

WHITE PAPER: 802.1X AUTHENTICATION & EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)

Written By: Philip Kwan
May 2003

WHITE PAPER: 802.1X AUTHENTICATION & EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)



Summary

The IronShield White Paper: 802.1X Authentication & Extensible Authentication Protocol document is designed to help network and security administrators understand how 802.1X, EAP, and the EAP authentication protocols are used to secure network access. Foundry devices support 802.1X Port Authentication that makes use of EAP authentication methods to secure network access.

IronShield Security is not meant to replace Data Security infrastructures. With careful planning and implementation, IronShield Security features can help improve Network Security and enhance Data Security where it's needed.

Contents

IRONSHIELD SECURITY	3
AUDIENCE	3
RELATED PUBLICATIONS.....	3
IEEE 802.1X AUTHENTICATION	4
EXTENSIBLE AUTHENTICATION PROTOCOL (EAP).....	5
THE ADVANTAGES OF EAP	6
EAP AUTHENTICATION PROCESS	6
EAP MESSAGE EXCHANGE	8
EAP AUTHENTICATION PROTOCOLS.....	9
EAP TECHNOLOGY REFERENCES	11
SUMMARY.....	11

WHITE PAPER: 802.1X AUTHENTICATION & EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)



IronShield Security

Foundry's IronShield Security "Best Practices" and "White Papers" serves as a guide to assist network and security designers in architecting and applying Foundry security features in their networks. Modern enterprise security is applied in layers – Defense in Depth. Consideration must be given to all the various layers with a full understanding of what threats are possible at each layer before implementing a defense strategy. By applying security in multiple layers, the defense is strengthened and vulnerabilities in one layer will not likely lead to successful attacks of corporate resources. The goal is to make it harder to attack your network by layering security chokepoints.

These practices should accompany your Security and Computer Usage Policies, not replace them. Applying the steps outlined in the "Best Practices" and "White Paper" guides does not guarantee that attacks will not be successful against your security defenses and network resources. The best security design is dynamic. It must be coupled with a strong security policy, proactive network monitoring, diligent network and security staff that are working to stay on top of security alerts and system software upgrades and patches. Enterprise data security is always changing and growing with the advent of new security threats. Thorough, rigorous, and continuous inspection of all security components and processes will help you keep on top of the enterprise network.

IronShield Security documents are specifically written to work with Foundry products and work in conjunction with related Foundry documentation. Reference to other Foundry documentation is made with regards to command syntax and general feature information.

Audience

IronShield Security "Best Practices" and "White Papers" are designed to help the personnel responsible for designing and configuring the network and security components of an enterprise network. The topics discussed are at an intermediate to advanced level and assumes a good understanding of TCP/IP and related technologies.

Related Publications

The following Foundry Networks documents supplement the information in this guide.

IronShield Best Practices: Hardening Foundry Routers and Switches – provides a detailed explanation of how Foundry devices can be protected from unauthorized access and other security related issues.

IronShield Best Practices: Enhancing Internal Network Security – provides a detailed explanation of how to implement Foundry IronShield Security features to harden internal network infrastructures.

IronShield White Paper: 802.1X Port Authentication With LDAP – provides a detailed explanation of how to implement Foundry's 802.1X Port Authentication feature with an LDAP directory.

IronShield White Paper: 802.1X Port Authentication With Active Directory – provides a detailed explanation of how to implement Foundry's 802.1X Port Authentication feature with Microsoft's Active Directory.

IEEE 802.1X Authentication

The IEEE 802.1X standard was originally developed to address open access in 802 Local Area Networks (LAN). Traditionally, LANs allowed access to all devices that can obtain a network connection to the network switches. Both authorized and unauthorized users were able to access information as long as the network port was not disabled. With DHCP services providing the necessary IP information, connecting to the LAN was even more simple and straightforward. To address the security concerns of unauthorized access, the IEEE developed the 802.1X standard to allow networking vendors to create a mechanism to control network access at the port level. 802.1X port-based security controls network access by requiring users to authenticate themselves before gaining access to the network. Through the use of authentication servers and standard messaging routines, a multi-vendor framework can be developed to secure access to the LAN.

802.1X makes use of the Extensible Authentication Protocol (EAP) to define how authentication messages are to be exchanged between the various network components – clients (supplicants), switches or wireless access points (authenticators), and authentication servers. The EAP standard does not define the security protocols or mechanisms for the authentication process. It only defines how the authentication messages are to be exchanged between the client, authenticator, and authentication server. For securing the authentication process, EAP supports an open architecture allowing multiple EAP authentication protocols to be used.

