices up to 1,000 employees
- LAN security with VLA-based segregation, MAC filtering and device control
- Advanced Firewall with Deep Packet Inspection, Geo-blocking, and Content Filtering
- Active Directory Services for resource control and user management
- Built-in storage for up to 8 terabytes & back up with ransomware protection and encrypted archives
- High performance Indoor and Outdoor Wi-Fi
- Enterprise-class PoE+ Ethernet Switches
- Remote Access and Site-to-Site VPN
- Dual WAN Failover and Load Balancing with QoS and VPN prioritization
- Automated notification for proactive management
- SNMP for management platform integration

### Highlights

Simplify and standardize deployment of all key IT infrastructure  
Manage from single cloud-based platform  
Infrastructure configuration held in cloud database, eliminating risk and downtime due to lost configurations  
Easy recover from disasters with automatic configuration replication  
Proactive detection, display, and alerting of warnings and failures  
Simplify configurations and reduce setup time with integrated and intelligent network management  
Quickly troubleshoot and resolve issues remotely  
Simplified no-surprises pricing with no per-seat or per-device costs

Uplevel's hybrid model combines powerful, high-performance on-site hardware with cloud-based intelligence and management to automate and standardize deployments, reduce troubleshooting time, and simplify scaling as the business grows.

## “Be there anywhere”:

A cloud-based multi-tenant dashboard streamlines management of client infrastructure with automated alerting, remote configuration, and always-on monitoring. MSPs can view, configure, troubleshoot, and scale a fleet of customer deployments **from a single pane of glass**. Notifications of failures or warnings can be sent to support e-mails or PSA tools. The simplicity of the system allows tier 1 technicians to become immediately productive without a steep learning curve.



- **Enterprise-class hardware** provides high performance for customers of all sizes. Dedicated network processors support not only wire-speed packet processing, but also solid WAN connections and reliable VPN access, and deep packet inspection up to gigabit rates.
- **Hybrid software services** allow infrastructure to be customized based on client needs. Remotely enable or disable services, or scale up and down infrastructure
- **Pervasive security** keeps customers safe from hackers and malicious threats. Additional protection can be enabled without hardware swaps as security postures change. Integrated end-to-end automatic configuration avoids security ‘holes’ due to oversights or inadvertent misconfiguration.
- **Cloud management** supports powerful and simplified remote infrastructure administration. Rule-based detection of issues and anomalies trigger notifications to alert administrators of failures or potential problems. No configuration files are needed and configuration information cannot be lost.
- **Automatic Updates** to equipment ensure that customers always have the latest capabilities, up-to-date patches and attack signatures, and the strongest security posture available. No downloads are ever required; the gateway continuously synchronizes to the cloud management infrastructure.

## Solution Highlights

### Fits SOHO, Small, Medium Businesses

Supports from factors and performance ratings ranging from in-office situations with up to 1,000 employees in a single office, down to SOHO and remote worker scenarios with 1-5 users. The same 'single pane of glass' dashboard is used to manage all sites in a unified manner. A common software stack across all devices eliminates the need to swap hardware as customer requirements change.

Uplevel's 'one-click' VPN setup allows all gateways under a single customer, whether office or remote worker, to securely cross-connect without static IPs, allowing remote workers to move seamlessly between office and home environments without changing access or other settings. The common feature is supported by all gateways with the exception of storage and Active Directory.

#### Capacity

- UG-204 gateway for small office and remote worker environments
- UG-101 gateway for midsize offices up to 99 employees per location
- UG-206 gateway for medium offices up to 200 employees per location
- UG-208 gateway for businesses with up to 1,000 employees per location

#### Storage Scalability

- Choose 1TB, 4TB (5TB for UG-101), and 8TB storage
- RAID capability for UG-206 and UG-208 gateways
- Storage capacity can be distributed across VLANs, users, etc.
- Fine-grained access control possible with Active Directory

