The Indestructible Network: Wireless LANs for Industrial and Outdoor Applications

Aruba White Paper
# Table of Contents

**Industrial and outdoor environments** 3  
- State-of-the-art in Enterprise Wi-Fi 3  
- Additional features for outdoor and industrial networks 5  
- Requirements for the industrial access point 6  
- Mounting options 10  
- Antenna options 11  
- Powering the industrial access point 14  
- Antenna alignment 18  
- Applications for the Industrial Enterprise AP 18  
- Point to point communications networks 19  

**Conclusion** 23  

**About Aruba Networks, Inc.** 24  

**Appendix: Brief specifications for some outdoor access points and antennas** 25
Industrial and outdoor environments

Many organizations require data and voice communications in industrial and outdoor environments. Historically these needs have been met by a patchwork of copper or fiber-optic cable in the ground, low-bandwidth 900 MHz and 2.4 GHz wireless links, and depending on the particular site, satellite networks too. While wire-line networks can support high data rates with high reliability, it is not always feasible or cost-effective to dig trenches or string overhead wire across chemical plants, container ports or off-shore oil platforms. Manufacturing plants and storage facilities with explosive atmospheres and ignition hazards have specialized installation requirements, raising the installation cost and complexity of wired networks. Consequently many deployments utilize both wired and wireless technologies, often combining licensed and unlicensed spectrum across a number of different frequencies.

Until recently this hybrid patchwork of communication technologies was the best achievable solution, particularly for mobile, data-intensive clients such as rugged handheld terminals and vehicle-mounted terminals. Still, the final results fall short of both IT requirements and user expectations. Wireless signal quality and available bandwidth is often highly variable across an industrial or outdoor site, resulting in user complaints. For the IT group, fault management and performance monitoring can be especially difficult; the lack of homogeneous monitoring and management for the diverse wireless links results in disparate alarm and reporting consoles. Indeed, many organizations find they must support separate, overlaid communication networks, each with its own infrastructure, resulting in duplicate management systems and IT effort. Worse yet, overlaid networks using legacy and new equipment on the same frequencies can result in unintentional interference.

Many communication services in industrial and outdoor environments require low bandwidth: telemetry and SCADA applications generate only a few kbps on average, easily within the range of any wireless technology today. Many organizations now need to support new applications for remote workers, such as data or Internet connections for ruggedized PC terminals, and even voice services in areas that are remote from cellphone coverage. These require considerably more bandwidth than SCADA. Finally, many applications such as power generation, water treatment and chemical plants intend to add real-time wireless video surveillance for security purposes, driving even higher data rates and predictable quality of service (QoS).

In recent years these new requirements on outdoor and industrial communications have increasingly stressed communications infrastructure designs. Meanwhile, a number of developments in Wi-Fi for enterprise customers have reached the stage where, with a small number of additional features, the technology is able to profoundly improve the outdoor experience and, in so doing, consolidate, simplify, and flatten the traditional patchwork and overlay of disparate communications networks.

State-of-the-art in Enterprise Wi-Fi

Many IT professionals in industrial enterprises will be familiar with the earlier generations of wireless products that provided the technology foundation for the original Institute of Electrical and Electronic Engineers (IEEE) 802.11 standard in the late 1990s. For the purposes of this paper, we distinguish between early 802.11 (Wi-Fi) networks consisting of many standalone access points (APs), and what is now termed ‘Enterprise Wi-Fi’ in which a centralized appliance controls hundreds or thousands of network-attached radios (‘thin’ access points) in a secure, reliable manner.

Enterprise Wi-Fi networking technology was pioneered by a number of small, startup companies advancing this new architecture, beginning around 2002. It grew out of the broader consumer market, where Wi-Fi rapidly became the accepted way to build home networks for Internet access, and from specialist vendors serving the warehouse and manufacturing markets, where wireless communications were often the only way to reach mobile workers and terminals.
Enterprise wireless LANs (WLANs) applied the same solutions for a broad range of indoor customers, including universities, retail stores, hospitals, hotels and carpeted office environments. Instead of searching for an Ethernet jack with which to connect to the LAN, users could avail themselves of Wi-Fi coverage. The low cost of Wi-Fi chips, and the widespread availability for interface cards and integral Wi-Fi in laptop PCs, aided the growth of enterprise WLANs to what is today a >$1 billion industry. While certain industries have been slower to adopt the new architecture, the IT workload associated with management, security and troubleshooting continues to extend the market for enterprise Wi-Fi equipment, replacing large networks of standalone or ‘fat’ access points across many industries.

In order for Wi-Fi to be accepted by enterprise IT groups, it had to be packaged and enhanced in a number of ways. The ‘thin’ access point architecture removed complexity from the edge of the network and introduced a central WLAN switch, or multi-service mobility controller, that manages large numbers of dependent access points. The multi-service mobility controller is responsible for managing and coordinating its dependent access points, and aggregates all Wi-Fi traffic, subjecting it to a firewall checks before connecting it to the Enterprise LAN.

Some of the advantages of the centralized enterprise WLAN architecture are presented below.

- **Identity-based security**
  Identity-based security applies rules to people and clients rather than to ports on the network, only permitting access appropriate to the specified role of the user as defined by a server such as RADIUS. Centralized WLANs support the full range of user authentication methods including the IEEE 802.1x framework that allows the use of PEAP, EAP-TLS, EAP-TTLS and LEAP, providing a state-of-the-art security regime only equaled by the most modern wired networks. Users can be authenticated against existing LDAP, RADIUS or Microsoft Active Directory servers, as well as a local database inside the multi-service mobility controller. Supported encryption methods include WEP, TKIP (WPA), AES (WPA2) and the L2 xSec encryption algorithm. Web-based authentication allows guest and clientless users to access the network secured with standard SSL.

  Unauthorized, user-installed ‘rogue’ APs are a continuing security threat to all enterprise and industrial WLANs. Centralized WLANs have many advanced features enabling detection, identification, location and suppression of rogue APs, both in the air and on the wired network. When a rogue is detected, alarms and logs alert the network manager.

