Cisco Network Admission Control (NAC) Architectures

Cisco MidAtlantic Users Group Meeting

January 2009

Rob Chee

CCIE #8188

rchee@netcraftsmen.net

Agenda

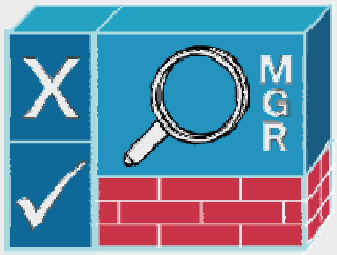
- NAC Overview
- Cisco NAC Terminology
- Cisco NAC Architectures

NAC Overview

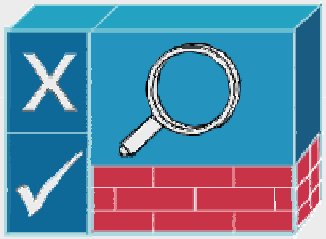
- **Security Policy Enforcement**
  - Enforce the company security policies
  - Minimize attack vectors used by worms and viruses
  - Meet compliance requirements
- **Enable granular network access**
  - Ensure only authorized users can access the network
  - Easier guest user access
- **Network Inventory (secondary measure)**
  - Reports show computer information
  - Computer MAC Addresses shown in certified device list and online users list

NAC Overview > NAC Components

- **NAC Appliance Manager (NAM)**
  - Central management
  - All policy configuration done here
  - All licensing tied to MAC on this device

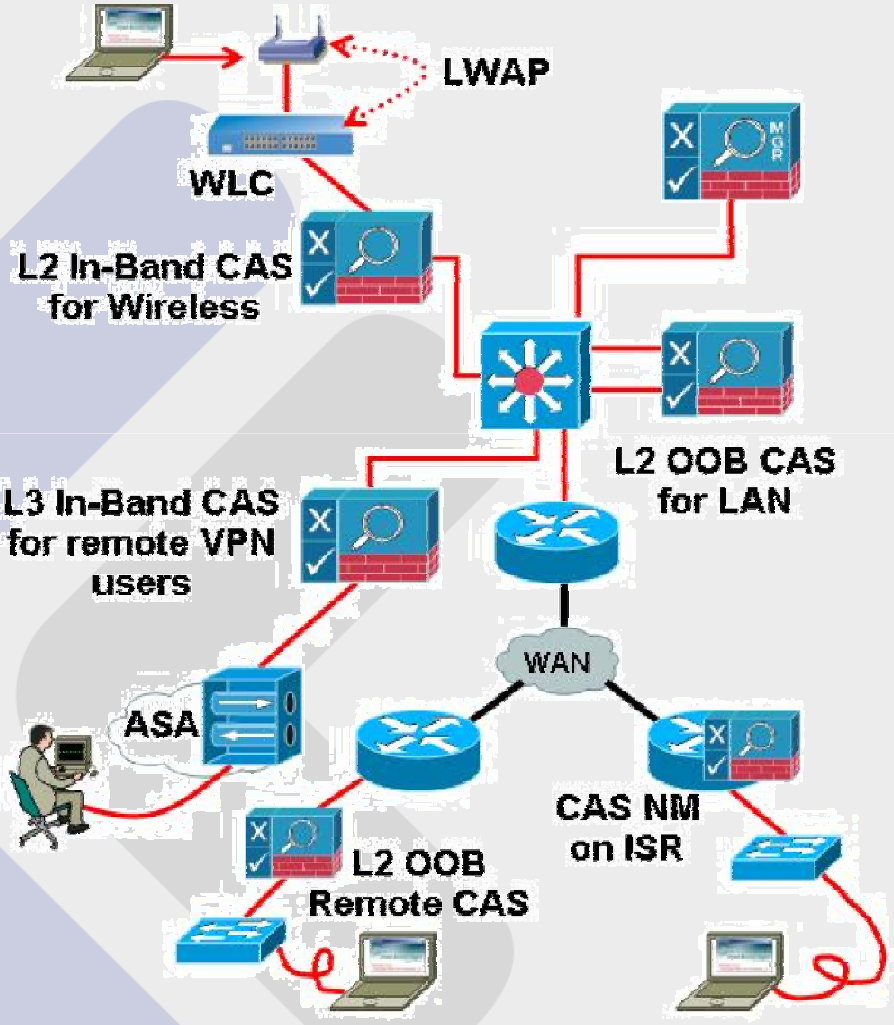


- **NAC Appliance Server (NAS)**
  - Enforcement point
  - Each NAS can only support one mode (L3 OOB Real IP GW, L2 IB VG,…)



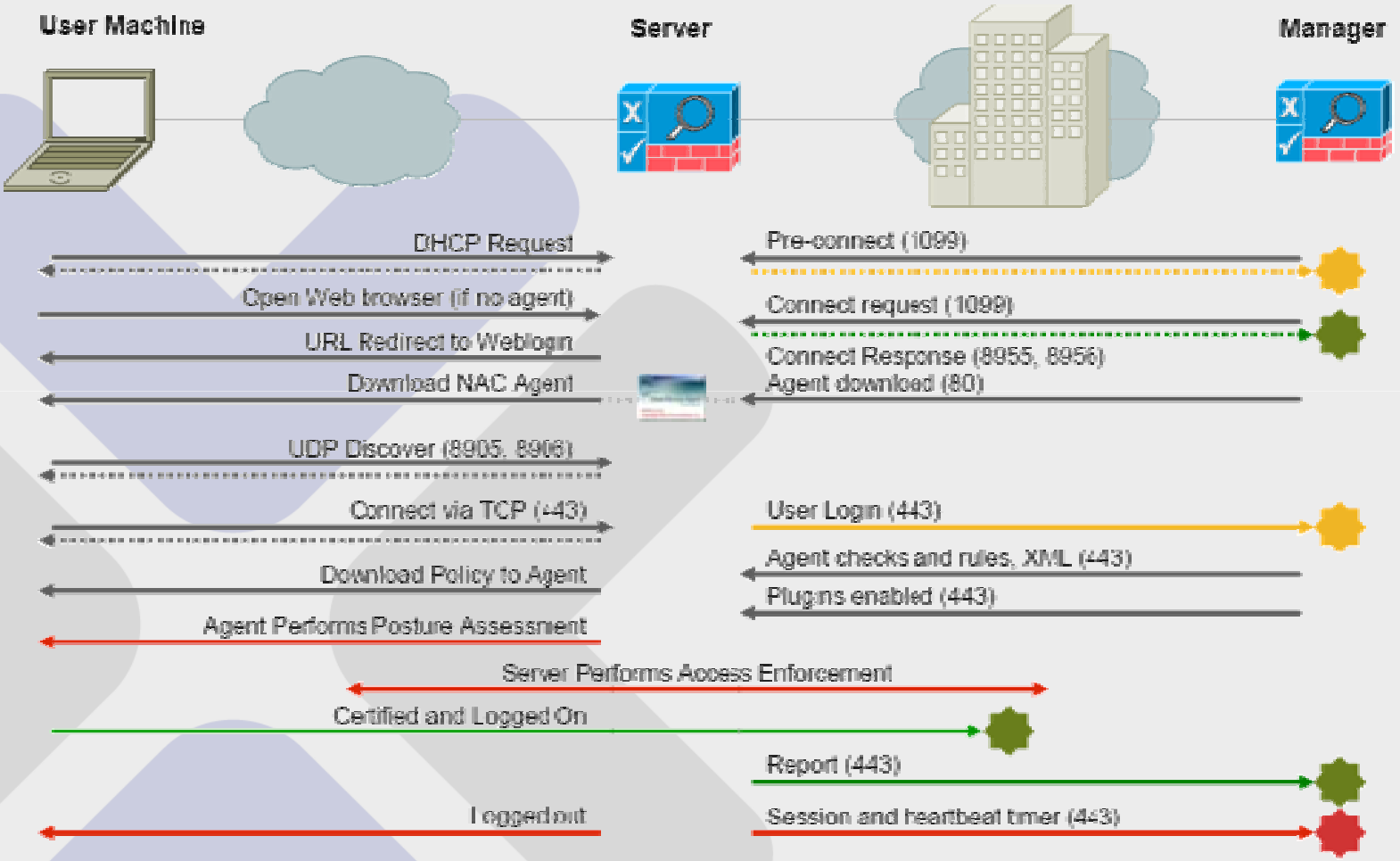
- **Agent**
  - NAC Agent (aka Clean Access Agent)
  - Web Agent (aka Temporal Agent)
  - No remediation

NAC Overview > High Level View



From Cisco Live 2008
"Deploying NAC"

NAC Overview > Traffic Flows



From Cisco Live 2008 "Deploying NAC"

NAC Overview > PCI Compliance

PCI Requirement Number	Description
5	Use and regularly update anti-virus software
6	Develop and maintain secure systems and applications
7	Restrict access to cardholder data by business need-to-know
12	Maintain a policy that addresses information security

From Cisco Live 2008: Enforcing PCI Security Compliance with Cisco PACE

NAC Overview > The Process

Steps
1. Authenticate and Authorize
2. Scan and Evaluate
3. Quarantine (if necessary)
4. Update and Remediate (if necessary)

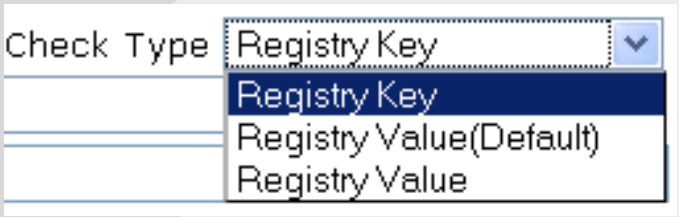
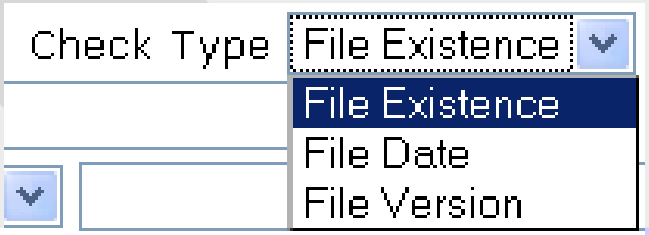
NAC Overview > The Process

- Authentication
  - Manual Login
  - VPN SSO
  - AD SSO

- Authorization/User role
  - Login name
  - RADIUS attributes
  - LDAP attributes

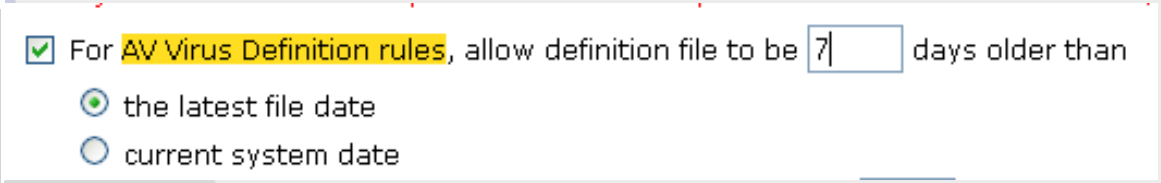
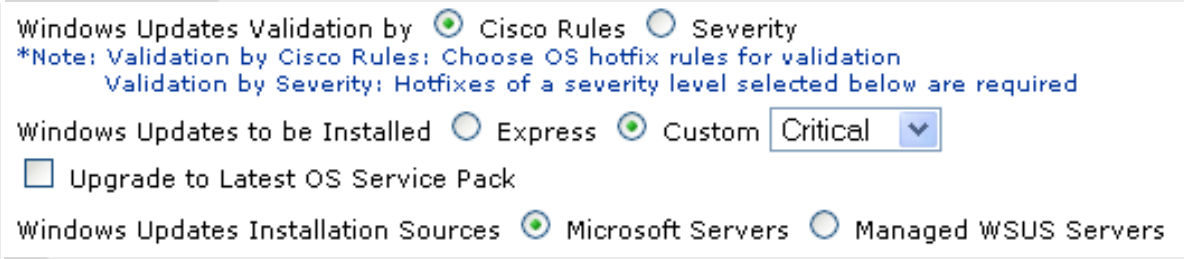
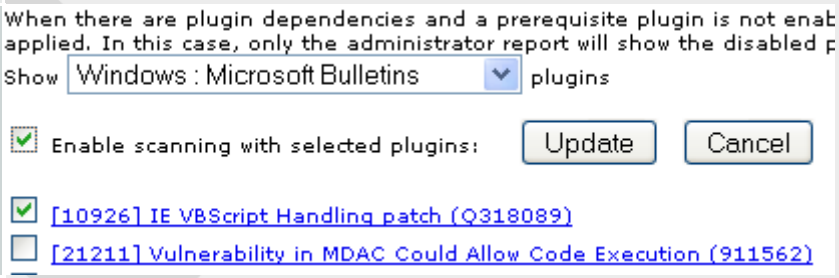
NAC Overview > The Process

