

White Paper

802.1X: Port-Based Authentication Standard for Network Access Control (NAC)



Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408.745.2000
1.888 JUNIPER
www.juniper.net

Table of Contents

Introduction	3
How Does 802.1X Work	3
802.1X and Extensible Authentication Protocol (EAP)	5
Network Access Control (NAC)	5
Standard vs. Proprietary Network Access Control	5
802.1X and Network Access Control.....	6
Juniper Networks Unified Access Control (UAC) v2.0.....	7
UAC v2.0 and 802.1X	7
Summary	9
About Juniper Networks	9

List of Figures

Figure 1 – Typical 802.1X Network Environment	4
Figure 2 – Juniper’s Unified Access Control (UAC) v2.0	7
Figure 3 – Juniper’s Unified Access Control (UAC) v2.0 showing 802.1X standards-based components integration	5

Introduction

Organizations continue to embrace mobility and wireless LAN (WLAN) access in record numbers. Mobility attracts them because it promises hassle-free, anytime, anywhere access that enables employees to be connected and productive 24/7. These same organizations are also motivated to implement WLANs because they are simple to install. A WLAN has limited need for wiring, making it less costly than traditional wired networks to deploy and more flexible for implementing physical office changes, saving additional expense. However, while mobility and wireless network access are highly desirable, maintaining security remains a key concern for enterprises. The greater the number of wireless LANs an enterprise has, the greater risk there is that their network can be hacked or attacked. And the open nature of WLAN access also brings its own security concerns as user information and corporate data are in danger of being snooped or stolen while the wireless connection is being established and even once the user is connected.

What organizations require is a mechanism that ensures network credentials remain secure over a wireless link or wired connection, one that guarantees that the user and device are who and what they claim to be, one that can assure users and administrators that they are connecting to the approved enterprise network, and that the network is not being spoofed or hacked. The proliferation of mobility and wireless access has also created the need for a standard authentication protocol framework to address the wide variety of authentication systems being used and deployed.

Enter 802.1X, the standard for port-based network access control. 802.1X was originally designed for use in wired networks but was adapted to address WLAN security concerns because of its robust, extensible security framework and powerful authentication and data privacy capabilities. An Institute of Electrical and Electronics Engineers (IEEE) standard, the 802.1X framework empowers the secure exchange of user and/or device credentials, and prevents virtually any unauthorized network access since authentication is complete before a network IP address has been assigned. (802.1X operates at Layer 2 or the Data Link layer of the Open System Interconnection (OSI) seven layer model for networking.)

It is the strong, durable security and authentication of the 802.1X standard framework that has led to its acceptance as a means of providing network access control (NAC). And while it may seem surprising that a five year old standard is being championed as a key component of one of today's hottest network technologies, one need only remember that 802.1X is the IEEE standard for port-based network access control. An additional benefit of 802.1X is that the standard has been field tested in WLAN deployments for years.

How Does 802.1X Work

An 802.1X network requires only three components to operate, each of which is referred to in terms that are somewhat unique to this standard. Those components are:

- **A Supplicant** – software that implements the client side of the 802.1X standard and works in wired or wireless environments. The Supplicant is loaded onto the user's device and is used to request network access.
- **An Authenticator** – a component that sits between the external user device that needs to be authenticated and the infrastructure used to perform authentication. Examples of Authenticators are network switches and wireless access points.
- **An Authentication Server** – a server which receives Remote Authentication Dial-In User Service (RADIUS) messages and uses that information to check the user's or device's authentication credentials, usually against a backend authentication data store such as Windows Active Directory, Lightweight Directory Access Protocol (LDAP), or other directory store or database.

In addition, a secure, flexible authentication framework for access control is also needed to ensure the secure passing and validation of network credentials. This framework should also simplify the creation and maintenance of additional authentication methods. The Extensible Authentication Protocol standard (EAP) was created explicitly to meet these requirements. An Internet Engineering Task Force (IETF) standard, EAP enables the creation of a variety of extensible access protocols providing flexible, expandable network access and authorization.

