
	<h2 data-bbox="842 562 1114 667">Wireless LAN Security</h2> <p data-bbox="890 770 1066 831">Holger Rank Project Manager</p> <p data-bbox="823 860 1129 904">HP Network Solutions Group Email: Holger.Rank@hp.com</p>
---	--

<h3 data-bbox="328 1272 529 1317">Vorstellung</h3> 	<h2 data-bbox="643 1473 898 1525">Holger Rank</h2> <p data-bbox="643 1532 978 1561">Project Manager HP Services</p> <p data-bbox="643 1579 978 1744">Hewlett-Packard GmbH Kieler Straße 147 22769 Hamburg Tel: 0172 4505057 Email: Holger.Rank@hp.com</p>
--	---

4/10/2003

HP presentation template user manual

page 2

	<h2 data-bbox="715 353 855 398">Agenda</h2> <ul data-bbox="715 730 1238 954" style="list-style-type: none">HP NSG VorstellungWireless LAN ÜberblickWireless LAN GefahrenWireless LAN Security LösungenW-LAN Security Konzept
---	--

	<h2 data-bbox="715 1290 1142 1429">HP Services Network Solution Group (NSG)</h2> <h2 data-bbox="715 1845 919 1890">Vorstellung</h2>
---	--

Network Solutions Group Deutschland




- Mitarbeiter an 10 Standorten in Deutschland
 - Business Management und Development
 - Sales und Sales Development
 - Technical Consultants
 - Projektmanager
 - Service Consultants
- Cisco Spezialisierung HP Deutschland
 - Wireless LAN
 - Voice Access
 - IP Telephony
 - VPN und Security
 - Content Networks
 - Network Management
- Zertifizierungen HP Deutschland
 - 14 CCIE's
 - 8 CCDP's
 - 14 CCNP's
 - 3 CCDA's
 - 4 CCNA's



4/10/2003
HP presentation template user tutorial
page 5

Netzwerk Lifecycle

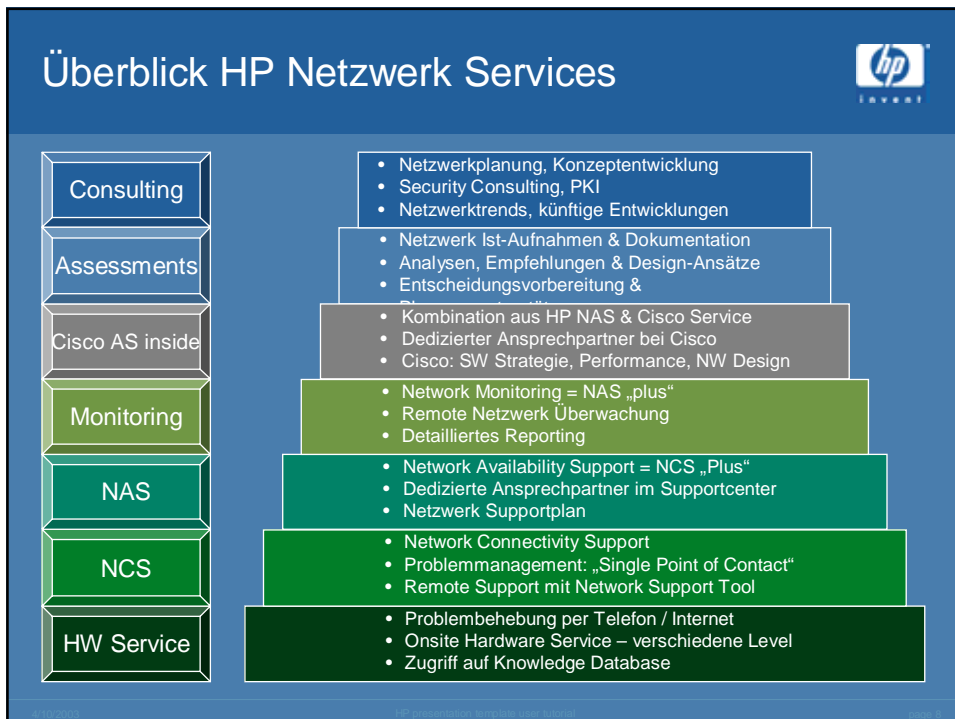
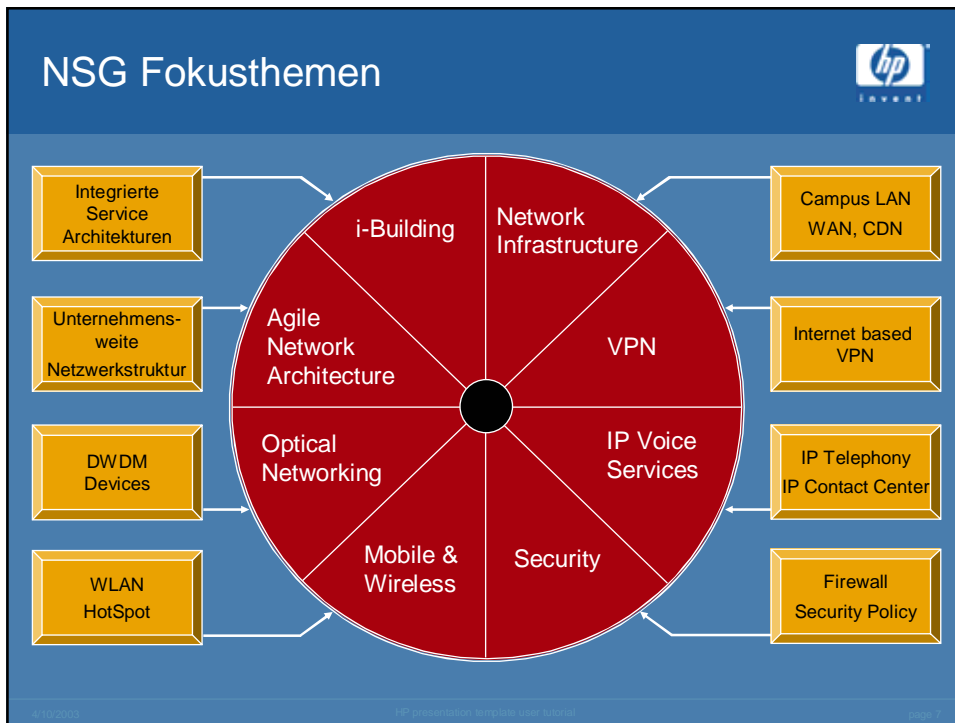



NSG Projekt- und Qualitymanagement

Network Integrations Services		Network Managed Services		Network Support
Planung	Design	Migration & Integration	Betrieb & Erweiterung	Support
Netzwerk Projekt Management	Installation	Outtasking/Betrieb	Netzwerk Account Betreuung	
Beratung	Infrastruktur	Beschaffung	LAN	Integrierter Lösungssupport
Assessment	Management	Konfiguration & Distribution	WAN	Netzwerk Lösungssupport
	Security	Installation & Abnahme	Security	Netzwerk Verfügbarkeitsupport
			Web Infrastruktur	Netzwerk HW & SW Support

