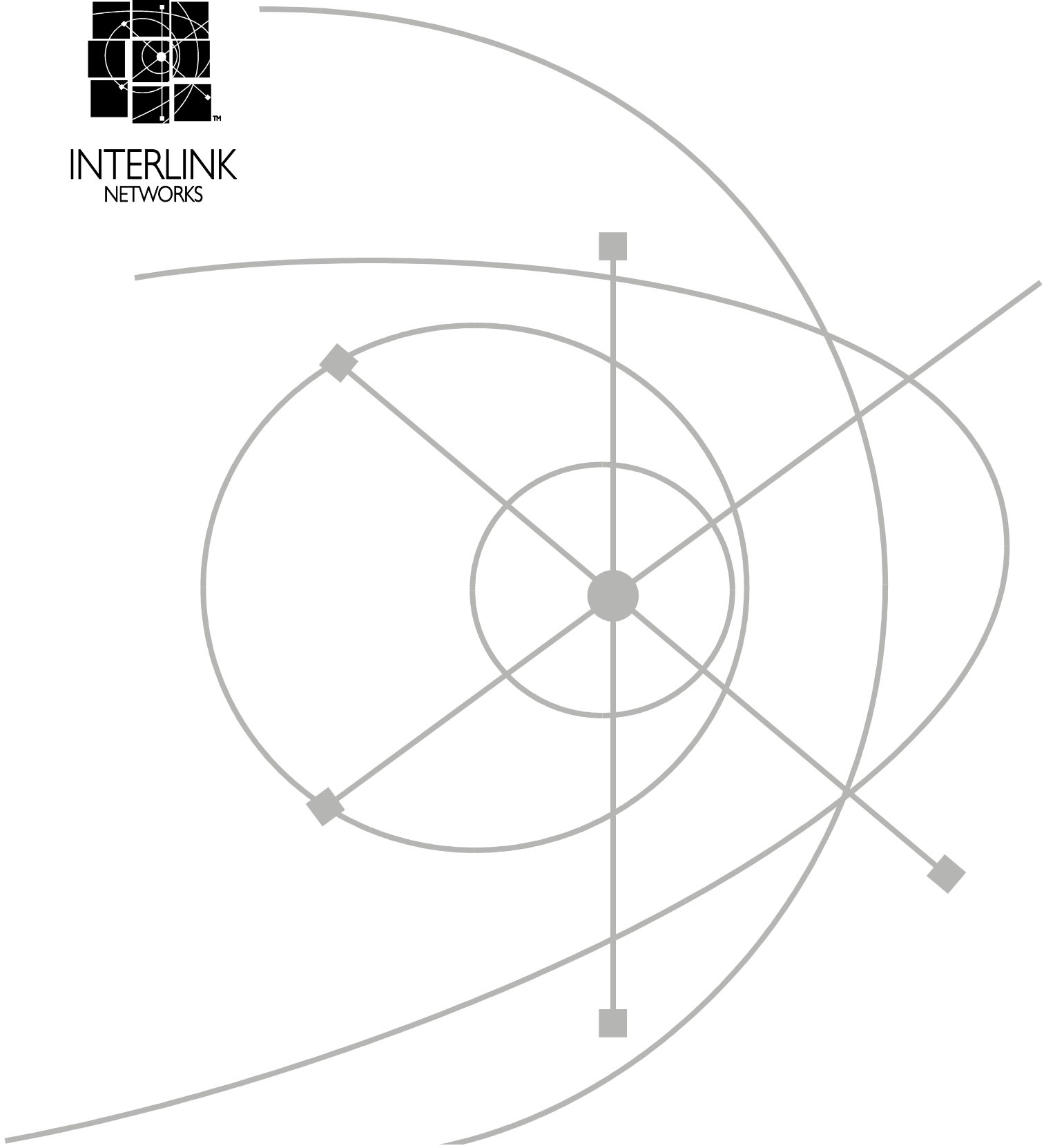


INTERLINK  
NETWORKS



© 2002 Interlink Networks, Inc.

