

Capacity Planning for EAP-Enabled RADIUS Servers

September 2004

ComWare
5 rue de Rome
Immeuble Jean Monet
93561 Rosny-sous-Bois Cédex
01 48 94 32 01
<http://www.comware.fr>

Introduction

At one time, a RADIUS server was a niche application on your network, responsible only for managing the authentication of users connecting to your network over a dial-up or VPN connection. While its benefits were clear – simpler user management and enhanced security – the RADIUS server was likely not managing a high percentage of users.

This is no longer the case. With the emergence of the 802.1X port security protocol, the RADIUS server has become a critical component of the enterprise network infrastructure, managing access by substantially more users, connecting via a secure wireless or wired 802.1X link.

It also has an expanded role within these emerging access methods. For WLAN access, it must both authenticates users and set up the encrypted connection to secure the wireless link. For identity-based (wired 802.1X) access, it plays a vital role in directing users onto the appropriate VLAN.

So, as you deploy RADIUS servers in support of these new access methods, a key consideration is ensuring that the RADIUS servers you select have the capacity and reliability to support the increased traffic load and cryptographic requirements of these emerging access methods.

In fact, you are probably asking yourself: “How many RADIUS servers will I need?”

The goal of this white paper is to help you answer that question. It covers the following topics:

- The load requirements that each 802.1X-based access method places on the RADIUS server
- The variables that affect performance within each type of access, with guidelines for configuring their values
- Results of performance testing of Steel-Belted Radius, Funk Software’s leading RADIUS server that is fully EAP-capable

Throughout the paper, we also outline the trade-offs between performance and security, so you can judge the best approach for your network and your corporate security requirements.

Load Requirements of Each Access Method

A RADIUS server is called upon to manage user access via the following access methods:

- **Remote/VPN** – Here, the RADIUS server interacts with the VPN server(s) to authenticate users connecting from a remote location

- **Secure 802.1X-based WLAN access** – For WLAN access, the RADIUS server interacts with the WLAN access point or switch to authenticate the WLAN client and set up its secure connection
- **Identity-based (wired 802.1X) access** – Here, the RADIUS server interacts with the 802.1X-compatible switch to authenticate users to the network and direct them to the appropriate VLAN

The scope of this paper is to discuss the performance requirements imposed on a RADIUS server by 802.1X-based access. We are omitting performance considerations around managing remote/VPN access for two reasons:

- Managing remote/VPN access is relatively lightweight in terms of CPU requirements. For each user session, a RADIUS transaction is usually handled by a single authentication request and authentication response; RADIUS accounting records may also be logged. More significantly, very little cryptographic processing is required. So, regardless of your remote/VPN traffic load, it is safe to assume, therefore, that a single copy of high-performance RADIUS server such as Funk Software’s Steel-Belted Radius plus a back-up copy is sufficient to manage your remote/VPN authentication requirements.
- Enterprises typically deploy RADIUS servers which are managing 802.1X-based access separately from those managing remote/VPN access, so deployment decision points differ between the two access methods.

The following sections explore the performance implications of 802.1X-based access methods.

802.1X-Based WLAN User Authentication and Security

802.1X-based access places significant demands on a RADIUS server.

In the first place, your RADIUS server must be EAP-compliant, and needs to support secure EAP methods such as EAP-TTLS, EAP-PEAP, and EAP-TLS. (Steel-Belted Radius is fully EAP compliant, and supports all secure EAP methods.)