- **Non-disruptive integration into existing networks**
  Centralized WLAN architectures allow a modular, phased introduction of mobility from pilot network to full-scale enterprise deployment, deploying on top of existing L2 and L3 LAN/WAN infrastructure. Access points are completely plug-and-play, requiring no manual configuration. They can be attached to any existing Ethernet switch or IP router and across any subnet boundary. Once connected, access points self-configure by automatically building a secure (GRE or IPSec) tunnel to the multi-service mobility controller. The controller automatically discovers and configures each AP based on the policies set by the administrator.

- **Secure convergence for mobile VoIP and video services**
  Centralized WLANs provide intelligent controls reliably and securely delivering voice, data and video services to fixed and mobile clients with PCs, dual-mode handsets, smartphones and video cameras. They support the end-to-end QoS required for multi-service applications, respecting relevant L2 and L3 QoS tags. Other features for voice include call admissions control based on the number of active calls on an AP, and bandwidth control to limit the amount of bandwidth lower priority devices can use. As users move from AP to AP, their security and session state is maintained in the multi-service mobility controller, assuring seamless handover without exposing security loopholes.
• **Adaptive radio management to automatically optimize performance**
  Unified Wi-Fi networks offer adaptive control of the air, automatically tuning the network of APs to respond to changing conditions in the RF environment and maintain optimal performance for users. The central multi-service mobility controller receives RF reports from its dependent access points and automatically configures, manages, and heals the network for optimum results, reducing the need for manual intervention and troubleshooting.

• **Remote access points for instant corporate hotspots**
  A ‘remote’ access point offers the same functionality as a standard access point, plus a stateful firewall, split-tunnel router, and the ability to register with a captive portal. A remote AP can be plugged in wherever a wired Ethernet jack connected to the Internet or corporate LAN is available. The remote AP establishes a secure IPSec tunnel – even through NAT routers – to the central multi-service mobility controller. It then brings up all the enterprise wireless services, including full encryption and authentication. A user’s end devices – such as notebook PCs, PDAs, or voice handsets – connect to the enterprise network through the remote AP exactly as if the user were in the enterprise facility using the wireless LAN.

• **Industrial-grade scalability, reliability and performance**
  The WLAN must be manageable in order to deliver scalable services. Network management systems allow administrators to centrally view, configure and manage all access points and multi-service mobility controllers, even those distributed at remote sites. Software upgrades and policies are configured centrally and propagated to all controllers and access points. Administrators at the central location can secure and control the RF environment, capture wireless traffic, and remotely troubleshoot problems anywhere in the wireless network. In turn, the WLAN management system can easily integrate with enterprise management systems such as HP Openview and CA Unicenter.

  Build-in redundancy mechanisms enable the highest uptimes and fast recovery in the event of unforeseen equipment or network outages.

  The centralized WLAN architecture is proven in many installations with >5000 access points and serving tens of thousands of users, including many who rely on Wi-Fi as their primary means of connection to the network.

**Additional features for outdoor and industrial networks**

In recent years, the ‘thin’ access point as used in centralized WLAN architectures has established itself as the preferred solution for indoor Wi-Fi coverage. It is fitting that the many innovations in management, security and reliability for indoor networks described above are now becoming available for the outdoor and industrial applications that gave birth to the wireless industry in the 1990s. These challenging environments have unique requirements for design, installation, and operation of individual hardware elements and the system as a whole.

The first requirement to be met is for an access point designed for harsh environments. While early needs for outdoor access points were met by using an environmental enclosure for an indoor-specification unit, the market has now advanced enough that vendors can offer self-contained, purpose-built equipment for outdoor and hazardous environments that meets all applicable certification requirements.

Secondly, a point-to-point, intermediate-distance capability is needed due to the long communication spans typical of many industrial and outdoor applications. Wi-Fi has been used for point-to-point and point-to-multipoint applications for some years, providing a good base of experience in designing and predicting link performance. Wi-Fi point-to-point links with appropriate antennas are in service over spans of >15 kilometers, supporting data rates in the tens of Mbps.
New developments, such as mesh technology for Wi-Fi, enable access point units to interconnect in a self-organizing, resilient multi-hop network backbone that can be leveraged to cover large and previously inaccessible areas.

A recent architectural breakthrough has combined the ‘thin access point’ with point-to-point wireless links. In this design a ruggedized outdoor radio unit can terminate a long-distance wireless link and simultaneously provide local area Wi-Fi coverage under a single management regime.

Outdoor design tools for the wireless network engineer are critical to any successful deployment. A number of such applications are now pre-integrated with GIS mapping systems, with field experience validating predicted coverage against the real-world performance of actual hardware.

Finally a complete line of off-the-shelf antennas, mounting systems and power solutions are necessary to provide the network architect with the tools required to tailor RF coverage to any site and environmental requirement.

Requirements for the industrial access point

Outdoor and harsh environments entail considerably wider temperature, particulate and humidity variation than would be experienced by an indoor unit. Additional requirements may apply for particular applications, such as explosive atmospheres or corrosive spray conditions. The following section lists standards that may be appropriate for different settings.

Temperature

Outdoor equipment is normally specified for a range of at least -20° to +55° C (-4° to +131° F). Depending on the actual environment, it may be necessary to extend this range at either or both extremes, and even then it may prove necessary in some environments to mount the unit with a sun shade or other external protection.

Very low temperature operation can only be assured by using an internal heater unit: this extends the lower end of the temperature range, but at the expense of a significant power draw, often in the range of 20 W when the heater is in operation.

Products that must operate over such a wide temperature range are typically built using electronic parts designed for the resulting stress and strain. One often sees a lag between the commercial introduction of a new technology and its availability in products for the industrial market, the new 802.11n high-speed Wi-Fi standard being a case in point.

Humidity

Standard humidity range for outdoor equipment is from 0% – 95% relative humidity (non-condensing). Some outdoor units also provide additional protection against high-temperature, condensing humidity conditions.
Dust & spray

The IP code-series is commonly used to specify the level of protection against dust and water ingress. IP codes are specified in an International Electrotechnical Commission standard, IEC EN60529, and use the form IP-XY, where X represents the level of protection against dry (solid) objects, and Y the protection against harmful ingress of water. Thus ‘IP-65’ specifies level 6 for dust and level 5 for water ingress. The following table includes some commonly specified IP options.

