DEPLOYMENT GUIDE

Aruba Instant On

November 2021

ABOUT THIS GUIDE

The Aruba Instant On Deployment Guide is designed to enable customers to achieve optimal results when using Aruba Instant On products. This document serves as a deployment guide and also provides product selection recommendations, network design considerations per desired use cases, and best practices for each deployment.

INTENDED AUDIENCE AND SCOPE

This document is intended for small business owners and Aruba Partners, who are responsible for deploying and configuring Aruba Instant On devices. It is expected that readers have a basic understanding of networking concepts.

RELATED DOCUMENTS

In addition to this document, readers are advised to check the following product documentation for step-by-step configuration details.

- Aruba Instant On User Guide

Acronyms	Description
WLAN	Wireless Local Area Networks
MU-MIMO	Multi User Multiple-Input and Multiple-Output
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
DHCP	Dynamic Host Configuration Protocol
NAT	Network Address Translation
ISP	Internet Service Provider
PoE	Power Over Ethernet

ARUBA INSTANT ON OVERVIEW

Aruba Instant On is a new family of access points (APs) and switches designed to address the current and future needs of small businesses. The Aruba Instant On products series are designed to meet the needs of small business network environments — simple to set up and manage and are secure and reliable. Aruba Instant On deployments can be managed through a mobile app supported on iOS and Android, through a cloud portal or using a local web GUI.

In today's environment, small businesses face several challenges to stay afloat and competitive. They are resource constrained, lack technical expertise, struggle with limited budget along with keeping up with an explosion of devices and bandwidth-heavy applications running on a network. These businesses want to acquire cost-effective, next-gen networking solutions that are focused on both high performance and cost optimization.

The Instant On product family provides a reliable, high-speed wired and secure Wi-Fi experience built on Aruba's decades' long heritage in enterprise networking. Instant On APs come with DHCP, NAT, firewall, PPPoE and router capabilities that allow them to be directly connected to an ISP modem. This purpose-built access point portfolio also supports Smart Mesh technology to satisfy the ever-growing coverage needs of small businesses. The switch portfolio has 2 high level models i.e. 1930 (8, 24 and 48 port PoE, non PoE SKUs) switches and 1960 (24, 48 PoE and non-PoE SKUs and a 12-port 10GBT aggregator) switches to meets the needs of use cases in small business environments including the need for higher PoE power as well as support for Class 4 (30W) and Class 6 (60W) PoE, flexible network management along with easy bring up.

PRODUCT PORTFOLIO

This product family includes indoor and outdoor access points to support multiple deployment scenarios. Refer to the following table for details.

Name	Device Type	Deployment Recommendations
AP11	Indoor, 2x2:2 MU-MIMO	Boutiques, cafes
AP11D	Desktop, Hospitality, 2x2:2 MU-MIMO	SOHO, in-room for small hotels
AP12	Indoor, 3x3:3 (5GHz), 2X2:2 (2.4GHz) MU-MIMO	Medical offices, larger cafes, smaller offices, connected homes, gaming use
AP15	Indoor, 4x4:4 (5GHz), 2X2:2 (2.4GHz) MU-MIMO	Larger offices, tech start-ups
AP17	Outdoor, 2x2:2 MU-MIMO	Open-air restaurants and cafes, poolside, receiving docks
AP22	Indoor, 2x2:2 Wi-Fi 6	Wi-Fi 6 access points for locations where client density is high
1930-8G-2SFP	8 (G) port 2SFP (fanless) 8 (G) port 2SFP Class 4 PoE 124W	Hotel, SOHO, small offices.
1930-24G-4SFP/SFP+	24 (G) port 4SFP/SFP+ (fanless) 24 (G) port 4SFP/SFP+ Class 4 PoE 195W 24 (G) port 4SFP/SFP+ Class 4 PoE 370W	Medium/Larger offices. Choose model based on port count and desired PoE budget

1930-48G-4SFP/SFP+	48 (G) port 4SFP/SFP+ (fanless) 48 (G) port 4SFP/SFP+ Class 4 PoE 370W	Larger offices. Choose model based on port count and desired PoE budget.
1960 12XGT 4SFP+	12 (10G) XGT port 4 SFP+ ports	Aggregation switch for small deployments and also for connecting 10G desktops, servers and storage for Small Businesses.
1960-24G-2XGT/2SFP+	24 (G) port 2XGT / 2SFP+ 24 (G) port 2XGT / 2SFP+ Class 4/6 PoE 370W	Coffee shops. Choose model based on port count and desired PoE budget
1960-48G-2XGT/2SFP+	48 (G) port 2SFP / SFP+ 48 (G) port 2SFP / SFP+ Class 4/6 PoE 600W	Healthcare, training facilities. Choose model based on port count and desired PoE budget.

The portfolio can be managed with a Cloud portal and a Phone App (iOS, Android) and provides an easy way to onboard, setup and manage the Instant On portfolio of APs and Switches.

DESIGNING AN INSTANT ON NETWORK

Site design

Instant On is a simple, easy to deploy turnkey networking solution consisting of one or more Instant On APs or Switches. A single site can include up to 25 Instant On Devices (mix of APs/Switches) supporting 8 wireless (SSID) and 22 wired (VLAN) networks. The Instant On portfolio offers a number of ever-expanding list of features including Smart Mesh, DHCP, NAT support, LAG, RSTP, client blocking, firewall rules that meets the needs of Small Business.

The first device to connect to the ISP equipment can either be an AP or a Switch. Instant On APs have the option of acting as a router (and can handle PPPoE configuration along with VLAN support) and can also act as a DHCP server providing IP addresses to the wireless network. The first device at a site can be configured either using DHCP or static IP using PPPoE.

Using DHCP: (applies to APs and Switches)
Connect the access point to power and connect the ethernet cable to the ISP modem/gateway. It will automatically obtain an IP address from DHCP and connect to the Internet and be ready to be onboarded to the site. Instant On 1960 switches support a DHCP server and can be used to provide IP address to devices including Instant On Access points, wired clients etc

Using PPPoE (applies only to APs):

- If you need to connect to the ISP's server and get authenticated, then follow these simple steps. After the AP boots, it will broadcast an SSID InstantOn-AB:CD:EF
- Connect to this SSID and use the web browser and enter the URL https://connect.arubainstanton.com. Enter the authentication credentials and you are done.

Please make sure the following ports (TCP 80, TCP 443, and UDP 123) are not blocked by the ISP modem/gateway, so that the Instant On device has connectivity to the Internet. If the ISP provides an IP address only on a particular

tagged or untagged VLAN, there is an option to choose the right uplink VLAN as well as specify if it is tagged or untagged.

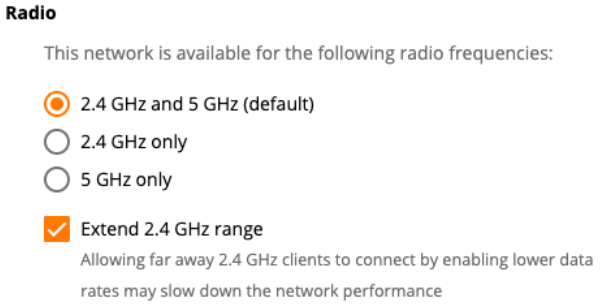
It is required that all Instant On APs that need to be part of the same network are connected to the same Layer 2 wired network. Instant On APs can act as a DHCP server for wireless clients only (i.e., it cannot hand out IP addresses to wired clients and other Instant On APs connected to the wired network).

RF Settings and Coverage
Users have the ability to tweak the AP settings to control the RF environment. With this comes the ability to:

1. Control network band of operation. There are 3 options:
    a. 2.4GHz and 5Ghz
    b. 2.4 GHz only
    c. 5GHz only
2. Select channels
3. Select channel width

It is important to recall that Radio Frequency signals with higher frequency cover short distance compared to the low-frequency signals. Most wireless client devices are available to communicate over the 2.4 GHz (low freq.) and 5 GHz (high freq.) bands and by default Instant On APs are available to negotiate with those clients over both bands. It is highly recommended for the clients to connect over the 5GH band for higher throughput and performance but there can be scenarios where a larger coverage area may be desired.

Instant On provides the option for clients to still be connected over long ranges with the tradeoff of the lower speeds offered by the 2.4 GHz band. This can also be useful if the environment has a lot of obstructions (metal structure, walls, etc.) and coverage over lower speed is preferred over no coverage over higher speeds.



Switch Port traffic authentication, control, and aggregation
Users have the ability to tweak the switch settings to control port traffic. With this comes the ability to:

1. Port access control (802.1X)
2. Only allow traffic from a defined network at the port level. (Default: all networks)
3. Link Aggregation (LAG) for Increased bandwidth/resilience. Instant On and LACP versions.

