

# Secure Wireless Internet Access in Public Places – The CHOICE Network

Anand Balachandran

*University of California, San Diego*

Victor Bahl, Srinivasan Venkatachary

*Microsoft Research, USA*

June 14, 2001

# Outline

---

- Motivation
- Recent Related Work
- CHOICE Network Overview
- CHOICE Architecture and Implementation
- PANS (underlying protocol for CHOICE)
- Performance
- Deployment and Conclusions

# Motivation

---

- To design, implement and deploy a system that would
  - empower individual users to seamlessly access the Internet from public areas
  - enable network service providers to control and monitor network access for each user
  - be lightweight, protocol-agnostic, hardware-agnostic and user-friendly
  - be secure for both the user and the host organization

# Recent Work

---

## ■ Related Technologies

### ■ Network Security

#### ■ Layer-2

- Mac-filtering
- WEP

#### ■ Layer-3

- IPSec

### ■ Authentication, Authorization, Access Control ...

#### ■ Layer-2

- 802.1X

#### ■ App-layer

- AAA, BURP

# Existing Security Mechanisms

---

- Mostly built for enterprise networks
- Layer-2 mechanisms
  - MAC-based filtering – is history
  - WEP key encryption – is being used today
    - ...but is insecure and key management is hard [Nikita01, Arbaugh01]
- Layer-3 mechanisms
  - IPSec
    - Not good in wireless scenarios, because seamless mobility is not easy; involves re-establishing security associations
    - Need something that is protocol agnostic

# Existing Authentication and Access Control Mechanisms

---

- Layer-2
  - 802.1x
    - Requires firmware upgrade on existing APs
    - Will not support APs that are based on different radio access technologies
- App. Layer
  - AAA
    - IETF WG – RFCs are still being revised
  - BURP
    - Proposed WG charter at IETF for individual-centric registration for network access

# Fully Developed Systems

---

- Authenticated DHCP – UC Berkeley (1996-97)
  - Hardware-centric approach, not viable for wireless
- Netbar System – CMU (1997-98)
  - Based on specialized and expensive hardware
- Insite System – U Michigan (1997-98)
  - Similar to the Netbar system
- Secure Public INternet ACcess Handler – Stanford (1998-99)
  - User-friendly, not robust against spoofing attacks

# Bottom Line

---

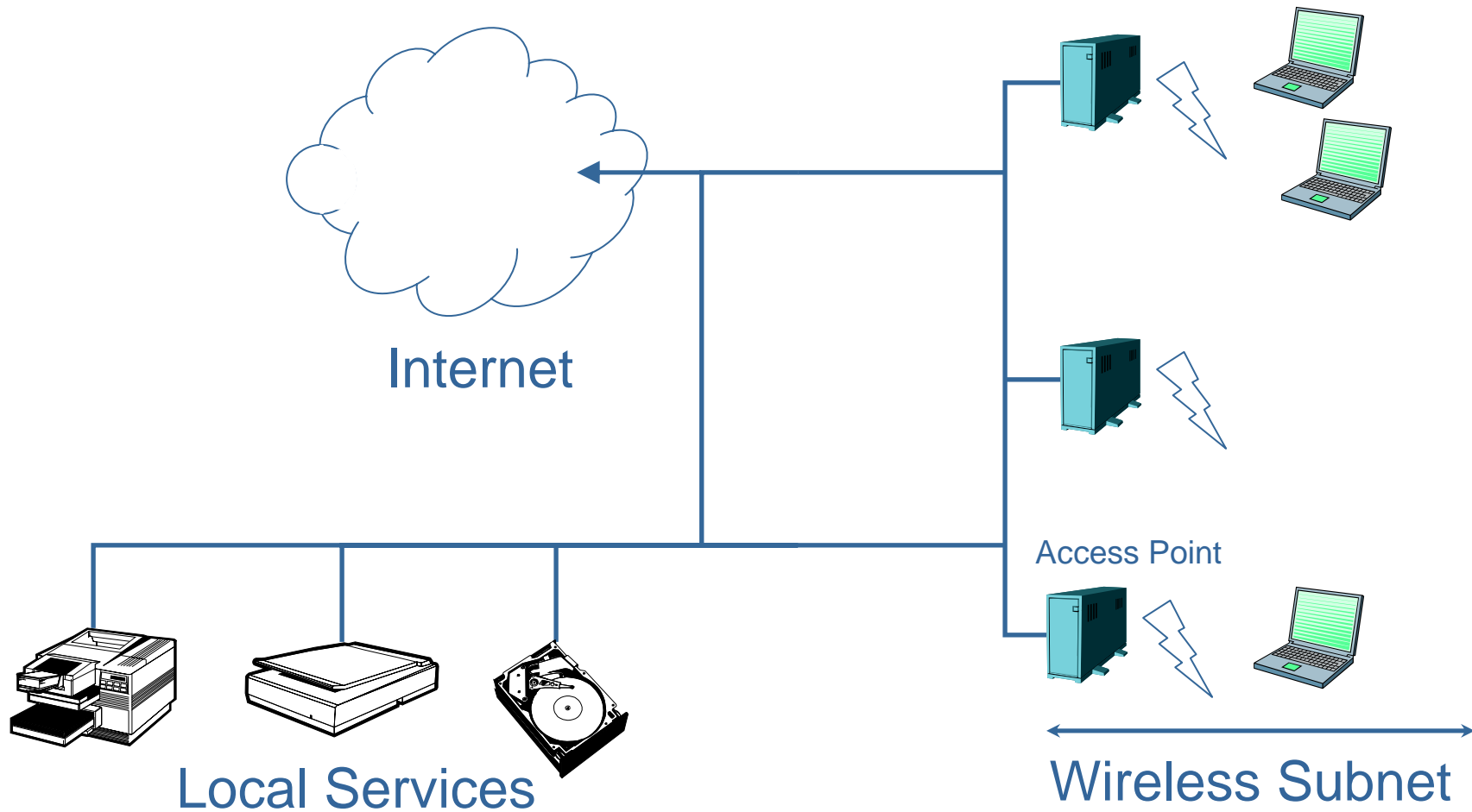
- A system for network access should be is:
  - Hardware-agnostic
    - work with any access technology (802.11, Bluetooth, HIPERLAN)
  - Protocol-stack agnostic
    - Work equally well in the TCP/IP stack and in WAP-based systems
  - Individual Centric
    - Allow network operators to track who is using the network and how it is being used
    - Give user a choice on how they are authenticated -- protect their privacy
  - Able to support multiple authentication schemes
    - AAA (Diameter), Global Authenticators, Credit cards
  - Able to support a viable business model
    - Everyone involved should benefit

