

Getting A Grip On Wireless

Edwin E. Mier and Robert B. Tarpley

The four packages reviewed deliver a rich array of wireless-network control capabilities—some common, some unique.

“**W**ireless security” used to be an oxymoron, but not any more. A year ago, *BCR* readers saw the results of our first hands-on review of a new product class: systems designed expressly for securing wireless networks (see *BCR*, October 2004, pp. 24–32). Much has happened since then, and the time had come to revisit the subject. So the results of this, the latest *BCR*-Miercom test round, are presented here.

First we re-surveyed the industry, looking for systems and packages that provide “enhanced and advanced management and control” of wireless networks. We uncovered several key new players. And at least one vendor in last year’s review, Chantry Networks, had been snatched up (acquired by Siemens).

An open solicitation to participate was issued to all potential candidates, and four vendors accepted (Table 1):

■ **Aruba Networks**, which submitted its A2400 Mobility Controller, featuring a modular, appliance-type platform. Modules included the vendor’s firewall, intrusion prevention system, and a 24-port switch that delivers PoE (power-over-Ethernet) to Aruba’s Access Points (APs). The system also works with other, 3rd-party APs, but full functionality requires Aruba’s APs.

■ **Cranite Systems**, which sent us its WirelessWall system. We ran the controller components of this software-only package on a Linux-based IBM server. Any 3rd-party APs are supported: We tested it with Cisco Aironet 1100 and 1200, and Buffalo AirStation G54 APs.

■ **Devicescape Software**, which provided its software-only Wireless Operations Center (WOC). Unlike the other products reviewed, Devicescape’s WOC is not an active controller. Rather, it is a passive, wireless-network management and monitoring package, which we ran on a Windows XP Pro laptop. (Linux is also supported.)

■ **Symbol Technologies**, which submitted its WS 5100 Controller, a fixed-configuration controller appliance. Symbol also included a new adjunct system, the W-IPS (Wireless Intrusion Prevention System), which augments the WS 5100 with extensive security capabilities.

As Table 1 shows, the packages are quite diverse. Aruba and Symbol address a nearly equivalent feature set—including many special voice over IP (VOIP)-handling capabilities, as well as rogue-AP detection and mitigation. Not unexpectedly, these two vendors’ offerings are also comparably priced.

Cranite’s WirelessWall system, while also an active controller, does not now support as full a range of features as Aruba or Symbol. Rogue-AP detection and mitigation, for example, can be addressed in the Cranite environment only via a third-party subsystem, which Cranite did not include for review with its package.

Devicescape’s software does an impressive job of *monitoring* the goings-on in a wireless network. And all third-party APs are supported. But the package does not actively *control* any aspects of the wireless network. For example, Devicescape will immediately notice and report the appearance of a new AP, and even provide signal strength and some directional information. But Devicescape takes no active measures to disable or contain a new or unauthorized AP—what the industry calls “rogue-AP mitigation.”

Due to this apples-and-oranges mix, the testers and editors agreed that a Best-in-Test scorecard, the hallmark of many *BCR*/Miercom reviews, would not be appropriate in this case.

Trends

Comparing the state of this year’s wireless control and security products with last year’s, some clear industry trends emerge:

■ Encryption is more advanced, more consistent and generally better done. The active controllers—from Aruba, Cranite and Symbol—all support wireless clients running 128-bit Advanced Encryption Standard (AES) encryption. This is fundamental to the latest and most secure wireless protocol, WPA2 (WiFi Protected Access, version 2—see this issue, pp. 14–16). The

Ed Mier is an industry analyst, consultant and author, and also founder of Miercom, a network consultancy and product test center based in Cranbury, NJ. Robert Tarpley is a test engineer at Miercom. They can be reached at 609/490-0200, or at ed@mier.com or rtarpley@miercom.com.

