SIEMENS

Access Control for Wireless LANs

Maximilian Riegel
<maximilian.riegel@icn.siemens.de>

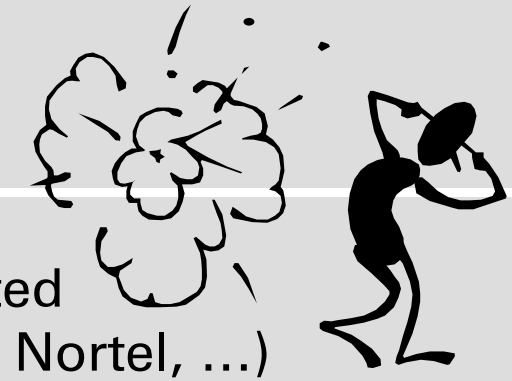
Information and Communication

Information and Communications

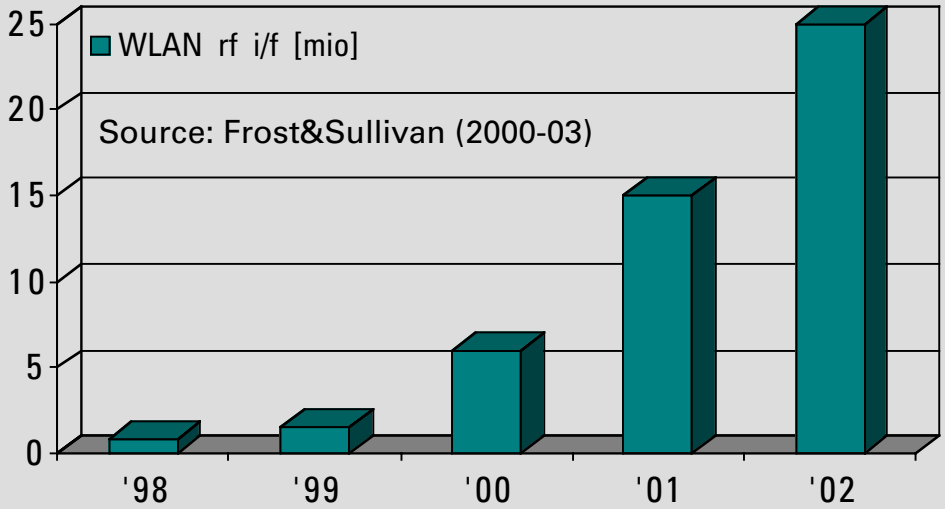
Outline

- WLAN is appearing on the market
- Access control provided by IEEE802.11
- Enhanced access control by IEEE802.11i
- Access control for public WLANs
- Functionality of an WLAN access gateway
- A last word about WLAN security
- Summary

WLAN has taken off ...



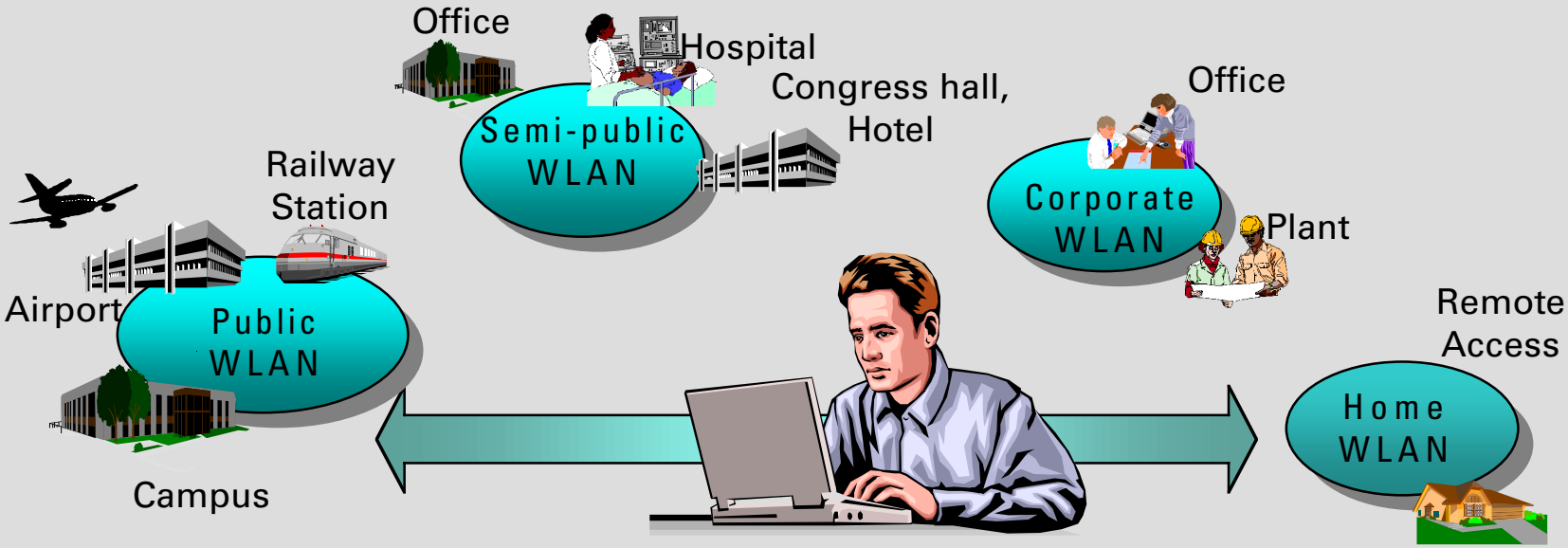
- Lots of serious WLAN activities have been started
  - All big players have products (Cisco, Lucent, Nortel, ...)
  - Integrated WLAN solutions appearing (Apple, IBM, Dell, ...)
- The prediction for '00 has been exceeded by actual market.



