IEEE802.1x とVLAN 認証を利用した無線 LAN システムの構築

東京大学生産技術研究所
電子計算機室
林　周志

Agenda

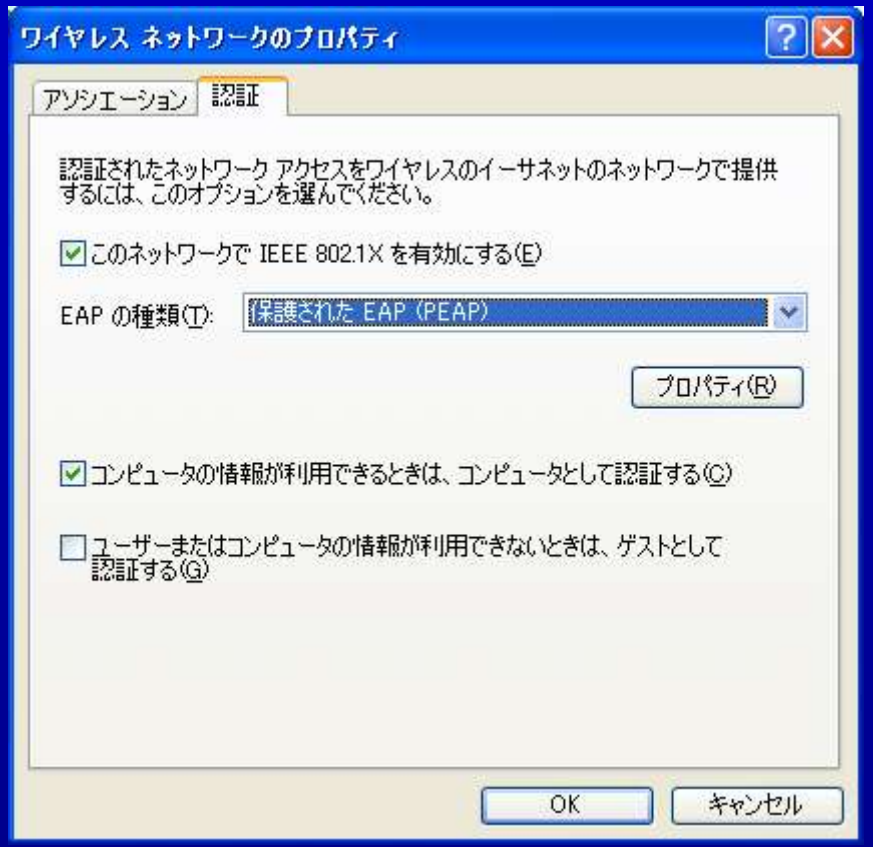
- 東大生研の無線 LAN システム概要
- 導入の背景
- 設計
- 実装
- 課題

東大生研 無線 LAN システム概要

- 2003 年春 導入
- 特徴
  - ほぼキャンパス (屋内) 全域で利用可能
  - WEP キー入力不要かつ高セキュリティ
  - どこでも自研究室の VLAN に接続
- 主な機器構成
  - IEEE802.11b AP　Cisco Aironet1200 200 台
  - RADIUS サーバ　Win2k Server + Cisco ACS　2 台
  - VLAN 認証スイッチ　Alcatel OmniSwitch 7700 1 台

概要ー実際の利用 (1)

