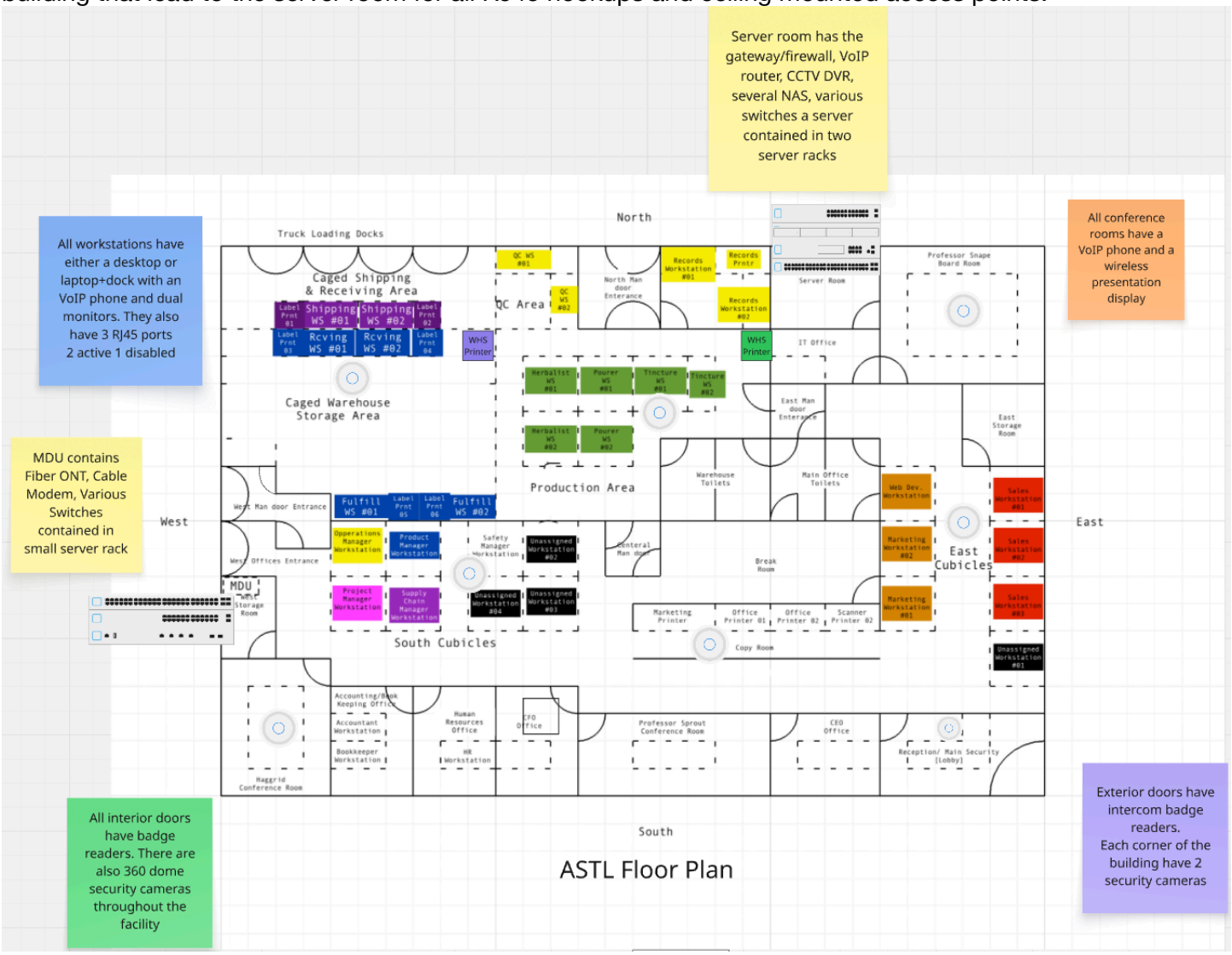
ASTL Network Design

Network Administrator: Jayce Mangum

***Note: for better visuals of the Topology and Floor plan they can be viewed on Miro, which I used to create them. CSNT-Captsone-Project: ASTL Network*

Floor Plan

Large warehouse space with a joined space for offices and conference rooms and a reception area. There is one large server room and two storage closets. The building has three employee entrances and one main entrance for guests. There are also three man door entrances that separate the office space and warehouse and two additional caged man door entrances inside of the main warehouse area. As well as cages separating the warehouse storage area, shipping, quality control and the research and devolvement. The offices consist of a shared break room, copy/print room, three conference rooms, two storage rooms, a large server room, six private offices, space for fifteen cubicles and a lobby for reception and security. All offices are on the south side for, accounting and bookkeeping, human recourses, IT, records, the CFO, and the CEO of ASTL. The warehouse is split into four major sections, production area with stations for two herbalist's, two pourers and two tinctures. There is a caged warehouse storage area that houses two desks for receiving and two desks for order fulfillment. The shipping and receiving dock is a separate cage that also housing shipping and a small quality control area with two desks. There is also conduit in the walls and ceiling throughout the building that lead to the server room for all RJ45 hookups and ceiling mounted access points.



- **Primary ISP**: Ziply Fiber will be the primary Internet Service Provider for ASTL with a 10 gigabits per second (gbps) download and upload speed business plan. A fiber line will be installed from their equipment out on the street to MDU in the West Storage Room.

- **Failover ISP**: Comcast Business will be used as. The failover Internet Service Provider for ASTL with a 2 gigabits per second (gbps) download speed and 300 megabits per second (mbps) business plan. A RG-11 coax line will be installed from their equipment hub out on the street to the MDU in the West Storage Room. An additional shielded CMP CAT6 cable will be ran from this MDU to the server room for the cable modem to connect to the router.

- **Office Desks**: Each office workstation will contain three ethernet ports, using shielded CMP CAT6 cable (as there are air ducts inside the walls and ceiling) and keystone jacks configured in the T-568B termination standard. One port with be used for the end user's company provided laptop (plugged into a docking station using a CAT6 patch cable with two RJ45 connectors on either end to going from the wall jack to the docking station port). Another port will be used for the Voice over IP (VoIP) phone. The third port will either be a failover port or if the employee's position requires a desktop as well as a laptop. There are a total of 23 workstations throughout the office spaces for a total of 69 Ethernet cable runs. Computers and phones will connect to the wall jack with a CAT6 patch cable with two RJ45 connectors on each end.

- **Warehouse Desks**: Each warehouse workstation (shipping, receiving, fulfillment, production, records and quality control) will contain two ethernet ports, using shielded CMP CAT6 cable (as there are air ducts running throughout the warehouse). For workstations that are against walls there will be wall plates with keystone jacks terminated in the T-568B standard. For workstations that are not against a wall a low-voltage box will be mounted to desk to allow for a keystone jack to be installed and terminated in the T-568B standard. One jack will be used for the end users company provided computer and the other will be used for a VoIP phone. There are a total of 16 workstations inside of the warehouse area for a total of 32 cable runs. Computers and phones will connect to the wall jack with a CAT6patch cable with two RJ45 connectors on each end. There is also a label printer connected via USB type A to a docking station.

