Learn About 802.1X Network Access Control (NAC)

This *Learn About* introduces you to 802.1X network access control (NAC) in campus and branch enterprise networks. Although 802.1X is widely deployed on wireless networks to secure access, also configuring 802.1X on wired networks enables network administrators to provide uniform NAC across both wired and wireless networks.

Network Access Control Challenges

Accessing a network is like waiting in line at stadium for a professional football game. Imagine fans lined up at dozens of gates (switch ports) showing their tickets (credentials) to get in. Once the fans are inside, their tickets, stadium signage, and helpful staff (policies) direct them to the level, section, and seats (resources) they are allowed to occupy during their time there (session).

Stretching this analogy a bit further, consider that the tickets can be stored on mobile phones, tablets, and watches, as well as paper, and that fans bring lots of devices into the stadium, thereby clogging network access. During the game, fans shoot video of the plays and stream it to their friends on the other side of the planet. Fans also check email, use social media, and even replay slow-motion clips of the last penalty that happened right in front of them. And, oh yes, they're making phone calls, too. This is your network today.

The impact of wireless network access, mobility, bring your own device (BYOD), social media, and cloud computing on enterprise network resources is huge. This expanded mobility increases exposure to network threats and digital exploitation, and when it comes to campus and branch work environments, the impact over the last five to ten years has been transformative. Figure 1 illustrates how challenging maintaining flexibility and access for consumers and business enterprises can be.

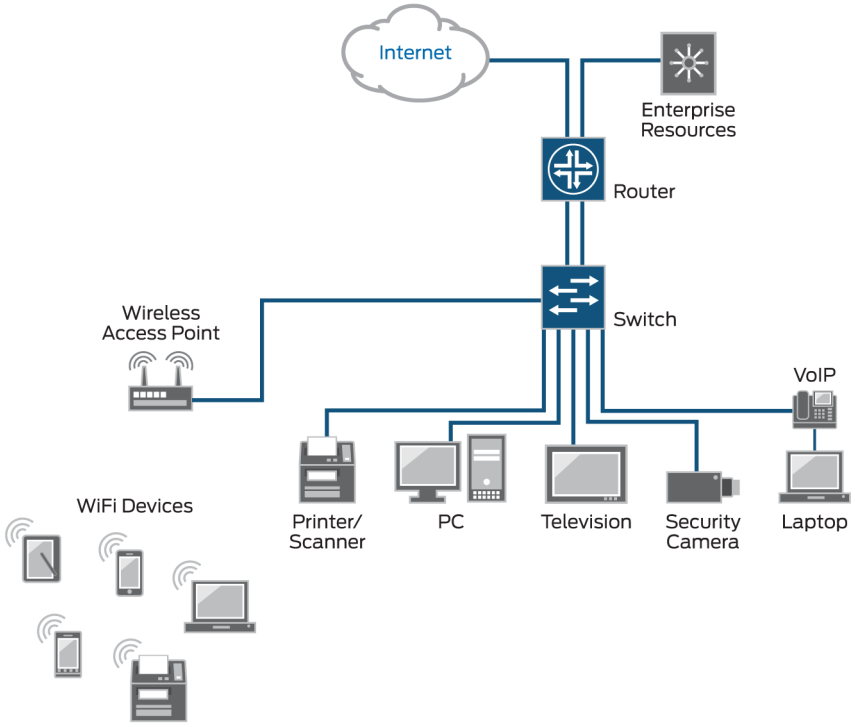


Figure 1 *Network Access Control Challenges*

The seemingly promiscuous nature of wireless access has made it the focus of heightened security efforts, but few enterprise networks are completely wireless. Wired access points and switch ports can be just as vulnerable to attack. Often, network administrators neglect to configure any security on their wired switch ports.

Some network administrators still believe in old myths: that switch ports are already inherently secure, without extra protection; that Layer 2 communications are safe because they operate at such a low level; that MAC addresses are too hard to spoof; that devices without user interfaces, like printers, are harmless to the network; and that because wireless access is secured with 802.1X, *wired* access doesn't need to be.

