WHITE PAPER

TEXAS INSTRUMENTS

Workhorse 802.1x standard authenticates network connections

Sébastien Brun
Voice Applications Support team, Communications Infrastructure and Voice group

Introduction

As the number of devices connecting to IP networks continues to grow, authentication serves as virtual law enforcement, protecting us from hackers seeking to gain illicit access to these networks.

The police chief of this virtual force is the 802.1x standard, which even after seven years continues to be a valuable and effective gatekeeper for physical network connections. With devices such as IP phones connecting to local area networks (LANs) at an increasing rate, it's time to revisit this security workhorse. Although it has some limitations, its success lies in its simplicity.

Foiling attempts to plug an unauthorized device directly into a local area network (LAN) has been the purview of the IEEE's 802.1x standard since it was introduced in 2001. Without the protection of 802.1x, hackers and other security risks might be able to wreak havoc not only on the LAN itself but also on wider Internet Protocol (IP) networks. Of course, this becomes increasingly critical as more and more devices such as IP phones connect to LANs and access the Internet through applications like Voice over IP (VoIP).

Plug-in authentication

The main tenet behind 802.1x is that any device plugged into a network must be authenticated before any regular data traffic occurs. As soon as the network cable from a device like a laptop computer or an IP phone is physically plugged into a network, or as soon as a device attempts to gain access to a wireless Wi-Fi network, 802.1x must determine the identity of the device and whether it is authorized to access that network. 802.1x is limited to authenticating physical connections at the data link level (Level 2 of the OSI model). Built on the Extensible Authentication Protocol (EAP), 802.1x offers no security for any of the data communications once it has authorized the connection.

Three entities come into play in every 802.1x authentication process. The standard calls any device that plugs into a network a supplicant because it must first seek and be granted authorization to access the network. The entity responsible for the 802.1x authentication process is called the authenticator. In many cases, this is an Ethernet switch on the LAN. The process is carried forward by an authenticating server, which determines whether the supplicant's traffic over the network can be authorized.

How it works

Typically, traffic of any unoccupied access point to a network, such as a port on a wired or wireless Ethernet switch, is blocked until the 802.1x authentication process is complete. The blocked traffic includes all configuration mechanisms like Dynamic Host Configuration Protocol (DHCP), as well as any other traffic like HTTP data. When a device plugs into a network and it is detected, the port on the switch is set as "unauthorized" and only 802.1x traffic is allowed.

As a first step in the 802.1x process, the authenticator requests the identity of the supplicant. When the supplicant responds with a packet containing its identity, the authenticator forwards

this information to the authenticating server, where the request for authentication and authorization for access to the network is either accepted or rejected. The authenticating server applies its authentication rules to make this determination.

When a request for authentication is accepted by the authenticating server, the authenticator sets the access port to "authorized" and normal network traffic can begin. Should the supplicant log off or simply unplug its network cable from the network, the authenticator is notified and the status of the port is returned to an unauthorized state, where only 802.1x traffic is allowed until another 802.1x authorization process has been completed.

