sasken
Make the Right Connection

Security Issues in 802.11b WLANs - An Application Developers Perspective

Anuj Seth <anuj@sasken.com>

22nd January 2002

Workshop on Wireless Ad Hoc Networking, IISc

Copyright © 2002, Sasken
Communication Technologies Ltd.

Agenda

sasken
Make the Right Connection

- Communication Security Requirements
- 802.11b Security Architecture
- Security Issues in 802.11b
- Proposed Solutions for Enhanced Security

Copyright © 2002, Sasken
Communication Technologies Ltd.

ommunication Security equirements

sasken
Make the Right Connection

- Privacy
- Data Integrity
- Authentication

Copyright © 2002, Sasken
Communication Technologies Ltd.

802.11b Security Architecture

sasken
Make the Right Connection

- Link-layer security protocol
- Prevent link-layer eavesdropping
- Control network access
- WEP (Wired Equivalent Protocol)
- Essentially, equivalent to wired access point security

Copyright © 2002, Sasken
Communication Technologies Ltd.

/EP Requirements

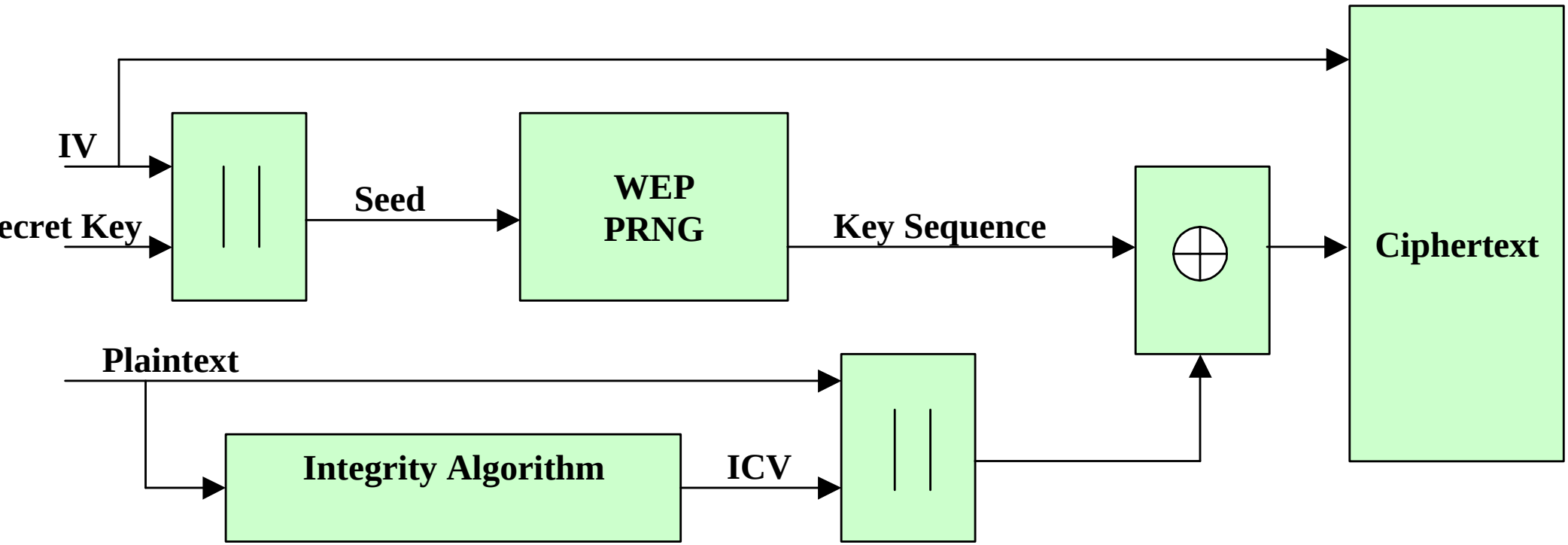
sasken
Make the Right Connection

- Reasonably Strong (??)
- Self-synchronizing
- Computationally efficient
- Exportable
- Optional

Copyright © 2002, Sasken
Communication Technologies Ltd.

