Carrier-Grade Infrastructure Solution Brief: Deploying Dynamic ARP Inspection

CARRIER-GRADE INFRASTRUCTURE SOLUTION BRIEF: DEPLOYING DYNAMIC ARP INSPECTION

MARKET POSITIONING

The exponential growth of man-in-the-middle and ARP spoofing attacks within enterprise and carrier Ethernet fabrics necessitates a proactive security posture at the access layer. Dynamic ARP Inspection (DAI) serves as a critical validation gatekeeper, intercepting all ARP requests and responses on untrusted ports. This document details the turnkey hardware specifications and architectural logic of our next-generation switching platform engineered for line-rate DAI enforcement. Our solution integrates DAI natively into the forwarding ASIC, eliminating the performance penalty traditionally associated with CPU-bound inspection. Designed for 1G to 400G edge deployments, this platform ensures that only valid ARP-to-MAC bindings, verified against the DHCP snooping binding database, are permitted to transit the network.

HIGH-AVAILABILITY REDUNDANCY

The hardware architecture implements a fully redundant control plane to manage the DHCP snooping database — the authoritative source for DAI validation. Two key pillars ensure continuous operation: 1) In-Service Software Upgrade (ISSU) capability for DAI logic, preventing ARP flooding during patching cycles; and 2) Stateful failover of the binding database between active and standby supervisors. Each line card houses dual forwarding engines that synchronize the ARP permit/deny list, achieving sub-50ms switchover time. The chassis supports N+1 power supplies and redundant fan trays, ensuring that security policies remain enforced even during hardware maintenance events.

PROTOCOL INTEROPERABILITY

This platform performs DAI in hardware, supporting up to 32,000 ARP inspection entries per forwarding instance. It interoperates seamlessly with

industry-standard protocols: DHCPv4/v6 Snooping (RFC 2131), Option 82 circuit-ID insertion, and IEEE 802.1X port-based authentication. DAI can be configured per VLAN, with granular trust/untrust port states. The hardware provides advanced validation checks beyond simple binding lookups, including destination MAC validation, IP source guard correlation, and ARP ACLs for static hosts. All logging and counters are hardware-accelerated to prevent control plane overload during ARP storms.

DETAILED PARAMETERS

- Inspection Rate: Up to 5 million ARP packets per second (line-rate) on 400G interfaces.
- Binding Database Capacity: 128,000 dynamic entries via DHCP snooping, expandable to 256,000 with optional TCAM expansion module.
- Logging Rate: 16,000 syslog messages per second to external collectors, zero packet loss.
- VLAN Support: DAI active on up to 4,096 VLANs simultaneously.
- Validation Checks: Source MAC (stricter), destination MAC, IP address binding, and ARP body validity.

TECHNICAL SPECIFICATIONS

Parameter	**Specification**

Form Factor	2RU Ruggedized Chassis (19-inch rack mount)
Switching Capacity	3.6 Tbps (non-blocking, full duplex)
Power Supply	2 x 2000W AC (1+1 redundant, hot-swappable), 48VDC optional
DAI Hardware Entries	128,000 (expandable to 256,000 with TCAM module)
Port Density	48 x 1/10/25G SFP28 + 8 x 100/400G QSFP-DD
Operating Temperature	-5°C to +55°C (extended range -40°C to +70°C with fan kit)
Forwarding Rate	2.1 Bpps (billion packets per second)

LIFECYCLE ASSURANCE (MTBF)

Hardware reliability is paramount for security enforcement points. The primary switching fabric exhibits a 35-year Mean Time Between Failures (MTBF) at 40°C ambient temperature, calculated per Telcordia SR-332. The power supply modules (1+1 redundant) provide a 350,000-hour MTBF each. The chassis includes environmental monitoring for temperature, voltage, and fan speed, with automatic shutdown protection. Our global RMA service guarantees a 24-hour advanced replacement for DAI-critical components.

TARGET NETWORK TOPOLOGIES

This DAI-capable hardware is ideal for multiple deployment scenarios: 1) Secure campus access: DAI enforced on user-facing ports (untrusted) while uplinks to distribution switches remain trusted. 2) Carrier Ethernet NID: Prevents spoofing at the customer demarcation point. 3) Data center leaf-spine: Protects ARP resolution between virtual machines and bare-metal hosts. 4) Smart city IoT backhaul: Hardens control plane against malicious ARP injections.

COMPLIANCE & CERTIFICATIONS

NEBS Level 3, ETSI 300 019-2-3 (class 3.1E environmental), IEC 62368-1 safety, FCC Part 15 Class A, CE Mark. The DAI implementation is Common Criteria certified under NDcPP (Protection Profile for Network Devices).