- **Conference/Board Rooms**: Each of these spaces will will have two shield CMP CAT6 cable runs with a keystone RJ45 jack configured in T-658B standard. One at the wall for a presentation display for users to connect to. A second one at the conference room table for a VoIP phone. Wireless connectivity will be used for employee provided laptops and guest clients.

- **Laser Printers & Scanners**: Each printer and scanner station will have one ethernet port, using shielded CMP CAT6cable (as there most likely will come in contact with air ducts) there will be a keystone jack terminated in the T-658B standard. Each printer/scanner will connect to the wall jack with at CAT6patch cable with two RJ45 connectors on each end. There are a total of eight cable runs needed for printers and scanners.

- **Network Devices**: If the network device is installed in a server rack they will connect to each other using SFP+ DAC cables rated for 10gigabit. If a network device is installed in a wall mounted MDU then an SFP+ rated for 10gigabit with fiber connections will be installed into the main switch and a fiber cable will be ran to the server room.

- **PoE Wireless Access Points**: Power over Ethernet Wireless APs will be mounted to the ceiling. A CAT6cable will be ran through the ceiling using shielded CMP CAT6cable terminated with RJ45 connectors to plug into each AP's ethernet port. There are a total of eight APs that will need cable runs.

- **Server Room**: The server room will have two 42U server racks to house all the servers, switches and routers. They will have patch panels for all the ethernet jacks that run throughout the facility including any ethernet connections that are running inside of the rack. The racks will also have locking doors to prevent unauthorized access.

- **West Storage Room MDU**: The west storage room is where the Internet Service Provider taps into the building. A wall mounted 15U server rack will be placed in here to house any of the ISPs equipment. There will also be a patch panel in the rack for all ethernet jacks on the south-western section of the offices. The rack will have locking doors to prevent unauthorized access. A dedicated fiber line will be ran from this MDU to the server room for the primary ISP to connect into. An additional shielded CMP CAT6ethernet cable will ran from this MDU to the server room for the failover ISP.

- **PoE Door Access Badge Readers**: Each exterior door (excluding the loading dock rollup doors) will have a badge access reader, as well as any of the Man door entrances. For any exterior door outdoor rated shielded CAT6cable will be used to prevent weather damage then once it has entered the building a coupler will be used to allow for transition to CMP rated CAT6that will lead to a patch panel. Interior doors will use only shielded CMP rated CAT6cable. These runs will be terminated with RJ45 connectors in the T-568B configuration at the device. There will be a total of four exterior runs and 41 interior runs.

- **PoE Security Cameras**: Exterior cameras will shielded outdoor rated CAT6cable, but once they enter the building a coupler will used to transition the run into shielded CMP CAT6cabling. Interior cameras will only use shielded CMP CAT6cabling. These runs will be terminated using RJ45 connectors using the T-568B configuration at the device. There are a total of 11 exterior camera runs and 53 interior camera runs.

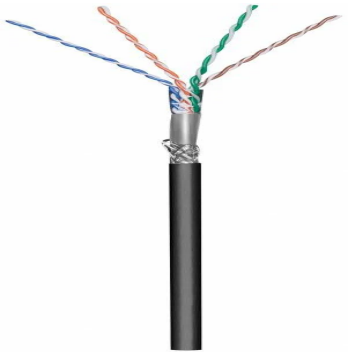
Part 1
Cabling and Hardware

Cables and Connectors

- **CAT6e**: For indoor runs shielded CMP cables will be run to prevent interference on the individual runs and to comply with running alongside air ducts and other fire hazards. For outdoor runs outdoor rated shielded CAT6cable will be used. Black jacketed cable will be used for outside runs and security equipment. White jacketed cable will used for computers and printers. Blue jacked cable will used for VoIP. At workstations and print stations an **RJ45 female keystone** jack will installed with a wall plate. The cable wiring will be configured in the **T-568B** IEEE standard. Pre-manufactured CAT6patch cables with RJ45 connectors will be used to connect all end devices at the keystone jack. They will also use the same coloring scheme as the cable runs. For security cameras, wireless access points and badge readers these runs will not use a keystone jack plus wall plate combo, instead they will use **RJ45 ethernet connectors** configured in the **T-568B** IEEE wiring standards.

White Shielded Plenum CAT6 Cable for user devices

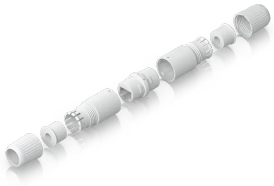
Blue Shielded Plenum CAT6 Cable for VoIP phones



Black Shielded Outdoor CAT6 Cable for exterior

White RJ45 Keystone Jack for user devices

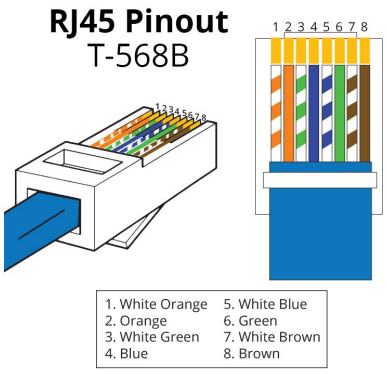
Blue RJ45 Keystone Jack for VoIP Phones



RJ45 Inline Coupler Outdoor for exterior and interior transitions

Patch Cables for end device connections & for connections going from patch panels to network device

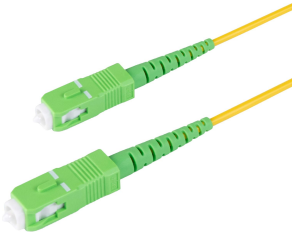
RJ45 Connectors for runs leading to a patch panel and specific security and network devices



IEEE T-568B RJ45 Standard to be used on all CAT6 runs

Patch panel w/ keystones and sections for location labels in server/network racks before connecting to network devices

- **Fiber Optic Cable**: Ziply Fiber will handle the drop from the street to the MDU, and will use a single-mode fiber (SMF-28) connector on the end. This will plug directly into a an SMF-28 10gigabit Long Range SFP+ transceiver into the gateway for fiber. Any MDU throughout the facility will have a dedicated multi-mode OS2 Duplex LC UPC Fiber cable with an 10gigabit Multi-Mode SFP+ module on both ends that plugs into the network device in the MDU and Server Room.



SMF-28 Fiber Cable

10G Bidirectional Single-Mode Optical Module (for SMF-28 Fiber Cable)

OS2 Duplex LC UPC Fiber Cable

10G Duplex LC UPC Optical Module (for OS2 Fiber Cable)

- **RG-11 Coax Cable**: Comcast will install the drop from the street to the MDU, using thicker RG-11 Coax cable with a RG-11 connector to be able to connect it to a DOCSIS3.1 cable modem. ASTL will use a customer owned modem to beat Comcast's monthly equipment rental cost.

