JUST-US®
Joint Users of Siemens Technologies
United States

VoIP Security

JUST-US May 2003

Kelly Kanellakis
Director of Technology
Office of the CTO

kellyk@enterasys.com

www.just-us.org

ENTERASYS NETWORKS™

JUST-US 2003
Annual Conference

Explore
Discover
Connect

May 18-21, 2003
The Westin Diplomat Resort & Spa
Fort Lauderdale (Hollywood), Florida

Please be considerate of others and silence cell phones and pagers.

Thank you!

JUST-US®
Joint Users of Siemens Technologies
United States

ENTERASYS NETWORKS™

www.just-us.org

Introduction and Agenda

- Introduction
- What you want to get from this presentation?

Agenda

- VoIP Basics (very basic)
- VoIP Concerns
- Security Threats
- Addressing the Threats
- VoIP Security “Best Practices”
- Summary

JUST-US®
Joint Users of Siemens Technologies
United States

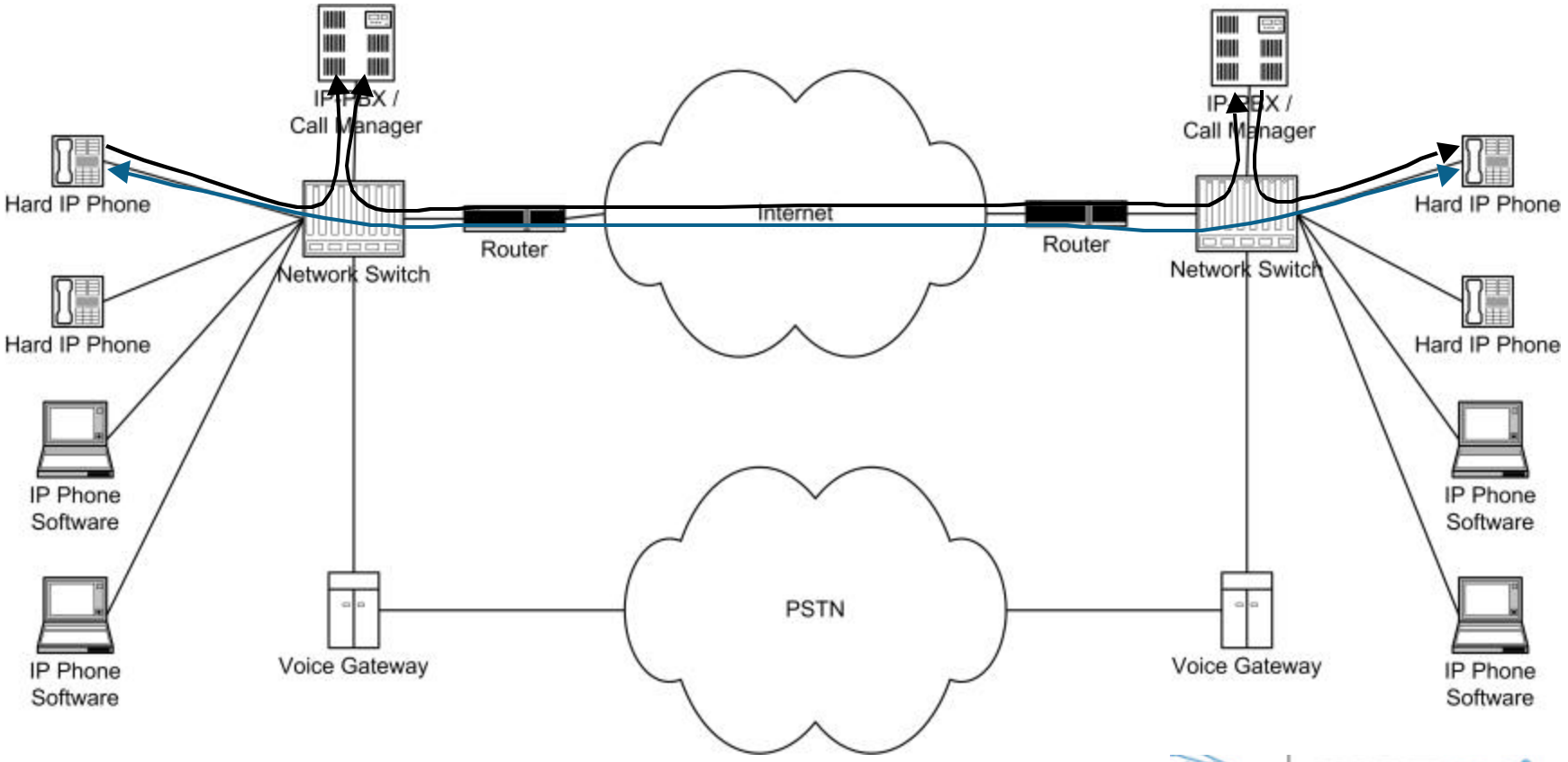
VoIP Telephony Basics

- VoIP (Voice over Internet Protocol):

  Changing a voice conversation to a stream of IP data and carrying it over the existing data infrastructure

- A number of devices involved in the conversation
- Different devices responsible for different parts of the “connection”
- Ecosystem consists of:
  - Phones (Hard or Soft)
  - Call Manager / IP-PBX OR hybrid PABX/PBX
  - Voice Gateway

VoIP Telephony Basics



JUST-US®
Joint Users of Siemens Technologies
United States

VoIP Telephony Basics

- IP Software Phone
  - A software application for a computer that acts as a telephone set, converting voice to packets
- Hardware IP Phone
  - Conventional form telephone. Actually a special purpose computer that converts voice to packets
- IP-PBX
  - Traditional PBX role – except acts as a call connector only. Once calls are connected only tracts state
- Hybrid PABX
  - Traditional PBX with VoIP capabilities added
- Voice Gateway
  - Allows connection from VoIP world to PSTN world or vice versa

VoIP Concerns

- Many concerns come up around VoIP
- More people concerned with
  - Cost justification
  - Functionality
  - Reliability
- Security is not generally one of them
- All of these are signs of a young technology
- As VoIP matures security will become a larger concern