- Ruling technology is IEEE802.11b (Wi-Fi) [11Mb/s, 2.4 GHz].

The WLAN killer app…

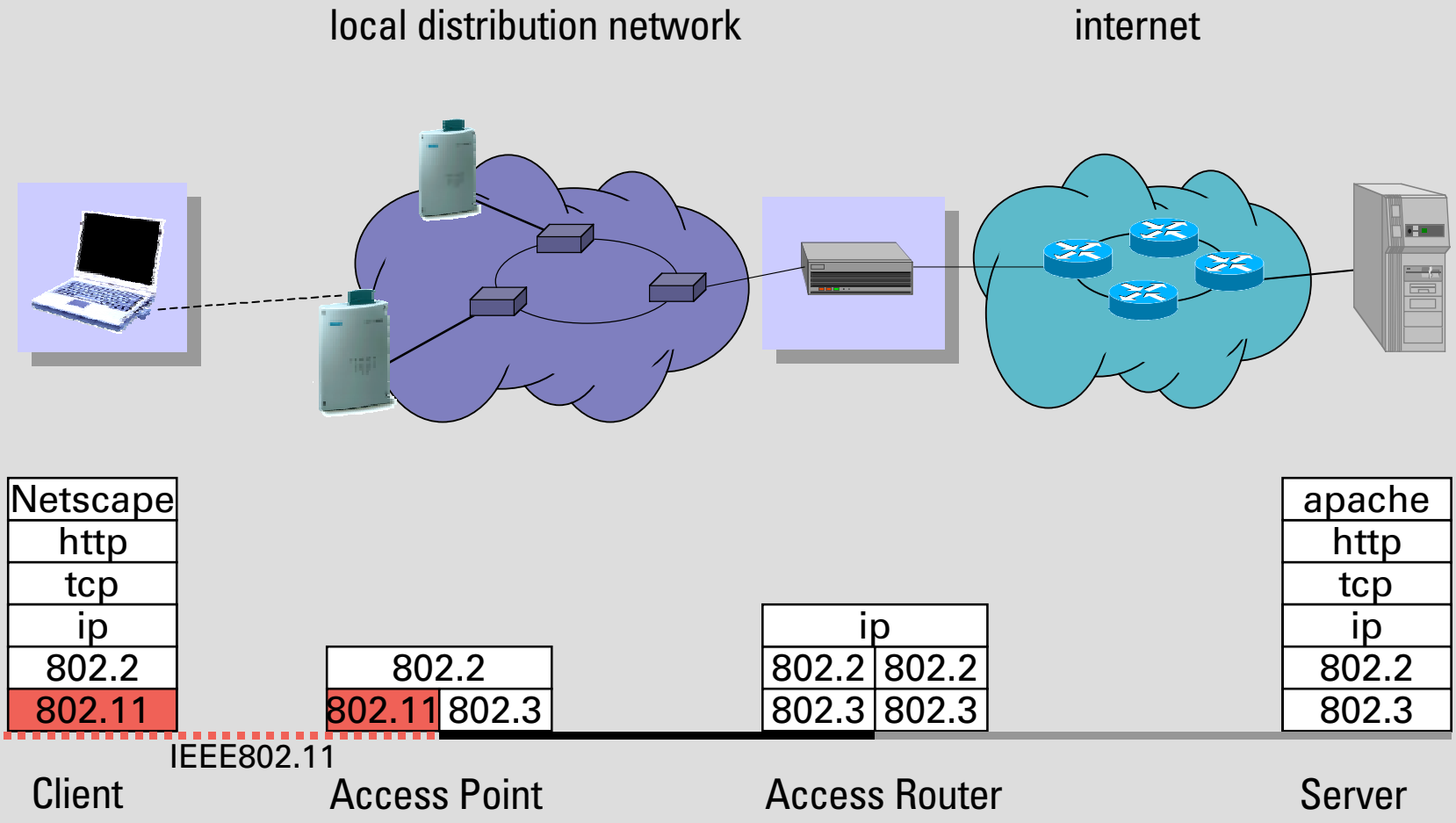
- WLAN is more than just cable replacement!
- It provides hastlefree broadband Internet access everywhere.