TABLE 1 Wireless Control Systems Tested

	Aruba Networks www.arubanetworks.com	Cranite Systems www.cranite.com	Devicescape Software www.devicescape.com	Symbol Technologies www.symbol.com
Product tested, version	A2400 Mobility Controller v2.5 24; AP-70 and AP-61 APs; xSec Odyssey Client v3.50 (1)	WirelessWall system v3.0.5e: Access Controller and Manager modules; and Client v3.3	Wireless Operations Center (WOC) v2.0.0.2	WS 5100 v2.0; Wireless Intrusion Prevention System (W-IPS) v6.6.2.1; AP 300; and Air Beam Safe client v2.0.3.36
Description	Modular appliance (controller) with vendor's APs; optional sensors; and optional PC-client software (1)	Software only (all modules ran on the same Linux-based, IBM server), and PC-client software (required)	Wireless-network <i>monitoring</i> software (tested on Windows based server; Linux also supported)	Fixed-configuration appliance (controller) with vendor's APs; optional PC-client software and wireless adapters
AP support	Aruba APs, or special models from Alcatel or Netgear, required for full functionality; can work with any APs	Works with any third-party APs; tested with Cisco Aironet 1100/1200 and Buffalo AirStation G54 APs	Works with any third-party APs; tested with Cisco Aironet 1100/1200 and Gateway 7001 APs	Symbol APs required; tested with vendor's AP 300s
Main functions performed	<ul style="list-style-type: none"> •Client authentication •Enhanced encryption •Rogue AP detection and mitigation •VOIP auto-detection and prioritization •QOS/prioritization by application •Firewall •IPS 	<ul style="list-style-type: none"> •Client authentication •Enhanced encryption, all done at Layer 2 •Rogue AP detection, mitigation via third party product (not tested) 	<ul style="list-style-type: none"> •Monitors and reports extensively on wireless activity •Immediately IDs new APs; provides some directional info 	<ul style="list-style-type: none"> •Client authentication •Rogue AP detection and mitigation (via optional W-IPS) •VOIP auto-detection and prioritization •Bandwidth management per AP •Session persistence while roaming •IPS (via W-IPS)
Price, U.S. list	\$8,995 for A2400 controller; \$295 to \$595 apiece for APs (several models offered)	Software license based on number of concurrent wireless clients; \$1,550 for 10, \$9,000 for 100; server not included; \$200 to \$500 apiece for third-party APs tested	\$990 for software for monitoring network of 10 APs (price based on number of APs)	\$2,180 for WS 5100 controller; \$5,995 for optional W-IPS system; \$345 for AP 300; \$625 per sensor (used with W-IPS)

(1) Optional xSec Odyssey client software, supporting 256-bit encryption, is offered in partnership with Funk Software. This client software is acquired from Funk Software.

main wireless protocols last year—including Static WEP, Dynamic WEP, and WPA version 1—all had notable security shortcomings, and have since generally fallen by the wayside.

■ **802.11a, b and g are now concurrently supported** in almost all wireless environments and equipment. Radio-transmission silicon has advanced so that 54-Mbps 802.11g is now widely available, with automatic fallback to, and concurrent backward support of, 11-Mbps 802.11b, as well as 802.11a. Some equipment tested last year still supported just 802.11b, with its performance and throughput limitations.

■ **Wireless is now accepted as secure-able**, thanks in large part to products such as these. Even the federal government has softened its “no wireless, no way, no-how” stance, due to wireless-security advances. A new Federal Information Processing Standard, FIPS 140-2, defines the basis for making wireless systems security-certifiable for government consumption. Cranite Systems touts its product's full FIPS 140-2 certifica-

tion. Aruba and Symbol both offer other models that are FIPS 140-2-certified, though the products they sent for our review were not.

■ **VOIP handling and QOS management**, long a sore point in wireless, is now being implemented. These are noteworthy new additions in Aruba's and Symbol's packages. Cranite does not yet support similar VOIP-prioritization or QOS/bandwidth-management capabilities.

■ **More restraint in neutralizing “rogue” APs.** We saw that last year, some systems could be set to automatically identify a new, unknown AP as a “rogue,” which they would then attack and disable—typically with sophisticated IP and other packet assaults. But this sometimes meant unintentionally disabling the APs of nearby businesses, or other isolated wireless networks, which posed no threat. Now, Aruba's and Symbol's packages, which provide rogue-AP mitigation, have added a definition called “interfering” AP. Added smarts now check whether a newly detected AP is actually passing traffic onto your wired network.

Intrusion prevention systems were a key security feature for several packages

If not, it can be classified as “interfering,” and then not summarily attacked.

Access Control

The security capabilities of the products reviewed are somewhat diverse, and in some cases subtly different. Consider authentication, for example, which means making sure wireless clients are authorized, and are who they say they are.

