



Public Safety Wireless Solutions Guide



High-speed networks that are
available anytime, anywhere—
just like the agencies they serve.





Introduction: A new era of wireless mobility

In 1928, a Detroit police officer and a young engineering student unveiled a radical new weapon in the war against prohibition-era gangsters and bootleggers: the first reliable mobile radio system.

After loading a bulky receiver into the back of a Model T Ford cruiser, the Detroit Police Department fired up a transmitter on Belle Isle in the Detroit River and went on the air with the call sign W8FS. It was a radio station unlike any other, and its impact extended far beyond its broadcast range, forever changing the way public safety agencies communicate.

Three-quarters of a century later, emergency services once again stand at the forefront of a technological revolution. Communities around the country are using next-generation wireless networks to improve inter-agency cooperation, protect the personal safety of first responders, and provide police, fire, and emergency medical personnel in the field with unprecedented access to critical information.

At the same time, these agencies are using wireless technology to ramp up productivity and lower operational costs, giving them more time and resources to devote to their core public safety missions.

In this guide, you'll learn how affordable, secure, easily managed wireless local-area network (LAN) solutions complement existing communications systems. You'll see how a properly designed and configured wireless LAN can mitigate perceived challenges, such as data security and in-band radio interference. You'll also see how agencies of various sizes are already taking advantage of Cisco Aironet® wireless LAN solutions, often with dramatic results.

In the suburbs of Columbus, Ohio, for example, long-range wireless bridges provide small agencies with a cost-effective means of sharing information and resources, including regional fingerprint and mug-shot databases.

In Buffalo Grove, Illinois, a mobile command post lets police and fire crews check departmental records and other information from the field, and even beam live video back to their stations.

And in Seal Beach, California, wireless links to bank security cameras enable officers to see a robbery in progress, even as they race to the scene.

In these and other ways, public safety professionals are leading the way into a new era of communications, demonstrating how extraordinary innovations can help protect the lives and property of ordinary citizens.



Applications: Wireless networking for public safety

First responders are no strangers to the vital importance of wireless communication. In addition to two-way radios, many use mobile computers to send and receive data over Cellular Digital Packet Data (CDPD) or private land mobile radio networks.

With an effective transmission rate of 9.6 Kbps, these networks offer adequate bandwidth for text-based applications such as e-mail, instant messaging, and simple database queries, but are too slow to support more sophisticated applications.

Now many agencies are enhancing and complementing these systems with wireless LANs based on international standards known as IEEE 802.11, making it possible to store and retrieve data at far greater speeds. In doing so, they've not only increased the performance and availability of existing text-based applications, but also opened the door to entirely new ones, such as digital imaging and streaming video. And they've saved money in the process, avoiding the cost of monthly service charges and reducing their reliance on wireless service providers.

Photographs, fingerprints, structural diagrams, telemetric information, voice calls, and video feeds can be transmitted over 802.11 wireless networks. E-mail and other Web-based applications are supported as well, giving personnel in the field mobile access to all the information and resources available through their wired networks.

As a result, public safety professionals can make faster, more informed decisions, potentially saving lives and property. They can also save considerable time filing reports and taking care of other administrative tasks, avoiding the need to transfer data between department servers and vehicle computers using floppy disks. And with so many tools at their disposal, they can be more self-reliant, easing the burden on dispatchers and other support staff.

Using a digital camera and a small-scale scanner, for example, a police officer can capture suspect mug shots and fingerprints at the point of arrest. The information can then be transmitted from the cruiser back to headquarters over a wireless LAN, then automatically relayed onto regional, state, and federal databases.

Case Study: Seal Beach, California

Most times police respond to a bank robbery, they have no idea what to expect when they get there. Obviously, this lack of information puts them at a major disadvantage. But that's no longer the case in the City of Seal Beach, thanks to a remarkable IP video surveillance solution developed by Cisco Systems and Loronix Information Systems.