Authenticate and Authorize | Scan and Evaluate | Quarantine | Update and Remediate

Application Check (check shown)	
Service Check (check shown)	
Registy Check (check shown)	
File Check (check shown)	

NAC Overview > The Process

Authenticate and Authorize → Scan and Evaluate → Quarantine → Update and Remediate

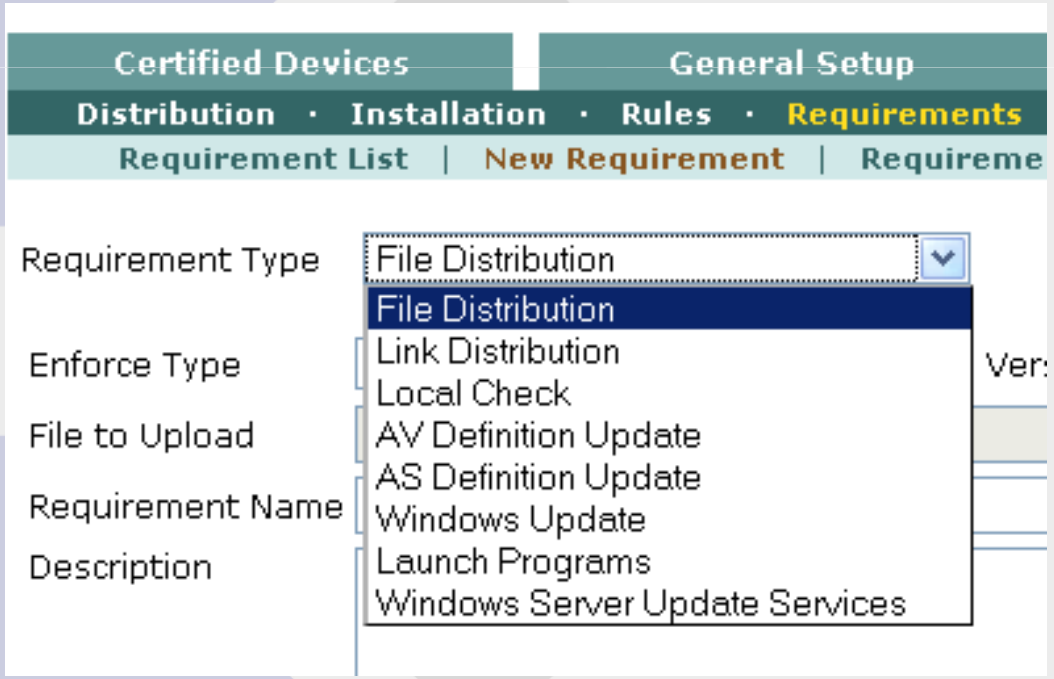
AV/AS Updates (requirement-rule shown)	
Microsoft Updates (requirement shown)	
Nessus Scans (Plugins shown)	

NAC Overview > The Process

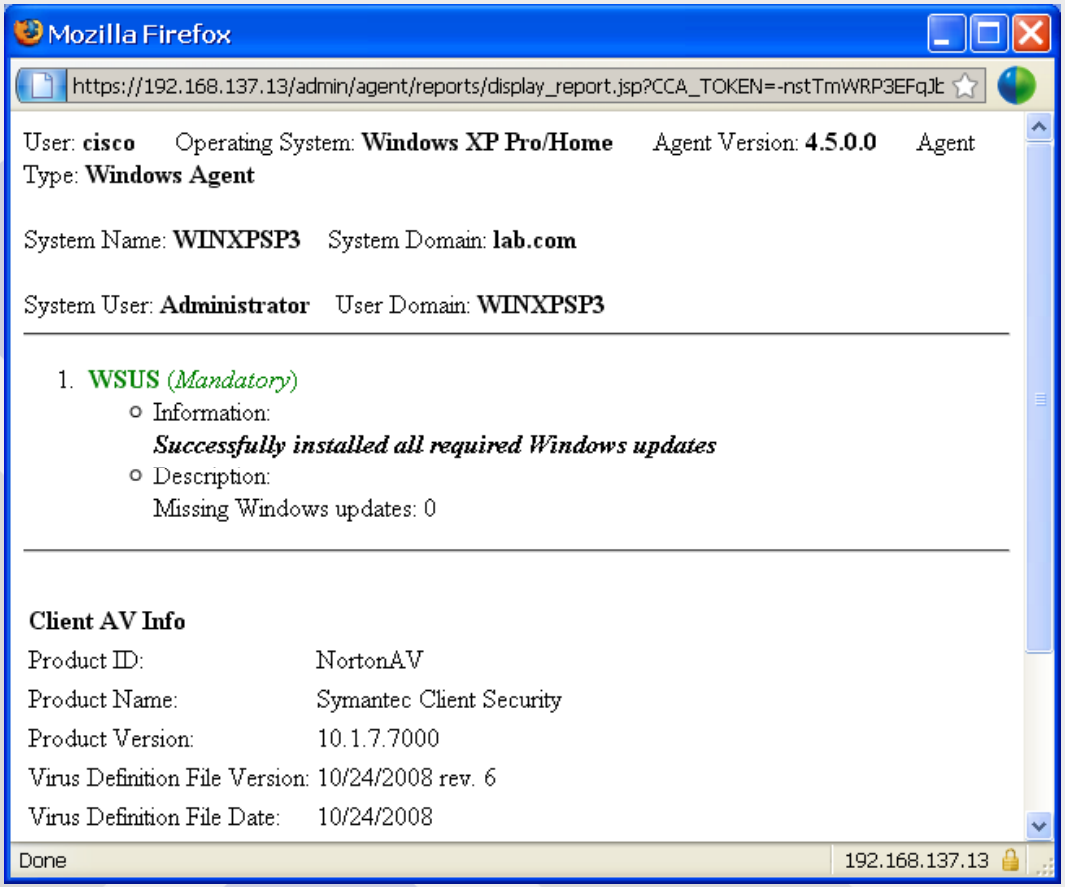
- Place in quarantine/temporary role for remediation
- Allow access to only remediation/update resources
  - Microsoft Update Server
  - Antivirus Definition Update Server

NAC Overview > The Process

Authenticate and Authorize → Scan and Evaluate → Quarantine → Update and Remediate



NAC Overview > Network Inventory



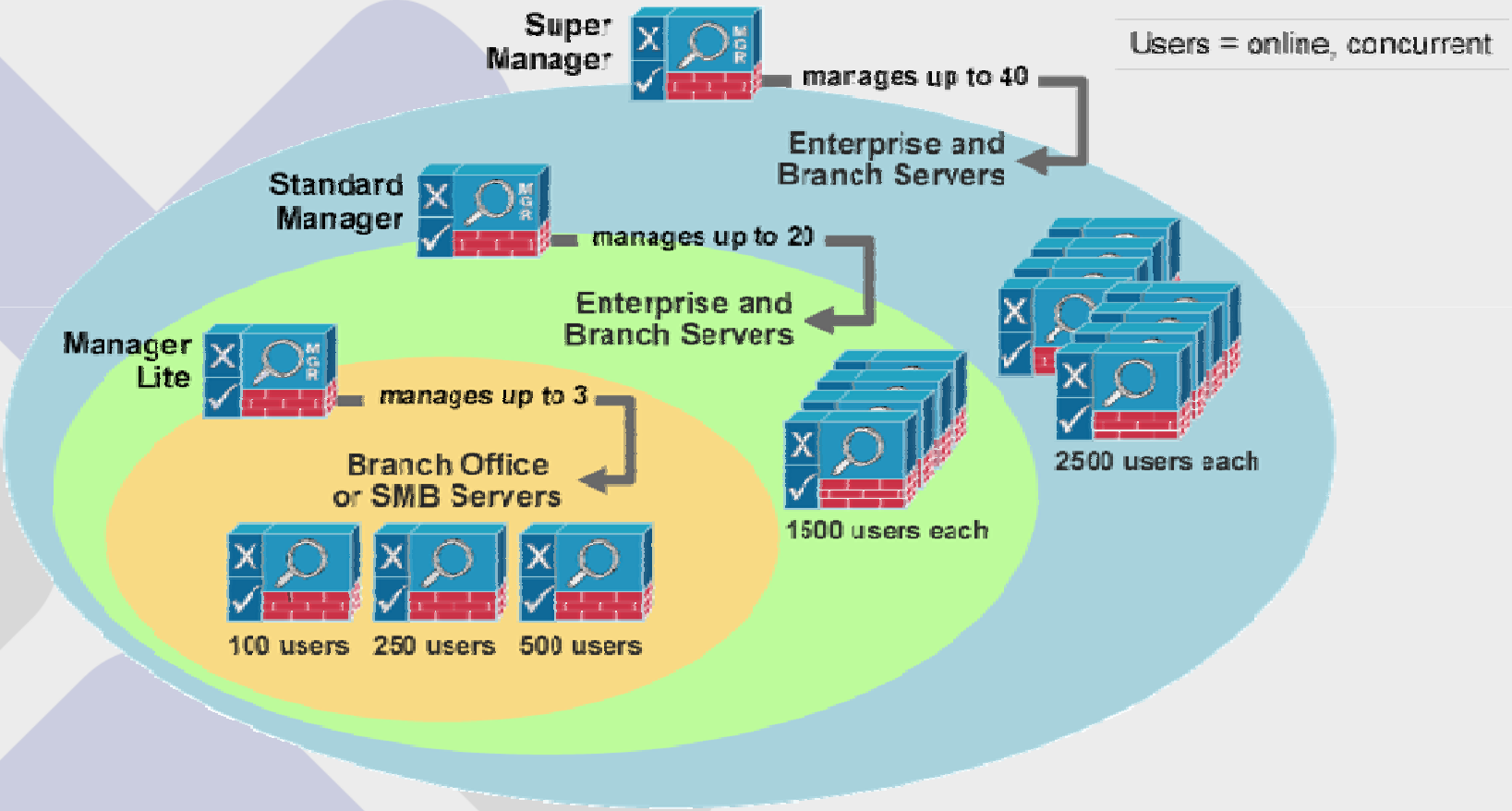
Report

Certified Device List

Certified Devices 1-1 of 1 | First | Previous | Next | Last |

CCA Server	MAC Address	User	Provider	Role	VLAN	Time	Location	
192.168.4.10	00:0C:29:FA:5B:7B	cisco	Local DB	Employee	X	2009-01-13 20:42:39		