This *Learn About* covers the advantages of using the 802.1X protocol in a wired or mixed environment (populated with both wireless and wired devices) and reveals the options you have for using 802.1X to improve your ingress security while lowering total cost of ownership. It's a worthy combination to learn about.

What Is NAC?

NAC, a proven networking concept, can identify users and devices by controlling access to the network using one or more forms of authentication, and controlling access to enterprise resources using one or more forms of authorization and policy enforcement.

There are many ways to deploy NAC, and many decisions you'll need to make during the design and implementation phase, all dependent upon the specific service level agreements (SLAs) your organization has with your users.

Over the years, customers of NAC solutions, academic researchers, vendors, and organizations like the IEEE have developed a NAC model, the parts of which are considered to be the basic requirements of any effective NAC system. The essentials can be summarized as:

- *Pre-admission control*: blocks any unauthenticated messages from reaching the network.
- *Device and user detection*: identifies users and devices with pre-defined credentials or machine IDs.
- *Authentication and authorization*: verifies and provides access.
- O*nboarding*: provisions a device with security, management, or host-checking software prior to allowing network access.
- *Profiling*: scans endpoint devices based on a specific set of properties, or a profile, defined by security and IT personnel.
- *Policy enforcement*: applies role and permission-based access, deployed at Layer 3 firewalls or secure routers.
- *Post-admission control*: enforces session termination and cleanup.

What Is 802.1X?

The 802.1X protocol is an IEEE standard for port-based network access control (PNAC) on both wired and wireless access points. The primary intent of 802.1X is to define authentication controls for *any* user or device trying to access a LAN or WLAN.

MORE? 802.1X is part of the 802-family of standards. Look to the *Resources* section of this *Learn About* for links to various technical discussions of 802.1X as well as the standard itself.

Elements of an 802.1X Environment

802.1X provides L2 access control by validating the user or device that is attempting to access a physical port, typically at a switch or network edge device. As you can see in Figure 2, the basic 802.1X authentication mechanism consists of three components: supplicant, authenticator, and authentication server.

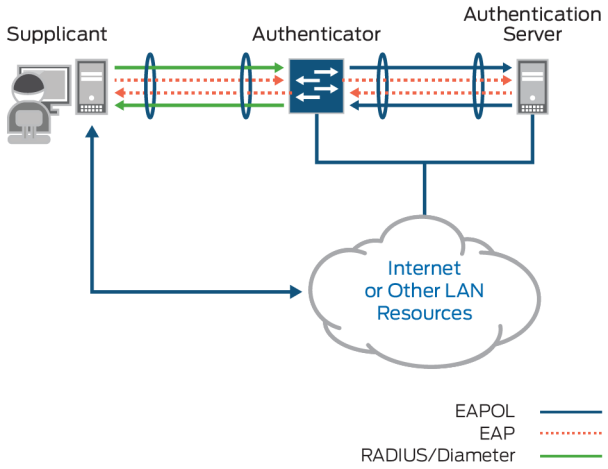


Figure 2 *802.1X Authentication Components*

- The *supplicant* is a client device that attempts to access the network. This could be a desktop or laptop computer, a tablet, a phone, a headless device such as a printer, or a wireless access point.
- The *authenticator* is the initial gateway, typically a switch, that intercepts the supplicant's access request.
- An *authentication server* compares the supplicant's ID with credentials stored in a database. If the credentials and the supplicant ID match, the supplicant gets to access the network.

Authentication Modes

When configuring 802.1X authentication, administrators can set one of three modes for the process: *single*, *single-secure*, or *multiple*. In single authentication mode only the first supplicant to request access gets authenticated. In single-secure mode one supplicant at a time gets authenticated and no other supplicant can be authenticated until the first supplicant finishes its network session. In multiple authentication mode many supplicants access the port, but each one is authenticated individually. Organizations often use multiple mode to deploy VoIP phones that each have a physical Ethernet port, allowing a user to chain a laptop onto the phone, thus cutting down on the cost of configuring and maintaining Ethernet connections.

