



# Cisco Catalyst 3560 Series Switches



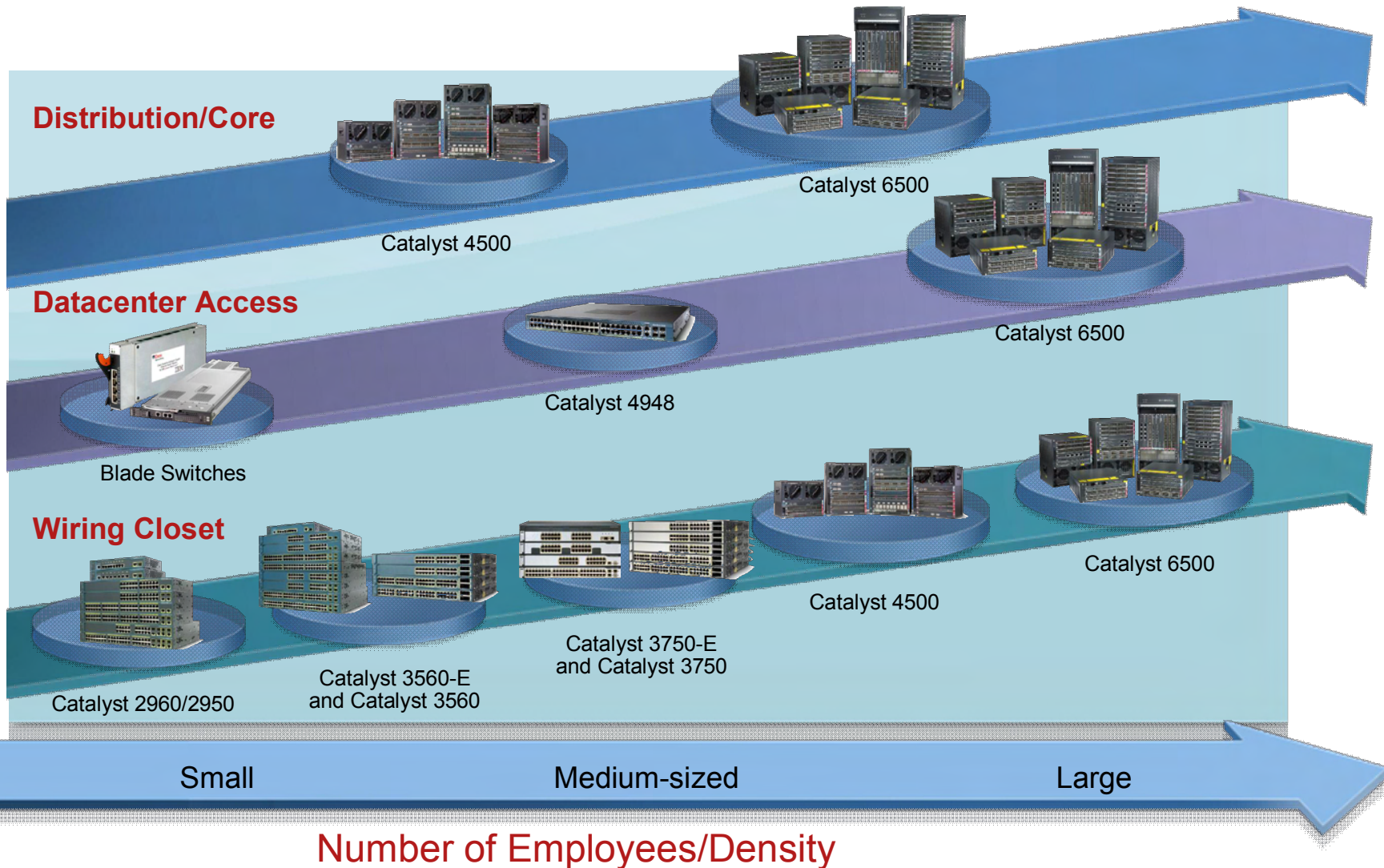
# Agenda



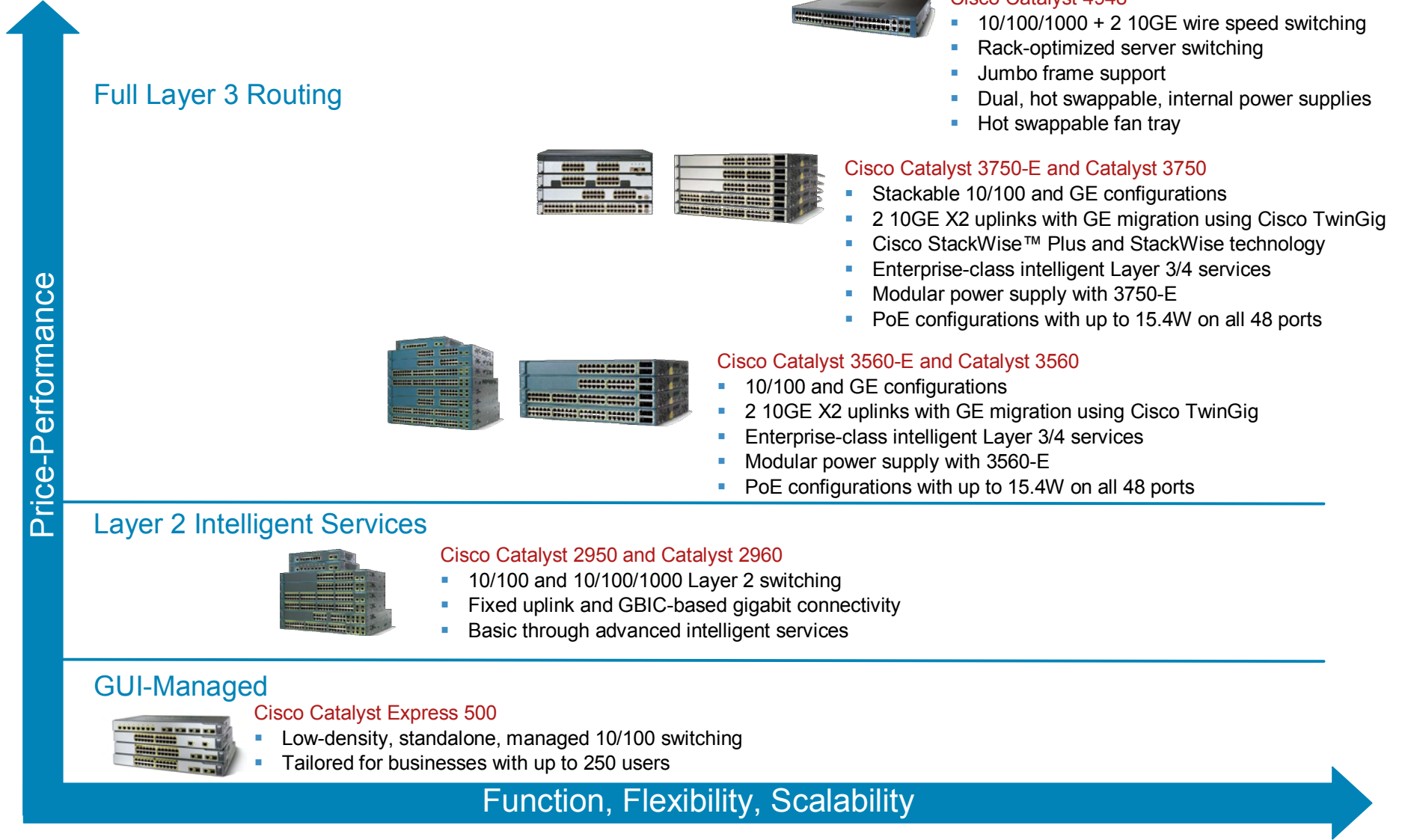
- Cisco® Catalyst® Switches Overview
- Catalyst 3560 Product Overview
- Power over Ethernet
- Intelligent Services
- Cisco Network Assistant
- Deployment Examples
- Service and Support

# Catalyst Switching Portfolio

Features, Scalability, Longevity



# Most Complete Line of Fixed Configuration LAN Products



# Agenda



- Cisco® Catalyst® Switches Overview
- Catalyst 3560 Product Overview
- Power over Ethernet
- Intelligent Services
- Cisco Network Assistant
- Deployment Examples
- Service and Support



# Cisco Catalyst 3560 Series Switches

## Positioning

- Enterprise-class, fixed configuration, multilayer switching line optimized for access layer deployments requiring IEEE 802.3af or Cisco® prestandard Power over Ethernet
  - Fast Ethernet and Gigabit to the desktop configurations
  - Ideal for small enterprise wiring closets and branch office environments
- Enables the deployment of network-wide intelligent services
  - Availability
  - Enhanced security
  - Advanced quality of service (QoS)
- Intelligent power management features enhance PoE capabilities
- New Express Setup and Cisco Network Assistant software supports easy deployment and configuration
- Familiar Cisco IOS® Software
- Uses Cisco ASICs for superior hardware and software integration, and innovative features

# Catalyst 3560 Series

## Product Overview

- Enterprise-class services
  - Availability: IP Routing, HSRP, STP enhancements, 802.1s/w, IGMP snooping
  - Security: ACLs, port security, 802.1x (IBNS), SSH, SNMPv3, ACLs, RADIUS/TACACS+, DHCP snooping, Dynamic ARP inspection, IP source Guard
  - Advanced QoS: L2-L4 QoS with CoS/DSCP, Shaped Round Robin, Strict Priority Queuing, Auto-QoS for VoIP
  - IPv6 hardware capability
  - GE & FE configurations—Performance up to 38.7Mpps routing & switching
- Power over Ethernet
  - Ability to support both Cisco prestandard PoE and IEEE 802.3af
  - Intelligent power management features maximize and prioritize available power
- Ease of deployment and management
  - Web-based Express Setup simplifies initial configuration
  - Cisco Network Assistant configuration wizards simplify configuration of Layer 3/4 services
  - Boots as a traditional Layer 2 Catalyst switch, configurable for Layer 3 routing and services
  - Auto-configuration through DHCP
- Small form factor pluggable (SFP) uplinks
  - SX, LX, ZX, 1000BaseT, CWDM options

# Cisco Catalyst 3560 Series Model Overview

## Catalyst 3560-8PC



- 8 10/100 + 1 dual purpose 10/100/1000 & SFP port
- 124W PoE

## Three Software Licenses

### IP Base Software License

- Enterprise-class intelligent services: advanced QoS, enhanced security, RIP, and static IP routing

### IP Services Software License

- IP Base feature set plus: dynamic IP unicast routing, smart multicast routing, and PBR

### Advanced IP Services License

- Adds IPv6 routing and ACLs

## Catalyst 3560-24TS



- 24 10/100 + 2 SFP ports

## Catalyst 3560-24PS



- 24 10/100 + 2 SFP ports
- 370W PoE

## Catalyst 3560G-24TS



- 24 10/100/1000 + 4 SFP

## Catalyst 3560G-24PS



- 24 10/100/1000 + 4 SFP
- 370W PoE

## Catalyst 3560-48TS



- 48 10/100 + 4 SFP ports

## Catalyst 3560-48PS



- 48 10/100 + 4 SFP ports
- 370W PoE

## Catalyst 3560G-48TS



- 48 10/100/1000 + 4 SFP

## Catalyst 3560G-48PS



- 48 10/100/1000 + 4 SFP
- 370W PoE

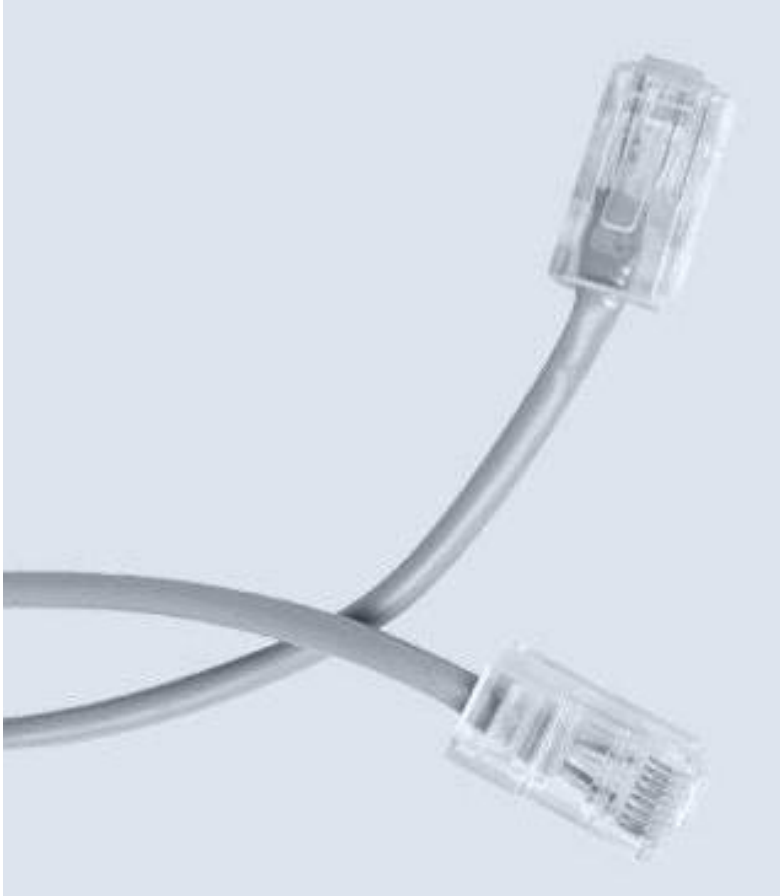


# Agenda



- Cisco® Catalyst® Switches Overview
- Catalyst 3560 Product Overview
- Power over Ethernet
- Intelligent Services
- Cisco Network Assistant
- Deployment Examples
- Service and Support

# What is Power over Ethernet?

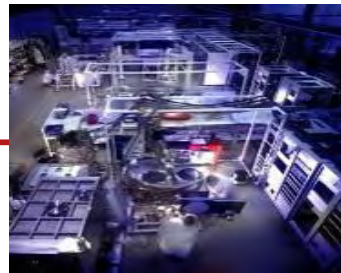


- Power over Ethernet (PoE) is the ability to deliver regulated—48V DC power over a standard copper Ethernet network cable
- This power is utilized by connected devices for their operation

# Extending the Versatility of Ethernet

## The Benefits of Powering Devices with Ethernet

**Power over Ethernet extends the value, simplicity and flexibility of Ethernet to enable new uses for the network**



- AC-Free Deployments
- Mobility and Simplicity
- Safety
- Operational Resiliency
- Simplified Manageability
- Reduced Capex and Opex

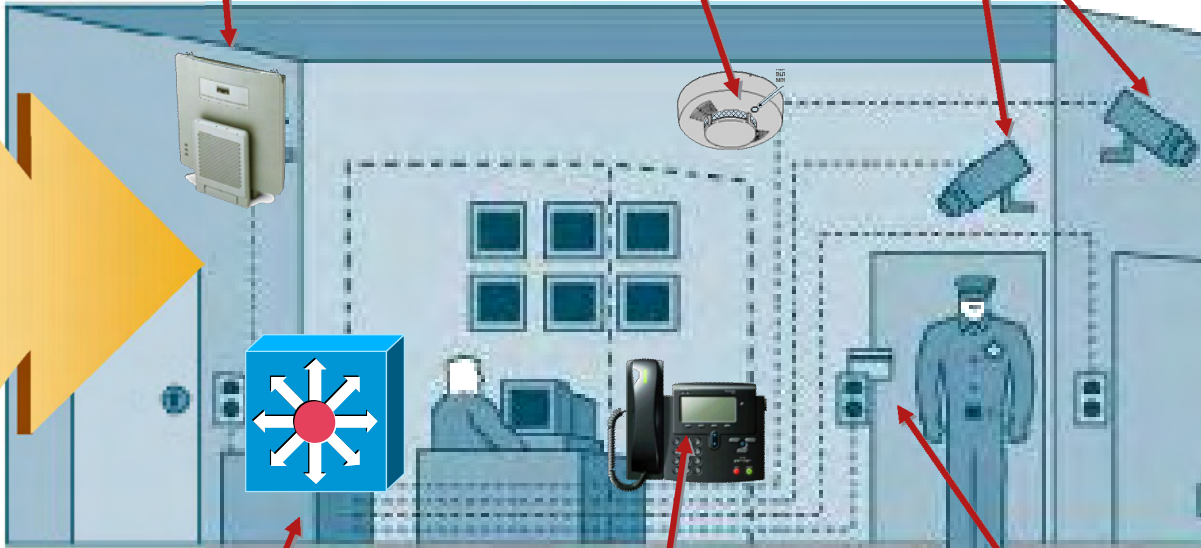
# A Glimpse into the Future...

