Authenticated Wireless Network Services using NoCatAuth

Implementation at College of Business
San Francisco State University

Sameer Verma, Ph.D.

Assistant Professor of Information Systems
College of Business
San Francisco State University
San Francisco, CA 94132

Wi-Fi and campus LANs

- Campus LANs
  - Existing Infrastructure
  - Well-defined core structure
  - Primary use in student labs
- Wi-Fi
  - Extension of the network via laptops (and perhaps PDAs)
  - Not a replacement for the core

The problem

How can SFSU provide wireless access without worrying about unauthorized use?

ISP’s Acceptable Use Policy

Using Wireless LANs on campus

- User (student) perspective
  - Minimum configuration
  - Cheap hardware
  - Mobility
  - Security
    - Email, IM, homework ☺

- Provider (admin) perspective
  - Authorized use
  - Minimal tech support
  - Network control
  - Protect network assets
    - Grades, accounts, etc.

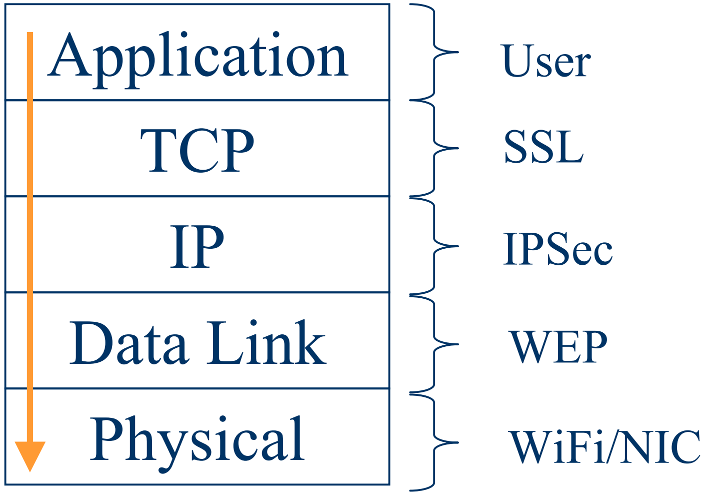
Security is a notion

- Three aspects of security
  - Authentication: Is my login being authenticated by the correct server? (credit card model)
  - Authorization: Am I authorized to use these network services? (login model)
  - Accounting: How many hours of use will I be billed for? (pay-per-use model)

Login processes

- Login is a user-related process. Where do we check the credentials of the user?
- Check credentials at TCP layer via SSL
- Check credentials via IPSec at IP layer
- Check credentials at Data Link layer via WEP
- Check credentials at the Physical layer…(lock the door to the Faraday Cage?)

TCP/IP-OSI Model



Application — User

TCP — SSL

IP — IPSec

Data Link — WEP

Physical — WiFi/NIC

Captive Portal: an alternative

- A portal that captures user’s request for a website.
- Checks user and machine credentials against a database.
- Forces the user to login.
- Maintains session for the duration of login.
- The user’s access is “captive”.
  - Sometimes also called “catch and release”

NoCatAuth

A captive portal solution

NoCat Group – http://nocat.net/

- Provides secure, browser-based *authentication* via SSL
- Requires login+password for *authorized* use.
- Maintains login and logout information for optional *accounting* purposes.
- An add-on feature provides Quality of Service via traffic shaping

Client-Side Requirements

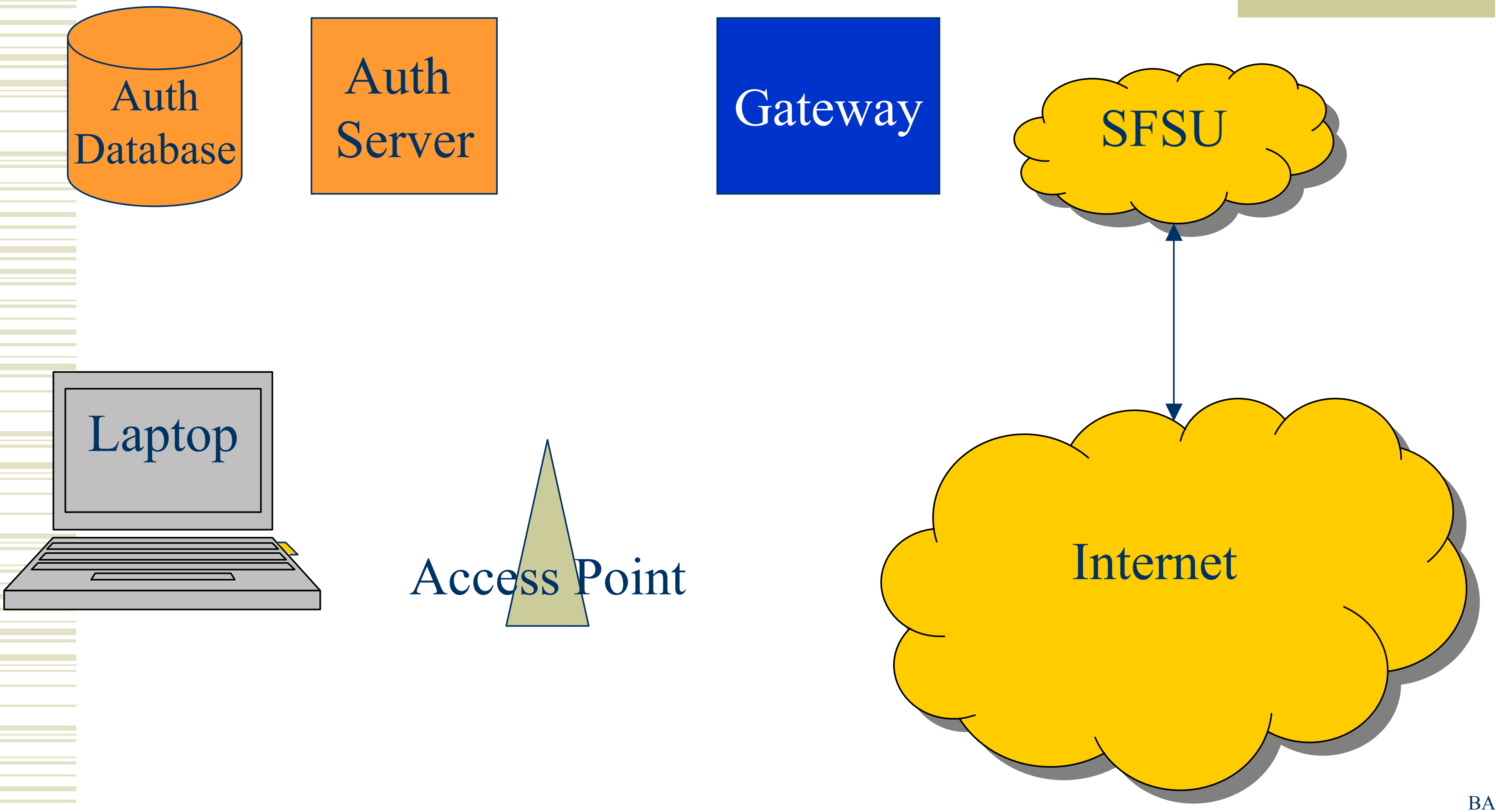
- Browser (Netscape, MSIE, Opera, Mozilla, Galeon, Konqueror)
  - Operating System independent*.
  - No extra software downloads required.
- Wireless card
  - Any Wi-Fi card will do.
- An account in the database.
  - User can request for an account via a form or the database can be pre-populated with account information

