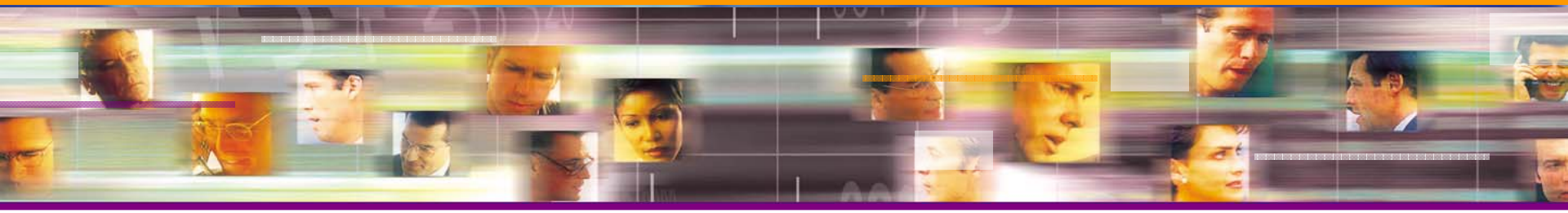
User Authentication in the Enterprise Network

Technology for secure accessibility to Enterprise IT services

Steve Hargis
Technical Director – Office of the CTO
Enterasys Networks

© 2001 Enterasys Networks, Inc. All rights reserved.



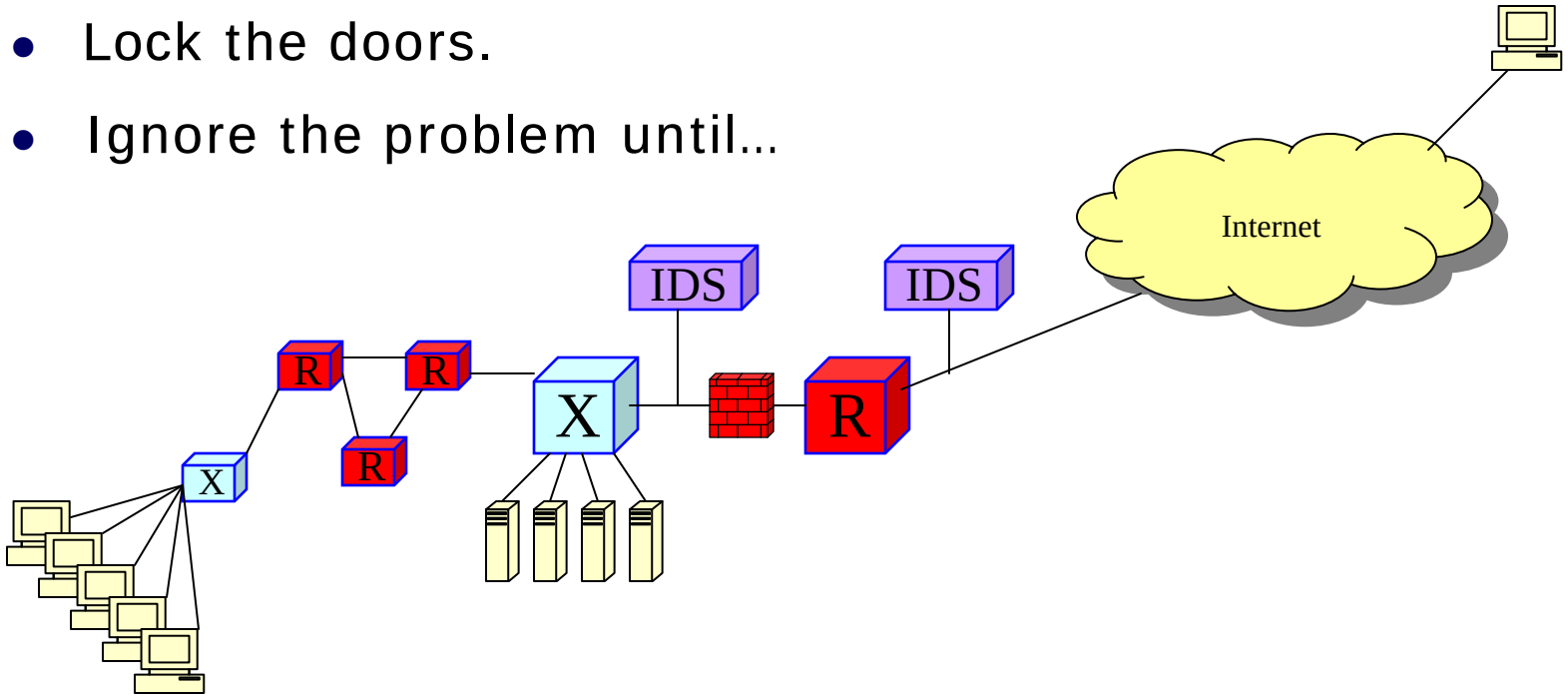
ENTERASYS NETWORKS™

Expectations: Utility-Like Data Services

- High performance (bandwidth)
- Predictability (latency, delivery, etc)
- Availability (total service availability)
- Reliability (utility-like uptime characteristics)
- Cost effective (system wide TCO)
- QoS capabilities (business policies)
- Simplicity (non-complex)
- Manageable (visibility)
- And ???????

