

White Paper

Architecting Your 802.1X-Based WLAN Deployment Using Odyssey[®] and Steel-Belted Radius[®]



Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

Part Number: 200164-001 Feb 2006

Introduction

While network managers recognize the obvious benefits of deploying WLANs – namely their flexibility, cost savings, and convenience – there still remain questions over which WLAN security method is best. VPNs have been tentatively adopted by some enterprises, both because they're well understood by network managers and because the security they provide has been time-tested and proved effective.

However, a new WLAN security method – based on the IEEE security standard 802.1X and strong EAP authentication methods such as EAP-TTLS – has emerged, which offers strong WLAN security, without the attendant administrative overhead and architectural restrictions associated with implementing VPN-based WLAN access.

This 802.1X-based solution is increasingly being adopted by enterprises of all sizes, for the following reasons:

- It's easily implemented, because it utilizes an authentication and security scheme – RADIUS – already widely deployed on enterprise networks
- Strong security is easily set up and deployed, putting secure WLAN access within any enterprise's reach
- It easily scales to accommodate growing or changing networks, and offers significant architectural advantages over other WLAN security solutions such as VPNs

The goals of this paper are to demonstrate the architectural advantages of deploying secure WLAN access based on 802.1X and a strong authentication method such as EAP-TTLS, to illustrate how this secure WLAN access can be architected in a variety of scenarios, and to offer guidelines on choosing the Juniper Networks RADIUS server that is appropriate for your network.

802.1X Overview

An 802.1X installation comprises the following major elements:

- WLAN users, running an 802.1X client which supports a strong EAP authentication method such as EAP-TTLS
- 802-1X-compliant access points
- RADIUS server which supports a strong EAP authentication method such as EAP-TTLS

On a simplified level, here's how a connection is established based on a strong authentication method such as EAP-TTLS¹.

In an 802.1X-based environment, the access point essentially acts as a conduit between the Client and the RADIUS server during the user authentication phase. So, via the access point, the WLAN Client and the RADIUS server negotiate to determine which EAP authentication method to use. Once agreed upon, the secure tunnel is set up, through which the user's credentials are passed from Client to RADIUS server. The RADIUS server authenticates the

¹ This paper assumes the use of a strong EAP authentication method – such as EAP-TTLS, EAP-PEAP, or EAP-TLS – with 802.1X. Other EAP authentication methods such as EAP-MD5 and LEAP have known security vulnerabilities and the claims this paper makes do not necessarily pertain to them.

user to determine if he is allowed access to the network. Once the user has been granted access, the RADIUS server issues an encryption key to the access point, which then sets up the secure, encrypted session. The RADIUS server may also be called upon to re-key during the session, to maintain data privacy.

Apart from the strong security put in place to protect credentials and data, an 802.1X architecture based on a strong EAP authentication method such as EAP-TTLS also offers the following security advantages:

- Clients can only connect to access points that are associated with a RADIUS server which presents a trusted certificate
- Access points only communicate with RADIUS servers they've been configured to know about
- The RADIUS server only trusts an access point it's been configured to know about and with which it shares a secret password
- Access points only trust RADIUS server responses which have been signed

Architectural Advantages of an 802.1X-based Solution

There are numerous architectural advantages associated with implementing an 802.1X-based WLAN security solution, particularly relative to a VPN-based WLAN solution. An 802.1X-based solution is more:

- **Scalable** – An 802.1X-based WLAN deployment easily accommodates a growing number of WLAN users
- **Distributable** – It's easy to distribute 802.1X-based WLAN access to separate departments, floors, branch offices or other off-site locations, with very little administrative overhead
- **Cost-effective** – An 802.1X-based WLAN deployment may be significantly less expensive

We'll discuss each of these advantages in turn.

Scalable

An 802.1X-based solution is designed to accommodate network growth and a changing network environment. Unlike VPNs, an 802.1X-based solution lets you set up your entire WLAN access infrastructure and users inside your corporate firewall – with full confidence in security. To accommodate a growing number of users, you simply need to add access points and, to a lesser degree, RADIUS servers.

With VPNs, all your WLAN users and access points are located outside the corporate firewall. As your WLAN user population grows, you'll need to add more equipment outside your firewall: you'll need to add access points, and more VPN servers or capacity. Plus, you'll be called upon to manage an increasingly complex VPN infrastructure, as you must configure and maintain rules on each firewall to permit access by an increasingly large number of users.