Revision

**All Rights Reserved.**

This document is copyrighted by Interlink Networks Incorporated (Interlink Networks). The information contained within this document is subject to change without notice. Interlink Networks does not guarantee the accuracy of the information.

**Trademark Information**

Brand or product names may be registered trademarks of their respective owners.

**Interlink Networks, Inc.**

775 Technology Drive, Suite 200

Ann Arbor, MI 48108 USA

Phone: 734-821-1200

Sales: 734-821-1228

Fax: 734-821-1235

[info@interlinknetworks.com](mailto:info@interlinknetworks.com)

[sales@interlinknetworks.com](mailto:sales@interlinknetworks.com)

[www.interlinknetworks.com](http://www.interlinknetworks.com)

# Introduction to 802.1X for Wireless Local Area Networks

## INTRODUCTION

Many new 802.11 wireless LAN access points are advertised as employing IEEE 802.1X for enhanced security. Trade articles about this new technology call it a “security protocol,” a “security feature,” a “security standard,” an “authentication method,” or a “user authentication protocol” and promise “enhanced security” and a “more secure environment.” These claims do not always provide an accurate picture of how 802.1X fits into wireless LAN security. Despite all the hype, 802.1X, if utilized properly, can indeed provide a network with a higher level of security.

## 802.1X OVERVIEW

The IEEE 802.1X standard, *Port Based Network Access Control*, defines a mechanism for port-based network access control that makes use of the physical access characteristics of IEEE 802 LAN infrastructure. It provides a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics. It also prevents access to that port in cases in which the authentication and authorization fails.

The 802.1X specification includes a number of features aimed specifically at supporting the use of Port Access Control in IEEE 802.11 LANs (WLAN). These include the ability for a WLAN access point to distribute or obtain global key information to/from attached stations, by means of the EAPOL-Key message, following successful authentication.

## MOTIVATION AND HISTORY

Several emerging trends and needs motivated the development of 802.1X:

### **The Increased Use of 802 LANs in Public and Semi-Public Places**

As network owners have extended their networks into public spaces, they must control which users have access. Prior to 802.1X, if a user could plug into a live 802 port, the user gained full access to the network. This issue is magnified with the rapid growth of WLAN use. Now, any user within physical range of a WLAN access point can attempt to utilize network resources.

### **The Need for Per-Port Network Control**

Since the port is a user's network attachment point, it is the logical place to control the user's access. It is also a logical point to apply packet and protocol filtering. Thus, by controlling the users network attachment point, the user's network environment can be personalized to meet the user's needs and access permissions.

### **The Need for AAA**

Many organizations have invested in authentication, authorization, and accounting (AAA) technology to control their users' network access, typically dial-in remote access or access via a firewall. 802.1X can leverage currently installed AAA servers, typically RADIUS servers, to provide these functions to new 802.1X clients.