How an 802.1X network works – whether it is wireless or wired – is straightforward, which is part of the reason for its popularity. When attempting to access an 802.1X-based network, instead of simply being granted Layer 3 access, the port challenges the user for their identity. If the user’s device is not configured for use in an 802.1X-based network – that is, it does not have a running Supplicant – the port will deny network access. With an operational Supplicant on the device, the Supplicant will respond to the port’s challenge for user identity and start the 802.1X authentication process. The Supplicant passes network credentials (user and/or device identification information) to the Authenticator, which verifies the connection to the network and passes the identification information on to the Authentication Server. Figure 1 below is a graphical representation of a typical 802.1X network environment. In an 802.1X compliant network, both the Supplicant and the Authenticator must support the 802.1X standard and there must be an Authentication Server component in the environment to complete the transaction.

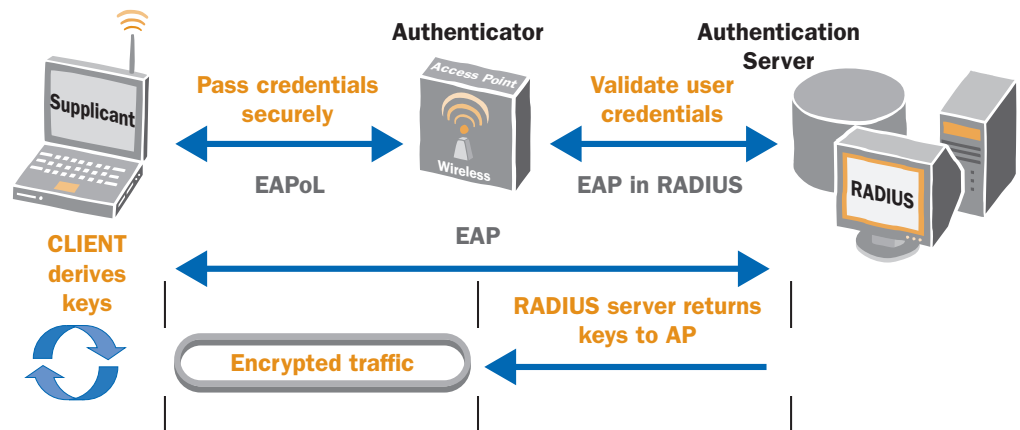


Figure 1 – Typical 802.1X Network Environment

Network credentials are presented by the Supplicant and passed to the Authenticator. These credentials must then be validated by the Authentication Server. Once that validation occurs, a network port on a switch or a wireless access point is opened and made available for the user or device to gain access to the network. If network credentials are in order and approved, the user can access the network. However, if the network credentials are not up to par and are not approved or if the service to check the network credentials is unavailable for any reason, the user can be denied access to the network. The combination of robust security with simple “on/off” control of network admission is another key reason for the popularity of 802.1X. In some cases, organizations may wish to allow holders of inappropriate, invalid, or unchecked network credentials limited access to the enterprise network, or allow them Internet access only. These options may be achieved through VLAN tagging or routing which must be supported by the network switch or access point (IETF Request For Comments (RFC) 3580).

802.1X and EAP

The 802.1X standard works in conjunction with powerful, robust EAP methods, such as tunneled EAP types like EAP-Tunneled Transport Layer Security (TTLS) or EAP-Protected Extensible Authentication Protocol (PEAP). Both EAP-TTLS and EAP-PEAP provide a secure EAP overlay which is useful for encasing other non-tunneled EAP methods or other authentication protocols carrying network credentials and other relevant data. By utilizing tunneled EAP methods, enterprises can be assured that their network credentials are fully protected and that data privacy is being achieved and maintained. Additionally, with network access control, there is a need to include more information with the authentication protocol about and from the user and their device, such as endpoint security and posture validation. This requires the expanded security and authentication capabilities available from tunneled EAP types.

Once an EAP method has been selected, both the Supplicant and Authentication Server must be communicating with this EAP method. EAP messages are transported between the Supplicant and the Authenticator over a Layer 2 authentication protocol specified by 802.1X, EAP over LAN (EAPoL). EAPoL is an encapsulated form of EAP that prefixes an Ethernet header onto EAP messages so they may be transmitted over an Ethernet network directly by a LAN media access control (MAC) service between the Supplicant and Authenticator. The Authenticator communicates with the Authentication Server which understands RADIUS messages via EAP in RADIUS, a Layer 3 transmission that allows for the secure passing of authentication messages (authentication request, authentication result) and port authorization (accept, reject) between the Authenticator and Authentication Server.

Network Access Control (NAC)

There is no universally agreed upon definition for what a solution should provide in the fast growing category of network access control. This is one of the most difficult aspects of the category since it is tempting to allow a vendor's solution to define an organization's needs rather than the other way around. Juniper's definition of access control is the dynamic combination of user identity, endpoint security state and network information with access policy. Combining these factors into one policy allows administrators to define flexible policies that meet their needs and the needs of their organizations.