RG-11 Coax Cable with connectors

Coax Connection Hookup

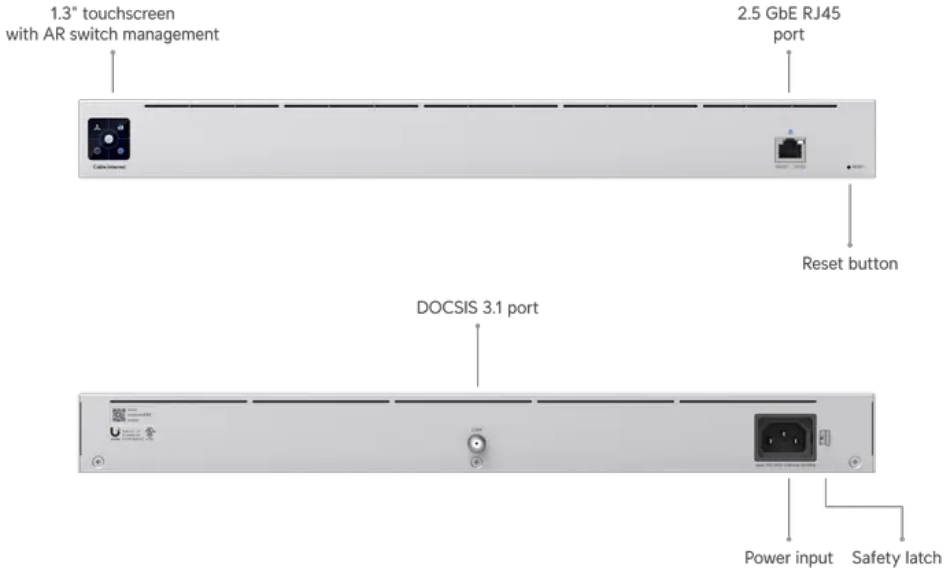
- **DAC Cables:** For network devices that are installed in the same rack a direct attach copper cable will be used to connect these devices together. Each DAC will have a 1-25gigabit Uplink SFP28 connector on either end. These DACs have auto link optimization that will change uplink speeds depending on the network usage, they can also be configured to a static speed manually within the device software.

Uplink DAC with 1-25G Auto SFP28 connectors

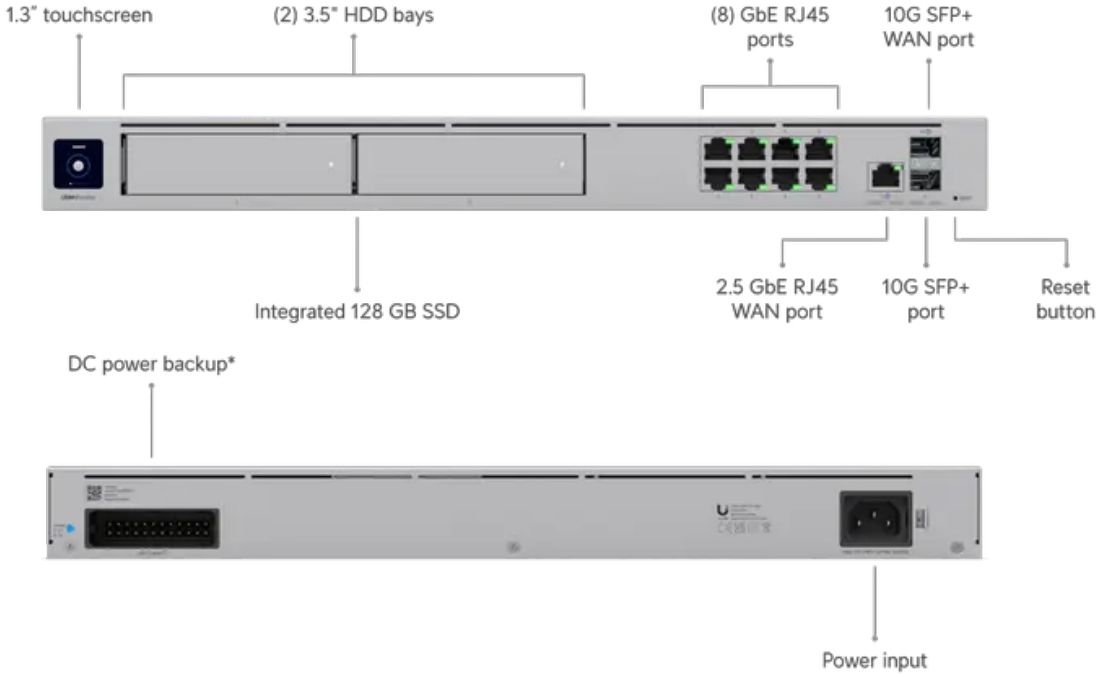
Network Hardware

ASTL will be using all Ubiquiti (UniFi) equipment to host all network devices and security management. They are reliable and easy to manage either using CLI or GUI. For upgradability the devices can be traded in for credit towards a new device. UniFi has excellent support

- **UniFi Cable Internet (UCI)**: This 1U device is a multi-gigabit DOCSIS 3.1 cable modem that will be used for the failover internet connect. It is compatible with Comcast Business and Xfinity as a customer owned modem. The Comcast technician will help get it activated during installation. This will connect to the router via CAT6. ASTL will only need 1 of these at a cost of $279.