Distributable

An 802.1X-based solution is easily distributed to separate departments, floors, branch offices or remote sites. As long as access points and, optionally, a RADIUS server are in place, any worker – including one who’s in for the day from headquarters – can easily and seamlessly connect to the WLAN, in the same manner he uses when he’s in his own office. [See the sections below for more detail on distributed 802.1X-based solutions.]

On the other hand, distributing VPN access to branch offices or remote sites requires you to install or add capacity to a VPN server at that site, and to set up all WLAN users outside the firewall. And, that visitor from headquarters must know which VPN server to connect to. If he doesn’t know, or can’t easily find out, you’ll likely be taking a support call from a frustrated user.

Cost-effective

Solutions based on 802.1X are generally more cost-effective than those based on VPNs for two reasons: first, with 802.1X, you are by-and-large augmenting the infrastructure you’ve already put in place; and second, the complexity associated with setting up and maintaining VPNs may require more of your or your staff’s time to manage.

Both 802.1X and VPN WLAN access obviously require clients and access points. With 802.1X, you’ll need to add an EAP-capable RADIUS server (or upgrade your existing RADIUS server); VPN access is also often managed by a RADIUS server. Most notably for VPN access, adding VPN servers with adequate capacity to handle a growing WLAN user population may be a significant expense.

[For both VPN and 802.1X, the use of enterprise-class access points and RADIUS servers is recommended.]

Common Architectures

This section of the paper will provide an overview of four common 802.1X architectures. Within these four architectures, we will describe the role of the RADIUS server, indicate for which types of networks the architecture is appropriate, and address the common concerns of network administrators, namely cost, performance, and reliability.

Scenario #1 – Single Site Deployment

This, the simplest scenario, is characterized as follows:

- All WLAN users are located at a single site
- A central authentication database handles all user authentication
- One or more RADIUS servers manage WLAN and/or remote access use, authenticating users and setting up secure WLAN connections.

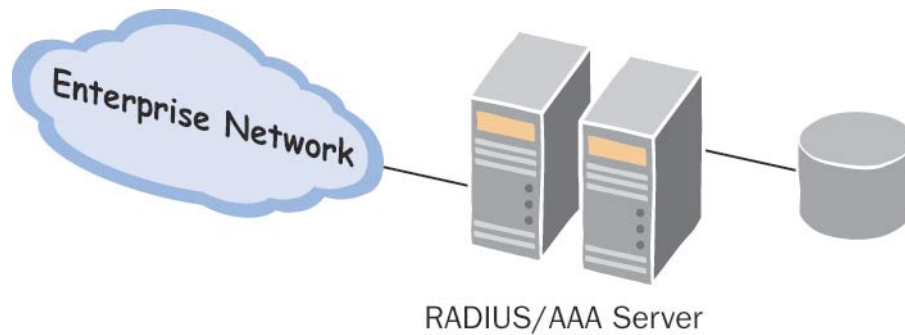


Figure 1.All WLAN users are located on a single network.

This architecture presents the following benefits:

- You can authenticate your WLAN users against any back-end authentication database your RADIUS server supports. [You'll see in the sections below that certain architectures are better suited to certain authentication schemes.]
- To scale, just add access points and RADIUS/AAA servers which would authenticate users against the central authentication database.

The only considerations are those associated with scaling. If you experience a large spike in your WLAN user population, it may make sense to re-architect your network into one of the distributed scenarios described below.

Scenario #2 – Distributed Autonomous Sites

This scenario is characterized as follows:

- Distributed autonomous sites or networks
- The authentication database is replicated from the central site downstream to each autonomous site or network, so that all user authentication happens locally
- One or more RADIUS servers managing WLAN and/or remote access use are located at each autonomous site or network. Each RADIUS server performs the following tasks:
 - Handles user authentication locally
 - Sets up secure WLAN connections
 - If required, records accounting data
- Availability of central site network or operating hub is not an issue

