

Develop a 'NAC' for Troubleshooting

The use of a network analyzer can be invaluable to assist you in troubleshooting and optimizing your Network Access Control (NAC) process. In the testing and implementation phases of NAC, a network analyzer offers visibility into the network and offers valuable assistance in troubleshooting potential configuration and compatibility problems.

Who you are should determine what you're allowed to do on the network. NAC's primary purpose is to ensure that a client has passed a health check or integrity validation before allowing it access to the corporate network. If not, the client may be placed on a quarantine LAN or one that has access to limited resources, such as firewall to Internet access only. Therefore, it is generally implemented as a component of a corporate network security policy to prevent potentially unsafe or unknown computers from connecting to the network. NAC represents the most significant change in the way that networks are secured since the invention of the firewall.

A NAC supplicant (or broker/trust agent) is required to run inside each PC or laptop. A supplicant can be as simple as a VLAN client but in most cases, will also include software to communicate policy reports containing such information as OS patches and anti-virus in use and virus definition version to a policy server that checks the integrity of these reports.

In the absence of such agents, the user (including a guest) can be placed into a specified 'quarantine' VLAN until the security policy violation is remedied and the user switched to the unrestricted VLAN. The latter is also sometimes called the protected VLAN.

Analysis of this entire process (VLAN/remediation/protected VLAN) can help keep NAC operating smoothly and ensure that the entire quarantine process occurs in a timely fashion and scales. The last thing you want is long delays due to OS patches or frequent virus definition updates rolled out to thousands of users simultaneously (such as when they login into the network in the morning).

NAC agents are smart in that any attempt to disable an antivirus or altering the OS in some way after booting results in the user going back to the quarantine VLAN for remediation. Again, use of an analyzer can verify that these changes are detected properly by the NAC process.

In the iLabs network at Interop 2007, there are three competing NAC implementations: Microsoft Network Access Protocol (NAP), Cisco CNAC (Cisco NAC), and TCG-TNC (Trusted Computing Group-Trusted Network Connect, an open standard) using a variety of protocols including HTTPS and EAP tunneling. Currently NAP is native only to Vista and Longhorn.

Each variation offers different nomenclature. Regardless of terminology, we can analyze and troubleshoot all implementations in essentially the same way: all have the NAC agent at the client, policy and authority servers (that work in conjunction with RADIUS) to handle policy/posture validation, and an enforcer to grant or deny

access. The enforcer can be a layer 2 switch that handles VLAN assignments on a port-by-port basis for each client or a firewall that allows/disallows VPN access.

In all three competing NAC implementations, the VLAN assignments are sent via RADIUS packets to the switch. These RADIUS packets can be easily captured and analyzed should you have any trouble with VLAN assignments, but the use of a good analyzer doesn't stop there. Once your NAC is 'tuned' and functioning as expected, continue to use the analyzer in a 'forensics' manner to monitor, track, and assess endpoint security.

The screenshot shows the OmniPeek interface with a list of captured RADIUS packets. Packet 36 is selected, and its details are shown below. The details include two RADIUS attributes: Attribute #3 (Tunnel-Type) with value 0x0100000D (tag = 13 VLAN) and Attribute #4 (Tunnel-Medium-Type) with value 0x01000006 (tag = 6 IEEE-802). The hex dump at the bottom shows the raw packet data, with the relevant bytes highlighted in green.

Packet	Absolute Time	Source	Destination	Protocol	Size	Summary
36	15:52:26.411226	cisco-acs	IP-45.200.1.42	RADIUS	335	R Access Accept User:dick
37	15:52:57.518337	IP-45.200.1.42	cisco-acs	RADIUS	203	C Access Request User:anonymous NASPort:50017
38	15:52:57.521667	cisco-acs	IP-45.200.1.42	RADIUS	123	C Access Challenge
39	15:52:57.528926	IP-45.200.1.42	cisco-acs	RADIUS	226	C Access Request User:anonymous NASPort:50017

Packet: 36 [X] ?

Radius Attribute #3

- Type: 64 Tunnel-Type
- Length: 6
- Value: 0x0100000D tag = 13 VLAN

Radius Attribute #4

- Type: 65 Tunnel-Medium-Type
- Length: 6
- Value: 0x01000006 tag = 6 IEEE-802

0000: 00 0B BE 4F 6D 80 00 16 35 5B CD E0 08 00 45 00 01 3D D7 40 00 00 80 11 04 70 2D C8 01 46 2D C8 ...Om...5{...E...=@...p...F-...
 0020: 01 2A 06 6D 06 6D 01 29 CA 9F 02 A9 01 21 A3 C5 FE 8B 69 14 8A C4 E9 30 ED 8D B4 6F 82 A2 1B 06 ...*..m.m.)...!...i...0...o...
 0040: 00 00 00 1E 1D 06 00 00 00 01 40 06 01 00 00 0D 41 06 01 00 00 06 51 05 01 31 32 1A 1F 00 00 00 ...@...A...Q...12...
 0060: 09 01 19 73 74 61 74 75 73 2D 71 75 65 72 79 2D 74 69 6D 65 6F 75 74 3D 31 30 1A 1D 00 00 09 ...status-query-timeout=10...
 0080: 01 17 70 6F 73 74 75 72 65 2D 74 6F 6B 65 6E 3D 48 65 61 6C 74 68 79 08 06 FF FF FF FF 4F 06 03 ...posture-token=Healthy...0...

Example VLAN Tag embedded in a RADIUS Accept Packet

Also common to all three implementations is the fact that a client must obtain an IP address via DHCP when switching VLANs. The DHCP server at iLabs is dual-homed to receive requests from both the corporate and quarantine VLANs which, of course, reside on different subnets.

Typically the NAC agent will request an IP address as if the PC was just booted. In the event that the previously used address is requested and a DHCP NACK is received due to a user's switch port assigned to a new VLAN/subnet, a new address must be requested. These NACKs are a good process to monitor with an analyzer since they are a strong indicator that a client is switching VLANs.

See NAC in Action

This document merely scratches the surface of various NAC implementations and troubleshooting processes. Unravel some NAC mysteries by visiting iLabs at Interop Las Vegas 2007 and interact with all of the NAC authentication schemes and clients. Be sure to take a 'peek' at the various NAC protocols using WildPackets OmniPeek. OmniPeek is the official analyzer for iLabs and is set to capture all traffic on the NAC backbone, including all Cisco, Microsoft, and TCG traffic.