An Overview of the CHOICE Network

Victor Bahl

http://research.microsoft.com/~bahl

December 18, 2000

Demos you will see today

CHOICE – Phase 1

- Demo 1 – Network advertisement, user authentication, access enforcement, security, accounting, and mobility management

CHOICE – Phase 2

- Location based personalized services
  - Demo 2 – Location based buddy list
  - Demo 3 – Mall On-Sale Service

Broadband Wireless Internet Access in Public Places

The CHOICE Network - Phase 1

Global authentication, Local access, First-hop security, Accounting, Differentiated Service, Mobility management & Auto-configuration

The Choice Network Project: Motivation

Enable high speed wireless internet access in public places (e.g. hotels, conferences, malls, airports)

- WLAN much faster than 3G cell phones

Design, implement, and deploy a network service that grants *secure, customized, and accountable* network access to *possibly unknown* users

A system that

- protects users and network operators
- supports different business models
  - e.g. free intranet and/or fee-based internet access
- makes access seamless and robust
  - Multiple authentication schemes for first-time users
  - Bootstrap network accesses for mobile clients
  - Scale to large network settings
  - Tolerate system failures

Review: Existing Access Mechanisms

Mostly built for enterprise networks

Layer-2 Filtering

- MAC based filtering – is on its way out
- Shared key encryption – is being used today
  - …but key management is broken

Several Problems:

- Network can be compromised easily
  - Key is flashed into the card
  - Large-scale re-keying very difficult
- User-level authentication is not available
  - No way to track who is using the network and how it is being used

Prior Research

- Authenticated DHCP @ UCB (1996-97)
- The NetBar System @ CMU (1997-98)
  - Dedicated specialized CISCO routers
- Secure Public INternet ACcess Handler @ Stanford (1997-99)
- InSite @ University of Michigan (1997)
  - Similar to CMU system

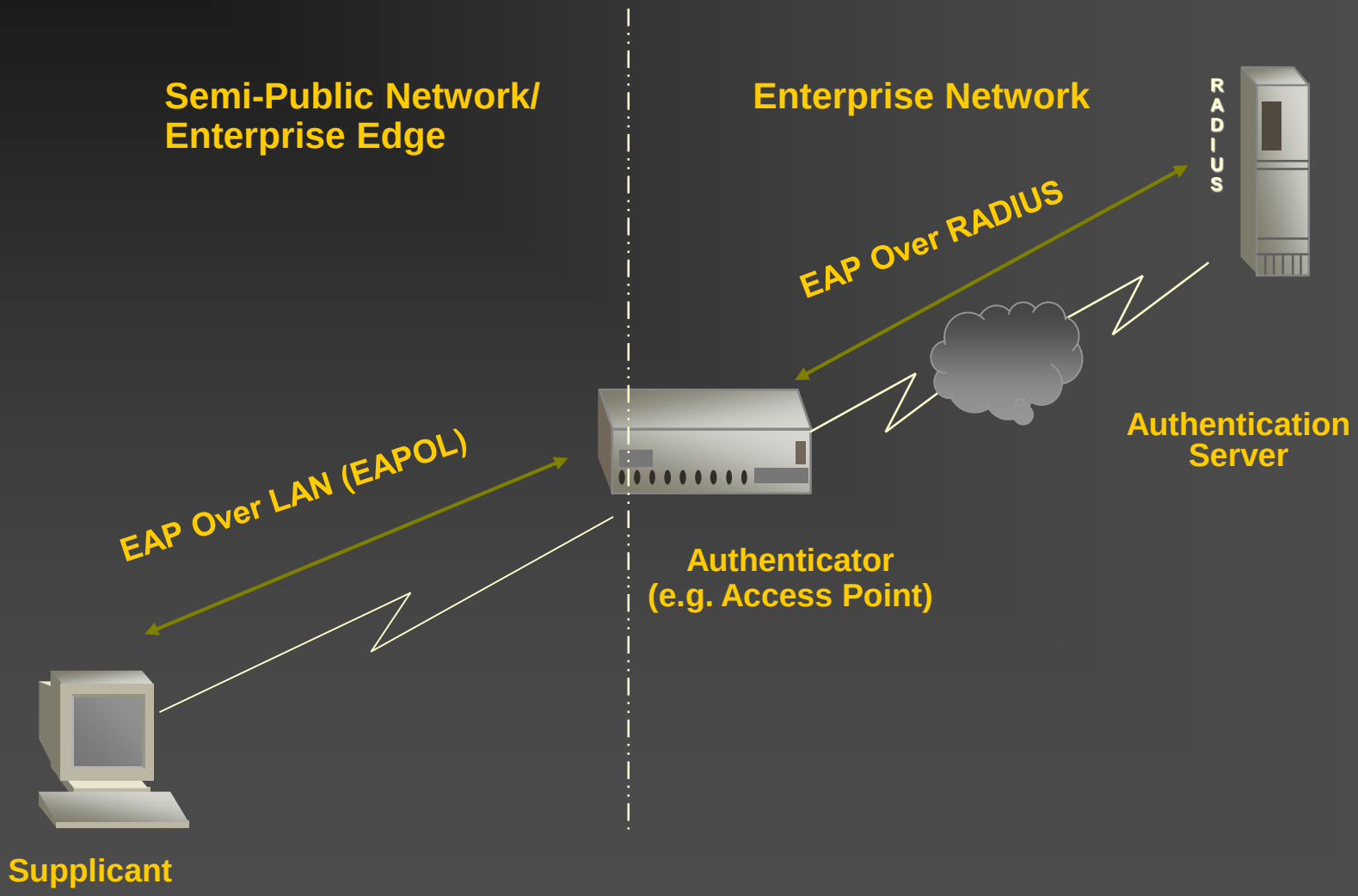
Shortly after we started

- IEEE 802.11 also recognized the problem with authentication and key distribution and issued a call for proposals.
- Simultaneously Windows NT group started working with IEEE 802.1x designing a security solution.
  - MS proposed EAPoE to the IEEE standard's body.