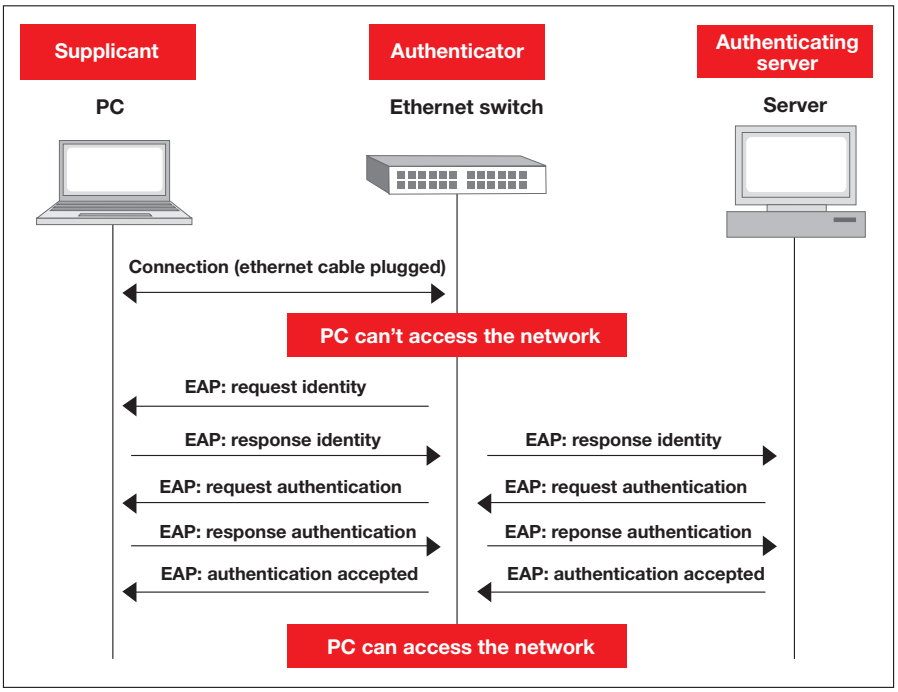

Figure 1

The messages that comprise the authorization process conform to EAP, which was developed by the Internet Engineering Task Force (IETF) in 1998 as RFC2284 and updated in 2004 as RFC3748. The messages between the supplicant device and the authenticator are carried in a certain EAP packet format known as EAP over LAN (EAPoL). The messages between the authenticator and the authenticating server are in a format understood by the authenticating server. For example, these messages are often encapsulated into EAP over Radius (EAPoR) packets if the authenticating server happens to be a Radius server, a popular type of 802.1x authenticating server.

Generally, the supplicant software for initiating 802.1x authentication is embedded in the operating system (OS) on practically all PCs. For example, 802.1x supplicant software is contained in the most popular OSs, including Windows XP, Windows Vista, Windows 2000 (Service Pack 3) and Linux. If this software is not included in the version of Linux present on the device, it can be added (wpa_supplicant). Other types of Ethernet devices also include 802.1x supplicant software, and practically all Ethernet switches have authenticator software.

Some limitations

The security offered by 802.1x is limited to some degree. For example, there is a gap in 802.1x protection if an Ethernet hub is inserted between an authenticated supplicant and the network. When this occurs, other devices connected to the hub can access the network. Ethernet switch suppliers have taken steps to fill this gap in the standard by blocking traffic on a port if the media access control (MAC) address of the supplicant changes. It is worthwhile noting that 802.1x is under revision to facilitate secure communication over publicly accessible LANs/MANs, as well as to allow its use in additional applications.

The 802.1x standard was never truly intended to offer security beyond authenticating and authorizing physical connections to a network. As a result, once a device has been authenticated and communication commences, 802.1x does not offer security on any of the ensuing data traffic. It is imperative that the security supported by 802.1x be supplemented by other measures such as the IP Security (IPSec) standard for authenticating and/or encrypting packets. 802.1AE (Media Access Control Security) together with 802.1af (Authenticated Key Agreement for MACSec) can also be used for data encapsulation, encryption and authenticity with key management.

Authenticating IP phones

An IP phone is essentially an Ethernet device with all of the capabilities needed for VoIP, as well as other functionality. Some IP phones have been enhanced significantly with processing power and other resources for additional applications above and beyond voice. Most IP phones plug directly into the LAN, but they include another LAN port – to which another device may be daisy-chained. IP phone manufacturers reason that most offices have only one Ethernet plug in the wall. The IP phone can be plugged directly into the office's LAN through this plug and then the user's PC can access the LAN through the IP phone's second network port.

Most IP phones feature an internal Ethernet switching device to support two connections to the LAN. Within the context of 802.1x, both the IP phone and the PC must be authenticated before they are able to send regular traffic over the LAN. This means that they both must have 802.1x supplicant capabilities and the internal Ethernet switch of the IP phone has to be able to pass 802.1x traffic to the PC.

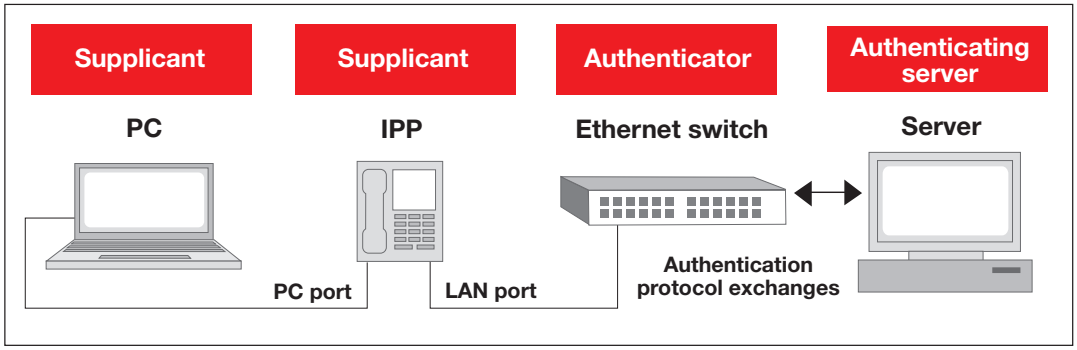

Figure 2

In some cases, to enable the authentication of a PC or any other device connected to the IP phone's LAN port, the Ethernet switch in the IP phone must be configured to allow the forwarding of reserved multicast packets.