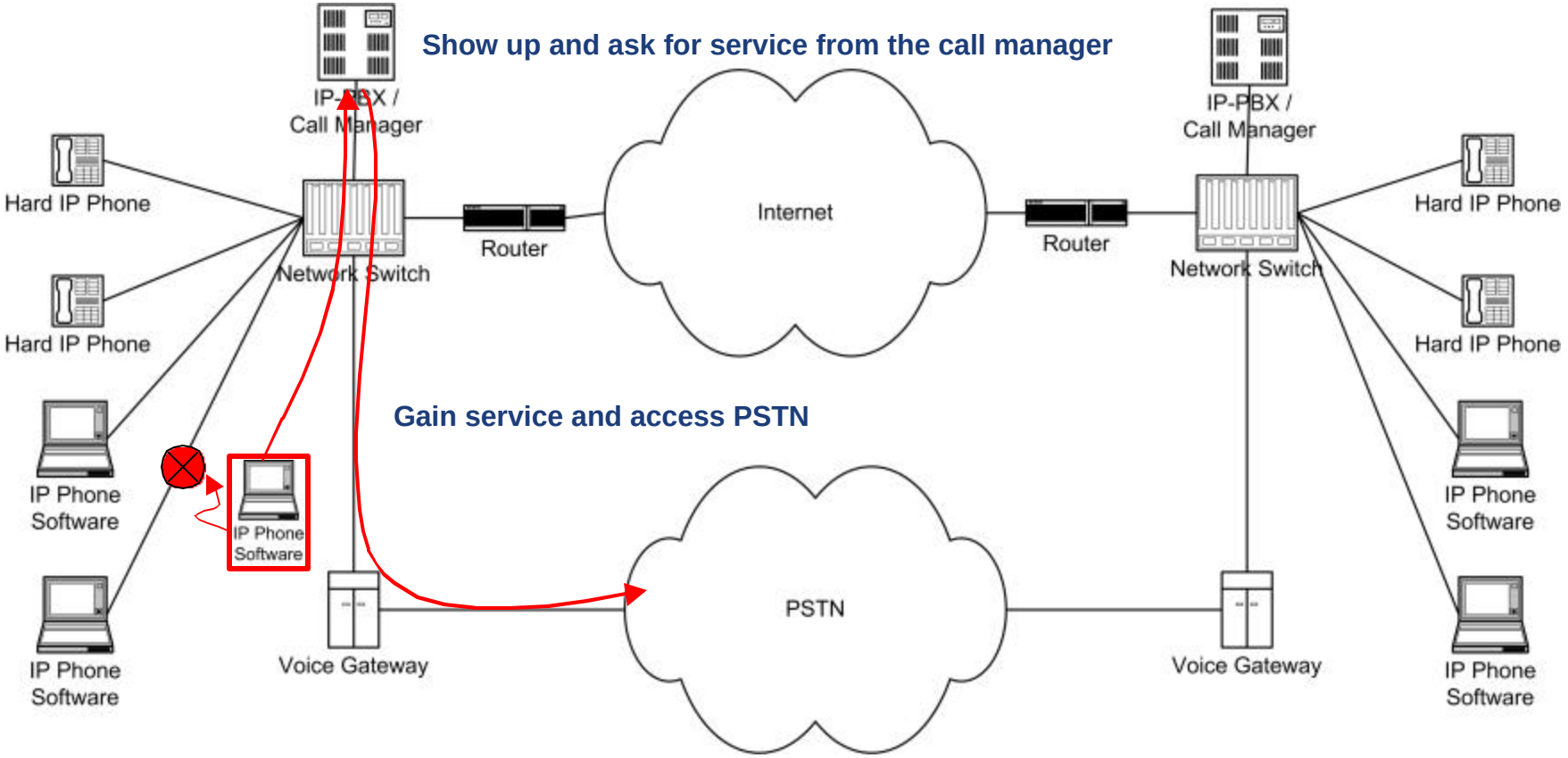
VoIP Security Threats

- These threats apply to ANY data stream
- Voice is interesting because it is considered more private
- Threat types:
  - Gain Services
  - Disrupt Services
  - Intercept Services

- Most security threats fall into these categories, but there are always new threats
- Voice is particularly susceptible to some security threats more than others

VoIP Security Threats – Gaining Service

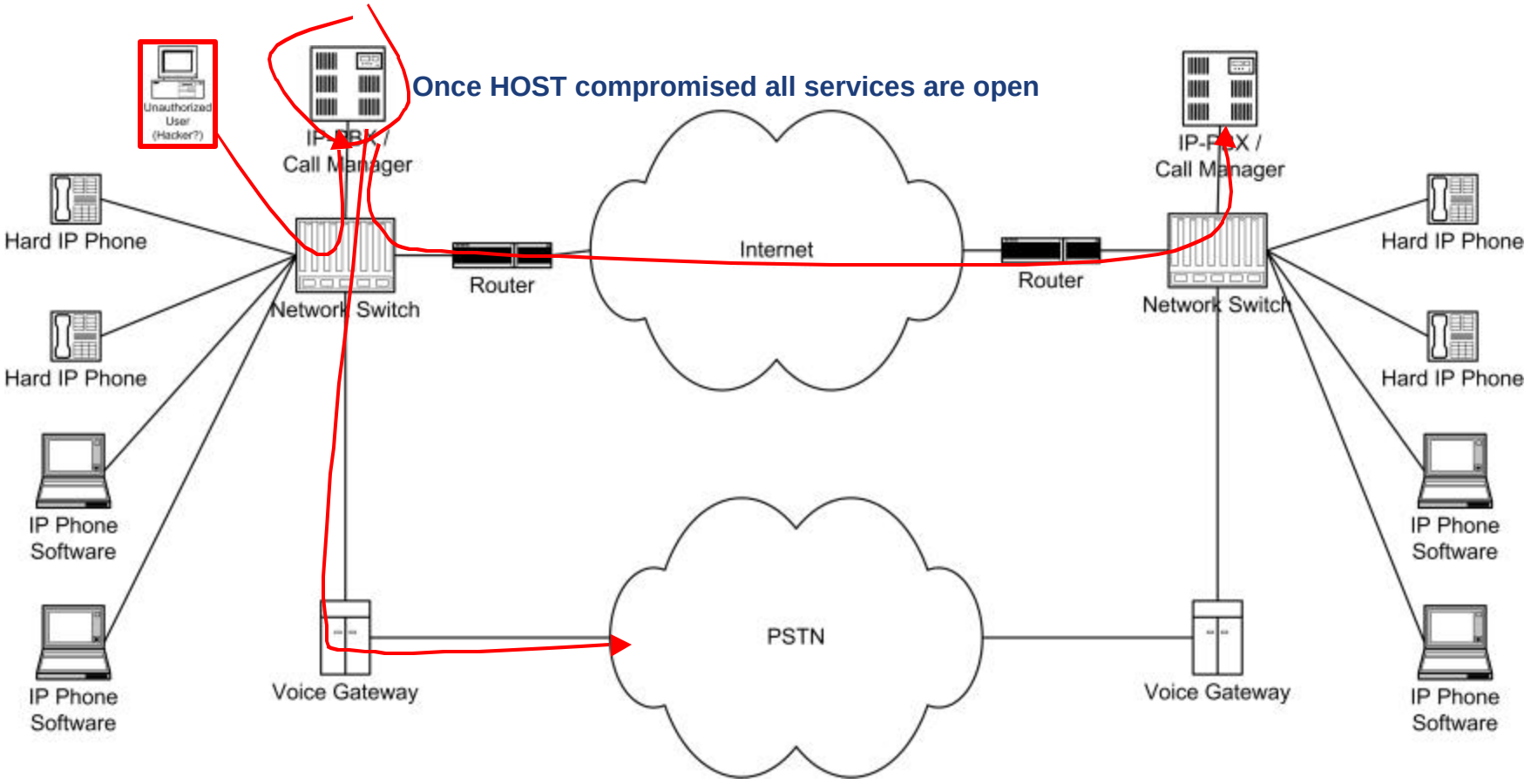
Unauthorized user appearing on the network