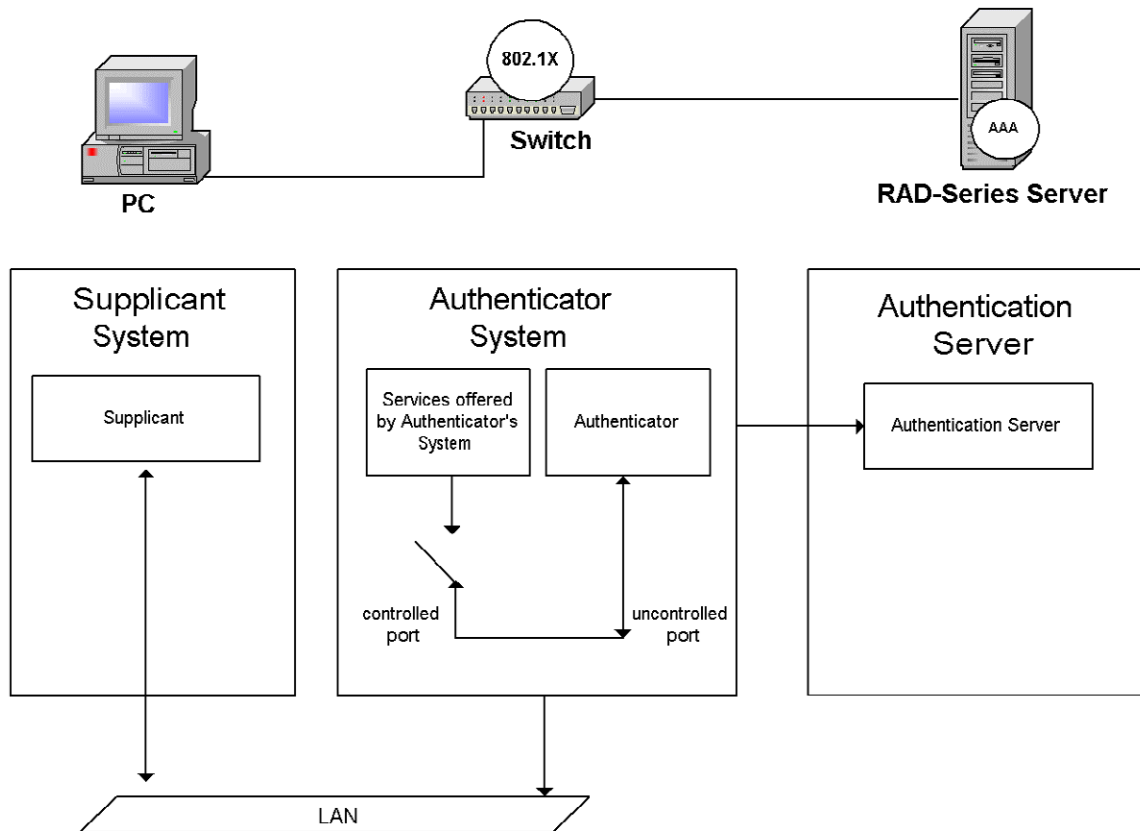
### **The Need to Distribute Dynamic Encryption Keys**

The goal of WEP (Wired Equivalent Privacy) is to provide a level of security roughly equivalent to that of a wired network. WEP was intended to provide security between communicating wireless peers through the use of symmetric encryption keys. One limitation has been the challenge of distributing and managing the encryption keys. 802.1X provides a method for distributing WEP keys to access points and stations.

802.1X is a collaborative effort by vendors in the software, server, and networking industries to address the above needs. Industry leaders proposed 802.1X to address these needs by providing access control and key distribution to any (wired or wireless) Ethernet port.

## TERMINOLOGY

In order to understand the various components in an 802.11 network utilizing 801.X, consider Figure 1.



**Figure 1.** This diagram shows the supplicant, authenticator, and authentication server in an 802.1X wired network. Note that 802.1X requires one authenticator per port. The controlled port shown above is not authorized and therefore is not allowing traffic.

### Port

A port in this context is a single point of attachment to the LAN infrastructure. Note that in the 802.11 LAN case, an access point manages “logical” ports. Each of these logical ports communicates one-to-one with a station’s port.

### Authenticator

The authenticator enforces authentication before allowing access to services that are accessible via that port. The authenticator is responsible for communication with the supplicant and for submitting 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.

It is important to note that the authenticator’s functionality is independent of the actual authentication method. It effectively acts as a pass-through for the authentication exchange.

## **Supplicant**

The supplicant accesses the services accessible via the authenticator. The supplicant is responsible for responding to requests from an authenticator for information that establishes its credentials.

## **EAP**

The Extensible Authentication Protocol (EAP) is a method of conducting an authentication conversation between a user and an authentication server. Intermediate devices such as access points and proxy servers do not take part in the conversation. Their role is to relay EAP messages between the parties performing the authentication. 802.1X employs the Extensible Authentication Protocol (EAP) as an authentication framework.

## **Extensible Authentication Protocol Over LAN (EAPOL):**

802.1X defines a standard for encapsulating the Extensible Authentication Protocol (EAP) messages so that they can be handled directly by a LAN MAC service. This encapsulated form of EAP frame is known as EAPOL. In addition to carrying EAP packets, EAPOL also provides control functions such as start, logoff, and key distribution.

