Enterprise Core Systems Engineering Reference Manual: Dynamic ARP Inspection (DAI) Security

PRODUCT IDENTIFICATION: DYNAMIC ARP INSPECTION (DAI) SECURITY MODULE

The Dynamic ARP Inspection (DAI) security feature represents a critical enforcement layer within the enterprise switching infrastructure, designed to mitigate Man-in-the-Middle (MITM) and ARP spoofing attacks at the access edge. This technical overview details the hardware-assisted inspection engine, validation logic, and integration parameters for carrier-grade and campus core deployments.



CORE INTERNAL TOPOLOGY & INSPECTION PIPELINE

The DAI subsystem operates as an inline packet validation engine integrated directly into the forwarding ASIC pipeline. Upon ingress of an ARP packet on an untrusted interface, the hardware comparator extracts the sender MAC address, sender IP address, and ingress VLAN identifier. This triplet is instantaneously cross-referenced against the Dynamic DHCP Snooping Binding Table resident in high-speed TCAM memory. Only ARP packets possessing a valid binding are permitted to update the system ARP cache; all invalid or gratuitous ARP replies are silently dropped at line rate. The architecture supports two operational validation modes: strict binding validation and destination check enforcement for ARP replies.

SWITCHING & SECURITY SUBSYSTEM CAPABILITIES

- LINE-RATE DAI ENFORCEMENT: 1.44 Tbps switching capacity enables DAI inspection without measurable latency penalty (sub-microsecond per packet).
- DHCP SNOOPING INTEGRATION: Automatic population of the inspection database via DHCP transactions; supports static IP address binding entries for non-DHCP clients.
- RATE-LIMITING CONTROL: Programmable ARP packet rate limiter per interface to prevent CPU overload during ARP storm attacks.
- TRUSTED INTERFACE DESIGNATION: Explicit port-level trust assignment to bypass DAI for uplinks and infrastructure device connections.

- VLAN-BASED ACTIVATION: Granular enable/disable per VLAN, allowing phased deployment across production and tenant networks.

Parameter	Specification
Form Factor	Fixed 1RU / 10-slot modular chassis option
Switching Capacity	Up to 1.44 Tbps non-blocking fabric
Power Supply	Dual hot-swappable redundant AC 100-240V (DC optional)
DAI Inspection Latency	< 1 microsecond per packet
Operating Temperature	0°C to 45°C (32°F to 113°F)

OPERATIONAL ADVANTAGES FOR CAMPUS & DATACENTER

- ZERO-KNOWLEDGE SPOOFING BLOCK: Prevents attackers from associating their MAC address with a legitimate IP address of a gateway or host.

- VALIDATION AGAINST LEASE TIMERS: Automatically invalidates bindings when DHCP lease expires, removing stale entries from the inspection table.

- INTEROPERABILITY STANDARDS: Fully compatible with 802.1Q VLAN tagging, Link Aggregation Control Protocol (LACP), and Virtual Router Redundancy Protocol (VRRP).

- LOGGING & TRAPPING: Syslog generation for each dropped ARP packet, including source port, VLAN, and offending MAC/IP pair.

SPECIFICATION MATRIX

PARAMETER: DAI SECURITY ENGINE SPECIFICATION

- Inspection Speed: Line-rate, up to 1.2 billion packets per second
- Binding Table Capacity: 64,000 entries (expandable to 128,000 w/ TCAM allocation)
- Supported ARP Types: ARP request, ARP reply, gratuitous ARP
- Validation Sources: DHCP snooping database, static IPv4 binding list
- Packet Drop Logging: Yes, with configurable throttle rate (10-1000 drops per second)

REGULATORY COMPLIANCE & NETWORK STANDARDS

- IEEE 802.1X Port-Based Network Access Control integration
- RFC 826 (Ethernet ARP) strict compliance
- RFC 5227 (IPv4 Address Conflict Detection) for gratuitous ARP validation
- Common Criteria EAL2+ certified for packet filtering subsystems
- RoHS 3 (Directive 2015/863/EU) compliant hardware components


DAI
Status