JUST-US®
Joint Users of Siemens Technologies
United States

VoIP Security Threats – Gaining Service

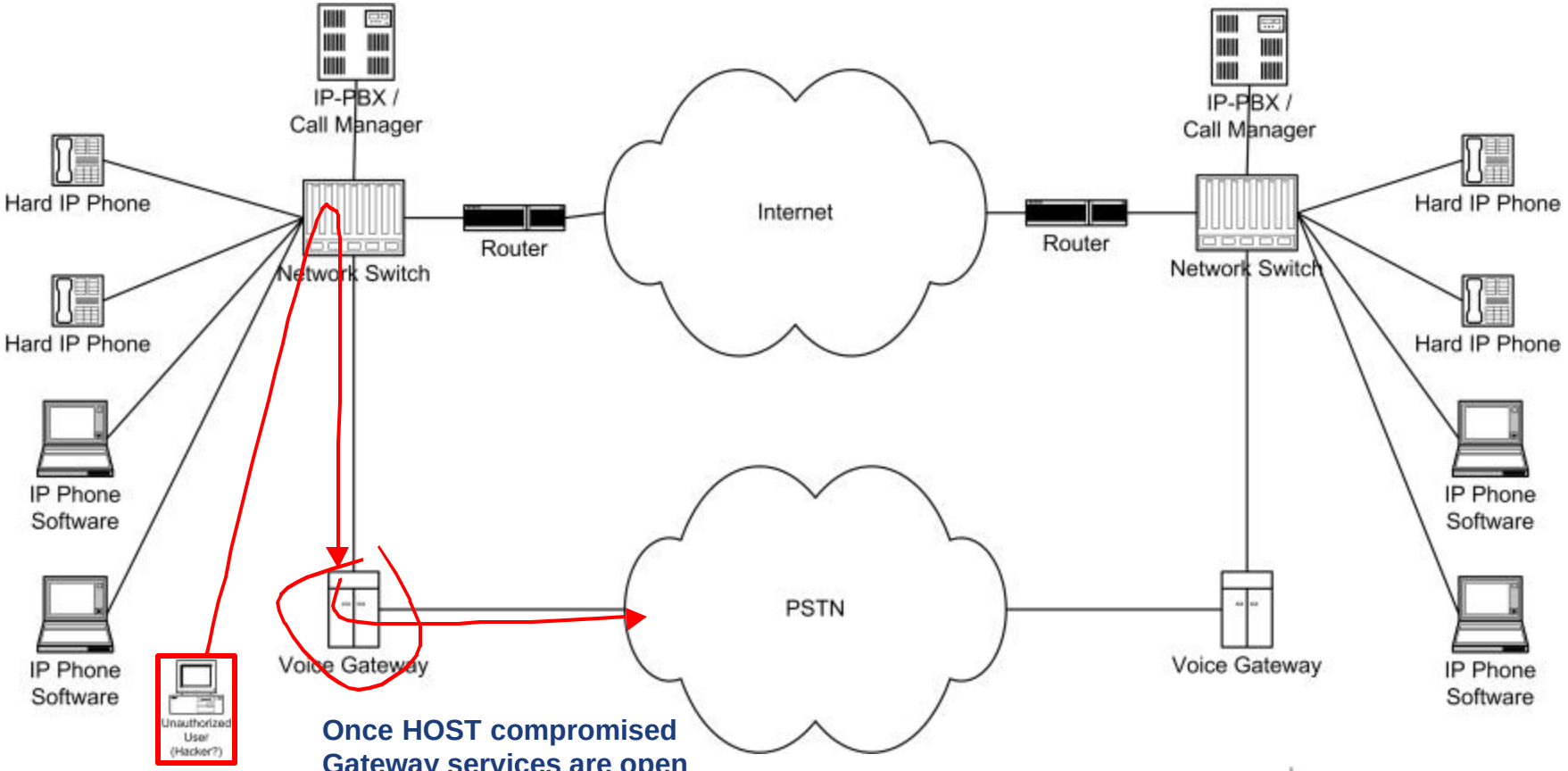
Attack underlying HOST of IP-PBX



JUST-US®
Joint Users of Siemens Technologies
United States

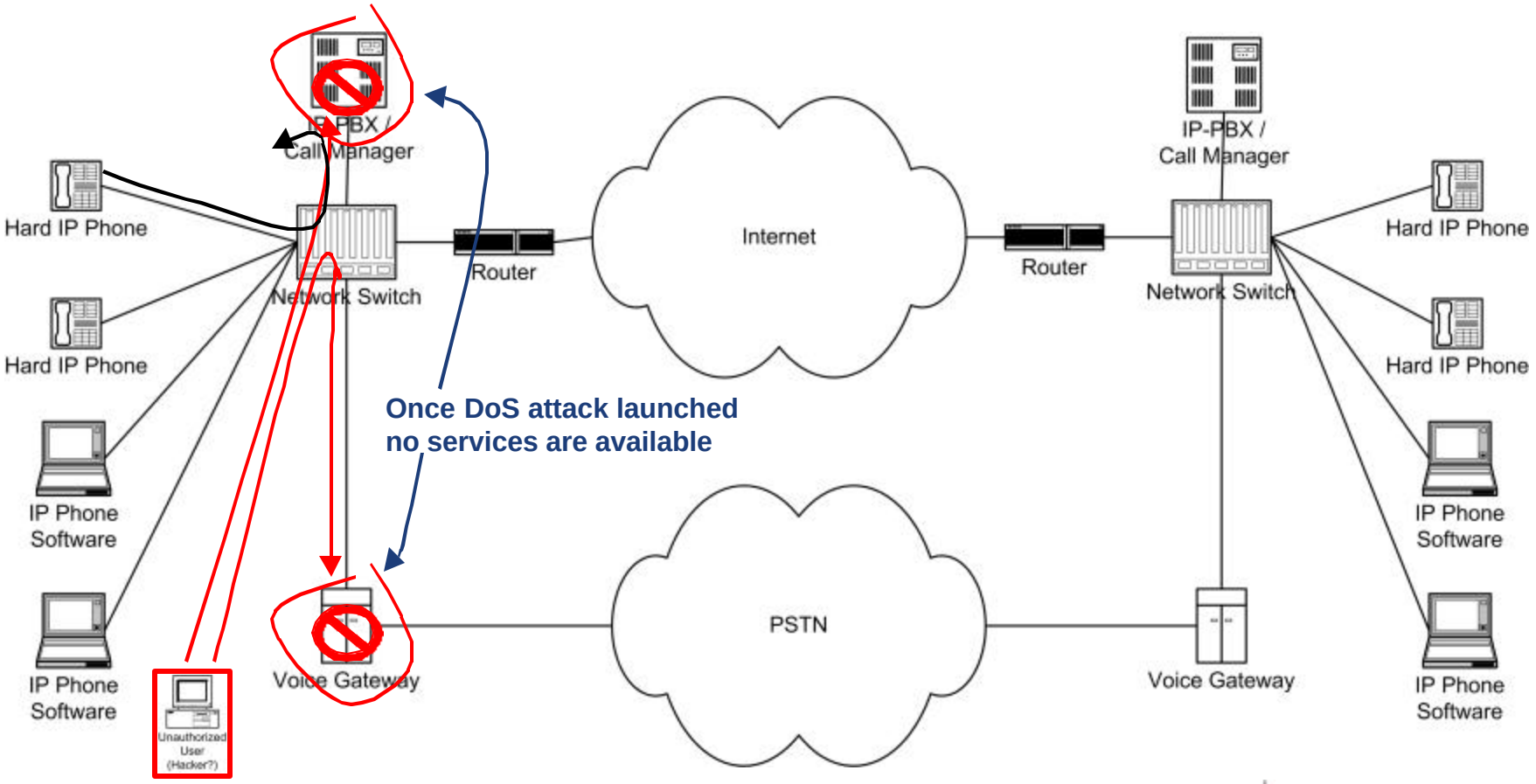
VoIP Security Threats – Gaining Service

Attack underlying HOST of Voice Gateway



