802.1X vs VPNs for Edge Access Security

Paul Congdon

Chief Architect

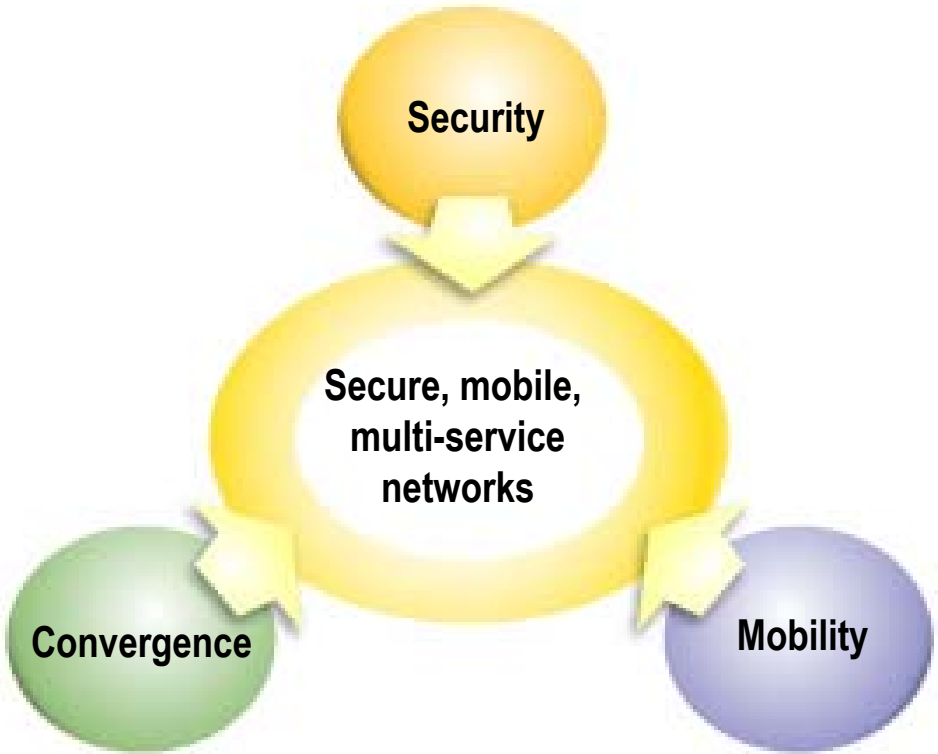
ProCurve Networking Business

Hewlett Packard Company

HP WORLD 2003

Solutions and Technology Conference & Expo

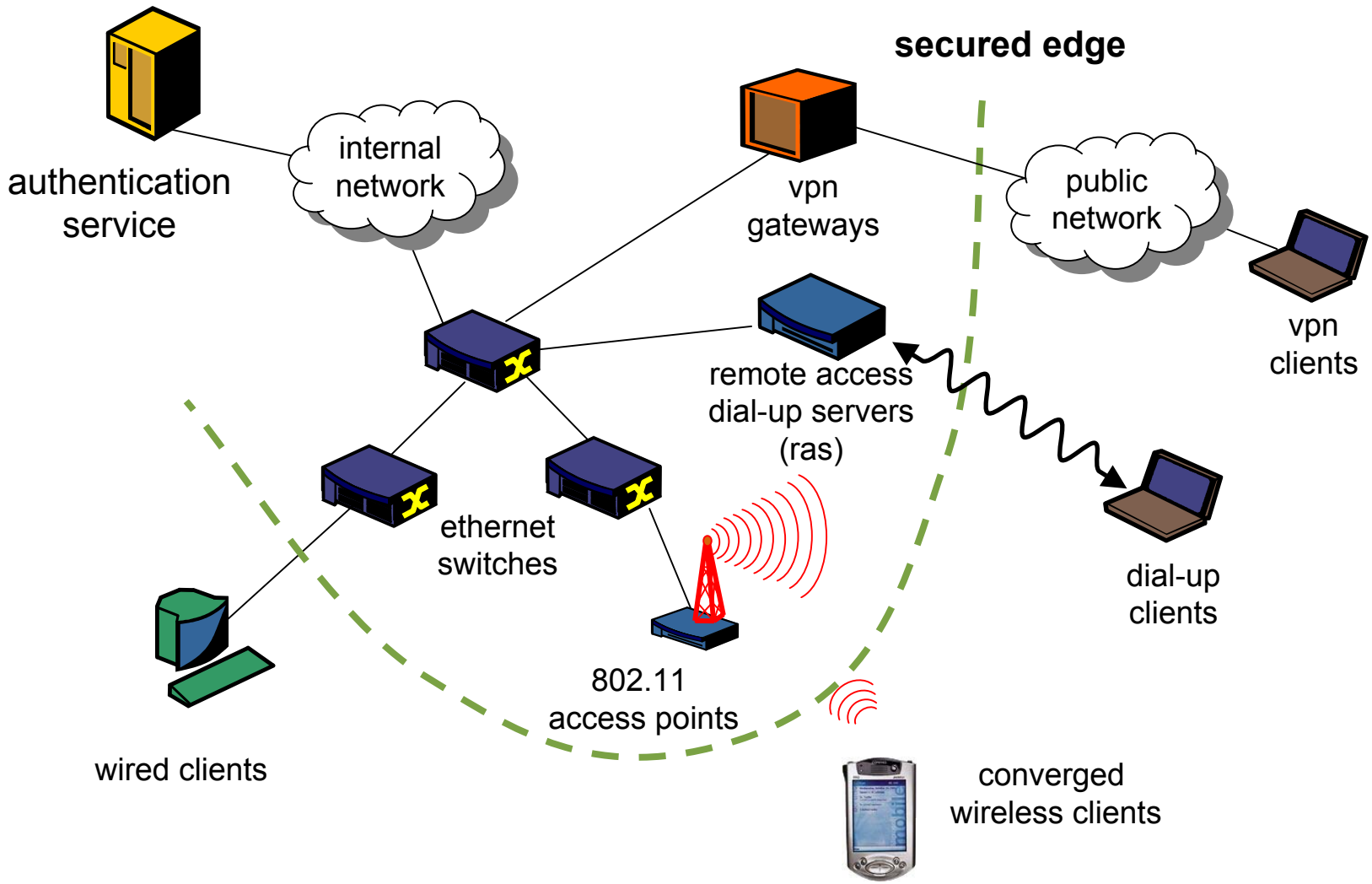
HP ProCurve Networking Adaptive EDGE Architecture ™



Solution approaches that focus on security, mobility and convergence independently are inherently insufficient.

Customers need a single network that provides an integrated approach to secure, mobile, converged networks.

What is Edge Access Security?



Important considerations

- Authentication
  - How is user identity verified?
- Authorization
  - How is access controlled?
  - How are access rights configured within the network?
- Encryption
  - How is data protected?