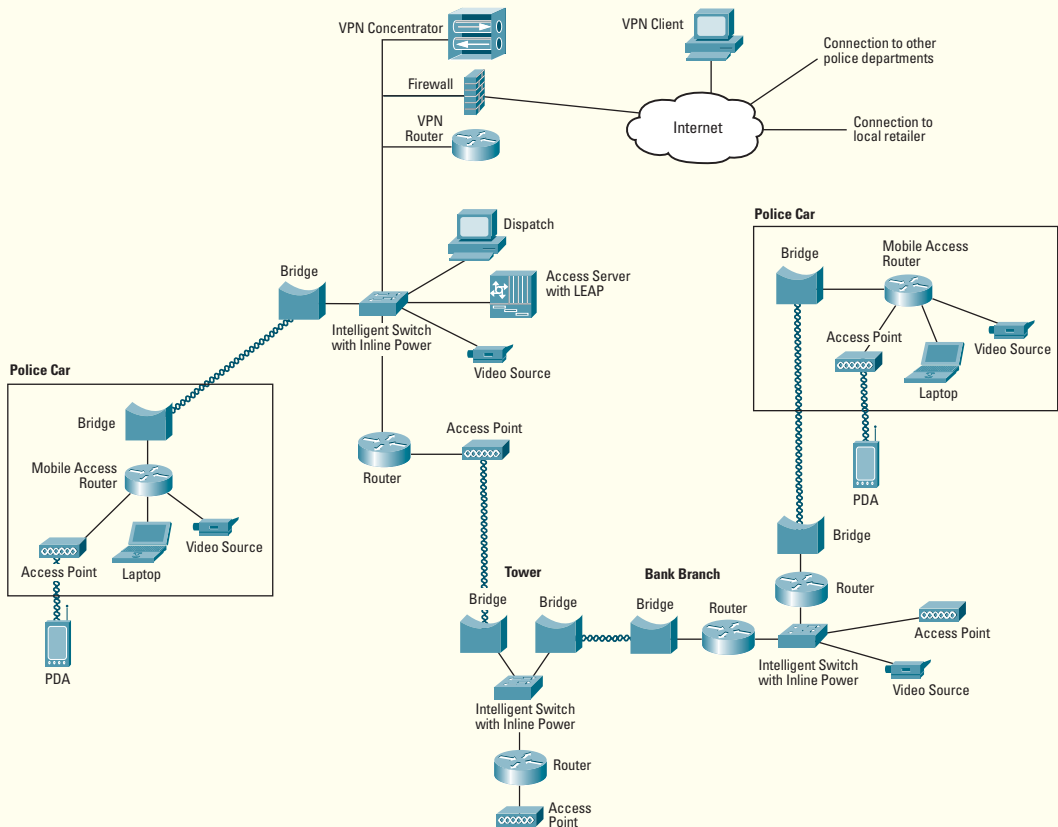
Now, if an alarm is triggered at a local bank, the bank's existing security cameras will automatically begin transmitting live video over a network of Cisco Aironet wireless bridges and access points. Officers of the Seal Beach Police Department can see what's happening inside the bank using touch-screen notebooks in their cruisers, which rely on Cisco mobile access routers to maintain the high-speed connections while in motion.

"It's like giving our officers remote, real-time x-ray vision," said Chief of Police Michael Sellers. "Instead

of waiting until after the crime takes place and after there are victims, we can see video of the crime actually taking place, allowing us to make better, safer decisions."

Ultimately, the city plans to extend the IP video surveillance solution to retail stores, schools, hospitals, and other organizations that wish to participate. Video feeds will also be accessible on specially equipped PDAs, providing even greater functionality.

"By using the PDA system, officers will be able to take a position of concealment away from our vehicles and still allow us to see what is happening in the bank," said Sgt. Dean Zanone. "Plainclothes detectives could maintain their concealment and perhaps get even closer. It will also make building searches, which are very tricky, much easier."