* Unless quirks in the browser are OS dependent

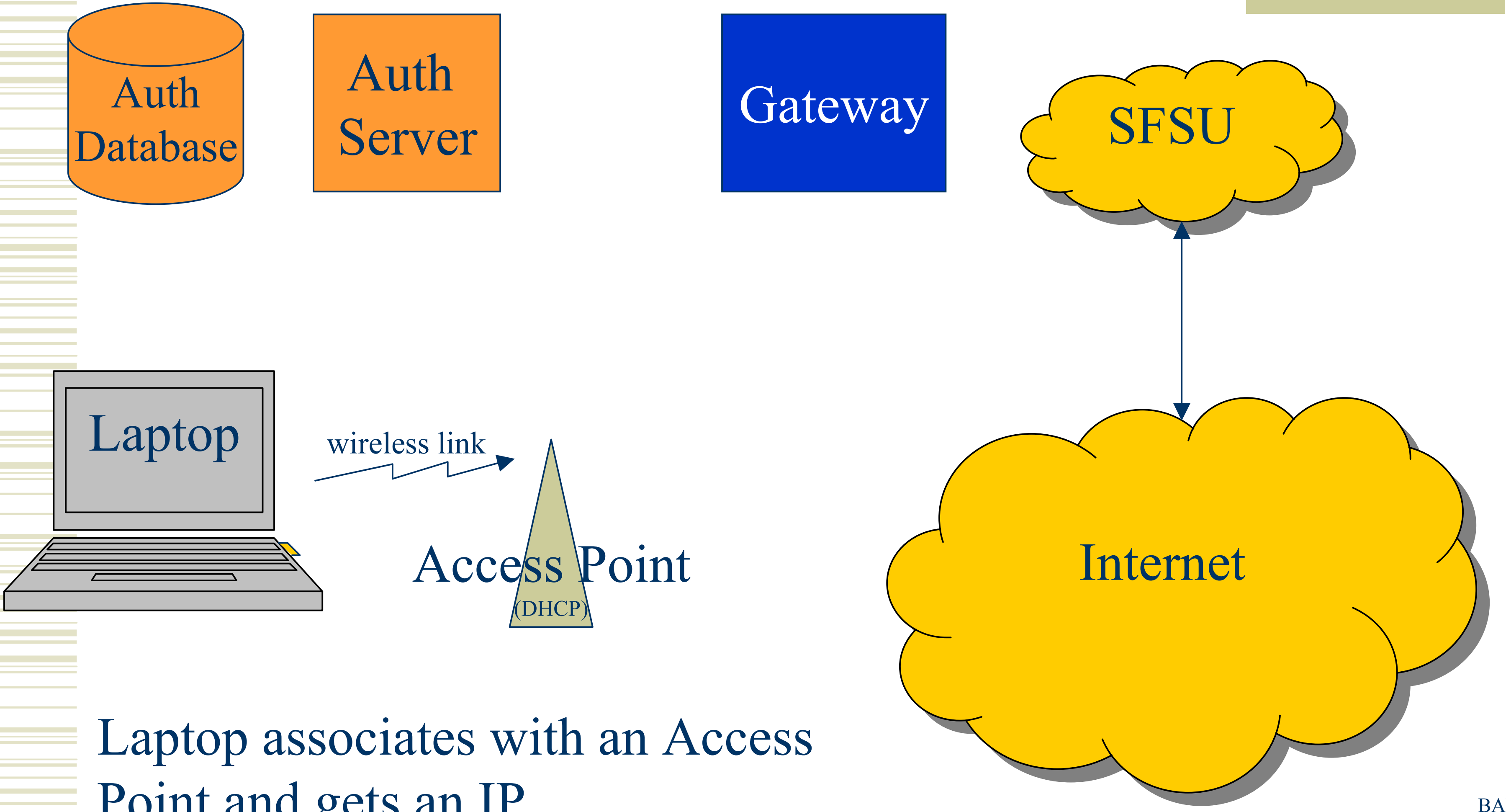
Authentication and Authorization Process

