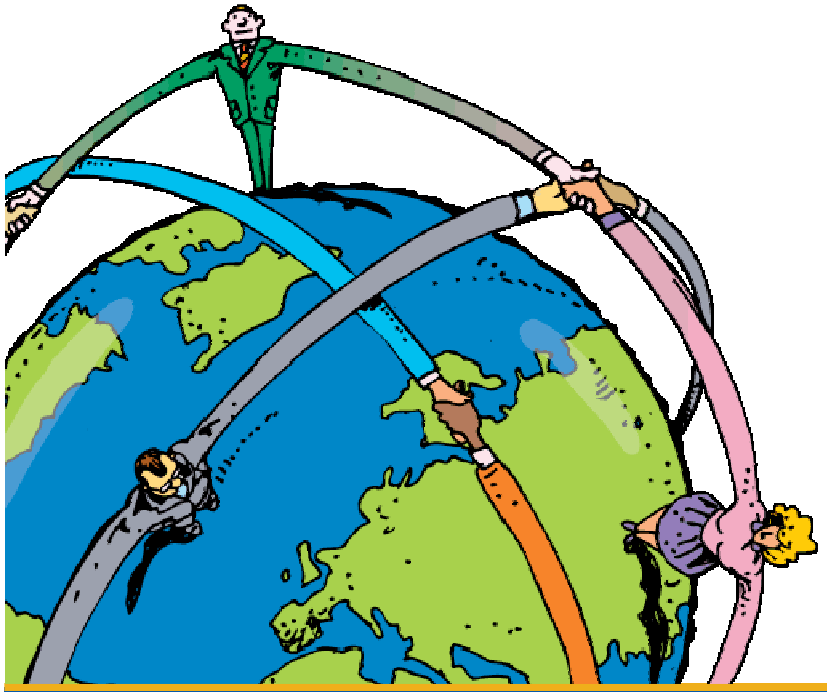


Juniper Networks

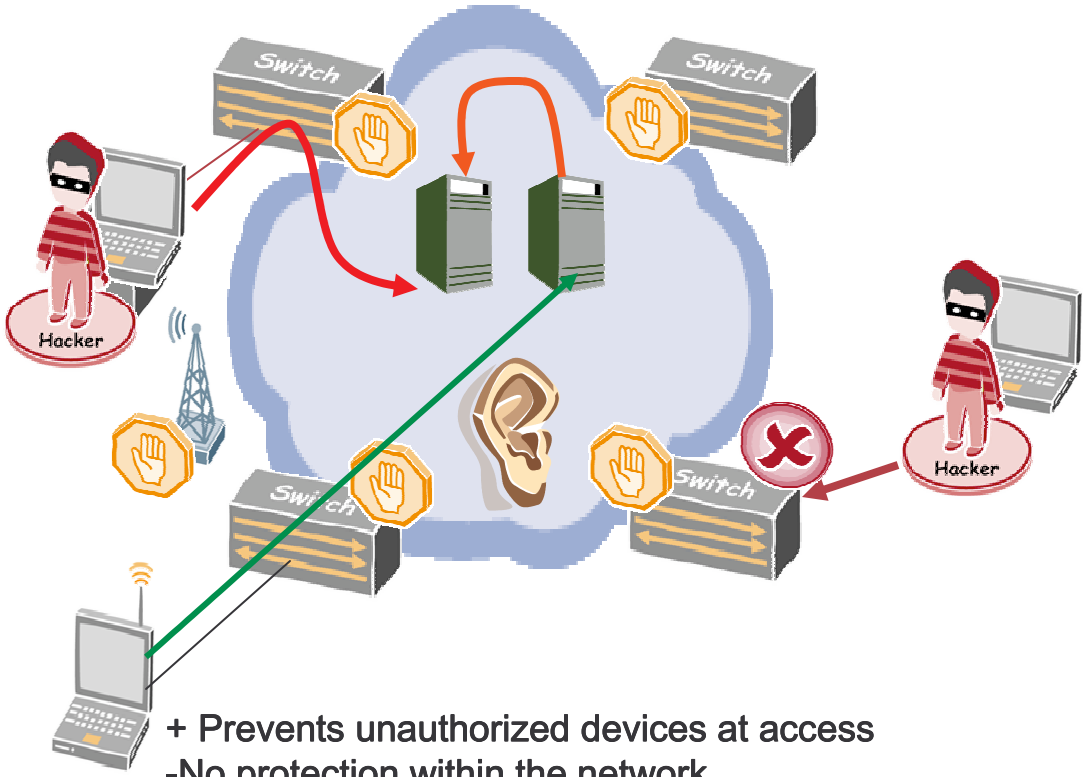
Unified Access Control (UAC)

Agenda

- **NAC : Layer-2 vs Layer-3 enforcement**
- **Juniper UAC**
  - Network Protection
  - Application and User Visibility
  - Coordinated Threat Control
- **Standards & why they matter**

