INTERLINK™
NETWORKS

Using 802.1X for Wireless Local Area Networks with Interlink Networks Software

Revision **B**

Trademark Information

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
sales@interlinknetworks.com
www.interlinknetworks.com

Using 802.1X for Wireless Local Area Networks with Interlink Networks Software

INTRODUCTION

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 connections characteristics. It also prevents access to that port in cases in which the authentication and authorization fails. Many new 802.11 wireless LAN access points are advertised as employing IEEE 802.1X for enhanced security.

802.1X, if utilized properly, can indeed provide a network with a higher level of security. 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).

For background information on 802.1X see the Interlink Networks white paper *Introduction to 802.1X for Wireless Local Area Networks*.

INTERLINK NETWORKS SUPPORT FOR 802.1X

To authenticate users with EAP, you will need to modify the configuration files to identify the wireless access point, the users' realms, and the user profiles. The following steps will configure the RAD-Series or Secure.XS servers to authenticate WLAN users:

Configure the Clients File

In the `clients` file, add the access point:

```
Name Shared-secret Type=Vendor:NAS+options
```

- ***Name*** identifies the IP address or DNS name of the access point.

- ***Shared-secret*** identifies the secret is the encryption key, or shared secret, between the access point and the authentication server.
- **Type=NAS** identifies the client as an access device.
- You may specify the *Vendor* of the access point if the vendor appears in the vendors file.
- Various *+options* may be appended to **Type=NAS** to define additional instructions to handle the Access-Request.

The following example clients file entry identifies a Cisco Aironet 350 access point named w03 with a shared secret of "secret":

```
w03.yourdomain.com secret Type=Cisco:NAS
```

Configure the Users File

For each individual user that will be authenticated through EAP, you will need to add a user profile to the users file:

```
User-name@Realm Authentication Type = Realm, Check-items
    Reply-items
```

- ***User-name@Realm*** identifies the user profile by user name and the user's realm.
- **Authentication Type = Realm** must be specified so that the authfile is checked to determine that EAP is the protocol for the user's realm.
- *Check-items* is a list of one or more check items and other configuration A-V pairs that define authentication and authorization for the user. Most user profiles will have a password and many will have other items.
- *Reply-items* is a list of one or more reply items that define authorization for the user.

The following example users file entry identifies the user, "Joe," in the mydomain.com realm.

```
Joe@mydomain.com Authentication-Type = Realm, Password = Joepassword
```

The Realm authentication type directs the server to the authfile. The authfile identifies EAP and what type of EAP to perform when authenticating the users.

Configure the authfile

For each realm using EAP, you must associate the realm name with the type of EAP to perform by adding the following entry in the RAD-P server's authfile:

```
Name EAP Description
    {
    EAP-Type Challenge
    ...
    }
```

- ***Name*** identifies the name of the realm that will use EAP.
- **EAP** indicates that EAP will be used as the authentication type.
- ***Description*** can be any string. Must be enclosed in quotes if the string contains spaces or tabs.

- **`EAP-Type`** indicates what type of EAP, as identified by ***`Challenge`***, to use. Multiple types may be listed. The AAA server will first attempt to resolve a challenge according to each listed type, starting with the first listed type. If the challenge fails for all listed types, the AAA server will return an Access-Reject.

The following example `authfile` entry instructs the server to use LEAP authentication for the realm mydomain.com:

```
mydomain.com EAP "CiscoLEAP realm"
    {
    EAP-Type CiscoLEAP
    }
```

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.