Confirming clients’ identities is straightforward with Cranite: for any supported device (PCs, PDAs) to gain access, the device must be running the vendor’s client software. Aruba doesn’t require that PCs run a particular client, but it has partnered with Funk Software, and supports Funk’s xSec Odyssey Client for enhanced security, including 256-bit, Layer-2 encryption. Similarly, Symbol offers its optional Air Beam Safe PC client.

Aruba, Cranite and Symbol all also support the 802.1x protocol, which is the standard for querying an external source, such as a RADIUS server, for authentication verification. Going one step further, Cranite’s and Symbol’s packages both also include integral RADIUS servers. Aruba also supports an added level of access control, where users first browser into a website. Another option, the Client Integrity Module, then enables a check of the client software—e.g., to be sure the latest version of anti-virus software is running.

Aruba and Symbol both offer additional features for defending the “wired” network from threats that may enter through wireless APs.

Aruba’s modular A2400 controller accommodates both firewall and IPS (intrusion prevention system) modules. Both were included in the system reviewed. Symbol’s package gains additional security capabilities via the separate W-IPS, or Wireless IPS—a separate server system. Besides intrusion prevention, this system works with special “sensor” units to detect and locate rogue APs, which can then be selectively dealt with.

Performance

We exercised several pertinent performance aspects of the wireless control systems (Table 2). Since Devicescape does passive monitoring only and cannot directly influence the behavior of the wireless network, we did not apply the same performance tests and metrics to Devicescape.

When deployed, the other packages all become critical network elements. So not unexpectedly, they all support high-availability topologies, where redundant controllers assure that a single failure will not shut down the wireless network.

In Aruba’s case, a hot-standby controller backs up the primary (called active-passive). Failure of the primary triggers a fail-over, which can be based on Layer 2 messages, or it can involve a full IP-layer re-routing, based on the Virtual Router Redundancy Protocol (VRRP). We found Aruba’s fail-over the fastest; wireless operations were fully restored in 14 seconds, on average.

Cranite runs two active, synchronized systems side-by-side (active-active). The system designated

TABLE 2 Performance of Wireless Controllers (1)

	Aruba Networks	Cranite Systems	Symbol Technologies
Product tested	A2400 Controller, Aruba AP-70 APs	WirelessWall system, AirStation G54 APs	WS 5100 Controller, W-IPS security system, Symbol AP 300 APs
High Availability, Redundancy Fail-Over			
High-availability configuration	Redundant controllers are active-passive; Layer 2 and Layer 3 (VRRP) fail-over modes	Redundant controllers are active-active; automatic recovery	Redundant controllers are active-passive; fail-over is permanent
Fail-over outage	14 sec. average	33 sec. average	50 sec. average
AP Recovery, Roaming Delay			
AP recovery time	37 sec. average	20 sec. average (AirStation APs)	40 sec. average
Roaming delay (hand-over time to second AP)	14 sec. average	17 sec. average	Less than 1 sec. average
VOIP Handling (2)			
R value rating: scale of 0 to 100 (3)	77.7	76.7	74.9
VOIP packet latency (avg); one-way	48.5 milliseconds	27.7 milliseconds	28.5 milliseconds
VOIP packet jitter (avg)	0.0 milliseconds	60.9 milliseconds	45.5 milliseconds

(1) A fourth product reviewed, Devicescape’s Wireless Operations Center, is a passive wireless-network management and monitoring system, and not an active control system.
 (2) VOIP metrics were reported by Veriwave’s VOIP over WLAN Suite v2.5. Wireless-to-wireless VOIP connections used SpectraLink NetLink e340 Wireless Telephones, G.711 vocoding. Call control was H.323 via a SpectraLink SVP Server.
 (3) “R value” is based on the ITU’s G.107 Recommendation, which defines an “E Model” for automatically assessing “mouth-to-ear” voice-transmission characteristics. It is similar to a MOS (Mean Opinion Score) rating, except on a 100-point scale, but similarly reflects loudness, delay and other impairments in the rating.

as secondary takes over for the primary in case of a failure. If and when the primary comes back up, control is usually then passed back automatically. Time to complete the fail-over: about 33 seconds, on average.

Symbol completely and permanently passes control from a primary to a hot-standby back up (active-passive). But in Symbol's case, the fail-over took 50 seconds, on average.

Where Symbol dazzled was in the speed that wireless connectivity is passed from one AP to another—called roaming delay, or hand-over time. The hand-over time was barely measurable with Symbol, and computer connections from wireless clients never dropped or timed out. Symbol credits this “session persistence” to its architecture: all packet control is centralized; the APs are essentially just Layer-1 radio antennas.