NAC Overview > Sizing



From Cisco NAC Chalktalk 1

Agenda

- NAC Overview
- Cisco NAC Terminology
- Cisco NAC Architectures

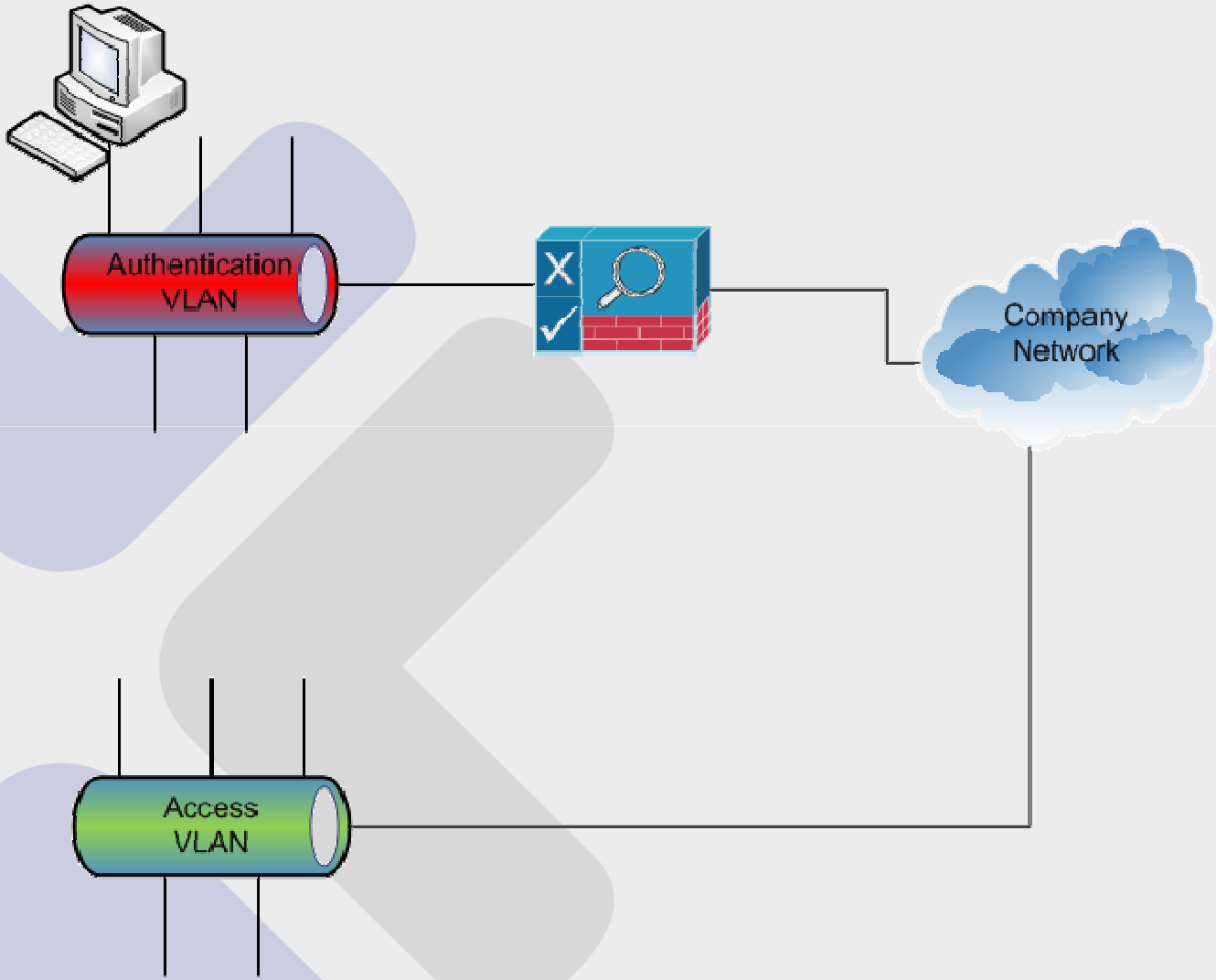
Cisco NAC Terminology

- Authentication VLAN
- Access VLAN
- L2
- L3
- Virtual Gateway
- Real-IP Gateway
- In-Band (IB)
- Out-of-Band (OOB)

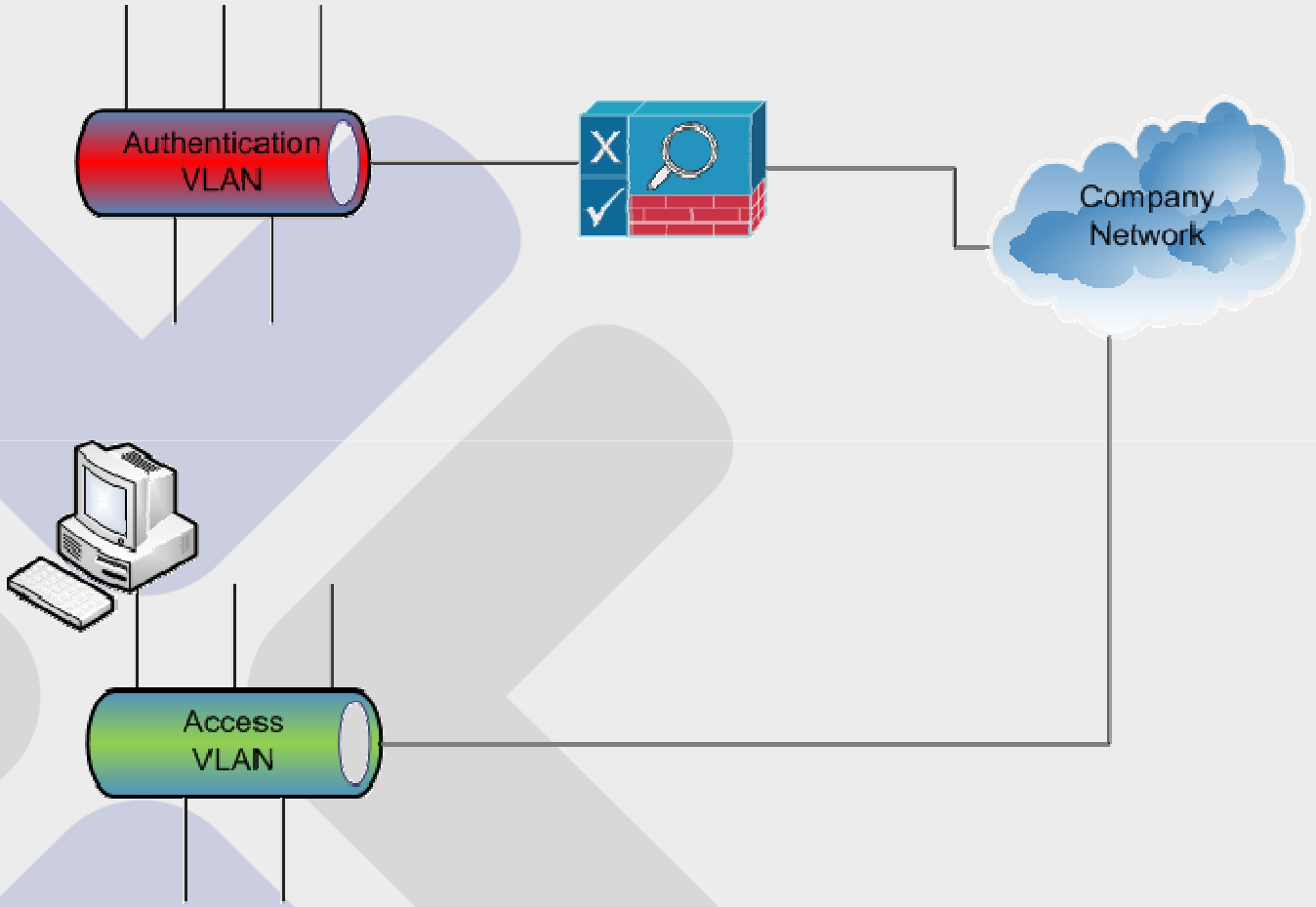
Common Combinations

- L3 OOB Real-IP Gateway
  - Central Deployments
- L3 In-Band Virtual Gateway
  - Remote Access VPN

Cisco NAC Terms > Authentication VLAN

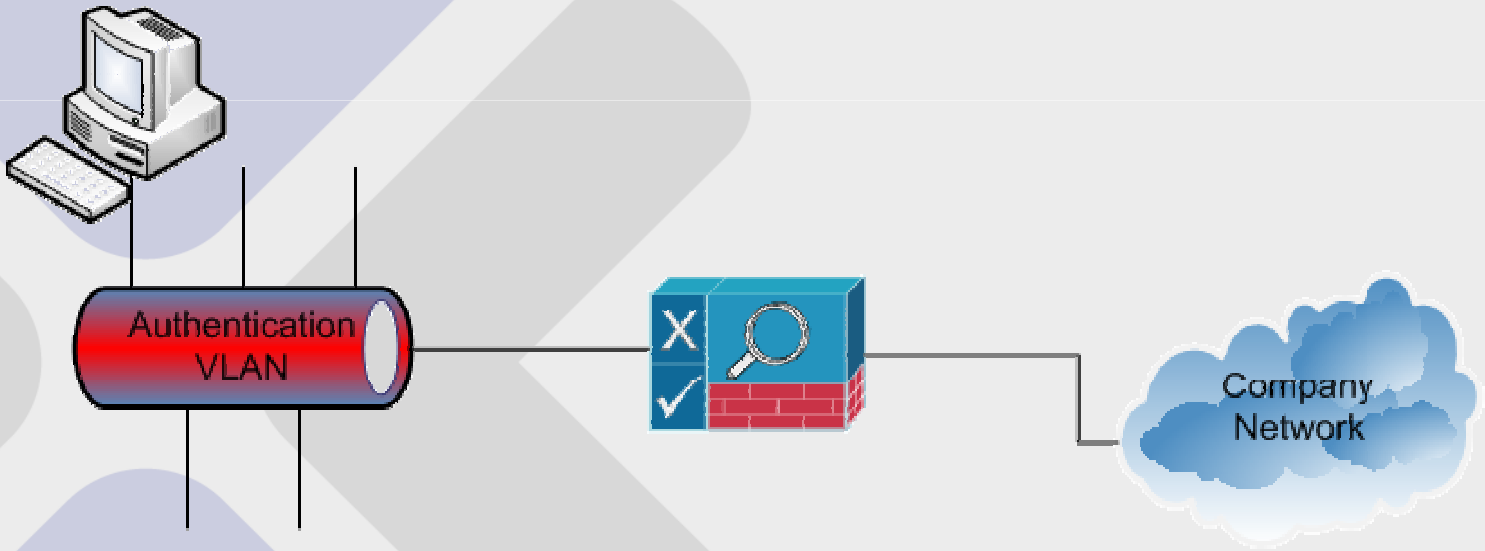


Cisco NAC Terms > Access VLAN



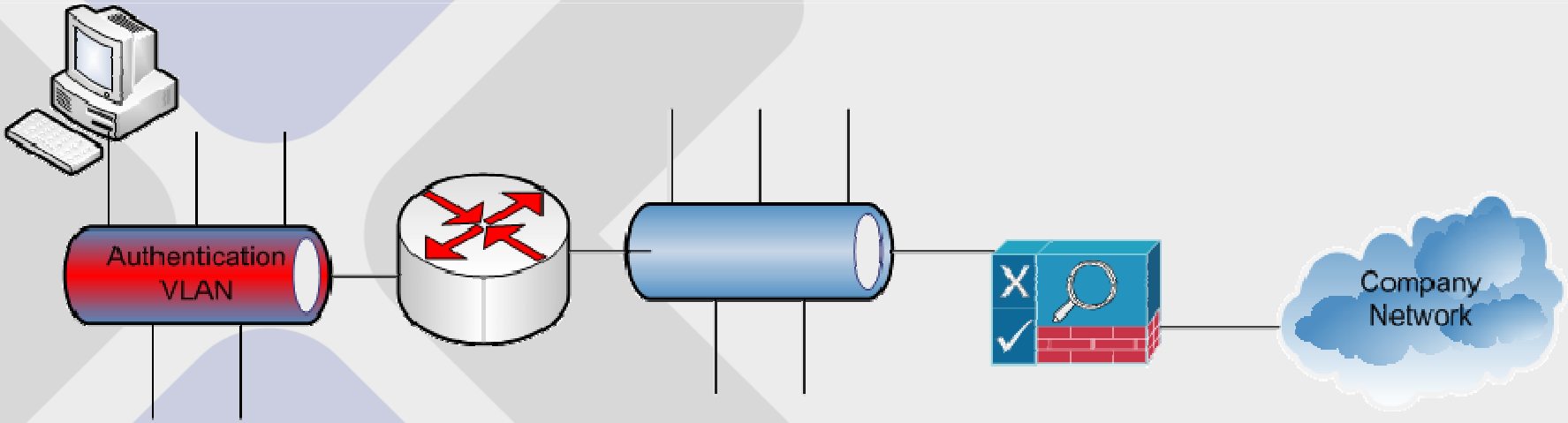
Cisco NAC Terms > L2

- Client is on the same subnet as NAC Server
- NAC Server can see MAC addresses of clients