## The Ethernet Powered Organization

**Wireless Access Points**

**Fire Protection**

**IP Integrated Video Surveillance**

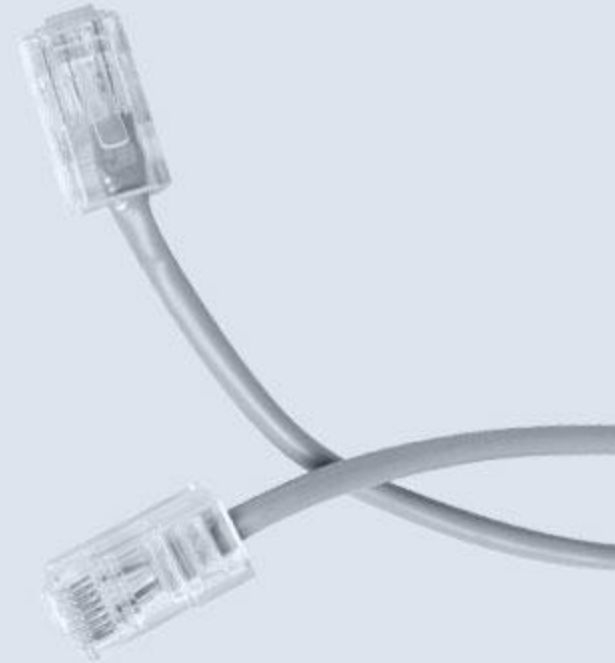


**Resilient, Available IP Network with Scalable Power Delivery**

**Powered IP Telephone**

**Building Access Control**

Power over Ethernet (PoE) Delivers 48V DC Power over a Standard Copper Ethernet Cable

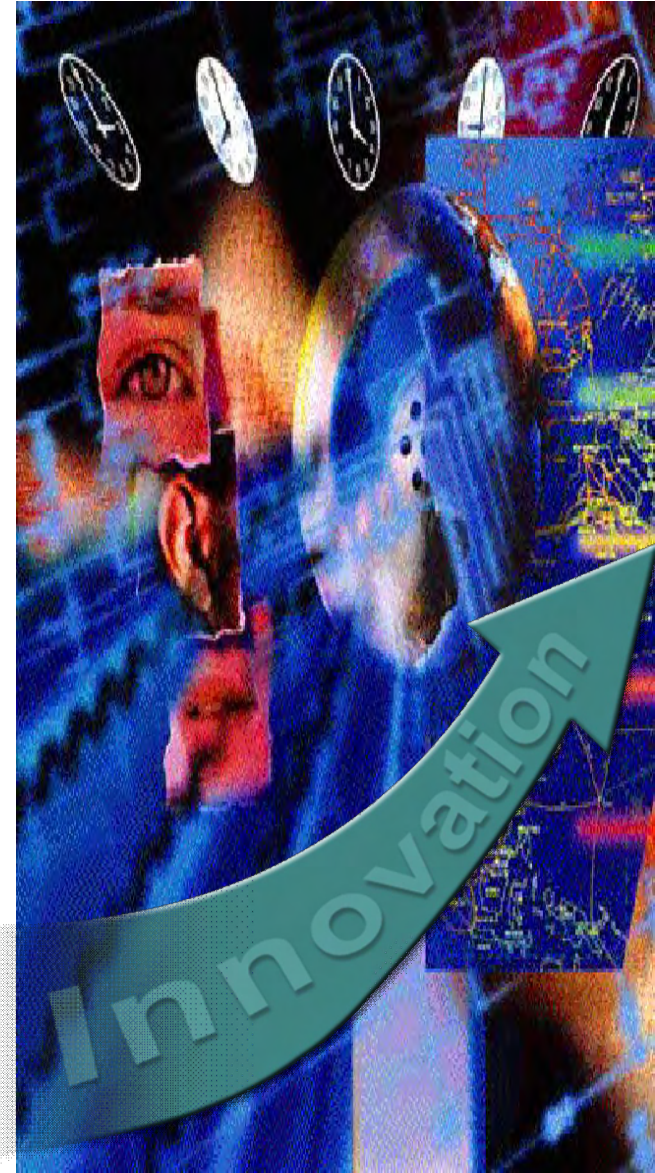


The Power and Network Is Used by the Connected Devices for Their Operation



# Evolution of the IEEE 802.3af PoE Standard

- Cisco was the industry's first to provide Power over Ethernet (inline power) in a LAN switch
  - Catalyst 6500 and Catalyst 4006 first chassis switches with PoE support and have been 802.3af PoE-ready since inception
  - Catalyst 3524-PWR-XL, shipped in May 2000 was first stackable to support PoE
  - Today there are well over 18 Million Cisco prestandard PoE ports deployed
- Cisco was deeply involved in the evolution of PoE innovation and throughout the IEEE standards process
- P802.3af, "DTE Power via MDI", was approved by the IEEE Standards Board and has been published as "802.3af-2003" standard





# How to Deploy Power over Ethernet (PoE)

There are two primary components of a PoE deployment:

- Power Sourcing Equipment (PSE) (such as a Cisco Catalyst LAN Switch Port)
- Inserts power over the Ethernet cable
- Powered Device (PD)
- Accepts and utilizes delivered inline power



# IEEE Power Classification

## Optional Feature

- IEEE 802.3af has an **optional** Power Classification feature and should be a minimum requirement for any PoE deployment
- LAN Switch (PSE) reserves required power based upon attached devices' "class"
- Significantly reduces power capacity requirements
  - With Power Classification**— switch identifies power needs and only reserves power based upon class
  - Without Power Classification**— unclassified devices treated at default with full 15.4 W per port
- All Cisco 802.3af Catalyst Switches (PSE) devices support the optional Power Classification feature

Class Number	Max Power at output of PSE per port
0 (Default)	15.4 watts reserved (actual device requirement can be much less)
1	4 watts
2	7 watts
3	15.4 watts
4	Future Expansion

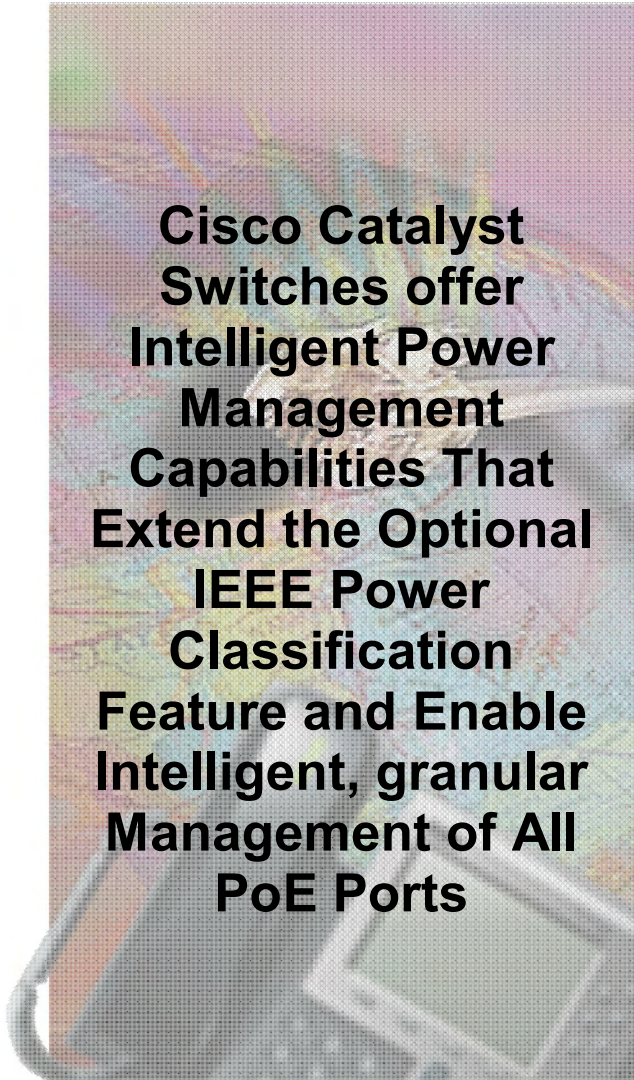
**Cisco's Intelligent Power management extends IEEE Power Classification for more granular control**

# Cisco Catalyst Intelligent Power

## Management Capabilities

### Enabling Optimization of Power Delivery

- Extend IEEE Power Classification with more granular power management
- Set pre-defined, per-port power allocation to limit high-power devices and minimize power draw
- Restrict power delivery from specific ports and identify ports where power is not being used to re-allocate power

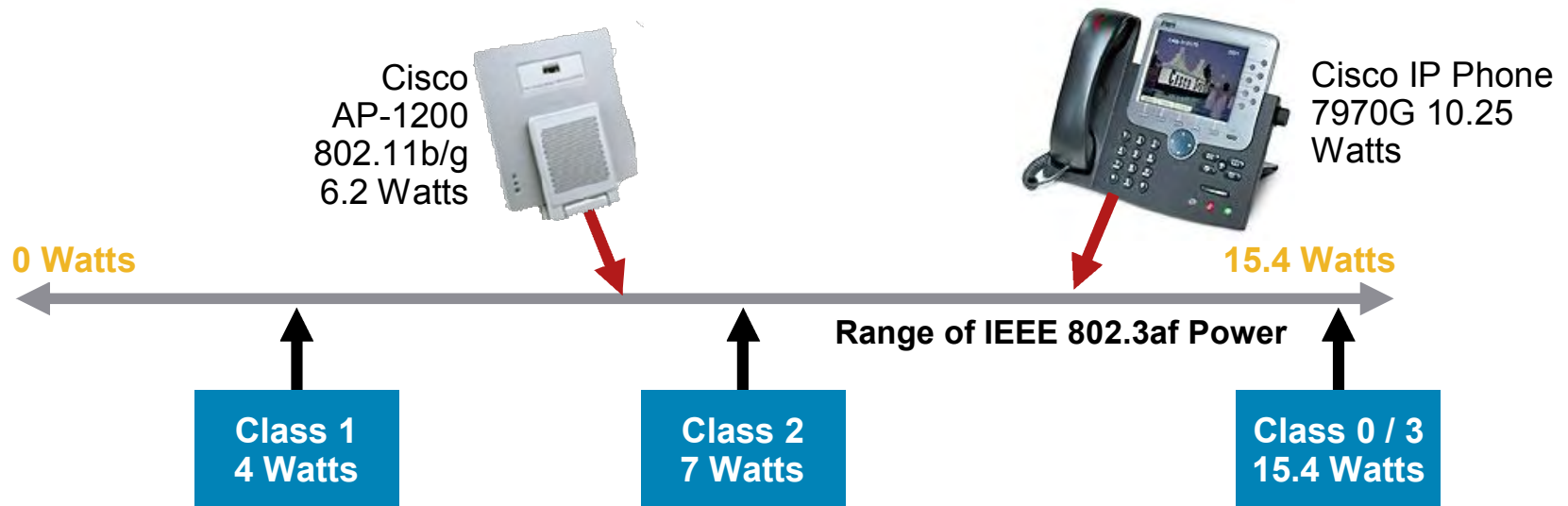
A photograph of a Cisco Catalyst switch, showing its front panel with various ports and a display screen. The image is slightly blurred and has a dark, textured overlay.

**Cisco Catalyst Switches offer Intelligent Power Management Capabilities That Extend the Optional IEEE Power Classification Feature and Enable Intelligent, granular Management of All PoE Ports**

# Cisco Intelligent Power Management

## More Granular than IEEE Power Classification

- Intelligent Power Management enables Cisco Catalyst switches to identify precise power requirements for compatible Powered Devices
- Precise power delivery optimizes power delivery by
  - Reducing the need for larger power supplies
  - Enabling higher numbers of Powered Devices to be supported
- Catalyst switch initially uses the IEEE Class structure to determine initial power requirements, then after start-up, Intelligent Power Management is used to further refine Power allocation for compatible devices



# Agenda



- Cisco® Catalyst® Switches Overview
- Catalyst 3560 Product Overview
- Power over Ethernet
- **Intelligent Services**
- Cisco Network Assistant
- Deployment Examples
- Service and Support



# Increasing Demands Placed on Networks



- Desktop computing power increasing
  - Acting as servers
  - Gigabit connections
  - Flooding network with traffic
- Multiple types of access devices
  - Voice and data traffic at the desktop
  - Traffic classification needs
- New, advanced applications with less-predictable traffic patterns
  - Greater reliance on servers
  - New, less-predictable traffic patterns
- Stronger network security
  - Increased flow of sensitive info on the network
  - Internal and external threats

# Cisco Catalyst Intelligent Switching Infrastructure

Intelligent Switching is a Common Foundation of Capabilities across Cisco® Catalyst® Switches



## Performance, Availability

- Wire-speed forwarding
- No performance effect with all services enabled



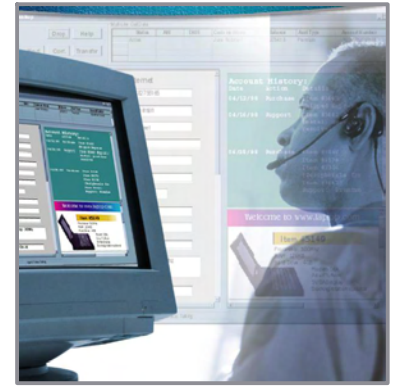
## QoS

- Layer 2, 3, 4 classification
- Policing and shaping
- Multiple queues
- Granular control



## Security

- Layer 2, 3, 4 access control
- Identity-based authentication
- Management security

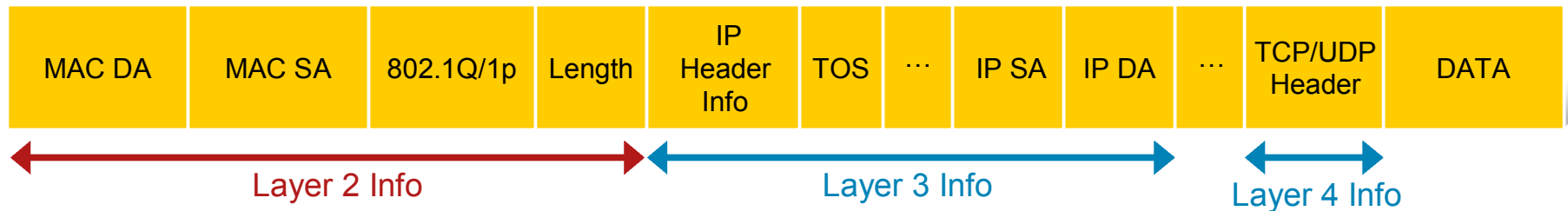


## Manageability

- End-to-end manageability for centralized administration
- Web-based or command-line interface (CLI)
- Analysis and planning tools

# Intelligence Through More Capable ASICs

\* Not to Scale



- Layer 2 switches are limited to the processing and forwarding of Layer 2 information.
- Multilayer switches can look deeper into the frame => intelligent decisions based on Layer 3 or Layer 4 information.
- Examples of why this scenario is useful:
  - Preserve bandwidth by limiting traffic based on a user's IP address.
  - Preserve bandwidth by limiting traffic based on applications using a constant TCP/UDP port number—Web browsing, enterprise resource planning (ERP) applications, etc.
  - Prevent access to network resources based on user's IP address.
  - Classify and mark traffic based on Layer 3 QoS (DSCP).
- Cisco® innovative ASICs with Cisco IOS® Software integration enable superior intelligent services that will not bottleneck the network.

# Cisco Catalyst Intelligent Switching Infrastructure

## Intelligent Switching



Advanced QoS

Security

Availability

Manageability

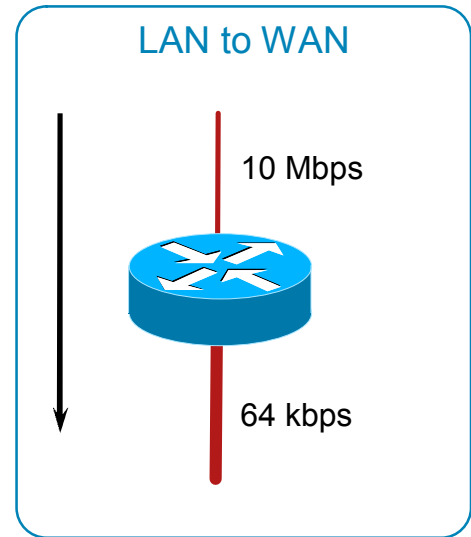
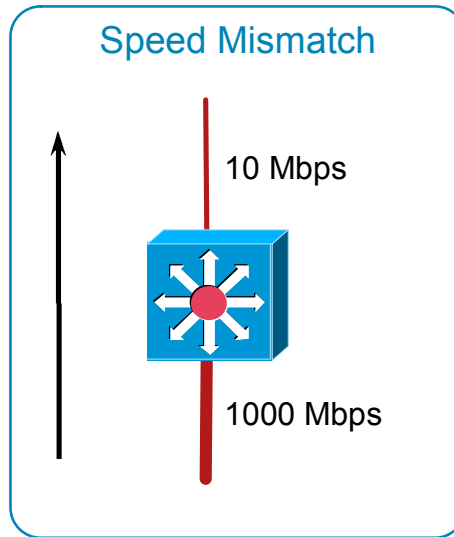
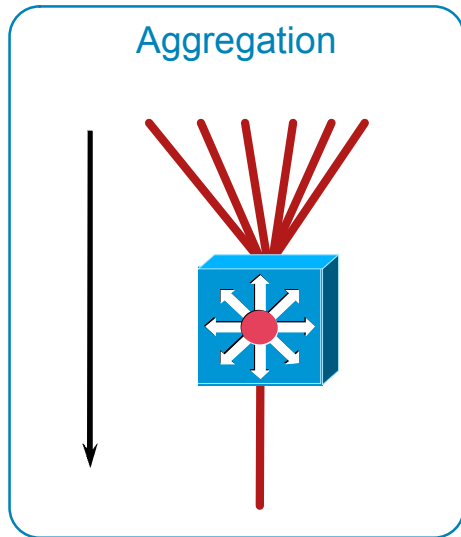
### Features

- Layer 2, 3, 4 traffic classification
- Shaping, sharing, and policing
- Granular control
- Wire-speed performance

### Benefits

- Manage bandwidth to meet business priorities
- Maintain performance for time-sensitive applications
- Better meet defined SLAs
- No performance degradation with services enabled

# Where Congestion Exists, QoS is Required



- Points of aggregation
- Links and buffers
- Points of substantial speed mismatch
- Transmit buffers tend to fill (TCP windowing)
- Buffering reduces loss, introduces delay



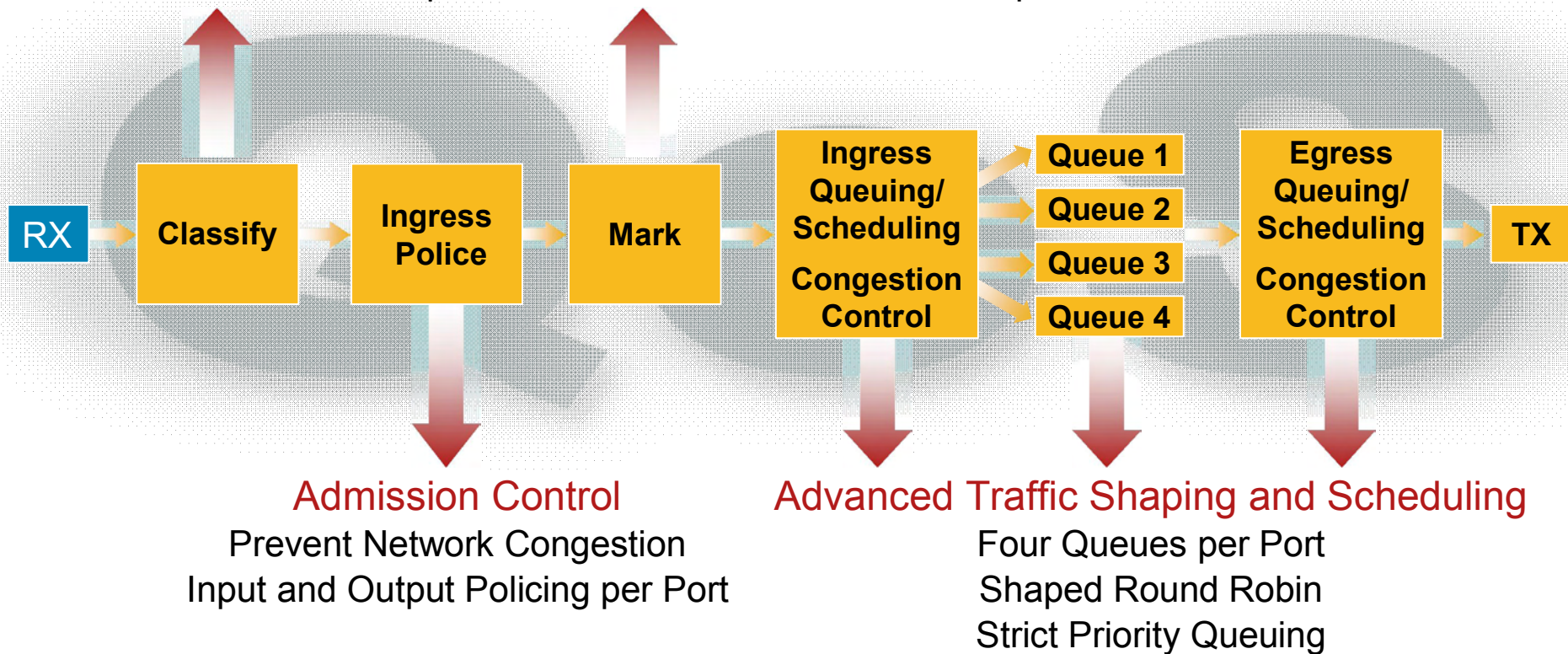
# Not All Traffic Is Created Equal

	Voice	Video	Data (Best-Effort)	Mission-Critical Data
Bandwidth	Low to Moderate	Moderate to High	Moderate to High	Low to Moderate
Random Drop Sensitivity	Low	Low	High	High
Delay Sensitivity	High	High	Low	Moderate to High
Jitter Sensitivity	High	High	Low	Low to Moderate