Without this technology, a suspect typically would be transported back to headquarters to be photographed and fingerprinted by police technicians, who would then manually enter the results into relevant databases.

In addition to saving time and effort, a wireless LAN can enable the officer to conduct a real-time database query on the suspect, comparing the fingerprints against thousands of others on file. This will not only verify the suspect's identity, but could potentially lead to a match with prints from an unsolved case.

Some of the most exciting applications for high-speed wireless LANs involve the ability to send and receive live video feeds. Known as IP video, since it's based on the Internet Protocol that defines how information is passed between systems across the Web, it can be used to remotely monitor public areas and to gain insight into rapidly developing or escalating situations.

Incident commanders can view structure fires, protests, and other events as they're happening, helping them to direct response teams and resources accordingly. Ground crews can share the bird's-eye view of helicopters overhead. Ambulances can transmit live video as they speed toward trauma centers, allowing medical teams to see the condition of patients before they arrive. Police can keep an eye on areas without actually driving there, and can even view fellow officers as they make traffic stops and respond to disturbances, instead of simply retrieving videotape from a cruiser after something's gone wrong.

"I have seen too many officers be disarmed or overwhelmed on car stops while those images were recorded passively," said Sgt. Dean Zanone of the Seal Beach Police Department, likening an IP camera in an officer's car to "a guardian angel looking over his shoulder."

Deployment: Flexible, scalable wireless solutions

The cornerstones of all these public safety solutions are high-speed wireless hot spots. Unlike public hot spots—which have begun to appear in airports, hotel lobbies and coffee shops as a convenience for visitors, allowing anyone with a wireless-enabled computer or PDA to access the Internet—the hot spots used by police, firefighters, and paramedics are highly secure and accessible only to authorized personnel.

High-speed wireless LAN coverage can be limited to one or two private hot spots measuring a few hundred feet in diameter, or can be extended across an entire community using multiple overlapping hot spots.

For many municipalities, one of the attractive features of 802.11 wireless technology is the fact it can be deployed in a modular fashion, starting with establishment of hot spots around police stations and firehouses, and expanding out to other areas as resources become available and utilization increases.

At the center of hot spots are devices known as access points, which plug into the wired network to create secure wireless gateways, enabling authorized personnel to send and receive data using wireless-enabled notebooks, PDAs, and other devices.

Case Study: Buffalo Grove, Illinois

Located 35 miles northwest of Chicago, the village of Buffalo Grove initially took a traditional approach to mobile communications. A wide-area network solution provided remote access to police department data, and patrol cars were equipped with notebook PCs containing basic information on license plates and vehicle registrations.

Still, the officers remained highly dependent on headquarters for other critical data while on patrol, and had to return to their station to write up incident reports. Illegible handwriting, misplaced paperwork, and an inability to quickly retrieve data added to frustrations.

