NEW!

TECHNICAL FACT SHEET

Remote Environment Management

Advanced Out-of-Band Management for the Resilient Edge

Lantronix has the LM-Series for the most advanced network automation and security available in an out-of-band product.

CONNECTIVITY OPTIONS

- RS-232 – the most reliable dedicated access method. RJ-45 wired as DCE to connect over standard CAT-5 patch cables to most networking equipment (adapters available)
- Console server option – SSH or RFC2217 (Serial over Telnet) TCP socket connection to a console server port that is already connected to a managed device
- SSH or Telnet connection to managed device – connect to device's management interface over TCP sockets
- Serial and TCP port forwarding back to the local workstation, enabling the use of vendor provided RS-232 tools and other interfaces
- HTTP(S) – ability to query an http interface to query web pages of devices; parse the results and trigger other HTTP(S) GET and POST types
- SSH – VTY Virtual Ports establish a secure connection using simply an SSH TCP port opposed to a dedicated serial or ethernet connection. These are useful for virtual controllers, devices like service processors or port-forwarding of the GUI and other application ports.

CONFIGURATION MANAGEMENT

- Managed Device OS Policies – Users can upload and define a standard OS image for a given managed device make and model in the Control Center to create an OS policy. When defined for a group in the Control Center inventory tree, this policy will automatically download the standard OS image for a given make and model from the Control Center to all Local Manager device ports in that inventory group and in its subgroups that match the make and model and store it as a named OS with the name "standard." The policy can be configured to alarm on ports that are configured with an Uplogix advanced driver that pull the OS from the managed device for the case where the current OS on the managed device does not match the standard OS defined in the policy for that managed device.
- Cisco Startup Config Recovery with Automatic OS update (OS Policies) – Users can define an OS policy for a Cisco IOS/IOS-XE device. If that device is replaced, our Cisco advanced driver functionality will ensure that the new device is loaded with that last known good current startup configuration and that the device is running on defined standard OS for that Cisco make and model.
- Automatically Backup And Restore Cisco IOS VLAN Database – The Uplogix Cisco IOS advanced driver supports backing up the VLAN database for Cisco switches and restoring the VLAN database during a configuration recovery procedure (such as a switch replacement). The driver will automatically schedule a job to back up the VLAN database for a port that is configured on this release. A single or recurring job can be scheduled to backup the VLAN database on ports that were already configured to manage Cisco IOS switches.
- Automatically retrieve and store device OS – includes six named versions, the current, previous, and candidate versions per managed device
- Automatically retrieve and store device startup configuration files – includes five named versions, the current, previous, candidate and up to 19 archived versions per managed device
- Automatically retrieve and store device running configuration files – includes five named versions, the current, previous, candidate and up to 19 archived versions per managed device
- Support scheduled recurring jobs that automatically retrieve the current OS, startup and running configuration files per managed device

LANTRONIX

- Support scheduling a job to update a startup or running configuration file for one or multiple devices across the network, where the device configurations to be updated are specified through advanced filtering that operates on hierarchical groups, Local Managers, managed devices, device make, device model, OS name and the OS version
- Support scheduling a job to upgrade the operating system for one or multiple devices across the network where the devices to be upgraded are specified through advanced filtering that operates on hierarchical groups, Local Managers, managed devices, device make, device model, OS name and OS version
- Display configuration changes made during a user session to a managed device when the session is complete so the user can confirm the changes are accurate and commit the changes.
- Automatic rollback of configuration changes made during a user terminal session to a managed device if the session times out and user does not commit changes
- Display configuration changes made during a user terminal session to a managed device and enable the user to automatically rollback the changes
- Support bare metal restore on a replacement device by installing OS and configuration files
- Support the ability to independently recover a configuration on a managed device for the case where the configuration is corrupted

EASE OF USE AND DEPLOYMENT

- Zero Touch Local Manager Deployment – New, factory fresh Local Managers can now use DHCP and/or DNS to automatically find and register themselves with the Uplogix Control Center (UCC), allowing network engineers to easily provision them via the UCC, eliminating the need to stage configurations or send technical personal to remote sites for deployment purposes.
- Automatic Configuration of NTP and DNS Servers via DHCP – The Uplogix Local Manager will automatically set primary and secondary NTP and DNS servers per those delivered in a DHCP Offer if NTP and DNS servers are not already configured. Any NTP and DNS servers configured via the CLI or the UCC will override server information delivered via DHCP.
- Automatically Detect and Configure Internal Modems – Uplogix will automatically detect and configure an internal modem if one is present – this includes setting the modem make, model and serial bit rate for all internal modems. PPP settings will be automatically configured for the case of a cellular modem.