# Cisco Catalyst 3560 Series Extensive QoS Features

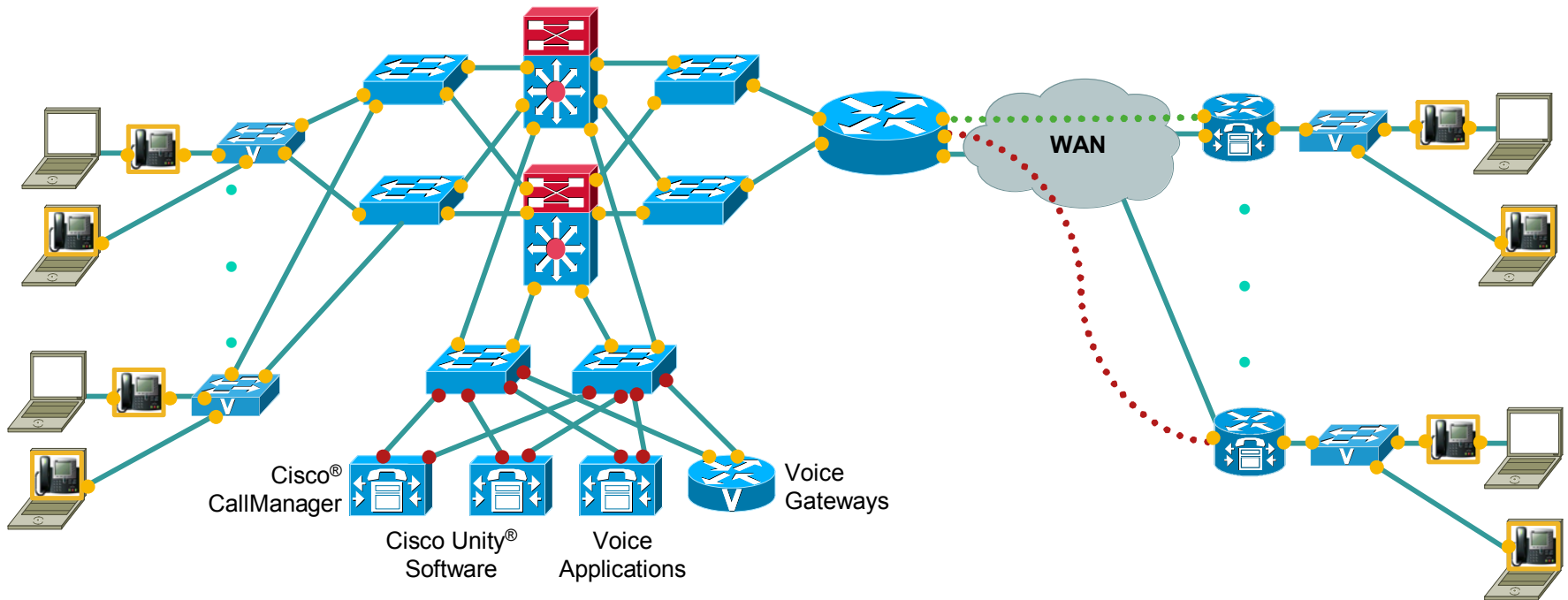
## Traffic Classification and Marking for Differentiated Services

Per port or individual/aggregate flow classification and rewrite  
MAC address, 802.1p CoS/DSCP, IP address, TCP/UDP port



# Auto QoS

One Command per Interface to Enable and Configure QoS;  
Modify Global and Interface Settings to Make QoS for VoIP Work



# Cisco Catalyst Intelligent Switching Infrastructure



Advanced QoS

Security

Availability

Manageability

## Features

- Identity-based authentication
- Wire-speed access control lists
- Controlled access to system maintenance
- Integrated security services

## Benefits

- Authenticate and control access based upon user identity
- Protect critical business assets
- Prevent downtime
- Prevent network attacks from within

# Catalyst Integrated Security Strategy



## Threat Defense

- Defend the Edge:  
Integrated Network FW+IDS  
Detects and Prevents External Attacks
- Protect the Interior:  
Catalyst Integrated Security  
Protects Against Internal Attacks
- Guard the Endpoints:  
Cisco Security Agent (CSA)  
Protects Hosts Against Infection



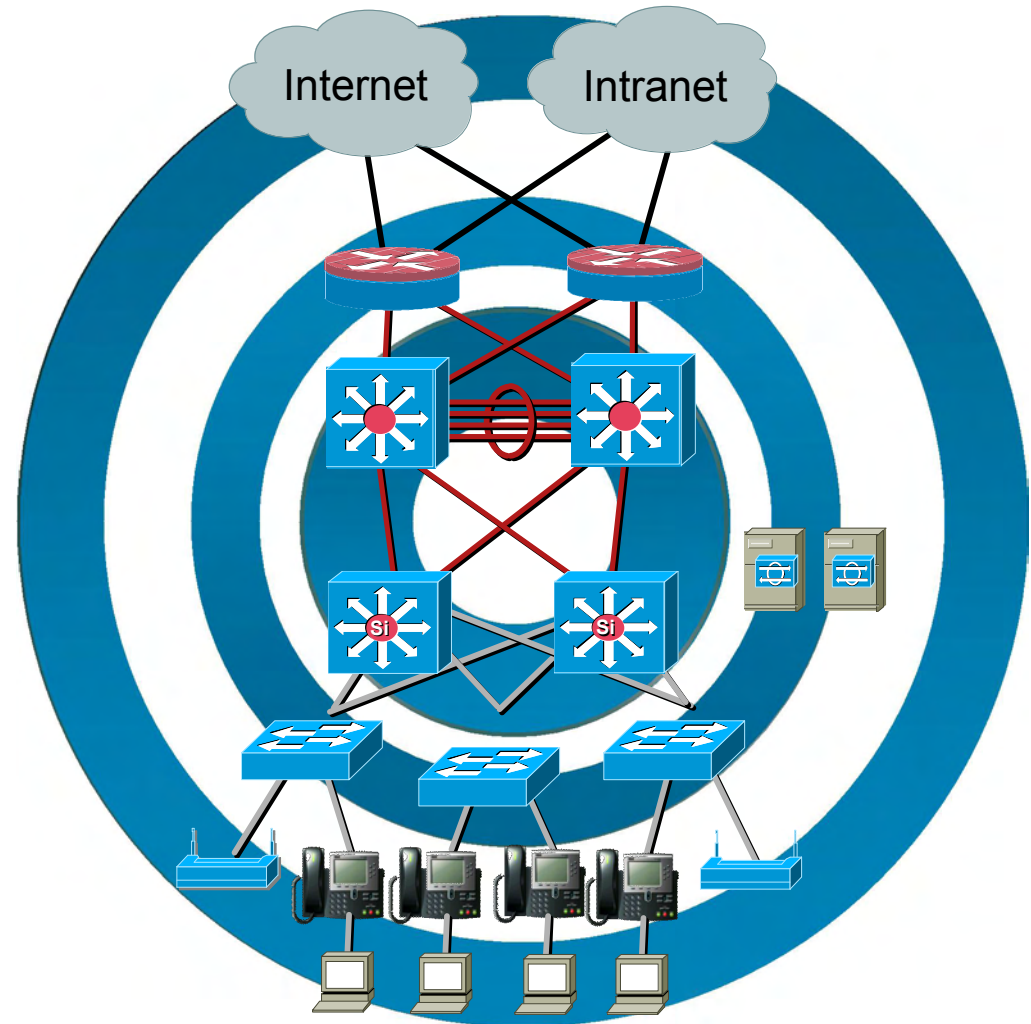
## Trust and Identity

- Guarding Network Access  
Identity-Based Networking  
Control Who/What Has Access



## Secure Communication

- Secure the Transport:  
IPSec VPN  
Protects Data/Voice Confidentiality



# Secure Connectivity

## Secure Shell (SSH)

- SSH encrypts administration traffic during Telnet sessions while configuring or troubleshooting switches

## Secure Sockets Layer (SSL)

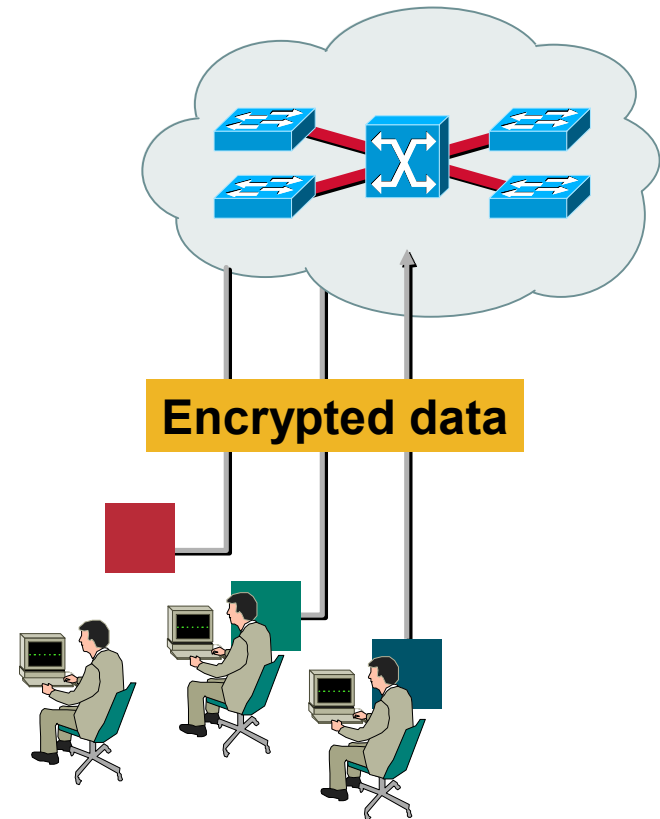
- SSL encrypts network management traffic allowing the secure use of tools such as the Cisco Network Assistant

## SNMPv3 (with crypto support)

- Provides network security by encrypting administrator traffic during SNMP session to configure or troubleshoot switches

## Kerberos

- Authenticates users and network services using a trusted third party to perform secure verification

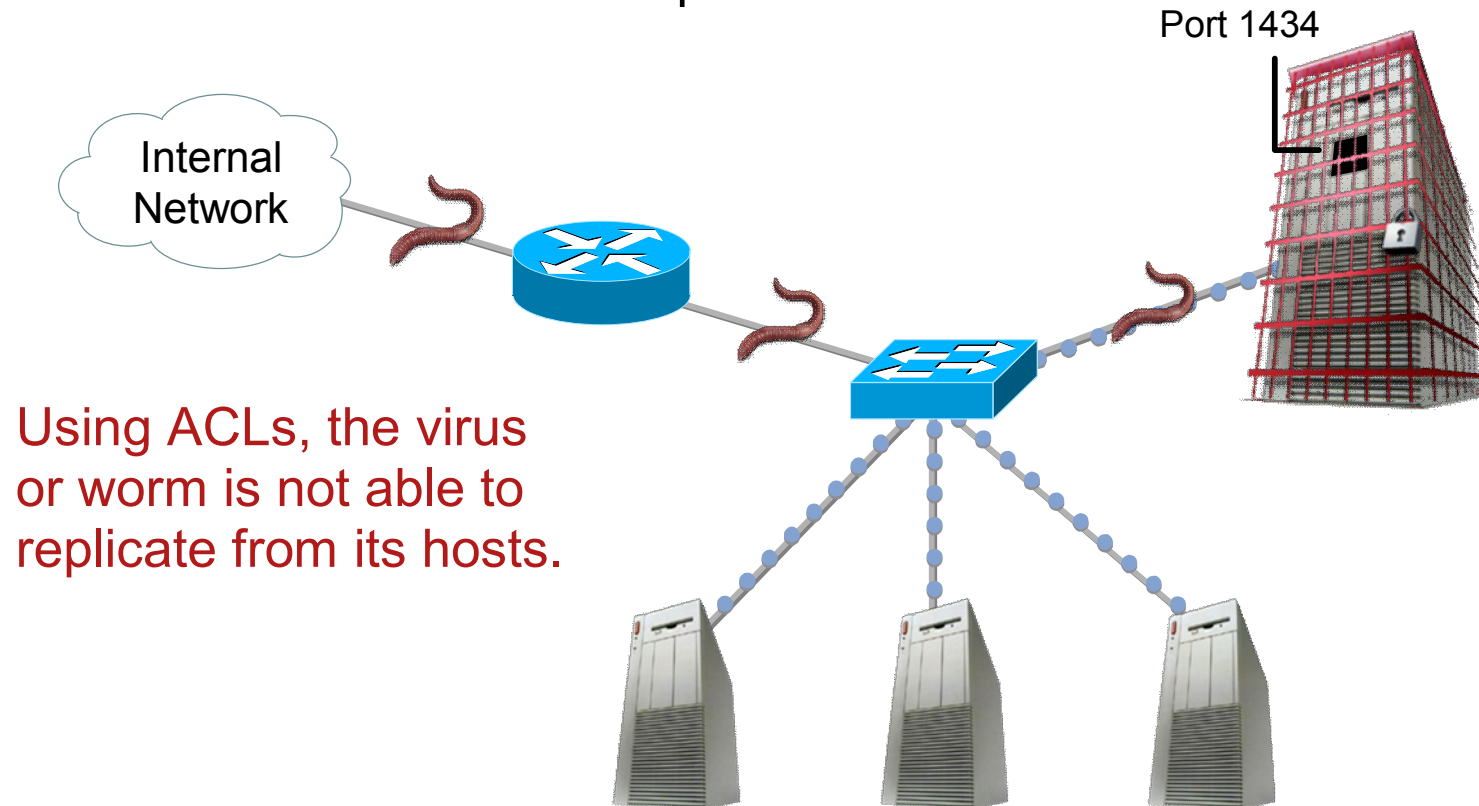




# Protecting Against Worms

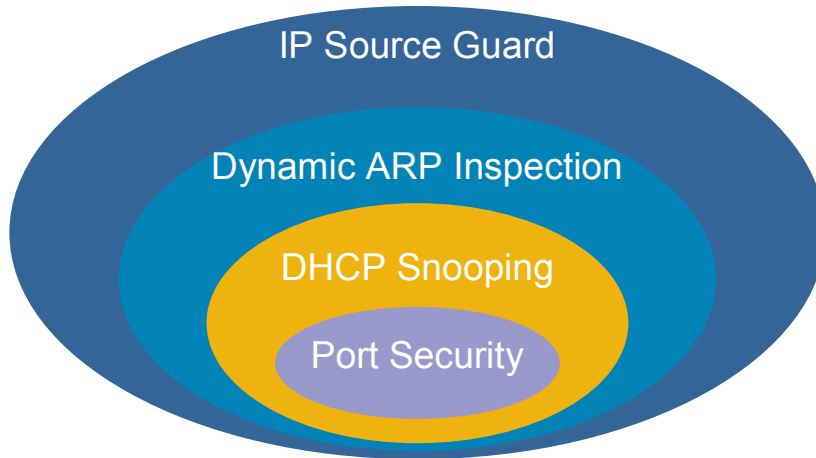
## How It Works:

- The ACL provides a mechanism to protect servers, users, and applications against worms by determining what traffic streams or users can access what ports.

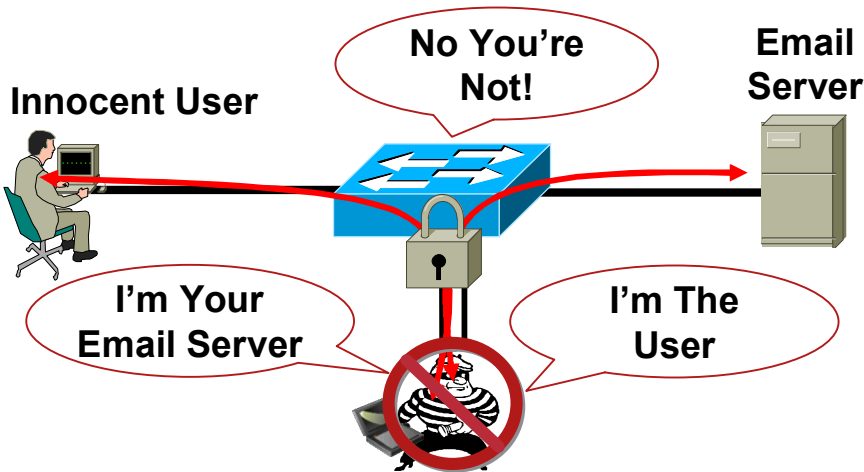


Using ACLs, the virus or worm is not able to replicate from its hosts.