#### Wi-Fi Coverage

- UAP-201 APs for indoor IEEE 802.11ax coverage
- UAP-101B APs for indoor IEEE 802.11ac coverage
- UAP-102 APs for outdoor IEEE 802.11ac coverage with IP65 environmental rating
- Connect up to 30 Uplevel Wi-Fi APs of any kind to UG-101 gateway, and up to 100 APs to UG-206 and UG-208 gateways
- Auto-detection and auto-configuration to allow the entire fleet of Wi-Fi APs across all sites to be managed as a single unified whole

#### Connectivity

- ULS-101 8-port 130W PoE+ switch
- ULS-102 24-port 410W PoE+ switch
- ULS-103 48-port 410W PoE+ switch
- All switches support both copper (RJ-45) and optical (SFP) Gigabit Ethernet ports:
  - ULS-101: 8 RJ-45 LAN ports, 2 RJ-45 uplinks, 1 SFP LAN, 1 SFP uplink
  - ULS-102: 22 RJ-45 LAN ports, 2 RJ-45 uplinks, 3 SFP LAN, 1 SFP uplink
  - ULS-103: 46 RJ-45 LAN ports, 2 RJ-45 uplinks, 3 SFP LAN, 1 SFP uplink
- Switches capable of powering APs and phones on all RJ-45 LAN ports
- Switches can be connected arbitrarily; autodetection and autoconfiguration allows all switches to be managed as a unified whole
- Uplevel APs connected to switches automatically configure VLAN trunks to isolate & secure traffic
- All switches fully-non blocking, switch backplanes capable of handling all ports at wire speed

#### Unified Dashboard

- Manage all sites for all customers in a single pane of glass
- Automated prioritization of alerts & notifications speeds up fault localization and drill-down
- Intuitive and simplified user interface makes it easy to manage HW fleets and services quickly

## Security

Pervasive security architecture structured to map easily to small and midsize business needs. Centrally defined 'security groups' allow the security posture to be intuitively adapted to the grouping of employees commonly found in SMBs (e.g., 'accounting', 'sales', etc.) and is automatically provisioned end-to-end across the entire infrastructure for secure, consistent access to all services. Once groups are created, specific rules can be applied to determine group-level policies.

### Stateful Firewall

- Stateful firewall with up to 2Gb/s throughput depending on gateway
- "No holes" approach blocks all unsolicited internet traffic and discourages random probes
- Simplified port forwarding rules to allow external access
- Routing and ACLs automatically configured throughout the system: WAN-to-LAN, VPN-to-LAN, and between VLANs
- DNSSEC guards against DNS hijacking

### Advanced Firewall Capabilities

- Intrusion Detection and Protection System (IPS/IDS) with up to 1.1 Gb/s throughput depending on gateway
- Deep packet inspection identifies threats embedded within inbound and outbound Internet traffic
- Geoblocking (country blocking) allows regions or countries to be excluded
- Content (Domain) Filtering supports company internet usage policies

### Equipment Protection

- Control access and PoE+ power of all Uplevel Ethernet ports

- Stolen equipment can be easily deactivated and services remotely disabled
- Encrypted storage prevents access to customer data if the drive is physically removed and tampered with

### Automatic Monitoring

- Infrastructure (AP/switch) presence monitoring and alerting defends against accidental or malicious infrastructure changes
- LAN device identification, monitoring, and reporting reports when critical servers are tampered with
- Automatic security service status and notification
- Internet connection monitoring and reporting

### User Authentication and Data Protection

- Active Directory user access control and NAS data access control
- Audit logs of all Active Directory access/login activity
- File server with snapshots retained both locally and remotely
- Automatic backup of local shares to the cloud
- Ransomware protection of locally stored data
- Encryption of data on local and cloud storage
- Encryption of all data transmitted between physical sites across site-to-site VPNs, or to cloud storage

# Solution Data Sheet



## **Built-in Active Directory-compatible Domain Controller with Storage Backup**

The Uplevel Active Directory-compatible Domain Controller, coupled to the built-in gateway data storage and backup, allows users to eliminate their server footprint without compromising functionality. The Domain Controller (DC) allows management and review of user activity in a single platform.