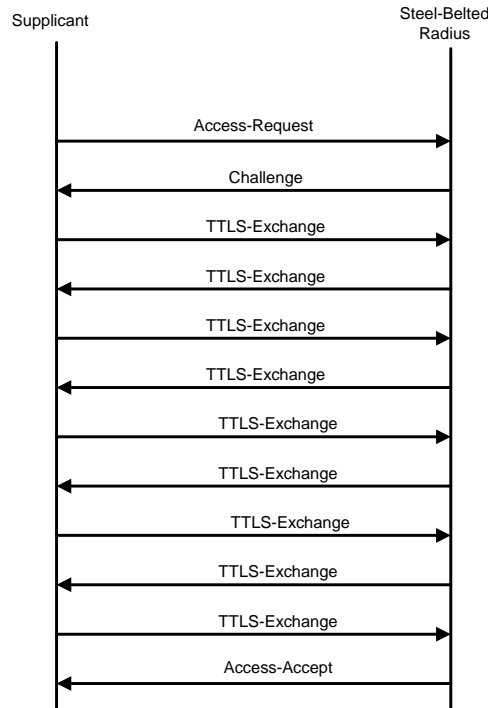
In addition, an 802.1X supplicant which supports strong EAP methods is required to run on all wireless clients. (Funk Software’s Odyssey Client is such a supplicant.)

For 802.1X-based WLAN access, the RADIUS server first determines how credentials will be exchanged for the authentication – i.e., what EAP method will be used. Once the RADIUS server and the 802.1X supplicant agree on an EAP method, authentication credentials are exchanged. This negotiation alone increases the number of RADIUS requests that the RADIUS server must process in order to authenticate the user. Once the authentication process is completed, the RADIUS server then must generate encryption keys and distribute them to the access point so that the secure wireless link can be established.

So, from a performance standpoint, 802.1X-based WLAN access is characterized both by an increased number of RADIUS transactions, and also by the requirement to perform CPU-intensive cryptographic computations.

This obviously directly affects the number of authentications that the RADIUS server can perform. The result is that the number of “802.1X authentications” per second that a RADIUS server can handle for is likely to be lower than the number of “traditional authentications” for remote/VPN access the same RADIUS server can handle.

Figure 1. This ladder diagram illustrates the steps required between a wireless client and RADIUS server to perform a full EAP-based user authentication, when a TLS-based EAP method is used.



With this in mind, your major considerations when determining how much RADIUS capacity you will need to manage 802.1X-based WLAN access are:

- **Traffic load** – How many WLAN users are you managing? Performance figures listed in the “Results of Steel-Belted Radius Performance Testing” section later in this document will allow you to gauge the impact your traffic load will place on RADIUS performance.
- **EAP method** – Your choice of EAP method will likely affect the performance of your RADIUS server
- **User re-authentication and session resumption** – How frequently will the user be re-authenticated, and will sessions be resumed?
- **Cipher suite** – What cipher suite and key length are you using?
- **RADIUS accounting** – Do you write RADIUS accounting records to a log file or SQL database?

EAP Method

A major factor that affects RADIUS server performance is the EAP method that you’ve implemented for secure WLAN access.

The most secure EAP methods are EAP-TTLS, EAP-PEAP, and EAP-TLS. These protocols provide credential security – i.e., your login credentials are not vulnerable as they cross the wireless link – and, when the encryption protocol WPA or WPA2 is in use, fully protect your session data. In addition, they provide mutual authentication of client and server. (For more information on EAP methods, see Funk Software’s white paper “Secure Authentication, Access Control, and Data Security on Wireless LANs.”)

While they provide strong security, these protocols do place more demands on the RADIUS server, because each uses certificates as part of the authentication process, which add CPU work to the authentication processing.

As you might expect, the more secure the protocol, the more its use will affect RADIUS server performance. Of course, most if not all enterprises gladly make this trade-off; the expense associated with adding RADIUS servers is considerably less than the expense associated with a security breach. Funk Software strongly recommends the use of these protocols.

The less secure EAP methods, EAP-MD5 and Cisco's LEAP, do not utilize certificates, and consequently have less of an impact on RADIUS server performance. While you will see better performance using these protocols, most organizations do not view these protocols as providing enterprise-class security. Funk Software recommends against the use of these protocols.

Keep in mind, too, that using multiple EAP methods can also negatively affect the performance of your RADIUS server, because it may require additional exchanges between the RADIUS server and the 802.1X supplicant to negotiate the appropriate EAP method to be used for authentication.