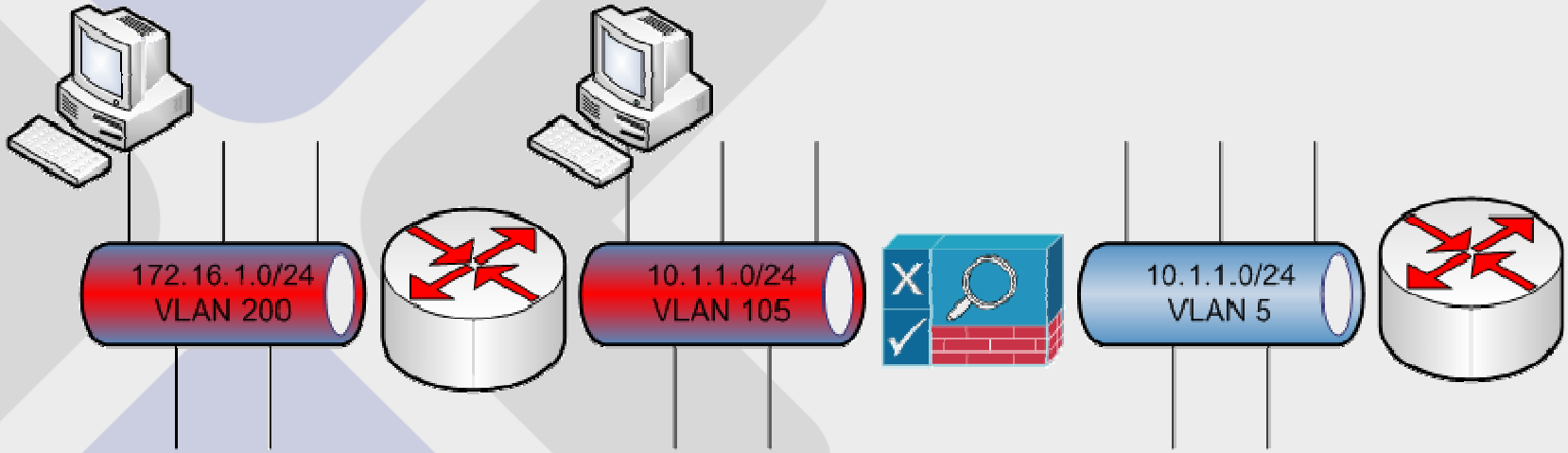
Cisco NAC Terms > L3

- Not on the same subnet as the NAC Server
- MAC address of clients provided by Agent



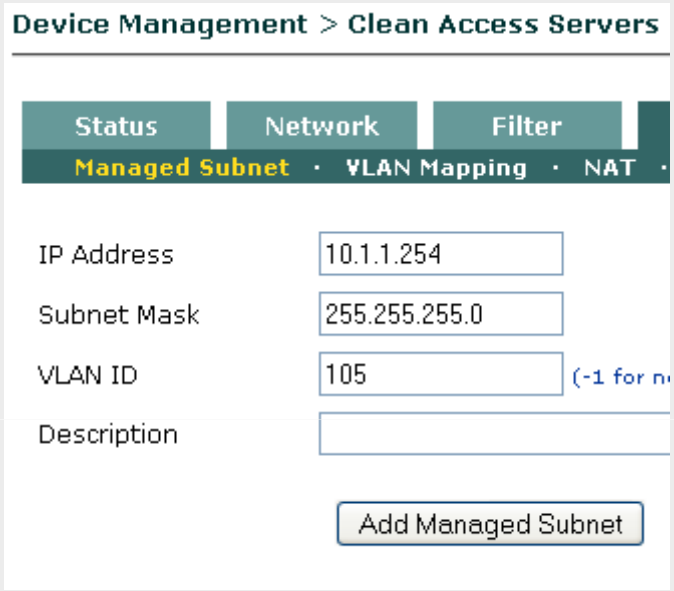
Cisco NAC Terms > Virtual Gateway

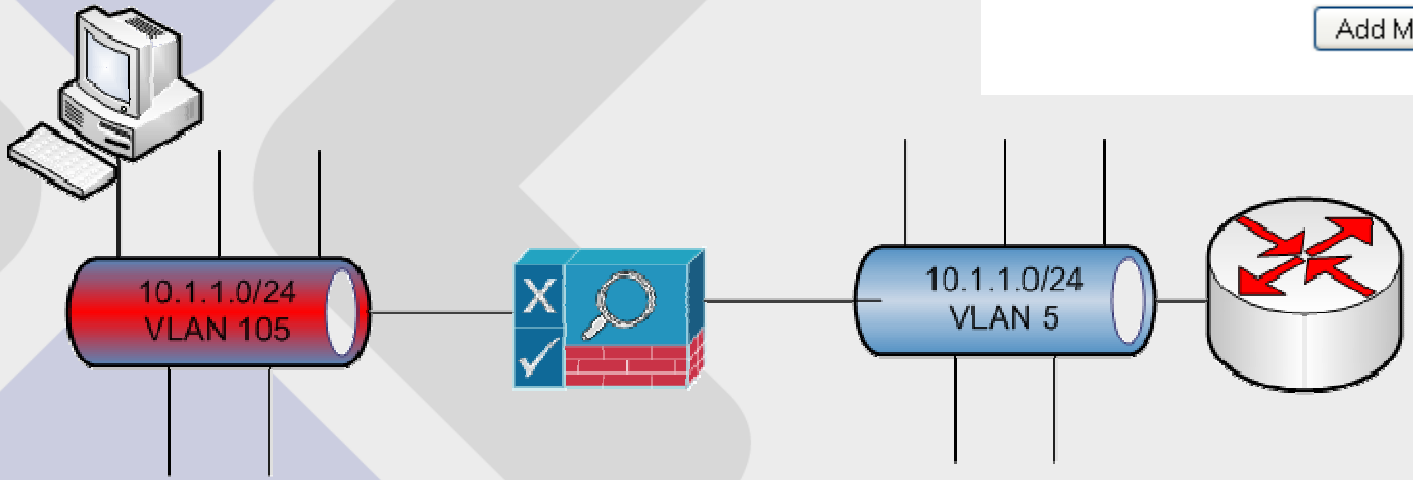
- NAC Server acts as a bridge
- Traffic directed through NAC Server in two ways
  - Route traffic through the NAC Server
  - Accept traffic requests using “Managed Subnets” (proxy arp)



Cisco NAC Terms > Virtual Gateway

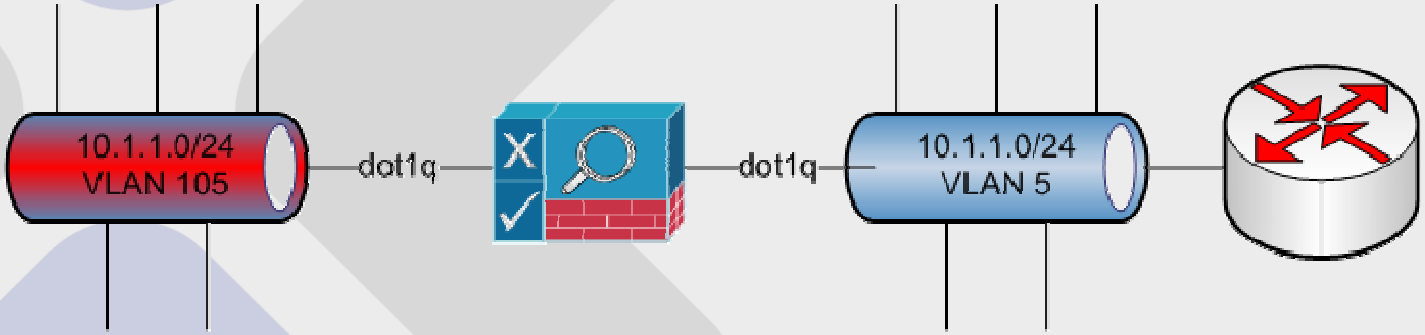
- **Use “Managed Subnets” for L2 adjacent clients**
  - **Use an unused IP in config**
  - **Provides a NAS IP for proxy arp services**





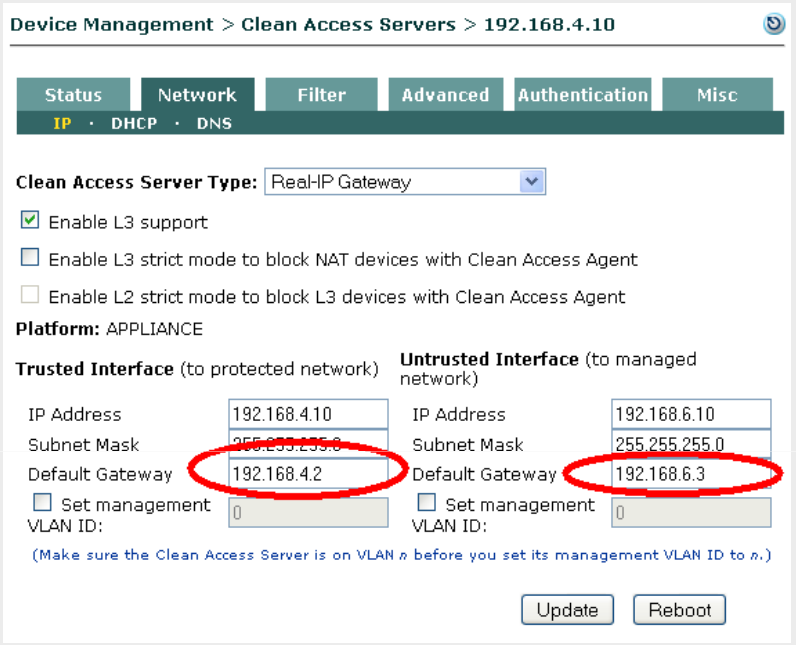
Cisco NAC Terms > Virtual Gateway

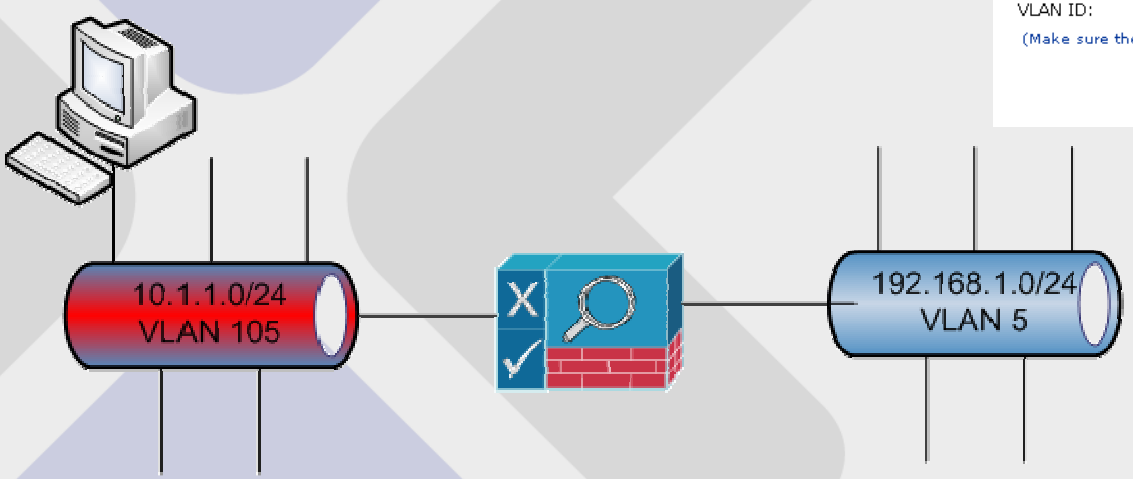
- VLAN Trunking
  - 802.1q VLAN trunk on interfaces is best practice
    - Allows for additional managed VLANs to be easily added
    - Allows for admin interface on separate VLAN
  - Use VLAN Mapping to retag untrusted VLAN to a trusted VLAN
    - Use only when VLAN trunking is used



Cisco NAC Terms > Real IP Gateway

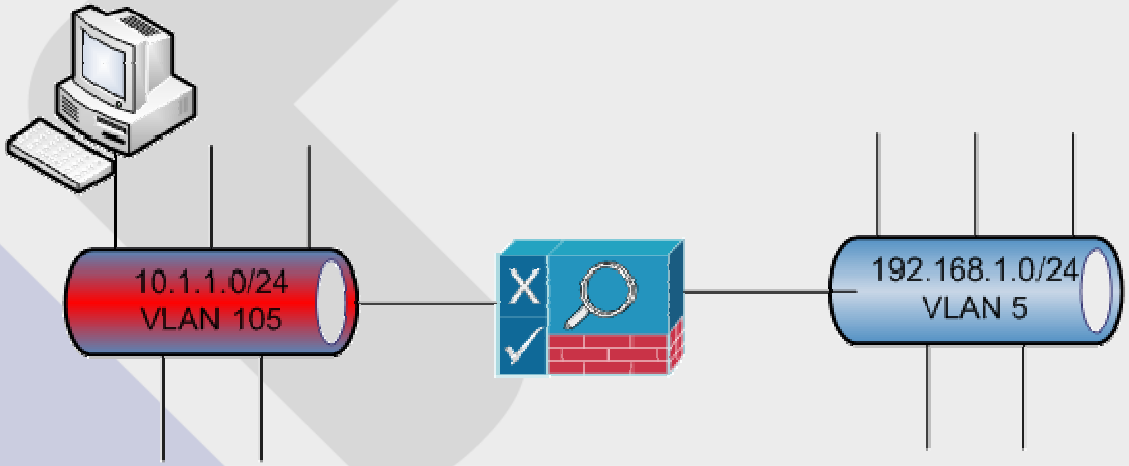
- NAC Server acts as a router
- Routing Protocols are not supported
- Route Configuration Notes
  - Default route is to the internal network
  - Create static routes for authentication VLAN networks in L3 mode