The gateway data storage has an integrated (optional) local and cloud backup capability, which greatly simplifies proper back-up of critical data, and facilitates recovery of lost or deleted data. Network shares can be automatically snapshot with “zero-cost” local snapshots, mirrored to the cloud for disaster recovery, and/or archived for long-term storage. The usual practice of “full” and “incremental” backups is not required: each snapshot is a copy of the complete file system, allowing rapid file recovery.

### **Local storage options**

- UG-101: single 1 TB or 5 TB rotating drives
- UG-206: single 1 TB, dual 1 TB, 4 TB, or 8 TB enterprise class drives
- UG-208: dual 1 TB, 4 TB or 8 TB enterprise class drives
- Dual drives are factory-configured as RAID-1 (mirroring) for reliability

### **Management**

- Alerts raised as drives near capacity (25% and 99%)
- Alerts raised if backups fail to complete

### **Security and protection**

- Local snapshots for fast recovery and protection against ransomware
- Encrypted cloud mirror for disaster recovery
- All data is fully encrypted with AES encryption, both at rest and in-flight
- Shares can be mapped to security groups for partitioning among employee groups
- Domain controller facilitates fine-grained user access management (file/folder level)

### **Data archiving**

- Encrypted, compressed archives can be made of data on share
- Archive retention period and number can be adjusted for weeks, months or years of storage
- Archive data can be recalled and recovered on demand, from dashboard

### **Simple to use**

- Accessed by users as a standard network drive (NAS)
- Accessible from Windows, MacOS, iOS, and Android (with suitable apps)
- Snapshots directly available to users via Windows Explorer for immediate recovery
- Shares can be up-sized at will (if sufficient space available) in minutes, from dashboard

### Reliable Wi-Fi Access

Wi-Fi access points (APs) are supplied to provide a seamless and secure solution for both employee and customer Wi-Fi access. The built-in Wi-Fi controller within the gateways automatically detects and provisions Wi-Fi access points, allowing the MSP to treat all APs as a unified whole. Wi-Fi services can thus be very easily scaled out to cover any size facility, providing automatic roaming across the entire office without the need to manage individual APs. This extends to multi-site setups as well.

Our new Wi-Fi 6 APs expand on the performance and capabilities of the current Wi-Fi access points through more efficient channel use and reduced latency between the AP and devices. Wi-Fi 6 APs are backward compatible to previous models.

All APs are dual-radio (concurrent dual-band) MIMO, with controllable power and channel. Indoor APs are low-profile with internal antennas; outdoor APs have external high-gain antennas for maximum range and coverage. Fully isolated guest Wi-Fi access can be set up very simply, with configurable bandwidth control to prevent guests from excessive internet bandwidth consumption.

#### **Indoor and Outdoor Use**

- Dual-radio dual-band low-profile IEEE802.11ac and IEEE802.11ax APs with ceiling mounts for indoor office environments
- Dual-radio dual-band IP65 class IEEE 802.11ac APs with external high-gain antennas for harsh outdoor environments

#### **Concurrent, Dual-Band Operation**

- 802.11ac in the 5GHz band
- 802.11n in the 2.4GHz band

#### **Intra-Site and Inter-Site Mobility**

- Seamless roaming between APs at a single site
- Devices automatically configure among sites

#### **Guest Access**

- Optional WPA2 Personal encryption or Open access
- Guest traffic completely isolated and firewalled from business traffic
- Option to provide protection to Guest Network or leave it unprotected.
- Place guest bandwidth limits for the entire group

#### **Security**

- Wi-Fi Protected Access 2 (WPA2 Personal) for secure employee usage
- Wi-Fi 6 APs are protected by WPA3 security
- Distinct network access credentials for each group

#### **Simplified Management**

- All APs can be managed as a single unit or individually
- Controller built directly into the Uplevel gateway
- APs do not require internet access to allow LAN access
- Automatic registration and configurations allow for easy deployments
- Automatic channel selection and transmit power control dynamically adjusts to RF environments as they change
- Optimize for specific device types for additional performance or compatibility
- Manual configurations can always override automatic selections
- APs can be added, moved, or removed with ease
- Run diagnostic tests on the RF signals or reboot access point directly from the dashboard

### Intelligent Load Balancing and QoS Prioritization

Software Defined WAN (SD-WAN) configurations intelligently determine traffic flows on dynamic ISP lines. In addition, prioritization of traffic with Quality of Service (QoS) and VPN optimizations automatically adjust to changing WAN environments for the best possible performance and connection experience.

