

X-Calibur

for VxWorks

802.1X Port Security

X-Calibur is a standards-based, small-footprint implementation of the Port-based Network Access Control (IEEE 802.1X PNAC) protocol for VxWorks®. It adds access authentication services to a supplicant or an authenticator in any scenario where one can abstract out the notion of a “network access port”, which makes it an excellent fit for authenticated Ethernet networks and wireless (WLAN) networks. It also provides a well-structured API to communicate with an authentication server on any platform, based on Extensible Authentication Protocol (EAP). **X-Calibur**'s robustness and lean implementation, and highly configurable design make it an ideal fit for resource-limited embedded environments.

LAN Access Authorization

While the concept of access authorization to a network is important

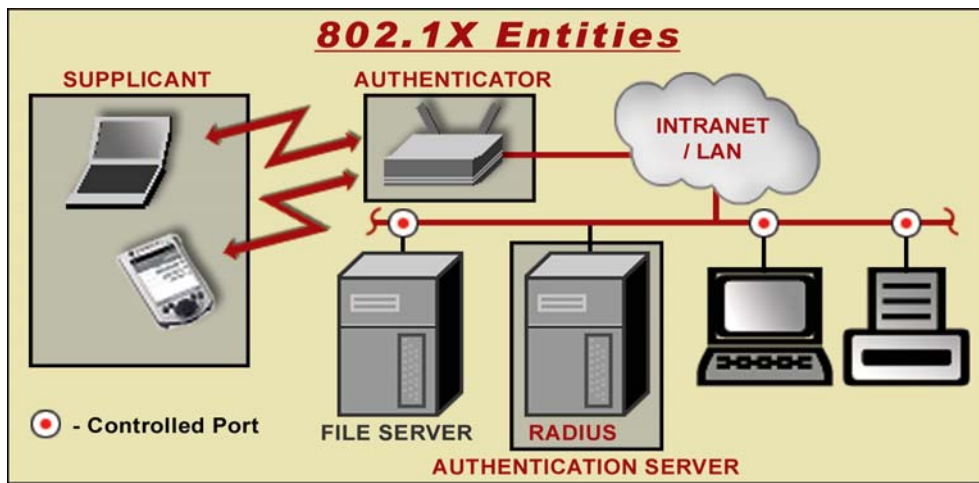
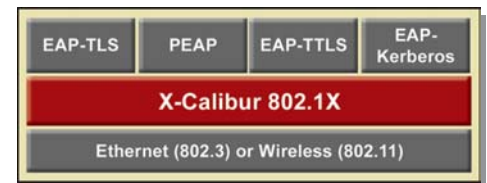
for wired networks such as Ethernet LANs, it is even more significant in wireless local networks. These networks present a unique set of issues, because the only restriction to access them is radio signal strength. There is no wiring to define membership in a network, and no physical method to restrict a system in radio range from becoming part of a wireless network. **X-Calibur**'s PNAC implementation, based on the IEEE 802.1X standard, authenticates devices and users connected to a LAN on a per-port basis, so that access is restricted to authorized entities.

IEEE 802.1X

X-Calibur's 802.1X framework is based on the IETF Extensible Authentication Protocol over LAN (EAPoL) messages. 802.1X defines an authentication dialog between the system needing network services and the network. This involves

Features

- ❖ Supplicant and Authenticator PAE.
- ❖ Implements IEEE 802.1X PNAC.
- ❖ Provides APIs for any EAP implementation.
- ❖ Works with wired (Ethernet) and wireless (WLAN/802.11) networks.
- ❖ 802.1X MIB Support.
- ❖ Support for CPU types of either endian-ness including PowerPC, MIPS, X86, ARM/XScale.
- ❖ Royalty-free, full-source distribution.



VxWorks Edition Features

- ❖ Designed Exclusively for VxWorks and VxWorks-based Platforms
- ❖ Native support for VxWorks 5.4.x, 5.5.x, and AE
- ❖ Easy integration with BSPs
- ❖ Enhanced memory management and partition support
- ❖ Integrated with Tornado build and install methodology
- ❖ Requires no special OS or networking source
- ❖ Works with existing 802.11 and Ethernet drivers

establishing identity in order to gain authorized access by binding a name to something known, such as a MAC address, and then using that name in all future interactions. 802.1X requires entities to play three roles in the authentication process: the device seeking network access i.e. the client to be authenticated (“Supplicant”), the server performing the authentication (“Authentication Server” or “AS”), and the device responsible for granting access based on authorization from the AS (“Authenticator”). The Supplicant and Authenticator coordinate with each other by using controlling logic called the Port Access Entity (PAE).

X-Calibur implements the 802.1X PAEs for Supplicants and Authenticators, allowing seamless integration of this functionality in embedded devices, and enabling communications to any standard AS in multi-platform networks. **X-Calibur** defines two logical ports of access between the Supplicant and the Authenticator: controlled and

uncontrolled. A controlled port only accepts packets from authenticated nodes, whereas an uncontrolled port accepts all packets. When in an unauthorized state, the Authenticator PAE filters out all traffic from the Supplicant to controlled ports. The Authenticator PAE communicates with the Supplicant PAE via EAPoL protocol data units (PDUs) allowed to go through the uncontrolled port in order for the authentication process to complete. Once authentication is successful, the controlled port is enabled and the Supplicant is granted access.

