Zero Touch Provisioning IOS

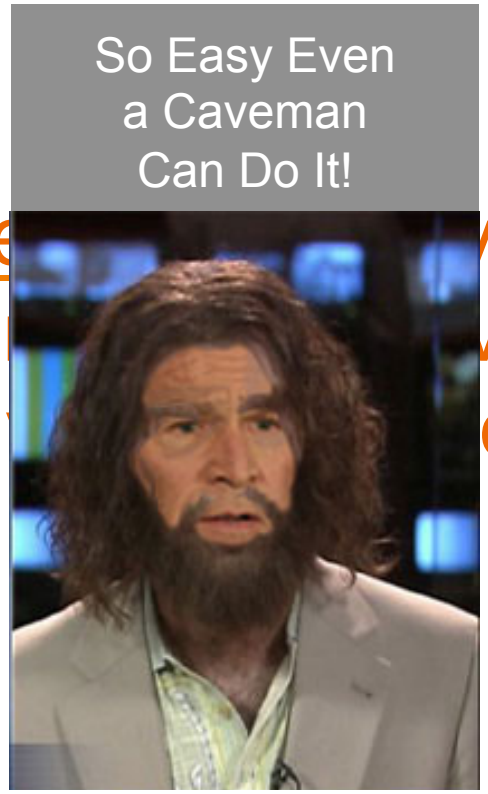
BRKCDN-2010

Housekeeping

- We value your feedback- don't forget to complete your online session evaluations after each session & complete the Overall Conference Evaluation which will be available online from Thursday
- Visit the World of Solutions
- Please remember this is a 'non-smoking' venue!
- Please switch off your mobile phones
- Please make use of the recycling bins provided
- Please remember to wear your badge at all times

The Zero-Touch Mantra

In IOS, you alre verything you need to ze vision and deploy evices



Agenda

- Zero-touch Provisioning Devices
  - Getting that thing booted – Autoinstall
  - Centralized Model - Web Services, Telnet, perl
  - Autonomous model – EEM/Tcl/IOS.sh
  - Commercial solutions – Cisco Config Engine
- Zero-touch Provisioning Services
  - Scripting - IOS.sh
  - Discovering - Auto-SmartPorts
- Demo – Let's Take it For a Spin

Q&A

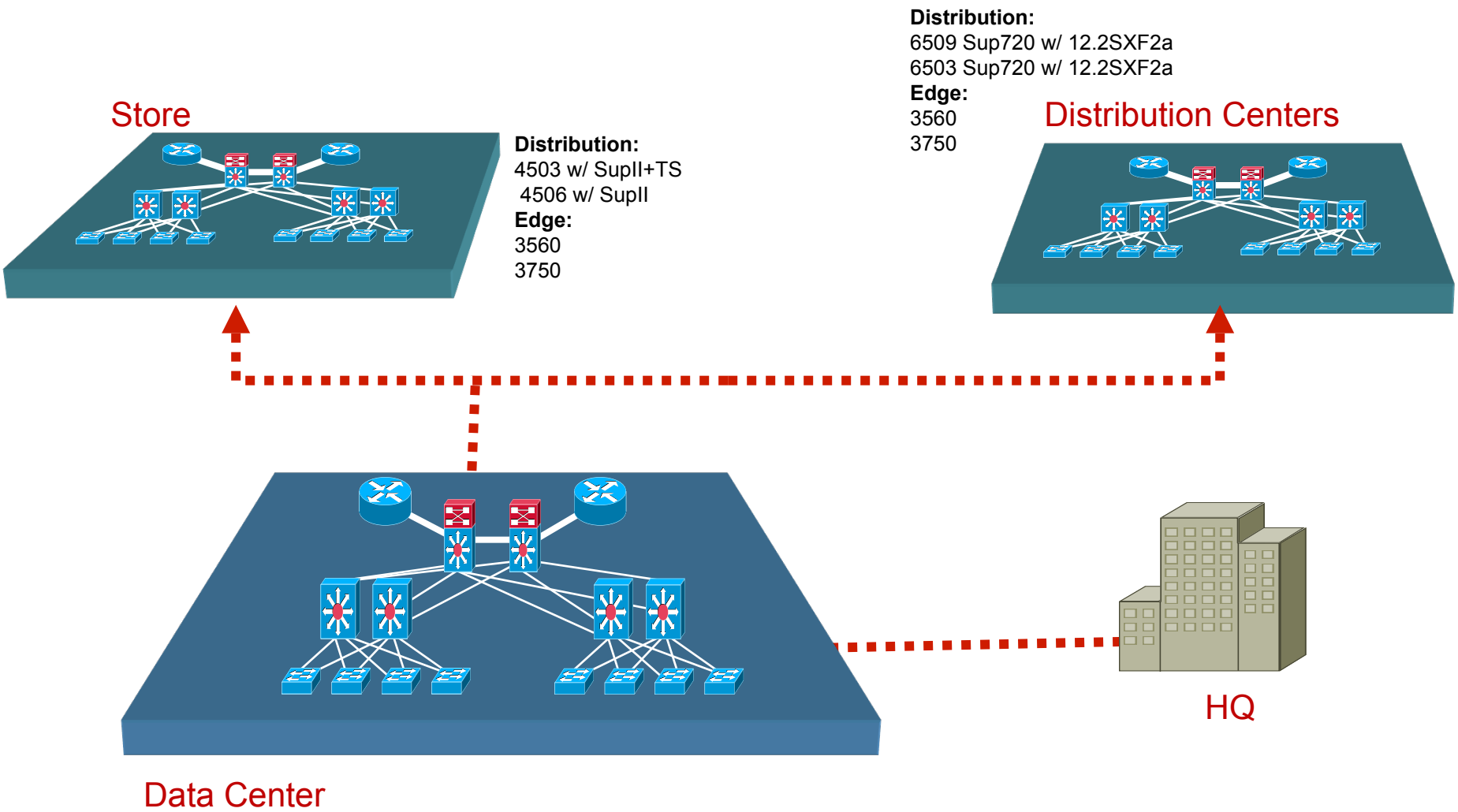
Why Zero-touch Provisioning?