EAP Message Format

The 802.1X standard specifies the Extensible Authentication Protocol (EAP) as its encrypted message format for transmission between supplicant and authenticator. Until a supplicant is authenticated and allowed access to the network, any messages between the supplicant and the authenticator are vulnerable.

EAP is widely used, and there are many variations for securing EAP messages. EAP *methods* generate a message frame, as shown in Figure 3, that contains the following pieces of data:

- MAC address header for the device that is the supplicant.
- A message type attribute.
- Length attributes.
- Encrypted keys.
- A frame check sequence for error detection and correction.

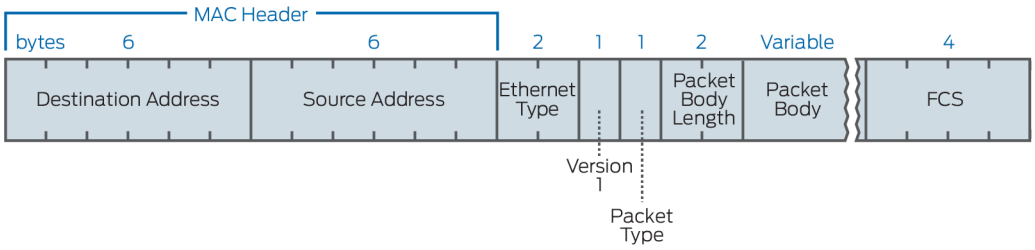


Figure 3 *EAP Message Frame*

NOTE EAPoL, or EAP over LAN, is an encapsulation technique used to protect communications only between the supplicant and the authenticator. EAPoL protects those communications that occur before authentication.

EAP methods, in contrast to EAPoL, specify the message format used for communications between the supplicant and the authentication server. Some EAP methods, such as Lightweight EAP or LEAP and EAP-MD5, have fallen out of favor, due to demonstrations of their inherent weakness. But there are many other robust EAP methods such as: PEAP, EAP-TLS, and EAP-TTLS. Each of these methods specifies a different way of protecting the credentials that are passed from a supplicant to an authenticator.

PEAP and its variants are widely used. PEAP-MSCHAPv2 is popular with Windows supplicants. EAP-TLS employs both client and server certificates, which are presented and verified at each point of the communication path. However, because certificates are very expensive for individuals and small organizations, EAP-TLS is used infrequently. EAP-TTLS, on the other hand, creates a secure, encrypted tunnel through which the switch passes the EAP messages. With EAP-TTLS, the client-side certificate is optional, which has made this message format very popular. Other EAP methods are developed as new requirements and updates to authentication servers evolve.

Authentication Server Components

RADIUS is the most commonly used authentication server in 802.1X environments. RADIUS provides secure authentication and can easily be paired with an organization's other identity databases, such as LDAP and Active Directory, to leverage existing credentials.

The typical 802.1X configuration includes fallbacks for those users or devices that do not, or cannot, authenticate using 802.1X, such as headless devices, contractors, and guests.

Headless devices cannot authenticate using 802.1X, primarily because these devices – printers, industrial controls – do not possess a user interface through which to pass credentials. Additionally, these devices often attempt to connect to a network automatically upon startup.

Configuring MAC RADIUS authentication on a port, along with 802.1X, is a common approach for authenticating headless devices. MAC RADIUS authentication allows the RADIUS server to authenticate supplicants by their MAC addresses.

Guests, contractors, and other temporary visitors are often authenticated by Web authentication. When a guest attempts to access the Internet over the enterprise network, the guest's Web browser is redirected to a website where the guest must enter guest credentials or agree to an acceptable use policy before being granted further access. The access granted to guests usually restricts them to Internet access only and blocks them from internal networks.