Aruba and Cranite delivered hand-over times of 14 and 17 seconds, respectively. These delays

are likely enough to sever many real-time communications sessions, such as VOIP. That is where Symbol's session persistence is a strong plus.

While Aruba and Symbol both provide automatic detection of, and prioritization of, VOIP traffic, Cranite does not. So we set up a test bed where we applied a respectable amount of VOIP traffic (12 concurrent conversations) and 1 Mbps of “background” (non-VOIP) traffic load per AP. The VOIP traffic, to and from 12 SpectraLink NetLink e340 Wireless Telephones, applied about 2 Mbps of bi-directional, G.711-encoded, real-time VOIP to the 802.11b portion of a single AP.

This traffic volume—about 3 Mbps—should not have overloaded the 802.11b capacity of any AP. And apparently it did not. Aruba, Cranite and Symbol all delivered fairly good quality VOIP, as measured by the Veriwave test system.

Using “R value” ratings (an ITU-defined voice-quality assessment akin to a MOS rating,

Roaming or hand-over time was an issue for two of the three vendors

Testing Wireless Control Systems

The test bed we used for reviewing these wireless control and management systems consisted of a “core” network, a “Site-A” network and a “Site-B” network, each a different subnet, interconnected via an Extreme Summit 48 backbone L2/L3 switch/router.

The core network included Windows 2003/Exchange 2003-based Domain Controller, DNS server and DHCP server. For 802.1x authentication of wireless clients we used Funk Software's Steel Belted Radius server, v5.0, on a Windows 2000 (SP4) Compaq Deskpro. The Steel Belted Radius worked in conjunction with Windows' Active Directory.

We reviewed each wireless package using a mix of Dell and Compaq wireless-client laptops. Two laptops ran Microsoft XP Pro; the others ran Windows 2000. We intentionally employed a different wireless adaptor in each laptop. These included: a Broadcom 54g Max-Performance 802.11g adaptor; a Proxim Orinoco Silver 802.11a/b/g adaptor; a D-Link AirPlus 802.11a/b/g adaptor; and a Linksys Wireless-G notebook adaptor, in a PC running the Funk Odyssey client v 4.0.

We used Veriwave's AP Management Performance Test Suite v2.5, running on an IBM R40 Win XP laptop to test AP performance. Test traffic was passed between Veriwave's WT 1210 802.11 a/b/g wireless Traffic Generator/Performance Analyzers and the APs under test. Each laptop client was required to be RADIUS-authenticated via 802.1x (using PEAP TTLS and MS-Chap v2 protocols), then all traffic was encrypted using “WPA TKIP.”

For checking VOIP performance, we used Veriwave's VOIP over WLAN suite v2.5 with a dozen SpectraLink NetLink e340 Wireless


Telephones. The wireless phones interconnected using H.323-based call control and SpectraLink's NetLink SVP Server.

All test traffic was verified using Network Chemistry's RFprotect Console ver 4.1.3, and three of the vendor's Intrusion Protection System 802.11 a/b/g Distributed Sensors.

AP recovery time was the time it took a “mistakenly unplugged” access point to “re-insert” in the network, regain connectivity with clients and begin passing wireless traffic again. This was measured both by a continuous ping stream, as well as the Veriwave test system.

For “roaming” hand-over time verification, we placed two of the vendors' APs 50 feet apart, one situated in Site A; the other in Site B. A laptop was wireless-connected to one AP, approximately 20 feet away. Then power was disconnected from that AP, forcing a handoff to the second AP, about 30 feet away. (Previous tests have shown us that walking with the laptop from one coverage area to the other opens up too many areas of variability.) A continuous Ping stream was run from the laptop to measure the elapsed “down” time it took for the roaming handoff.

For “rogue AP detection,” we inserted Avaya AP-3 AE and AP-7 access points into the network. These were undefined and unknown to the system under test. We then carefully noted each system's ability to identify, locate and issue a notification that the rogue APs had been detected. We also then exercised the abilities of the Aruba and Symbol systems to “mitigate” the connections and traffic of the rogue APs and clients connected to them. The Cranite and Devicescape systems do not now support



All the controllers allowed for good voice quality over the WLAN

except on a 100-point scale), the products delivered very good VOIP voice quality, ranging from 78 (Aruba) to 75 (Symbol). An R-value rating of 78 equates to a MOS score of nearly 4.0, generally regarded as “excellent” and telephone “toll quality.” IEEE documents equate a “70” R-value rating to a MOS score of 3.6, which it describes as “medium” speech-transmission quality, and an “80” R value to a 4.03 MOS score, which it terms “high” quality connections.

