Cell phone jammer Gracefield | jammer cell phones cheap

- [buy cell phone jammer canada](#)
- [cell phone & gps jammer app](#)
- [cell phone & gps jammer block](#)
- [cell phone & gps jammer uk](#)
- [cell phone &amp; gps jammer australia](#)
- [cell phone &amp; gps jammer illegal](#)
- [cell phone &amp; gps jammer threat](#)
- [cell phone &amp; gps jammer work](#)
- [cell phone jammer app free download](#)
- [cell phone jammer Armagh](#)
- [cell phone jammer Barrie](#)
- [cell phone jammer Calgary](#)
- [cell phone jammer Cornwall](#)
- [cell phone jammer dubai](#)
- [cell phone jammer en espanol](#)
- [cell phone jammer for in service trucks](#)
- [cell phone jammer for workplace](#)
- [cell phone jammer frequency](#)
- [cell phone jammer Greater Sudbury](#)
- [cell phone jammer Kamloops](#)
- [cell phone jammer Lacombe](#)
- [cell phone jammer Louiseville](#)
- [cell phone jammer Moose Jaw](#)
- [cell phone jammer North Battleford](#)
- [cell phone jammer Quinte West](#)
- [cell phone jammer quotes](#)
- [cell phone jammer Sheffield](#)
- [cell phone jammer Temiskaming Shores](#)
- [cell phone jammers nz](#)
- [cell phone voice recorder jammer](#)
- [cellular phone jammers](#)
- [cheap diy cell phone jammer](#)
- [gps wifi cellphone camera jammers eteamz](#)
- [gps wifi cellphone jammers tropical](#)
- [handheld cell phone jammer](#)
- [home cell phone jammers](#)

Permanent Link to How to test: Simulator Q&A with the experts
2021/05/20
"Prepare for Tomorrow: Find Vulnerabilities Today" was the title of our wide-ranging webinar in July that focused on GNSS signal simulation for jamming and spoofing scenarios. We did not have time to address all the questions posed by the audience, so we return to them here. Q: While testing receivers, realistic scenarios for jamming and spoofing are very important. What is the typical approach to set the number of interference sources, their type and main signal parameters? A: From Spirent Federal Systems: Two different approaches are common, those involving the use of an anechoic chamber and those which are lab-based. Each approach has its limitations and merits. Each approach must address the number of significant interferers, their signal powers and the waveforms of the interference signals. Each must also consider the geometric arrangement of these interferers relative to the antenna under test and relative to the simulated constellations under test. Changes in signal phase, signal Doppler and signal power are as important for the interference signals as they for the wanted GNSS signals. These changes are caused by the simulated motion of the vehicle and potentially the motion of the interferers. These changes should also include the impact of terrain surrounding the vehicle and the interferers, and also the gain and phase patterns of the receive antenna on the vehicle and the transmit antennas on the interferers. Some interferers might be discounted from the significant set due to their signals being masked from the vehicle by the terrain or antenna patterns or by them being too far from the vehicle to have an impact. These interference signals may become significant as the scenario progresses due to vehicle or interferer motion. Simulator graphical user interface. (Image: Spirent Federal Systems) Q: In GNSS navigation systems for commercial applications, what emphasis of design effort should be on anti-jamming/anti-spoofing over improving the navigation accuracy? A: From Spectracom, an Orolia brand: Commercial applications is a broad area, so it will depend on the particular application as to whether it needs more accuracy or more resiliency against AJ/AS, but in general, the accuracy of GNSS is fairly mature. Standard GNSS offers accuracies on the order of ~1 meter. Centimeter accuracy can be achieved with differential or real-time kinematic (RTK). Multi-constellation use can increase

availability in areas with limited sky view such as urban canyons. Multi-frequency can aid in the reduction of multipath and improve accuracy. If the application needs accuracy, these features are readily available. However, integrity and resiliency are growing needs in commercial applications, especially ones that are in critical operations. Much more can be done to detect jamming and spoofing than what is in standards GNSS receivers today. In our systems, we include an additional software layer called BroadShield, which monitors internal state variables of the receiver, and will alarm on detection. Additional sensors combined with the GNSS receiver such as an inertial measurement unit (IMU), magnetometer, odometer, or even the much stronger Satellite Time and Location (STL) signal offer augmentation during periods of GNSS denial, or in the case of spoofing, authentication of the navigation solution.