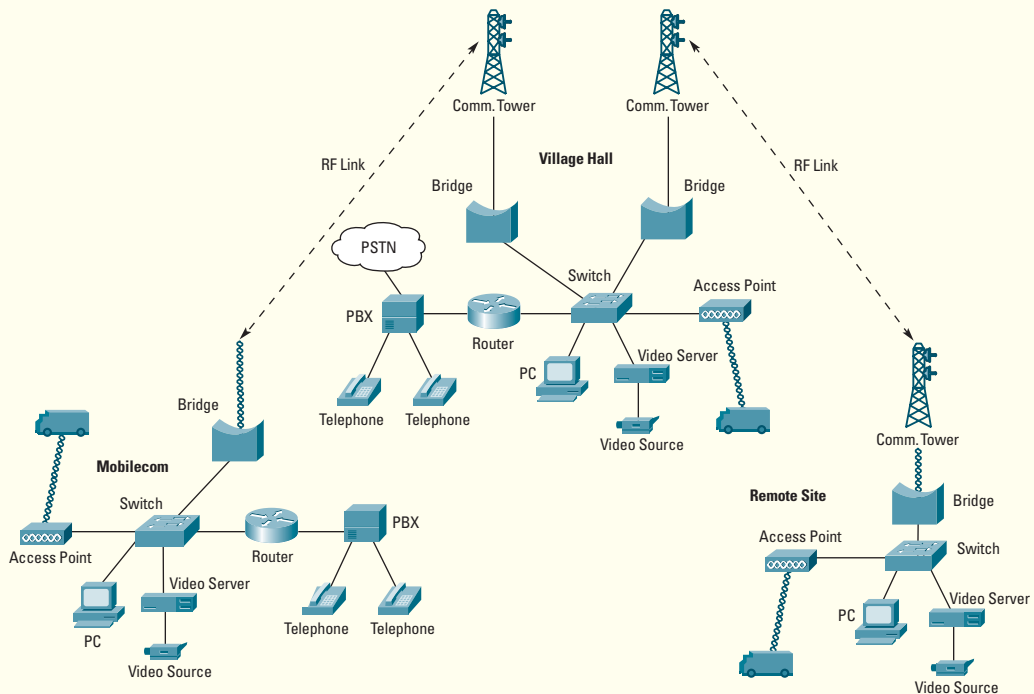
“Our officers were spending countless hours tethered to a desk writing reports instead of out on the street, helping our citizens,” recalled Robert Giddens, the village’s Director of Managed Information Services.


To solve these problems, the village deployed a high-speed wireless network based on Cisco Aironet solutions. Using wireless hot spots located outside fire stations and police headquarters, officers were able to transmit reports directly from their squad cars.

Now officers are spending more of their shift time out in the community. If an incident report needs to be written up, an officer has to drive only a few miles at most to transmit it to headquarters. Meanwhile, the department is saving over \$4,000 every month that would otherwise have been spent on T1 lines linking the fire and police departments together.

High-speed wireless connectivity was later extended to the village’s mobile incident command vehicle. A directional antenna was placed on the vehicle’s 53-foot pneumatic mast, linking into the village’s network via a Cisco Aironet wireless bridge. A wireless access point was also placed on the vehicle to provide network access for patrol cars.

Finally, a camera was mounted atop the mast, allowing emergency personnel to look down on developing situations, such as a burning building. An IP video server allows anyone back at the fire or police stations to view the scene as well using a standard Web browser.






Another kind of device, the wireless bridge, can be used to create high-speed wireless links between buildings. Wireless bridges deliver several times the throughput of T1 lines at a fraction of the cost, since there are no recurring service charges.

Wireless bridges can be configured for point-to-point or point-to-multipoint applications, allowing two or more sites to connect into a single LAN and share a single high-speed Internet connection. They have a maximum range of about 25 miles, and can be used in tandem to cover even greater distances, with data transmissions hopping from one bridge to the next.

Wireless bridges can also be used to create hot spots in areas far beyond the reach of the wired LAN, because unlike access points, they don't need to be physically plugged into the network. All they require is a power source, and a link to the network via another wireless bridge.



For seamless wireless connectivity while in motion, public safety vehicles can be outfitted with mobile access routers. These rugged, compact devices make it possible to maintain secure network connections as the vehicles move from one hot spot to the next, avoiding the need to re-authenticate users each time they come within range of another access point.

Between hot spots, the mobile access router will automatically switch over to any other available wireless technology, taking advantage of slower radio, cellular, and satellite networks to maintain an uninterrupted connection until high-speed wireless LAN coverage resumes.

The mobile access router seamlessly hands off the connection from one network to the next, so applications continue to run independent any particular wireless technology.

Security: New safeguards for sensitive data

For obvious reasons, public safety organizations are extremely cautious about any technology that might leave their networks vulnerable to intrusion. The Cisco Wireless Security Suite offers the most comprehensive set of wireless LAN authentication and encryption features available, closely paralleling the security services in a wired LAN.