Windows XP SP1 での設定



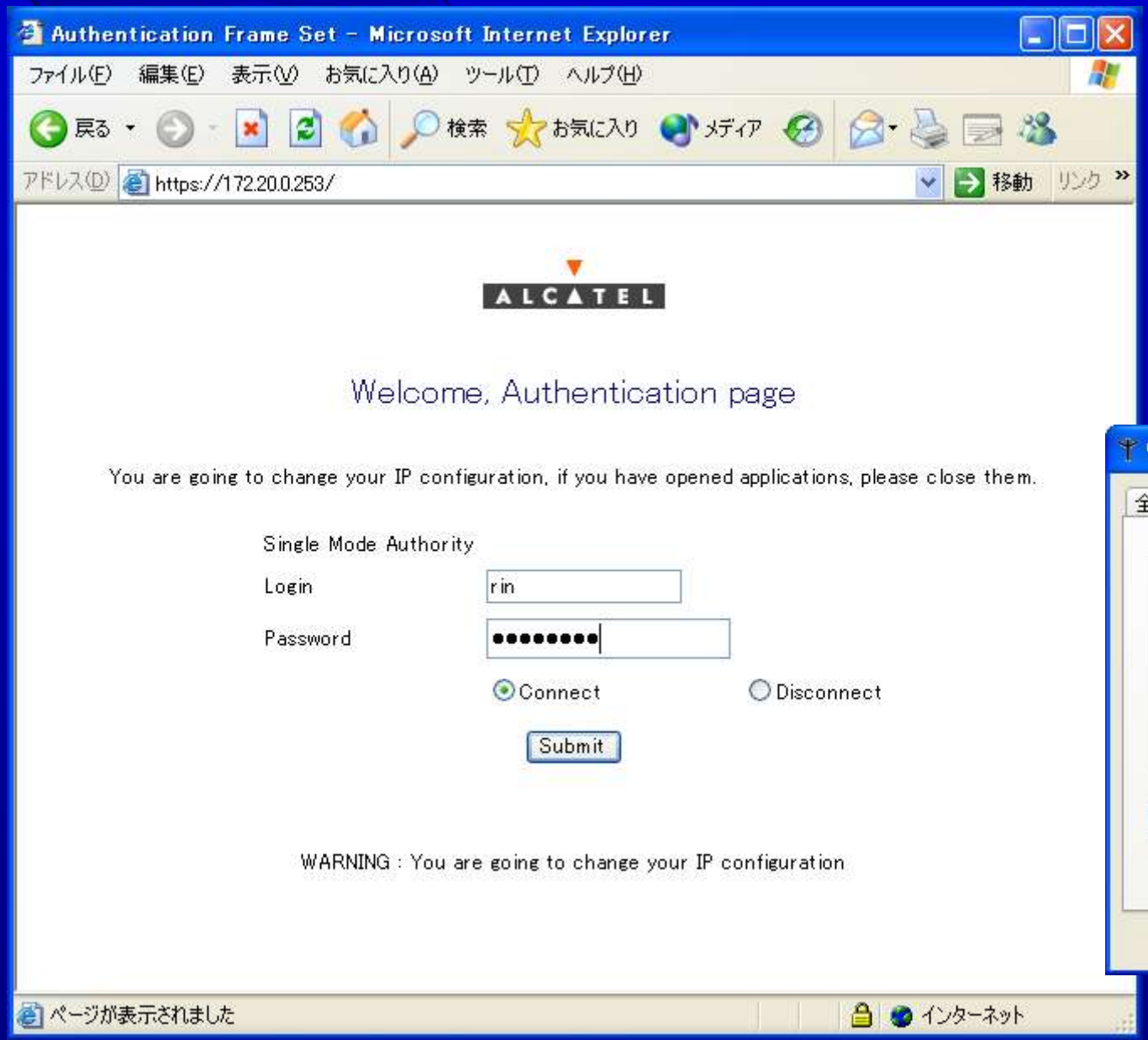
概要ー実際の利用 (2)

PEAP 認証
(1 回限り)

仮 IP アドレス割り当て

概要－実際の利用 (3)