At the very least, the IP phone itself must support 802.1x supplicant software. The two most dominant embedded OSs in IP phones include supplicant capabilities for both the IP phone and devices plugged into the phone's second Ethernet port. In its Platform for Customer Device (PCD) 3.2, VxWorks from WindRiver includes 802.1x LAN supplicant software, which performs 802.1x authentication for both the IP phone and any network devices connected to its LAN port. Under Linux, a supplicant module (wpa_supplicant, GPLv2/BSD license) can be added to the IP phone's OS; this module will handle the 802.1x authentication process for the IP phone and will relay the 802.1x packets to the network device plugged into the second network port. This will allow the network device to be 802.1x authenticated.

The workhorse

The flashy story that catches the headlines in regards to 802.1x focuses on the spec as a gateway to next-generation multimedia applications. In fact, the 802.1x standard's greatest and often overlooked value is in authenticating and authorizing physical connections to a network. As a growing number of devices that consumers and businesses depend on access the Internet through advanced applications like VoIP, security remains an essential component of effective communication.

Since its introduction, the IEEE's 802.1x standard has provided advanced protection against prospective hackers as any device that is plugged into a network must be authenticated before any regular data traffic occurs. Protecting both the LAN and the wider IP network, 802.1x is the always-working gatekeeper protecting users' network connections.

IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, modifications, enhancements, improvements, and other changes to its products and services at any time and to discontinue any product or service without notice. Customers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All products are sold subject to TI's terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its hardware products to the specifications applicable at the time of sale in accordance with TI's standard warranty. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by government requirements, testing of all parameters of each product is not necessarily performed.

TI assumes no liability for applications assistance or customer product design. Customers are responsible for their products and applications using TI components. To minimize the risks associated with customer products and applications, customers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any TI patent right, copyright, mask work right, or other TI intellectual property right relating to any combination, machine, or process in which TI products or services are used. Information published by TI regarding third-party products or services does not constitute a license from TI to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of TI information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. Reproduction of this information with alteration is an unfair and deceptive business practice. TI is not responsible or liable for such altered documentation. Information of third parties may be subject to additional restrictions.

Resale of TI products or services with statements different from or beyond the parameters stated by TI for that product or service voids all express and any implied warranties for the associated TI product or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

TI products are not authorized for use in safety-critical applications (such as life support) where a failure of the TI product would reasonably be expected to cause severe personal injury or death, unless officers of the parties have executed an agreement specifically governing such use. Buyers represent that they have all necessary expertise in the safety and regulatory ramifications of their applications, and acknowledge and agree that they are solely responsible for all legal, regulatory and safety-related requirements concerning their products and any use of TI products in such safety-critical applications, notwithstanding any applications-related information or support that may be provided by TI. Further, Buyers must fully indemnify TI and its representatives against any damages arising out of the use of TI products in such safety-critical applications.

TI products are neither designed nor intended for use in military/aerospace applications or environments unless the TI products are specifically designated by TI as military-grade or "enhanced plastic." Only products designated by TI as military-grade meet military specifications. Buyers acknowledge and agree that any such use of TI products which TI has not designated as military-grade is solely at the Buyer's risk, and that they are solely responsible for compliance with all legal and regulatory requirements in connection with such use.

TI products are neither designed nor intended for use in automotive applications or environments unless the specific TI products are designated by TI as compliant with ISO/TS 16949 requirements. Buyers acknowledge and agree that, if they use any non-designated products in automotive applications, TI will not be responsible for any failure to meet such requirements.

Following are URLs where you can obtain information on other Texas Instruments products and application solutions:

Products		**Applications**	
Amplifiers	amplifier.ti.com	Audio	www.ti.com/audio
Data Converters	dataconverter.ti.com	Automotive	www.ti.com/automotive
DSP	dsp.ti.com	Broadband	www.ti.com/broadband
Clocks and Timers	www.ti.com/clocks	Digital Control	www.ti.com/digitalcontrol
Interface	interface.ti.com	Medical	www.ti.com/medical
Logic	logic.ti.com	Military	www.ti.com/military
Power Mgmt	power.ti.com	Optical Networking	www.ti.com/opticalnetwork
Microcontrollers	microcontroller.ti.com	Security	www.ti.com/security
RFID	www.ti-rfid.com	Telephony	www.ti.com/telephony
RF/IF and ZigBee® Solutions	www.ti.com/lprf	Video & Imaging	www.ti.com/video
		Wireless	www.ti.com/wireless

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265