One-way VOIP packet latency and jitter were also measured. Aruba’s latency, about 48 milliseconds, was twice that of Cranite’s and Symbol’s—and 48 ms of added latency is not insignificant in a VOIP network’s delay budget. But in Aruba’s case, this appreciable latency is offset by virtually no measurable packet jitter.

As jitter increases, VOIP equipment has to buffer more voice packets to prevent loss. And this adds to the latency. So latency and jitter need to be viewed in combination. Cranite exhibited 61 ms of average jitter, which is considerable. Symbol’s was less, about 46 ms. So which delivers the best VOIP quality, all things considered? We accept Veriwave’s R-value rating: It’s pretty close, all things being equal, but it’s Aruba, by a nose.

The following profiles summarize our key findings and conclusions.

Aruba’s A2400

Aruba’s wireless-control package reflects the vendor’s leading role in the industry and years of refining and enhancing its product. Modularity—with available plug-ins including firewall, IPS, even 24-port PoE switch module—and management through a clean, consistent interface are clear advantages and differentiating factors.

And valuable new features keep coming. One of the latest is the “Remote AP.” This is special software that runs on any Aruba AP, and lets it securely communicate with an Aruba Mobility Controller (like the A2400) from anywhere over the Internet. Practical uses for remote hotel stays and temporary work sites are obvious.

There isn’t much to fault with Aruba’s management, either. All operations are accessed via a clean Web interface, although a CLI—not unlike Cisco’s IOS command line—is also offered. Both are secure and encrypted (the browser connection, for example, is HTTPS-based).

Aruba’s management interface is perhaps the easiest to use of the products reviewed. This is quite an achievement given the functional diversity and richness of the Aruba package; it’s all under one consistent, consolidated-management roof. Especially noteworthy are the pre-planning and site-survey tools for initial wireless deployments. You need only import a background map, and Aruba’s system tells you where to place your APs.

Also notable: Aruba’s legendary rogue-AP detection and mitigation, and the addition of QOS and auto-VOIP detection and prioritization.

What could be improved? The ability to graphically represent, in real-time, selected APs, their activity and client associations, would be a super addition to an already excellent package.

Cranite’s WirelessWall

The WirelessWall is software that runs on a Linux server, and requires that PC users run the vendor’s client. The package supports all leading APs and provides a very secure wireless environment. Cranite touts the fact that all the software components we reviewed are FIPS 140-2-certified. A key to Cranite’s security, according to the vendor, is that 128-bit encryption is done at Layer 2 from endpoint to endpoint—unlike IPSec-based VPNs, which encrypt at Layer 3, IP, from the client to the VPN gateway/controller.

The strong encryption and security of the WirelessWall client is not without a few administrative drawbacks. First, support is currently limited to Win2000, XP and later, Pocket PC 2002, and Win Mobile Pocket PC 2003 platforms. For other wireless endpoints, like the SpectraLink wireless phones, special policies—opening certain ports through the controller—have to be defined and applied. Finally, Cranite’s client software has to be directly installed on the client platform; it can’t be network-downloaded and installed.

New to the WirelessWall suite is a high-security remote-access kit—a special controller and client software, collectively called SafeConnect. The package reportedly extends the same Layer 2 encryption to clients that operate in WiFi hotspots or other insecure wireless environments, and supports secure connectivity back to the enterprise across the Internet.

While the Cranite system was not as functionally diverse as Aruba, it did feature an effective, Web-based management interface. Still, we feel it was not quite as granular or easy to use as Aruba’s. A noteworthy plus is that configuration changes to the Cranite system can be made in real-time (changes take effect immediately).

Strengths include: The Layer 2 encryption process reportedly thwarts such intrusion techniques as MAC address spoofing and man-in-the-middle attacks. Improvements? Integral rogue-AP detection and mitigation would be a valuable addition. (Currently this can be accomplished only via an added, third-party package, which was not a part of the system reviewed). And QOS management, including VOIP auto-detection and prioritization, is conspicuously absent.