- Today's road worriers require access to the Internet everywhere.
- Only coverage in 'hot-spots' needed.
- WLAN meets the expectations for easyness, cost and bandwidth.

SIEMENS

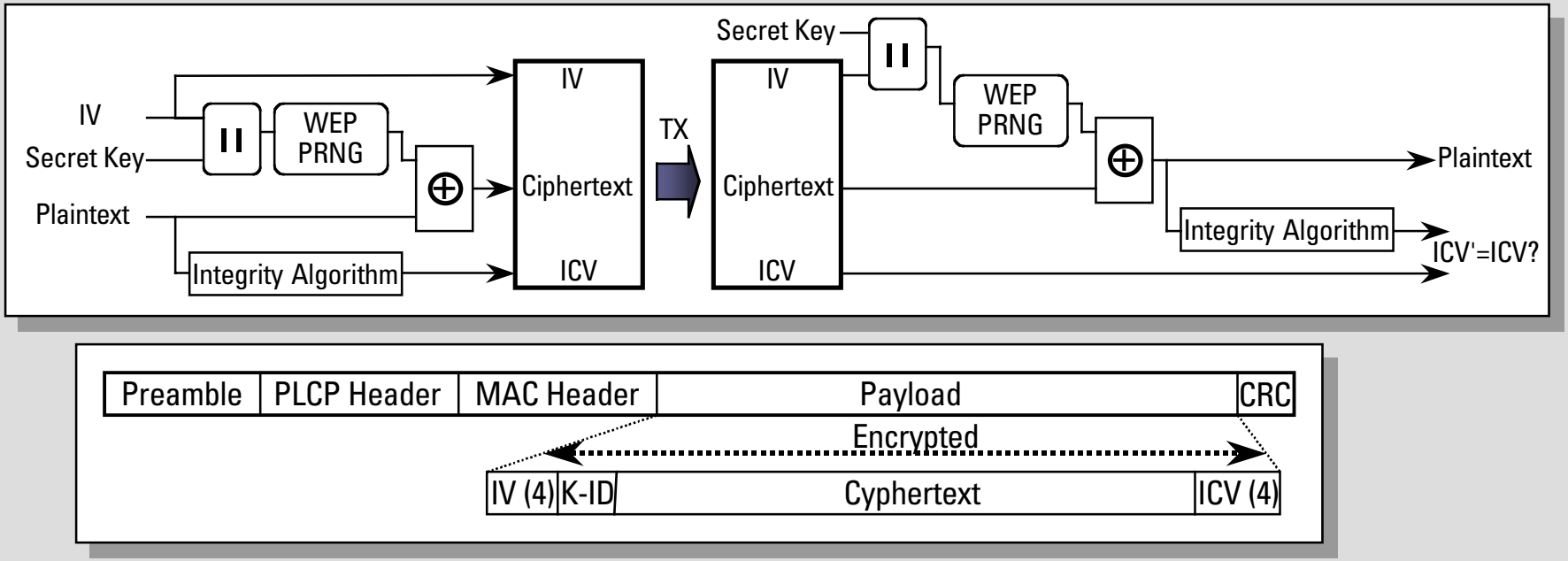
Wireless LAN IEEE802.11 Basic Architecture



IEEE802.11 privacy and access control

- Goal of 802.11 is to provide “Wired Equivalent Privacy” (WEP)
  - Usable worldwide
- 802.11 provides for an authentication mechanism
  - To aid in access control.
  - Has provisions for “OPEN”, “Shared Key” or proprietary authentication extensions.
- Shared key authentication is based on WEP privacy mechanism
  - Limited for station-to-station traffic, so not “end to end”.
  - Uses RC4 algorithm based on:
    - a 40 bit secret key
    - and a 24 bit IV that is send with the data.
    - includes an ICV to allow integrity check.

