FRIDAY AI VS. SNMP

What Being Inside the Broadcast Domain Makes Possible

Why deep network visibility and automated remediation require local presence.

ABSTRACT

SNMP asks devices how they're doing and receives back a predefined set of statistics. Friday AI establishes an encrypted command-line session directly inside the network and reads everything the device knows, then acts on it.

The difference between the two is not a matter of degree. It is a matter of architectural position. SNMP works from outside the network. Friday AI works from inside. That single difference determines what is visible, what is diagnosable, and what is fixable, without a truck roll.

01

The Broadcast Domain: Why Local Presence Changes Everything

Every network is divided into broadcast domains (the neighborhood within which devices communicate directly at Layer 2) the Ethernet layer. VLANs define these neighborhoods. Within a broadcast domain, devices continuously exchange diagnostic traffic that reveals rich, real-time intelligence about network health, device identity, and physical topology.

This traffic never crosses a Layer 3 boundary. It cannot be seen from outside the network. It cannot be tunneled, proxied, or captured by any remote monitoring service; regardless of bandwidth, credentials, or software sophistication. It exists only within the local segment.

Friday AI's physical appliance connects to the network's core switch via a trunk port; a single connection point that carries traffic from all VLANs simultaneously. This positions Friday AI inside every broadcast domain on the network at once, with complete visibility across all segments from a single device.

What Lives in the Broadcast Domain

Traffic Type	What It Reveals
ARP requests & responses	Real-time IP-to-MAC mapping for every active device. New device detection the instant it sends its first packet. IP address conflict identification.
DHCP discover / offer / request / ack	New devices join events with vendor fingerprinting. IP lease assignments. Rogue DHCP server detection. Device type identification before any SSH session.
LLDP / CDP neighbor announcements	Physical topology: which device is connected to which port of which switch. Link speed, duplex state, device model, and firmware version from neighbor data.
Spanning Tree BPDUs	Loop-prevention topology. Root bridge identity. Topology change events that precede outages. Rogue bridge detection. Loop identification before cascade failure.
Gratuitous ARP	IP address conflicts. Device reboot detection. Unauthorized device spoofing. Network change events.
Broadcast storms	The storm itself is visible from inside (source port, storm type, propagation). Remote tools see only the symptom: everything stops responding.

Physics, Not Policy

The reason remote monitoring tools cannot see broadcast traffic is not a software limitation or a configuration choice. Layer 2 broadcast traffic is architecturally constrained to the local segment by the fundamental design of Ethernet networking. No cloud service, no remote agent, and no software update can change this. Local physical presence is the only solution (which is why the Friday AI appliance must be on-site) connected to a trunk port.

02 SNMP: What It Can & Cannot Do

SNMP (Simple Network Management Protocol) has been the network monitoring standard since the 1980s. It works by polling devices for a predefined set of metrics called MIBs (Management Information Bases). Each device vendor decides which metrics to expose. The monitoring system asks; the device returns the data it was programmed to provide.

What SNMP Does Well

- **Interface up/down status:** knows whether a port is administratively active or operationally down
- **Basic traffic counters:** bytes in and out per interface over time
- **CPU and memory utilization:** aggregate device health metrics at a coarse level
- **Predefined threshold alerting:** notify when a metric exceeds a configured value
- **Vendor-standard MIB data:** consistent baseline metrics across devices that implement the same MIBs

What SNMP Cannot Do

- **See broadcast domain traffic:** ARP, DHCP, STP, and LLDP are invisible to any remote polling tool
- **Build physical topology maps:** neighbor discovery data does not cross Layer 3 boundaries
- **Detect new devices instantly:** only sees devices after they appear in routing tables, not at join time
- **Identify root cause:** can tell you something is wrong; cannot tell you why
- **Issue any remediation command:** SNMP is strictly read-only by design
- **Access vendor-specific diagnostics:** any metric outside the standard MIB is invisible
- **Detect configuration drift**: no ability to compare running configuration to a known-good baseline
- **Identify unauthorized devices:** MAC address tables and ARP caches are not accessible remotely
- **Correlate events across layers:** sees symptoms in isolation, not causes in context

03

Friday AI: SSH-Based Discovery and Remediation from Inside the Network

Friday AI uses patent-pending SSH-based discovery and monitoring. SSH (Secure Shell) is an encrypted protocol that establishes a full authenticated command-line session on a network device; identical to the session a network engineer uses at a terminal. From this session, Friday AI issues any CLI command the device supports, reads the complete output, and acts on the results.