Steps involved in Authentication, and Authorization

NoCatAuth

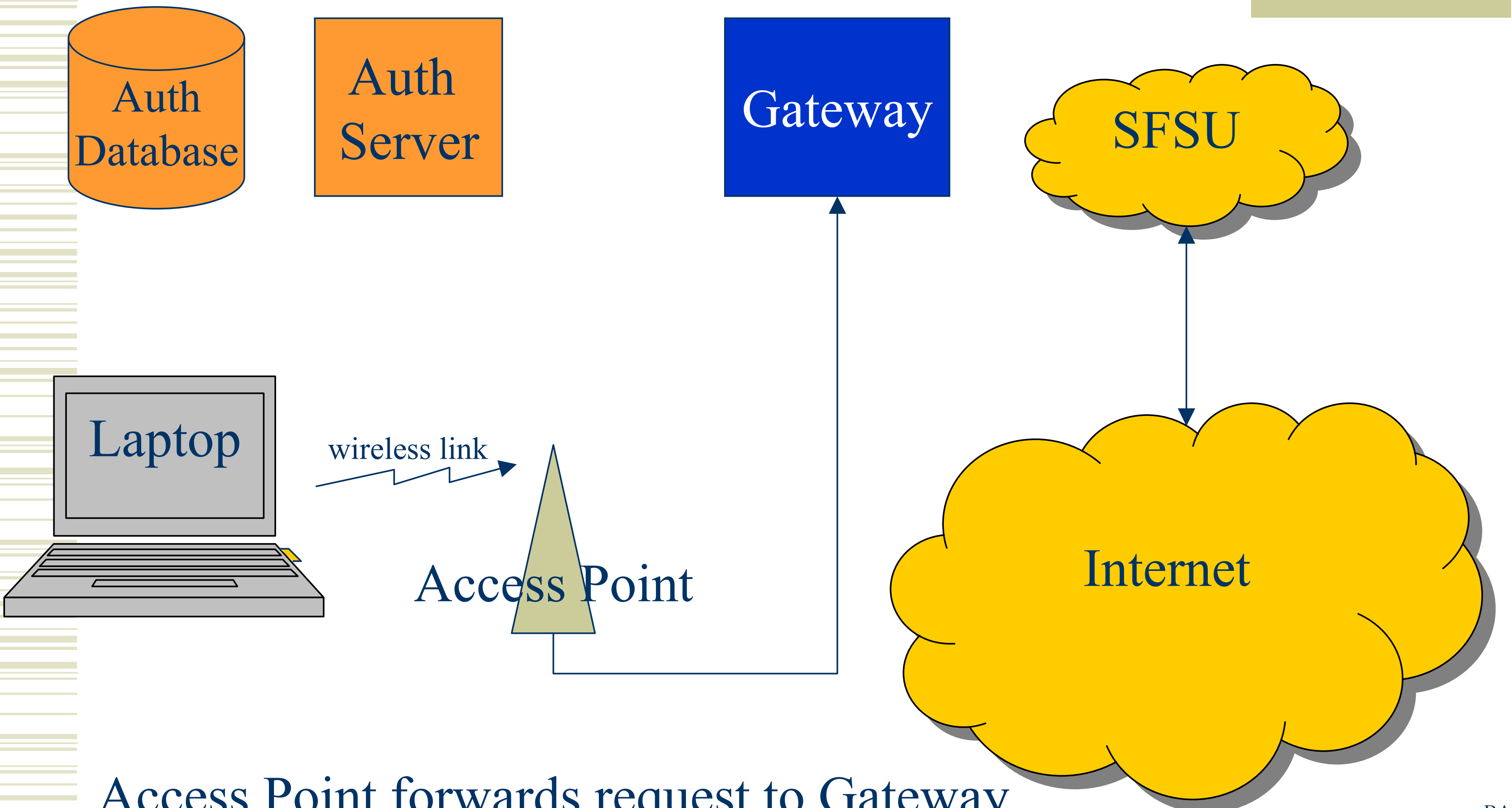

Auth Database
Auth Server
Gateway
SFSU
Laptop
Access Point
Internet

NoCatAuth



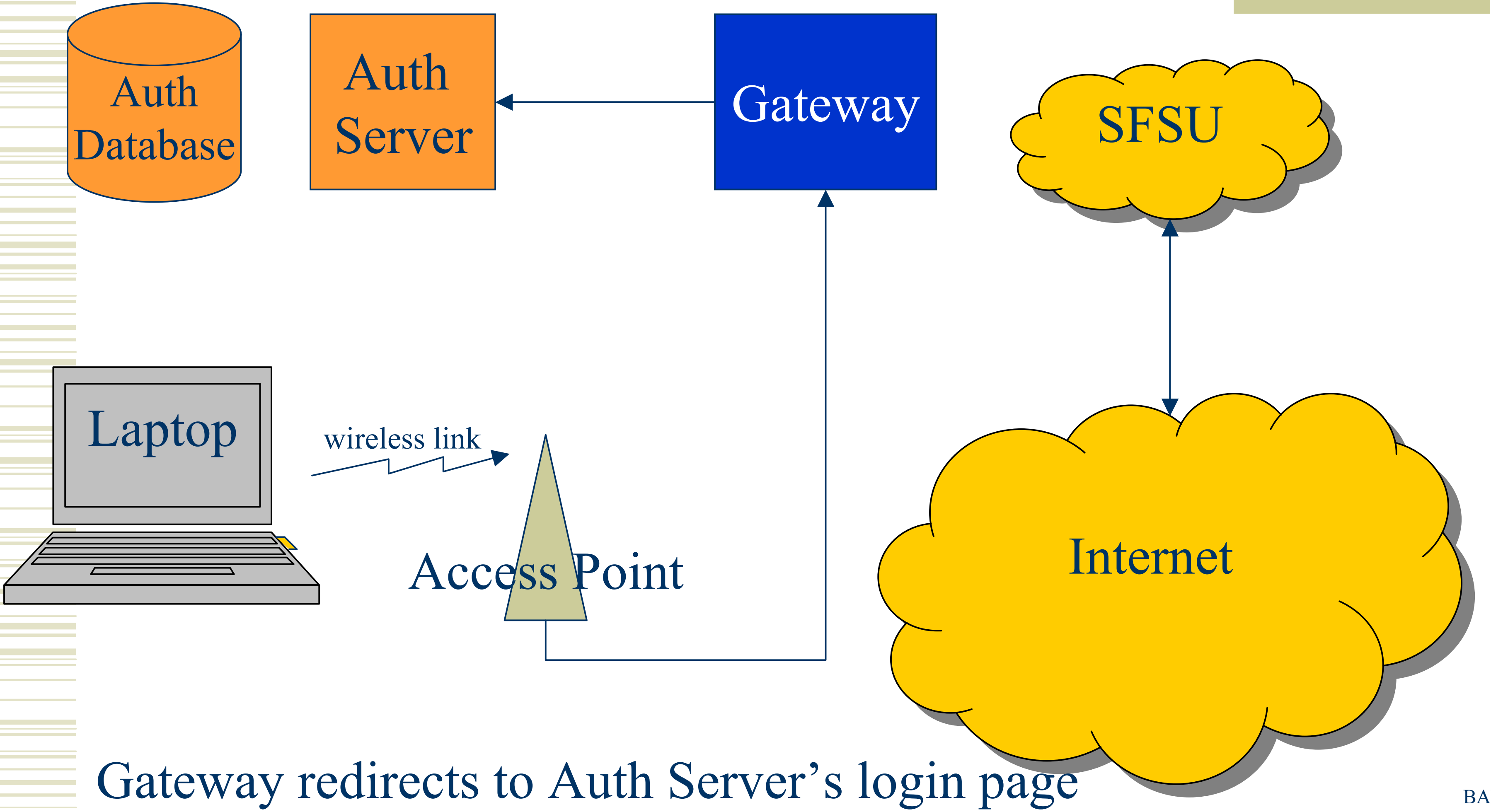
Laptop associates with an Access Point and gets an IP

