



INFORMATION TECHNOLOGY SERVICES

Adding Intelligence to the Network

An Enterprise View

INFRASTRUCTURE SERVICES/INFRASTRUCTURE ARCHITECTURE

Key Takeaways

◆ Infrastructure attributes

- Enables business needs
- Becoming more complex
- Fewer “clean, easy” introductions/updates
- Issue resolution can become more complex

◆ Success enablers

- Integrated strategy
- Proper preparation of operations support
- End to end testing
- Improved troubleshooting skills
- Strong policy agreement & process support

Add Intelligence to the Network?

- ◆ Debate is not new

- ◆ Developments in

 - Technology

 - Marketplace

have dramatically increased options

- ◆ Many vendors & technologies - new options every day!

 - Economical bandwidth improvements

 - Supplier: Carrier vs Enterprise

 - Location: Network vs Client

If are responsible, make sure your voice is heard!

Intelligence in the Network has Proliferated

- ◆ Caching
- ◆ Filtering
- ◆ Compression
- ◆ Load Balancing
- ◆ Remote Access
- ◆ Single Sign On & Identity Management Technologies
- ◆ Routing & Switching
- ◆ Firewalls
- ◆ Access Control Systems & Authentication Engines
- ◆ Directory Services
- ◆ Encryption
- ◆ DHCP, DNS & WINS

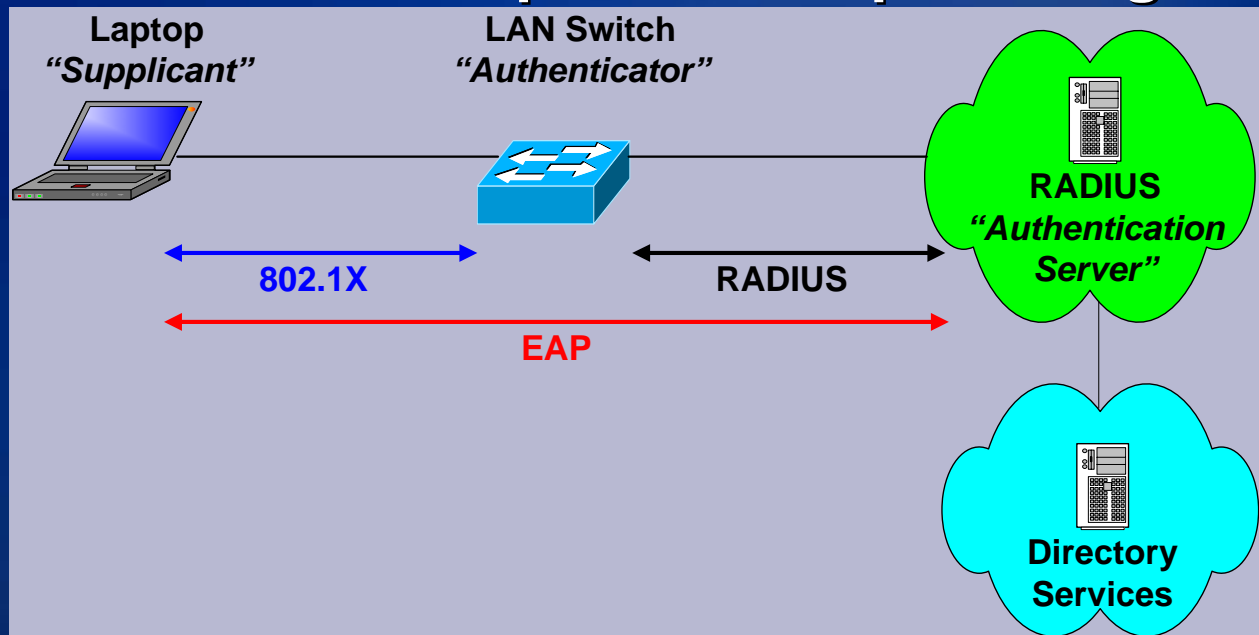
***Client interactions complicate troubleshooting –
Fewer problems are “stand alone”!***



802.1X Wired Case Study

What is 802.1X?