Access Control - L2 vs L3 enforcement

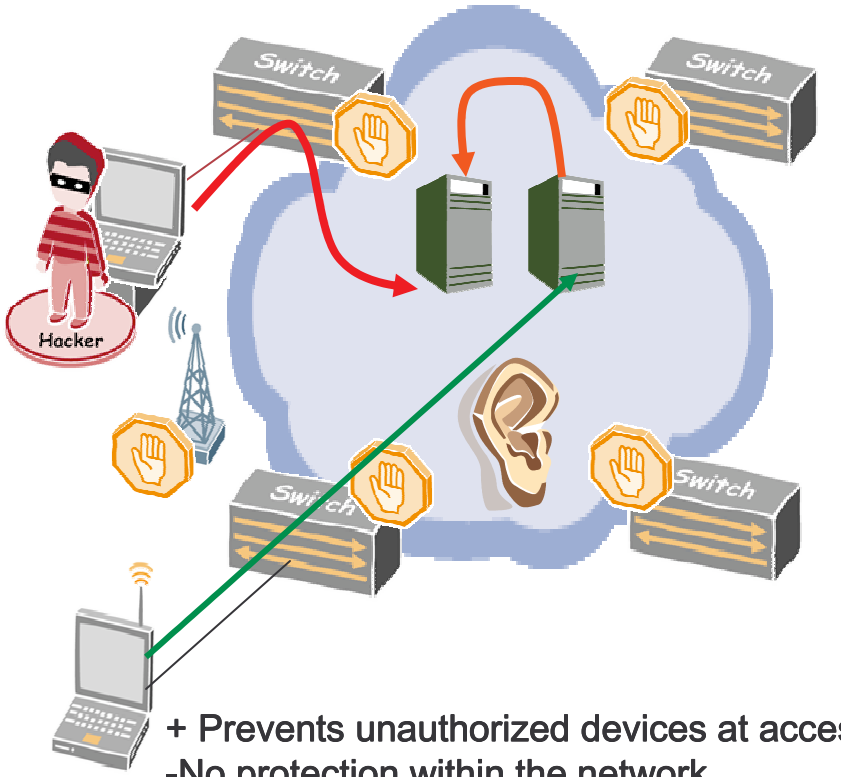
L2 = Protection around the network



+ Prevents unauthorized devices at access
-No protection within the network
-All connected devices does not have a user..

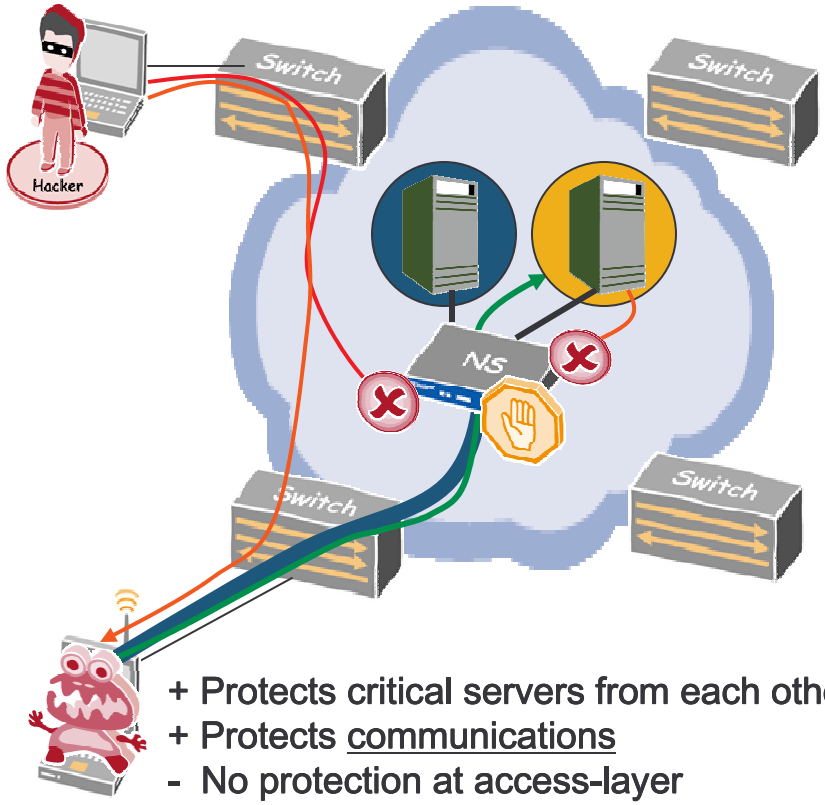
Access Control - L2 vs L3 enforcement

L2 = Protection around the network



+ Prevents unauthorized devices at access
-No protection within the network
-All connected devices does not have a user..