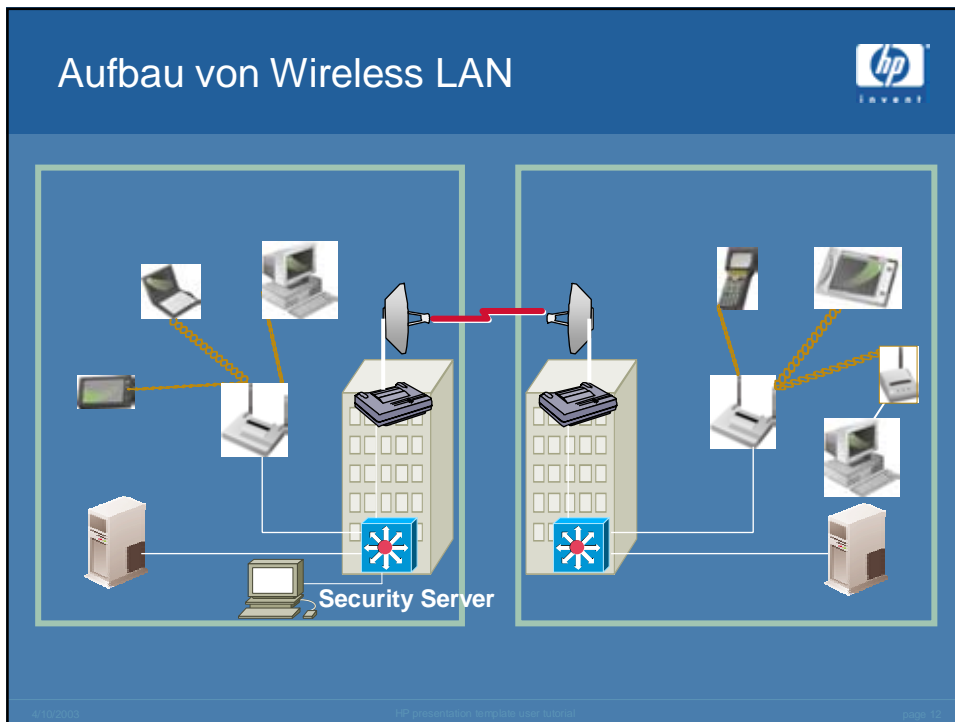
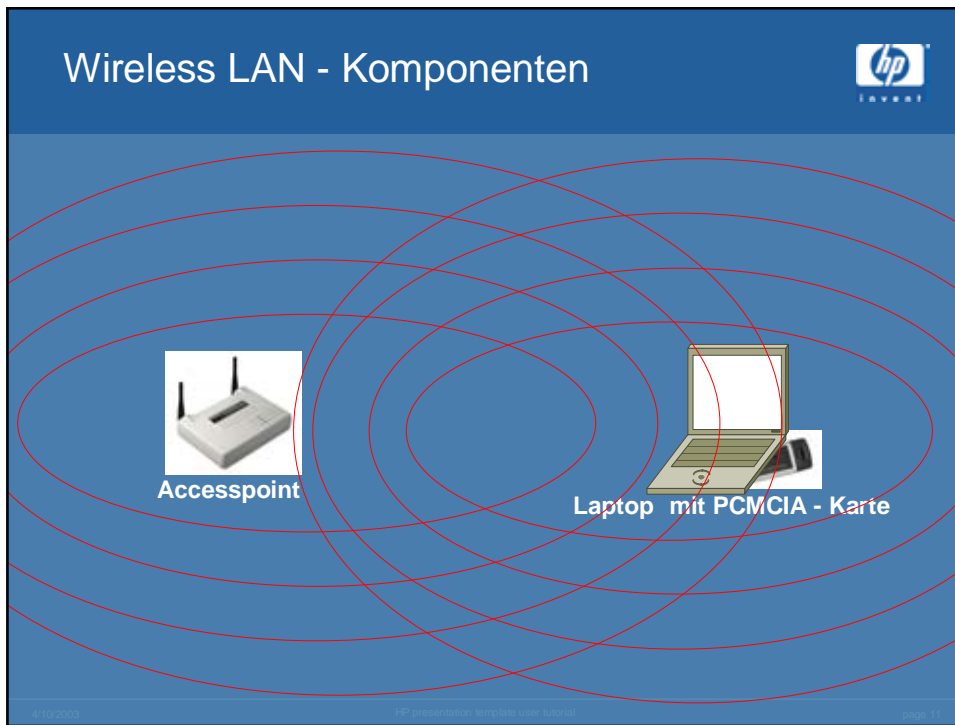
NSG Leistungen
MS
NSG

4/10/2003
HP presentation template user tutorial
page 6




	<h2 style="color: white;">Wireless LAN</h2> <h2 style="color: white;">Überblick</h2>
---	---

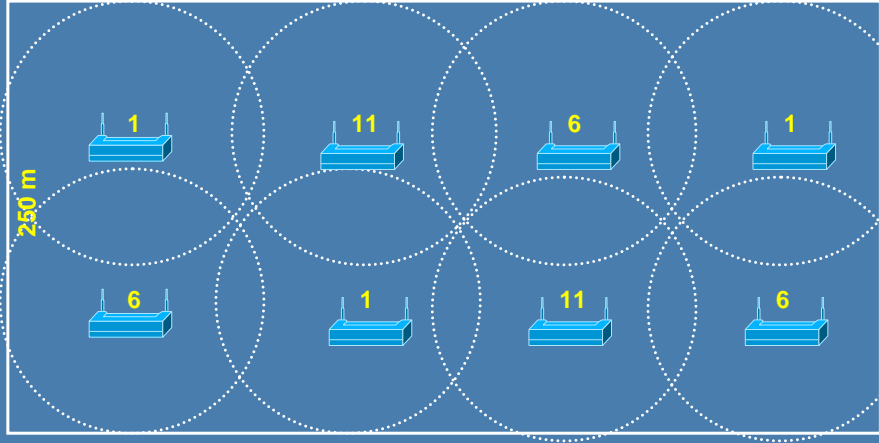
<h2>Überblick</h2>	
<h3>Wireless LAN 802.11b</h3>	<ul style="list-style-type: none">•Aktueller Standard 802.11b/ 2,4Ghz•Übertragungsrate 11 Mbit•3 nutzbare Kanäle von 11 (1,6,11)•Antennen, je nach Bedarf•Image: Flexibel aber unsicher!
<h3>Neue Standards 802.11a + 802.11g</h3>	<ul style="list-style-type: none">•Übertragungsrate 54Mbit•802.11g (2,4Ghz):<ul style="list-style-type: none">- kompatibel und ähnliche Eigenschaften wie 802.11b•802.11a (5Ghz):<ul style="list-style-type: none">- nicht kompatibel- geringere Reichweite- Standard sehr länderspezifisch- 8 – 19 nutzbare Kanäle unterteilt in In + Outdoor!