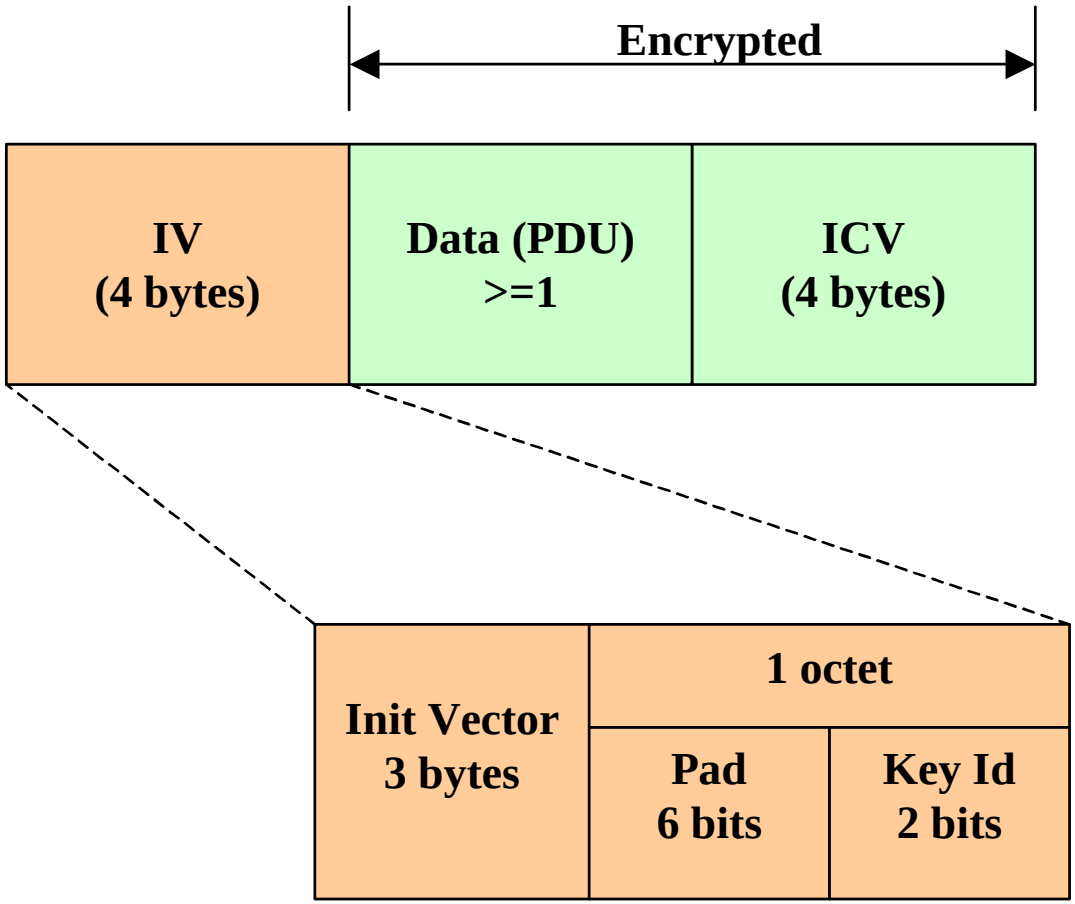
WEP Encryption

sasken
Make the Right Connection



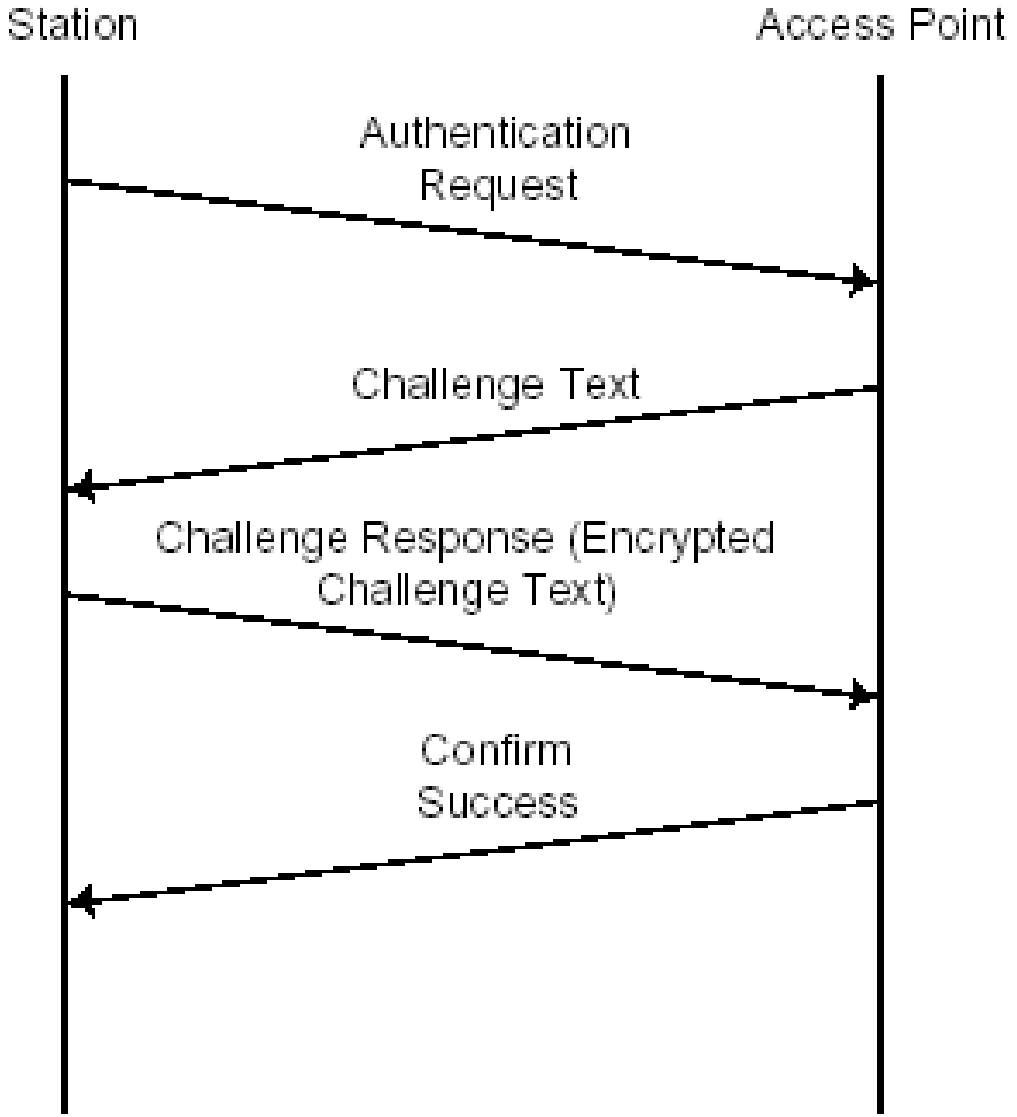
Copyright © 2002, Sasken
Communication Technologies Ltd.