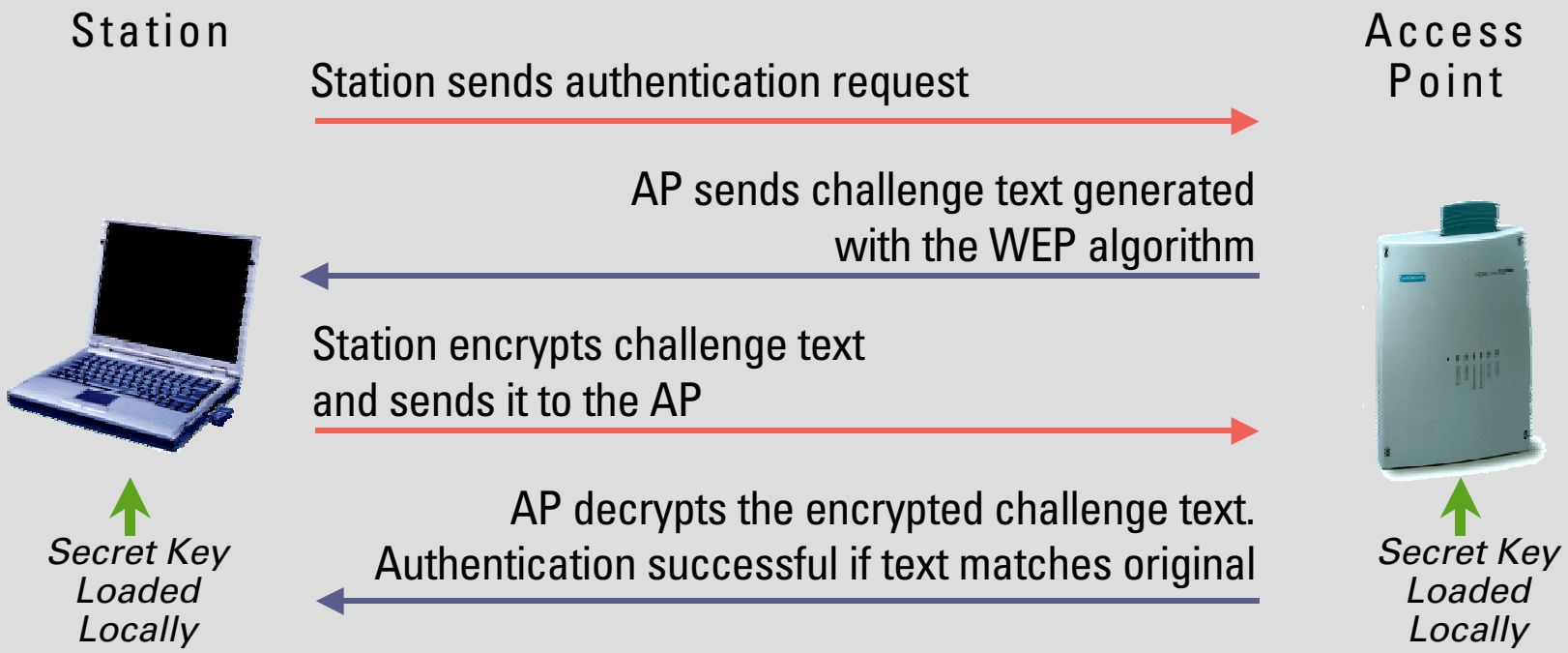
WEP privacy mechanism



- WEP bit in Frame Control Field indicates WEP used.
  - Each frame can have a new IV, or IV can be reused for a limited time.