<table>
<thead>
<tr>
<th>IEC 60529 Levels of protection from dry (solid) objects</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IEC 60529 Levels of protection from dry (solid) objects</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
</tbody>
</table>

Another common specification for appropriate protection levels is the U.S. National Electrical Manufacturers’ Association (NEMA) standards publication 250-2003. NEMA provides a set of classification ‘Types’ that address similar requirements to the IP codes. However, NEMA Types go much further and include:

- Corrosion resistance
- Icing effects
- Oil resistance and gasket effects
- Enclosure construction including door/cover security
Therefore, while it is possible to specify a NEMA Type that meets the minimum requirements of a given IP code, it is not possible to specify an IP code that is equivalent to a NEMA Type.

<table>
<thead>
<tr>
<th>IP First Character</th>
<th>NEMA Enclosure Type</th>
<th>IP Second Character</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP0_</td>
<td></td>
<td>IP_0</td>
</tr>
<tr>
<td>IP1_</td>
<td></td>
<td>IP_1</td>
</tr>
<tr>
<td>IP2_</td>
<td></td>
<td>IP_2</td>
</tr>
<tr>
<td>IP3_</td>
<td></td>
<td>IP_3</td>
</tr>
<tr>
<td>IP4_</td>
<td></td>
<td>IP_4</td>
</tr>
<tr>
<td>IP5_</td>
<td></td>
<td>IP_5</td>
</tr>
<tr>
<td>IP6_</td>
<td></td>
<td>IP_6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IP_7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IP_8</td>
</tr>
</tbody>
</table>

A = A shaded block in the “A” column indicates that the NEMA Enclosure Type exceeds the requirements for the respective IEC 60529 IP First Character Designation. The IP First Character Designation is the protection against access to hazardous parts and solid foreign objects.

B = A shaded block in the “B” column indicates that the NEMA Enclosure Type exceeds the requirements for the respective IEC 60529 IP Second Character Designation. The IP Second Character Designation is the protection against the Ingress of water.

Conversion of NEMA Types and IEC 60259 environmental protection levels (from NEMA publication ‘A Brief Comparison of NEMA 250 & IEC 60259’)

Some commonly used NEMA Types include:

- **NEMA 4.** Type 4 enclosures are intended for indoor or outdoor use primarily to provide a degree of protection against windblown dust and rain, splashing water and hose-directed water, and to be undamaged by the formation of ice on the enclosure. They are not intended to provide protection against conditions such as internal condensation or internal icing.

- **NEMA 4X.** This adds corrosion protection to NEMA 4.

NEMA 4 and 4X are functionally equivalent to the IP-56 level of protection.

**Explosive atmospheres**

A surprisingly diverse range of industries must contend with and successfully manage potentially explosive atmospheres. Chemical manufacturers, refineries, fixed offshore platforms, mines and flour mills are just some of the facilities in this category. Many of these facilities gain significant productivity and other benefits from wireless systems that are designed to operate safely in these environments and avoid the spark-generating potential of wired networks.

The European ATEX standard is one of several dealing with equipment operating in potentially explosive atmospheres. Under ATEX, areas of a facility in which hazardous explosive atmospheres may occur must be classified into ‘Zones’. The specific size, location and classification of a particular Zone depends on the probability of an explosive atmosphere occurring, and the persistence of this condition. Zones where such conditions do not occur are called ‘Safe Areas.’ ATEX Directive 94/9/EC Category 2 identifies Zones 0 – 3, specifying how prevalent a potentially explosive atmosphere may be. Also, ATEX Zones 20 – 22 classify potentially explosive dust conditions. In both cases the lower number (Zone 0, Zone 20) identifies the most rigorous condition.
### ATEX zones applicable to gas, mists or vapors

<table>
<thead>
<tr>
<th>Zone</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>An atmosphere where a mixture of air and flammable substances in the form of gas, vapor or mist is present frequently, continuously or for long periods.</td>
</tr>
<tr>
<td>1</td>
<td>An atmosphere where a mixture of air and flammable substances in the form of gas, vapor or mist is likely to occur in normal operation occasionally.</td>
</tr>
<tr>
<td>2</td>
<td>An atmosphere where a mixture of air and flammable substances in the form of gas, vapor or mist is not likely to occur in normal operation but, if it does occur, will persist for only a short period.</td>
</tr>
</tbody>
</table>

### ATEX zones applicable to dust

<table>
<thead>
<tr>
<th>Zone</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>An atmosphere where a cloud of combustible dust in the air is present frequently, continuously or for long periods.</td>
</tr>
<tr>
<td>21</td>
<td>An atmosphere where a cloud of combustible dust in the air is likely to occur in normal operation occasionally.</td>
</tr>
<tr>
<td>22</td>
<td>An atmosphere where a cloud of combustible dust in the air is not likely to occur in normal operation but, if it does occur, will persist for only a short period.</td>
</tr>
</tbody>
</table>

In North America, an alternative system for classifying areas of plants with potentially flammable conditions uses the term ‘Division’ instead of ‘Zone’. Whereas ATEX refers to gas and dust by name, the National Electrical Code (NEC) in the United States, and Canadian Electrical Code (CEC) in Canada, define ‘Classes’ as follows:

### Class I, II, III Hazardous Locations

(US Department of Labor, OSHA Office of Training and Education summary)

<table>
<thead>
<tr>
<th>Class</th>
<th>Groups</th>
<th>Division 1</th>
<th>Division 2</th>
</tr>
</thead>
</table>
| Class I gases, vapors and liquids | A: Acetylene  
B: Hydrogen, etc.  
C: Ether, etc  
D: Hydrocarbons, fuels, solvents, etc. | Normally explosive and hazardous. | Not normally present in an explosive concentration (but may accidentally exist). |
| Class II dusts | E: Metal dusts (conductive, explosive)  
F: Carbon dusts (some are conductive, all are explosive)  
G: Flour, starch, grain, combustible plastic or chemical dust (explosive) | Ignitable quantities of dust normally are or may be in suspension, or conductive dust may be present. | Dust not normally suspended in an ignitable concentration (but may accidentally exist). Dust layers are present. |
| Class III fibers and flyings | Textiles, wood-working, etc  
(easily ignitable but not likely to be explosive) | Handled or used in manufacturing. | Stored or handled in storage (exclusive of manufacturing). |
Mounting options

Outdoor radio units and associated antennas must be installed in a variety of attitudes and elevations, often under working conditions involving personnel lifts and requiring specialized safety training and personal protective equipment. Strict code requirements, such as electrical grounding and sealing of penetrations must be observed. The most common mounting techniques involve attaching to a pole or mast, and attaching to a fixed structure such as a building.