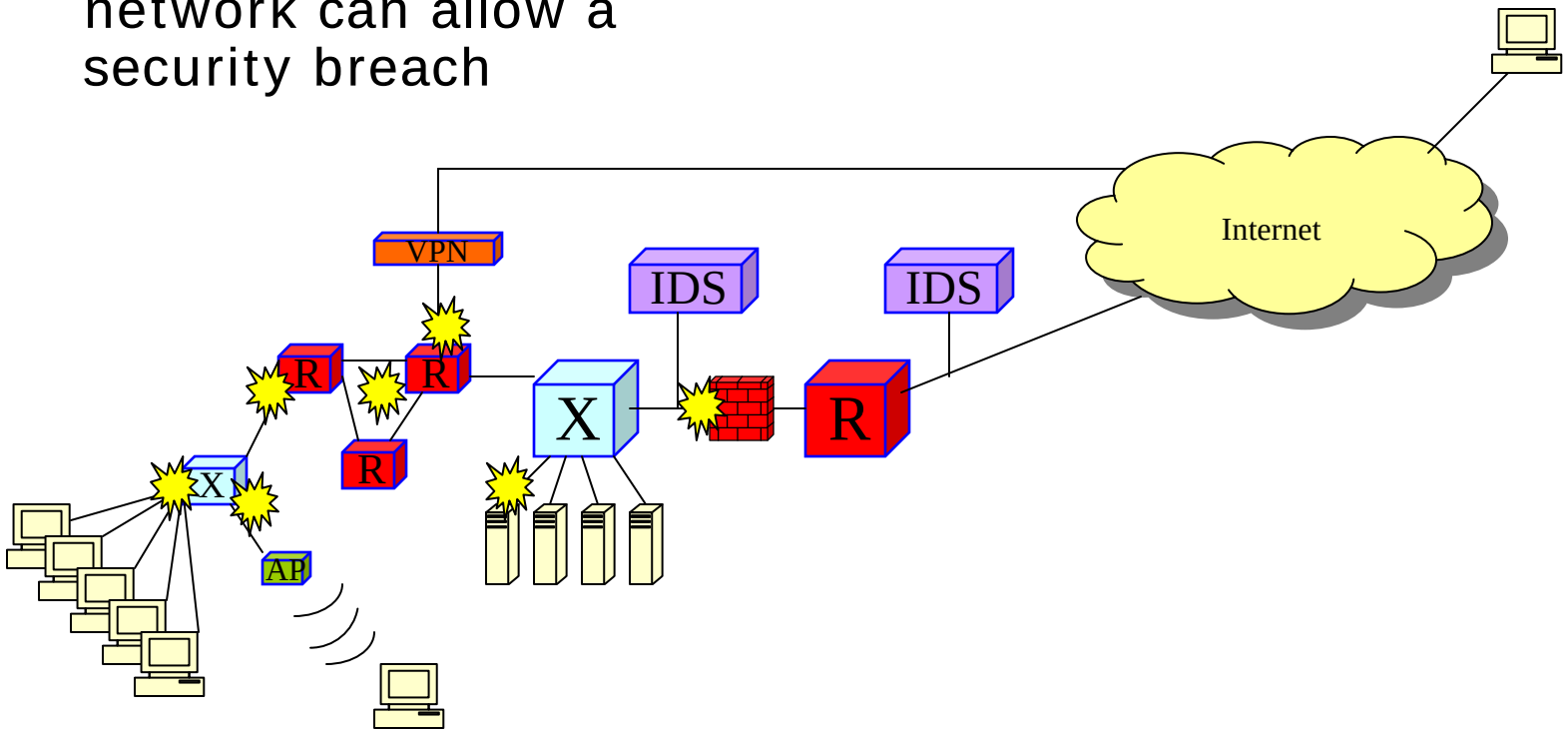
A Traditional View of Security

- Keep the “Bad Guys” out!
- Lock the doors.
- Ignore the problem until…



A Traditional View of Security

- Any point of access to the network can allow a security breach

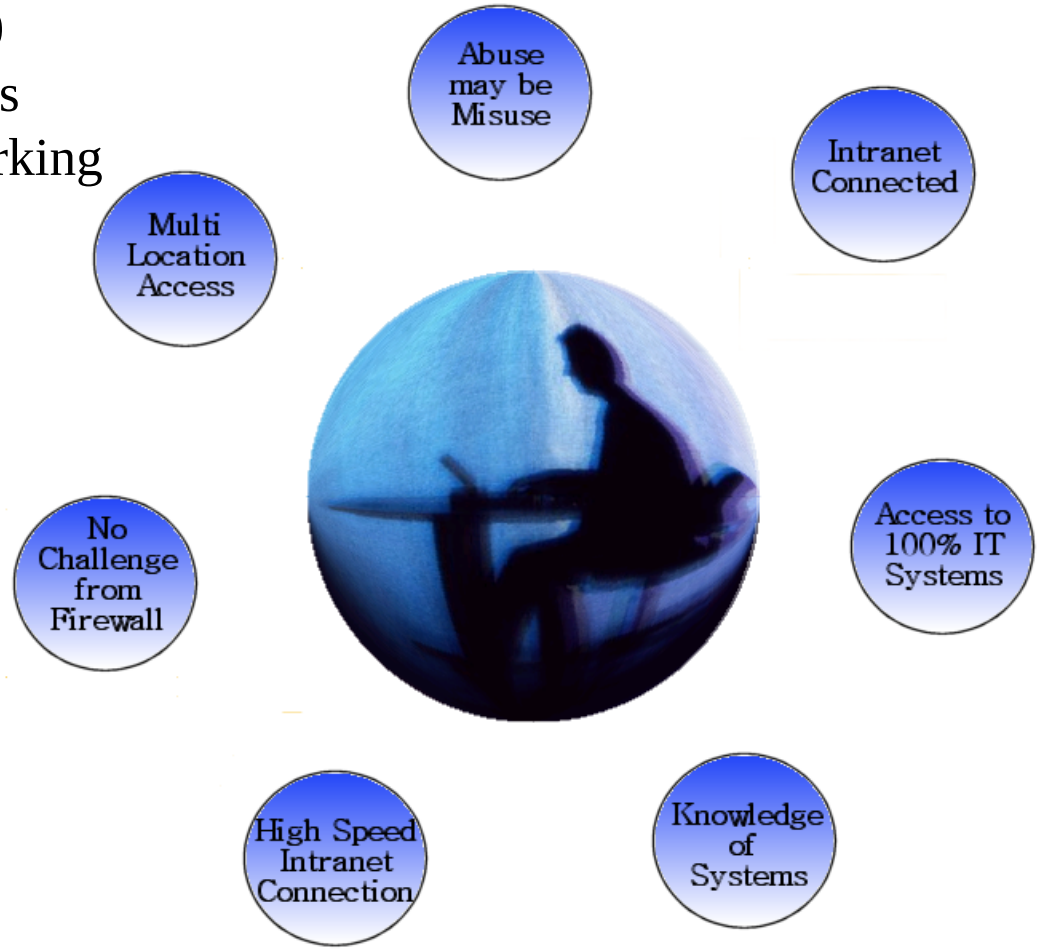


Importance of Infrastructure Security

- Trouble can come from outside or inside
  - "Traditionally, about **70%** of security breaches were being reported as having originated from within the organization itself" - **META Group**
- There are many security holes in most networks
  - The idea of the “trusted machine” is obsolete