Fast Failover monitors the connection of the primary internet link at all times. In the event the link is unresponsive, unable to establish a TCP connection, or does not route out accordingly within 3 seconds the system will failover to the secondary link, if established. This failover threshold can manually be altered to accommodate more or less aggressive failover times.

Load Balancing aggregates two links together to utilize more than one ISP link simultaneously. A constant measure of drop packets, latency, and jitter to intelligently determine the correct traffic allocation as the lines change. Users can also input an additional data point to influence the quality of traffic flowing over each link. When all things are equal (drop packets, latency, and jitter), traffic will flow over the two lines based on the user entered values.

Next generation Quality of Service (QoS) prioritizes traffic across one, multiple, or VPN links. Quality of Service allows customers to prioritize time sensitive packets to ensure audio, video, and phone call packets leave the gateway first, and data flowing to the WAN is capped at the link speed of the ISP. As additional WAN links are added (in failover and load balancing) QoS intelligently determines which link to push traffic over and how much traffic to allow out.

With the addition of automated select voice service configurations, prioritizing voice traffic can be completed in four easy steps. Phone systems, both physical and cloud based, can be prioritized using VLAN tagging along with daisy-chained computers. Phones and PC's will be placed in separate VLANs/subnets and receive their respective IP address along with prioritization of traffic automatically.

#### **Dual WAN Failover**

- Automatically detects issues in ISP line failure
- Determines a failure by establishing connections
- Intelligently fails over when link is down for 3s
- Allows for manual changes to failover threshold
- Maintains phone connections during failover

#### **Dual WAN Load Balancing**

- Consistently monitors links to determine drop packets, latency, and jitter
- User input allows for manual manipulation of traffic allocation
- Intelligently determines traffic allocation for highest link performance.

#### **Quality of Service**

- Prioritize traffic based on VLAN assignment
- Qualify traffic over one or multiple links
- Prioritize traffic over VPN connections

#### **Automatic Voice Configurations**

- Works with Cloud and on-premises solutions
- Preset configurations for common vendors
- Supports daisy chained phones and PCs
- Supports physical voice service addresses using DHCP options 66 and 150
- Automatically configured routes for select on-prem manufacturers and cloud-based solutions
- Manually configured rules can always be added

### Secure Remote Access/Site-to-Site VPNs

Retailers with multiple storefronts, business owners who work from home, and others need to access network resources remotely. The Uplevel gateway supports extending service to multiple locations with both an easy-to-use site-to-site VPN and remote access VPN.

VPNs deliver identical services including security, Wi-Fi access, and storage from any of the user's business locations. This powerful capability ensures consistency of operation, security, and compliance. Multi-site VPNs connect multiple end customer sites together. A gateway is deployed to each site and users access resources from other sites without installing any special software on their computers.

VPN tunneling enables users to consistently access the network and resources, independent of both their site of operation and the location of the network resources. For instance, the 'boss group' at location A can be linked to the 'boss group' at location B by a simple click of the button. Anyone in the 'boss group' can access data at both sites, while ensuring that other employee groups or third parties in between the sites can't access the group's data.

#### ***Simple Operation***

- Single checkbox per site enables extensions of a site-to-site VPN on a per-user group basis
- Users access the network and are granted the same privileges in each location
- Drive data is available to all sites

#### ***Secure***

- All traffic traversing the public network is encrypted



### Remote Access VPN

Remote access VPNs provide direct access to networks from home computers or at offsite locations such as coffee shops, airports, and hotels. Using the native VPN clients on the devices, users can easily connect to the office and access data files, securely access computers using software such as remote desktop, and print files.