  - How are encryption keys distributed and installed?
- Mobility
  - How are security associations maintained while roaming?
- Performance
  - How are application requirements supported?

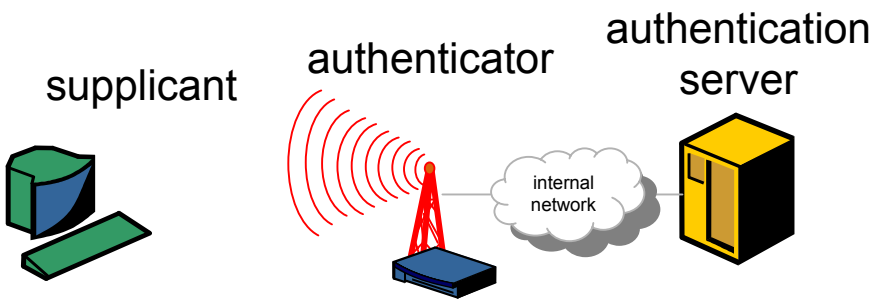
Two mobile access security approaches

- IEEE 802.1X
  - Originally designed for wired networks
  - Adopted as a standard component to 802.11 wireless solutions
  - Modeled after dial-up access security
  - A Layer-2 solution
  - Embedded in HP ProCurve switches and access points

- VPN Gateway solutions
  - Originally designed for remote access via the Internet
  - A Layer-3 solution
  - Key component of the HP ProCurve 700wl Series

IEEE 802.1X

physical topology



Supplicant

- The entity desiring access to the services of the authenticator.