# Typical Internal Attacks

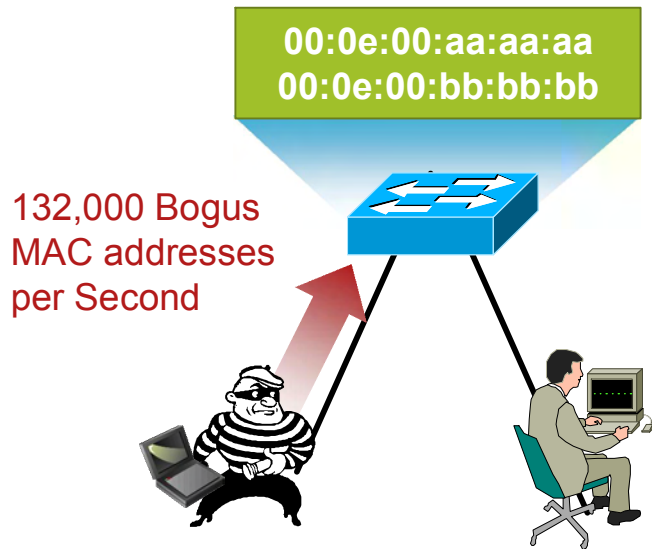


Attack	Catalyst Feature
MAC Address Flooding	Port Security
DHCP Rogue Server for Default Gateway Interception	DHCP Snooping
ARP Spoofing or ARP Poisoning	Dynamic ARP Inspection
IP Spoofing	IP Source Guard



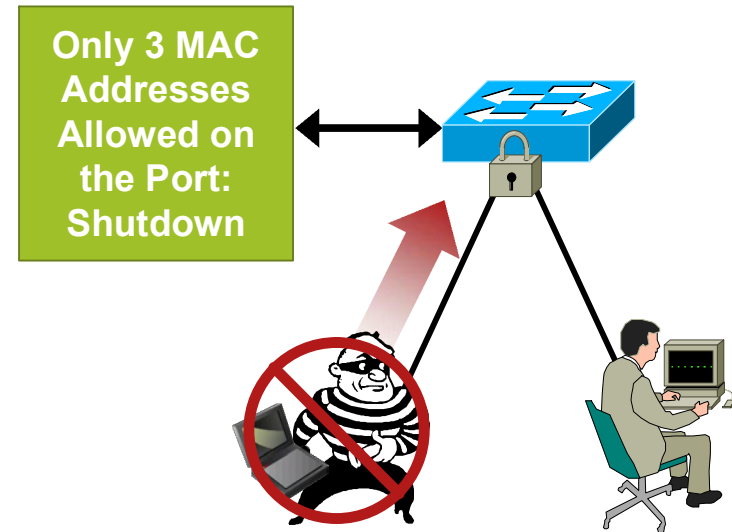
# MAC Address Flooding Attacks

## Cutting off MAC-Based Attacks



### Problem:

- “Script Kiddie” Hacking Tools Enable Attackers’ Flood Switch CAM Tables with Bogus MAC Addresses, Turning the VLAN into a “Hub” and Eliminating Privacy
- Switch CAM Table Limit of 32K Mac Addresses



### Solution:

- Port Security Limits MAC Flooding Attack and Locks Down Port and Sends an SNMP Trap

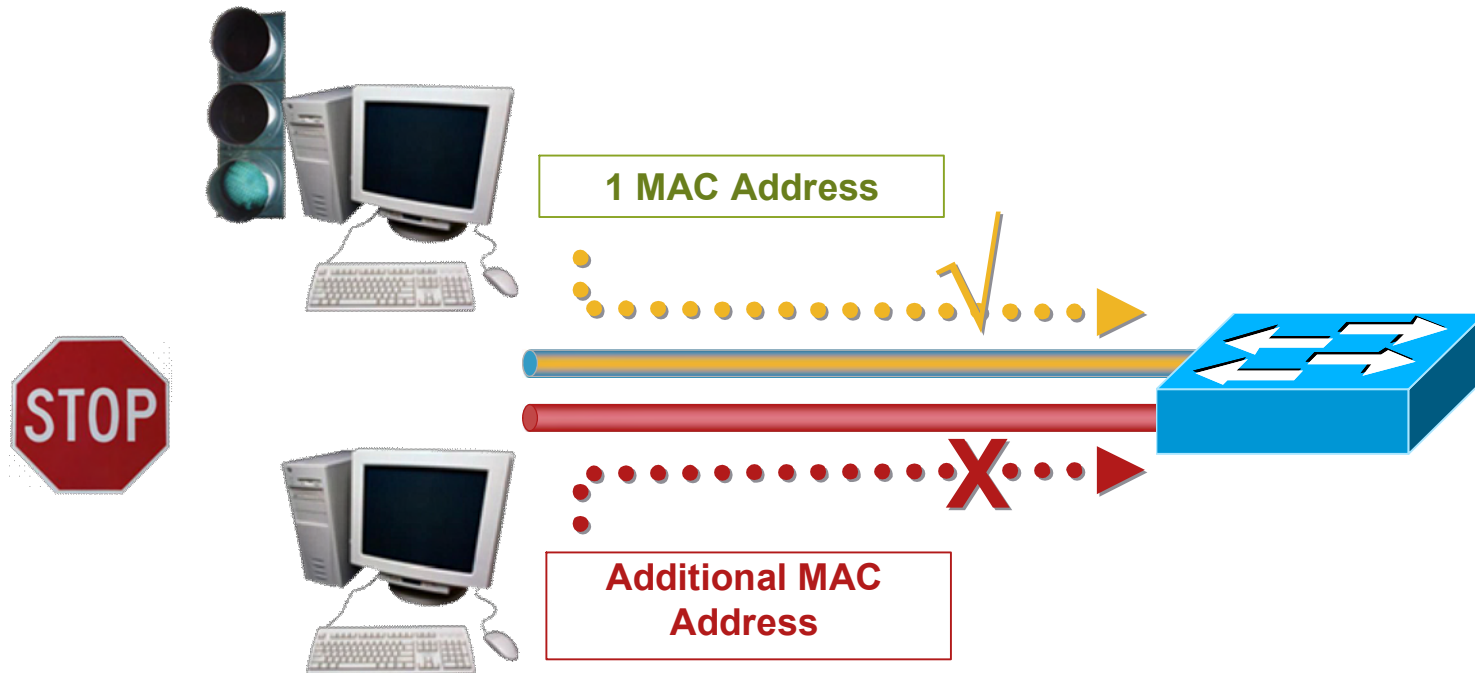
# Port Security

## What It Does:

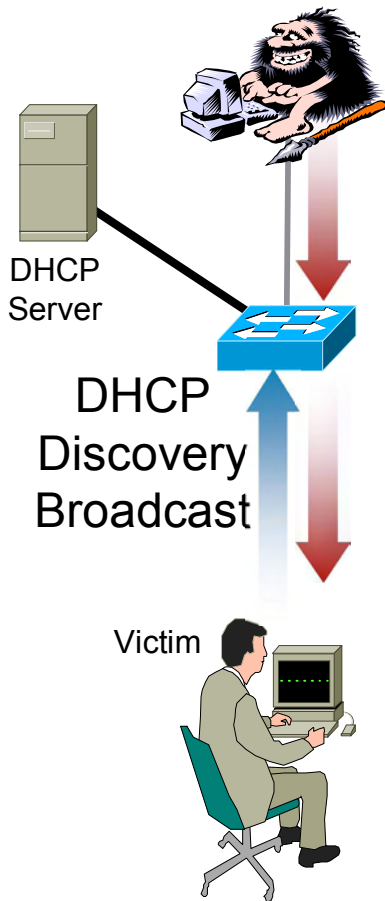
- Limits the number of MAC addresses that are able to connect to a switch and ensures only approved MAC addresses are able to access the switch.

## Benefit:

- Ensures only approved users can log on to the network.



# DHCP Spoofing Attack



## Rogue DHCP Offer

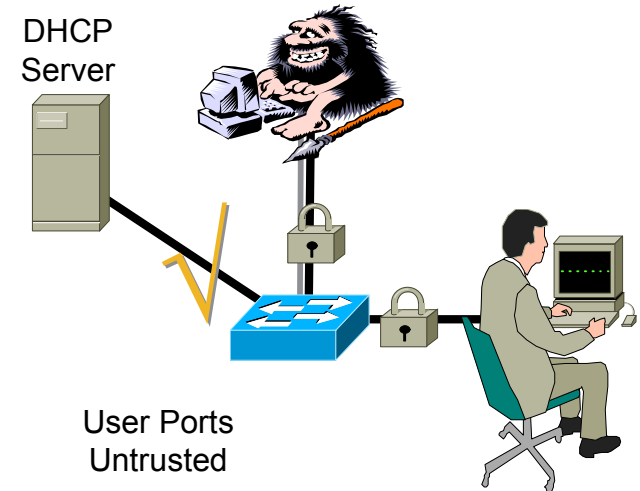
IP: 10.1.1.20/24

GW: 10.1.1.1

DNS: 192.168.1.122

## Problem:

- Malicious user pretends to be the network DHCP server.
- Misconfigured user starts up a DHCP server incorrectly.
- Malicious user can send out bogus address, deplete the address space, or spoof the default gateway.



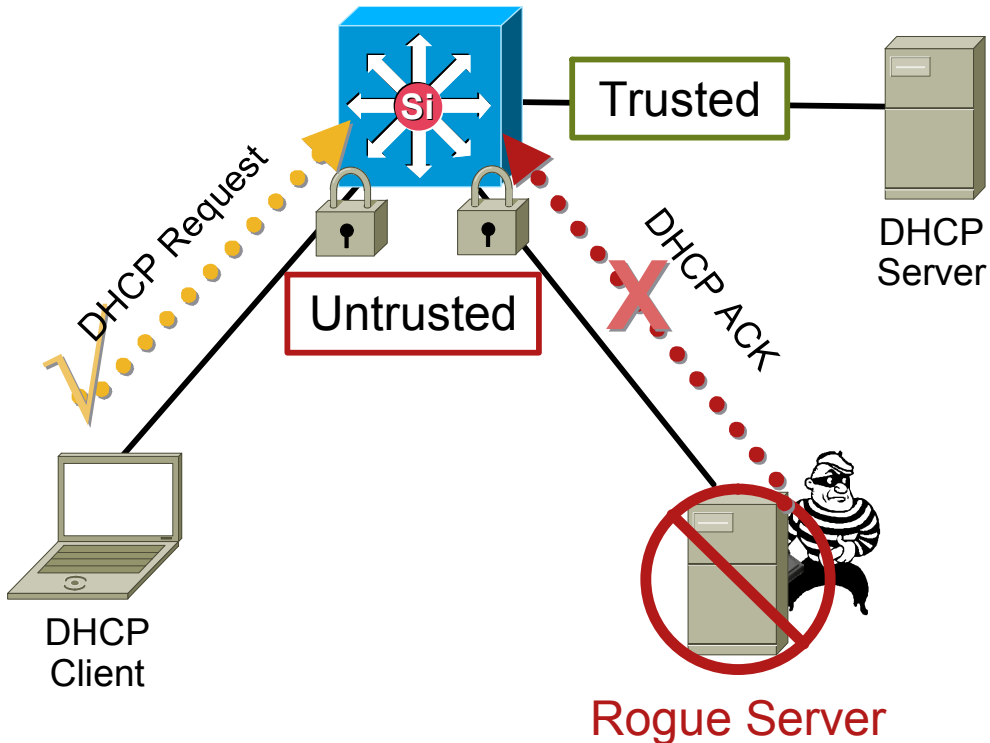
## Solution

- Do not trust user ports so only DHCP requests can be sent.
- Snoop DHCP information for integrity.



# DHCP Snooping

## DHCP Snooping Enabled



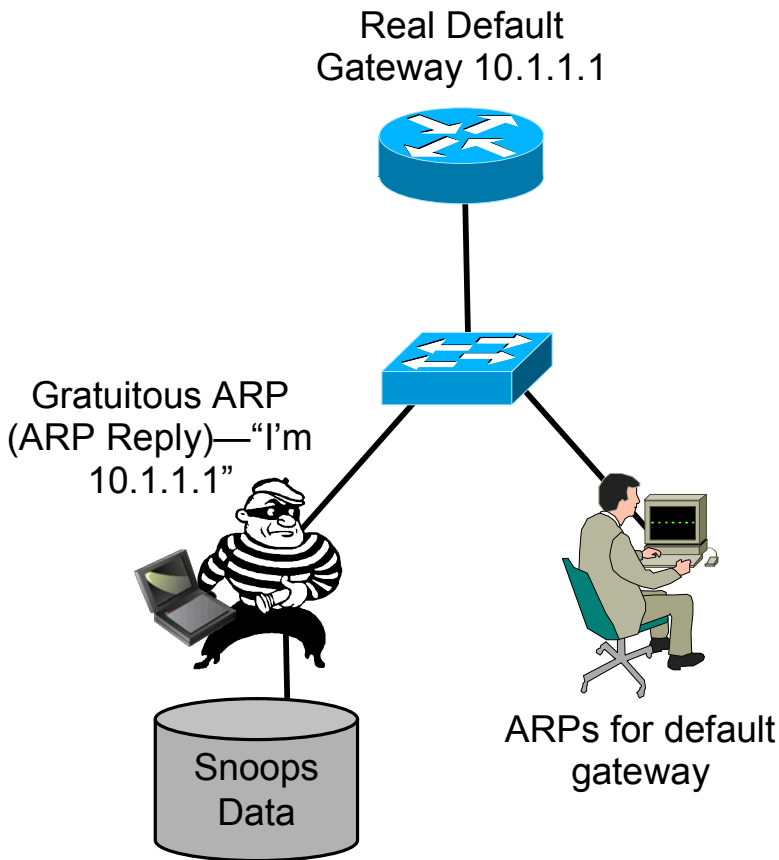
## What It Does:

- Switch forwards only DHCP requests from untrusted access ports, and drops all other types of DHCP traffic. DHCP snooping allows only designated DHCP ports or uplink ports trusted to relay DHCP messages. It builds a DHCP binding table containing client IP address, client MAC address, port, and VLAN number.

## Benefit:

- DHCP snooping eliminates rogue devices from behaving as the DHCP server.

# ARP Spoofing Attack— The Man-in-the-Middle



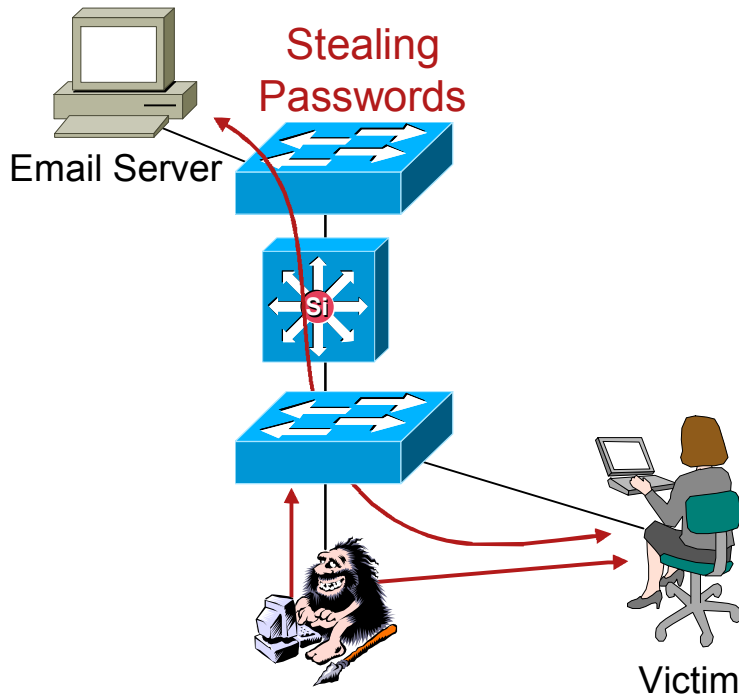
- Attacker only needs to be attached on same subnet as one victim—sends Gratuitous ARP onto subnet.
- IP/ARP bindings incorrectly set at innocent endstation
- Tools Easily Downloadable and is simpler than most video games (GUI or CLI)

```
ettercap 0.0.7
SOURCE: 192.168.0.76 <
DEST : 192.168.0.22 <
      doppleganger - illithid - ettercap

48 hosts in this LAN (192.168.0.30 : 255.255.255.0)
1> 192.168.0.76:05:2F:77 <-> 192.168.0.22:17: & ACTIVE
2> 192.168.0.76:17 <-> 192.168.0.22:34 & silent
3> 192.168.0.76:34 <-> 192.168.0.22:68 & silent
4> 192.168.0.76:51 <-> 192.168.0.22:192 & silent
5> 192.168.0.76:68 <-> 192.168.0.22:136 & silent
6> 192.168.0.76:85 <-> 192.168.0.22:178 & ACTIVE

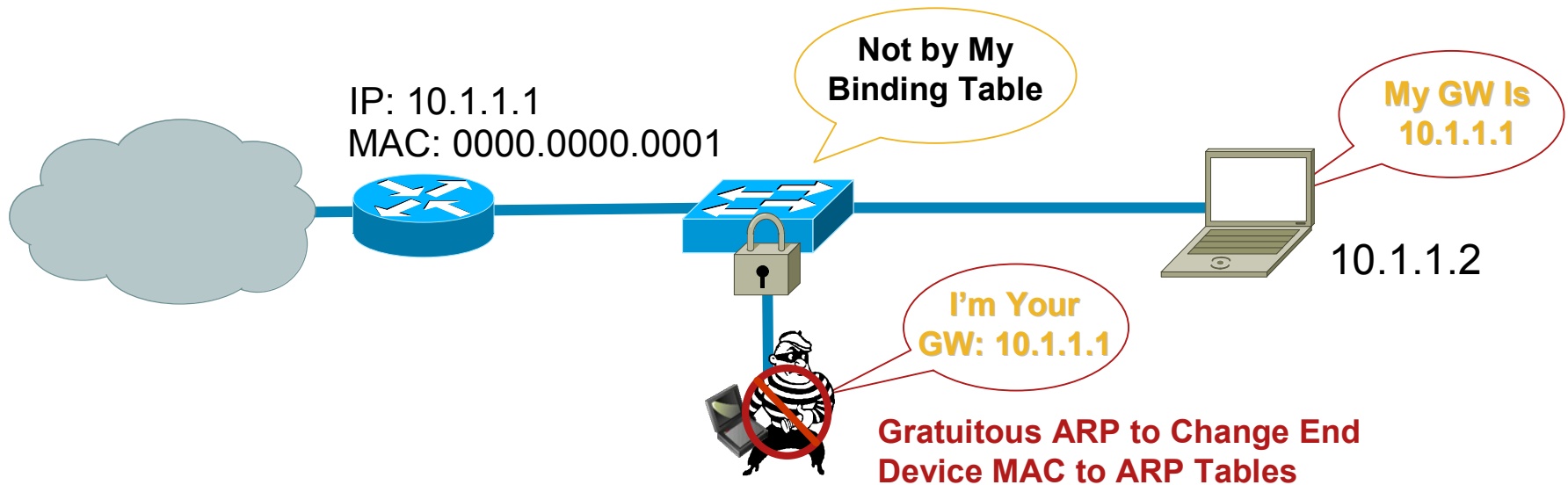
Your IP: 192.168.0.30 with MAC: 00:00:24:4C:00:F9 on IFace: eth0
```

# A Simple Tool, Some Dangerous Consequences...



- Neither the victim nor the default gateway is aware of the attack
- Passwords can be snooped
- Client, employee or company-confidential information can be compromised

# Dynamic ARP Inspection



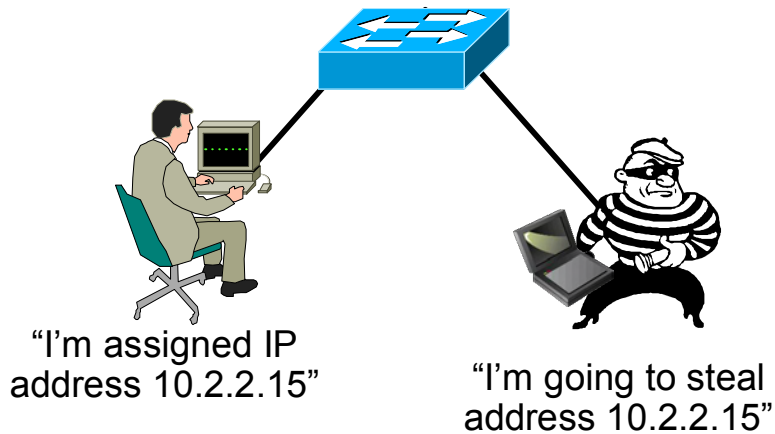
## What It Does

- Maintains a binding table containing IP and MAC address associations dynamically populated using DHCP Snooping

## Benefit

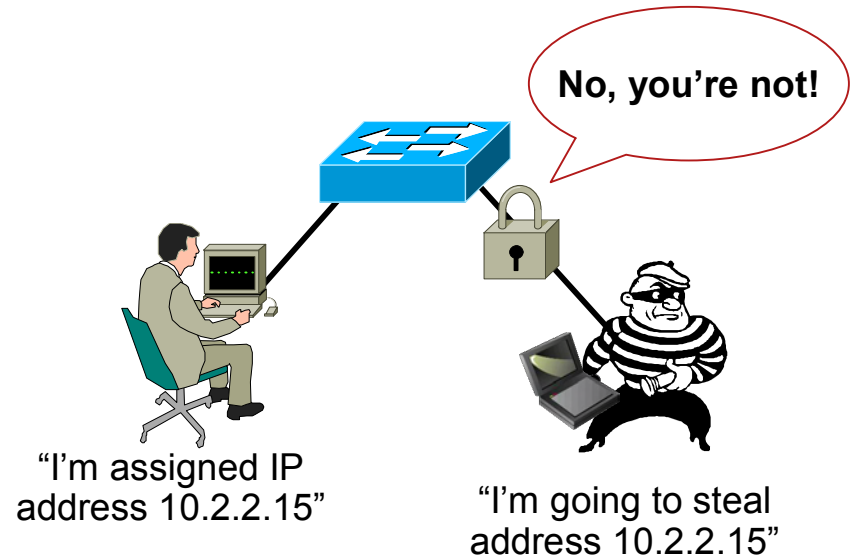
- Ensures integrity of user and default gateway information such that traffic cannot be captured

