



Comprehensive Network, User, & Endpoint Security

Confidential

www.bradfordnetworks.com



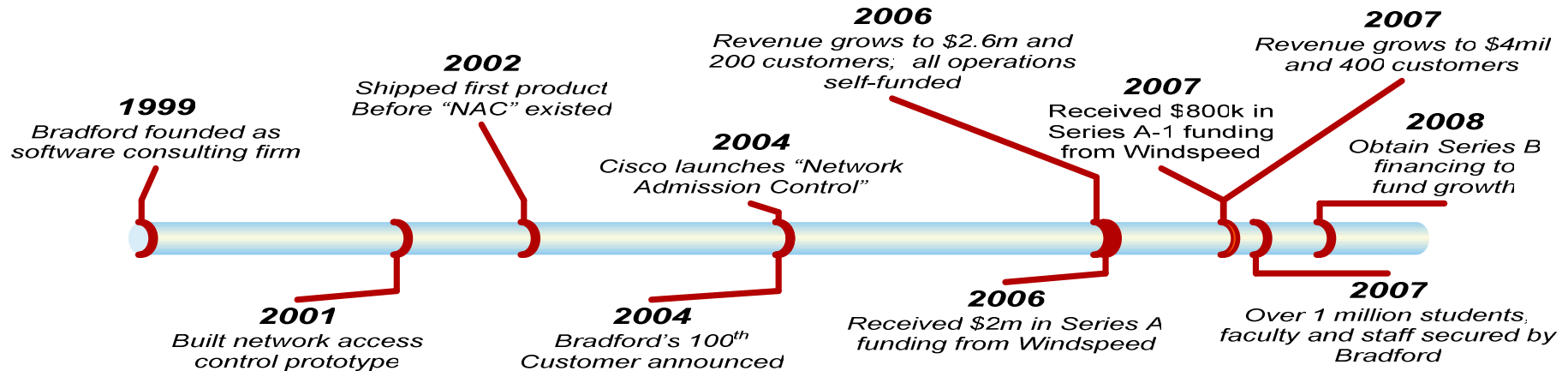
Derin Mellor – EMEA SE
E dmellor@bradfordnetworks.com
M +44 7798 522710



Confidential

www.bradfordnetworks.com

Bradford Evolution

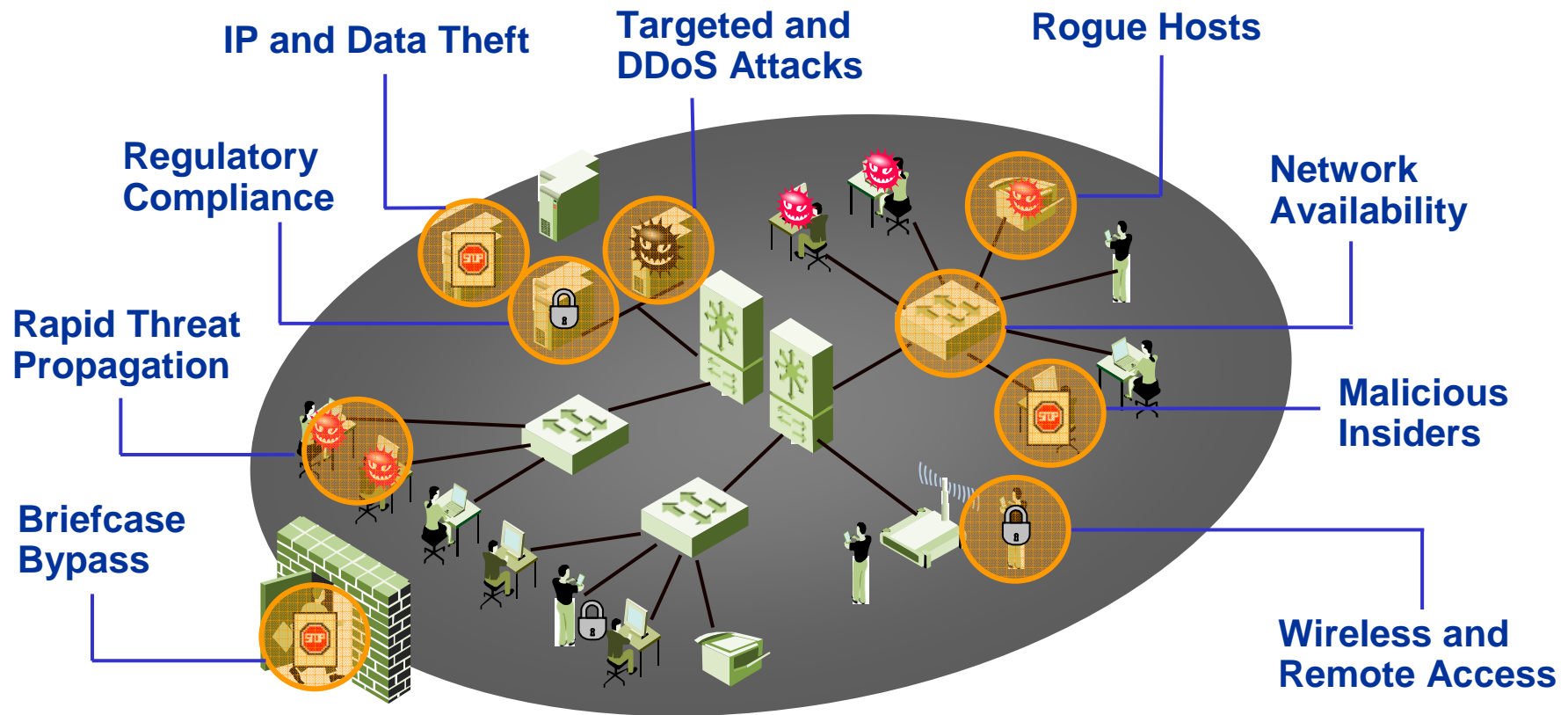


- One of the first Network Access Control solution providers
- Early and leading NAC supplier to the Education market
- Solving enterprise challenges as NAC becomes increasingly critical
- Efficiently built the company and technology foundation
- Focused on growing and scaling the business