Pole or mast mounting

This is perhaps the most common method. For a typical 5 – 10 cm (2 – 4”) vertical mast or horizontal lamp arm, a supplied installation kit includes clamp mounted to the pole using an adjustable retaining bolt. Next the adjustable mounting plate is bolted to the pole clamp. Finally, the radio unit is bolted to the base plate. The mounting plate is adjustable to provide for mechanical up-tilt or down-tilt when installed in a vertical orientation, with easily visible degree markings for mounting angle. Larger diameter poles such as street lamps or high masts do not require the pole clamp. Instead, stainless steel band clamps are used to permanently secure the mounting plate to the pole. The radio unit is again bolted to the base plate. With this option, the access point can accommodate diameters from 10 – 41 cm (4 – 16”).

Wall and building mounting

Figure 1. Pole mounting options for the Aruba-85 outdoor access point

Figure 2. Wall mounting options for the AP-85 outdoor access point
Most radios include mounting points for metal brackets or adaptor plates, or can be screwed directly to a solid structure. Care must always be taken to align the antennas properly. Omni-directional antennas are always oriented exactly vertically. In general, the access point will also be mounted vertically as well, with the antenna connectors facing upwards. If the application calls for a directional antenna to be mounted directly to the access point using an optional standoff bracket, then mechanical up-tilt or down-tilt may be required to properly align antennas at each end of a link.

**Wind rating**

Antennas, mounting brackets and radio units are usually specified for wind exposure in the order of 160 km/hr (100 mph) steady-state and 260 km/hr (165 mph) gusts – but of course this only holds when they are properly installed to a solid mounting point. Wind speeds vary by elevation, and may be higher at the top of high masts or towers. Radio unit-mounted antennas increase wind resistance and stress on the mounting brackets.

**Antenna options**

Antennas shape the RF coverage of an access point, essentially focusing the available energy into a narrow beam that has high power, or spreading it over a wider area with lower power. Whereas indoor deployments commonly use omni-directional antennas, spreading the RF energy uniformly in the horizontal plane, outdoor applications often require a more carefully-considered antenna choice: distances are longer, the number of access points and availability of mounting sites are limited, stationary and moving obstructions are common, and the vertical dimension is often more important. The following is a brief discussion of antenna options for outdoor and harsh environments.

![Figure 3. Omni antenna and polar gain plots (Aruba ANT-10, 5.150 GHz)](image)

**Omni (omni-directional) antenna**

Omni-directional antennas (or ‘omnis’) are usually constructed of a series of dipoles in rod form, and are usually oriented vertically, spreading RF energy in a disk-like figure like a donut: ‘Omni-directional’ is not a true description, as the pattern does not extend uniformly in the vertical plane. Omnis have passive gain (compared with an ideal or ‘isotropic’ uniform radiator) of 2-8 dBi depending on their design. As a rule, the higher the gain, the flatter the coverage disk. The ANT-10 shown above is about 30 cm (12") tall and has a gain of 6 dBi in the 5 GHz band; the ANT-86, of similar form factor but 51 cm (20") tall, has a 9 dBi gain in the same band.
Omni antennas are often mounted to a mast using a supplied pipe clamp that includes a fitting for the base of the specified antenna. Omnis can also be mounted directly to outdoor access points, particularly if they use ‘N-type’ connectors. They are relatively easy to mount, and are little affected by wind and snow conditions.

![Figure 4. 3-D coverage pattern of an omni antenna](image)

Omni antennas are often used to cover geographic areas where mobile client devices may be moving in all directions and there is a clear line-of-sight (LOS) between clients and the access point. An omni in an elevated position can cover a wide area. Note that gain has an effect on the shape of the antenna pattern. For instance, a tower-mounted high-gain omni may lead to a dead spot of coverage immediately underneath the tower.

Under ‘clean’ outdoor conditions, a 6 dBi omni working with 2.4 GHz Wi-Fi (802.11b/g) can cover an area of approximately 400 meter (1300’) radius, with a data rate of 6 Mbps at the edge of that zone.

The vertical dimension of the antenna must be considered when selecting and siting the device. A common mistake is to place an antenna high above ground in order to improve LOS without modeling the resulting coverage and data rate delivered at ground level. If high data rates are desired, the antenna must not be placed so high that the increased vertical distance reduces the achievable data rate at ground level.

**Dish antennas**

![Figure 5. 25 dBi grid-parabolic dish antenna at 5 GHz (Pacific Wireless GD5W)](image)
Dish antennas are sometimes used for point-to-point links. Offering gains in the range of 20-27 dBi, they are often tower-mounted and can support links extending to 15 km (9.3 miles) using 5 GHz band (802.11a) Wi-Fi. Dish antennas are more complex to mount, and must be pointed accurately at the far antenna; alignment aids such as LED displays on the radio can assist with pointing, however, the higher-gain the antenna, the narrower the beam and the more stable the mounting must be in order to maintain alignment through the inevitable physical settling of foundations, thermal flexing of towers, etc. While sometimes constructed as a solid dish, similar to a home satellite TV antenna, it is common to see a grid construction used to reduce wind loading. The spacing of the grid causes the dish to appear solid to RF energy at the operating frequency. Dish antennas can be affected by snow and ice build-up, and flexible covers (radomes) that are transparent to RF energy are available to mitigate this effect.