SIEMENS

Shared key authentication



- Shared key authentication requires WEP
- Key exchange is not specified by IEEE802.11
- Only one way authentication

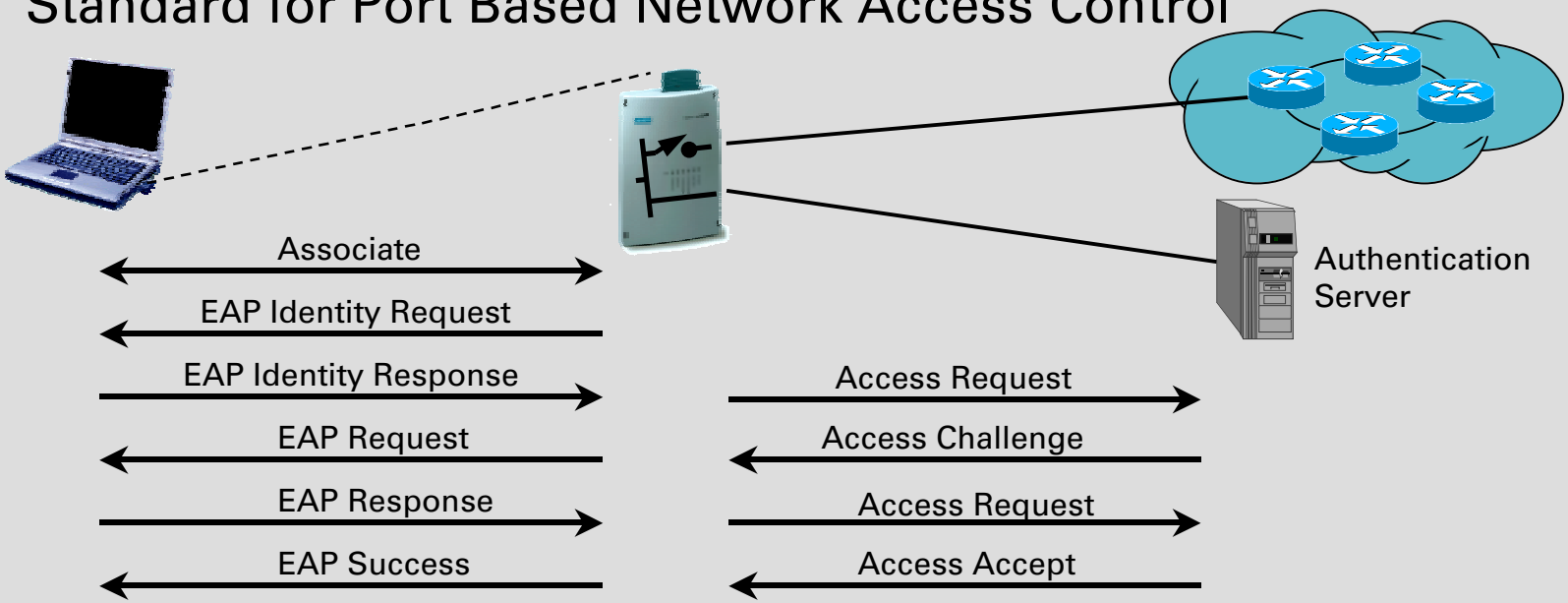
Shortcomings of plain WEP security

- WEP unsecure at any key length
  - IV space too small, lack of IV replay protection
  - known plaintext attacks
- No user authentication
  - Only NICs are authenticated
- No mutual authentication
  - Only station is authenticated against access point
- Missing key management protocol
  - No standardized way to change keys on the fly
  - Difficult to manage per-user keys for larger groups

- WEP is no mean to provide security for WLAN access,
  - … but might be sufficient for casual cases.

Eliminating the flaws: IEEE802.11i

- Enhanced encryption
  - WEP2 w/ increase IV space to 128bit, key length 128bit
  - optional: Advanced Encryption Standard (AES)
- Authentication and key management by adoption of IEEE802.1X Standard for Port Based Network Access Control



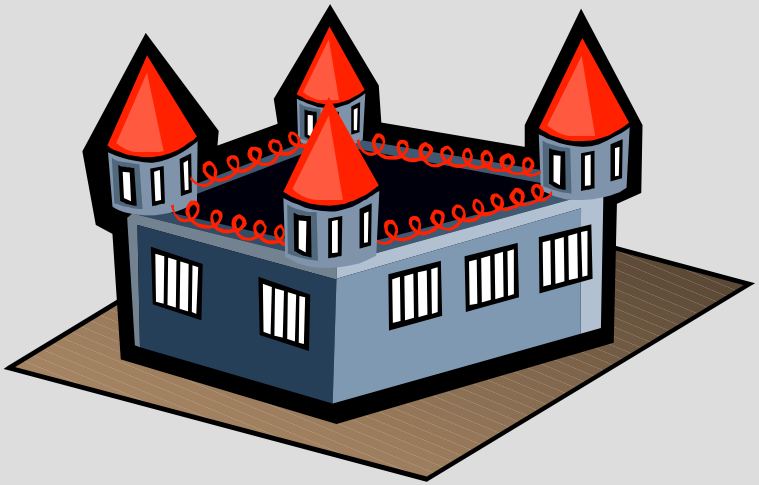
SIEMENS

Going public ...

