Odyssey® Client – The Lowest TCO Secure 802.1x Access Client

December 2005

FUNK SOFT WARE

A Juniper Networks company

Funk Software, Inc.
222 Third Street
Cambridge, MA 02142
(617) 497-6339
http://www.funk.com

Executive Summary

Increasingly, WLAN access is moving into the mainstream of enterprise computing. What used to be limited to pockets of power users has now been embraced by the enterprise IT staff – no doubt due in large part to the widespread acceptance of WLAN security based on the IEEE security standard 802.1x and strong WLAN security protocols such as EAP-TTLS.

With the security problem solved, enterprises feel confident in their ability to safely deploy WLAN access across their enterprise. However, security is not the only consideration in your WLAN roll-out; you must also evaluate your 802.1x solution – in particular your 802.1x access client – in terms of how easy it is to deploy and manage, and how well it accommodates all usage scenarios. The impact on your IT organization of choosing a client which does not meet these requirements are costly indeed.

Funk Software's 802.1x access client Odyssey Client is ideally suited to enterprise deployment, and can even lower your deployment and support costs. In particular, Odyssey Client provides:

- Strong security, with support for numerous strong WLAN security protocols

  Odyssey Client supports EAP-TTLS, EAP-PEAP, EAP-FAST, EAP-TLS, and LEAP. This multi-protocol support ensures strong security, while permitting a flexible security architecture and easy migration from one protocol to another.

- Unsurpassed multi-vendor, multi-protocol compatibility

  Odyssey Client runs with equal security on Windows XP, 2000, 98, Me, Pocket PC 2002, and Windows Mobile 2003 for Pocket PC, and supports any 802.1x-compatible adapter card. It's a complete implementation of the 802.1x standard; its support for numerous WLAN protocols enables it to easily interoperate with 802.1x solutions from other vendors.

  Odyssey Client reflects the multi-vendor compatibility and support for market standards that have been the hallmark of Funk Software's RADIUS solutions.

In addition, Odyssey Client is characterized by:

- **Lower deployment costs** – Unlike other 802.1x clients, Odyssey Client is easily pre-configured with network settings and distributed to all wireless users. Multi-platform compatibility, strong multi-vendor support, plus powerful Enterprise Wireless Client Provisioning capabilities ensure rapid deployment of new installations and upgrades with no hardware limitations or platform upgrades required.

- **Lwer ongoing support and training costs** – Unlike other 802.1x clients, Odyssey Client provides a simple, intuitive end user experience; most of the time, users will be automatically connected to the correct network, with the correct security settings, on device boot. Detailed logging provides all the information required for troubleshooting.

This paper describes these points in more detail, and demonstrates why Odyssey Client is your best choice for enterprise-wide deployment.

Strong Security

Odyssey Client supports the strong WLAN security protocols EAP-TTLS, EAP-PEAP, EAP-FAST, and EAP-TLS. [In addition, it supports Cisco's proprietary LEAP protocol.]

EAP-TTLS, EAP-PEAP, and EAP-TLS provide strong credential security over the wireless link, manage encryption keys effectively to ensure data security, and provide mutual authentication of client and server to ensure that only authorized users gain access to the network and that users can only connect to an authorized network.

For more information on these security protocols, and how they secure WLAN access, refer to Funk Software's white paper "Secure Authentication, Access Control, and Data Privacy on Wireless LANs.

Multi-vendor, Multi-protocol Compatibility

Odyssey Client reflects the multi-vendor compatibility and support for market standards that have been the hallmark of Funk Software's RADIUS solutions.

As we've stated, Odyssey Client offers equivalent security and functionality across Windows XP, 2000, 98, Me, Pocket PC 2002, and Windows Mobile 2003 for Pocket PC with support for EAP-TTLS, EAP-PEAP, EAP-FAST, EAP-TLS, and LEAP. It runs on any 802.1x-compatible adapter card.

Because Odyssey Client fully implements the 802.1x standard and WLAN protocols EAP-TTLS, EAP-PEAP, EAP-FAST, EAP-TLS, and LEAP, it is fully interoperable with solutions from other vendors which support these protocols. For example, an Odyssey Client user can easily be authenticated by a RADIUS server from Cisco or Microsoft.

In addition, Odyssey Client's support for multiple security protocols lets you accommodate the use of a number of different EAP types within the 802.1x security infrastructure. For example, you may deploy today using EAP-TTLS with the intention of moving to PEAP as that protocol matures. An Odyssey Client solution easily accommodates this scenario.

This multi-vendor, multi-protocol compatibility is vital to a successful deployment: it ensures support for any network environment and provides the flexibility you need to facilitate solution deployment.

