Solution Guide

Allied Telesis

Network Access Control (NAC)

Allied Telesis provides advanced edge security for Enterprise networks

Security Issues

The security issues facing Enterprise networks have evolved over the years, with the focus moving from mitigating outward attacks, to reducing internal breaches and the infiltration of malicious software. This internal defense requires significant involvement with individual devices on a network, which creates greater overhead on network administrators. Allied Telesis lowers this overhead and provides an effective solution to internal network security, by integrating advanced switching technology as a part of Network Access Control (NAC).

The evolution of network defense

For many years, the focus in Enterprise network security was on defending against external threats. Firewalls were installed to protect the LAN from the hackers, worms, spammers and other security dangers of the Internet.

However, with the growth in mobile computing and the proliferation of Ethernet-capable devices, LAN-based attacks now outnumber external threats as the main security issues facing network administrators. Thus, attention has turned towards the 'enemy within'—the security dangers lurking within the local LAN.

Malicious software, known as malware, makes its way onto a network via employees, contractors and visitors. Personal laptops, wireless gadgets, and ever-popular USB flash drives all provide excellent vectors through which malware can enter the workplace. Even careful employees can unwittingly bring in malware, by using their equipment outside of the network. Visitors and contractors may be careless carriers of malware or, even worse, may be planning a malicious attack to steal data or cause disruption.

Defense against the enemy within

To effectively defend the network against internal threats, network administrators need secure LAN switches that provide protection against common attacks. They also need to implement policies that ensure that each device connecting to a network is as secure as possible. This combination of secure LAN switches and anti-malware policy can be very effective.

Allied Telesis switches have always provided a comprehensive range of defenses to combat internal attacks. These attacks range from data stealing attacks, such as Address Resolution Protocol (ARP) spoofing, to Denial of Service (DoS) attacks such as Tear Drop or Ping of Death. Correct deployment of these defenses can create a network that is impermeable to most of the harm these attacks cause.

Additionally, network administrators can institute a policy whereby network users are required to install and maintain anti-malware scanners, and to install security patches as they are released by Operating System vendors. However, this has required network administrators to spend time ensuring that users are adhering to policies, and has even generated counter-productive tension between network administrators and users.

More detailed information on how Allied Telesis secure LAN switches defend against the various types of LAN threats can be found on our website: http://www.alliedtelesis.com/solutions/netsecurity

The solution is NAC

This is where Network Access Control (NAC) provides a solution. NAC allows network administrators to automate policy enforcement. Rather than requesting that users ensure their devices conform to anti-malware policies, administrators can simply let the network do the job instead.

NAC has very quickly become an industry requirement, and is clearly much more than a new buzzword for network professionals. NAC offers an excellent way to control network access with automated policy enforcement, and to manage network security without vast administration overhead.

Put simply, NAC lets you define a comprehensive security policy for your network, implement that policy on a centralized server, and have the network automatically enforce that policy on all network users. NAC is much more than just user authentication—it is also designed to protect the network from users and devices that may be authorized, but still pose threats.

The most sensible place for this to occur is at the edge of the network, removing security threats before they gain any form of access. A NAC solution, which includes switches that act as enforcement points, ensures a proactive approach to network security.

How NAC secures your network

Today, network access for multiple device types or temporary users is an expectation, not an exception. Modern Enterprise network requirements include:

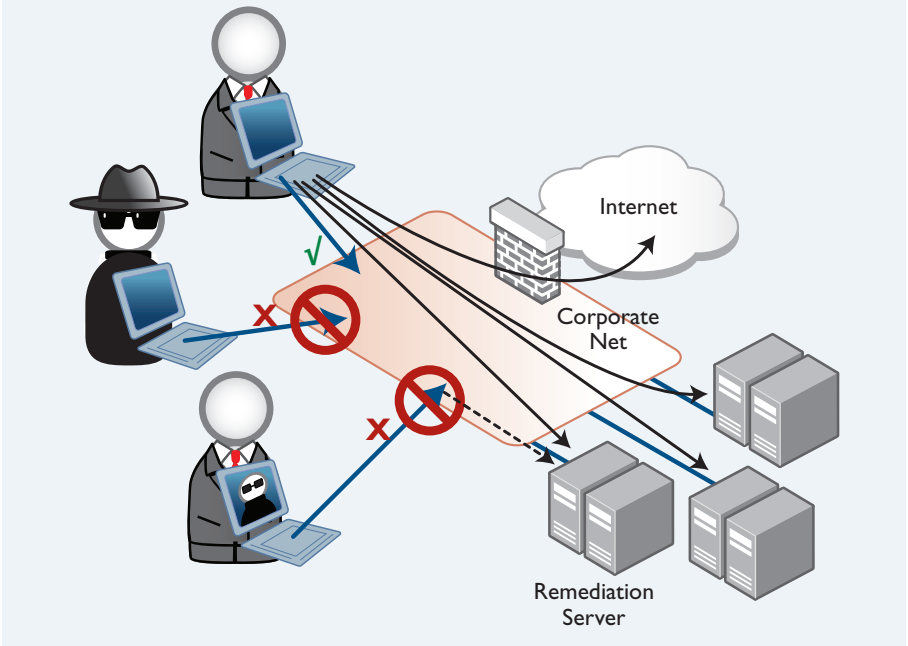
- some level of access, no matter who or where you are
- access for guests such as sub-contractors, partners and remote employees
- access control for a new range of connected devices, for example smartphones, tablets and digital cameras.

Allied Telesis LAN switches meet these emerging requirements, with comprehensive NAC features and integration. Used in conjunction with appropriate server-side and client-side software tools, they provide a remarkable level of control over the security status of the devices that connect to your network. The Allied Telesis NAC implementation is Trusted Computing Group's Trusted Network Connect (TCG-TNC) standards-based, to guarantee interoperability with the major third-party suppliers of NAC software, such as Microsoft and Symantec. This provides customers with the confidence to create a comprehensive NAC solution from trusted vendors.

At the heart of using NAC for your network security are three key elements:

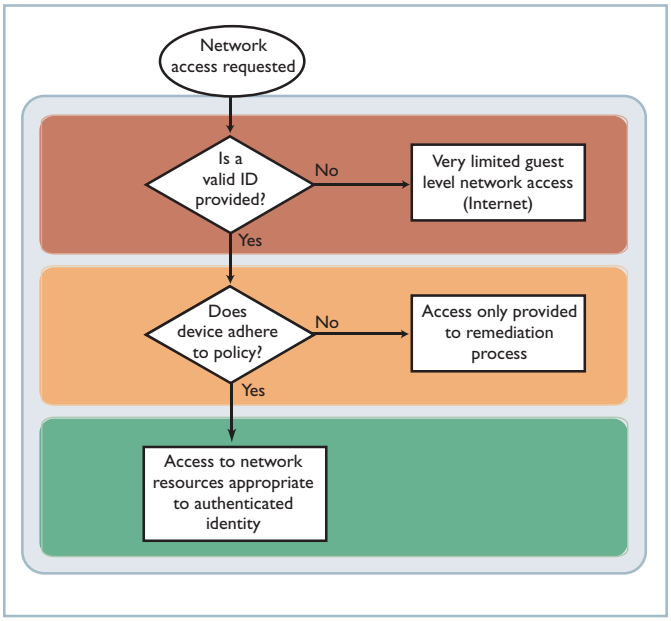
- no (or very limited) access without identification
- the quarantine and remediation of non-compliant devices
- setting the level of access to network resources based on a device's authenticated identity

NAC Solution



In practice, this means that every device is required to identify itself when it connects, and if appropriate, is then examined for its compliance to security policies. On a typical network, devices that:

- **Cannot provide a valid identity:** are completely barred from the network (or alternatively could have restricted access to the Internet, and nothing else).
- **Authenticate successfully but fail the policy adherence test:** are given access to a remediation process, and nothing else.
- **Authenticate successfully and are deemed policy adherent:** are given access to the network resources that match their identity.



This layered approach to network access control is illustrated in the figure above.

In this way, security policy enforcement and resource access control are performed by the network itself, utilizing NAC. Malware cannot harm the network, as it is never allowed access to the network. Intruders cannot commit theft or cause disruption, as they are either blocked or very tightly constrained.