When Web authentication is configured on a port, it usually kicks in after 802.1X and MAC RADIUS authentication fails. Most enterprises implement Web authentication so that the switch port redirects the guest to a central Web authentication server for authentication. Using central Web authentication simplifies the management of guest accounts and enables the unified management of both wired and wireless guest access.

802.1X Authentication Process

Let's follow a typical 802.1X authentication process.

The process starts with the initial message flow. By default, no messages are allowed to pass the access point, other than an EAP-start-request message from the supplicant, or an EAP request from the authenticator to the supplicant, as shown in Figure 4.

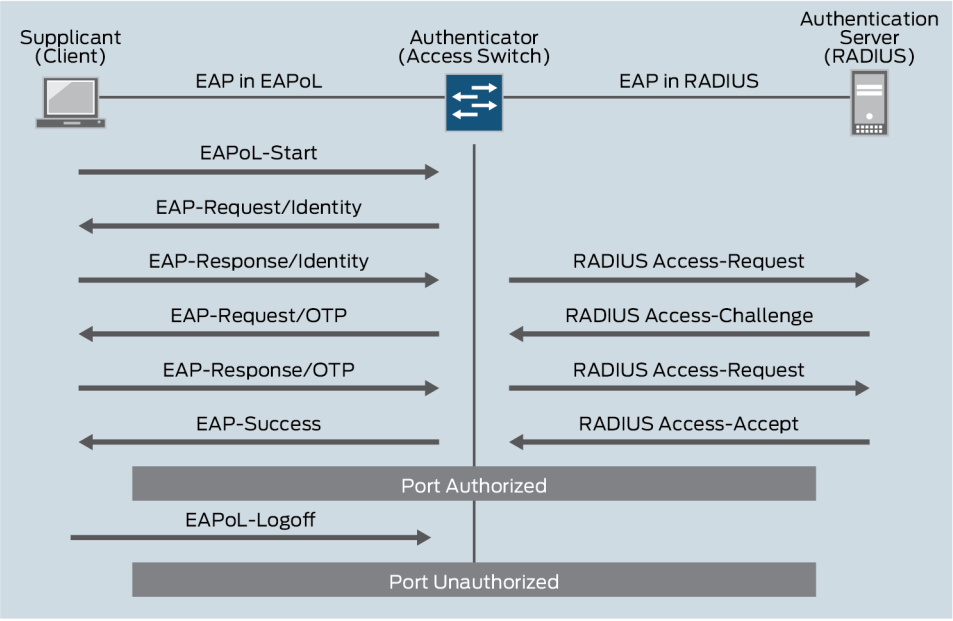


Figure 4 *802.1X EAP Message Flow*

The typical 802.1X NAC operation sequence consists of initiation, authentication, authorization, accounting, and termination.

Session initiation – Either the authenticator or the supplicant can send a session initiation request. In many networks, the authenticator periodically polls a specific port address with an identity request. A supplicant that intercepts the request sends an EAP-response message back to the authenticator, which then encapsulates the message in a RADIUS access request packet and forwards it to the authentication server. Note that the three components may pass many different types of messages back and forth during this exchange.

The 802.1X standard defines two logical port states: *controlled* and *uncontrolled*. In the *uncontrolled* state, the authenticator blocks all traffic with the exception of Extensible Authentication Protocol over LAN (EAPoL) frames between the supplicant and the authenticator, and between the authenticator and the authentication server. When the supplicant has been successfully authenticated, the port is put into the *controlled* state, allowing traffic into and out of that port as depicted in Figure 5.