● Bradford Networks

- Leading NAC supplier
 - 5 years real world experience
 - Deployments ranging from 100 to 50,000 users
 - Over 1 million users secured
- Bradford delivers comprehensive NAC
 - Identity Management
 - Endpoint Compliance
 - Usage Policy Enforcement
- Out of band architecture leverages existing network
 - Appliances easily integrated without network downtime
 - No forklift upgrades required
 - No performance impact

● Yesterday's DMZ is Today's LAN

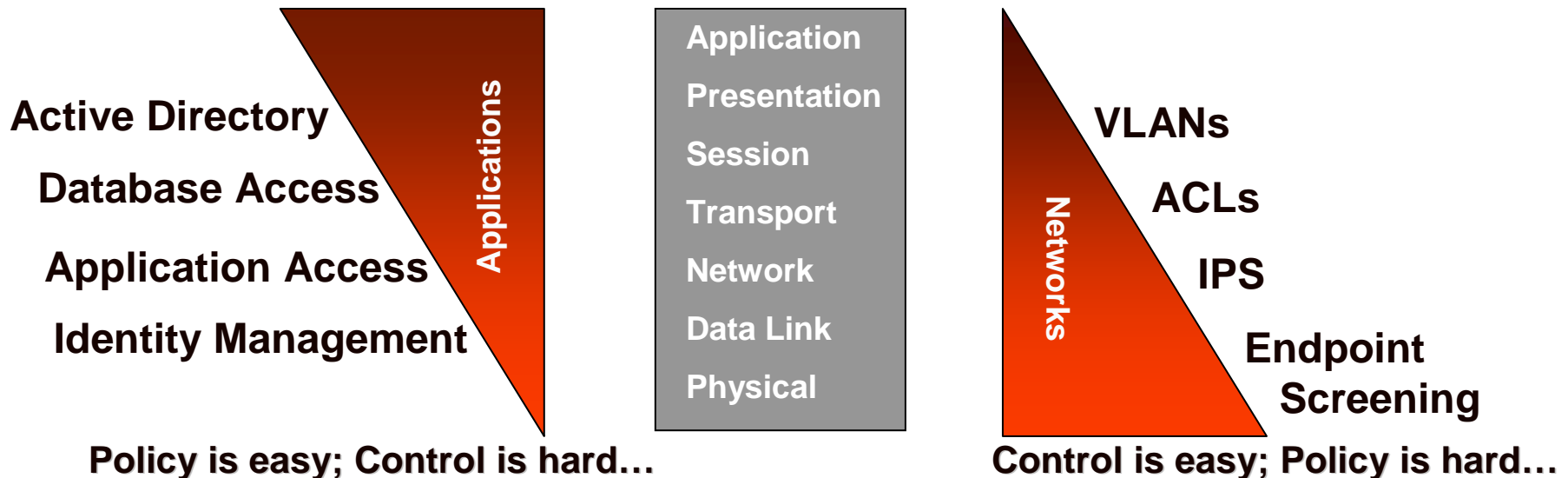


● Network & Application Convergence

Application team defines application policies

Application Policy + Network Control
Application Driven LAN Security

Network team defines network control

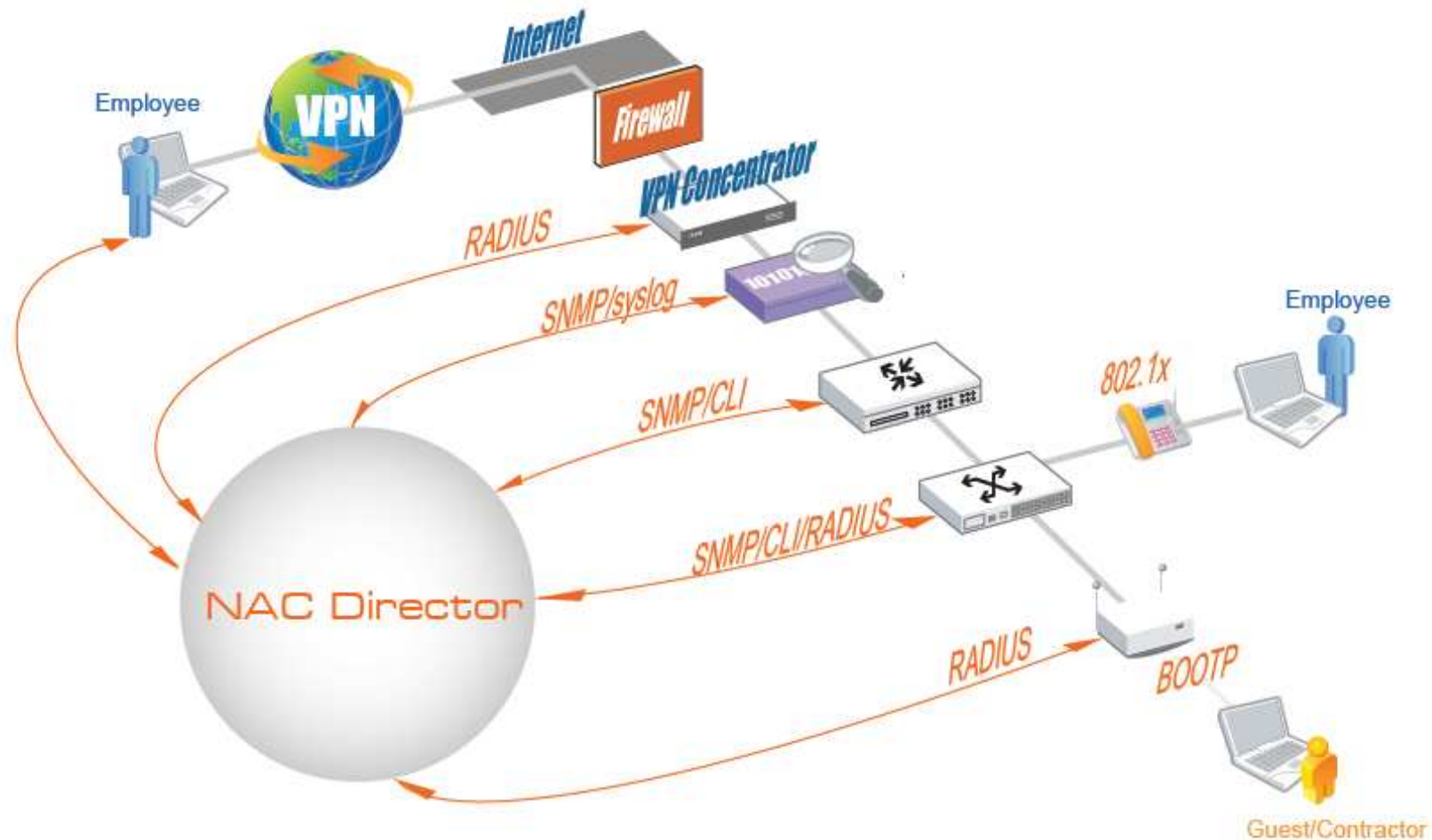


● Network Manager's Day to Day Problems

- Identify rogue devices
- Secure wireless access
- Provide guest access
- Asset and track employee devices
- Find and control users
