

NAC Impact to the Network

Comparing Low Impact NAC Approaches



Background

- Experience from VLAN NAC in 2004
 - Groups: Security, network, help desk, desktop
 - Issues: Embedded devices, unknown devices, port and ACL configuration, coordinating groups and activities
 - Scaling challenges: LAN changes, new subnets, guests, employee changes
- Conclusion
 - Managing the network is good as long as the cost to manage the management doesn't outweigh the benefits



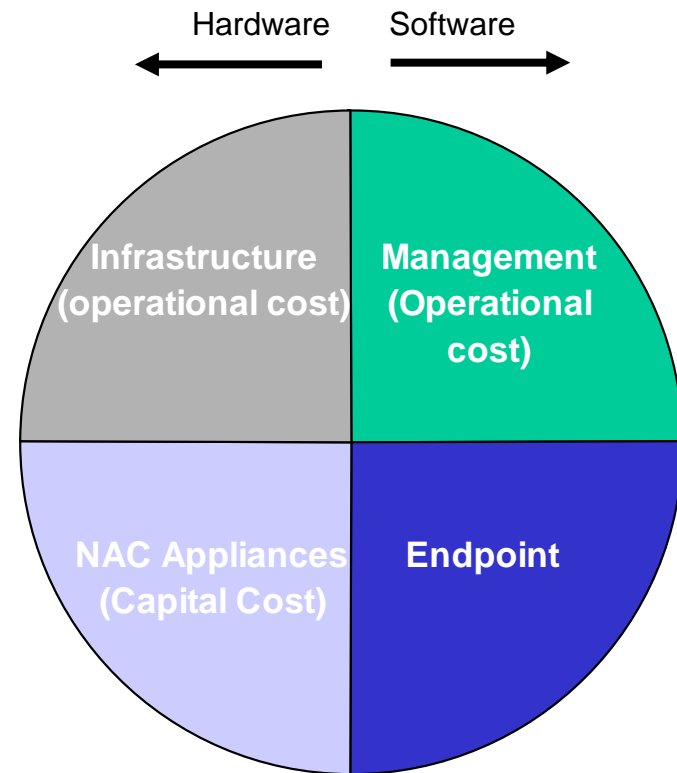
Scope of Discussion

- In Scope
 - Enterprise environment
 - Authentication
 - Pre and Post Admission Checking
 - Pre and Post Admission Quarantine / Enforcement
 - Support for Guests and Employees
 - LAN and WLAN access to the network
 - Support for computers and embedded devices
- Out of Scope... But Worth Considering
 - Remote access NAC (in-line and built in)
 - Policy management (specific to each vendor)
 - Hardware upgrades (specific to organization and NAC method)



Areas Potentially Impacted by NAC

- Infrastructure Configuration – Network equipment including switches, routers, firewalls, and other physical packet transfer devices
- Management - Policy definition, report analysis, monitoring, user support
- NAC Appliances – Additional appliances in proportion to network components, sites, subnets, or VLANs
- Endpoint – Agent software and plugins



