[APPLICATION NOTE #20]

The Communications Process of PowerChute^{TM} Network Shutdown

By Sarah Jane Hannon

ABSTRACT

PowerChute^{TM} Network Shutdown software works in conjunction with the UPS Network Management Card (NMC) to provide graceful, unattended shutdown of multiple computer systems over a network. Understanding how UPS information is sent over the network as well as an awareness of network availability, scalability to a large number of clients and a reliable architecture are essential to ensure system protection and availability.

This Application Note describes how the UPS Network Management Card and PowerChute Network Shutdown communicate with each other and outlines some reliability challenges and recommended steps to ensure system protection.

CUSTOMER BENEFITS

- Graceful network-based shutdown
- Sequenced server shutdown
- Integration with VMware & Hyper-V
- Support for virtual clusters
- Virtual machine migration/shutdown
- Intuitive PowerChute setup wizard
- Browser accessible
- Command file integration
- Redundant & Parallel UPS support
- Event logging
- HTTPS communications
- IPv6 support

How UPS information is sent over the Network

The UPS Network Management Card (NMC) provides an interface between the UPS and your network. The NMC[1] sends UPS information to PowerChute Network Shutdown via UDP packets which are limited to a few hundred bytes.

The condition under which the packet is sent determines its frequency:

a) 'Normal UPS Status' packet - sent every 25 seconds.
b) 'UPS Status Update' packet - sent immediately if the UPS goes on battery.

UPS information is sent over the network in the following manner:

- The NMC in the UPS has a list of IP addresses (up to 50)[2] of computers running PowerChute Network Shutdown. This NMC broadcasts UPS information on the local network segment (the segment on which the UPS Network Management Card resides), as long as it has at least one IP address on its list that is on the local segment. It will also send unicast messages to each IP address on its list that is on a different network segment.

[1] The UPS Network Management Card (NMC) has an IP address and is accessible via FTP, Telnet, SSH, SNMP and the Web.
[2] Please see also App Note #101 (AN-101) "PowerChute Network Shutdown with more than 50 computers connected to one UPS".

- While Broadcast messages only reach the local network segment, unicast messages are sent to provide connectivity to PowerChute Agents outside the local network segment.

- Each PowerChute Network Shutdown Agent that receives a unicast message from the UPS NMC will rebroadcast that message on its local network segment. Other PowerChute computers on that segment will receive this broadcast message, even if they received a unicast message.

- A PowerChute Agent will not rebroadcast the message if it has already received a broadcast message from another PowerChute Agent. This is done to reduce the amount of broadcast traffic on a network segment. [Note: If there are 3 PowerChute Agents in Segment Two, and they each receive a Unicast packet, they **could** all rebroadcast it in their segment depending on the timing of when they received it. To stop this, it checks if it has already received it as a broadcast, and only rebroadcasts if no one else has yet].

Recommendation: As all PowerChute Agents on the same local network segment as the NMC will receive broadcast updates and every Agent that receives a Unicast message sends a broadcast message within its local segment; it's recommended to reduce the number of Agents in each segment to limit the amount of broadcast traffic. The minimum requirement is one PowerChute Agent per segment but as the Agent has to be running to rebroadcast to other Agents, registering a few Agents to the NMC per network segment provides a more robust system.

***Figure 1** – Broadcasts and Unicasts*

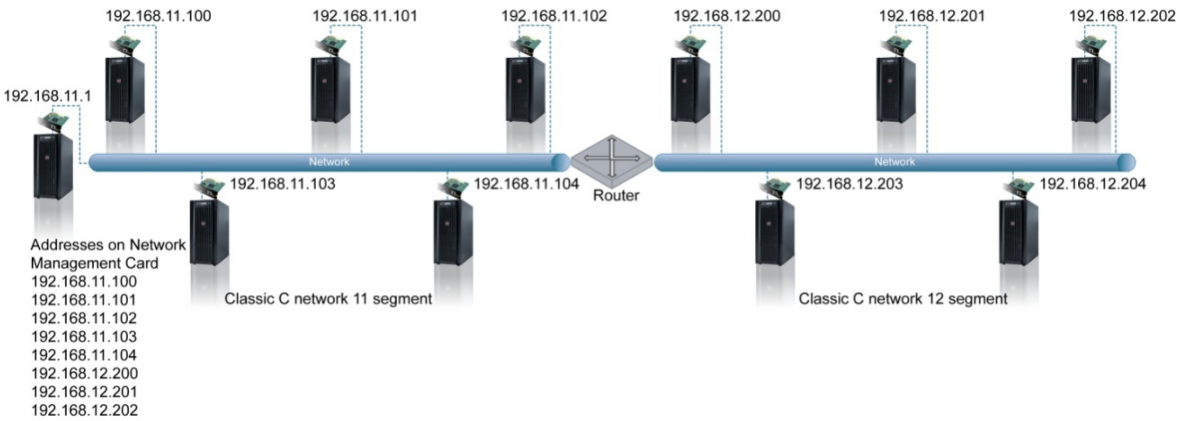
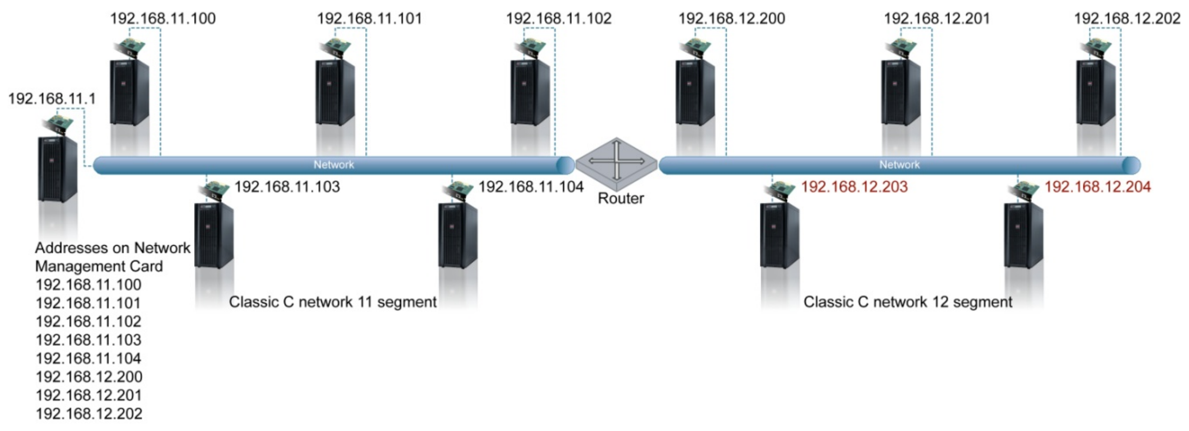