User Re-authentication and Session Resumption

One way that 802.1X solutions ensure enterprise-class security is to require the RADIUS server re-authenticate users at specified intervals, and as part of this process refresh their encryption keys.

This user re-authentication can take one of two forms:

- **Session resumption**, where the 802.1X client provides the information that it used the last time it was authenticated (or re-authenticated) to the network. Most 802.1X solutions allow you to set a session resumption interval. The stronger your encryption protocol, the longer that interval can be. For example, if you're using dynamic WEP, you should set your interval no longer than 1 hour; if you're using WPA, your interval can be 8 hours; for WPA2, your interval can be as long as 24 hours.
- **User re-authentication**, where the entire authentication process is performed, complete with certificate negotiation

A session resumption is triggered when any of the following events occurs:

- The wireless user moves and his connection is controlled by a different access point
- The access point times out the user's connection
- The 802.1X client is configured to resume to the session
- The session resumption interval set on the RADIUS server expires
- The user restarts his laptop

Session resumption, because it does not involve certificate negotiation, does not significantly affect the performance of the RADIUS server.

A user re-authentication is triggered when any of the following events occurs:

- The user moves and his user is controlled by a different RADIUS server

- The user re-authentication interval set on the RADIUS server expires

Because of the certificate negotiation required, user re-authentication places more demand on the RADIUS server.

All the TLS-based protocols (EAP-TTLS, EAP-PEAP and EAP-TLS) provide for session resumption. Provided that both the RADIUS server and the 802.1X supplicant permit session resumption, then the session resumption process, while still secure, is more efficient, taking fewer requests and lighter CPU load.

On Funk Software RADIUS servers, you can specify how long a session can be active before requiring a full re-authentication. The default Funk Software setting is 12 hours; you can specify any value that you wish.

The security trade-off associated with a long re-authentication interval is generally acceptable to most enterprises. With a long re-authentication interval, a security gap may occur if you de-authorize a user who is currently connected; the de-authorization won't take effect until the time specified for the de-authentication interval has elapsed.

When considering how many RADIUS servers you need to manage your WLAN, consider how mobile your user population is likely to be. For example, if you are managing a hospital WLAN, your wireless users may be quite mobile as they perform rounds, and their connections move from access point to access point. This type of use places more demands on a RADIUS server than for those environments where your users work wirelessly from their cubicles and may only roam once or twice per day.

Cipher Suite

When configuring all TLS-based protocols (EAP-TTLS, EAP-PEAP, and EAP-TLS), the strength of the cipher suite used and the length of the certificate key both affect RADIUS server performance.

A cipher suite is a cryptographic technique for authentication and data privacy between 802.1X client and RADIUS server. The TLS protocol supports a variety of cipher suites, including `TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA` and `TLS_RSA_WITH_RC4_128_MD5`.

Cipher suites depend on the type of certificate you install. If the installed certificate uses DSA, then only DSS cipher suites are used. If the installed certificate uses RSA, then only RSA algorithms are used.

All cipher suites provide good security; enhanced security is provided by those that provide *perfect forwarding secrecy*; these cipher suites are prefaced with "DHE" (Diffie-Hellman Ephemeral). Perfect forwarding secrecy provides a measure of added protection: even if a certificate is compromised, previous sessions encrypted with keys developed using that certificate are not compromised. In other words, if you have been using the same server certificate for years to perform EAP-TTLS authentication and key generation, and then eventually its private key is revealed, an eavesdropper who recorded sessions prior to revelation of the private key still cannot decrypt those sessions, even though the private key is known.

With the DHE cipher suites, the RADIUS server must provide a set of cryptographic parameters, including a large prime number. (For maximum security, Funk Software RADIUS servers create a new prime number daily.)

As you probably expect, the larger the prime number, the greater the security – but the longer it takes to perform the cryptographic operation. Unless you have corporate guidelines that indicate otherwise, choose a prime number that is 1024 bits, the default setting of Funk Software RADIUS servers.

