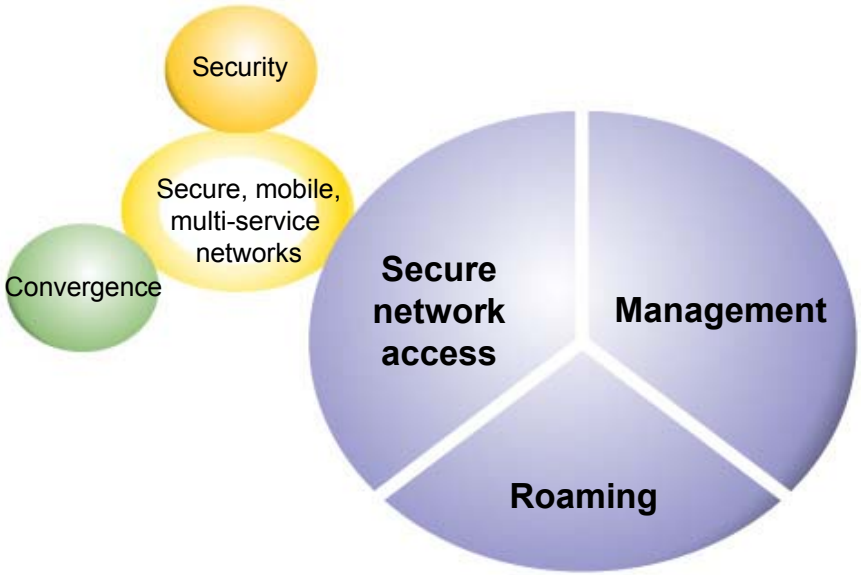
HP ProCurve: Making Secure Mobility Possible for the Enterprise Network

Rodney Turner
Solution Architect
Hewlett-Packard

HP WORLD 2003
Solutions and Technology Conference & Expo

HP ProCurve Mobility on the EDGE



Mobility

Featuring . . .

- Enterprise 802.11a/b wireless
- Control of mobile users' access
  - By user
  - By location
  - By time of day
- Secure, seamless roaming between access points and across subnets

Delivering . . .

- Secure mobility across large enterprise campus environments
- A dependable, persistent connection
- Central control of wireless environments

HP ProCurve Wireless Access Point 520wl—unique features

- Dual-slot design (802.11a, 802.11b) radio cards available today; 802.11g radio cards coming later this year
- Wireless repeater—can bridge up to 6 additional APs not connected to an Ethernet port. The dual-radio design permits each AP to use one radio to handle wireless traffic among AP's, with the second radio dedicated to serving wireless users—providing more bandwidth/greater capacity.
  - Other APs rely on the same (single) radio to handle all wireless traffic.
- The embedded HTTP Web server interface offers a tab-based interface with configuration and monitoring screens logically grouped for ease of navigation.
  Initial configuration and subsequent changes can be performed quickly and easily.
- Lifetime warranty

HP ProCurve Wireless Access Point 520wl—accessories

HP WORLD 2003
Solutions and Technology Conference & Expo

HP ProCurve Wireless Range Extender Antenna 100wl

J8134A

Indoor 2.5 dBi gain antenna for increasing range of the Access Point 520wl

HP ProCurve 802.11b Wireless Access Point Card 150wl

J8135A 11CH (North America)

J8136A 13CH (Europe/Asia)

J8137A 14CH (Japan)

802.11b, 11 Mbps radio component for the Access Point 520wl

HP ProCurve 802.11a Wireless Access Point Kit 160wl

J8138A North America

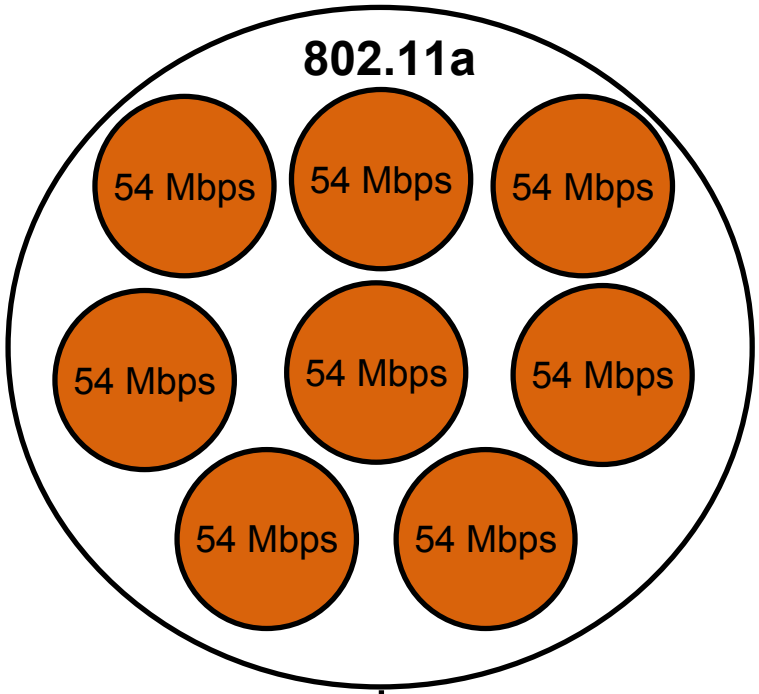
J8148A Singapore

J8149A Europe

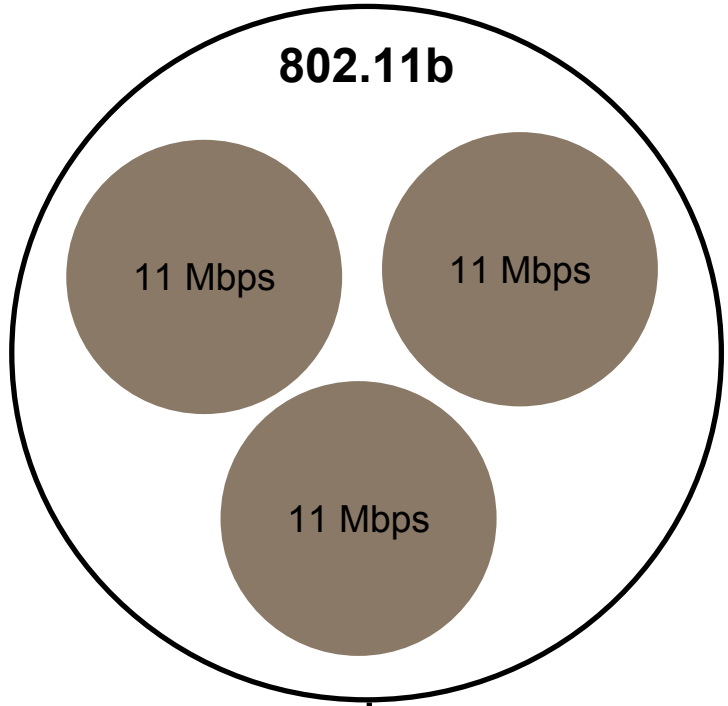
J8150A Japan

802.11a, 54 Mbps radio component for the Access Point 520wl

802.11a versus 802.11b

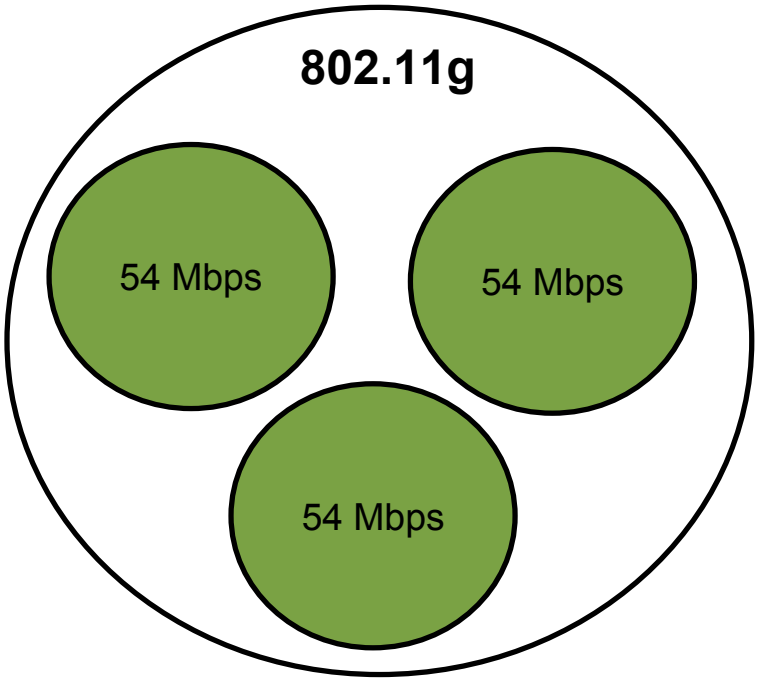


Pros	Cons
More bandwidth for higher user density	Short range
No interference	More access points = higher costs

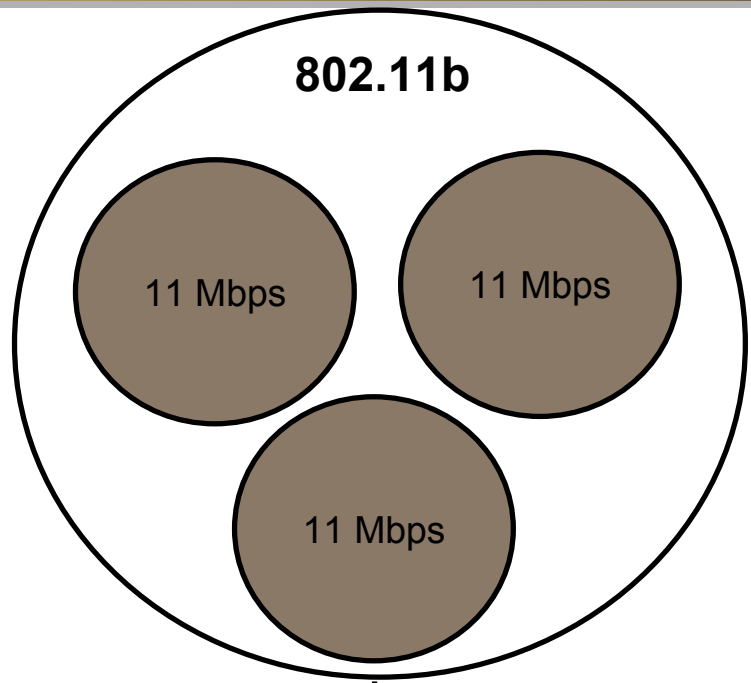


Pros	Cons
Greater range	Lower bandwidth
Lowest cost	Shares same frequency spectrum with 802.11g, Bluetooth, cordless phones
Widely deployed	

802.11g versus 802.11b

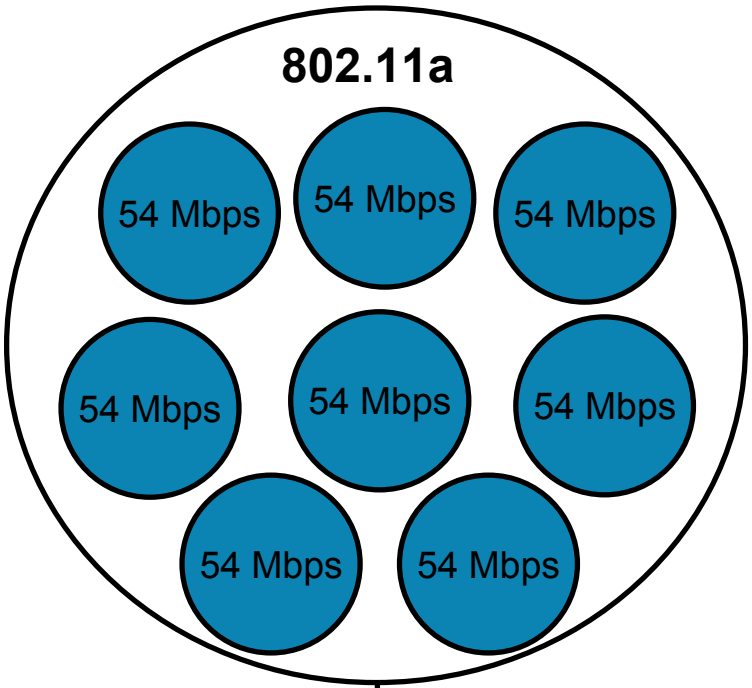


Pros	Cons
Low cost	Shorter range
Performance lift	Shares same frequency spectrum with 802.11g, Bluetooth, cordless phones
Compatible with 802.11b	

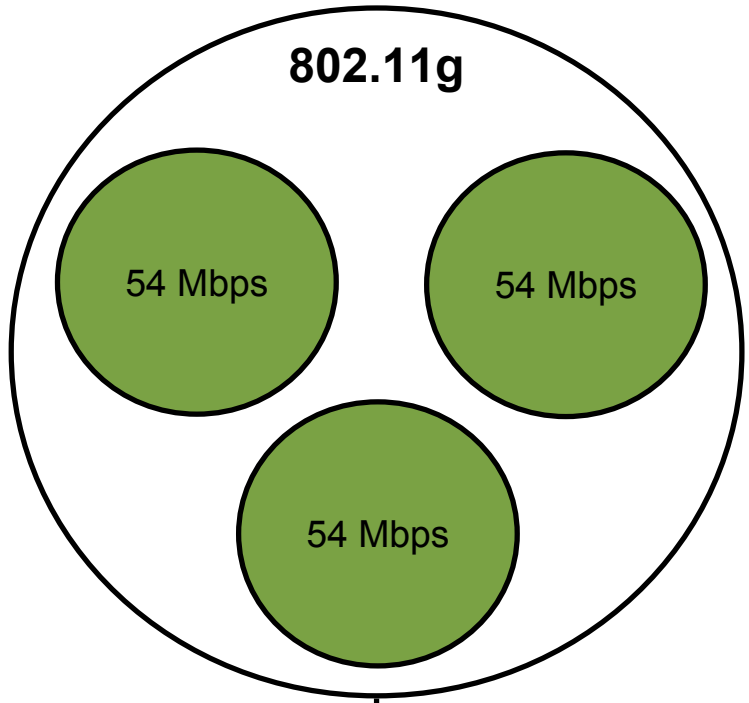


Pros	Cons
Longer range	Lower bandwidth
Lowest cost	Shares same frequency spectrum with 802.11g, Bluetooth, cordless phones
Widely deployed	

802.11a versus 802.11g

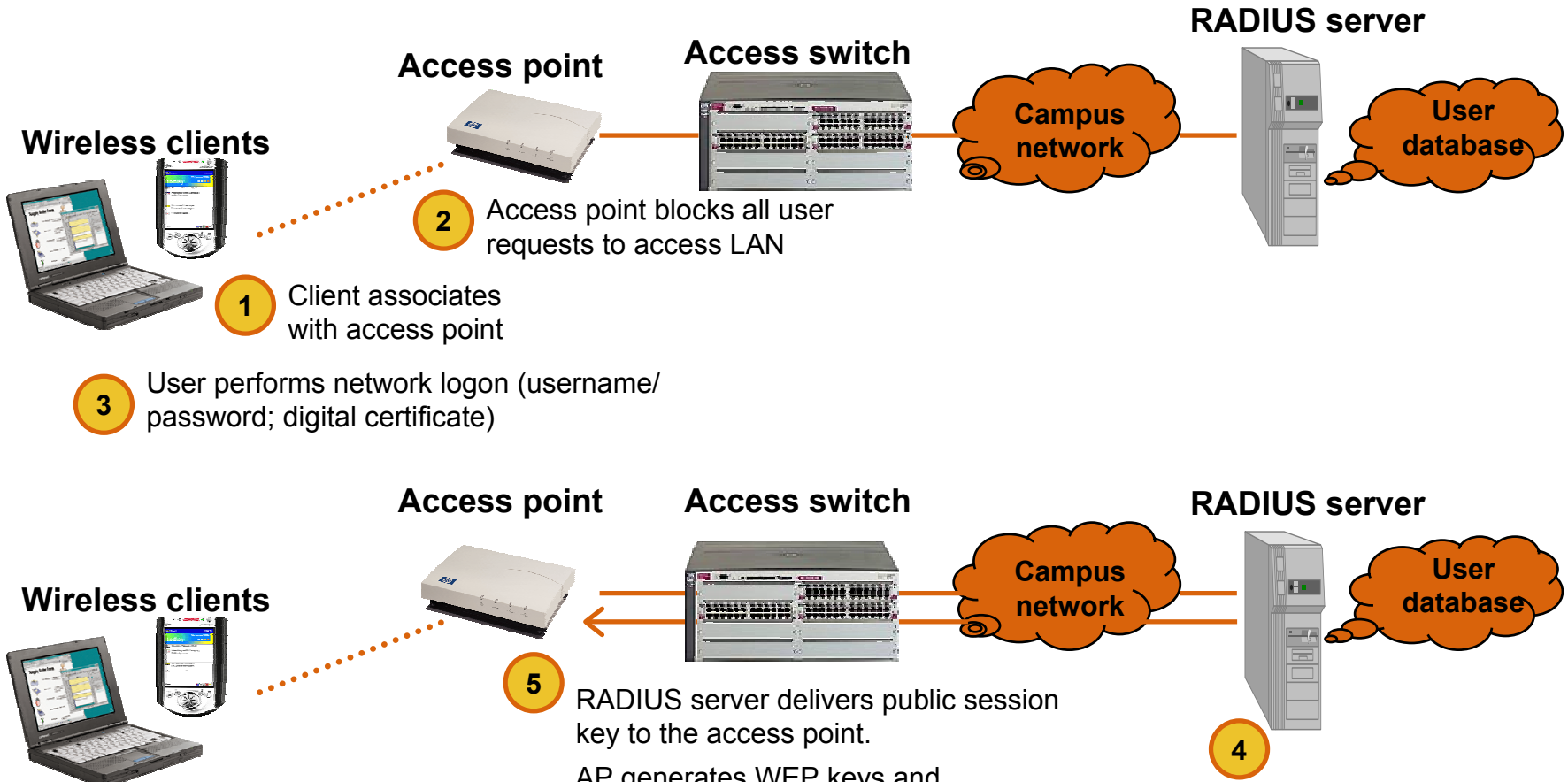


Pros	Cons
Higher user density	Shorter range
Performance lift	More access points = higher costs
No interference	



Pros	Cons
Low cost	Shorter range
Performance lift	Shares same frequency spectrum with 802.11g, Bluetooth
Compatible with 802.11b	