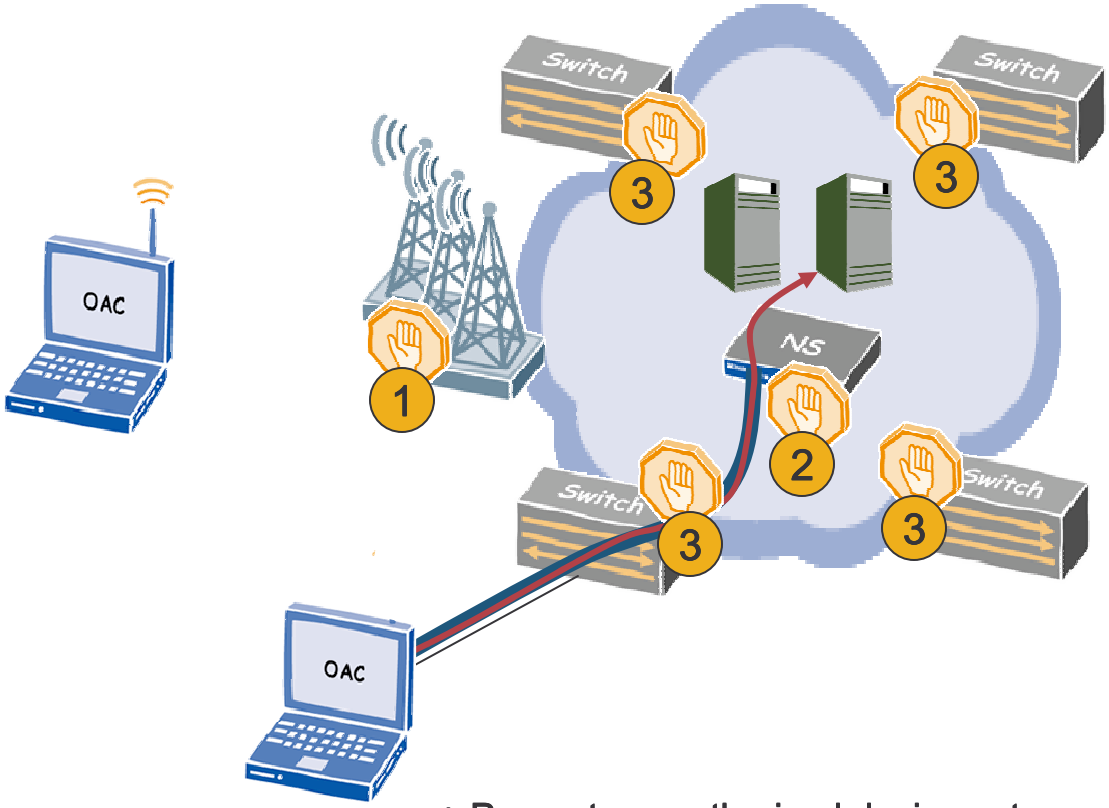
L3 = Protection within the network



+ Protects critical servers from each other
+ Protects communications
- No protection at access-layer

Juniper UAC = L2 and L3 enforcement

L2 + L3 = Protection around and within the network



+ Prevents unauthorized devices at access
+ Protects critical servers and communications

Juniper UAC enables a phased implementaion !!!

Example:

Phase-1
Protect the Wireless Network

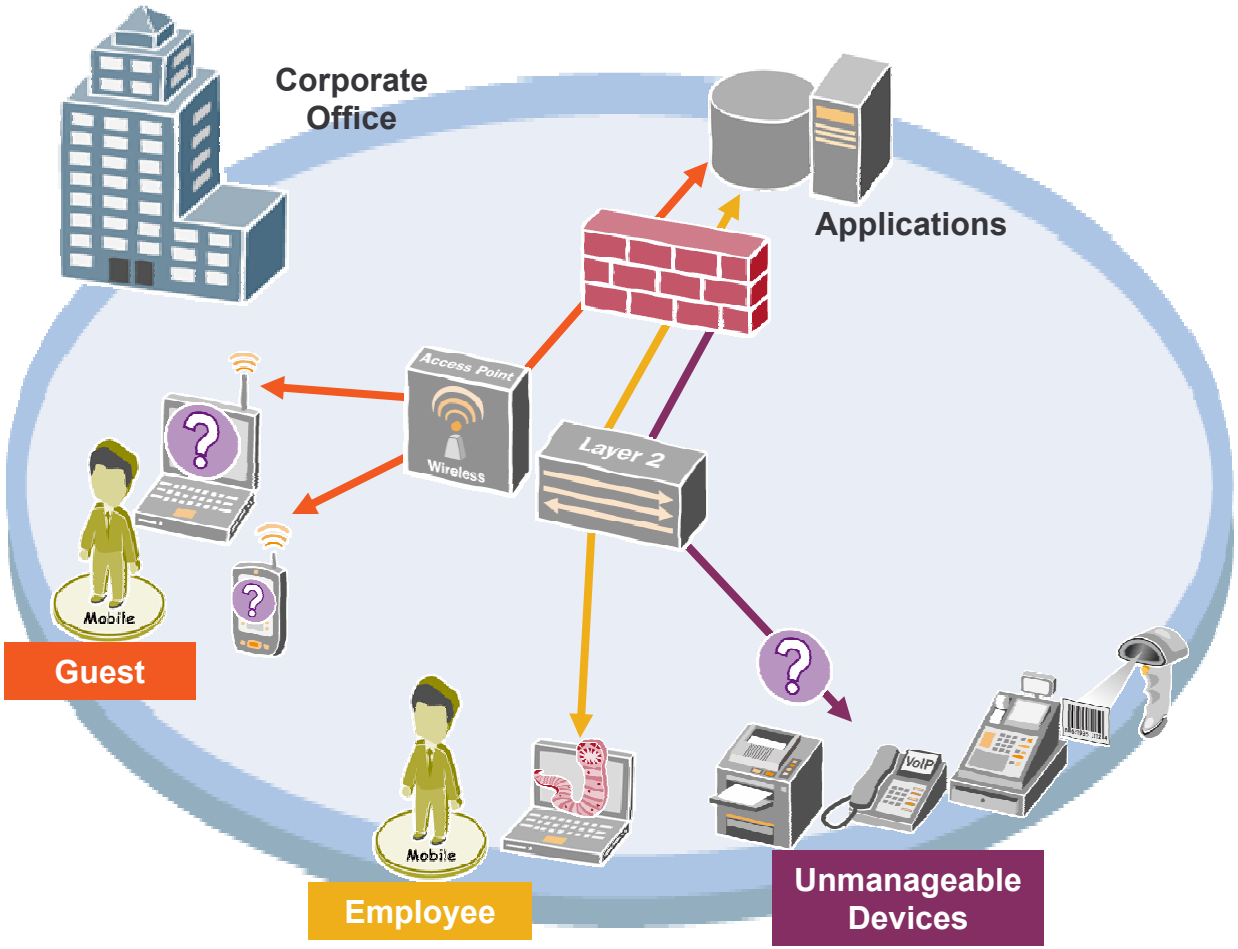
Phase-2
Limit access to, and protect communication to the most critial servers

Phase-3
Start rolling out access control to all switches in the company.

Agenda

- NAC : Layer-2 vs Layer-3 enforcement
- **Juniper UAC**
  - Protection
  - Visibility
  - Threat Control
- Standards & why they matter