The length of the certificate key also affects RADIUS server performance. The length of the key is a characteristic of the certificate you choose to use; the longer the key, the more work for the RADIUS server.

RADIUS Accounting

Enabling RADIUS accounting will increase the load on your RADIUS server.

For each user authentication, one accounting START record and one accounting STOP record are generated. In addition, when a user roams from access point to access point, a STOP record will be generated for the access point being left, and a START record will be generated for the one newly accessed.

802.1X-Based Wired User Authentication

From a RADIUS server performance standpoint, identity based (wired 802.1X) access places the same demands on a RADIUS server as 802.1X-based wireless access, with one notable exception. In wired 802.1X access, users do not roam from access point to access point. Hence, the demands placed by session resumption on a RADIUS server in a wireless environment are not made in a wired 802.1X environment.

Results of Steel-Belted Radius Performance Testing

To test the EAP performance of Steel-Belted Radius, under the following conditions:

- **RADIUS server:** Steel-Belted Radius v4.71
- **802.1X supplicant:** Odyssey Client
- **Platform:** 2GHz Windows XP workstation
- **EAP method:** EAP-TTLS
- **Session resumption:** Enabled
- **Cipher suite:** default cipher suite (TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA) and default key length
- **RADIUS accounting:** Not enabled

Under these conditions, Steel-Belted Radius performed approximately 50 full 802.1X user *authentications* per second. (As we've described before, a user authentication occurs after all EAP transactions have been completed and the RADIUS server has issued its Access-Response message.)

Because they operate similarly, we expect that EAP-PEAP, EAP-TLS, and EAP-FAST (in secure mode), will produce similar performance numbers on the same platform.

Our testing also showed that Steel-Belted Radius could perform approximately 400 *session resumptions* per second on the same platform.

If we changed cipher suites (from TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA to TLS_RSA_WITH_RC4_128_MD5) we noticed a significant increase in both full authentications per second and sessions resumption rates.

Steel-Belted Radius Deployment Recommendations

These Steel-Belted Radius performance numbers illustrate that it is more than capable of handling the transaction and cryptographic load associated with EAP-based authentication.

We recommend that, for EAP-based authentication, you distribute Steel-Belted Radius in pairs (primary and back-up), on an administrative domain basis. Doing so ensures reliable network connectivity for your users – i.e., their access to the network won't be at the mercy of an unreliable link back to the central network operations center – and distributes the computationally intense EAP transactions across multiple RADIUS servers, to optimize performance.

For additional deployment guidelines, see Funk Software's white paper "Architecting Your 802.1X-Based WLAN Deployment."

Reliability

It's worth noting that, you may be more concerned about the reliability of your EAP-based connections, in particular during peak traffic periods (e.g., first thing in the morning when everyone is booting up his laptop).

For this reason, we recommend that you add secondary Steel-Belted Radius servers to ensure that your 802.1X users are always able to access the network. 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.

And, Steel-Belted Radius/Global Enterprise Edition 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

Conclusion

Moving to 802.1X-based WLAN and wired access carries with it numerous benefits – foremost among them, increased security, better user management, and lower . However,

as we've seen, these new access methods place additional demands on your RADIUS server, making your choice of RADIUS server more critical than ever. It needs to be able to manage your peak traffic periods, set up the level of security you need, and reliably handle mobile users.

Funk Software's RADIUS server Steel-Belted Radius is an enterprise-class RADIUS server that is more than able to manage whatever type of access or volume of users you require. It provides the fastest performance available, with the ability to handle at a minimum 50 WLAN user authentications per second. In combination with its powerful functionality – its market-leading multi-vendor support, its ability to query the widest number of authentication databases including Active Directory, LDAP, and token systems, and its powerful reporting capabilities – it's more than capable of acting as the linchpin of your network access security policies.

We look forward to working with you.

ComWare

5 rue de Rome

Immeuble Jean Monnet

93561 Rosny-sous-Bois Cédex

01 48 94 32 01

<http://www.comware.fr>