NoCatAuth



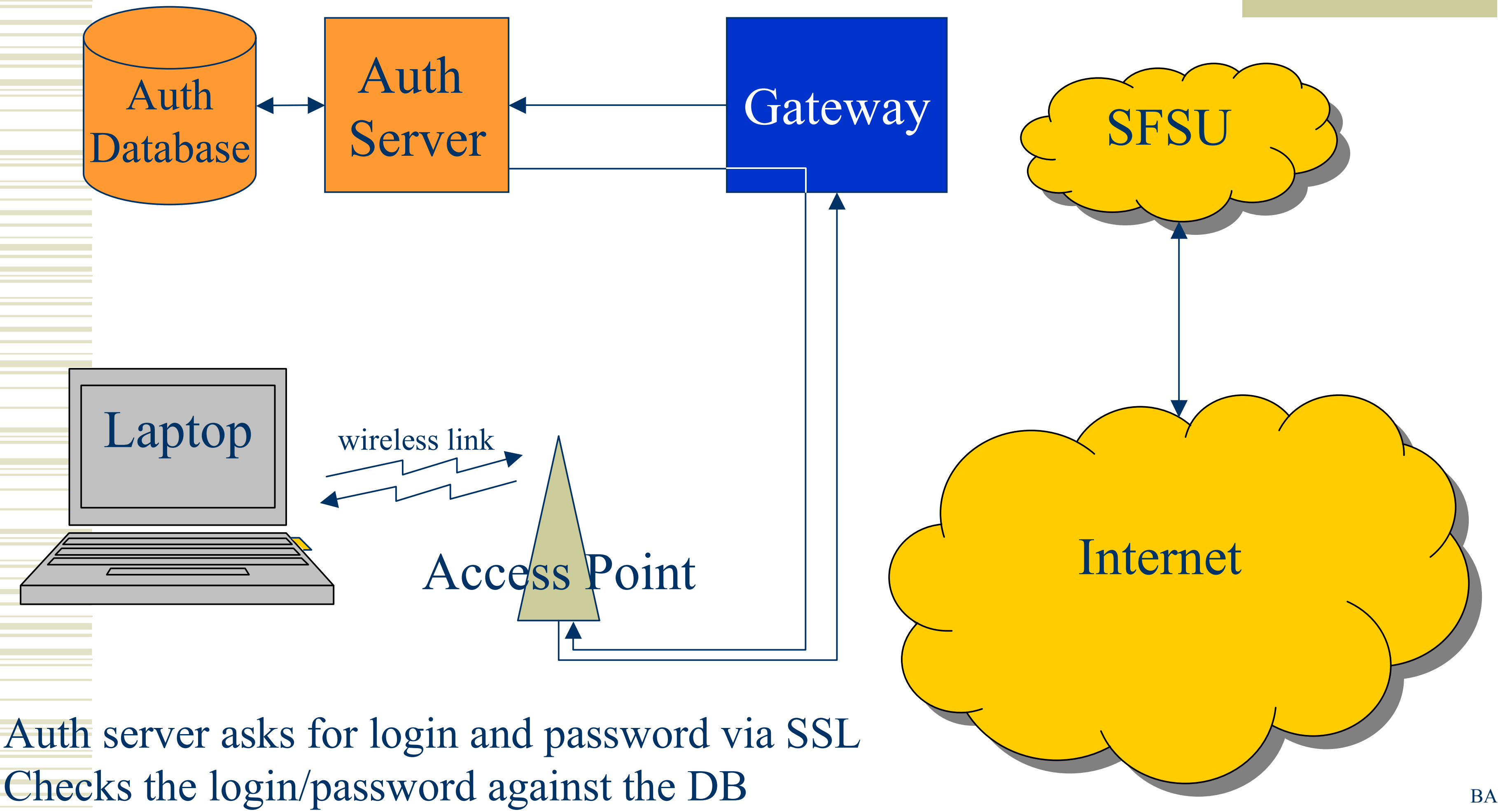
Access Point forwards request to Gateway