However, that's not the full story: While multi-vendor compatibility will undoubtedly ease your deployment, there are other 802.1x-client-specific considerations. In particular, you need to evaluate your 802.1x client in terms of how easy it will be to deploy across all the wireless devices in your organization and, once deployed, what its ongoing support impact will be.

The sections below outline the unique features of Odyssey Client which will enable you to easily and rapidly deploy it across your network.

Odyssey Client Lowers Deployment Costs

Critical to your ability to successfully install an 802.1x solution is the ability to easily install the 802.1x access client across all the wireless PCs in your organization. Particularly in large organizations, any requirement to individually configure each PC to support secure WLAN access creates a significant burden for your IT staff. This burden is dramatically increased if the PC platform needs to be re-configured or upgraded prior to being able to support WLAN access.

When considering an 802.1x access client, evaluate it in terms of its:

- **Pre-configuration capabilities** – With the proper pre-configuration tools, you are able to enforce corporate standards of security without having to travel from PC-to-PC to get your users up and running.

- **Ability to be updated** – Beyond deploying the client to every PC, you also need to think about how you will push updated configuration settings to your end users if your security requirements or network infrastructure change.

- **Level of administrative control** – If you are very security conscious, you may wish to prevent your end users from changing their configuration settings, or from using network connections that you have not configured.

- **Operating system dependencies and multi-vendor compatibility** – Client dependencies such as late-model service pack version can significantly increase the amount of time it takes to deploy an 802.1x client. And, as laptop vendors increasingly integrate wireless functionality, you will have less and less control over what type of wireless adapter card your users run. It's critical that your 802.1x client minimize platform dependencies and support cards from numerous vendors.

- **Ability to handle all desired functions** – A client which controls both radio and security settings, and supports wired and wireless connections is easiest and fastest to deploy, and requires the least amount of end user training.

Odyssey Client addresses these requirements fully, allowing you to easily and rapidly deploy it across all the wireless devices in your organization.

The first three requirements – pre configuration, ability to be updated, and level of administrative control – are accomplished by a set of features within Odyssey Client called Enterprise Wireless Client Provisioning.

Enterprise Wireless Client Provisioning

Enterprise Wireless Client Provisioning is a set of features within Odyssey Client that provides the ease of deployment and manageability that are vital to desktop managers on large enterprise networks. These features permit:

- Pre-configuration of Odyssey Client, for easy installation across any number of wireless devices

- Global or selective updates of users' wireless configurations

- Control over whether or not users can update their WLAN configuration settings

Odyssey Client is the only 802.1X access client on the market to provide these features across multiple Windows platforms – so you'll enjoy all benefits whether you're running

4

an XP-only network, or a mixture of XP, 2000, 98, Me, and Pocket PC devices on your network.

Pre-Configuration

Odyssey Client includes a utility called the ***Odyssey Client Administrator*** which allows a network administrator to easily customize the Odyssey Client Installation package prior to distributing the software to end users.

Using the Odyssey Client Administrator, a network administrator can set up and enforce the corporate standard for trusted wireless networks (in and out of the office), and make these networks available to end users immediately upon installing Odyssey Client, without any additional configuration.

First, the network administrator uses the Odyssey Client Administrator to build a list of Trusted Wireless Networks, and the default authentication profiles to use when these networks are encountered. If necessary, Trusted-Root-Certificates required for server authentication are installed on the template machine.

When all of the default settings have been specified, the network administrator can use the Odyssey Client Administrator to merge the settings from the template machine with an Odyssey Client Installation image, so that these default settings will be applied, and certificates installed, at the same time that Odyssey Client is installed. Once the Odyssey Client installation image has been prepared, it can be distributed to end users via a standard software distribution package such as SMS, or launched silently via a network login script. When properly configured, Odyssey Client will seamlessly discover and connect to known trusted networks without any intervention from the end user.

In addition to establishing user-specific settings, you can use the Odyssey Client Administrator to configure machine-level credentials and authentication profiles that can attach machines to the corporate network at boot time rather than at user logon time. Machine connections are often required in complex network environments where wireless servers or workstations need to be available, regardless of who happens to be logged into them. The Odyssey Client Administrator makes configuring a machine connection quick and painless. [See "Client Deployment – Lower Ongoing Support Costs" section for more information on machine connection options.]