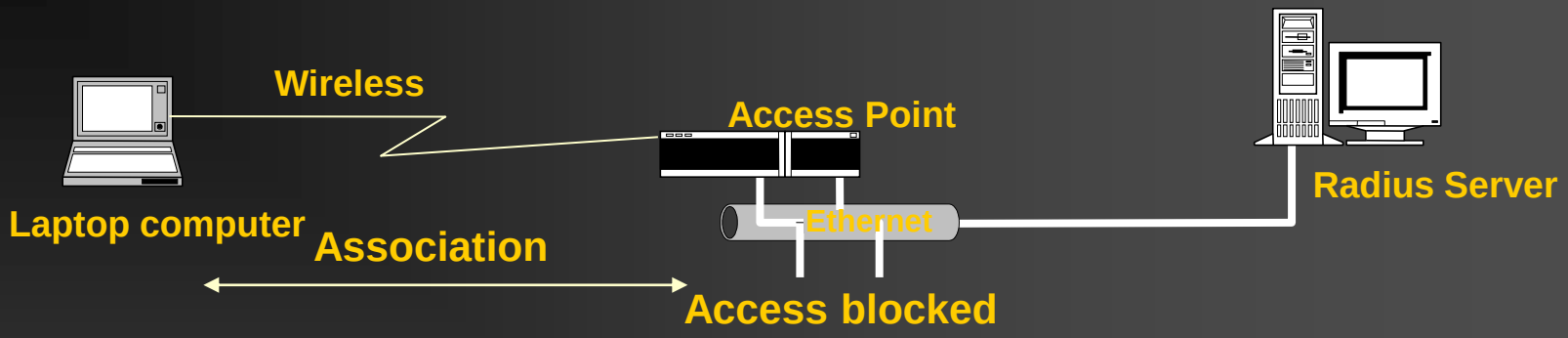
A Primer on IEEE 802.1X

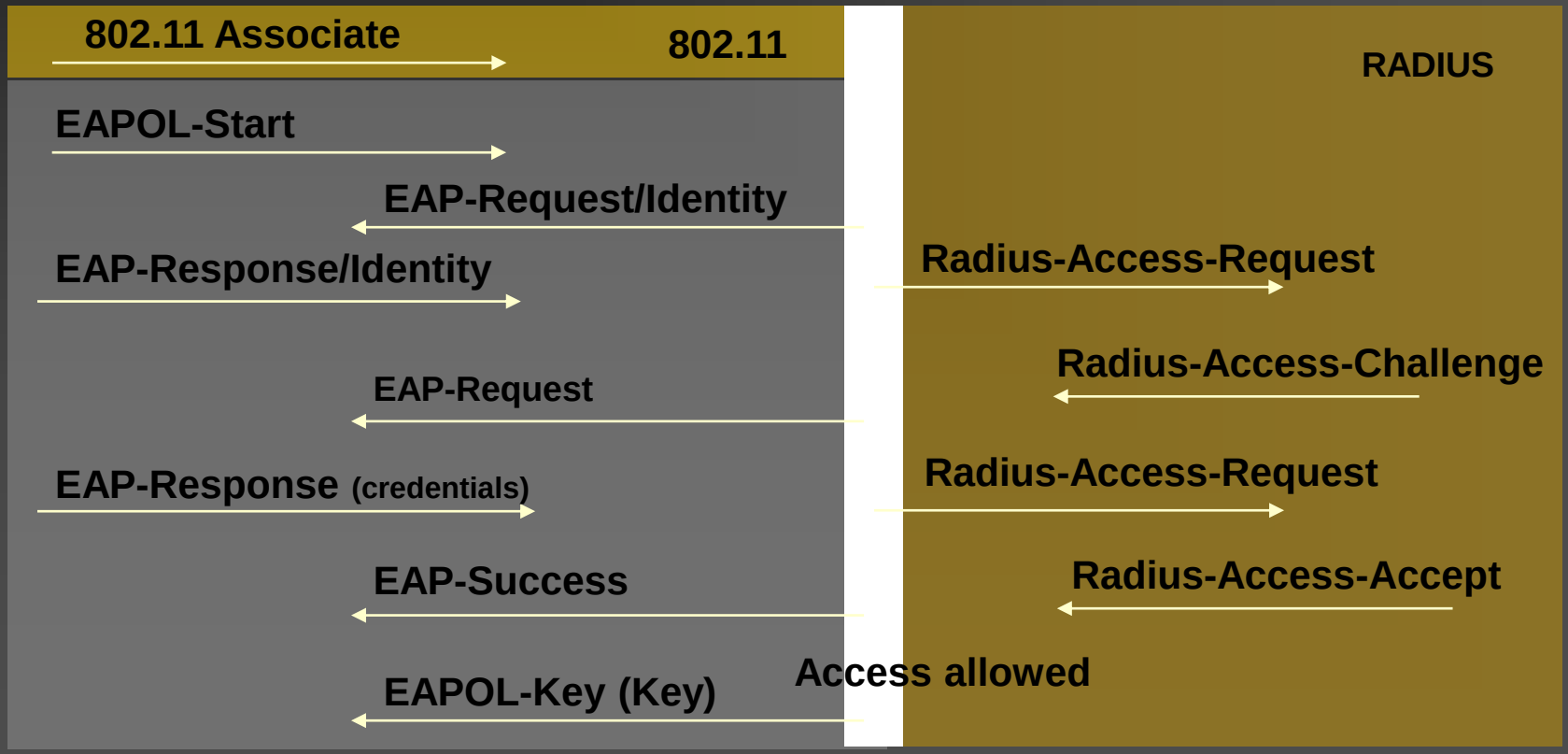
- Network port based access control mechanism
  - layer-2 authentication
  - EAP over 802.11 (EAPoE)
  - Similar in flavor to the UC Berkeley proposal
- AP treats EAP encapsulated Ethernet frames with a specific multicast address in a special way
- AP forwards these packets to an authentication server (RADIUS)
- IPSEC between AP and RADIUS server
- After authentication RADIUS passes key to AP which passes it over to the client

802.1X Network Topology



802.1X on 802.11





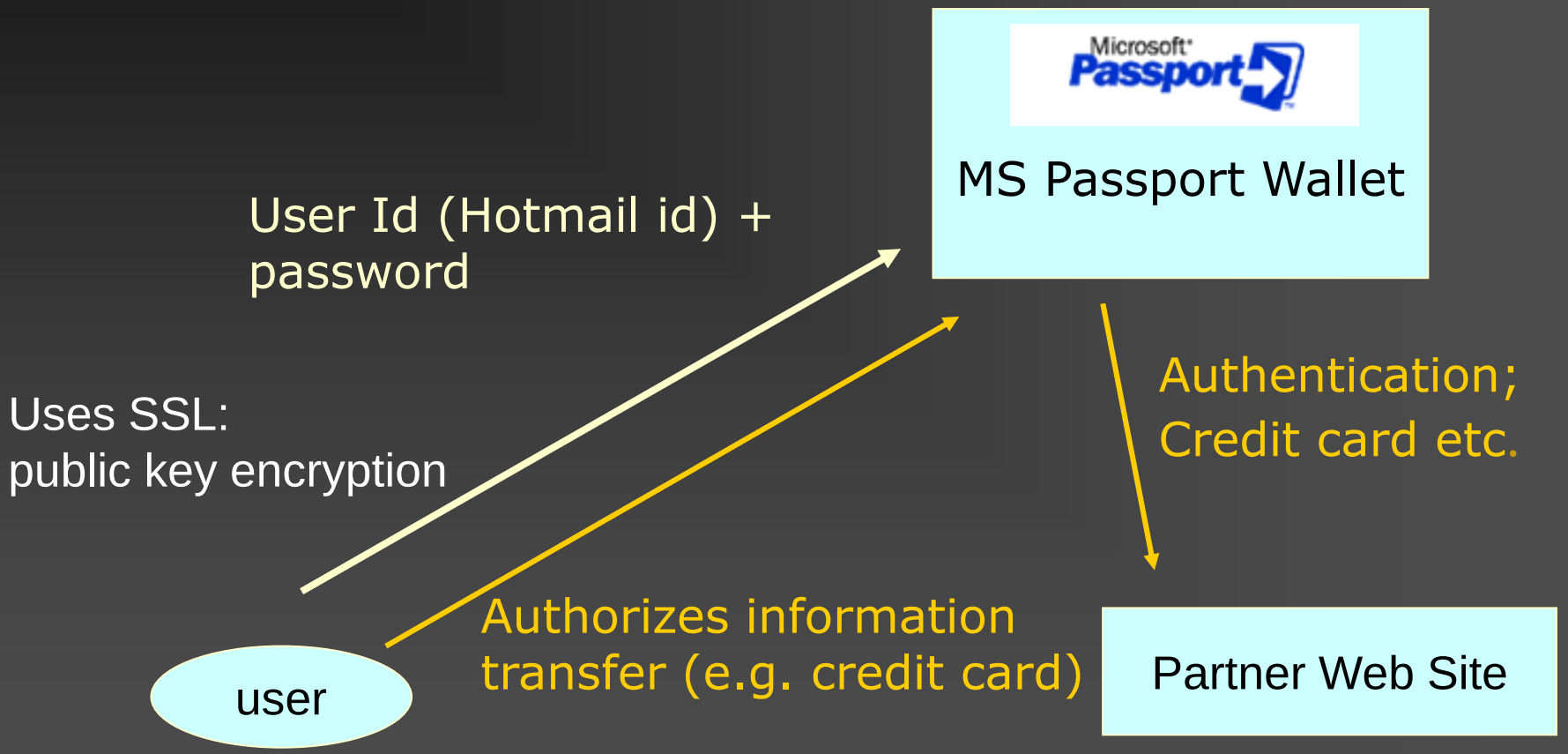
802.1x in Public Places – Deployment Issues

- Requires specialized AP hardware
- Requires support in the base stack
- Requires RADIUS (AAA) backend
- Uses TLS which requires user certificates
- http/SSL based Passport authentication not supported
- Handoff latency is high, VoIP calls may be a problem for mobile users
- Not a complete solution (will show next)

802.1x works well in enterprise networks

A Primer on MS Passport (Global Authenticator)

http://www.passport.com



The CHOICE Network

Focuses on wireless Internet connectivity & location services in public places

Built-in features

- IP address management
- Global authentication
- Comprehensive billing
- Packet level accounting
- Secure for both users and network operators
- Policy based services
- Mobility management bet. networks
- Differentiated service levels (VoIP)
- Improved battery/device lifetime
- Location-aware applications
- Local content provider

- Easy to deploy
- Future-proof
  - Hardware- and IP version agnostic

http://choice

Service Models in CHOICE

Model 1: Free access to local resources

- A non-routable IP address is provided without requiring authentication
- Intranet access allowed
  - e.g. Mall portal, splash screens, indoor navigation service, coffee ordering etc.
- Payment is implicit – drives resident business for the host organization

Model 2: Authenticate and pay

- Allows access to the Internet
- Allows applications like location-based buddy list, spontaneous sales that are based on profiles etc.
- Differentiated charging

CHOICE Components

Authorizer, Verifier, and Client

Authorizer

- Runs network announcer daemon – *announce.exe*
- Manages authentication, key generation, distribution & expiration – *getkey.asp*
- Interacts with *Verifier* and *Client*