- Locate stolen/lost equipment
- Document user access
- Control bandwidth use



- Leverage Existing Network and Investment



● 3 Pillars of Network Access Control



● Identity Management

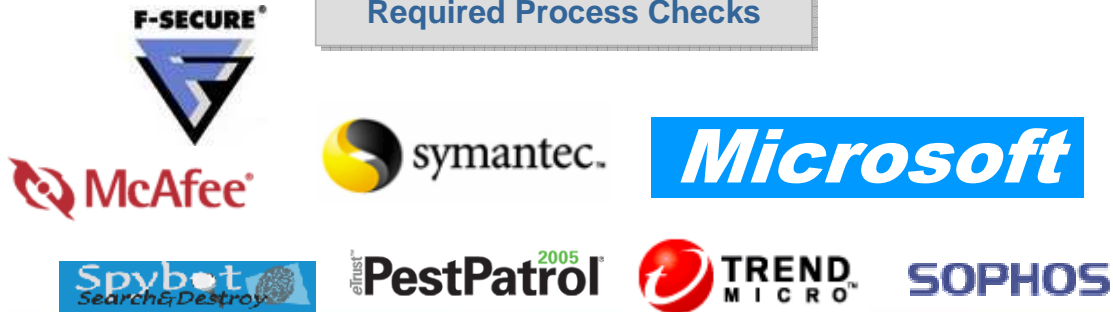
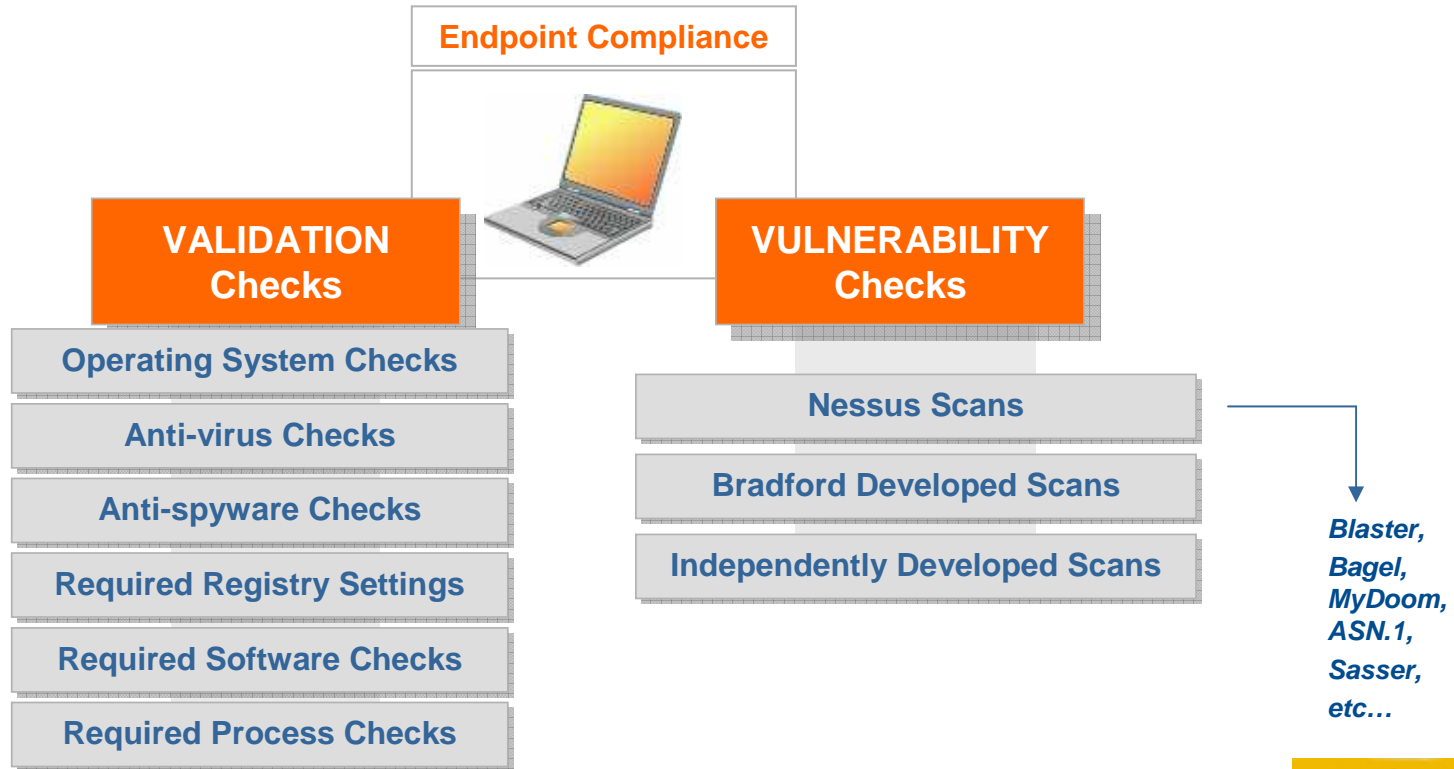
- Registration policy → Security Level 1
 - Identity equals MAC Address
 - Ownership & Accountability for the network device
 - Track by MAC, IP address, port and assigned name
- Authentication policy → Security Level 2
 - Identity equals Username
 - Requires 'valid' username/password
 - Integrates with LDAP directories
 - AD, eDirectory, SunOne, OpenLDAP
 - 802.1X functionality without supplicant requirements
- Role-based access management
 - Different VLAN ID association for employees, contractors, guests, ...
 - Determines levels of access
 - Switch and port flexibility
- Phased policy activation
 - 100% voluntary