This robust solution provides scalable, centralized security management and supports dynamic per-user, per-session encryption keys to protect the privacy of transmitted data. Other enhancements include the ability to encrypt every data packet with a different key, thwarting attempts to hack into the network by deciphering the key for an intercepted packet.

Cisco Aironet solutions support all 802.1X Extensible Authentication Protocol (EAP) types, including EAP Cisco Wireless, also known as LEAP. Cisco LEAP supports a broad range of operating systems and allows existing security procedures, such as user-name and password prompts, to be integrated into a single sign-on and authentication process.

From the user's perspective, the log-on process appears the same as it always has. After the user's name and password are entered, the access point will block all traffic until the user's credentials are authenticated. Once that's completed, a



unique 128-bit cipher and temporal key integrity protocol (TKIP) enhancements from Cisco Systems are used to safeguard all information transmitted over the air.

For organizations looking to provide a seamless security framework between a radio networks, an added layer of security can be achieved through the use of virtual private network (VPN) solutions. Cisco VPN solutions meet the highest security requirement of the federal government, providing strong triple DES encryption and authentication through digital certificates, one-time password tokens, and pre-shared keys to further protect sensitive information transmitted over wireless networks.

A recognized leader in network security issues and solutions, Cisco believes that no single point of defense can guarantee data privacy and protection; for true network security, an end-to-end approach is required across both the wired and wireless LAN, from the network core to the network edge.

For more information on wireless LAN security, visit:
www.cisco.com/go/aironet/security

Availability: Reliable and predictable performance

For public safety organizations, keeping the network up and running can literally be a matter of life and death. It's critical that the wireless LAN solutions they deploy offer enterprise-class performance and reliability.

Cisco Aironet wireless solutions allow organizations to build highly resilient, available wireless LANs with fault-tolerant configurations. Using hot-standby capabilities, for example, the network can be designed so that a backup access point will immediately take over in the rare event a primary access point fails.

Because wireless bandwidth is a shared medium, organizations may wish to deploy multiple access points in areas where they expect high user densities. In such situations, the load-balancing features of Cisco Aironet solutions can be utilized to ensure the different access points work as a system, evenly distributing bandwidth among the various users and optimizing performance in real time.

Radio Interference: Simple steps for clear connections

Accustomed to using privately licensed radio frequencies for voice and data transmissions, public safety organizations are sometimes leery of technologies that operate in the unlicensed spectrum, including 802.11 wireless LANs. Fortunately, these concerns are easily addressed.

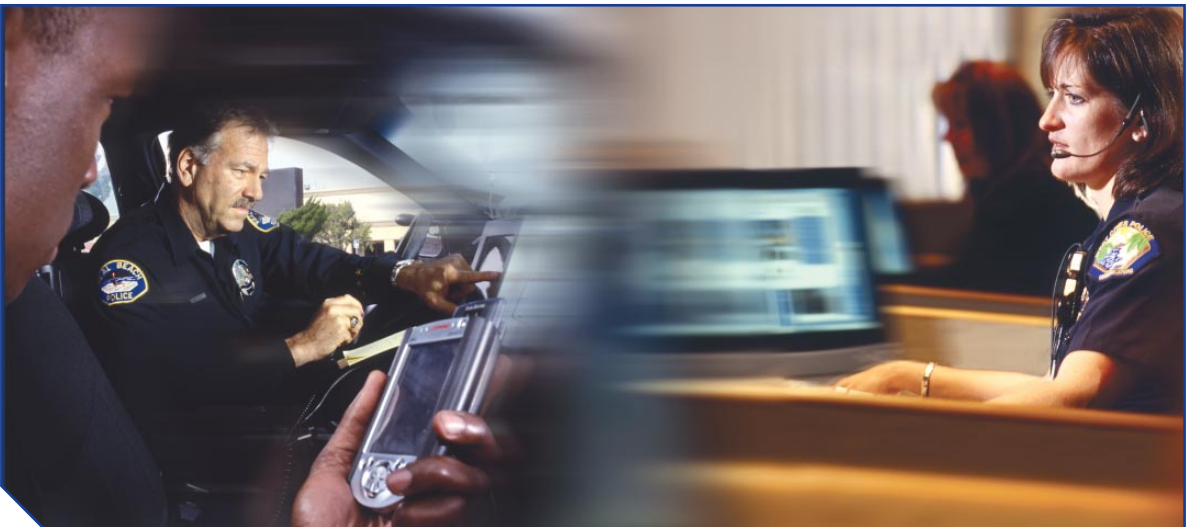
One of the perceived problems with unlicensed frequencies is the fear of in-band interference from other devices, leading to signal degradation and an unreliable wireless network. Although the possibility of interference does exist—cordless phones, microwaves, and Bluetooth™ wireless devices share the 2.4 GHz band with 802.11b wireless LANs—it is not a serious threat to a properly designed network.