  - Unnecessary daemons (processes) running on networked machines allow vulnerabilities to be exploited
  - Defaults (passwords, SNMP community strings, etc) are often left in equipment creating vulnerabilities.
  - "Network complexity combined with a never-ending stream of software upgrades and patches leave many networks vulnerable to attack" - **IDC**

The Threat from PETE

"One in 700 employees is actively working against the company"



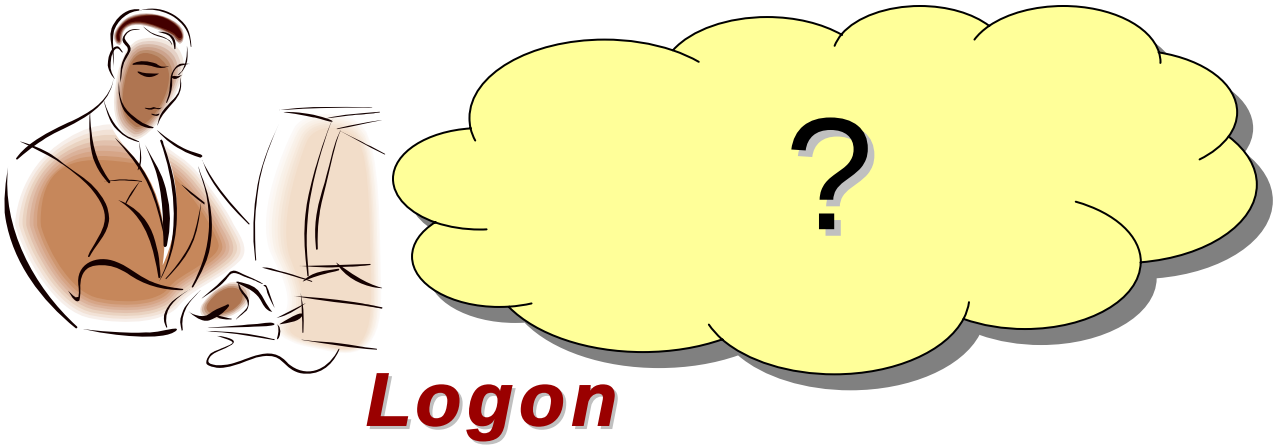
"75% of all technology losses occur from employees and those with trusted relationships"