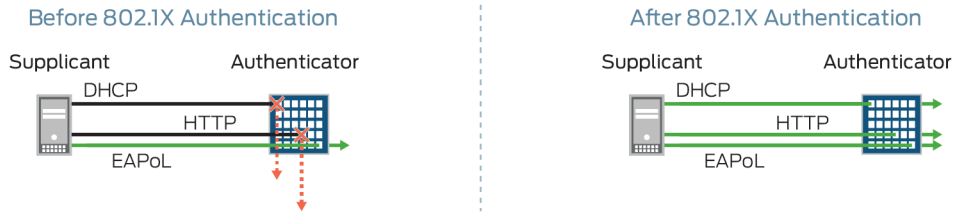


Figure 5 *Controlled Versus Uncontrolled Port Traffic*

Session authentication – During session authentication, messages pass between the authentication server and the supplicant via the authenticator to validate several pieces of information: Does the authentication server possess a valid certificate? Is the supplicant able to communicate properly using a valid EAP method? The agreed-upon EAP method defines the type and format of credential that will be passed to the authentication server for authorization.

Session authorization – *If the credentials are valid*, the authentication server notifies the authenticator to give the supplicant access to the port. Some switches apply a level of policy enforcement at this point, following access control list (ACL) or VLAN prescriptions for the specific user or device. *If the credentials are rejected as invalid*, the supplicant can retry authenticating, or the network may force the supplicant into a more restrictive form of authentication.

Session accounting – RADIUS accounting keeps detailed session records including user and device details, session types, and service details, all of which you need for troubleshooting, class-of-service (CoS) control, and billing purposes.

Session termination – EAPoL-Logoff messages have been found to linger, raising potential security risks when sessions are not properly terminated. All 802.1X sessions should be terminated by disconnecting the endpoint device, or by using management software to send a logoff command or to simulate a downed link state.

Juniper Networks NAC Solution

Juniper's NAC solution is one component within the Juniper Networks Unite Architecture, as shown in Figure 6, and consists of 802.1X-enabled EX Series switches and solutions provided by our NAC partners, Aruba Networks and Pulse Secure.

Juniper Networks Unite Architecture is a secure cloud-enabled network infrastructure that supports a diverse set of devices, applications, people, and things. Juniper's NAC solution includes devices and software components that simplify access control management for campus and branch enterprise networks. Simplification means easier configuration, functionality to dynamically control access across the network, and monitoring tools that span device types, delivering a complete picture from a single-pane-of-glass interface.