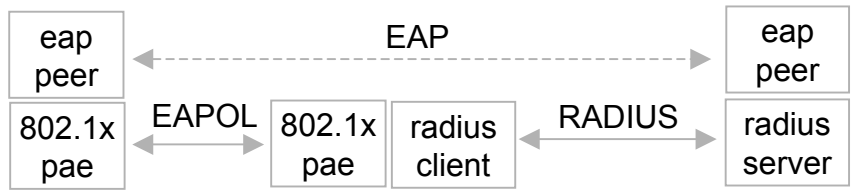
Authenticator

- The entity that requires the entity on the other end of the link to be authenticated

Authentication server

- An entity providing authentication service to the authenticator. Typically a RADIUS server

logical topology



802.1x port access entity (pae)

- The protocol entity associated with each port. Implements eap over lans (EAPOL)

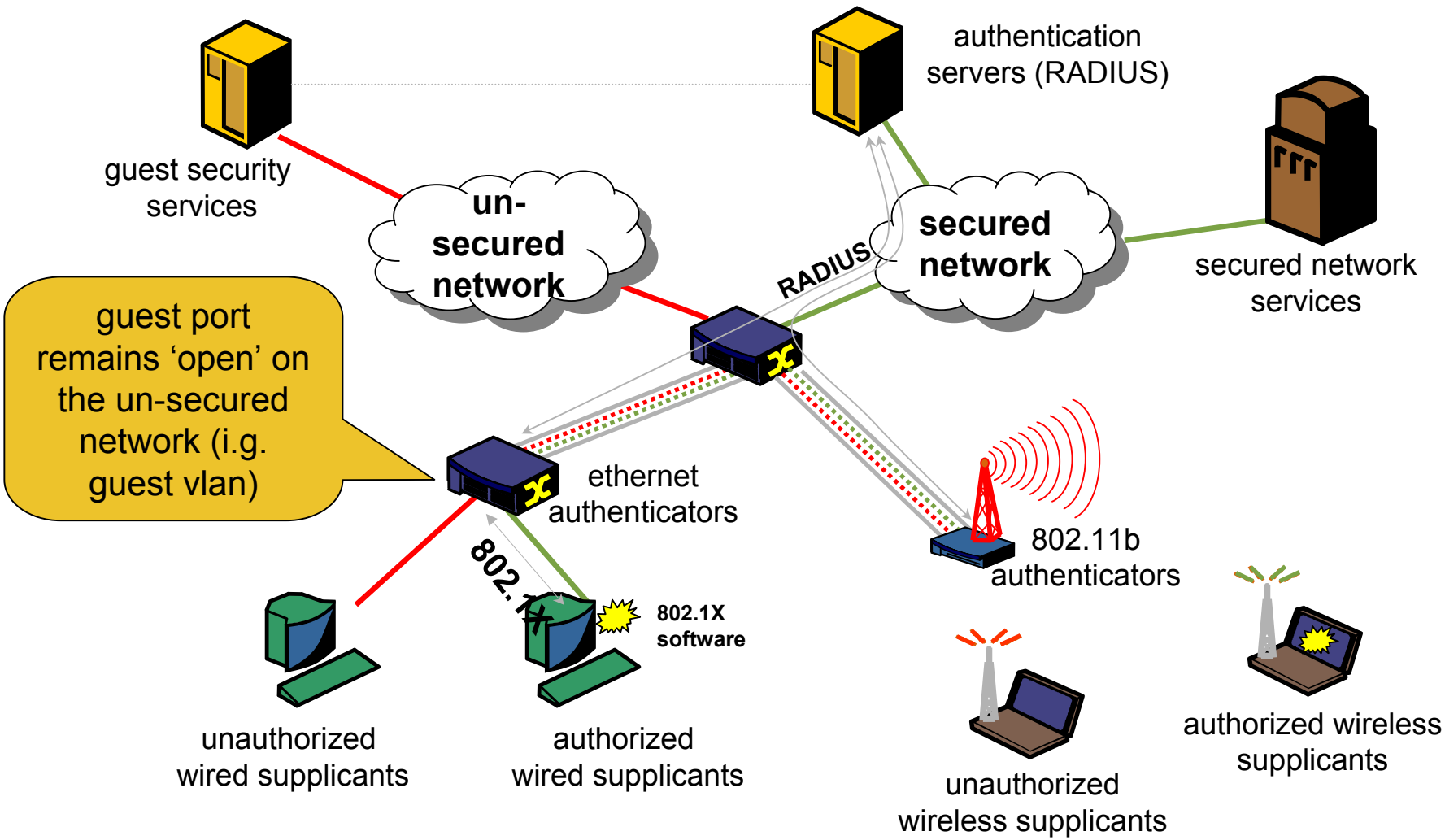
Radius client and server

- The backend protocol entity supporting authentication, authorization and accounting for network access (rfc 2865)