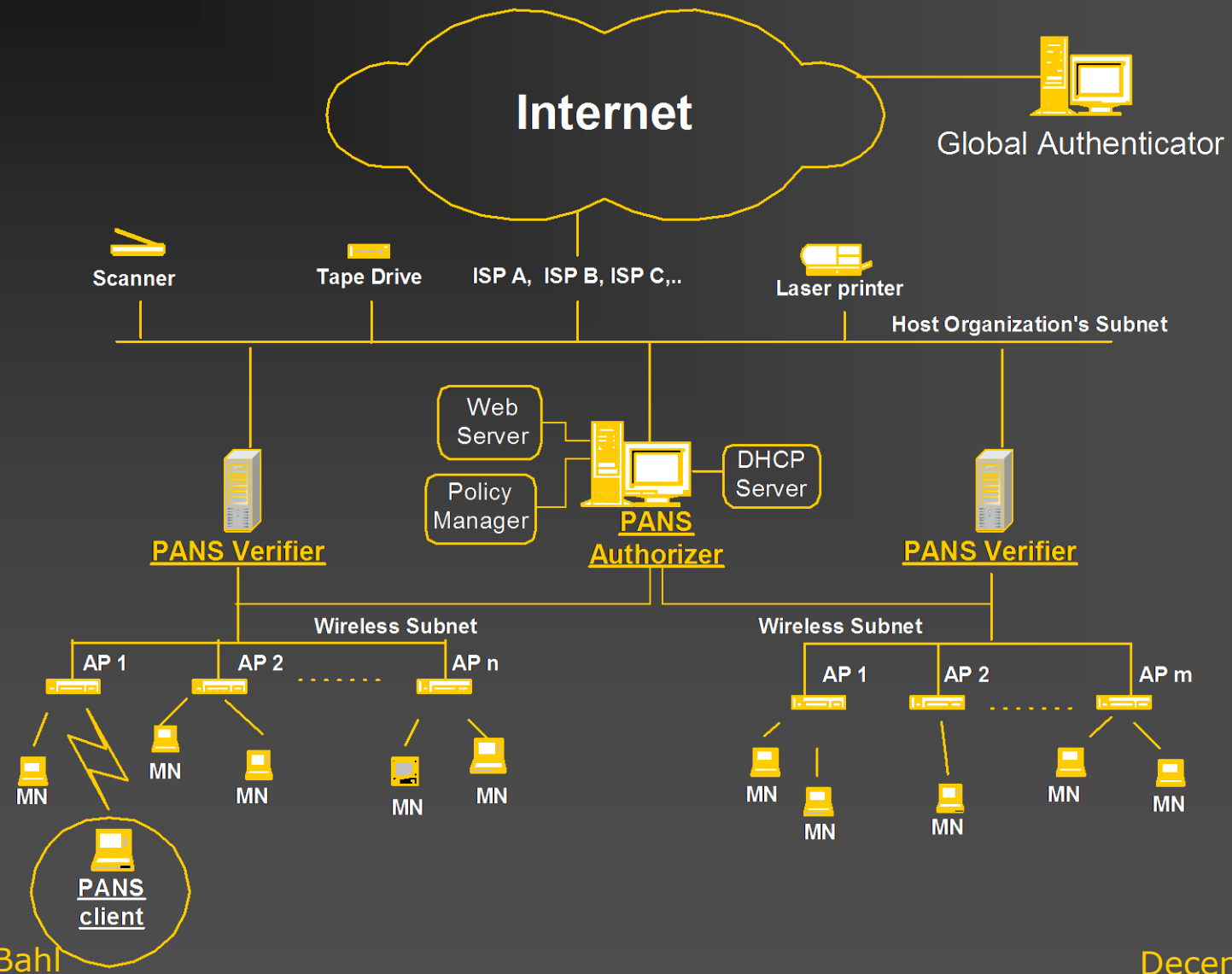
Verifier

- NDIS IM driver - *pansKLVe.sys* – decrypts packets, verifies key validity for every passing packet, keeps account of packets processed per user, enforces service levels

Client

- Detector daemon – *detect.exe* – locates CHOICE network
- NDIS IM driver *pansKLCl.sys* – tags and encrypts packets

CHOICE Edge-Server Architecture



Bootstrapping Network Access

- Authorizer advertises CHOICE via lightweight beacons
- User's machine gets a non-routable IP address (DHCP) and default gateway
- On-site network access software installation is supported for first-time users
- Network discovery logic enables / disables network access protocol

Discovering the CHOICE Network

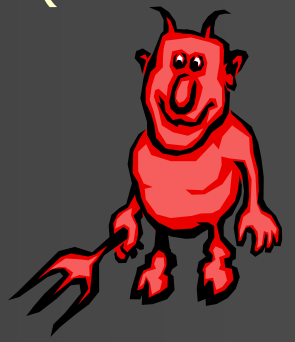
Basic Beacon

(IP Broadcast)
Advertised at random intervals with
average frequency ≈ 1 per second

For mobility management - Advertise both IP addresses to allow controller daemon to bypass or proceed with authentication Process *(*will become clear later)

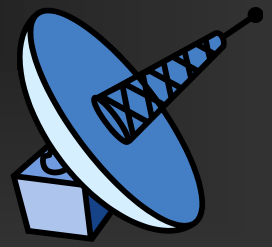
Controller Daemon Manages Network Access

Controller Daemon
(on Mobile)



- For first-time users, downloaded from *Authorizer* and installed on-site

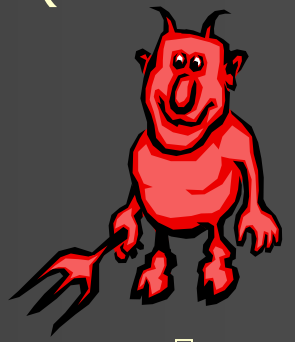
Network Access Service Discovery



Announcer Daemon
(on Authorizer)

beacon

Controller Daemon
(on Mobile)



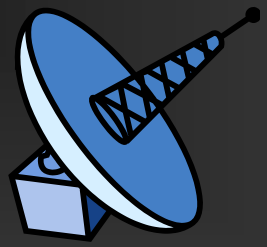
Authorizer

- IP address (DHCP)
- Set Default Gateway
- Prompt User

Authentication in CHOICE

- User “logs-on” to a global authenticator (e.g. MS Passport)
  - Web based User Interface
  - Credentials are passed via end-to-end SSL connection. WLAN provider is not privy to credentials
- *Authorizer* generates time-bounded session key and sends it to client via SSL and to the *Verifier* via IPSEC
- Client sets *Verifier* as a gateway and tags every outgoing packet using key
- *Verifier* un-tags packet, checks key, does integrity check, checks service policy, and forwards packet.
- Certificates guarantee legitimacy of *Authorizer* and *Verifier*

User Authentication



Announcer Daemon
(on Authorizer)

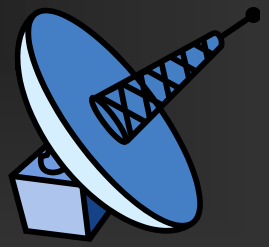
beacon

Controller Daemon
(on Mobile)

Authorizer

- User performs authentication
- Daemon waits for response from *Authorizer*

Key Distribution



Announcer Daemon
(on Authorizer)

beacon

Controller Daemon
(on Mobile)