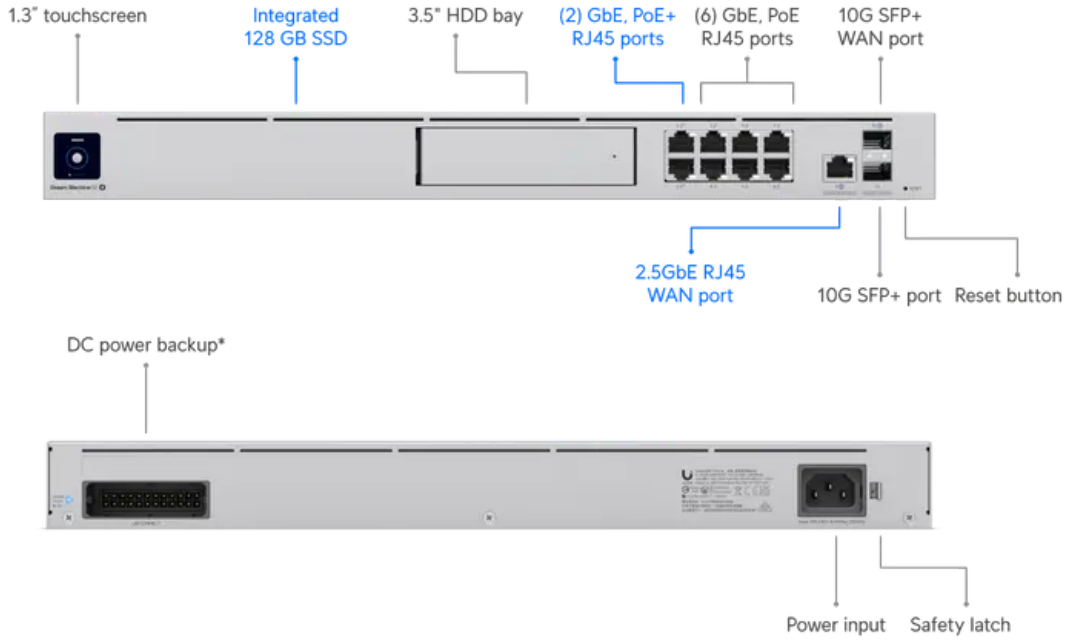


- **UniFi Dream Machine Pro Max (UDMPM)**: This is Layer-7 1U device will be the main hub as serve as the firewall, gateway, router, VPN functionality, and CC-TV DVR for the network. It consists of 8x gigabit RJ45 ports, 1x 2.5 gigabit WAN port (this will be used for t he failover ISP), 1x 10 gigabit SFP+ WAN port (this will be used for the primary ISP), and 1x 10 gigabit SFP+ port (this will be used to connect to the aggregation switch). The front 7 ports will be disabled. Port 8 will be enabled as the console port. There will be 2x 24TB 3.5” HDDs installed for CCTV capture. OpenVPN will be set up for those who want to work remote.



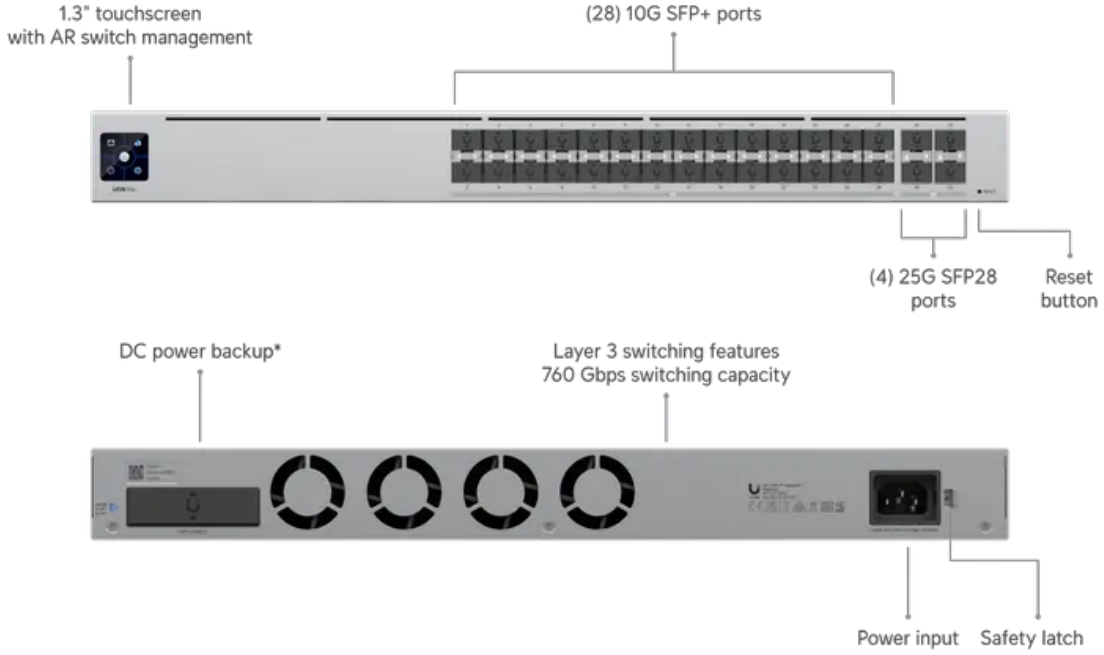
*Requires UniFi Power Backup.

- **UniFi Dream Machine Pro SE (UDMPSE)**: This Layer-7 1U device does everything the Pro Max does, except this ones use case is going to be for VoIP routing only. This will connect via a DAC cable to the aggregation switch. Ports 1-7 will be disabled and port 8 will be configured as a console port. The WAN RJ45 port will also be disabled. The regular 10G SFP+ port will also be disabled. If needed, ASTL can install an additional 3.5” HDD for CCTV capture if needed, it will not be used at this point.



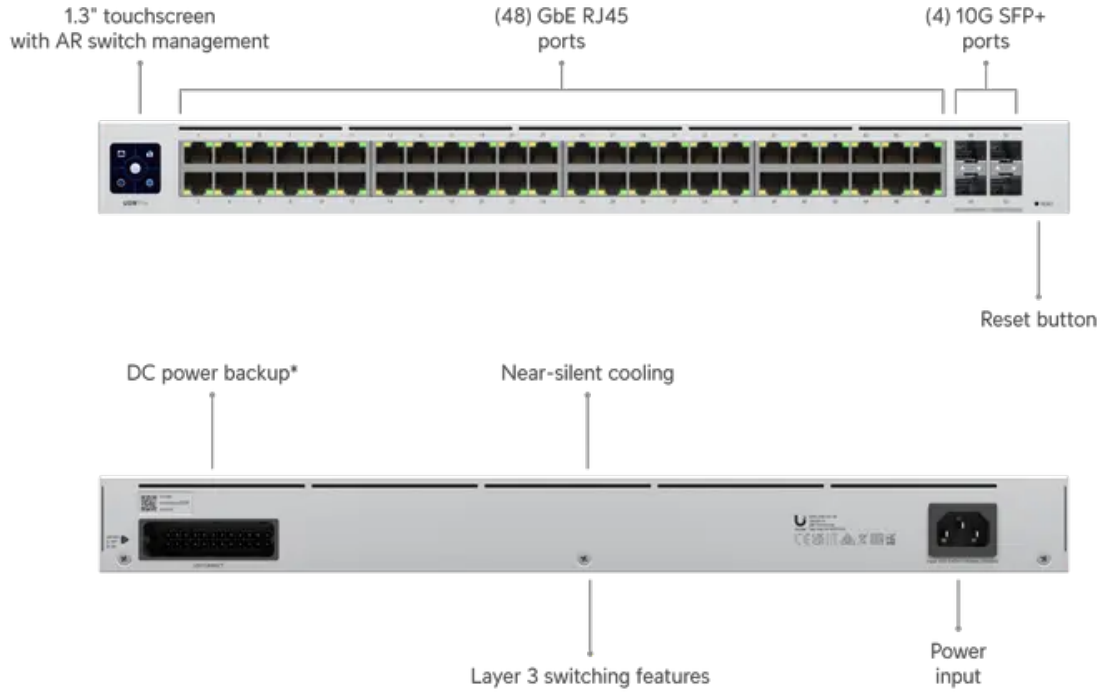
*Requires UniFi Power Backup.

- **<u>UniFi Hi-Capacity Aggregation Switch</u> (USWPA):** This is a Layer-3 1U 32 port 10G SFP+ switch. This will be used to connect all the switches and routers together within the network. For the MDU in the West Storage Room a fiber optic 10G SFP+ transceiver will be installed to connect that switch to the network. All of the other devices will be connected to this switch via DAC cables. Any unused ports will be disabled.