Standard vs. Proprietary Network Access Control

There are a variety of network access control solutions on the market today. Many of these solutions are proprietary in that the NAC solution's foundation was produced under exclusive legal right or for the benefit of the company that developed it. A proprietary NAC solution may seem attractive and might provide some benefit in the short term but it can prove very costly in the long run. It is best to be wary of specifications that appear to be or call themselves "standards", when in reality that simply describes interoperability with a specific vendor's solutions. At present, there is only one network access control architecture on the market that is based on a defined set of publicly available interoperability guidelines or specifications that have been agreed upon, adopted, or approved either universally or by a large group of interested parties. This network access control architecture also uses existing industry standards as its foundation. The Trusted Network Connect (TNC) architecture from the not-for-profit Trusted Computing Group (TCG) is an open architecture that defines several standard interfaces. These standard interfaces enable components from different vendors to securely operate together, creating endpoint integrity and network access control solutions that interoperate with existing installed equipment and heterogeneous networks. The TNC architecture has been designed to build on established standards and technologies such as 802.1X, RADIUS, IPSec, EAP, and TLS/SSL.

Standards are vital for enterprises that want to avoid being locked into a single vendor for their technology, products or ongoing support. By using standards-based technologies, enterprises can be immune to price increases or other similar actions that may be taken by a single source supplier. Standards also enable technologies to be open and accessible and provide enterprises deploying those solutions a variety of options from which to choose. As an example, by selecting a standards-based network access control solution, enterprises can enjoy a decrease in total cost of ownership (TCO) and acceleration in their Return on Investment (ROI) because they are able to leverage their existing networking infrastructure components and benefit from complete freedom of choice for their network infrastructure and technology in the future. Network access control solutions integrate a number of user, device, and network related security and access control technologies. A network access control solution based on standards eases the integration of these diverse technologies. As the IEEE standard for port-based network access control, 802.1X provides a strong framework for authentication, access control, and data privacy. It is at the top of the list of standards implemented as an integral component of a complete, unified network access control solution.

802.1X and Network Access Control

Network access control requires a secure, strong-yet-flexible framework for authentication, access management, network security and data privacy. The 802.1X standard delivers that and more by enabling the creation of a powerful network perimeter defense via robust admission controls that will not allow users onto the enterprise network unless they are compliant with specified policy. Also, 802.1X provides network access control solutions with a resilient, easily applied and integrated authentication process which assures that the enterprise network is protected against improper access and use. The 802.1X standard completes the authentication of network credentials before a network IP address has been assigned, thus ensuring that viruses and other threats are halted before they can spread into an organization. This is one of the core strengths and benefits of securing an enterprise network with products compatible with the 802.1X standard.

When used in concert with EAP and RADIUS as part of a comprehensive network access control deployment, 802.1X ensures that a network access control solution provides many benefits for an organization, including:

- Interoperability with new or existing network components using established standards, increasing the enterprise's Return-on-Investment (ROI) for the network access control solution by reducing the need for equipment replacement. Interoperability also gives enterprises the opportunity to select best-in-class technologies for their network security and access control.
- Security by disallowing unauthenticated or unauthorized network access before users are even able to reach the network, ensuring confidence in the safety and uninterrupted operation of the network.
- Flexibility to enable operation with and over a variety of network components, protocols and methods, providing solid, assured access control in heterogeneous network environments, independent of network equipment vendor or network environment.
- Simplicity in the deployment and integration of 802.1X standard components into an existing, diverse network environment.

Market and industry analysts have been tracking the intersection of network access control and the 802.1X standard for some time and are just now heralding the benefits that the 802.1X standard brings to network access control solutions. According to a recent Infonetics Research survey, 55% of all enterprises will have deployed some 802.1X technology in their networks by 2007¹. The same Infonetics Research report also states that "NAC...is closely linked to deployment of the 802.1X protocol for authentication".

¹"Enforcing Network Access Control: Market Outlook and Worldwide Forecast", Infonetics Report, Jan 2006

Juniper Networks Unified Access Control (UAC) v2.0

Juniper Networks Unified Access Control (UAC) is a comprehensive solution combining powerful, standards-based user authentication and authorization, identity-based policy control and management, and endpoint security and intelligence to extend access control across the enterprise network.