http://www.asisonline.org

Trends in Intellectual Property Loss

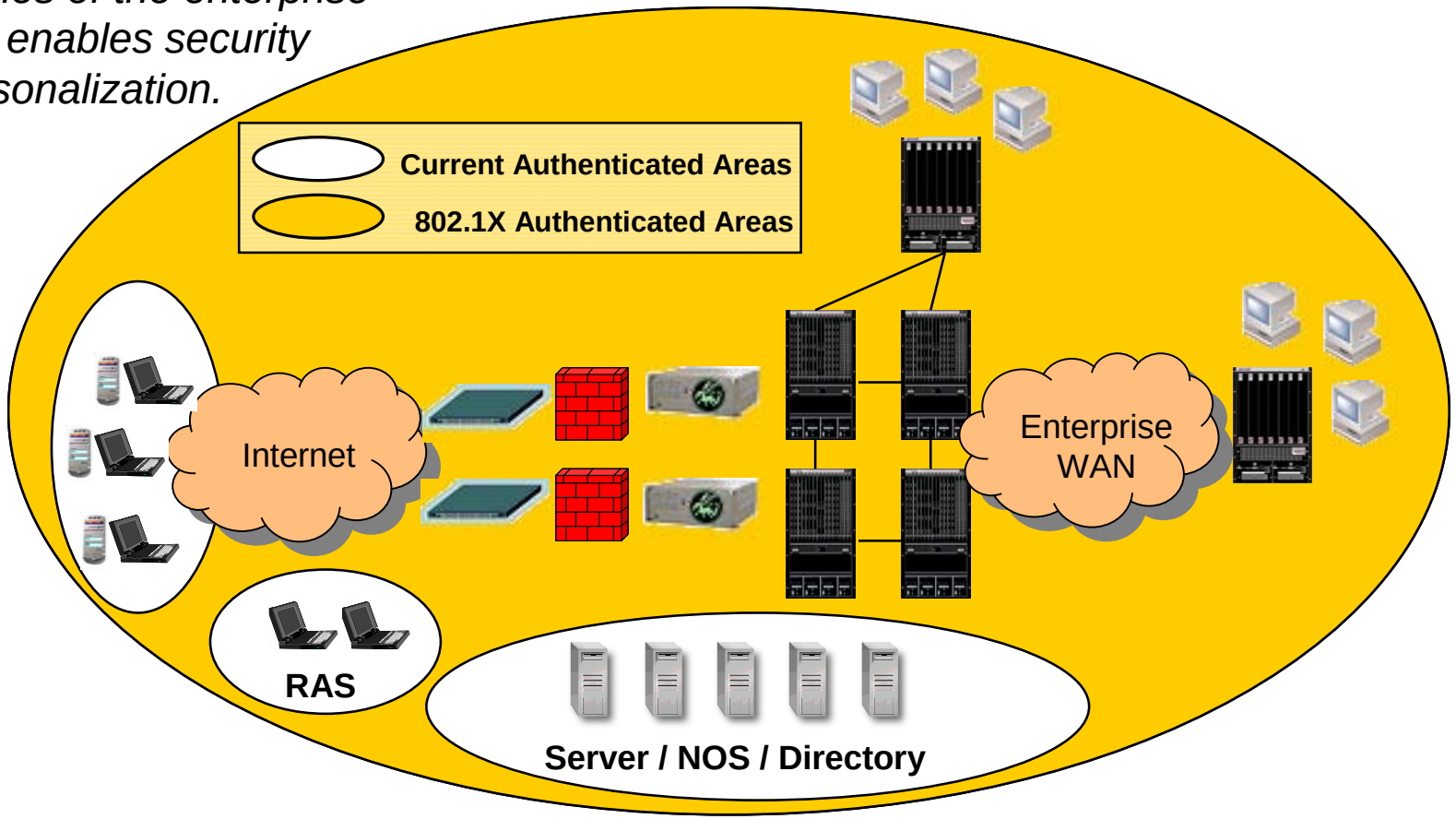
So What About Authentication?

- Who Authenticates today?
  - Remote Access Users (dial-up)
  - VPN Users
  - Everyone – to the Domain and Application Servers



The Need for User Based Authentication

Extending the traditional Authentication boundaries of the enterprise network enables security and personalization.



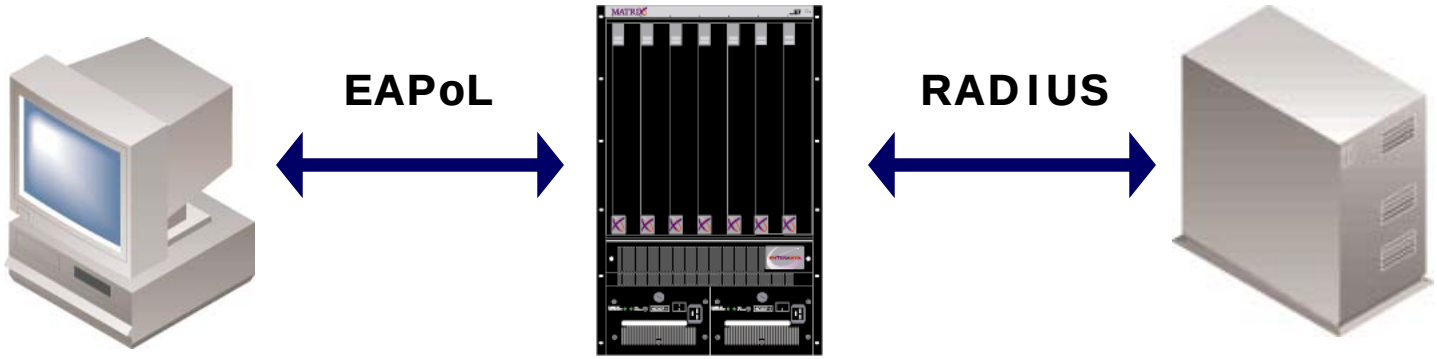
IEEE 802.1X

- Leverages well defined Extensible Authentication Protocol (EAP) {RFC 2294} with some specific extensions for characteristics of 802 LANs (EAPoL)
- EAP is a general protocol supporting various authentication methods (MD5, TLS, Smartcards, Certificates, PKI, 2-Factor, etc.)
- 802.1X is a method for performing authentication to obtain access to IEEE 802 LANs.
- Ideally occurs at the first point of attachment (edge device)
- Specifies a protocol between devices desiring access to the LAN and devices providing access to the LAN
- Specifies the requirements for a protocol between the Authenticator and an Authentication Server (e.g. RADIUS)
- Specifies management operations via SNMP

