Practical Steps to Gaining Control of the Network Access

Steven Thomason

East Carolina University
Abstract

Most companies are concerned about unauthorized access to their corporate network through their wireless infrastructure and rightly they should. With BYOD, wireless hackers, and others trying to infiltrate the network it is a constant challenge for the security staff to maintain a secure environment where only authorized personnel are utilizing the company resources. Today more and more programs are dedicated to managing and monitoring the wireless infrastructure but they seem to forget about LAN access and security. While some companies such as banks and government controlled or regulated sites have physical controls that help prevent this most companies don’t even know where all of their physical cables run. A manufacturing plant, for example, may have many different nooks and crannies where someone can access switches and routers on the wired network. There are cabling runs to manufacturing equipment, security devices such as badge readers and time clocks, department LANS, and the main corporate wired network. What is in place to stop anyone from finding an out of the way location and just plugging in their laptop or tablet? This paper will look at what steps companies looking to implement a network access control system should take at before making any decisions.
While many companies are now much more interested in what Network Access Control (NAC) systems can allow them to control, many miss implementing the basics of security before proceeding towards a full NAC solution. Many of these solutions are nothing more than good basic network design and already available to them but never implemented. Why implement complicated application layer solutions to stop from someone from flooding a port with MAC addresses that will use all available DHCP addresses when just making a few configuration commands on a switch will accomplish the same thing. When it comes to security concerns the good news is that you only need to worry about two groups of people, internal and external. The bad news is that is everyone and it doesn’t matter if the damage is accidental or intentional. The damage has been done. The growth of “Bring Your Own Device” (BYOD) has increased the need to find a way to control access to the company network and data. This trend has greatly increased the number of internal threats where users either on purpose or accidentally bring in an infected devices or purposely attack company resources. According to the US State of Cyber Crime Survey study over 20% of network attacks were done by current and former employees¹.

Companies need to control who connects to the network and what they connect with, whether it is a PC, tablet, USB device, Bluetooth, or phone. Usually the first solution that IT departments think of is that “we need to have a network access control system.” NAC is becoming the new buzzword again. NAC has improved a great deal since it was first introduced years ago. However before rushing out to purchase the lasts NAC appliance or software, start with the basics.
Before purchasing or even evaluating network access software an IT department should do a requirement assessment. Many IT departments think that they need to start with specialized network access control software. They start looking at the big names in NAC. These are companies such as Cisco, ForeScout, HP, Juniper Networks, Checkpoint, and Symantec. They all have products that mainly address access utilizing applications that reside at the upper levels of the OSI level. These applications have the ability to do endpoint assessments, authentication, and remediation. Some come as complete packages while others rely on hooks into other software packages. For instance a NAC solution may not do virus checking but look to the virus software console to determine if the client is up to date or not and if not hand it off the virus software. After the virus software and DAT files have been updated, the client gets re-assessed.

The Organization of International Standardization’s (ISO) Open System Interconnection (OSI) model divides IP communications into 7 layers. Each of these layers has been designed to operate separately from each other. ISO security services as defined by the ISO are confidentiality, integrity, access control, authentication, and non-repudiation. Confidentiality is intended to prevent unauthorized access to information. Integrity is meant to check to make sure that any unauthorized change to data has not been made. Access is a means to either grant or deny access to data or information. Authentication checks to see that the entity should be allowed to access the information and non-repudiation prevents an entity from denying that data was either sent or received. The lower layers of the OSI design are Physical, Data link, network, and transport.
NAC systems are usually designed to operate in the upper layers of the OSI model which are the application, presentation, and session and are considered the upper layers for security functions. Lower layer functionality and security are usually independent of the user’s application and more likely to be implemented at a switch or router level.

To begin with there is still not anyone that has the perfect solution for protecting your network. No NAC system knows about every device. Access needs to be addressed at all levels of the OSI model. Security can be looked at as having three separate components; physical security, lower layer security, and upper layer security. Physical security is just that physical objects designed to stop an authorized person from getting physical access. The lower layers commonly refer to layer 2 and layer 3 of the OSI level. Upper layer security usually refers to application level control. Some processes can overlap. It doesn’t matter how great your NAC software is if someone can just walk into a wiring cabinet and take their time trying to get into your network. Almost any device can be hacked if you have physical access. Just Google the phrase “Forgot switch password” and you will find instructions for getting into a switch if you have physical access. All layers of security need to be addressed.