Extensible authentication protocol (eap)

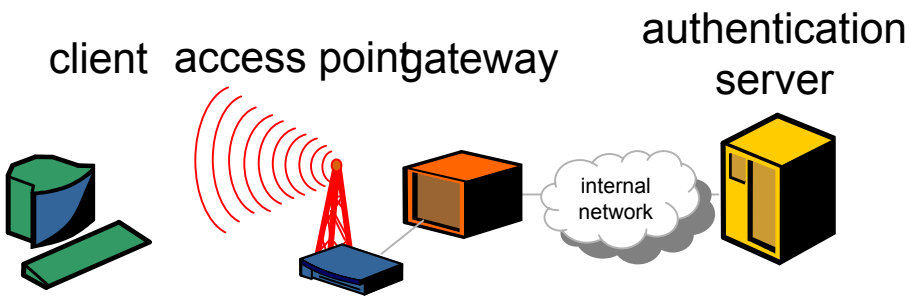
- A simple encapsulation protocol support numerous authentication methods (rfc 2284)

Today's 802.1X Solution

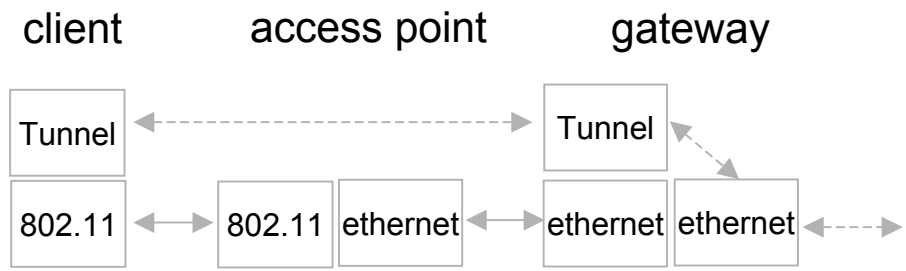


VPN Gateway

physical topology



logical topology



Client

- The entity desiring access to the network

Gateway

- The entity that provides access to the internal network

Authentication Server

- An entity providing authentication service to the gateway. Could be RADIUS, LDAP or Kerberos