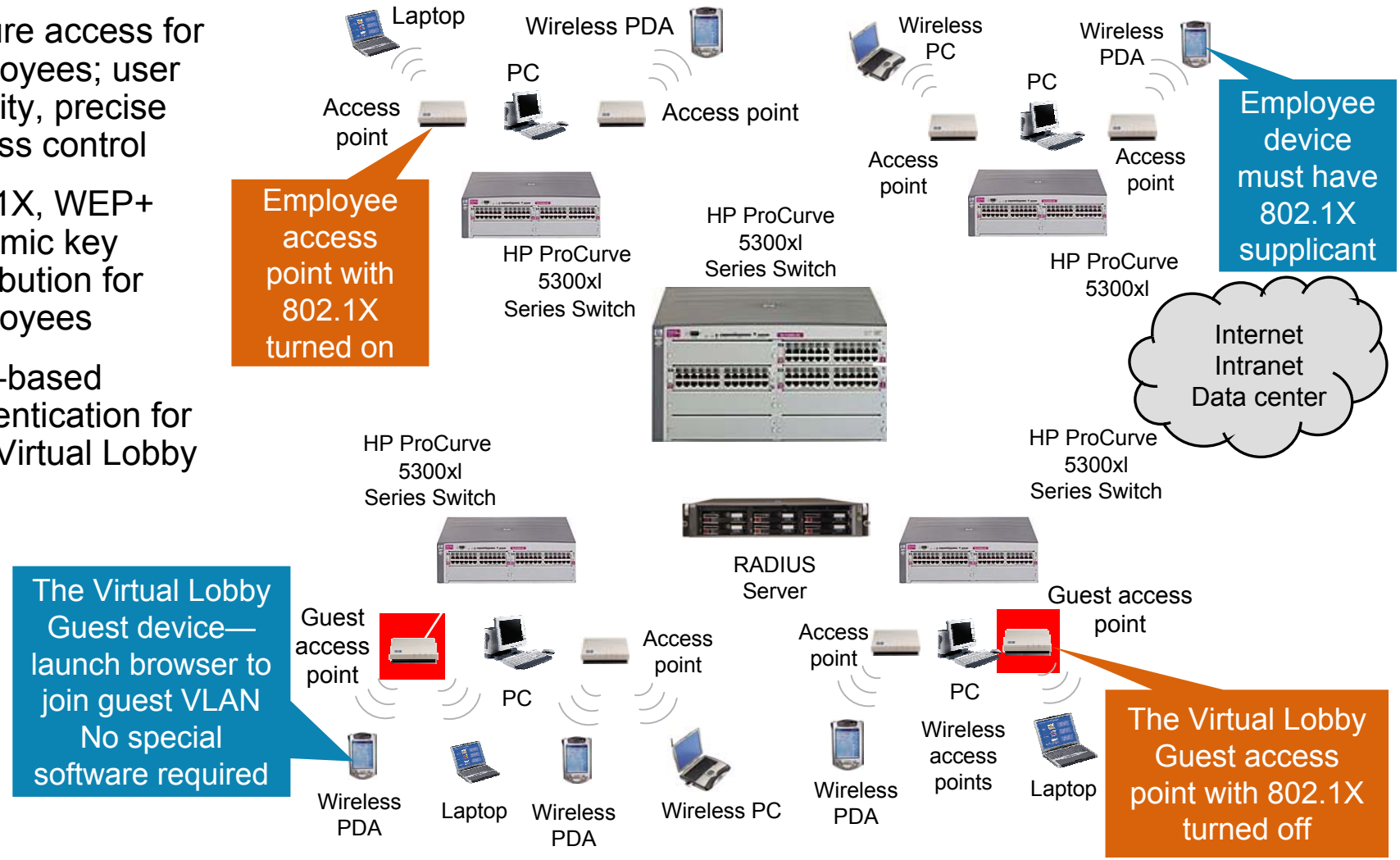
802.1X WLAN authentication and data encryption



Mobile workers in mid-size enterprise

Improved user access and wireless productivity

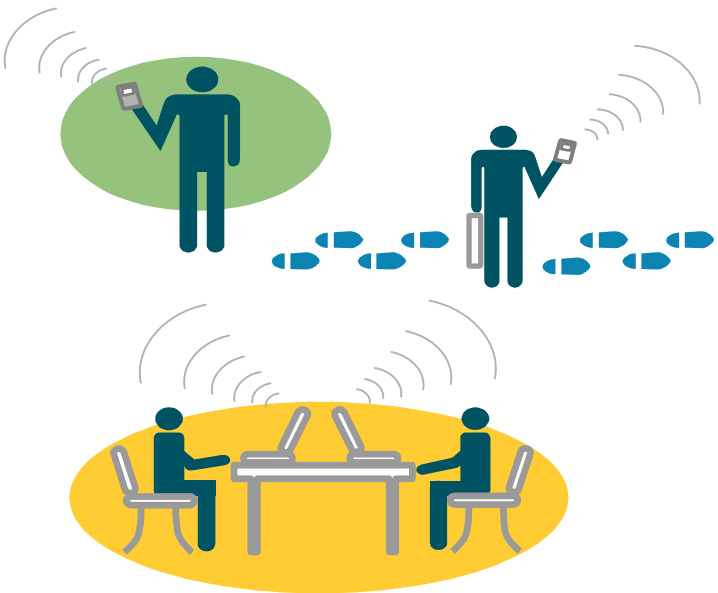
- Secure access for employees; user identity, precise access control
- 802.1X, WEP+ dynamic key distribution for employees
- Web-based authentication for The Virtual Lobby



Today's Wireless World: Key business challenges

- Granting secure, appropriate user access
- Guaranteeing the privacy of wireless traffic
- Providing flexible, secure user authentication
- Supporting secure roaming with application stability
- Safeguarding network integrity

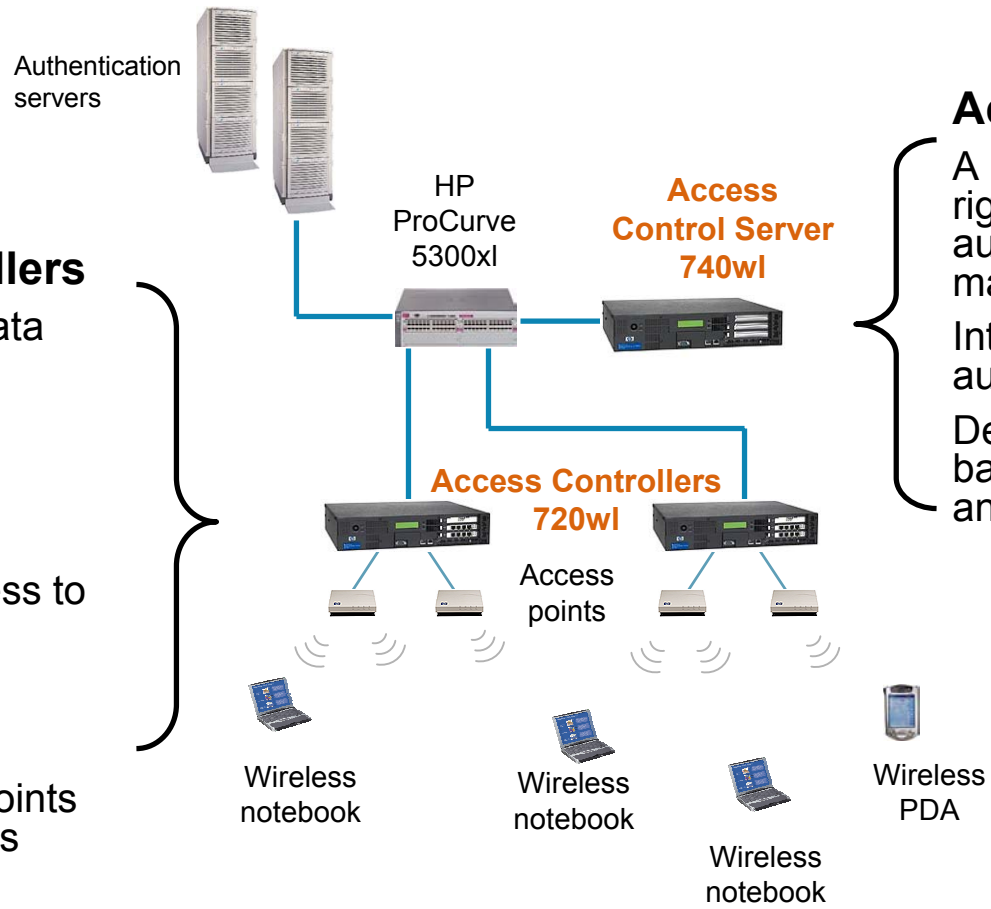
HP ProCurve Secure Access 700wl Series supports secure mobility



State-of-the-art enterprise-level security

- Simplified user and security policy management
- Data privacy
- Standards-based authentication
- Access control
- Secure roaming
- Investment protection

Secure access overview



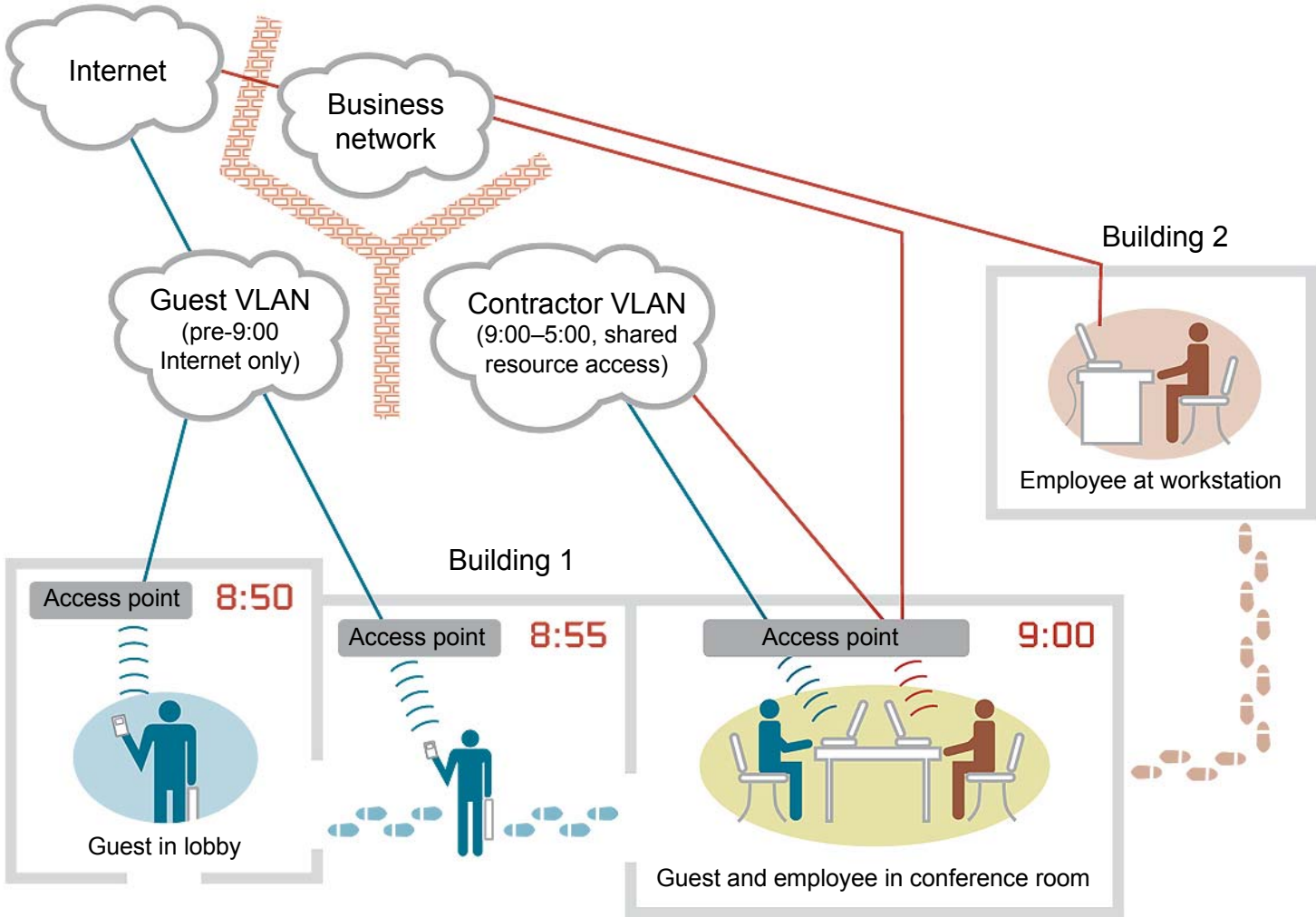
Access Controllers

- Secure wireless data privacy
- Enforce access policy and deny unauthorized network access
- Enable guest access to specific network resources
- Manage secure, seamless roaming between access points and across subnets

Access Control Server

- A centralized, user rights manager that authenticates users and manages policy rights
- Integrates with existing authentication services
- Determines access rights based on user ID, location, and time of day

Large enterprise campus user experience



HP ProCurve Secure Access 700wl Series—a complete, secure wireless mobility solution

HP ProCurve Access Controller 720wl

HP ProCurve Access Control Server 740wl

HP ProCurve Integrated Access Manager 760wl

HP ProCurve Access Controller 720wl

J8153A

Enforces security policies and manages access points at the wireless network edge

- Resides between the wireless access points and the network
- Enforces user authentication and access rights
- Supports robust industry-standard security protocols
- Used with either the HP ProCurve Access Control Server 740wl or the HP ProCurve Integrated Access Manager 760wl

HP ProCurve Access Control Server 740wl

J8154A

Centralized access and rights management of WLAN infrastructure reduces complexity and operating costs

- Configuration and policy management for all users
- Supports secure, uninterrupted roaming
- Offers centralized policy management
- Seamlessly integrates into an existing network infrastructure
- Used with the HP ProCurve Access Controller 720wl

HP ProCurve Integrated Access Manager 760wl

J8155A

Provides WLAN security and access management and enforcement for departments or small networks

- Combines the functionality of the HP ProCurve Access Controller 720wl and the HP ProCurve Access Control Server 740wl into a single, cost-effective device
- Manages user authentication and roaming of users among multiple locations
- 2U device with integrated 10/100/1000Base-T uplink

Product accessories

For use with Access Controller 720wl and Access Control Server 740wl

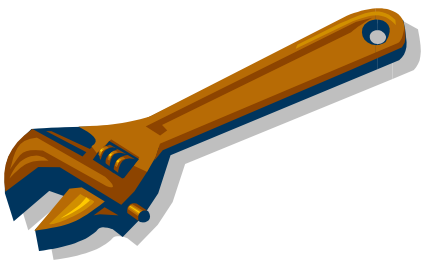
- HP ProCurve Secure Access 4-port 10/100 card (J8156A)
  - Provides 4 10/100Base-T ports for expanding control ports on the HP ProCurve Secure Access 720wl and 760wl products
- HP ProCurve Secure Access Acceleration Card (J8160A)
  - Accelerates DES and 3DES throughput

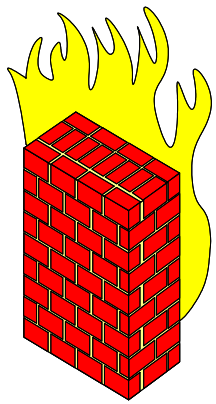
For use with all Secure Access 700wl products

- HP ProCurve Secure Access 1-port Gigabit-SX card (J8157A)
- HP ProCurve Secure Access 1-port Gigabit-LX card (J8158A)
- HP ProCurve Secure Access 1-port 10/100/1000Base-T card (J8159A)
- Gigabit adapter cards for ease of integration into a Gigabit network

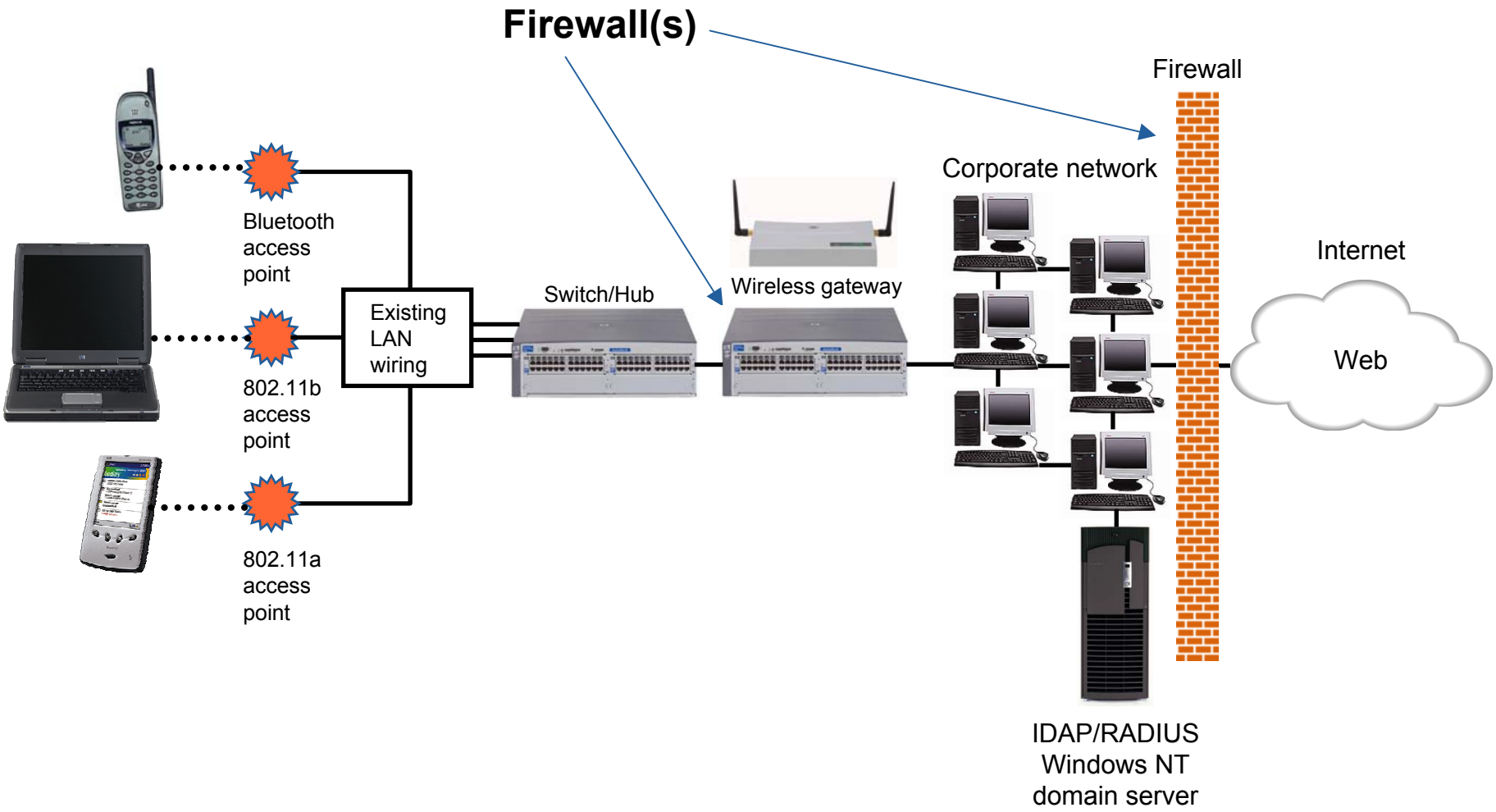
Post 9/11 wireless security blues…What is the answer?

Is a firewall the answer?
Is a firewall the only solution for wireless security?
What is the answer for wireless security?