Authorizer

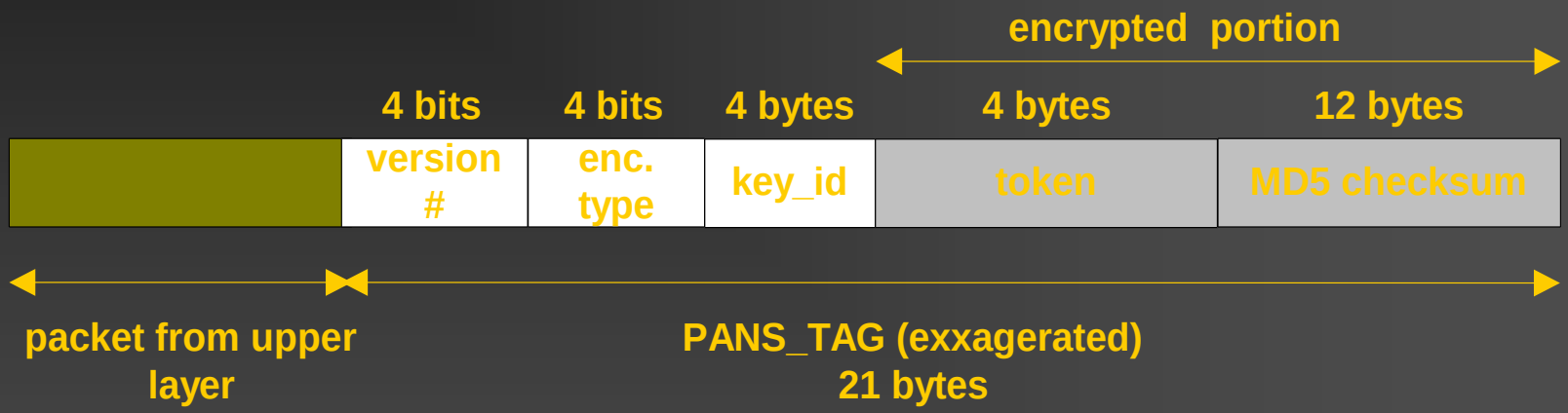
MIME over
SSL

Keygive

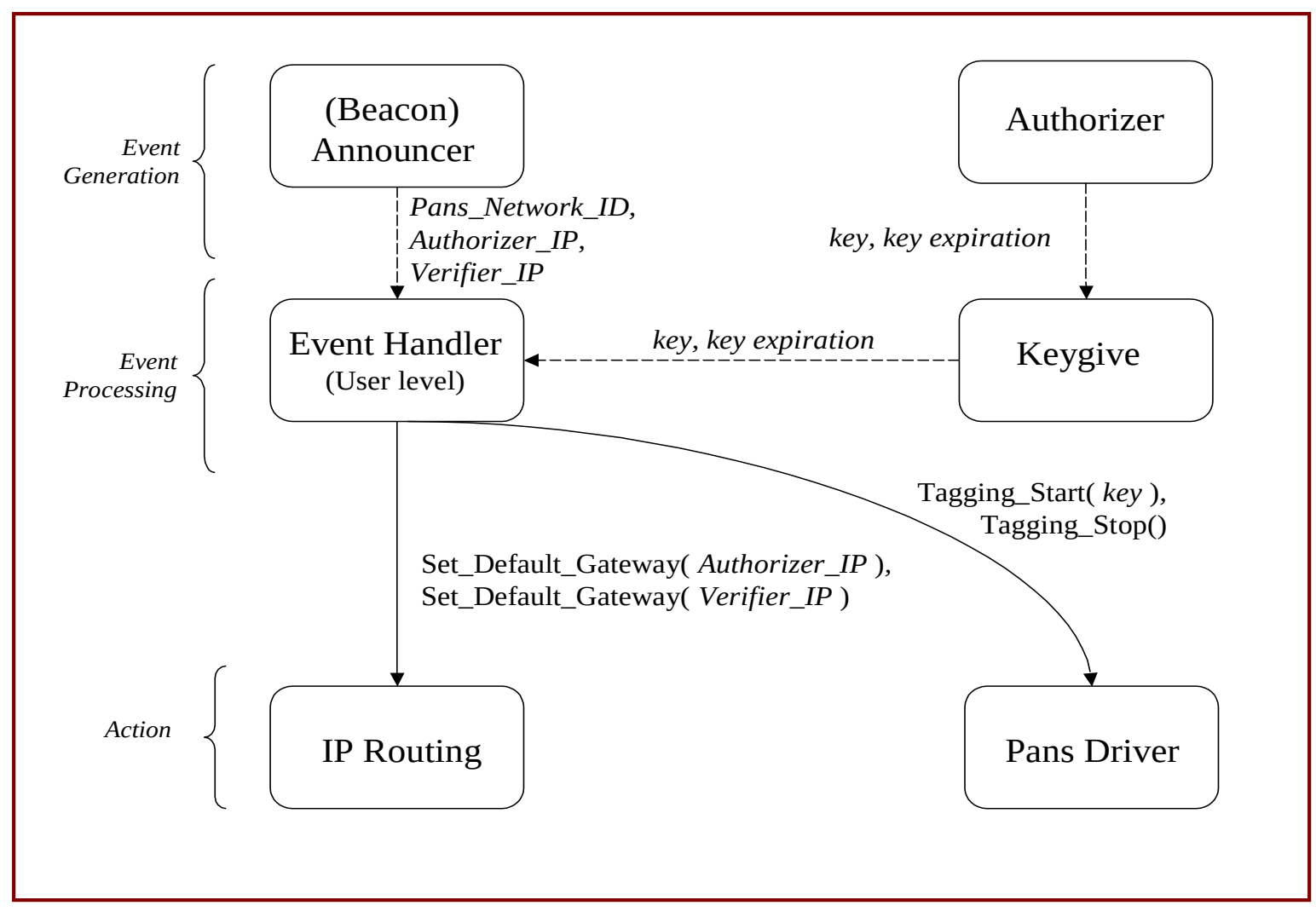
key

- User-level program receives key, redelivers to daemon
- Set default gateway
- Enable packet tagging

Packet Tagging



In a Nutshell: Auto Configuration



Service Negotiation in CHOICE

Different levels of service offered as part of “log-in”

- First-hop provider negotiates with ISPs and offers the best available rate to users

Policies take into account special user contracts

- MCI, AT&T deals for home phone customers
- Corporate discounts
- Gold Club member benefts etc.

Access Enforcement in CHOICE

- Access control is per packet based
- An encrypted secret code is placed in each packet for different levels of service
  - Premium Service (e.g. unlimited BW, higher level of security, location services,…)
  - Basic (e.g. limited BW e.g. *$ C_0 for n kilobits transferred,* Medium to no security, …)
- Quota overflow is regulated at the client and enforced by the *Verifier*
- Encryption is a combination (secret code, sequence number) – more later

First-Hop Security in CHOICE

- Software based - Upgrade easily
  - Download latest encryption code into clients and servers
  - Unlike WEP no need for upgrades to AP hardware
- Encryption method is flexible

  Client negotiates with servers at attachment time
  - 3DES, RC4, ECC etc. [3DES is implemented]
- Key length is flexible
- Key can be changed multiple times in a session
  - Frequency set by the server/client
- Data integrity obtained via MD5 checksum

Mobility Management in CHOICE

Network Discovery

- Already discussed

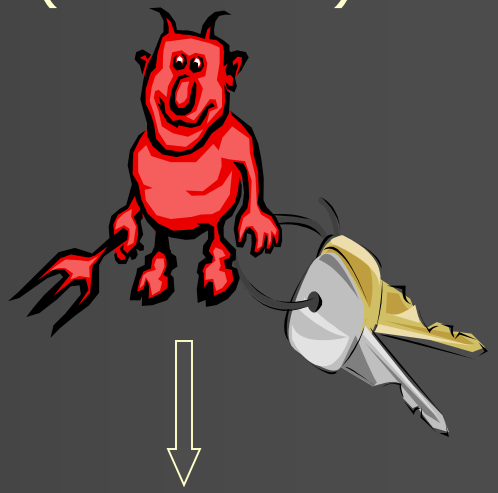
Key Management for handling mobility

- Store/invalidate session keys collected from multiple networks
- Roaming: always bypass authentication process if possible
- Renew keys within a session to enhance security

Mobile Client Leaves

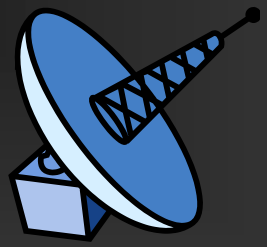
No Beacon heard for a while

Controller Daemon
(on Mobile)



- Disable tagging
- Restore client's default network setting

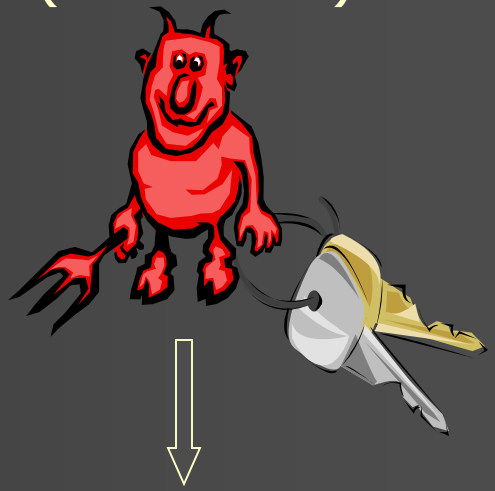
Bypassing Authentication (when key is still valid)



Announcer Daemon
(on Authorizer)

beacon

Controller Daemon
(on Mobile)