Wireless-Design 802.11b



- Maximale Abdeckung
- Automatische Bandbreitenvergabe
- Roaming
- 11 Mbit Durchsatz



250 m

600 m

4/10/2003 HP presentation template user tutorial page 13

802.11 Wireless Security




Allgemein bekannte Wireless LAN Security Verfahren:

- Service Set Identifier (SSID)
- Wired Equivalent Privacy (WEP)
- Open Authentication
- Shared Key Authentication
- MAC Address Authentication

nicht wirklich sicher!

4/10/2003 HP presentation template user tutorial page 14


Wireless Security Anforderungen 

Starke Authentifizierung

Kontinuierlich wechselnde WEP- bzw. Encryption Keys sowie starke Verschlüsselung

Zentrales Wireless- und Key-Management

4/10/2003 HP presentation template user tutorial page 10



Wireless LAN

Gefahren

Wireless Gefahren



- Standard Konfiguration
- Reichweite größer als das Firmengelände
- Keine Kontrollinstanzen zum Hausnetz
- Direkter Zugriff auf Firmendaten / Endgerät!
- Kein Logging wer, wann und wie lange verbunden war
- Einfache Technik für jeden
- Statisches Key Handling
- Keine Regeln definierbar
- Keine Trennung der Benutzergruppen / VLANs
- Leichtfertiger Einsatz ohne Sicherheitskonzept
- Schwache Authentikation
- Keine zentrale User/PC Verwaltung

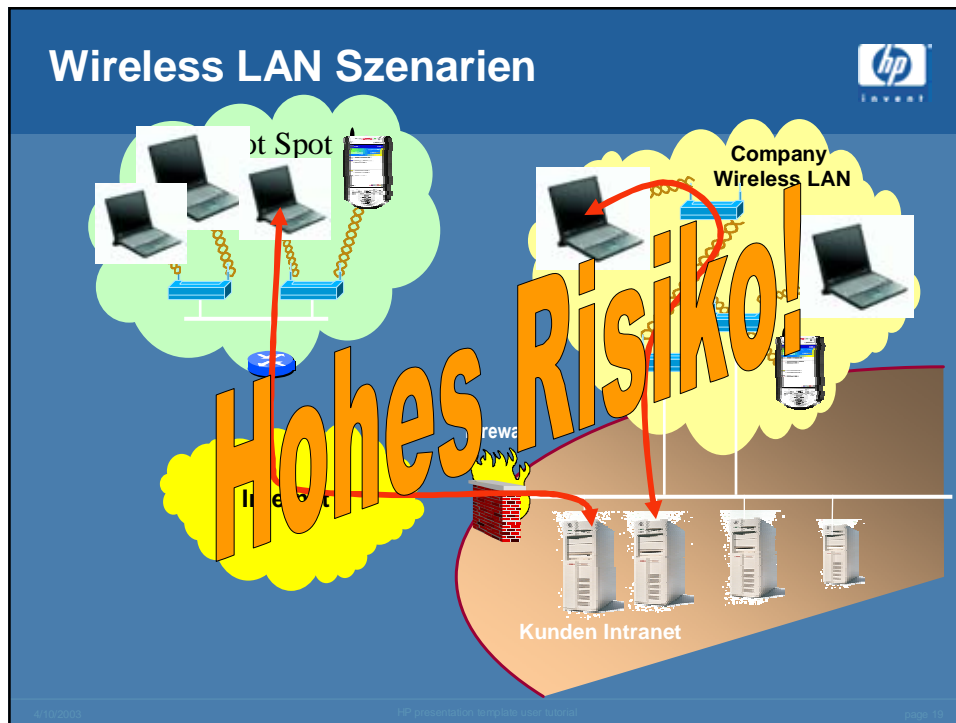
4/10/2003

HP presentation template user tutorial

page 17

Wireless LAN Security Lösungen





Wireless LAN Lösungen

The slide is titled 'Wireless LAN Lösungen' and features the HP logo and 'invent' tagline in the top right corner. It lists requirements for a secure wireless LAN solution and provides a list of products.

Was wird benötigt?

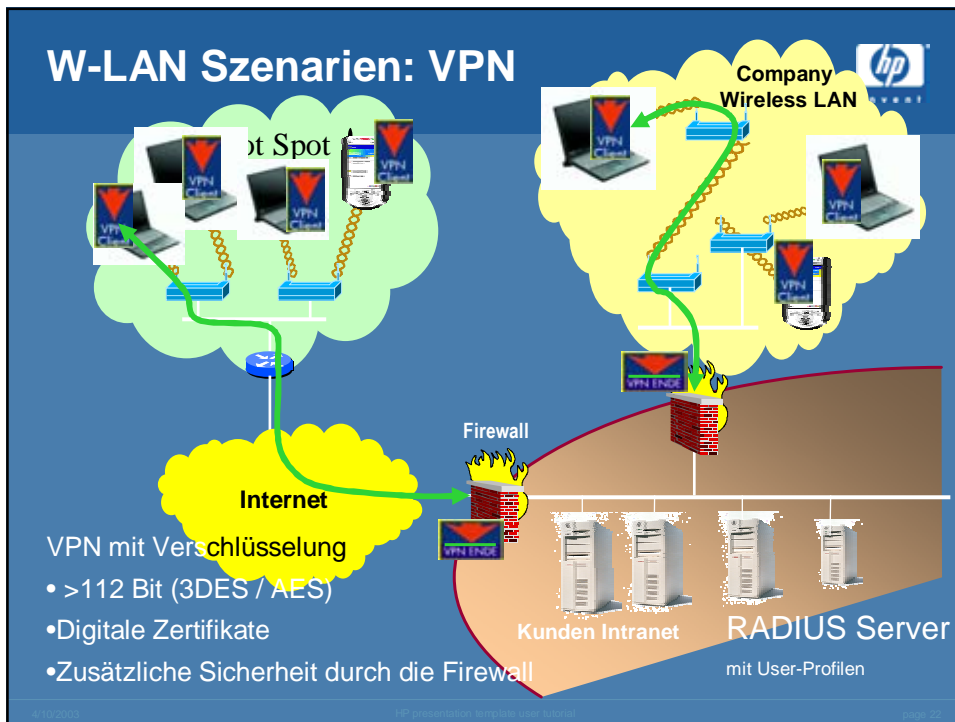
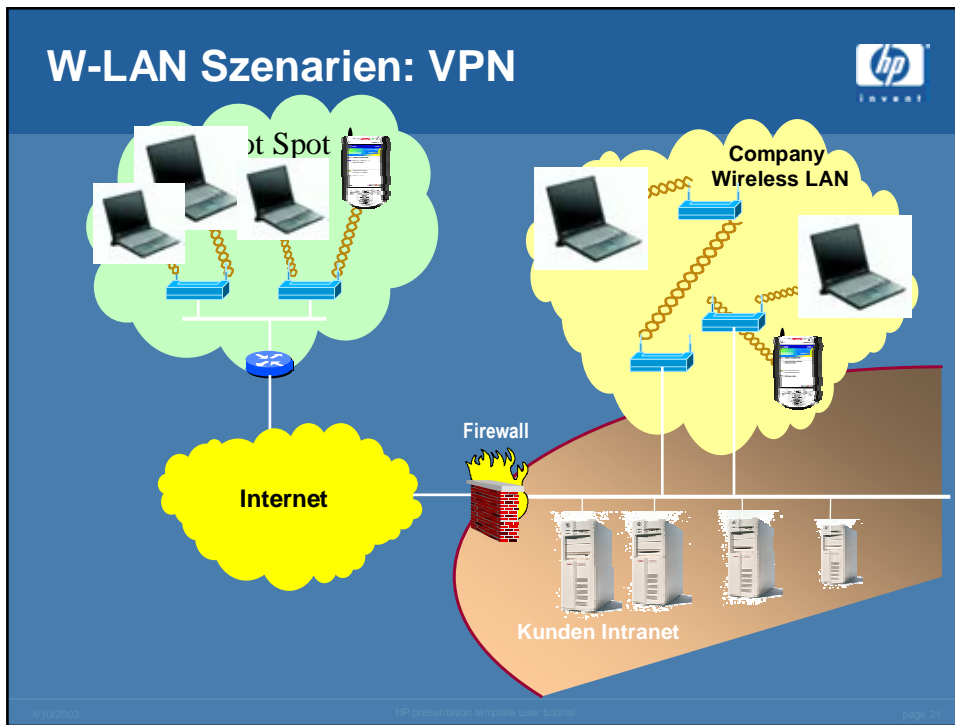
1. Sicherheitskonzept
2. Starke Authentikation
3. Min. eine 128 Bit Verschlüsselung
4. Optimale Produkte
5. Security Know How