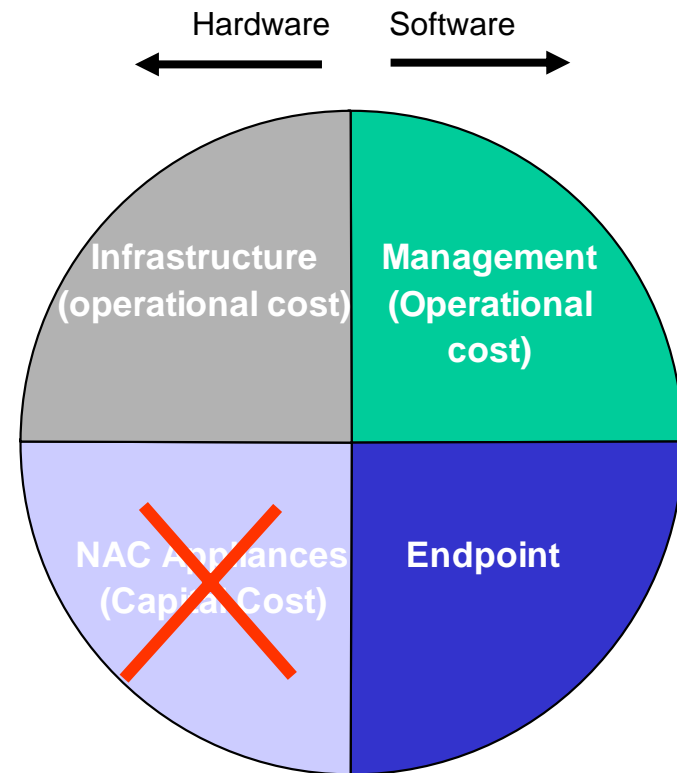
NAC Enforcement Methods

	Description	Quarantine Method
802.1x Management	Uses switch 802.1x with RADIUS server to authenticate and transfer audit compliance data	Filters using ACLs on router or switch
DHCP Management	Uses DHCP server or in-line appliance to modify DHCP replies to alter routes and subnets based on endpoint compliance audits.	Downloads quarantine subnets or routes via DHCP
In-Line Traffic Management	Uses appliance between edge and distribution switches to monitor and filter traffic.	Filters traffic inline
Out of Band Spanning Port Management	Uses monitor/spanning port to check for traffic compliance and sends layer 2 or 3 packets to endpoint to disallow certain traffic.	Sends DOS traffic or layer 2 management to endpoints
Peer Based Management	Neighboring endpoints use layer 2 management to intercept and inspect unknown devices.	Peers use filters and layer 2 management to endpoints



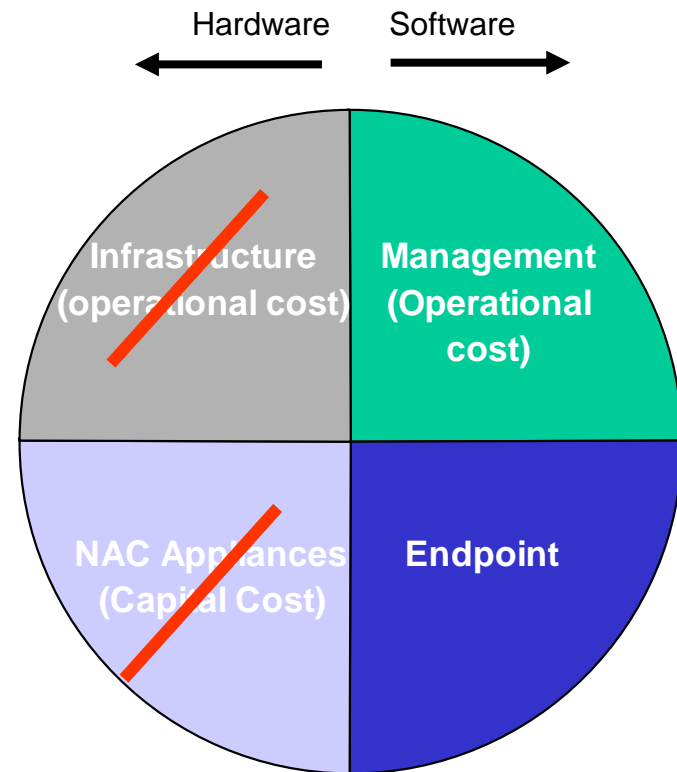
802.1x NAC

- Infrastructure Impact
 - Switch – 802.1x port configuration, VLAN creation
 - Router – ACL, NICs, subnets
 - DHCP configuration – Quarantine subnets
- Endpoint Impact
 - Supplicant and plugins for framework
- Scalability Considerations
 - Switch Configuration ~ Number of ports/switches/subnets
 - Router Configuration ~ Number of subnets
 - Clients ~ Number of endpoints
 - Non-802.1x embedded devices
 - Software-hardware interoperability



