802.1x White Paper

Executive Summary

Security and flexibility are often seen as mutually exclusive requirements in a network, yet both are equally important. Security is crucial on any network. Flexibility, in particular the ability to roam, is increasingly fundamental.

Therefore, Ethernet networks need a device authentication method that is highly secure but not tied to a port's physical location. In addition, the appropriate network access for users needs to be determined from their authentication credentials.

802.1x user authentication solves these multiple requirements. What is more, it is relatively uncomplicated and has very little impact on network performance.

It is also a protocol that is medium-independent – equally effective on wireless and wired connections.

802.1x user authentication is rapidly becoming an expected component of any Ethernet infrastructure.

This white paper includes the following sections:

Contents

A. What Does 802.1x Do?

The IEEE 802.1x standard manages port-based network access. It authenticates devices attached to a LAN port by initiating a connection and requesting login details. Access is prevented if authentication fails.

As well as being valuable for authenticating and controlling user traffic to a protected network, 802.1x is effective for dynamically varying encryption keys. 802.1x attaches the Extensible Authentication Protocol (EAP) to both wired and wireless LAN media, and supports multiple authentication methods, such as token cards, one-time passwords, certificates, and public key authentication.

Why Was 802.1x Developed?

802.1x was designed to accommodate the following requirements:

Network Control Right at the Port Level

The best place to control network access is where the user attaches - at the port. It is also logical to apply packet and protocol filtering at the port. By controlling a user's network attachment point, the network environment can be customized to meet that user's needs and access agreements.

Authentication, Authorization and Accounting

If an organization already uses Authentication, Authorization, and Accounting (AAA) technology to control users' network access, (either through a firewall or dial-in remote access), 802.1x can use these AAA servers to provide AAA functions to new 802.1x clients.

Public Network Security

Network owners that extend their networks into public arenas (for example, universities) must control user access. Before the advent of 802.1x, a user could plug into a live 802 port and gain full access to a network. This problem became even greater as the use of wireless LANs grew, because any user within physical range of a wireless access point could attempt to access the network.

Distribution of Dynamic Encryption Keys

Wired Equivalent Privacy (WEP) was designed to provide the security level equivalent to that of a wired network. WEP uses symmetric encryption keys to provide security between wireless devices, but this is limited by the complications of allocating and managing the encryption keys. 802.1x counters this by providing a method for the allocation of WEP keys to access points.

The Main Elements of the 802.1x System

Supplicant

The supplicant is the client that wishes to access services offered by the authenticator's system. The supplicant is responsible for answering any requests from the authenticator for information that establishes the supplicant's identity.

Port

A port is where a device is attached to the LAN, either directly into the switch or a wireless access point.

Authenticator

The authenticator challenges the supplicant for appropriate authentication before it allows access to the services available via the port. The authenticator communicates with the supplicant and submits the information received from the supplicant to a suitable authentication server. This allows the verification of user credentials to determine the consequent port authorization state. The authenticator's functionality is independent of the authentication method. It acts as a go-between for the supplicant and authentication server.

Extensible Authentication Protocol

802.1X uses Extensible Authentication Protocol (EAP) as an authentication tool. EAP carries out the authentication exchange between the supplicant and the authentication server. No other devices such as access points and proxy servers take part in this exchange.

Extensible Authentication Protocol Over LAN

The Extensible Authentication Protocol Over LAN (EAPOL) captures the EAP messages so they can be managed directly by a LAN MAC service. Management functions such as start, logoff, and key distribution are also provided by EAPOL.

Remote Access Dial In User Service

The Remote Authentication Dial In User Service (RADIUS) server:

- Manages a database of users.
- Provides authentication by verifying username and password.
- Optionally, provides authorization such as dynamic VLAN assignment.
- Optionally, provides accounting information about how long a user was connected, and how much data they transferred.