By measuring in-band interference beforehand, agencies can design around any possible sources of interference. If interference is detected on one channel, two others are still available.

Deploying additional access points also helps mitigate the risk of in-band interference, as mobile devices will automatically seek out a clear channel on another access point if performance drops below acceptable thresholds.

It's important to note that even when interference is encountered in the 2.4 GHz band, it does not disable 802.11b wireless networks. In most cases, performance will degrade by no more than 15 to 20 percent.

Cisco Aironet solutions also offer support for 802.11a wireless LANs, which operate in the 5 GHz band and aren't subject to interference from devices using the 2.4 GHz frequency. 802.11a wireless LANs also offer faster data rates up to 54 Mbps—compared with the 11 Mbps of 802.11b devices—but are more limited in their range and may not be as ideal for outdoor applications.



Case Study: Columbus, Ohio

In the Columbus metropolitan area, information didn't always follow criminals across jurisdictional borders.

The Columbus Department of Police (CDP) and its smaller counterparts in the area maintained independent records, and generally shared information only when officers had reason to suspect cross-boundary criminal activity.

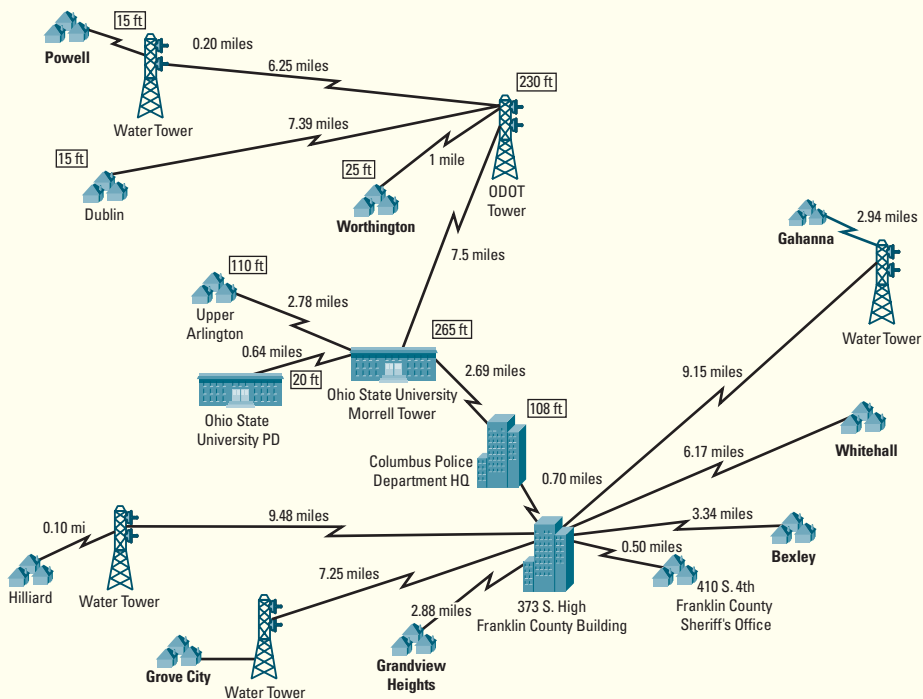
As a result, cases sometimes resembled jigsaw puzzles, with no one agency holding all the pieces. The situation was particularly frustrating for officers in the suburban areas, since they needed to travel to CDP headquarters to access important resources, such as fingerprint and mug-shot databases. For some, that meant a 20-minute drive each way. Once there, it could take an hour or more to retrieve requested information.