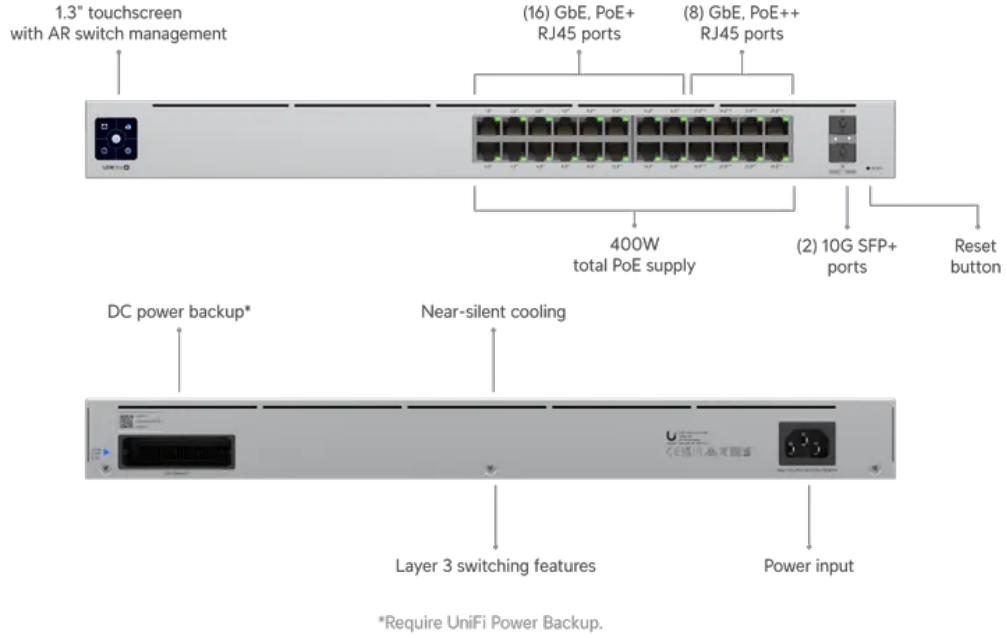
*Require UniFi Power Backup.

- **<u>UniFi Pro 48 Switch</u> (USWP48)**: This is a Layer-3 1U 48 port RJ45 switch. These will be used to connect all client devices and printers. Any unused ports will be disabled.

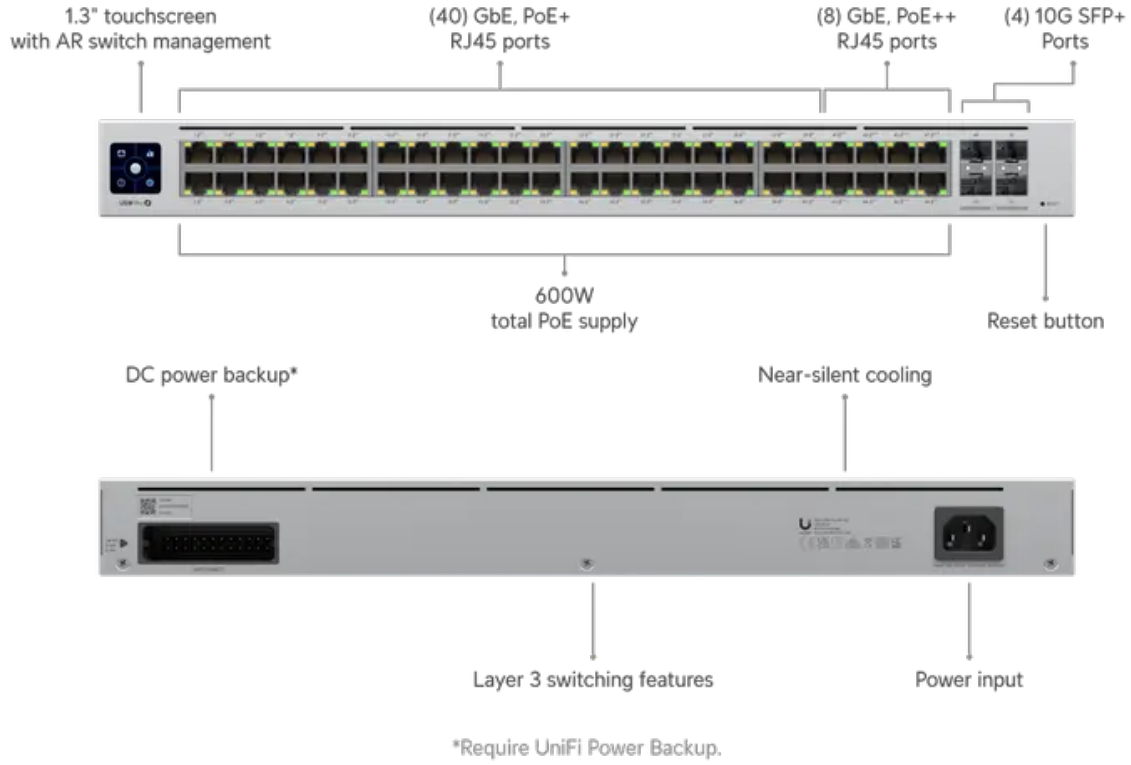


*Require UniFi Power Backup.

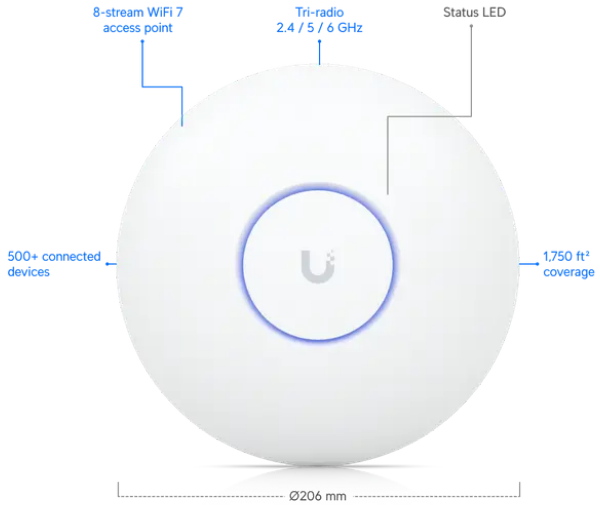
- **UniFi Pro 24 PoE Switch (USWP24POE):** This is a Layer-3 1U 24 port Power over Ethernet switch. These switches will provide connectivity used for the VoIP phones, wireless access points, badge access readers and security cameras. This switch will even power these devices without the need for power adapters. This will give them plenty of ports for the needed amount of VoIP phones, APs, badge readers and cameras; as well as room for growth. Any unused ports will be disabled.