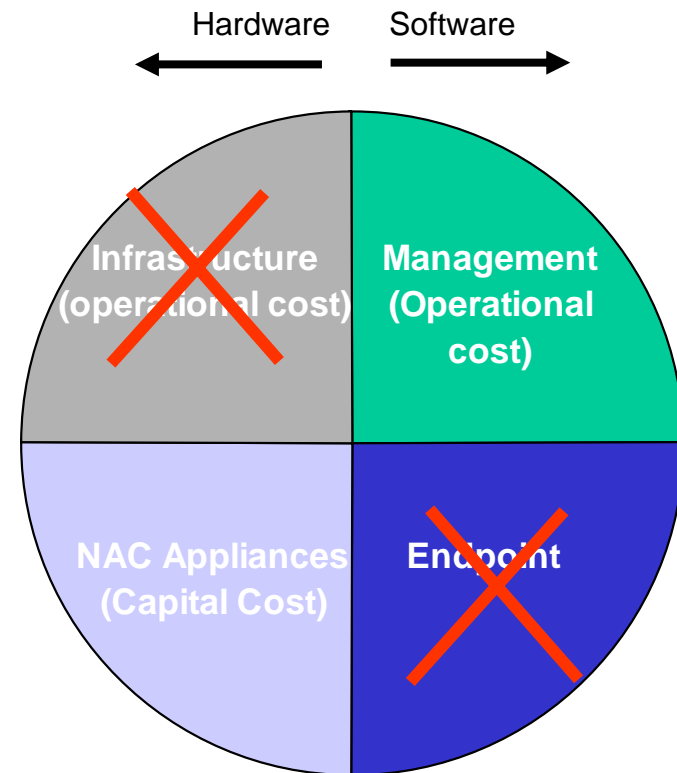
DHCP NAC

- Infrastructure Impact
 - Router – ACL, NICs, subnets
 - DHCP server
- Endpoint Impact
 - Agent
- Scalability Considerations
 - Router Configuration ~ Number Subnets
 - NAC Appliances ~ Number of DHCP Sites
 - Agents ~ Endpoints
 - Static IP addresses



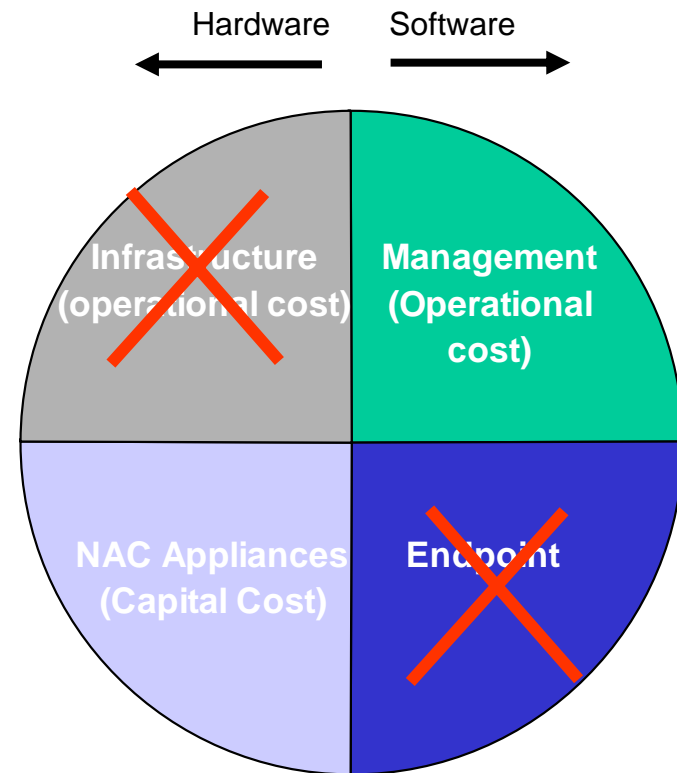
In-Line NAC

- Infrastructure Impact
 - Switches
- Endpoint Impact
 - Typically none
- Scalability Considerations
 - NAC Appliances ~ Switches (expense)