VLAN 認証

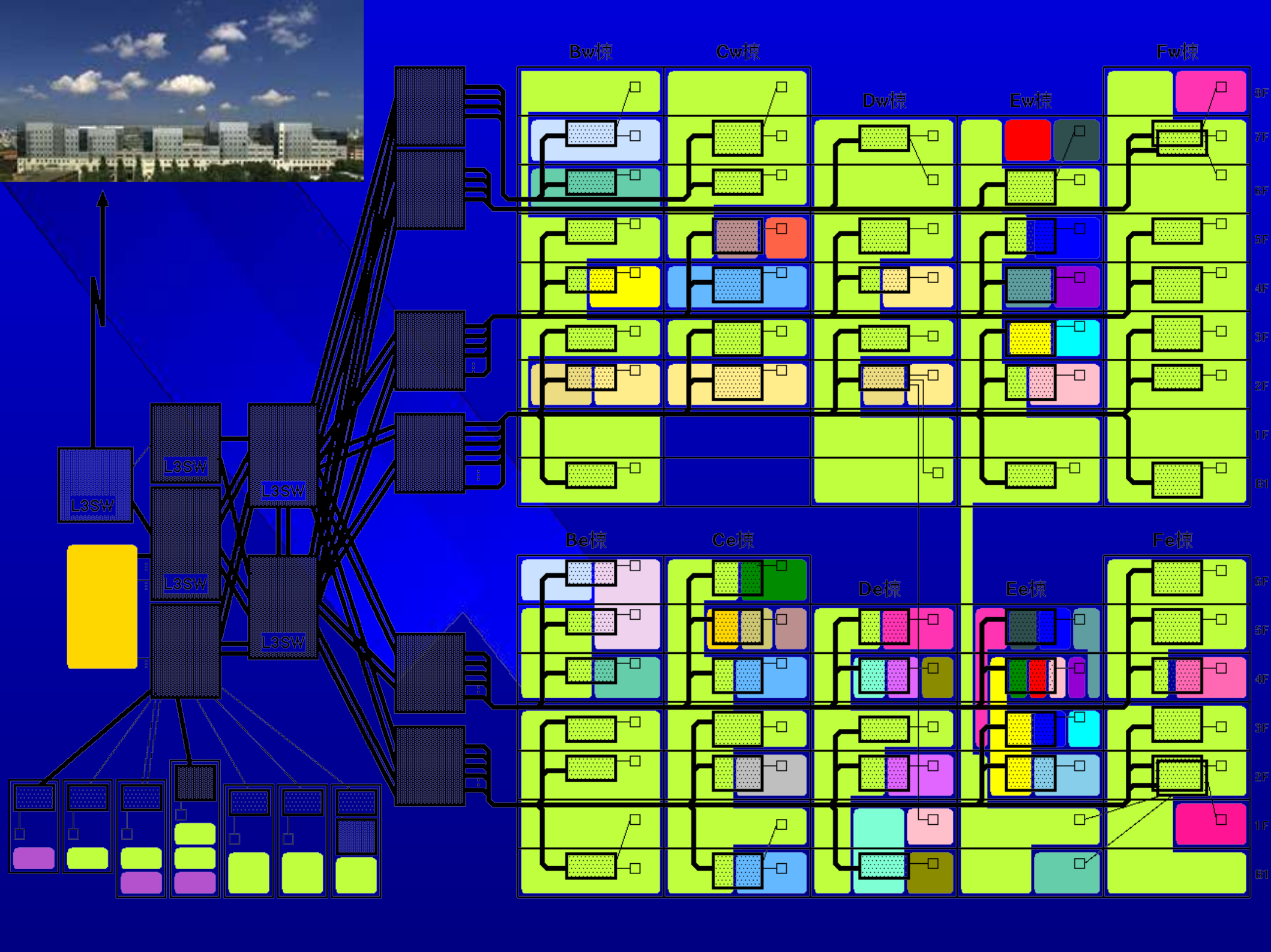


IP アドレス再割り当て

背景

背景ー東大生研ネットワーク概要

- ユーザ数 約 1400 人 (教職員、大学院生)
- 端末数　約 4200 台 (内無線 440 台)
  - マシンと OS はさまざま
- 有線のネットワーク構成
  - CISCO Catalyst6506 × 7
  - CISCO Catalyst5509 × 4
  - CISCO Catalyst4003 × 25
  - CISCO Catalyst4006 × 33
  - CISCO Catalyst2916MXL × 10


Bw棟
Cw棟
Dw棟
Ew棟
Fw棟
Be棟
Ce棟
De棟
Ee棟
Fe棟
8F
7F
6F
5F
4F
3F
2F
1F
B1
L3SW
L3SW
L3SW
L3SW
L3SW

背景－旧無線 LAN システム

- 2001 年春導入
- NoWiresNeeded(NWN) 社製　AP 140 台
- AP は建物ごとの共用 VLAN に接続
- WEP なし、MAC アドレスフィルタのみ
  - WEP で接続できない無線 LAN カードの存在
  - WEP の脆弱性
  - WEP キーの配布、更新がめんどう
  - NWN 製カードは独自暗号方式、キー入力不要

背景ー旧無線 LAN システムの課題

- サポート不安
  - 導入直後に Intersil に買収され、製造中止
- ハングアップが頻発、不安定
  - 頻繁に現場に出向いてリセット (会議室は 2 台設置)
- MAC アドレスフィルタは AP ごとに設定
- ユーザの意見
  - 自分の研究室 VLAN に入れない
  - ローミングしても VLAN が変わってしまうときがある
  - セキュリティに不安