## **RADIUS**

RADIUS is the Remote Access Dial In User Service. It is the standard way of providing Authentication, Authorization, and Accounting services to a network. Although RADIUS protocol support is optional within IEEE 802.1X, it is expected that many IEEE 802.1X authenticators will function as RADIUS clients. In fact, Annex D of the 802.1X standard describes guidelines for 802.1X RADIUS usage and most access points that support 802.1X support it using RADIUS.

## **802.1X ARCHITECTURE**

802.1X Port-based access control has the effect of creating two distinct points of access to the authenticator's attachment to the LAN. One point of access allows the exchange of frames between the system and other systems on the LAN. Often, this uncontrolled port allows only authentication messages (EAP messages) to be exchanged. The other (controlled) point of access allows the exchange of frames only if the port is authorized.

When a host connects to the LAN port on an 802.1X switch the authenticity of the host is determined by the switch port according to the protocol specified by 802.1X *before* the services offered by the switch are made available on that port. Until the authentication is complete, only EAPOL frames are allowed exchanged. Once the host authentication is successful, the port switches traffic as a regular port.

Recall that 802.1X was developed to address point-to-point networks. In other words, there must be a one-to-one relationship between a supplicant and an authen-

enticator. In a wired LAN, a supplicant is directly connected to an authenticator. As shown in Figure 1 above, a workstation is directly connected to a LAN switch port. Each port on the LAN switch has an associated authenticator. The workstation gains access to the network when its supplicant authenticates to the LAN port authenticator.

## 802.1X IN 802.11 WIRELESS LANS

The 802.1X specification includes two main features aimed specifically at supporting the use of Port Access Control in IEEE 802.11 LANs:

1. **Logical Ports.** The ability to make use of the MAC address of the station and access point as the destination address in EAPOL protocol exchanges.
2. **Key Management.** The ability for an access point to distribute or obtain global key information to/from attached stations, by means of the EAPOL-Key message, following successful authentication.

### Logical Ports and MAC Address Association

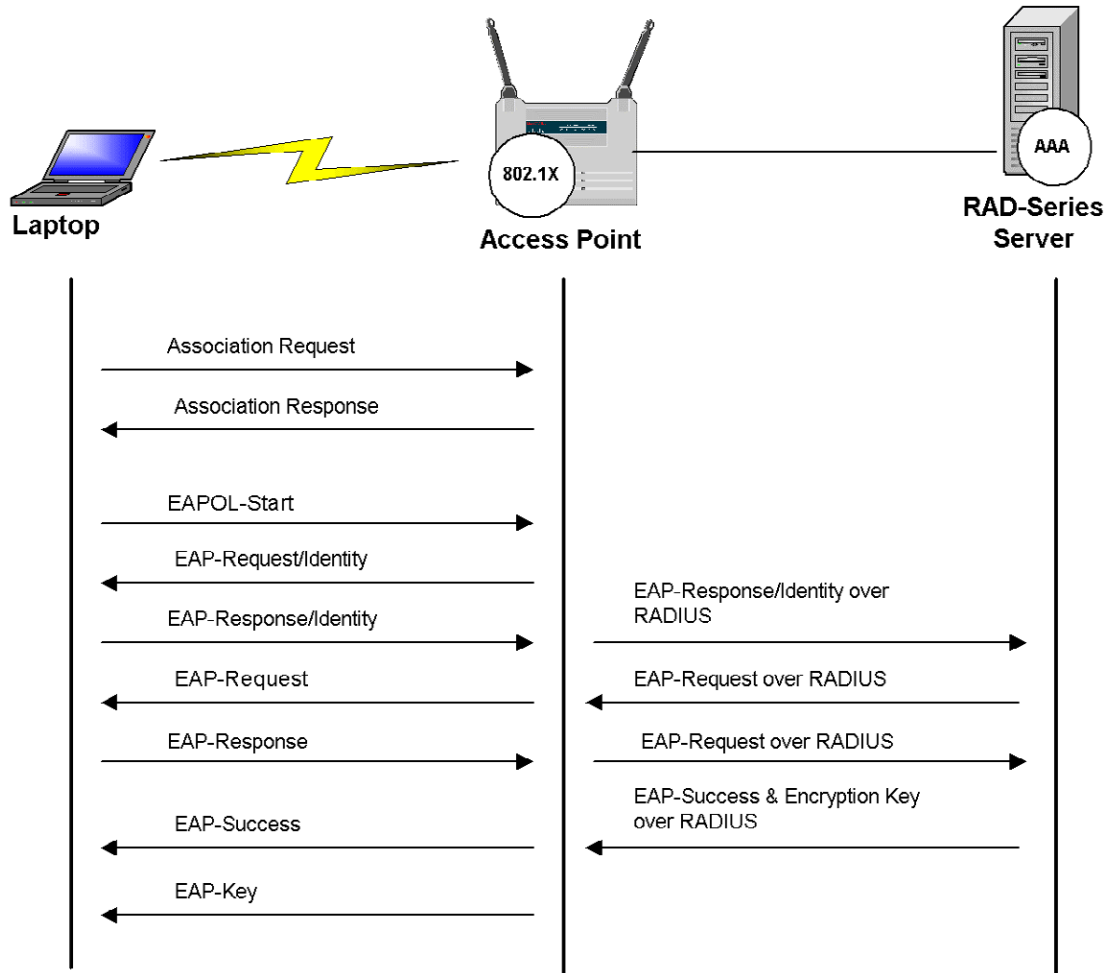
In an 802.11 LAN environment, stations are not physically connected to the network. In addition, multiple connecting stations share the network access media (the RF airspace). A special case of shared media access exists in IEEE 802.11 Wireless LANS in which a station must form an association with an access point in order to make use of the LAN. The protocol that establishes the association allows the station and access point to learn each other's MAC addresses. This effectively creates a "logical port" that the station can use to communicate with the access point. Access points are configured to use Open Authentication. This allows the supplicant to associate with the Access point before dynamically derived WEP keys are available. Once the association has been established, that attached station may authenticate using the Extensible Authentication Protocol (EAP).