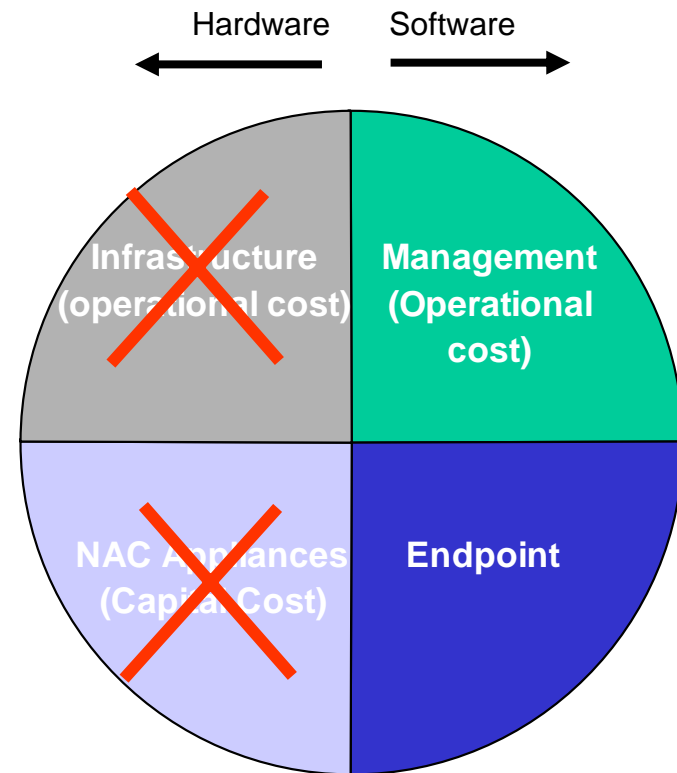
Out-of-Band Spanning Port NAC

- Infrastructure Impact
 - Add appliance to span port
- Endpoint Impact
 - Typically none
- Scalability Considerations
 - NAC Appliances ~ Switches or VLANs