NAC features on Allied Telesis switches

To provide this advance in network security, the significant elements included in Allied Telesis switch functionality are **tri-authentication**, **roaming authentication, two-step authentication**, and **integration with NAC infrastructure**.

Tri-authentication

Tri-authentication allows the network to identify all devices connecting to it. It can be used as part of a comprehensive NAC solution, or on its own where it provides a low overhead method of implementing network access security.

Roaming authentication

Mobile users move from one attachment point to another. Once a user has been given acccess, Allied Telesis roaming authentication ensures they are not inconvenienced by the need to re-authenticate as they roam.

Two-step authentication

Devices and users can be separately authenticated, to prevent sophisticated attempts to circumvent security.

Integration with NAC infrastructure

Allied Telesis equipment can integrate as a key component in network-wide NAC solutions.

Other documents you may be interested in:

Solutions:
Find out how our products and industry-leading features create solutions to meet your business needs.

How To Notes:
Find out how to set up and configure key features on Allied Telesis advanced switches and routers.

Success Stories:
Read customer success stories featuring Allied Telesis superior products and features.

For these documents and many more, visit:
http://www.alliedtelesis.com/library

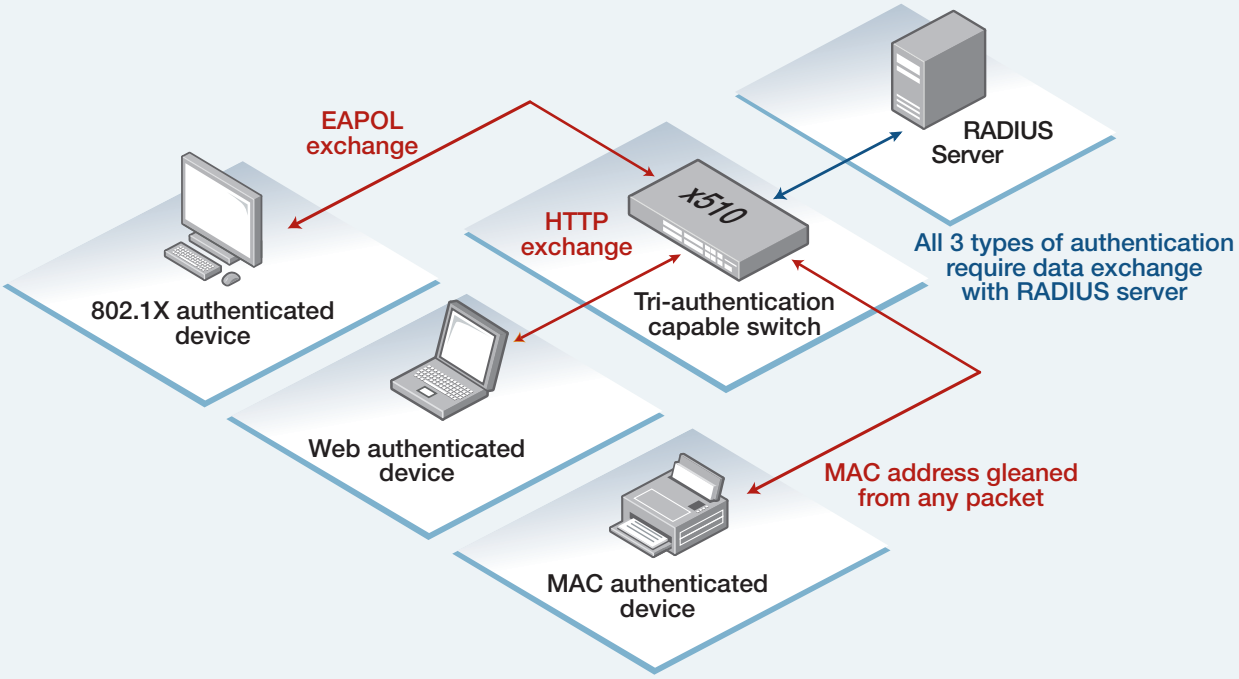
Tri-authentication: the Three Methods

802.1X is a highly secure authentication protocol that enables encrypted password exchange and certificate validation. A user is prompted for their name and password, and this is then checked against a user database before they are able to access the network. It is secure and configurable, but does require that 802.1X software is embedded and also configured in the client device. Not all devices connecting to the network will have this software embedded or pre-configured—this is particularly so for users who are temporary visitors.