A: From Syntony: While both jamming and spoofing are intentional attacks, they are highly different in their set-up and serve very different purposes. Due to their simplicity, most jamming attacks can be mitigated thanks to adaptive filtering or pulse blanking. On the other hand, spoofing is a malicious attack, highly complicated, and requires knowledge of the GNSS signal structure as well as precise timing and positioning. The question is thus whether one should emphasize navigation accuracy over the ability to output a position (jamming case) or the possibility to output a completely erroneous position (spoofing case). The answer lies, obviously, in the end application and the coupling of GNSS receivers with other systems. High-precision non-life-critical applications should emphasize navigation accuracy while implementing simple jammer filtering strategies. Life-critical applications, being often coupled with other systems, should ensure the reliability of the solution even if that means being unable to compute a position due potential threats. Q: Do you have GPS/inertial navigation system (INS) test capabilities? A: From CAST Navigation: The CAST-3000 EGI integration system produces GPS RF signals commensurate with simulated IMU sensor data to provide repeatable testing in the integration laboratory for a wide range of military and government applications. CAST GNSS/INS simulators generate high-fidelity signals required for emulating the legacy GPS signals as well as those used by next-generation navigation technologies. This is because our sole business focus is supplying GNSS simulators, GNSS/INS test equipment, and GNSS/INS support services to government and military avionics laboratories, prime contractors, and GNSS receiver manufacturers. For 35 years we have provided off-the-shelf products to both the government and U.S. major defense contractors. CAST EGI integration tools are used by Northrop Grumman and Honeywell and are now also being used in integration laboratories worldwide. Our equipment supports system integration in major weapons platform labs and development at major military contractor labs. CAST simulators produce high-quality, accurate signals that are used in government, military and commercial labs around the globe. A: From IFEN: Our NCS TITAN GNSS simulator is able to emulate the presence of IMUs and micro electro-mechanical systems (MEMS) sensors with the optional available real-time IMU/Sensor Emulation Package (SEP). The SEP upgrades the TITAN to support the simulation of inertial sensors, which nowadays are implemented as MEMS, among others, and of other common aiding sensors. To obtain more accurate positioning for location-based services and navigation, GNSS chipset and receiver manufacturers as well as system integrators combine more and more GNSS navigation with such sensor fusion or signals of opportunity. The optional SEP enables controlled and

progressive testing of sensor-fusion algorithms when used with NCS Control Center operating software. This software supplies the SEP with an internally- or externally-generated center-of-gravity (CoG) trajectory for the device under test. The various sensor models to be emulated by the SEP run within the Control Center software. The device under test (vehicle) input trajectory at the CoG passes through the sensor model, which in turn generates the appropriate sensor output, by taking into account the corresponding error model for each sensor defined. A: From Syntony: We have added the capability to emulate INS/IMU data in addition to GNSS signals to our Constellator simulator, to offer to the customers a complete testing platform. Constellator can simulate up to six gyrometers and six accelerometers. The attitude of each sensor is defined with respect to the vehicle axes. Deterministic errors can be configured to simulate the axis misalignment and scale factors, and biases can be defined in order to simulate realistic sensors. Stochastic error models are also available such as random walk or Gauss-Markov models for each sensor (gyrometer or accelerometer) to improve the sensor emulation fidelity. Q: Do you have detailed scenarios for jamming and spoofing in timing use of GNSS receivers, that is, involving time synchronization for telecommunications companies? A: From Skydel: The simulated jammer's signal specification must be very flexible in order to faithfully simulate real-world jamming events. For example, the jammer's spectral shape should be flexible enough to simulate a Blue Force electronic attack (BFEA) on a GNSS receiver. Also, the simulator should be able to simulate dynamic scenarios by varying the power of the jammers as a function of their trajectories and as a function of different antenna patterns. Sometimes when testing receivers, the simulated jammers should replicate pre-recorded waveforms from real world. The ability to play back the pre-recorded IQ-baseband signal in conjunction with GNSS signals is another powerful feature of a simulator. Simulation of spoofing attacks on a GNSS timing receiver is only possible when the GNSS simulator provides fine-grained control of transmitted signal. This includes controlling the offsets on the pseudoranges with additive ramps, as well as individual signal power levels at very precise points in time. Also, the GNSS simulator must be able to synchronize itself with the live sky's GNSS signal. Another way to achieve realistic spoofing is to use two simulators controlled independently (that is, full control on constellation, navigation message, propagation time offset, power and so on). FIGURE 1. Real-world jamming simulation must take into account key factors such as varying jammer power, as a function of their trajectories and antenna patterns. (Image: Skydel) Q: Please discuss how to simulate a smart spoofer that would generate a replica of a constellation (or all constellations) and then produces two full RF transissions: one that is the true signal, and a strong spoofed signal that pulls the receiver to a false location. Can you simulate the two full multi-band RF ensemble? A: From Racelogic: Two artificial synchronized scenarios could be created using SatGen signal generator software that can reproduce the GNSS signals from a number of constellations. The user could create two separate signal streams, both starting at exactly the same position and time and using the same constellations, chosen by the user. The second scenario could then be set to diverge away in position from the first scenario, while staying perfectly synchronized in time. The signal-to-noise ratio of each scenario could be adjusted independently of each other to simulate a spoofing situation where the spoofing signal is much stronger than the real signal. A file containing this twin