WEP Data Frame (Payload)



Communication Technologies Ltd.

02.11b Shared Key Authentication



Copyright © 2002, Sasken Communication Technologies Ltd.

Security Issues

sasken
Make the Right Connection

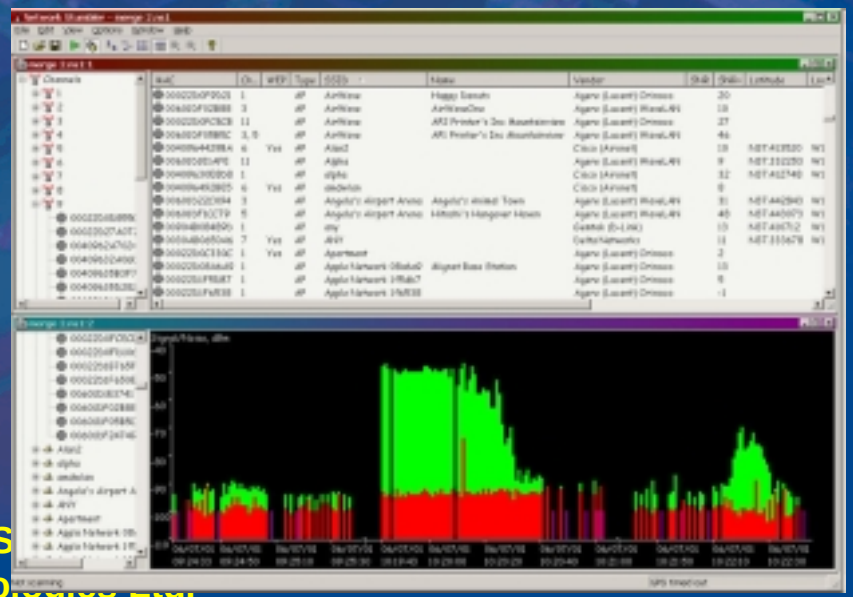
- War Driving / Sniffing
- Rogue Access Points
- MAC Address
- SSID
- WEP

Copyright © 2002, Sasken
Communication Technologies Ltd.