- **UniFi Pro 48 PoE Switch (USWP48POE)**: This is a Layer-3 1U 48 port Power over Ethernet switch. These switches will provide connectivity and power for badge readers and security cameras without the need for power adapters. There will be enough ports for expandability, any unused ports will be disabled. ASTL will need 2 of these at a cost



- **<u>UniFi U7 Pro Max</u> (U7PROMAX):** This is a ceiling-mounted WiFi 7 AP with 8 spatial streams, 6 GHz, 5 GHz, and 2.4GHz band support with a spectral scanning engine to help provide reliable interference-free WiFi connectivity. These use a band steering wireless mesh network and use up to 802.11v technologies. They work with RADIUS technology, VLANs, and Captive Portals. These use MIMO technology and have a speed capacity of up to 2.5 gbps. They also can support up 500 client devices simultaneously. ATLS will have 8 of these throughout the facility to ensure reliable connectivity to client devices. These cost $279 each.



Security Devices

There are a few security devices that ASTL will need to ensure their products and data are safe. Surveillance cameras will be used throughout the interior and exterior of facility as well as badge readers at all exterior doors, warehouse entry internally as well as each office and of course the server room.

- **<u>AI Dome</u> Cameras:** will be used throughout the exterior of the facility. They record in 4K, use PoE for power and use an ultra wide dome camera with enhanced AI capabilities for motion detection and license plate detection. They also have long-range IR night vision.

- **AI 360 Cameras**: will be used throughout the interior of the facility. These offer 360 degree surveillance. These have enhanced AI capabilities as well as IR night vision.

- **G3 Intercom**: These will be placed at every exterior door. They have a built in camera, microphone and speaker. Guests can call the person they are visiting. Employees can also enter in a PIN or scan their badge to unlock the door to gain entry into the building.

- **G3 Reader Pro**: These will be placed at all office doors, storage room doors, conference rooms, and interior warehouse entry points. These have built in cameras, NFC card readers (for scanning badges) or a PIN maybe entered. These have a doorbell function, which can be disabled in the UniFi software.

Other Devices

- Each employee will be given either a Desktop or Laptop depending on what their work entails. They will all be able to connect to the network either using a wired or wireless connection. Accessories will be provided for these devices as well.
- Shipping, Receiving and Fulfillment workstations are equipped with a label printer that connects directly to their computer via a USB cable.
- There are several printers throughout the warehouse and a copy room where the all office printers are located. 1 printer is a color marketing printer for large banners, product labels and other marketing tools, which is only accessible to the marketing team. There is also one Multifunction printer (laser printer/scanner/copier) in the copy room which all employees have access to with a login. The other five printers are black and white only laser printers, which all employees have access to with a login.
- Each conference room will have a display for presentations. The presenter will be able to connect to it wirelessly.
- Private Internal Web server will be used for day-to-day operations which will give certain employees to cloud services, time management and other resources.
- Onsite Back Up Network Attached Storage device to back up all computers.
- File Storage NAS for FDA and other records.
- File Storage NAS for Marketing and Artwork storage.
- File Storage NAS for CC-TV footage to backed up to.
- G3 Touch Enterprise phones will be installed in all conference rooms and the lobby, copy room and IT office.
- G3 Touch Pro phones will be installed at all workstations.

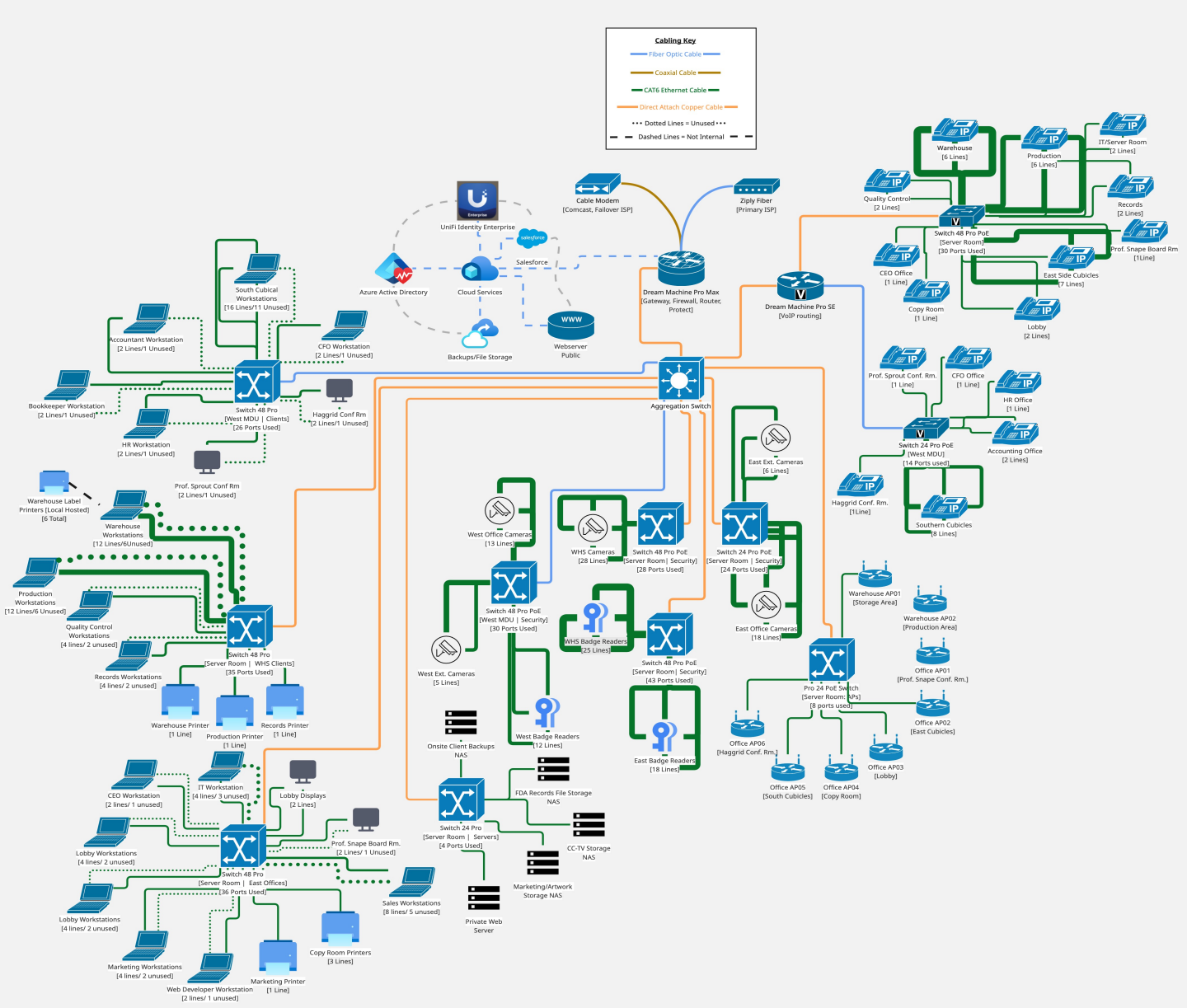
Cloud Services

- **UniFi Identity Enterprise:** this will integrate all employees to the network, give VPN access (using OpenVPN), see CC-TV footage (management only), and authenticate to additional cloud services via Single Sign-On (SSO).
- **SalesForce:** will be used for inventory management, order fulfillment and shipping.
- **Azure**: will be used for active directory, company issued device monitoring and virtual machine environments.
- **Microsoft 365:** will be used for documentation, email, OneDrive backups and Teams for instant communication.
- **Public Web Server**: to host ASTL's website for customers to view information on the company as well as be able to place online orders with payment options. This will be synced with SalesForce.