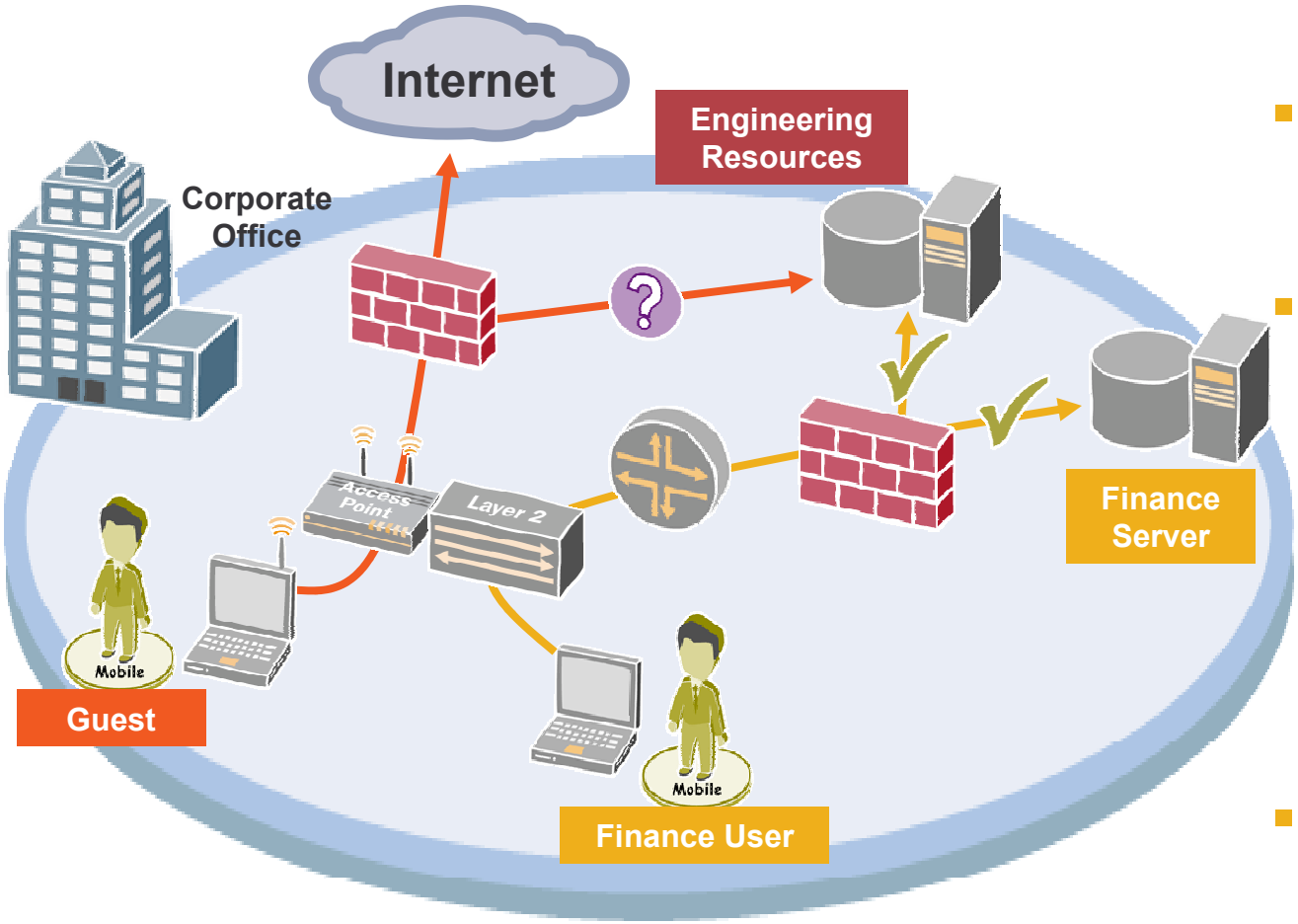
Network Protection



- **Ever-increasing number of mobile users (guests, employees, others) with diverse unchecked, unknown, or distrusted devices**
  - Just 1 infected device can take down a network and resources
- **Guest networking**
  - Need to identify guest users and grant them appropriate access, ***different*** from employees
- **Unchecked unmanageable devices can threaten LAN security**

CHALLENGE: User mobility, widespread use/deployment of unmanaged, distrusted, and unmanageable devices, and guest networking