Switch Features

1. **Support for 10G uplinks – Instant On 1930 as well as 1960** provide 10G ports for uplinks to build high-bandwidth interconnects between switches and the 12 port 1960 switch supports downlink 10GBase-T RJ45 ports for connecting other access switches as well as servers and storage designed for Small Business networks.
2. **Up to 60W of PoE** – Instant On 1960 switches provide Class 6 (up to 60W) and Class 4 (up to 30W) PoE support along with an increased power budget of 600W on the 48-port PoE model. Instant On 1930 switches support Class 4 PoE to support use cases that need PoE.
3. **Stacking –** simplifies management of multiple switches as one single entity and reduces management overhead and helps build resilient networks. Stacking can be configured either using Local Web GUI or through the Cloud portal or mobile APP. Hybrid stacking allows access and aggregation switches to be combined into one logical L2 entity. Support for stacking is available only on Instant On 1960 series switches.
4. **Support IEEE VLANs -** up to 256 VLANs, VLANs 4094 and 4093 reserved for internal usage (available ID 1-4092). Supports VLAN tagging and trunk port configs as well.
5. **Support 803.az EEE** - Energy Efficient Ethernet (EEE) technologies which are designed to reduce per-port power usage by shutting down ports when no link is present or when activity is low. Low power idle mode the ports will enter a low-power mode to reduce power consumption during periods there is notraffic on a network port. PoE scheduling for individual ports to power devices based on user configs are also available.
6. **Support for QoS** - switch can prioritize traffic based on the 802.1p tag attached to the L2 frame, 802.1p priorityvalues to various traffic classes which helps in better prioritization of the traffic. Also, Interface Shaping rate configuration can be enabled to all ports or to a specific port.
7. **Security Features** - named ACL support for both IP and MAC ACL support. RADIUS provides additional security for networks. Switch includes a RADIUS client that can contact one or more RADIUS servers for various Authentication and Accounting (AAA) services. The RADIUS server maintains a centralized databasethat contains per-user information and connect upto 4 RADIUS servers. At each given time only 1 of these RADIUS servers is used for both authentication and Authorization.
8. **IEEE 802.1 D/W/S** - supports loop free topology in a network, also allowing to have redundant links with use of spanning tree protocol. RSTP helps faster convergency and MSTP supports multiple spanning tree instances to efficiently channel VLAN traffic over different interfaces.
9. **DHCP Server / client modes** – Instant On 1960 switches can act as a DHCP server to provide IP address to its local clients as well work on DHCP client mode by receiving IP address from other DHCP server capable devices. Also support DHCP fallback feature where switch fallback to static default IP address when there is no DHCP server on the network. Can also be configured to act as a DHCP relay to relay packets between a DHCP client and server on different subnets. Support for DHCP server functionality is available only for 1960 series switches.
10. **Interface Auto recovery** – switch supports an Auto Recovery feature that allows ports to be placed in a suspended state when defined error conditions are met. Auto Recovery can help recover ports that are suspending with conditions like BPDUGuard, Storm Control, Port Security, Loop Protection and Link Flap Prevention.
11. **Port Mirroring -** Upto 4 port mirroring sessions can be configured and can be enabled on any member port of a stacked or standalone switch.

Cloud / AP Features:

1. **Application Visibility** – Instant On provides detailed visibility into the applications used in your network. It also shows a quick summary consisting of the top 5 apps. Users also have the ability to turn off application visibility which may improve performance. In this case, they will be able to view the traffic usage per client.
2. **Multiple Networks and Bandwidth control** – Control the amount of bandwidth each user/network can access. Users can set up multiple networks for different use cases. For example, in a Work From Home scenario, there can be one network for work related activities with no bandwidth control, another network for kids and yet another one for guests with limited bandwidth and site restrictions.
3. **Two Factor Authentication** – Ensure that your account is secure by using your mobile phone and a second token to access your account.
4. **Client Blocking** – Easily block clients if they interfere with network operations and unblock them after they start behaving again. This is useful to prevent attacks from endpoints that are compromised.
5. **Installation Wizard** – Follow the simple guided steps to setup your network according to your unique requirements in minutes. The AP placement wizard provides suggestions on where to place your meshed APs.
6. **RADIUS proxy** – For authentication with an external RADIUS, simplify your configuration by using a proxy IP address.
7. **IP Reservation** – For legacy and IoT devices that always should get the same IP address across reboots, The DHCP server on the AP allows for reservation of IP addresses.
8. **PoE Scheduling** – This feature not only saves energy but also improves the security posture for Small Businesses. Use PoE scheduling to automatically turn off (PoE powered) APs after a certain time (say 10 pm) to not only save energy but also prevent unwanted access to the network overnight.
9. **LED quiet mode** – Turn off the LEDs easily on the app to ensure the AP blends into its surroundings
10. **Editable Client Name –** Gives an ability to change client names for wired as well as wireless clients. Maximum supported length up to 32 characters, special characters are not supported though. This feature will be useful to identity personal devices such as cell phones and shared resources like printers.
11. **Shared Services –** Instant On supports Apple Bonjour, and Google Cast to discover devices and services on same L2 network without requiring any configuration. Instant on supports four types of shared services namely, print remote management, sharing, streaming. These services are available only on Employee type network.
12. **Built-in Customizable Captive Portal –** Use the capabilities of the built-in captive portal partners to customize the logo, welcome message and the terms and conditions for the Guest users in your network.
13. **External Captive Portal –** For capabilities such as analytics and to improve marketing capabilities for Guest networks, Instant On offers support for following providers:
    1. Aislelabs
    2. Purple
    3. Skyfii
    4. Wavespot
    5. Zoox

    The customer benefits are summarized below
    - Free features on Captive portal with Instant On
    - Easy integration with captive portal
    - High ROI, customer loyalty, advanced analytics and marketing capabilities to improve business
    - For Partner managed service, Partner can buy a pool of licenses and have the ability to manage all their customers
14. **Firewall Rules** - New network access control page will allow the site administrator to configure network access. User can set network to be either Restricted or Unrestricted to their subnet. User can also set restricted access with a list of accessible IPs from other subnets. Only supported for wireless clients/networks.
15. **Nord VPN Partnership** – Aruba Instant On supports multiple VPN vendors such as OpenVPN, KeepSolid VPN, ProtonVPN and has a partnership with NordVPN with discounted pricing.

For Instant On customers discounted pricing is available when ordering via the Instant On app. The joint solution offers many unique added-value capabilities as mentioned below

- Works with any sized Aruba Instant On deployment, anywhere in the world, from a single access point in a home to a medium sized business.
- Discounted pricing when ordered via the Instant On app.
- 256-bit AES encryption, no tracking of visited sites, and high throughput for streaming
- Optional ad blocking

Site management

Instant On APs and Switches support two options for hassle-free remote network management at the tip of your fingers. You may manage your Aruba Instant On deployments either using a Mobile App that is supported on iOS and Android or via a cloud portal that is accessible via a web browser. Administrative rights can be delegated to another user so that two users can manage and administer the same Instant On site.

For convenience, AP and Switch software updates are automatically performed to ensure you always have the latest and greatest software with the ever-expanding set of features and functionality. An administrator can schedule the default time that updates are performed to ensure consistency of updates.

The Instant On Mobile App offers multi-lingual support for a variety of regional languages, such as Simplified Chinese, Japanese, French, German, Italian, Spanish and Portuguese to ensure global usability. When the mobile app is opened, it detects the locale of the phone and sets the language accordingly. This configuration is saved and used every time the app launches. If the phone's locale changes the next time the app starts, it will set this new language as the default and save it. Mobile app trouble-shooting push notifications use the same local language.

Please make sure the onboarding device (laptop or mobile phone with Instant On app) is in-sync with the local time zone as Instant On APs will be configured per the time zone of the onboarding device. It is important to note that the web portal, as well as the mobile app, support feature parity between both options.

Wi-Fi security recommendations

Aruba Instant On supports employee as well as guest networks that include multiple security options. For instance, the latest wireless authentication security standard called WPA3 (aka Wi-Fi Protected Access 3) and the latest version of WPA2 are supported. For the employee network, more robust security options are available via an External Radius server. For the guest network, there is also an ability to have open guest network which requires no steps/authentication procedures to be followed to connect to the network. This simplifies user experience but is not recommended.

Guest users should be isolated from employee and business devices for security protection by creating a dedicated network for guest usage. A customizable internal captive portal for guest access is provided to make sure that the guest users agree to use Wi-Fi per your specified terms and conditions. You can also choose to turn on advanced features like Time-of-Day based network scheduling to restrict Wi-Fi availability outside of business hours. You also have the ability to hide the guest SSID although that is not part of the best practice recommendation.

Instant On APs can assign a dedicated VLAN each to one or more employee networks so that each employee network and its resources can be isolated from other employee networks. Instant On APs also offer a client blocking option to protect the network from malicious users.

LAN security recommendations

Aruba Instant On switches support employee and guest networks (as stated above) including include multiple security options support of time of day features as well. Network management supports IGMP v1, v2, Loop protection, Flow Control and 802.3x Storm Control. Ingress Rate limiting also supported via 802.1Q and 802.1p / DSCP support 4 queues for effective traffic mapping.

Loop control supported and option to enable RSTP (rapid spanning tree protocol) for efficient convergence times once a loop is detected. RADIUS supported for wired clients on a per port basic. with 4 readily available services and option to utilize own private server if required.

By default, the switch is in DHCP mode and provisioned using untagged VLAN 1. It is possible to configure the Static IP, Netmask, Gateway IP and DNS. A different management VLAN can be specified if required. In case the uplink port of the switch requires tagging, the tagged VLAN will be set on one port of the switch (Ethernet or SFP). All other ports will remain untagged.

AP placement recommendations

Where you place APs plays a crucial role in RF coverage. Here are placement recommendations for Instant On APs.

1. AP coverage: APs can cover up to 2500 square feet under ideal conditions, but the real coverage is dependent on the location of placement and the type of construction materials used in the location surrounding it.
2. Cable types: Always use Cat5(e) or Cat6 Ethernet cables to connect APs to the switch and Internet gateway.
3. Mounting APs: Mount the APs below the ceiling with the wires running above. APs that are mounted below the ceiling perform better because their signals are not affected by any surrounding ducting, power cables, and other construction elements. For the AP11D, mount the AP directly to the wall using a single-gang wall-box, or use the supplied desk mount.
4. AP location: identify the areas where Wi-Fi coverage is required, then place the APs accordingly. For example, place the APs inside of offices or hotel rooms rather than in hallways. This provides more efficient coverage with minimal interference. Also, avoid placing APs in the closet or behind solid metal objects. For more guidance, refer to the installation guide available in the Instant On online community.
5. Automatic channel selection: Instant On APs are dual-band access points (i.e., supports 2.4 GHz as well as 5 GHz frequencies). Selection of the optimal channels and transmission power is critical for optimal Wi-Fi performance and experience. Instant On APs support automatic selection of the best channels, transmission power and channel width to ensure that each AP offers the optimum experience to the users at any given point in time. When choosing an operating channel, the Instant On AP factors in how busy the surrounding wireless medium is, as well as if there is any Wi-Fi interference generated by other W-Fi and non-Wi-Fi sources like microwaves, in order to select the least crowded channel. Given that the interference and noise levels in wireless medium can change frequently, APs regularly scan the air to optimize the channel selection and power. If the operating channel becomes too busy due to surrounding Wi-Fi or non-Wi-Fi interference, then Instant On APs will change the channel automatically without any user intervention.
6. Outdoor APs: When using an outdoor AP, you should place it where coverage is desired. If the outdoor AP is connected using mesh from a wired Instant On AP, the outdoor AP should be placed in the line of sight of the wired AP, if possible. The maximum distance between the wired Instant On AP and mesh outdoor AP should not be more than 100 meters. For the better client connectivity AP17 has a range of 50 meters considering there are no apparent obstacles such as thick concrete walls. Outdoor APs should be installed within 3 meters minimum, 15 meters maximum height from the ground.