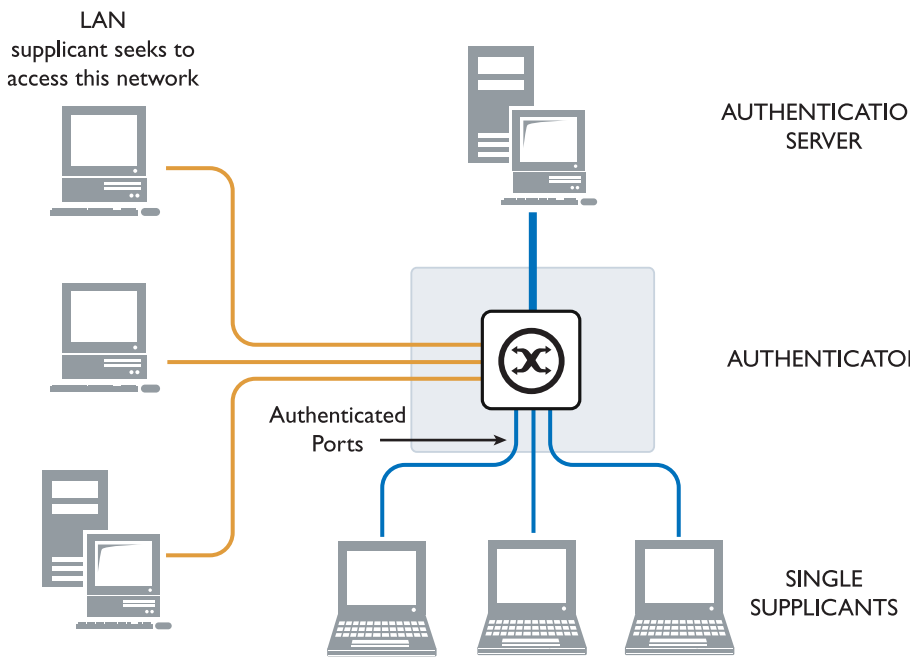

Figure 1: The 802.1x System

B. An Overview of the 802.1x Standard

To appreciate 802.1x, we need to begin with its authentication method: EAP.

EAP

Because most enterprises want more access security than just the employment of usernames and passwords, EAP was designed. EAP sits inside the PPP authentication protocol, and provides a general structure for several different authentication methods. Designed to prevent several proprietary mechanisms from evolving for the transfer of different authentication types, EAP enables the smooth operation of everything from passwords to challenge-response tokens to digital certificates.

IEEE 802.1x

The IEEE 802.1x standard is simply a standard for passing EAP over a wired or wireless LAN, without PPP. With 802.1x, EAP messages are packaged in Ethernet frames and don't use PPP. This is beneficial when the rest of PPP isn't needed, where protocols other than TCP/IP are used, or where the overhead and complexity of using PPP is undesirable. 802.1X is especially well suited for wireless LAN applications as it requires very little processing power on the part of the Authenticator. In wireless LAN applications, the Authenticator is the Wireless Access Point (WAP).

The Authentication Process

Devices make use of EAP packets for the port authentication process. Until authentication is successful, the supplicant can only access the authenticator to perform authentication message exchanges. Initial 802.1x control begins with an unauthenticated supplicant and an authenticator. A port under 802.1x control, acting as an authenticator, is in an unauthorised state until authentication is successful. The following steps outline the authentication and authorization process:

1. Either the authenticator or the supplicant initiates an authentication message exchange. The authenticator initiates the authentication message exchange by sending an EAP-Request/Identity packet. The supplicant initiates an authentication message exchange by sending an EAPOL-Start packet, to which the authenticator responds by sending an EAP-Request/Identity packet.

2. The supplicant sends an EAP-Response/Identity packet to the authentication server via the authenticator, confirming its identity.

3. The authentication server chooses an authentication algorithm to verify the supplicant's identity, for example, EAP-MD5 (Message Digest 5) or EAP-OTP (OneTime Password). It then sends a corresponding EAP-Request packet to the supplicant via the authenticator.