Web authentication is provided to cater for computers in which 802.1X is not present or configured. The switch detects web-browsing activity from the client computer, and presents a login screen to the web browser. The user can progress no further until they have submitted a valid identity using the login screen. This authentication can either be performed in clear text, using the HTTP protocol, or performed in encrypted form using the HTTPS protocol.

MAC authentication is a fallback option you can use for non-interactive devices like printers or web cameras. A device's MAC address provides a unique identity that can be used to authenticate the device.

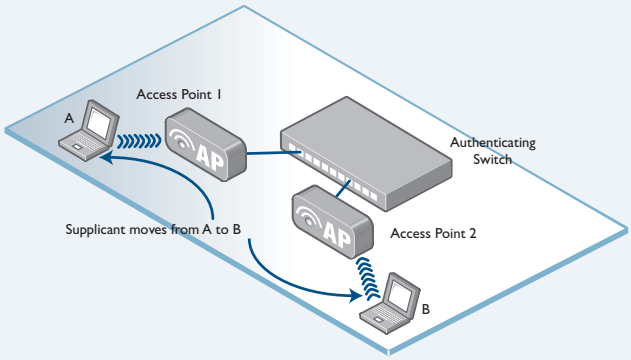
By providing these three authentication options, Allied Telesis switches make it possible to build a network in which you can authenticate all devices attaching to the network.



Roaming authentication

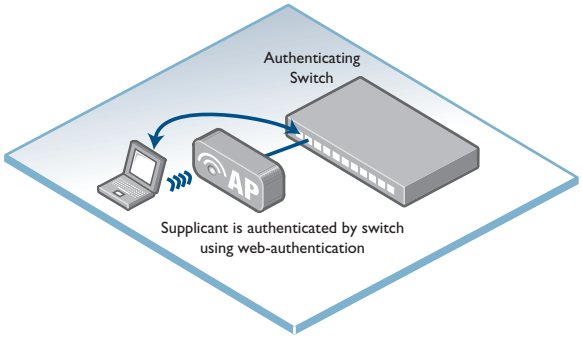
Wireless Ethernet users are mobile, and can roam from one access point to another. A user can be authenticated to a switch, behind the access points. By default, an authenticated session is associated with a specific switch port, which can make it inconvenient for the user to re-authenticate when moving between access points that are attached to different ports.

To solve this problem, Allied Telesis switches allow authentication status to roam along with the user. This capability is called "roaming authentication". With roaming authentication, when a user moves from one port to another, the authentication information about the user is transferred from the original port to the new one. Therefore, the user does not need to re-authenticate—their port transition is transparent.

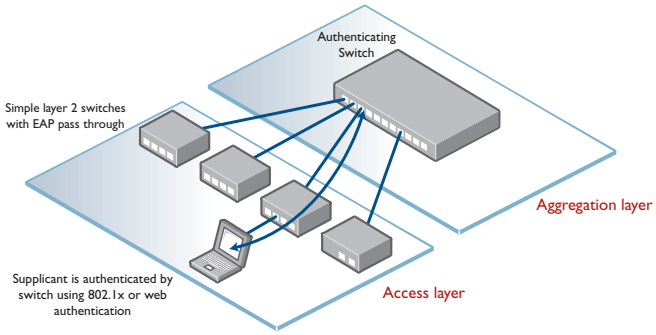


Roaming authentication in wireless and wired environments

In environments where 802.1X authentication is not used at the access point, the alternative is to use web authentication at the switch behind the access point. In this situation, roaming authentication is most valuable.

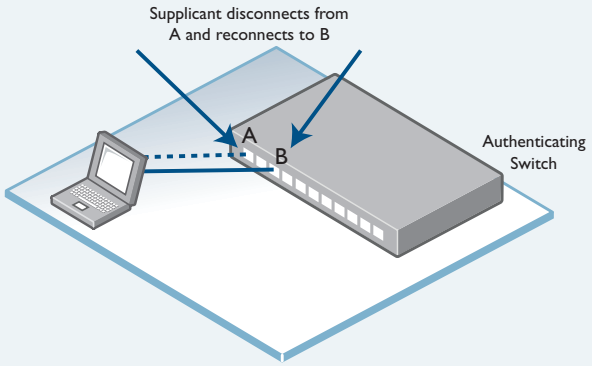


In a wired environment, where simple Extensible Authentication Protocol (EAP) pass-through switches are used at the edge of the network, then 802.1X or web authentication is performed on the authentication-capable switch at the aggregation layer.