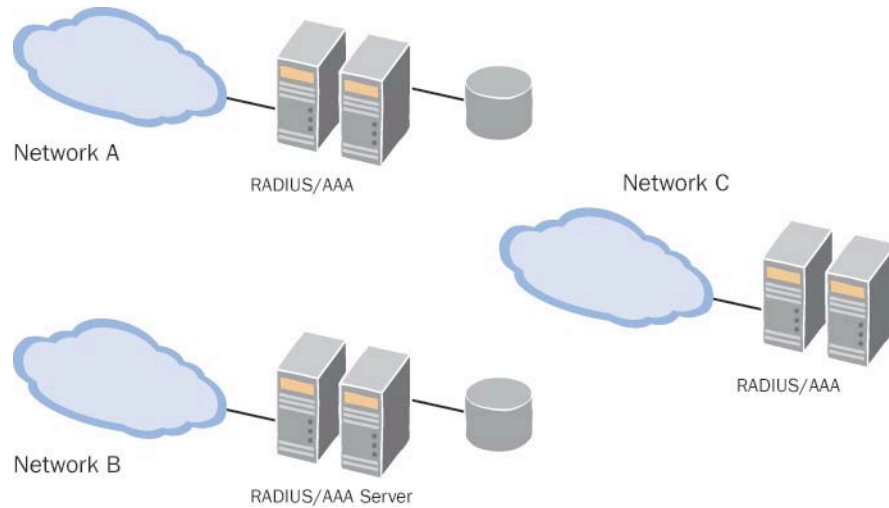


Figure 2. Autonomous networks are set up to handle all WLAN and/or remote access authentication and security locally.

This architecture presents the following benefits:

- Access to your network is governed locally, and is not subject to the reliability of a link back to a central authentication store.
- The distributed RADIUS servers handle the full computational load associated with setting up the secure WLAN connection. You can easily add RADIUS servers to absorb the performance hit associated with adding new WLAN users.

This architecture is appropriate for networks on which authentication databases are deployed which can be easily and reliably replicated, for example Windows or LDAP. It may not be appropriate for authentication systems which are not easily replicated, such as some token systems or SQL databases.

Scenario #3 – Distributed Sites, Centralized Authentication and Security

- This scenario is characterized as follows:
 - Distributed sites, networks, or clusters of access points
 - WLAN access points at each site or on each network authenticate users against an authentication database located at a central site or operating hub.
 - One or more RADIUS servers at the central site manage all WLAN and/or remote access use. The central site RADIUS server:
 - Handles user authentication locally
 - Sets up the user's secure connection
 - If required, records accounting data
- Availability of central site network or operating hub is an issue
- Link bandwidth usage may be an issue

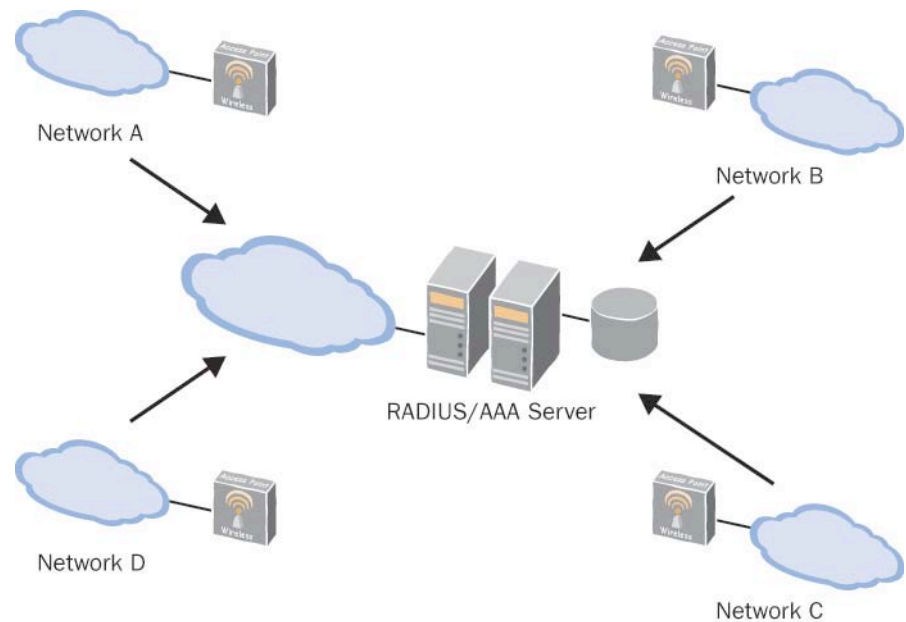


Figure 3. Distributed sites point back to a centralized authentication and security RADIUS server.