VoIP Security Threats – Denying Service

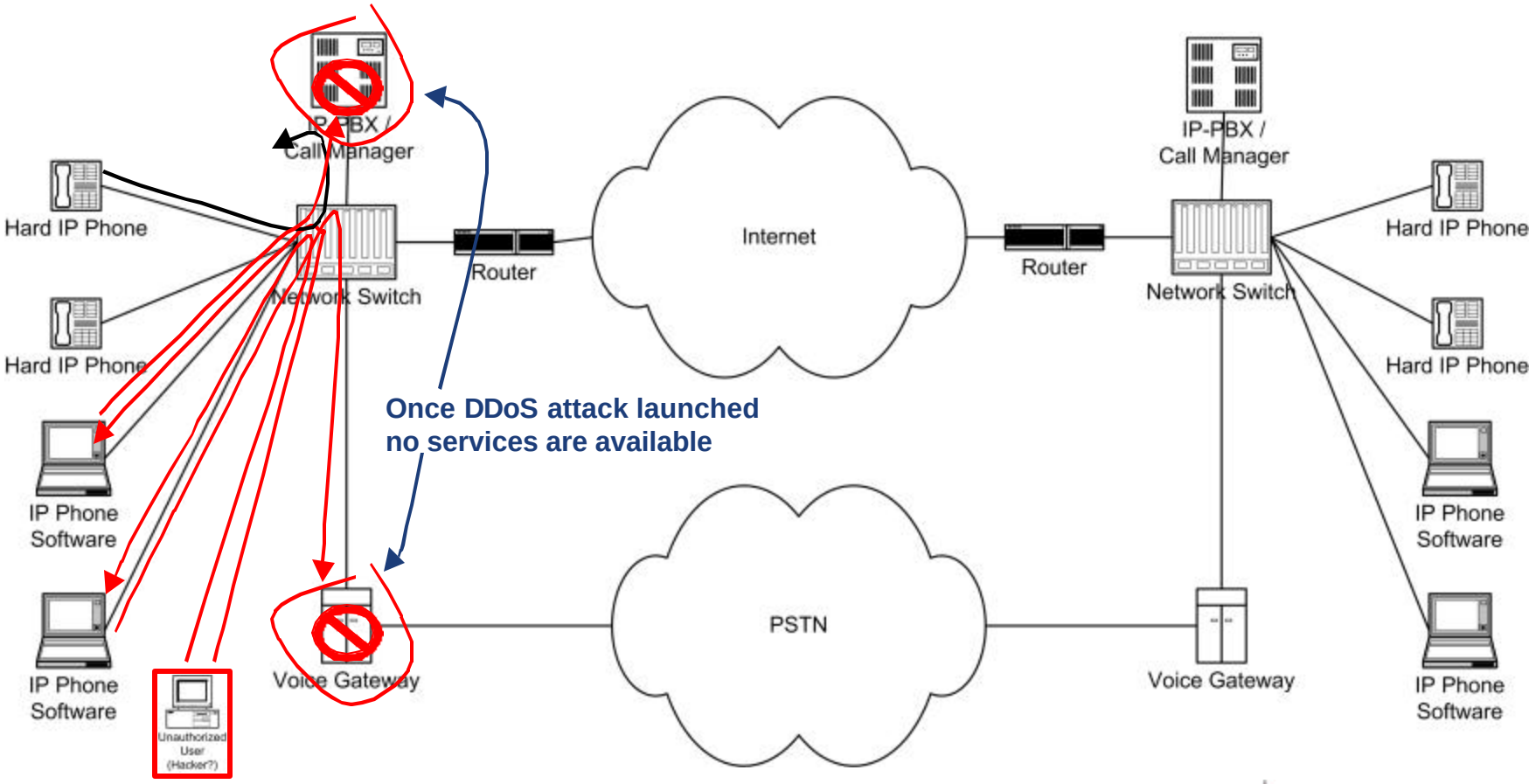
Attack key devices providing Voice Services – DoS / DDoS



JUST-US®
Joint Users of Siemens Technologies
United States

VoIP Security Threats – Denying Service

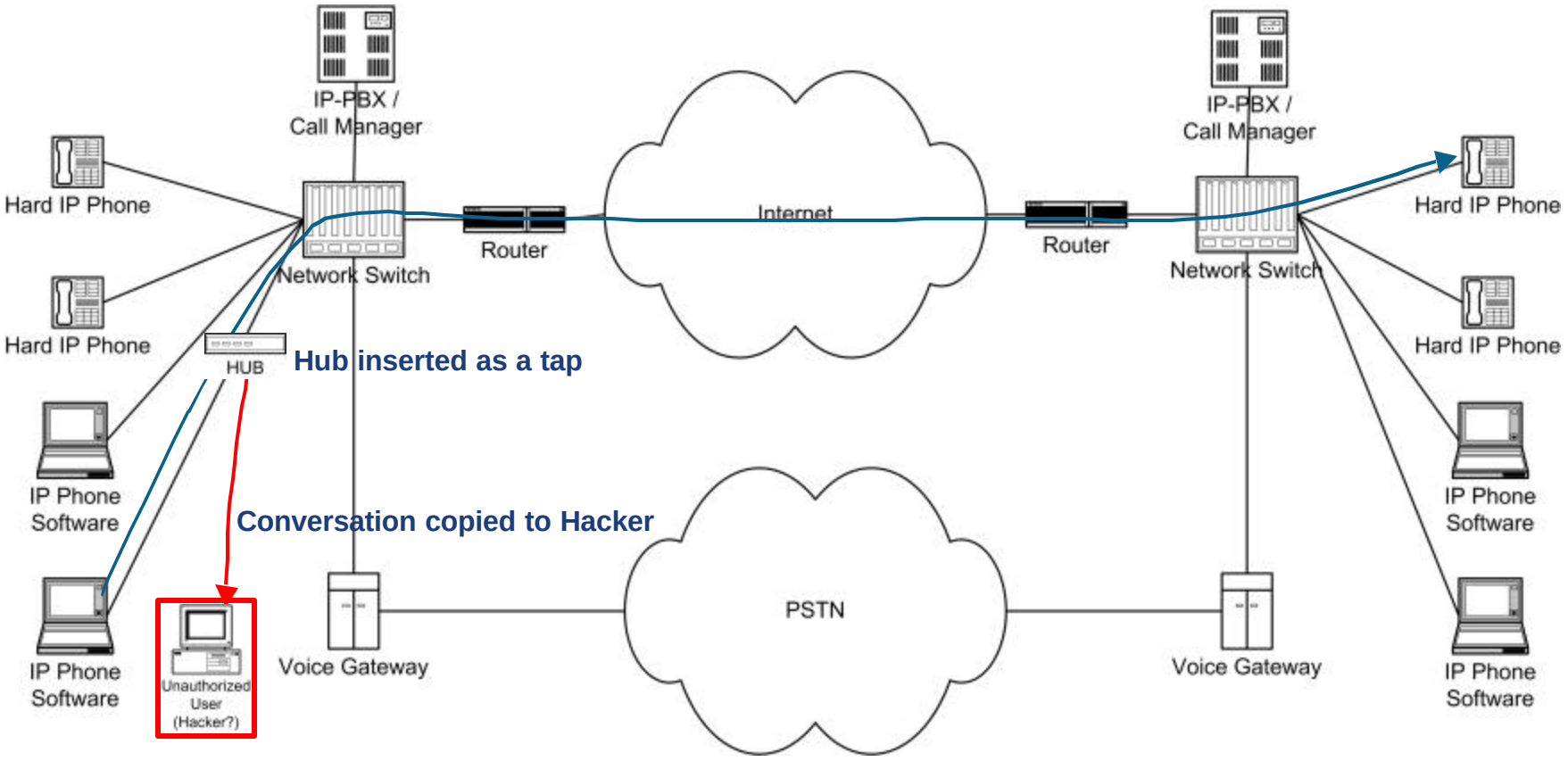
Compromise general devices and have them attack – DoS / DDoS