This is not polling a predefined set of metrics. This is full administrative access to the device's complete diagnostic intelligence; everything the device knows about itself, its connections, its current state, and its history.

Read: What Friday AI's Show Commands Reveal

Show commands are read-only CLI queries. They impose no change on the device and can be run continuously without disruption. Friday AI issues these commands on a configurable schedule across every managed device.

SSH Show Commands: Device Diagnostics

show interfaces	→ port status, error counters, CRC errors, traffic rates, duplex
show interfaces counters	→ accumulated error statistics: cable and SFP fault identification
show power inline	→ PoE consumption per port, budget remaining, per-device baseline.

(continued)

show mac address-table	→ every connected device: IP, MAC, switch port, VLAN
show arp	→ complete IP-to-MAC mapping across all VLANs
show cdp neighbors detail	→ physical topology; what is connected where
show lldp neighbors detail	→ vendor-agnostic topology for multi-vendor environments
show spanning-tree	→ loop-prevention topology, root bridge, port states
show vlan brief	→ VLAN assignment for every port; misconfiguration detection
show running-config	→ complete current configuration for drift detection
show version	→ firmware version, uptime, license status, hardware serial
show logging	→ recent system events, error history, unexpected reboots
show processes cpu	→ CPU utilization, high-CPU process identification
show processes memory	→ memory utilization ; degradation before failure
show environment	→ temperature sensors, fan status, power supply health
show ip route	→ routing table; path changes, missing routes
show access-lists	→ firewall ACL states; traffic policy verification

Act: What Friday AI Can Do That SNMP Cannot

The same SSH session that reads can also write and remediate. Friday AI's IR Flow engine executes remediation commands autonomously; working through a least-to-most-disruptive hierarchy, confirming recovery at each step, and escalating to human intervention only when automated options are exhausted.

SSH Remediation Commands

interface {port}

shutdown	→ disable a misbehaving port
no shutdown	→ re-enable port (bounce sequence)
switchport access vlan {n}	→ correct a VLAN misconfiguration
power inline reset	→ PoE power cycle a connected device

clean arp	→ flush stale ARP cache entries
clear mac address-table dynamic	→ flush stale MAC table entries
clear spanning-tree detected-protocols	→ force STP reconvergence
copy tftp running-config	→ restore known-good configuration
write memory	→ save running config to startup
reload	→ full switch restart (last resort before escalation)
[Smart PDU REST API]	→ power cycle any 110V plugged device
[Device REST API]	→ health queries and actions on supported systems

04 Complete Compatibility Comparison

Capability	SNMP- External Monitoring	Friday AI- Inside the Broadcast Domain
Device online/ offline	Yes → ICMP ping or SNMP poll	Yes → continuous ping with SSH context
Interface up / down status	Yes → standard SNMP MIB	Yes → with full error counter context
Traffic volume per interface	Yes → basic byte counters	Yes → with error breakdown by type
CRC / physical layer errors	Limited → interface status only	Full → cable and SFP fault identification
PoE consumption per port	Limited or unavailable	Full → per-port baseline and anomaly detection
CPU / memory / temperature	Basic → aggregate metrics only	Full → per-process detail, thermal sensors, fan status

MAC address table	Not visible	Full → every device, every port, every VLAN
ARP cache across VLANs	Not visible	Full → real-time across all segments
Physical topology (LLDP/CDP)	Not visible	Full → complete neighbor map, device model, firmware
VLAN assignment audit	Not visible	Full → detects port misconfiguration instantly
Spanning tree topology	Not visible	Full → detects loops and rogue bridges before failure
New device detection	After routing table update	Instant → ARP broadcast captured at join time
Unauthorized device detection	Not possible	Instant → unknown MAC on any VLAN triggers alert
Configuration drift detection	Not possible	Yes → running config compared to known-good baseline
Broadcast storm root cause	Not visible → sees only outage symptom	Full → source port and storm type identified
Root cause diagnosis	Not possible → symptom only	Yes → identifies cause, not just effect
Port bounce remediation	Not possible	Yes → shutdown / no shutdown via SSH
VLAN fix remediation	Not possible	Yes → switchport access vlan reassignment