# IP Spoofing Attack



## Problem:

- Users change their assigned IP address either due to:
  - Innocent reasons
  - A way to hide an attack by bypassing ACLs, appearing to be on a different subnet or launch anonymous DoS attacks

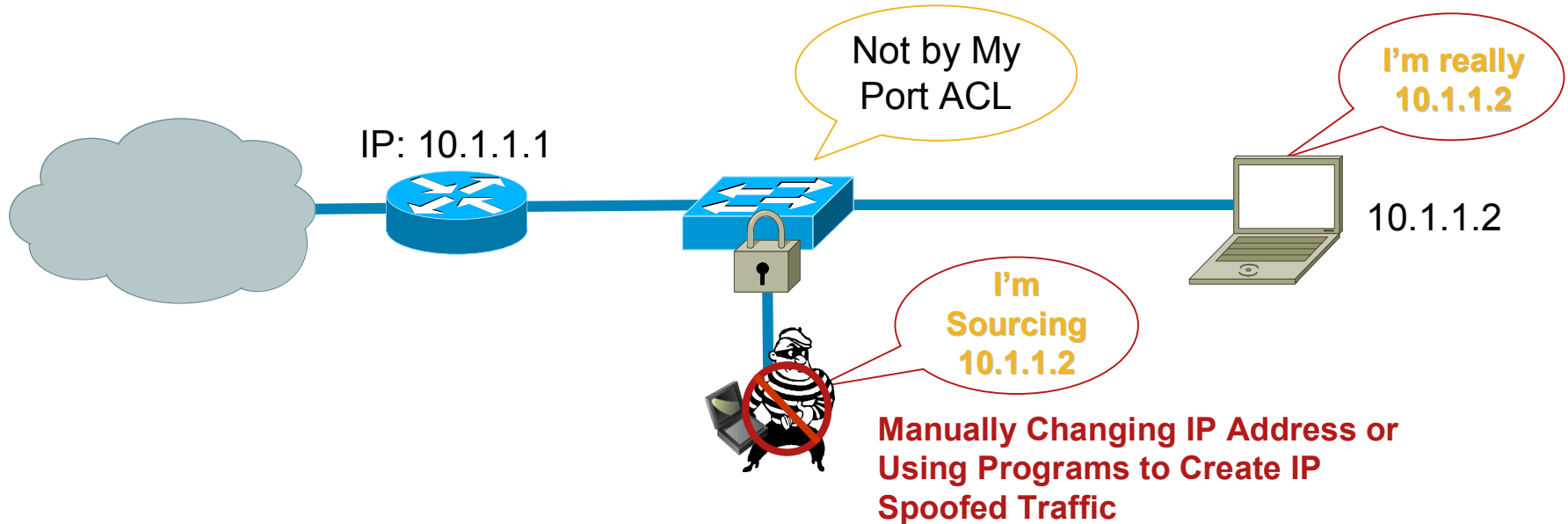


## Solution:

- Discarding attacker's packets with spoofed source IP address by binding client IP address, client MAC address, port, VLAN number



# IP Source Guard



## What It Does:

- Automatically configures a Port ACL for IP address and adds MAC address to port security list for the port. DHCP Snooping allows learning and binding of IP address and MAC address by the switch
- Removes ACL and MAC entry when lease expires

## Benefit:

- Prevents snooping of data or anonymous launching of attacks

# Identity-Based Network Services

## What It Does:

- Using the 802.1x protocol with cisco enhancements, the network grants privileges based on user logon information, regardless of the user's location or device

## Benefits:

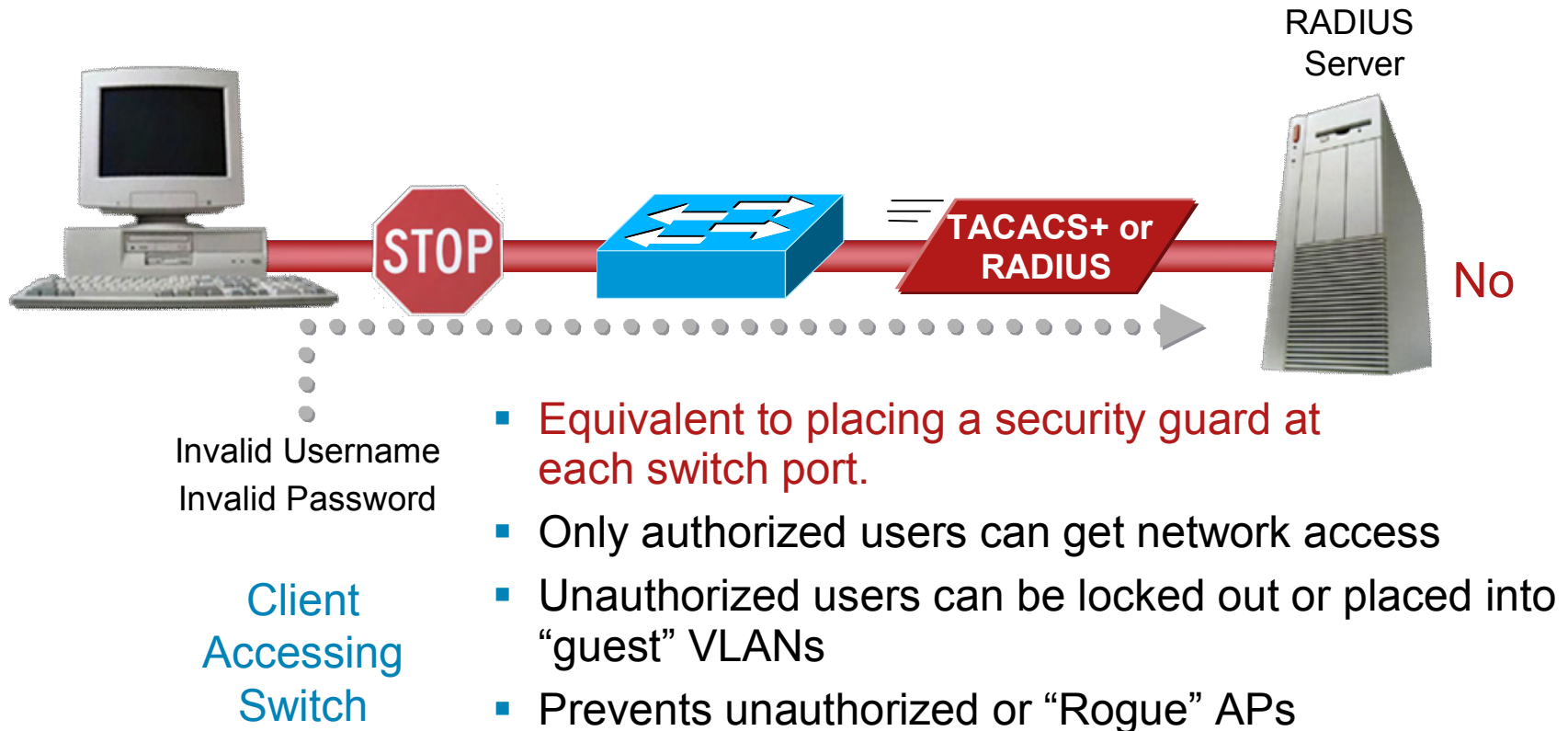
- Allows different people to use the same pc and have different capabilities
- Ensures that users only get their designated privileges, no matter how they are logged onto the network
- Reports unauthorized access



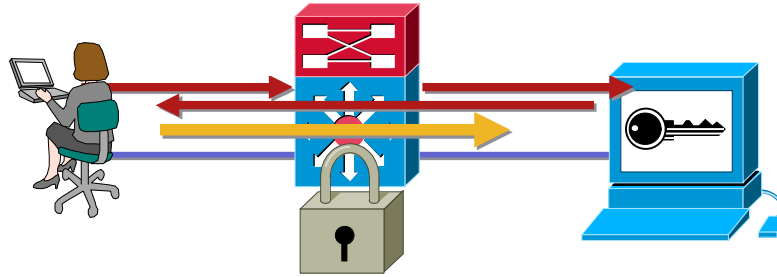
# Identity-Based Network Services

## How It Works:

All users trying to enter the network must receive authorization based on their personal username and password



# 802.1x Enhancements



- Allow to function concurrently with Port Security
- VLAN assignment
  - The user will be assigned to a VLAN-based on the response from the RADIUS server to the catalyst switch
- 802.1x with VVID support
  - 802.1x will support interoperability with the IP phone handsets
- Apply Extended ACLs
  - Enables configuration of extended ACLs to provide network security based on 802.1x authenticated users
- MAC-based authentication
  - MAC-based authentication for non-supplicant capable user
- Web-based “proxy-supplicant” authentication
  - Non-supplicant user is recognized by switch
  - User given screen to enter username and password—**simulates supplicant**

# The Next Step: Cisco Network Admission Control (NAC)

- Cisco-led, Multi-partner Program
  - Limits damage from viruses and worms
  - Coalition of market leading vendors
- Restricts and Controls Network Access
  - Endpoint device interrogated for policy compliance
  - Network determines appropriate admission enforcement: **permit, deny, quarantine, restrict**
- A Cisco Self-Defending Network Initiative
  - Dramatically improves network's ability to identify, prevent, and adapt to threats



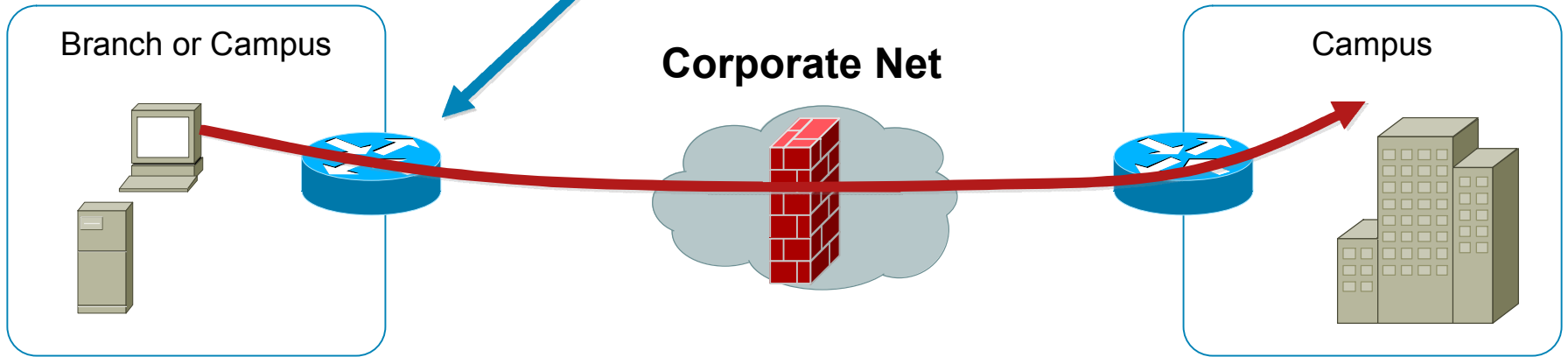


# Why Network Admission Control?

1. Non-compliant endpoint attempts connection

2. Connection allowed

3. Infection spreads; endpoints exposed

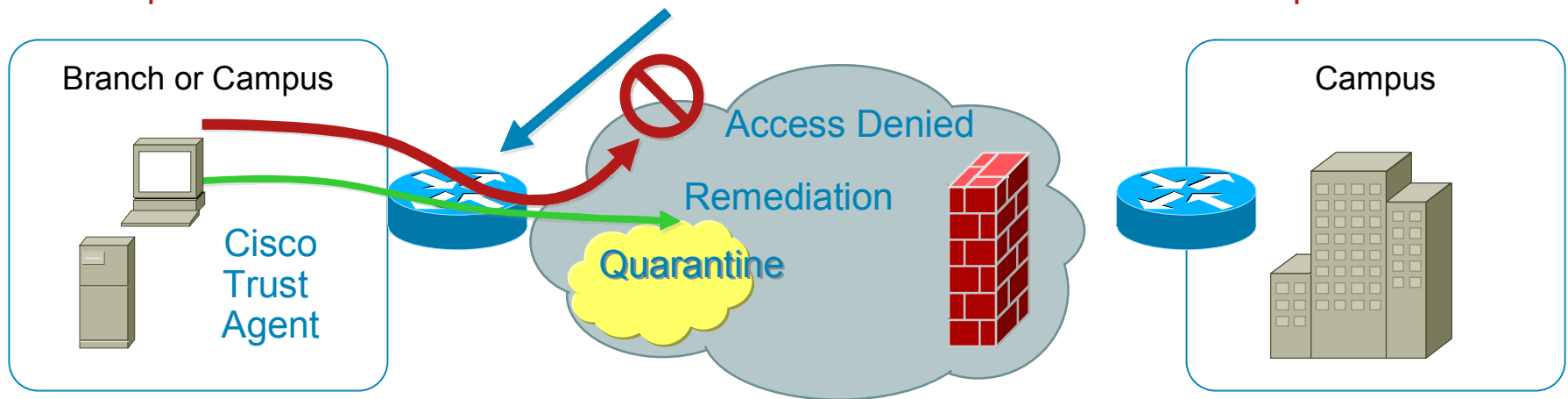


# Cisco Network Admission Control: What It Does

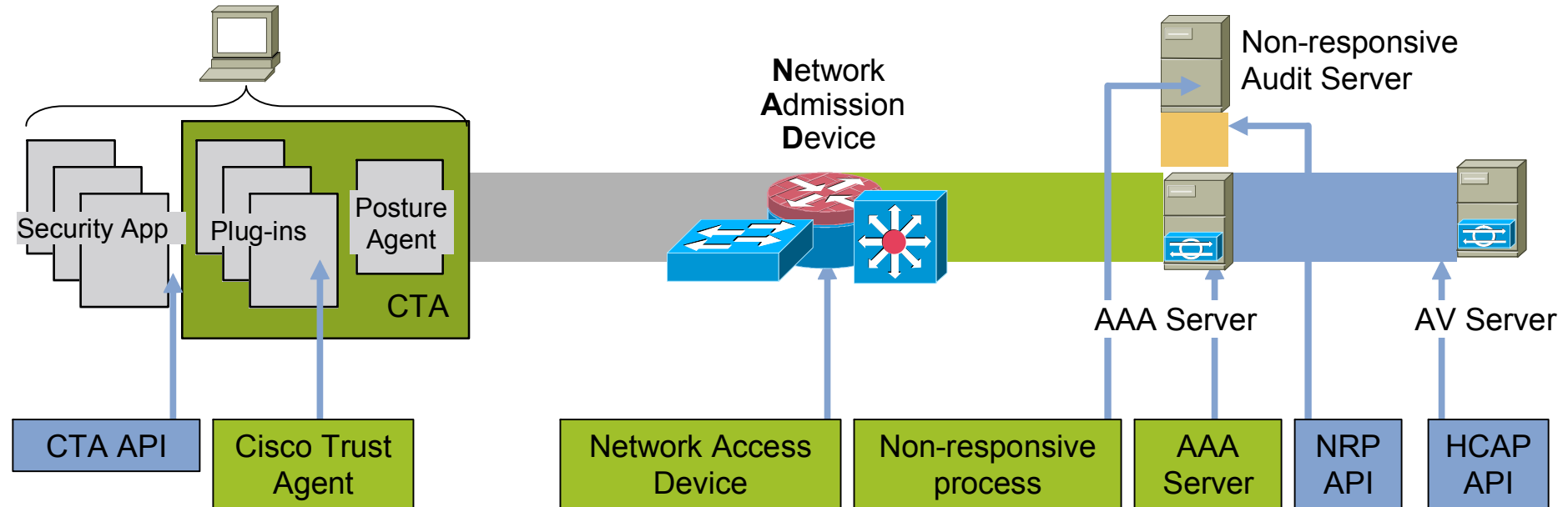
1. Non-compliant endpoint attempts connection

2. Non-compliant status determined

3. Infection contained; endpoints secured

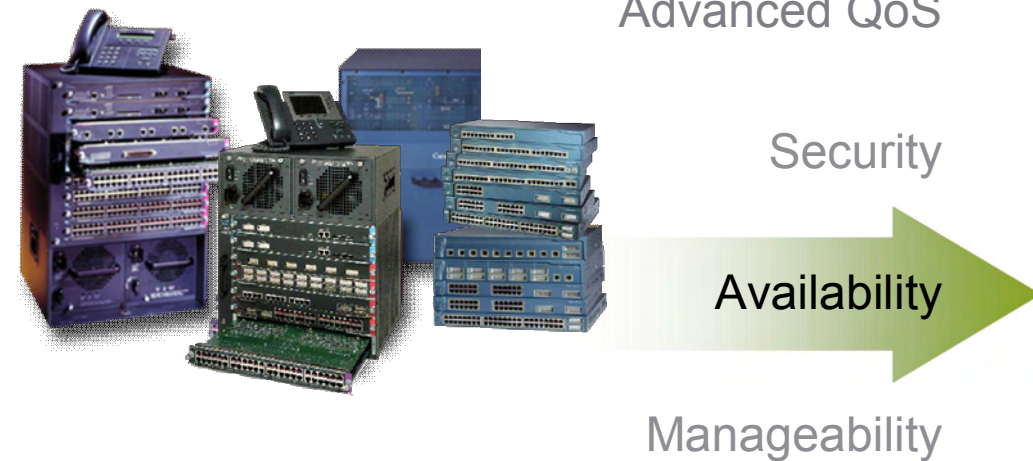


# How it Works— Network Admission Control



1. New **L2** or **L3** connection detected by smart Cisco device
2. Smart device acquires **AV Posture** (802.1x, IPsec, LEAP/PEAP, etc)
3. **ACS Svr** (AAA RADIUS) receives AV posture and sends access action (OK, Deny, Quarantine)—may involve Vendor Svr
4. Smart devices enforce access actions

# Cisco Catalyst Intelligent Switching Infrastructure



## Features

- Wire-speed forwarding
- No performance effect with all services enabled
- Load balancing
- Redundancy

## Benefits

- Network remains operable despite failures
- Ability to meet defined SLAs
- Business resiliency
- Reduced maintenance cost

# Higher Availability with the Cisco Redundant Power System 675

- Internal power supply redundancy
- Cisco® RPS 675 senses failure and delivers uninterrupted power to device
- Supports up to six Cisco networking devices including all Cisco Catalyst® 3750, 3560, 3550, 2970, and 2950 switches
- Small form factor—1 RU
- 675W (300W 12V system power, 375W 48V inline power)
- Cisco RPS 675 automatically resets into standby mode when the failed unit is replaced with a new unit