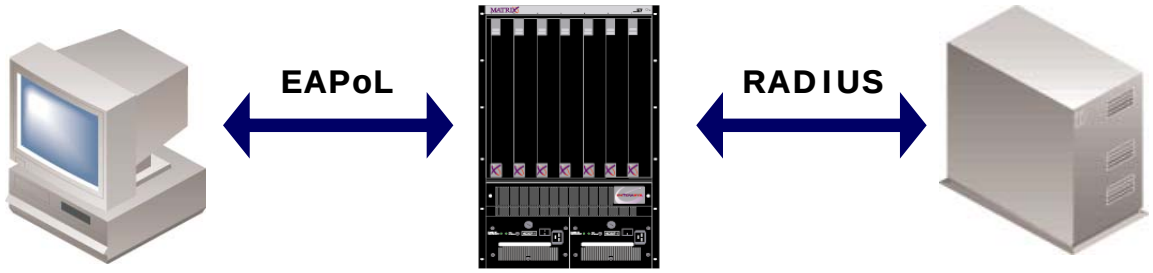
Definitions

- Authenticator
  - An entity that requires the device on the end of an attached link to be authenticated.
- Supplicant
  - The device entity requesting to be authenticated by the Authenticator and thereby gain access to the services of the Authenticator.
- Authentication Server
  - An entity providing authentication administration to the Authenticator.

General Topology



Authentication Process



Supplicant | **Authenticator** | **Authentication Server**

EAPoL

EAP Start

EAP Request/Identity

EAP Response/Identity

RADIUS Access-Request

EAP Request

RADIUS Access-Challenge

EAP Response (cred.)

RADIUS Access-Request

EAP Success!

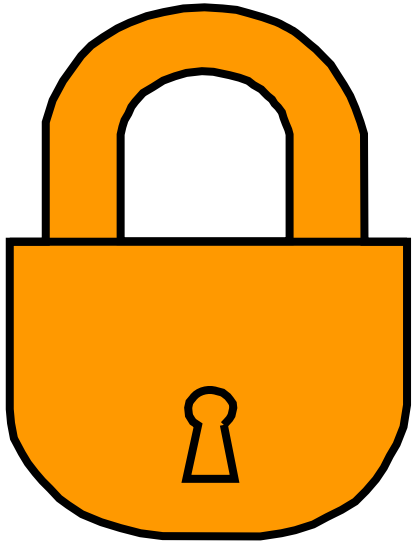
RADIUS Access-Accept

RADIUS

ACCESS ALLOWED!

Why is Authentication So Important?

- The Obvious
- The Not So Obvious…



The User Personalized Network - UPN

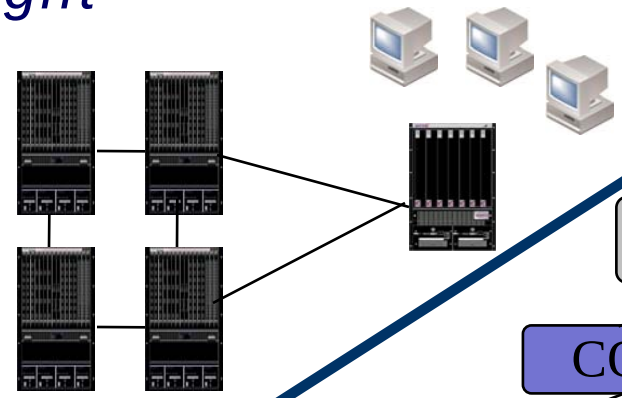
- Mass Customization of the application and information experience is the unavoidable trend and goal
  - Past : www.yahoo.com
  - Present : www.myyahoo.com
  - Future : www.JohnSmith.com or just “John Smith”
- Unfortunately your infrastructure has no idea of the persons using it
  - We think falsely that we “log into the network”
  - Infrastructure is not user personalized today
- A UPN is:
  - A heterogeneous virtual enterprise connectivity system that
  - Provides homogeneous services to people
  - Based on their relation to the business

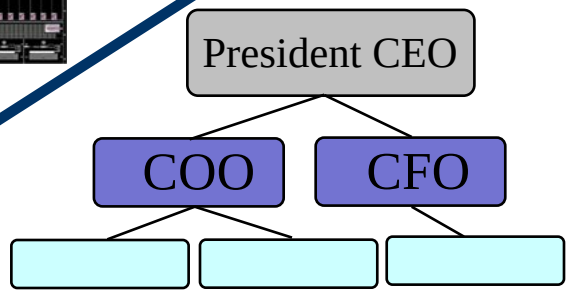
The Current Model

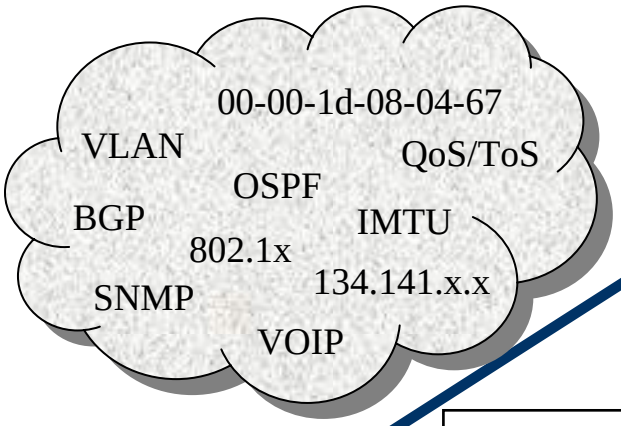
To date, ships in the night

The Network…

```
IP interface add 134.141.x.x/24 vlan blue
IP route add static 134.141.130.x/24
ACL 100 IP permit 134.141.x.x 192.168.x.x any any
VLAN create IP 134.141.x.x interface et.2.5,8
```