802.11 Interface

- The wireless interface

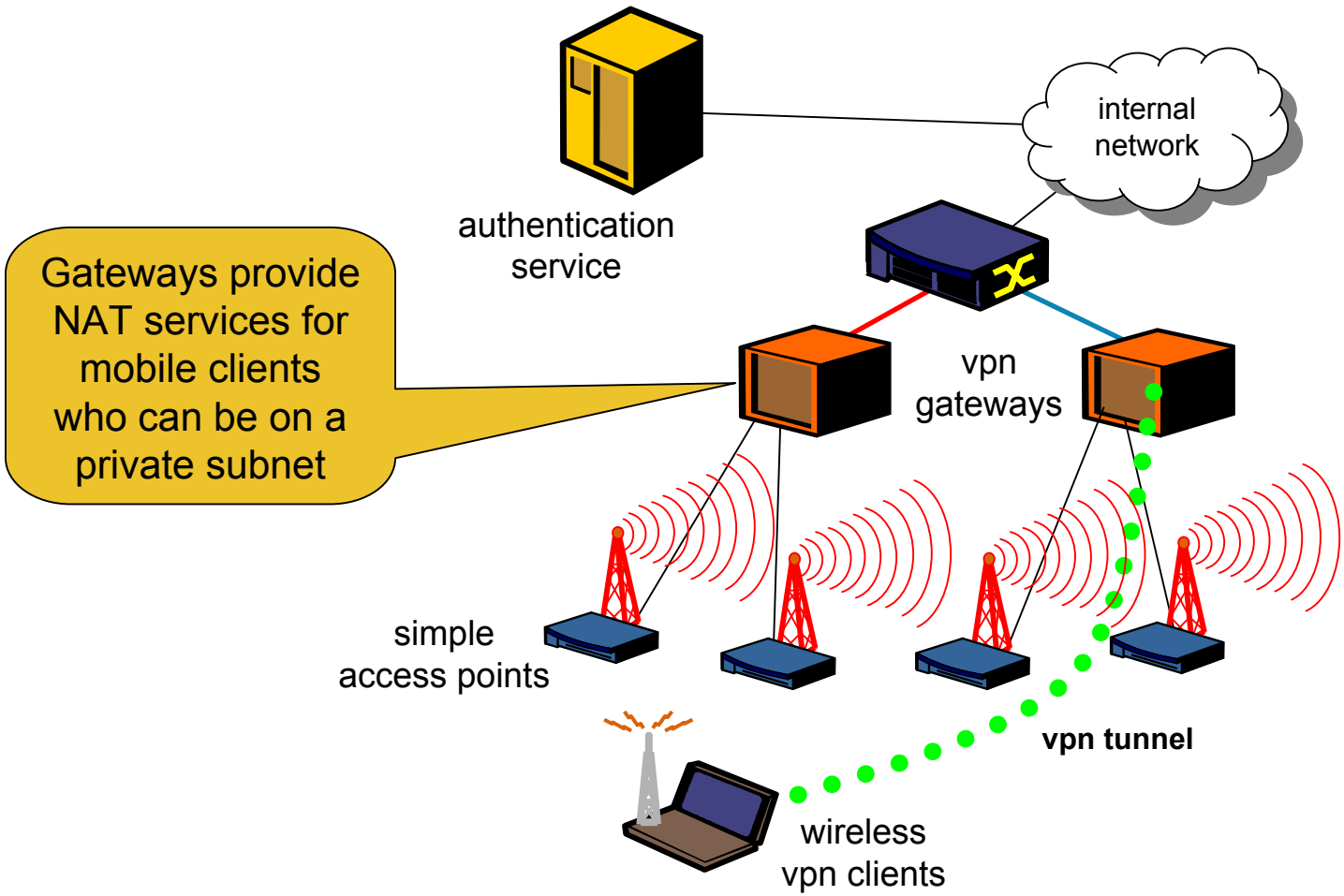
Ethernet Interface

- The wired interface

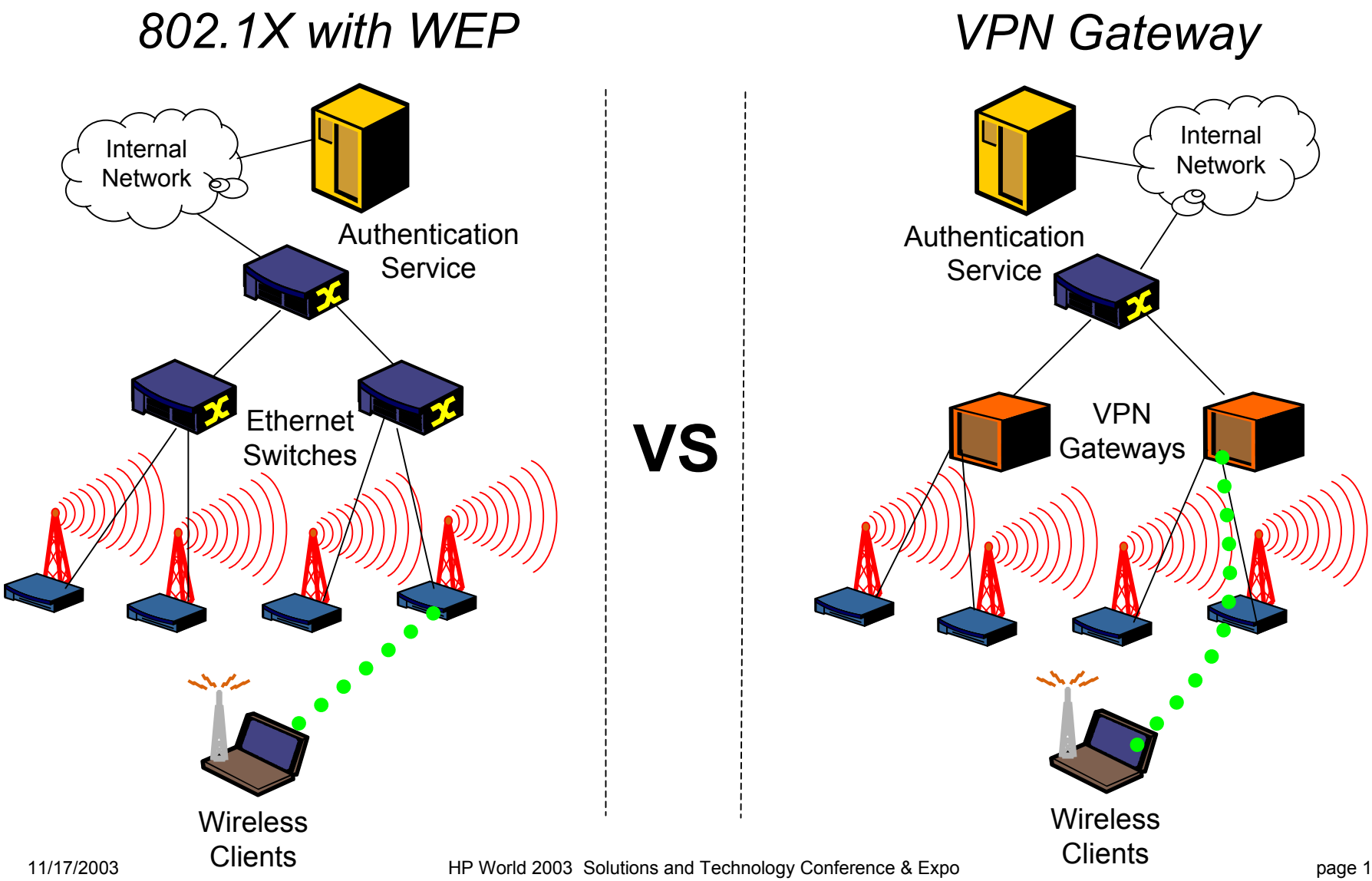
Tunnel Interface

- The interface used to communicate with the internal network via an encrypted tunnel. Can be PPTP, L2TP or IPSec

Today's VPN Gateway Solution



Comparing models



Authentication

802.1X with WEP

- May use any EAP method
- Certain EAP methods provide mutual authentication (e.g EAP-TLS, EAP-TTLS, PEAP)
- Access points themselves are RADIUS clients
- No supplicant configuration needed to locate authenticator

VPN Gateway

- Many choices based upon VPN client software. Typically RADIUS with MS-CHAP or IKE for IPSec
- Access points are unprotected and simple
- Gateway contains authentication client software
- Client software configuration required

Authorization

802.1X with WEP

- Authorization parameters are returned to the authenticator via Radius attributes
- Dynamic VLAN assignment
- Dynamic Key installation
- Other non-standard attributes are possible (bandwidth limits, access control lists, etc)

VPN Gateway

- Authorization parameters (aka access rights) are returned to the gateway by a control server software
- Typically very flexible policy based management and authorization