# CHOICE Network Overview

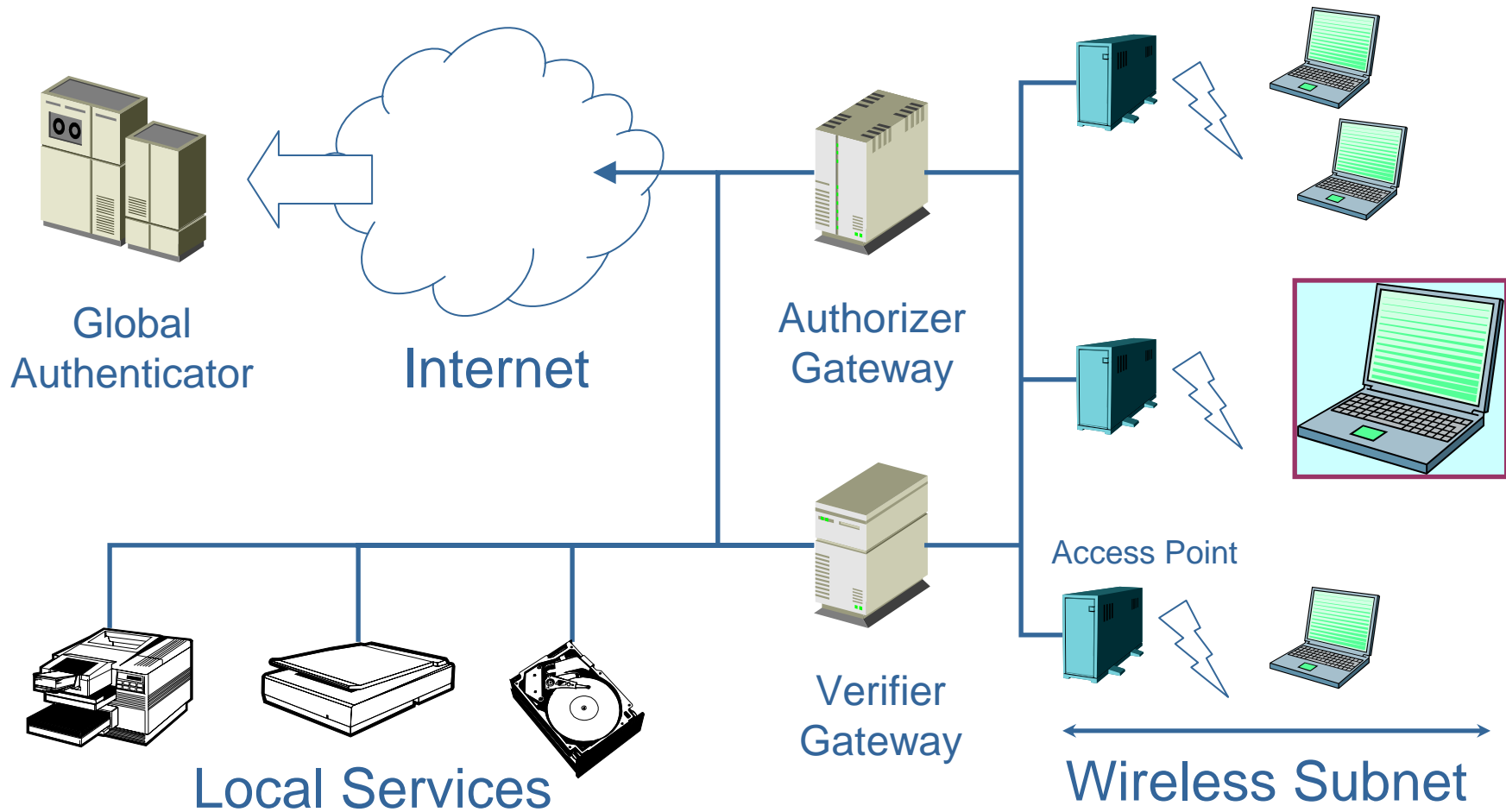
---

- Network Service Detection
  - Broadcast beacons [MIU01]
- Authentication
  - Global Authenticator (MS Passport)
- Authorization (Key generation)
  - Key issued by authorizer to client and verifiers
- Access Control
  - Per-packet Verification at verifier
- Service Provisioning
  - Free access to local services, differentiated charging