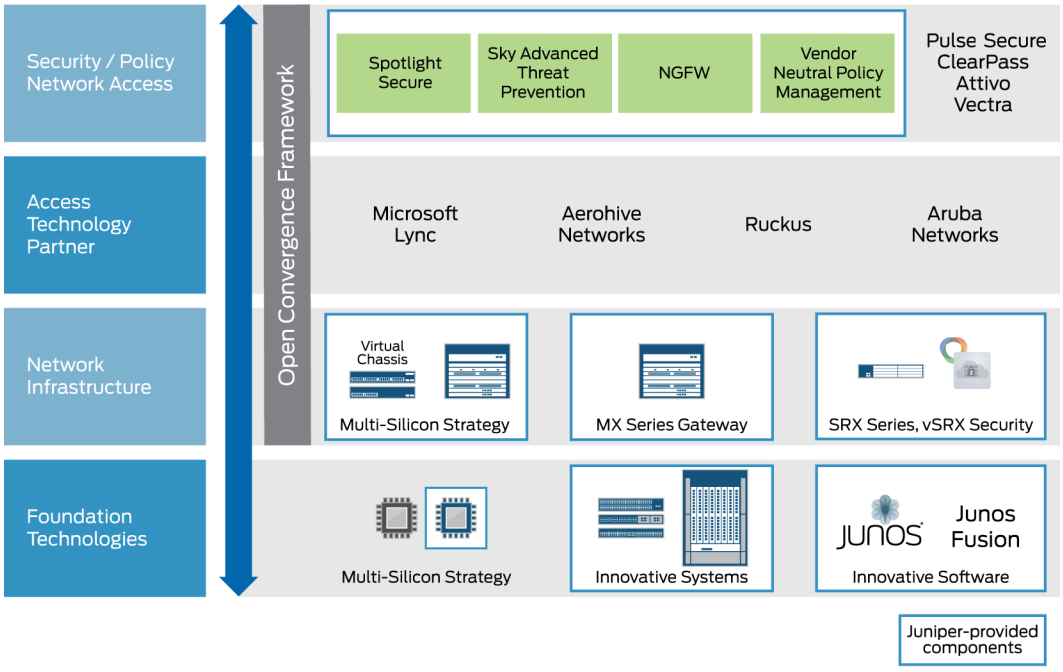


Figure 6 *The Unite Cloud-Enabled Enterprise Reference Architecture*

EX Series 802.1X Support

The EX Series Ethernet Switch family is Juniper's gatekeeper in the campus and branch enterprise network. The EX Series provides extensive 802.1X and RADIUS support. In addition, the EX Series delivers several enhancements to the standard 802.1X authentication functionality by expanding the number of ways to deal with incoming access requests, and by simplifying wide-scale deployment of network access control.

For instance, by default, the authentication sequence starts with 802.1X, falls back to MAC RADIUS authentication, and, finally, redirects to central Web authentication, if all else fails. No need to manually configure this fallback sequence.

Dynamic VLANs

The dynamic VLAN feature supported by EX Series switches and RADIUS gives you powerful flexibility in controlling access to your 802.1X environment.

You define dynamic VLANs on the switch without associating them to a specific port; on the RADIUS server, you associate the VLAN IDs with specific MAC addresses or other user identifiers. During the 802.1X authentication sequence, if RADIUS supplies the VLAN ID in the authorization response for any authenticated supplicant that matches the supplicant, it stays in that VLAN during its entire session, regardless of which part of the network it accesses.

The benefit of using dynamic VLANs is that traffic can be assigned to different VLANs, which increases security, policy enforcement, accounting, monitoring and flexibility. Different endpoints can be plugged into the same port at different times, and can be automatically assigned to different VLANs without reconfiguring the port.

Dynamic Firewall Filter (ACL) Support

EX Series switches support both *static* and *dynamic firewall filters*. These filters allow you to control access to parts of the network and discrete network resources, based on conditions you configure on the switch port.

You can define firewall filters on the EX Series switch or on the RADIUS server. When a supplicant has been authenticated by RADIUS, the RADIUS server passes a dynamic filter name to the EX Series switch, which then applies it to the supplicant's session traffic.

The RADIUS server can also pass the entire firewall filter to the EX Series switch, which then installs and applies the filter dynamically. This eliminates the need to configure the firewall filter on each and every access switch in your network. Sending the filter from a centralized RADIUS server lets you update all access switches with the same filter at once.

Central Web Authentication

The EX Series offers central Web authentication as an optional authentication method, in addition to 802.1X and MAC RADIUS. As mentioned previously, central Web authentication can be used as a fallback when 802.1X, MAC RADIUS, or static MAC fails to authenticate the supplicant. You can also configure local Web authentication on the EX Series.

Guest VLAN

EX Series switches support straightforward configuration of guest VLANs. Supported policy management platforms, such as Aruba ClearPass Guest, provide workflows that make it easy to deploy automated guest, visitor, and contractor access and maintain consistent access security across wired and wireless networks.

Server Reject VLAN

The server reject VLAN (sometimes known as a quarantine VLAN) is an EX Series feature that allows the switch to put rejected supplicants into a restricted VLAN where they are quarantined pending additional password authentication.

MAC RADIUS and Static MAC Support

The EX Series supports the use of both MAC RADIUS and static MAC, as well as MAC authentication bypass. Let's consider the most common scenarios of their use:

You can enable MAC RADIUS authentication on a port together with 802.1X, meaning that if the port doesn't receive EAP packets from an endpoint, the EX Series switch instead sends the MAC address of the endpoint to the RADIUS server for authentication. The

RADIUS server can be configured to maintain a database of MAC addresses of authorized endpoints, such as printers or other headless devices, or it can base authentication on device profiling (assuming you also use a policy manager that supports device profiling).