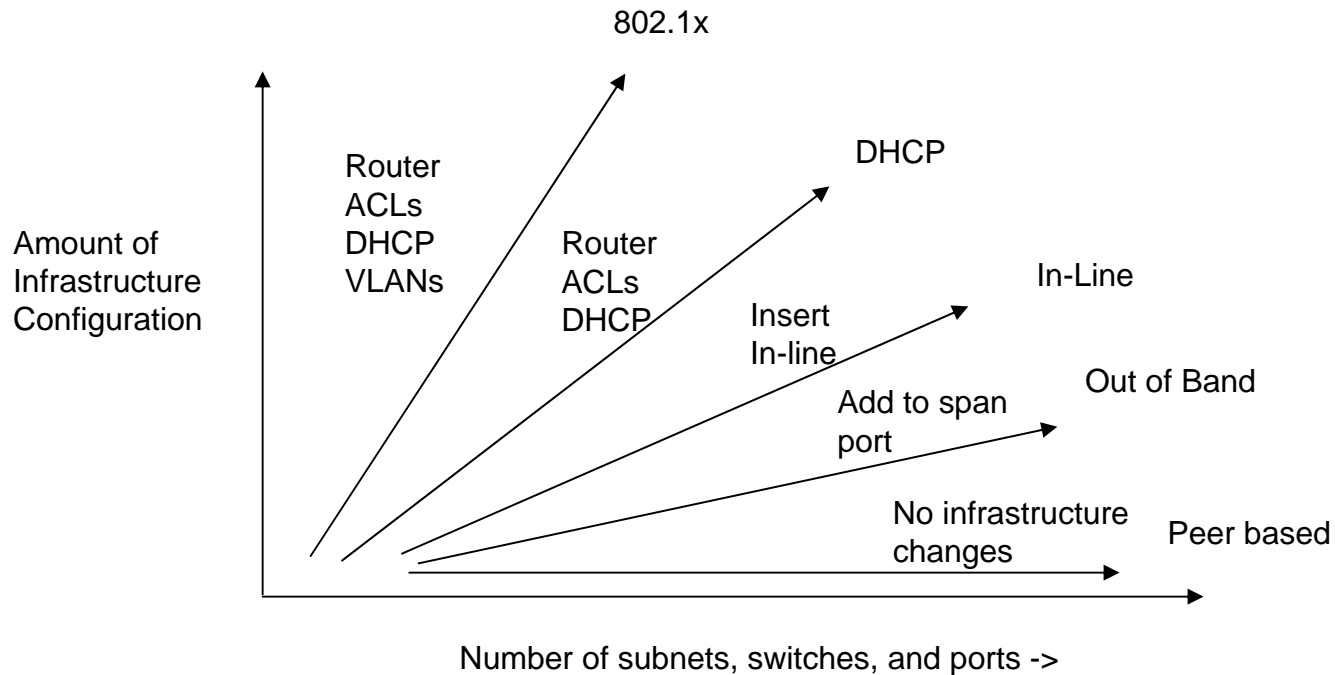


Peer Based NAC

- Network Impact
 - None to minimal
- Endpoint Impact
 - Agent on most endpoints
- Scalability Considerations
 - Agents ~ Endpoints



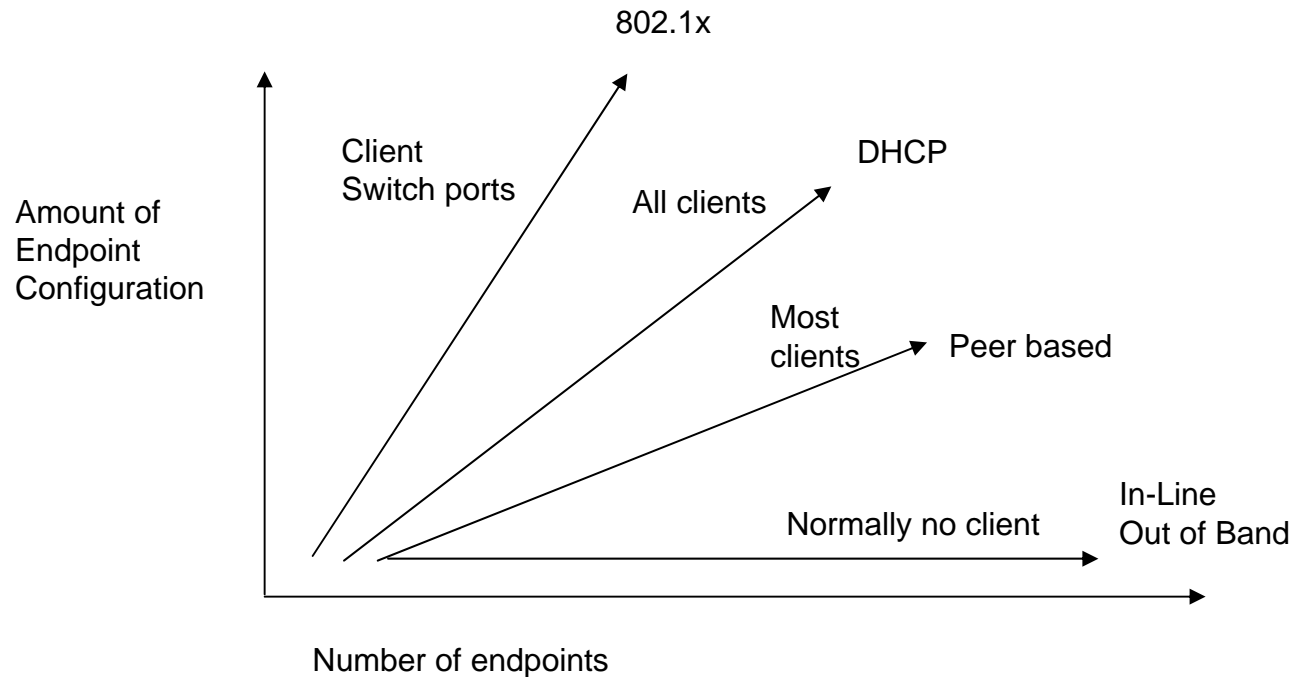
Infrastructure Configuration Effort



Infrastructure configuration effort is highest when an organization has more network equipment diversity such as: managed and unmanaged switches, different vendors for routers, switches, WLANs, and different revs of the software.