Other 802.1x clients – including the Microsoft Windows 2000 802.1x client – do not support pre-configuration or zero-configuration installations.***Ability to be updated***

Of course, your requirements don't end at deployment. Your network and security requirements will likely evolve, and as they do, you'll need to change your users' WLAN configuration. You may need to add or remove networks; or change your security policy – for example to strengthen it by moving from LEAP to TTLS, or from WEP to WPA, or from WPA to WPA2. With other 802.1X clients, you'll have to publish instructions for your users to follow (or travel from PC to PC yourself to make the changes). With Odyssey Client, you can globally or selectively deploy updates to all devices – silently, with no end user intervention required. You'll be able to:

- Add new networks to everyone's auto-scan list, so they can easily (or automatically) connect to the new network

- Require connection via a new EAP type to accommodate a different security requirement or scheme (such as token authentication)

- Remove obsolete networks, or change network settings when you've made a change to how an existing network is configured.
- Deploy any other WLAN settings you need to.

Administrative control

Beyond the ability to deploy and update configuration settings, you may also want to control whether or not end users can change the configuration settings they've been issued. This is a particularly important capability if you must enforce stringent security requirements.

With Odyssey Client, you can lock down any or all of your users' WLAN settings, to give you the control you need over how users can connect. This capability is optional, of course, but if you need to enforce stringent security policies, it will help you keep your network safe.

Settings that can be locked down include EAP policies – so, for example, a user can be prevented from connecting using a less secure protocol such as LEAP; security settings such as encryption protocol, so you can force the use of WPA or WPA2; and network lists, so you can prevent users from adding (and connecting to) networks that have not been sanctioned by you.

Of course, beyond having enforce a stringent security policy, you may simply want to prevent changes to users' configuration settings to reduce support calls. Either way, Odyssey Client gives you the control you need over how your users connect to the network.

Platform Dependencies

Odyssey Client runs with equivalent security functionality on Windows XP, 2000, 98, Me, Pocket PC 2002, and Windows Mobile 2003 for Pocket PC with no dependencies on late-model service pack versions. In addition, it supports any 802.1x-compatible wireless adapter card.

Other clients do not provide this level of compatibility. For example, the Microsoft Windows 2000 802.1x client requires that Service Pack 3 be installed. In addition, the encryption protocol WPA, which is the widely adopted follow-on to WEP – is not supported by the Microsoft 802.1x client running on Windows 2000.

The Cisco ACU requires that Cisco adapter cards be used.

Integrated Client

Odyssey Client is both a total WLAN client – controlling both radio and security settings

– as well as able to connect to both 802.1x wireless and wired networks.

These capabilities significantly decrease your deployment burden. Deploying Odyssey Client for WLAN access is simple, and, because it controls both radio and security settings, you won't need to configure any other driver software.

Plus, it fully supports 802.1x wired connections, so your access client will already be in place as you begin rolling out 802.1x-based access to your wired network.

6

The Microsoft 802.1x client on Windows 2000 does not control the radio signal, requiring twice the deployment effort, and potentially creating a significant support load.

Odyssey Client Lowers Ongoing Support Costs

A second critical issue to consider when deploying an 802.1x access client is support costs. Rolling out a new, complex technology across numerous desktops in your organization can potentially create a significant support burden; to guard against this, evaluate your 802.1x client in terms of its:

- **User experience** – Needless to say, the simpler the client is to understand and use, the fewer support calls you'll receive.

- **Troubleshooting/diagnostics** – Sophisticated logging features and status indicators are critical to your ability to quickly troubleshoot user problems if they do arise.

Odyssey Client addresses these requirements fully, significantly minimizing support calls and training requirements associated with WLAN access.

User Experience

Odyssey Client:

- Requires no user interaction at all in most cases; users will be automatically placed on the correct network at device booth.

- Supports numerous conveniences such as Auto-Scan Networks with Associated

- Profiles that significantly simplify how users connect to the WLAN. Plus, its user interface is identical across all Windows platforms.

- Smoothly handles network login in Windows and NetWare environments, supporting GINA and machine connections.

Auto-Scan Shelters Users from WLAN Complexities

Odyssey Client lets you associate an ordered group of wireless networks with an *auto-scan lis*t, so that you can be connected to any of the networks available in the list. Users will be connected automatically to the network with the strongest signal. These networks and auto-scan lists can be pre-configured by the network administrator.

Through its Auto-Scan capability, Odyssey Client provides significant usability benefits over other 802.1x clients:

- First and foremost, with Odyssey Client, an end user can move seamlessly between different networks, for example, home, office, and hotspot.

- Odyssey Client will automatically associate with the correct network upon PC startup, regardless of location. *The user need not interact with Odyssey Client at all*.

- Users can automatically connect to networks which have different security requirements – *again, with no user interaction required*. This lets users easily move between office and hotspot networks, for example, where secure authentication via Windows password is required for one and no security is required for the other.

To connect to new networks, Odyssey Client will scan for available networks, and walk the user through setting the connection up correctly. If the new network will be visited regularly, it can easily be added to the auto-scan list.

This feature is especially appropriate for users who need to connect to different networks (for example, networks at different offices, at hotspots, or different departments), or if these different networks have different security requirements.