**Cisco RPS 675**

# Wire-Speed Services

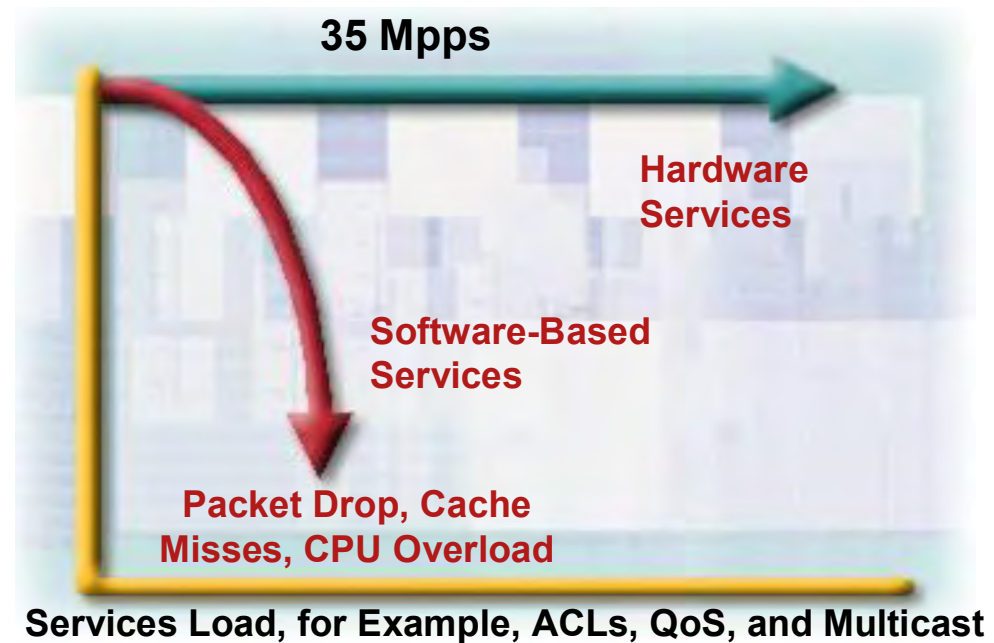
- Wire-speed, high-touch services with no performance hit:

- 512 QoS policies

- 1024 security policies

- 64 policers

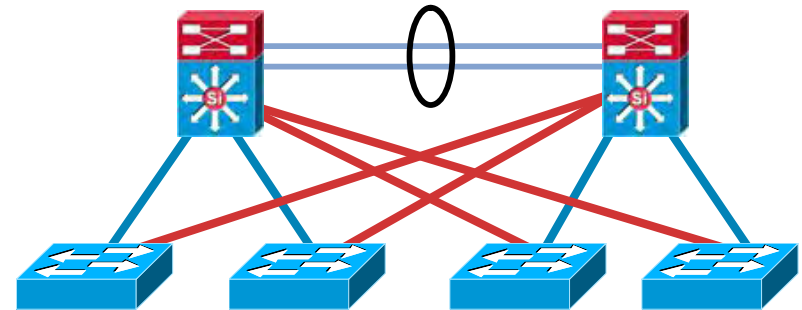
- 4 queues per port





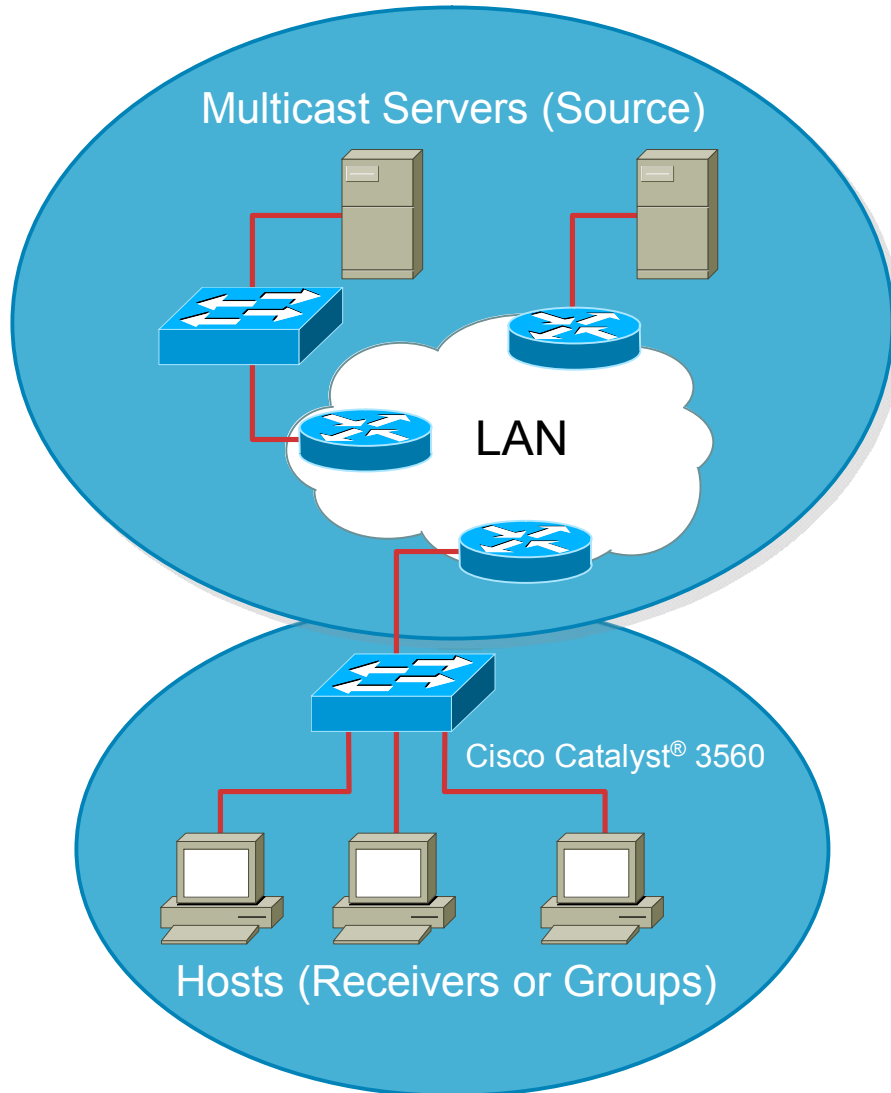
# IEEE 802.1s/w

- 802.1s and 802.1w enable loop-free Layer 2 network
  - Uses as few spanning tree instances as possible
- Multiple spanning-tree system allows for larger Layer 2 topologies
  - Rapidly accelerates convergence in event of a failure
- Saves CPU cycles and is interoperable across multiple vendors
- Cisco® implementation enables smooth migration to Multiple Spanning Tree from Per VLAN Spanning Tree Plus (PVST+) while preserving full standards compliance



Cisco extended the 802.1s/w standards by automatically running the spanning tree 802.1w when 802.1s is configured.

# Cisco Catalyst 3560 Multicast Support

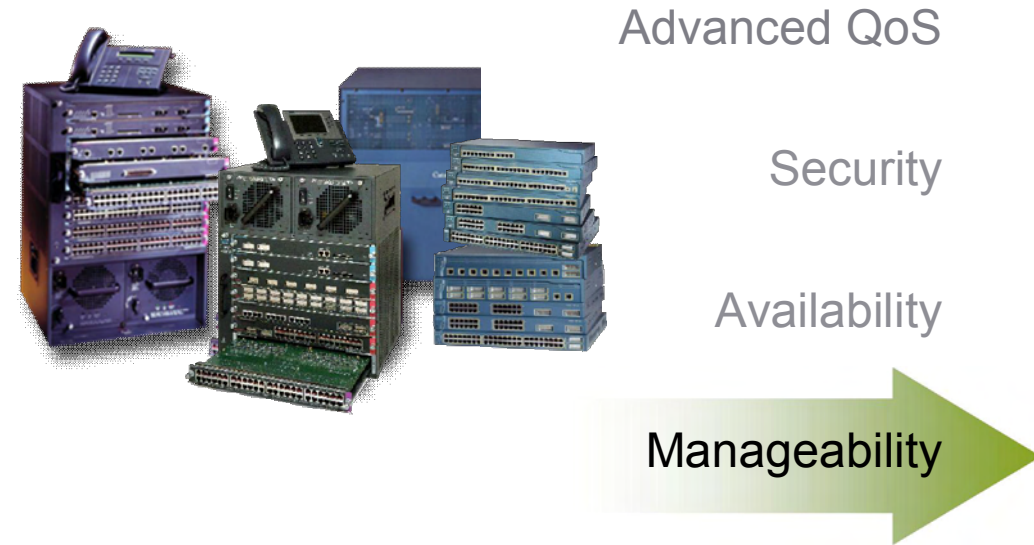


- Cisco® Group Management Protocol (CGMP), IGMP snooping is used for the managing group membership information
- Per-port broadcast, multicast, and unicast storm control
- Multicast VLAN registration
- Virtual Trunking Protocol pruning

# IGMP Snooping

- Default behavior of a Layer 2 switch is to flood multicast packets to ports in the ingress VLAN
- This behavior is not desirable—IGMP snooping resolves this issue
- Implemented in hardware
  - “Snoops” or intercepts IGMP Joins and Leaves received on interfaces from hosts
  - Enable or disable on a global or per-VLAN basis
  - Ingress port parses packet and sends to CPU for processing, CPU suppresses redundant IGMP joins, and sends one proxy report to router
  - Overrides forwarding or flooding in VLAN

# Cisco Catalyst Intelligent Switching Infrastructure



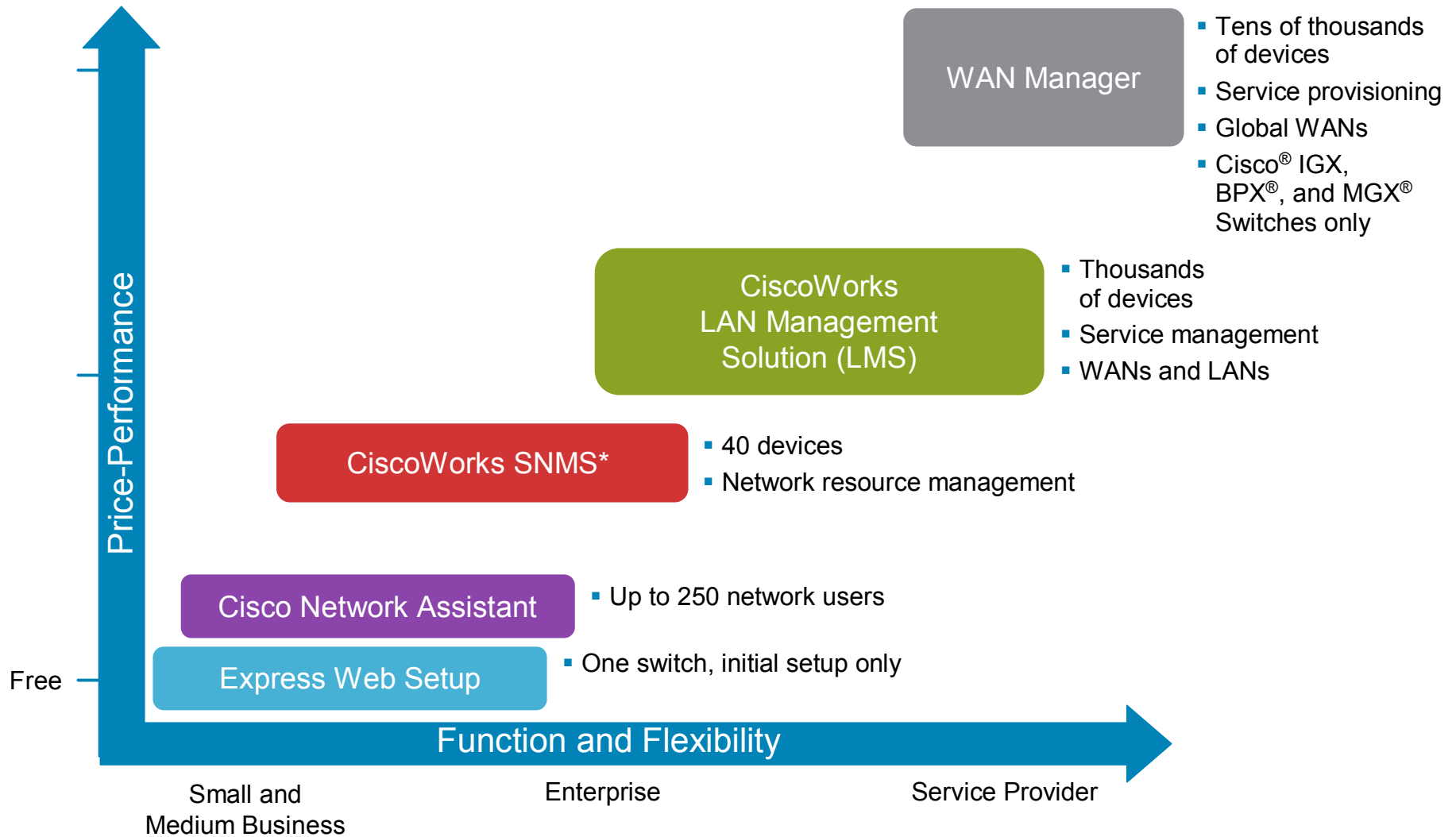
## Features

- End-to-end manageability through common set of management tools
- Centralized administration and software upgrades
- Web-based access

## Benefits

- Simplify implementation, troubleshooting, and upgrades
- Reduce operational costs
- Simplify intelligent service implementation
- Reduced maintenance cost

# Broadest Range of Network Management Products



\*Small Network Management Solution (SNMS)

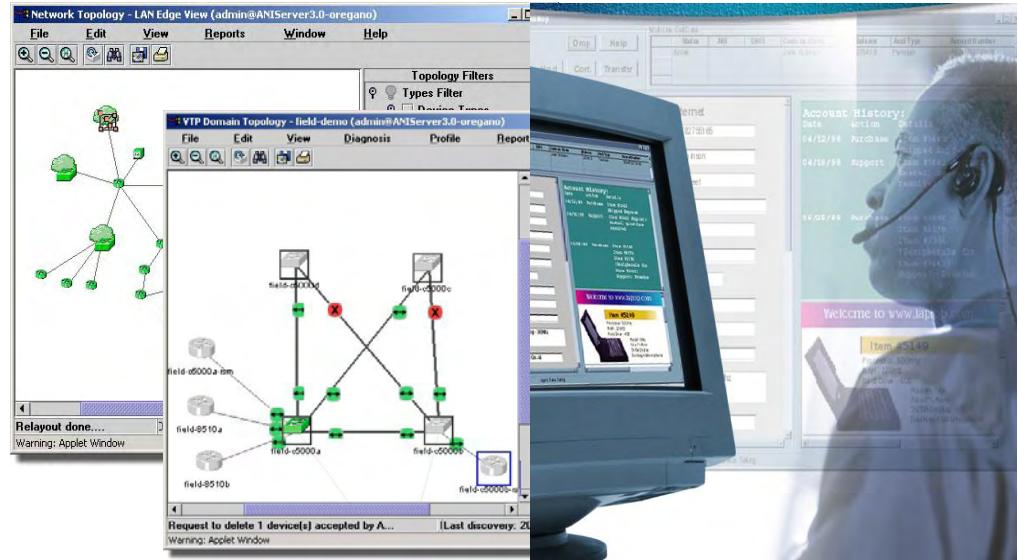
# CiscoWorks

## Configuration

- Single Console Login
- Telnet
- IOS configuration management

## Network Management

- Single IP address to manage system
- RMON1, RMON2, HC-RMON: comprehensive fault diagnostics and performance tuning information
- 4 RMON I groups: stats, history, alarm, events
- SNMP v1, v2, v3 and Standard MIB support



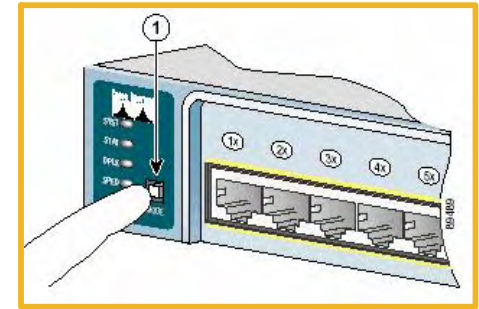
## Network Analysis

- SPAN: port monitoring of one or multiple switch ports
- 4 egress, 2 ingress sessions
- VLAN trunk filtering



# Express Setup

1. Power up switch and hold the mode button for a few seconds until all the mode LEDs are green
2. Connect the PC into the Ethernet port and launch browser
3. Launch Express setup page by entering IP address of 10.0.0.1 in browser
4. Assign switch IP address, management VLAN, enable secret password, (the following is optional) telnet password and SNMP configuration



Close Window

Cisco SYSTEMS

Cisco WS-C2940-8TT-S

HOME  
EXPRESS SETUP  
CLUSTER  
MANAGEMENT SUITE  
TOOLS  
HELP RESOURCES

Express Setup

Management Interface: VLAN1 - Default

IP Address:  IP Subnet Mask: 255.255.255.0

Default Gateway:

Switch Password:  Confirm Switch Password:

Optional Settings

Host Name:

System Contact:  System Location:

Telnet Access:  Enable  Disable

Telnet Password:  Confirm Telnet Password:

SNMP:  Enable  Disable

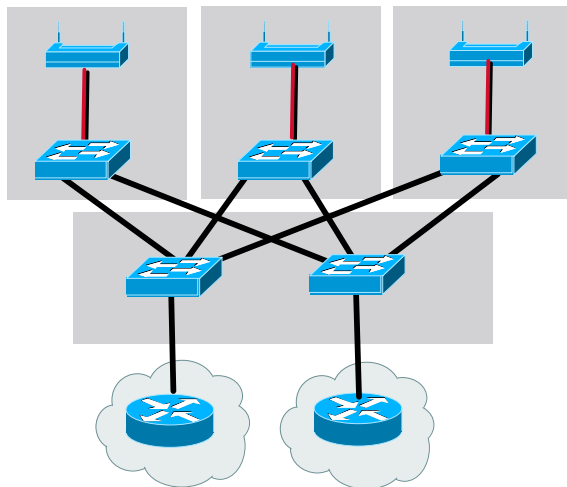
SNMP Read Community:  SNMP Write Community:

Toolkit: Roll over tool

# Smartports Macros

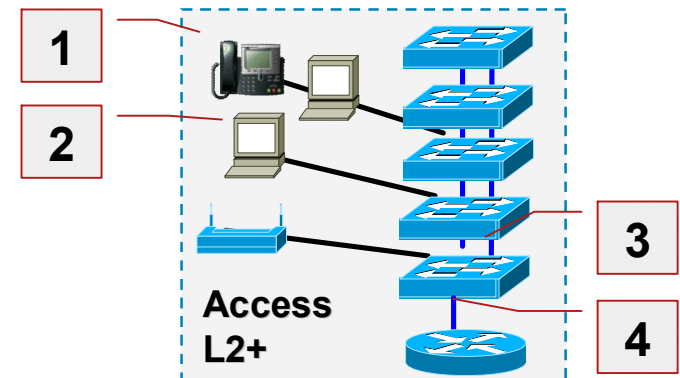
Addressing Complexity and Consistency of Operation within A Role

