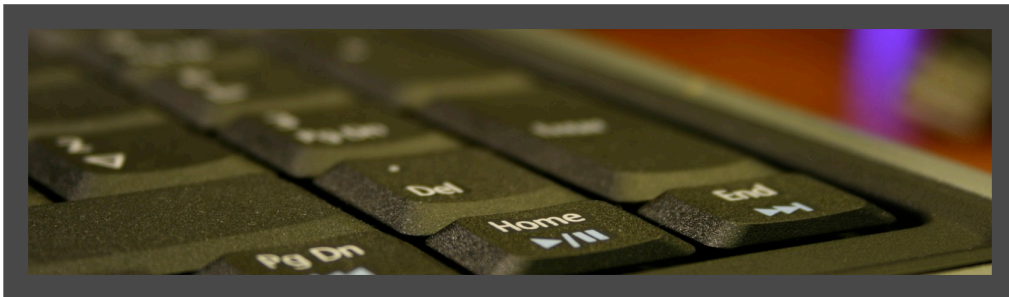


# CONVERGING WIRED AND WIRELESS AUTHENTICATION



*Bringing it all Together*

Bruce Potter  
Fall 2007

# CONVERGING WIRED AND WIRELESS AUTHENTICATION

## *Bringing it all Together*

Bruce Potter (bpotter@pontetec.com)

Ponte Technologies LLC

Fall 2007

Look at any network diagram in any large enterprise, and you will see two very different types of networks; wired and wireless. Wired networks are depicted as an array of boxes and lines, connecting through routers and switches in a manner we have become accustomed to over the last several decades. Wireless networks, on the other hand, are usually just clouds, a testament to the unstructured nature of wireless LANs and our ability to architect them. Wireless networks are often surrounded by numerous security mechanisms such as attack sensors, authentication servers, and VPN gateways. A wireless network often looks like a wart on a network diagram, waiting for someone to remove it when the users aren't looking.

Thankfully, our ability to architect and manage secure wireless networks has improved over the last several years. In the past, wireless networks were a completely separate entity from their wired counterparts and had high costs associated with them. But due to changes in technology, changes in wired networks, and even changes in laws and regulations, wired and wireless networks are beginning to converge. The first major aspect of convergence is authentication; bringing users and devices onto the network in a secure and consistent fashion.

## History of Wireless Authentication

Wireless LANs took the world by storm around 2001. At the time, user demand for wireless networking far outstripped the sophistication of the security protocols. The basic 802.11 security mechanism, WEP, did not stand up to even a casual attack. The encryption mechanism used in WEP provided very minimal confidentiality, and the authentication mechanism used was easily bypassed. On top of that, the authentication mechanism in WEP was based on pre-shared keys with a rudimentary key rotation scheme. WEP-based authentication was not scalable in even small enterprises, let alone in large, multi-national organizations.

In the face of the lack of a usable authentication mechanism, many new forms of wireless authentication were devised. Using IPSec VPN's became a popular means for controlling access to wireless networks. The basic premise is that the wireless network itself is completely open at layer 2. The layer 3 gateway, a VPN device, forces users to authenticate before building an IPSec tunnel and allowing outbound traffic from the wireless to the wired network. While effective at controlling access, this model is architecturally difficult to integrate and still leaves space

for some layer 2 attacks against the client devices. Other authentication mechanisms, such as captive web portals, work in niche environments but are not suited for general-purpose use.

The standards bodies addressed the security issues with the original 802.11 spec through the creation of 802.11i. 802.11i utilizes 802.1x authentication for network access. 802.1x has an extensible authentication and authorization model that allows for arbitrary authentication methods to be used including passwords, one-time passwords, and certificate-based authentication.

802.1x has become nearly ubiquitous in the last several years including default support in Windows XP, Vista, Mac OS X, and Linux. Almost every major piece of wireless networking gear, from consumer grade to enterprise capable, has 802.1x support integrated in. While there are other authentication methods available, 802.11i with 802.1x has emerged as THE standard for wireless authentication.

## History of Wired Authentication

For decades, the term “wired authentication” has made virtually no sense. The pinnacle of wired authentication was making sure you had a cable long enough to reach between your computer and the wall jack. The security of a wired network was dictated by the physical security protecting access to the infrastructure. With strong physical security, attackers wouldn’t be able to plug in and therefore your network would be protected. With weak physical security, an attacker could at least connect to the network and obtain layer 2 access. If the attacker had any skills, and had access to a port inside the firewall, they generally had full network access.