Cisco NAC Terms > In-Band (IB)

- Traffic always flows through the NAC Server
- Mostly used for VPN and Wireless scenarios
- Advantages
  - Can limit bandwidth based on policy
  - User role policy enforced on NAC Server
- Disadvantages
  - Bandwidth limited by what can flow through the NAC server

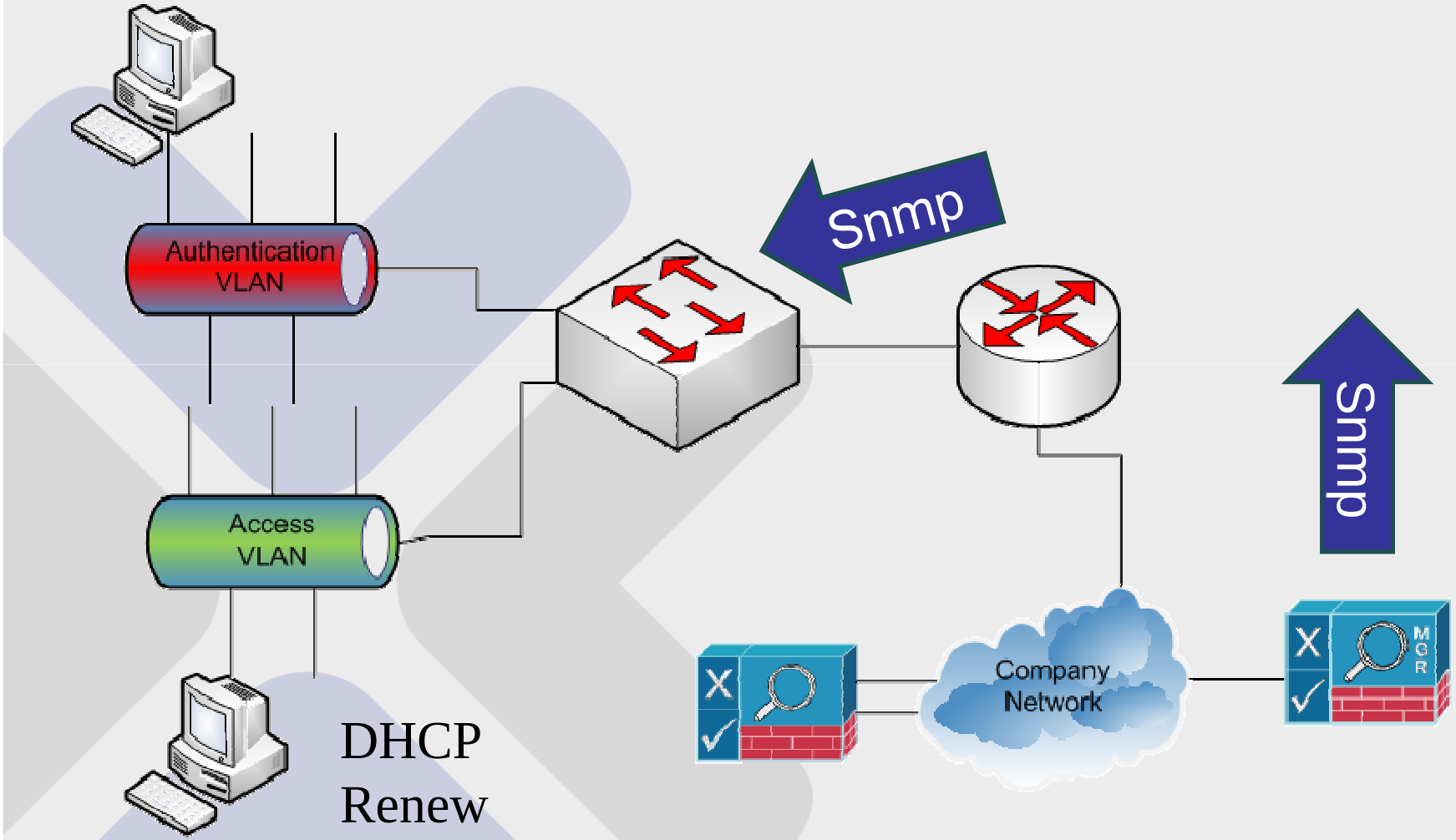


Cisco NAC Terms > Out-of-Band (OOB)

- Traffic is still in-band for authentication

- Traffic moved OOB by VLAN change on access switch
- VLAN change via SNMP from NAM to switch
- Removes BW limitation by NAC Server
- Relies on using Cisco supported switches

Cisco NAC Terms > Out-of-Band (OOB)



Cisco NAC Terms > Out-of-Band (OOB)

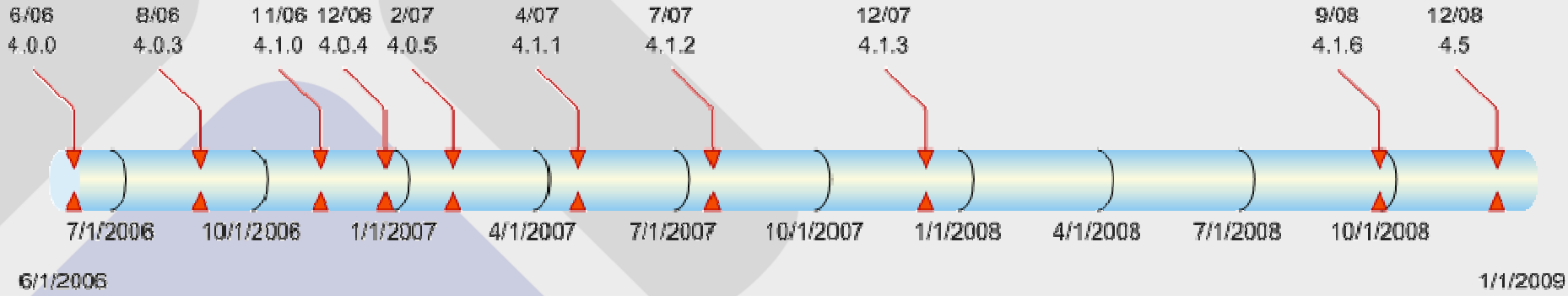
- Advantages
  - Bandwidth not limited by NAC Server
- Disadvantages
  - User role not limited by NAC Server
  - Relies on reliable NAM to switch communication

Agenda

- NAC Overview
- Cisco NAC Terminology
- **Cisco NAC Architectures**

NAC Architectures Notes

- Showing Common Scenarios
- Best Practices can still change as NAC changes
  - Simplify Login Process
    - (4.0) AD SSO option
  - Updates to assist with IP phone integration
    - (4.1.0) DHCP release/renew through Agent
    - (4.1.1) DHCP release/renew through Agent Stub
  - Enhanced Features
    - (4.5) Wireless can be OOB with NAC 4.5 and WLC 5.1



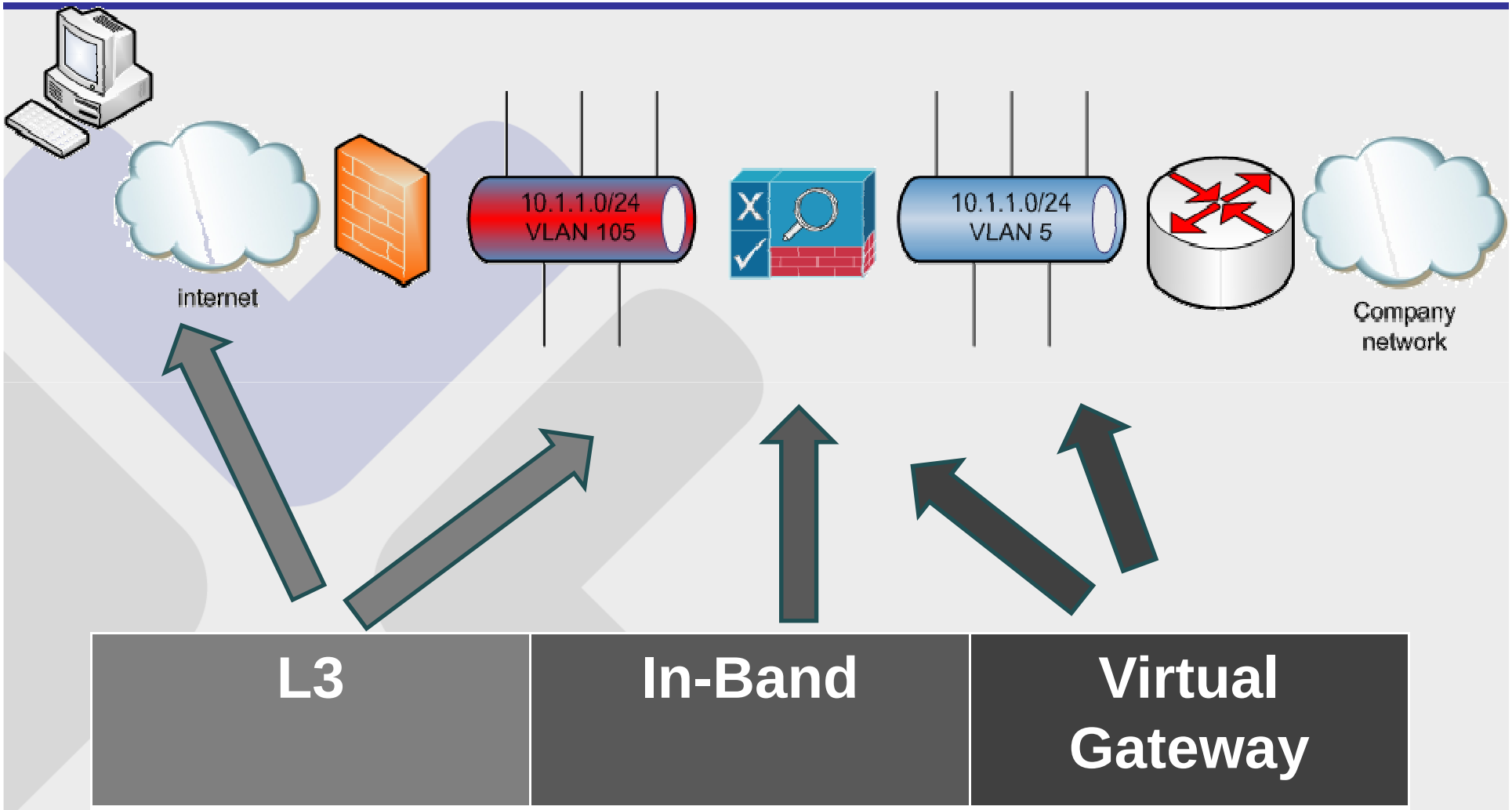
NAC Arch > Mapping

Network Design	NAC Architecture
Remote Access VPN Users	L3 IB Virtual Gateway
Wireless Users	L2 IB Virtual Gateway or L2 OOB Virtual Gateway (ver 4.5)
Collapsed Backbone (VLAN trunking to NAS)	L2 IB or OOB Virtual Gateway
Distributed Backbone (L3 pushed to the edge)	L3 OOB Real-IP Gateway
Remote Office	NAC Server at Remote Office • L2 or L3 IB Virtual Gateway NAC Server at Central Site • L3 OOB Real IP Gateway