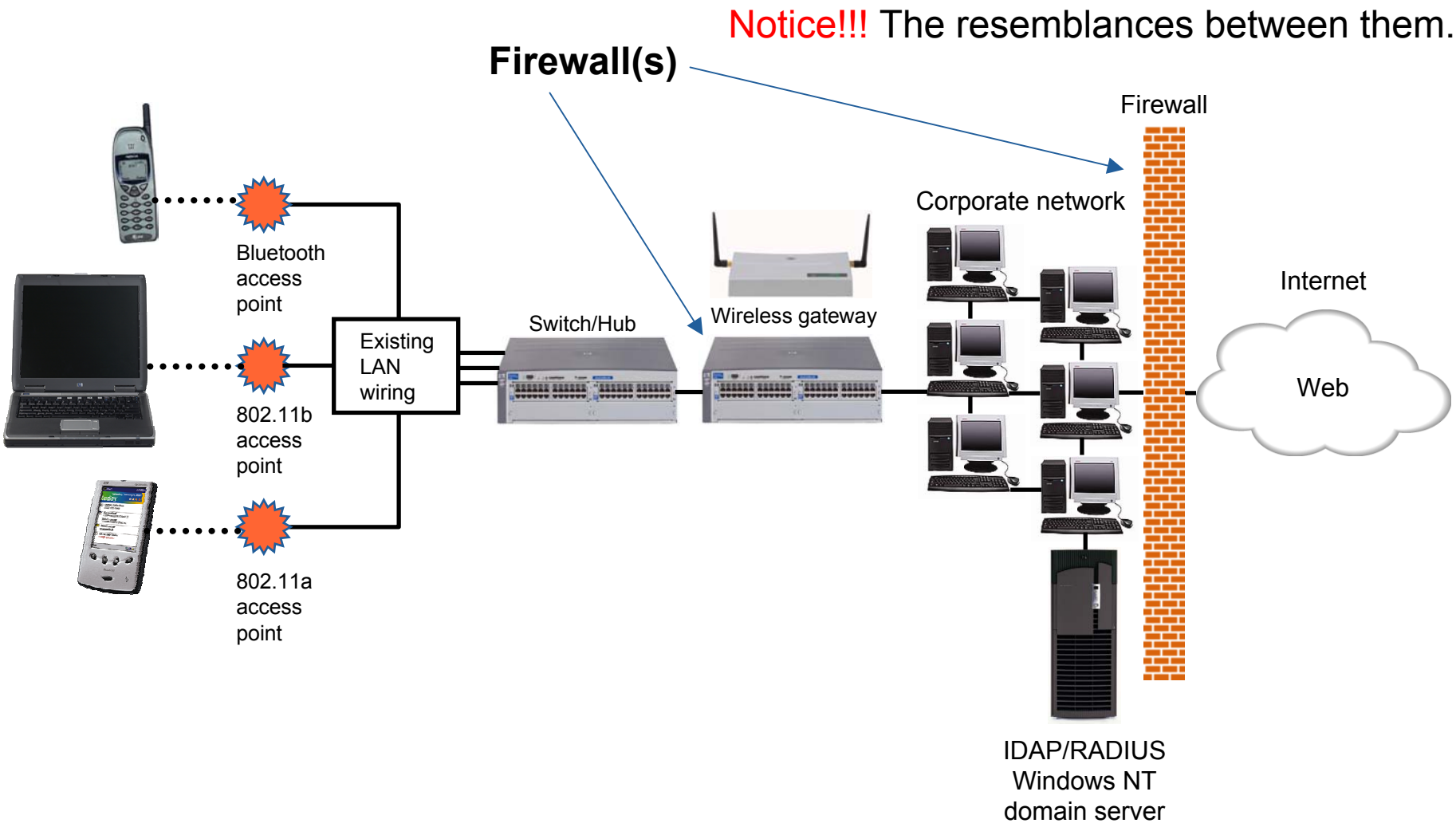




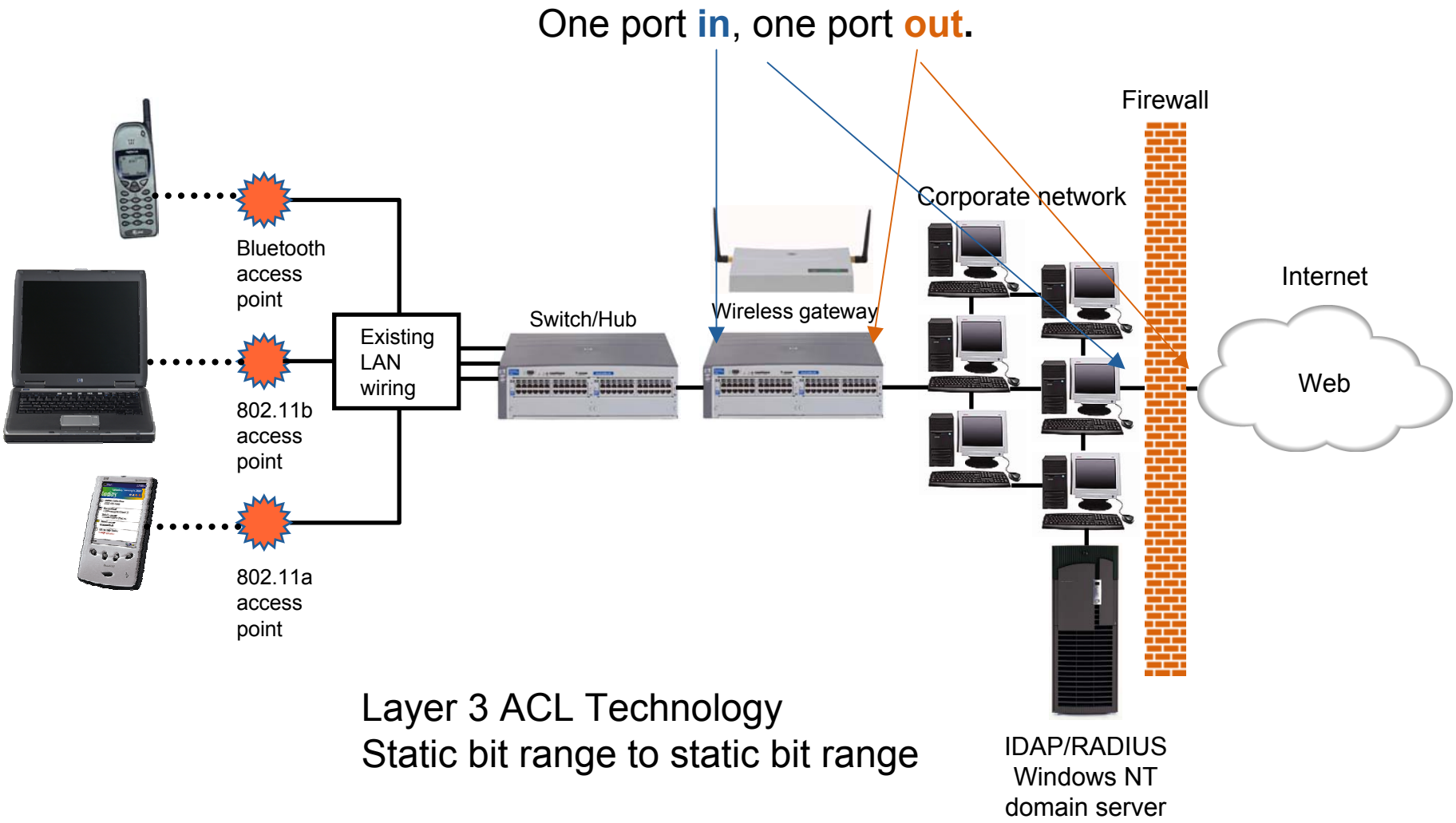
Typical wireless solution



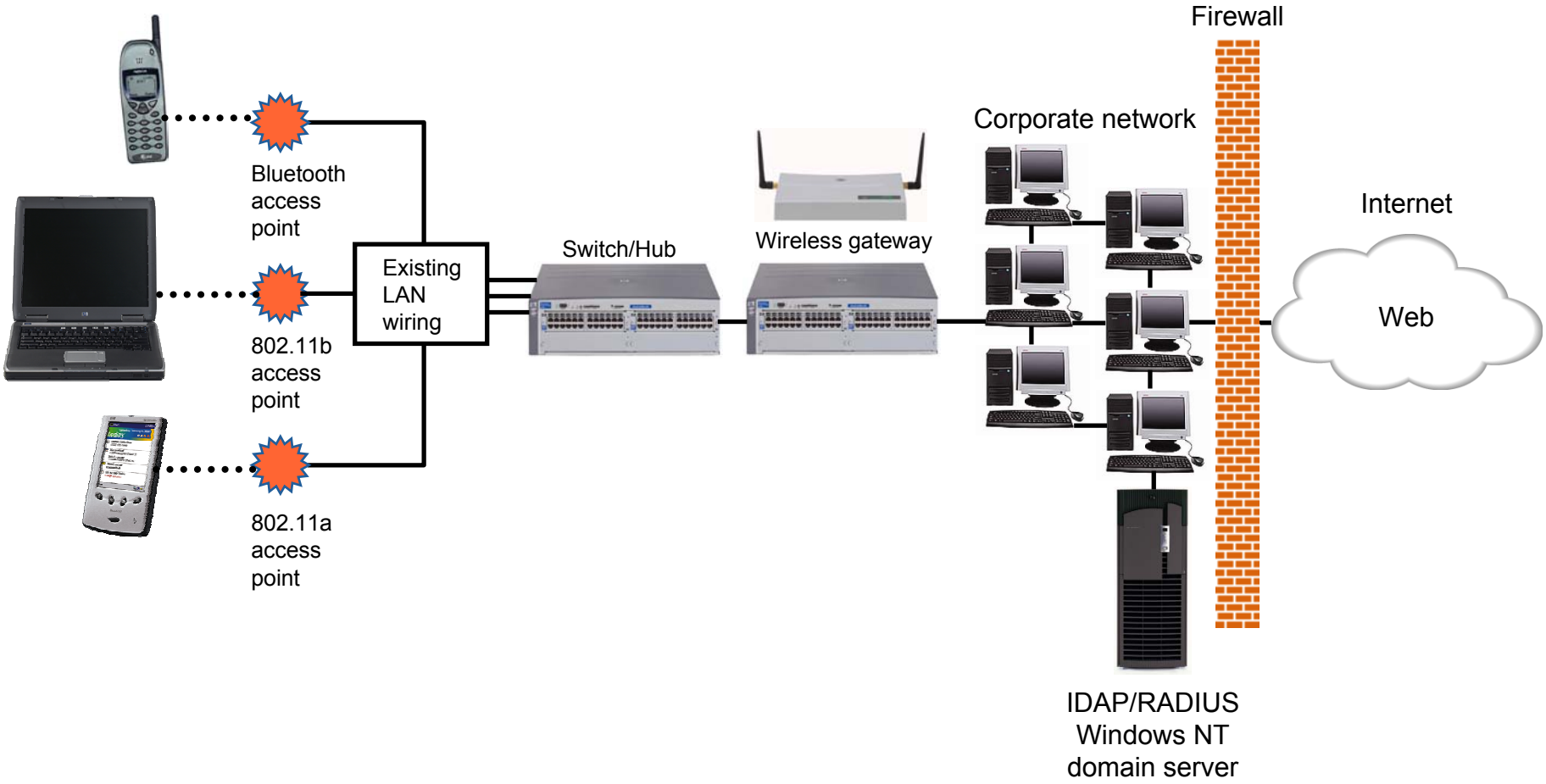
Typical wireless solution



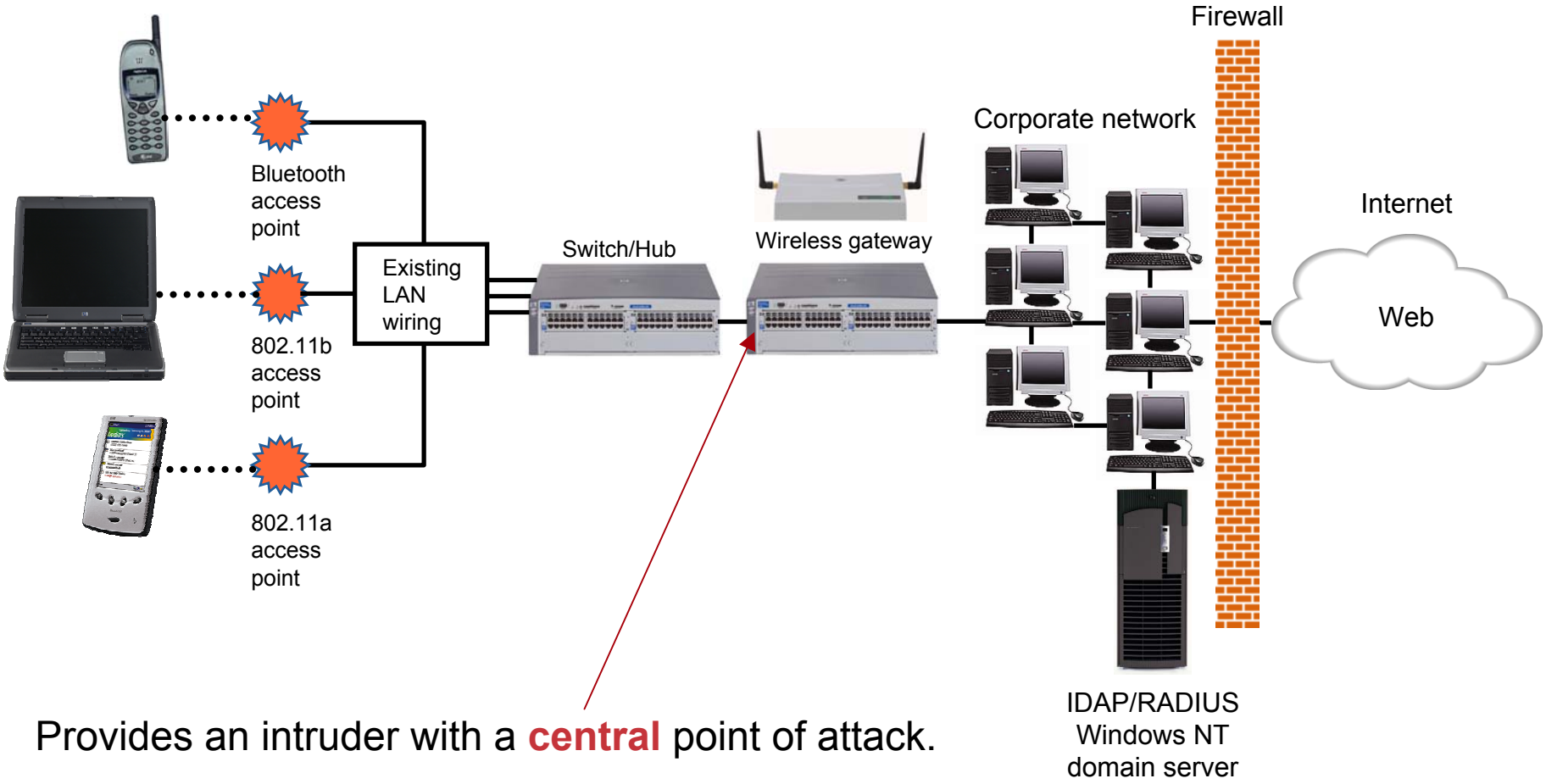
Typical wireless solution



Why is one input/output port a bad idea?

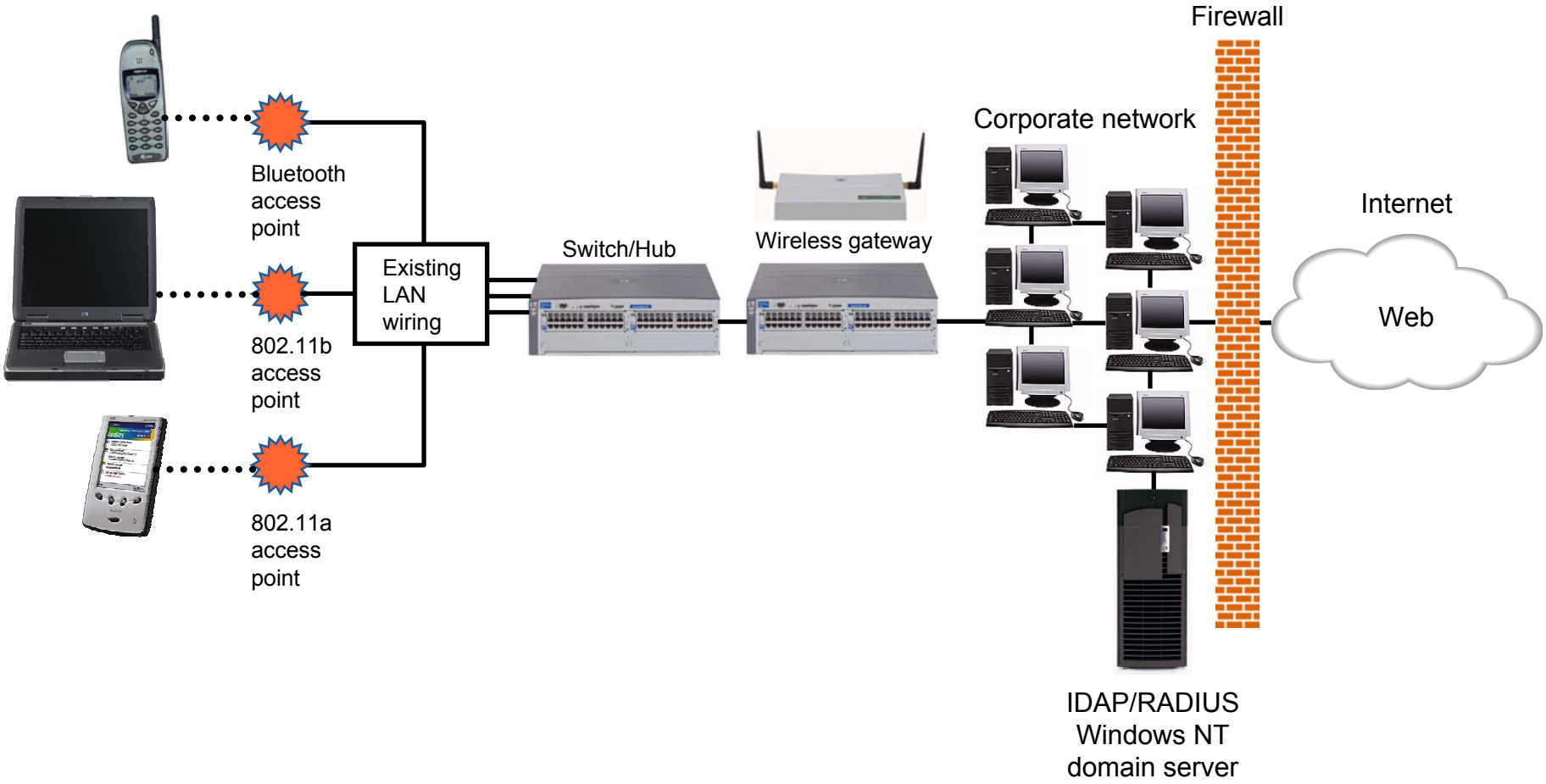


Why is one input/output port a bad idea?

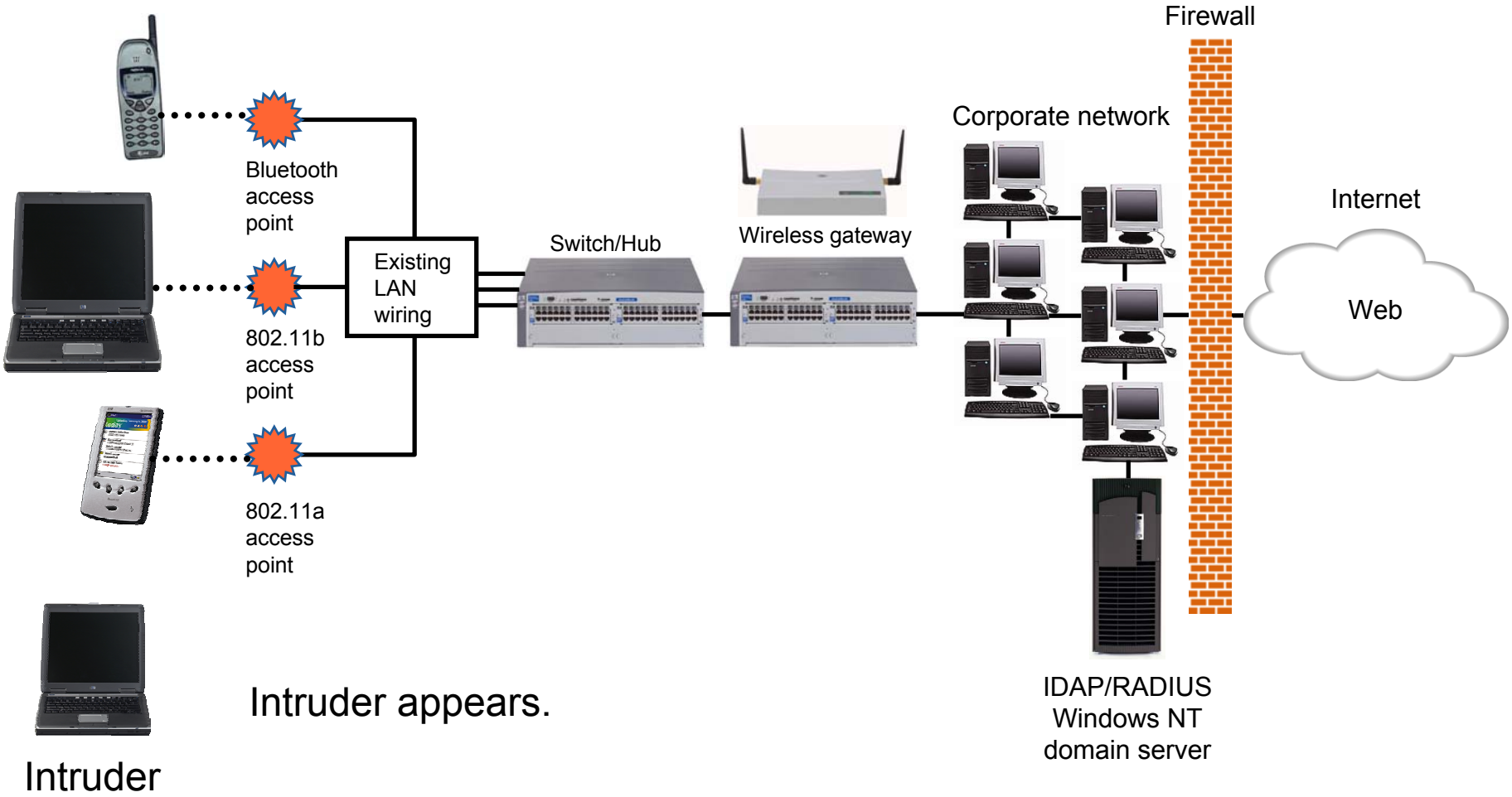


Provides an intruder with a **central** point of attack.