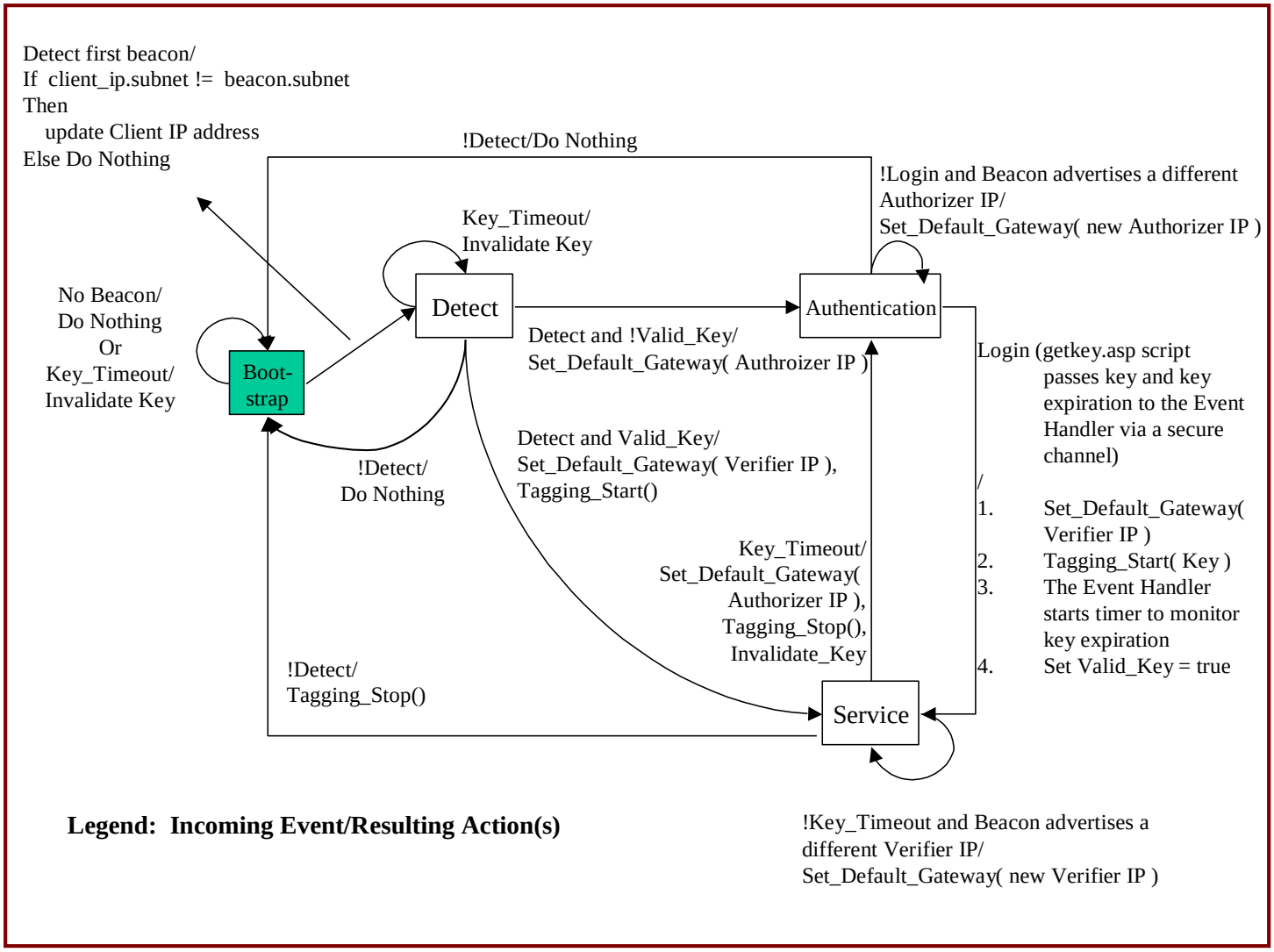


Verifier

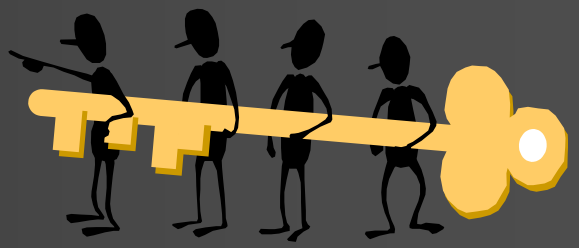
- IP address (DHCP)
- Set Default Gateway
- Enable tagging(*key*)

In a Nutshell: Client Operation

State Transition Diagram

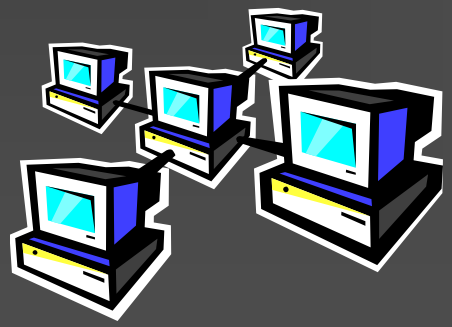


Scalability: Wide-Area Key Distribution

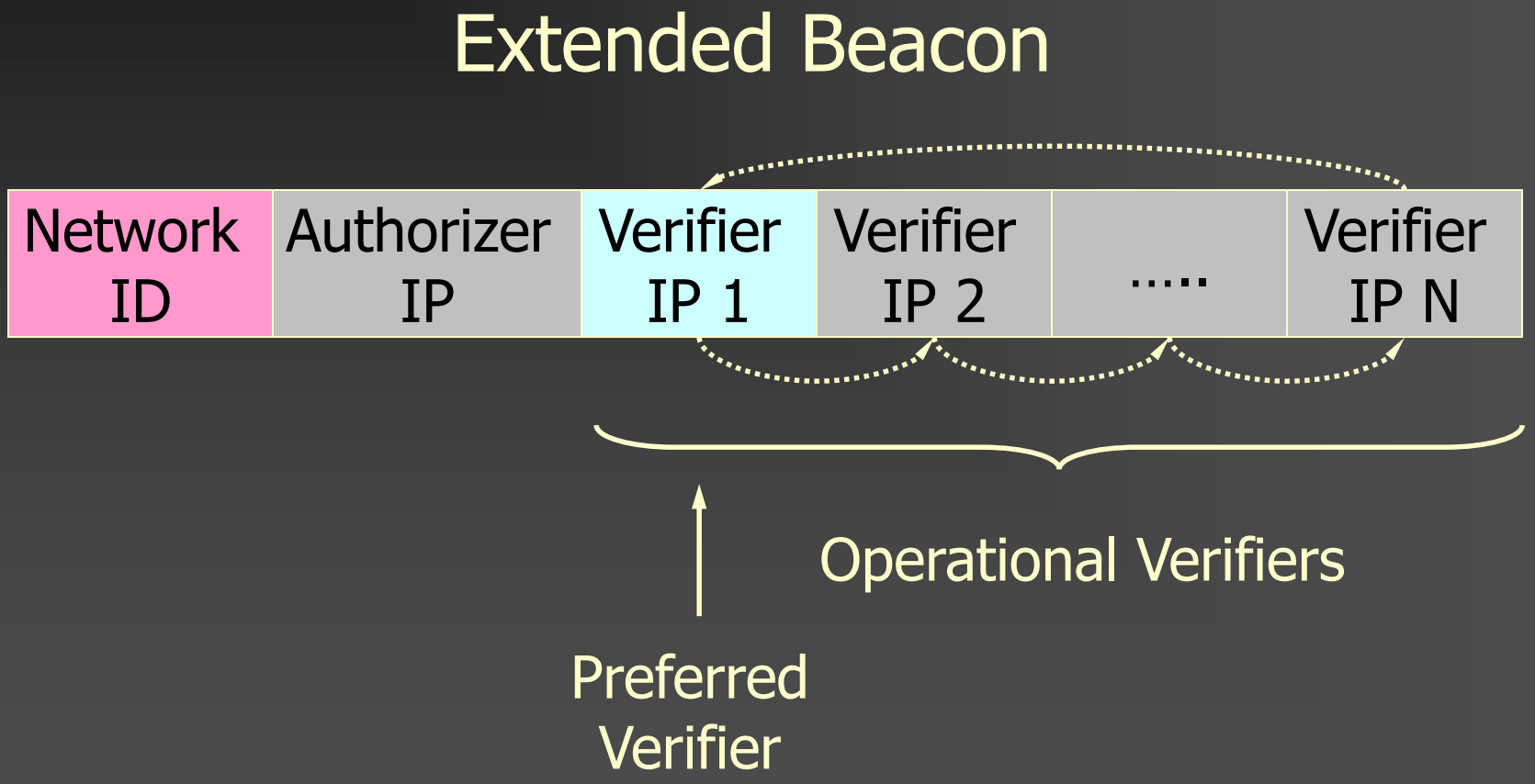


Wide-area key distribution among different subnets

- Global key distribution is costly
- Solution → On-demand session key migration:
  - Detect roaming event between subnets
  - Initiate session key migration request
  - Bypass user-level authentication process