The advantages of using 802.1X port-based network authentication include:

- Multi-vendor standard framework for securing the network.
- Improves security through session based dynamic keying of encryption keys.
- Standards based message exchange based on EAP.
- Uses open security architecture allowing the addition of newer authentication methods without replacing network equipment.
- Uses industry standard authentication servers (example: RADIUS).
- Centralizes management for network access.
- Uses existing user security information, if necessary.
- Supports both wired and wireless networks.

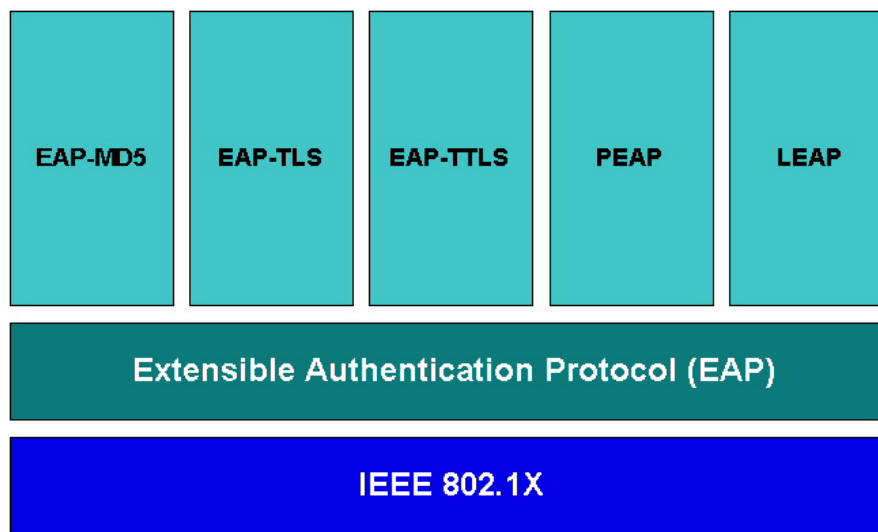


Figure 1. 802.1X Authentication Components

WHITE PAPER: 802.1X AUTHENTICATION & EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)



Extensible Authentication Protocol (EAP)

RFC 2284 – Point-to-Point Extensible Authentication Protocol (EAP) is a mechanism that defines a standard message exchange between devices using an agreed upon authentication protocol. EAP is used as one of the base technologies to allow both wired and wireless clients to authentication to network devices. Because the EAP protocol does not require the IP protocol to communicate (it uses the link layer), it can transport messages between devices without the EAP clients requiring an IP Address. EAP is effective in networks that rely on DHCP for their IP addresses - as the client will not be able to retrieve an IP address from the DHCP server until they are authenticated to the network and given a network connection.

EAP by itself cannot be used as an authentication protocol - as it is merely a standard by which to exchange authentication messages between a client and an authentication server. EAP supports a number of authentication protocols to provide security during the authentication process. The security features and encryption strength vary with each EAP authentication protocol allowing companies to choose which EAP authentication protocol makes the most sense for their 802.1X application.

Some of the more common authentication protocols supported by EAP include:

- EAP-MD5 (Message-Digest 5)
- EAP-TLS (Transport Level Security)
- EAP-TTLS (Tunneled TLS)
- EAP-PEAP (Protected EAP Protocol)
- Cisco LEAP (Lightweight EAP Protocol)

EAP was originally developed for use with PPP in RFC 2284 and has since been widely deployed with IEEE 802 on both wired and wireless networks. With the growing popularity of wireless networks, securing the authentication process between the client, authenticator, and authentication server have become a high priority. Security concerns that were once benign on wired networks have become challenges and open security holes on wireless networks.

Depending on the EAP authentication protocol used, 802.1X authentication can help solve the following security issues:

Dictionary Attack Attacker obtains the challenge and response message exchange from a password authentication session and uses a brute force method to crack the password. 802.1X solves this type of attack with the use of TLS tunnels to protect the username and password exchanges between the client and the authenticator.

Session Hijack Attack Attacker obtains the packets passed between the client and the authenticator and recovers the identity information of the client. It forces the “real” client off the network through a form of DoS attack and impersonates the client to continue the conversation with the authenticator. 802.1X’s authentication abilities with dynamic session-based keys (with user configurable re-keying) can help encrypt the conversation between the client and authenticator to thwart Hijacking attacks.