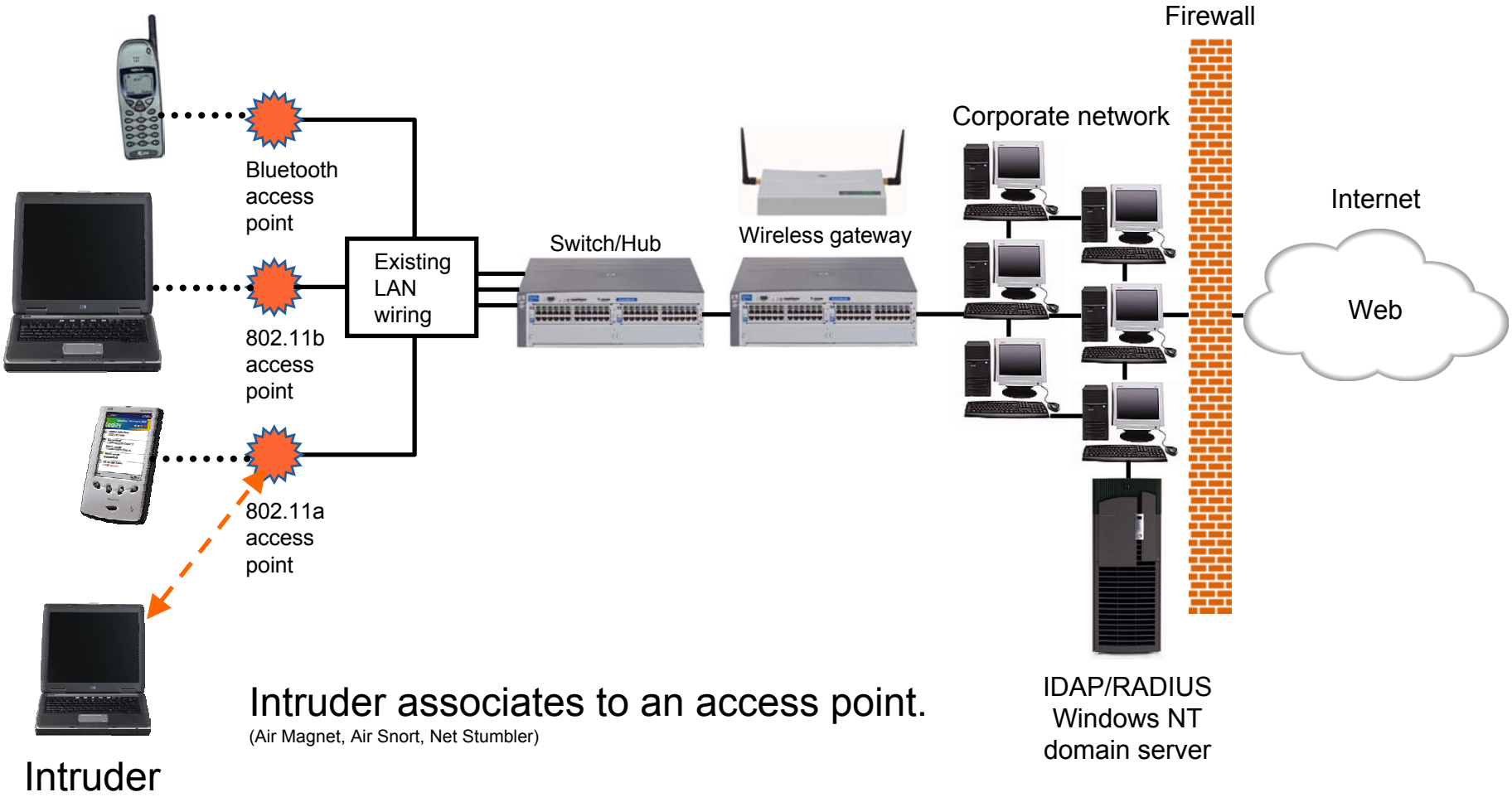
Case study 1: Single port based attack



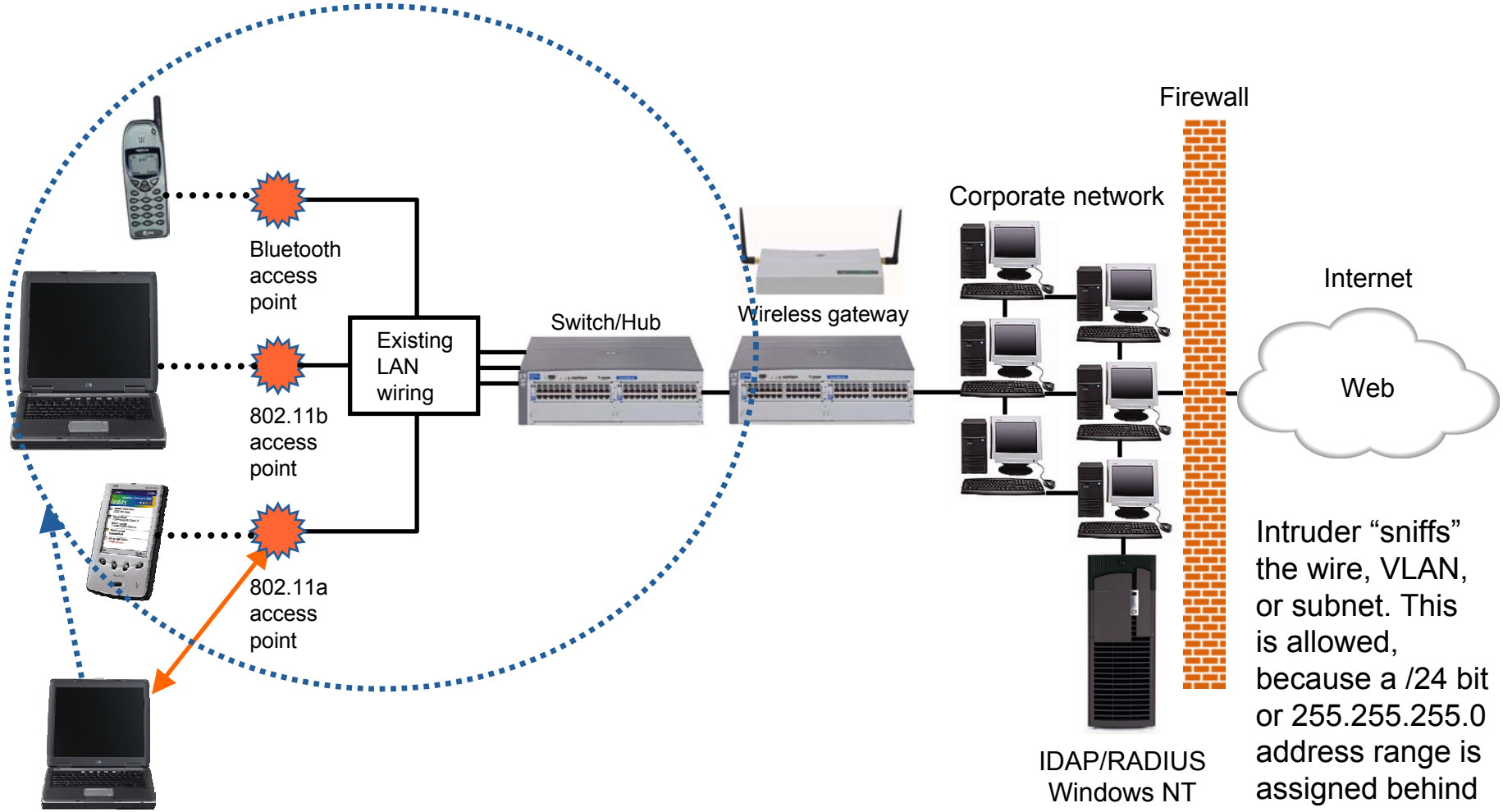
Case study 1: Single port based attack



Case study 1: Single port based attack

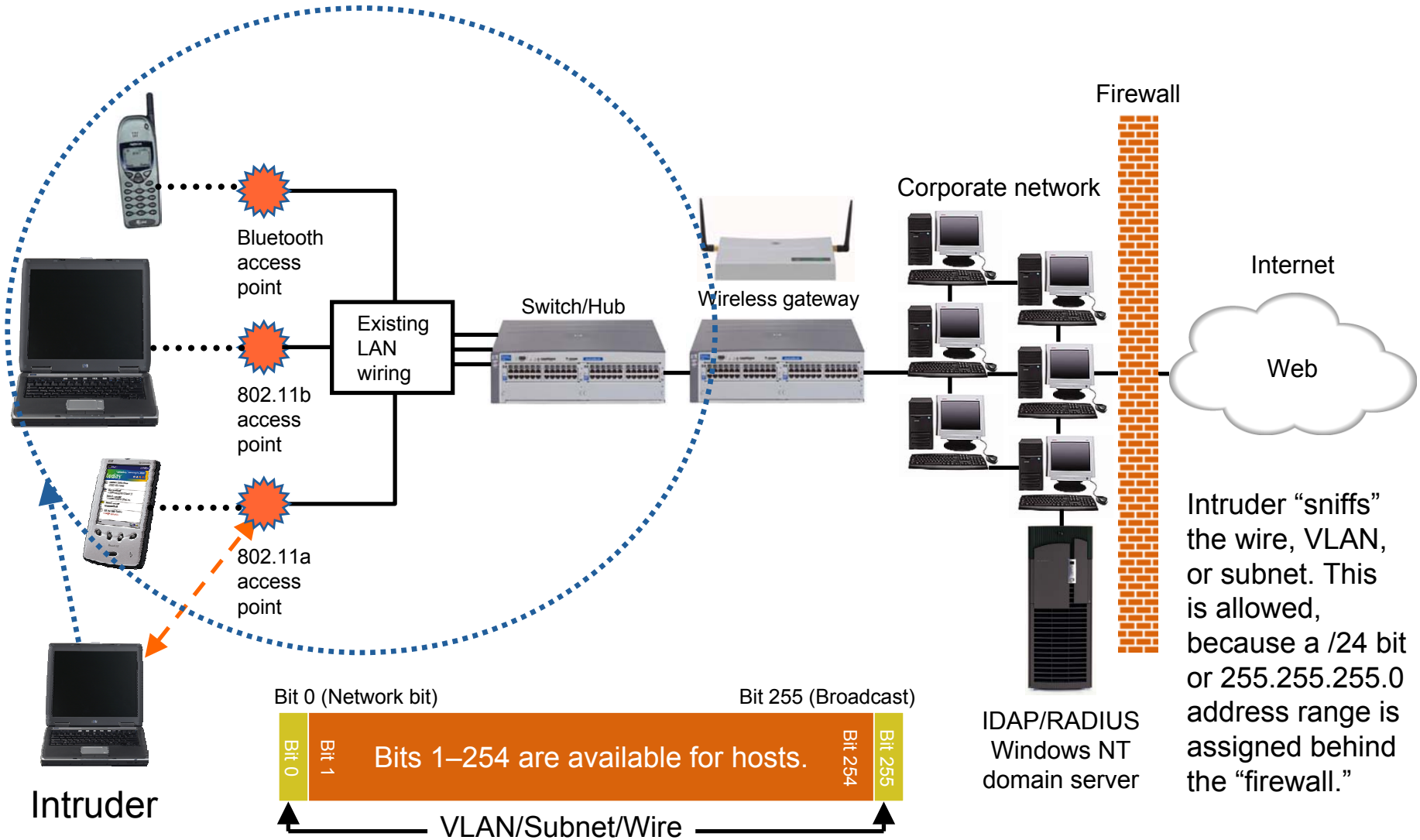


Case study 1: Single port based attack



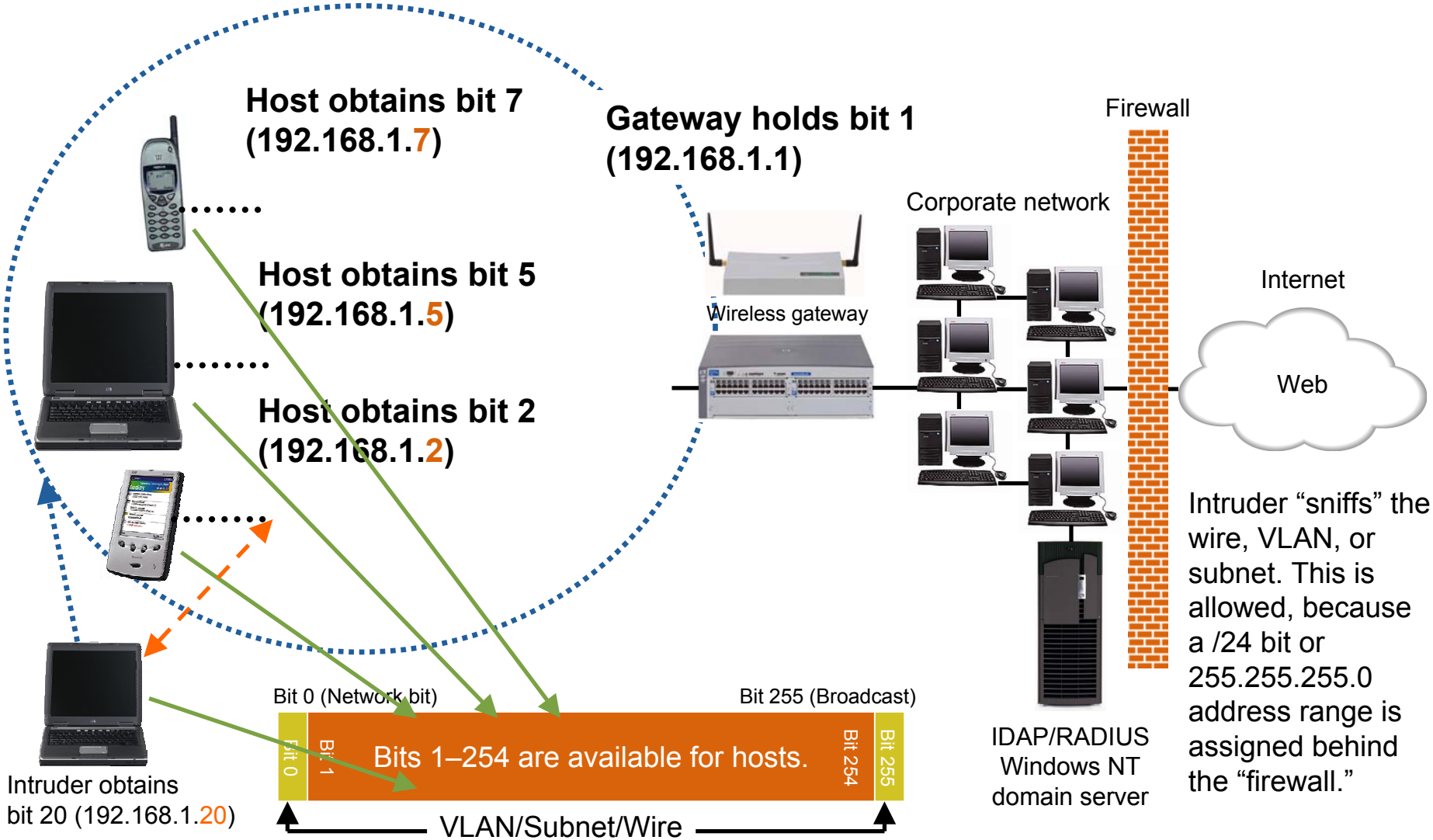
Intruder "sniffs" the wire, VLAN, or subnet. This is allowed, because a /24 bit or 255.255.255.0 address range is assigned behind the "firewall."

Case study 1: Single port based attack

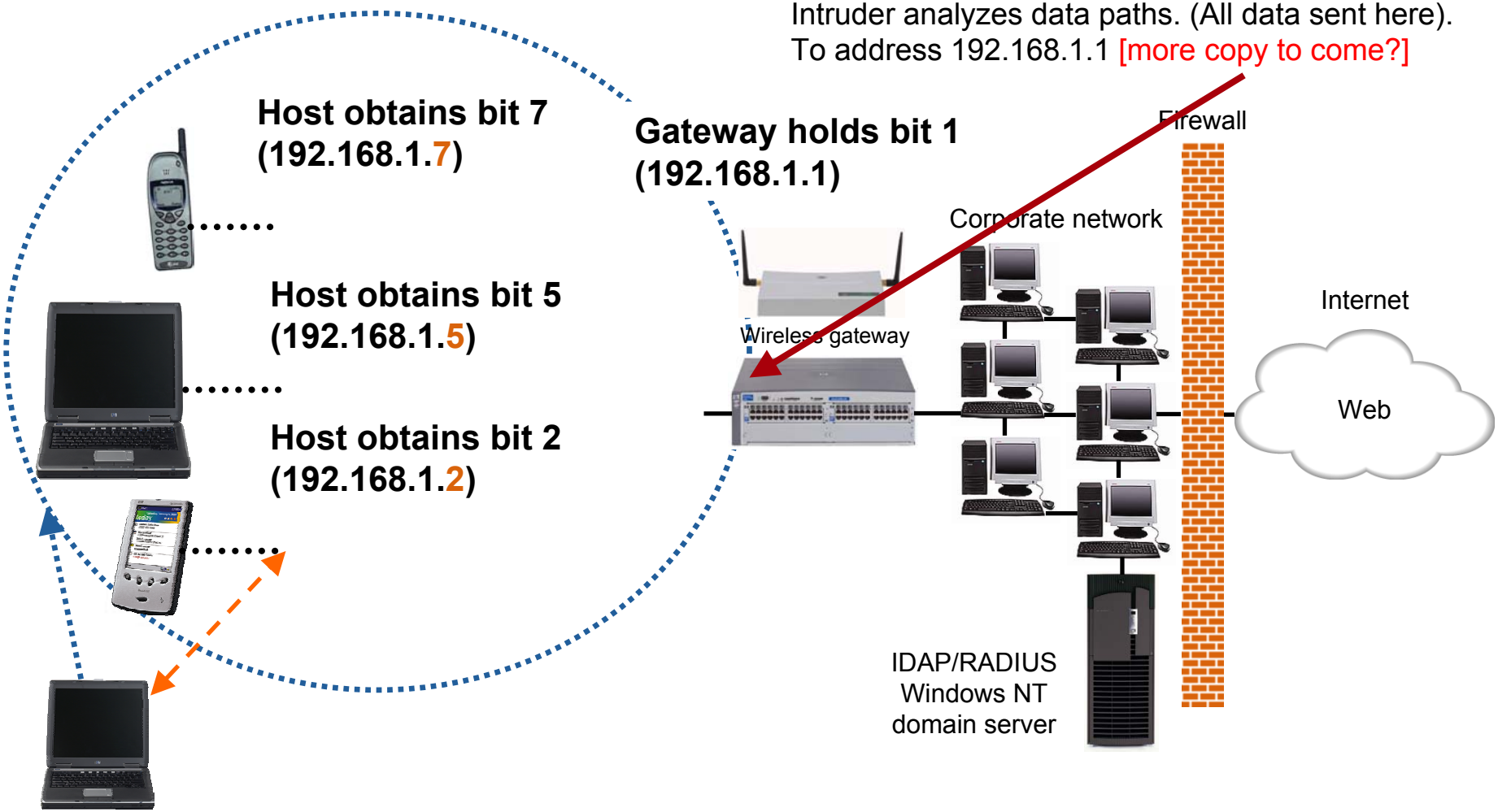


Intruder "sniffs" the wire, VLAN, or subnet. This is allowed, because a /24 bit or 255.255.255.0 address range is assigned behind the "firewall."