Smart Mesh design

The Aruba APs support Mesh Wi-Fi to provide the ability to extend the network to hard-to-wire areas. Instant On APs offer simple to configure Smart Mesh that you can set up in minutes. After the first Instant On AP (wired AP) has been added to the site, you can configure additional APs to connect over the air, if desired.

Although a single Instant On AP may support up to 8 Mesh APs, we recommend no more than 2 or 3 mesh APs connected to a single AP for enhanced performance. Instant On APs automatically determine the best node to connect based on signal quality and performance. For optimal performance, we recommend 1-hop mesh deployments.

For Mesh AP placement, we recommend a minimum of 16 feet (5 meters) and a maximum of 60 feet (18.25 meters) from the parent AP (the one that is wired to the switch or modem). Distance between the APs also depends on obstacles, such as thick walls, metal structures or glass. Mesh APs use the 5GHz band for backhaul connection while serving the clients on both radio bands (2.4 GHz, 5 GHz).

Another way to extend Wi-Fi coverage is by adding more Instant On APs to the same L2 switch using a network cable. As mentioned earlier, a single Instant On site may contain up to 25 access points (including those in a mesh). When available, wiring up the AP is recommended for better performance.

Partner-managed Instant On services

Instant On also offers remote multi-site management via the mobile app and cloud to support partner-managed IT services. IT partners can securely manage multiple customer sites (i.e., different customer networks) using a single instance of the Instant On Mobile App, without jeopardizing customer info, for convenient network administration. The Instant On app also supports real-time alerts regarding network health via email in order to initiate user intervention, if needed. This helps to eliminate dependence on on-site staffing for the end customer.

USE CASES

Let's look at a few representative use cases for deployment of Instant On Switches and APs. We will discuss how to design and deploy these switches and access points for each of these use-cases. We will also review the features that may be relevant to enable for each of the scenarios.

Although Instant On devices may be deployed for a number of different Small Business use cases, there's a good chance that your needs align with one or more of the use cases discussed below.

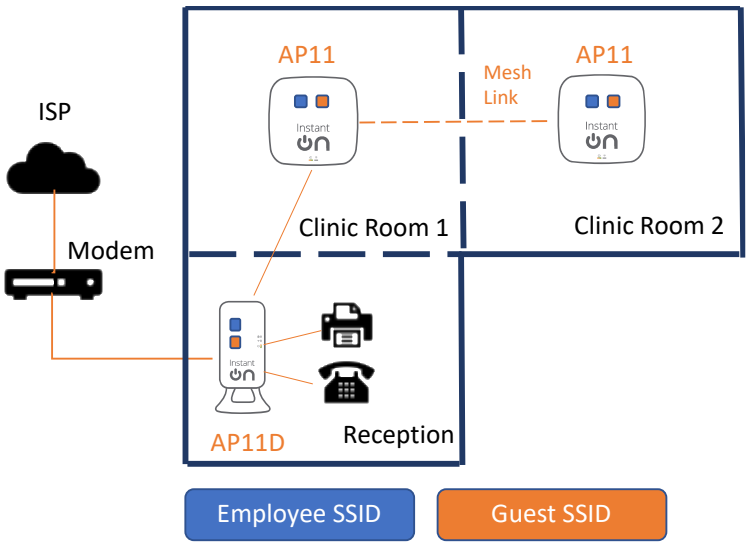
USE CASE #1: Small Clinic

- **Customer Requirements**
  - Simple to deploy and easy to manage Wi-Fi solution for a small clinic with a reception and 2 rooms
  - Separation of traffic for employees and guests
  - Connectivity for wired devices including printer and desk phone
  - Client Density: 10-20 active client devices at a time

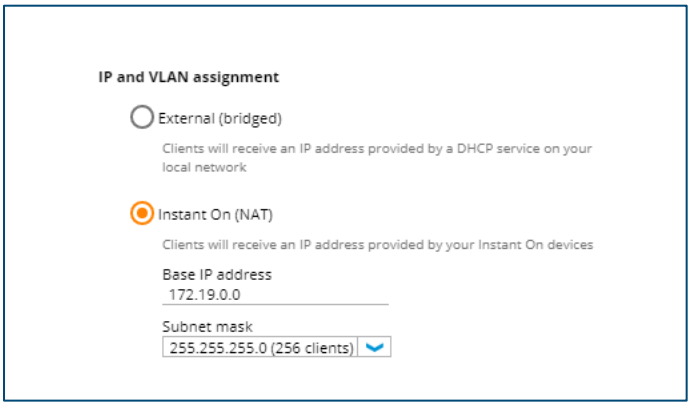
- **Hardware Guidelines**

  - Total of 3 APs – 2 units of AP11 (2x2:2) for the 2 rooms and 1 unit of AP11D (2x2:2, Desk Mount) for the reception

  - **Topology**



- **Configuration Guidelines**
  - Step 1: AP Onboarding and Site Creation
    - We recommend the desk mounted AP11D to help in connecting desk phones and wired printers in the reception
    - When creating a new wireless network, by default the network will be assigned to the wired management network or a new wired management network will be created if one has not been created.
    - If the AP is connected directly to the ISP modem, ISP should provide the management IP address Instant On AP. If ISP only offers a single IP address, then an external gateway or router is required to hand out IP address for the AP.
    - Choose Router mode for the Instant On AP. It also has a built in NAT and firewall for security.
    - The first Instant On AP will act as a DHCP, NAT server for wireless clients (picture below)



  - Step 2: Extend the network using one-touch Mesh
    - Add an AP11 by wiring it to the AP11D in the reception

- Extend the coverage to the second room by creating a mesh link between the two AP11 in the clinic rooms

- **Recommended Feature Set**

Instant On Feature/Offerings	Benefits
Separate networks for different users	Separate network for Employees and Guests to keep traffic isolated
WPA3	Enhanced Wi-Fi security for Employee as well as Guests. WPA3 Enterprise for Employee network and WPA3 Personal for Guest network
Smart Mesh	Aruba Instant On APs offer One click mesh easy way extend the Wi-Fi coverage at hard to wire areas and ensure better coverage. For e.g., patios and multiple floors and larger rooms.
PoE Scheduling	Automatically turn off PoE controlled APs after business hours and automatically turn on PoE cameras during nights
Internal Captive Portal	Customize your Guest logon portal with the logo and name of your clinic
Router mode	If no switch is needed for wired connections (cameras, cash register, etc.), Instant On AP can be connected directly to the modem

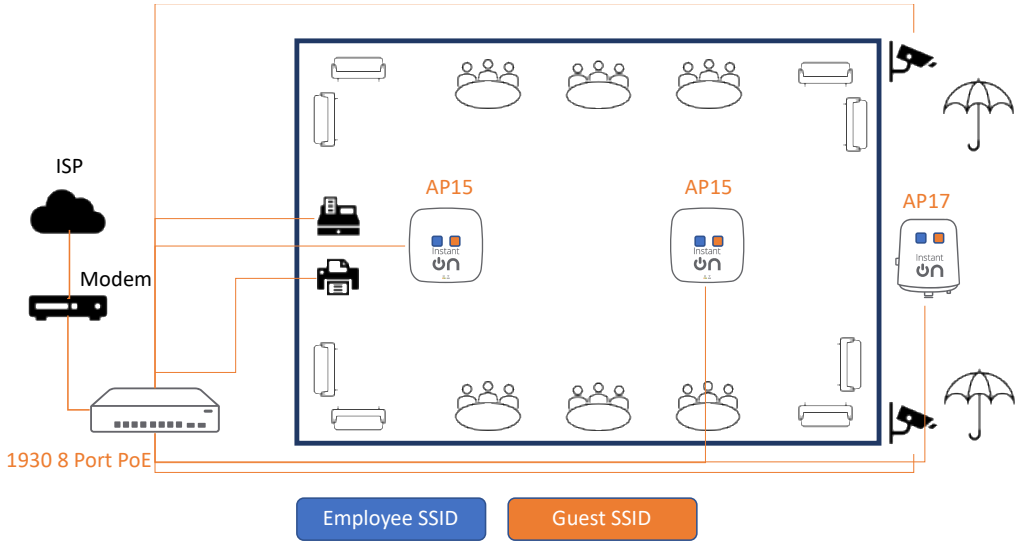
USE CASE #2: Medium/Large Coffee Shop

- **Customer Requirements**
  - Hassle-free, reliable Wi-Fi experience for customers indoors (large open hall) and outdoors (patio)
  - Simple to deploy and easy to manage Wi-Fi solution
  - Secured Wi-Fi access for employees and guests with the ability to scale during peak times
  - Client Density: 40-50 active client devices at a time (indoors and outdoors) with client count doubling during peak hours

- **Hardware Guidelines**

  - Total of 3 APs – 2 units of AP15 (4x4:4) for the wide-open large hall and 1 unit of AP17 (2x2:2) for outdoor use
  - One Instant On Switch – 1930 8G 4SFP/SFP+ Class 4 PoE to support APs and other wired devices such as printers, cameras and cash registers

- **Topology**



- **Configuration Guidelines**
  - Step 1: Instant On Switch Onboarding and Site Creation
    - If the coffee shop has the need for wired PoE connections such as cameras, cash registers or printers, they can be connected to the Instant On 1930 8-port PoE switch
    - Connect the Instant On Switch to the ISP modem
    - ISP should provide the management IP address to Instant On Switch. If ISP only offers a single IP address, then an external gateway or router is required to hand out IP address for the Switch.
    - At the time of site creation on the cloud portal, a default wired network is created
  - Step 2: Instant On AP Onboarding
    - We recommend AP15 (a 4x4 AP) to provide the wide coverage needed in an open space such as a coffee shop
    - When creating a new wireless network on the cloud portal to onboard the AP, by default the network will be assigned to the wired management network or a new wired management network will be created if one has not been created.
    - Add another AP15 to the switch and place optimally (see section on AP placement) to ensure coverage for the coffee shop
  - Step 3: Extend the network
    - Add an outdoor AP (AP17) to extend the coverage to outdoor spaces such as a patio using a wired connection to the switch
- **Recommended Feature Set**