Man-in-the-Middle Attack Attacker obtains the necessary information from the client and the authenticator and inserts their host between the two. The attacker’s host becomes the “middle man” and has access to the packets that are passed between the client and the authenticator. Through 802.1X’s authentication and dynamic session-based keys (with user configurable re-keying), the data stream between the client and authenticator is encrypted to prevent Man-in-the-Middle attacks.

WHITE PAPER: 802.1X AUTHENTICATION & EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)



The Advantages Of EAP

EAP specifies how a standard messaging exchange is setup between a client, authenticator, and authentication server and does not specify the actual authentication protocol. As such, it has several advantages:

- EAP allows multiple authentication protocols to be supported without having to pre-negotiate a specific one.
- Its flexibility to support multiple authentication protocols without requiring the authenticator to be programmed with the specific authentication mechanisms. EAP allows the authentication server to control which authentication protocols are supported between itself and the client without the authenticator being fully configured with the authentication protocol. The authenticator can act as a pass-through device between the Client and the authentication server for the authentication protocol (pass-through is optional).
- The authenticator may authenticate local clients while at the same time, act as a pass-through for non-local clients using authentication protocols it doesn't support locally.
- Having a separate authenticator and authentication server working in pass-through mode allows standard messaging to be developed and simplifies credential management. The authenticator only determines the outcome of the authentication from the Access-Accept or Reject message supplied by the authentication server. The authentication outcome is not affected by the contents of the EAP packets - which may be vulnerable to attacks, manipulation, etc.

EAP Authentication Process

The components of an 802.1X EAP enabled network consists of three parts: Client/Supplicant, Authenticator, Authentication Server.

Client/Supplicant

The client, or supplicant, is the device that needs to be authenticated. The client supplies the authentication credentials (such as certificate or username and password information) to the authenticator and requests access to the network. The client uses EAP Over LAN (EAPOL) to talk to the authenticator. Examples of clients include workstations (both wired and wireless), PDA's, and wireless Voice Over IP phones.

Authenticator

The authenticator is the device performing the 802.1X port-level security and it controls access to the network. The authenticator receives the user credentials from the client, passes it onto the authentication server, and performs the necessary block or permit action based on the results from the authentication server. Depending on the EAP authentication protocol negotiated between the client and authentication server, the authenticator relays the necessary messages between the client and authentication server to facilitate the authentication request.

The authenticator can operate in two different modes: it can perform the EAP messaging functions locally and communicate with the authentication server using the RADIUS protocol or it can operate as an EAP pass-through device to allow the authentication server to perform the necessary EAP protocol messaging functions. Examples of authenticators include network switches and routers (wired network application) and wireless access points or wireless gateway switches.

WHITE PAPER: 802.1X AUTHENTICATION & EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)

Authentication Server

The authentication server validates the user's credential information from the client and specifies whether or not access is granted. The authentication server also specifies the EAP authentication protocol to be used between the client and itself and may specify optional parameters once access is granted. Optional parameters may be used to authorize access to specific areas of the network using dynamic VLAN or user policies. Examples of authentication servers include RADIUS and Active Directory servers.

Before the Client is authenticated, the authenticator sets the network port to the **uncontrolled** (unauthorized) state and only allows EAP/EAPOL authentication messages to be exchanged between the client and the authentication server. All other traffic is blocked. When the client is successfully authenticated and authorized, the **controlled** port is set to the authorized state to grant network access.