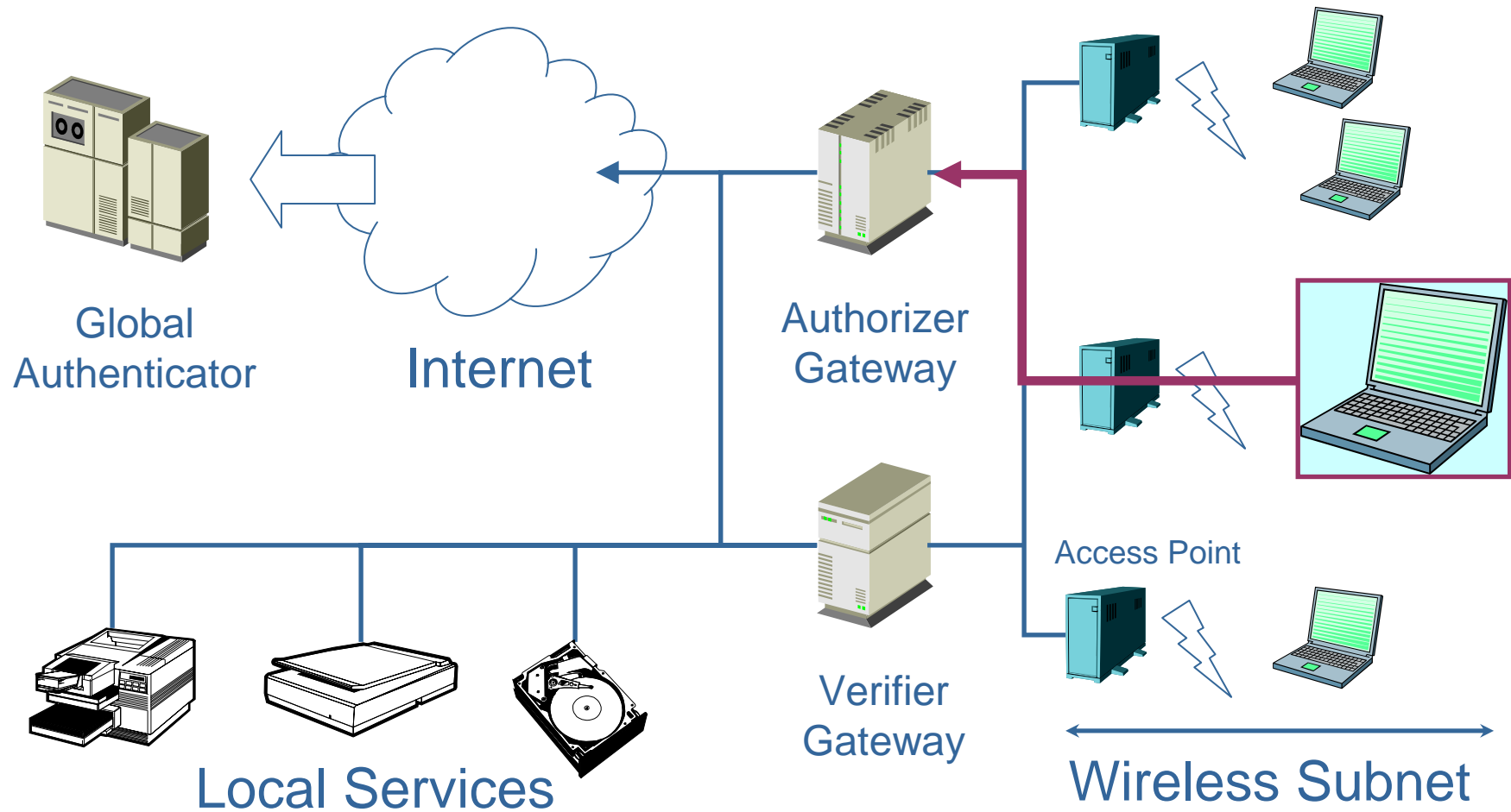
# A Public-area Wireless Network



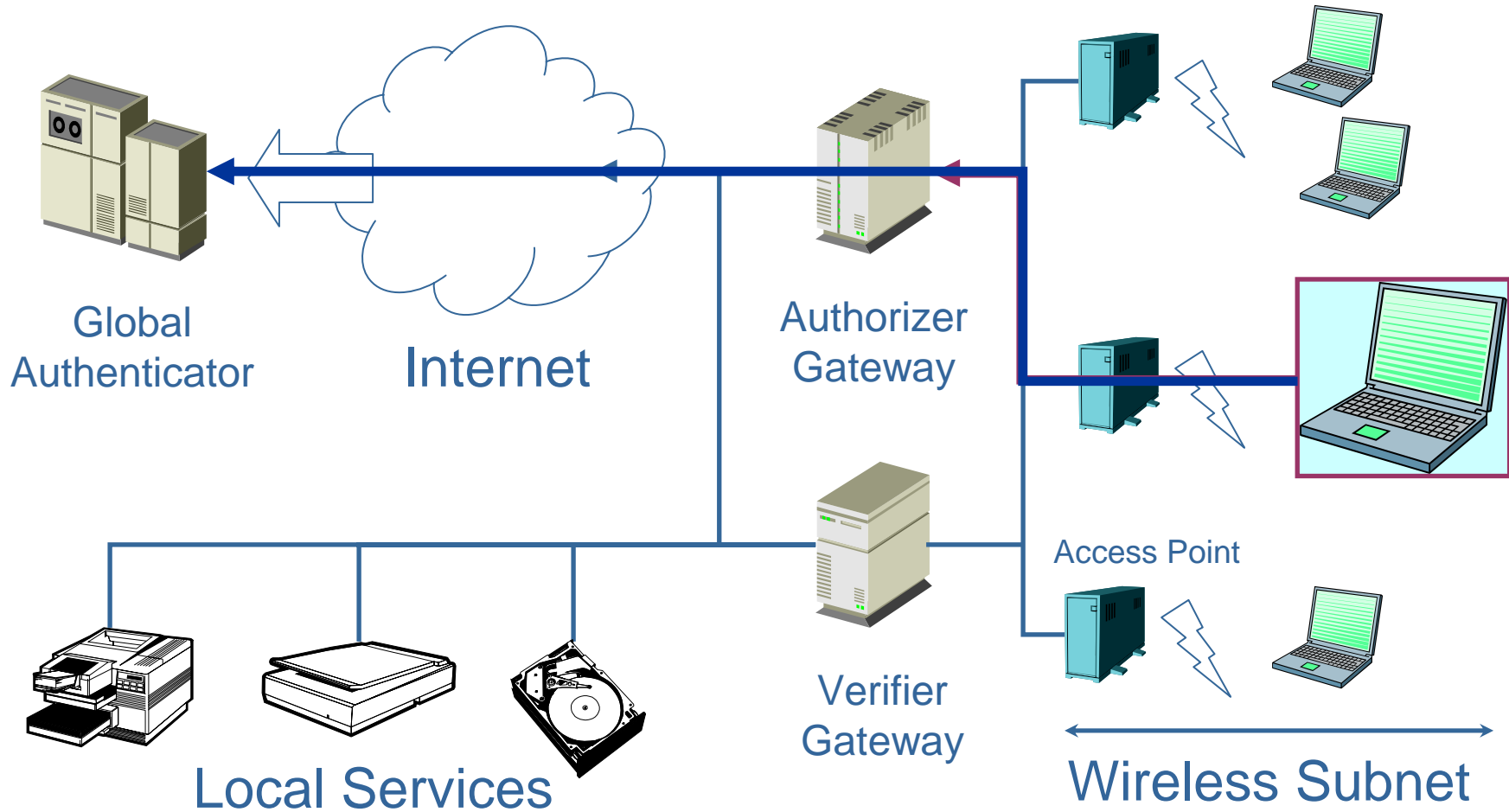
# CHOICE Network Architecture



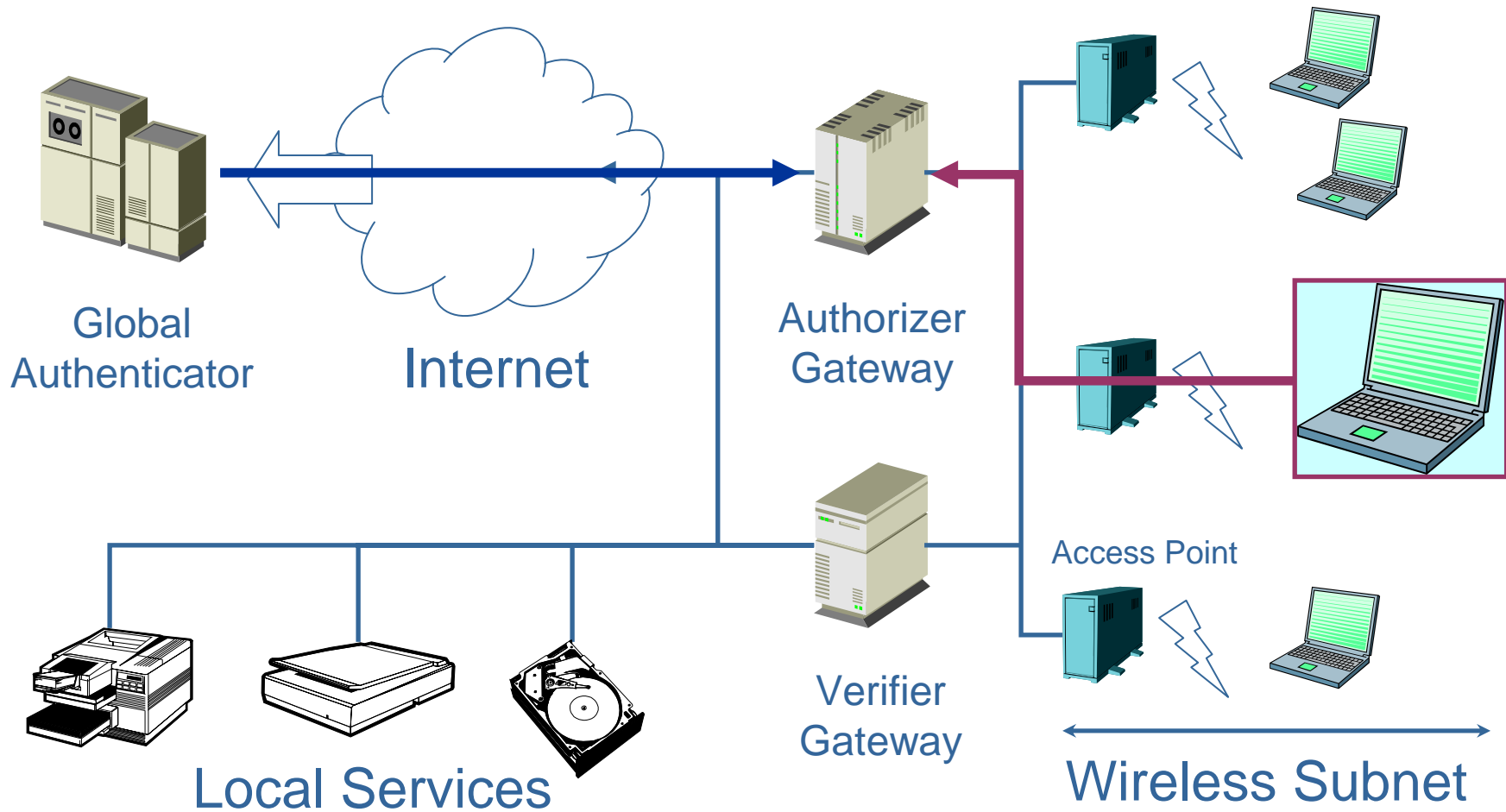
# 1. Network Service Detection



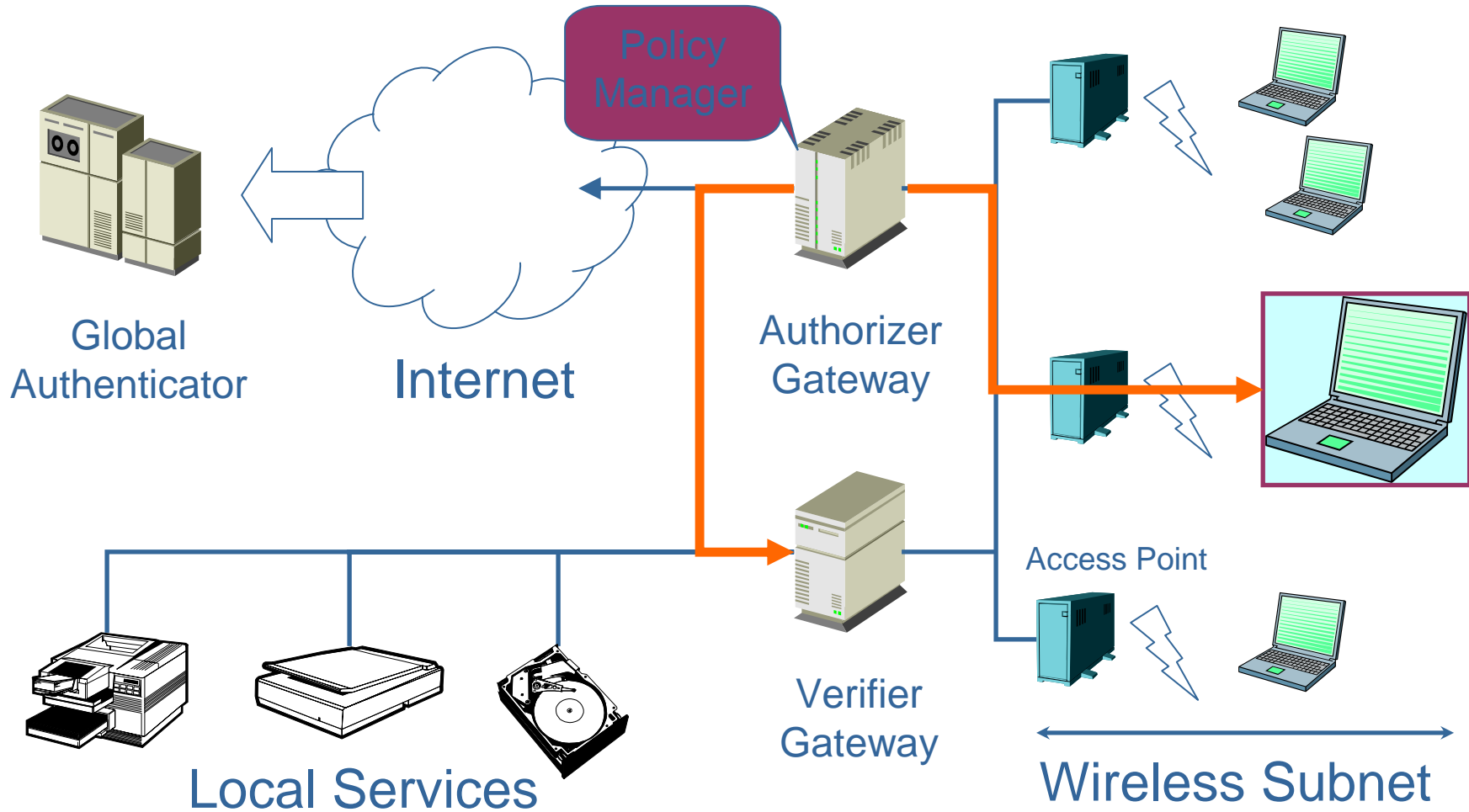
# 2. Authentication



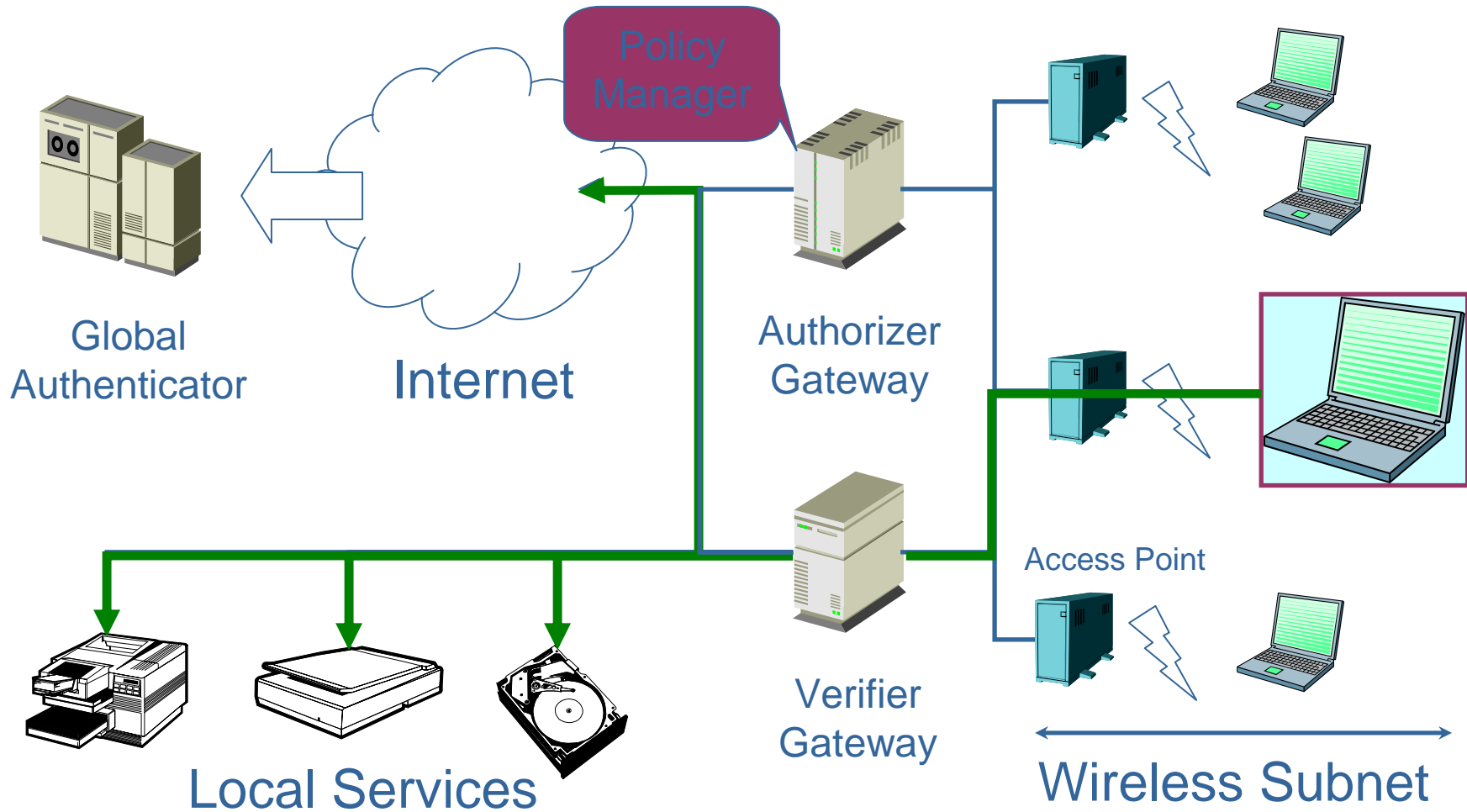