Extensible Authentication

While 802.1X provides for an interoperable authentication PDU transport, it does not dictate or provide the authentication mechanism. **X-Calibur** allows the use of a number of EAPoL based authentication protocols such as passwords, EAP-TLS (EAP over Transport Layer Security), EAP-TTLS (EAP over Tunneled TLS), EAP-Kerberos, PEAP (Protected EAP), one-time passwords, etc. These protocols can be deployed over **X-Calibur** using built-in APIs that allow the Supplicant or Authenticator to easily implement EAPoL interfaces to standard servers (e.g. RADIUS Authentication Servers) for packaging EAP messages in link-layer frames.

802.11 Companion

The WPA industry standard and the upcoming 802.11i standards specify the use of 802.1X for station authentication. In WLAN infrastructure mode, **X-Calibur** can provide the Supplicant PAE functionality for stations as well as an Authenticator PAE implementation for access points. Authentication is typically achieved by identifying a station by its MAC address, and determining its level of authorization in the AS. **X-Calibur** APIs can be used to act as an EAP proxy between the Supplicant and AS, and pass-through EAPoL frames which a RADIUS server will interpret as EAP message attributes. The AS then provides the authentication state of the supplicant to the authenticator via the secure RADIUS channel between the two, and also provides for dynamic re-keying transparent to the end-user. Other EAP mechanism implementations are also possible using the same APIs.

Flexible Framework

The **X-Calibur** framework contains APIs and abstractions to integrate the client or the server of any EAP based authentication protocol to the Supplicant or Authenticator module respectively. It also includes flexible hooks to configure the operational parameters of the

Also Available

- ❖ **Merlink**
Link Aggregation, Fail-over, Load-Balancing, LACP, 802.3ad
- ❖ **Spantasmic**
STP, RSTP, and MST (802.1d, w, s)
- ❖ **AuthAgent Kerberos**
Embedded Kerberos Agent
- ❖ **SSLimSecure**
Secure Sockets and TLS

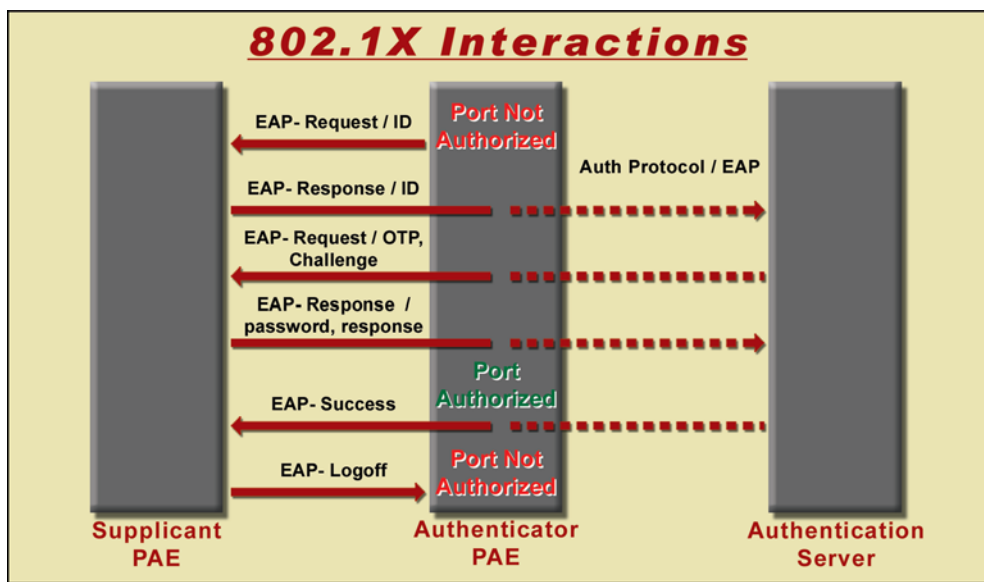
Custom Solutions

TeamF1's professional services can provide the resources and expertise to build customized implementations of **X-Calibur** including support for custom and standard EAP authentication, integration with custom applications and implementation of extended features.

Supplicant and Authenticator. Management capabilities include the ability to maintain and retrieve the Authenticator statistics through a MIB interface, and to override the protocol by statically configuring the access control of an authenticator port. **X-Calibur's** 802.1X implementation also supports the ability to transmit key information from the Authenticator to/from the Supplicant once authentication is successful, if the server supports it. Reference implementations for various EAP types is included.

Built for VxWorks

The **VxWorks** edition of **X-Calibur** is a drop-in component for **VxWorks 5.x** and **AE**. It has been extensively validated on a variety of CPU architectures, which minimizes development and integration efforts. **X-Calibur** is especially optimized for **VxWorks** with support for memory partitions, native OS services, and Tornado IDE component integration. It is well integrated with the **VxWorks** build & install methodology and enables secure authentication for network access applications with the fewest changes required for integration.



Email: sales@TeamF1.com
 Web: www.TeamF1.com
 Ph: 510-505-9931 ext. 5
 Fax: (510) 505-9941



© 2002-2004 TeamF1, Inc.