War Driving

sasken
Make the Right Connection

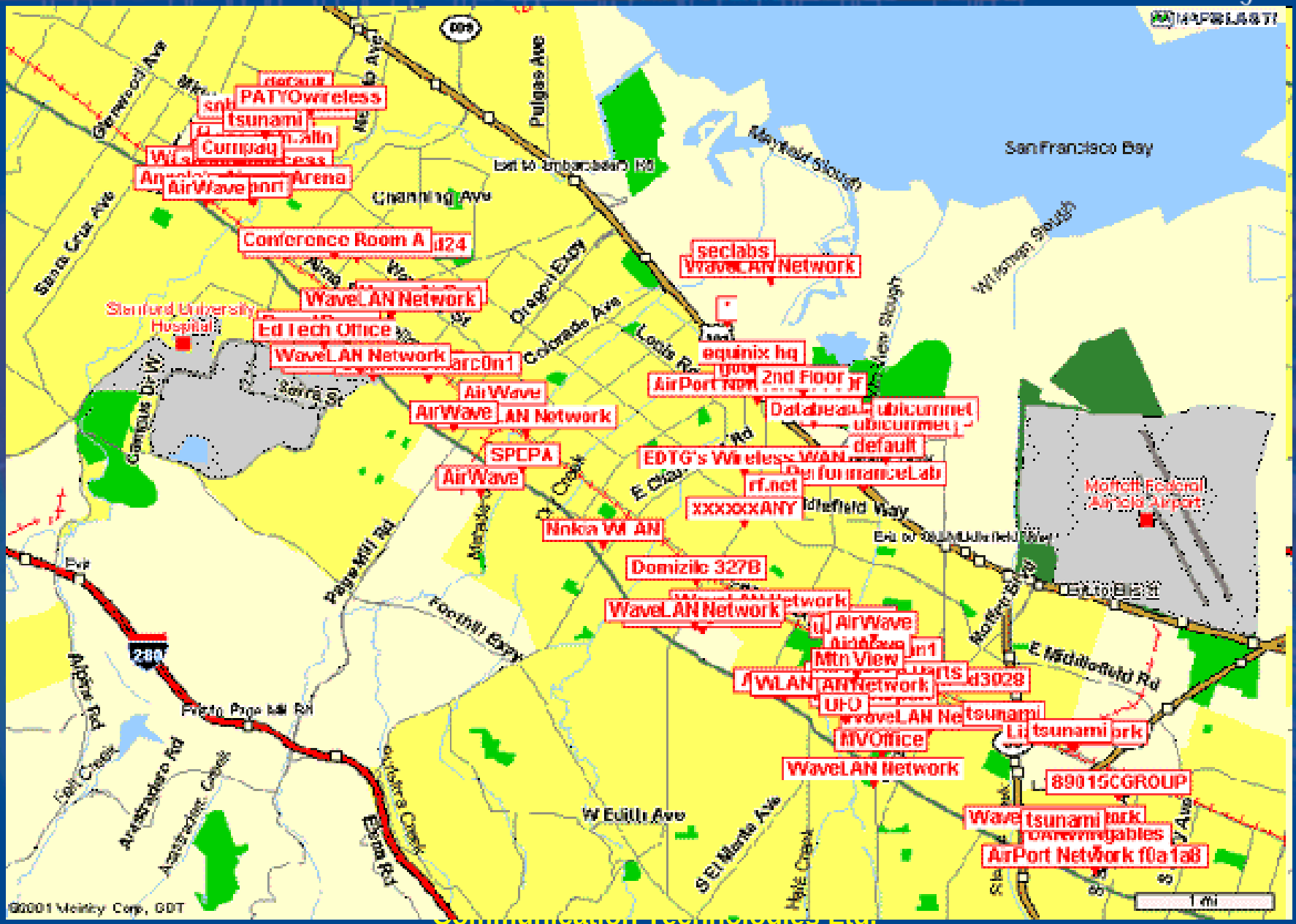
- War driving is one of the latest hacker fads
  - http://www.wardriving.com/
- Involves driving around and scanning in search of unprotected 802.11 wireless networks
- Several War Driving tools are available
  - NetStumbler
  - AiroPeek
  - MobileManager
  - Sniffer Wireless
  - THC-WarDrive



Copyright © 2002, S
Communication Technologies Ltd.

War Driving Example

sasken
Make the Right Connection



Rogue Access Points

sasken
Make the Right Connection

- Employees install access points without the knowledge of IT departments
- Security is rarely enabled
- Network becomes vulnerable to war driving / sniffing attacks

Copyright © 2002, Sasken
Communication Technologies Ltd.

MAC Address

sasken
Make the Right Connection

- Can control access by allowing only defined MAC addresses to access the network
- Complicated and difficult to maintain list of valid MAC addresses
- MAC addresses can be spoofed

Copyright © 2002, Sasken
Communication Technologies Ltd.

Service Set ID (SSID)

sasken
Make the Right Connection

- Service Set ID (SSID) is the network name given to a wireless network
- Can be used to access a specific access point by name
- The more people that come to know about the SSID the more likely that it will be misused
- Changes in SSID requires communicating it to all people who access the network

Copyright © 2002, Sasken
Communication Technologies Ltd.