Instant On Feature/Offerings	Benefits
Separate networks for different users	Separate network for Employees and Guests to keep traffic isolated

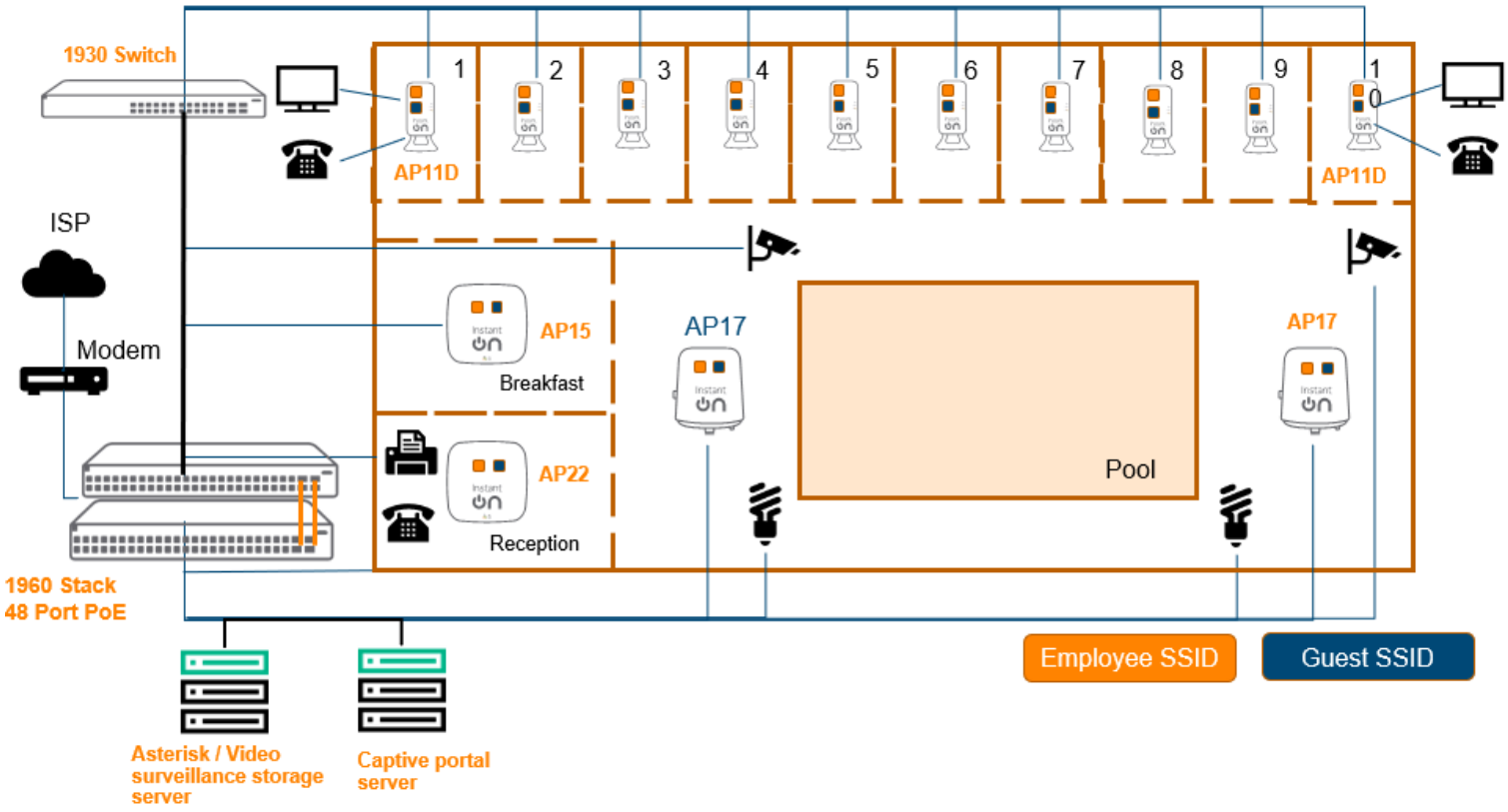
Two Factor Authentication	To Factor Authentication can be enabled for employees for privileged access
WPA3	Enhanced Wi-Fi security for Employee as well as Guests. WPA3 Enterprise for Employee network and WPA3 Personal for Guest network
Client Blocking	To protect the network from a malicious user/client
External Captive Portal	Get advanced analytics and improve marketing capabilities and customer loyalty by partnering with an External Captive Portal
PoE Scheduling	Automatically turn off PoE controlled APs after business hours and automatically turn on PoE cameras during nights

USE CASE #3: Boutique hotels or Bed and Breakfast

- **Customer Requirements**
  - Easy to manage Wi-Fi solution for the reception, breakfast area (high density), ten rooms and pool (outdoor)
  - Each room needs to have a wired desk phone, an IPTV and an optional wired port for further expansion
  - Secured Wi-Fi access with separate networks for employees and guests
  - The network should be able to scale with business growth and provide redundancy with no impact to day to day business.
  - Connectivity for phones, cameras, printers and IoT devices such as door locks and PoE lighting for pool areas
  - Ability to connect storage severs for surveliance recordings, voice server for telephony and captive portal servers for guest login.
  - Isolation of clients connected to the guest network to prevent direct inter-client communication
  - Client Density: 75 – 100 active client devices at a time (indoors and outdoors)

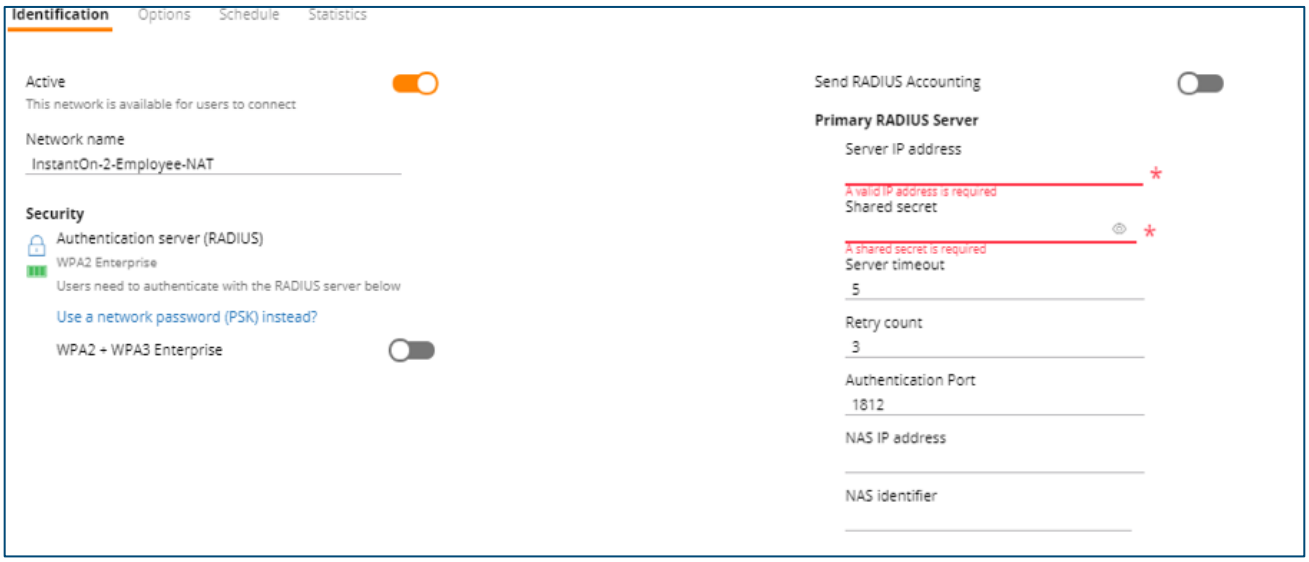
- **Hardware Guidelines**
  - Total of 14 APs – 10 units of AP11D (2x2:2 with Desk mount) – one for each room, 1 unit of AP15 (4x4:4) for the breakfast area, 1 unit of AP22 (2x2:2 Wi-Fi 6) for the reception and 2 units of AP17 (2x2:2) for outdoor use
  - Total 3 Instant On Switches – 1930 48G 4SFP/SFP+ Class4 PoE 370W and two units of 1960 24 and 48 port PoE switches with 600W of PoE to support APs and other wired devices such as printers, door locks and IoT lighting devices

- **Topology**

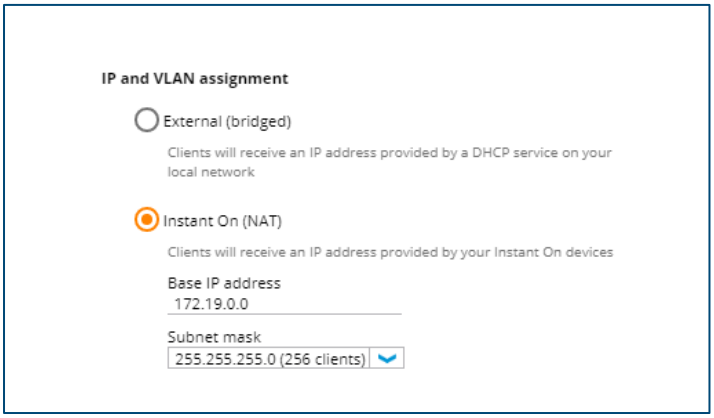


- **Configuration Guidelines**
  - Step 1: Instant On Switch Onboarding and Site Creation
    - We recommend both 1960 as well as 1930 for this deployment. A two-switch 1960 stack should be able to meet the needs of local server needs such as captive portal server or storage for video surveillance and also provide enough PoE power to keep IoT lights in the pool area. Depending on the density, we also recommend a 1960 stack of PoE SKUs for this deployment to handle the additional PoE devices as the business grows. The uplink 10G ports can be used for connecting VoIP server, surveilenace storage server, streaming devices and captive portal server for guest logins.
    - Also recommend another 1930 switch 24G which can act as a access SKU powering further PoE devices and APs for further business expansion.
    - Connect the Instant On Switch 1960 switch stack to the ISP modem
    - ISP should provide the management IP address to Instant On switch. If ISP only offers a single IP address, then DHCP server functionality on the 1960 can be turned on to distribute IP addresses for the deployment.
    - At the time of site creation on the cloud portal, a default wired network is created which can be customized as per the needs of the deployment.
  - Step 2: Instant On AP Onboarding
    - We recommend AP11D (2x2 Desk mount AP) to provide the additional wired connections needed in the reception area including wired printers and desk phone

- When creating a new wireless network on the cloud portal to onboard the AP, by default the network will be assigned to the wired management network
- The first wireless network will always be an employee network. Create three networks with different network quality and control to separate high-priority employees (IT team) from other employees and guests. For this deployment, select Authentication server (RADIUS) for first employee network, add server IP, and shared secret for the same. Select WPA3 personal for the second employee network and the guest network.
- The first Instant On AP will act as a DHCP, NAT server for wireless clients.



