FEATURE SHEET

Dynamic PSK™

Ruckus™ WIRELESS

Dynamic Pre-Shared Key (PSK) is a patent-pending technology developed to provide robust and secure wireless access while eliminating the arduous task of manual configuration of end devices and the tedious management of encryption keys.

Dynamic PSK creates a unique 63-byte encryption key for each user upon accessing the wireless LAN for the first time and to automatically configure end devices with the requisite wireless settings (i.e. SSID and unique passphrase) without any manual intervention.

Wireless Security Choice for SMBs

Wireless security remains a primary concern for any enterprise (large or small) when deploying a WLAN. But securing a WLAN is complex and time consuming. This is a major problem for smaller businesses with limited IT staff that require the same security as large organizations but don't have the time or expertise to implement robust wireless security.

Security option	Benefits	Drawbacks
Open network	• Simple to use and deploy	• Completely insecure • Some client configure still required
Pre-Shared Key	• Straightforward implementation • Link layer encryption	• Easily compromised • Same key for all employees • Client configuration required
802.1x	• Robust and comprehensive framwork • Strong encryption and authentication	• Expensive • Requires 802.1x supplicant on end device • Highly complex • Time-consuming to implement
Dynamic PSK	• Easy to use • Strong encryption • No admin intervention • Works with existing authentication	• Manual configuration required for handheld devices (eg. phones, PDA)

Authentication (i.e. who is the user and what device are they using) and encryption (the scrambling of data) are the two primary security issues to be addressed.

Three popular security options available to SMBs tradeoff security and ease of deployment (see Table). But none of these options provides an optimal solution.

While simple to implement, an open wireless network is clearly not a secure solution as it leaves user transmissions in the clear inviting would-be snoopers to easily grab data out of the air or penetrate the internal network.

A more commonly used wireless security option is using a common pre-shared encryption key. A key or passphrase is configured on the APs and on every laptop.

While this option is perceived to be more secure, it's not. Using the same PSK for all employees means that key can be easily compromised.

The common PSK also tends to be a relatively short string that can be easily compromised. And for every new employee, IT staff must configure the laptop with the SSID and the key. If there's a need to replace the key (eg. employee leaves), every laptop must be reconfigured.

The third option is using an enterprise-class solution such as 802.1X. A highly secure solution, 802.1X is very complex for an SMB. It requires having the right infrastructure starting with the RADIUS server all the way to 802.1X supplicants on each client. Configuring and maintaining 802.1X is an overkill for SMBs as they do not have the time or resources to manage such an endeavour.

A new approach, Dynamic PSK solves these problems.

FEATURES

- Automatic provisioning of unique encryption key to each user/device
- No manual client configuration
- Unique 63-byte pass-phrase per user per machine
- Easily deactivated when employee leaves
- New key can be generated periodically
- Configurable per WLAN

BENEFITS

- Robust security simplified for SMBs
- Highly secure
- IT Lite - simple to deploy and maintain

FEATURE SHEET

Dynamic PSK™

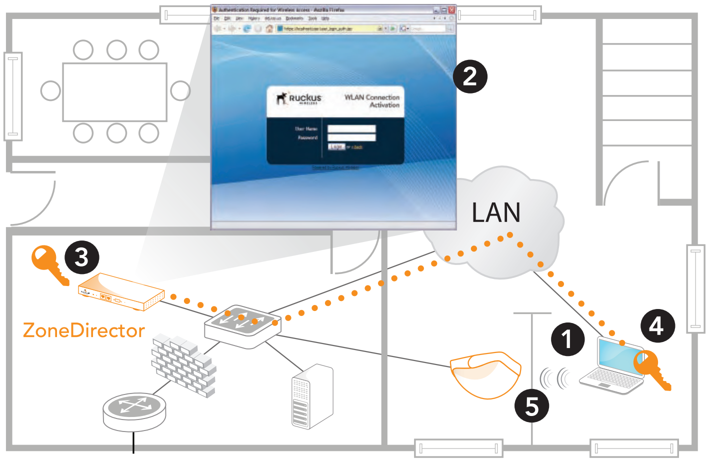
How Dynamic PSK Works?

Instead of manually configuring each individual laptop with an encryption key and the requisite wireless SSID, Dynamic PSK automates and centralizes this process within the network.

Once enabled for the entire system, a new user simply connects to the Ethernet LAN and authenticates via a captive portal hosted on the Ruckus ZoneDirector. This information is checked against any standard back-end authentication system such as Active Directory, RADIUS or an internal user database on the ZoneDirector.

Upon successful authentication, the ZoneDirector generates a unique encryption key for each user. A temporary applet with the unique user key and other wireless configuration information is then pushed to the client. This applet automatically configures the user's device without any human intervention.

The user then detaches from the LAN and connects to the wireless network. Once associated, the Dynamic PSK is bound to the specific user and the end device being used. The Dynamic PSK has a configurable lifetime.


Authentication Required for Wireless access - Mozilla Firefox
WLAN Connection Activation
User Name
Password
Login
2
LAN
3
ZoneDirector
1
4
5

1. User attaches to wired LAN
2. User challenged to authenticate at captive portal page
3. Upon authentication, a unique encryption key is dynamically generated for user by the ZoneDirector
4. Key is passed to user device where it is automatically configured within the wireless configuration
5. User detaches from the LAN and can now safely connect to the WLAN

ZoneFlex Security Features

Authentication & Authorization

Per WLAN configuration

Captive Portal with authentication and authorization

- Local database – with role-based authorization
- ActiveDirectory - with group-based authorization
- RADIUS

Wireless Auth

- Open
- Shared (pre-shared key)
- 802.1X
- Dynamic PSK

Encryption

Open

WEP

WPA/WPA2 (TKIP and AES)

AP/Director communication is LWAPP-based control messages encrypted (AES)

Access Control

Role-based authorization

Blocking clients

Access Lists (ACLs)

- Layer-2 (MAC address based ACL)
- Layer-3 (IP address based ACL)
- L2 Client isolation

Wireless Intrusion Detection (WIDS)

Rogue AP detection

DoS attack prevention

Password guessing protection

Rate limiting

Management and Other

Secure management via HTTPS

Statistics and troubleshooting

Option for manual control of APs joining the Director

Multiple BSSIDs and VLANs

Hidden SSID

Ruckus Wireless, Inc.
880 W. Maude Avenue. Suite 101
Sunnyvale, CA 94085 USA
TEL +1 650-265-4200 FAX +1 408-738-2065
www.ruckuswireless.com