## Example—Access Switch in Campus



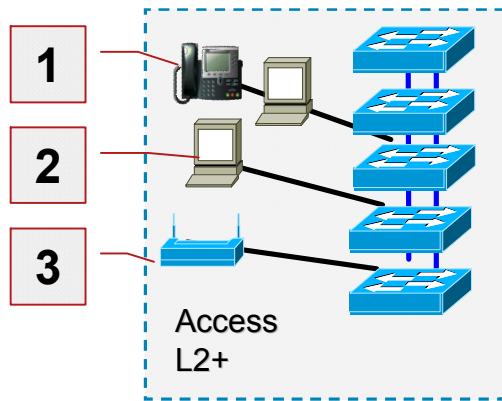
Access Switch

- Breaks a **Role** down to the port level
  1. IP Phone + Standard Desktop
  2. Standard Desktop
  3. Inter Switch
  4. Switch to Router Uplink
- **Standard templates** can be applied for **Products** on a per Role basis
- Apply sophisticated Layer 2 and Layer 3 Features
- Provide “Secret Sauce” that represents Cisco “Best Practices”
- **SMARTPORTS Templates** for this

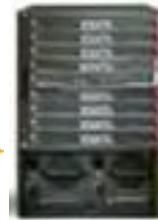


# Smartports Example for Campus

## Narrows the Deployment Options for Customers



Products



6500



4500



3750

### Global Commands for Access Switch Role

```
! Enable dynamic port error recovery for link
state failures.
errdisable recovery cause link-flap

errdisable recovery cause udd
errdisable recovery interval 60

! VTP requires Transparent mode for future
802.1x Guest VLAN
! and current Best Practice
vtp domain [smartports]
vtp mode transparent

! Enable aggressive mode UDLD on all fiber
uplinks
udd aggressive

! Enable Rapid PVST+ and Loopguard
spanning-tree mode rapid-pvst
spanning-tree loopguard default
spanning-tree extend system-id
```

```
! Enable dynamic port error recovery for link
state failures.
errdisable recovery cause link-flap

errdisable recovery cause udd
errdisable recovery interval 60

! VTP requires Transparent mode for future
802.1x Guest VLAN
! and current Best Practice
vtp domain [smartports]
vtp mode transparent

! Enable aggressive mode UDLD on all fiber
uplinks
udd aggressive

! Enable Rapid PVST+ and Loopguard
spanning-tree mode rapid-pvst
spanning-tree loopguard default
spanning-tree extend system-id
```

```
! Enable dynamic port error recovery for link
state
!failureserrdisable recovery cause link-flap
errdisable recovery cause udd
errdisable recovery interval 60

! VTP requires Transparent mode for future
802.1x Guest VLAN
! and current Best Practice
vtp domain [smartports]
vtp mode transparent

! Enable aggressive mode UDLD on all fiber
uplinks
udd aggressive

! Enable Rapid PVST+ and Loopguard
spanning-tree mode rapid-pvst
spanning-tree loopguard default
spanning-tree extend system-id
```

### Access Switch in Campus Role

- Consistent Short form Macros across Products
- Consistent operation for all Products

### Interface Commands for Port Type by Role

```
interface range FastEthernet0/[1 - 48]
switchport access vlan [data]
switchport mode access
switchport voice vlan [voice]

! Enable port security limiting port to 3 MAC
addresses. Ensure age is
! greater than one minute and use inactivity
timer
switchport port-security
switchport port-security maximum 3
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity

! Enable auto-qos to extend trust to attached
Cisco phone
auto qos voip cisco-phone

! Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable
```

```
interface range FastEthernet0/[1 - 48]
switchport access vlan [data]
switchport mode access
switchport voice vlan [voice]

! Enable port security limiting port to 3 MAC
addresses. Ensure age is
! greater than one minute and use inactivity
timer
switchport port-security
switchport port-security maximum 3
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity

! Enable auto-qos to extend trust to attached
Cisco phone
auto qos voip cisco-phone

! Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable
```

```
! Reset all end-station interfaces to default
configuration (global command)
default interface range FastEthernet[1]0/[1 - 48]
! VoIP enabled interface - Enable voice (VVID)
and data VLAN
interface range FastEthernet[1]0/[1 - 48]
switchport access vlan [data]
switchport mode access
switchport voice vlan [voice]
! Enable port security limiting port to 3 MAC
addresses. Ensure age is
! greater than one minute and use inactivity
timer
switchport port-security
switchport port-security maximum 3
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity

! Enable auto-qos to extend trust to attached
Cisco phone
auto qos voip cisco-phone

! Configure port as an edge network port

! Ensure that another switch cannot become
active on this interface
spanning-tree portfast
spanning-tree bpduguard enable
```

# Cisco Catalyst 3560 Series Intelligent Features Summary

## Availability

- IP Unicast Routing
  - Static, RIPv1/v2, OSPF, IGRP, EIGRP, BGPv4
- IP Multicast Routing
  - PIM, DVMRP tunneling
- Hot Standby Router Protocol (HSRP)
- Web Cache Comm. Protocol (WCCP)
- Policy Based Routing (PBR)
- Spanning-Tree Protocol enhancements
  - UplinkFast, BackboneFast, PortFast
  - 802.1s/w
- Port Grouping
  - EtherChannel (Gigabit, Fast)
  - 802.3ad
  - Port Aggregation Protocol (PAgP)
  - Link Agg. Control Protocol (LACP)
- Layer 2 load balancing (PVST)
- Layer 3 load balancing (ECR)
- Cisco® Express Forwarding
- Redundant Power Supply (RPS 675)

## Security

- IBNS through 802.1x
- Access Control Lists
- Unicast MAC filtering
- SSH, Kerberos, SNMPv3
- Private VLAN Edge
- DHCP interface tracker
- DHCP Snooping Option 82
- CMS security wizard
- Private VLAN edge
- Port security
- MAC address notification



## Quality of Service

- Queue servicing:
  - Shaped round robin and strict priority queuing
  - Weighted tail drop
  - Ingress traffic policing
  - Egress traffic shaping
- 802.1p CoS and DSCP
- Congestion avoidance
  - Granular rate limiting
  - Auto QoS

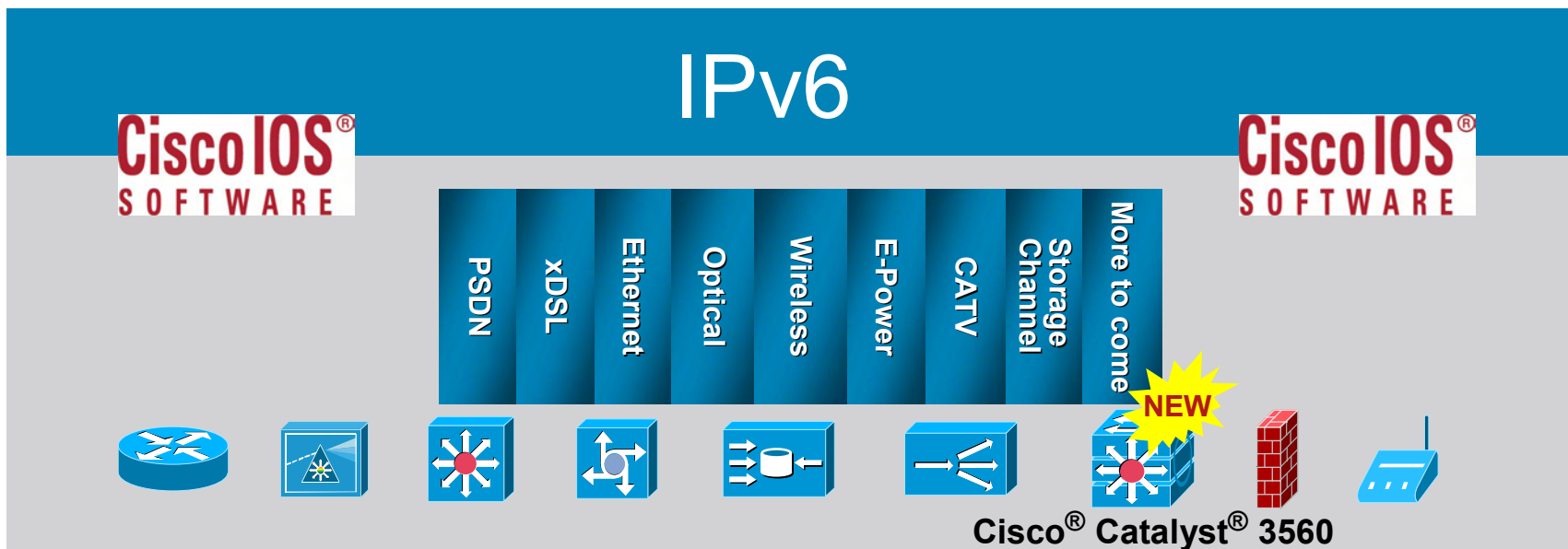
## Manageability

- Autoconfiguration
- Cisco Intelligent Power Management
- Cisco CMS Software
- CiscoWorks
- Cisco Express Setup
- Voice VLAN
- Dynamic VLAN
- SmartPorts
- DHCP Server

# Cisco Catalyst 3560 Series Switches— IPv6-Capable Routing in Hardware



With millions of new devices becoming IP aware, the need for increased addressing and “plug-and-play” networking is only met with the implementation of IPv6





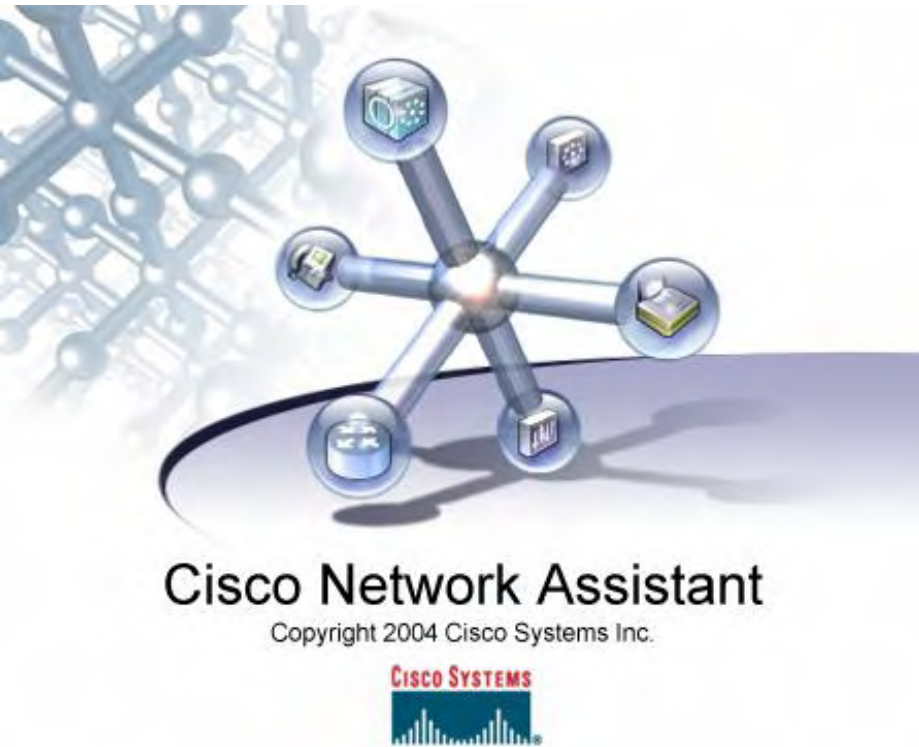
# Agenda



- Cisco® Catalyst® Switches Overview
- Catalyst 3560 Product Overview
- Power over Ethernet
- Intelligent Services
- Cisco Network Assistant
- Deployment Examples
- Service and Support



# Cisco Network Assistant



- Automatic network discovery
- Front panel view
- Dynamic Application Update
- Smartports
- Cross launch device managers
- No additional cost!

# Single Point of Management

- Autodiscovery of Cisco® devices: Switches, Routers, Access Points, and IP Phones

- Displayed physical network topology along with network elements details such as:

Name

IP address

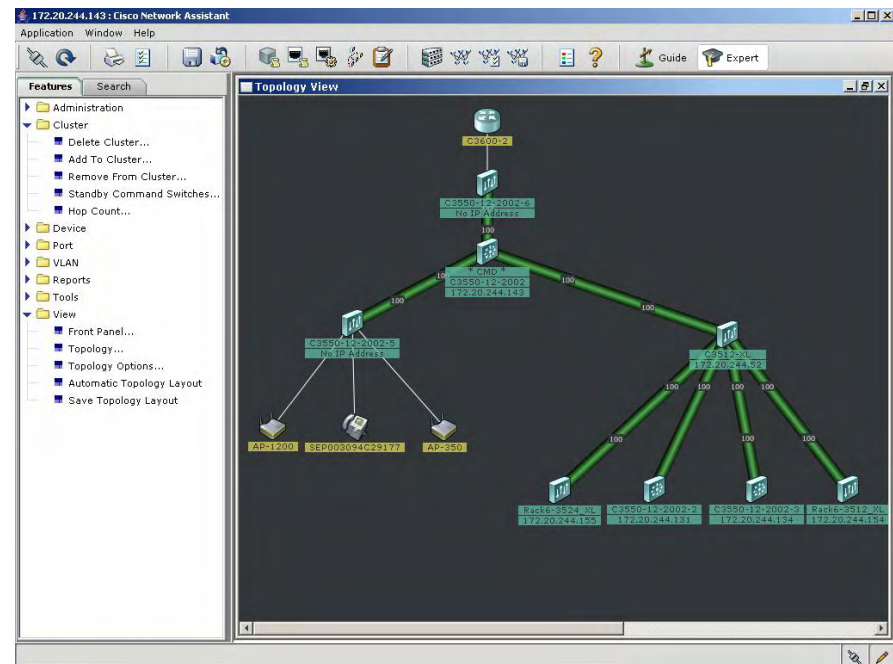
MAC address

State of the network element

- Links between network elements are also represented with:

Link speed

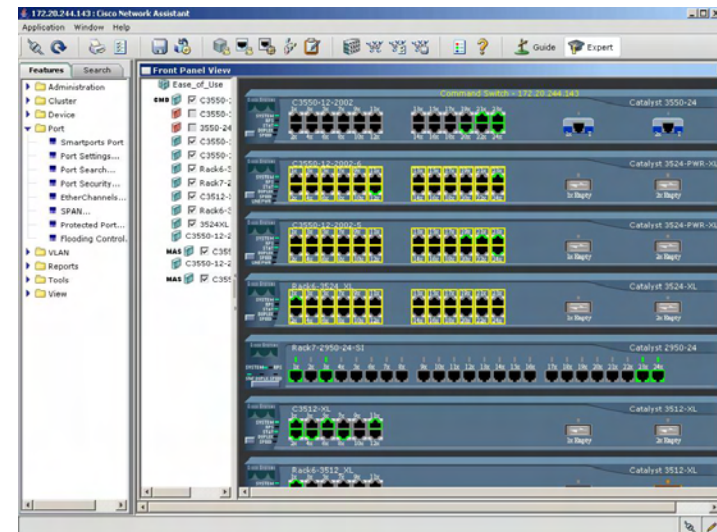
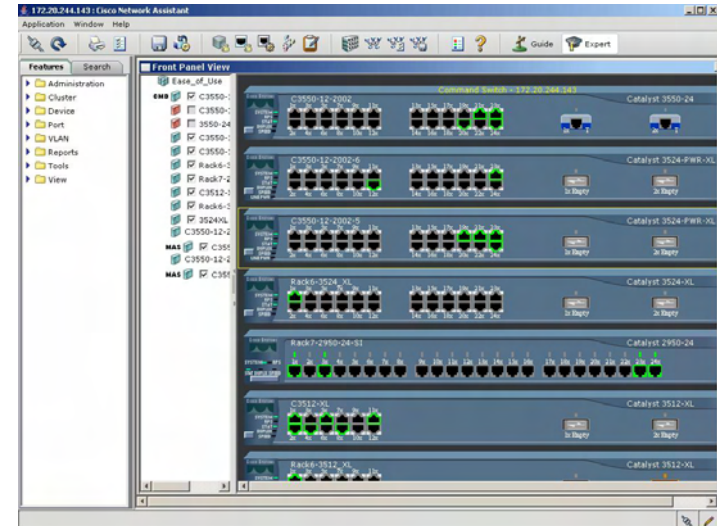
Link status



Allows administrator to view live network information, including the status of switches and network connection

# Front Panel View

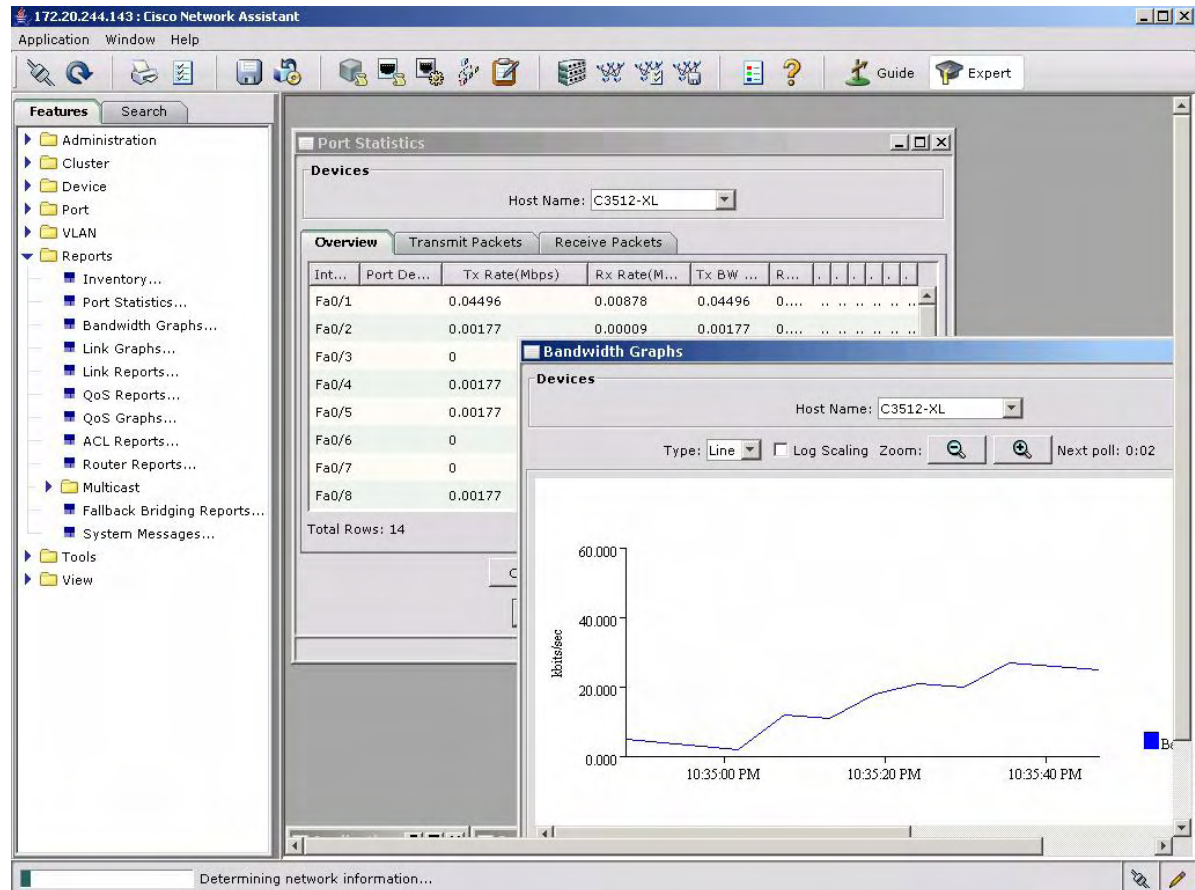
- Front Panel View give the administrator a rapid view of the status of his switches. Each interfaces (ports) are depicted using different color to depict it state (speed, duplex, up, down, disable)
- Also allows the user to simply use their mouse to select ports in order to configure such a thing like VLANs across multiple switches