- IP and VLAN assignment: Select Instant On (NAT) option for guest network so that clients will receive an IP address provided by the Instant On AP.



- Step 3: Guest Network Creation
  - Since the first network has been created, now we can create the second employee network and the guest network.

- Client isolation is enabled by default for guest network. That means clients connected to the guest network are isolated from reaching other clients directly over the WLAN. Note that any network resources for e.g., printers connected to guest network are not reachable directly by the guests.

- Step 4: Extend the network
  - To the AP11D via a wired connection, we recommend adding a AP22 (2x2 Wi-Fi 6) in the lobby area where there can be high wireless client density (to handle incoming visitors)
  - All AP11D AP in the rooms need to be connected directly to the 1930 switch via a wired connection. The desk phone and the IPTV in the rooms can use the wired ports on the AP11D present in each room
  - Add couple of outdoor APs (AP17) to extend the Wi-Fi coverage to the pool area by connecting them to the switch
  - Regardless of where a user goes, all wireless networks will be available and provide seamless transition across locations in the hotel

- **Recommended Feature Set**

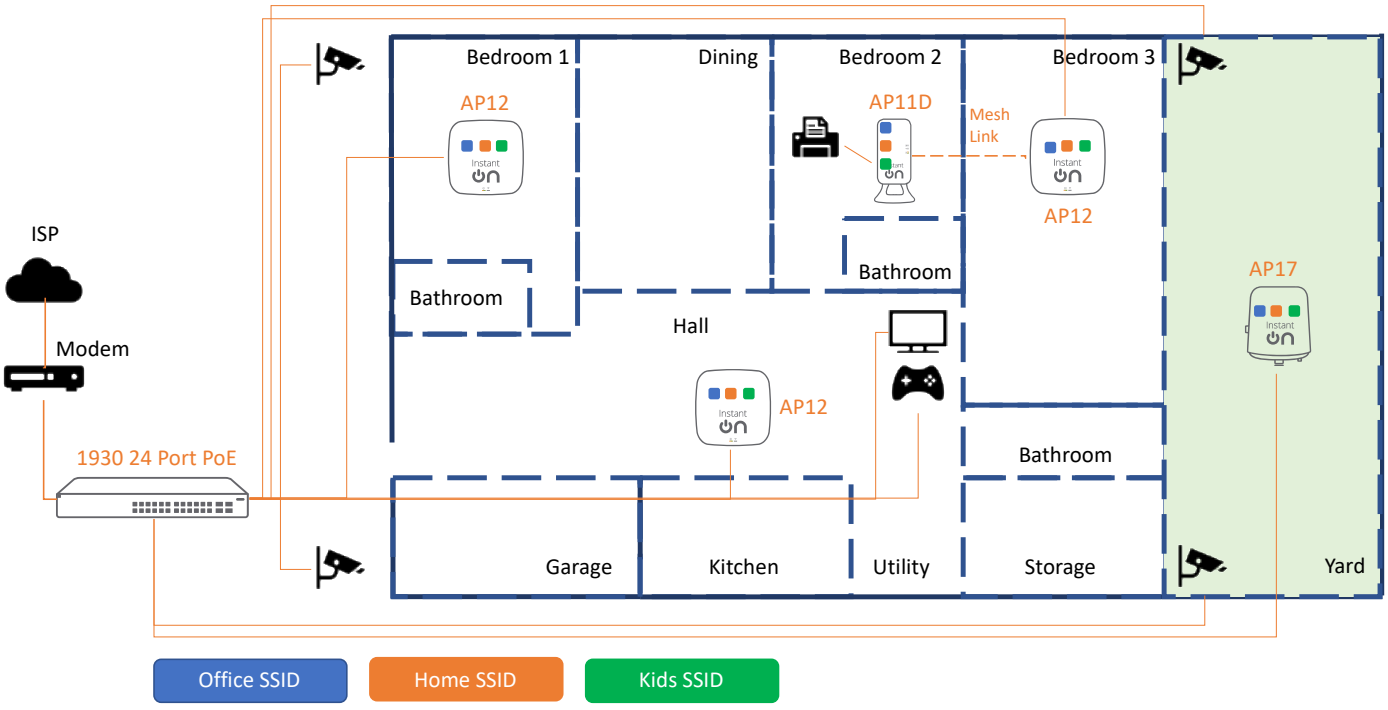
Instant On Feature/Offerings	Benefits
Separate networks for different users	Separate network for Employees and Guests to keep traffic isolated
Two Factor Authentication	Two Factor Authentication can be enabled for employees for privileged access
WPA3	Enhanced Wi-Fi security for Employee as well as Guests. WPA3 Enterprise for Employee network and WPA3 Personal for Guest network
External RADIUS Server	Simplify authentication setup for users on the Employee network using an external RADIUS server
Client Blocking	To protect the network from a malicious user/client
External Captive Portal	Get advanced analytics and improve marketing capabilities and customer loyalty by partnering with an External Captive Portal
Editable Client Name	Easily identify devices important to you such as IoT devices (pool light, lobby camera, etc.)
IP Reservation	Reserve static IPs in your network for legacy and IoT devices that always expect to operate with a specific IP address
LED Quiet Mode	For in-room APs where the LEDs can be turned off to blend in with the rest of the room
PoE Scheduling	Automatically turn on and off PoE controlled lighting and other IoT devices based on a set schedule for areas in the hotel

USE CASE #4: Work from Home

- **Customer Requirements**
  - Reliable and secure Wi-Fi solution, for running a business from home
  - Separate network for business, home and children's' use with different QoS and bandwidth settings
  - Ability to support streaming, audio video content
  - Parental control, ability to block web content as well as restricting duration of network access
  - Minimal configuration, hardware and setup needed
  - Extend the network to an outdoor area (yard)
  - Mesh networking needed in hard-to-wire location with option to have a wired printer from the meshed AP
  - Connectivity for cameras, TV and gaming devices
  - If AP is planned to be directly connected without a switch, should support tagging of uplink VLAN based on ISP requirement.
  - Client Density: 10 – 30 active client devices at a time (indoors and outdoors)

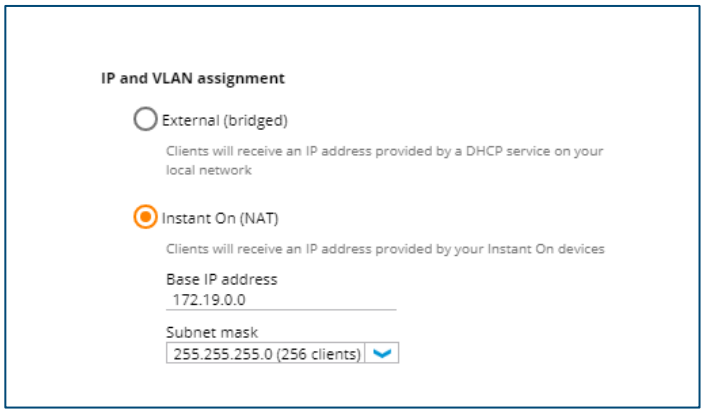
- **Hardware Guidelines**
  - Total of 5 APs – 3 units of AP12 (3x3:3) for the bedrooms as well as the open area (Hall), 1 unit of AP11D (2x2:2 with Desk mount) for the hard-to-wire location and 1 unit of AP17 (2x2:2) for outdoor use
  - Total 1 Instant On Switch – 1930 24G 4SFP/SFP+ Class 4 PoE 370W to support APs and other wired devices such as cameras, TVs and gaming devices

- **Topology**



- **Configuration Guidelines**
  - Step 1: Instant On Switch Onboarding and Site Creation
    - We recommend a 1930 24-port PoE switch for this deployment to handle a number of wired connections to cameras, APs, TV and gaming devices across the home
    - Connect the Instant On Switch to the ISP modem
    - ISP should provide the management IP address to Instant On Switch. If ISP only offers a single IP address, then an external gateway or router is required to hand out IP address for the Switch.
    - At the time of site creation on the cloud portal, a default wired network is created

  - Step 2: Instant On AP Onboarding
    - We recommend AP12 (3x3:3) for running your business from home while also hosting the home and children's' SSID on the same wireless network
    - When creating a new wireless network, by default the network will be assigned to the wired management network or a new wired management network will be created if one has not been created.
    - The first Instant On AP will act as a DHCP, NAT server for wireless clients



  - Step 3: Home and Kids Network Creation
    - Since the first network has been created, now we can create the second network for Home users and Kids network for children
    - Client isolation is enabled by default for the two new networks. That means clients connected to the home network are isolated from reaching other clients directly over the WLAN. Note that any network resources for e.g., printers connected to home network are not reachable directly.
    - Set per-network bandwidth limits for the Home network to prevent unlimited usage from consuming a large portion of the bandwidth
    - Do the same for the Kids network and also use the Time of Day SSID feature to make the network available only at specific times of the day.
    - On the Kids network, additional restrictions to visiting sites can be achieved by using the Application Blocking feature and turning off access to unwanted categories of traffic

  - Step 4: Extend the network
    - Add the two other AP12 access points and the three networks will also be made available to those APs

- Set up Mesh networking for the hard-to-wire room with AP11D and use the downlink port to connect legacy wired devices such as printers. AP11D allows wired devices in remote corners of the house get a wired connection through a Mesh link to the nearest AP
- For outdoor use (yard), add an outdoor AP (AP17) and have it wired to the switch
- Now the same set of access points will be serving 3 different SSIDs regardless of where the user may be located