While this scenario carries certain cost benefits – you don't need a RADIUS/AAA server on each satellite site, network, or AP cluster – it presents two issues which bear consideration:

- First, the ability of a WLAN user to connect to the network is dependent on the status of the link between the distributed networks and the central site or operating hub. If that link goes down, users will not be able to connect to the network. Users who are already connected will be disconnected once they are required to re-key for security purposes.
- Second, not only is the RADIUS/AAA server at the central site responsible for authenticating users, it must also perform the cryptographic computations necessary to set up the secure WLAN connection. This may result in a performance bottleneck if you are managing – or plan to manage – a large number of WLAN users. You can alleviate this problem by adding RADIUS servers as your WLAN user population grows.

This scenario is likely to be deployed in environments where it is not practical (or you do not wish) to replicate the authentication database to each distributed network, for example when you're requiring your WLAN users to authenticate via some types of tokens. It is also appropriate for networks which are connected by very fast, highly reliable links.

Scenario #4 – Distributed Sites and Security, Centralized Authentication

- This scenario is characterized as follows:
 - Distributed sites, networks, or clusters of access points
 - The authentication database is located at the central site or network hub
 - One or more RADIUS servers managing WLAN and/or remote access use are located at each site, network, or AP cluster. The distributed RADIUS server performs the following tasks:
 - Queries the central site for user authentication
 - Handles setting up the secure connection itself
 - If required, records accounting data locally, or forwards data to the central site
- Availability of central site network is an issue

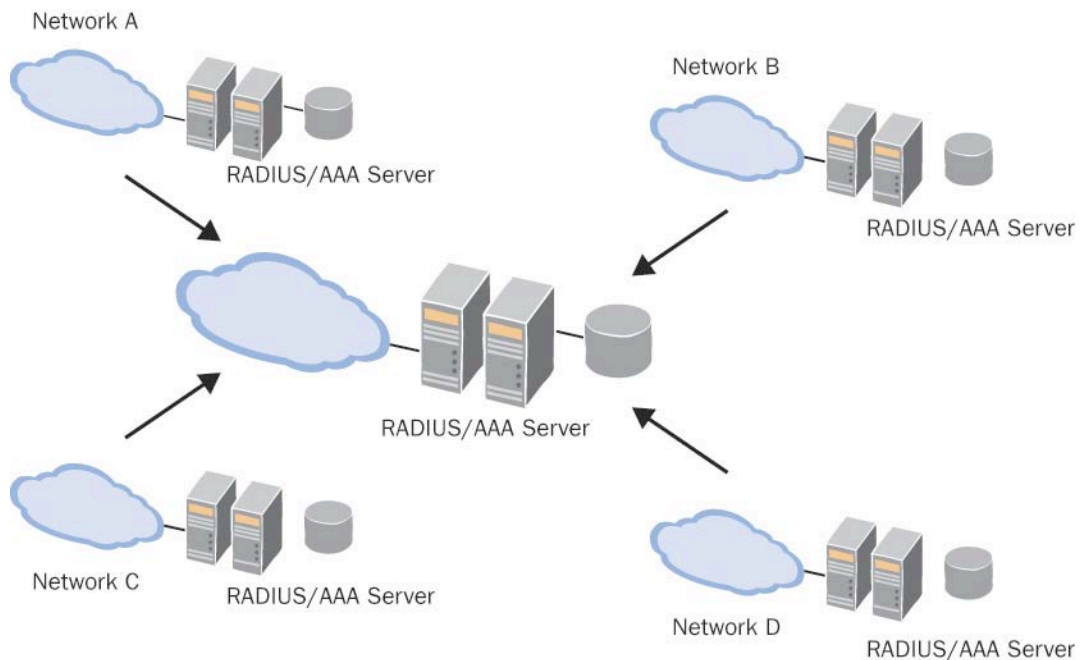


Figure 4. Distribute user authentication to a central site, and handle setting up security on each network.

While this scenario presents the same issue as Scenario #3, namely that you're at the mercy of the reliability of the link between the distributed network and the central site or operating hub, it does present an additional benefit. Here, you can distribute the load associated with setting up the secure WLAN connection to the RADIUS servers located on the distributed networks. This may result in better performance, and will use less bandwidth on the link between the distributed and central sites.

As above, this scenario is probably most appropriate in environments where it is not practical (or you do not wish) to replicate the authentication database to each satellite network, for example when you're requiring your WLAN users to authenticate via some tokens. It is also appropriate for networks which are connected by very fast, highly reliable links.