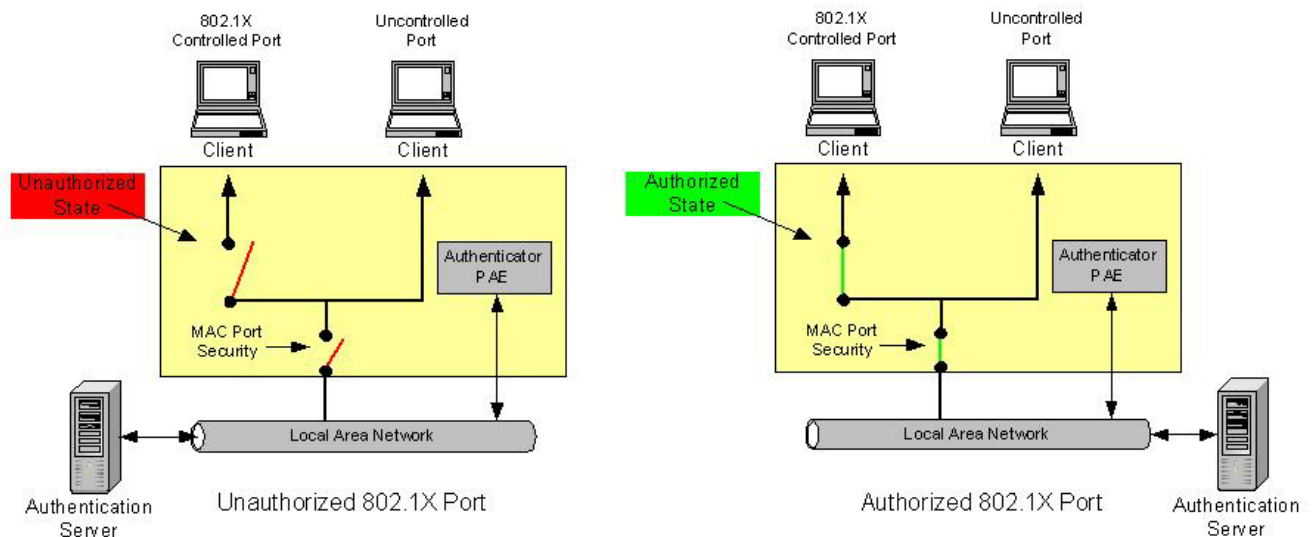


Figure 2. 802.1X Port Authentication

802.1X port authentication can be coupled with MAC port security for tighter access control (see Figure 2). With MAC port security enabled, the network port can control access through enforcement of the client's MAC address as well as the user's 802.1X credentials.

EAP Message Exchange

The EAP standard creates a common messaging structure to authenticate the client to the network. Depending on the authentication protocol agreed upon by the client and authentication server, the exact details of the message exchange might vary slightly.

Figure 3 illustrates the general conversation that occurs between an EAP client, authenticator, and authentication server.

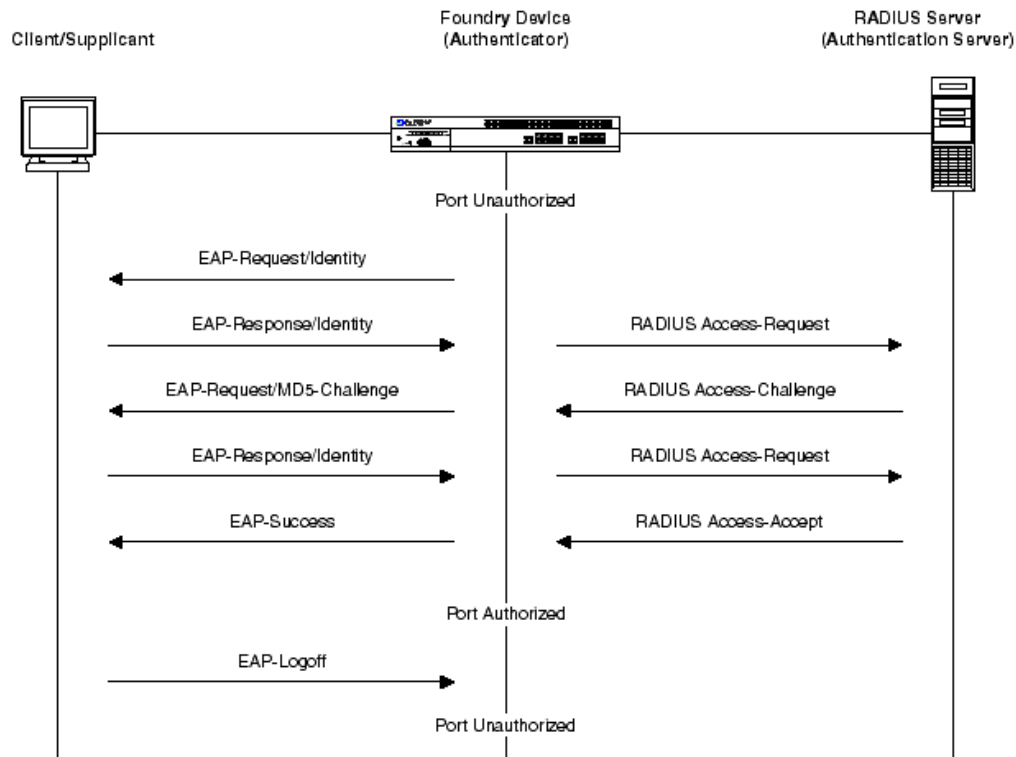


Figure 3. Port Authentication Process

1. The EAP client connects to the network and tries to access information on the network. Remember that a valid IP address is not required to transfer EAP messages between the client and the authenticator. The communication is performed using the EAP over LAN (EAPOL) protocol.
2. The authenticator responds to the client by asking for its identity using EAPOL.
3. The client responds to the authenticator with its identity information using EAPOL.
4. The authenticator forwards the client's identity information to the authentication server using the necessary protocol agreed upon by the authentication server and the authenticator or client. The EAP standard supports multiple backend authentication servers and RADIUS is currently the most widely supported by most vendors. Figure 3 illustrates the procedure using RADIUS as the authentication server.