- ◆ An IEEE 802.1X standard
- ◆ An access control and authentication protocol
- ◆ Restricts unauthorized clients/machines from connecting to LAN switch ports
- ◆ Authentication servers verify each client/machine that connects to a switch port before providing it access

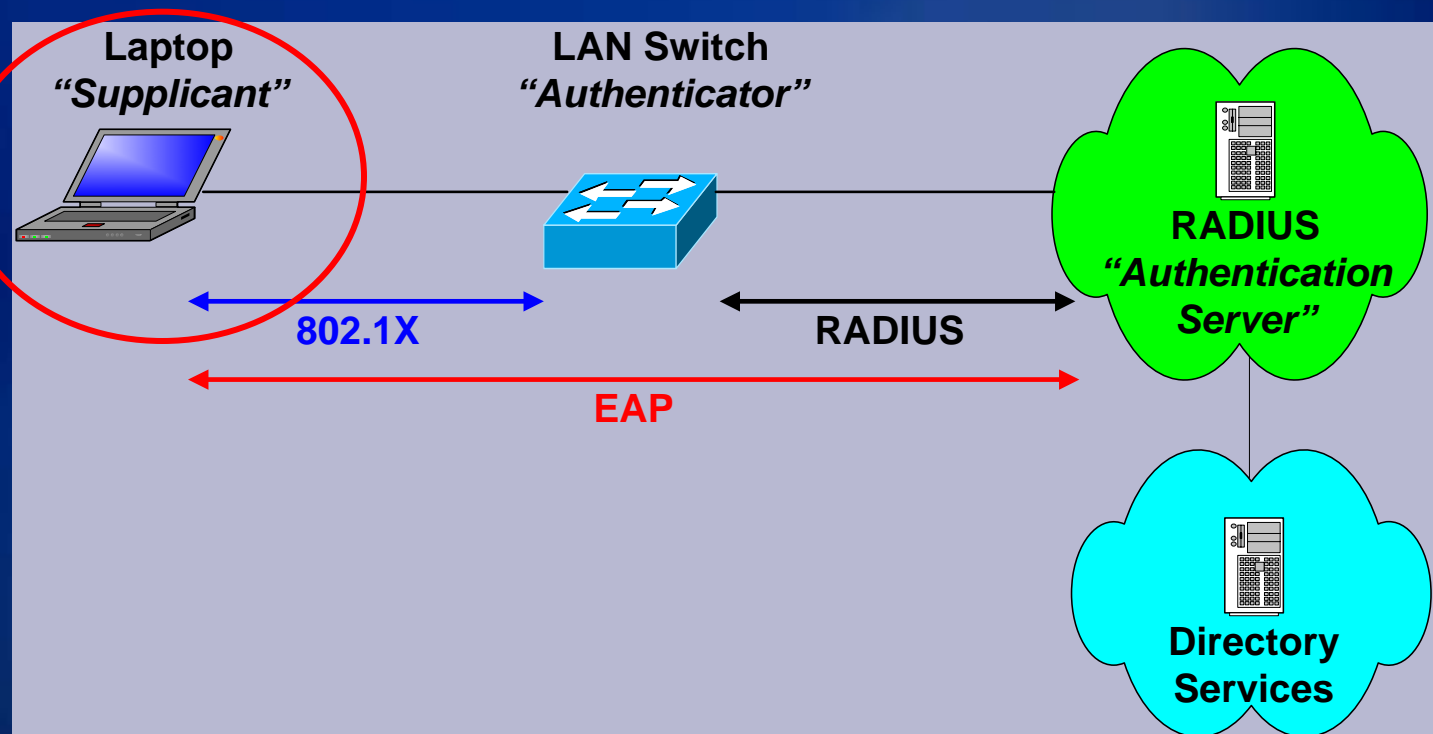


Why 802.1X?

- ◆ Desire to secure data network via Directory Services authentication
- ◆ Lockout rogue or nonstandard systems
- ◆ Provide automated guest access
- ◆ Sets the foundation for NAC?