NAC Arch > Remote Access VPN Users

- L3 In-Band Virtual Gateway
- VPN SSO when using RADIUS for authentication

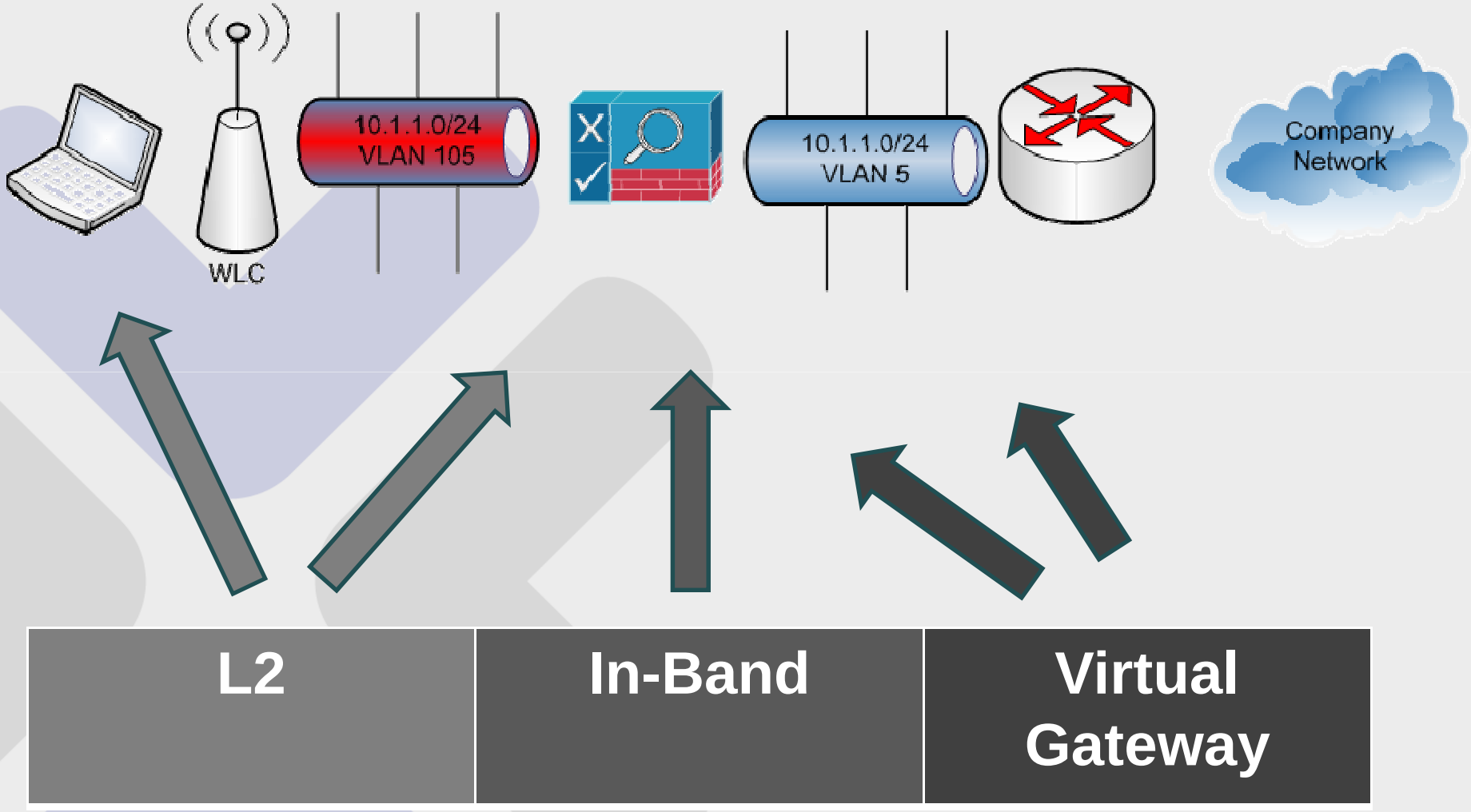
NAC Arch > Remote Access VPN Users



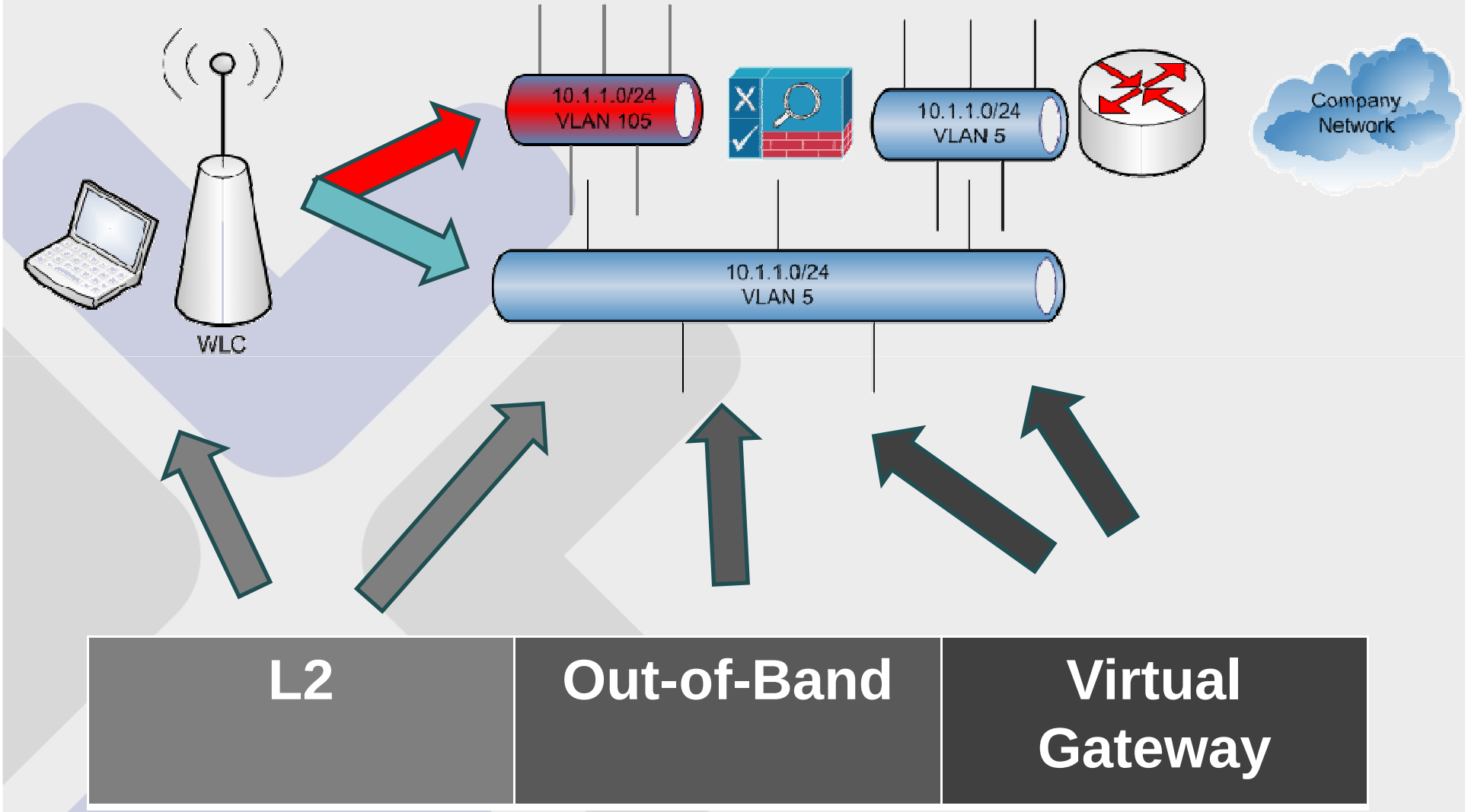
NAC Arch > Wireless Users

- Wireless users must always be L2 adjacent to NAS
- Pre 4.5 was only L2 In-Band Virtual Gateway
- 4.5 allows for L2 Out-of-Band Virtual Gateway

NAC Arch > In-Band Wireless Users

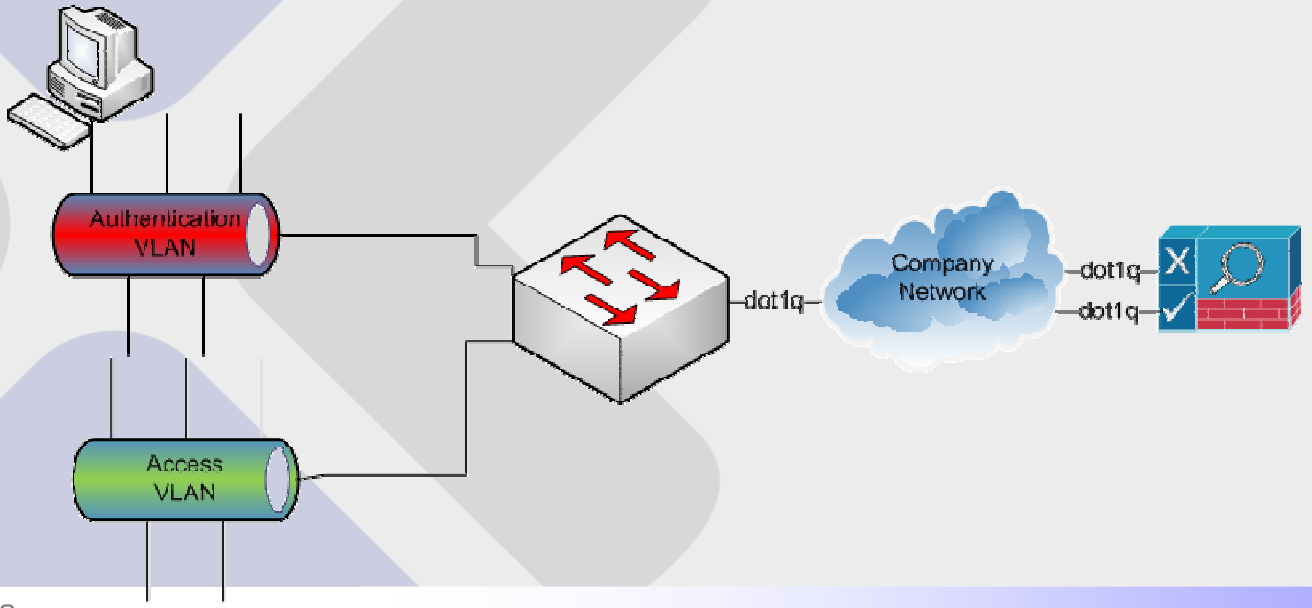


NAC Arch > Out-of-Band Wireless Users



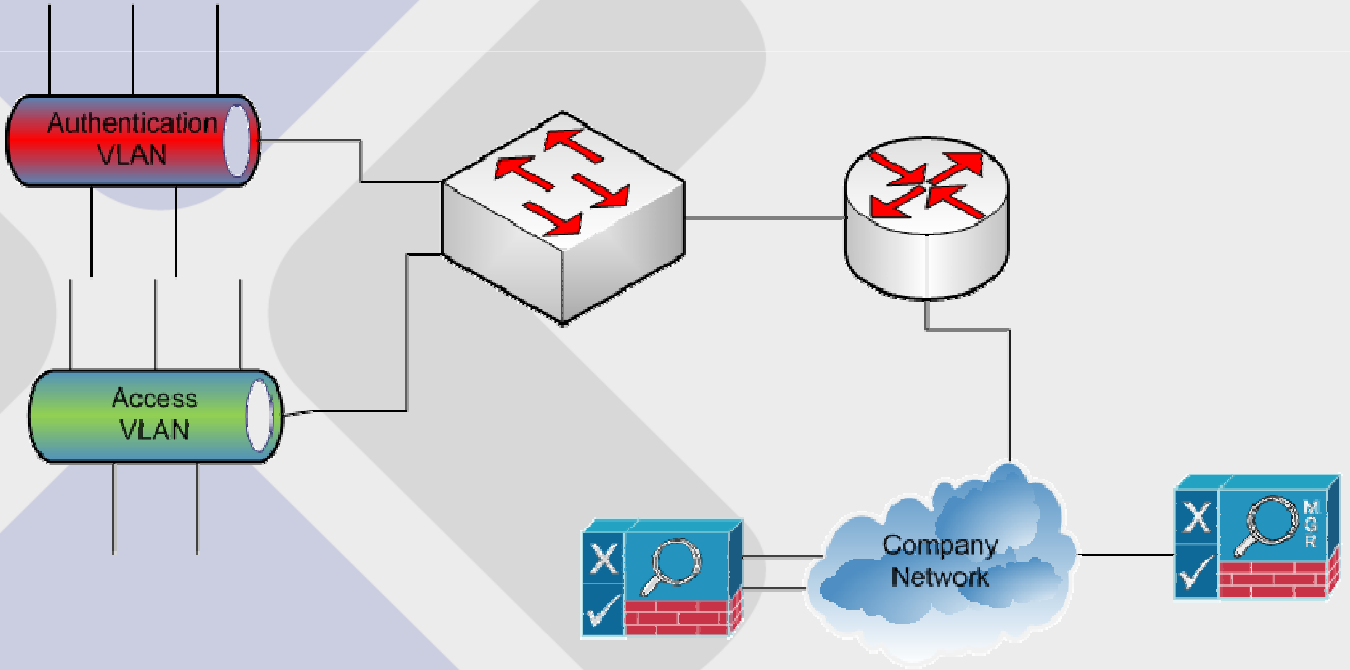
NAC Arch > Collapsed Backbone

- Switches use 802.1q VLAN trunks from access switches to the NAS at the core
- L2 In-Band Virtual Gateway
- L2 Out-of-Band Virtual Gateway
- Not as common