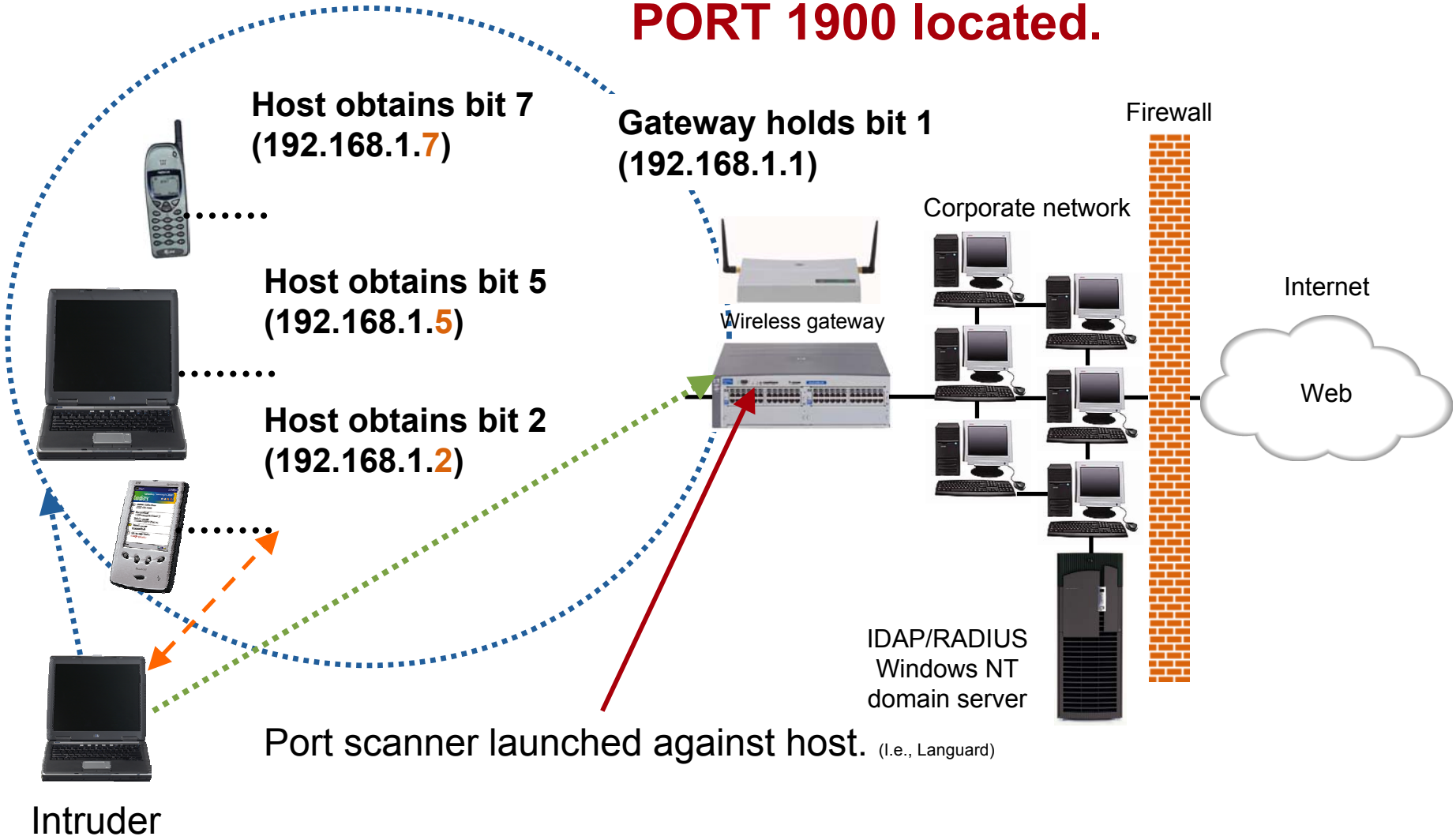
Case study 1: Single port based attack



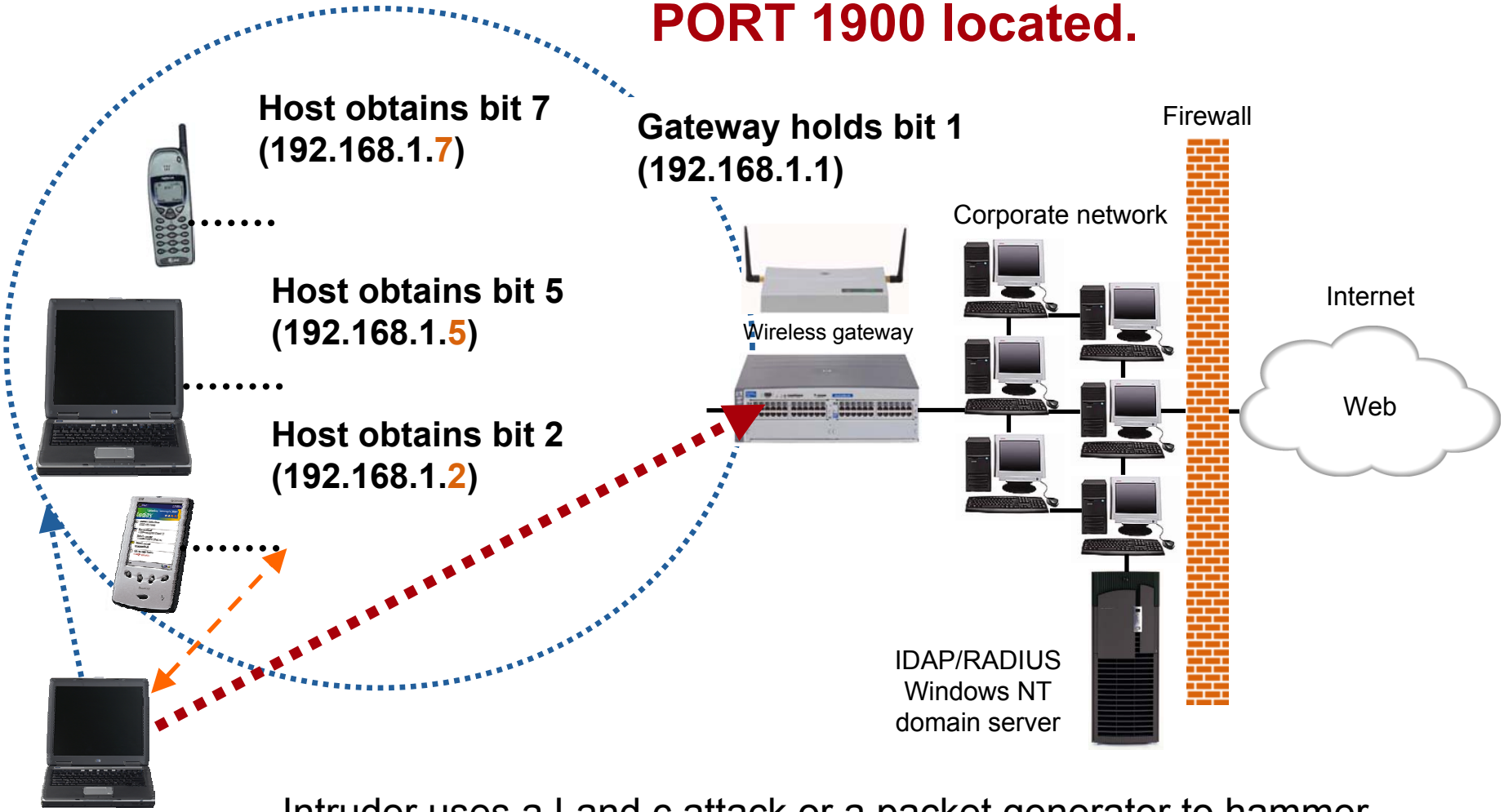
Case study 1: Single port based attack



Case study 1: Single port based attack

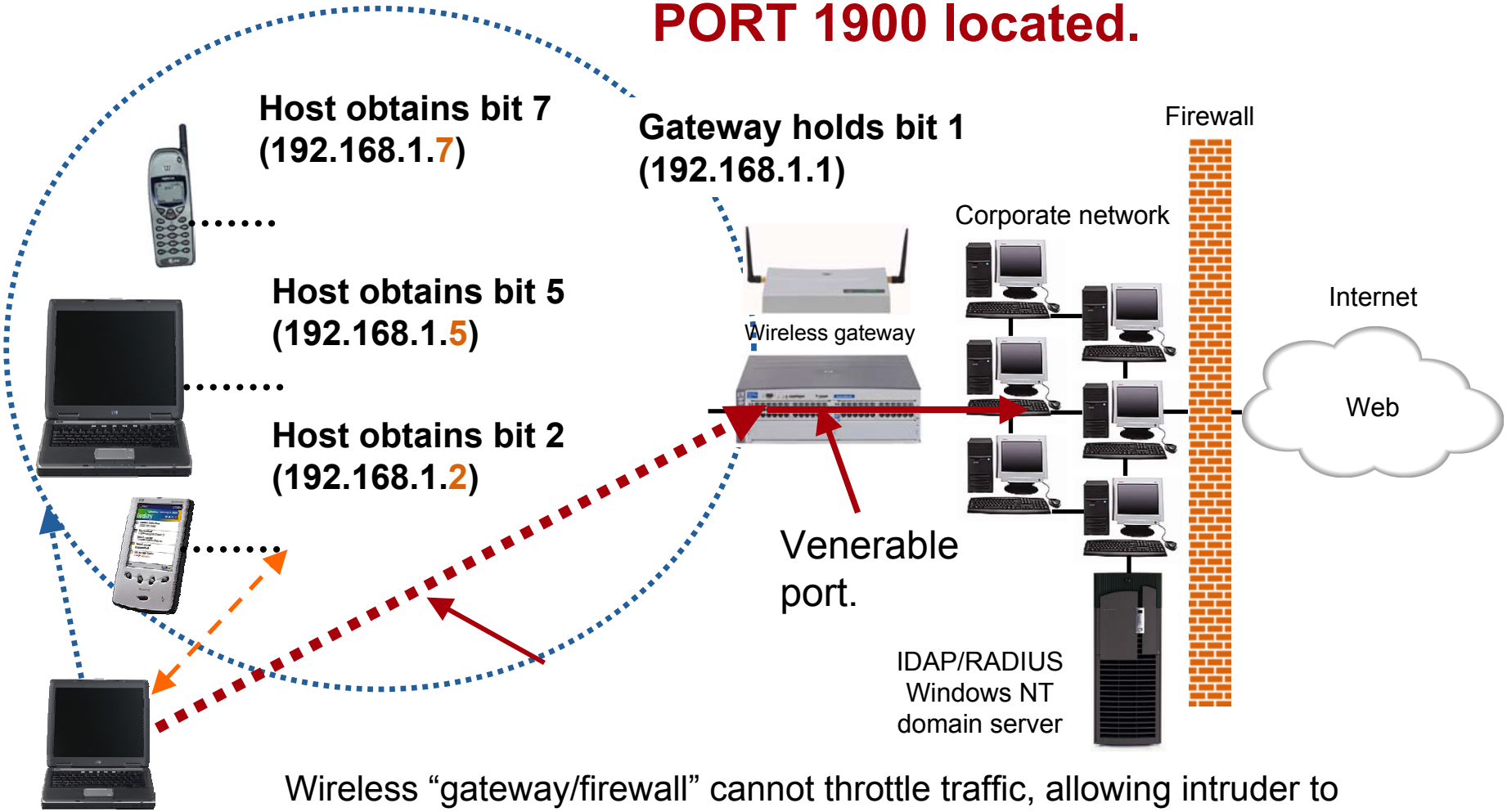


Case study 1: Single port based attack



Intruder uses a Land.c attack or a packet generator to hammer the single port of entry 192.168.0.1.

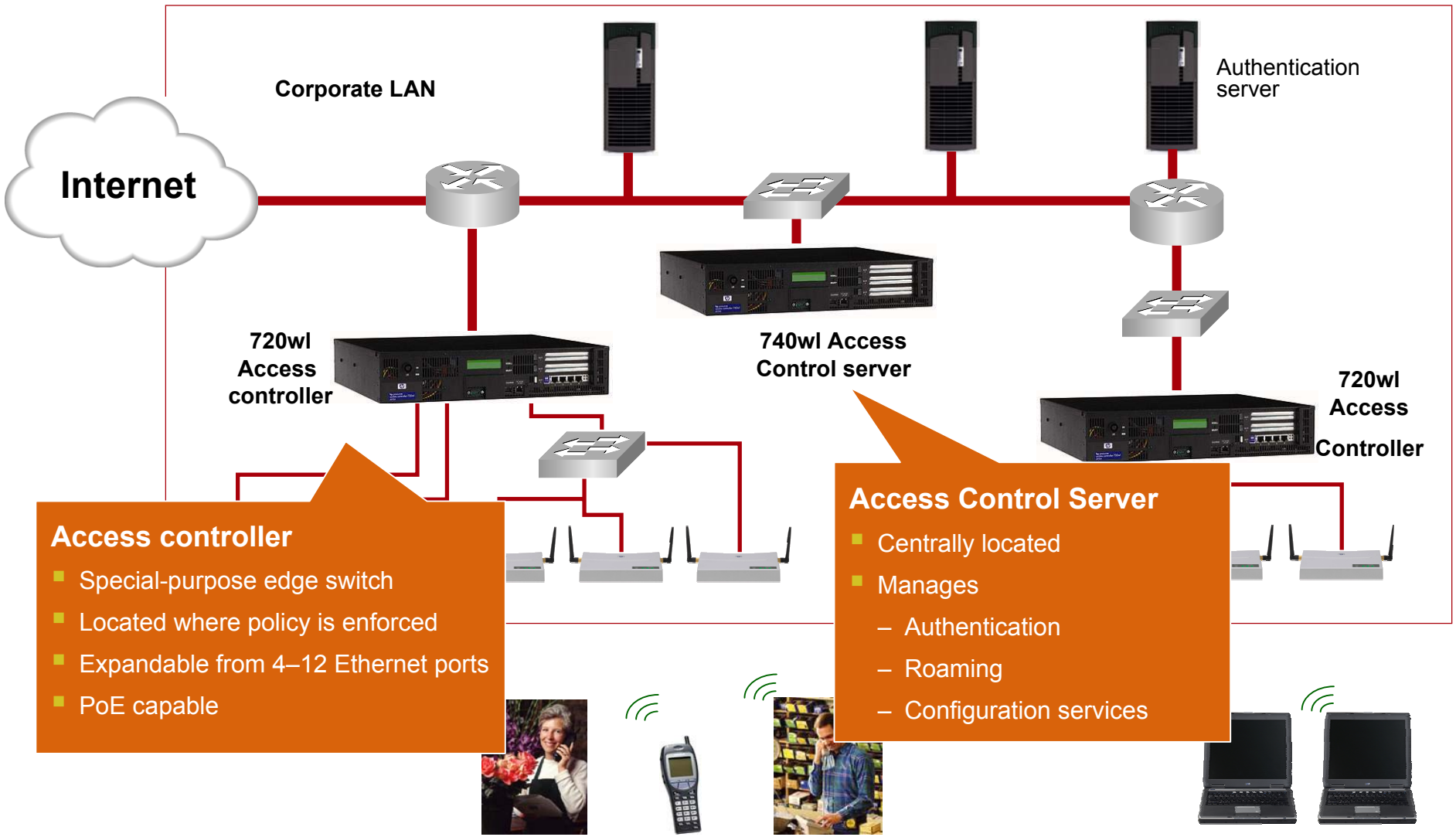
Case study 1: Single port based attack



Wireless “gateway/firewall” cannot throttle traffic, allowing intruder to run a proxy agent to enter the box on port 1900 (example), or to circumvent the security box.

HP ProCurve secured mobility

Distributed solution



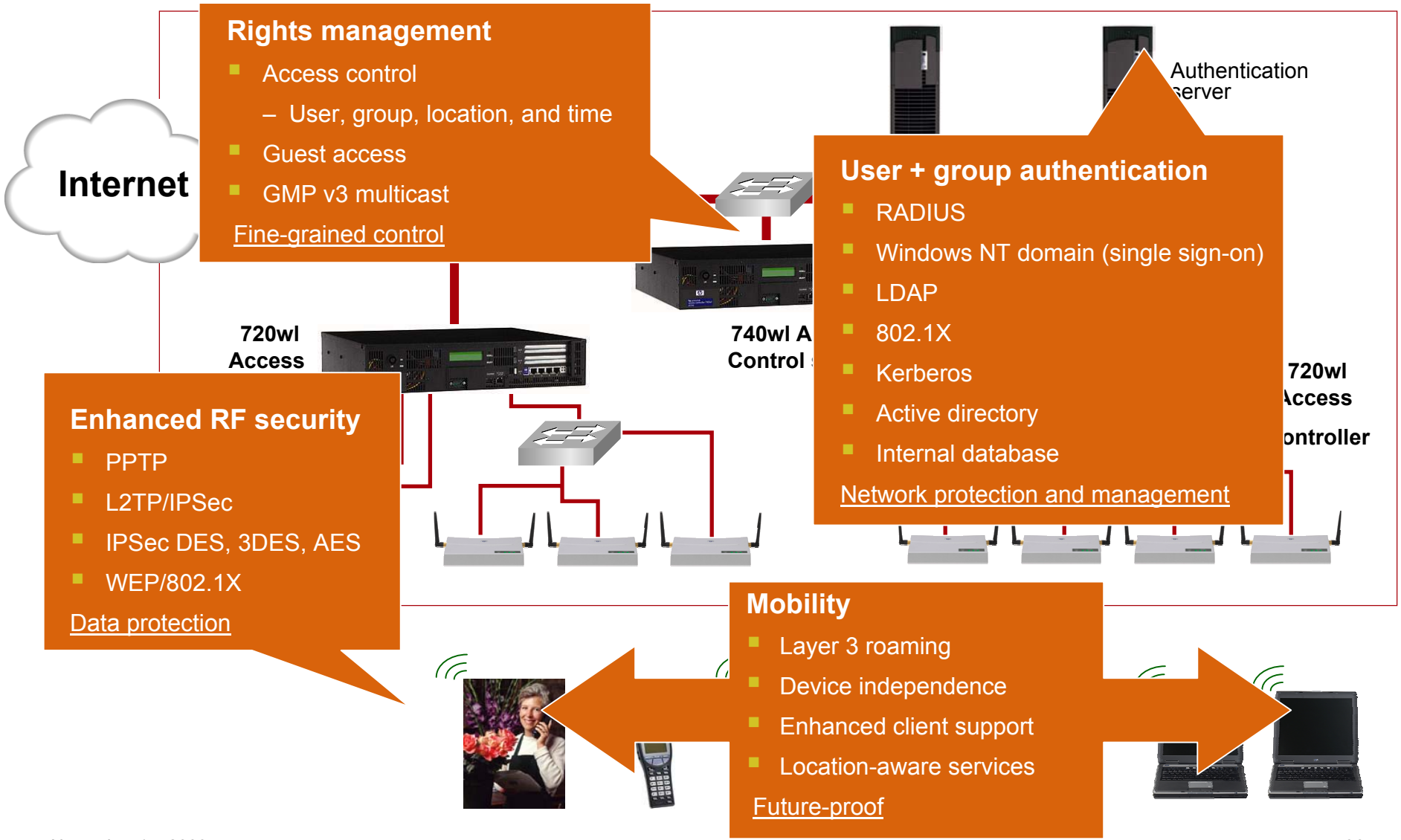
Access controller

- Special-purpose edge switch
- Located where policy is enforced
- Expandable from 4–12 Ethernet ports
- PoE capable