JUST-US®
Joint Users of Siemens Technologies
United States

VoIP Security Threats – Intercepting Service

Tap conversations by intercepting data



JUST-US®
Joint Users of Siemens Technologies
United States

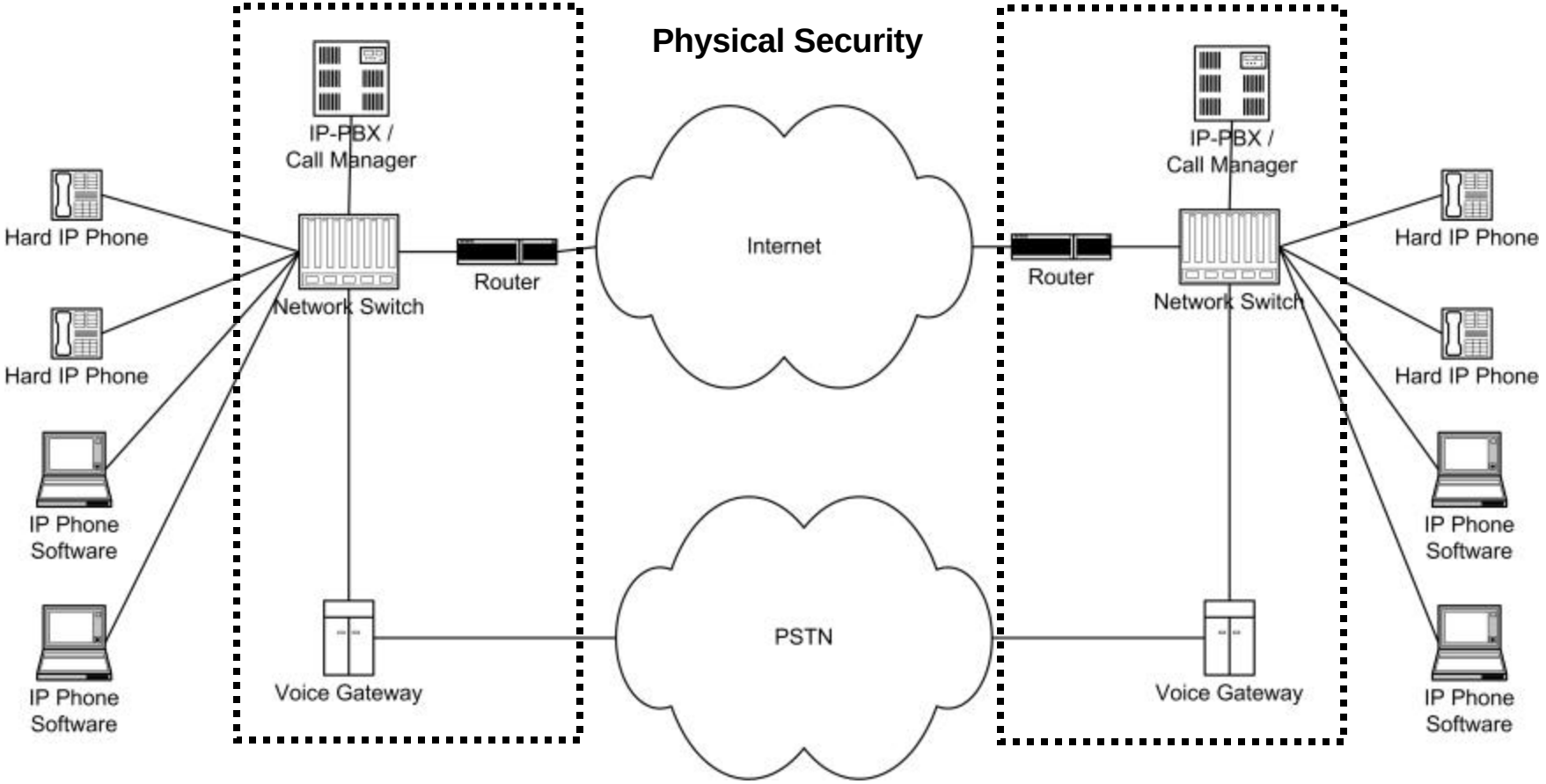
VoIP Security – Combating the Threats

- While the threats can be very serious they can also be minimized
- Standard security practices MUST apply to VoIP
- Each component and type of threat must be examined
- Security staff should be involved in deployment
- Each threat type requires different responses