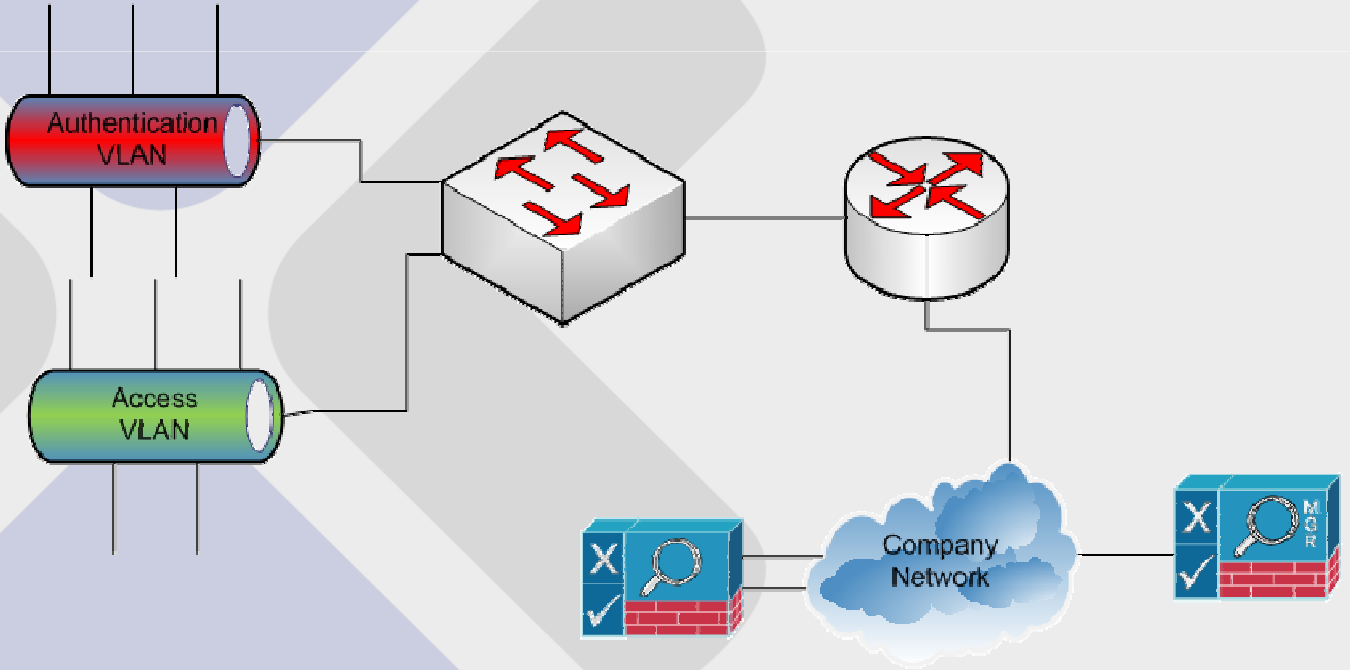
NAC Arch > Distributed Backbone

- L3 pushed to the edge
- L3 Out-of-Band Real IP Gateway
- Relies on Cisco NAC supported switches



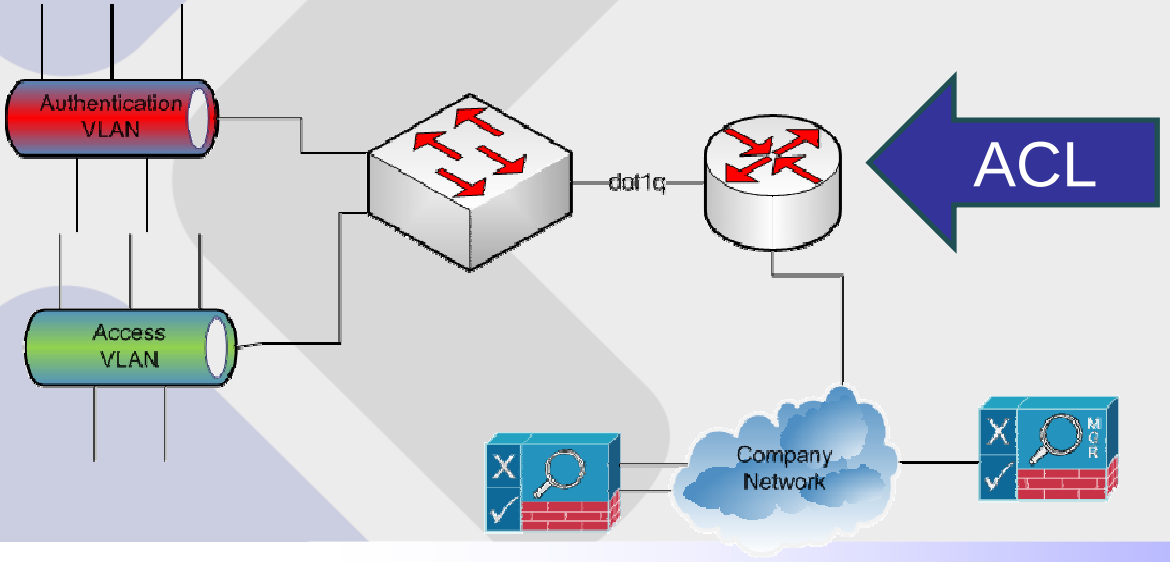
NAC Arch > Dist BBone > Communication Options

- ACL
- PBR
- VRF-Lite
- GRE Tunnel



NAC Arch > Dist BBone > Comm Option > ACL

- Most popular method today
- Restrict authentication VLAN at the edge
- Advantage
  - Easier to implement
- Disadvantage
  - Guest Users need a special URL to login
  - ACLs must be added to all access routers/switches

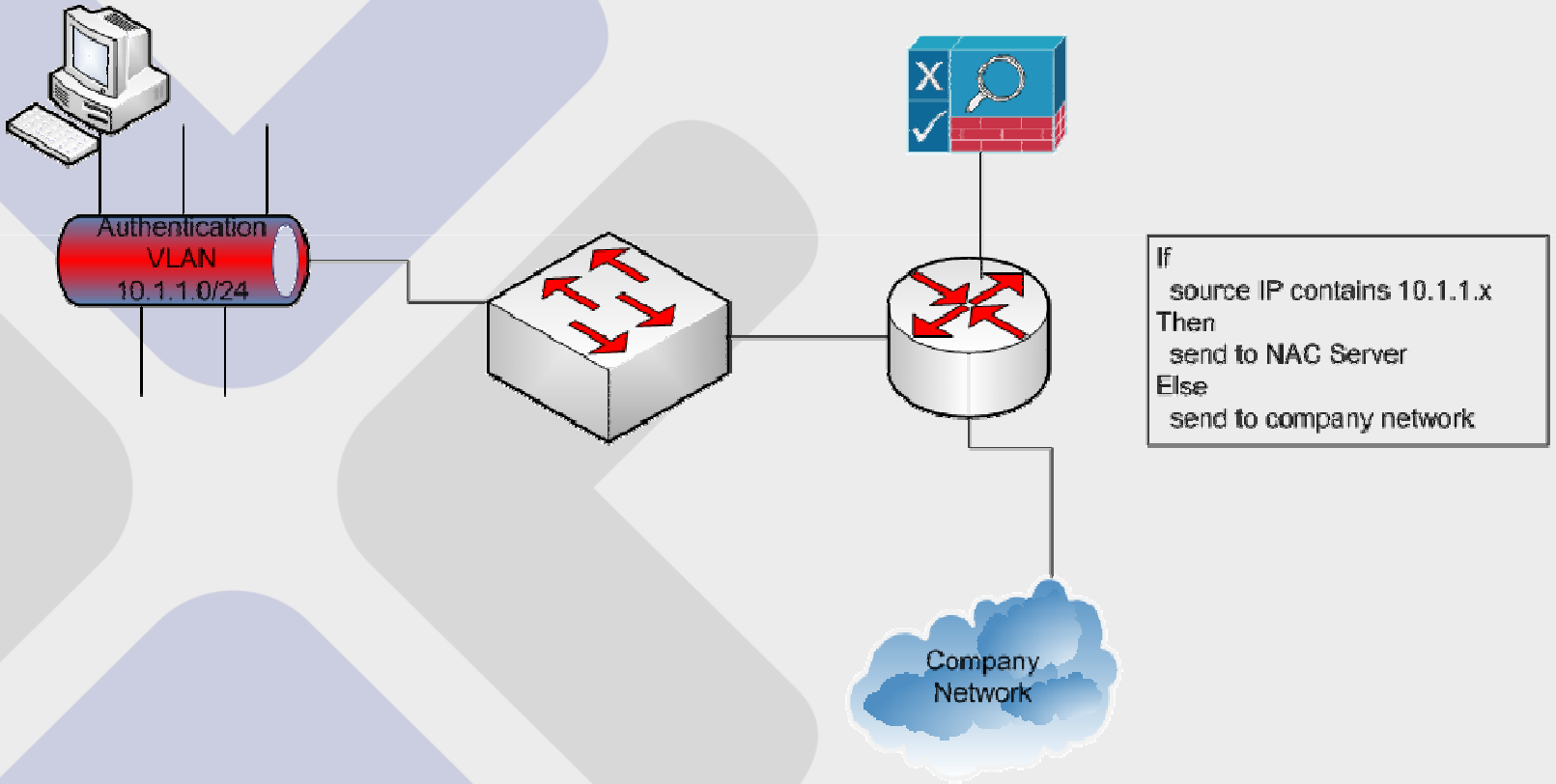


NAC Arch > Dist BBone > Comm Option > ACL

Authentication VLAN ACL	Access VLAN ACL
Ip access-list extended authentication **remark allow NAC Server traffic** permit ip any host 10.1.1.1 **remark allow WSUS updates** permit tcp any host 10.2.2.10 eq 80 **remark allow AV traffic** permit tcp any host 10.2.2.11 eq 80 deny ip any any	Ip access-list extended access **remark Deny Agent traffic** deny udp any any eq 8905 deny udp any any eq 8906 permit ip any any

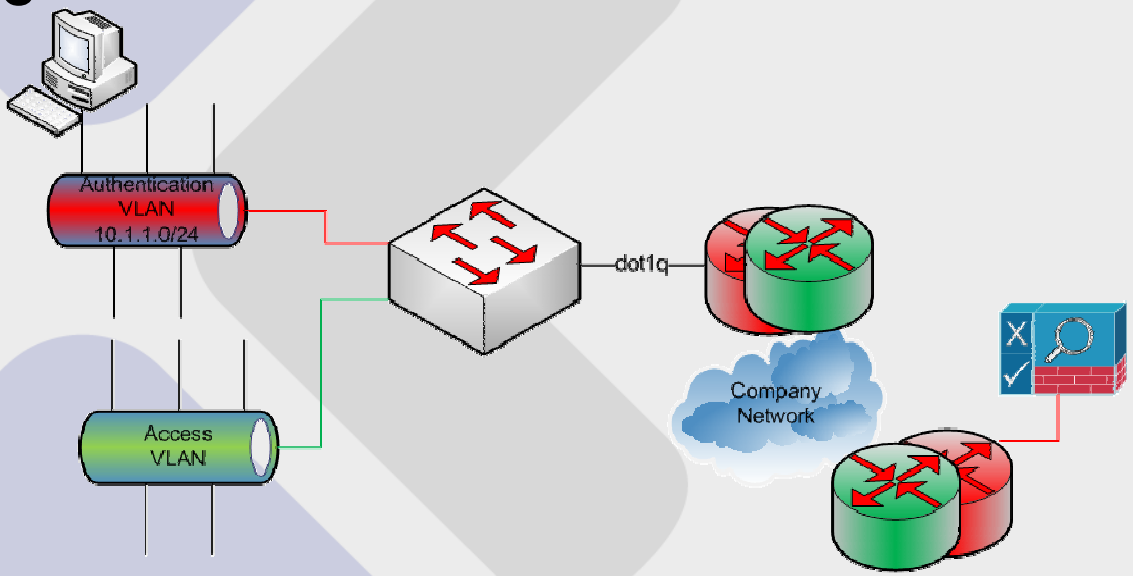
NAC Arch > Dist BBone > Comm Option > PBR