NoCatAuth



Gateway redirects to Auth Server's login page

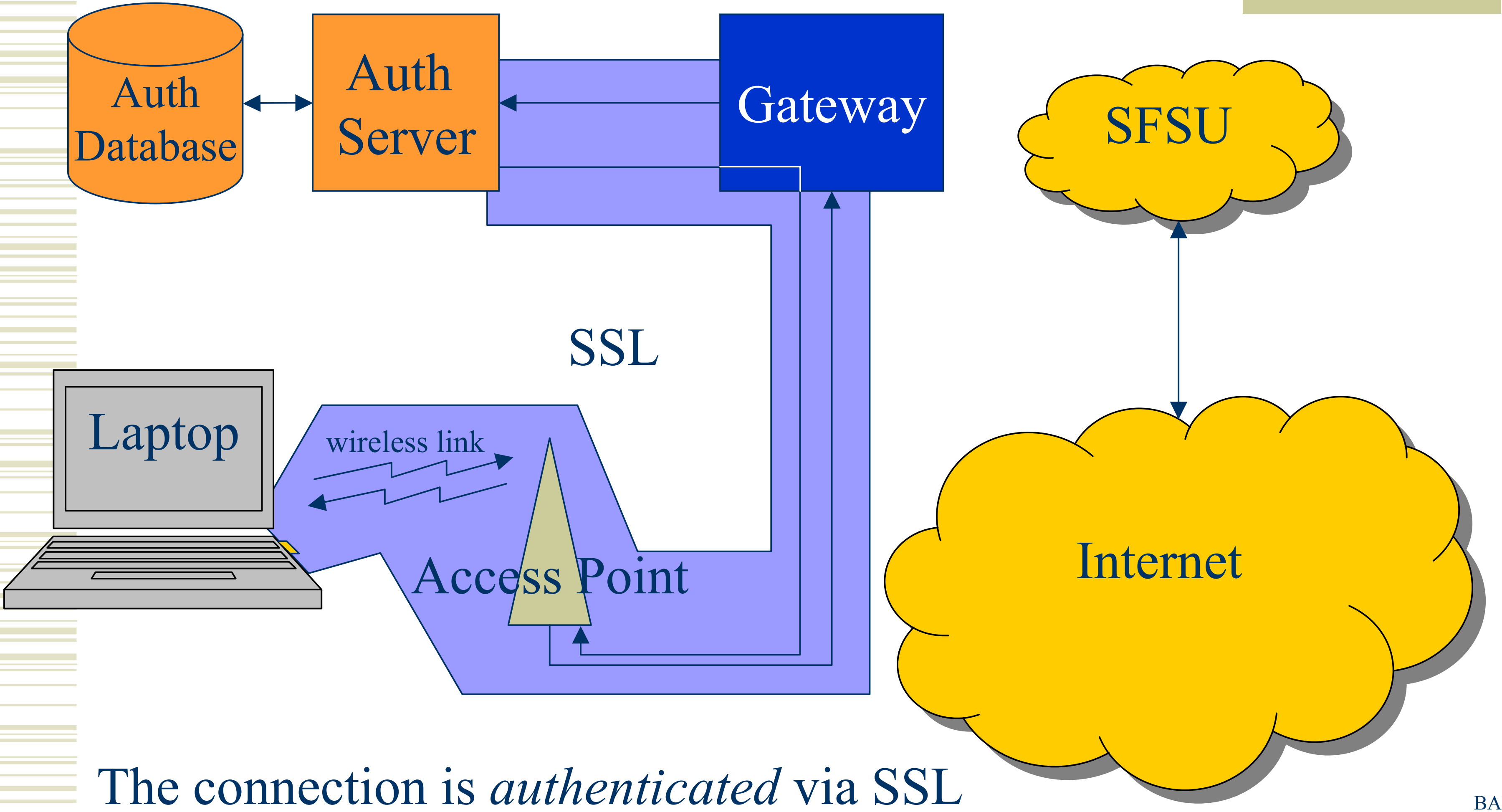
NoCatAuth



Auth server asks for login and password via SSL

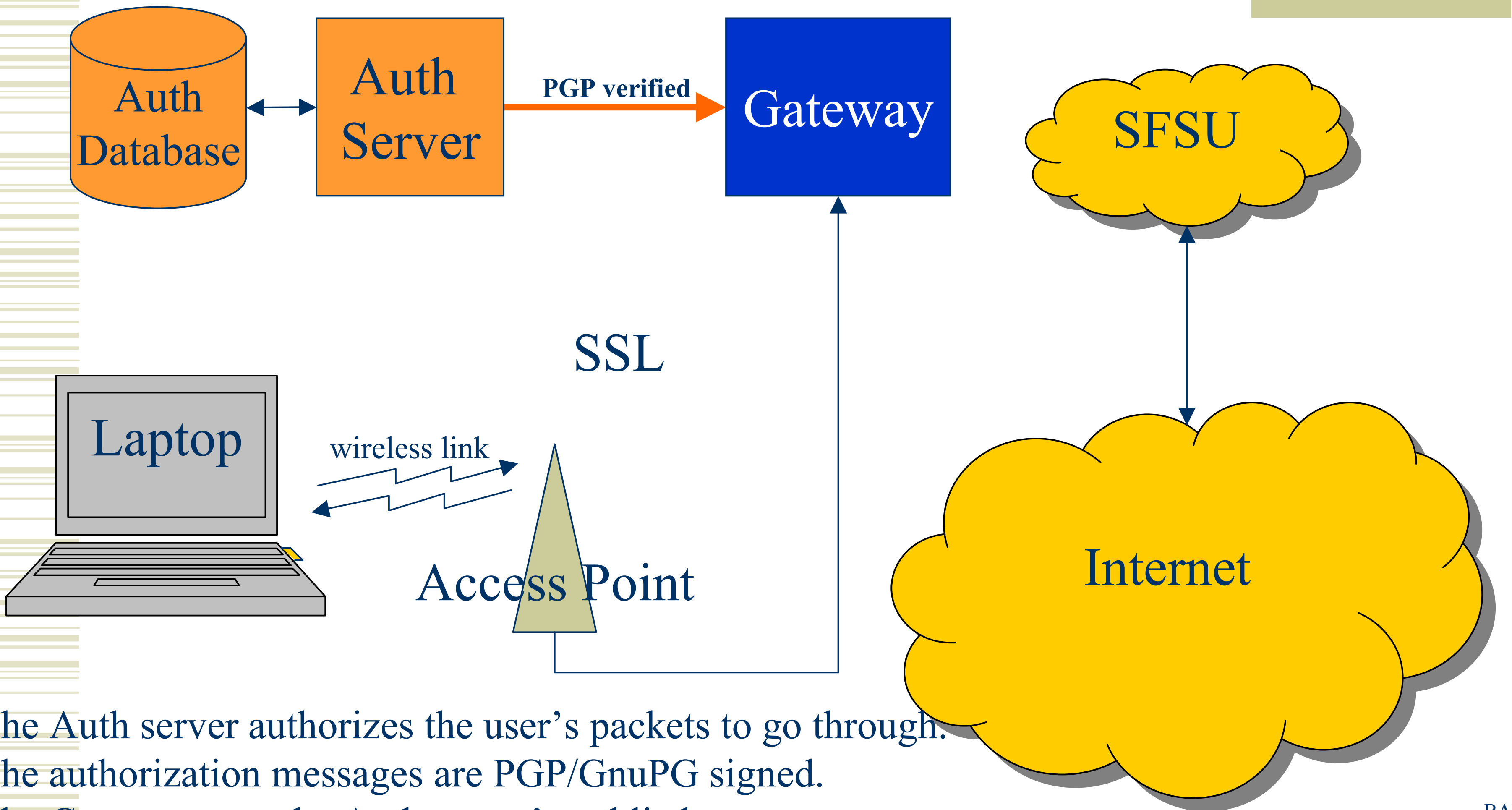
Checks the login/password against the DB

NoCatAuth



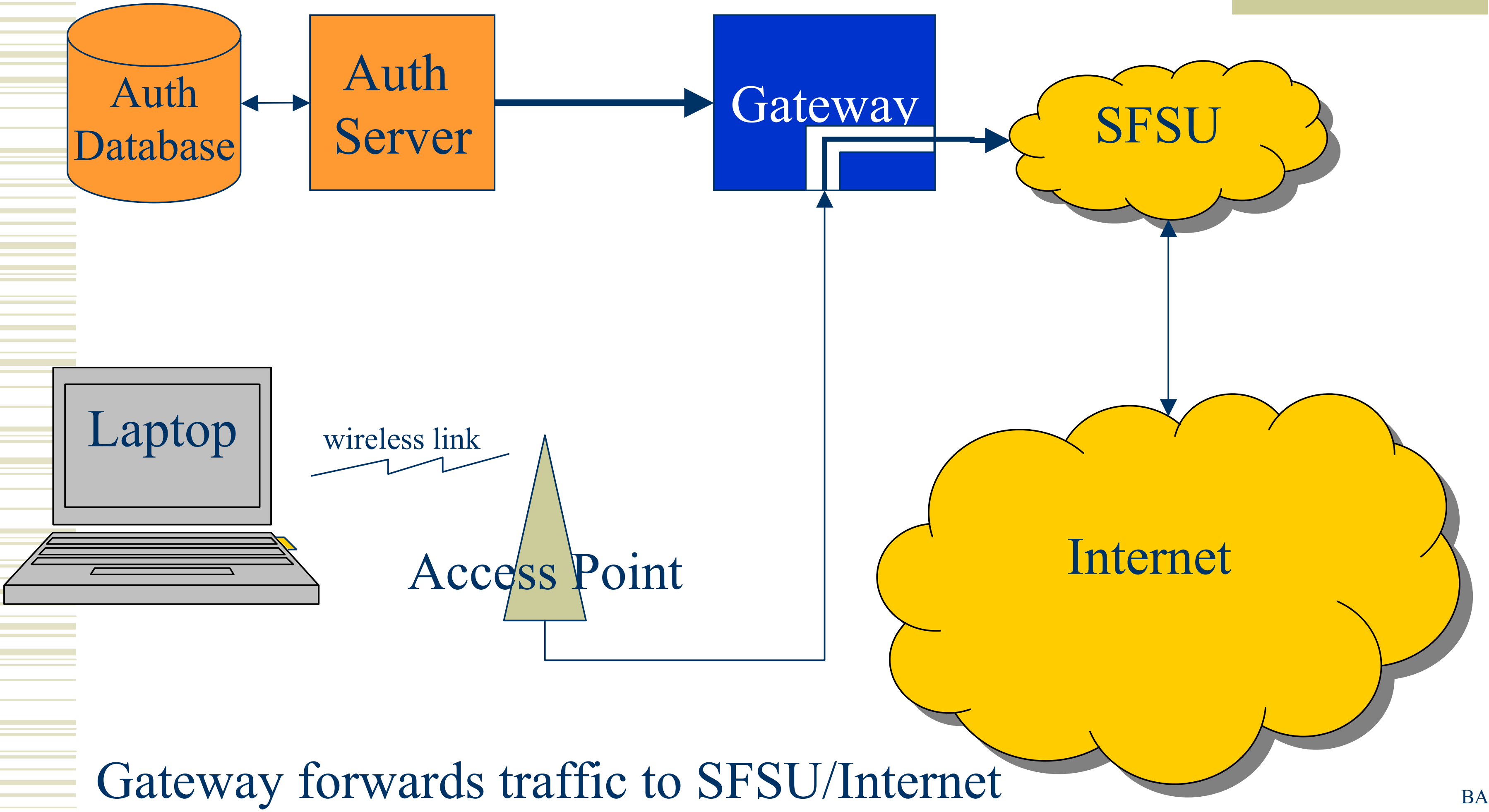
The connection is *authenticated* via SSL