# 3. Authentication Response



# 4. Key Generation



# 5. Access to Intranet and Internet



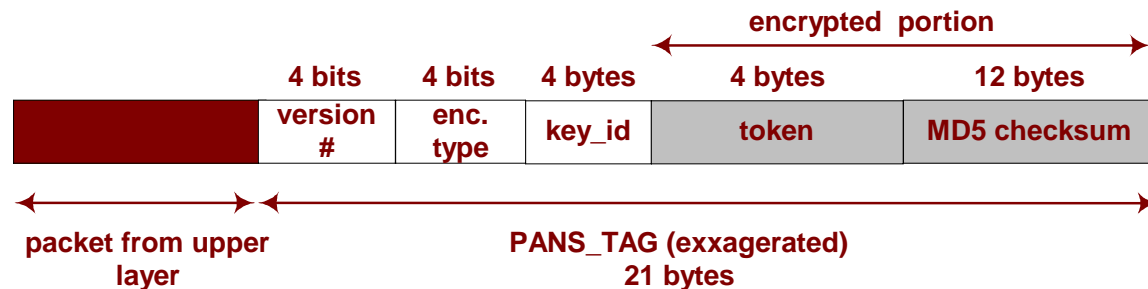
# Key Generation – Behind the Scenes

---

## ■ Underlying Protocol

### ■ **PANS** (**P**rotocol for **A**uthorization and **N**egotiation of **S**ervices)

- A (**key**, **token**) pair is issued to each client
- “**token**” is tagged to the packet and encrypted with the “**key**”