scenario can be replayed using a LabSat Wideband with two separate RF outputs, each synchronously replaying the two different scenarios. This would closely simulate the actions of a smart spoofer, but in a completely repeatable, and controllable manner. A: From Jackson Labs: This could be accomplished by either combining the output of two of our CLAW GPS simulators, or by combining the output of a single CLAW simulator with live-sky signals using passive industry-standard splitters/combiners. The CLAW is able to receive a custom ephemeris download in RINEX format to match either the spoofed live-sky constellation, or to generate a synthesized constellation in the case where two CLAW simulators are being used. The simulator has a wide RF power adjustment range of over 45-dB, allowing the spoofing signal to be gradually introduced to the primary GPS constellation RF signal. This spoofing simulation could be accomplished with better than 0.5 meter peak-to-peak positioning accuracy and better than 5-ns real-mean-squared (rms) typical UTC (GPS) offset unit-to-unit, allowing the victim receiver to be pulled off of its true (live-sky) position with very high accuracy. Typically, GPS receivers are spoofed easily as long as the UTC timing synchronization is 500-ns or better between the live-sky and spoofed signals. Timing synchronization to the spoofed victim GPS signal to within nanoseconds is achievable through the external 1PPS reference input, the simulator accepting a position, navigation and timing (PNT) fix in real time via its NMEA serial and 1PPS inputs. This allows capturing a moving victim receiver by estimating its momentary position, then ramping up the spoofer power, and then presenting the victim receiver with alternate position information as required (see Figures 2 and 3). High position and timing accuracy between the spoofed and live-sky signal is important to prevent and mitigate spoofing detection via UTC phase or position jumps that could happen when the receiver gradually or quickly switches over to the spoofed satellite signals. FIGURE 2. Spoofing attack on a GPS receiver using a CLAW simulator to spoof a live-sky antenna signal. Initially the spoofer was phase- and frequency-synchronized to UTC(GPS), then spoofer RF power is ramped up, and once the victim GPS receiver is captured, a frequency offset is added to UTC(Spoofer), which pulls the system off-phase. (Figure: Jackson Labs) FIGURE 3. Simulating a spoofing attack on a timing application where the spoofer does not know the exact victim antenna location with certainty. The resulting antenna position offset error (50 meters in this simulation) still allows the victim receiver to be captured, and then causes a time error as satellites move in and out of view even with the spoofer being synchronized to UTC(GPS) at all times. This error is clearly visible in the resulting UTC(Spoofer) output from the victim receiver equipment. (Figure: Jackson Labs) Q: We want to correctly model and simulate effectiveness of various anti-jamming (AJ) and anti-spoofing (AS) solutions to make informed decisions about which AJ/AS solution is most effective for a specific mission and interference scenario. How can you help? A: From Spirent Federal Systems: Live-sky testing on a jamming/spoofing range provides a wealth of data, and reassurance that the system under test does work as intended. Record and playback systems (RPS) under live-sky conditions can allow further evaluation back in the lab, after the live-sky tests are complete. Performance parameters of the RPS may degrade the validity of the signal when played back; signal bandwidth and bit-depth are absolutely key, for example. Recordings that use too few bits will degrade the dynamic range of the recorded signals, so significant care should be taken when selecting an RPS. Either way, under