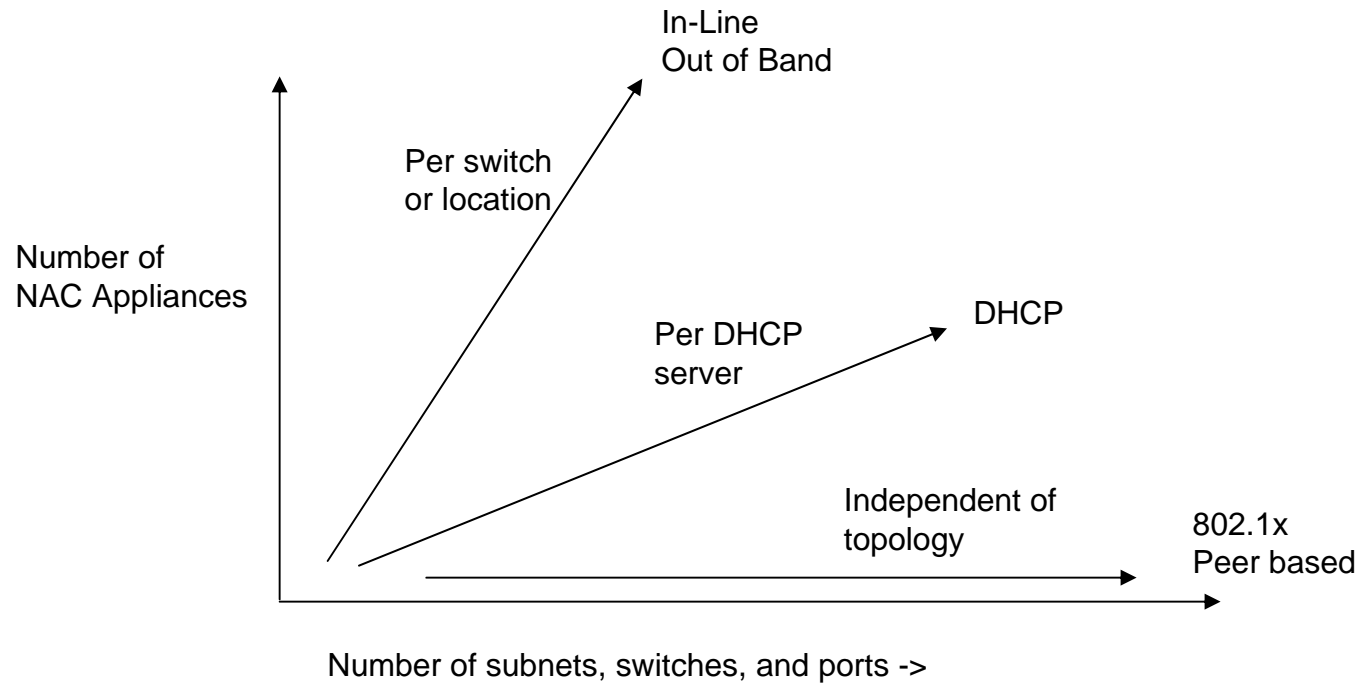
Endpoint Configuration Effort



Endpoint configuration effort is highest when there are diverse endpoints such as different endpoint OS, unmanaged endpoints, or many embedded devices



NAC Appliance Count



NAC appliance count is more critical when the networks, servers, and data centers are distributed across many locations



Operational Costs

- One time
 - Central policy server installation and configuration
 - Policy definition (depending on product)
 - Client rollout, imaging, distribution
- Recurring
 - Subnet configuration
 - impacts routers, switches, DHCP servers
 - Port configuration
 - impacts switches
 - Policy updates
 - impacts tests, policies
 - Help desk



Summary

- Identify areas requiring special attention
 - Infrastructure diversity
 - Network distribution
 - Endpoint diversity
- Select NAC solutions that match the security needs and fit the network
- By using a solution that complements the network, ROI is greatly improved