Wired Equivalent Protocol (WEP)

sasken
Make the Right Connection

- Not an “industrial strength” encryption protocol
- Vulnerable to attack
  - Passive attacks to decrypt traffic based on statistical analysis
  - Active attacks to inject new traffic from unauthorized mobile stations, based on known plaintext
  - Dictionary-building attack that, after analysis of a day’s worth of traffic, allows real-time automated decryption of all traffic
- All users share the same encryption key
- Data headers are not encrypted
- Initialization Vector (IV) Misuse
- Weakness in RC4’s Key Scheduling Algorithm

Copyright © 2002, Sasken
Communication Technologies Ltd.

ttacks on WEP

sasken
Make the Right Connection

Downloadable procedures

To crack the key

- AirSnort: http://airsnort.sourceforge.net/
- WEPCrack: http://sourceforge.net/projects/wepcrack/

To brute force enter into WLAN

- THC-RUT: www.thehackerschoice.com/releases.php

Copyright © 2002, Sasken
Communication Technologies Ltd.

Proposed Solutions to Enhance Security

sasken
Make the Right Connection

- Virtual Private Network (VPN)
- Secure LAN (SLAN)
- Remote Authentication Dial In User Services (RADIUS
- IPsec
- 802.1x
- Proprietary WEP Implementations

Copyright © 2002, Sasken
Communication Technologies Ltd.

PN

sasken
Make the Right Connection

Enables you to send data between two computers across a shared or public network in a manner that emulates th properties of a point-to-point private link

Provides a scaleable authentication and encryption solution

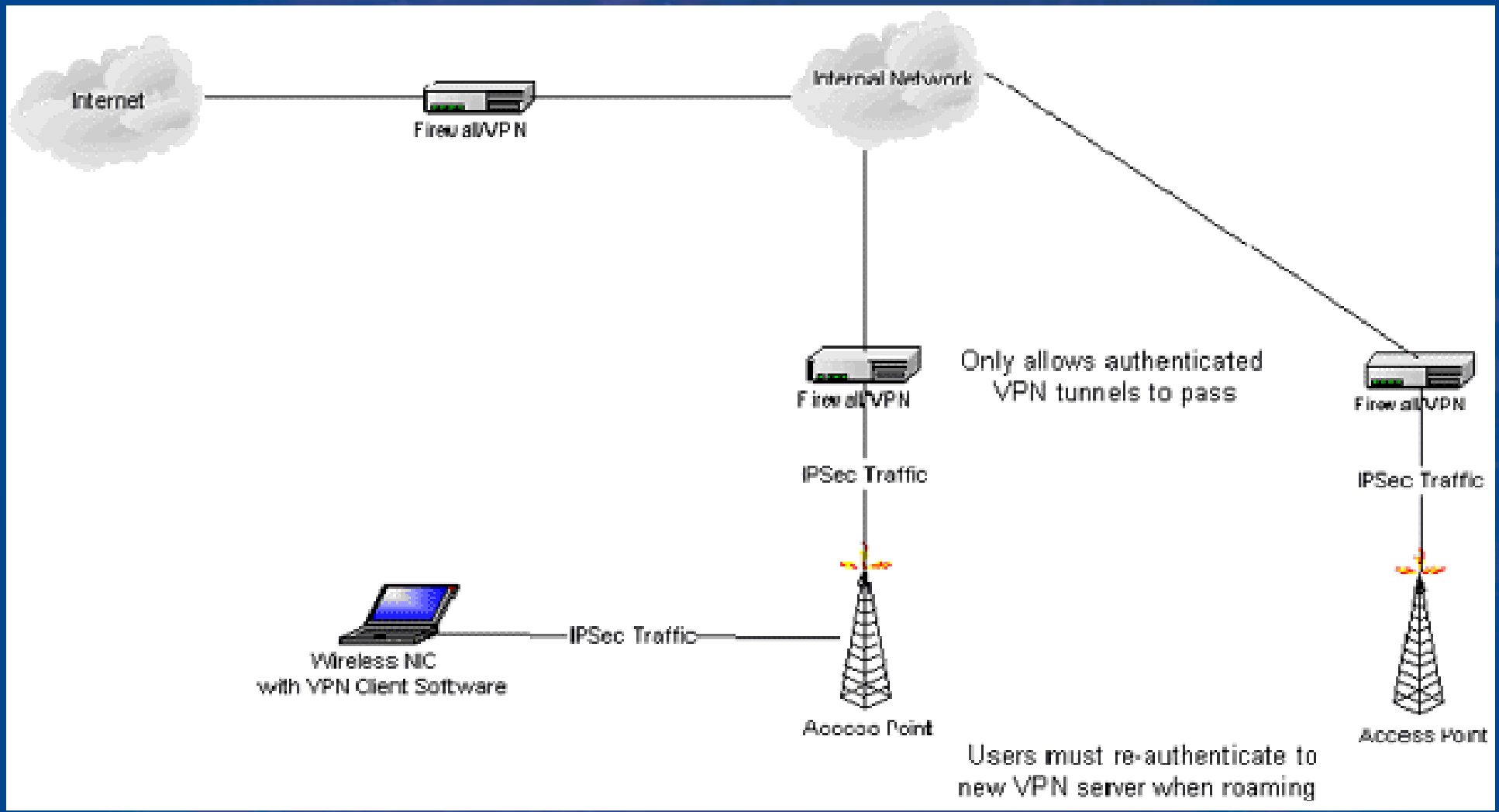
Does require end user configuration and a strong knowledge of VPN technology