Network Topology

The topology was created using Miro and made public to anyone with a link: (which gives a better view than a still image, and allows you to zoom in on certain segments of the network.
CSNT-Capstone-Project : ASTL Network

The topology for this network is a Hybrid Topology. It has elements of 4 different topologies.



1. **Start Topology**: is used for. The central nodes with multiple devices such as the desktops, printers, access points, etc. Where each switch serves as a hub, and the clients connect directly to it.

2. **Bus Topology (Logically)**: is used connecting the Dream Machine's firewall to multiple routers, internet and cloud services via a common pathway, which resembles a bus-style backbone. It's not physically a bus, but it is a single point of network aggregation before distribution.

3. **Mesh Topology**: is used in the interconnected routers/switches which offer redundant paths between segments for the VoIP system, office devices and warehouse devices.

4. **Hierarchical Topology**: is used in a tiered structure, with the firewall, core routers, and distribution switches, followed by access devices which resemble a tree topology design.

Part 2

Network Configuration

The overall network will contain elements of a Class A network that is segmented and subnetted (10.x.VLAN ID.CLIENT ID).

VLANs

The network will have VLANs separating the different departments and devices. VLANs will be subnetted to only contain the amount of IP Addresses the device needs. This will be configured in the UniFi Network Controller on UniFi Identity Enterprise Admin Console. These are necessary to isolate specific devices on the network.

VLAN ID	Name	Devices Included	Purpose	Device Count	CIDR	Avali. IPs
5	Accounting	Accountant & Bookkeeper Computers	Isolate financial systems for compliance and security	4	10.0.5.80 /29	6
10	Development	Developer computers	Secure Development environments for code and tools	2	10.0.10.104/30	2
15	Office	Security Devices (Badge Readers/Cameras), Receptionist and Security Guard	Segment for front office and security-related systems	102	10.0.15.0 /25	126
20	Management	CEO, CFO, HR, Safety Manager Computers	Isolated segment for executive and management teams	8	10.0.20.48/28	14
25	Marketing	Marketing Computers & Marketing Printer	Segment for marketing team and related devices	4	10.0.25.88/29	6
30	Operations	Herbalist, Pourer, Tincture, Opperations Manager, QC, Project Manger, Computers	Used by production and operations management teams to give the access to specific tools	20	10.0.30.224/27	30
35	Records	Records Computers	Access for record keeping and compliance staff	4	10.0.35.96/29	6
40	Sales	Sales Computers	Devices used by internal or field sales teams	6	10.0.40.64/28	14
45	Supply Chain	Receiving, Shipping, Fulfillment, Supply Chain Manager, Product Manager, Computers	Used for supply chain logistics and fulfillment systems	16	10.0.45.0 /27	30
60	Conference Room	All conference devices (excluding phone)	Reserved for conference room AV and collaboration tools	6	10.0.60.72/29	6
70	VoIP	All IP Phones	Handles IP phones and voice traffic using QoS	41	10.0.70.128/62	62

VLAN ID	Name	Devices Included	Purpose	Device Count	CIDR	Avali. IPs
90	Servers/ Printers	Servers, NAS, Printers (excluding label & marketing printer)	Segment for backend servers and shared print resources	10	10.0.90.32/28	14
99	Network Management	All switches, routers, IT & Access Points	For managing core network infrastructure	26	10.0.2.192/27	30
180	Guests	Guest WiFi	Public WiFi with limited access and prompts users with a Captive Portal to gain access	250	10.0.180.0/24	254
199	Black Hole	All unused switch ports	Security sink for unused switch ports	192	10.0.199.0/24	254

Device Communications

- All office, warehouse and computers can communicate with printers, the file storage storage NAS and Back Up NAS.
- All DHCP and DNS will be handled using the UniFi Identity Network Controller that is installed on the Dream Machine
- VoIP Phones connect through a separate Dream Machine with it's own dedicated switches. This Dream Machine has UniFi Connect installed to manage and monitor all VoIP devices. This dream machine also has it's own dedicated Firewall setup for VoIP. This Dream Machine also allows access back to the LAN.
- The internal web server can only be accessed by office and warehouse computers.
- Wireless Access Points (APs) provide wireless connectivity for all company devices and guest devices. Company devices can connect use the WPA3 Enterprise standard by either using SSO or their company email address and password. RADIUS will be enabled to automatically connect company laptops. Personal devices or guest devices can connect to the guest wireless network after providing required information via a Captive Portal.
    - ASTL-Corporate - Uses RADIUS and WPA Enterprise standards to login.
        - MAC address filtering will allow for the company device to connect to proper VLAN
    - ASTL-Guest - Uses a captive portal to get the person's name, email address and phone number, and the reason for their visit.
        - Employees have a sign in option for their personal smartphone or tablet.
        - Connections, for the guest connection will expire after 8 hours.
        - The guest network will be isolated from the companies resources to prevent them from accessing sensitive data, printers, etc.
- All endpoints access off-site backup servers and cloud services via the 5506-X firewall to the ISPs.

Firewall & Security Configuration

The Dream Machine has a built in firewall that can be configured as well as other built in security features:

- Firewall:
    - Outside Interface (WAN): Connects to the two ISPs for redundancy
    - Inside Interface (LAN): Connects to routers
    - DMZ: Configured for off-site backups, remote file access and OpenVPN
    - Web Filtering is enabled to prevent access to rogue websites and NSFW (Not Safe For Work) content.
- Access Control Lists (ACL):
    - VoIP VLAN (70) —> UniFi Connect on UDP ports 5060 (SIP) and RTP range
    - Block VLANs 5, 10, 15, 25, 30, 35, 40, 45, 70, 99, 180, 199 from each other
    - Allow VLAN 60 to be accessible to all other except 90, 99, 180 and 199
    - Allow VLANs 5, 10, 20, 25, 30, 35, 40, 45, 60, 180 and Receptionist/Security Guard computer filtered internet access (TCP 80, 443)
    - Allow VLANs 15, 90, 99 restricted internet access to specific websites
    - Deny any inter-VLAN communication by default; only allow what's explicitly needed
    - Static IPs will be used on VLANs 15, 70, 90, 99
- Security Best Practices:
    - Enable DHCP snooping and port security on all switches
    - SSH enabled for specific users for device access
    - All unused ports are disabled and assigned to VLAN 199
    - Configure SNMPv3 for monitoring hardware

Part 3

Storage, Virtualization, Wireless & Physical Security

Storage Area Network (SAN) Usage:

SAN, will be used specifically in the server room (VLAN 90). There are several centralized Network Attached Storage (NAS) devices that contain critical business data. High-speed access to shared volumes for virtualized hosts. And efficient backup and disaster recovery through snapshots. This will benefit ASTL since it reduces I/O load on servers, enabled scalable storage independent of server hardware and facilitates clustering and failover.