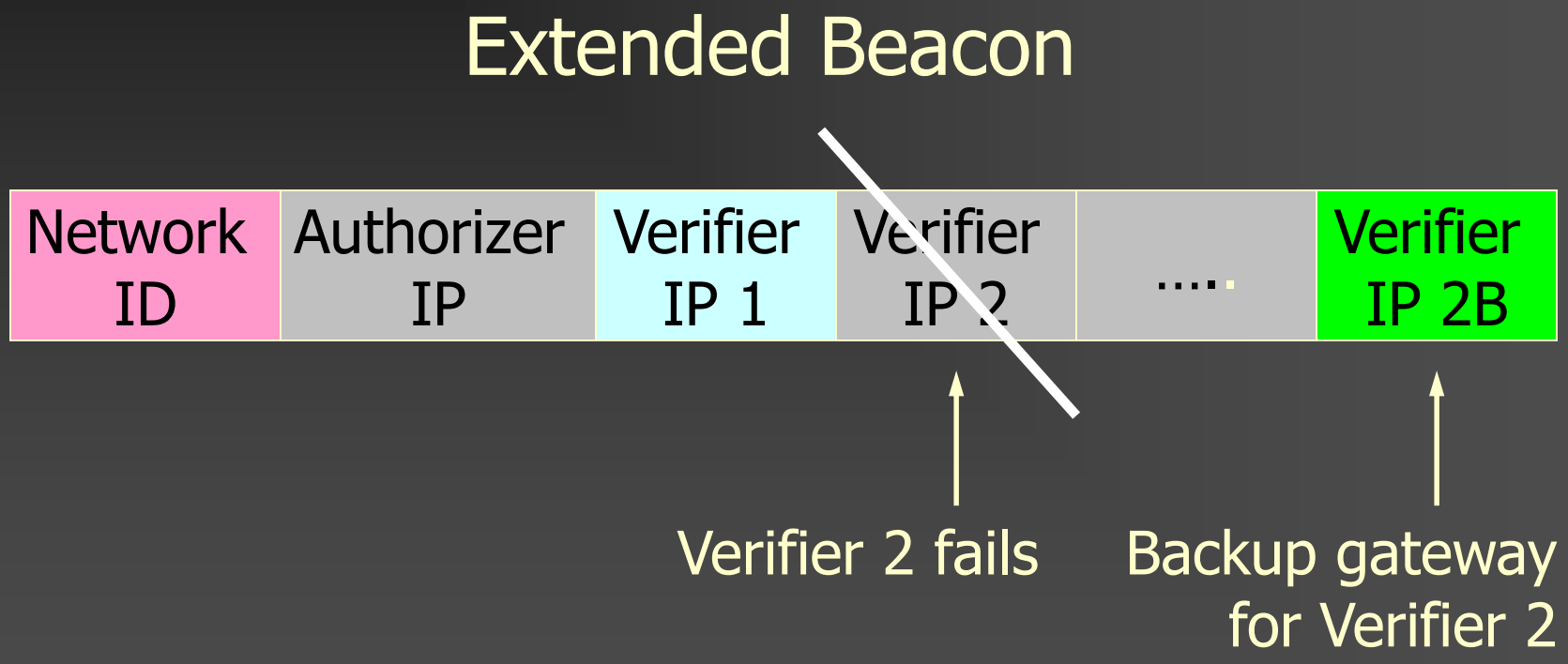
Scalability: Load Balancing among Verifiers