PoE power cycle	Not possible	Yes → power inline reset via SSH
Smart PDU power cycle (110V)	Not possible	Yes → REST API via secure local tunnel
Configuration restoration	Not possible	Yes → restore from known-good backup
Automated remediation workflow	Not possible	Yes → IR Flow: detect → diagnose→ act → confirm

OSI Layer Coverage

05

Layer	What Lives Here	SNMP Sees	Friday AI Sees
Layer 1 Physical	Cables, SFP modules, PoE power levels, port signal quality	Interface status only	Full → error counters, PoE draw, CRC errors, signal levels per port
Layer 2 Data Link	MAC addresses, VLANs, ARP, STP, LLDP/CDP, all broadcast traffic	Not visible → stays inside broadcast domain	Full → topology maps, device inventory, unauthorized device detection
Layer 3 Network	IP routing, firewall ACLs, NAT, inter-VLAN routing	Basic SNMP MIB data only	Full CLI → routing tables, ACL states, path verification
Layer 4 Transport	TCP session states, port reachability, connection tracking	Not visible	Yes → session states, reachability confirmation, flow diagnosis

06 The Trunk Port: One Appliance, Total Visibility

Friday AI's appliance connects to the network's core switch via a single trunk port. A trunk port carries IEEE 802.1Q tagged frames from all VLANs simultaneously. This single architectural choice delivers complete network visibility from one physical connection point.

- One appliance provides visibility across every VLAN on the network simultaneously
- All broadcast domain traffic (across all segments) is observable from a single connection
- No per-floor or per-closet agents required; the core switch trunk port is the leverage point
- VLAN isolation is maintained; Friday AI observes each segment independently without bridging
- Cross-VLAN correlation becomes possible; relating a switch port failure to the device it serves
- Complete physical topology mapped automatically; no manual documentation required
- New devices detected on any VLAN the moment they join; regardless of segment

Why This Cannot Be Replicated Remotely

A remote SNMP poller, cloud monitoring service, or VPN-connected engineer cannot capture Layer 2 broadcast traffic regardless of credentials, bandwidth, or software sophistication.

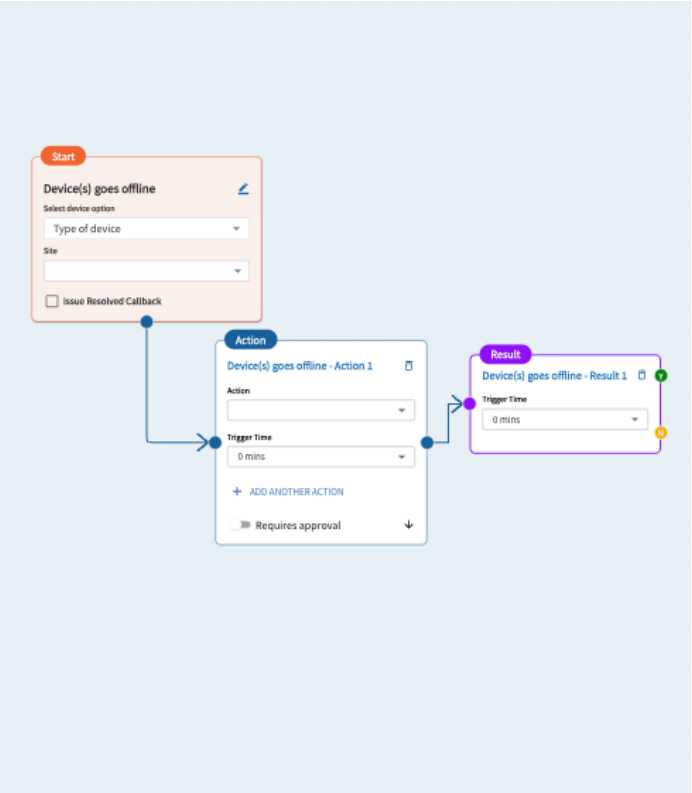
Layer 2 broadcast frames are physically constrained to the local segment by the architecture of Ethernet. They do not traverse Layer 3 boundaries. They never reach the internet. They are invisible to any device outside the broadcast domain.