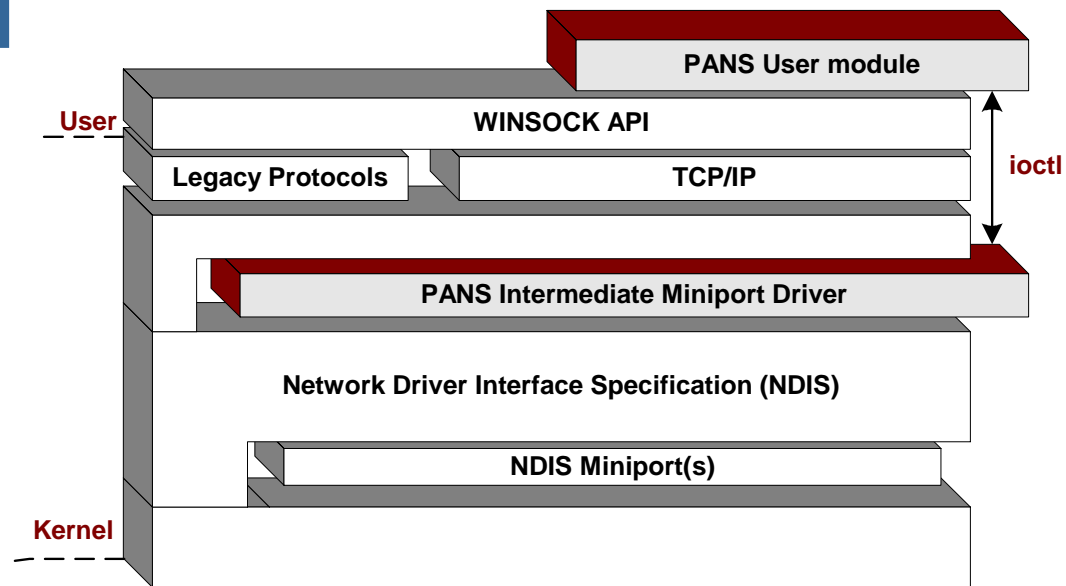
# Key Generation – more

---

- Encryption algorithm is flexible and negotiable
  - 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.
- Key length is flexible
- Key can be changed multiple times in a session
- Data integrity obtained via MD5 checksum