**Directional antennas (patch, sector, panel, yagi)**

![Directional antennas](image)

Other types of antenna result in patterns between the all-around coverage of an omni and the narrow beam of a dish. There are various semi-directional types:

- **Patch (or panel) antennas** are built on a flat printed circuit board and support gains in the 8-14 dBi range, with patterns from 60-180 degrees in the horizontal plane, and 20-90 degrees vertically. They can measure from 10-30 cm (4-12"), and are usually square or rectangular. Patch antennas are useful for extending range for zone coverage; and are sometimes mounted to the inside of windows to cover outdoor areas. High-gain patch antennas can be used for point-to-point links. Patch antennas must always be oriented with the polarization matched at both ends of the link (a ‘V’ or other marking denotes vertical).

- **Sector antennas** are often used in the cellphone industry, and have a 60-90 degree horizontal pattern with a relatively tight vertical range. They are typically tall and thin, maybe up to a meter high for high-gain models. If sector antennas are mounted on towers, they are often given a down-tilt to ensure good coverage in the desired area. Alternately, panel-form antennas can be designed to cover defined sectors, usually with lower gain.

- **Yagi antennas** consist of many radiating elements, like an old-style television antenna or a hedge-trimmer, and a moderately tight beam. They are often used in large warehouses, sighting down the aisles between racking where their gain of about 10 dBi is useful.

The above are all external antennas, the most likely configuration for outdoor radios. Some access points include integrated antennas, usually a combination of a patch for backhaul and omnis for local coverage. If the particular combination satisfies the application, integrated solutions can save cost and installation time.
Where resistance to multipath interference is important, in locations such as container ports and refineries, the antennas can be mounted to radio units in diversity pairs. This is normal practice for indoor access points, allowing the radio unit to switch antennas per-transmission; if the client is positioned in a multipath null for one antenna, it will often have a good signal from the other. To be effective, the antennas should be spaced a full wavelength apart, about 12 cm (4.7”) for 2.4 GHz or 5 cm (2”) for 5 GHz. At any given time only one antenna is in use, however, adding the second antenna greatly improves link reliability at the expense of installation complexity and cost.

**Powering the industrial access point**

Indoor access points are normally powered either from a local AC power supply, or over the Ethernet connection using power-over-Ethernet (PoE), e.g., the IEEE 802.3af standard. For outdoor applications, access to a suitable power feed may be a significant cost of installation, so equipment should be capable of using a more diverse range of power specifications.

**AC power**

Standard indoor access points are often shipped with 100-264 V switching power supplies, connectorized for common domestic usage. These power supplies are versatile, but are often not designed for extended temperature ranges or for outdoor use. Also, outdoor applications may require specialized connectors and seals to combat moisture or dust. If the design calls for an external power supply to be used outdoors, it is important that they are procured to the same environmental standards as the access points they serve. When using this method, the voltage range of the outlet should be checked, as voltages higher than 250 V are not uncommon in industrial environments, and most common power units are specified only to this limit.

**Power over Ethernet**

IEEE 802.3af PoE is a standard method for powering indoor access points: using the Ethernet cable installed for backhaul, it allows the Ethernet switch, or an in-line power injector called power sourcing equipment (PSE) typically mounted in the wiring closet to distribute 48V DC power to the access point, the powered device (PD). Since most outdoor access points are derived from indoor versions, PoE is likely to be an option for Wi-Fi radio units. The 802.3af standard limits each PoE link to a maximum of 100 meters including the length of any patch cords. When using PoE with outdoor radio units, it is important to calculate power loss in the cable, both because the cable run may be long, and the equipment may take more power than an indoor unit, whether for an internal heater or because it transmits at higher RF power.

When using PoE to power outdoor access points, the cable used should be UV-rated CAT5E or CAT6, as it may be exposed to direct sunlight. Where heavy equipment, vehicles or other risks exist in the environment the cable may be protected by rigid metal conduit. Also, indoor-to-outdoor transitions must incorporate lightning protection to comply with local codes and protect core network equipment from transient voltage surges during lightning strikes.
Street lights and poles

Most light poles use from 105-480 VAC and incorporate a light sensor. It is possible to tap into the sensor and hence power a pole-mounted radio unit, using a standard connectorized cable available from various vendors. Depending on the radio equipment’s power requirements, it may be necessary to mount an external power supply unit with it.

High lighting masts

High lighting masts are the most common lighting method in large industrial yard environments, as well as public venues, ports, prisons and along freeways. High masts range from 20-60 meters (70-200’) in height and typically include from 6-14 lamps in the 1000 W range which attach to a central ring or hub. This ring can be lowered to the ground for maintenance using a lift system built into the center of the pole. An umbilical cord providing power traverses the length of the pole, terminating in a junction box located on the ring and distributing power to each lamp. Unlike the street lamp scenario, a stepdown transformer is generally required to make use of this high voltage power source.
High lighting masts are attractive mounting locations for wireless networks in a yard environment due to their line of sight over the area. However, as noted above they may need special consideration for power, and the antennas must be chosen very carefully. A 'down-tilt' omni-directional antenna which directs a vertically-polarized pattern straight down, such as the Aruba ANT-90, is generally required, as a traditional omni or sector antenna will not be effective at such an elevation.

**DC power from solar**

Most indoor radio units accept low voltage DC power delivered by an external power supply or via PoE. However, the indoor unit can assume power is conditioned in a narrow range, and so need not be forgiving of fluctuations in power on this connector. In outdoor installations, particularly in yard environments with high voltage equipment, power quality cannot be assumed and voltage fluctuations are routine. A useful option that is available on some equipment is an unconditioned 12 V facility. This is generally designed to allow a lead-acid or other heavy-duty 12 V battery to power the access point directly, without any extra power conditioning. The battery may be charged from an external constant or occasional power source using an intelligent AC inverter. Another variation of this model uses a solar panel and 12 V battery combination, allowing easy construction of a self-contained, solar-powered unit for deployment in remote locations. The size and weight of the batteries can be significant, and the associated electrical equipment requires an appropriate NEMA enclosure to house and protect the components at ground level. Such enclosures may in turn require protection by guardrails or concrete pylons against damage from vehicles moving in a yard.