In this case, roaming authentication for dot1x or web authentication enables a user to unplug from one edge switch and plug into another without needing to re-authenticate. Roaming authentication can support the case that the user is connected directly to the authenticating switch.

The roaming authentication for disconnected ports feature enables a user to be disconnected from a port on the authenticating switch and connected to another port of the switch without needing to re-authenticate.



Two-step authentication

Traditionally, network access authentication has involved just a single authentication method. Once a user or device has been authorized by MAC authentication, web authentication or 802.1X, then the authentication process is complete.

This single-step approach to authentication has potential security risks:

- an **unauthorized** user can access the network with an **authorized** device, for example by stealing a device that is authenticated by MAC authentication.

- an **authorized** user can access the network with an **unauthorized** device. The 802.1X and web authentication methods verify the identity of the user, but not of the device they are using.

To resolve these security risks, Allied Telesis has introduced "two-step authentication".

Two-step authentication involves authenticating both the user and the device. The supplicant will only become authenticated if both these steps are successful.

The process that occurs in two-step authentication is quite literally that the supplicant is authenticated twice, by two different methods.

The following authentication sequences are supported for two-step authentication:

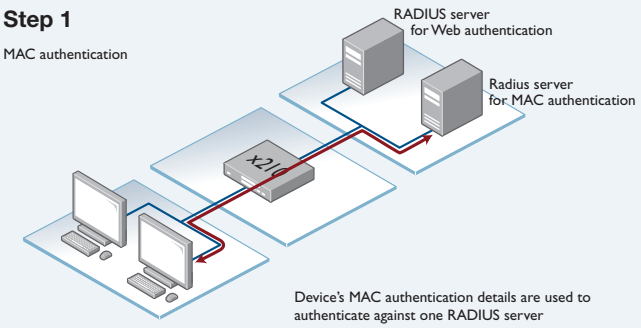
- MAC authentication followed by 802.1X authentication
- MAC authentication followed by web authentication
- 802.1X authentication followed by web authentication

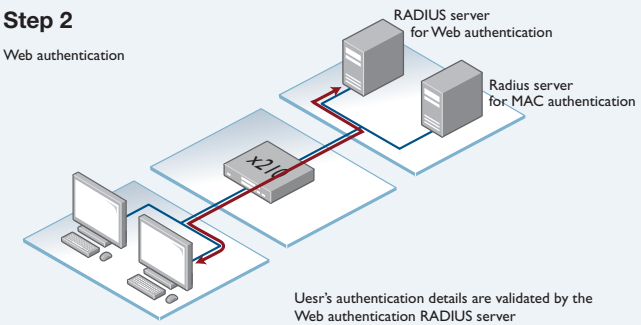
Per-method RADIUS servers

As another, further level of security, Allied Telesis supports the use of different RADIUS servers for different authentication methods.

Different RADIUS servers can be used for each of the three authentication methods. This allows for complete separation of the RADIUS databases used for the authentication methods that are used in two-step authentication.

Because of this database separation, a malicious user cannot circumvent two-step authentication by using the same username/password combination for both of the methods. The username/password that exists on one RADIUS server, for authentication by one method, should not be present on the RADIUS server used by the second method.