WHITE PAPER: 802.1X AUTHENTICATION & EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)



5. The authentication server responds with a challenge to the authenticator and will specify the EAP authentication type supported by the authentication server. This message is transmitted over the RADIUS protocol back to the authenticator.
6. The authenticator forwards the challenge back to the client with the authentication type requested by the authentication server using EAPOL.
7. The client examines the challenge and determines if it can support the requested EAP authentication protocol. If it cannot support the authentication type requested by the authentication server, the client will issue a NAK request and try to negotiate an alternative authentication method. If the client can support the authentication type requested by the authentication server, it responds with its credential information using EAPOL.
8. The authenticator relays the client's credentials to the authentication server using the RADIUS protocol.
9. If the client's credentials are valid, the authentication server authenticates and authorizes the client. Otherwise, the client is rejected and the appropriate RADIUS Access-Accept or Access-Reject message is sent back to the authenticator using the RADIUS protocol.
10. The authenticator receives the RADIUS Access-Accept or Access-Reject message and configures the network access accordingly.

EAP Authentication Protocols

EAP by itself cannot protect the authentication message exchange between the client, authenticator and authentication server. In order to secure the message exchange, an EAP authentication protocol is necessary. The commonly used EAP authentication protocols include:

EAP-MD5 RFC 1994

EAP-MD5 is the base security requirement in the EAP standard and uses username and passwords as the authentication credentials. EAP-MD5 protects the message exchange by creating a unique "fingerprint" to digitally sign each packet to ensure that the EAP messages are authentic. EAP-MD5 is very "light weight" and performs its operations very quickly, making it easy to implement and configure. EAP-MD5 does not use any PKI certificates to validate the client or provide strong encryption to protect the authentication messages between the client and the authentication server. This makes the EAP-MD5 authentication protocol susceptible to session hijacking and man-in-the-middle attacks. EAP-MD5 is best suited for EAP message exchanges in wired networks where the EAP client is directly connected to the authenticator and the chances of eavesdropping or message interception is very low. For wireless 802.1X authentication, stronger EAP authentication protocols are used.

EAP-TLS RFC 2716

EAP-TLS (Transport Level Security) provides strong security by requiring both client and authentication server to be identified and validated through the use of PKI certificates. EAP-TLS provides mutual authentication between the client and the authentication server and is very secure. EAP messages are protected from eavesdropping by a TLS tunnel between the client and the authentication server. The major drawback of EAP-TLS is requirement for PKI certificates on both the clients and the authentication servers - making roll out and maintenance much more complex. EAP-TLS is best suited for installations with existing PKI certificate infrastructures. Wireless 802.1X authentication schemes will typically support EAP-TLS to protect the EAP message exchange. Unlike

WHITE PAPER: 802.1X AUTHENTICATION & EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)



wired networks, wireless networks send their packets over open air making it much easier to capture and intercept unprotected packets.

EAP-TTLS Internet-Draft

Proposed by Funk and Certicom, EAP-TTLS (Tunneled TLS) is an extension of EAP-TLS and provides the benefits of strong encryption without the complexity of mutual certificates on both the client and authentication server. Like TLS, EAP-TTLS supports mutual authentication but only requires the authentication server to be validated to the client through a certificate exchange. EAP-TTLS allows the client to authenticate to the authentication server using usernames and passwords and only requires a certificate for the authentication servers. EAP-TTLS simplifies roll out and maintenance and retains strong security and authentication. A TLS tunnel can be used to protect EAP messages and existing user credential services such as Active Directory, RADIUS, and LDAP can be reused for 802.1X authentication. Backward compatibility for other authentication protocols such as PAP, CHAP, MS-CHAP, and MS-CHAP-V2 are also provided by EAP-TTLS. EAP-TTLS is not considered full proof and can be fooled into sending identity credentials if TLS tunnels are not used. EAP-TTLS is best suited for installations that require strong authentication without the use of mutual certificates. Wireless 802.1X authentication schemes will typically support EAP-TTLS.