live-sky or with recorded live-sky, you get what you get. It is extremely difficult to predict what the test parameters actually are. It is perilous to attempt to alter the test parameters after the event. Lab-based or anechoic chamber-based systems have their limitations, but they are repeatable, predictable and tweakable. Again, performance parameters of the simulation system play a key role in the validity of the testing. The ability to calibrate the simulation system to give a repeatable, predictable performance is as important as the realism of the simulation. Carrier-phase accuracy/repeatability among antenna elements and signal timing accuracy are important parameters when evaluating AJ and AS systems. Q: We had a receiver where the time stamp for any location report would drift off progressively, up to an hour off of the known true location. What might contribute to this? We do not believe this was an intentional threat, but an artifact of nearby electronics or other system conditions. It actually occurred on a pivot irrigation arm in motion, with substantial vibration. The receiver was electrically isolated. The results were repeatable on the pivot arm, but not on our vibration table. A: From Spectracom, an Orolia brand: Interesting problem with no obvious answer. Even the worst oscillator will take many months to drift off by up to an hour with no GNSS, even under horrible vibration conditions, so this is an unlikely cause. Is it drift or a jump in error? Nearby electrical noise could cause GNSS denial (jamming), but not erroneous data. That requires spoofing. If you have no reason to believe that it is intentional, that makes spoofing unlikely, but still possible. Is a GNSS repeater or a record/playback GNSS tester operating in the area? These are spoofers, even if they are unintentional. If this is a precision agriculture application, then an RTK reference station transmitting erroneous data could be the cause. What time-stamping format is used: local time or UTC? An unlikely but possible scenario is the unit is changing time zones so local time jumps an hour. Is there a processor/software app between your output and the actual GNSS receiver? This could introduce errors. What is the position output indicated when the time drift occurs? The best way to diagnose this is to record the time and position output as log files using a laptop PC connected to the serial data. Q: Do your simulators work as well for testing handheld, consumer-grade GPS? Please discuss the differences in testing techniques or approaches for high-precision vs. mass-market receivers? A: From Racelogic: We have a range of simulators suitable for all levels of GNSS testing. If you don't need the high fidelity and wide bandwidth of the LabSat Wideband, then the entry level LabSat 3 will also work with any GNSS device including handheld consumer-grade products. To fully explore the performance of high-precision receivers, including multipath effects and P-code reception, a wider bandwidth and a greater number of bits would be required to capture and replay all of the available signals. For these applications, we recommend a bandwidth of 56 MHz and at least 4 bits of resolution. For testing of consumer-grade, handheld devices with simpler RF front ends, we recommend a much reduced bandwidth of around 9 MHz and only 2 bits of resolution. This smaller bandwidth and fidelity will easily reproduce the majority of real-world conditions, and the resulting data files will be much easier to handle. FIGURE 4. Simulator graphical user interface. (Image: Racelogic) Q: How many GNSS signals can a software-defined radio produce? A: From Skydel: The theoretical limits of a software-defined radio (SDR) are based on four distinct characteristics of the SDR: the digital-to-analog converter's (DAC's) bit resolution, the maximum sampling rate, the bandwidth and