JUST-US®
Joint Users of Siemens Technologies
United States

VoIP Security – Combating the threats

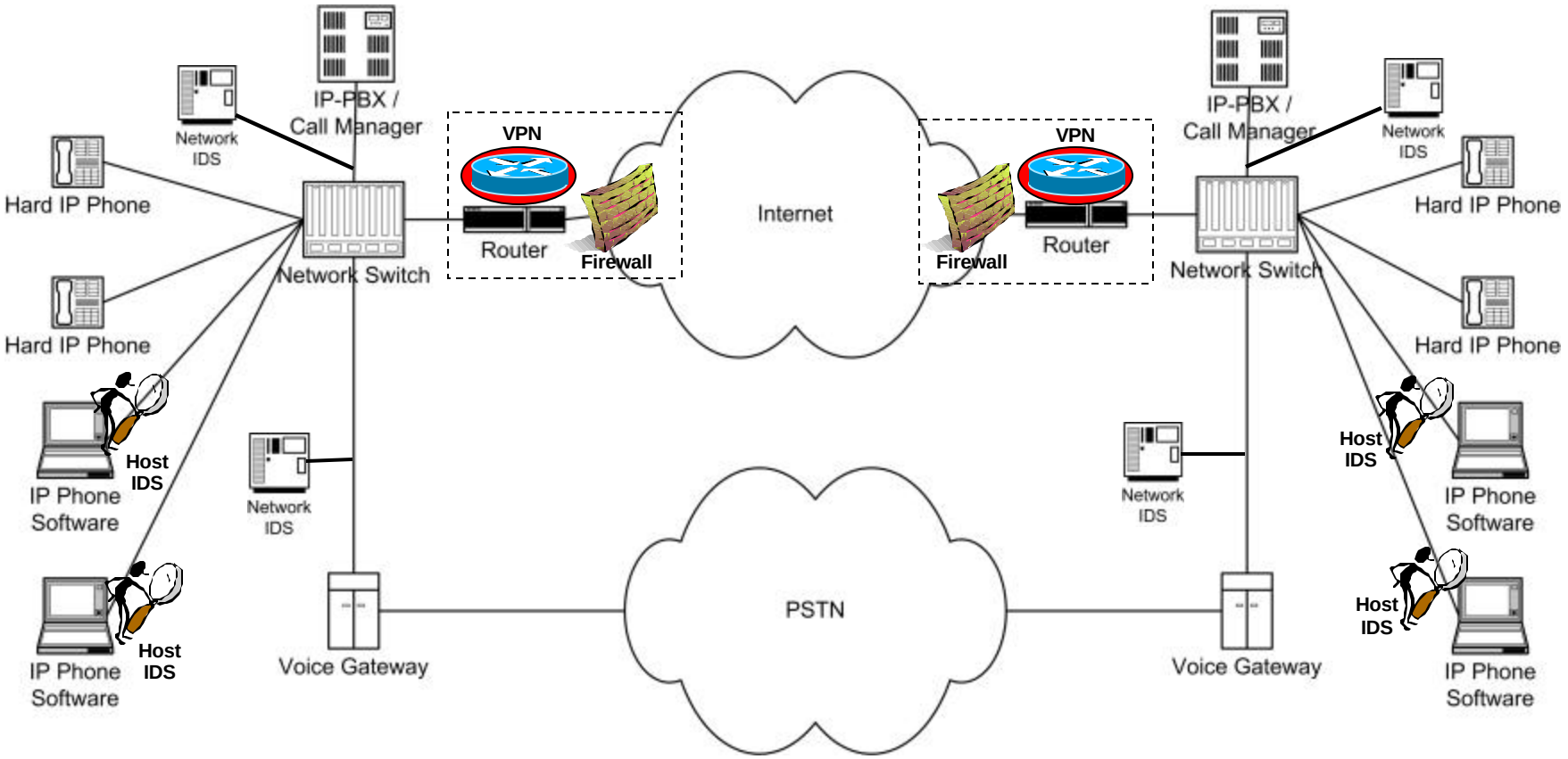
Standard Enterprise Security Practices



JUST-US®
Joint Users of Siemens Technologies
United States

VoIP Security – Combating the threats

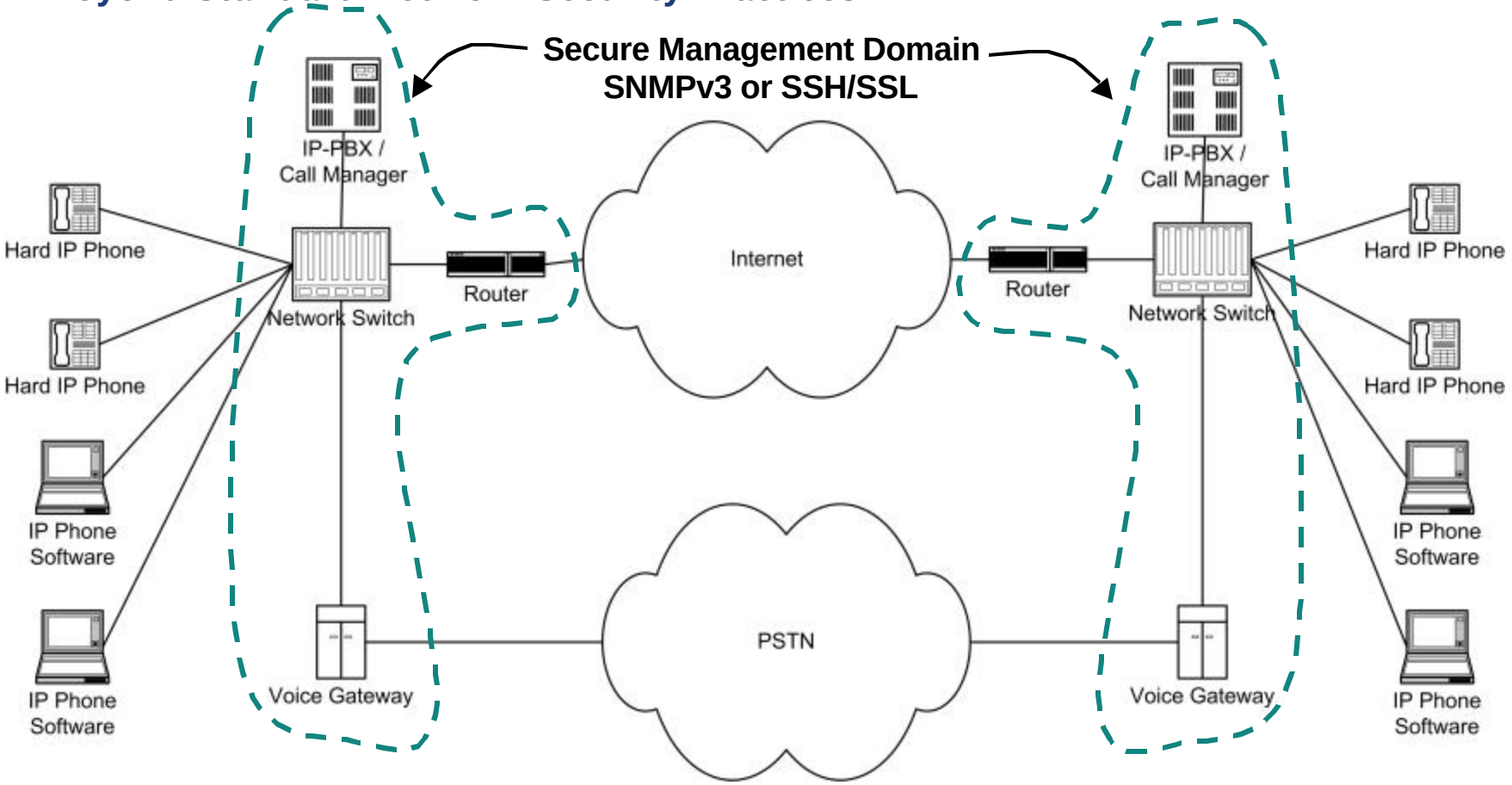
Standard Network Security Practices



JUST-US®
Joint Users of Siemens Technologies
United States

VoIP Security – Combating the threats

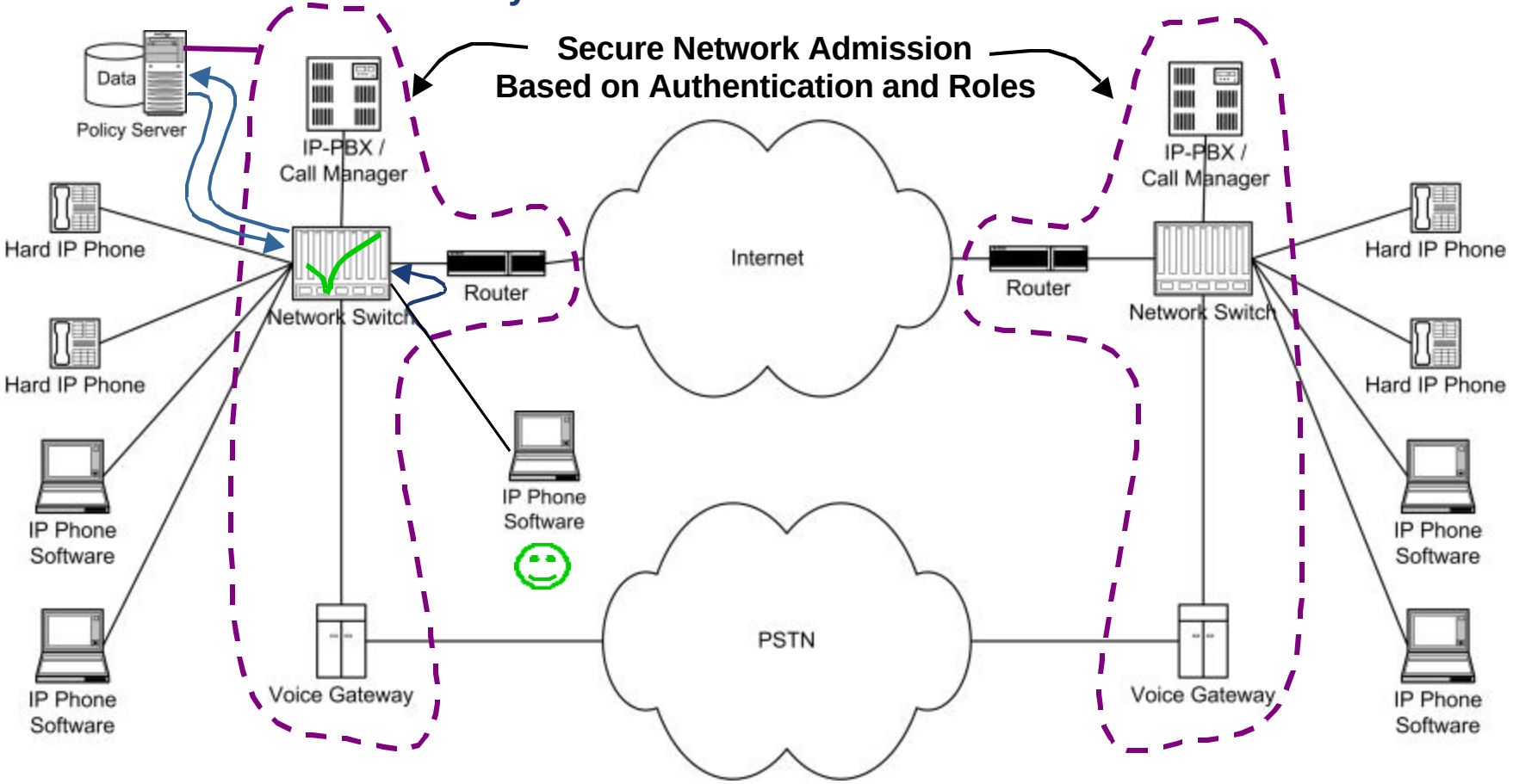
Beyond Standard Network Security Practices