The Friday AI appliance must be physically present (connected to a trunk port on the core switch) to provide this level of visibility. Not for access. For physics.

07

Automated Remediation: The Complete IR Flow Hierarchy

Because Friday AI is inside the network with full SSH access and REST API integration, it executes a complete remediation hierarchy autonomously. The IR Flow engine works from least to most disruptive; confirming recovery at each step before escalating.



Step	Action	Method	Disruption Level	Truck Roll Eliminated?
1	Flush stale ARP / MAC entries	SSH CLI: clear arp / clear mac	Zero	Yes
2	Bounce switch port	SSH CLI: shutdown / no shutdown	Single port, ~30 sec	Yes
3	Correct VLAN misconfiguration	SSH CLI: switchport access vlan	Single device, instant	Yes
4	PoE power cycle	SSH CLI: power inline reset	Single device, ~60 sec	Yes
5	110V device power cycle	Smart PDU REST API:outlet off → on	Single device, 3–8 min	Yes

6	Restore configuration from backup	SSH CLI: copy tftp running-config	Switch, brief outage	Yes
7	Full switch restart	SSH CLI: reload	All ports, 2–3 min	Yes
8	Escalate with full incident package	NOC dispatch → informed, never blind	Human on-site required	Physical fault only

07 Security Architecture — Remediation Without Exposure

For a remote engineer or external monitoring service to perform SSH-based remediation, the network's management interfaces would need to be either exposed to the internet or accessible via VPN; both of which compromise the security posture that a well-managed network exists to provide.

The Problem with Remote Remediation

- Exposing switch management interfaces to the internet creates inbound attack surface on every managed device
- VPN access requires certificate management, credential rotation, and audit complexity at scale across every site
- Both approaches require inbound connections; the opposite of a secure, closed network architecture

Friday AI's Architecture: Outbound Only, Zero Inbound

Friday AI's appliance communicates exclusively via outbound Cloudflare tunnels. The network's management interfaces remain completely isolated behind the firewall. No inbound connections are required. No management ports are exposed to the internet.

Required Firewall Rules: Outbound Only, No Exceptions

TCP 443	→ *.clusterai.net, *.fridayai.net, api.cloudflare.com	
TCP/UDP 7844	→ *.argotunnel.com, *.cftunnel.com (Cloudflare tunnel)	
TCP 22	→ [managed device IPs — local network only]	(SSH)
UDP 53	→ 1.1.1.1, 8.8.8.8.	(DNS)

Zero inbound rules. Zero exposed management ports. Zero VPN required.
The network stays completely closed. Friday AI delivers full remediation capability.

When the Friday AI cloud issues a remediation instruction, it travels down the outbound tunnel to the appliance. The appliance executes the action locally against the isolated device. Results travel back up the tunnel. The network never opens an inbound connection, ever.

> **The Security Equation**
>
> Friday AI delivers the full remediation capability of a network engineer with physical presence at every device without exposing a single management interface to the internet, without requiring VPN, and without creating any inbound attack surface. The network stays completely closed. Automated remediation is completely available.

09 Multi-Site and Multi-Vendor: Built for the Real World

Most networks are not single-vendor environments. Switches from one manufacturer, firewalls from another, access points from a third. Friday AI is designed for exactly this reality.

Vendor Support

- Cisco Catalyst, Cisco Meraki, Cisco ASA/FTD
- Aruba / HP ProCurve
- Fortinet FortiGate, FortiSwitch
- Juniper EX series
- Ruckus / CommScope
- Ubiquiti UniFi
- Palo Alto Networks
- Additional vendors supported; Friday AI parses CLI output for any SSH-accessible device

Multi-Site Architecture

For organizations with multiple locations, each site requires one Friday AI appliance at the MDF. All appliances connect to the Friday AI cloud platform via outbound-only Cloudflare tunnels. The central dashboard provides unified visibility across all sites simultaneously; a single pane of glass for the entire network portfolio.

- **One appliance per site:** no per-floor agents, no distributed infrastructure
- **Unified dashboard across all sites:** compare health, incidents, and trends portfolio-wide
- **Per-site IR Flow automation:** remediation logic customized to each location's environment
- **Cross-site incident correlation:** identify patterns that span multiple locations
- **Centralized credential management:** device credentials managed once, applied everywhere

Welcome to Intelligent Technology