### WEP Key Management

The 802.1X neither excludes nor requires WEP or any other encryption algorithm. It does provide a mechanism for distributing encryption key information from an access point to a client using the EAPOL-Key message. This may be performed on a per-session basis, which helps to thwart WEP key discovery. If an eavesdropper manages to obtain a WEP key, it will not be useful after the current user session terminates.

## Association and EAP Authentication Procedure

As previously mentioned, a station must first associate with a given access point. Once the station is associated with an access point, it can exchange EAP messages with the authentication server to authorize the port. Before the logical port has been authorized, it only exchanges EAP messages. Figure 2 details a typical EAP exchange between a station and an authentication server.



**Figure 2. This diagram shows the steps that occur for association, authentication, and key distribution.**

Note that the EAP dialog is carried by EAPOL between the station and access point. The dialog is carried by EAP over RADIUS between the access point and the authentication server. This effectively creates an EAP conversation between the station and authentication server that allows the user to authenticate. Once the user is authenticated, the EAP-Key message is sent to relay keying information between to the station.

## **ADVANTAGES OF USING 802.1X IN THE WIRELESS LOCAL AREA NETWORK**

There are many advantages to using 802.1X in 802.11 LANS.

### **Control at the Network Edge**

802.1X allows a network to restrict access at the edge, where it is most easily managed. Controlled ports, wired or wireless, stop unauthenticated intruders from ever gaining access to your network.

### **Dynamic Session Key Management**

802.1X has a framework that allows a system to use dynamic session encryption keys; to periodically re-key a session; and to periodically re-authenticate a user. This enhances security by eliminating static encryption keys and by foiling attacks on the encryption key that require the collection of large amounts of data encrypted with a single key.

### **Low Overhead**

802.1X does not involve encapsulation, so it adds no per-packet overhead (other than that imposed by enabling WEP) and can be implemented on existing switches and access points with little performance impact. This means that it is scalable, and can be enabled on most existing switch hardware with a firmware upgrade. Since 802.1X can be implemented in the NIC driver, updated drivers from the NIC vendor can usually provide this functionality without the need to install a new operating system.