Integration with NAC Infrastructures

NAC integration makes it possible for switches to act as enforcement points in a NAC infrastructure with third-party software vendors. Specifically, this means that the switch will:

- transport the packets that constitute the NAC server's interrogation of the client device
- receive notification of the decision made at the decision point, and enforce that decision

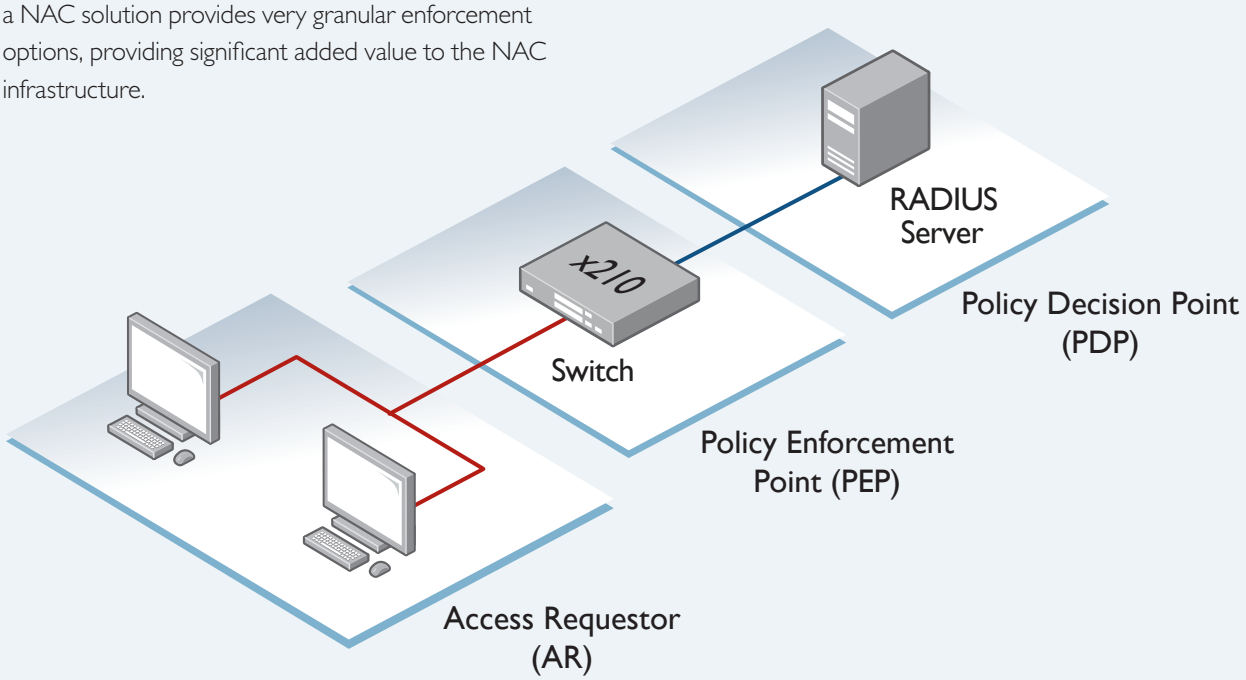
The below figure illustrates the role of the switch as Policy Enforcement Point (PEP) in a NAC solution.

The NAC server decides the level of network access a user can have, or the remedial action required to bring the user's computer or other end-point up to an acceptable level of compliance. The switch acts as the policy's enforcer, ensuring the ongoing security of the network, and the appropriate access to resources. The integration of advanced switching technology in a NAC solution provides very granular enforcement options, providing significant added value to the NAC infrastructure.

A more secure network

In conclusion, the modern enterprise has seen a phenomenal increase in the convergence of functionality on the network, with voice, video, security monitoring and more added to the traditional data and internet access. The need to control network access and provide a secure infrastructure is greater than ever.

Network Access Control can mitigate threats by combining access control with automated management of the security compliance of devices attached to the network. The advanced edge features on Allied Telesis switches ensure a secure environment for business to thrive.



About Allied Telesis

For nearly 30 years, Allied Telesis has been delivering reliable, intelligent connectivity for everything from enterprise organizations to complex, critical infrastructure projects around the globe.

In a world moving toward Smart Cities and the Internet of Things, networks must evolve rapidly to meet new challenges. Allied Telesis smart technologies, such as Allied Telesis Autonomous Management Framework™ (AMF) and Enterprise SDN, ensure that network evolution can keep pace, and deliver efficient and secure solutions for people, organizations, and "things"—both now and into the future.

Allied Telesis is recognized for innovating the way in which services and applications are delivered and managed, resulting in increased value and lower operating costs.
Visit us online at **alliedtelesis**.com

C618-31006-00 RevG