Users must re-authenticate if roaming between VPN servers

Copyright © 2002, Sasken
Communication Technologies Ltd.

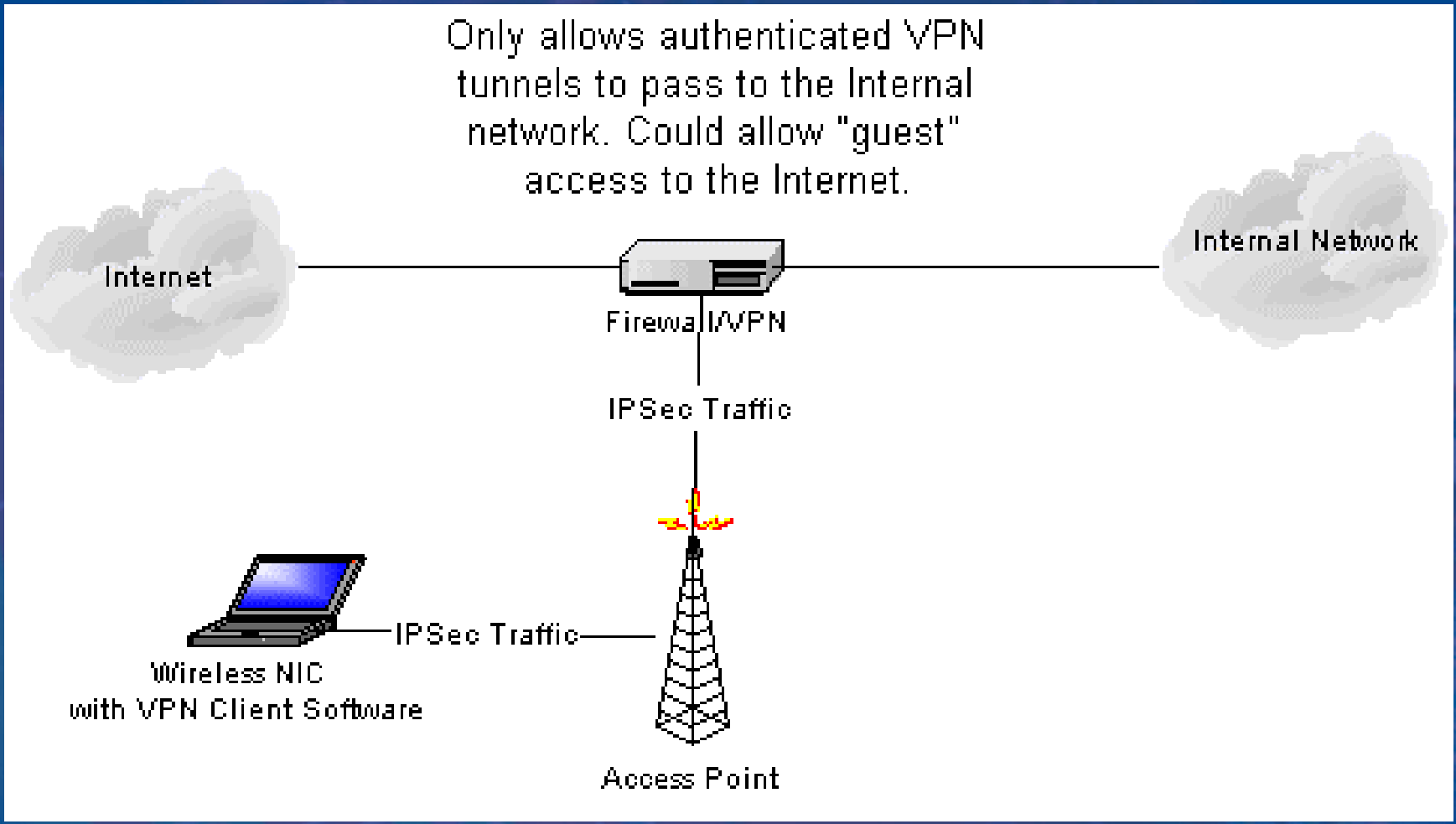
PN Architecture

sasken
Make the Right Connection



Copyright © 2002, Sasken
Communication Technologies Ltd.