... making
WLAN access
a business.

Probably to consider …

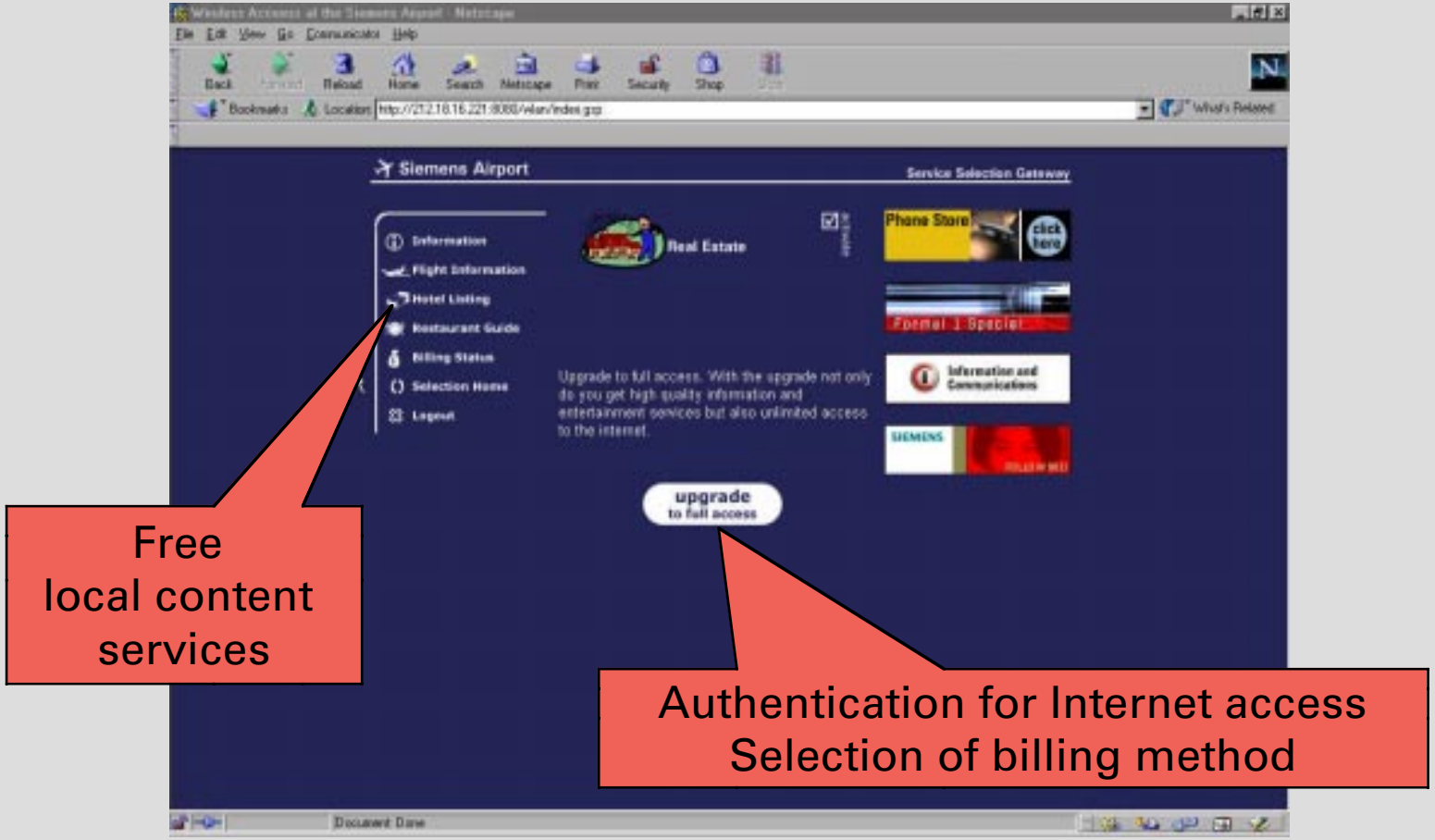
- How does your favorite storefront look like?