新無線 LAN システムの目標

- 無線 LAN セキュリティの強化
- ユーザごとの VLAN 割当による利便性の向上
- 管理の簡素化

設計

設計― APの選定

- ポイント
  - 会社、製品とも安定していること
  - IEEE802.1x 認証に対応していること
  - MAC アドレスフィルタは RADIUS で管理すること
- 候補
  - Avaya Wireless AP-3
    - 東大情報基盤センターで導入
  - Cisco Aironet 1200
    - IEEE802.1q VLAN 対応
    - IEEE802.1x LEAP 対応 (AirMac が対応)
    - CDP 対応

設計ー無線セキュリティ

- Static WEP
  - ○ どのクライアントでもサポートされている
  - × 脆弱
  - × 全 AP/ 端末が同一キーを設定しなければならない
- IEEE802.1x EAP (Extensible Authentication Protocol)
  - ○ ユーザ / 端末ごとに個別に認証、AP からキー配布
  - ○ 定期的にキーを変更できる
  - ○ RADIUS サーバで集中管理できる
  - × 対応している OS(サプリカント) が少ない

設計ー IEEE802.1x 認証方式の選択

- IEEE802.1x EAP の種類

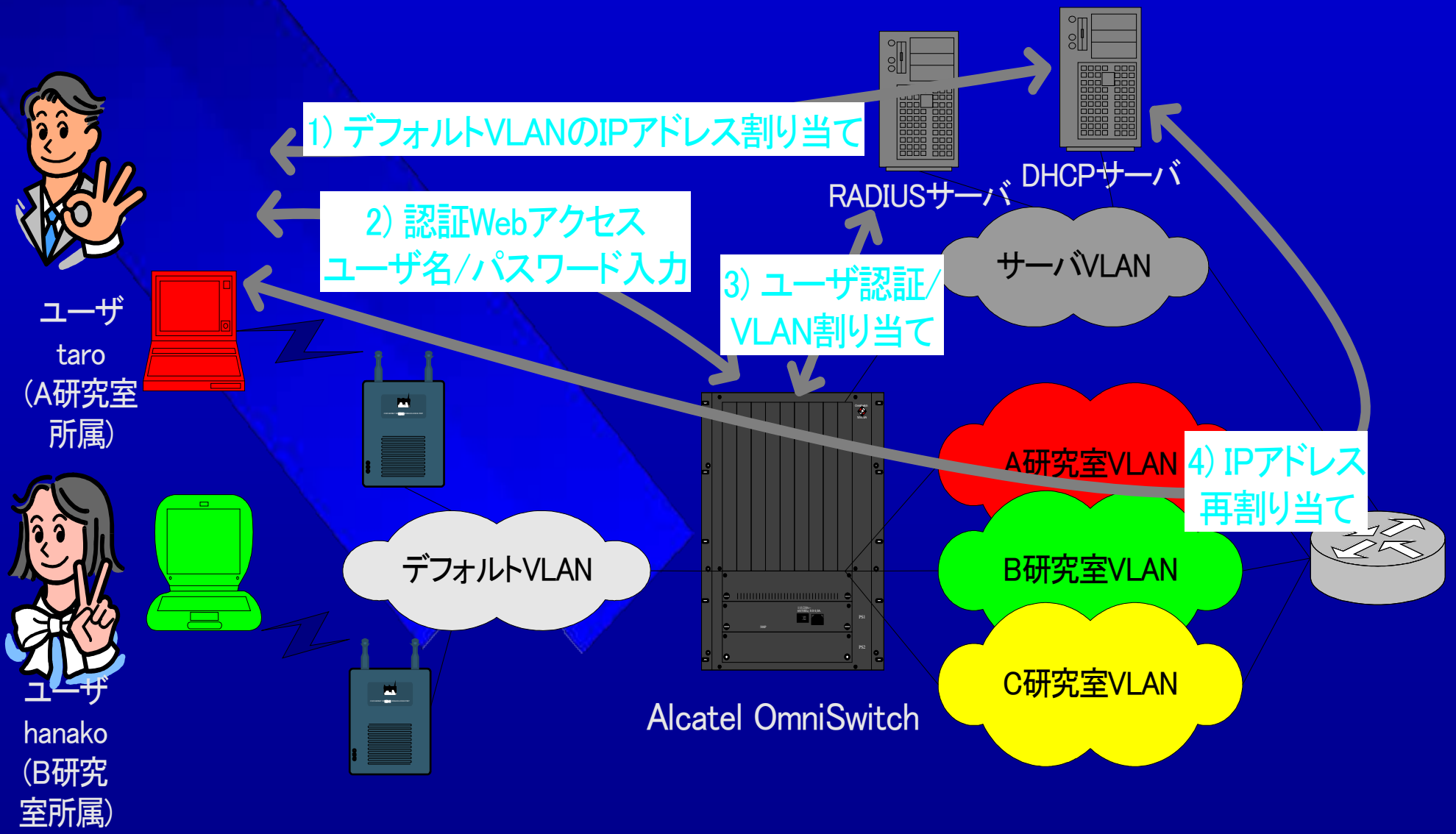
	認証方法	対応
EAP-TLS	デジタル証明書	WindowsXP/2000
PEAP	ユーザ名とパスワード	Windows
LEAP	ユーザ名とパスワード	Cisco, AirMac