Devicescape’s WOC

The Wireless Operations Center (WOC) is all about wireless monitoring and management, and can be considered the definitive help-desk tool for wireless-network monitoring. The software package works with any APs and can be deployed in any network. It operates passively and does not affect anything in the wireless network.

Setup is almost a non-issue. Once loaded and running, the WOC software auto-discovers the wireless network and lays it all out for you. We tested the 30-minute “discovery” process, involving a mix of vendors’ APs, and were impressed with the results. Signal strength and location information were excellent. You can also import your own floor plans and have the network superimposed on these, for more effective tracking.

The system features excellent graphics and maps, which can be made even more effective by importing your own background floor plans. On the wireless-topology map, you can right-click on any AP, and browse directly into that AP’s management, or drill down into any AP or wireless-client for more details. The system updates all information in real-time, and even shows each client’s security settings and type of encryption.

Users considering the Devicescape WOC should also get APs with SNMP support. The WOC is adept at interrogating SNMP agents and collecting valuable additional information, such as the management objects defined in the IEEE 802.11 MIB (SNMP management information base). The WOC can also serve as a Syslog alert-message repository for the many network devices that support Syslog reporting.

Some features of the WOC need to be seen to be appreciated. One is the animated Historical Scroll Bar. You set this feature to record wireless activity for the last hour, 8 hours, day or week. Then, via a scroll bar, you can graphically go back in time and see as clients came and went, as well as all other wireless-network events.

The WOC should be enhanced and expanded to include some of the active controls provided by the other packages we reviewed. At a minimum, we’d suggest wireless-client authentication, and then adding on from there. Also, while new APs that show up are immediately identified, we think rogue-AP identification could be better developed.

Symbol’s WS 5100 And W-IPS

Last but certainly not least of the wireless-network control packages reviewed this year was Symbol Technologies’. Two discrete subsystems are involved: the WS 5100 controller, a thin, self-contained, rack-mounted server appliance; and the Wireless Intrusion Prevention System, or W-IPS.

The W-IPS is the latest addition. It brings intrusion prevention, rogue-AP detection and mitigation, real-time signal-strength monitoring, and other security-oriented features to the wireless-control picnic. However, when tested, the two systems were managed via discrete and incongruent management interfaces. These need to be integrated. Also, for detecting rogue APs, Symbol’s own APs are used, but they need to first be reprogrammed for this change in roles. Aruba’s APs similarly do double-duty as APs plus rogue detection, but they already have the programming on board to perform in either mode.

A key advantage of Symbol’s is the aforementioned near-instantaneous roaming hand-over. The vendor says this is possible because the APs (Symbol’s own APs are required) are just antennas that funnel packets to the WS 5100, with no AP packet processing to slow things down. We laud this innovation, and the “session persistence” it provides to mobile users who routinely traverse multiple APs.

Otherwise, pound-for-pound, Symbol offers nearly the same breadth of options as Aruba. For example, Symbol, too, offers a security-enhancing PC software client, called Air Beam Safe, which features nicely settable configuration options.

Symbol is still catching up in a few areas, however. We feel a firewall capability is needed, for example. Otherwise, Symbol has to work on integrating the WS 5100 and the W-IPS. Behind a single interface they could truly be a dynamic duo.

Conclusion

WiFi continues to spread at a breakneck pace. And security and management of wireless environments, while still lagging, are catching up.

Four packages were reviewed. Three—from Aruba, Cranite and Symbol—actively control the wireless network, and all three perform some common functions, such as authenticating wireless clients before they are granted access to the wired environment. Symbol and Aruba deliver many more features, functions and capabilities.

A fourth system, from Devicescape, is a passive wireless-network monitoring system, but one that provides more complete and visually effective monitoring of the wireless environment than any other we have seen □

Wireless security and management are developing well

Companies Mentioned In This Article

Aruba (www.arubanetworks.com)
Avaya (www.avaya.com)
Buffalo Technology (www.buffalotech.com)
Cranite Systems (www.cranite.com)
Cisco (www.cisco.com)
Compaq (www.compaq.com)
D-Link (www.dlink.com)
Dell (www.dell.com)
Devicescape Software
(www.devicescape.com)
Funk Software (www.funk.com)
Gateway (www.gateway.com)
IBM (www.ibm.com)
Linksys, now a Cisco company
(www.Linksys.com)
NetworkChemistry
(www.networkchemistry.com)
SpectraLink (www.spectralink.com)
Symbol Technologies (www.symbol.com)
Veriwave (www.veriwave.com)