Change ordering of *Verifiers* to load balance new users

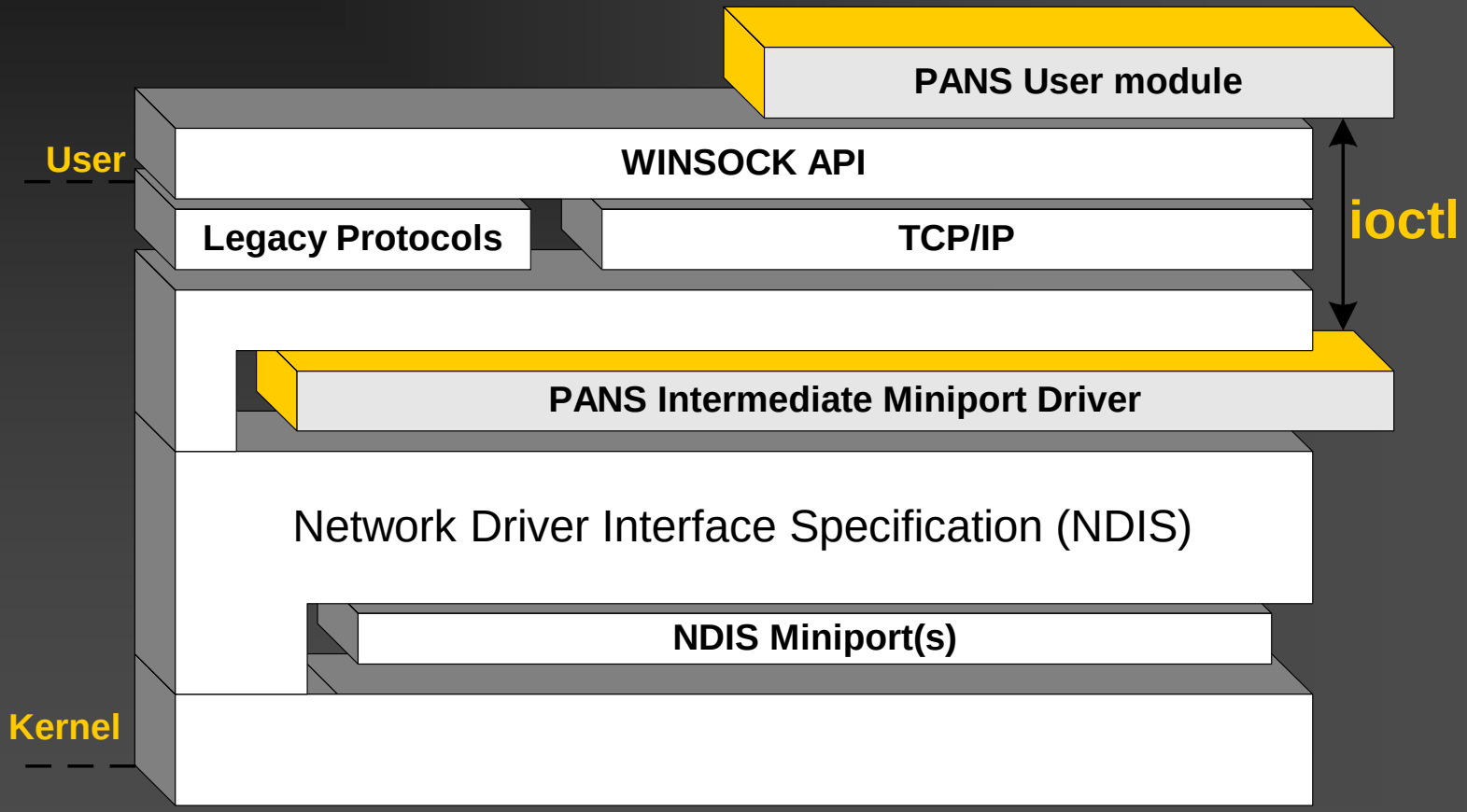
Fail-over in CHOICE

Migrating clients from a failed verifier to a mirror

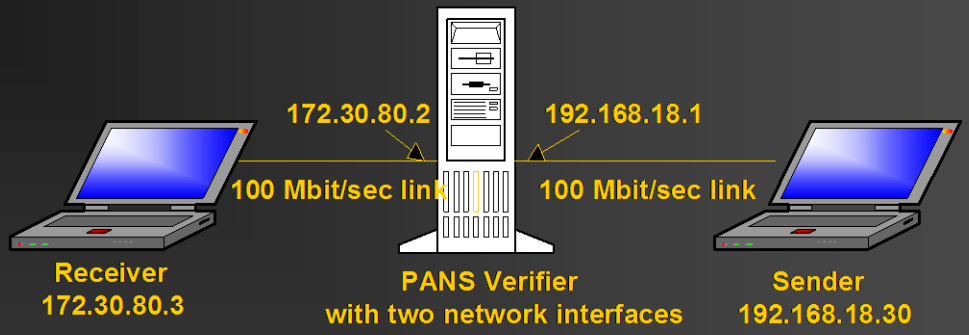


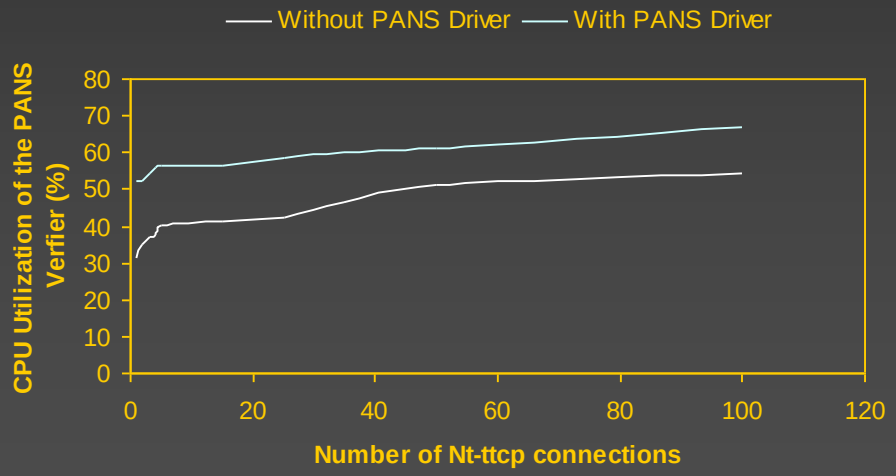
All clients are migrated at the same time!

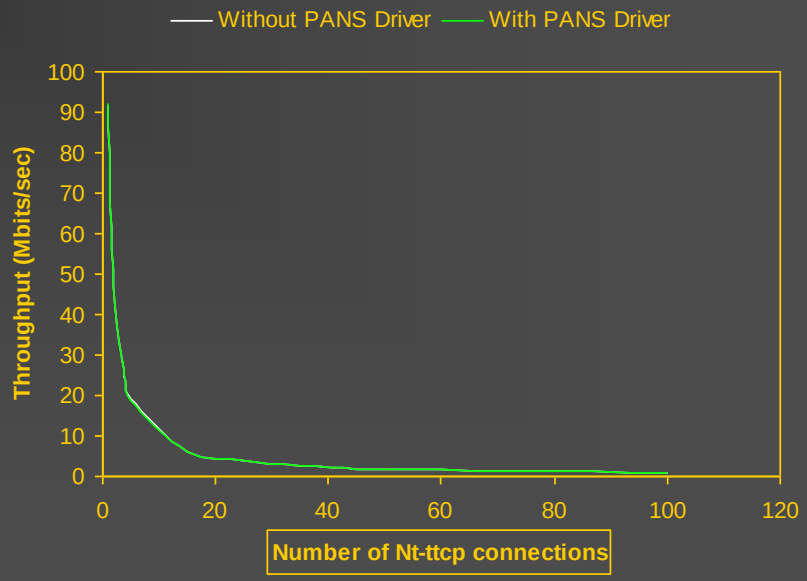
PANS (**P**rotocol for **A**uthorization and **N**egotiation of **S**ervices) Driver Implementation



Protocol Performance







Contrasting CHOICE with 802.1X

802.1X is attractive to hardware vendors as it lets them sell new APs

- ✓ CHOICE is hardware agnostic. APs are commoditized as dumb bridges

802.1X incurs high handoff latency and VoIP support is poor

- ✓ Handoff latency in CHOICE is minimal

802.1X is only about first-hop security

- ✓ CHOICE is a complete system for public wireless-LAN deployment
  - last-hop security is only one piece of it.
  - Other aspects include global authentication, differentiated services, network discovery, load balancing, fail-over mechanisms, packet-level accounting and congestion management.
- ✓ CHOICE provides Location based personalized services
- ✓ CHOICE support multiple authentication schemes
  - AAA (DIAMETER), Global authenticators, E-cash systems (MasterCard, Visa)
  - Support users who do not have a “home” domain

CHOICE -- Accomplishments

- Phase 1 is complete
- Phase 2 is in final stages

Phase 1 Achievements:

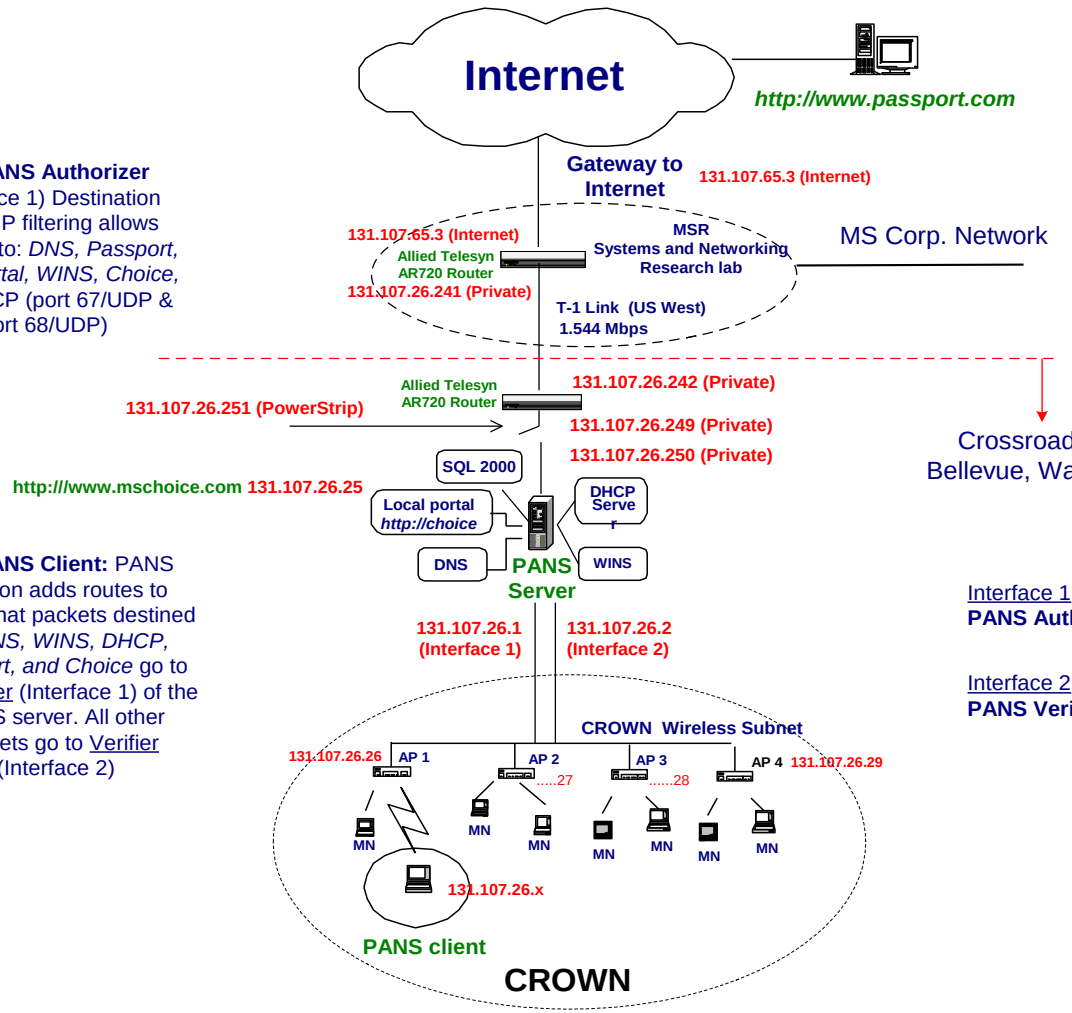
- **System:** has been built and deployed @ the Crossroads Mall in Bellevue
  - Operational since June 2000
  - Result of cooperation between Microsoft & Terranomics Inc. (Mall owner)
  - Result of 11,750+ lines of C, C++, Javascript and VBScript code
  - Result of overcoming logistic nightmares in deploying a huge system.
- **Patents:** 7 applications filed
- **Papers:** IEEE Wireless Communications Magazine + USENIX Internet Technical Symposium'01 + IEEE International Conference on Communications 2001
- **Reports**: MSR-TR-2000-21 (January 2000), MSR-TR-2000-85 (August 2000)
- **Press:** New York Times (Feb. 28, 2000), Microsoft Web Report (Jul. 2000), MicroNews News Service,…

External URL: http://www.mschoice.com

Internal URL: http://choice

Crossroads Shopping Center Deployment

CROWN CONFIGURATION



On PANS Authorizer (Interface 1) Destination based IP filtering allows passage to: *DNS, Passport, Local Portal, WINS, Choice,* and DHCP (port 67/UDP & port 68/UDP)

On PANS Client: PANS daemon adds routes to ensure that packets destined for *DNS, WINS, DHCP, Passport, and Choice* go to Authorizer (Interface 1) of the PANS server. All other packets go to Verifier (Interface 2)

Interface 1 is the **PANS Authorizer**

Interface 2 is the **PANS Verifier**

passport.com believes http://www.mschoice.com only

DHCP Internet addresses available at Crossroads: 131.107.26.0/26(128). Lease time for each address is set to 6 hours. (Key expiration is set to 3 hours)

The CHOICE Network -- Phase 1 Demo

What you will see today:

- CHOICE network discovery (+ Software Installation)
- Access to Local Portal but nothing else
- Passport authentication (and corporate authentication)
- Key generation, distribution and time-limited access
- Key expiration and access-denial
- Sensing of disconnection from CHOICE Network

Test Platform

- Nearly identical to CROWN configuration

Comments on WLAN in Public Places

Everyone Benefits!