You can also restrict the ingress port to MAC RADIUS authentication only. In this case, the switch never tries 802.1X but passes the MAC address to the RADIUS server directly.

Alternatively, you can enable static MAC authentication bypass, which avoids RADIUS authentication altogether. In this case, you statically configure, on the EX Series switch itself, a list of MAC addresses allowed on the port. The switch looks up the endpoint in this local list and never contacts the RADIUS server.

Juniper Networks and its policy management partners, Aruba Networks and Pulse Secure, support the implementation of all of these access methods, as well as combinations to fit your unique needs.

RADIUS Change of Authorization

RADIUS Change of Authorization (CoA) support allows you to specify midstream changes to any session, based on subscriber and session attributes. EX Series CoA lets you terminate a session or change the current VLAN, firewall filter, voice VLAN ID, and the session timeout.

RADIUS Accounting Support

RADIUS accounting features on EX Series switches allow you to track supplicant access and supplicant termination. The EX Series device sends this statistical data to the RADIUS server, which then logs these network traffic and usage patterns. You can use these statistics to analyze traffic and usage, and to bill subscribers, if desired.

Vendor-Specific Attribute Support

The vendor-specific attribute (VSA) is a RADIUS feature that allows vendors like Juniper Networks to supply a set of unique attributes that the RADIUS server can pass back to the switch to direct or set policies on the authenticated session—for example, returning a VLAN ID indicating where to put the current supplicant session. Juniper Networks supports a number of VSAs, including those that allow midstream configuration changes.

VoIP Support

EX Series switches support VoIP, including the direct connection of an IP phone to an EX Series switch port. Most commonly, VoIP solutions are connected through a voice VLAN, which keeps voice and data traffic separated for improved performance and security. You can authenticate VoIP devices using 802.1X, in *single* and *multiple* supplicant modes. *Single-secure* mode is not supported. You can also employ the Juniper VSA that allows you to dynamically assign a VLAN ID to the voice VLAN as part of the authentication sequence.

Partner NAC Solutions

The solutions offered by Juniper's select vendors provide full-spectrum management of your network access control. By centralizing management and monitoring functionality in easy-to-use visual interfaces, these solutions give your staff great leverage over the growing and complex access demands on your network.

Aruba ClearPass Policy Management Platform

Aruba Networks ClearPass Policy Management Platform provides access layer security for user authentication, policy management, and BYOD onboarding across both wired and wireless networks.

ClearPass acts as a RADIUS server and policy manager, providing role-based policy management for end users and devices. ClearPass provides enterprise-grade authentication, authorization, and accounting (AAA), through RADIUS and TACACS+, 802.1X, and non-802.1X services.

Its ability to deliver high-bandwidth performance makes ClearPass a powerful tool in environments where HD video, unified communications and collaboration tools, and other cloud-based applications make increasingly greater demands on your network.

ClearPass offers a range of other NAC services including guest access, device profiling, and device onboarding.

ClearPass integrates with both EX Series switches and SRX Series services gateways. This deep integration provides protection at both the edge and in the center of your network, making it a perfect component of the Juniper Networks Unite Architecture.

See the *References* section at the end of this *Learn About* for links to more information about ClearPass and to configuration examples using ClearPass and EX Series switches.

Pulse Secure

Pulse Secure is a leading provider of secure access products for today's networks. Juniper Networks relies on integration with Pulse Secure products to provide its customers with flexible and powerful NAC solutions.

Pulse Policy Secure

Pulse Policy Secure delivers an easy-to-use access control solution for the most complex data center and cloud environments. Pulse Policy Secure provides complete network access control, including device onboarding, auditing and monitoring, guest access control, and unified policy management across your entire network.

Pulse Policy Secure Profiler

The Pulse Policy Secure Profiler provides automatic network-attached device identification, audit, and policy enforcement, even for headless devices, such as printers, fax machines, or VoIP handsets. The Pulse Policy Secure Profiler offers tight integration with EX Series switches, as well as with other devices in a multi-platform environment.