● Granular Access Control

- Identity Management: “7 point match”
 - User, User role, Device name, MAC address, IP address, Network access point, Time of access
- Roles
 - Port level granularity
 - Role assignment determined by location as well as time
- “LockOut/StayOut” feature
 - Quickly locate and disable any user/device
 - Identify and disable “sibling” MAC addresses
 - Other devices
 - Prevent access from other wired, wireless or VPN ports

● End Point Compliance (1)



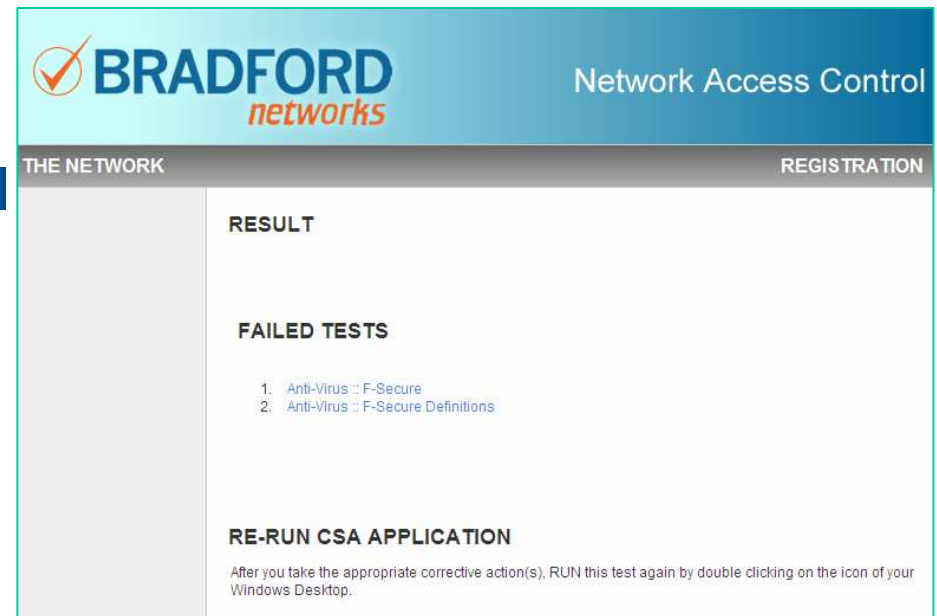
● Endpoint Compliance (2)

- Agents support Windows, Mac and Linux
- Persistent agents
 - Loaded via MSI/GPO, executable, web
 - State monitored
- Dissolvable agents – via web
- Verifies
 - OS and patchlevel
 - AV and antispware version and recently scanned
 - Registry settings, File non/existence, Process non/existence
- Agents can run without “admin” privileges
- Multiple notification mechanisms
- Nessus scanning for non-agent environments

● End Point Compliance (3)

Fails end point compliance: Quarantine the user

- Mark 'at risk' and switch to quarantine VLAN
- Quarantine Web CaptivePortal explains compliance failure
 - Includes links to resolve problem



The screenshot displays the Bradford Networks Network Access Control interface. The header includes the Bradford Networks logo and the text "Network Access Control". Below the header, there are two tabs: "THE NETWORK" and "REGISTRATION". The main content area shows a "RESULT" section with a "FAILED TESTS" list containing two items: "1. Anti-Virus :: F-Secure" and "2. Anti-Virus :: F-Secure Definitions". Below this, there is a "RE-RUN CSA APPLICATION" section with a note: "After you take the appropriate corrective action(s), RUN this test again by double clicking on the icon of your Windows Desktop."

- Email and message box notification
- Customizable web pages
- Integration with patch management systems
 - BigFix, PatchLink, Shavlik

● Behavior Monitoring and Control

- Internal events
 - Rogue DHCP detection
 - Custom Events
 - Duplicate MAC, Spoofed MAC, Critical devices disconnect, Stolen PC, Devices moved, etc...
- External events
 - SNMP Traps or Syslog feed
 - Firewalls
 - Intrusion Detection Systems (IDS)
 - Intrusion Prevention Systems (IPS)
 - Enforce network bandwidth usage policies
 - Control unwanted activities
 - Gaming
 - P2P - Peer to Peer
 - Chatting
 - Illegal file sharing
 - Limit bandwidth usage



Lancope.



Yahoo! Messenger



● Management

- 3 Types of Management

- Help Desk: locate devices/users
- Operator: as Help Desk + configure and manage devices/users
- Administrator: all of above and define policy

- Comprehensive auditable logs

- Integrate with event correlation systems

- Custom Alarms

- Reported on NAC Management
- SNMP to Management system
- Emailed to appropriate authorities

- Comprehensive reports

- Standard reports: Registration, Registration failure, Scan results, Connections Logs
 - Extensive range of user details
 - Formats support: HTML, CSV, EXCEL, XML, RTF, PDF
- Integrates with 3rd party reporting tools – Crystal Reports



The screenshot shows the NAC Director interface with a scan result for a failed test. The interface includes a header with the NAC Director logo, a user profile for Mellor, Derin, and navigation links for Go, Help, and Logout. The main content area displays the following information:

Date	10/21/08 06:11 AM EDT	Scan ID	25794
Test Result	Failed	Host Name	DMellor-It
Policy Name	Guest		
OS	Microsoft Windows XP 5.1 Service Pack 3		
Detected Physical Addresses			
Physical Address	ID		
00:1F:3C:69:DC:E9	Intel(R) PRO/Wireless 3945ABG Network Connection - Packet Scheduler Miniport		
00:21:70:99:18:16	Broadcom NetXtreme 57xx Gigabit Controller - Packet Scheduler Miniport		
00:50:56:C0:00:01	VMware Virtual Ethernet Adapter for VMnet1		
00:50:56:C0:00:08	VMware Virtual Ethernet Adapter for VMnet8		
Test Results			
Category	Name	Result	
Operating-System	Windows XP	Passed	
Operating-System	Windows XP Service Pack	Passed	
Operating-System	XP Critical and Security Updates	Passed	
Operating-System	Windows XP AutoUpdate	Passed	
Operating-System	BitTorrent	Passed	
Anti-Virus	F-Secure	Failed	
Anti-Virus	F-Secure Definitions	Failed	

- **Bradford's Point Solutions**

Campus Manager



**Device Profiling
& Control**



**User Visibility
& Control**



**Behavior Monitoring
& Control**

● Campus Manager product line

Under 1000 users

NETWORK SENTRY 500
Network Control and Application Server

1K→6K users

NETWORK SENTRY 1200
Network Control Server

NETWORK SENTRY 8200
Network Application Server

6K→12K users

NETWORK SENTRY 2200
Network Control Server

NETWORK SENTRY 9200
Network Application Server

Above 12K users

NETWORK SENTRY 550
Network Control Manager

NETWORK SENTRY 2200
Network Control Server

NETWORK SENTRY 9200
Network Application Server

NETWORK SENTRY 1200
Network Control Server

NETWORK SENTRY 8200
Network Application Server

NETWORK SENTRY 500
Network Control and Application Server

● Unmatched Interoperability

Network Infrastructure - Wired & Wireless



Security Infrastructure - IDS/IPS/Firewall/LDAP



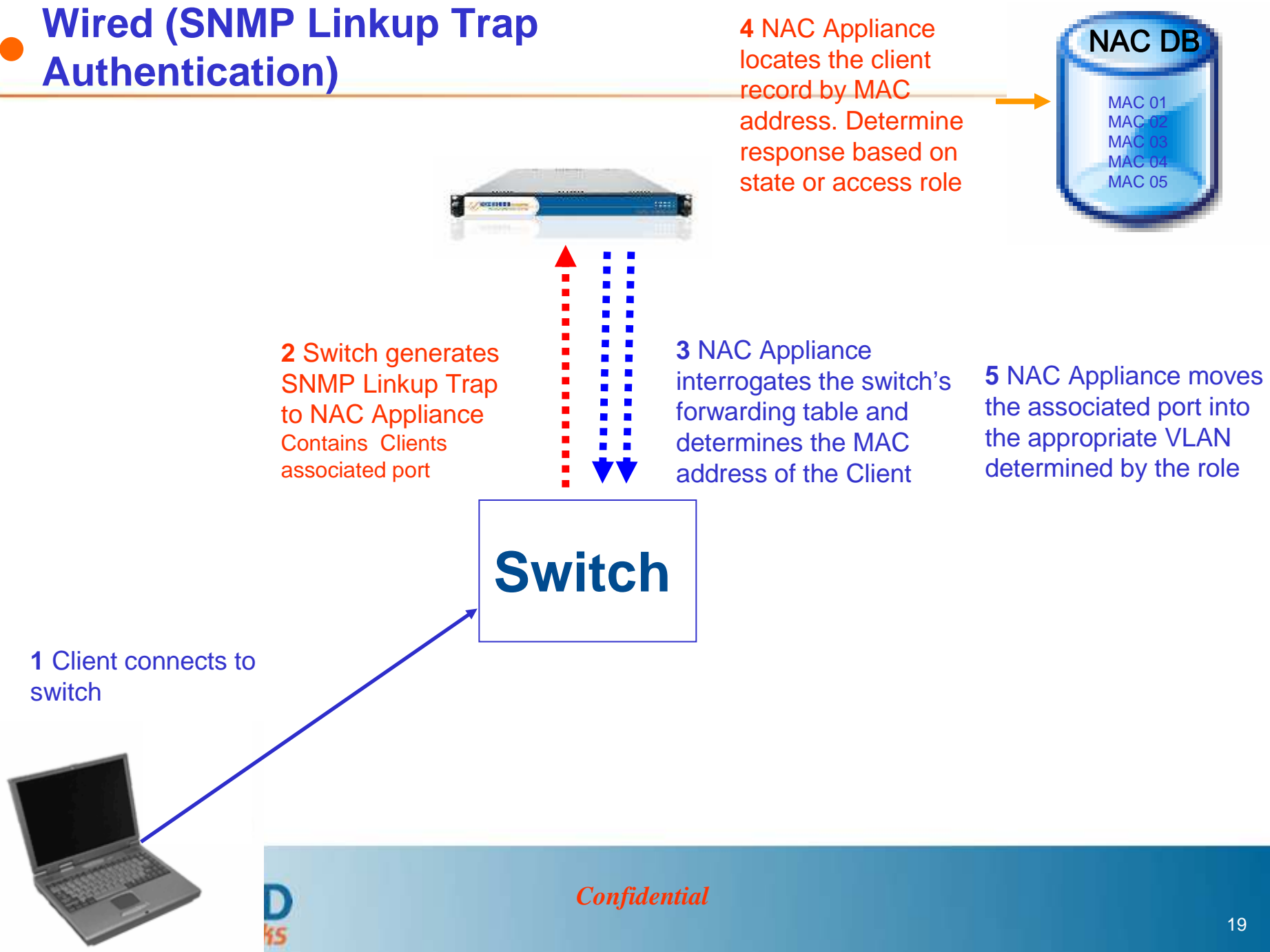
Operating System



Security Application



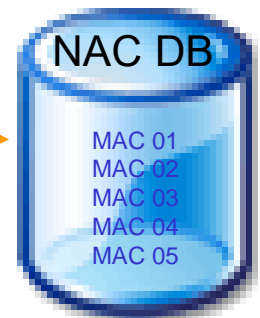
Wired (SNMP Linkup Trap Authentication)