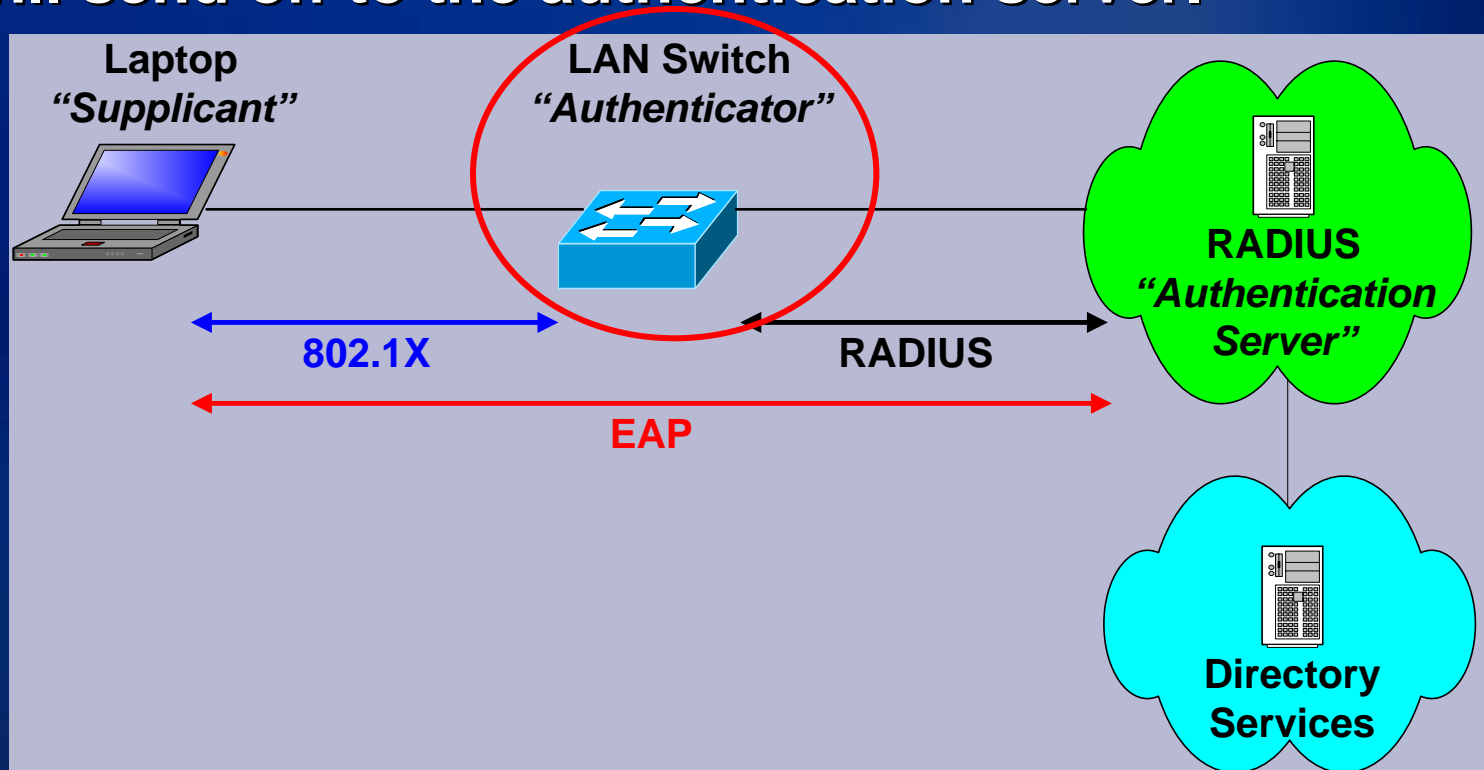
Technology Definition - Supplicant

- ◆ The host or client - must be running 802.1X compliant software
- ◆ The supplicant/client requests access to the LAN and can respond to requests from the switch (or authenticator)