One remote access VPN session is available to MSPs at no additional cost, so MSPs can gain secure access to the customer network. A single, additional license is needed to provide remote access VPNs to all users of a particular site.

#### ***Simplicity***

- No need to download extraneous VPN software onto customer laptops
- Laptops can be tested and verified before leaving the customer site

#### ***Affordability***

- Single monthly fee, no per user pricing
- No need to pay for static IP addresses

#### ***Security***

- Seamless integration with predefined security groups
- Safe remote access to traditionally risky services such as Remote Desktop

MSP benefits from the VPN are:

#### ***Simple operation***

- Provision a new user in less than 1 minute.
- Configure, verify, and train client devices without leaving the customer site
- Works with Windows, MacOS, iOS, and Android client devices
- Supports both L2TP and SSTP

#### ***Cost Savings***

- Replace paid remote desktop services such as logmein and TeamViewer; MSP's VPN connection allows for secure use of free software such as Windows Remote Desktop or VNC to access desktops

#### ***Reliable Management***

- All traffic traversing the public network is encrypted using AES encryption
- Incorporates Uplevel Security Groups and extends customer security over VPN

### Ethernet Switching

Many deployments need more than the eight Ethernet ports available in the gateway either because end users have a larger number of wired devices, or APs are being deployed. Uplevel switches offer optional Power over Ethernet (PoE+) capable switches for these situations.

Managed from the dashboard as an integral system element, Uplevel switches are simple to deploy and manage. The dashboard intelligence automatically ensures system security by configuring separate VLANs for each security group and ensuring they are configured coherently with other system elements such as the gateway and Wi-Fi APs.

- **Scalable**-8, 24, 48-port switch configurations. Multiple switches can be stacked and managed via a single pane of glass
- **Integrated**-Dashboard automatically configures groups' security and ensure consistency with other systems elements' configurations
- **Power over Ethernet (PoE+)**
  - 802.3at PoE+ (30W max per port) on every LAN RJ-45 port for powering Uplevel Wi-Fi APs and PoE/PoE+ user devices such as third-party APs, phones, and cameras
  - PoE power delivery can be enabled and disabled from the dashboard

**Centralized Cloud-based Management**

The Uplevel system makes it easy to deliver and support more services and more clients with vastly simplified remote configuration and monitoring. See every customer’s services from one power, highly graphical dashboard, and easily drill down as needed.

- **Central configuration of network policies:** The Uplevel system automatically configures all physical equipment and software for a consistent and secure implementation
- **Web-based management interface** hosted in the cloud works with any Internet-connected smartphone, tablet, or laptop. See any client’s data while on-the-go
- **Proactive monitoring** alerts you to failures or degradation and suggests a set of fixes—in plain English—so you can identify and resolve issues remotely, often, before customers become aware a problem exists
- **Automatic configuration** of all network elements in accordance with the policy defined for the group
- **Email notifications** are sent to a technician’s inbox or can easily integrate with Professional Services Automation (PSA) tools

Sample Notifications:

Category	Notifications
Internet	<ul style="list-style-type: none"> <li>● Internet connection is down</li> <li>● Internet connection is unstable</li> <li>● Internet connection is back inline</li> <li>● Internet WAN IP address changed</li> </ul>
File Server	<ul style="list-style-type: none"> <li>● Drive is nearly full (&lt;25% free remaining)</li> <li>● Drive is full</li> <li>● Drive is busy resizing</li> </ul>
Backup	<ul style="list-style-type: none"> <li>● Backup failed</li> </ul>
Ethernet Switch	<ul style="list-style-type: none"> <li>● Switch unplugged or down</li> <li>● Switch is back online</li> </ul>
Wi-Fi	<ul style="list-style-type: none"> <li>● Wi-Fi AP unplugged or down</li> <li>● Wi-Fi AP is back online</li> <li>● Wi-Fi client is experiencing a poor signal</li> </ul>