- **Recommended Feature Set**

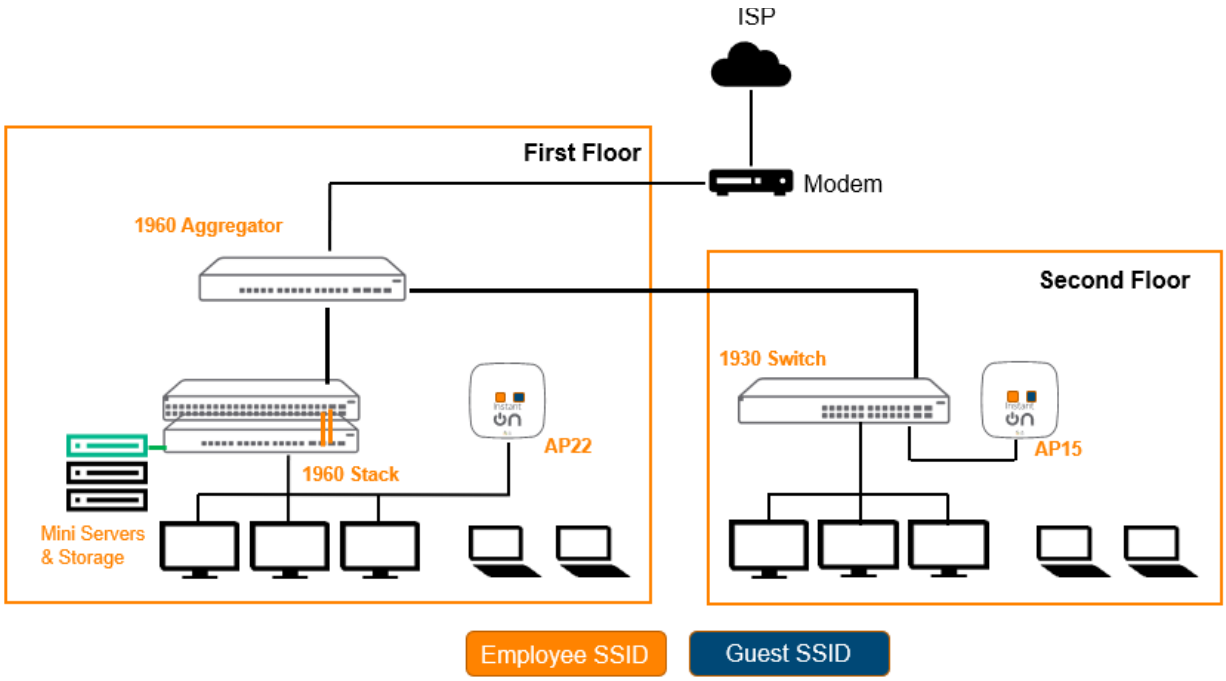
Instant On Feature/Offerings	Benefits
Separate networks for different users	Separate network for Office, Home and Kids usage to ensure bandwidth availability and to keep traffic isolated
WPA3	Enhanced Wi-Fi security for Office, Home and Kids network. WPA3 Enterprise for Office network and WPA3 Personal for Home and Kids network
Block unsolicited traffic	Aruba Instant On APs come with a built-in firewall that can block any unwanted or unsolicited traffic coming in from the Internet to keep malicious hackers at bay
Block undesired traffic categories	Aruba Instant On APs have a built-in deep packet inspection (DPI) engine and firewall to offer you visibility into the different application and website categories that users on each of the networks are accessing. You also have the ability to block one or more traffic types. This can be used by parents to block age-restricted content for the home network.
Editable Client Name	Easily identify devices important to you such as IoT devices (pool light, lobby camera, etc.)
LED Quiet Mode	For in-room APs where the LEDs can be turned off to blend in with the rest of the room
QoS	Instant On has enabled this feature in the background to automatically prioritization for voice/video traffic (enabled by default)
Dynamic RF Optimization	Instant On has enabled this feature in the background to dynamically change the operating channel and adjust Tx power in case of co-channel interference (enabled by default)
Time of the Day SSID	Controls Wi-Fi usage outside of configured time. Very handy feature to reduce screen time for children
Smart Mesh	Aruba Instant On APs offer One click mesh easy way extend the Wi-Fi coverage at hard to wire areas and ensure better coverage. For e.g., patios and multiple floors and larger rooms.

Nord VPN Partnership	256-bit AES encryption, no tracking of visited sites, and high throughput for streaming Discounted pricing when ordered via the Instant On app
Uplink VLAN tagging	APs acting in router mode as first device connecting to the ISP modem, can be configured to use an Uplink VLAN based on ISP requirements.

USE CASE #5: Small Startups

- **Customer Requirements**
  - Need for a low budget network solution which is simple to deploy and easy to manage with limited IT expertise.
  - Connectivity for high end application servers and power number of PoE devices like wired desk phone, IP cams, Access points etc,
  - Ability for network to scale to adapt business growth without much restructuring or additional expenses
  - Secured and reliable fast Wi-Fi networks for employees and guests to support bandwidth-heavy applications.
  - Isolation of clients, connected to corporate network and guest Wi-Fi
  - Easy Management and remote administration, monitoring of the network.
  - Client density: 100 – 150 clients at a given peak business hours

- **Hardware Guidelines**
  - Mix of 1960 switches Aggregator and Access –
    - Aggregator switch which acts as a first switch connecting to ISP on uplink and dowlink connects with other access switches and servers, and storage devices.
    - Access switch to support Class 6 / 4 PoE devices like APs, surveillance cameras and other wired devices like desktops.
  - Mix of Wireless Access points supporting Wi-Fi 5 AP15 (4x4:4) for better coverage in reception and conference rooms & Wi-Fi 6 AP22 (2x2:2) for better performance to provide secure Wi-Fi to employees and guest for office work area.
- **Topology**

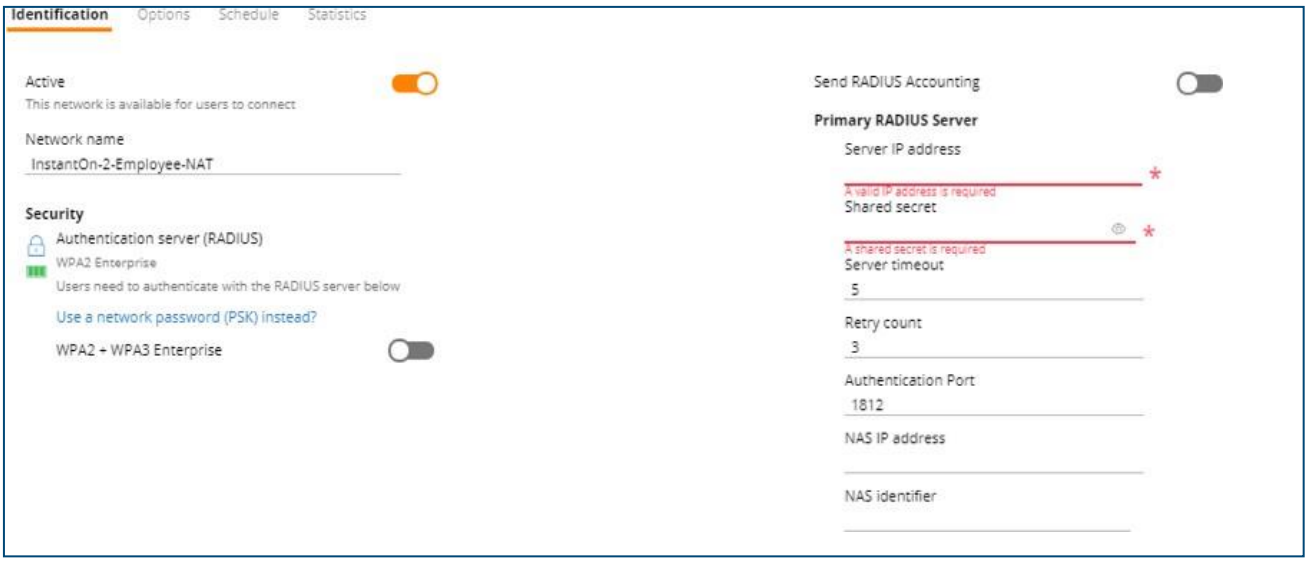


- **Configuration Guidelines**
  - Step 1: Instant On Switch Onboarding and Site Creation
    - Recommend the 12-port aggregator model which can help connect servers with high speed 10G connections and serve as an uplink to the access models
    - Access model switches can be used to serve individual cabins and power up the Access points, IP cameras on the network
    - Recommend PoE model which reduces the installation cost by avoiding an extra line and ability to do better PoE management.
    - Connect the Instant On 12-port Aggregator Switch to the ISP modem.
    - ISP should provide the management IP address to Instant On Switch. If ISP only offers a single IP address, then the DHCP server on the 1960 can be turned to provide IP address to the local networks.
    - At the time of site creation on the cloud portal, a default wired network is created following whichr equired VLANs and SSIDs can be configured as per the need.

  - Step 2: Instant On AP Onboarding
    - We recommend Wi-Fi 6 AP 22 (a 2x2 AP) for greater performance to the clients and AP15 (a 4x4 AP) to provide the wide coverage needed on the floors or training halls
    - When creating a new wireless network on the cloud portal to onboard the AP, by default the network will be assigned to the wired management network or a new wired management network will be created if onehas not been created.
    - Instant On APs will act as a DHCP, NAT server for wireless clients or can be allowed to get local IP from DHCP server configured on the network.

  - Step 3: Employee and Guest Network Creation

- The first wireless network will always be an employee network. Create SSIDs and select based on need either employee or guest SSID so that guest users can have access only to Internet. Client isolation is enabled by default which means traffic between employees and guests are separated. For this deployment, select Authentication server (RADIUS) for first employee SSID, add server IP, and shared secret for the same so the employees can be authenticated using dot1x authentication and select WPA3 personal for the guest network.
- Client isolation is enabled by default for the two new networks. That means clients connected to the guest network are isolated from reaching other clients directly over the WLAN. Note that any network resources for e.g., printers connected to employee network are not reachable directly.
- Set per-network bandwidth limits for the guest network to prevent unlimited usage from consuming a large portion of the bandwidth.
- Do enable Time of the Day feature for guest network to make the network available only at specific times of the day for ex. business hours
- On the employee network, additional restrictions to visiting sites can be achieved by using the Application Blocking feature and turning off access to unwanted categories of traffic affecting productivity.
- To ensue Wi-fi coverage newer APs can be placed appropriate extending the Wi-Fi coverage as these support Mesh and avoid any Wi-Fi dead spots.