JUST-US®
Joint Users of Siemens Technologies
United States

VoIP Security – Combating the threats

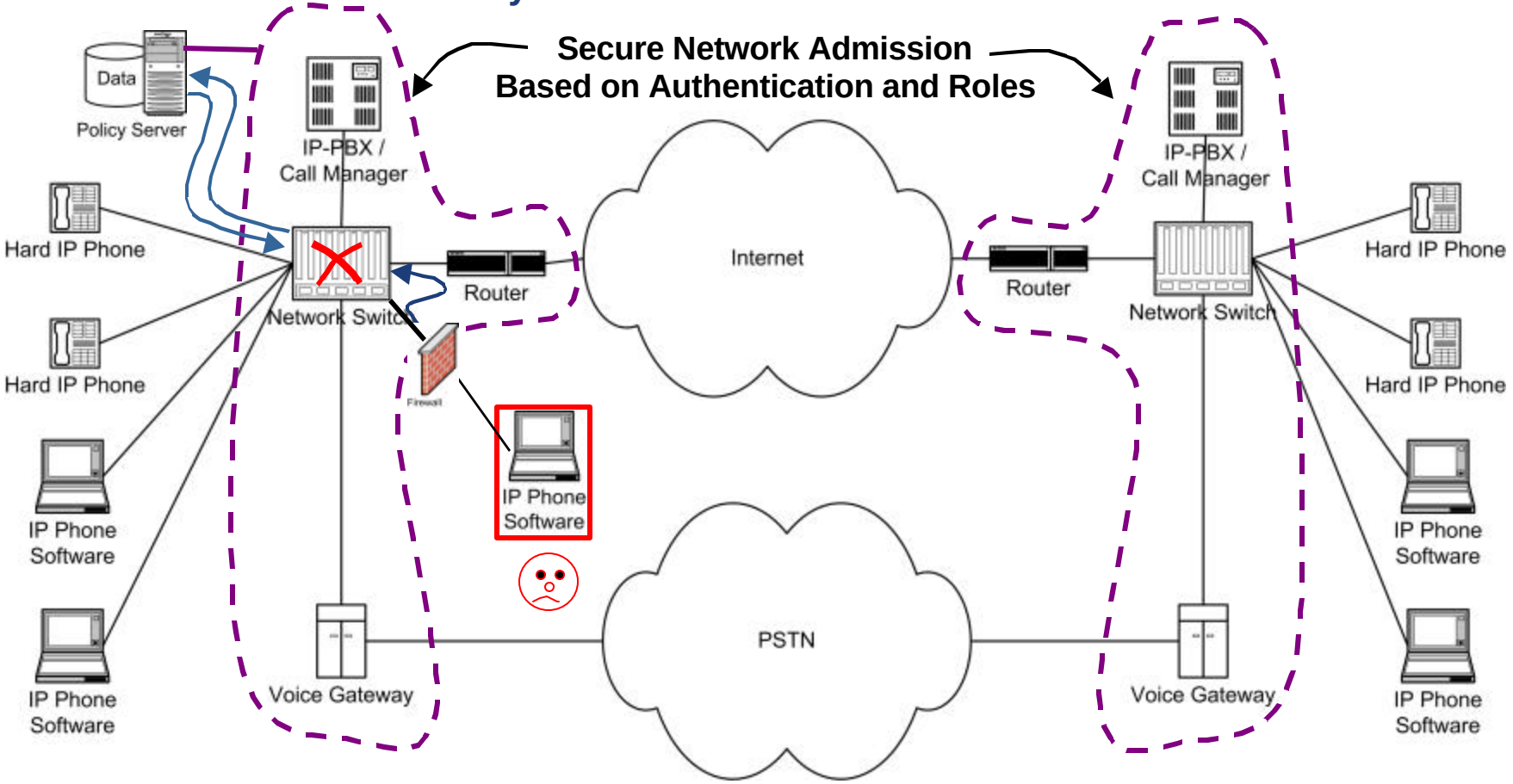
Ultimate Network Security Practices



JUST-US®
Joint Users of Siemens Technologies
United States

VoIP Security – Combating the threats

Ultimate Network Security Practices



JUST-US®
Joint Users of Siemens Technologies
United States

VoIP Security – The Options

Traditional VLANs versus User Personalized Networks

VLANS

- Group based security
- Authentication based on port
- Access control handled by core devices – performance hit
- QoS assigned based on VLAN

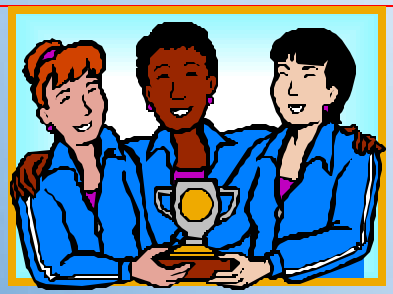
UPN

- User Based Security
- Authentication based on credentials (user identity)
- Access control handled at the edge – performance unaffected
- QoS assigned based on user

