The Zero-Downtime Migration Checklist for ISPs

This checklist aims to provide ISPs with a step-by-step guide on how to migrate from existing serial consoles, such as the Raritan Dominion SX II, to ZPE Systems' Nodegrid. *Following this checklist ensures ISPs can migrate without downtime, while improving their operational resilience and recovery capabilities.*

☑ 1. Pre-Migration Planning

Before any hardware is moved, careful planning ensures your migration is low-risk and predictable. This stage aligns teams, sets success criteria, and documents the full scope of your current environment.

- **Inventory & Audit**
  - Document all current SX II deployments (location, role, connected devices).
  - Identify dependencies (network devices, PDUs, power supplies, cellular backup, cabling).
  - Note firmware versions and end-of-support risks.
- **Define Success Metrics**
  - Downtime tolerance (target: 0 minutes for critical sites).
  - Truck roll reduction goal (target: 50% or more).
  - Replacement provisioning speed (target: <15 minutes per replacement)
- **Align Stakeholders**
  - Engage NOC, field engineering, security, and procurement teams.
  - Assign a migration lead per region.
  - Establish communication and escalation protocols.

☑ 2. Infrastructure Assessment

The next step is to thoroughly evaluate your current infrastructure to identify readiness gaps. This ensures the new solution design is based on an accurate picture of existing connectivity, security, power, and operational policies.

- **Connectivity Requirements**
  - Validate redundancy of primary and OOB links.
  - Confirm availability of secondary transport (4G/5G, satellite/Starlink).
  - Ensure serial access paths are available for critical routers and switches.
- **Security Baseline**
  - Map zero trust requirements: RBAC, least-privilege, MFA.
  - Define encryption requirements (FIPS 140-3, TLS).
  - Identify integration points (RADIUS, TACACS+, LDAP, SAML).
- **Power & Rack Readiness**
  - Ensure power cycling capability is mapped for connected devices.
  - Confirm rack space and cabling requirements (Ethernet, fiber, serial, USB) for Nodegrid.
  - Check rack density and airflow constraints.
- **Operational Constraints**
  - Identify compliance mandates (PCI, SOX, GDPR, FCC).
  - Document remote vs. on-site access policies.
  - Establish change windows and maintenance policies.

☑ 3. Solution Design

This step helps you prescribe the right Nodegrid hardware, management tools, redundancy, and security controls for data center, POP, and last-mile deployments.

- **Hardware Selection**
  - **For Data Centers:** Deploy high-density NSR or NSC models with redundant power.
  - **For POPs:** Deploy mid-range GSR units for regional aggregation sites.
  - **For Last-Mile Sites:** Deploy compact BSR devices with built-in 5G/LTE.
  - **Keep in mind:** Consolidate as many legacy appliances (console server, PDU manager, cellular gateway) into a single Nodegrid.
- **Management Strategy**
  - Decide between ZPE Cloud (centralized SaaS) or on-prem Nodegrid Manager.
  - Define RBAC roles across NOC, field engineers, and vendors.
  - Enable policy push for config templates, firmware, and audit controls.
- **Failover & Redundancy**
  - Integrate 5G/LTE or Starlink for out-of-band continuity.
  - Configure automatic failover for high-priority sites.
  - Build escalation rules for NOC alerts during failover events.
- **Security & Compliance Design**
  - Apply zero trust across OOB plane.
  - Define immutable logging policies.
  - Segment vendor access for audited sessions.

☑ 4. Configuration Preparation

To help you avoid long periods of on-site work, this step helps you create, test, and validate configurations and policies ahead of time. This preparation ensures you can swap devices with minimal effort and only one on-site visit during rollout (next step).

- **Create Templates**
  - Build Nodegrid configuration templates for each site type.
- **Set Up Automation**
  - Enable zero-touch provisioning workflows.
- **Integrate Security**
  - Pre-configure access controls, logging, and audit settings.

☑ 5. Migration Execution

This is where planning pays off. By validating everything beforehand, you can replace hardware in a single site visit with zero downtime.

- **Pre-Deployment Validation**
  - Finalize and test Nodegrid configurations, automation templates, and security policies in a lab or staging environment.
  - Validate integration with NOC workflows, RADIUS/TACACS+, and ZPE Cloud before any site visit.
- **Swap Hardware**
  - Arrive on-site with pre-configured Nodegrid devices ready for immediate replacement of SX II.
  - Minimize time on-site by ensuring rack space, cabling, and power requirements were confirmed during Phase 2 (Infrastructure Assessment).
- **Data & Mapping Migration**
  - Import port mappings, credentials, and automation scripts into Nodegrid prior to installation, ensuring parity with existing SX II setups.
- **Test Failover & Continuity**
  - Immediately after installation, simulate outage scenarios to verify OOB continuity (via 5G/LTE/Starlink) and validate remote access without requiring a return visit.

☑ 6. Post-Migration Validation

With the physical migration complete, it's time to verify performance against defined metrics. This step helps you ensure that the migration achieves its goals and meets all security and compliance requirements.

- **Verify Functions**
  - Test remote access, power control, provisioning speed.
- **Audit Security**
  - Ensure all connections meet Zero Trust and compliance requirements.
- **Review/Compare Performance**
  - Compare against baseline success metrics.

☑ 7. Ongoing Optimization

This stage helps you ensure that staff are trained, monitoring is in place, and automation keeps evolving.

- **Training & Handover**
  - Train NOC and field teams on Nodegrid interface and workflows.
- **Proactive Monitoring**
  - Set up alerts and dashboards in ZPE Cloud.
- **Continuous Improvement**
  - Update automation templates and security policies quarterly.