NoCatAuth



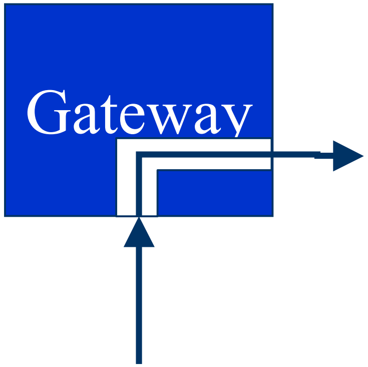
The Auth server authorizes the user’s packets to go through.
The authorization messages are PGP/GnuPG signed.
The Gateway uses the Auth server’s public key.

NoCatAuth



Gateway forwards traffic to SFSU/Internet

NoCatAuth - Gateway



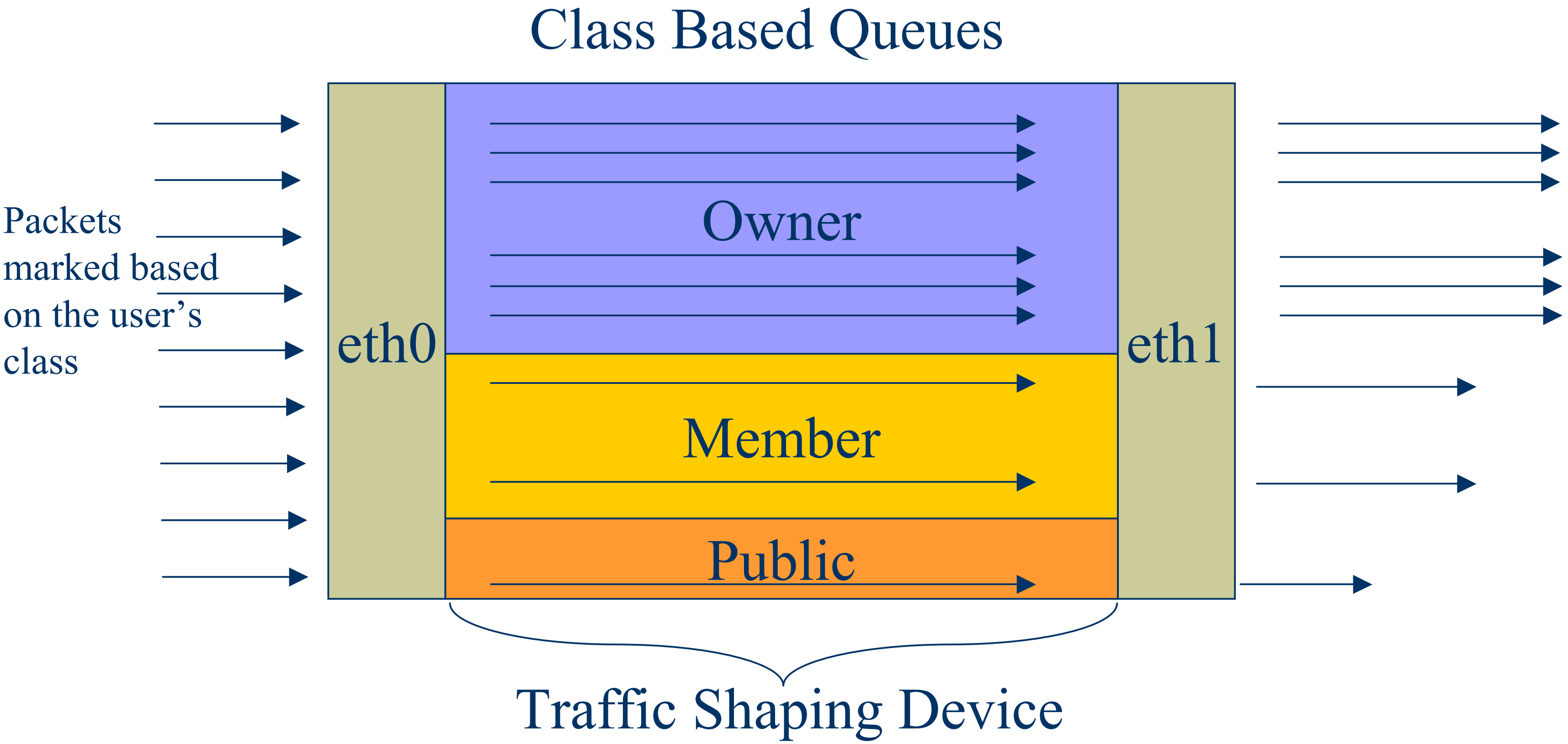
Possible Firewall Implementations

- IPTables (linux 2.4)
- IPChains (linux 2.2)
- IPFilter (*BSD)

Possible Permissions

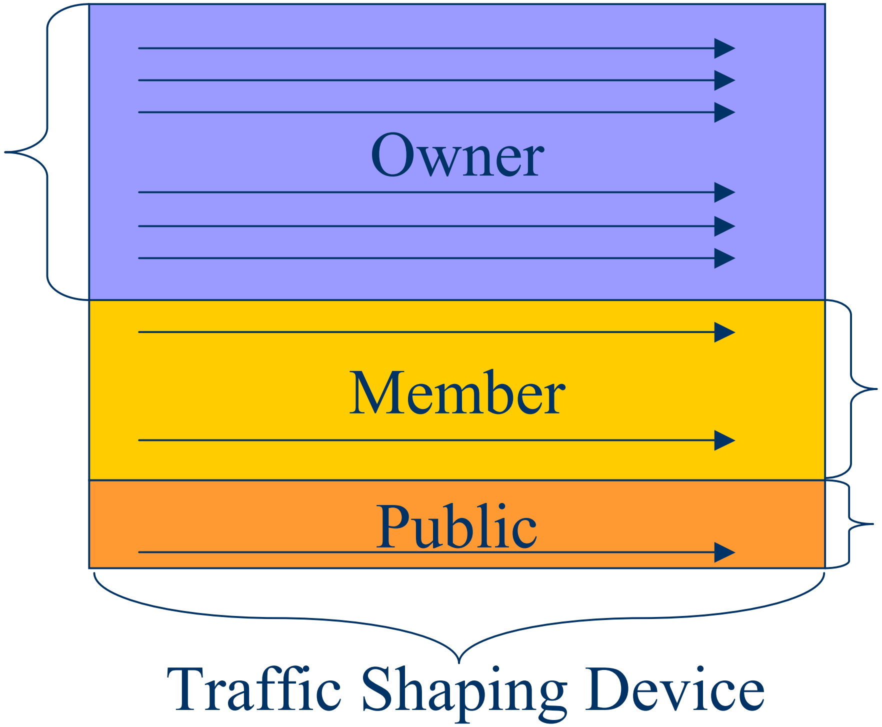
- (Allow/Deny)
- (Allow/Deny) + (Exclude/Include Ports)
- (Allow/Deny) + (Exclude/Include Ports) + (Bandwidth Control via Class Based Queues)