- Near-ubiquitous information access (end users win)
- More WLAN hardware sold (vendors & manufacturers win)
- More backbone network resources get used (ISP's win)
- Business owners attract more people (store owners win)
- More software and services sold

Revenue Sources

- Local portals (advertisement revenues, …)
- Long distance phone model
- Location service providers

Technical Details:

- P. Bahl, A. Balachandran, A. Miu, W. Russell, G. Voelker and Y.M. Wang, :*PAWNs: Satisfying the Need for Ubiquitous Connectivity and Location Services"*, IEEE Personal Communications Magazine (PCS), Vol. 9, No. 1
- A. Miu and P. Bahl, "Dynamic Host Configuration for Managing Mobility between Porivate and Public Networks," to appear in *The 3rd Usenix Internet Technical Symposium*, San Francisco, California, USA (March 2001)
- P. Bahl, A. Balachandran, and S. Venkatchary, "Secure Broadband Wireless Internet Access in Public Places," to appear in the *IEEE Conference on Communications*, Helsinki, Finland (June 2001)
- Also MSR-TR-2000-85 and MSR-TR-2000-21
- Or send mail to bahl@microsoft.com, full contact info (http://research.microsoft.com/~bahl)

Broadband Wireless Internet in Public Places

The CHOICE Network - Phase 2

Location Services

Computing in Public Places

Phase 1

- Authentication, access, security, accounting, differentiated serves, mobility management & deployment

Phase 2

- Location services in public places
  - Location based buddy list
  - Mall On Sale server
  - Location Chat

Current Prototypes

Location Information Service

- ✓ Demo today

Location Alert Service

- ✓ Demo today

Location-Based Buddy List Service

- ✗ Deployed but no demo

OnSale Mall Buddy Service

- ✗ Deployed but no demo

Location Information Service

WISH (Where IS Harry?)

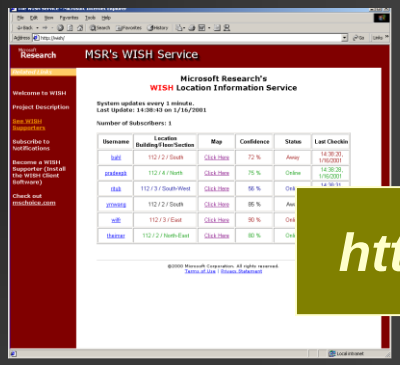
“I wish I knew where Harry is.”

User location system that works with Wireless LANs

Usage scenarios

- Locate people and devices
- Discover nearby resources (printers, offices, restrooms, etc.)

Location Information Service Architecture



http://wish

Eventing Infrastructure

WISH Client

WiLIB

Device Driver

Every 2 minutes

Every 30 seconds

Every 30 seconds

WISH Server

Every 30 seconds

Access Point

Location Alert Service

- When I can't find Harry…

  "Alert me when you find Harry."

- Use soft-state eventing infrastructure for robustness of dynamic distributed systems

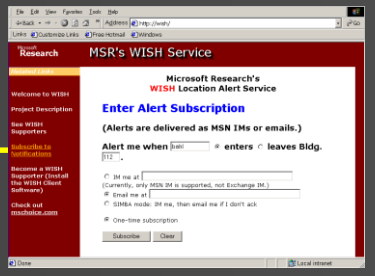
- Use a personalized alert delivery mechanism through instant messaging, emails, cell phone SMS

Location Alert Service Architecture

Wish Client

Wish Server

Wish Alert Service



Alert Subscription Page

Eventing Infrastructure

SIMBA Library

IM

Email

SMS

MyAlertBuddy

Email

IM

Location-Based Buddy List Service

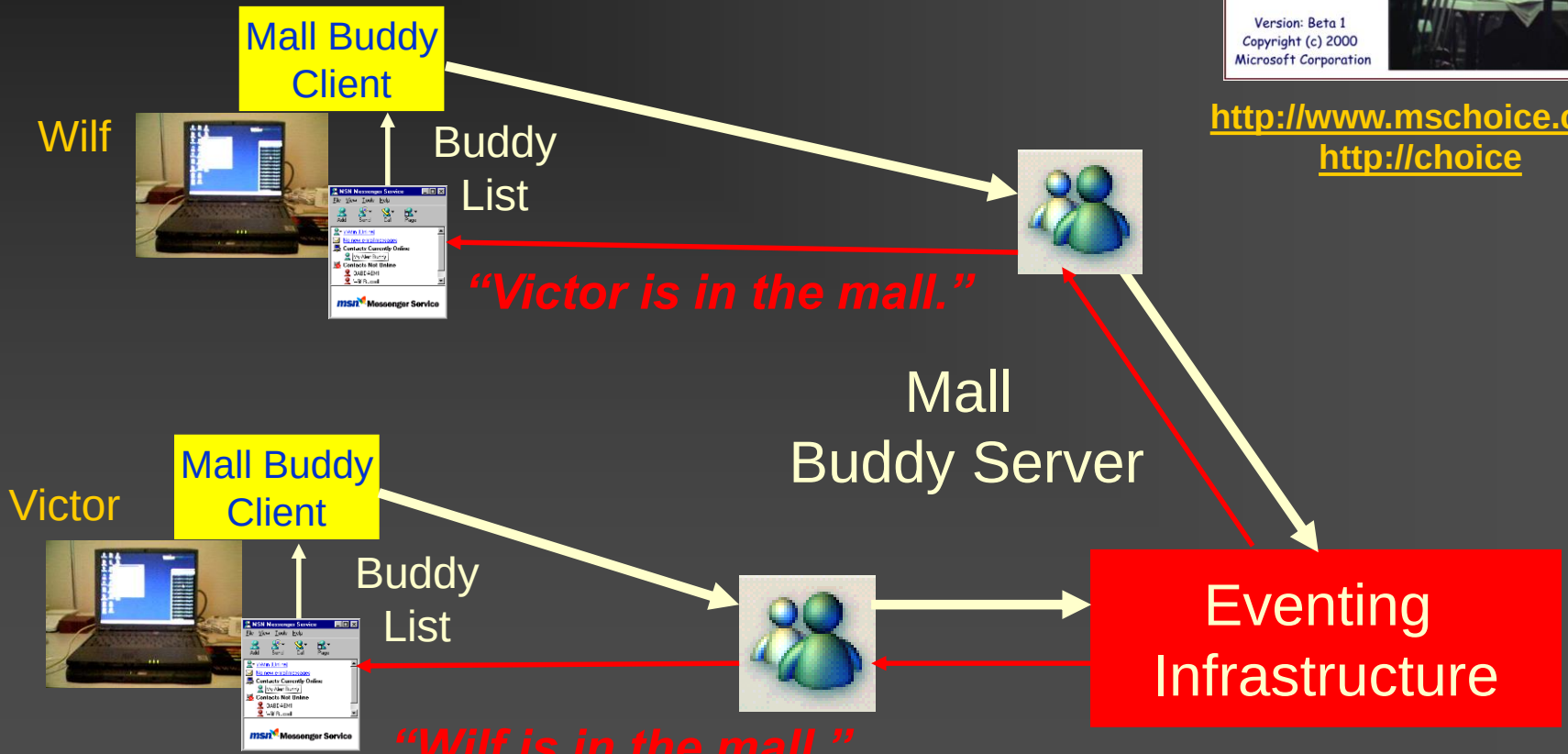
- Extend MSN IM buddy list

  “Alert me when my buddy is nearby and include a map.”

- Proximity detection & location determination in addition to presence detection

Location-Based Buddy List Service Architecture

http://www.mschoice.com
http://choice



OnSale Mall Buddy Service

- Personalized sales announcements

  “Alert me when electronics are on sale.”

- Subject-based publish/subscribe eventing based on product categories and user profiles

OnSale Mall Buddy Service Architecture