# Access Control – Implementation

packet from upper layer



Client

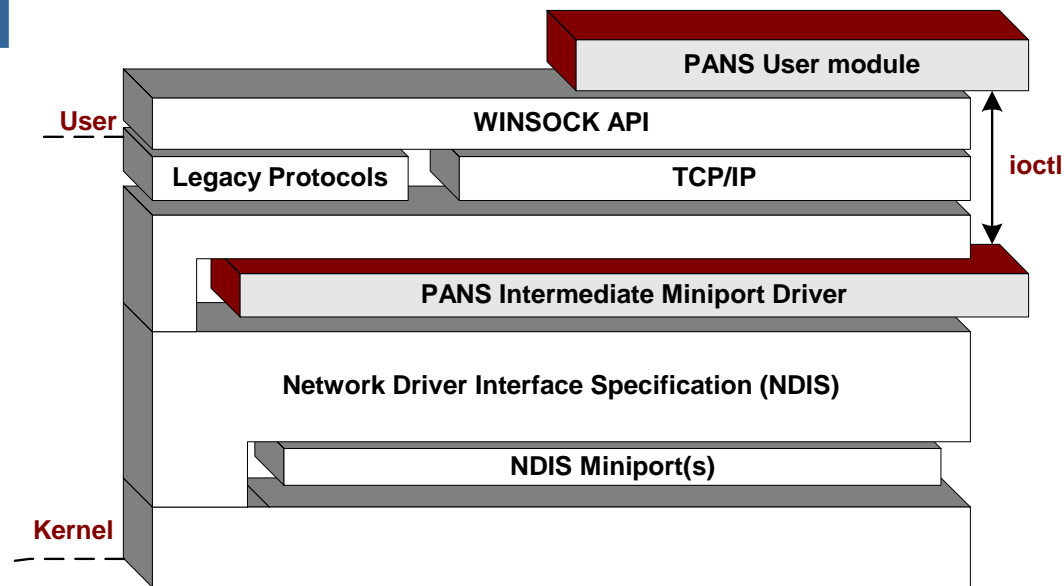


Verifier



# Access Control – Implementation

packet from upper layer



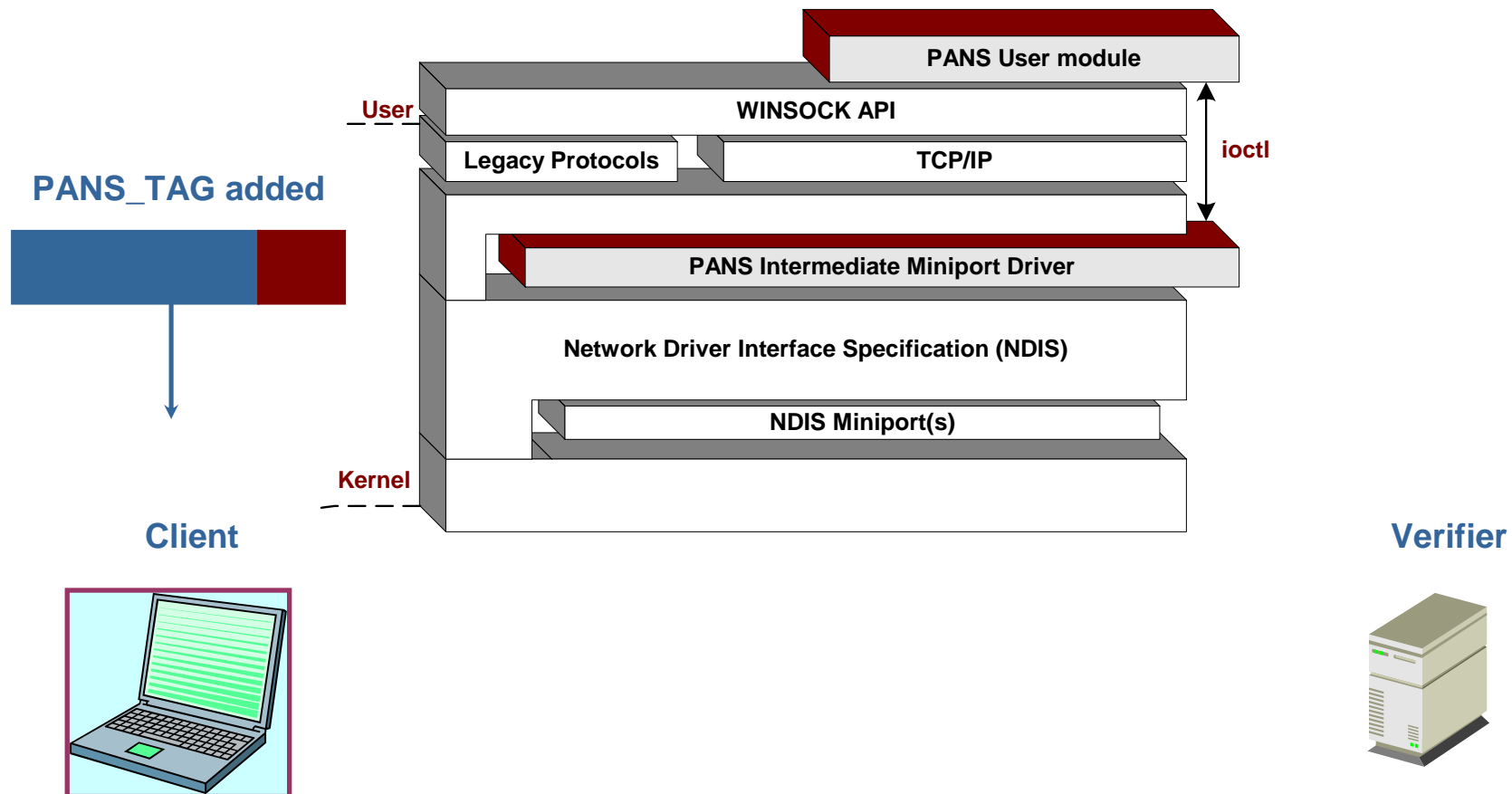
Client



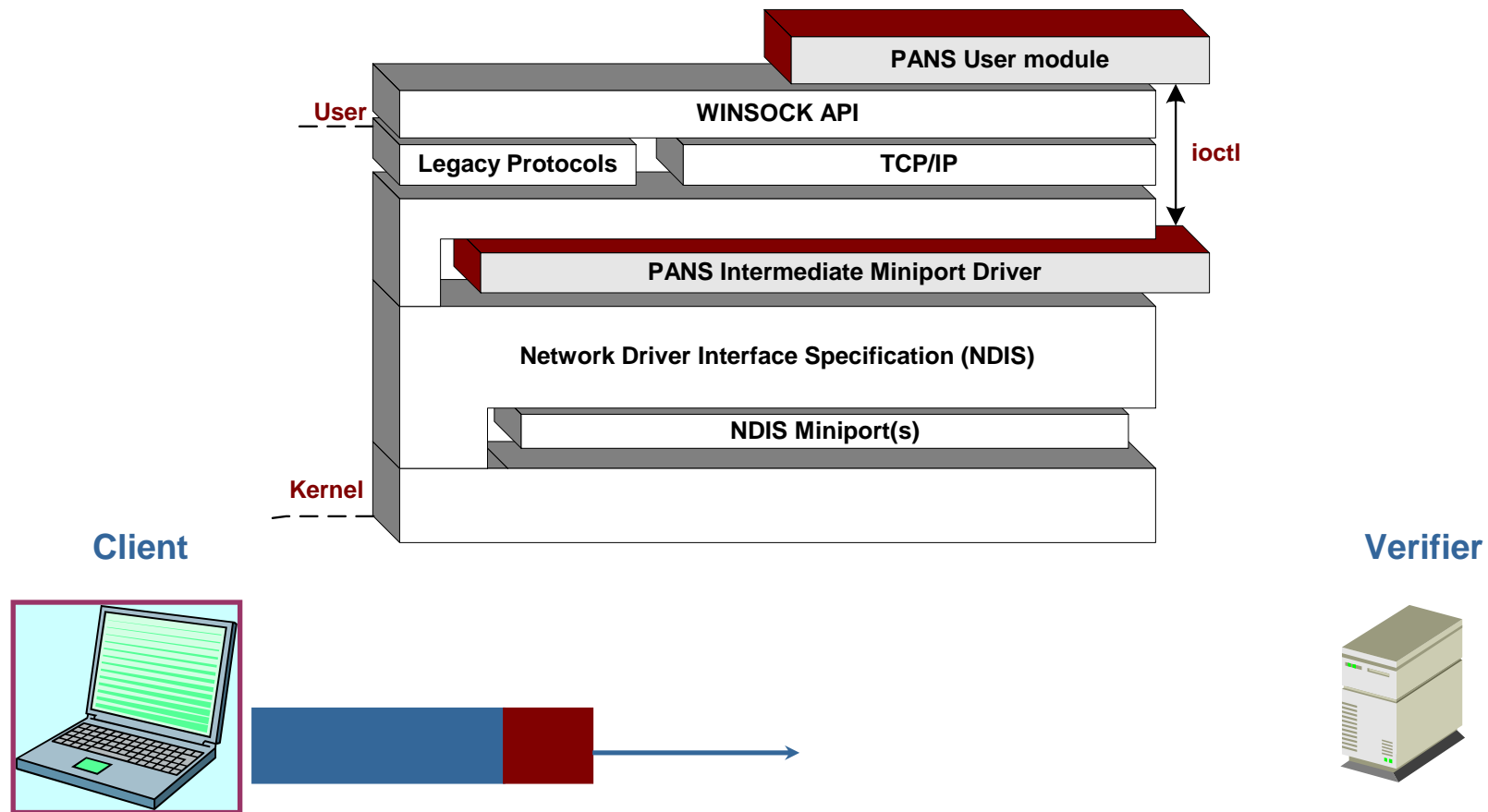
Verifier



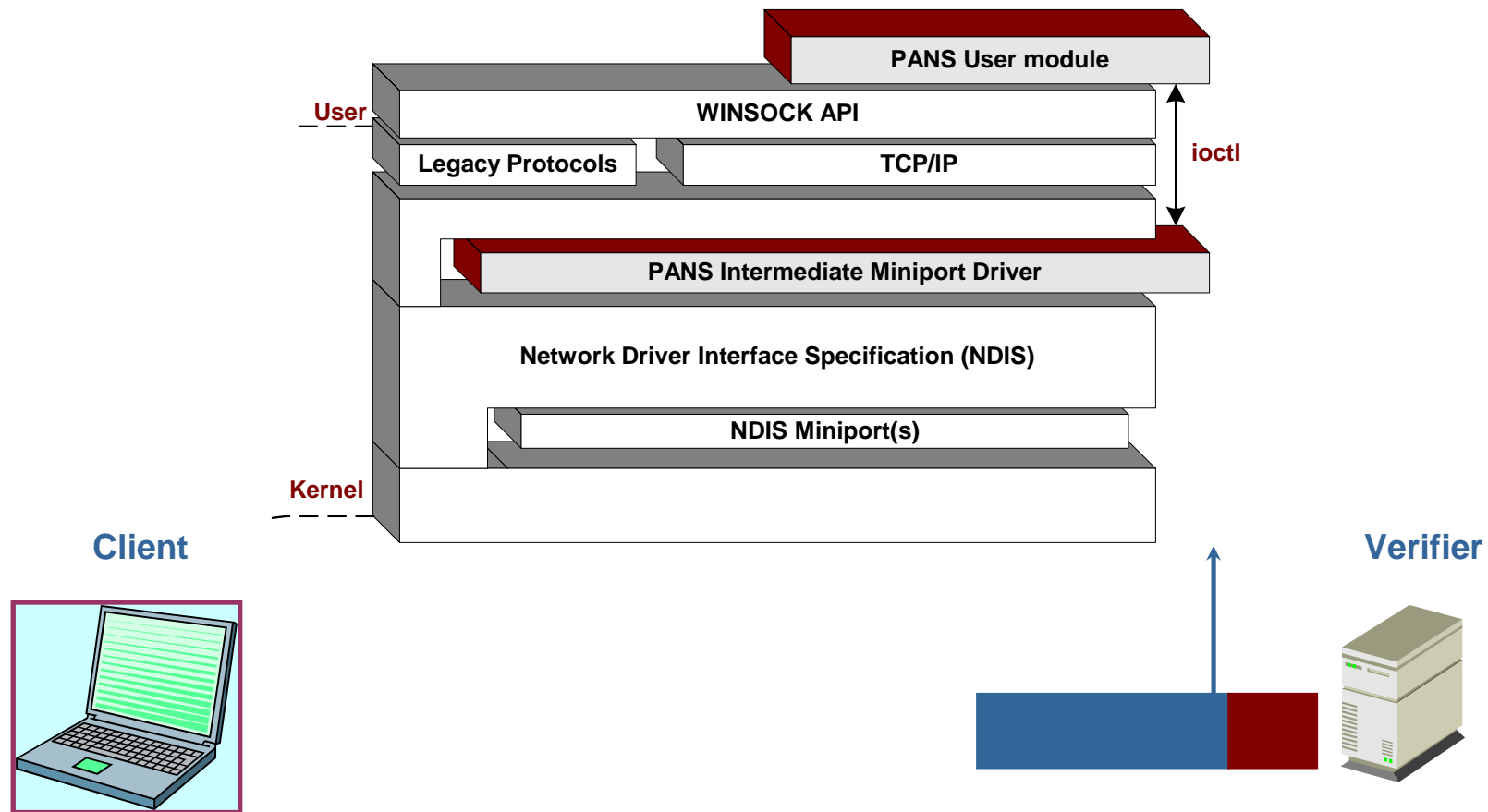
# Access Control – Implementation



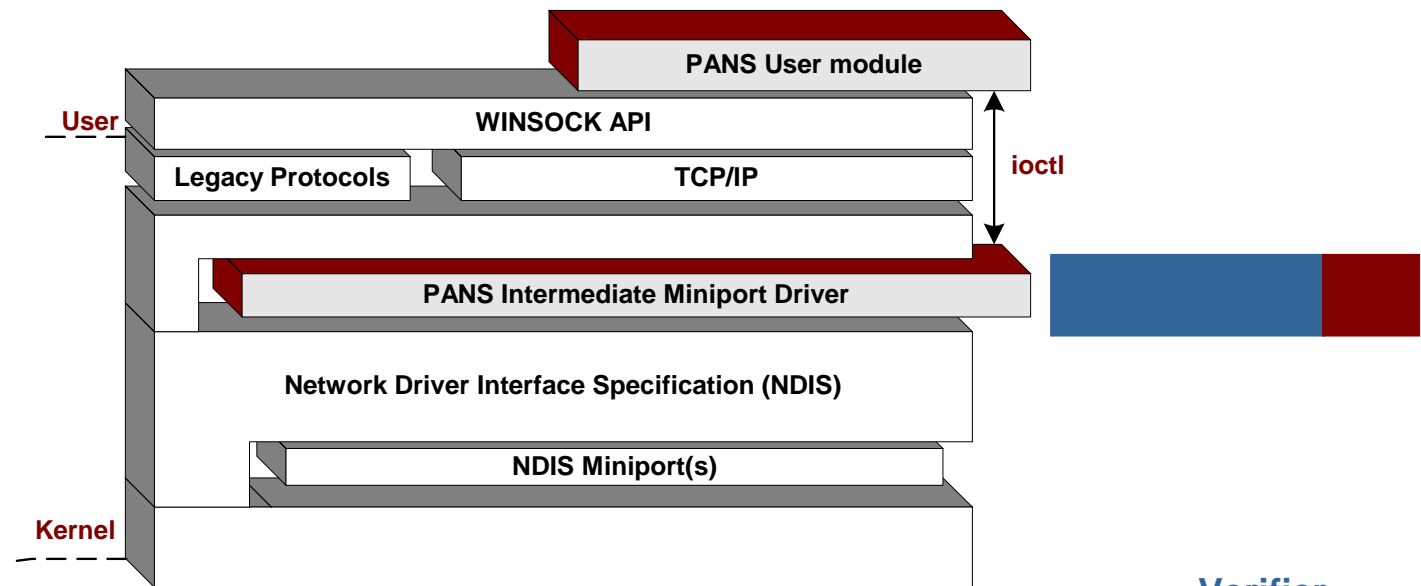
# Access Control – Implementation



# Access Control – Implementation



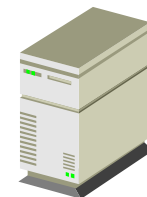