Fortunately, wireless LAN technology provided a simple and affordable solution.

The agencies deployed Cisco Aironet wireless bridges at each facility, creating a network of high-speed links that allowed them to share data more easily, and provided everyone with immediate, around-the-clock access to fingerprint and mug-shot databases.

Using wireless bridges allowed the agencies to avoid the recurring costs of leasing high-speed data lines, savings that proved pivotal in securing the participation of some of the smaller municipalities.

"If we were to ask them to purchase a T1 or T3 or fiber, it would be cost-prohibitive for them," said CDP Commander Stan Parlow. "For some of these agencies, there is no way that they can afford the monthly service charges for the link. We looked at wireless and said, really, after you make the initial investment, you are done."



Equipment: Cisco Aironet access points, bridges, adapters, and accessories

Cisco Aironet wireless access points, bridges, adapters, and accessories provide a secure, reliable, easy-to-manage foundation for high-performance wireless LANs. Cisco Systems recommends the following equipment for the rigorous demands of public safety solutions:

Cisco Aironet 1200 Series Access Points set the standard for secure, manageable, and reliable wireless connectivity. With simultaneous support for 2.4 GHz and 5 GHz radios, the Cisco Aironet 1200 Series enables public safety organizations to deploy wireless LANs based on the 802.11b standard, the faster 802.11a standard, or both. Its field-upgradable design also provides a migration path to future 802.11g equipment, when available. With its plenum rating, inline power support, and two separate locking mechanisms, the Cisco Aironet 1200 Series is an ideal choice for the rigorous demands of public safety applications, including outdoor deployments.



For a **Cisco Aironet 1200 Series Access Point data sheet**, please visit:

www.cisco.com/en/US/products/hw/wireless/ps430/products_data_sheet09186a00800937a6.html

For a **Cisco Aironet Power Injector data sheet**, please visit:

www.cisco.com/en/US/products/hw/wireless/ps430/products_data_sheet09186a00800f927d.html

Cisco Aironet 1100 Series Access Points offer an affordable, intelligent, and upgradable 2.4 GHz wireless LAN solution that's highly secure and easy to manage. Equipped for the IEEE 802.11b standard, the Cisco Aironet 1100 Series features a field-upgradable design to ensure a smooth migration to the future IEEE 802.11g standard. The compact size, integrated diversity dipole antennas, and innovative bracket design of this Cisco IOS-based access point allow for quick, easy installation in a variety of orientations. It's an ideal choice for indoor applications, allowing dispatchers, watch commanders, and other personnel to maintain network connections without being tied to desks.



For a **Cisco Aironet 1100 Series Access Point data sheet**, please visit:

www.cisco.com/warp/public/cc/pd/witc/ps4570/ps4612/prodlit/airap_ds.htm

For a **Cisco Aironet Power Injector data sheet**, please visit:

www.cisco.com/warp/public/cc/pd/witc/ps469/prodlit/pwrin_ds.htm

Cisco Aironet 350 Series Wireless Bridges enable high-speed building-to-building links of up to 25 miles (40 km) in FCC regulated areas. Delivering throughput several times greater than T1 lines at a fraction of the cost, wireless bridges are ideal for data-intensive, line-of-sight applications, such as connecting public safety headquarters, substations, and mobile command vehicles. They can be configured for point-to-point or point-to-multi point applications, allowing two or more sites to connect into a single LAN and/or share a single high-speed Internet connection.