- ×EAP-TLS は証明書発行がめんどう
- ○PEAP/LEAP は既存の認証システム利用可能

設計ー VLAN 振り分け方式の選択

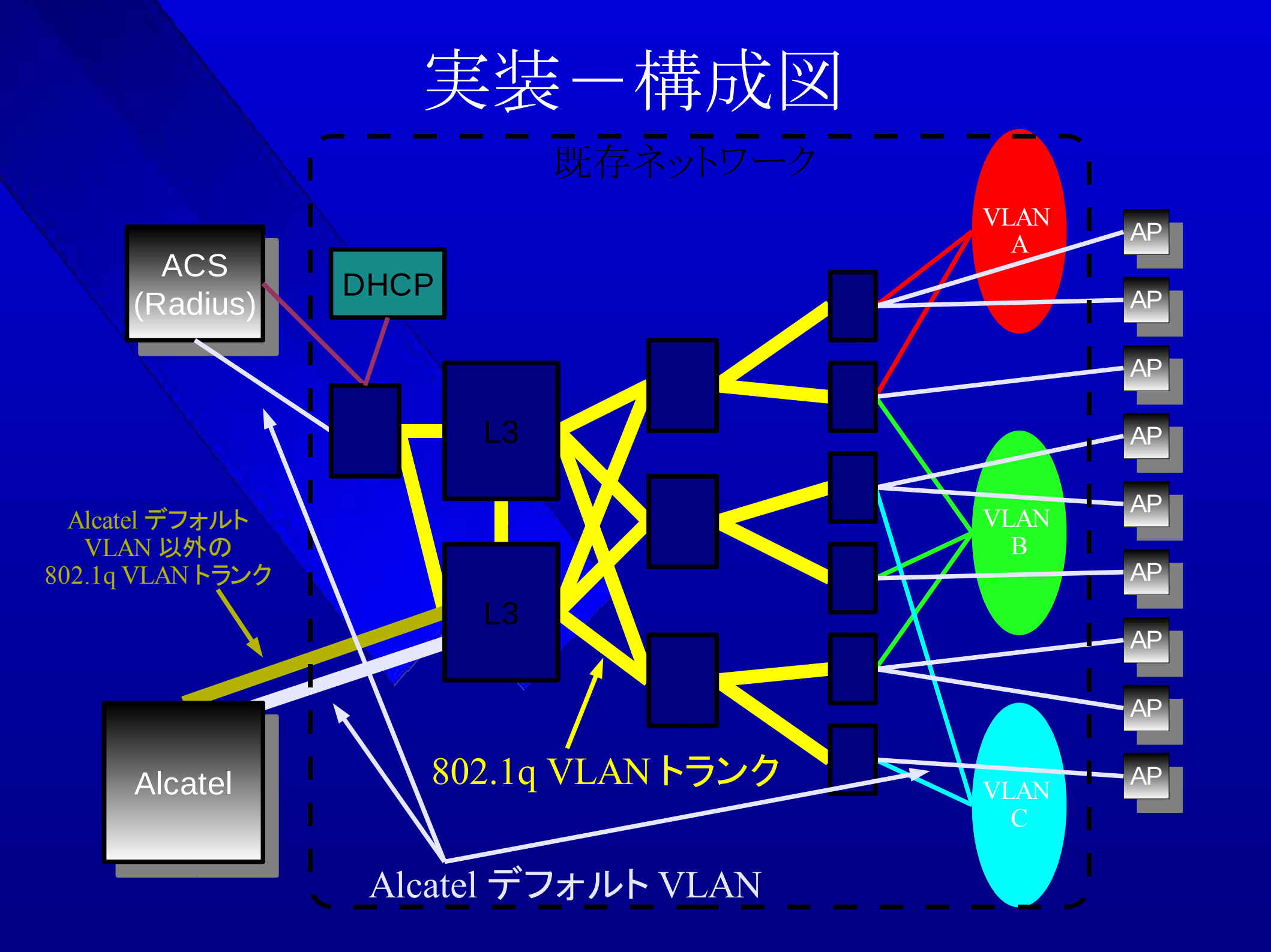
- Cisco Aironet1200 AP の VLAN サポート
  - ○ IEEE802.1x 認証と同時に VLAN 振り分けがすむ
  - × 最大 16VLAN(64 は必要)
- Toplayer Secure Edge Controller
  - ○ ZONE という概念で柔軟なアクセス制御ができる
  - × ZONE とVLAN がマッチしない
- Alcatel 認証 VLAN
  - ○ 設定が簡単
  - × WWW ブラウザで URL を指定して認証が必要