JUST-US®
Joint Users of Siemens Technologies
United States

JUST-US®
Joint Users of Siemens Technologies
United States

Enterasys Best Practices



ENTERASYS NETWORKS™

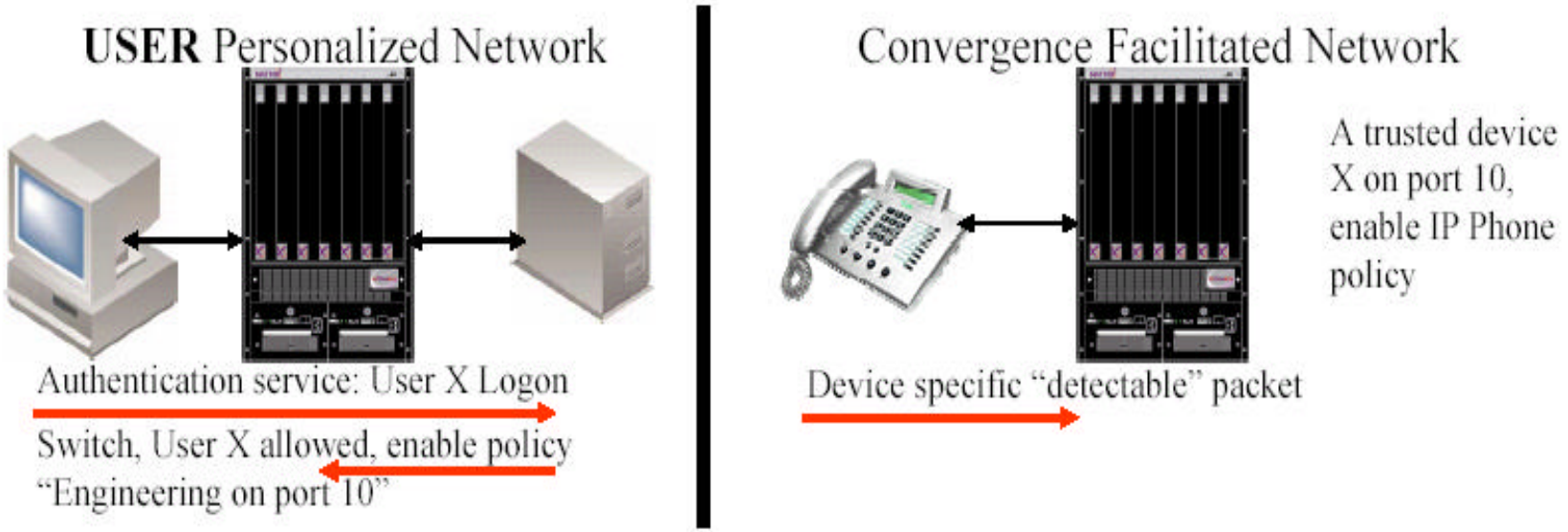
VoIP Security – Best Practices

- Deployment should always secure the physical access first
- Standard data network security practice should be followed
  - Firewalls
  - VPNs
  - Intrusion detection systems (network and host)
  - Secure management of devices

JUST-US®
Joint Users of Siemens Technologies
United States

VoIP Security – Best Practices

Policy Profiles



VoIP Security – Best Practices

- Beyond standard practices – policy based security is the ultimate control
- In this scheme access is controlled at first ingress
- Users and devices are authenticated at connection
- Quality and access is controlled BEFORE network is entered
- Policy applied to individuals and individual devices NOT to groups based on port location
- Policy follows user and “device” regardless of location

JUST-US®
Joint Users of Siemens Technologies
United States

VoIP Security – Best Practices

- Security policy authenticates at edge
- Policy should applies to wired and wireless
- Policy should integrate with organization's existing policies (and back-end databases)
- Policy should be a "one" click system – otherwise it does NOT get used

JUST-US®
Joint Users of Siemens Technologies
United States

VoIP Security – Best Practices
High Availability

Design your network to be highly available

- Highly available routers and switches
- Redundant uplinks
- VRRP, 802.1w Rapid Spanning Tree , 802.3ad Link Aggregation
- Include advanced management and monitoring capabilities
- Keep in mind only a secure network is a reliable network!

VoIP Security - Summary

- Security is important, but not considered yet because VoIP is new. This is a problem.
- Security for VoIP must consider traditional security as well as network security
- Ultimate security provided by a user and policy based approach with authentication
- Tying authentication to policy of the organization is key
- Security must be easy to use or it will not be used

Don't forget to fill out a session evaluation after this session. Your opinion matters for future content!

www.just-us.org

JUST-US®
Joint Users of Siemens Technologies
United States

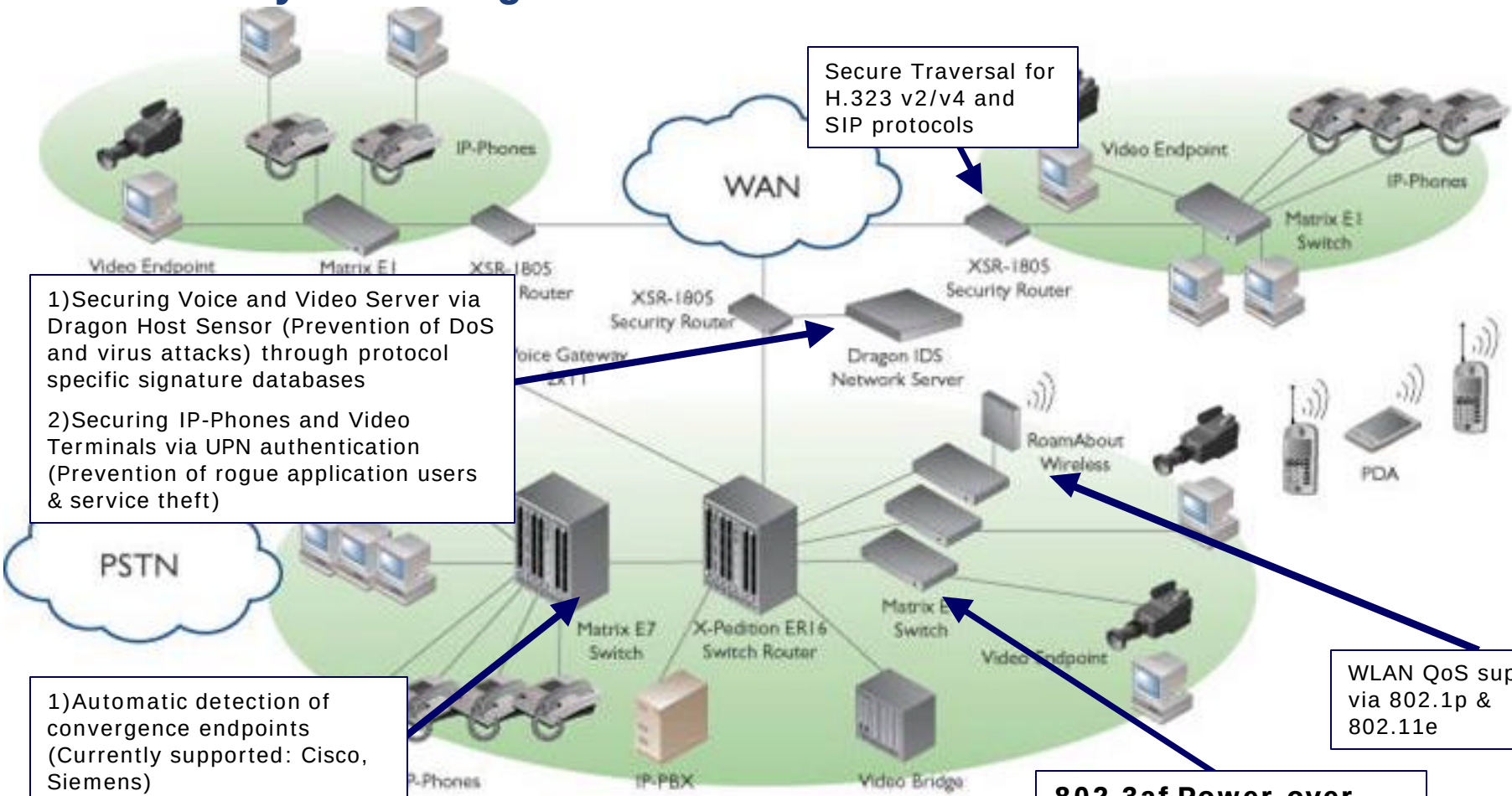

JUST-US
Joint Users of Siemens Technologies
United States
Thank You!
Any Questions?
ENTERASYS
NETWORKS

JUST-US®
Joint Users of Siemens Technologies
United States

Enterasys' Technologies Deployed

ENTERASYS NETWORKS™

Enterasys Convergence-Enablement Features & Services



Secure Traversal for H.323 v2/v4 and SIP protocols

1)Securing Voice and Video Server via Dragon Host Sensor (Prevention of DoS and virus attacks) through protocol specific signature databases

2)Securing IP-Phones and Video Terminals via UPN authentication (Prevention of rogue application users & service theft)

1)Automatic detection of convergence endpoints (Currently supported: Cisco, Siemens)

2)Automatic policy rule assignment for convergence endpoints (Prioritization, Bandwidth Management) to ensure security, QoS and management

WLAN QoS support via 802.1p & 802.11e

802.3af Power-over-Ethernet

Providing 802.3af capabilities in edge switches to increase the reliability of IP phones and remote cameras