The first step to securing your network is to lock everything up. Equipment that cannot be locked in a room needs to be in a lockable cabinet and actually locked. Which is more inconvenient, going back for the cabinet key you forgot or rebuilding a network that someone destroyed? Rooms that can be locked need to be controlled through an access system such as requiring badge swipe and possibly include a camera system. You also need to have a basic network monitoring system that will alert you if anyone recycles the power on a device and even better let
it would let you know if a configuration change was made – such as to the password or user access.

The next and most overlooked step is to lock down your devices at layer 2 of the OSI model. Once you have physically secured your networking devices you should then proceed to look at layer 2 of your network. Many attacks today are successful because switches and routers have not been locked down at layer 2. A common saying is that you are only as secure as your weakest link. Who cares how strong the doors and locks are if you left the windows open. The layer two configuration on your switch is the window.

There are problematic issues that can occur when someone brings a home PC or wireless access point to work. One issue can occur when an infected computer has a Trojan on it and the Trojan starts poisoning the network by filling the CAM tables of the local switch stopping traffic from flowing. Another common problem that networks have is when a user wants a wireless network where the company doesn’t have one so he brings in his own wireless router. He connects it to the main network and it starts advertising DHCP addresses. The next thing you know a users calls the help desk and says that he can’t get anywhere on the network. When the help desk asks what his IP address is they get an address that isn’t even used within the company. Doing some basic configuration on the local switches could have prevented both of these problems.

Layer two attacks are much easier if using a shared device such as a hub, however most companies have fully switched networks which helps to eliminate some types of broadcast storms. DDOS attacks are more effective in the LAN than in the WAN due to available bandwidth. Attacks can happen much more quickly. Some of the more common attacks at layer
two are VLAN hopping, MAC attacks, ARP attacks, Spoofing attacks, CAM table overflow, and general attacks. Dynamic trunk protocol (DTP) operates between switches using trunked ports. VLAN hopping occurs when an end station spoofs itself as a switch using ISL or 802.1q. The end station then becomes part of all VLANs. To keep this from happening you should disable all unused ports on the switch and put them into an unused VLAN. On all trunk ports explicitly define the VLANs allowed. Nowadays most companies are moving or have moved to VoIP and today’s phones are also switches so they need to be taken into account when securing trunk ports.

An configuration example is shown below:

```
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 2,5,6,10
switchport mode trunk
```

MAC addresses are stored in content addressable memory (CAM) and mapped to appropriate VLAN and physical ports. Switches have fixed CAM sizes that are dependent on the model and manufacturer. Attacks take advantage of the limited size by sending multiple random source MAC and IP addressing and filling the CAM table. This keeps any new MAC address from being part of the table, which keeps it from communicating. At this point with the table full no new computer or other device can become part of the network. This also affects the table of the neighboring switches as well. Putting port security limits on switch ports can restrict the number of addresses that can be broadcast from one port keeping the CAM table from filling up.

The commands below shows a standard configuration for a port connected to an IP phone.

```
switchport port-security
switchport port-security maximum 3
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```
Other options include allowing the MAC address of the first device connected to be remembered by using sticky ports or manually restricting the port to a specific device’s MAC address.

One type of DHCP attack involves grabbling all of the available DHCP addresses by generating multiple DHCP requests using different MAC addresses from the same switch port. An end point would also advertise itself as the DHCP server thus giving out incorrect information or even advertising itself as the default gateway so that it could sniff all traffic. To combat DHCP snooping and abuse of DHCP requests enable both the switchport security listed earlier and enable dhcp snooping.

Global Commands

```
ip dhcp snooping vlan 2,20
no ip dhcp snooping information option
ip dhcp snooping
```

Interface Commands