PEAP Internet-Draft

Protected EAP Protocol (PEAP) is an Internet-Draft that is similar to EAP-TTLS in terms of mutual authentication functionality and is currently being proposed by RSA Security, Cisco and Microsoft as an alternative to EAP-TTLS. PEAP addresses the weaknesses of EAP by:

- protecting user credentials
- securing EAP negotiation
- standardizing key exchanges
- supporting fragmentation and reassembly
- supporting fast reconnects

PEAP allows other EAP authentication protocols to be used and secures the transmission with a TLS encrypted tunnel. It relies on the mature TLS keying method for it's key creation and exchange. The PEAP client authenticates directly with the backend authentication server and the authenticator acts as a pass-through device, which doesn't need to understand the specific EAP authentication protocols. Unlike EAP-TTLS, PEAP doesn't natively support username and password authentication against an existing user database such as LDAP. Vendors are answering this need by creating features to allow this. PEAP is best suited for installations that require strong authentication without the use of mutual certificates. Wireless 802.1X authentication schemes will typically support PEAP.

Cisco LEAP

Cisco's Lightweight EAP Protocol (LEAP) was developed in November 2000 to address the security issues of wireless networks. LEAP is a form of EAP that requires mutual authentication between the client and the authenticator. The client first authenticates itself to the authenticator and then the authenticator authenticates itself to the client. If both authenticate successfully, a network connection is granted. Unlike EAP-TLS, LEAP is based on username and password schemes and not PKI certificates, simplifying roll out and maintenance. The drawback is that it is proprietary to Cisco and has not been widely adopted by other networking vendors. LEAP is best suited for wireless implementations that support Cisco AP's and LEAP compliant wireless NIC cards.

WHITE PAPER: 802.1X AUTHENTICATION & EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)



As the wireless security requirements push the development of 802.1X and secure data transport, newer EAP authentication protocols will be developed to answer the security issues. With IEEE 802.1X and the EAP standard, these new EAP security protocols should continue to work with existing hardware.

EAP Technology References

For more information on 802.1X and EAP technology, refer to the following web sites and documents:

EAP	http://www.ietf.org/rfc/rfc2284.txt
EAP-MD5	http://www.faqs.org/rfcs/rfc1994.html
EAP-TLS	http://www.faqs.org/rfcs/rfc2716.html
EAP-TTLS	http://www.watersprings.org/pub/id/draft-ietf-pppext-eap-ttls-02.txt
PEAP	http://www.globecom.net/ietf/draft/draft-josefsson-pppext-eap-tls-eap-02.html
LEAP	http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1515_pp.htm

Summary

Network security is complex and is constantly changing. It requires careful planning, implementation, and monitoring to achieve its goals. To help address the security issues of unauthorized access, 802.1X was developed to provide a standard mechanism for port-based authentication. Through the use of standard authentication messaging protocols provided by EAP, multi-vendor solutions are being created to support network authentication. With EAP's flexibility to support multiple EAP authentication protocols, companies can select the right level of authentication security to meet their environment's security requirements and upgrade to newer solutions in the future without sacrificing their hardware investment.

Foundry Networks offers many network-based security features in its portfolio of Layer 2, 3, and 4 – 7 products. By using IronShield Security features such as 802.1X Port Authentication and 802.1X Dynamic VLANs from Foundry Networks, IT and Security managers can implement the necessary security features to layer security defenses at different points of their network. Coupled with the Port Security feature, defending against unauthorized access becomes even more powerful with Foundry's switch products. Each IronShield Security feature can be layered with other security features to achieve the desired security results, allowing companies to not only control what and who gains network access, but also where they can venture.

For more information on products and features offered by Foundry Networks, visit its corporate WEB site at:

<http://www.foundrynet.com>

WHITE PAPER: 802.1X AUTHENTICATION & EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)



Foundry Networks, Inc.
Headquarters
2100 Gold Street
P.O. Box 649100
San Jose, CA 95164-9100

U.S. and Canada Toll-free: (888) TURBOLAN
Direct telephone: +1 408.586.1700
Fax: 1-408-586-1900
Email: info@foundrynet.com
Web: <http://www.foundrynet.com>

Foundry Networks, BigIron, EdgeIron, FastIron, NetIron, ServerIron, and the "Iron" family of marks are trademarks or registered trademarks of Foundry Networks, Inc. in the United States and other countries. All other trademarks are the properties of their respective owners.

© 2003 Foundry Networks, Inc. All Rights Reserved.