PN Architecture (contd.)



Copyright © 2002, Sasken
Communication Technologies Ltd.

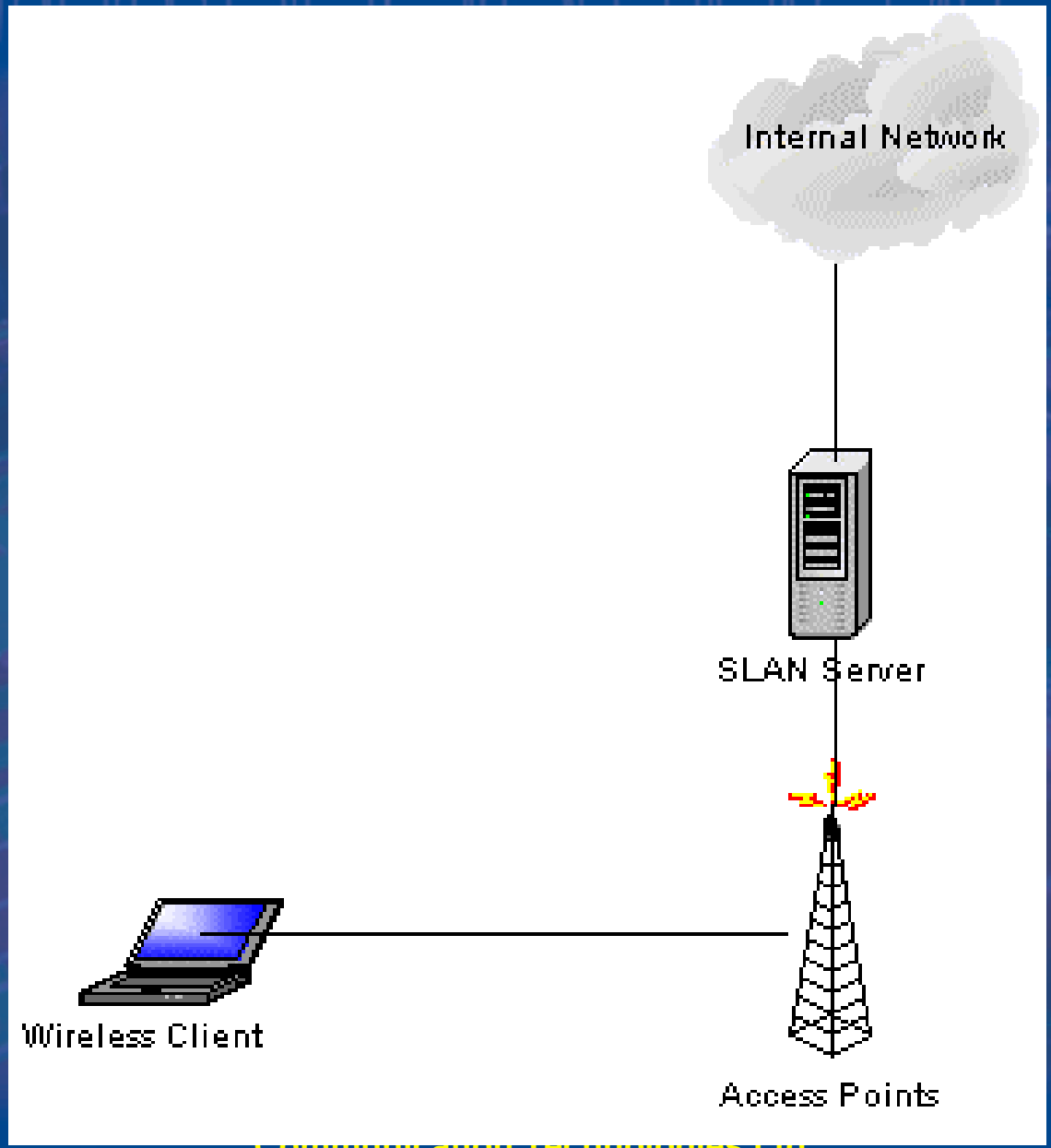
Secure LAN (SLAN)

sasken
Make the Right Connection

- A GPL open-source “VPN” System
- Provides server authentication, client authentication, data privacy, and integrity using per session and per user short life keys
- Simpler and more cost efficient than a VPN
- Support for Windows and Linux
- Website: http://slan.sourceforge.net/

Copyright © 2002, Sasken
Communication Technologies Ltd.