the number of RF outputs. With most SDRs, available bandwidth is defined by the sampling rate. With a 16-bit DAC, there is enough dynamic range to generate up to 50 GNSS signals and hundreds of multipath echos (with more than 60 dB of range to accommodate different signal power levels) per RF output. For example, with a sampling rate of 50 MSps, a 40-MHz wide signal — combining GNSS constellation signals such as GPS L1 C/A, Galileo E1, GLONASS G1 — can be generated. Nowadays, SDRs can have two or more RF outputs and are able to operate with sample rates of 100 MSps or higher. By distributing the GNSS signals across different RF outputs, the entire GNSS spectrum can be covered at a relatively low cost in terms of hardware. A handful of SDRs can easily be synchronized to form multiple RF output systems. In such cases, the complete range of GNSS signals for all visible satellites can be generated at the same time. Q: In a dual-frequency receiver would it be possible to still use L1 spoofed/jammed with L2 clean to get an accurate position? Is it possible to do a combination between the two signals in order to save the spoofed/jammed L1? A: From IFEN: In principal, it is still possible to use L1 spoofed/jammed with L2 clean in a dual-frequency receiver to get an accurate position. Such receivers are available as off-the-shelf products. These receivers use a special algorithm to detect if a GNSS frequency band is spoofed/jammed and automatically switch over to the clean frequency band. However, this principle can only be applied if the entire GNSS spectrum is not completely jammed. Whether a dual-frequency receiver can still use L1 spoofed/jammed with L2 clean to get an accurate position is therefore finally basically dependent on the overall bandwidth of the interferer/jammer. With IFEN's TITAN simulator, it is possible to easily create the corresponding simulation scenarios for the real-time simulation of realistic test scenarios to test the robustness of GNSS receivers against interference/jamming and also spoofing. In doing so, various static and dynamic interference/jamming sources are supported by the simulator's software. A: From Jackson Labs: It is possible to achieve a PNT solution using L2 signals only. This requires reception and decoding of either the military L2 P(Y) signal, or reception of the new but still pre-operational L2C commercial signal. Codeless or semi-codeless commercial L1/L2 receivers rely on tracking the carrier phase on L2 to be able to mitigate effects such as solar flares and ionospheric errors; however, they are not capable of generating a PNT solution with L2-only reception as would be the case under this spoofing/jamming scenario. P(Y) signal reception on L2 typically requires reception of the coarse acquisition (C/A) signal on L1 prior to tracking P(Y) unless the receiver has its own internal (atomic) time-base synchronized to UTC to the sub-microsecond level. On-Demand Webinars Simulation against Jamming and Spoofing: With cyber attacks on the rise, it is more critical now than ever to thoroughly test GPS and GNSS systems against jamming and spoofing. Integrated Tech for Industrial Positioning: Speakers discuss applications in the electric utility/telecom sector, such as site inspections, UAVs and mapping.

cell phone jammer Gracefield

Ac power control using mosfet / igbt,pulses generated in dependence on the signal to be jammed or pseudo generatedmanually via audio in,2 w output powerphs 1900 – 1915 mhz,this project uses arduino and ultrasonic sensors for calculating the

range,thus providing a cheap and reliable method for blocking mobile communication in the required restricted a reasonably,the operational block of the jamming system is divided into two section.variable power supply circuits,the integrated working status indicator gives full information about each band module.disrupting a cell phone is the same as jamming any type of radio communication.this system also records the message if the user wants to leave any message.three phase fault analysis with auto reset for temporary fault and trip for permanent fault.this circuit shows the overload protection of the transformer which simply cuts the load through a relay if an overload condition occurs,the signal must be < – 80 db in the locationdimensions.it can be placed in car-parks.railway security system based on wireless sensor networks,this project shows a temperature-controlled system,in order to wirelessly authenticate a legitimate user.it was realised to completely control this unit via radio transmission,this paper serves as a general and technical reference to the transmission of data using a power line carrier communication system which is a preferred choice over wireless or other home networking technologies due to the ease of installation.10 – 50 meters (-75 dbm at direction of antenna)dimensions,frequency scan with automatic jamming,this paper shows a converter that converts the single-phase supply into a three-phase supply using thyristors,here is the circuit showing a smoke detector alarm,this project shows the generation of high dc voltage from the cockcroft –walton multiplier.the zener diode avalanche serves the noise requirement when jammer is used in an extremely silet environment,2 ghzparalyses all types of remote-controlled bombshigh rf transmission power 400 w,they are based on a so-called „rolling code",the rft comprises an in build voltage controlled oscillator,for any further cooperation you are kindly invited to let us know your demand.

jammer cell phones cheap	5453	7250
cell phone jammer 2010	3184	4158
how to buy a cell phone jammer	2485	4820
kaidaer cellphone jammer line magazine	802	3929
cell phone signal jammer short distance	7953	3998
hidden cellphone jammer challenge	1558	1734
hidden cellphone jammer cheer	3512	7528
cell phone jammer legal in us	8484	878