By incorporating industry standards with well established, market tested network and security products, Juniper Networks UAC solution v2.0 enables organizations to mandate policy compliance prior to granting network access as well as ensure compliance throughout the user session. This approach helps organizations achieve comprehensive, uniform security policy compliance and works effectively to defeat ever-present network threats.

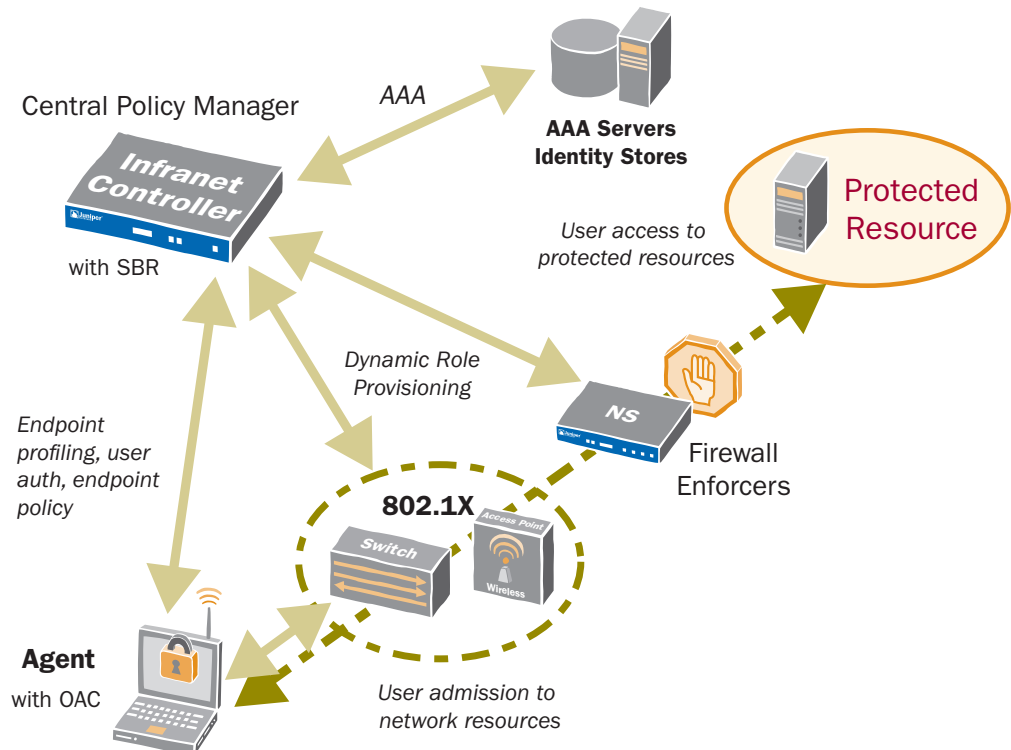


Figure 2 – Juniper's Unified Access Control (UAC) v2.0

UAC v2.0 and 802.1X

Juniper's Unified Access Control (UAC) solution v2.0 features integrated 802.1X (Layer 2) functionality in addition to Layer 3 through Layer 7 access control.

By supporting access control and enforcement through standards-based 802.1X network infrastructure components such as 802.1X-compatible network switches and access points, Juniper delivers a complete, flexible network access control solution. UAC v2.0 enables organizations to maximize their investments in new and existing infrastructure and to minimize network component and design changes, while at the same time improving the overall security of their enterprise network. This is all in addition to the powerful Layer 3 through Layer 7 access control capabilities already available in earlier versions of Juniper's Unified Access Control solution. The UAC v2.0 solution provides a fine grained Layer 2 - 7 solution for the full spectrum of use cases, including guests and contractors that have their own devices as well as mobile employees that need very specific access – all before an IP address is even assigned. Enterprises may choose to deploy UAC v2.0 using existing 802.1X-enabled switches or access points, Juniper

firewalls or both. In addition, the enterprise can add an enforcement method – for example, adding Juniper firewalls to an 802.1X wireless deployment – without having to redeploy key components of UAC v2.0.

In contrast, network access control solutions from other vendors utilizing the 802.1X standard often require deployment of vendor-specific switches, access points and backend systems. This can limit the interoperability, compatibility and cost savings for organizations who implement these NAC solutions.