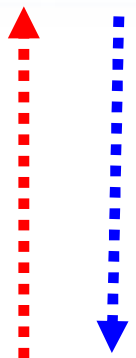
Confidential

Wired (SNMP MAC Notification Trap Authentication)

3 NAC Appliance locates the client record by MAC address. Determine response based on state or access role



2 Switch generates SNMP MAC Notification Trap to NAC Appliance
Contains clients MAC address and associated port



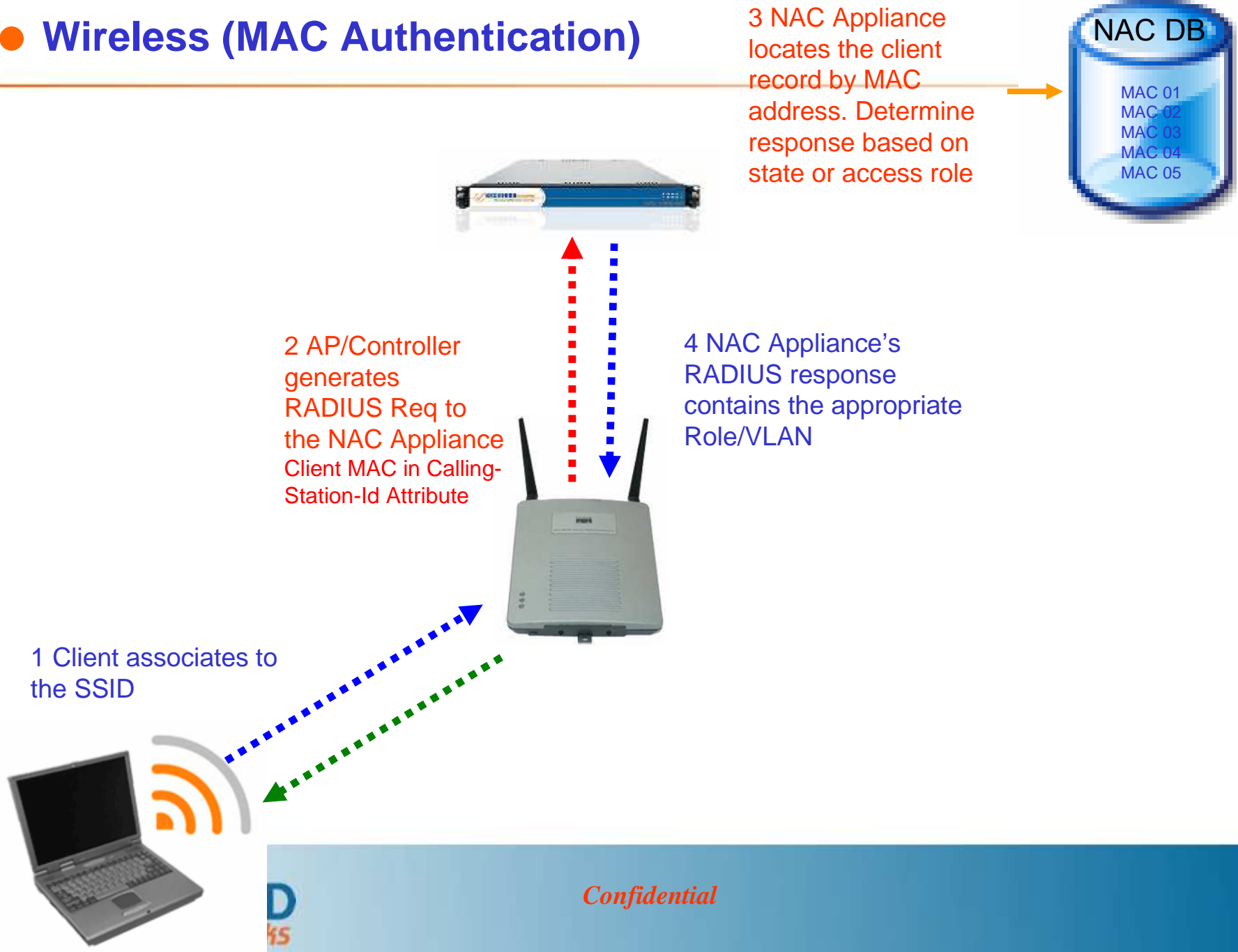
5 NAC Appliance moves the associated port into the appropriate VLAN determined by the role