"The Directory"

12,073	Revenue
(121,098)	Utilities
(1,23)	IT budget
(8,467)	Gambling
(101,601)	Compensation
(240)	Restocking
=========	==========
XXX,XXX	**Net Income**

The Business…

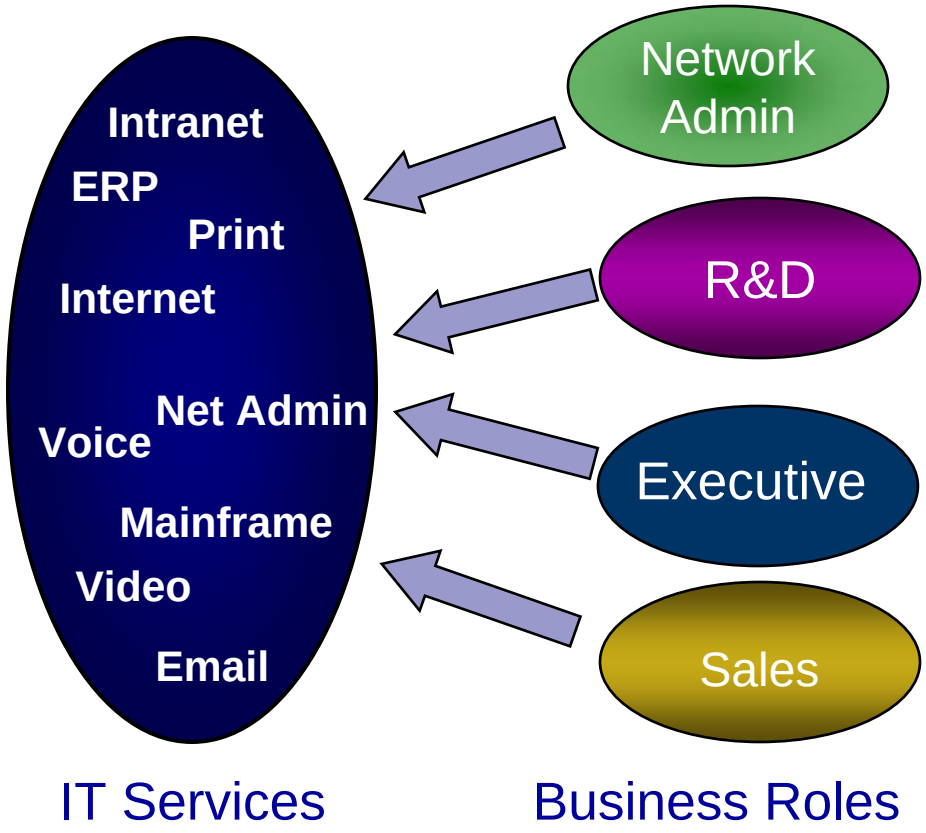
Aligning IT with the Business Model

The **User Personalized Network** understands who individual users of a network system, as well as their relationship to the business.