Access Control Server

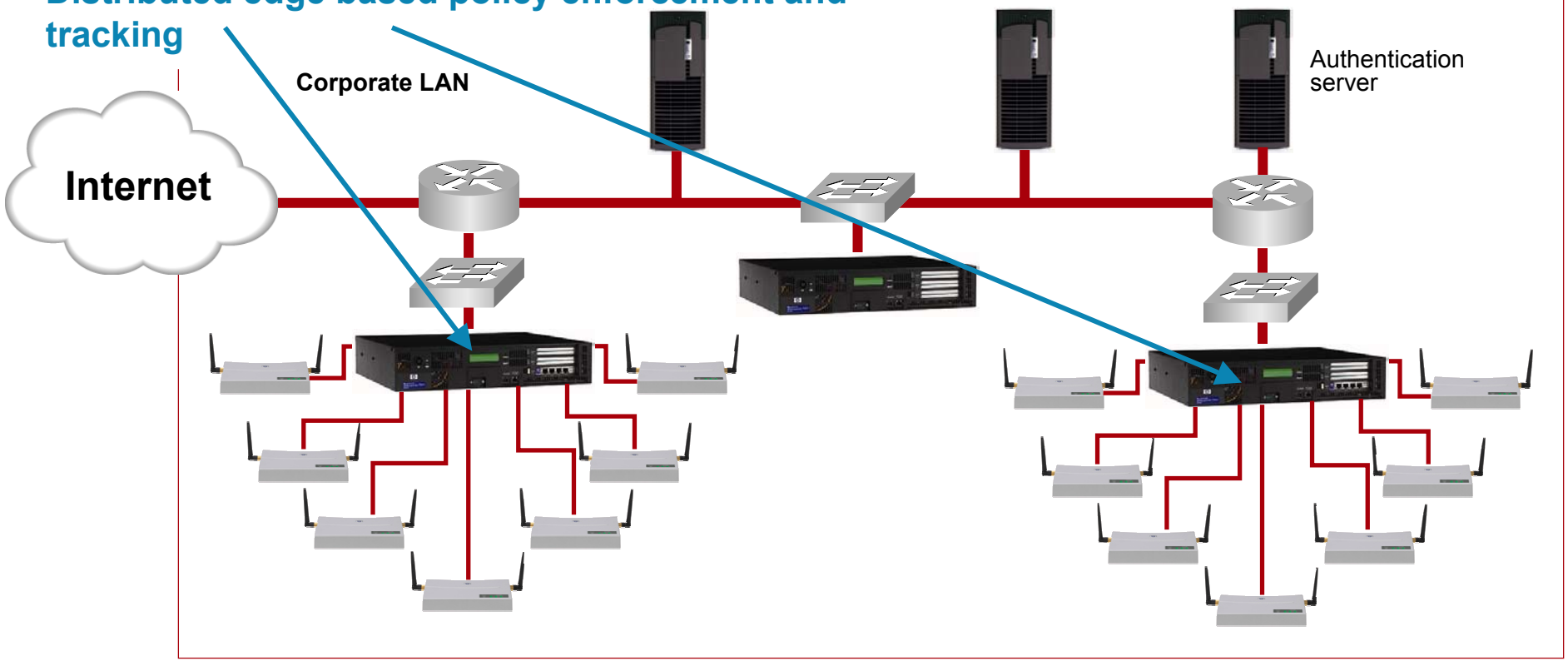
- Centrally located
- Manages
  - Authentication
  - Roaming
  - Configuration services

HP ProCurve enterprise WLAN distributed solution



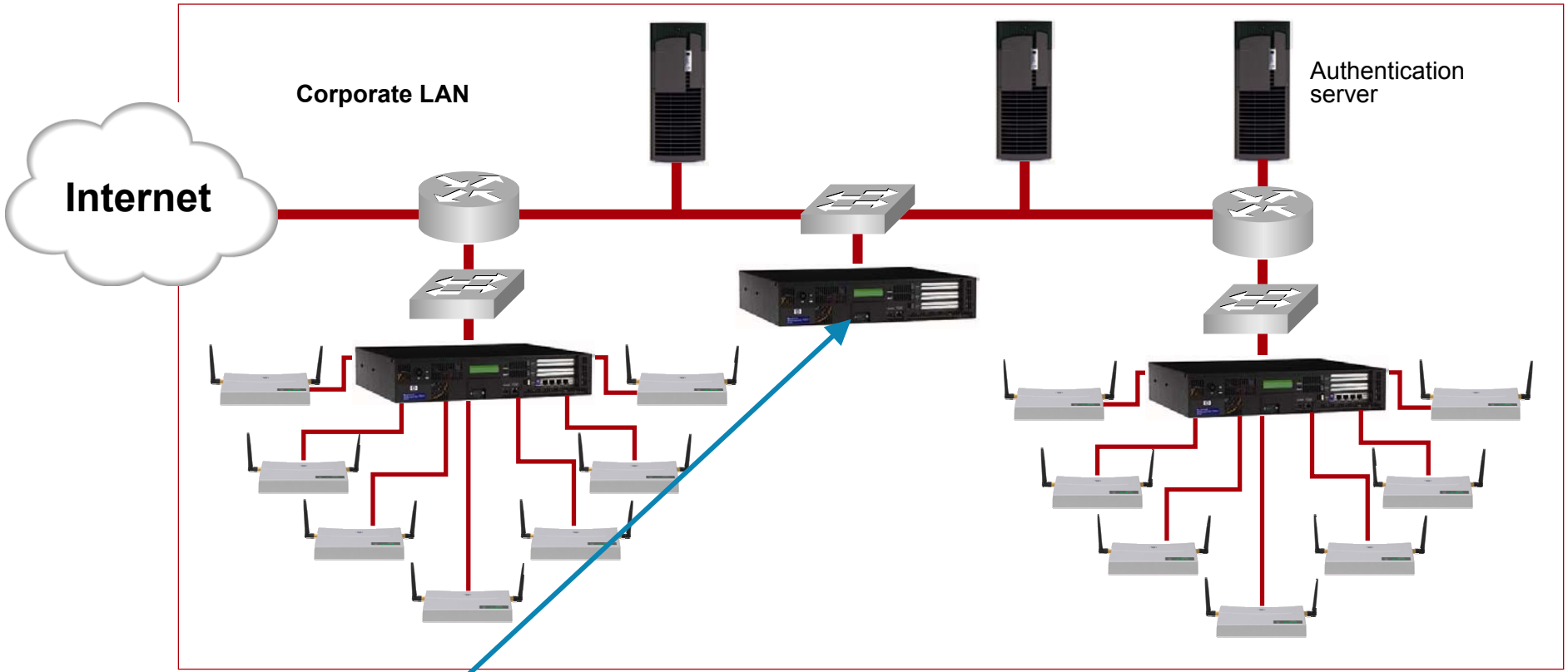
HP ProCurve secured mobility solution

Distributed edge based policy enforcement and tracking



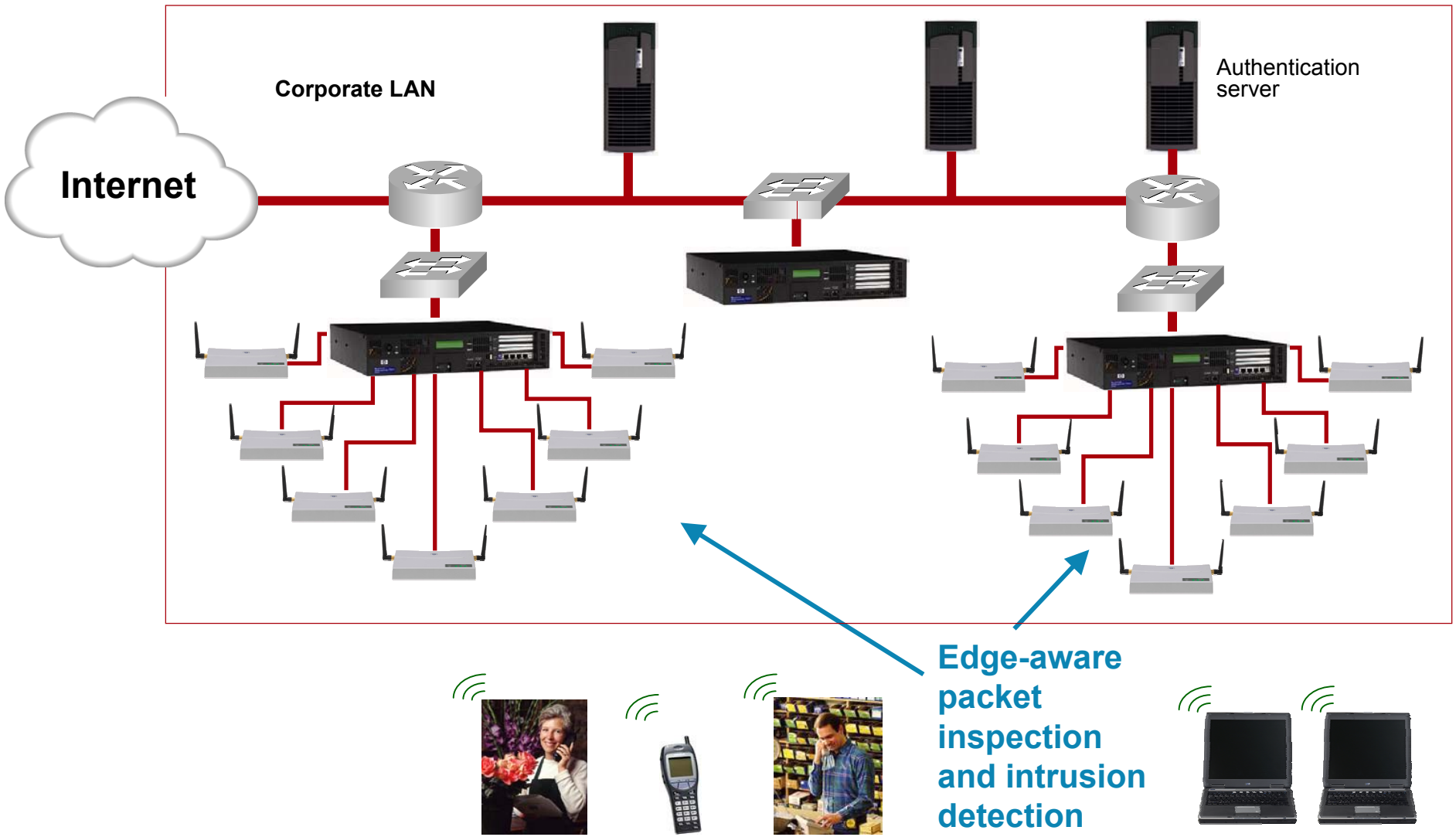
Layer 2-through-7
Active and dynamic packet control

HP ProCurve secured mobility solution

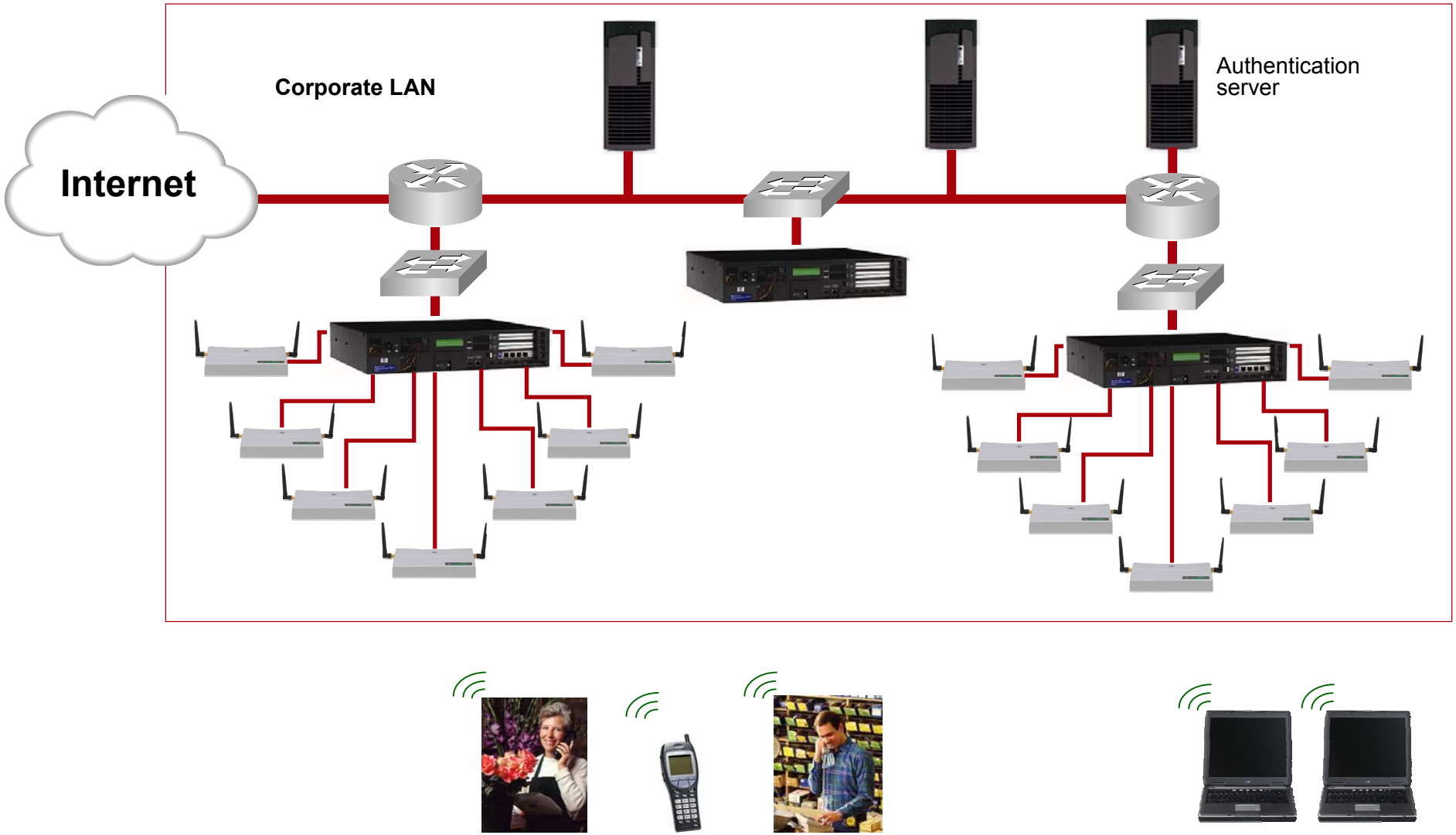


Central configuration, monitoring, and inspection

HP ProCurve scured mobility solution

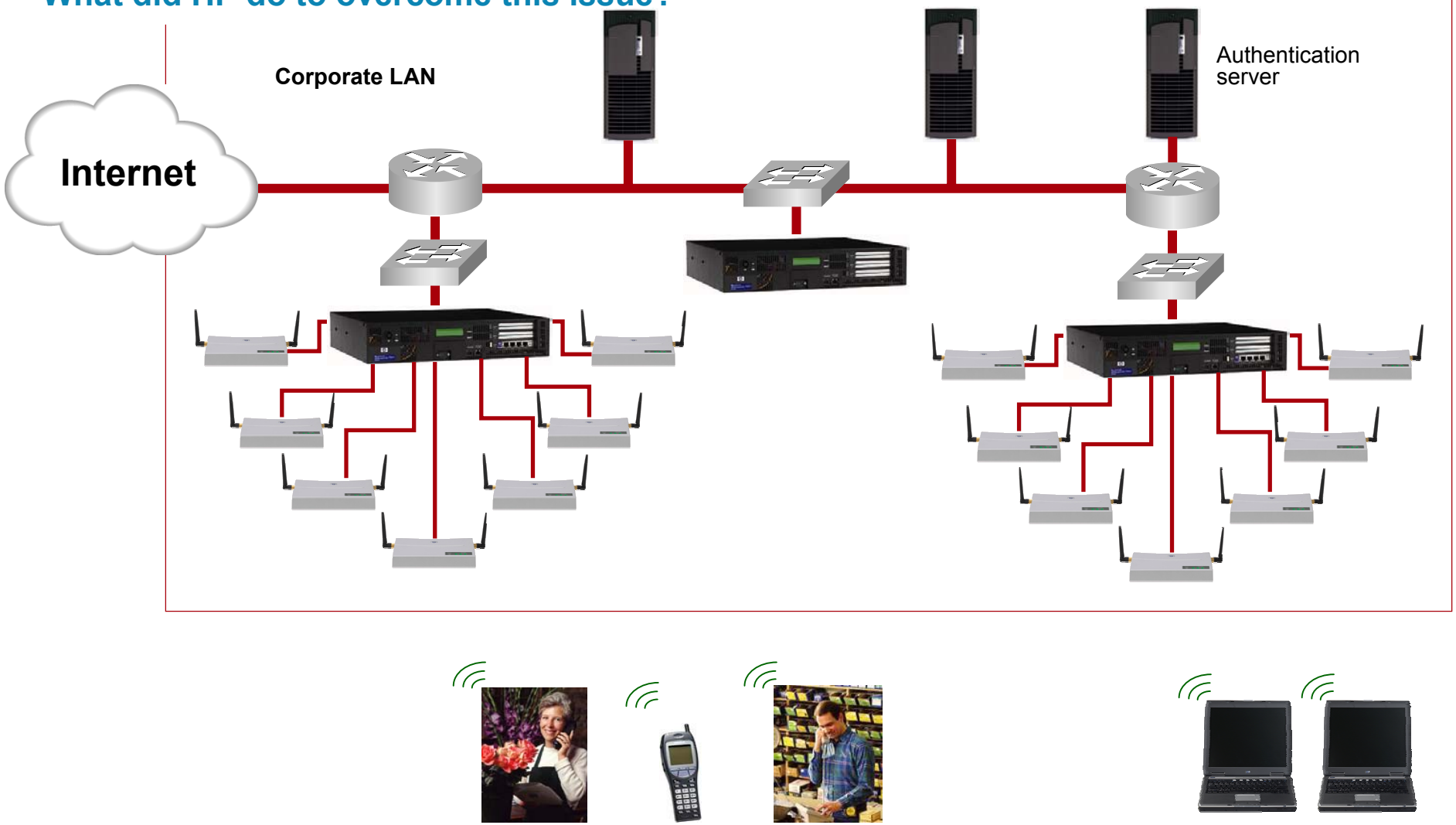


We know why one input/ output port is a bad idea



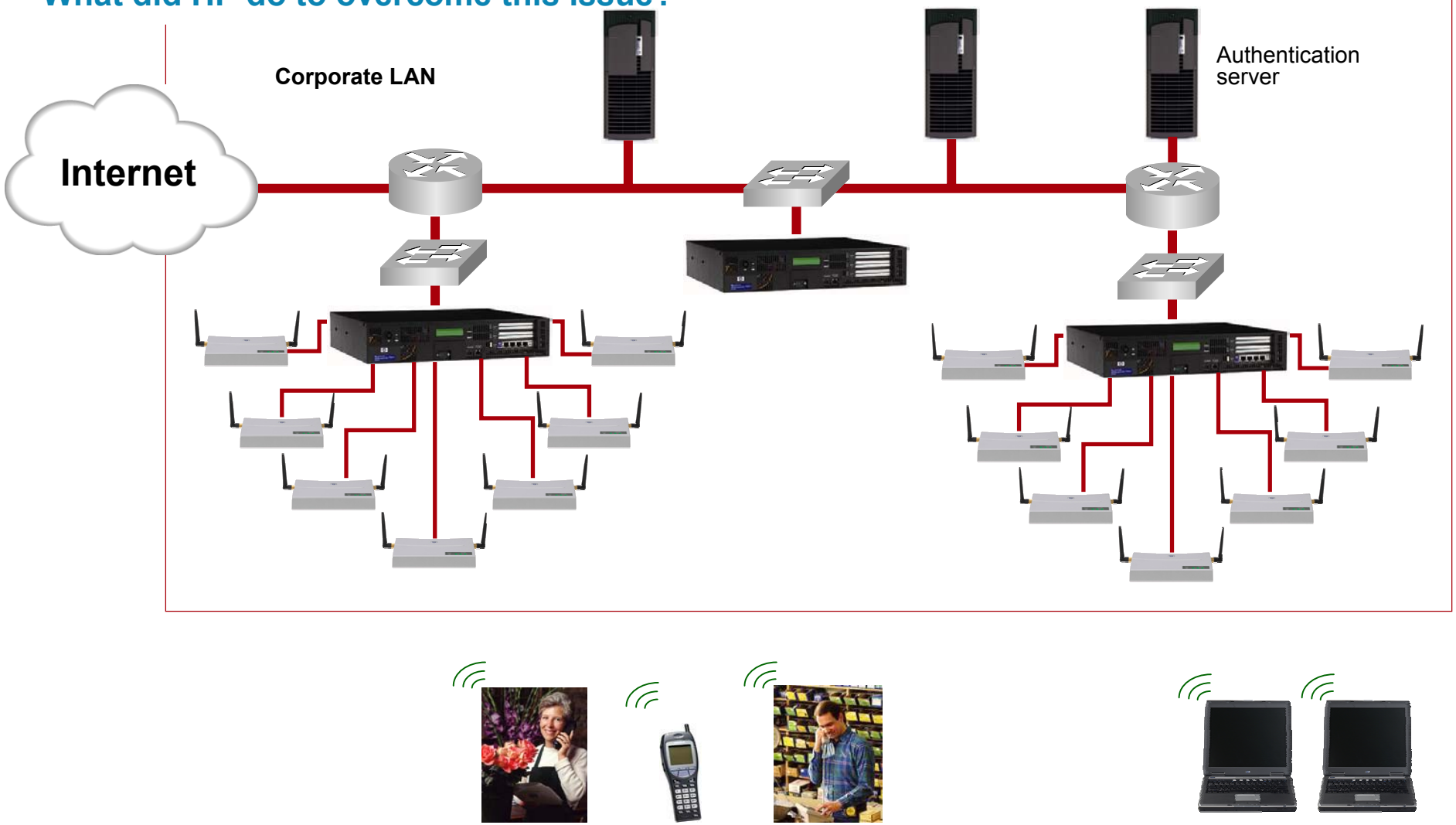
We know why one input/ output port is a bad idea

What did HP do to overcome this issue?

