

Testing, Packaging & Shipping Procedures

Hula Networks Standard 12 Point Certification Process

We physically inspect all equipment for noticeable damage	Port by port diagnostic testing	Clean chassis and modules from dust and debris
Ensure fans are operational	Restore factory default configurations	Remove any passwords
Live network testing	24 hour stability testing	Test all power supplies
Verify all serial numbers are valid	Verify all chassis are error free	Verify all modules and Interfaces are error free

In addition to the above 12 point Certification Process Hula Networks Inc will perform the following for all orders.

Initial Setup

- Unpack and inspect the network device for physical damage.
- Ensure that the network device is placed on a stable surface with proper ventilation.

Hardware Inspection

- Check all ports (Ethernet, SFP, etc.) for physical damage, cleanliness, and proper labeling.
- Inspect the fans for any obstruction or unusual noise.
- Verify that power supplies are securely connected and powered on.
- Check for loose or disconnected cables.
- Inspect the chassis for any visible damage or loose components.

Factory Default Restoration

- Reset the network device to its factory default settings to eliminate any prior configurations.
- Confirm that the default settings have been applied successfully.



Password Removal

- Ensure that any passwords or access control measures are removed or reset.
- Verify that the network device is accessible without authentication (for initial testing purposes).

Power Supply Testing

- Monitor the power supplies for stable voltage and current levels.
- Test redundancy by disconnecting one power supply and ensuring the network device continues to operate without interruption.

Port Testing

- Connect devices to all network device ports, one at a time.
- Verify link status and negotiate appropriate network settings (e.g., speed and duplex).
- Test data transfer between devices connected to different ports.

Module and Interface Verification

- If the network device has modular components (e.g., expansion modules), verify their proper insertion and functionality.
- Check the status of all interfaces, including virtual LAN (VLAN) configurations.
- Test the functionality of specialized interfaces (e.g., trunk ports, management interfaces).

Error-Free Operation

- Monitor the network device logs and counters for any errors, collisions, or unusual events.
- Confirm that there are no error messages in the logs or on the console.
- Verify that the network device maintains stable CPU and memory utilization levels.

VLAN Configuration Testing

- Create and configure VLANs as needed for your network.
- Ensure that VLAN tagging and untagging are working correctly.
- Test inter-VLAN routing if applicable.

Quality of Service (QoS) Testing

- Configure and test QoS policies to prioritize traffic as needed.
- Confirm that QoS settings are effective in ensuring the desired network performance.

Security Testing

- Implement and test security features such as Access Control Lists (ACLs) and port security.
- Verify that unauthorized access attempts trigger appropriate security measures.



Redundancy and Failover Testing

- If the network device supports redundancy protocols (e.g., HSRP, VRRP), configure and test them.
- Simulate hardware failures (e.g., disconnect a power supply or network cable) to verify failover mechanisms.

Load Testing

- Simulate heavy network traffic to assess the network device's performance under load.
- Monitor for dropped packets, increased latency, or any other performance issues

Documentation

- Update network documentation with the network device's configuration details, test results, and any issues encountered.
- Ensure that all test procedures and results are recorded for future reference.

User Acceptance Testing (UAT)

- Involve end-users or stakeholders in testing to ensure that the network device meets their specific requirements and expectations.

Reporting

- Generate a comprehensive test report summarizing all test procedures, results, and any identified issues.
- Include recommendations for remediation and future maintenance.

Final Verification

- Once all tests pass and issues are resolved, confirm that the network device is ready for production use.

Backup Configuration

- Take a backup of the final configuration for disaster recovery purposes.

This comprehensive testing procedure covers various aspects of network device testing to ensure the network device's functionality, performance, and security meet the desired standards. It is essential to adapt these steps to your specific network environment and requirements.



Package Contents

- Verify that rack mount hardware is included.
- Verify that all port adapters are locked in.
- Remove power supplies from chassis. Package separately.
- Verify that a console cable is included with all chassis.

Shipping Guidelines

- Make sure all equipment is shipped in thick double walled cardboard boxes, wrapped in 4-5 layers of bubble wrap, foam popcorn or foam to elevate any open areas for movement in shipping.
- Secure contents so there is absolutely no movement inside the box once sealed up.
- Tip: give a healthy shake to see if contents move within.
- Enclose with at least 2 inches of padding around all sides of units.
- Cards need to be enclosed in a static bag prior to being wrapped in bubble or put in a pizza box.
- Any boxes weighing over 75 lbs. please call or email prior to shipment. Make sure equipment is palletized.
- Multiple items in a box need to be wrapped individually.
- Remove and wrap fans and power units separately to avoid bent handles.
- Include any accessories rack mounts, power and console cables needed.
- New equipment needs to be double boxed. DO NOT tape over Cisco tape or labeling.
- Palletized items need to be boxed and padded between before placing on the pallet.

Contact your Hula Sales Rep for more details!

929 Berryessa Road Suite 10 San Jose, CA 95133 | P: 1-866-485-2638 (HULANET) | F: 1-650-625-4101
sales@hulanetworks.com | www.hulanetworks.com