4. The supplicant provides its authentication credentials to the authentication server via an appropriate EAP-Response message.

5. The authentication server either sends an EAP-Success packet or EAP-Failure packet to the supplicant via the authenticator.

6. Upon successful authorisation of the supplicant by the authentication server, a port under 802.1x control is in an authorised state, and the supplicant is allowed full access to services offered via the controlled port.

7. When the supplicant sends an EAPOL-Logoff message to the authenticator the port under 802.1x control is set to unauthorised.

A successful authentication message exchange, initiated and terminated by a supplicant using the EAP-OTP mechanism is shown in Figure 2.

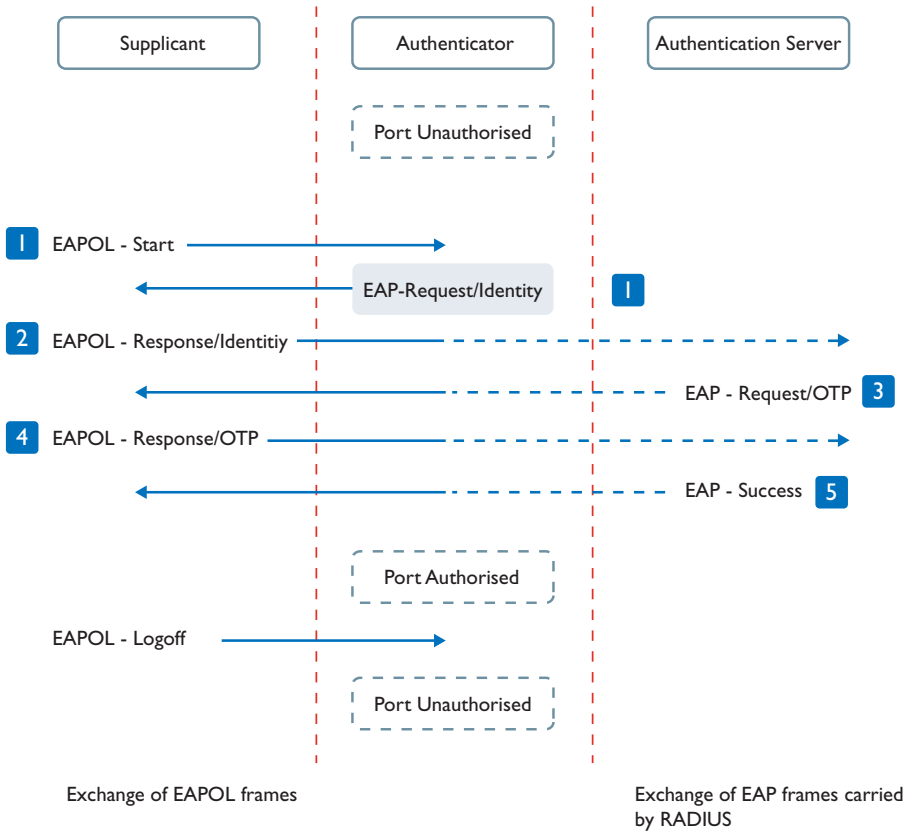

Figure 2. The authentication process

EAP Types

Various types of EAP have been designed to support authenticators and their related network security policies. The most widely used EAP types are:

	Server Authentication	Supplication Authentication	Dynamic Key Delivery	Security Risks
EAP-MD5	None	Password Hash	No	Man-in-the-middle (MitM) attack, Session hijacking
LEAP	Password Hash	Password Hash	Yes	Identity exposed, Dictionary attack.
EAP-TLS	Public Key (Certificate)	Public Key (Certificate or SMART Card)	Yes	Identity exposed
EAP-TTLS	Public Key (Certificate)	CHAP, PAP, MS-CHAP (v2), EAP	Yes	MitM attack
PEAP	Public Key (Certificate)	Any EAP such as EAP-MS-CHAPv2 or Public Key	Yes	MitM attack; identity hidden in phase 2 but potential exposure in Phase 1