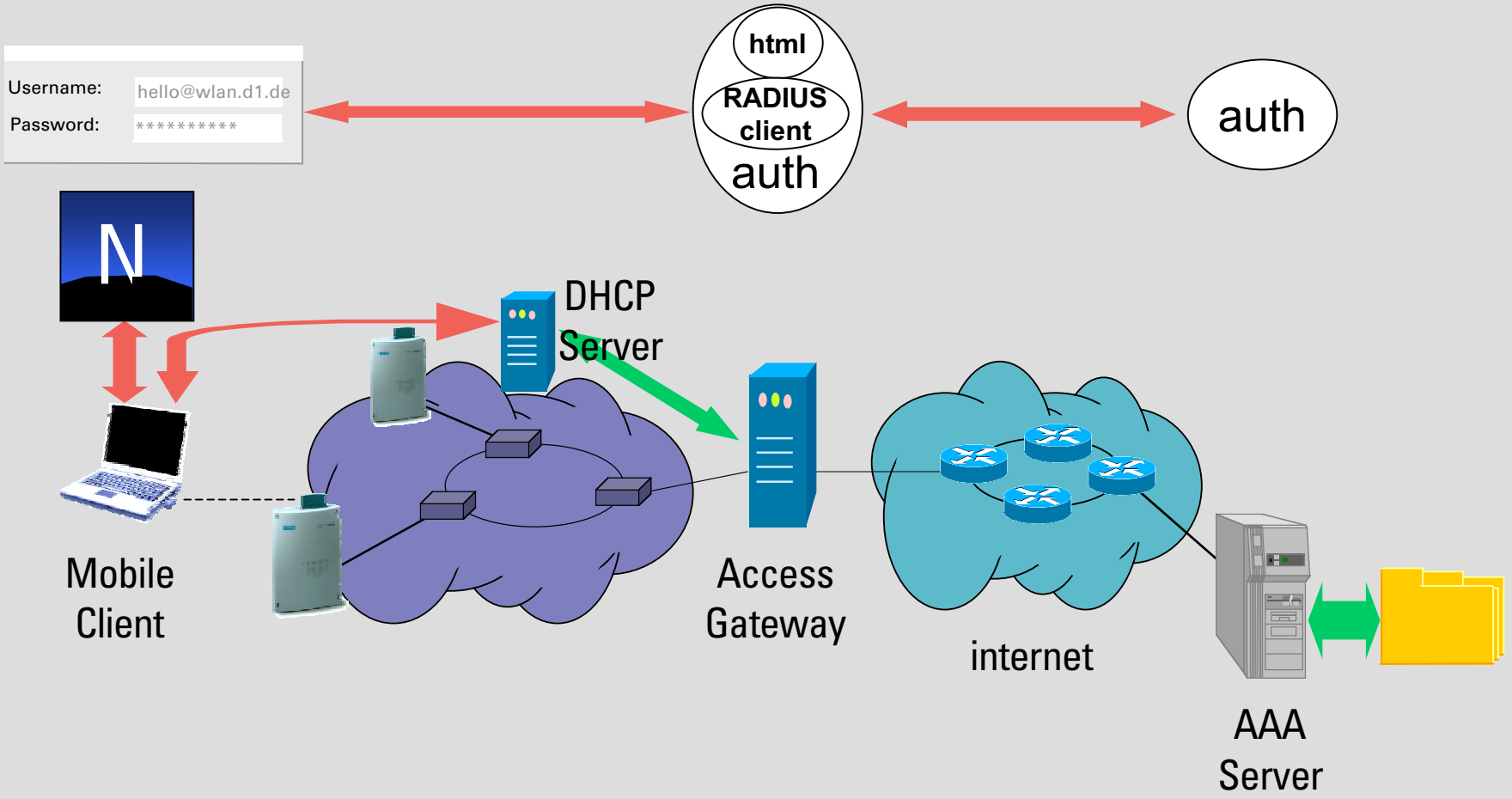
To much security might hinder your business!