Combine Architectures

One of the benefits of 802.1X is its flexibility. It's worth noting that the architectural scenarios presented above can be mixed and matched on your network. For example:

- Even if you have adopted a more distributed approach to your WLAN deployment (Scenario #2 or #4), some of your distributed networks may be quite small, consisting of only a few WLAN users. If those networks are linked reliably to your central site, you may want forego installing a RADIUS server there, and instead just have your central site RADIUS server handle their authentication and security.
- Even if you've deployed a centralized authentication and security scheme (Scenario #3), you may have one or two remote offices which are not reliably linked to your central network. In this case, you will probably need to distribute RADIUS servers to those networks – even if only a few WLAN users are there – so these users can reliably connect.

Which Juniper Networks RADIUS Server Should I Choose?

Juniper Network's RADIUS servers – Odyssey Access Server and Steel-Belted Radius – are each uniquely suited to particular WLAN deployment strategies. Depending on your requirements, you may find that a combination of OAS and SBR presents the most functional and cost-effective solution.

- **OAS** – OAS is a RADIUS server specially designed to handle WLAN access control and security. It is ideally suited to smaller organizations or autonomous networks in larger organizations where network access is governed by Windows user names and passwords. Beyond being able to safely authenticate WLAN users against a Windows database and set up their secure connections, OAS can communicate with SBR to authenticate WLAN users in branch offices or distributed departments against a central security infrastructure which may or may not be based on Windows.
- **SBR Enterprise Edition** – SBR EE is Juniper Network's market-leading RADIUS server, and is uniquely capable of managing both remote and WLAN access and security. It provides the same high level of WLAN security that OAS provides, and extends that capability to remote users as well, ensuring that only authorized users can connect – whether they're connecting via VPN, dial, or firewall – and that they receive the appropriate level of access. Plus, SBR lets you authenticate your remote and WLAN users against a wider variety of back-end authentication systems, including token systems and LDAP-based user name and password stores. Finally, SBR fully supports RADIUS accounting, so you can easily track and document remote and WLAN user access.
- **SBR Global Enterprise Edition** – SBR GE extends the capabilities of SBR EE to meet the security management needs of global enterprises who are managing thousands of remote and WLAN users across multiple sites. In addition to offering all the capabilities of SBR EE, SBR GE permits sophisticated distribution of authentication and accounting requests – to easily handle centralized management of far-flung users, and seamlessly

integrate new users acquired, for example, as a result of a merger. Plus, it supports the advanced reliability features you need to ensure 99.999% uptime, and is easily managed from an SNMP-based network monitoring system.

So, how do you know which to use, and where you should deploy it? Your choice is determined by the answers to the following questions.:

For each autonomous site or network, where are you authenticating your WLAN users?

Choose OAS if you need to authenticate WLAN users against a Windows authentication database (Windows XP or Windows 2000 Native Domain, Windows NT Domains).

Choose SBR if you need to authenticate WLAN and remote users against Windows, as well as databases based on SQL/LDAP, token systems such as RSA Security's Authentication Manager, TACACS+, NIS/NIS+ (if running on Solaris), and a native database.

OAS can also forward WLAN user authentication requests to SBR for authentication against any of the back-end databases SBR supports. This feature is important for two reasons:

Performance – WLAN security is computationally intensive. To enhance performance, you can add OASs to handle the security computations, while optionally have them forward to SBR for user authentication. (For more detail, see the Performance section below.)

Cost – OAS costs less than SBR. So, in Scenario #4, for example, you could deploy OAS on the distributed networks, and SBR at the central site.

Note: In addition to SBR, OAS can forward authentication requests to legacy RADIUS servers which may already be in place on your network.

For each autonomous site or network, are you managing remote access in addition to WLAN access and security?

Choose OAS if you only need to manage WLAN access control and security. OAS can only manage users who connect via WLAN access points; it cannot manage remote users connecting via firewalls, VPN servers, dial-in servers, or other RADIUS clients.

Choose SBR if you need to manage access control and security for both WLAN and remote users. Users connecting via WLAN access points, firewalls, VPN servers, or dial-in servers can be authenticated via SBR.

Performance

The computational load associated with setting up EAP-TTLS and/or EAP-TLS connections is higher than that associated with standard remote access RADIUS transactions. This additional overhead is caused by the cryptographic work that the RADIUS server must do to set up the secure authentication tunnel, generate 128-bit per-session keys, and possibly re-key at specified intervals.