- **Recommended Feature Set**

Instant On Feature/Offerings	Benefits
Mix of Fibre & copper 10G ports	Instant On 1960 switch supports 10G fiber / copper uplinks, support heavy bandwidth application and access models support more wired devices
Options to scale based on growth	With support for stacking provides flexibility to scale by adding member switches as the

	business grows.
Support for High Availability with no business downtime	Enabling stacking helps in handling extreme scenarios such as switch or link failure, Backup unit takes over for the role of conductor creating a reliable network.Conductor and keeps both L2 and L3 services running.
Hybrid Stacking	Allows mix of access and aggregator model SKUs to form a stack.
Separate networks for different users	Separate network for employees and guests to keep traffic isolated and secured.
Support to power more PoE devices	Total power budget of 600W for 48p and 370W for 24p more number of PoE devices can be powered
Class6 PoE devices	Supports powering of Class6 60W PD devices in addition to the Class4 30W devices and also support legacy 15.4W Class3 devices.
Secure Wi-Fi	Enhanced Wi-Fi security for employee as well as guests. WPA3 Enterprise for employee network and WPA3 Personal for guest network
QoS and AVC support	Supports ACL & CoS, shows drill down view of top applications used & one click to block them
Remote Management	Supports both local management using Web GUI and cloud Management using web portal or mobile APP. With cloud management, monitor sites from anywhere and receive alerts when devices are offline.
PoE Configuration & scheduling	Automatically turn off PoE controlled APs after business hours and automatically turn on PoE cameras during nights with easy config options
Support for External authentication server	Supports external RADIUS to be configured as authentication server for employee SSID to authenticate employees to gain access to WIFI
Ability to block access to specific users	Supports both IP and Mac based Access control lists to authorize users to specific resources while blocking off others.

USE CASE #6: Health Care

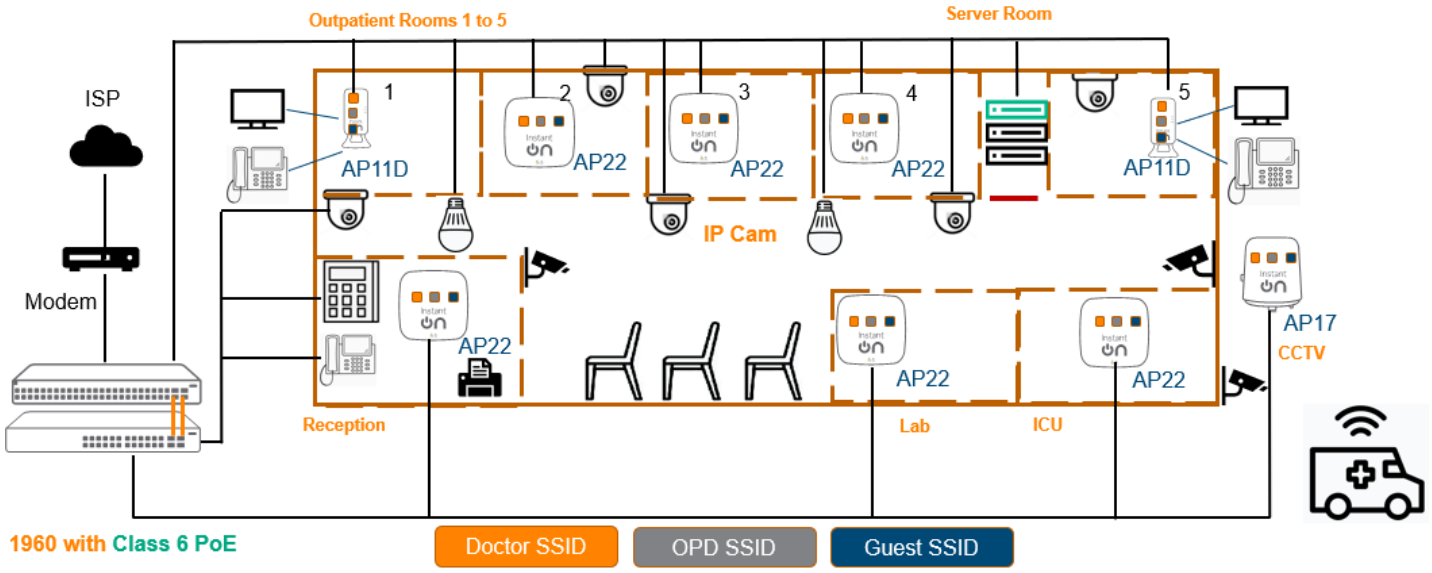
- **Customer Requirements**
  - Need a stable and reliable network which support high bandwidth applications (image scanning) and high availability infrastructure.
  - Better communication means better care. Faster and secure network communication with doctors access patients medical reports as quick as possible improving patients health.
  - Need PoE switches to power devices like IP cameras, VoIP phones, medical equipment, PoE

controlled lighting and reduce installation costs.

- Confidentiality of patient records and the need for a high level of security.
- Provide guest access Wi-Fi networks for guests, visitors, patients
- Support Separation of traffic for Admins, Doctors, Patients and Guests with different QoS and bandwidth settings.
- 10G Connectivity for medical servers, wired devices including printer, desk phone, medial equipment's etc.
- Ability to analyze network issues with enhanced troubleshooting capabilities to quickly pinpoint network outages.

- **Hardware Guidelines**
  - Total of two 1960 Switches PoE Switches 48 /24 Port which has total power budget of 600W and 370W respectively, which helps to power a greater number of PoE devices like Access points, IP Cameras, Lights,Biometric devices, VoIP phones.
  - APs – 6 units of AP22 Wi-Fi 6 (2x2:2) for the common area, lab, ICU & doctor rooms, and 2 units of AP11D Wi-Fi 5 (2x2:2, Desk Mount) for doctors room supporting wired devices like old desktops, printers etc. and 1 unit of AP17 Wi-Fi5 (2x2:2) for Outdoor use.

- **Topology**



- **Configuration Tips**
  - Step 1: Instant On Switch Onboarding and Site Creation
    - The second 1960 switch can be stacked together with the first for meeting the needs of the growing network and for simpler management.Note : recommend calculating total PoE power budget and plan to pick the correct PoE SKU as part of network design. This deployment saves costs as it reduces the need for separate electrical power lines and provides flexibility for device installation such that the PD can be installed anywhere without theneed for AC/ DC power inputs.
    - Connect the Instant On Switch to the ISP modem.

- ISP should provide the management IP address to Instant On Switch after which we can enable DHCP services on 1960 switches to provide local IP address to the local clients like Servers, Wired Desktops, access points, IP phones, IP cameras, printers, medical devices etc.
- At the time of site creation on the cloud portal, a default wired network is created, which can be customized as per the needs i.e. create multiple wired interfaces for different networks and map switch ports accordingly and enable traffic isolation as needed.

- Step 2: Instant On AP Onboarding
  - We recommend AP22 (a Wi-Fi 6 2x2:2 AP) which provides better performance and support high-dense client environments and also provide the wide coverage needed in an open space.
  - When creating a new wireless network on the cloud portal to onboard the AP, by default the network will be assigned to the wired management network or a new wired management network will be created if one has not been created. Later which can be customized as per the need by creating new wireless networks like and map wireless networks to the respective wired networks so that clients receive IP address based on the wired network VLAN mappings.
  - Configure AP11D wired ports with respective VLANs which can help in connecting desk phones and wired printers in Doctors room and onboard AP17 for outdoor Wi-Fi access.
  - If needed, we can extend Wi-Fi network by connecting wireless APs through Mesh networks to ensure coverage and avoid dead spots.

- Step 3: Doctor, Patient, Guest Network Creation
  - Since the first network is created as employee, modify the networks as per this deployment need by creating different wired and wireless networks for Doctor, Patient and Guest networks.
  - Isolation of clients is enabled by defauly and clients connected to the guest network is prevented for any inter-client communication and allowed only to access internet.
  - Configure switchports and AP11D downlink ports as per the VLAN needs and a enable AP17 for outdoor access

- **Recommended Feature Set**

Instant On Feature / Offerings	Benefits
Simple and reliable network	Easy to setup the network and with stacking feature high availability can be achieved for any unexpected failures.
Connectivity for storage servers	Support for fibre and copper ports help connect servers, storage devices.
Separate networks for different users	Separate network for Admins, Doctors, Patients, Guests to keep network isolated.
Support for Stacking	Simplifies management of multiple switches as one single logical device and help build resilient networks to have an Always On Network.
Cloud Managed stacking	Easy bring of stack, easy stack management and ability to remotely monitor stack using cloud portal.