```
For an untrusted client
no ip dhcp snooping trust (Default)
ip dhcp snooping limit rate 10 (pps)
For a trusted client
ip dhcp snooping trust
```

Another option is to block udp port 68 from all switch ports except for valid ports hosting DHCP servers using an ACL.

There are many different types of ARP tools\textsuperscript{vi} that can be used to intercept ARP requests. These tools have the ability to be used to capture and hack passwords and replace communication session with their own instead of the originator. To combat this problem you want to restrict how MAC addresses are viewed on a switch. It is possible to set your switches to learn where MAC
addresses belong and only allow that particular MAC to only communicate from that port. Someone injecting their MAC in place of the true MAC address would not be considered to have a valid sourced packet and causing it to be dropped.

Global Commands

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp snooping vlan 2, 20, 30</td>
</tr>
<tr>
<td>no ip dhcp snooping information option</td>
</tr>
<tr>
<td>ip dhcp snooping</td>
</tr>
<tr>
<td>ip arp inspection vlan 2, 20, 30</td>
</tr>
<tr>
<td>ip arp inspection log-buffer entries 1024</td>
</tr>
<tr>
<td>ip arp inspection log-buffer logs 1024 interval 10</td>
</tr>
</tbody>
</table>

Interface Commands

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip arp inspection trust</td>
</tr>
<tr>
<td>ip dhcp snooping trust</td>
</tr>
</tbody>
</table>

MAC and IP spoofing can be used to fool other devices into believing that they are something that are not. A MAC address is a 16 bit number that identifies the manufacturer and the specific device. There is currently nothing that binds the MAC to the IP address other than a table in a switch. This is a weak link between the two OSI layers. While completely eliminating spoofing is not possible you can reduce the threat. By using DHCP snooping a switch builds a table listing what devices are associated to what port. This way the switch can validate if a device is using the correct MAC and IP address. The commands below check for both. To only check for MAC address enter the command no ip dhcp snooping information option.

Global Commands

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp snooping vlan 2, 20</td>
</tr>
<tr>
<td>ip dhcp snooping information option</td>
</tr>
<tr>
<td>ip dhcp snooping</td>
</tr>
</tbody>
</table>

Interface Commands

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip verify source vlan dhcp-snooping</td>
</tr>
</tbody>
</table>
Spanning Tree does not use authentication before sending out updates so anyone can send out a BPDU packet by simply saying that they are the root bridge. Enabling BPDU guard globally can prevent users from becoming the root bridge and corrupting the topology. It can be disabled at the port level if necessary.

Below is a list of Layer 2 Security Best Practices. This list can be found in multiple locations on the web and different vendors may have slight variations. The list below is predominately from Cisco switching.

- Restrict switch management access to specific subnets or specific devices where possible
- Restrict any SNMP access to specific IP address using ACLs
- Use a dedicated VLAN ID for all trunk ports.
- Never use VLAN 1
- Disable DTP on all non-trunking access ports.
- Use ACLs to filter undesirable traffic (IP and non-IP).
- Use Private VLANs where possible to segment network traffic at Layer 2.
- If possible use an authentication method MD5 authentication.
- Disable CDP where possible. (be careful as it is needed for functions such as IP Phones)
- Disabling unused services and protocols.
- Shut down unused ports and put them in an unused VLAN.
- Use port security mechanisms to provide protection against a MAC flooding attack.
- Use port-level security features such as DHCP Snooping, IP Source Guard, and ARP (MAC address) security where applicable.
- Enable Spanning Tree Protocol features
- Use SSH, authentication mechanism, access list, and set privilege levels.

Some of the layer two security options for wireless include the following methods: WPA, WPA2, 801.x, WEP, and CKIP. MAC filtering is also another layer method of controlling access to a wireless network. IPSec and VPN pass-through are two layer 3 methods for security wireless access. Layer three services should be disabled if not being used. ACLs can be used to control IP spoofing.
There are several upper level authentication services commonly found on corporate networks. One very common service is LDAP which is mostly associated Microsoft but also provided by Novell and OpenLDAP. Radius services can be used for authentication purposes and can be provided by a Cisco ACE or ICS device, a Radius server of which several versions are available, and Microsoft NPS.