# Access Control – Implementation



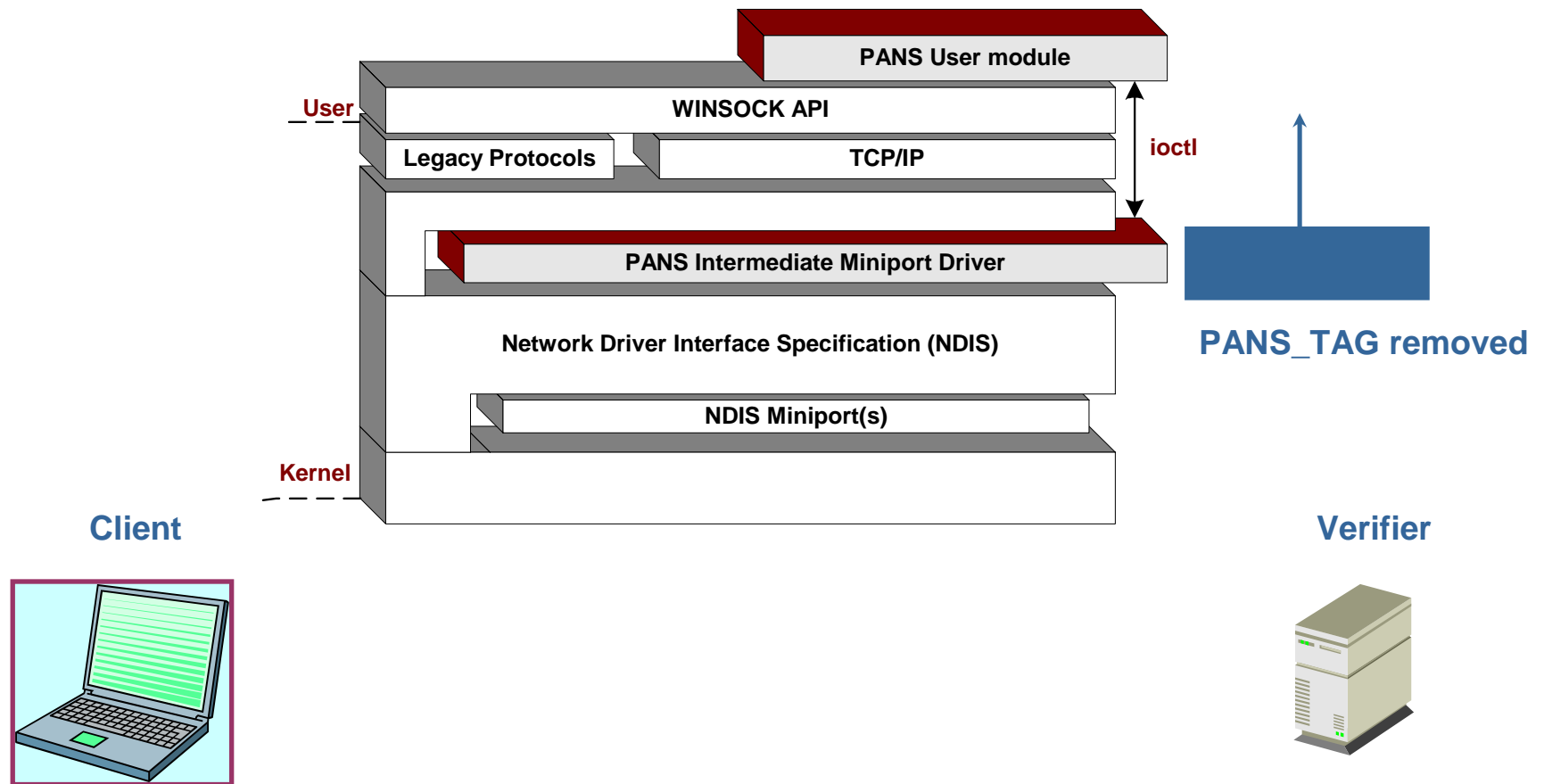
Client



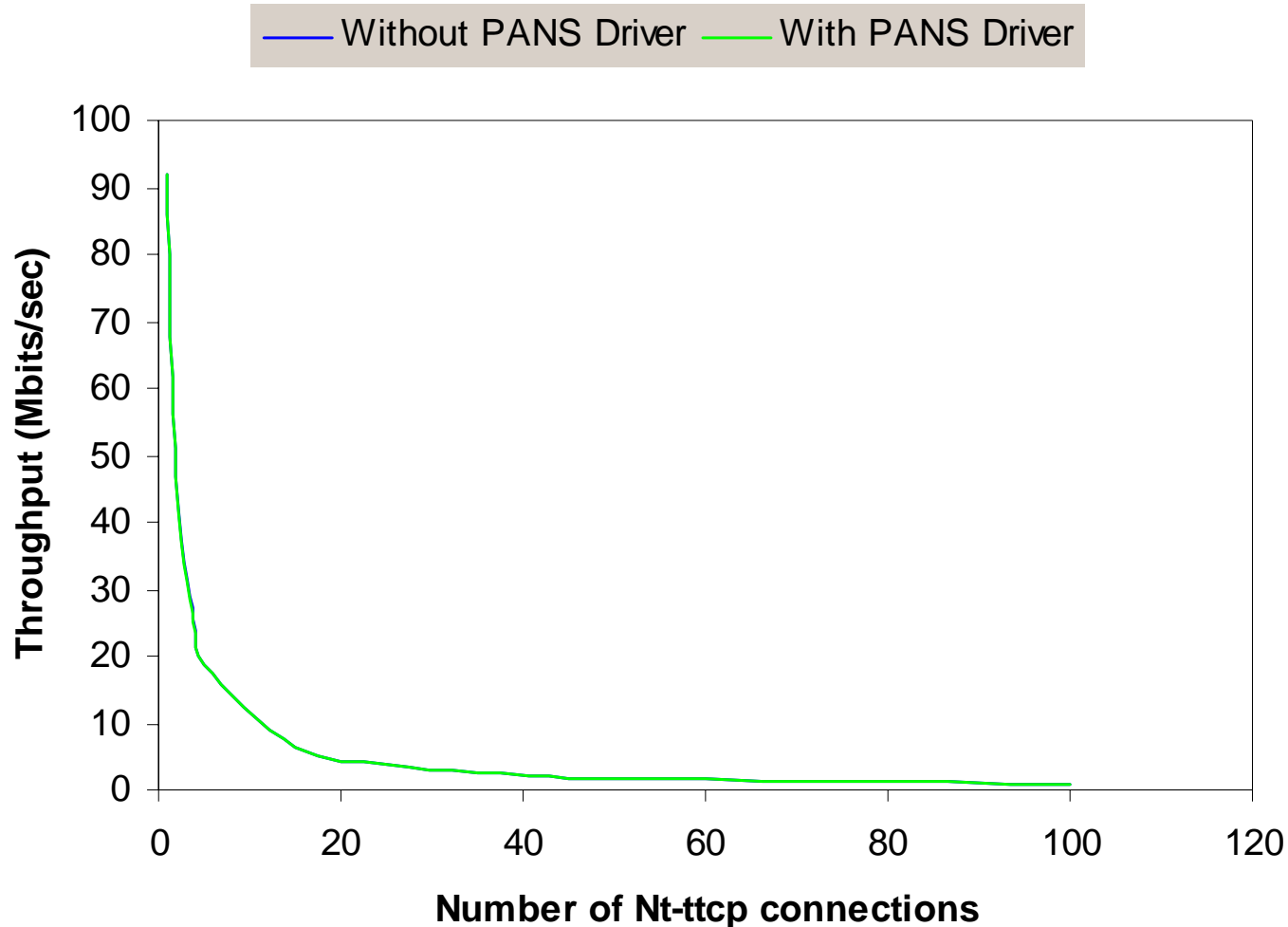
Verifier



# Access Control – Implementation

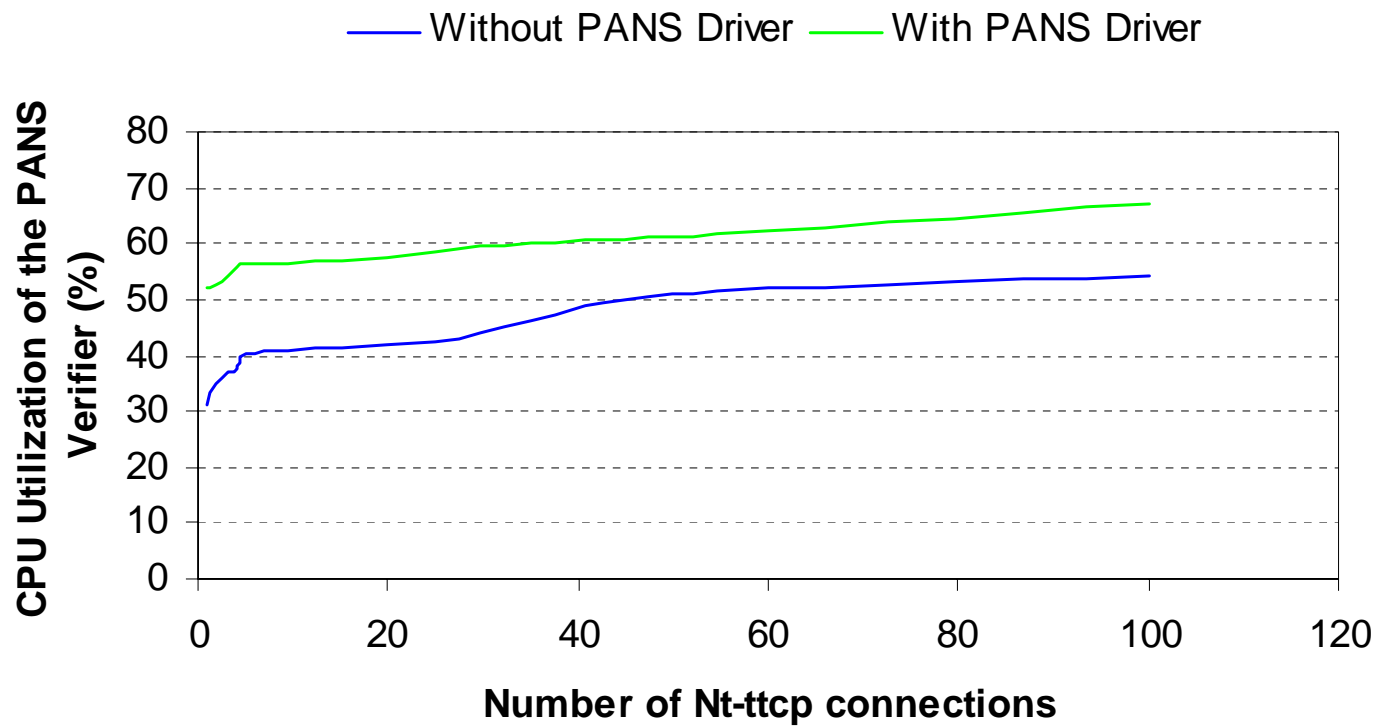


# Verifier Throughput With PANS



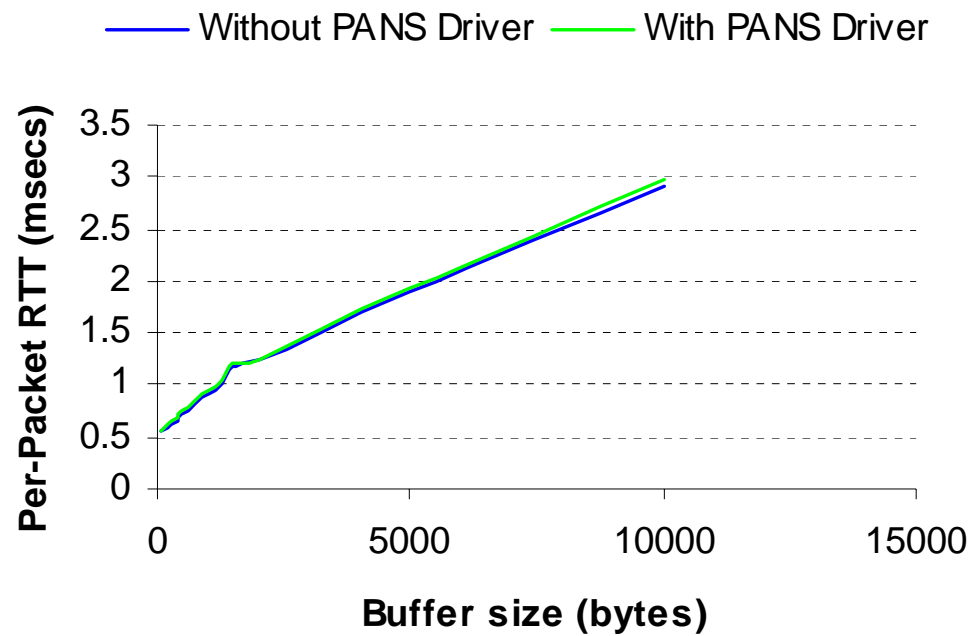
# Verifier CPU Utilization with PANS

---



# Per-packet RTT with PANS

---



# Summary – CHOICE benefits

---

## ■ CHOICE is:

- Complete software solution – hardware- and access-technology agnostic
- Easily downloadable and requires no modifications to protocol stack
- User-friendly – registration and authentication are web-based
- Prevents unauthorized access – safe for the host organization
- Robust against address spoofing and eavesdropping – safe for the end user

**Network deployed and operational in a mall**

# CHOICE Deployment

---



- Deployed at Crossroads Shopping Center, Bellevue, WA
- Operational since Fall 2000
- Provides free access to local services
- Able to track user locations

- Location-based services
  - Active maps, guides
  - Mall buddy discovery
  - Location-based chat
  - On-sale Mall Server