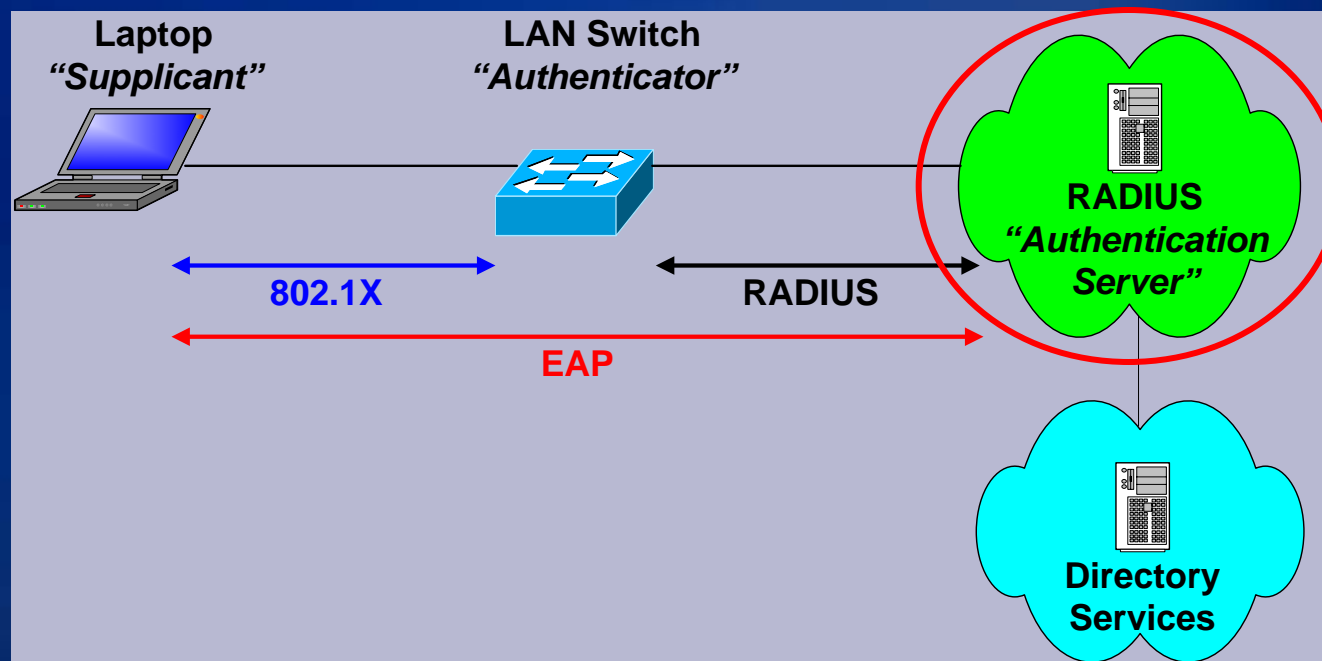
Technology Definition - Authenticator

- ◆ LAN switch - speaks the 802.1X language on behalf of the client with the backend authentication server
- ◆ The client will send EAPOL frames to the switch who will in turn encapsulate EAP into a Radius frame and will send off to the authentication server.



Technology Definition - Authentication Server

- ◆ RADIUS device - performs the actual authentication of the client
- ◆ The authentication server validates the identity of the client and informs the authenticator (switch), which allows the client access to the switch
- ◆ Authentication server accesses Directory Services



Challenges to an 802.1X Deployment

- ◆ 802.1X can be a complex solution to deploy
- ◆ Can be “disruptive” at several levels
- ◆ **Assessment**
 - Industry Alignment
 - Deployment Approach
 - Operations & Support

Industry Alignment

- ◆ **Limited identifiable wired industry deployments**
 - Can introduce significant cultural changes
 - Can increase and reduce risk at same time
- ◆ **Industry agrees 802.1X**
 - Is most secure authentication approach
 - Should be long term goal for organizations
- ◆ **Used extensively in wireless environments**

Where on the technology adoption curve do you wish to be?

Design Considerations

To better position 802.1X, consider the following:

- ◆ **Ensure an active DR solution and test for integrity**
- ◆ **Identify Enterprise-wide shutoff capabilities**
- ◆ **Check availability of Authentication Failure and Guest VLANs**
 - Can address more use cases
 - May improve support options if available on vendor hardware/software
- ◆ **Analyze and utilize full vendor feature set**
 - E.g., to improve security Multi Authentication feature can be used to address hubs, etc.

Operations & Support

- ◆ **Are workstations “locked down”?**
 - Users may configure themselves out of “compliance”
- ◆ **End to end testing must include:**
 - 802.1X testing
 - All client and network components
 - Changes to any of the above
- ◆ **Support issues may become more complex**
- ◆ **Process required for non standard users and/or workstations?**
- ◆ **Exceptions may require manual intervention and/or workarounds**

Alternative Approaches?

- ◆ Workstation compliance solutions have developed significantly over the last 3 years
- ◆ Combined with specific VLAN scoping, may be able to effectively match 802.1X functionality
- ◆ Is 802.1X a foundation for NAC solutions?

Conclusions Going Forward

- ◆ Consider enterprise requirements & priorities
- ◆ Utilize design options as appropriate
- ◆ Prepare operations support
- ◆ Integrate testing
- ◆ Improve troubleshooting skills
- ◆ Ensure policy agreement and process support
 - Should include Approval & Communications
 - Especially important for potentially “disruptive technologies”



Presenter's contact details

Peter J. Hughes

KPMG LLP

(201) 505-6084

pjhughes@kpmg.com

<http://www.kpmg.com>

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.