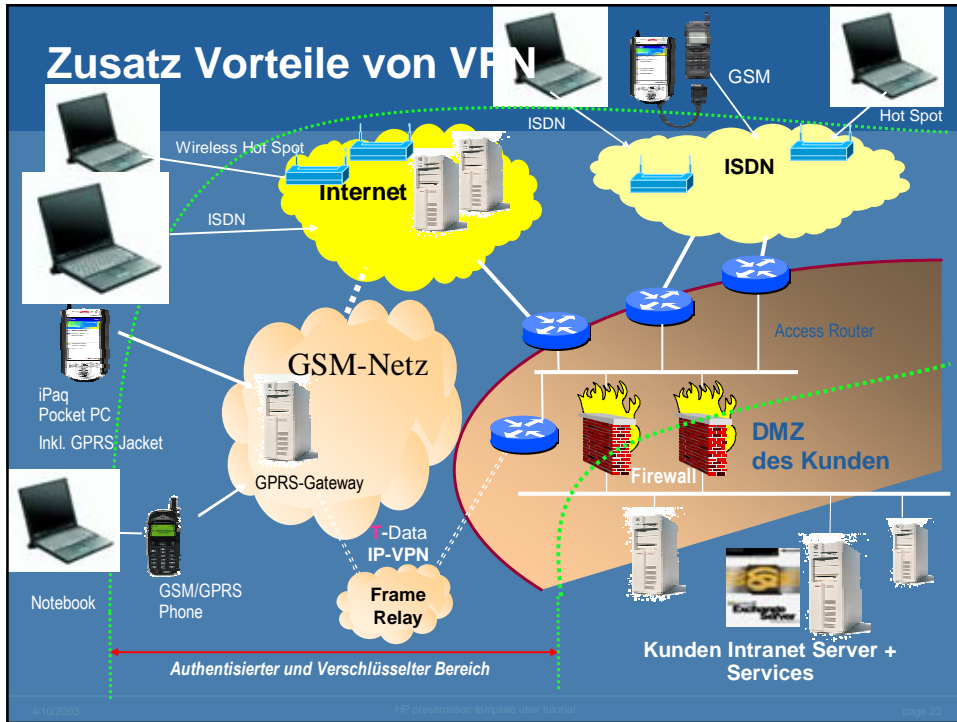
Produkte:

- Wireless LAN AP's + PC-Cards
- Firewall/VPN Concentrator
- VPN Client

...die Lösung: VPN
(Virtual Private Network)


4/10/2003 HP presentation template user manual page 20





Wireless LAN Security

Weitere Lösungsbausteine...



Wireless LAN Security

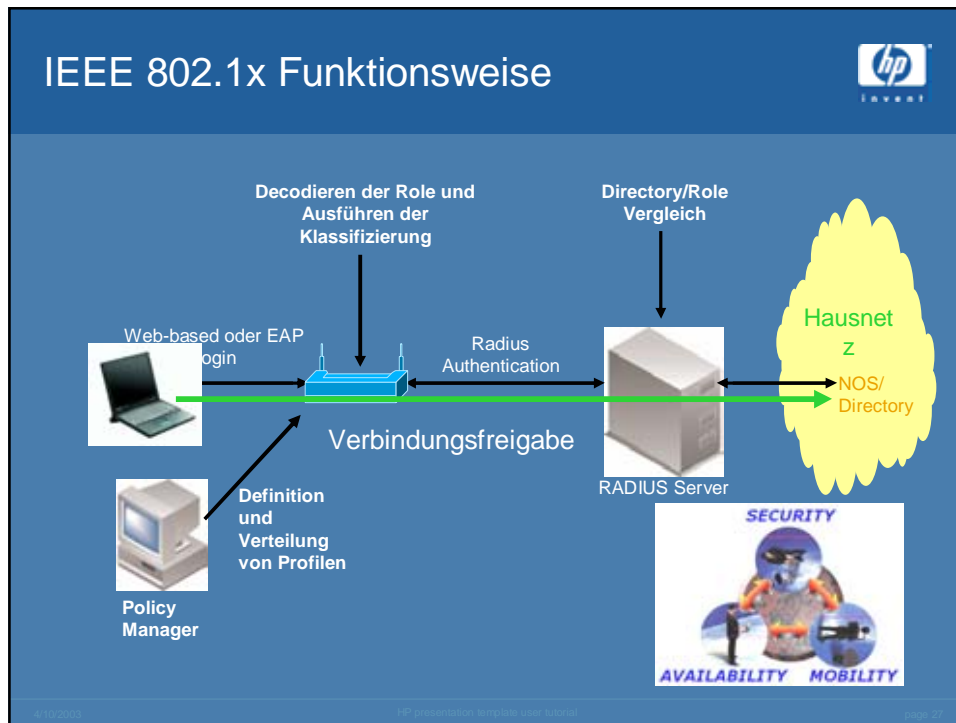
Security Standard 802.1x


IEEE 802.1x



- **Standard verabschiedet Juni 2001**
- **Port based Network Access Control**
- **Definiert**
 - Authentication Framework
 - Mechanismen zur Zugangskontrolle
 - Verschiedene Level zur Zugangskontrolle
 - Verhalten der Ports innerhalb dieser Level (transmission, reception of frames)
 - Protokolle zur Kommunikation zwischen Authenticator und Authentication Server
- **Ermöglicht interoperable Benutzer-Identifikation, zentralisierte Authentisierung, Key Management**
 - Nutzt existierende Standards: EAP, RADIUS, MD5
 - Compatibel mit existierende Roaming Technologien, ermöglicht Nutzung in Hotel und öffentlichen Plätzen
- **Unterstützt wird Ethernet, Token Ring und IEEE 802.11(Wireless)**