Juniper Networks UAC v2.0 solution combines identity-based policy and endpoint intelligence to deliver real-time visibility and policy control to enterprises throughout their network. Standards-based, market-leading 802.1X networking components, including the Odyssey® Access Client (OAC) supplicant (802.1X client) and key pieces of the Steel-Belted Radius® (SBR) AAA/RADIUS server are integrated into the UAC v2.0 solution. UAC v2.0 also includes Juniper’s Infranet Controller integrated appliance, dynamically pushed UAC Agent, and optional enforcement points dispersed throughout the network to protect core enterprise assets. (See Figure 3, below.) This provides the enterprise with flexibility when deploying UAC v2.0. Leveraging Juniper Networks open application program interfaces (APIs) and its 802.1X-enabled and open standards-based UAC solution, enterprises can now deploy superior, standards-driven network access control, prevent security threats, ensure regulatory compliance, and provide a secure, interoperable network for their users, increasing organizational and user productivity. And, through the integration of its existing Layer 3 - 7 access control technology, Juniper protects enterprises with even more granular access control and security for all users, independent of role, device, location or access method.

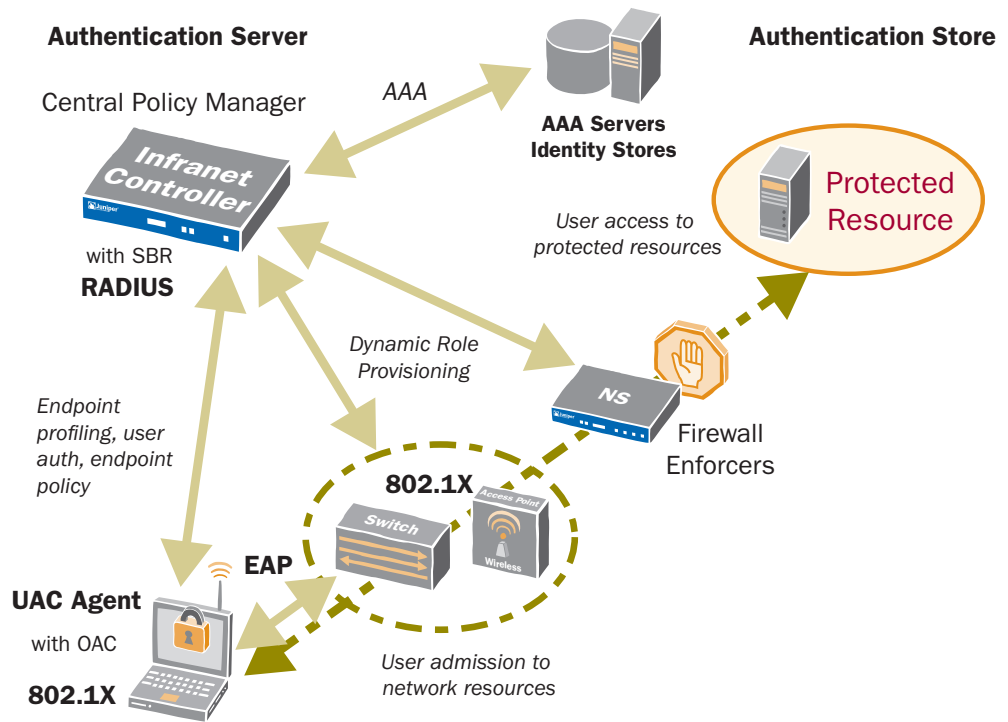


Figure 3 – Juniper’s Unified Access Control (UAC) v2.0 showing 802.1X standards-based components integration

Summary

The 802.1X specification is the standard for port-based network access control and as such, is one of the standards driving and defining today's network access control solutions. Juniper's Unified Access Control v2.0 solution integrates and draws on the 802.1X standard to supplement or substitute for an overlay deployment with firewalls, in order to deliver comprehensive network access control. It also uses the Trusted Network Connect (TNC) open specifications as a foundation, ensuring compatibility with and easy deployment in existing heterogeneous network environments. The incorporation of the 802.1X standard in UAC enables enterprises to select best-in-class network appliances and components and provides support for vendor-neutral interoperability, avoiding potentially expensive, restrictive vendor lock-in.

About Juniper Networks

Juniper Networks develops purpose-built, high-performance IP platforms that enable customers to support a wide variety of services and applications at scale. Service providers, enterprises, governments and research and education institutions rely on Juniper to deliver a portfolio of proven networking, security and application acceleration solutions that solve highly complex, fast-changing problems in the world's most demanding networks. Additional information can be found at www.juniper.net.