**Lightning protection**

Outdoor radio equipment is susceptible to lightning strikes, even if not directly hit, lightning strikes in the area produce transient voltages sufficiently intense to destroy electronic equipment.
In some cases it is possible to mount the radio unit indoors, driving an outdoor antenna. This configuration is often not practical because of the RF power loss over the potentially long antenna cable, the cost or feasibility of making a building penetration for the cable, or for regulatory reasons. Where such a configuration is allowed, the cables entering the building will be RF coax, and an appropriate lightning protector must be installed and properly grounded on each one. If the antenna is fixed to a tower or mast, depending on the local codes it may also have to be grounded.

It is more common to find the entire radio unit and antenna assembly installed outdoors, and an Ethernet cable, often carrying PoE, connecting it to indoor network equipment. In this case, a CAT5 lightning protector may be appropriate, if lightning conditions are expected to exceed the standard IEC 6100-4-5 or IEEE802.3 induced surge levels (1500 Volts). The lightning protector must be properly attached to an appropriate grounding conductor. In many cases it is appropriate to use lightning protectors at both ends of the Ethernet cable to prevent damage to the radio unit in case of a near-miss. In the most severe lightning conditions, shielded twisted pair (STP) cabling is recommended instead of standard CAT5 unshielded twisted pair (UTP), and appropriate grounding procedures followed.

Regardless of the required grounding at the antenna or tower, the most effective way to protect a wired network from atmospheric electrical discharges is to isolate each radio using fiber-optic cabling. Some manufacturers offer advanced models that support either multi-mode (MM) or single-mode (SM) fiber connections directly to the access point. Alternately, fiber-optic transceivers may be used on both ends of a backhaul link and then connected to radios installed throughout a yard to provide the desired isolation. While the optical components add to the cost, this is the only way to completely protect a wired network.

In all cases, lightning protection for equipment must be part of an overall lightning protection system, as even the above provides protection only against nearby strikes and assumes that the tower or building has an approved lightning protection system in place. This paper is only an introduction to common installation practices: installers are required to be aware of and comply with all applicable local codes and regulations.

**Special or standard connectors**

Outdoor Wi-Fi access points may require connectors for power, network and antenna. Indoor connectors, while inexpensive and readily available, are usually precluded because of environmental, corrosion, moisture or dust concerns. The use of special ‘MIL-SPEC’ connectors adds to the cost of the unit, and increases the cost and difficulty of procuring or fabricating appropriate cables, especially if fabrication is required in the field at the job site. For this reason, a superior approach is to use standard connectors and protect them with external covers or other mechanisms that meet or exceed an IP-68 rating. Experienced installers will often place a protective hot- or cold-shrink type seal around all connectors on an outdoor unit to provide an additional degree of protection. Other outdoor installation ‘best practices’ include the use of ‘drip-loops’ on cabling and orienting antennas and access points so that cables always exit from the bottom of the unit.
Antenna alignment

An important part of installation involves aligning directional antennas. Alignment aids such as access point-mounted LED displays for signal strength, can save considerable commissioning time.

For installations in very remote areas, it may be possible to use the network itself as the infrastructure for mobile (Wi-Fi) voice communications – an ‘order-wire’ on the Wi-Fi network. This is readily achievable through the use of Wi-Fi phones, available in many form factors including ruggedized outdoor versions.

Applications for the Industrial Enterprise AP

Planning tools

RF link and network design is a difficult task, even for experienced RF engineers. RF planning tools are used to model expected network characteristics and predict eventual performance. However, adjustments are often required once the equipment is installed, because RF characteristics on the ground are complex and difficult to measure accurately, even with an RF site survey. It is not possible to remedy a poor design by tweaking the installation phase, making it important to devote attention to the planning phase so the network requires only minor adjustments to optimize operation after installation.
The RF planning tool shown above uses a mash-up to superimpose antenna radiation patterns on a 3D Google-Earth representation of outdoor terrain. Different antenna patterns and transmit power levels can be chosen to visualize the expected coverage map.

**Point to point communications networks**

Many outdoor operations require communication between sites, and within sites, that cannot be accessed by wired or public cellular connections. Examples include oil fields and other upstream sites, rail lines and military bases. Unlicensed wireless has been the traditional solution for these communication needs, and new outdoor Wi-Fi radios offer a cost-effective, IP-oriented solution for extending or bridging networks to hard to reach sites.

The usual topology is to set up a radio unit at a central site, driving a narrow-beam antenna such as a dish for point-to-point bridging. At the far end is an essentially identical unit, where the Ethernet connection links the local TCP/IP network to the central location.

![Image](figure14.png)

*Figure 14. Point-multipoint wireless backhaul (Aruba planning tool)*

Following this, the next level of complexity is a point-to-multipoint topology, where the central site uses an omni or multiple high-gain antennas to send beams to a number of remote, fixed locations. In this case it is necessary to coordinate transmissions among the multiple sites to avoid interference: Wi-Fi accomplishes this using standard protocols.
Example. An offshore oilfield cluster requires inter-platform communications. The main platform's radio mast has line-of-sight to four other platforms, so a central radio unit is mounted on the mast with one antenna directed at each of the other platforms. The distant platforms have a single radio unit connected to one or two antennas depending on the degree of resilience required. Such a network can carry 10-30 Mbps per link, using standard radio units, over distances to >10 km (6.2 miles).

**Mesh protocols**

Networks can be extended over multiple wireless transmission hops using mesh technology. This requires several new protocols for neighbor discovery, security, route selection and loop avoidance. While these protocols are in development at the Wi-Fi standards bodies, enterprise Wi-Fi infrastructure vendors currently use their own proprietary technologies to accomplish these tasks. Each node in the network requires a radio unit with DC or AC power, and this node can act just as a repeater or additionally connect the local TCP/IP network via Ethernet.
Example. An onshore oil field consists of 30 'nodding donkey' well-head installations over an area of 500 sq km, each with electrical power but no wired communications or public wireless service. In order to support telemetry and SCADA traffic, a Wi-Fi radio unit is installed at each well-head. The wireless network is self-organizing and resilient, with each node choosing the shortest path back to the main location. All control and monitoring traffic uses the wireless backbone, connecting to the Ethernet on the local radio unit in bridging mode. Networks such as this require the highest levels of security to deter disruptive exploitation.