© 2003 HP
HP übernimmt keine Haftung für die Inhalte
Seite 26





Wireless LAN Security

TKIP


(Temporal Key Integrity Protocol)


TKIP Encryption



- Vorteile von TKIP:
 - Erweitert die WEP Encryption Funktion
 - Verwendet 802.1x Funktionen
 - Key Generierung per Paket
 - Message Integrity Check (Integritätsprüfung pro WEP-Frame!)
 - Broadcast Key Rotation (benötigt in 802.1x)
 - Base WEP Key muss über 802.1x regelmäßig geändert und generiert werden
 - NACHTEIL: Pre-Standard TKIP Unterstützung nur von Cisco

© 2003 HP HP Wireless LAN Security User Manual page 28

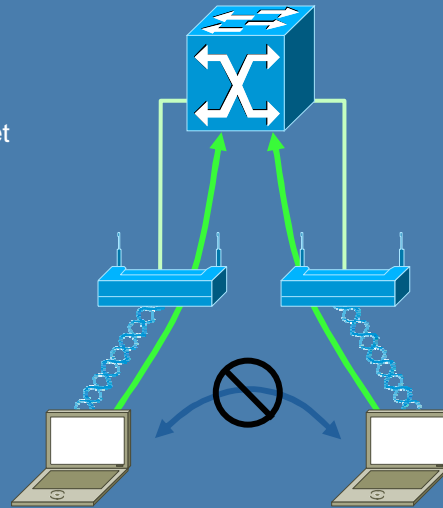
	<h2>Wireless LAN Security</h2> <h2>PSPF</h2> <p>(Public Secure Packet Forwarding)</p>
---	--

<h2>Public Secure Packet Forwarding</h2> 	
<p>Kommunikation nur in eine Wirkrichtung möglich!</p> <p>Verhindert Wireless LAN Client-Client Kommunikation</p>	

PSPF—Blocking Inter-Client Communication



- PSPF—Publicly Secure Packet Forwarding
- Prevents WLAN inter-client communication
- Relies on MAC address
- Same subnet devices only



4/10/2003

HP presentation template user tutorial

page 33

Wireless LAN Security



Cisco
Wireless VLANs

Cisco Wireless Virtual LANs



- 16 VLANs supported
- Wireless Encryption Funktionen notwendig
- Basierend auf SSIDs
- Supported ab IOS 12.2

SSIDs (Service Set Identifier)

- Client-Access Point Zuordnung
- Client supported eine SSID
- Alphanumerische SSID
- Länge 2-32 Zeichen

VLANs:

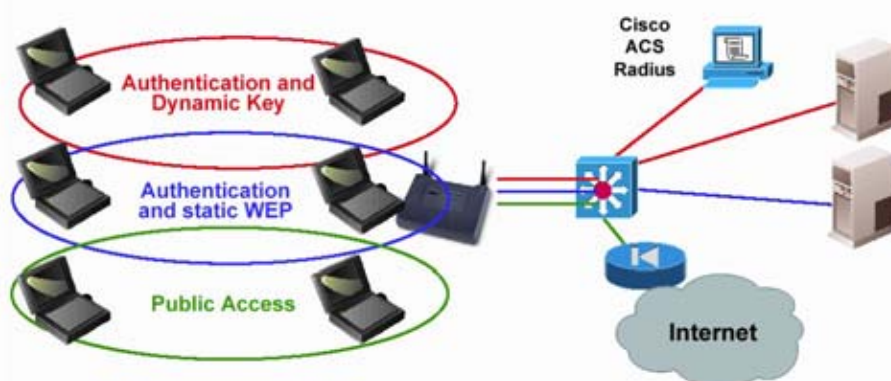
- VLAN1=default ohne Encryption
- VLAN2-16 benötigen WEP und EAP Funktionen

4/10/2003

HP presentation template user tutorial

page 36

Cisco Wireless Virtual LANs

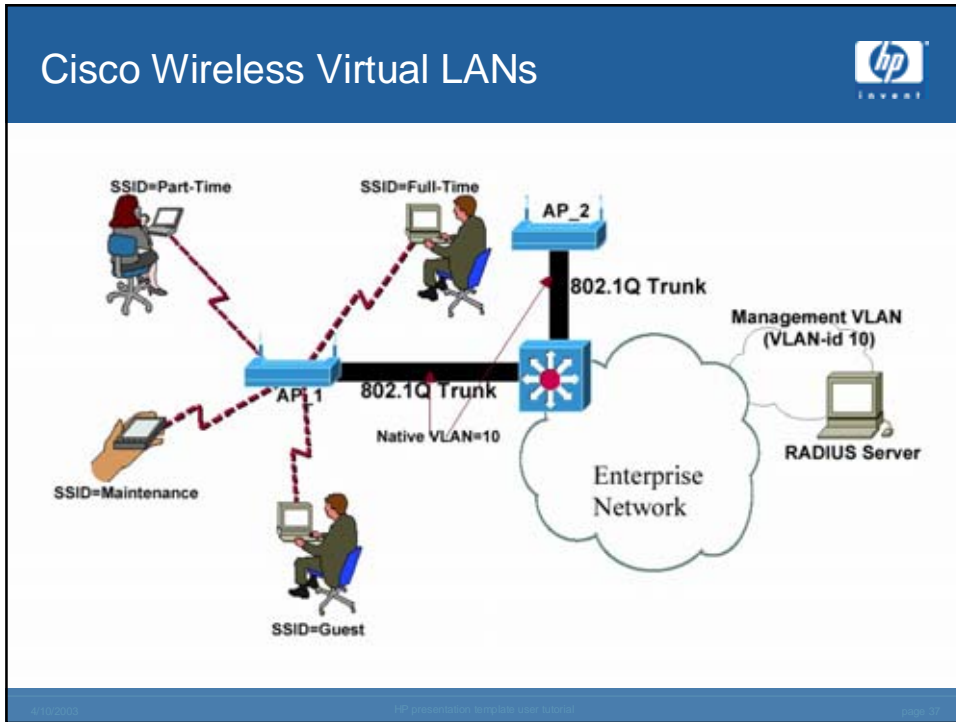


- One physical Infrastructure
- Multiple logical networks (VLAN's)
- different security levels

4/10/2003

HP presentation template user tutorial

page 37



Wireless LAN Security

Device Security

The slide features a blue background with the HP logo and the word 'invent' on the left side. The main title 'Wireless LAN Security' is at the top, and 'Device Security' is at the bottom.