# Monitor, Analyze and Troubleshoot

The Network Assistant offers a wide array of tools that allow users to:

- Monitor bandwidth utilization, power consumption
- Analyze port/QoS/ACL statistics
- Examine link performances
- Test using Ping and Trace





# Reports

The screenshot displays the Cisco Network Assistant interface for device 172.20.244.143. The left-hand navigation pane shows a tree structure with 'Reports' expanded to show various report types, including 'ACL Reports...'. The main window is titled 'Topology View' and contains a 'Bandwidth Graphs' sub-window with a line graph showing traffic in Kbits/sec over time. Below the graph, the 'ACL Reports' sub-window is open, displaying 'ACL Hardware Counters' for device C3550-12-2002. The counters table is as follows:

ACL Hardware Counters	
Input Drops:	0 matches (0 bytes)
Output Drops:	0 matches (0 bytes)
Input Forwarded:	6211026615 matches (710266984471 bytes)
Output Forwarded:	0 matches (0 bytes)
Input Bridge Only:	0 matches (0 bytes)
Bridge and Route in CPU:	0 matches (0 bytes)
Route in CPU:	1285488244 matches (82271482208 bytes)

# Smartports

From This:

## Global Commands

```
failureserrdisable recovery cause link-flap
errdisable recovery cause udd
errdisable recovery interval 60
vtp domain [smartports]
vtp mode transparent
udld aggressive
spanning-tree mode rapid-pvst
spanning-tree loopguard default
spanning-tree extend system-id
```

## Interface Commands

```
default interface range FastEthernet[1]/0/[1 - 48]
interface range FastEthernet[1]/0/[1 - 48]
switchport access vlan [data]
switchport mode access
switchport voice vlan [voice]
switchport port-security
switchport port-security maximum 3
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
auto qos voip cisco-phone
spanning-tree portfast
spanning-tree bpduguard enable
```

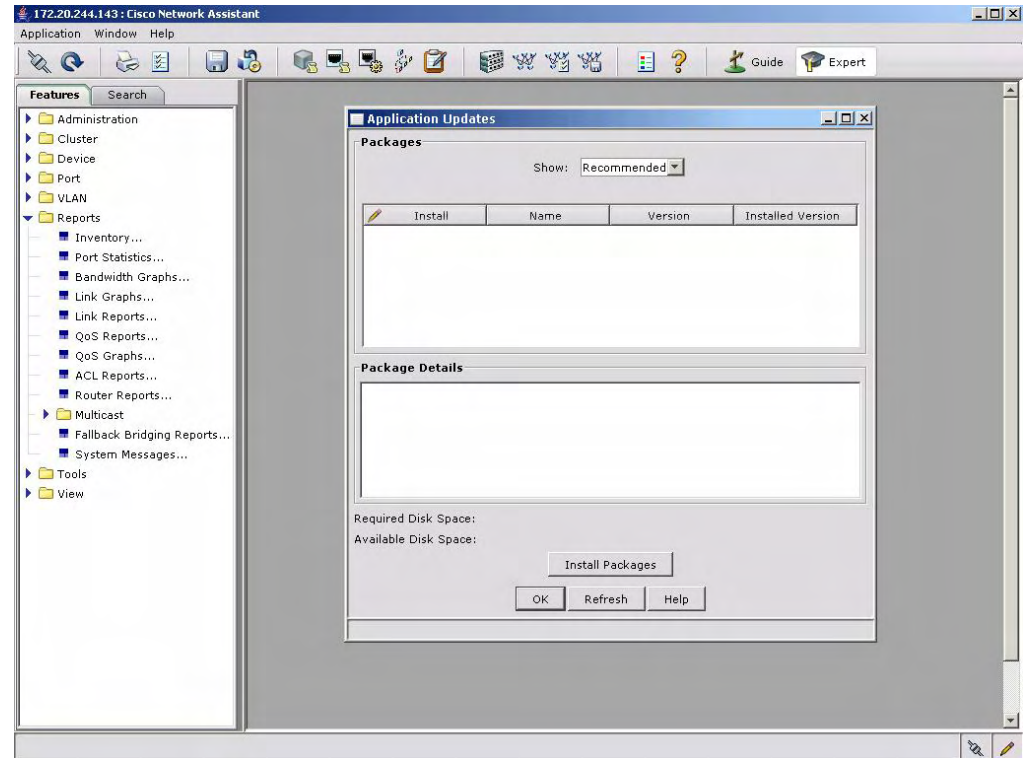
To This:





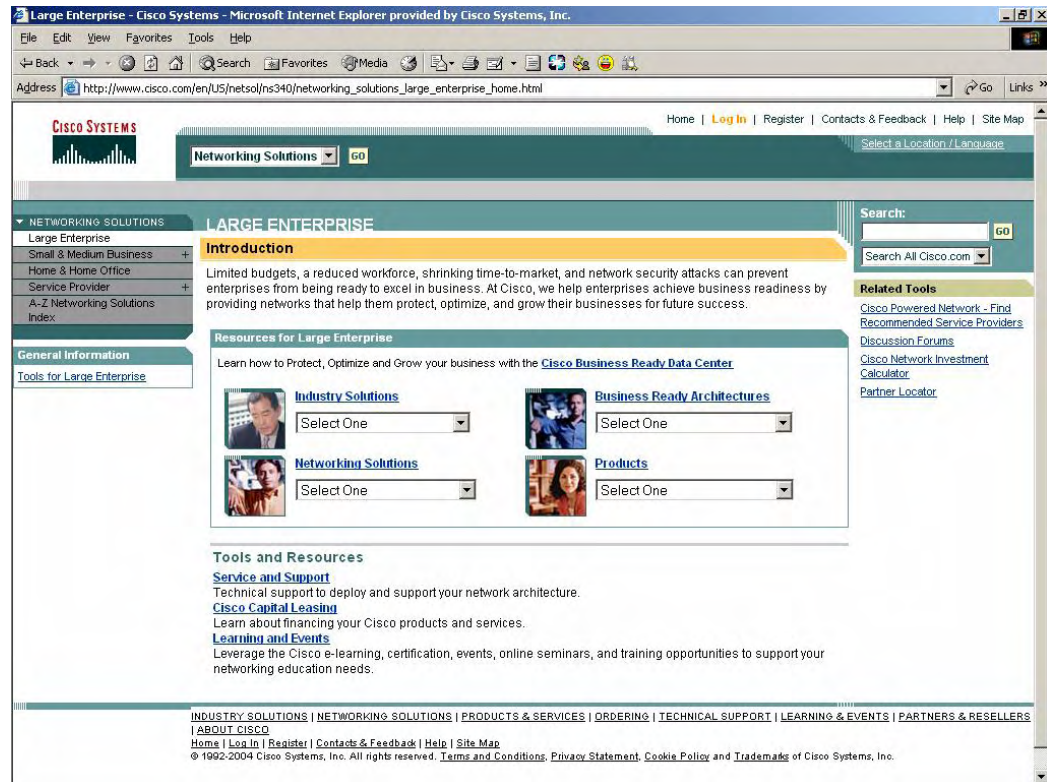
# Automatic Application Update

- The Network Assistant automatically update itself via Cisco.com
- Users will be able to use the most current and updated version without having to wait for a new versions of to be released.



# Download Network Assistant

- Free download
- Guest Login
  - No CA contract requirements
  - Answer a few questions



<http://www.cisco.com/go/NetworkAssistant>

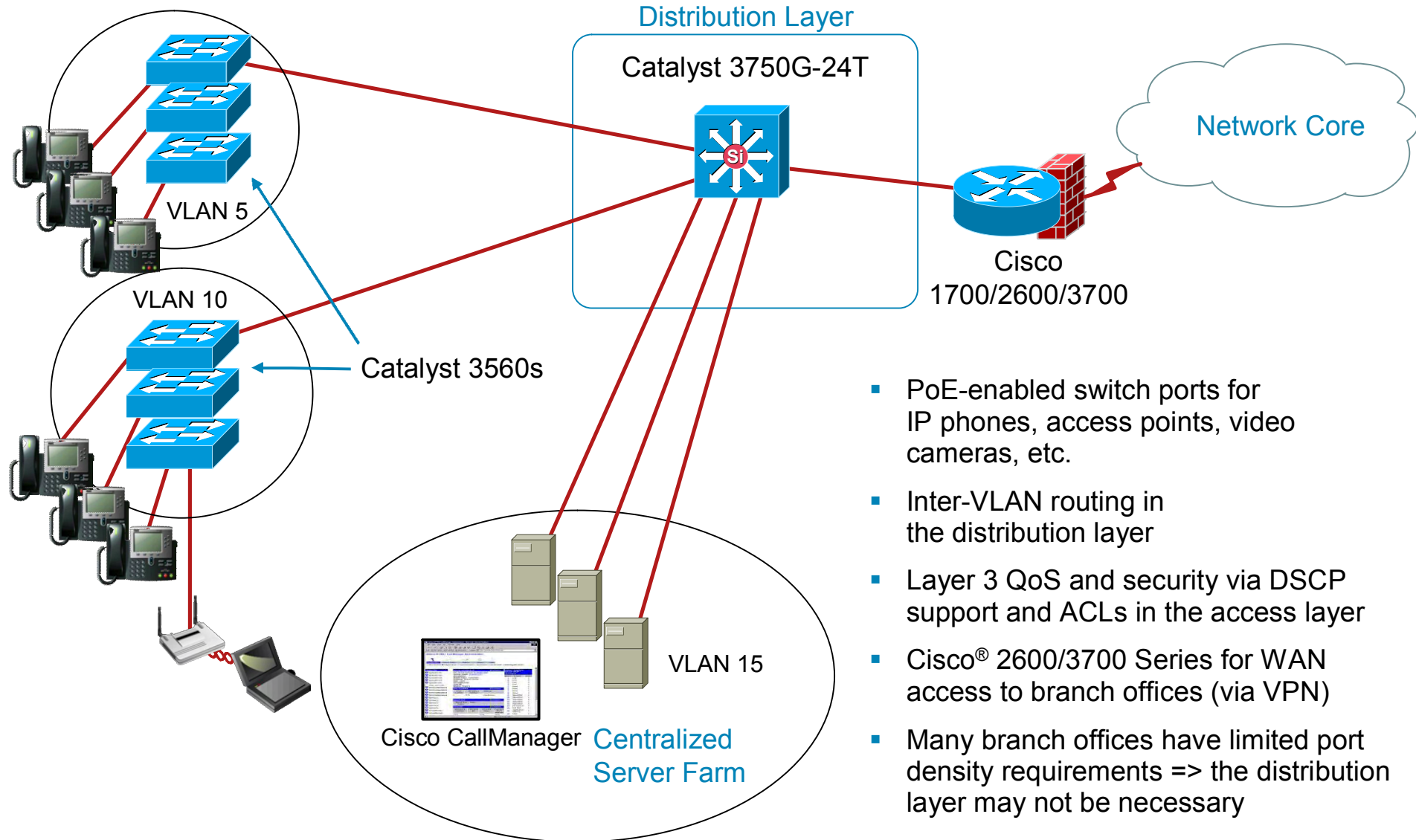
# Agenda



- Cisco® Catalyst® Switches Overview
- Catalyst 3560 Product Overview
- Power over Ethernet
- Intelligent Services
- Cisco Network Assistant
- **Deployment Examples**
- Service and Support

# Enterprise Branch Office

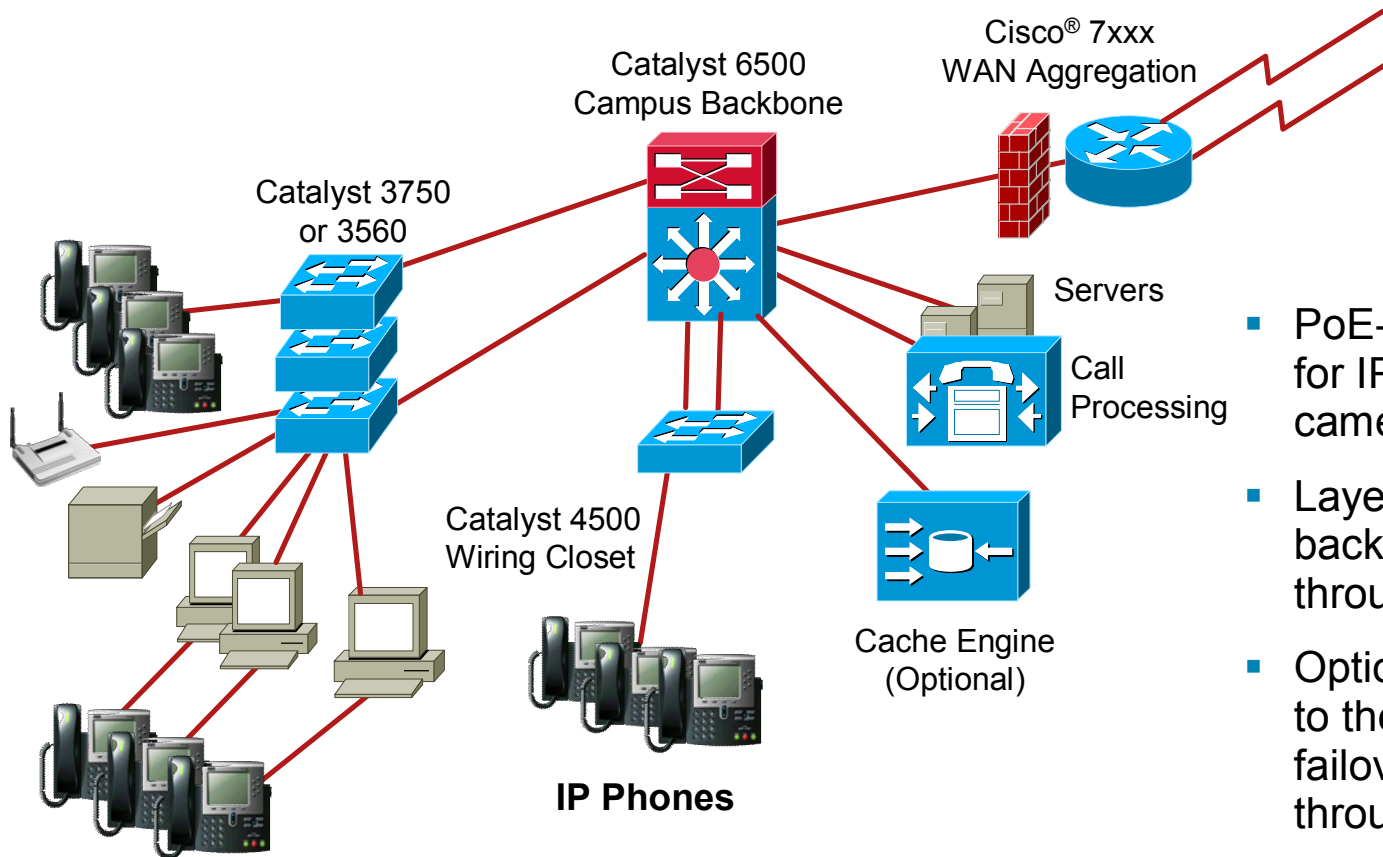
## Catalyst 3560 Switches Aggregated by a Catalyst 3750



- PoE-enabled switch ports for IP phones, access points, video cameras, etc.
- Inter-VLAN routing in the distribution layer
- Layer 3 QoS and security via DSCP support and ACLs in the access layer
- Cisco® 2600/3700 Series for WAN access to branch offices (via VPN)
- Many branch offices have limited port density requirements => the distribution layer may not be necessary

# Enterprise Wiring Closet:

## Cisco Catalyst 3560/4500/6500 Integrated Campus



Layer 2 or Layer 3 Wiring Closet Uplinks

- PoE-enabled switch ports for IP phones, access points, cameras, etc.
- Layer 2 uplinks to the backbone—load sharing through PVST+
- Option for routed uplinks to the backbone for faster failover—load sharing through equal cost routing
- Layer 3 QoS and security via DSCP support and ACLs in the access layer

# Agenda



- Cisco® Catalyst® Switches Overview
- Catalyst 3560 Product Overview
- Power over Ethernet
- Intelligent Services
- Cisco Network Assistant
- Deployment Examples
- **Service and Support**



# Services and Warranty for the Cisco Catalyst 3650 Series Switch

- **Limited lifetime hardware warranty**
  - Advance Replacement shipping within 10 business days
  - Guest access to Cisco.com
- **Cisco® Total Implementation Solutions (TIS)**
  - Project management and training
  - Installation, test, and cutover
  - Major moves, adds, and changes
  - Design review and product staging
- **Configuration and verification services that ease deployment of networkwide intelligent services—QoS and multicast management**
- **Cisco SMARTnet® and SMARTnet Onsite**
  - 24-hour access to technical support through the Web, e-mail, and phone
  - Advance Replacement of hardware parts in as little as 2 hours
  - Onsite field engineer (Cisco SMARTnet Onsite) to assist in hardware replacements



# Operational Technical Support Services

Service Category	Service Description	Warranty	SAS	SASU	NBD	8x5x4	24x7x4	24x7x2	NBD	8x5x4	24x7x4	24x7x2
Onsite Services	24 hr/day, 7 days/wk, 2-hr response											✓
	24 hr/day, 7 days/wk, 4-hr response											✓
	8 hr/day, 5 days/wk, 4-hr response										✓	
	8 hr/day, 5 days/wk, next business day									✓		
Advance Replacement of Hardware	24 hr/day, 7 days/wk, 2-hr response							✓				✓
	24 hr/day, 7 days/wk, 4-hr response						✓				✓	
	8 hr/day, 5 days/wk, 4-hr response					✓				✓		
	8 hr/day, 5 days/wk, next business day				✓				✓			
	10 business day replacement	✓										
Diagnostics	24 hr/day, 7 days/wk Cisco® TAC access		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Registered Cisco.com access		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Technology Refresh	Software updates			✓	OS	OS	OS	OS	OS	OS	OS	OS
	Software maintenance	✓	✓	✓	OS	OS	OS	OS	OS	OS	OS	OS

# Cisco is Your Partner for Delivering Intelligent Networks

- More than 1600 support engineers, 40 percent with CCIE® certification
- Average 15 years experience
- 80 percent issues resolved online
- Multiple awards for service
- 30,000 Cisco® Technical Assistance Center cases per month
- 5000+ partners worldwide deliver direct and subcontracted services for Cisco technology
- 1200+ partner-employed CCIE professionals



# Summary



- IEEE 802.3af and Cisco® prestandard PoE fixed configuration switch offerings
  - Integrated ASIC technology allows both PoE implementations on the same switch
  - Cisco intelligent power management features that enhance PoE management capabilities
- Enables the deployment of network-wide intelligent services
- Comprehensive set of Cisco IOS® Software features for advanced functions and control
- Lowers operating expenses by easing deployment and management