- Base routing decisions based on source IP
- Not Scalable b/c every router needs custom config



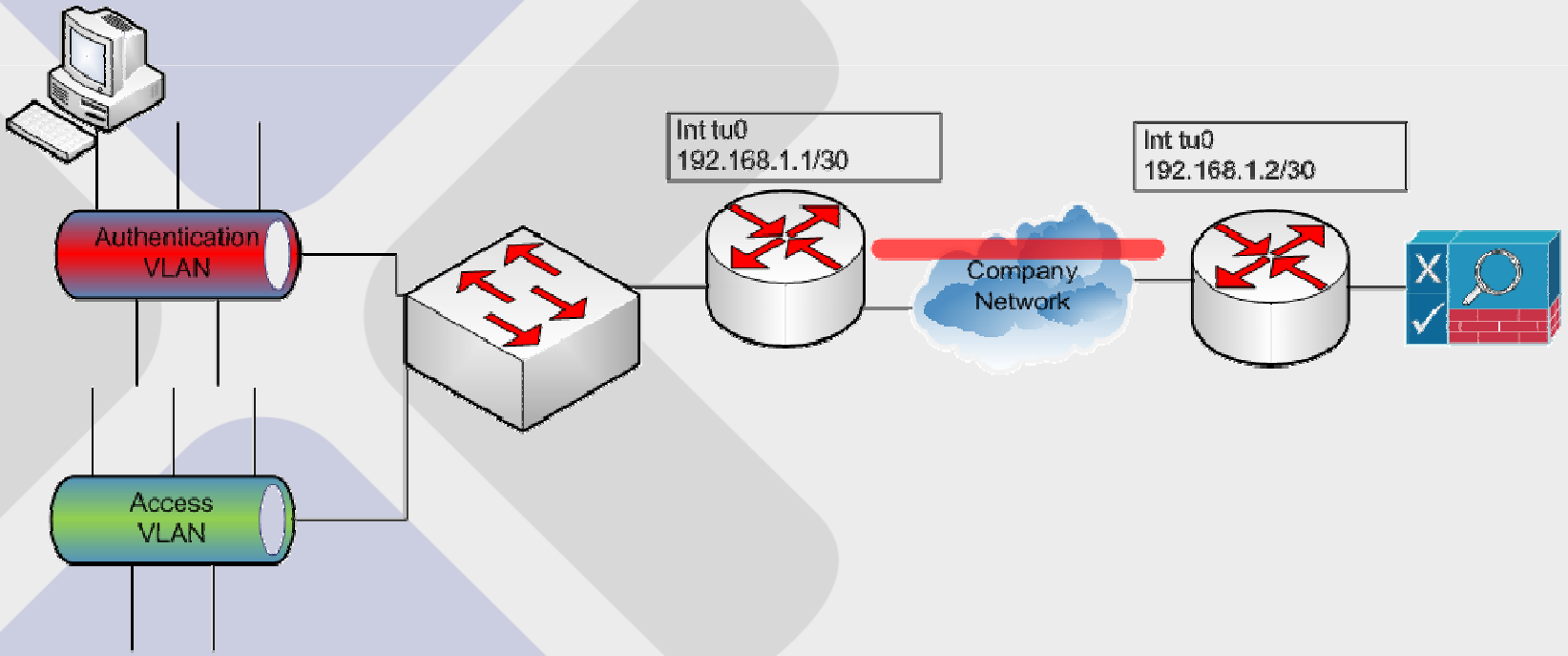
NAC Arch > Dist BBone > Comm Option > VRF-Lite

- Provide a separate routing instance for authentication VLAN traffic
- Adds to complexity
  - New router must have VRF-Lite applied
- Recommended for networks already using VRF-Lite



NAC Arch > Dist BBone > Comm Option > GRE Tunnels

- A tunnel is created between the access layer and NAC Server
- Difficult to scale
- Can be used in conjunction with VRF Lite

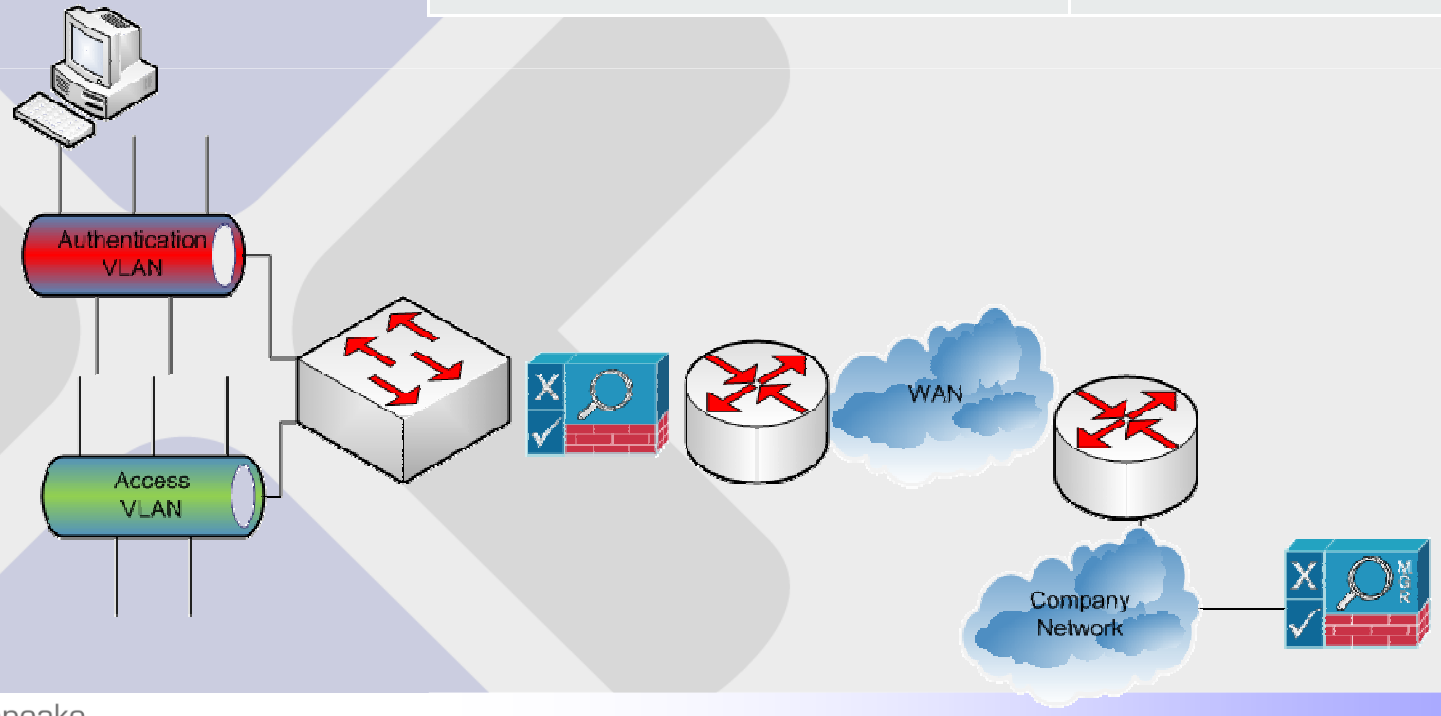


NAC Arch > Remote Offices

- Two Options
  - NAC Server at remote office
  - NAC Server at central office
- NAC Server Placement Guideline
  - Put NAC Server at large remote office
- Traffic Guidelines
  - Apply QoS for NAC traffic (SNMP, NAC ports)

NAC Arch > Remote Offices > Remote Office NAC Server

Description	Architecture
One user subnet at remote site	L2 IB Virtual Gateway
Multiple subnets at remote site	L3 IB Virtual Gateway



NAC Arch > Remote Offices > Remote Office NAC Server

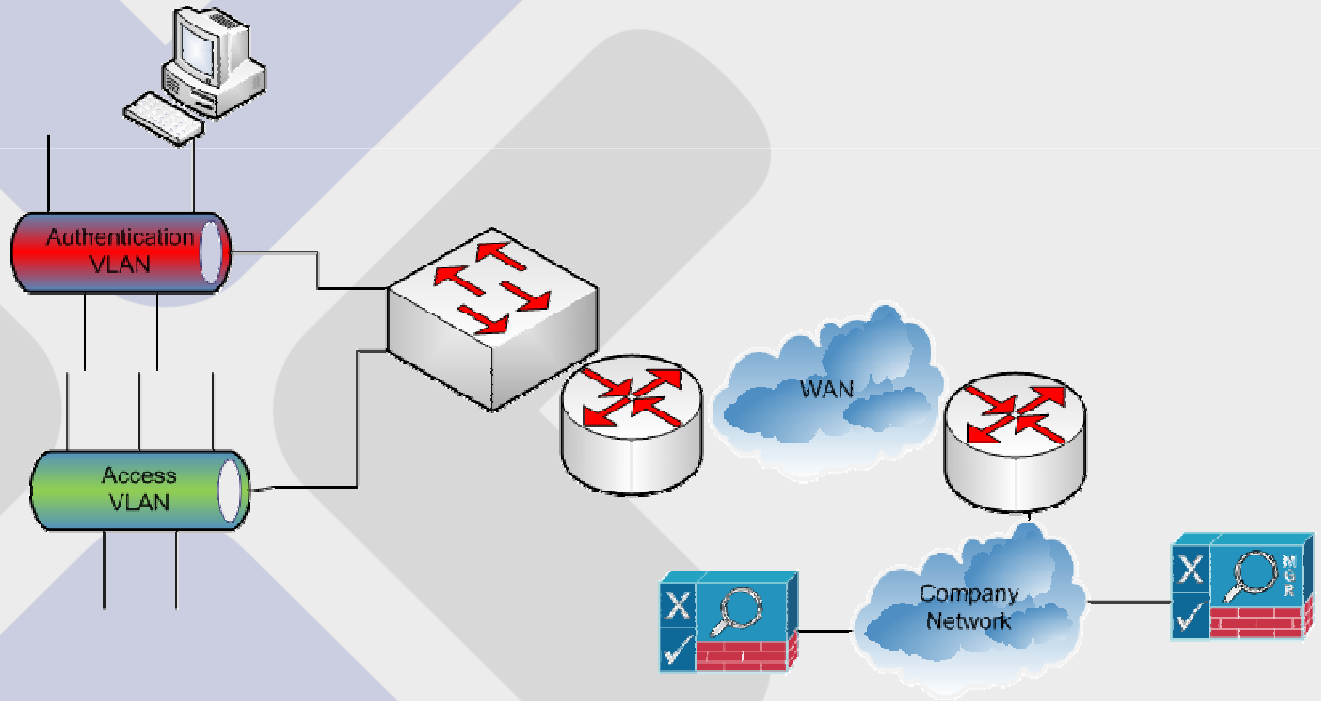
- Can use NAC Module for 2800 and 3800 ISR routers
  - Can support
    - L2 or L3
    - in-band or out-of-band
    - Real IP Gateway or Virtual Gateway
  - Limitations
    - No High Availability
    - No NAC Profiler support
    - No wireless OOB
    - 100 User Maximum

NAC Arch > Remote Offices > Remote Office NAC Server

- Advantage
  - In-Band can limit traffic and bandwidth access by role
  - Fail-Open option
- Disadvantage
  - Cost
  - More devices to upgrade

NAC Arch > Remote Offices > Central Office NAC Server

- L3 OOB Real IP Gateway
- Use QoS to ensure SNMP and NAC traffic takes precedence



NAC Arch > Remote Offices > Central Office NAC Server

- Advantage
  - Less Expensive
- Disadvantage
  - Less Managablility
    - No bandwidth limit
    - No traffic policy limit
  - More traffic on the WAN
    - Agent updates
  - Rely on reliable WAN connectivity

Summary

- NAC Overview
- Cisco NAC Terminology
- Cisco NAC Architectures

References

- Main Cisco NAC page
  - http://www.cisco.com/go/nac/appliance
- Cisco NAC Chalk Talks
  - http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps8418/ps6128/prod_presentation0900aecd80549168.html
- Cisco NAC Wiki
  - http://supportwiki.cisco.com/ViewWiki/index.php/Category:Cisco_NAC_Appliance_(Clean_Access)
- Miami of Ohio Mailing List
  - http://listserv.muohio.edu/scripts/wa.exe?A0=cleanaccess
- NAC Book by Jamey Heary
- Netcraftsmen Security Blog
  - http://security-blog.netcraftsmen.net