Times change, however, and wired authentication has started to come in vogue. There are a variety of drivers to the push to allow only authorized users to connect to a wired network. Systems have become very complex and the firewall/network security model we have used for the last decade is not able to effectively protect applications. In order to stay secure, IT security architects are pushing security all the way to the physical boundary. Some networks are now requiring authentication to be performed at the link layer as soon as a cable is plugged in. Without network-based authentication, the port the attacker is plugged into is useless and therefore cannot be leveraged to launch internal attacks.

Worms, viruses, and other malware have also increased dramatically over the last decade. Most enterprises have been hit by at least one (if not many) catastrophic virus outbreak that has caused massive loss of productivity and cash. Even with the best anti-virus money can buy, some end systems will have the AV software disabled, be missing a patch, or have some other critical problem that leads to a virus infestation. Network authentication provides a spigot to control what devices connect to the network and if the devices have a security configuration in accordance with an organization’s policy. The idea of quarantining a device to determine patch level and security posture before it is admitted on the network is being pitched hand in hand with network authentication. Microsoft, Cisco, and many smaller companies have network access and quarantine solutions that are deployable today.

Finally, there are now regulations being implemented across the globe aimed at raising the bar with respect to information security within the enterprise. Information security, or the lack therein, has created problems for consumers and investors; federal governments are getting involved to help fix the problem. Protecting personal identifying information (PII) and the assets that access PII has become a big problem for business. A company must be able to demonstrate they are attempting to protect access to PII or else they may face civil or criminal penalties in the event of a security failure. Network authentication and access control are becoming key parts of protecting sensitive information on corporate networks.

There are two competing technologies aimed at controlling network access. The first is the same 802.1x authentication mechanism that is already being used on wireless networks. 802.1x is a natural fit for network vendors since 802.1x is a layer 2 access control mechanism. Switches that natively understand 802.1x authentication can be very effective at keeping out unauthorized users and stopping attacks before they can even get started.

The other mechanism for controlling network access is the Microsoft Network Access Protection (NAP) capability. NAP, unlike 802.1x, is not geared at the networking equipment directly but rather at the supporting infrastructure. NAP controls access by controlling other aspects of the network such as preventing unauthorized users from obtaining a valid address via DHCP. NAP also leverages XP and Vista's built in capabilities in order to determine the health and security of the system prior to granting access. Unfortunately a dedicated attacker will be able to sniff other traffic on the network to determine the proper addressing and should be able to easily by-pass NAP's DHCP-based access mechanisms. The NAP solution is effective at keeping the good actors honest but is not as robust at keeping dedicated attackers off the network.

## Bringing It All Together

What were historically two very discrete aspects of an enterprise's network, wired and wireless, have reached a point where both have a common authentication solution. It is interesting that the reason wireless networks have reached a point where 802.1x makes sense is totally different than why wired users will use 802.1x. Wireless networks are natively physically unconstrained and therefore need strong authentication regardless of the specific assets being protected or the underlying legal constructs. Wired networks have become complicated enough on the last few years that network access control suddenly makes sense.

Enterprises are now at a point where a great leap forward can be made with respect to the economics and effectiveness of network-based authentication. While it is entirely possible to use proprietary wireless authentication and a non-interoperable wired network access control mechanism, there is no real need to. From a security and scalability perspective, 802.1x solutions provide a real economy of scale while meeting most organizations' security needs. The same factors for authentication can be used on both networks without any increased user education or burden. There is an obvious difference between wired and wireless in the need for confidential-

ity. Wireless networks still need to use some form of encryption for ensuring the confidentiality of the network transmissions. However this is a separate need and is easily addressed through the use of standards such as 802.11i.

## Parting Shots

Wireless networks are relative newcomers to the networking world. However, in the short time wireless LANs have had wide acceptance, they have pushed the boundaries for authentication, authorization, and confidentiality of large deployment networks. Through a series of technological and legal steps, wired networks are starting to bump up against the same problems that wireless networks have. While wired confidentiality is not an issue (yet), wired and wireless authentication is a big problem within many enterprises. With the advent of 802.1x and the authentication mechanisms therein, enterprises can unify what would otherwise be two disparate and individually expensive systems into one, unified authentication model.