Providing local Wi-Fi coverage

Thus far, the topologies discussed have used wireless for point-to-point links between fixed locations. However, all Wi-Fi access points are capable of providing local, zone coverage for scattered or mobile Wi-Fi clients. This can be extremely useful, for example in providing voice and data coverage for mobile workers moving around a large site. A combination of a rugged notebook PC and a Wi-Fi phone provides comprehensive communications, so workers in the field have the same level of access as at their desks.
• Example. A large construction project will involve several tower cranes, site entrance gates and a site office. The continuous activity would require communications wires to be re-strung regularly, but by using a small number of locations for Wi-Fi access points (crane towers make good locations for down-tilt antennas), full coverage of the site is possible. Workers can use Wi-Fi phones to communicate with each other, and with their home offices via an IP-PBX. Wireless surveillance cameras can monitor and record access at entrance gates and provide security video. Digital drawings and work orders can be accessed on the job from rugged notebook PCs, speeding turnaround.

Combining backbone links with local coverage

Many Wi-Fi outdoor access points include two separate radio units, allowing one to be used for point-to-point links while the other provides local access: each node in the mesh networks described above can also cover its immediate area of the site.
Example. A port moves thousands of containers through the site every week. Wi-Fi communications allow mobile workers, cranes, and vehicles to stay in constant contact. However, the steel containers, stacked up to five-high, present a formidable RF obstacle, and one that shifts from day to day as on-site storage requirements fluctuate. A number of Wi-Fi radios around the site, connected by point-to-point links can form a mesh backbone, that dynamically creates alternate paths as RF conditions change.

Example. A rail road track operator has many miles of track with isolated switching, monitoring and maintenance buildings. A robust, low-cost communications network uses Wi-Fi outdoor radios spaced a few kilometers apart to provide multi-Mbps communications links to these locations. Since Wi-Fi incorporates a standard quality of service protocol, voice-over-IP (VoIP) phones may be installed at these remote offices, controlled by a central IP-PBX and allowing 5-digit dialling desk-to-desk. Printers in remote locations can be controlled remotely, and video surveillance cameras can provide continuous monitoring for security purposes.

Conclusion

Wireless technology began outdoors to help industrial customers meet business needs where they could not run cable. As this technology was standardized as Wi-Fi, dramatic cost reductions fuelled by economies of scale made it accessible to the consumer and enterprise markets.

Enterprise Wi-Fi technology has evolved over the last ten years to the extent that it has now solved many issues involving management, scale, reliability and performance: many enterprises now rely on their indoor Wi-Fi networks as the primary means of connecting to the corporate LAN for PC users, and organizations such as hospitals, retail stores and universities rely on Wi-Fi for voice communications for mobile workers. Video surveillance is another important service today leveraging the Wi-Fi network, and benefits from Wi-Fi's high bandwidth and quality of service capabilities.
These networks are highly secure, supporting the latest 802.1x authentication and encryption techniques, and many CIOs now confirm that their wireless network is more secure than the wired LAN. Role-based WLANs can support a mix of sophisticated, capable devices such as PCs, as well as low-complexity devices such as bar-code scanners, without compromising security.

A recent addition to state-of-the-art enterprise Wi-Fi is mesh technology, where access points can use wireless links for their backhaul connection rather than wired Ethernet. Since many enterprise access points include two radio units, it is possible to maximize performance by using one radio for backhaul while the other serves local users.

This combination of Wi-Fi technologies is now capable of serving outdoor and hazardous environments. Ruggedized access points can be used to drive point-to-point and point-to-multipoint links over distances of several miles, offering comparable performance to previous specialized radio equipment at very cost-effective price points due to Wi-Fi's high production volumes. The networks formed from these links may be used to bridge wired LAN segments, or to light up remote areas with Wi-Fi coverage, enabling a variety of Wi-Fi terminals including telemetry, ruggedized PCs, Wi-Fi phones, and video surveillance cameras.

The new generation of outdoor access points is versatile, with many options for mounting and power, and provides installation options such as integral signal strength meters for antenna alignment. The units are small, lightweight, and have modest power requirements compared to their predecessors, while they are specified for harsh conditions such as explosive and corrosive atmospheres.

By using Wi-Fi, organizations can consolidate the current patchwork of communications links and services onto a single Wi-Fi network, with central management, reporting, and alarms. The networks can be self-organizing in RF channel selection and connection routing, reacting automatically to remedy failures. Quality of service features across all products assures multi-service capability throughout the network.

The wide availability of inexpensive, ruggedized Wi-Fi terminals allows new options for a mobile workforce, providing a level of services on the move that was previously only available when workers returned to their offices.

These new capabilities will be of special interest in the upstream and downstream petroleum industry, for chemical plants, power and water treatment facilities and many other applications where networks must cover distances of several miles with offered data rates of several Mbps.

About Aruba Networks, Inc.

Aruba Networks is a leading provider of next-generation network access solutions for the mobile enterprise. The company’s Mobile Virtual Enterprise (MOVE) architecture unifies wired and wireless network infrastructures into one seamless access solution for corporate headquarters, mobile business professionals, remote workers and guests. This unified approach to access networks enables IT organizations and users to securely address the Bring Your Own Device (BYOD) phenomenon, dramatically improving productivity and lowering capital and operational costs.

Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, Africa and Asia Pacific regions. To learn more, visit Aruba at http://www.arubanetworks.com. For real-time news updates follow Aruba on Twitter and Facebook, and for the latest technical discussions on mobility and Aruba products visit Airheads Social at http://community.arubanetworks.com.
# Appendix: Brief specifications for some outdoor access points and antennas

<table>
<thead>
<tr>
<th>Aruba AP-85TX – selected specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Point</strong></td>
</tr>
<tr>
<td>802.11a radio: Frequency 5.180-5.825 GHz</td>
</tr>
<tr>
<td>Transmit power 20 dBm</td>
</tr>
<tr>
<td>Association rates 108, 54, 48, 36, 24, 18, 12, 9, 6 Mbps</td>
</tr>
<tr>
<td>802.11g radio: Frequency 2.400-2.480 GHz</td>
</tr>
<tr>
<td>Transmit power 20 dBm</td>
</tr>
<tr>
<td>Association rates 108, 54, 48, 36, 24, 18, 12, 9, 6 Mbps</td>
</tr>
<tr>
<td>Also supports 802.11b clients</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

The AP-85 has two radios, one each for 2.4 and 5 GHz. It is an all-purpose access point for outdoor and harsh conditions. The AP-85 has two antenna connectors per radio for full diversity, and accepts a range of power inputs. This version of the AP-85 has a copper Ethernet connection accepting standard power-over-Ethernet and also accepts 12 VDC.