Consequently, depending on the volume of WLAN traffic, you may wish to add RADIUS servers to accommodate peak usage and avoid performance bottlenecks.

As previously mentioned, you can enhance performance while keeping costs down by deploying additional (lower-cost) OASs. Depending on how you've architected your WLAN, you can:

- Configure the additional OASs to handle authentication against Windows and set up the secure connection
- Configure them to forward non-Windows authentication requests to SBR, but still handle setting up the secure connection

Note that OAS and SBR are equally capable of handling the computational load associated with WLAN user authentication and security.

Reliability

You may be more concerned about the reliability of your WLAN connection than you are for remote access connections.

Some enterprises may perceive remote access to the network as less “mission critical” than LAN access. A traveling worker can always try again later to retrieve his email. However, a LAN user needs constant network access to get his or her job done.

For this reason, you may want to consider adding secondary RADIUS servers to ensure that your WLAN users are always able to access the network. Both OAS and SBR support this capability. Here, the access points are configured with a primary and a secondary RADIUS server. If the primary server is unavailable, the access point will query the secondary RADIUS server for authentication and security information. (This is a feature of the RADIUS specification.)

And, SBR GE supports additional reliability features when authentication information is stored in SQL or LDAP databases. These advanced reliability features include:

- Load balancing among databases
- “Failover” to back-up database if the primary database becomes unavailable
- Full support for reliable database configuration and reliable hardware configurations
- Guaranteed delivery of accounting log files

802.1X Client Considerations

While the focus of this paper has been to illustrate how to deploy RADIUS/AAA servers in support of secure WLAN access, another crucial aspect of WLAN security that bears mentioning is the 802.1X client that’s running on the user’s wireless device.

When choosing an 802.1X client, ensure that it offers the following capabilities:

- **Support for strong EAP authentication methods for maximum security** – including EAP-TTLS and/or EAP-TLS.
- Juniper Network’s Odyssey Access Client supports both EAP-TTLS and EAP-TLS.
- **Ease of deployment** – Ensure that you can easily roll out secure WLAN access to your entire population of WLAN users, regardless of platform or adapter card.

Juniper Network’s OAC provides unsurpassed multi-platform and multi-vendor support of 802.1X-compliant WLAN adapter cards. It also offers numerous auto-configuration tools so you can streamline large-scale deployments of WLAN access and mandate enterprise-level security.

- **Confidentiality of user credentials** – Ensure that corporate credentials stay private, whether a user is connecting on the WLAN or via a hotspot or service provider.

OAC fully protects users' identities between the client node and the trusted network, to protect their locational privacy against surveillance, undesired acquisition of marketing information, and other intrusions from monitoring and eavesdropping.

- **Multi-platform compatibility** – OAC runs on Windows XP, 2000, 98, ME, Windows Mobile 2003, and Pocket PC 2002 for compatibility in your network environment.

RADIUS Server Requirements

The choice of RADIUS server is a critical component of an 802.1X-based WLAN security solution.

Juniper Network's RADIUS servers – OAS and SBR – are appropriate for use on your 802.1X WLAN. They provide full support for strong WLAN protocols, have been time-tested on rigorous networks so are fully capable of handling the performance load associated with WLAN access, and reflect the technical excellence for which Juniper Network's products are known. In addition, they offer:

- **Enterprise-level performance** – so they can handle your peak WLAN or remote access traffic
- **Support for EAP, and strong authentication methods EAP-TTLS, EAP-PEAP, and/or EAP-TLS** – so you can rest assured that your network is protected against the known hazards of wireless computing, including dictionary attack on password, wireless eavesdropping, and other cryptographic attacks.
- **Reliability features** which meet your requirements, whether you're running a small business or global enterprise
- **Accounting**, with sophisticated features which let you easily and reliably track and document WLAN and remote access activity.
- **Flexibility** to support any security method or authentication scheme you implement on your network.

Conclusion

WLAN security based on the IEEE security standard 802.1X and strong authentication methods such as EAP-TTLS is an extremely scalable, distributable, and cost-effective way to move toward widespread deployment of WLAN access across your enterprise. Critical to this deployment is a RADIUS server, and Juniper Network's OAS and SBR provide the functionality, performance, and reliability you need in this mission-critical function. For more information, visit us at www.juniper.net.