Device Security



- Normales Username/Password Verfahren reicht nicht
- Einfaches aber sicheres Verfahren notwendig
- Rechtevergabe auf Basis der Policy (LDAP/AD)
- Bereitstellung von Applications nach Userpolicy
- Besitztum und Wissen als „Passwort“ (Smartcard + PIN)
- Einsatz von biometrischen Verfahren (Fingerprint, Iris Scan usw.)
- Single SignOn

4/10/2003

HP presentation template user tutorial

page 39

Device Security – weitere Maßnahmen




- Lokale Virens Scanner mit automatischen Update
- Lokale Festplattenverschlüsselung (Notebook) in Hard- oder Software
- Bios Passwort
- Keine FileShares freigeben!!
- Personal Firewall – sehr wichtig!
- Wirkliche Rechtevergabe für Access und Filezugriff lokal und remote
- Regelmäßige lokale Backups oder generelle Fileablage auf dem „sicheren“ Fileserver
- Persönlich auf sein Device achten (Sperren usw.)

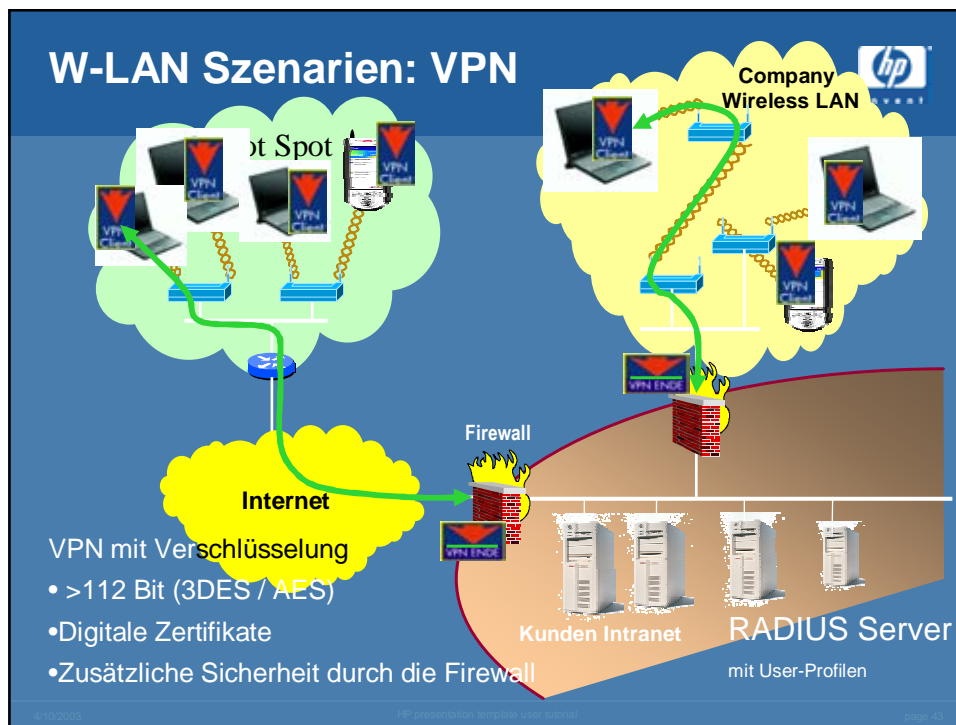
4/10/2003

HP presentation template user tutorial

page 40

	<h1>Wireless LAN Security</h1> <h2>Gesamtbild</h2>
---	---

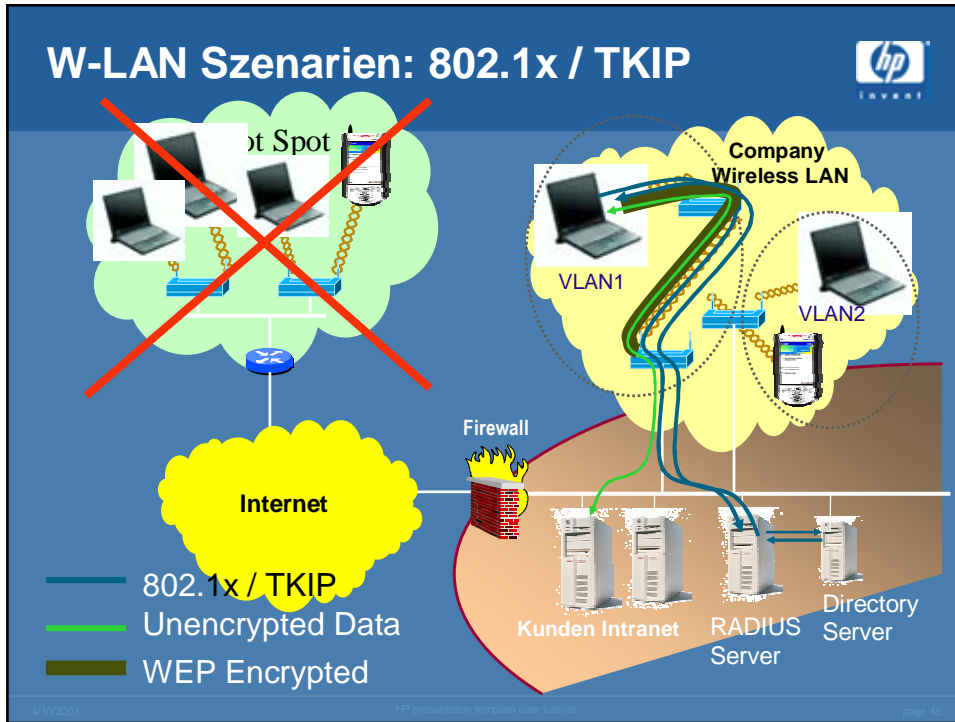
	<h1>Wireless LAN Security Variante 1:</h1> <h2>VPN</h2> <ul style="list-style-type: none">• Standard Wireless LAN• 802.1x, WEP, EAP nicht notwendig• Überall zu verwenden• Sehr hohe Sicherheit• Flexibel nutzbar auch unterwegs mit GSM, ISDN, Hot Spots usw.• Zusätzliche HW/SW benötigt• Performance-Verlust: durchschnittlich 30-40%
---	--





Wireless LAN Security Variante 2: 802.1x + TKIP

- Am Standard angelehnt
- Keine zusätzliche HW/SW
- Sehr flexible Regelvergabe
- Unterstützung der Cisco Roaming
- Hardware WEP Encryption
- Packet Keying + Frame Integrity Check
- Performance-Verlust: ca 10-15%
- Zentrale Verwaltung
- Company gebunden!



Wireless LAN Security

Cisco Wireless LAN Security Level

Cisco Wireless LAN Security Level



No Security	Basic Security	Enhanced Security	Specialized Security
<p style="text-align: center; color: white;">No WEP and Broadcast Mode</p> 	<p style="text-align: center; color: black;">Wi-Fi 40-bit, 128-bit, and Static WEP</p> 	<p style="text-align: center; color: black;">Dynamic Key Management System, Mutual Authentication, and 802.1x via EAP</p> 	<p style="text-align: center; color: black;">End-to-end security using VPN</p> 
Public Access	Telecommuter and Small Business	Mid-Market and Enterprise	Mobile User and Public Access

4/10/2003
page 17



Wireless LAN Security

Generell:

- Device Security nicht vergessen!
- 802.1x/TKIP für Company User
- VPN für Mobile User
- Bei Hot Spots immer VPN verwenden
- Wireless LAN nie ohne Sicherheitsfunktionen einsetzen, wenn kein Hot Spot ist!
- Integration ins Company Security Konzept

Security Grundlagen

Company Security

Security bedeutet:

- Hohe Verfügbarkeit
- Integrität der Daten
- Vertraulichkeit der Daten

Was wird benötigt?