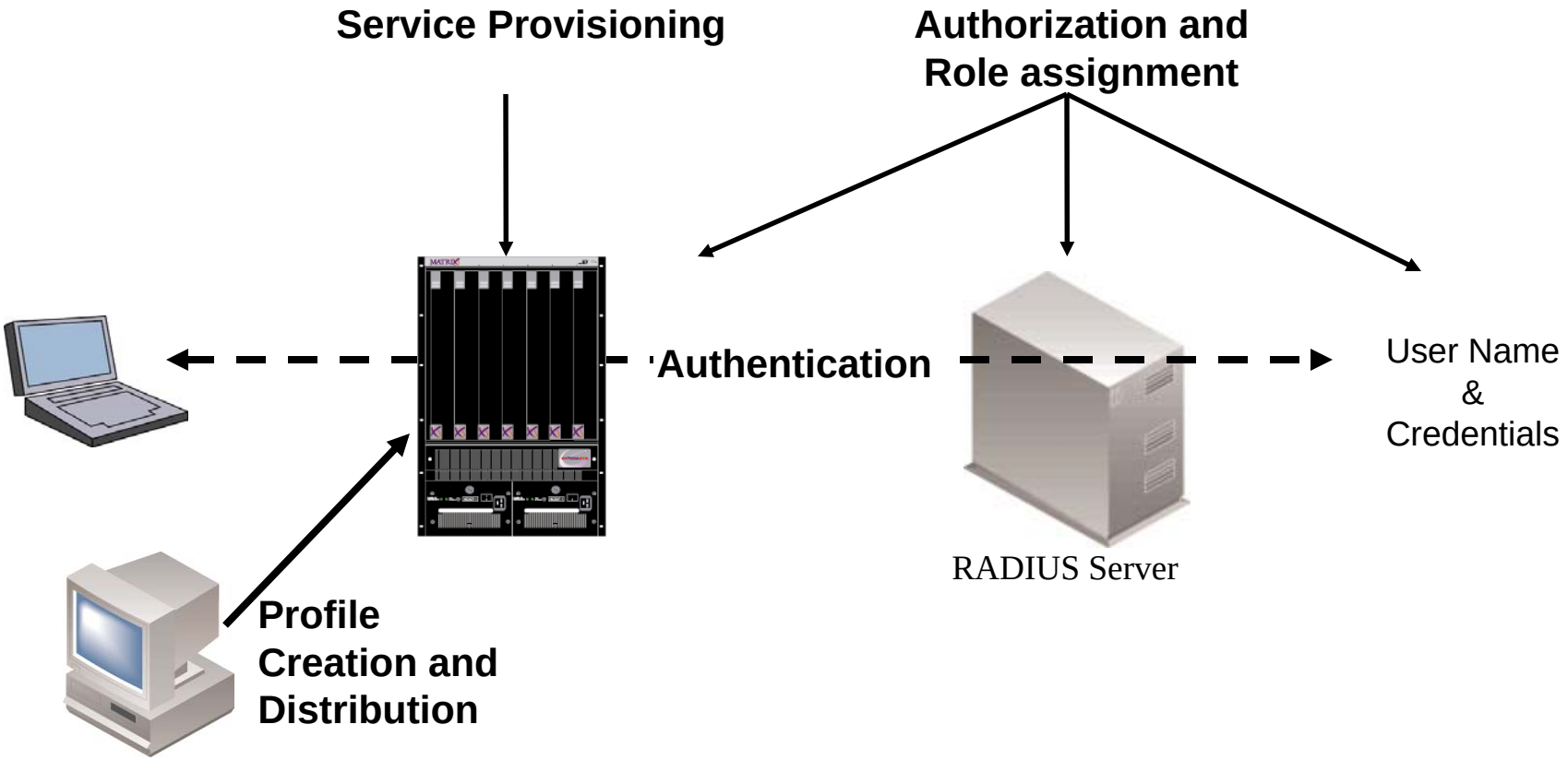
UPN allows you to manage a user's relationship to the organization through the use of Profiling and Authentication.

By configuring peoples access to services and information, a new paradigm is realized….