### **Utilizes Open Standards**

802.1X integrates well with open standards for authentication, authorization and accounting (including RADIUS) allowing it to be implemented on the existing infrastructure for managing dialup networks and VPNs. RADIUS servers that support EAP can be used to authenticate 802.1X-based network access requests.

## **INTERLINK NETWORKS SUPPORT FOR 802.1X**

Interlink Networks supports 802.1X in the RAD-E and RAD-P AAA RADIUS servers. To authenticate users with EAP, the RADIUS server's configuration files are easily modified to identify the wireless access point, the users' realms, and the user profiles. To see how the RAD-Series server is configured to use 802.1X see the application note, *Using 802.1X for Wireless Local Area Networks with Interlink Networks RAD-Series RADIUS Server*.

## REFERENCES

- IEEE Standard 802.11-1999 - Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications
- IEEE Standard 802.1x-2001 – Standard for Port based Network Access Control
- Intercepting Mobile Communications: The Insecurity of 802.11 - <http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf>
- Weaknesses in the Key Scheduling Algorithm of RC4 - [http://www.eyetap.org/~rguerra/toronto2001/rc4\\_ksaproc.pdf](http://www.eyetap.org/~rguerra/toronto2001/rc4_ksaproc.pdf)
- draft-congdon-radius-8021x-16.txt - IEEE 802.1X RADIUS Usage Guidelines
- draft-ietf-pppext-eap-srp-03.txt - EAP SRP-SHA1 Authentication Protocol
- draft-ietf-pppext-eap-ttls-00.txt - EAP Tunneled TLS Authentication Protocol (EAP-TTLS)
- RFC 2246 – The TLS Protocol Version 1.0
- RFC 2284 - PPP Extensible Authentication Protocol (EAP)
- RFC 2548 - Microsoft Vendor-specific RADIUS Attributes
- RFC 2716 – PPP EAP TLS Authentication Protocol
- RFC 2865 - Remote Authentication Dial In User Service (RADIUS)
- RFC 2866 - RADIUS Accounting
- RFC 2868 - RADIUS Attributes for Tunnel Protocol Support
- RFC 2869 - RADIUS Extensions
- RFC 2945 – The SRP Authentication and Key Exchange System
- RFC 3079 - Deriving Keys for use with Microsoft Point-to-Point Encryption (MPPE)<http://www.netmotionwireless.com/resource/> - top

## **ABOUT INTERLINK NETWORKS**

### **THE COMPANY**

Interlink Networks is a leader in securing access to public and private networks. Our products manage user access to dial-in, broadband, mobile, and wireless LAN networks. Interlink Networks' RADIUS-based access control software provides the authentication, authorization, and accounting infrastructure that enables secure and reliable network access for thousands of enterprise and service provider networks worldwide.

Interlink Networks is headquartered in Ann Arbor, Michigan. We have a worldwide network of resellers and distributors.

### **OUR MISSION**

Interlink Networks' mission is to be a worldwide leader in providing solutions for securing access to public and private networks. By securing access to the network, we provide network operators the first line of defense against unauthorized access to an organization's computing resources.

### **OUR HISTORY**

In July 2000, Interlink Networks was formed by a spin out of technology and developers from Merit Network, Inc., a world-renowned designer, developer, and implementer of Internet technology, hosted at the University of Michigan.

The founders of Interlink Networks spent over a decade defining and developing the world's best carrier-class RADIUS (Remote Access Dial-In User Services) server. Mr. John Vollbrecht, Interlink Networks' Founder and CTO, issued the first RFP for centralized AAA ten years ago, and championed the resulting RADIUS standards through the IETF Standards Groups. Mr. Vollbrecht's name is on many of the RFCs that define RADIUS and AAA.

The charter of Interlink Networks is to expand upon its vision of providing the most advanced authentication products, and to expand its solution set beyond remote access into other network access mechanisms that require authentication and authorization. As networks become more complex, and the means to access networks expands, Interlink will continue to assure that the "interlinks" between users and their networks are protected and secure.