- Security Beauftragter
- Management Unterstützung
- Security Policy
- Security Konzepte
- Security HW/SW
- Security Sensibilisierung
- Security Audits / Reviews

4/10/2003 HP presentation template user tutorial page 49


Vielen Dank!

...noch Fragen?





Wireless LAN
Security



Anhang

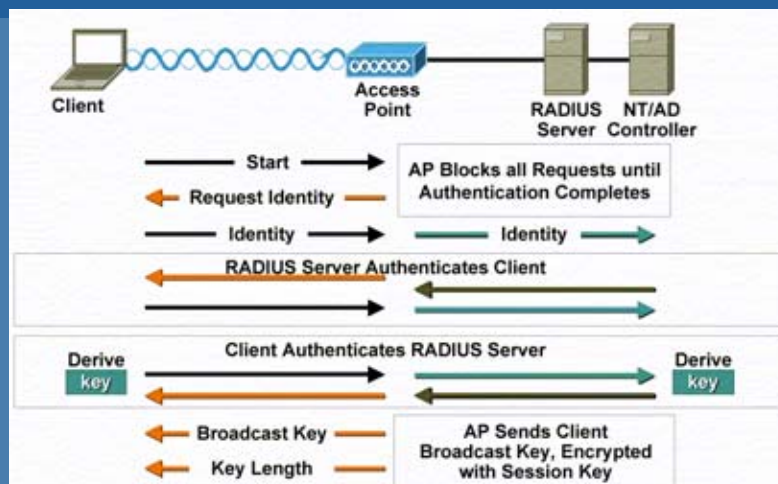
The image is a rectangular block divided into two vertical sections. The left section is black and contains a small version of the HP logo and the word 'invent' below it. The right section is a solid blue color and contains the text 'Wireless LAN Security' at the top and 'Anhang' at the bottom.

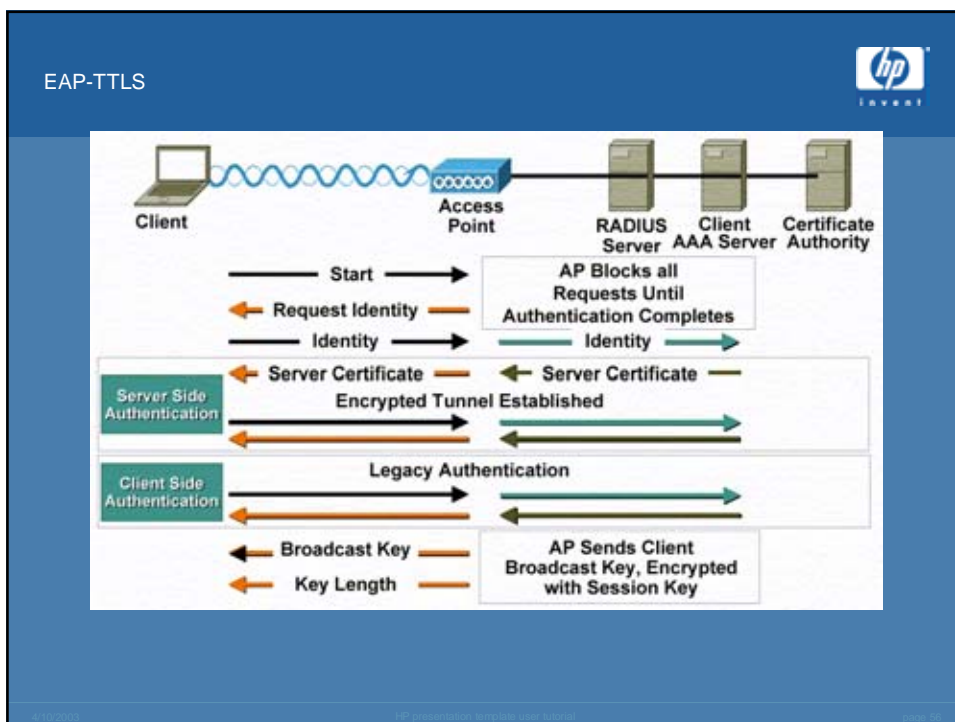
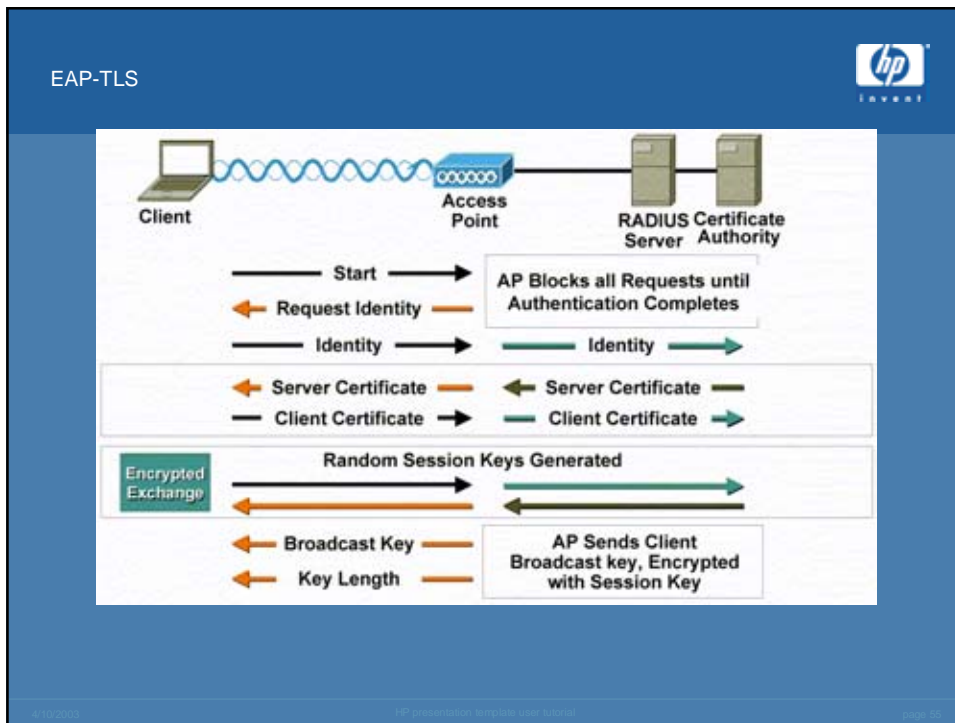
802.1x EAP Authentikations Typen für Wireless LANs