## Hardware Specifications

### SOHO Gateway (UG-204)

PARAMETER	SPECIFICATION
Connections	4 x RJ45 10/100/1000 Ethernet ports: 2 WAN ports (primary, auxiliary) 2 LAN Ports
Throughput	900 Mb/s Stateful Firewall 500 Mb/s IDS/IPS Supports up to 50 users (per site) Supports up to 20 concurrent VPN users
LED Indicators	Power LAN link (per port) & device status
Temperature	14°F- 122°F (-10°C – 50°C) Operating -4°F- 140°F (-20°C – 60°C) Storage
Power	100-240 VAC, 50/60 Hz, 16W max
Dimensions	4.5" x 4.3" x 1.5" (11.4 x 11 x 3.8 cm) 1.1 lbs (0.5 kg)

### Standard Office Gateway (UG-101/UG-102)

PARAMETER	SPECIFICATION
Connections	4 x RJ45 10/100/1000 Ethernet ports: 2 WAN ports (primary, auxiliary) 7 LAN Ports
Throughput	900 Mb/s Stateful Firewall 220 Mb/s IDS/IPS Supports up to 99 users (per site) Supports up to 50 concurrent VPN users
Storage Capacity	1TB 5TB
LED Indicators	Power LAN link & speed (per port) Status LEDs- booting, upgrading, fault
Temperature	14°F- 122°F (-10°C – 50°C) Operating -4°F- 140°F (-20°C – 60°C) Storage
Power	100-240 VAC, 50/60 Hz, 36W max
Dimensions	9.6" x 5.9" x 1.9" (24.4 x 15 x 48 cm) 1.5 lbs (0.7 kg)

**Midrange Office Gateway (UG-206)**

PARAMETER	SPECIFICATION
Connections	6 x RJ45 10/100/1000 Ethernet ports: 2 WAN ports (primary, auxiliary) 4 LAN Ports
Throughput	1500 Mb/s Stateful Firewall 900 Mb/s IDS/IPS 1100 Mb/s IPsec VPN Supports up to 200 users (per site) Supports up to 128 concurrent VPN users
Storage Capacity	1TB (HDD) Dual 1 TB (RAID-1) Dual 4 TB (RAID-1) Dual 8 TB (RAID-1)
LED Indicators	Power, Storage Access Combined LAN & status LEDs (per port)
Temperature	14°F- 122°F (-10°C – 50°C) Operating -4°F- 140°F (-20°C – 60°C) Storage
Power	100-240 VAC, 50/60 Hz, 36W max
Dimensions	18.9" x 9.8" x 1.75" (48 x 25 x 4.45 cm) 7.7 lbs (3.5 kg)

**High-end Office Gateway (UG-208)**

PARAMETER	SPECIFICATION
Connections	8 x RJ45 10/100/1000 Ethernet ports: 2 WAN ports (primary, auxiliary) 6 LAN Ports
Throughput	2000 Mb/s Stateful Firewall 1100 Mb/s IDS/IPS 1500 Mb/s IPsec VPN Supports up to 1,000 users (per site) Supports up to 128 concurrent VPN users
Storage Capacity	Dual 1 TB (RAID-1) Dual 4 TB (RAID-1) Dual 8 TB (RAID-1)
LED Indicators	Power, Storage Access Combined LAN & status LEDs (per port)
Temperature	14°F- 122°F (-10°C – 50°C) Operating -4°F- 140°F (-20°C – 60°C) Storage
Power	100-240 VAC, 50/60 Hz, 36W max
Dimensions	17.3" x 19.75" x 1.75" (44 x 50 x 4.45 cm) 15 lbs (6.8 kg)