NoCatAuth – Traffic Shaping



BAWUG
July 25 2002

NoCatAuth – Traffic Shaping



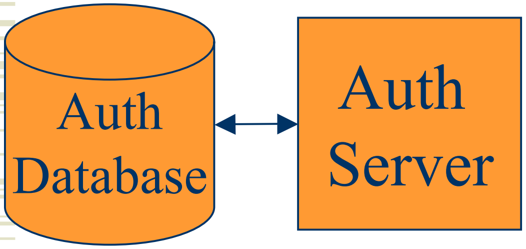
Owner Class gets most bandwidth and can override all priorities and queues.

Member Class (user who logs in, but is not a node owner) gets limited bandwidth

Public Class (user who skips login) gets *very* limited bandwidth. This is more like a guest login.

Note: Default values in NoCatAuth’s throttle.fw are Owner=3mbit, Member=1mbit and Public=128kbit

NoCatAuth – Auth Service



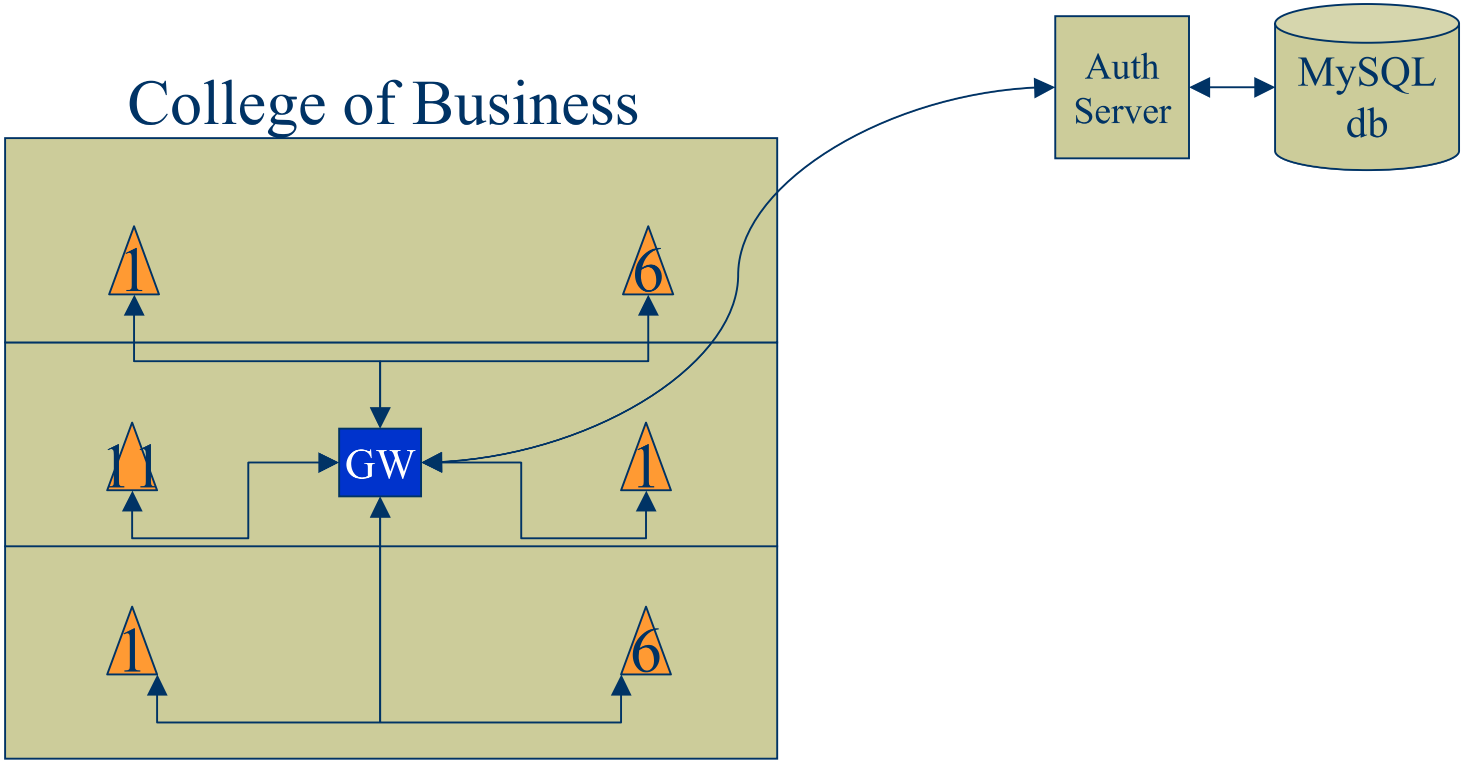
Authentication Server

- WebServer + SSL