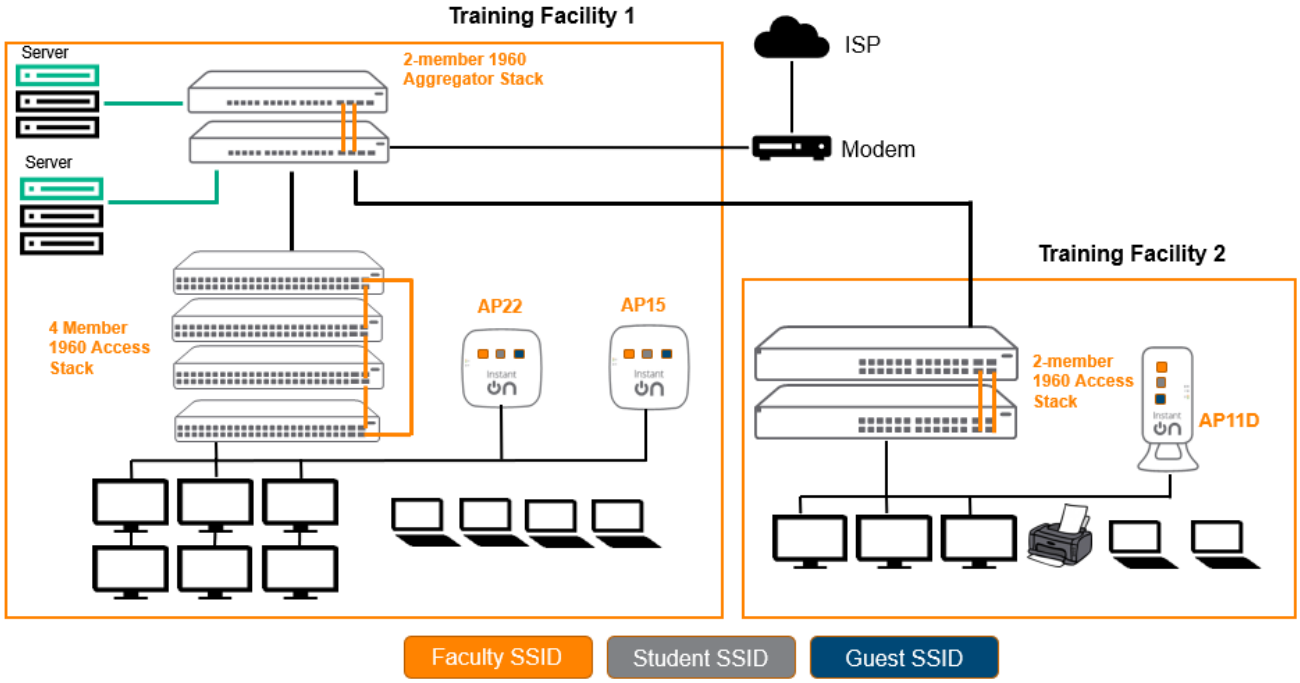
Class6 / Class4 PoE Support	Ability to power more PoE devices with IEEE 802.3bt, at, af support also allow remote reboot of PoE devices incase of any issues
PoE Configuration and Statistics	Allows configuration of PoE priority, Class of support and provide status of total / actual power consumption for individual ports
Secure and stable Wi-Fi with guest access support	WPA3 secuirty helps create secure Wi-Fi networks along with guest network support.
SSID to VLAN mapping	Ability to do mapping of SSID to specific VLANs allowing wireless clients to be on the network.
Dynamic RF Optimization	Instant On has enabled this feature in the background to dynamically change the operatingchannel and adjust Tx power in case of co- channel interference (enabled by default)
Extend Wi-Fi network	Support for Mesh allows Wi-Fi coverage to be extended and allows provide better RF optimization.
Internal Captive Portal	Customize your Guest logon portal with the logoand name of your hospital or clinic
DHCP Server	Supports internal DHCP sever which reduces the need for another device to provide local IP address to clients.
Analyse network issues faster	Supports logging features like RMON, SNMP and latest event log features to know the latest updates. Also provides port mirroring option to trouble shoot issues.

USE CASE #7: Training Facility

- **Customer Requirements**
  - Need for an easy deployable IT solution with less IT knowledge / experience considering budget needs and remote monitoring possible to manage networks remotely.
  - Reliable wired connection for students connecting remotely to access training servers and secure Wi-Fi solution, for students to stay connected inside the facility.
  - Separate network for Faculty, student, guest with different QoS and bandwidth settings.
  - Ability to support heavy bandwidth application for online streaming which class recording with audio video content
  - Ability to block web content as well as restricting duration of network access.
  - Mesh networking needed in hard-to-wire location from the meshed AP and also eliminate Wi-Fi dead spots.
  - Connectivity for CCTV cameras with PoE support reducing substantially in installation costs.
  - Client Density: 40-60 active client per AP during class hours.

- **Hardware Guidelines**
  - Total of 3 APs – 1 unit of AP22 & AP15 to support classrooms, open area (reception), 1 unit ofAP11D (2x2:2 with Desk mount) with mesh support for the hard-to-wire location and support wired printers, legacy desktops.
  - Propose mix of 1960 Instant On Switch like 12-port aggregator SKU to connect SMB servers / storage devices and other access switches. Access switches to support high number of wired devices like desktops PCs, student lab devices, connect wireless APs and other wired devices such as IP cameras,TVs etc. Enabling stacking causes multiple switches to act as a single logical device for easy management and scalability to extend as facility grows.

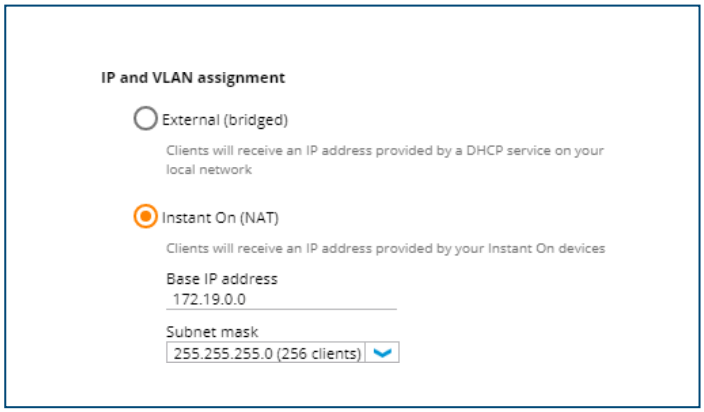
- **Topology**



- **Configuration Guidelines**
  - Step 1: Instant On Switch Onboarding and Site Creation
    - We recommend a 1960 12 port aggregator for 10G connectivity to servers and act as an uplink switch to other access 1960 models.
    - Recommend picking 48-port switch with more port capacity which will help connect more wired clients / media servers.
    - Also, PoE model is recommended for this deployment to handle more PoE devices including AP's, IP surveillance cams etc. which reduces the installation costs
    - recommend stackable switches so management of switches are easier and providehigh availability in case of a link or switch failure with no or less traffic disruption on the network.
    - Connect the Instant On Switch to the ISP modem
    - ISP should provide the management IP address to Instant On Switch. If ISP only offers a single IP address, then an external gateway or router is required to hand out IP address for the Switch. Additionally, local DHCP feature can be turned on 1960 for local devices to get an IP address.

- At the time of site creation on the cloud portal, a default wired network is created which can be customized and mapped to networks as per the site needs.
- Enable IGMP as part of the configs for multicast delivery which will help stream content to group of users on the network.

- Step 2: Instant On AP Onboarding
  - We recommend mix of APs AP22 which is Wi-Fi 6 capable AP to higher data rates and more clients suitable for open area auditoriums & AP 15 for classrooms.
  - When creating a new wireless network, by default the network will be assigned to the wired management network which can later can be mapped to networks as per the need like different SSIDs like Faculty, student, guest with different VLANs.
  - The Instant On AP can also act as a DHCP, NAT server for wireless clients and support guest SSID configurations for guests



- Step 3: Tuning Wireless Configurations.
  - Since the first network has been created, now we can create the other networks for student and guest Wi-Finetworks. Now the same set of access points will be serving 3 different SSIDs regardless of where the user may be located.
  - Client isolation is enabled by default for the two new networks. That means clients connected to the teacher network are isolated from reaching other clients directly over the WLAN. Note that any networkresources for e.g., printers connected to teacher network are not reachable directly, however can be enabled based on the needs.
  - Set per-network bandwidth limits for the student network to prevent unlimited usage from consuming alarge portion of the bandwidth.
  - Do enable Time of Day SSID feature to make the network available only at specific times of the day for example class house and also PoE scheduling such that APs can be turned off over the weekend whenthere is no activities in the facility.
  - On the student's network, additional restrictions to visiting sites can be achieved by using the Application
  - Blocking feature and turning off access to unwanted categories of traffic
  - Set up Mesh networking for the hard-to-wire room with AP11D and use the downlink port to connect legacy wired devices such as printers. AP11D allows wired devices in remote corners of the facility toavoid Wi-Fi dead spots and also get a wired connection through a Mesh link to the nearest AP.

- **Recommended Feature Set**

Instant On Feature/Offerings	Benefits
10G Uplink / downlink	Provides support for both Fibre / copper 10G uplinks which helps server connectivity and connecting access switches.
Separate networks for different users	Separate network for Faculty, students , guestsand restrict bandwidth availability and to keep traffic isolated
Stacking	For easier management of switches and to provide a resilient infrastructure even during link and switch failures.
PoE Scheduling	Automatically turn on and off PoE controlled based on a set of schedule like weekends.
QoS	Instant On has enabled this feature in the background to automatically prioritization for voice/video traffic (enabled by default)
Block unsolicited traffic	Aruba Instant On APs come with a built-in firewall that can block any unwanted or unsolicited traffic coming in from the Internet to keep malicious hackers at bay
Block undesired traffic categories	Aruba Instant On APs have a built-in deep packet inspection (DPI) engine and firewall to offer you visibility into the different application and website categories that users on each of the networks are accessing. You also have the ability to block one or more traffic types. This can be used by parents to block age-restricted content for the home network.
WPA3	Enhanced Wi-Fi security for all wireless networks. WPA3 Enterprise / personal supported
Dynamic RF Optimization	Instant On has enabled this feature in the background to dynamically change the operating channel and adjust Tx power in case of co-channel interference (enabled by default)
Time of the Day SSID	Allows scheduling of Wi-Fi SSID broadcast i.e. during no class days Wi-Fi can be disabled
Smart Mesh	Aruba Instant On APs offer One click mesh easy way extend the Wi-Fi coverage at hard to wire areas and ensure better coverage. For e.g., patiosand multiple floors and larger rooms.

SUMMARY

Aruba Instant On access points and switches are designed with small businesses in mind. It is a simple, secure, and reliable solution that small businesses deserve. Instant On APs come with two years of hardware warranty and Instant On Switches limited lifetime warranty respectively. Instant On APs and Switches offer 24x7 phone support

for 90 days, 24x7 chat support (one year for APs and limited lifetime for Switches) and an active online community to take care of any product questions or concerns. Click here to learn more about Aruba Instant On devices.

To keep you worry free, Aruba offers optional Foundation Care support services for Aruba Instant On. Adding Foundation Care support is simple and extends the warranty and support to a period of 3 or 5 years. Add Foundation Care with new Instant On purchases within 90 days of original purchase to obtain these benefits.

- Three years of Next Business Day advanced replacement of defective network equipment and parts – so your network can stay up and functioning as expected.
- 24x7 telephone support access to our Aruba experts – delivered by the Aruba Technical Assistance Center (TAC).
- Three years of software support along with advice from our Aruba experts on any questions or concerns.
- Three years of chat support provided through our Aruba Instant On community.

Speak to your Aruba authorized business partner today about adding Foundation Care support services for Aruba Instant On Access Points and Switches.