

The Communication Process of PowerChute® Network Shutdown

Abstract

The APC Network Management Card and PowerChute Network Shutdown allow remote shutdown of multiple systems from a single UPS over a network. Awareness of network availability, scalability to large numbers of clients, limited impact on network traffic, and a reliable architecture are of prime concern for such a system. This paper describes how the Network Management Card and PowerChute Network Shutdown communicate with each other to address these concerns.

Background

Historically, many UPS installations were on a one server to one UPS basis, which drove communications over dedicated serial lines. Two trends have been changing this dynamic: re-centralization of servers and more reliable networking technology. As customers power multiple servers or workstations from one UPS more often, reliable network-based shutdown capability is increasingly critical in the event of an extended power outage. This technical note outlines various challenges to reliability and the approaches that are necessary to ensure safe shutdown.

Network Availability

Availability of the network is obviously a key requirement for network-based shutdown solutions. Power protecting the network equipment itself such as switches, routers, and hubs is essential to ensure communications in the event of a power outage. Despite power protection, if the network should become unavailable (for whatever reason), the shutdown clients on the protected servers or workstations must be able to detect this and take appropriate action. Since many customers implement network shutdown within a single segment, the Network Management card performs **UPS Status Update** within the local network segment (via a UDP broadcast). It is important that this be implemented in a fashion that does not generate an undue amount of network traffic. UPS Status Updates include very small amounts of information, are limited to a few hundred bytes once every 20 seconds, and are limited to the local segment; therefore, it does not adversely affect network traffic. If the PowerChute Network Shutdown clients do not receive a UPS Status Update within 1 minute, they can be configured to respond by automatically shutting down their systems (under the assumption that the network is no longer available).

The APC Network Shutdown solution also takes into account that customers have varying network architectures and some may wish to power systems that are not on the same network segment as the Network Management card. To accommodate this, once a minute the Card sends an **Individual Client Notification** (via a "Unicast") to each client IP address that is outside of the local network segment. Since Unicasts are not guaranteed to occur, PowerChute Network Shutdown includes a **UPS Status Propagation** feature. All PowerChute Network Shutdown clients in the target segment that receive an individual

notification will attempt to relay a **UPS Status Update** to other clients within their segment, provided a UPS Status Update has not yet occurred. Once the first client successfully sends a UPS Status Update, the other clients are barred from sending one. This ensures that only one broadcast will occur in the segment (limiting network traffic), and ensures redundant communication (essentially using the PowerChute Network Shutdown clients as proxies for the Card).

Authentication

Communications between the Card and PowerChute Network Shutdown uses an MD5-based **authentication** scheme. This scheme ensures the password phrase is never compromised, that the UPS Status Update originated from the Card, that the UPS status has not been modified, and that the UPS status is not being "replayed". Likewise, shutdown signals from the servers are also validated in this manner. This scheme *does not encrypt* any UPS status data, prevent most denial of service attacks, or guarantee that a brute force attack will fail to determine the password phrase. A well configured firewall and solid security policy is integral to the security of any network.

UPS Turnoff

The last step for a UPS after shutting down all attached systems is to turn itself off (to allow for a minimum level of charge to ensure protection when power returns, for instance). The Network Management Card's **Client Shutdown Coordination** feature proactively coordinates the shutdown of all attached clients before allowing the UPS to power off, ensuring graceful shutdown has occurred and avoiding the scenario of ungracefully dropped loads. Additionally, if there is a requirement to order shutdown of various clients, PowerChute Network Shutdown allows individual delays for each client.

Environment Changes

Any complex system that requires initial configuration should take into account that customer's requirements change over time. PowerChute Network Shutdown's **Configuration Conflict Detection** feature automatically detects situations where the UPS runtime has decreased (for instance, due to additional servers being installed and protected) to a point shorter than the individual client shutdown delays.

Conclusion

Robust communication and a robust architecture are key for any network-based shutdown solution. The approach of Individual Client Notification, Redundant Status Propagation, Authentication, Shutdown Coordination, and Configuration Conflict resolution ensure reliable, coordinated behavior of all affected nodes in the event of an extended power outage, thus increasing availability and time-to-recovery.