DEVICE MONITORING

- Regularly monitor a device and automatically restore the startup configuration and standard/certified OS for the device if the device is replaced (due to RMA) or found without its configuration
- Regularly monitor a device and automatically recover the device if the OS is missing or corrupted, or if the device is stuck in a boot loader state
- Monitor and save device CPU and memory utilization
- Monitor and save device interface status and statistics
- Monitor and save device log messages
- Monitor and save power on self test (POST) messages when managed device powers up
- Monitor commands typed by user in a terminal session
- Monitor device connectivity using ICMP Ping

SERVICE LEVEL MONITORING

- Represent interfaces on multiple networks, QOS tagged, performed just as end user devices
- Regularly monitor network based services to validate availability
- Execute tests ad-hoc for troubleshooting

- Available types include Voice, Web Transaction and TCP:
  - Voice – executes a synthetic call using similar codecs of humans speaking phonetically balanced "Harvard" sentences – provides 47 RTCP elements.
  - Web Transaction – executes a HTTP(S) transaction including DNS lookup, SYN/ACK round trip time, time to first/last byte, HTTP result codes, and includes the ability to parse the first 1000 bytes for a keyword or phrase
  - TCP Port – Executes a SYN/ACK round trip to measure network latency and availability for any TCP-based application

FLEXIBLE AUTOMATION

- Support a customizable rules engine that takes action when collected data meets specified conditions, allowing users to create specialized, automated operations based on their run book and best practices
- Support following actions:
  - Execute any CLI command on device
  - Generate alarms
  - Generate events
  - Power on/off/cycle device
  - Initiate out-of-band connection
  - Push configuration file to device
  - Pull configuration file from device
  - Reboot device
  - Issue "show tech" on device
- Send email alerts for device and system alarms
- Temperature and humidity can be monitored by an optional USB-connected sensor. Data can be used by the rules engine.

SECURE OPERATIONS

- FIPS 140-2 Level 2
- On-board storage: SSDs available with 256-bit AES compliant data encryption
- Encrypt all data transferred to centralized management server
- Support local authentication and authentication to RADIUS, TACACS and Microsoft Active Directory servers (LDAP)
- Support local authentication and authorization to TACACS and RADIUS servers (AD/LDAP proxy via Uplogix Control Center)
- Support specification of preferred and allowed ciphers, hashing, compression and key exchange algorithms for SSH
- A robust granular authorization model:
  - Access can be defined by groups, with users only able to see devices they have proper credentials for
  - Limit the functions a user is able to implement based on their role
  - Roles and responsibilities can be broken down by user, device, location and label
- SSH certificate authentication
- LM can establish a reverse SSH tunnel back to the UCC over in- or out-of-band connections that carry SSH terminal connections with the UCC acting as a proxy to overcome network address translation (NAT) and other issues servers (AD/LDAP proxy via Uplogix Control Center)
- Support specification of preferred and allowed ciphers, hashing, compression and key exchange algorithms for SSH

OUT-OF-BAND MANAGEMENT

- Collect and Display Technical Information for Internal Modems – The "pull tech" and "show tech" CLI commands collect and display detailed information about internal modems and their state.
- Out-Of-Band Setup Wizard – The UCC provides an out-of-band setup wizard with context sensitive help in order to simplify out-of-band configuration for the LM – this wizard can be run for a group in the hierarchy (where settings are applied to all LMs under that group) or for an individual LM.

- Local Manager Secure Tunneling to UCC – An LM can be configured to establish a reverse SSH tunnel back to the UCC over in-band and out-of-band connections that will carry SSH terminal connections to it (with UCC acting as a proxy) in order to overcome network address translation (NAT) and other issues that can make it unreachable when initiating a SSH session to it. When in place, the LM can optionally be configured to no longer listen to port 22 for SSH connections as an additional security measure.
- With the loss of the primary WAN connection, Uplogix can provide a tethered WAN traffic failover option by sharing its cellular out-of-band connection with the local router
- With a secure out-of-band connection back to the NOC, administrators can connect to remote managed devices during the network outage, and Uplogix continues to forward alarms, events, alerts and SYSLOG messages.
- Monitor primary network connectivity during an outage and automatically tear down the out-of-band network connection when primary network connectivity is restored.
- Support encrypted dial-in access with caller-ID filtering

LOGGING

- Log all keystrokes typed by a user while logged into the Local Manager to a session file that is stored locally and on the Uplogix Control Center
- Send SYSLOG message for all Local Manager alarms and events to a designated SYSLOG server
- Forward log messages collected from a managed device to a SYSLOG server on behalf of the managed device
- Generate and store events for the Local Manager and its managed devices that are viewable locally and on the centralized management server
- Store device changes made by users in terminal sessions to managed devices locally and to the Uplogix Control Center

REPORTING

- Provide hourly, daily, weekly and monthly reports for configuration changes, alarms, events, and logins

INTEGRATION

- Full multi-tenant support – granular authorization and roles allow multiple tenants to share the same Uplogix Control Center
- Send SNMP messages to northbound management system for all alarms/events
- Send Console log entries to SYSLOG servers
- User interface integration with centralized management tools

Americas
americas_sales@lantronix.com
www.lantronix.com
NASDAQ: LTRX

Europe
eu_sales@lantronix.com

Asia/Pacific
asiapacific_sales@lantronix.com

LANTRONIX