After reviewing the lower security layers of the OSI model it is time to look at the upper layers which is where a more comprehensive security applications resides. This is network access control (NAC). It would be difficult to find a company with a connection to the Internet that doesn’t have a firewall. Many of these companies also have intrusion detection and prevention systems installed and of course the required virus protection system. All of these system are separate entities that either don’t usually integrate well together or are primarily aimed at restricting exterior threats or access. BYOD changed that thought process. Nowadays more and more companies are thinking more about addressing the security threat from within. The basic function of NAC is to give the company greater control of who and what is connected to the network and what its status. Is the person or device authorized? What access are they allowed? Is there system up-to-date in company required software and updates? Can we isolate access until the device has been updated and patched to meet company requirements?

In 2012 Gartner analyst Lawrence stated that NAC had been around for almost 10 years but has not been adopted except by a financial institutions and high-security environments. With the proliferation of mobile devices and BYOD growing there has been a renewed interest in revisiting NAC and looking to see what has changed. In June 2010 Network World tested 12
NAC products. While the idea of NAC is having only one product to manage they found out that many offerings were actually a suite of offerings that may or may not integrate well. One key they found was that you really needed to know what you wanted to get from the product before purchasing. There were many different approaches in methodology. For instance, Cisco Systems preferred to let the virus problem be handled elsewhere whereas McAfee wanted to control everything including network switch access. Your selection needs to be well planned and researched.

Before proceeding in your search for the right NAC solution, you need to have a strongly worded company policy stating what the company expects from the users and what their actions will be if not followed. If the company policy doesn’t state that users are not allowed to install games on their work computer then you can’t very well enforce it. From the end user’s perspective there is no issue to installing games on a company owned computer.

One key component for selecting a product is deciding who controls what function. Who scans the PC or device to see that is up-to-date? Do you use a program like Microsoft System Center to tell you who current or a package such as Trustware’s scanning tool? Is NAC an end user support group function or does it belong with the security team? This decision will affect whether you want a product that combines all functions into one part of the organization or one that has separate security, network management, and end-point checking. Can the system support all of the approved devices in your company such as Linux, Mac, IOS, Windows, and anything else you may want to allow?
Why don’t many companies already have NAC installed? According to Bradford Networks\textsuperscript{xiii}, most existing technologies have a limited ability to fully automate actions based upon a set of actions or inputs. Their system looks to provide “for the automation of configuration actions applied to a network infrastructure devices as the result of various forms of network stimulus.” NAC can be extremely difficult to install and manage especially when a multitude of products and systems are integrated. Improperly planned and implemented NAC can bite you. One example from Network World in 2012\textsuperscript{xiv} is where a CEO’s 5-year-old daughter picked up his phone and started playing with it while on vacation. After the phone saw 5 attempts at entering the password incorrectly it followed the procedures as defined in NAC policy and wiped the phone of all information – including all of the vacation pictures he had taken. One would think that that would be easy to fix, just don’t delete photos. However, how many people had been in a meeting and then taken a quick snapshot of the board for later reference? Again before doing anything have a company policy.

NAC solutions have a variety of ways to register devices. Some of them such as PackFence which is an OpenSource solution, can use lower layer services such as MAC addresses, DHCP fingerprinting and third party programs such as Snort or Nessus\textsuperscript{xv}. One significant use for NAC is to help reduce the spread of malware\textsuperscript{xvi}. Most companies at some time will have a contractor, vendor, or other outside person come into their business and plug in their computer. That computer will then start communicating on the network possibly causing unknown problems. NAC is designed to stop that from happening or at least control the extent of the communications by segmenting it to a specified VLAN.
Different NAC vendors have different offerings but most should have the following functions:\(^\text{xvii}\):

- Immediate discovery of any device that is connects to the network.
- Be able to identify the device type
- Determine the compliance status of that device
- Decide whether or not to block, allow, or limit access based on compliance
- If determined that the device is not compliant bring it up-to-date
- Monitor the entire process.