Virtualization

Hypervisors will be used using Microsoft Azure cloud services to virtualize intranet and HR tools, the Domain controller and an internal backup file server. SalesForce will also be used on a virtualized server for all sales, inventory management, shipping and order fulfillment. This benefits ASTL by having efficient use of hardware, easier system recovery an snapshots ad faster deployment and cloning for testing and development environments.

Cloud Computing

- Off-site backups using OneDrive
- Workday for HR tools
- Quickbooks for Accounting
- Azure Active Directory - for device and user onboarding
- Email, Productivity and collaboration using Microsoft 365 (Exchange Server for email, Office for productivity and Teams for team collaboration)
- Failover DNS & Monitoring Tools
- SalesForce for inventory management, sales,
- Ubiquiti's UniFi Identity Enterprise for SSO applications, RADIUS, VPN (OpenVPN), Network Configuration and Monitoring, Support Tickets, Building Access Control, VoIP monitoring, and Time Keeping

Wireless Network

There a total of 8 Wireless Access Points throughout the offices and warehouse. They are configured as follows:

- SSIDs:
    - ASTL-Corporate
        - WPA3-Enterprise via RADIUS/Active Directory Login
    - ASTL-Guest
        - Captive Portal Login (VLAN180)
            - Guest will be required to enter in their Name, Email Address or Phone Number (to send a code they must enter), and the Reason for their visit. They must also accept the Terms of Use Agreement.
            - Employees can bypass the form by clicking/tapping a Login button and sign in using their company credentials.
    - Security Practices:
        - VLAN segmentation to isolate guests from internal traffic
        - APs configured to block inter-client communication
        - MAC address filtering will be used on ASTL-Corporate

- Strong WPA3 with 802.1X used where possible

Physical Security Measures

- Device Security:
  - Server racks are locked in a locked equipment room with badge access (this includes the MDU in the West Storage Room)
  - CCTV and badge readers throughout the building to secure assets and monitor theft risks
  - NAS devices and switches are secured in locked cabinets (this includes the MDU in the West Storage room)
- Building Security:
  - Receptionist and Security Guard monitors the main entrance
  - Visitors must sign-in with the receptionist and receive a visitor badge, they must also be escorted by an ATSL employee. Truck Drives may not use the restrooms and can only enter the Loading Docks with an Supply Chain employee escort.
  - All employee workstations require strong passwords (at least 12 characters long and expire every 90 days) or biometric authentication with auto-lock features turned enabled. VoIP phones require the employee's badge number and a pin to sign in.

Part 4
Intrusion Detection, Hardening, Monitoring & Data Protection

Intrusion Detection and Prevention

Ubiquiti's UniFi Dream Machine Pro has bultin-in Threat Management tools that are enabled by default, since ASTL will be using UniFi Identity Enterprise as well it will allow the Dream Machine to use Ubiquiti's AI threat detection to ensure potential threats get blocked and reported immediately. The primary Dream Machine (Pro Max) is placed in-between the WAN and LAN interfaces to monitor all traffic in and out. Which the AI threat detection should have no issues preventing attacks. Detections will focus on port scans, suspicious login attempts and malware signatures. For prevention measures, all known malicious IPs via threat intelligence feeds will be blocked, traffic will be rate-limited from unknown origins and geo-blocking will be enabled for regions not severed by the company.

System Hardening

Operating systems will be regularly updated, and software will be updated once it has been tested in a virtual sandbox, to ensure there aren't any major issues for end users. All servers will use CIS Benchmarks. All unused services will be disabled and only the necessary port will be opened on client devices and network devices.

Access Controls are enabled, UniFi Identity Enterprise will be used for Multi Factor Authentication and Passkey management on trusted devices. Employees will be required to install the UniFi Verify application onto their personal smartphone to get push notifications for MFA. Role-Based Access Control (RBAC) will be configured. Principle of Least Privilege will also be enforced on all accounts.

Patching, Linux servers will receive automatic security updates. Windows Servers will use Windows Server Update Services for Windows Devices. Mac devices will also receive all security updates and major releases will be postponed until IT approves them and pushes the updates through MDM policies. This all can be managed with Azure Active Directory and UniFi Enterprise MDM tools.

Monitoring

Monitoring tools that will be used include, Zabbix for network performance and uptime monitoring. SNMPv3 will be configured for secure polling. Syslog server will be used to collect logs from routers, switches, firewalls, and critical systems.

All devices will have CPU, Memory and Disk Usage tracked. Bandwidth utilization will be tracked. Unusual login attempts will be tracked and reported. Network device statuses will be tracked. Anything critical the IT department will be automatically notified by either push notifications or email.

Data Management and Protection

- Backup Strategy:
  - Local backups are stored on a NAS in the secured server room
  - Off-site encrypted backups are pushed automatically to cloud
  - Snapshot-based backups for Virtual Machines every 6 hours
- Backup Schedule:
  - Full backups nightly starting at 6PM
  - Incremental backups ever 4 hours
- Data Encryption
  - Data at rest: Encrypted using LUKS on Linux servers, BitLocker on Windows Devices and FileVault on Mac devices.
  - Data in transit: enforced via HTTPS, SMB over TLS and VPN
- Data Recovery Plan:
  - RPO (Recovery Point Objective): 4 Hours
  - RTP (Recovery Time Objective): 6 Hours
  - Regularly tested disaster recovery drills for IT/Network Admin employees

Summary

ASTL's network design includes a primary 10Gbps fiber ISP (Ziply Fiber) and a failover 2Gbps coax ISP (Comcast Business). The network will utilize shielded CAT6 cable for Ethernet connections, with color-coded jackets for different devices (black for security, white for computers, blue for VoIP). The design includes two 42U server racks in the server room, a 15U rack in the West Storage Room MDU, and PoE-powered access points, security cameras, and door access badge readers.

ASTL's network infrastructure will utilize UniFi equipment for reliability and ease of management. The network will include a failover internet connection, a main hub (UDMPM), a VoIP routing device (UDMPSE), aggregation switches, and access switches. Security measures include surveillance cameras, badge readers, and intercoms.

The network will utilize VLANs for departmental separation and subnetting to optimize IP address usage. All office, warehouse, and computers can communicate with printers, file storage, and backup NAS. VoIP phones will connect through a separate Dream Machine with dedicated switches and firewall for VoIP management.

Full backups are performed nightly at 6PM, with incremental backups every 4 hours. Data is encrypted at rest and in transit, and a data recovery plan with RPO of 4 hours and RTP of 6 hours is in place.

Image Sources:

UniFi Device Pictures were found on https://store.ui.com

Other cables and hardware images were found on https://amazon.com

Floor Map was created in Draft Paper app: https://apps.apple.com/us/app/draft-paper/id911636555

Network Topology was created using Miro: https://miro.com/app/board/uXjVIqFxX1s=/?share_link_id=309423665351