For a **Cisco Aironet 350 Series Wireless Bridge** data sheet, please visit:
www.cisco.com/en/US/products/hw/wireless/ps458/products_data_sheet09186a008008883c.html



Cisco 3200 Series Mobile Access Routers allow public safety personnel to maintain secure data, voice, and video connections while their vehicles are in motion. These compact, high-performance devices offer seamless mobility and interoperability, so automobiles, aircraft, and boats can stay connected while roaming between radio, cellular, and satellite networks. Support for industry-standard IP enables the Cisco 3200 Series to accommodate any type of standard wireless connection, with IP traffic remaining independent of the wireless transmission medium.

For a **Cisco 3200 Series Mobile Access Router** data sheet, please visit:
www.cisco.com/en/US/products/hw/routers/ps272/products_data_sheet09186a00800f9ecb.html



Cisco Aironet 350 Series Client Adapters complement Cisco Aironet 1200 Series access points utilizing one or more 2.4 GHz radios. Available in PCMCIA and PCI form factors, these 802.11b-compliant client adapters quickly connect desktop and mobile computing devices to the wireless LAN.

For **Cisco Aironet 350 Series Client Adapters** data sheets, please visit:
www.cisco.com/en/US/products/hw/wireless/ps4555/products_data_sheet09186a0080088828.html

www.cisco.com/en/US/products/hw/wireless/ps4555/products_data_sheet09186a0080092471.html



Cisco Aironet 5 GHz Wireless LAN Client Adapters complement Cisco Aironet 1200 Series access points using one or more 5 GHz radios. The 802.11a-compliant CardBus adapter operates in the UNII-1 and UNII-2 bands to provide up to 54 Mbps throughput.

For **Cisco Aironet 5 GHz Client Adapters** data sheet, please visit:
www.cisco.com/en/US/products/hw/wireless/ps4555/products_data_sheet09186a00800c61ea.html



Cisco Aironet Antennas and Accessories are available for client adapters, access points, and bridges to customize wireless solutions. With the industry's widest selection of directional and omnidirectional antennas (2.4 GHz or 5 GHz), low-loss cable, mounting hardware, and other accessories, public safety organizations can create a wireless solution that meets the requirements of even the most challenging applications.

For **Cisco Aironet Antennas and Accessories** data sheets, please visit:
www.cisco.com/en/US/products/hw/wireless/ps469/products_data_sheet09186a0080092285.html

www.cisco.com/en/US/products/hw/wireless/ps469/products_data_sheet09186a008008883b.html

Service and Support: The backing of a world leader

From initial installation to future upgrades, Cisco Systems makes it easy for public safety organizations to complement their existing communications systems with secure, reliable, high-speed wireless LANs.

Deployment assistance is available through Cisco Total Implementation Solutions, and extended technical support is offered through Cisco SMARTnet and SMARTnet Onsite service programs.

For municipalities that require advanced deployment, design, and integration services, Cisco Systems has a variety of partners with the expertise to assist in all phases of the process, including:

- Site surveys
- Coverage mapping
- Hot-spot design and deployment
- Wireless bridge installations
- 700 MHz/2.4 GHz/5 GHz systems integration
- Mobile device installation and configuration
- Training and support
- System certification

For information on how to get started, visit:

www.cisco.com/en/US/products/svcs/ps2961/ps2738/serv_group_home.html





For more information

www.cisco.com/en/US/netsol/ns110/ns175/net_solution_home.html

www.cisco.com/en/US/products/hw/wireless/index.html



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic
Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy
Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2002, Cisco Systems, Inc. All rights reserved. CCIP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)