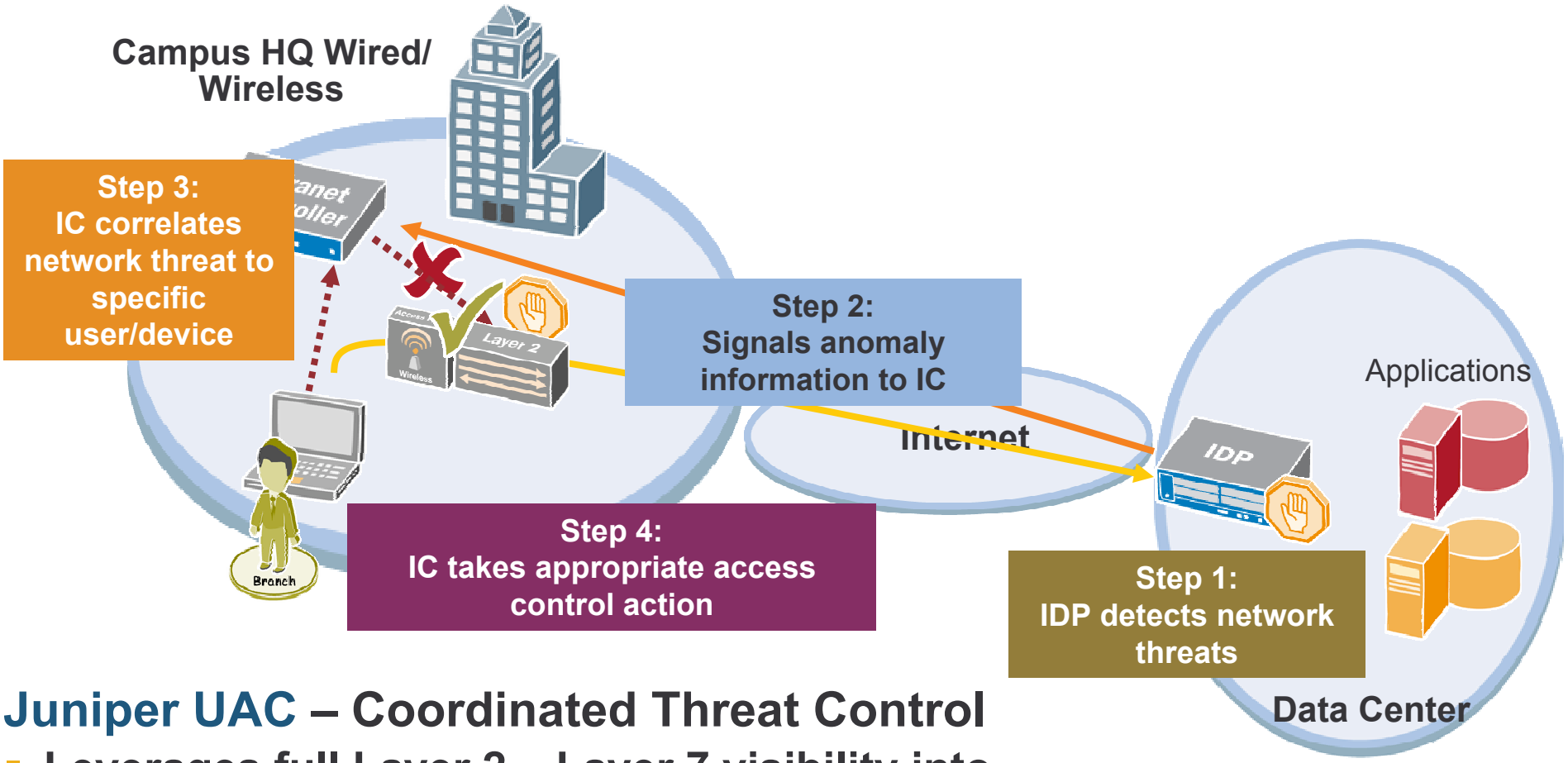
Access Control, Visibility & Monitoring



- **Lack of visibility into network and application access**
- **Regulatory compliance driving enterprises to demonstrate control over and visibility into corporate resources**
  - Monitor, audit, and log access
- **Enterprises must know what is happening within their LAN**

CHALLENGE: Ensure and prove only authorized users can access network and sensitive data

"Coordinated Threat Control"



Juniper UAC – Coordinated Threat Control

- **Leverages full Layer 2 – Layer 7 visibility into application traffic, minimizing downtime and delivering ability to:**
  - Quarantine malicious users/infected devices
  - Disable the user session
  - Log the event and notify administrators

Agenda

- NAC : Layer-2 vs Layer-3 enforcement
- Juniper UAC
  - Protection
  - Visibility
  - Threat Control
- **Standards & why they matter**