Encryption

802.1X with WEP

- Uses native 802.11 encryption schemes (WEP, TKIP, AES)
- Encryption is performed by WLAN hardware and access point
- Only wireless frames are protected
- Layer-2 scheme

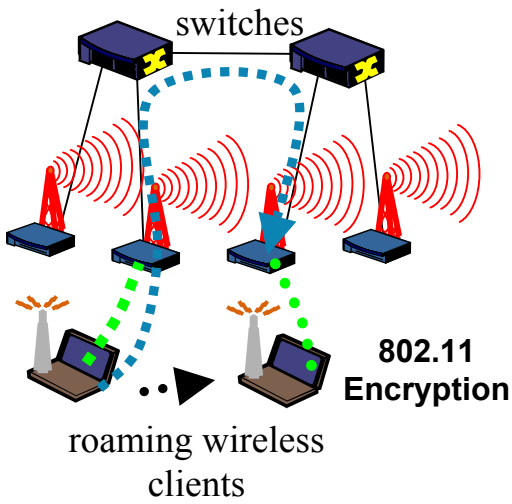
VPN Gateway

- Numerous VPN encryption schemes are supported (DES, 3DES, Blowfish, etc)
- Host software performs encryption operations
- Frames are encrypted on all links between the host and the gateway
- Layer-3 scheme

Mobility

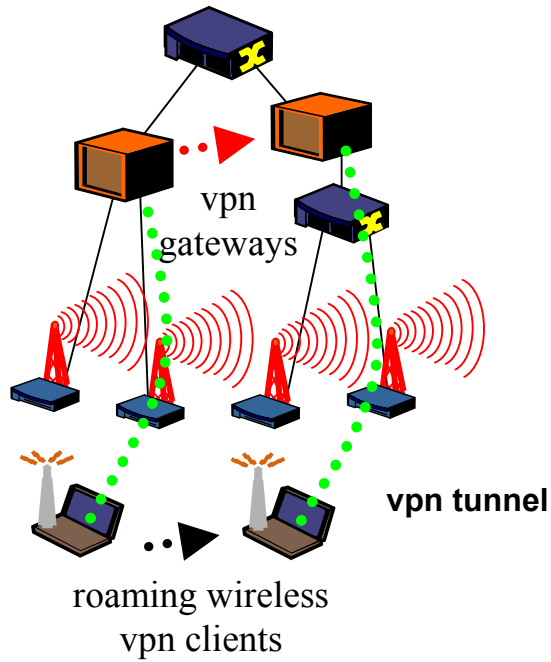
802.1X with WEP

- Today security associations must be re-established
- Future schemes involve pre-authentication



VPN Gateway

- Intra-gateway roaming is easy
- Inter-gateway roaming uses tunneling



Performance

802.1X with WEP

- Encryption performed in hardware on the WLAN interface card
- Access control at the very edge of the network
- Performance bounded by wireless link (54 Mbps)

VPN Gateway

- Encryption performed in software
- Access control within the network at aggregation points
- Performance limited by architecture of gateway (software ~= 30 Mbps, accelerator ~= 400 Mbps)