### Indoor Wi-Fi 6 Dual-Band Access Point (UAP-201)

PARAMETER	SPECIFICATION
Supported 802.11 versions	802.11b/g/n/ac/ax on 5 GHz 802.11b/g/n/ac/ax on 2.4 GHz
Maximum Transmission Rate	1,200 Mb/s on 5 GHz 574 Mb/s on 2.4 GHz
LED Indicators	Power, LAN, 2.4 GHz & 5 GHz activity, Upgrading
Radio TX Power	2.4 GHz: 0 dBm to +20 dBm 5 GHz: 0 dBm to +20 dBm
Security	WPA3
Temperature	32° to 104°F Operating -22° to 176 °F Storage
Dimensions	6.3" (16 cm) x 6.3" (16 cm) x 1.3" (3.3 cm) thick
Weight	.95 lbs (0.43 kg)
Power Consumption	Max 12.5 W, typical 6W
Power Supply	AC adapter, 100-240V 50/60 Hz, 24W max 48-52V PoE+ (IEEE 802.3af) operation

### Indoor Wi-Fi Dual-Band Access Point (UAP-101)

PARAMETER	SPECIFICATION
Supported 802.11 versions	802.11n/ac on 5 GHz 802.11n on 2.4 GHz
Maximum Transmission Rate	867 Mb/s on 5 GHz 300 Mb/s on 2.4 GHz
LED Indicators	Power, LAN, 2.4 GHz & 5 GHz activity, Upgrading
Radio TX Power	2.4 GHz: 0 dBm to +20 dBm 5 GHz: 0 dBm to +20 dBm
Security	WPA2/PSK, AEC-CBC encryption
Temperature	32° to 122°F Operating -4° to 140 °F Storage
Dimensions	6.4" (16 cm) dia, 1.65" (4.2 cm) thick
Weight	1.4 lbs (0.6 kg)
Power Consumption	Max 24W, typical 6W
Power Supply	AC adapter, 100-240V 50/60 Hz, 24W max 48-52V PoE+ (IEEE 802.11at) operation

Outdoor Wi-Fi Dual-Band Access Point (UAP-102)

PARAMETER	SPECIFICATION
Supported 802.11 versions	802.11n/ac on 5 GHz 802.11n on 2.4 GHz
Maximum Transmission Rate	867 Mb/s on 5 GHz 300 Mb/s on 2.4 GHz
LED Indicators	Power, LAN, 2.4 GHz & 5 GHz activity, Upgrading
Radio TX Power	2.4 GHz: 0 dBm to +20 dBm 5 GHz: 0 dBm to +20 dBm
Security	WPA2/PSK, AEC-CBC encryption
Temperature	-4° to 140°F <90% R.H. Operating -22° to 176 °F <90% R.H. Storage
Dimensions	7.5" x 4.5" x 1.9" (excluding antennas) (19 x 11.5 c 4.8 cm)
Weight	1.1 lbs (0.5 kg)
Power Consumption	Max 24W, typical 10W
Power Supply	Proprietary 24V PoE injector, max 24W

PoE+ Ethernet Switches (ULS-101, ULS-102, and ULS-103)

PARAMETER	SPECIFICATOIN		
	ULS-101	ULS-102	ULS-103
Gigabit LAN Connections	9 (8 RJ-45, 1 SFP)	25 (22 RJ-45, 3 SFP)	49 (46 RJ-45, 3 SFP)
Gigabit Uplink Connections	2 (1 RJ-45, 1 SFP)	2 (1 RJ-45, 1 SFP)	2 (1 RJ-45, 1 SFP)
Switching Capacity	24 Gbps	56 Gbps	104 Gbps
PoE+ Capable Ports	8	22	46
Maximum PoE Budget	130W	410W	410W
Temperature	32° to 122°F Operating -40° to 158°F Storage		
Dimensions (W x D x H)	13" x 9" x 1.75" (33 x 23 x 4.4 cm)	17.3" x 10.24" x 1.75" (44 x 26 x 4.4 cm)	17.3" x 10.24" x 1.75" (44 x 26 x 4.4 cm)
Weight	4/4 lbs (2 kg)	7.8 lbs (3.5 kg)	14.3 lbs (6.5 kg)
Power	Internal 100-240V, with 3-pin IEC power cord		