設計ー Alcatel 認証 VLAN 概要

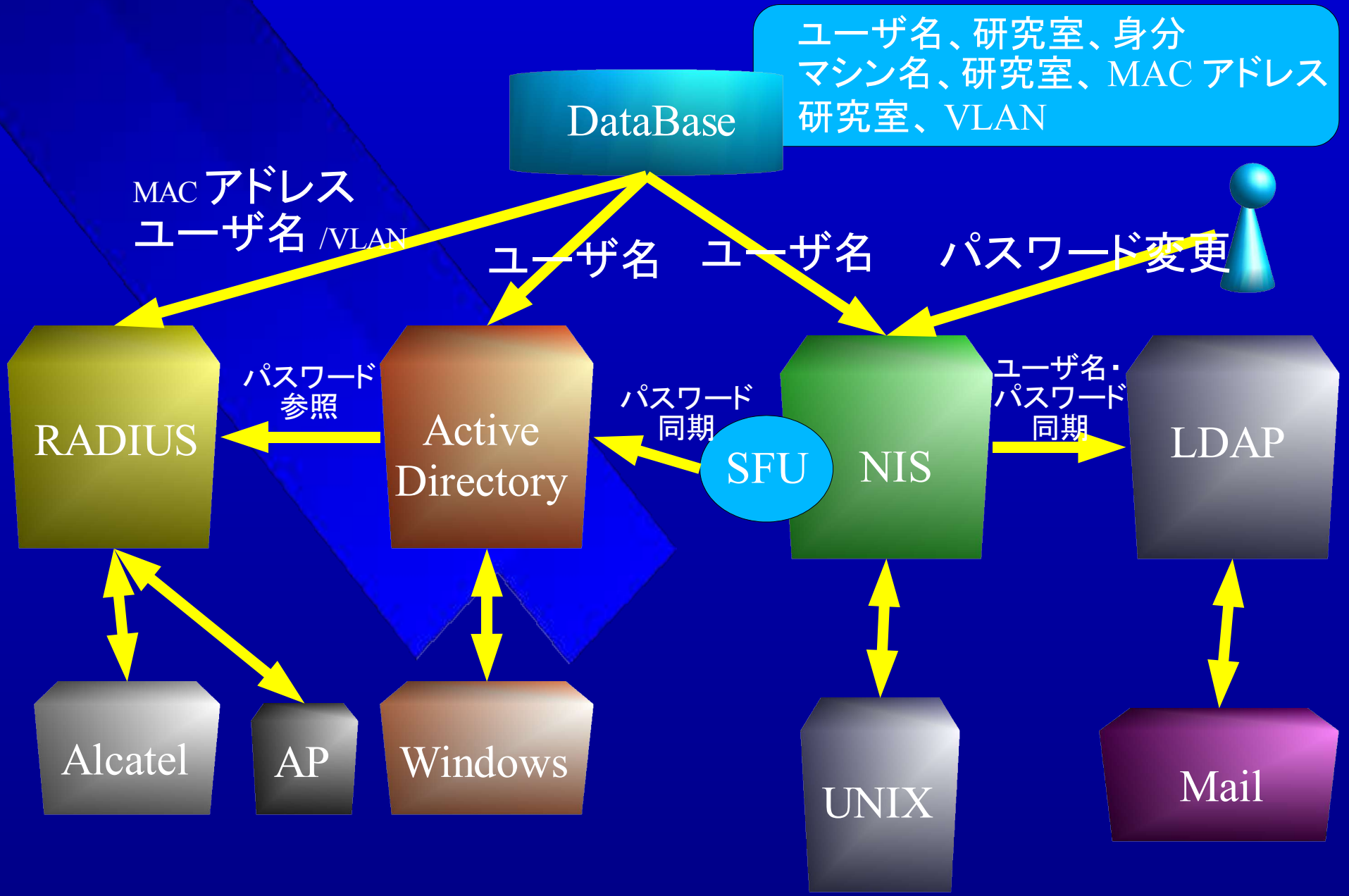


実装

実装ー構成図


既存ネットワーク
ACS
(Radius)
DHCP
L3
L3
Alcatel デフォルト
VLAN 以外の
802.1q VLAN トランク
Alcatel
802.1q VLAN トランク
Alcatel デフォルト VLAN
VLAN
A
VLAN
B
VLAN
C
AP
AP
AP
AP
AP
AP
AP
AP

実装－認証システム


ユーザ名、研究室、身分
マシン名、研究室、MAC アドレス
研究室、VLAN
DataBase
MAC アドレス
ユーザ名 /VLAN
ユーザ名
ユーザ名
パスワード変更
RADIUS
パスワード
参照
Active
Directory
パスワード
同期
SFU
NIS
ユーザ名・
パスワード
同期
LDAP
Alcatel
AP
Windows
UNIX
Mail

実装－従来からの利用者への配慮

- 従来の AP は撤去
- 2003 年 4 月には新しい使い方に移行できず
  - 従来の使い方からの大幅な変更
  - テスト不十分
- 従来の利用方法も可能に
  - AP に 2 つの VLAN と ESS-ID を割り当て

    従来と同じ ESS-ID … 従来の使い方 (棟ごとの共用 VLAN)

    新しい ESS-ID … 802.1x & Alcatel 認証 (自研究室 VLAN)
  - ESS-ID ブロードキャスト停止→接続できないマシン発生
    - 無線 LAN カードのドライバアップデートが必要 (3Com など)

課題

課題

- いまだユーザに公開するにいたらず ...
  - 計算機室員と一部のユーザのモニタのみ
- 問題点
  - RADIUS サーバ
  - クライアントの対応
  - AP の動作
  - 使い勝手

課題－ RADIUS サーバの問題

- PEAP は 2 種類存在
  - MS-CHAPv2 … Microsoft
  - Generic Token Card(GTC) … Cisco