Person = Behavior

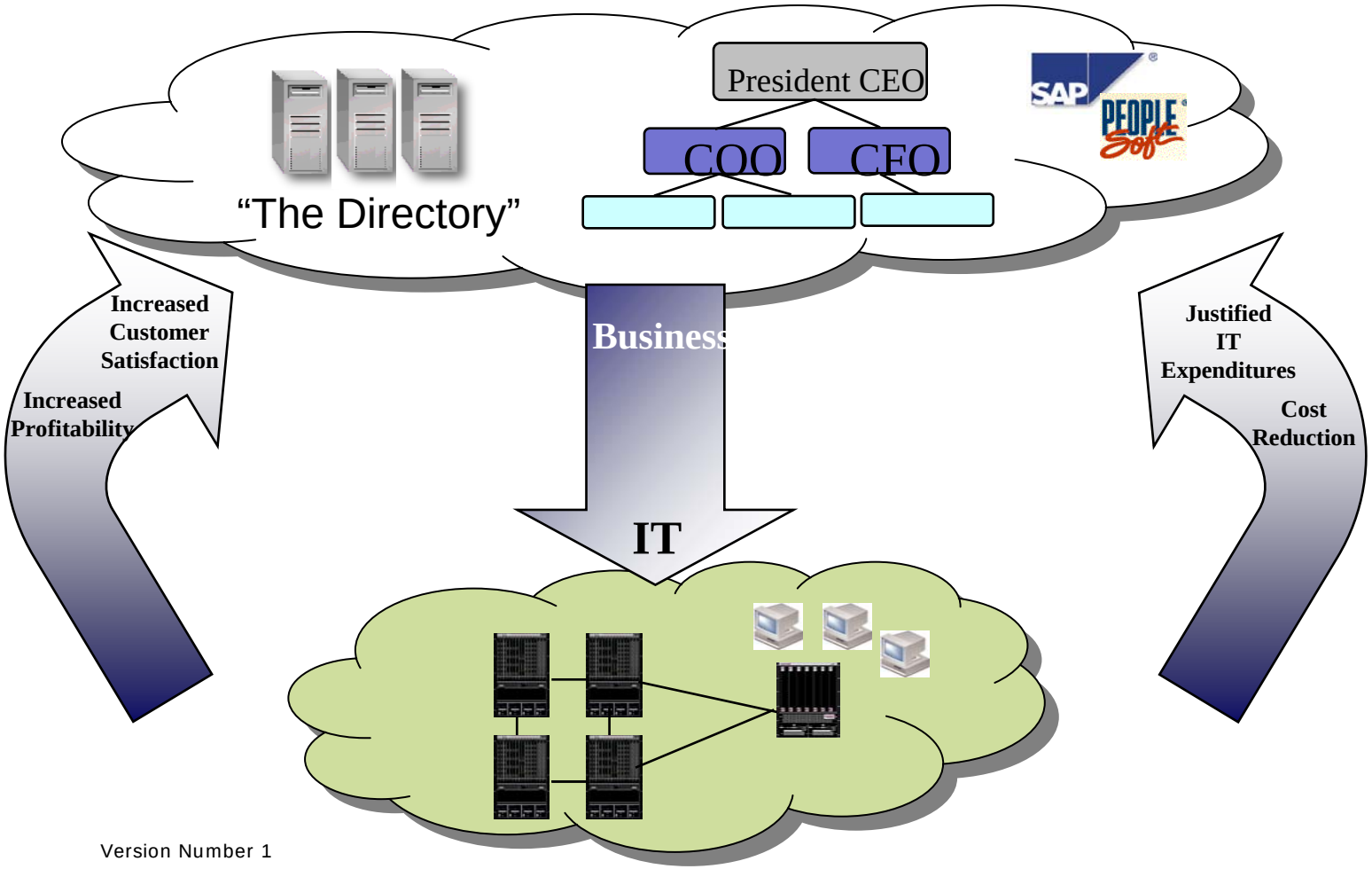


4 Stages of the User Personalized Network



The new IT/Business Model

The Business rules are enforced by the network system



Summary

Understanding the Problem Is the Only Way to a Solution…

The Problem:

•Aligning IT with the Business •Securing Mission-Critical Data

•Deploying QoS,CoS Easily and in a Meaningful Way

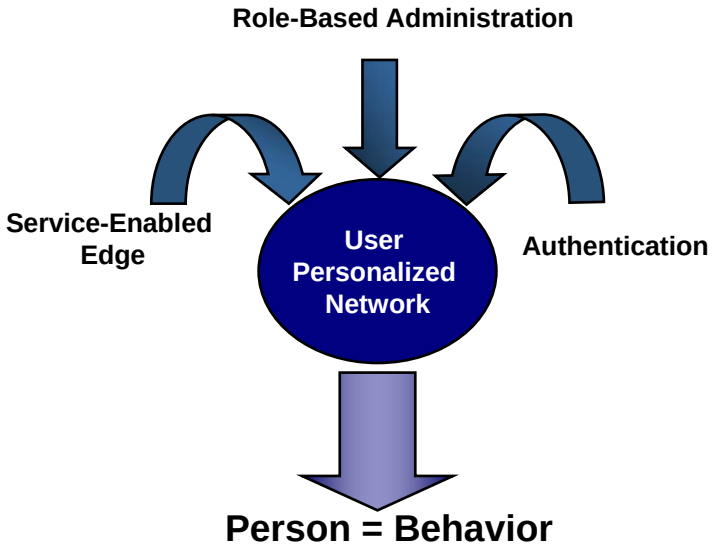
The Solution:

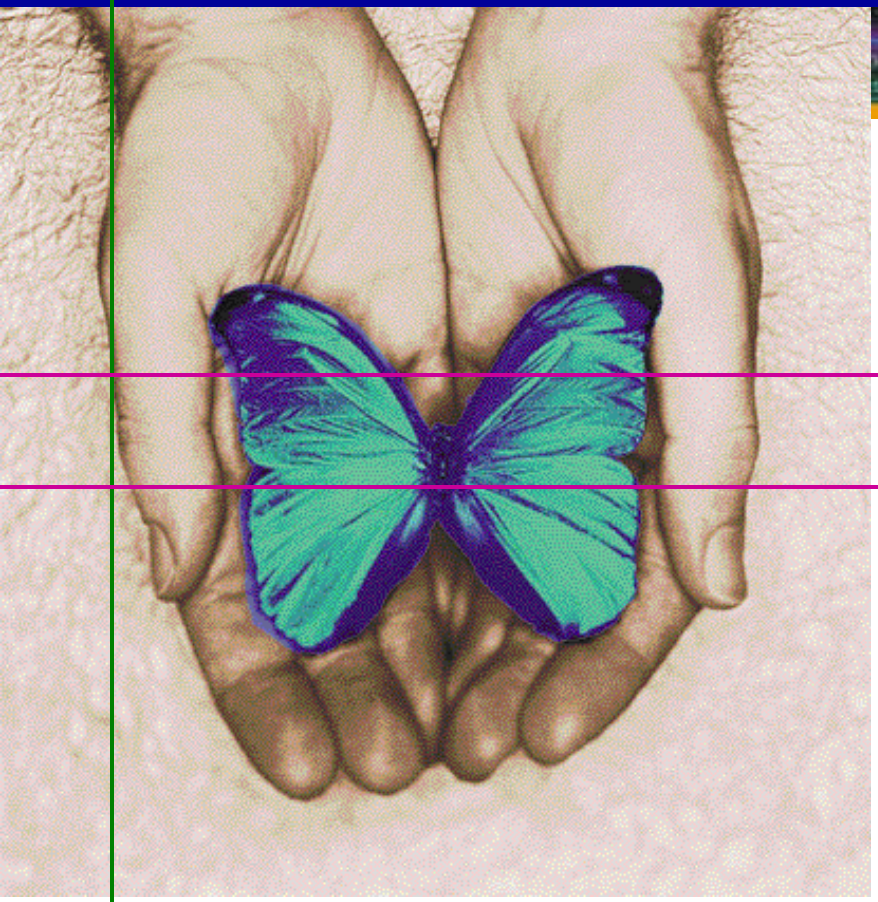
Enterasys User Personalized Network

Authentication—John Roese (Enterasys CTO) co-authored the standard

Role-Based Administration—Innovation in software to match IT rules with business roles

Service-Enabled Edge—Years of experience in architecting advanced features in our products.





Realize your vision

Thank You

Visit us at:

www.enterasys.com

ENTERASYS NETWORKS™