Standards & why they matter

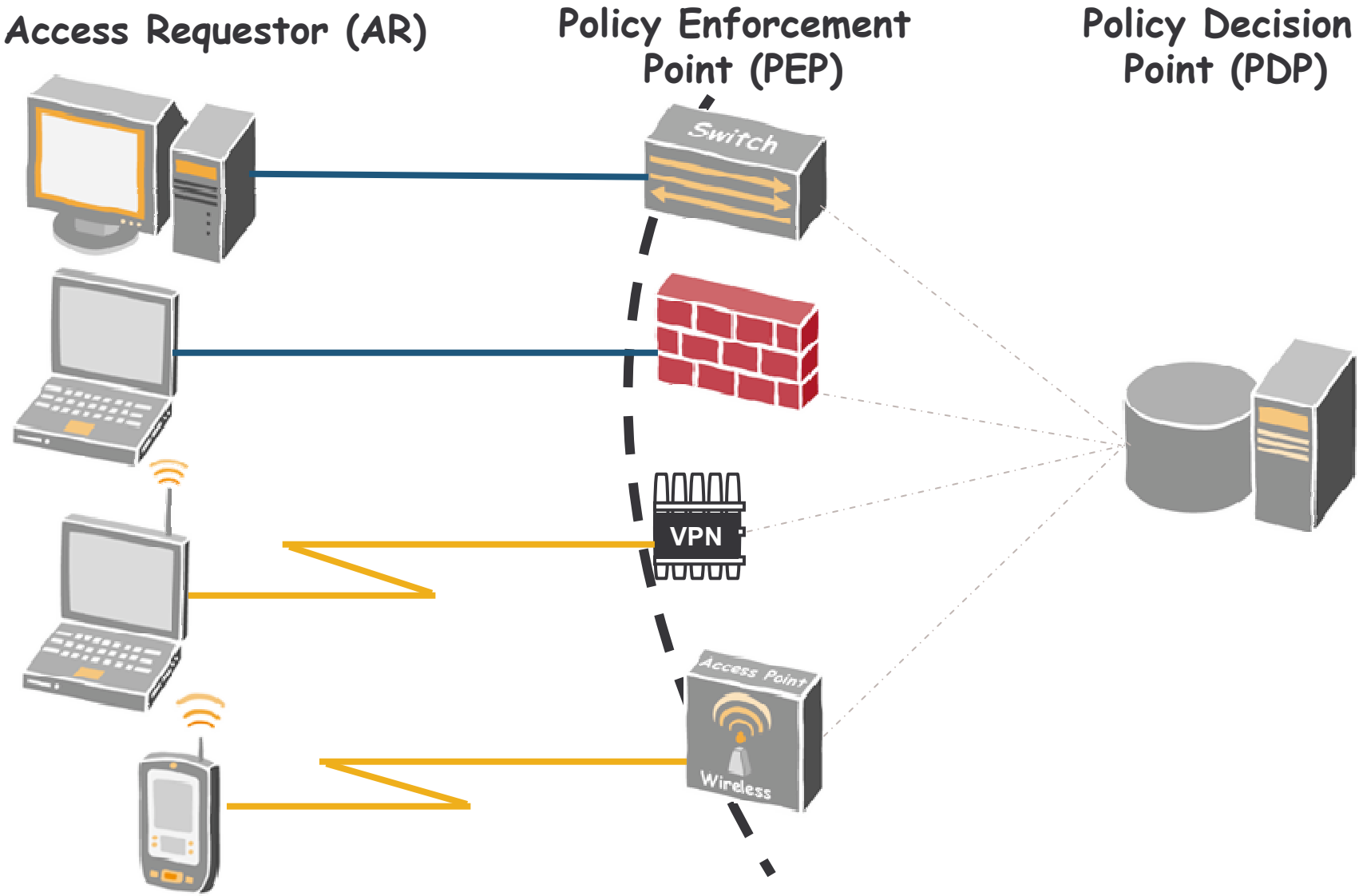
802.1X

- **Standard for Layer-2 Authentication/Authorization**
- **Vendor-agnostic, multi-vendor compatibility**
  - Supports heterogeneous network environments
- **Reduces costs and deployment time**
  - Leverages existing, installed products – software and hardware
  - Empowers choice, an advantage over single vendor lock-in
- **Increases security**
  - Better security through consistency
- **Higher, faster Return on Investment (ROI)**

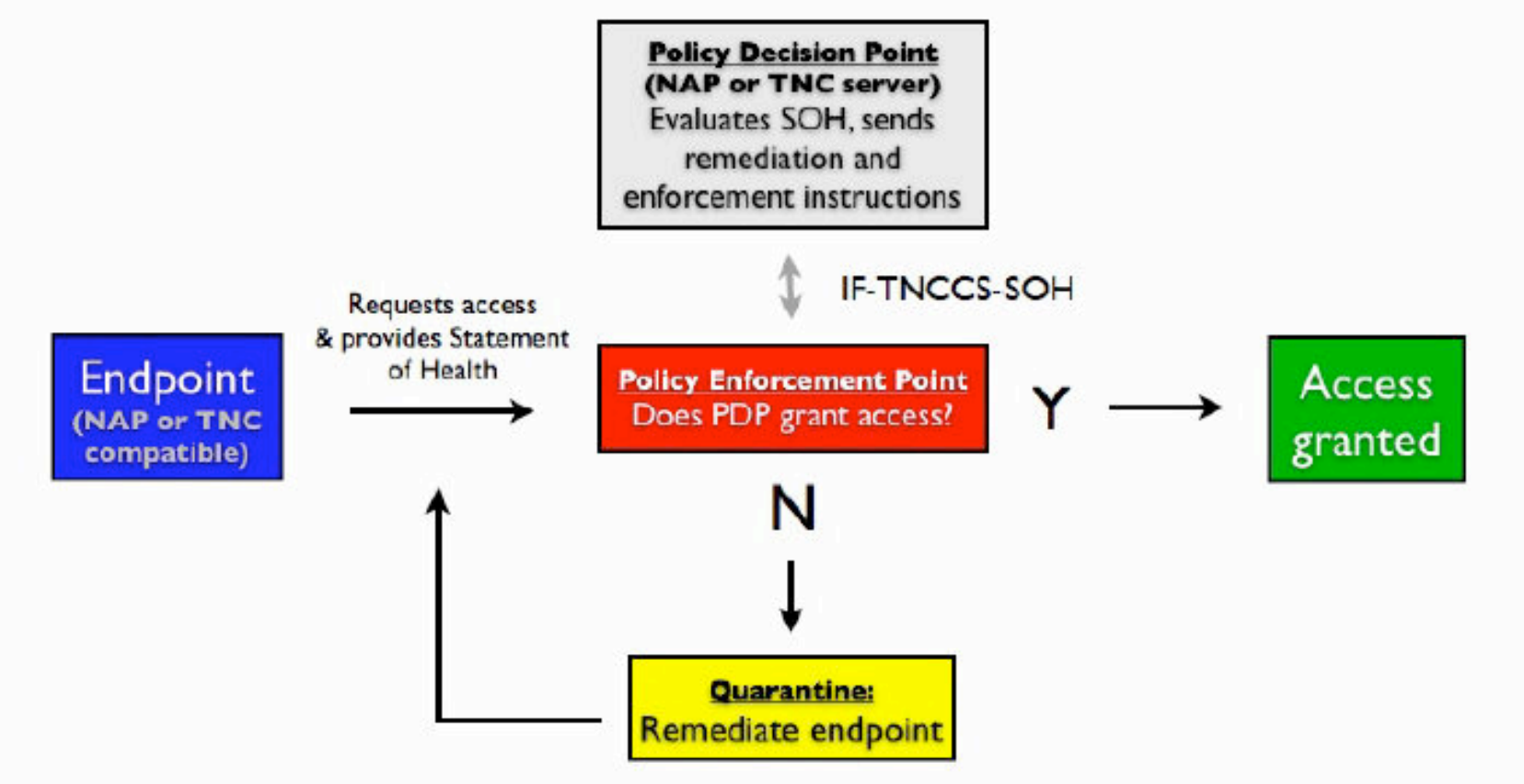
TNC - Trusted Network Connect

- **An open network access control architecture & standard**
- **A subgroup of the Trusted Computing Group (TCG)**
- **Vendor-agnostic, multi-vendor compatibility**
  - Supports heterogeneous network environments
- **Reduces costs and deployment time**
  - Leverages existing, installed products – software and hardware
  - Empowers choice, an advantage over single vendor lock-in
- **Increases security**
  - Thorough and open technical review of all standards
  - ALL endpoints are covered and secured