***Figure 1** All 11 segment computers (192.168.11.xxx) will receive broadcasted UPS data while PowerChute computers on the 12 segment (192.168.12.xxx) will receive unicasted UPS data every 25 seconds.*

An Individual Client Notification packet (MACONFIG packet) is sent by each NMC every ~100 seconds. The propagation of this packet to PowerChute Agents through various network segments is managed the same way as the UPS Status Update Packets; only the purpose of the packet is different. This packet contains a list of all IP addresses on the NMC thereby identifying which PowerChute Agents are registered.

Note: While all PowerChute Agents can be configured to protect their systems in the event of an extended power outage, only those Agents that receive this MACONFIG packet can issue a UPS Turn Off Command.

Figure 2 – PowerChute Packet Propagation



*In **Figure 2**, computers 192.168.11.100, 192.168.11.101, 192.168.11.102, 192.168.11.103, and 192.168.11.104 receive broadcast information from the UPS Network Management Card.*

Computers 192.168.12.200, 192.168.12.201, and 192.168.12.202 will receive unicast information containing the UPS data from the UPS Network Management Card.

Computers 192.168.12.203 and 192.168.12.204 will receive re-broadcasted data from PowerChute computers on the 12 segment only. These computers do not receive unicast information from the UPS Network Management Card (as they are not registered to the NMC).

Network Availability

Power protecting network equipment such as switches, routers, and hubs is essential to ensure communications in the event of a power outage. Despite power protection, if the network becomes unavailable (for whatever reason), the PowerChute Network Shutdown Agent on the protected servers must be able to detect this and take appropriate action. PowerChute Network Shutdown expects a **UPS Status Update** once every 25 seconds so if the Agents do not receive a UPS Status Update within 1 minute, if required, they can be configured to respond by automatically shutting down their systems (under the assumption that the network is no longer available).

Authentication

The communications mechanism between the NMC and PowerChute Agents uses an MD5-based authentication scheme (MD5 Media Access Control hash), which has the goals of:

- Ensuring that the password is never sent in plain text.
- Proving that the sender of a message is an authentic user as only those with knowledge of the password phrase can send valid messages.
- Detecting if a message has been tampered with in transit.
- Detecting if a message is being replayed.

This mechanism does not guarantee:

- That all data is encrypted.
- That a brute-force attack will fail to determine the password phrase.
- Prevention of most Denial of Service attacks.

A well configured firewall and solid security policy is integral to the security of any network.

PowerChute Shutdown Coordination

The UPS Network Management Card's **Client Shutdown Coordination** feature uses the longest time required by the registered PowerChute Agents as the delay when coordinating a safe system shutdown to ensure all attached PowerChute Agents have safely shut down their systems. Additionally, PowerChute Network Shutdown allows individual delays for each client to sequence the shutdown of various Agents if required.

PowerChute Network Shutdown's **Configuration Conflict Detection** feature automatically detects situations where the time required for any PowerChute Agent to shut down is greater than the 'Maximum Required Delay' (UPS without Outlet Groups) or the 'Power Off Delay' for the UPS Outlet Group the PowerChute Agent is connected to. If the time required to shut down PowerChute is greater than the Maximum Required Delay/Power Off Delay, then a Runtime Exceeded Event is triggered and the PowerChute Agent requests the NMC to increase its delay accordingly.

The Maximum Required Delay/Power Off Delay is set to the same value as the 'Low Battery Duration' on the NMC by default. This is usually 2 minutes. When the NMC is reset or Force Negotiation is applied, the Maximum Required Delay/Power Off Delay for the Outlet groups is re-set to match the Low Battery Duration value. These updated values are included in the UDP status packet and PowerChute Network Shutdown will request an increase of these values if necessary.

Recommendation: If this Runtime Exceeded Event occurs, it's advisable to increase the Low Battery Duration Threshold on the NMC to greater than the Maximum Required Delay/Power Off Delay so that all PowerChute Network Shutdown Agents have sufficient time to safely shut down before the UPS battery is exhausted.

Additionally, if you change the Low Battery Duration on the NMC you should always apply '**Force Negotiation**' (otherwise the Maximum Required Delay/Power Off Delay will remain unchanged) on the NMC so that PowerChute Agents can check their required shutdown time against the updated Delay values in the UDP packet and request an increase in these delays if necessary.

Conclusion

Robust communications and a robust architecture are essential components for any network-based shutdown solution. Individual Client Notification, Authentication, Client Shutdown Coordination, and Configuration Conflict Detection ensure reliable, coordinated behavior of all impacted PowerChute protected computers in the event of an extended power outage, thus increasing availability and reducing time-to-recovery.