The AP-85FX and AP-85LX have two radios, one each for 2.4 and 5 GHz. They all-purpose access points for outdoor and harsh conditions. All AP-85 models have two antenna connectors per radio for full diversity. Instead of a copper Ethernet connection, these units are fiber-connected, allowing much longer cabling runs. These variants also support AC power directly on an integral connector, and also accept 12 VDC.
### Aruba AP-ANT-80

<table>
<thead>
<tr>
<th>Antenna</th>
<th>Specification</th>
<th>Antenna Pattern</th>
<th>Mounting Options</th>
</tr>
</thead>
</table>
| ANT-80  | Band: 2.4 – 2.5 GHz  
Gain: 8.0 dBi  
Polarization: Vertical  
Beamwidth: 13º E-plane, 360º H-plane  
Dimensions: 25 x 1”; 63.5 x 2.5 cm  
Input: 20 W; 50Ω; VSWR <1.5:1  
Operating temperature: -40º to 158º F; -40º to 70º C  
Connector: N-male; 36” pigtail or direct-mount using N-male connector (ANT-80D) | ![Antenna Pattern](image) | ![Mounting Options](image) |

ANT-80 is an omni antenna for the 2.4 GHz band. It has a relatively high gain at 8 dBi, but coverage in the vertical plane is 13 degrees. This is the most commonly used antenna for 2.4 GHz (802.11b/g) area coverage outdoors.

### Aruba AP-ANT-86

<table>
<thead>
<tr>
<th>Antenna</th>
<th>Specification</th>
<th>Antenna Pattern</th>
<th>Mounting Options</th>
</tr>
</thead>
</table>
| ANT-86  | Band: 5 GHz  
Gain: 9.0 dBi  
Polarization: Vertical  
Beamwidth: 8º E-plane, 360º H-plane  
Dimensions: 19.5 x 1”; 49.5 x 2.5 cm  
Input: 10 W; 50Ω; VSWR <2.0:1  
Operating temperature: -22º to 149º F; -30º to 65º C  
Connector: N-male; 36” pigtail | ![Antenna Pattern](image) | ![Mounting Options](image) |

ANT-80 is designed for mast mounting as shown below (AP-86).

A variant, ANT-80D, can be mounted directly on outdoor APs such as Aruba’s AP-85, using the integral N-type connector.
### Aruba AP-ANT-89

<table>
<thead>
<tr>
<th>Antenna</th>
<th>Specification</th>
<th>Antenna Pattern</th>
<th>Mounting Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Band: 5 GHz</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gain: 14.0 dBi 5.1-5.3 GHz 13.5 dBi 5.4-5.9 GHz</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Polarization: Vertical</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Beamwidth: 30° E-plane, 30° H-plane</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dimensions: 4 x 4 x 1.4&quot;; 10.2 x 10.2 x 3.5 cm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Input: 10 W; 50Ω; VSWR &lt;2.0:1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating temperature: -40° to 158° F; -40° to 70° C</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connector: N-male; 36&quot; pigtail</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ANT-89 is a high-gain directional antenna used for point-to-point links in the 5 GHz band. A line-of-sight path provides best performance. Two antennas can be mounted a few feet apart to provide diversity, when used with the Aruba AP-85 access point.

![ANT-89](image)

### Aruba AP-ANT-90

<table>
<thead>
<tr>
<th>Antenna</th>
<th>Specification</th>
<th>Antenna Pattern</th>
<th>Mounting Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Band: 2.4 &amp; 5 GHz</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gain: 2.6 dBi @ 2.45 GHz 3.3 dBi @ 5.55 GHz</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Polarization: Vertical</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Beamwidth: 55°-60° E-plane, 360° H-plane</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dimensions: 6.2 x 0.9 x 3.7&quot;; 15.7 x 2.3 x 9.3 cm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Input: 2 W; 50Ω; VSWR &lt;2.0:1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating temperature: -40° to 158° F; -40° to 70° C</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connector: N-male; 36&quot; dual pigtail</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ANT-90 is a diversity downtilt omni antenna for both Wi-Fi bands. Each unit includes two antennas, and has two connector pigtails. ANT-90 is ideally mounted on a high ceiling, lighting mast or other structure. It provides coverage in an even circular (omni) pattern on the floor below.

![ANT-90](image)
### Aruba AP-ANT-91

<table>
<thead>
<tr>
<th>Antenna Specification</th>
<th>Antenna Pattern</th>
<th>Mounting Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Band:</strong> 2.4 &amp; 5 GHz</td>
<td><img src="image" alt="E-plane" /></td>
<td>ANT-91 is wall-mounted using screws. For dual-band, diversity installations as shown above, two units will be mounted a feet or more apart. Each unit will connect to one 2.4 GHz and one 5 GHz antenna connection on the access point.</td>
</tr>
<tr>
<td><strong>Gain:</strong> 5.0 dBi</td>
<td><img src="image" alt="H-plane" /></td>
<td></td>
</tr>
<tr>
<td><strong>Polarization:</strong> Vertical</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Beamwidth:</strong> 65° E-plane, 120° H-plane</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Dimensions:</strong> 2.2 x 5.2 x .14”, 5.5 x 13.1 x 3.5 cm</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Input:</strong> 5 W; 50Ω; VSWR &lt;2.0:1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Operating temperature:</strong> -40° to 158° F; -40° to 70° C</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Connector:</strong> N-male; 36” dual pigtail</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ANT-91 is a dual-band diversity antenna: it is two antennas in one unit. Its pattern is suitable for wall-mounting: 120 degrees in the horizontal and 65 degrees in the vertical plane.