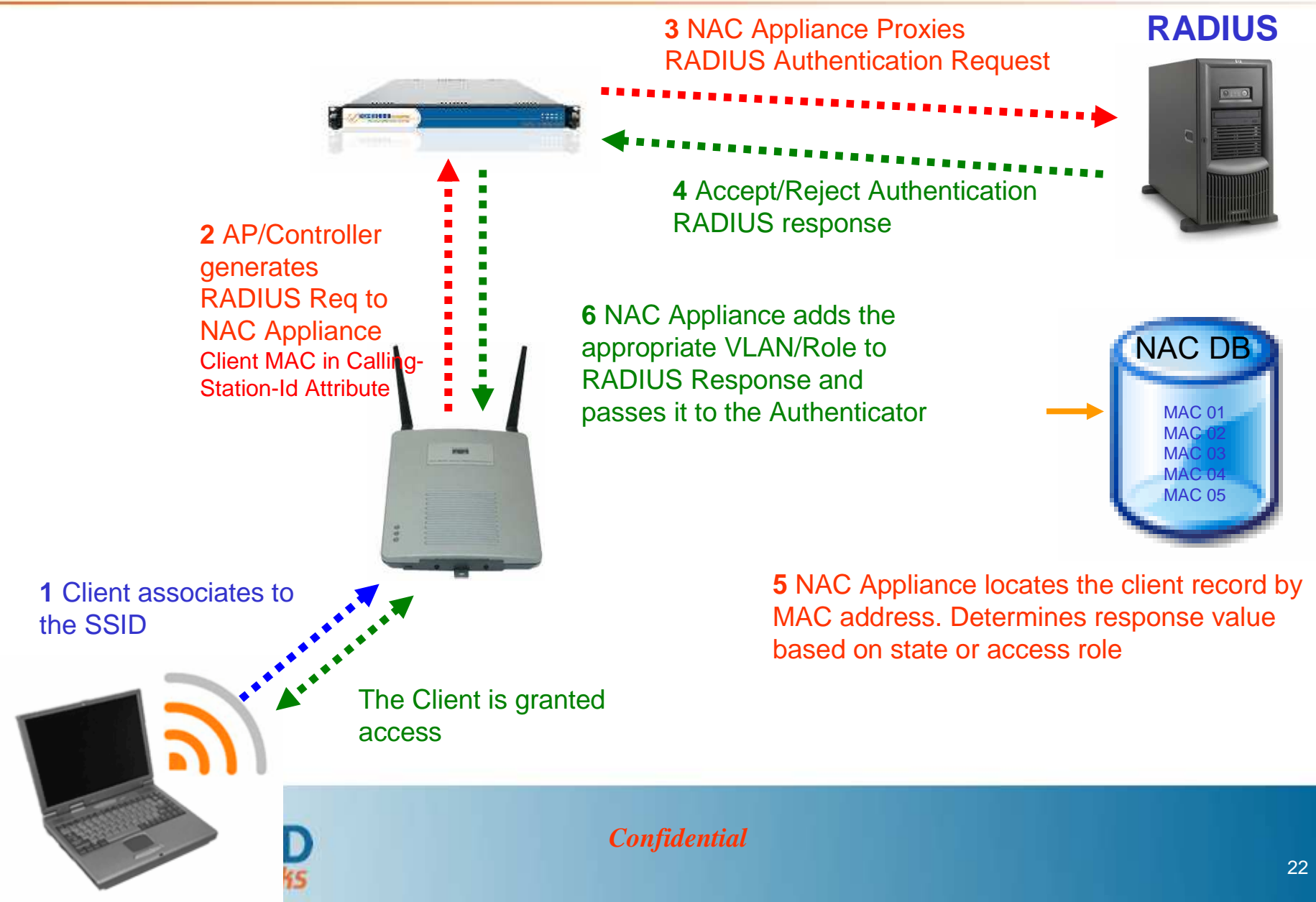
1 Client connects to switch



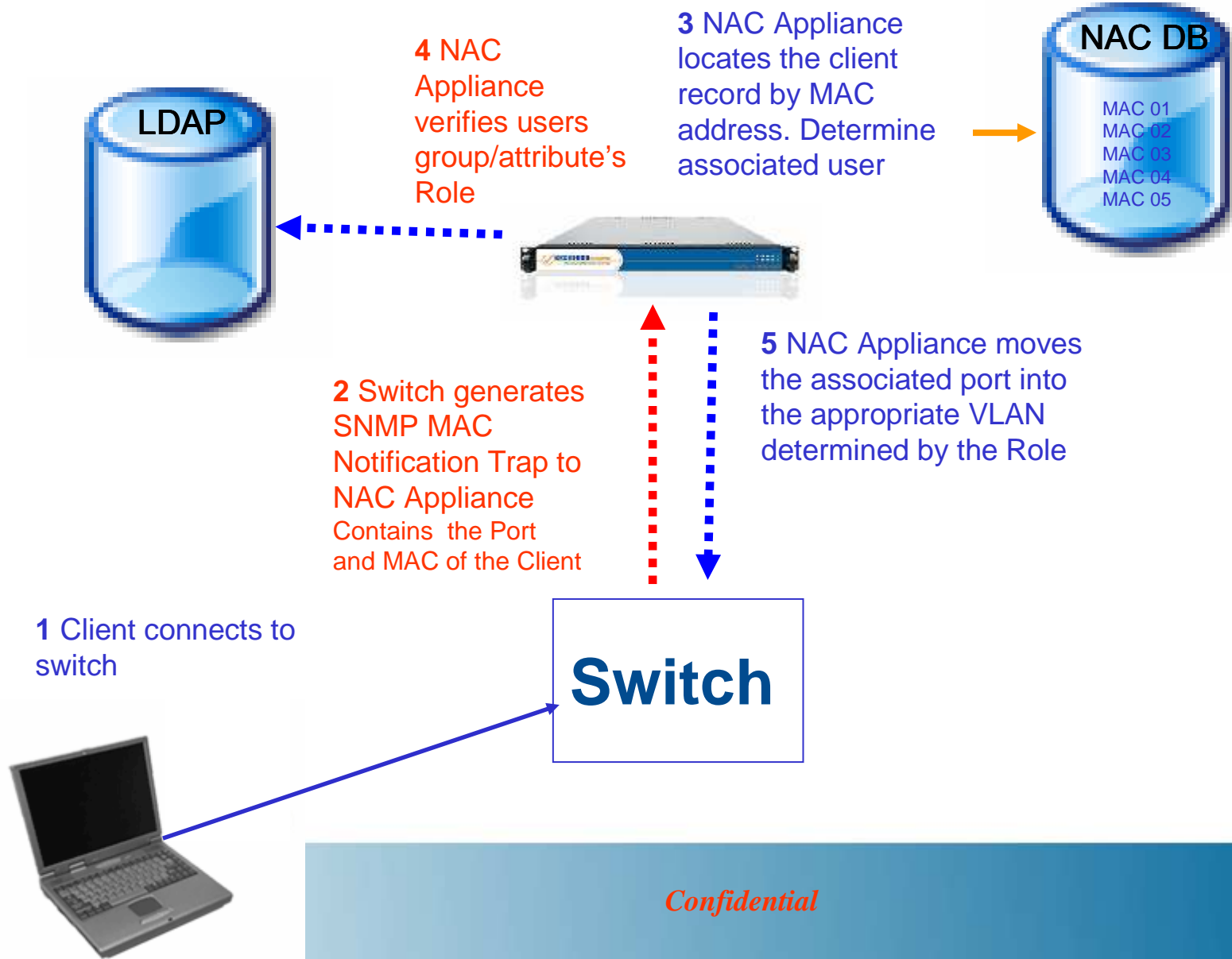
● Wireless (MAC Authentication)