More advanced systems should be able to integrate with other systems such as mobile device management services and desktop management tools. There are basically two ways to go in endpoint security, agent or agentless NAC. Agents give you greater control as the devices have already been identified. The agent model basically looks at the device and if there is not an agent on the device denied access. This can be a problem is your company uses a large number of devices that may not work with that agent or if the NAC does not have an agent for your device. Another issues arises when you take into account the number of IP devices that can be found on a network. Some examples include commonly though of items such as printers, computers, scanners, and phones. What many companies forget is that they also have devices such as paging systems, door locks, badge systems, time clocks, heating & cooling systems, cameras, and UPS systems on their network\(^\text{xviii}\). One NAC provider, Juniper is trying to patent a method for improving systems to make them better at identifying anything that is plugging into a network device.

Creating the NAC policy can in itself be a major undertaking. There are many variables to take into account. How are your users going to respond the enforced policies and audits? How are you going to track all of the permitted applications and what are you going to do with unauthorized software? You need to be able to track applications, their versions, and other information relevant to each package. Can your system identify each system’s OS, tell if it has been patched
or in the case of a phone has it been jailbroken? There is also the need to know as much
information as possible about the device including everything from the IP and MAC address to
what switchport or access point the device is connect to. All of those criteria need to be taken
into account when designing a NAC policy.

There are many functions on a network that need to be monitored and controlled which increases
the complexity of a fully integrated NAC solution. Some of the major functions include network
access, security access, storage, and end point usage. All of this takes place on switches, routers,
access points, gateways, and other connectivity devices.

Before choosing a NAC solution you need to answer the following questions:
• Do you have a fully developed company policy and is it in place?
• Do you know what types of access you want to control?
• Do you know what the result of an event should be? Do you want the device blocked or
  isolated and remediated?
• Do you want a complete NAC solution in one package or do you want a separation of
  processes and systems?
• Do you know who should have ultimate responsibility for the product? Is it the end-user
  support group? Is it the security group?
• Do you already have in-house expertise for any of the options? How can you best utilize
  that expertise with the available products?
• Are you willing to learn a new vendor’s product?
• Is everyone involved on board and agreeable with how the product works and interacts
  with different groups?
• Does NAC have upper management support?

Answering the questions above are almost more important than what product you choose and can
help you to eliminate products that will not fit with your company culture. NAC products and
offerings are way to complicated and intrusive to be purchased without being certain that the
product will be used and supported. Below is a list of the most common NAC vendors and their
websites.
### NAC Vendors | Website address
--- | ---
Bradford Networks | http://www.bradfordnetworks.com/network_access_control
Check Point Software Technologies, Ltd | http://www.checkpoint.com/
ForeScout | http://www.forescout.com/solutions/network-access-control/
Infoblox | http://www.infoblox.com/
InfoExpress | http://www.infoexpress.com/
Insightix | http://www.insightix.com/
Lockdown Networks | http://www.lockdownnetworks.com/
Trustwave | https://www.trustwave.com/network-access-control/

Overall network security needs to have a comprehensive plan for implementation. First of all you need to physically control access to your switching and routing infrastructure. It doesn’t matter how good a solution you have if someone can just walk into your wiring cabinet and break into any device located there. Most switches and many other types of devices can be password broken with physical access. You next need to address the configurations within your infrastructure.

Many security basics require nothing more than the time to implement. Just take care not to remove any service or protocol you might need such as CDP if using Cisco phones. Most switches and routers have the ability to protect the network at layer 2 and layer 3 of the OSI model. You just need to review the best security practices documentation of your switch and router vendor to see what you can implement. The next and important step is that you have a documented company security policy in place before moving forward. What you can and cannot implement as far as network access control is going to be based on what you have stated in your
written policy. After determining what you actually want to monitor and control make a specific list of goals and requirements. Using this list look at each of the vendors previously listed to see what solution best meets your requirements. Network security needs to take a multilayered approach, it needs to be reviewed often, and it needs to have the full support of upper management.


Practical Steps to Gaining Control of the Network Access