LAN Architecture



ADIUS

sasken
Make the Right Connection

Several 802.11 access points offer RADIUS authenticatio

Clients can gain access to the network by supplying a username and password to a separate server

This information is securely sent over the network eliminating the possibility of passive snooping

Copyright © 2002, Sasken
Communication Technologies Ltd.

Psec

sasken
Make the Right Connection

Provides encryption and authentication services at the I
level of the network protocol stack

Can be used to secure nearly any type of Internet traffic

Legacy applications not implementing secure communications can be made secure using IPsec

Examples:

- Free S/WAN - http://www.freeswan.org/

Copyright © 2002, Sasken
Communication Technologies Ltd.

IPsec - Disadvantages

sasken
Make the Right Connection

- IPsec authenticates machines, not users
- IPsec does not stop Denial-of-Service attacks
- IPsec is not true end-to-end security
- IPsec cannot be secure if your system isn't

Copyright © 2002, Sasken
Communication Technologies Ltd.

02.1x

sasken
Make the Right Connection

Provides enhanced security for users of 802.11b WLANs

Provides port-level authentication for any wired or wireless Ethern
client system

802.1x was originally designed as a standard for wired Ethernet, bu
is applicable to WLANs

It leverages many of the security features used with dial-up
networking (RADIUS)

Also uses Extensible Authentication Protocol (EAP, RFC 2284)

Built in support in Windows XP

Copyright © 2002, Sasken
Communication Technologies Ltd.

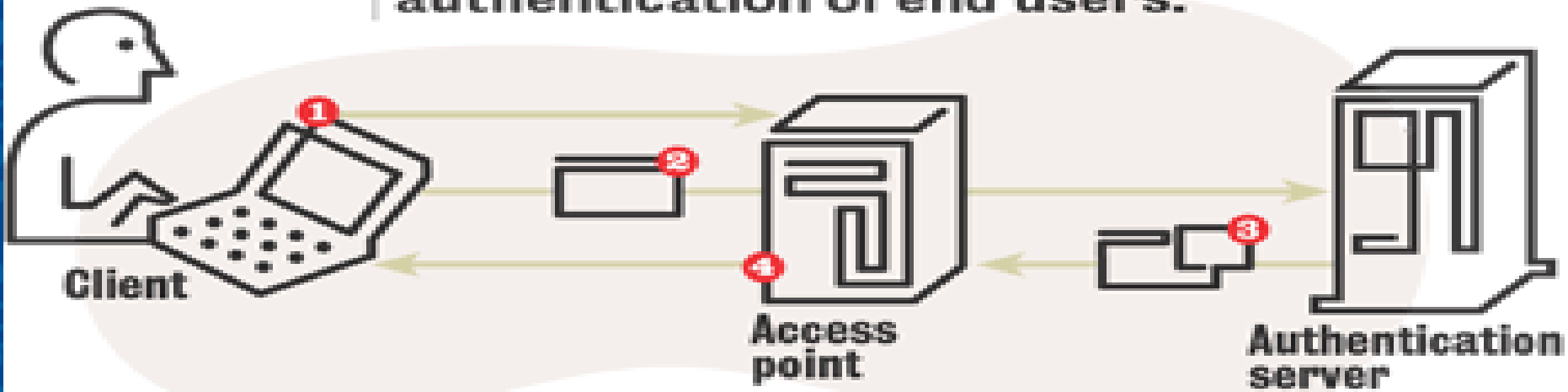
02.1x Authentication

sasken
Make the Right Connection

802.1X Authentication

HOW IT WORKS

802.1X authentication for wireless LANs provides centralized, server-based authentication of end users.



1. A client sends a "start" message to an access point, which requests the identity of the client.
2. The client replies with a response packet containing an identity, and the access point forwards the packet to an authentication server.
3. The authentication server sends an "accept" packet to the access point.
4. The access point places the client port in authorized state, and traffic is allowed to proceed.

Copyright © 2002, Sasken
Communication Technologies Ltd.

roprietary WEP Security

sasken
Make the Right Connection

Dynamic Key Refresh instead of static keys

Use of 3DES/AES instead of RC4 (NetMotion Wireless)

Disadvantages:

- Interoperability Issues (non-WiFi Compliant)

Copyright © 2002, Sasken
Communication Technologies Ltd.

onclusion

sasken
Make the Right Connection

Wireless LANs are very useful and convenient, but curre
security state not ideal for sensitive environments

Care must be taken before sensitive information is made
available over Wireless LANs

Copyright © 2002, Sasken
Communication Technologies Ltd.

sasken
Make the Right Connection

sasken
Make the Right Connection

Thank You

Please visit our website at
www.sasken.com

Sasken Communication Technologies Limited

Copyright © 2002, Sasken
Communication Technologies Ltd.