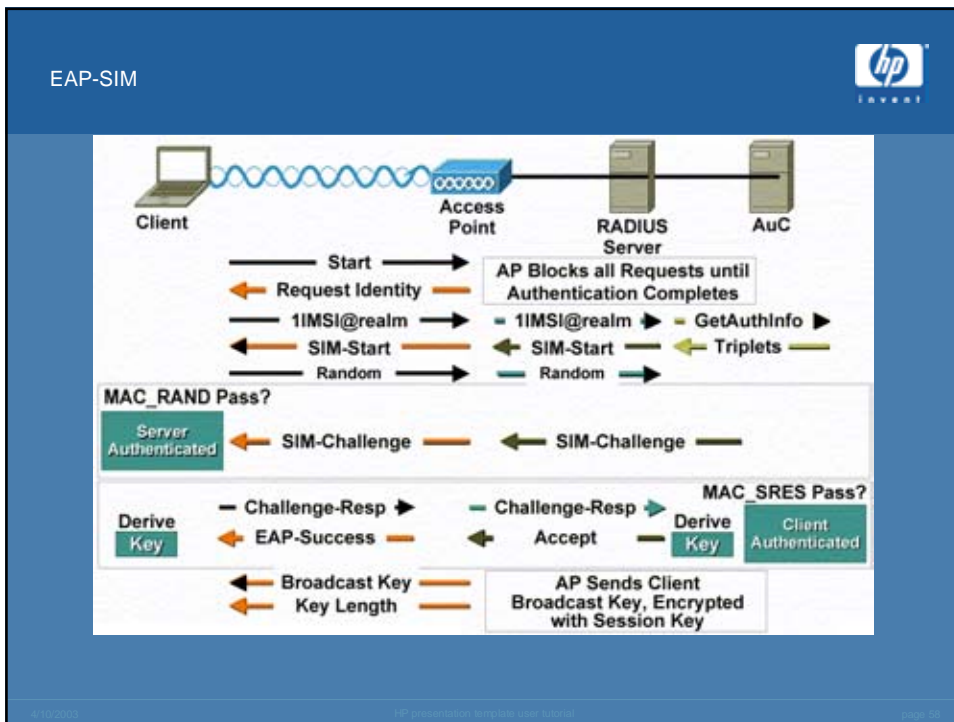
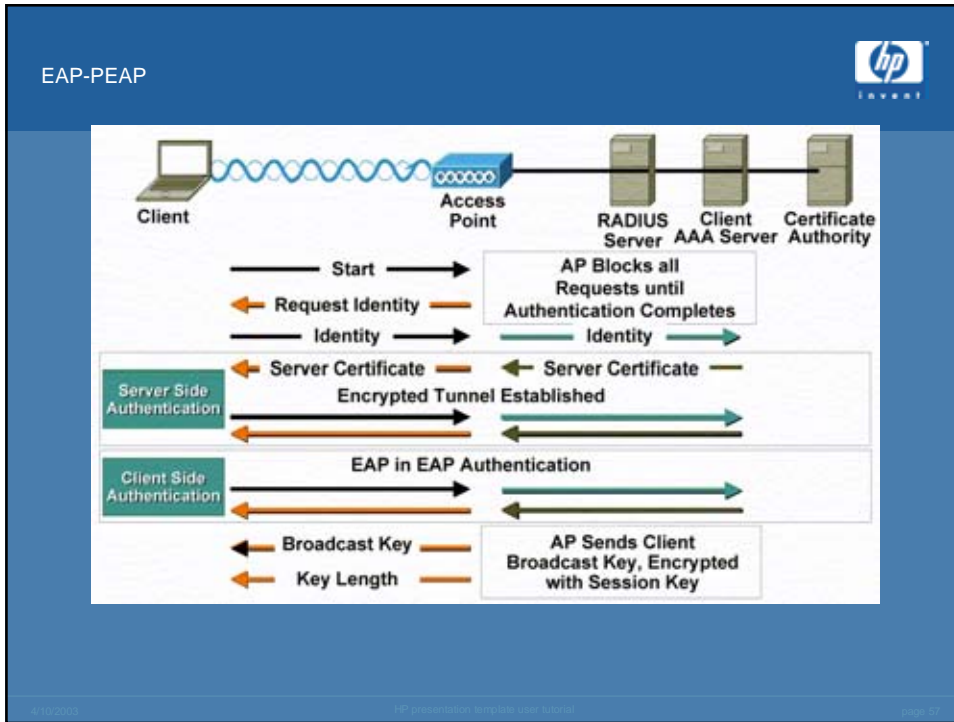



- EAP-Cisco (früher LEAP)
Passwort-basierend
- EAP-TLS (Transport Layer Security)
Zertifikats-basierend
- EAP-PEAP (Protected EAP)
Hybrid-Zertifikat/Password
- EAP-TTLS (Tunneled TLS)
Hybrid-Zertifikat/Password
- EAP-SIM (SIM Card)
Authentikation mit SIM Cards

EAP-Cisco










invent

Wireless LAN Security

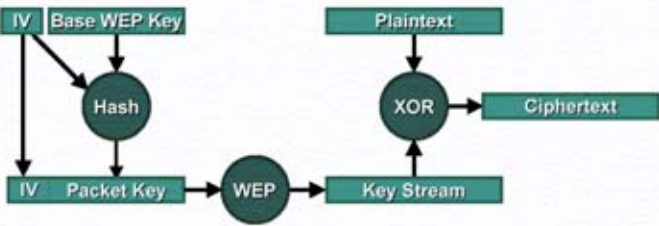
TKIP

(Temporal Key Integrity Protocol)

TKIP Keying



invent

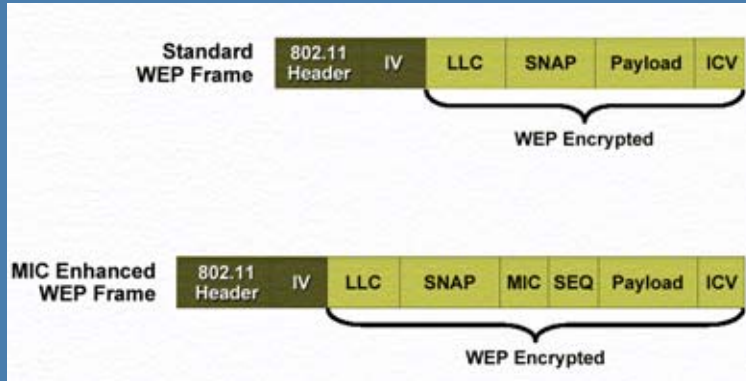


The diagram illustrates the TKIP keying process. It shows two parallel paths. On the left, an 'IV' and a 'Base WEP Key' are inputs to a 'Hash' function. The output of the hash is a 'Packet Key'. This 'Packet Key' is then processed by a 'WEP' function to generate a 'Key Stream'. On the right, a 'Plaintext' is input to an 'XOR' function, which also receives the 'Key Stream' as an input. The output of the XOR function is the 'Ciphertext'.

- IV Sequencing—IVs increment by one
- Per Packet IV is hashed with base WEP key
- Result is a new 'Packet' WEP key
- The Packet WEP key changes per IV

© 2003 HP
HP reserves all rights. All rights reserved.
page 28

TKIP
MIC



4/10/2003

HP presentation template user manual

page 51

Wireless LAN Security



Wireless LAN Blue Prints