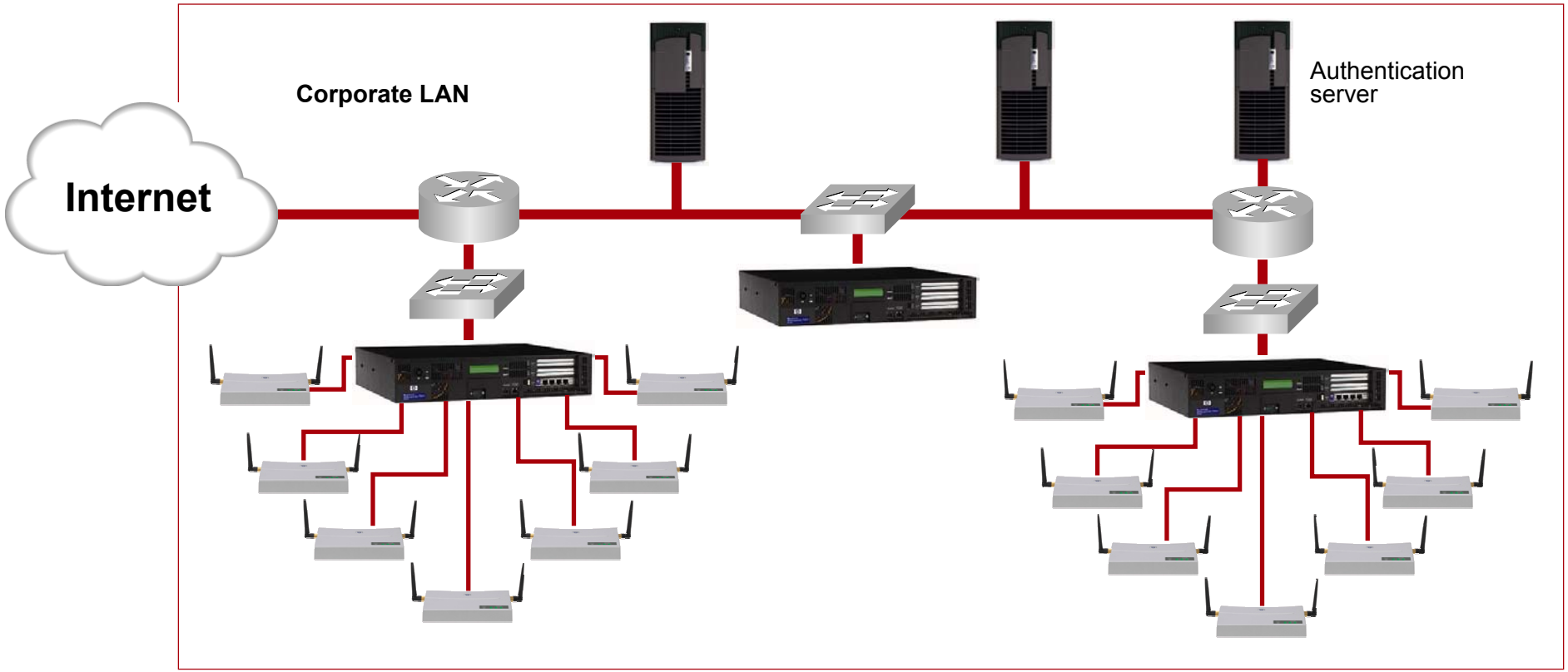


We know why one input/ output port is a bad idea

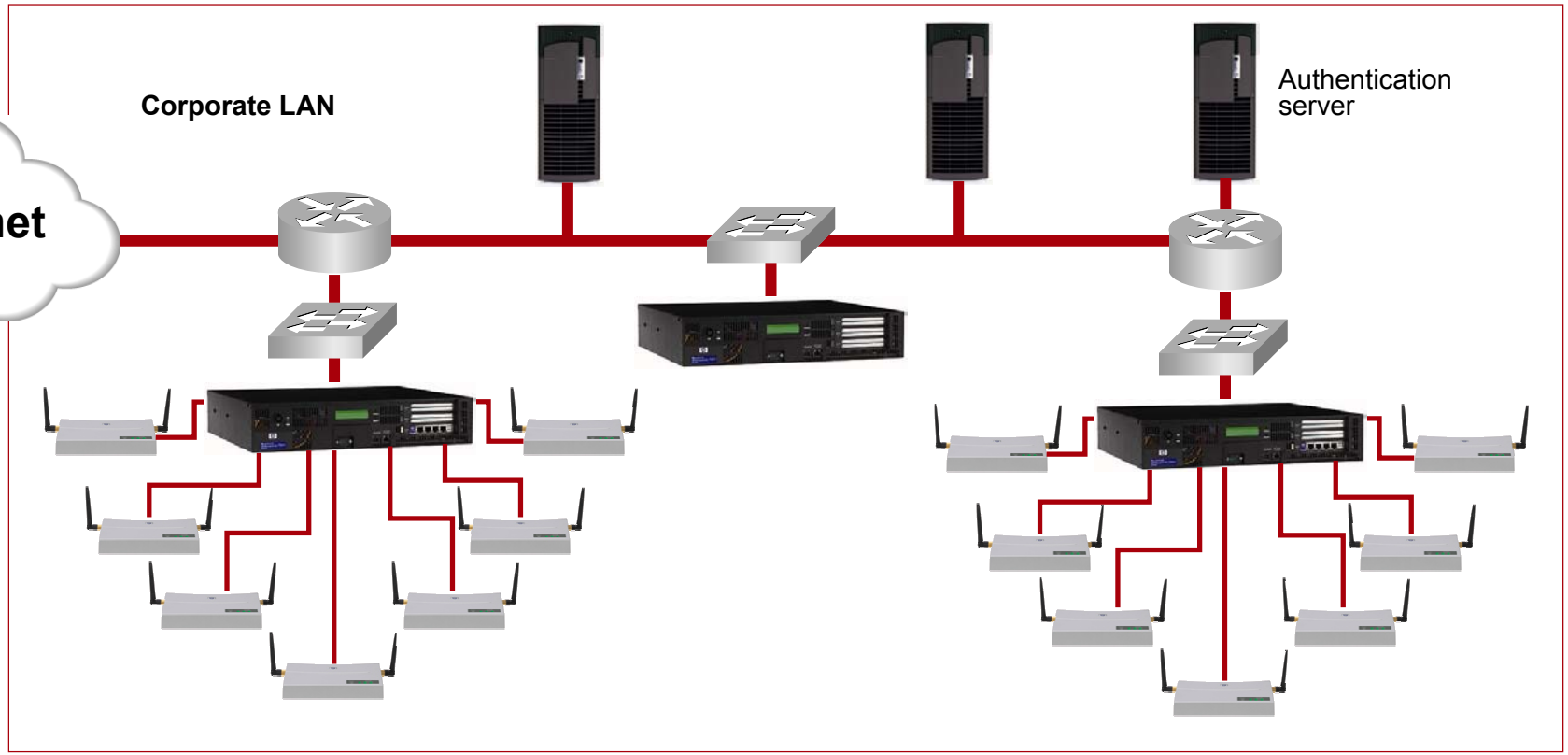
What did HP do to overcome this issue?



Case study 1: Single port based attack



Case study 1: Single port based attack

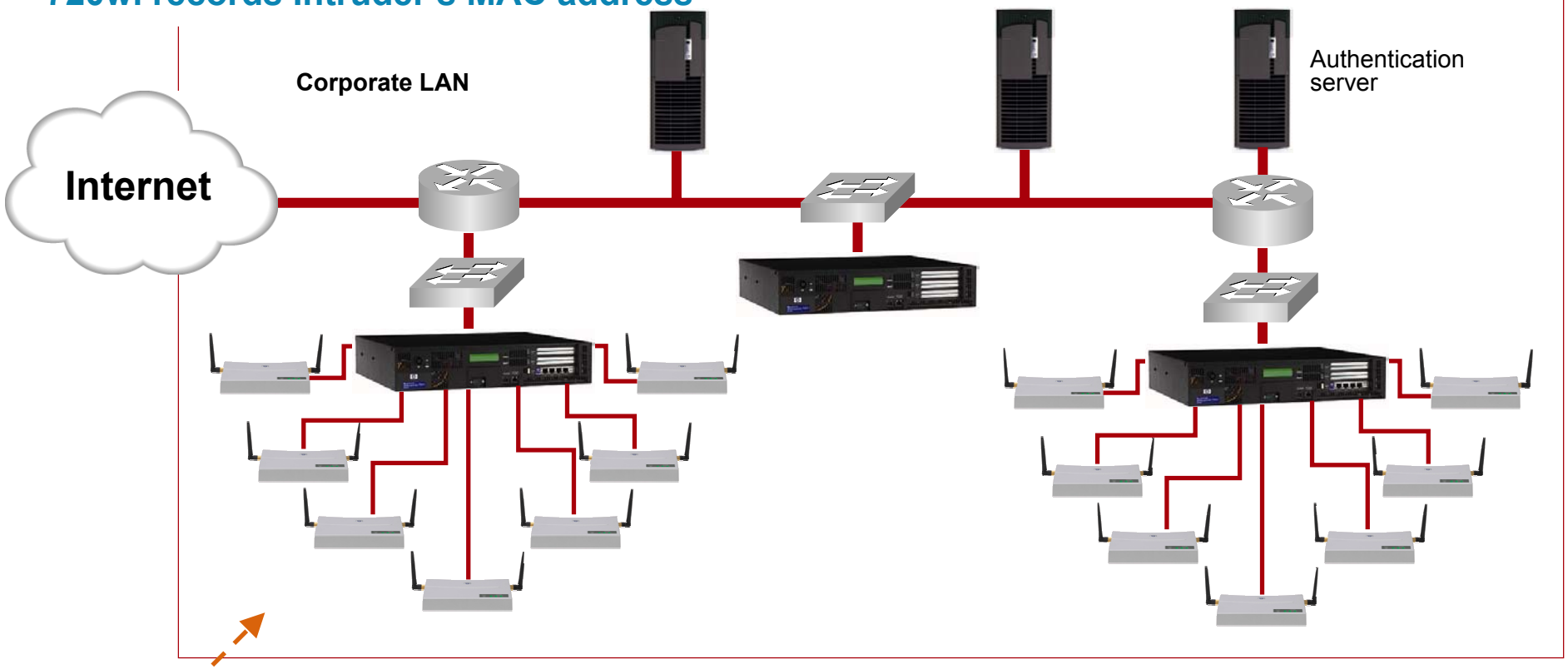


Intruder

Intruder appears.

Case study 1: Single port based attack

720wl records Intruder's MAC address

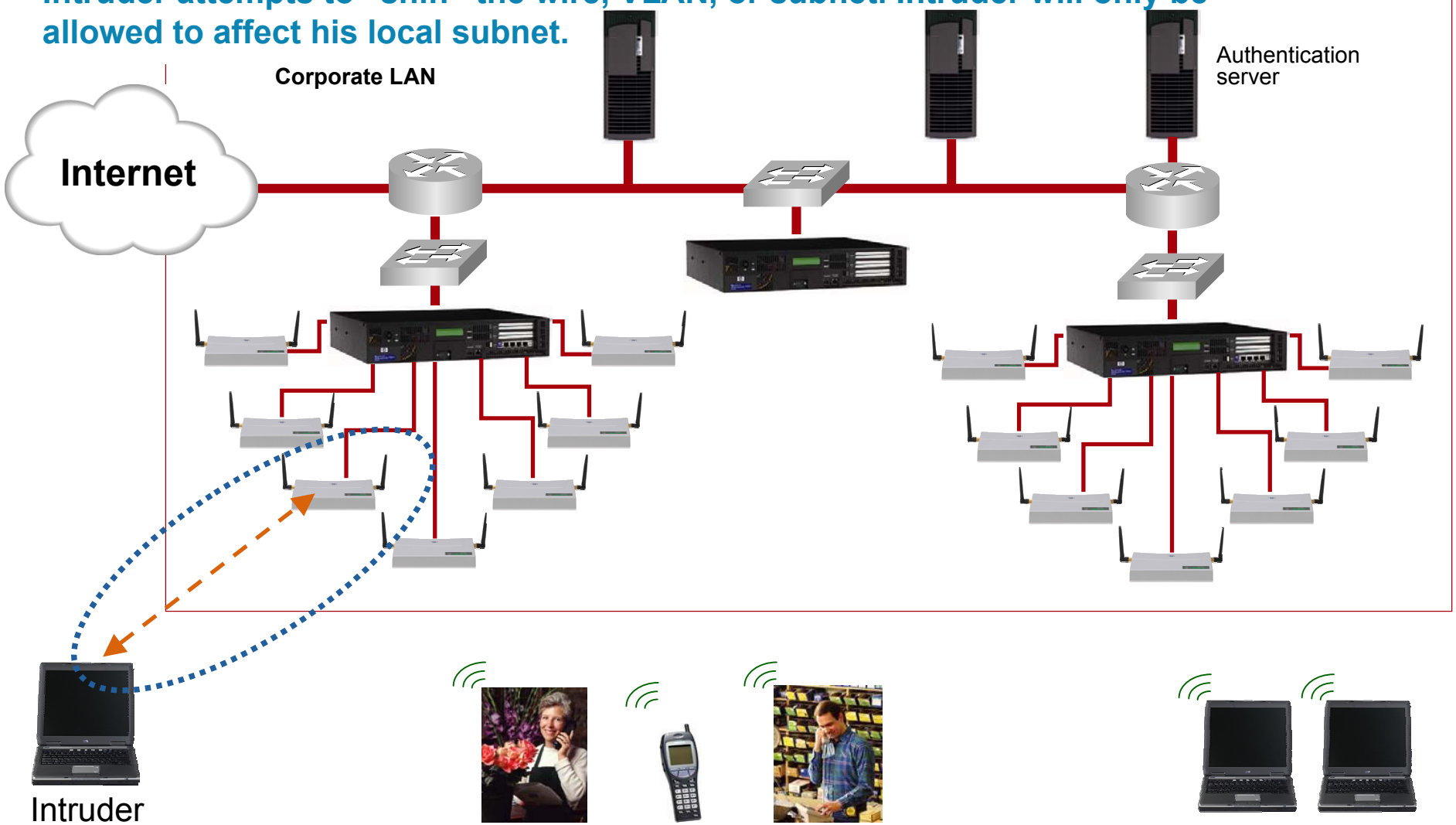


Intruder

Intruder associates to an access point.
(Air Magnet, Air Snort, Net Stumbler)

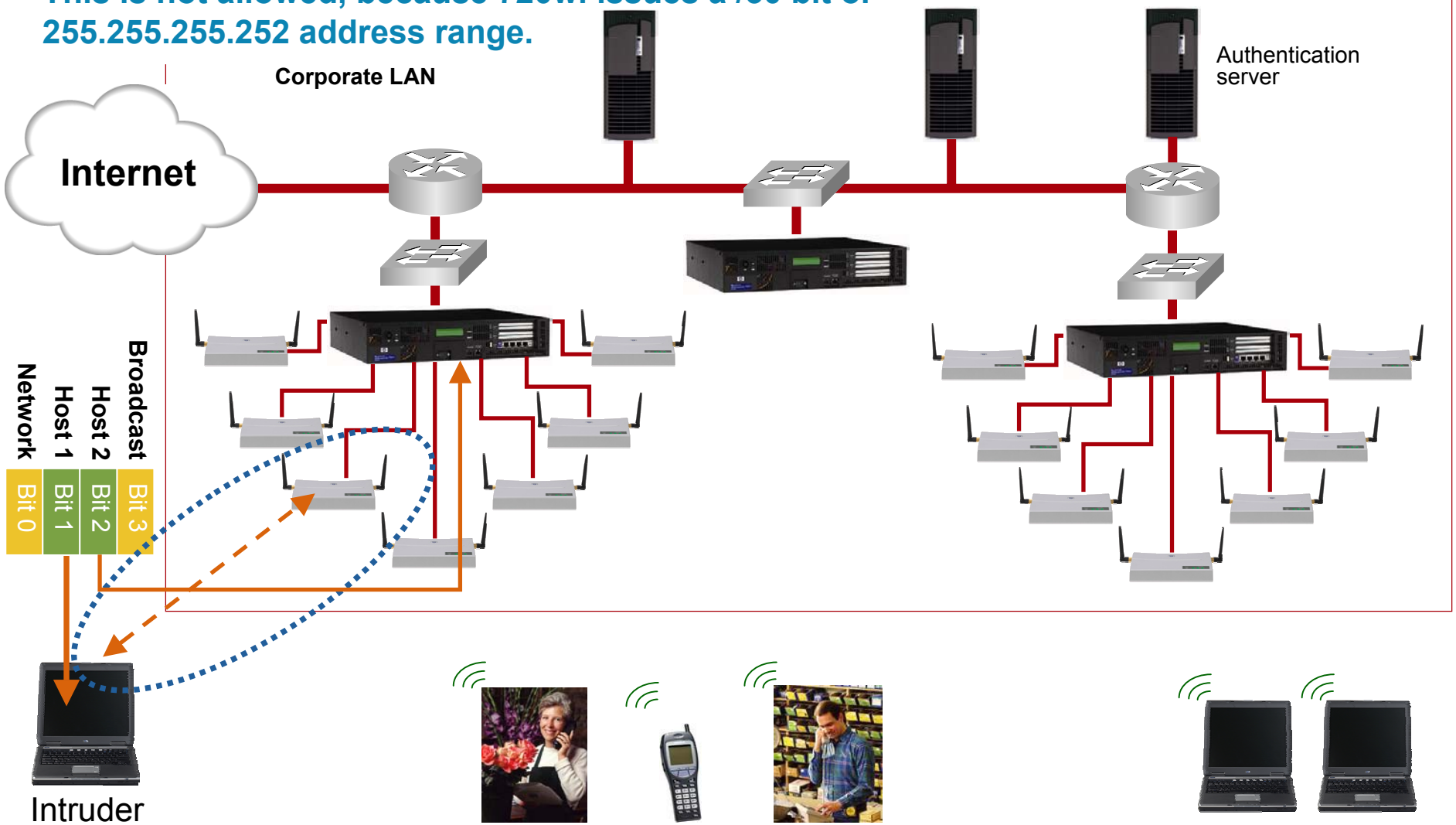
Case study 1: Single port based attack

Intruder attempts to "sniff" the wire, VLAN, or subnet. Intruder will only be allowed to affect his local subnet.