- 導入した ACS 3.1 は GTC のみに対応
  - 結局 Aironet カードでしか PEAP が使えない
- 10 月に ACS3.2 にバージョンアップ、 MS-CHAPv2 にも対応

課題―クライアントの対応

- Windows XP SP1
  - 一部のマシンで PEAP の認証ができない
  - 802.1x を使うと IP アドレス取得に時間がかかる
    - BIOS やドライバアップデートで一部改善
    - WPA サポート修正 (KB 826942) でも一部改善
- Windows 2000 SP4
  - WEP の設定は無線 LAN カードのユーティリティ依存
    → WEP キーを入力しなければならない
  - → キーローテーションを有効にするとつながらない
- Funk Software Odyssey のライセンス取得を検討

課題— AP の動作

- 802.1x と WEP との併用不可
  - PEAP と WEP の併用不可
    - (LEAP と WEP の併用は可能だがキーローテーション不可)
- 数日間で 1 台の割合でハングアップ
  - 190 台の AP が同一 VLAN に存在
  - IAPP を各 AP が 15 秒おきにブロードキャスト
  - 推奨は同一 VLAN 内 30 台以内
    - スイッチ側で MAC アドレスフィルタを設定

課題－ユーザの使い勝手

- Alcatel 認証タイムアウトと DHCP リース時間
  - 一定時間通信がないとデフォルト VLAN に戻る
  - IP アドレスは DHCP リースが切れるまで不変
    - デフォルト VLAN に戻っているのに IP アドレスは自研究室のままの場合も
- Alcatel の認証はめんどう
  - 新しい OS では HTTP のトラップができる
  - ユーザ認証は 802.1x だけで十分？
    - MAC アドレスと VLAN のマッピングに変更？

まとめ、今後の計画

- 802.1x EAP 認証とVLAN 認証
- 認証の手順さえ理解できれば便利に利用できる
- 細かなチューニングをしつつ、来年公開予定
- WPA 対応