References and Resources

To learn more details about the topics discussed in this document, visit the following links.

802.1X Network Access Control

IEEE 802.1X Port-Based Network Access Control (IEEE Std 802.1X™-2010)

RADIUS and EAP

IEEE 802.1X RADIUS Usage Guidelines (RFC 3580)

Extensible Authentication Protocol (EAP) (RFC 3748)

Juniper Unite Architecture

Juniper Unite Reference Architecture

Juniper Networks EX Series Switches

Understanding Authentication on EX Series Switches

Firewall Filters for EX Series Switches Overview

Understanding 802.1X and VoIP on EX Series Switches

Understanding 802.1X and RADIUS Accounting on EX Series Switches

Understanding Dynamic Filters Based on RADIUS Attributes

Applying a Firewall Filter to 802.1X-Authenticated Supplicants by Using RADIUS Server Attributes on an EX Series Switch

Understanding Central Web Authentication

Network Configuration Example Midsize Enterprise Campus Solution

Aruba Network ClearPass Policy Management Platform

Aruba Networks ClearPass Policy Management Platform Network Access Control

Configuring 802.1X PEAP and MAC RADIUS Authentication with EX Series Switches and Aruba ClearPass Policy Manager

Aruba ClearPass Profiling Technote

Device Profiling with EX Series Switches and Aruba ClearPass Policy Manager

Configuring Central Web Authentication with EX Series Switches and Aruba ClearPass

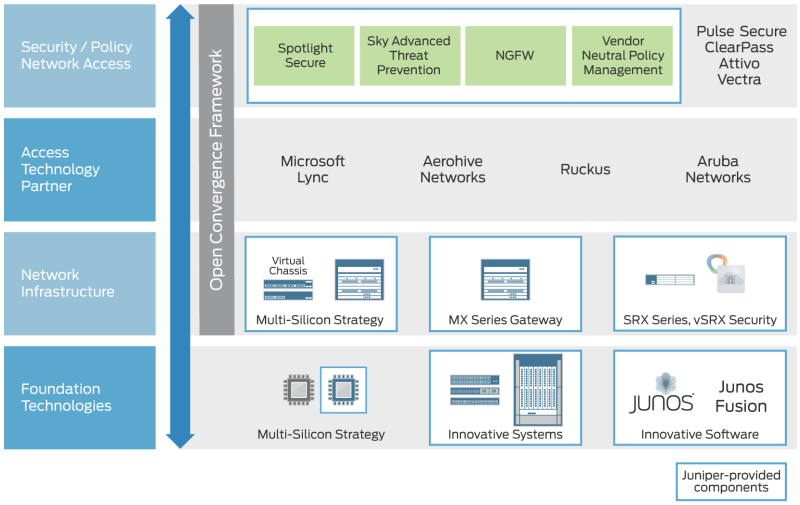
Pulse Secure

Pulse Policy Secure Resources

Learn About 802.1X Network Access Control (NAC)

by Mark Smallwood

The impact on enterprise network resources from wireless network access, mobility, bring your own device (BYOD), social media, and cloud computing over the last years has been transformative. To keep pace, standards around 802.1X and Network Access Control (NAC) have evolved, including the products and partners of Juniper Networks. Learn about how to keep your enterprise network secure yet operational to both wired and wireless users.



About the Author:
Mark Smallwood is a professional writer with over 25 years of experience in Silicon Valley. Formerly, he was a senior manager at Juniper Networks.

Author's Acknowledgments:
Many thanks to Brooke Doverspike, whose technical knowledge and writing advice were invaluable on this project. Thanks also to Patrick Ames, Karen Joice, Suresh Palguna Krishnan, Nancy Koerbel, Lisa Eldridge for their help reviewing and editing the manuscript, and finally to Jerry Isaac, who invited me to get involved.

Version History: First Edition, May 2016 2 3 4 5 6 7 8 9

For more information go to the TechLibrary at: www.juniper.net/documentation