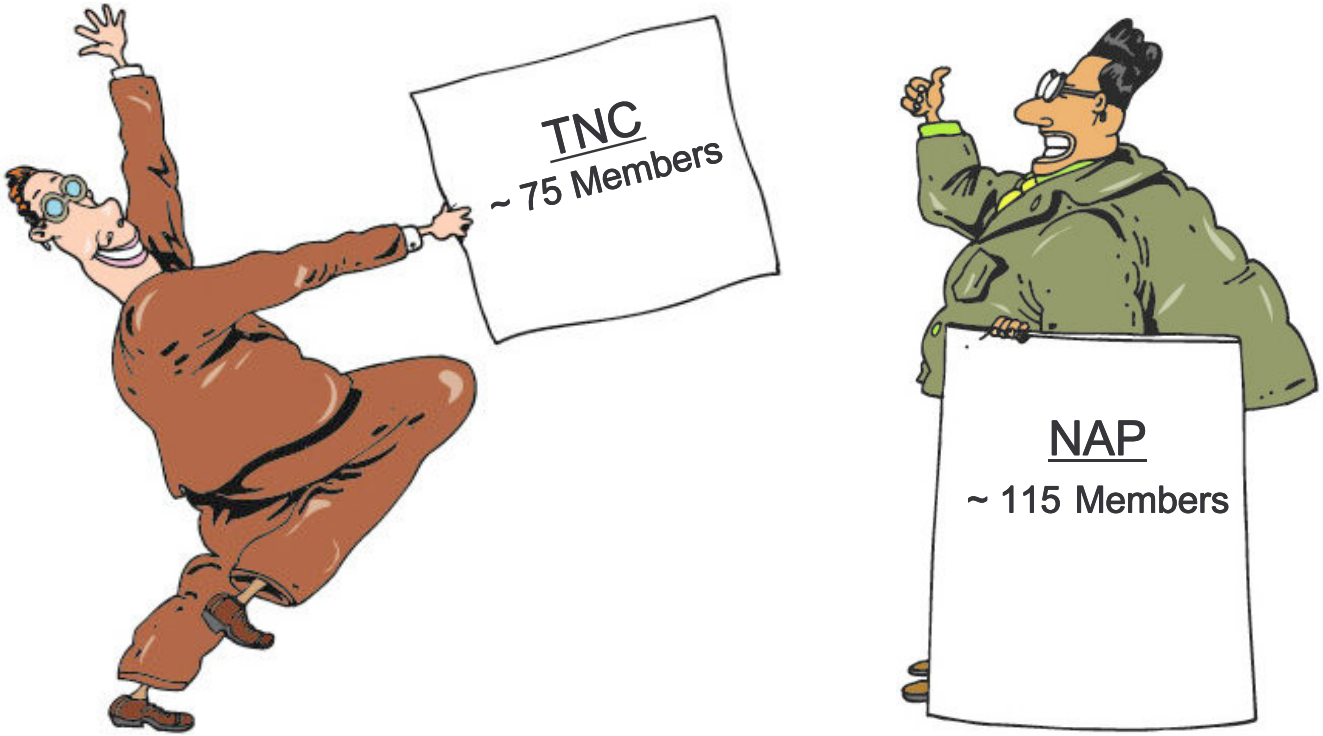
Basic TNC Architecture



Controlling Network Access with TNC and NAP



Controlling Network Access with TNC and NAP



Expect widespread adoption of IF-TNCCS-SOH protocol !!!

- Complements 802.1x as Endpoint Assessment “standard”

Summary - Juniper's UAC Solution Delivers

- Does what you need it to do
  - Pre AND post authentication security checks
  - Network admission AND network access controls
  - Easy, self-service remediation
- For all use cases – guests, contractors and employees
  - Cross platform
  - Managed, unmanaged and unmanageable devices
- Ideal for a phased deployment
  - L3-L7 overlay satisfies the immediate need
  - Roll 802.1X-based infrastructure (from any vendor) when you choose
  - Both solutions in one appliance
- Standards-based – 802.1X & TNC
- All elements are field tested

Thank you for listening !

Juniper your Net™

Stefan Lager, CISSP
slager@juniper.net