The following sections describe each type:

EAP-MD5 (Message Digest)

EAP-MD5 is an EAP security algorithm that provides base-level EAP support. EAP-MD5 uses a 128-bit message (the hashed value of a server challenge and the user's password) to verify the authenticity of the supplicant. Suitable for trusted Ethernets where there is a low security risk, EAP-MD5 is not recommended for public Ethernets or wireless LANs because it provides only one-way authentication. Without mutual authentication outsiders can easily sniff station identities and password hashes, or masquerade as access points to trick stations into authenticating them.

EAP-OTP

EAP-OTP is similar to EAP-MD5, except it uses the One-Time Password (OTP) as the response. The request contains a displayable message. The OTP mechanism is employed extensively in VPN and PPP scenarios but not in the wireless world. The OTP method is defined in RFC 2289.

Lightweight EAP (LEAP)

LEAP supports mutual authentication and uses dynamically generated WEP keys to encrypt data transmissions. Mutual authentication reduces the risk of access point masquerading — a type of Man-in-the-Middle (MitM) attack. However, station identities and passwords remain vulnerable to attackers armed with sniffers and dictionary attack tools. LEAP is mostly attractive to organizations that want to modestly raise the security bar.

EAP with Transport Layer Security (EAP-TLS)

EAP-TLS is based on Secure Sockets Layer (SSL), which is used for authentication of the majority of today's secure web transactions. EAP-TLS requires certificate-based and mutual authentication of the client and the network. Both the station and the RADIUS server have to prove their identities via public key cryptography in the form of digital certificates or smart cards. If applied to wireless solutions, user-based and session-based WEP keys can also be dynamically generated to secure future communication between the WLAN client and the access point. An encrypted TLS tunnel, making EAP-TLS very resistant to dictionary or other MitM attacks, secures this exchange. EAP-TLS does have its drawbacks - outsiders can still sniff the station's identity (the name assigned to the certificate). Also, certificates must be managed on both the client and server side. EAP-TLS is most attractive to large enterprises that use only Windows XP/2000/2003 with deployed certificates.

EAP with Tunneled TLS (EAP-TTLS) and Protected EAP (PEAP)

EAP-TTLS and PEAP were both designed to simplify 802.1X application, and use similar means of authentication.

EAP-TTLS uses the certificate-based, mutual authentication of the client and network through an encrypted tunnel and dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.

Like the EAP-TTLS, PEAP authenticates wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN. EAP-TTLS and PEAP are just as safe from sniffing attacks as EAP-TLS.

Advanced Features

Allocating VLAN Membership

In a network environment that contains multiple VLANs, it can be beneficial to assign roaming users to the same VLAN no matter where they connect to the network. This means that network can control which VLAN the user is placed on, restricting access to resources and services according to the user's profile, irrespective of the physical point at which they connect to the network.

When users move from one part of the office to another, or require the same access in meeting rooms as they have at their desk, they require either complete access to the network, or restricted access based on the needs of their job. If different configuration capabilities need to be provided to staff, contractors and guests, it will to have to be the latter. Fortunately, the following 802.1x extensions provided by some vendors, including Allied Telesis, offer a solution to this.

Guest VLAN

When visitors are offered an Internet connection so they can reach their own company network, unlimited access to the host network must be prevented. With the Guest VLAN feature, if a user tries to connect but doesn't have an 802.1x client, they are migrated to a Guest VLAN that is set up with limited services (Internet access only, for example).

A failed authentication attempt prevents the user from accessing any VLAN, including the Guest VLAN.

Access Control

The Access Control feature allows you to create access lists (by setting filters) dynamically on a port depending on who has logged in, access lists can be applied over and above VLAN membership. This allows the network to be partitioned into zones where similar users are given similar access. For instance, rate limiting could be applied on the Guest VLAN ports, so that visitors cannot monopolise the host's Internet connection.