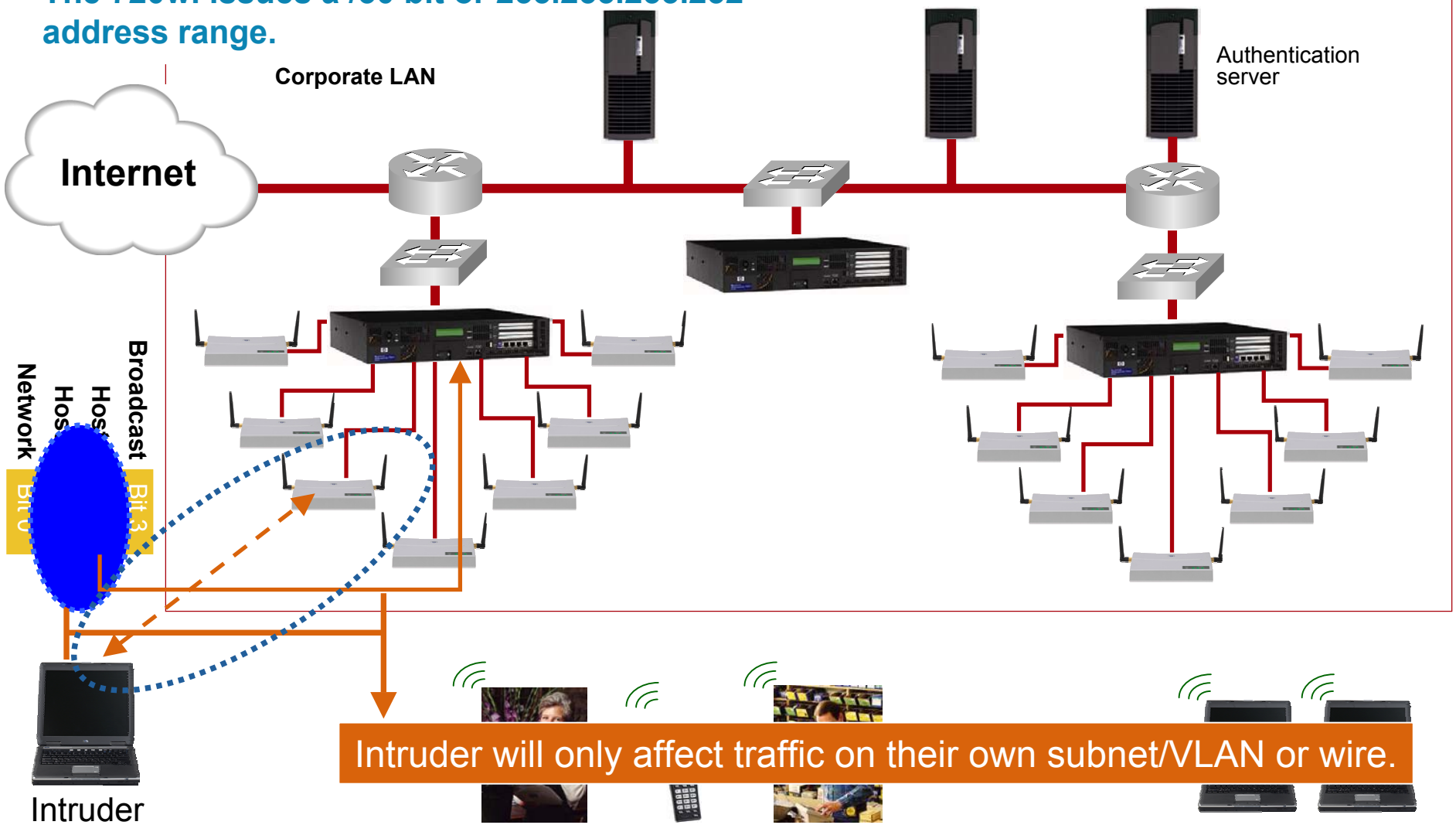
Case study 1: Single port based attack

This is not allowed, because 720wl issues a /30 bit or 255.255.255.252 address range.



Case study 1: Single port based attack

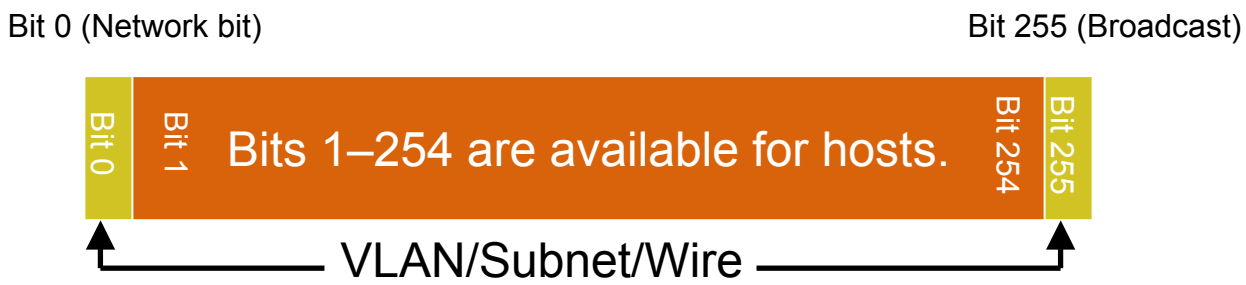
The 720wl issues a /30 bit or 255.255.255.252 address range.



Subnetting 101

Why a /30 bit address? What does this mean?

Traditionally, wireless products hand out a /24 bit or a 255.255.255.0 subnet.



Subnetting 101

Why a /30 bit address? What does this mean?

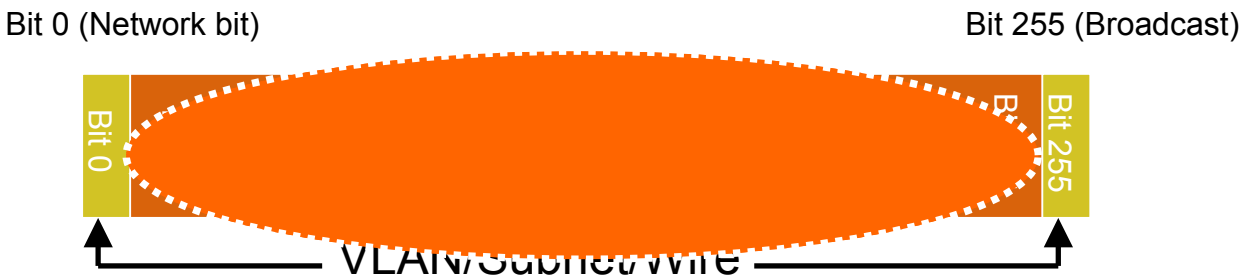
Traditionally, wireless products hand out a /24 bit or a 255.255.255.0 subnet.

- Allowing intruders the ability to attach to the network through extra network bits
- Once attached, they can sniff the subnet or broadcast domain, gaining access to network resources.

Subnetting 101

Why a /30 bit address? What does this mean?

Traditionally, wireless products hand out a /24 bit or a 255.255.255.0 subnet.



HP ProCurve 700wl series hands out a /30 or a 255.255.255.252 subnet.

Broadcast	Bit 3
Host 2	Bit 2
Host 1	Bit 1
Network	Bit 0

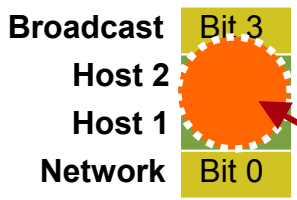
Subnetting 101

Why a /30 bit address? What does this mean?

Traditionally, wireless products hand out a /24 bit or a 255.255.255.0 subnet.

HP ProCurve 700wl series hands out a /30 or a 255.255.255.252 subnet.

253 points of attack and opportunity for intruders.

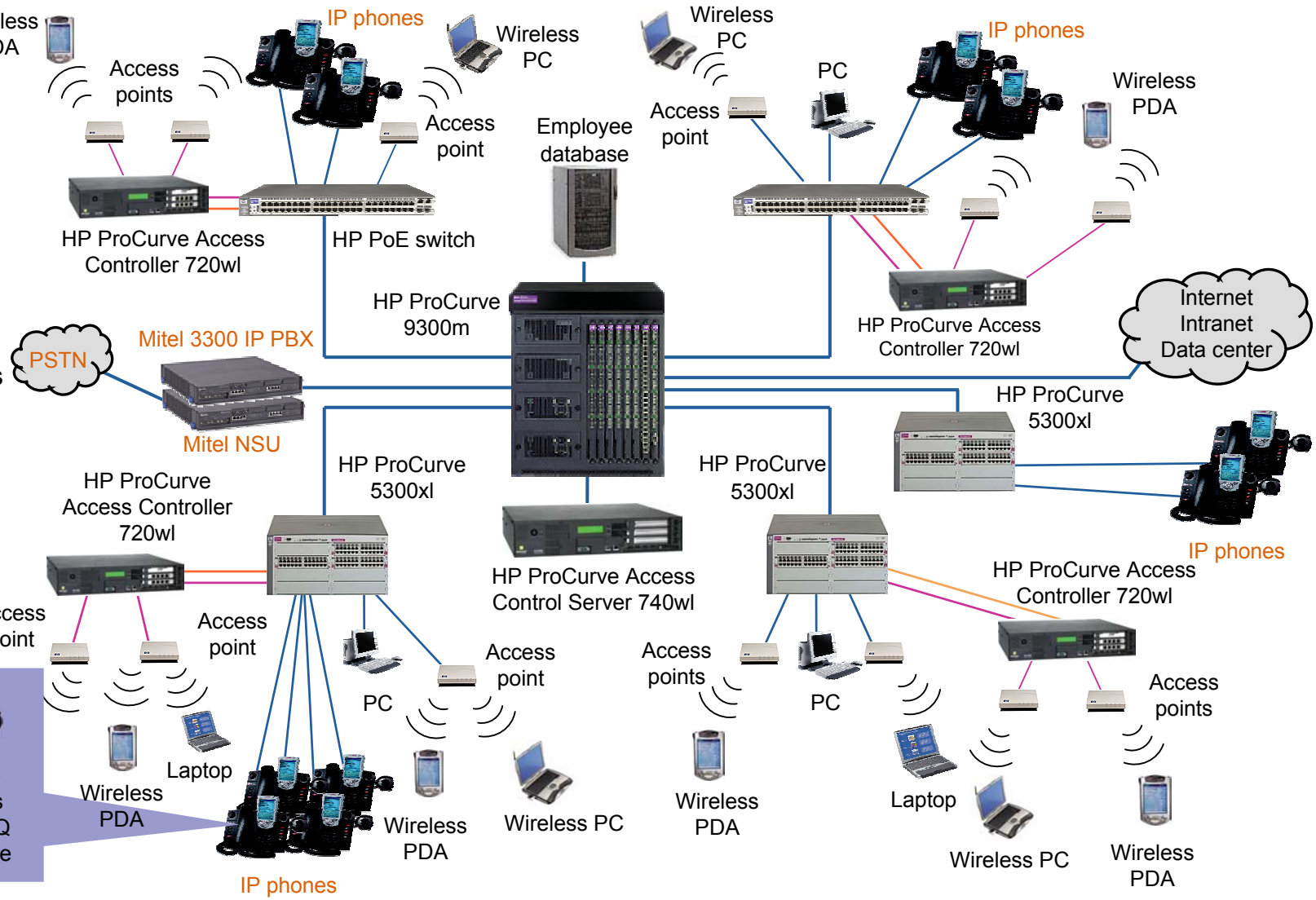


The 700 series provides 1 bit for the host/client and 1 bit for the Gateway/HP 700 series device.

Large enterprise campus network

Improved competitiveness and productivity **with VoIP deployment**

- Campus-wide Virtual Lobby support
- High security and continuous connection
- Seamless wireless roaming across multiple subnets without client software
- Campus-wide VoIP and VoWLAN



Enterprise scenario

Needs

- Safeguard network integrity
- Ensure privacy of wireless traffic
- Grant appropriate visitor access

HP ProCurve solution

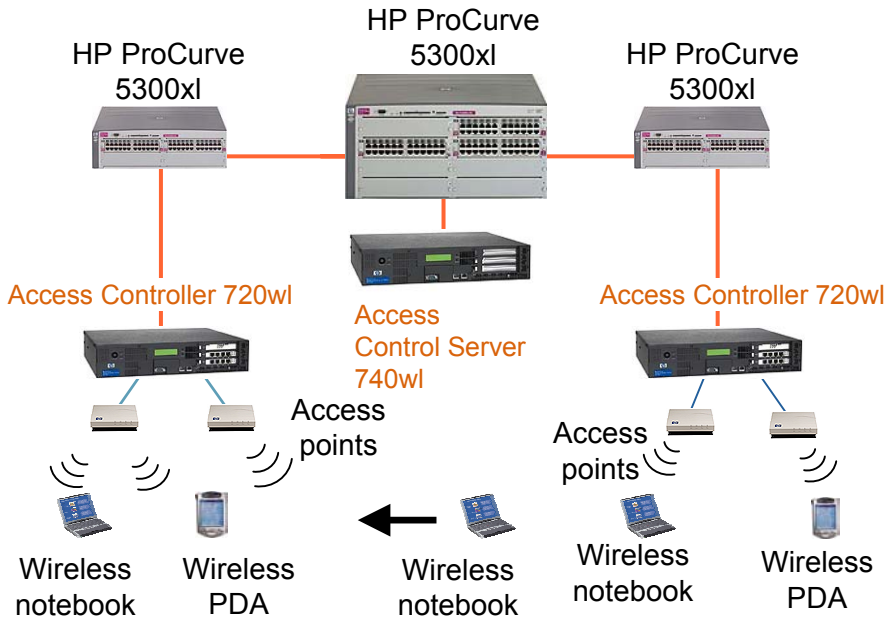
Access Control Server 740wl

- Offers centralized user authentication and policy rights management

Access Controller 720wl

- Enforces user policy rights, security, and roaming

HP ProCurve Wireless Access Points or non-HP access points



Deployment configuration

- Uses VPN client native in OS to authenticate employee and secure wireless traffic
- Visitors granted Internet access through HTTP redirect to logon page
- Uninterrupted roaming across subnets

Education scenario

Needs

- Wireless in the classroom
- Notebooks or PDAs for interactive learning

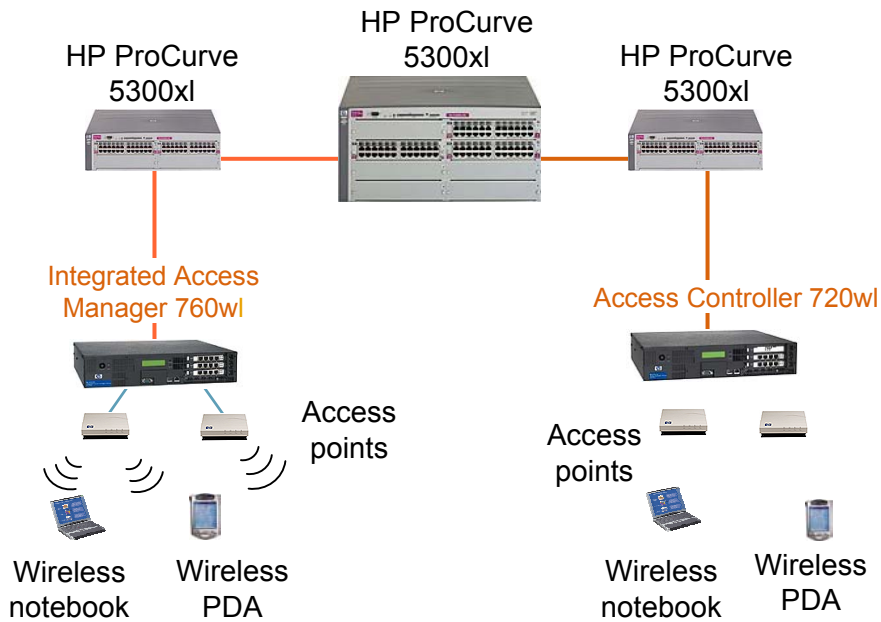
HP ProCurve solution

Integrated Access Manager 760wl

- HP ProCurve wireless combines the functionality of the Access Control Server and Access Controller

HP ProCurve Wireless Access Points or non-HP access points

Can expand wireless coverage with additional Access Controllers



Deployment configuration

- All network users are granted Internet access through HTTP redirect to logon page
- VPN session used to authenticate teacher and secure wireless traffic with unrestricted network access

Higher-education scenario

Need

- Wireless LAN to extend network access into common areas and classrooms

HP ProCurve solution

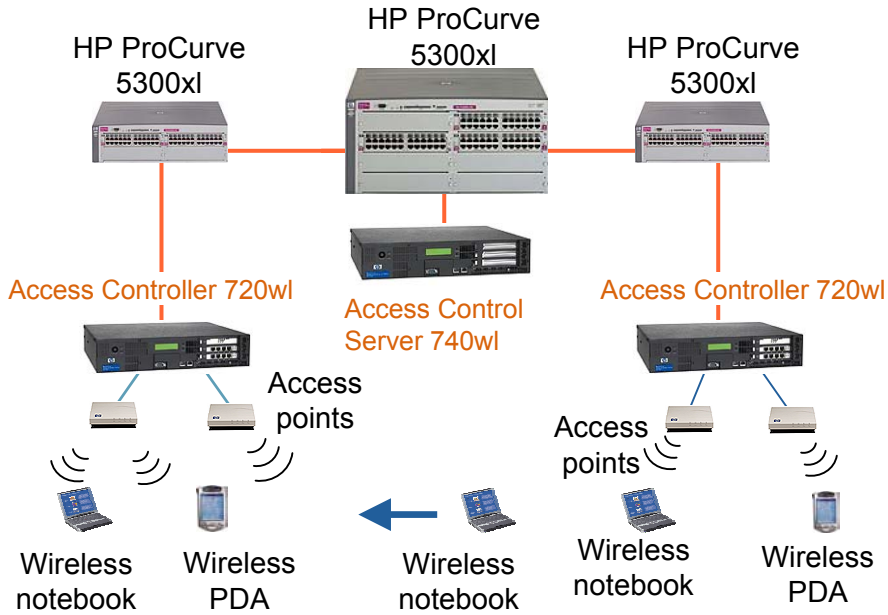
Access Control Server 740wl

- Offers centralized user authentication and policy rights management

Access Controller 720wl

- Enforces user policy rights, security, and roaming

HP ProCurve Wireless Access Points or non-HP access points



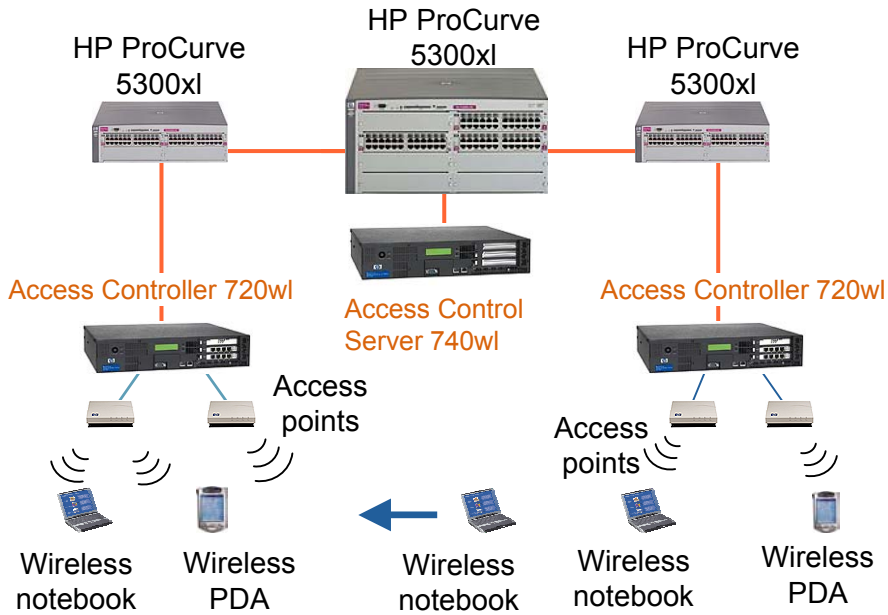
Deployment configuration

- All users to the network are granted Internet access through HTTP redirect to logon page
- VPN session used to authenticate student or teacher
- VPN sessions secure the wireless traffic
- All other access attempts are denied

Healthcare scenario

Needs

- Wireless LAN network for real-time access to patient data, prescribed medication—at bedside



HP ProCurve solution

Access Control Server 740wl

- Offers centralized user authentication and policy rights management

Access Controller 720wl

- Enforces user policy rights, security, and roaming

HP ProCurve Wireless Access Points or non-HP access points

Deployment configuration

- Secure VPN session used to authenticate healthcare provider, secure wireless traffic
- User policy rights restrict access to specific application databases
- Enable secure roaming across subnets

HP ProCurve Secure Access 700wl Series solutions meet your needs

- Secure mobility based on industry standards
- Robust access control and authentication
- Secure roaming and application persistence
- Professional network design and integration services

Interex, Encompass and HP bring you a powerful new HP World.