SIEMENS

Using a web page for initial user interaction



Web based authentication



SIEMENS

Functions of an integrated access gateway (User management)

- Authentication via secure (HTTPS) web-based GUI for registered and unknown users based on
  - External database, supports ISP roaming via RADIUS
  - Integrated LDAP directory
  - GSM phone (Transmission of one-time passwords by SMS)
  - Credit card
- Authorization based on user profiles assigned to different user groups having particular access
  - Dynamic subscribtion to additional services
  - Personalized portal page
- Real-time accounting based on service, duration and volume
  - Instant user feedback on portal page or by SMS

SIEMENS

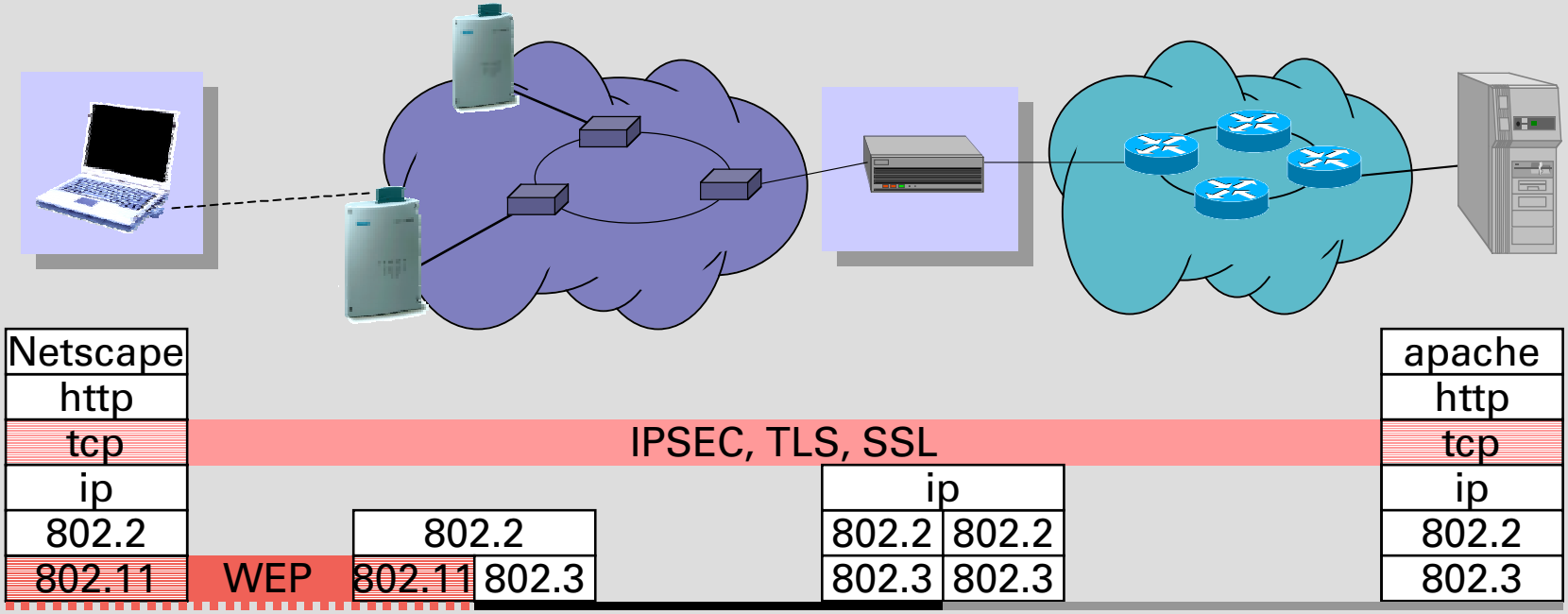
Functions of an integrated access gateway (Network services)

- DHCP server for assigning IP addresses to WLAN clients
  - Retaining session if user is temporarily out of WLAN coverage
  - Detection of session end
- Policy engine
  - Loadable user profiles
  - User-specific routing configuration
  - Dynamic firewalling rules
- IP router with NAT engine
  - Assignment of private addresses for free services
  - Must allow IPSEC connections

- Example of an integrated access gateway:
  Siemens i250 Access Gateway
  http://www.siemens.com/wlan

A last word about security:

- WEP/WEP2 is probably not sufficient in public hot-spots:



- Only VPN technologies (IPSEC, TLS, SSL) will fulfil end-to-end security requirements.
- VPN technologies might even be used in corporate networks.

Conclusions

- There is not a single solution to control acces to a WLAN
  - WEP might be sufficient for simple cases.
  - IEEE802.11i provides enough security for corporate networks.
- Public access needs a more open entrance
  - Web based authentication is a user friendly way to attract everybody.
  - Access gateways for public hotspots have broad capabilities.
- End to end security by IPSEC or TLS might fulfill the security requirements of users and can even applied for access control in corporate WLAN networks (...as Siemens is doing).

The end

- Thank you for your attention.
- Please do not hesitate to contact me if you have questions.

Maximilian Riegel
<maximilian.riegel@icn.siemens.de>
http://www.max.franken.de