C. How do Allied Telesis Products Support 802.1X?

A range of Allied Telesis switches support the 802.1X functionality described in this paper. Our advanced Layer 3+ switches reach new and unmatched heights in performance, flexibility, and reliability.

The following switches incorporate 802.1x features:

X900 Series:

AT-9924Ts
24 x 10/100/1000BASE-T (RJ-45) copper ports
2 x 20 Gigabit expansion bays

AT-9924T
24 x 10/100/1000BASE-T copper ports and
4 x 1000BASE-X SFP combo ports

AT-9924T/4SP
24 x 10/100/1000BASE-T copper ports
4 x 1000BASE-X SFP combo ports
High performance IPv6

AT-9924SP
24 x 1000BASE-X SFP ports

AT-8948
4 x 1000BASE-X SFP uplinks
48 x 10/100BASE-T copper ports

SwitchBlade Series:

AT-SB4004
4 line card capacity
Up to 96 Gb ports

AT-SB4008
8 line card capacity
Up to 192 Gb ports

AT-9800 Series:

AT-9816GB V2
16 x 1000BASE-X GBIC ports

AT-9812T V2
12 x 10/100/1000BASE-T copper ports
4 x 1000BASE-X GBIC ports

AT-8800 Series:

AT-8824
24 port 10/100 TX Fast Ethernet
2 GBIC slots
Single PSU (Redundant PSU (RPS) is an optional extra)
PAC connection

AT-8848
48 port 10/100 TX Fast Ethernet
2 GBIC slots
Single PSU (Redundant PSU (RPS) is an optional extra)
PAC connection

Rapier 'i Series:

Rapier 16fi
16 port 100FX (SC or MT-RJ) Fast Ethernet Layer 3 switch with 2 uplink bays and WAN access bay

Rapier 24i
24 port 10/100TX Fast Ethernet Layer 3 switch with 2 uplink bays and WAN access bay

Rapier 48i
48 port 10/100TX Fast Ethernet Layer 3 switch with 2 uplink bays

AT- 8700XL Series:

AT-8724XL
24 x 10/100 Layer 2 - Layer 4 with essential
Layer 3 functionality and 2 Uplink Bays

AT-8748XL
48 x 10/100 Layer 2 - Layer 4 with essential
Layer 3 functionality and 2 Uplink Bays

AT-8600 Series:

AT-8624T/2M
24 x 10/100BASE-T + 2 x Uplink Module Bays
Layer 3 switch with Layer 2/3/4+ intelligence

AT-8648T/2SP
48 x 10/100BASE-T Switch
2 x combo ports and
2 x 10/100/1000T uplink ports (RJ-45)*

AT-8624POE
24 x 10/100BASE-T with PoE + 2 x Uplink Module Bays

The following routers incorporate 802.1x features:

AT-AR770S
2 x WAN combo ports (100/1000 SFP or 10/100/1000TX)
4 x LAN 10/100/1000TX ports
2 x PIC
1 x Asynchronous console / Modem port

AT-AR750S
2 x WAN 10/100BASE-T ports
5 x LAN 10/100BASE-T ports
2 x PICs
1 x Asynchronous console / Modem port

AT-AR450S
1 x 10/100B-TX WAN port
1 x 10/100B-TX DMZ port/second WAN port
5 x 10/100B-TX LAN ports
2 x asynchronous RS232 ports

AT-AR440
1 x ADSL port
5 x 10/100BASE-T ports
1 x PIC
1 x Asynchronous port

For more information about our products, contact your local Allied Telesis representative or visit our website: www.alliedtelesis.com

** The RJ-45 ports use the same physical interface as the SFP ports. When an SFP is inserted into an SFP port, the corresponding RJ-45 port is disabled.*

USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com

Connecting The IP World

Allied Telesis