    - Apache
    - OpenSSL

Possible Backend Data Sources

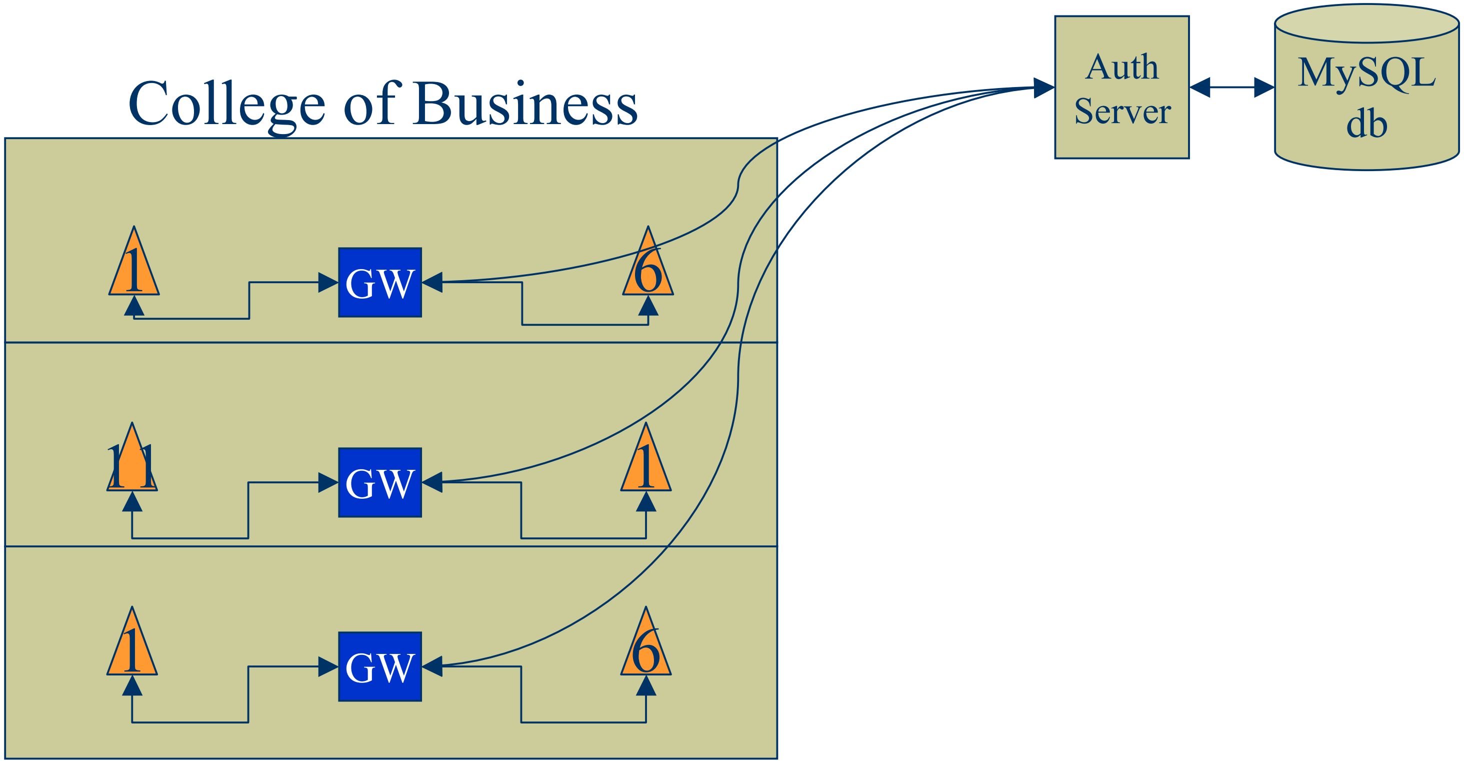
- Flat File (md5 passwords)
- Databases (via DBI)
- Pluggable Authentication Modules (PAM)
- Samba
- LDAP

NoCatAuth – Current Implementation at SFSU

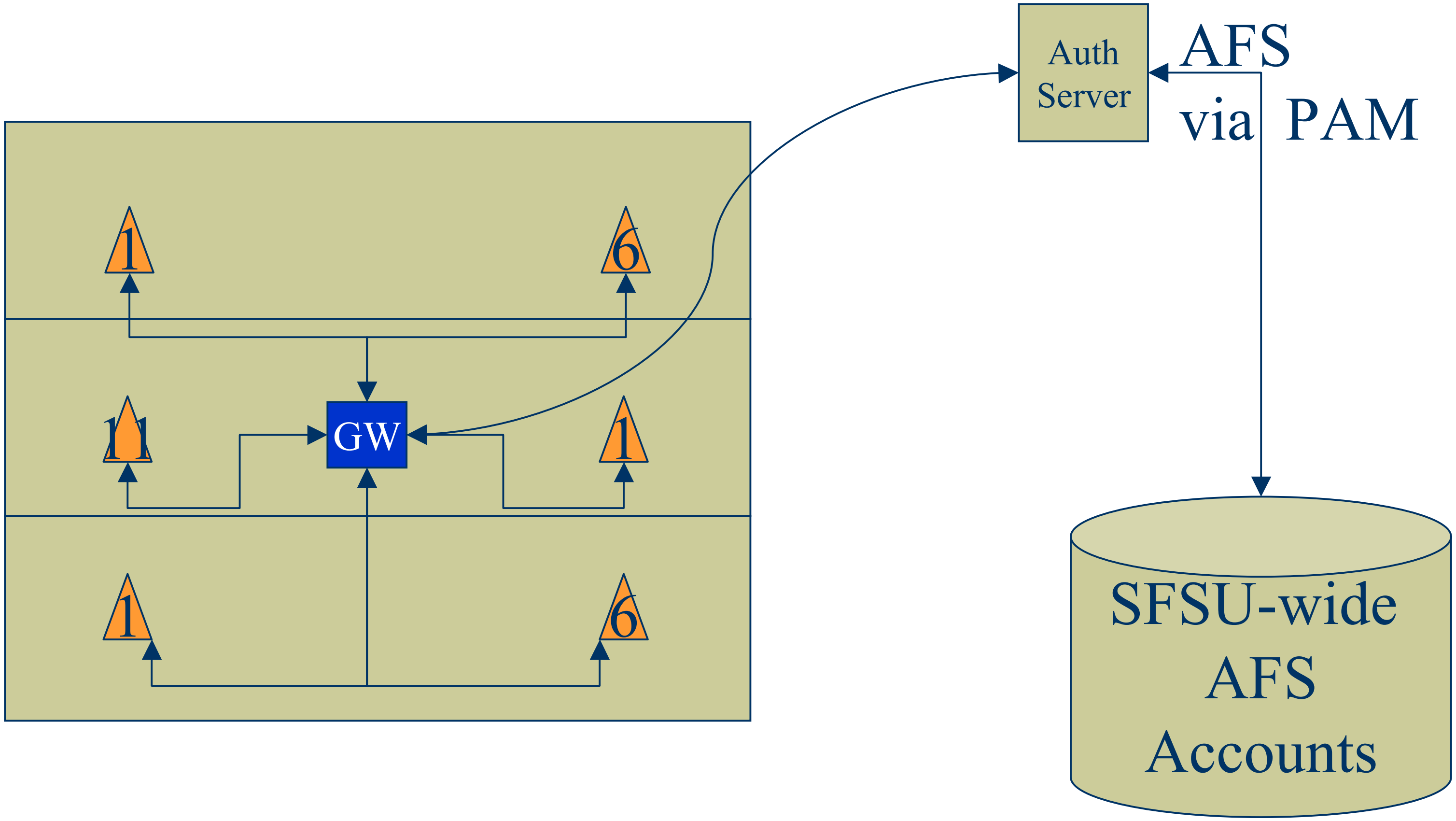


APs are on non-overlapping channels 1, 6 and 11

NoCatAuth – Alternative Implementation at SFSU



NoCatAuth - Future Implementation at SFSU



Further Information

- NoCatAuth
  - http://nocat.net/
- Implementation report
  - http://verma.sfsu.edu/users/wireless/nocatauth_report.pdf