● Wireless (802.1X)

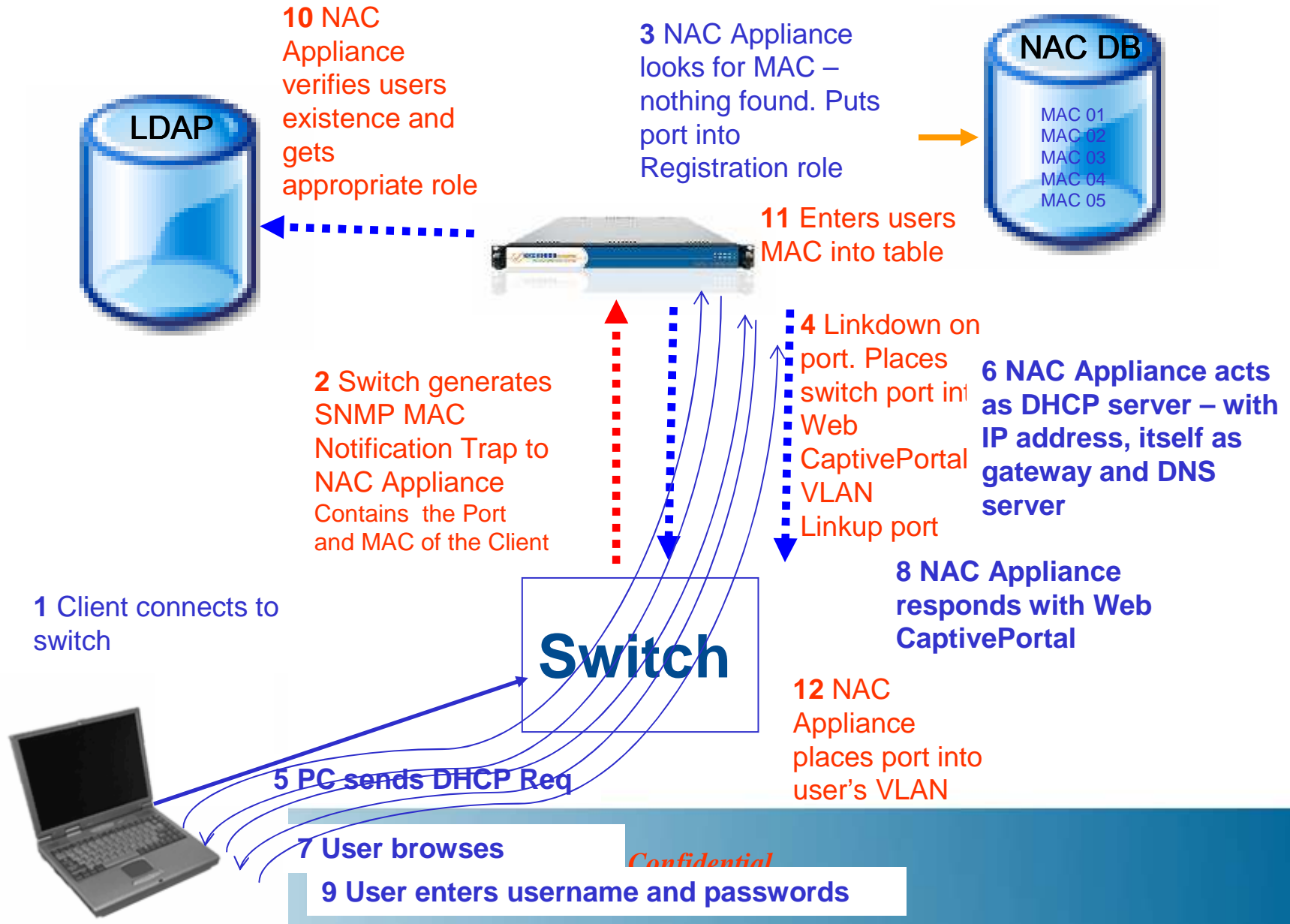


Wired (SNMP MAC Notification Trap Authentication) with LDAP Role



Confidential

Unknown device Wired (SNMP MAC Notification Trap Authentication) with LDAP Role



Confidential

● Typical Deployment

1. *Network Discovery & Visibility*

Switches: SNMP traps to CM

AP: RADIUS to/via CM

2. *Static Device Inventory*

- *Import known device information*

3. *Device Identification & Profiling*

- *Manually identify devices*

Poll router to get IP/MAC mapping

4. *Passive User Identification*

- *Authentication through login scripts*

5. *Pro-active User Identification*

- *Registration through Captive Portal*

VLANs, and associated routing, must be setup

6. *Passive Endpoint Compliance*

- *Persistent Agent via A/D group policy*
- *Notification to Help Desk and/or client, no network isolation*

Unknown devices are controlled

7. *Pro-active Endpoint Compliance (PA & DA via Captive Portal)*

- *Notification Only Initially*
- *Isolation to Quarantine for self remediation*

8. *Post-Connect “Activity” and/or “Behavior” Enforcement*

● Summary: Who is doing What, Where and When

- Accommodate virtually all networks
 - Leverages existing infrastructure
- Scales to required size
 - High availability solutions
- Device profiling and control
 - Effective asset management
 - Rogue device identification
- User visibility and control
 - Comprehensive endpoint posture compliance
- Behavior monitoring and control
 - Integration with firewalls, IDS, IPS, bandwidth managers, ...
- Comprehensive Reports

● The future...

- Minimizing carbon footprint
 - Government policy
- Minimizing electricity usage
 - Electricity prices are rising
- Controlling power to non-essential device out-of-hours
 - VoIP
 - Available today
 - AP
 - Available today
 - Switches
 - Requires intelligent power supplies
 - Routers
 - Requires intelligent power supplies