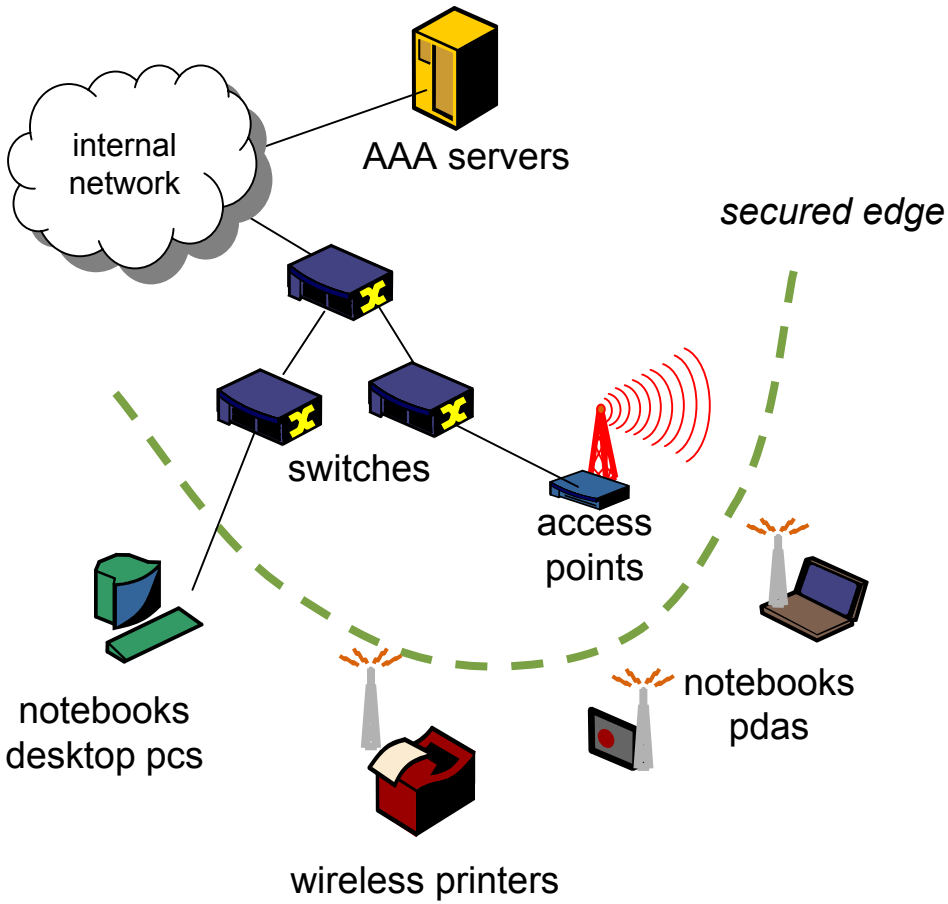
Usage Considerations

- Client and deployment considerations
  - VPN clients are abundant and free
  - 802.1X supplicant OS support is growing but not complete
- Performance considerations
  - PDAs and low-end devices may have trouble with VPN software
  - 802.1X authenticators are at the very edge of the network
  - VPN gateways typically inspect every packet in software
- Cost considerations
  - VPN gateways are an additional device in the network
  - 802.1X components are typically included

More Usage Considerations

- Policy considerations
  - Today, 802.1X configures VLANs and installs WEP keys
  - VPN gateways provide extensive rights management
- Mobility considerations
  - Today, hand-off with 802.1X requires re-authentication
  - VPN gateway tunnels may span multiple access points and sub-networks
- Protocol considerations
  - 802.1X is a Layer-2 solution
  - VPN gateways are a Layer-3 solution and require IP
  - VPN gateways must replicate protected multicast traffic for each client
  - Wireless QoS has no effect on VPN traffic

802.1X Solutions from HP



Desktops, Notebooks, PDAs

- Microsoft Windows XP Support
- Integrated wireless adapters

Printers

- HP 680x 802.11b print server

Ethernet Switches

- HP ProCurve Switches (25xx, 26xx, 41xx, 53xx, 93xx)

Access Points

- HP ProCurve 520wl

AAA Servers

- HP-UX AAA Radius Server
- Microsoft Win2K Server Support

HP ProCurve 700wl Secure Access Series

A Complete Wireless Mobility Solution

HP ProCurve Access Controller 720wl

HP ProCurve Access Control Server 740wl

HP ProCurve Integrated Access Manager 760wl

- HP ProCurve Access Controller 720wl
  - Enforces user access rights at the edge of the network
  - Secures wireless traffic between users and the network
  - Manages application persistence as users roam between APs or across subnets
- HP ProCurve Access Control Server 740wl
  - Consolidates user configuration and policy management
  - Maintains and reassigns user access rights based on location or time of day
- HP ProCurve Integrated Access Manager 760wl
  - Policy management, enforcement, security and roaming – all-in-one solution
  - Ideal for smaller wireless LAN or branch office deployments
- A Complete family of accessories

Interex, Encompass and HP bring you a powerful new HP World.