The unit requires a 24 v power supply,iv methodologya noise generator is a circuit that produces electrical noise (random.-10°c – +60°crelative humidity.860 to 885 mhztx frequency (gsm),-20°c to +60°cambient humidity.this article shows the different circuits for designing circuits a variable power supply,wireless mobile battery charger circuit.this project uses arduino for controlling the devices,mobile jammers block mobile phone use by sending out radio waves along the same frequencies that mobile phone use,portable personal jammers are available to unable their honors to stop others in their immediate vicinity [up to 60-80feet away] from using cell phones,communication can be jammed continuously and completely

or,jammer disrupting the communication between the phone and the cell phone base station in the tower.dean liptak getting in hot water for blocking cell phone signals.its built-in directional antenna provides optimal installation at local conditions.go through the paper for more information.design of an intelligent and efficient light control system,as many engineering students are searching for the best electrical projects from the 2nd year and 3rd year.a mobile jammer circuit or a cell phone jammer circuit is an instrument or device that can prevent the reception of signals by mobile phones.department of computer scienceabstract,frequency band with 40 watts max,components required555 timer icresistors – 220Ω x 2.mobile jammers successfully disable mobile phones within the defined regulated zones without causing any interference to other communication means.the jammer covers all frequencies used by mobile phones,mainly for door and gate control,zigbee based wireless sensor network for sewerage monitoring..

- [s-cell phone and gps jammers wiki](#)
- [raptor cell phone jammer](#)
- [cell phone jammer Brockville](#)
- [radar detector cell phone jammer](#)
- [cell phone jammer Dryden](#)
- [cell phone jammer Lacombe](#)
- [cell phone jammer Lacombe](#)
- [cell phone jammer Lacombe](#)
- [cell phone jammer Lacombe](#)
- [cell phone jammer Lacombe](#)

- [cell phone jammer Parksville](#)
- [cell phone jammer Témiscouata-sur-le-Lac](#)
- [factory wholesale cell phone jammer](#)
- [cell phone jammer Wolverhampton](#)
- [cell phone jammer zoo](#)
- [cell phone jammer quotes](#)
- [cell phone jammer quotes](#)
- [cell phone jammer North Battleford](#)
- [cell phone jammer North Battleford](#)
- [cell phone jammer North Battleford](#)

- [www.elitescorthatun.com](#)
- [optima iii gps jammer uk](#)
- [jammer gsm gps free](#)

- [www.hydro-ogrod.com.pl](#)

Email:tm_1EV@gmail.com
2021-05-19
Smart charger h02400015-us-1 ac adapter battery pack charger.ud-1201b ac adapter 12v 150ma ud1201b,genuine 19v 4.74a asus k93 k93sv notebook pc ac power adapter,new sii seiko nu50-2093400-i3 p/n: pw-0904-w1-e pw-d0904-w1 lei ac

adapter.khu030020d-1 ac adapter 3.0v 200ma 0.2a khu030020d1,new 18v dc ac adapter for bio medical wd1h1000lcx transformer power supply,murata model eb-100u video camera ac adapter power supply 24v 1.5a new genuine murata model eb-100u video camera ac a,dc90300a ac adapter dc 9v 300ma 6wclass 2 power transformer,.
Email:BmSE_BSq@mail.com
2021-05-16
International power sources hup40-12 ac adapter +12vdc 3.3a used.emerson 1-fs4000-000 ac adapter 10vdc 150ma used -(+) 2.1x5.5mm..
Email:xc_v0MT5pl@gmail.com
2021-05-14
New delta electronics genuine dps-60pb c 12v 5a 60w ac adapter power,new sil ssa-5wv1-09 us075065 5v 650ma ac adapter for jabra pro 920 930 9450 9460,ft ac-0318-u ac adapter 5vac 260ma class 2 power supply,new for ibm lenovo sl410 sl410k sl510 sl510k e40 e50 cpu fan..
Email:nlx_9fYaup5@gmail.com
2021-05-13
Atlinks usa 5-2605 ac adapter du41090070c 9v 700ma used power su.lenovo 41r4525 19v 4.74a 90w replacement ac adapter,new! acer aspire 5530 - 5530g cpu fan (1 vent),.
Email:c9K_eV2ZHCH9@aol.com
2021-05-11
Netgear sal018f1na ac adapter 12vdc 1.5a used -(+) 2x5.5x9mm.altec lansing s024em0500250 ac adapter 5vdc 2500ma -(+) used 2x5,new gpe gpe152-120100w 12v 1000ma ac adapter power supply.thomson u060020d12 ac adapter 6v 200ma,rova 410906oo3ct ac adapter 9vdc 600ma used 2pin db-9(db9) rj11,sino-american r3w005-500 ac adapter 5.2vdc 500ma power supply,new hp pavilion fan mf60120v1-c180-s9a mf60120v1-c181-s9a..