The Microsoft 802.1x client running on Windows 2000 does not support an auto-scan-like capability. The burden associated with training enterprise users to connect to different networks, with potentially different security requirements, would be daunting.

No other 802.1x client permits simple connection to different networks which have different security requirements.

Network Login Issues

Issues that are potentially significant but may be overlooked when evaluating an 802.1x client may arise when clients attempt to login to the network, either in Windows or NetWare environments. For example, in some cases, when running Windows XP or Windows 2000 – for example, on new laptops that have never logged into a domain controller – the user will find himself unable to connect. If no cached credentials are present or if cached credentials are out of sync with the domain controller, the user will be unable to start up his desktop and run the 802.1x client to establish a physical connection to the network (and hence cannot be authenticated by the domain controller). If cached credentials are present, the user will be able to start up his desktop, but any feature requiring network connectivity will fail. Similar issues may arise in NetWare environments.

If these complex issues are not handled properly by the 802.1x access client, numerous support calls relating to inability to connect to the WLAN will be generated.

Odyssey Client offers considerable flexibility and power in handling these issues, in both Windows and NetWare environments. With Odyssey Client, you can choose the following ways to perform network authentication:

- At boot time

  This option allows Odyssey to be configured with a set of *Machine credentials* that can be used to perform a network authentication (i.e., establish a physical connection to the network) at startup time. By the time a user logs into this machine it will already be authenticated to the network, so the Windows Domain Authentication or NetWare authentication will succeed.

- At GINA (or NetWare login screen) time

  This option causes Odyssey to interact with the Windows GINA (Graphical Identification and Authentication) or NetWare login process to retrieve the user credentials from the login dialog, and perform a *Network Authentication* before handing control back to the Windows GINA or NetWare login screen, which will then perform the Windows or NetWare authentication.

- After GINA (or NetWare login screen) time, prior to user desktop

This option causes Odyssey to perform the Network Authentication immediately after the Windows Domain or NetWare authentication is completed, but prior to the user desktop being loaded. A user would choose this option only if conflicts with other applications or processes on the system prevented him from choosing a GINA or NetWare login screen time login.

- After user desktop

  This option will cause the Odyssey Client to perform a network Authentication at the end of the Windows or NetWare login process, after the user's desktop has fully loaded.

  This option would only be chosen if the user had no requirements for advanced Windows or NetWare logon capabilities.

Odyssey Client even allows the machine to stay connected to the network, even though the user has logged off. This allows the network administrator to access the machine to perform network support operations, such as pushing updates, performing backups, distributing software, and performing security audits.

Odyssey Client supports the capabilities listed above on Windows XP and Windows 2000 running the Microsoft or NetWare client.

The flexibility of machine connection and GINA (or NetWare login screen) support with Odyssey Client will ease end users' WLAN experiences, can provide a single sign-on to the network, and are implemented to address TCO for the enterprise by reducing support calls centered around cached credentials and domain controller issues.

Troubleshooting

Ability to troubleshoot user problems is also a significant consideration when selecting an 802.1x client. Without troubleshooting ability, a user is not able to offer valuable information when he places the support call, nor is the administrator able to easily diagnose what might be going wrong. This can significantly increase a user's frustration and network downtime, and increase the length of time a help desk technician takes to resolve user problems.

Odyssey Client:

- **Reports success and failure to connect** – Odyssey Client provides detailed information about connections – for example, status of authentication and encryption – plus provides error messages describing unsuccessful connections, to significantly facilitate troubleshooting.

- **Reports on status of connection and security** – Odyssey Client reports the status of the connection in its interface. It is very easy to determine if the connection succeeded or failed.

The Microsoft 802.1x client running on Windows 2000 supports neither logging nor status reporting. Troubleshooting users' problems would likely be a time-consuming and expensive task.

Conclusion

Funk Software's Odyssey Client is uniquely able to meet the functionality, deployment, and support requirements of your enterprise. Odyssey Client not only offers strong security, but, unlike other 802.1x clients, offers the deployment tools and usability features a large enterprise requires to successfully roll out this new technology across hundreds or thousands of desktops, at the lowest TCO possible.

And, Odyssey Client is very well-suited to a heterogeneous network environment: it runs with equal security and interface on multiple platforms, and easily accommodates a user's moving between different networks, which may even have different security requirements.

When you choose Odyssey Client, you can rest assured you've chosen an 802.1x access client that will meet your requirements today, and that will continue to evolve to meet your requirements in the future.

We look forward to working with you.

 A Juniper Networks company

Funk Software, Inc.
222 Third Street
Cambridge, MA 02142
(617) 497-6339
 http://www.funk.com