- It is estimated that over 80% of all network downtime can be attributed to human error
- Networks are getting more complex
- Manual configuration is slow
- People are expensive
- Travel is expensive

When to Zero-Touch

- Large number of smaller devices
- Geographically distributed devices
- “Cookie cutter” setups
- Policy/rule driven setups
- Policy/rule driven “service” enablement
- Large number of “services”

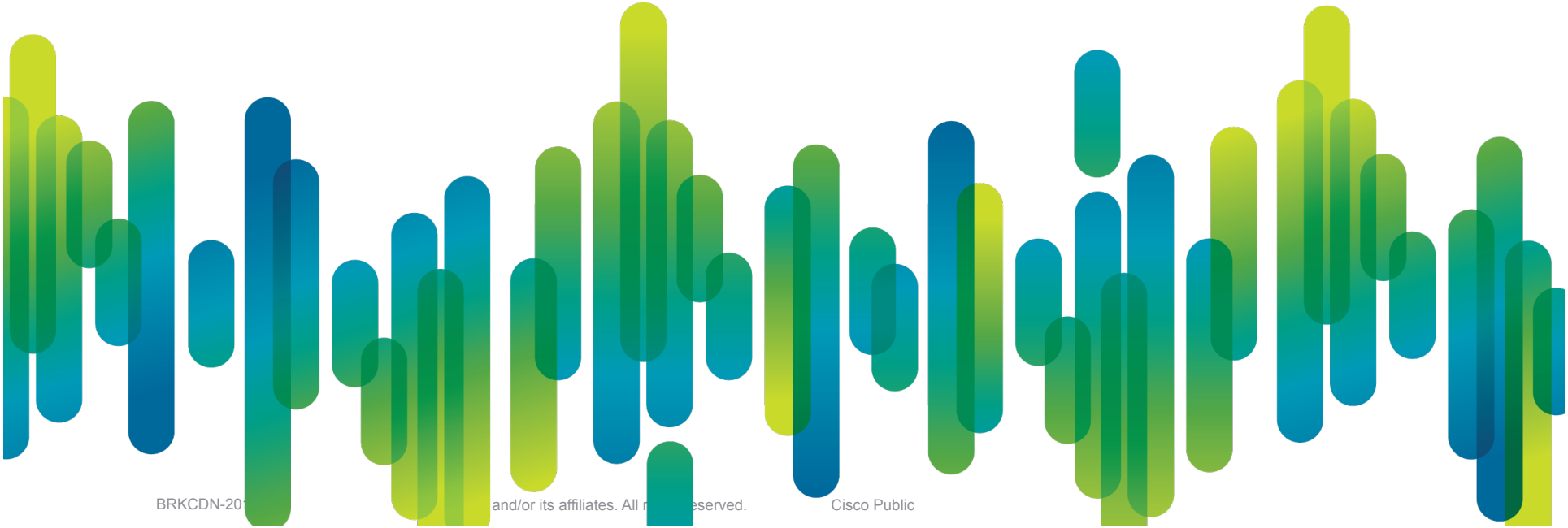
ZTP Use Case



Zero-touch – Build or Buy?

- Commercial products
  - Cisco Config Engine
  - CNS agent (in IOS for years)
- In-house Built
  - Off-box scripts
  - On-box scripts
  - Auto-install
  - Web Services Management Agent with DHCP option 43

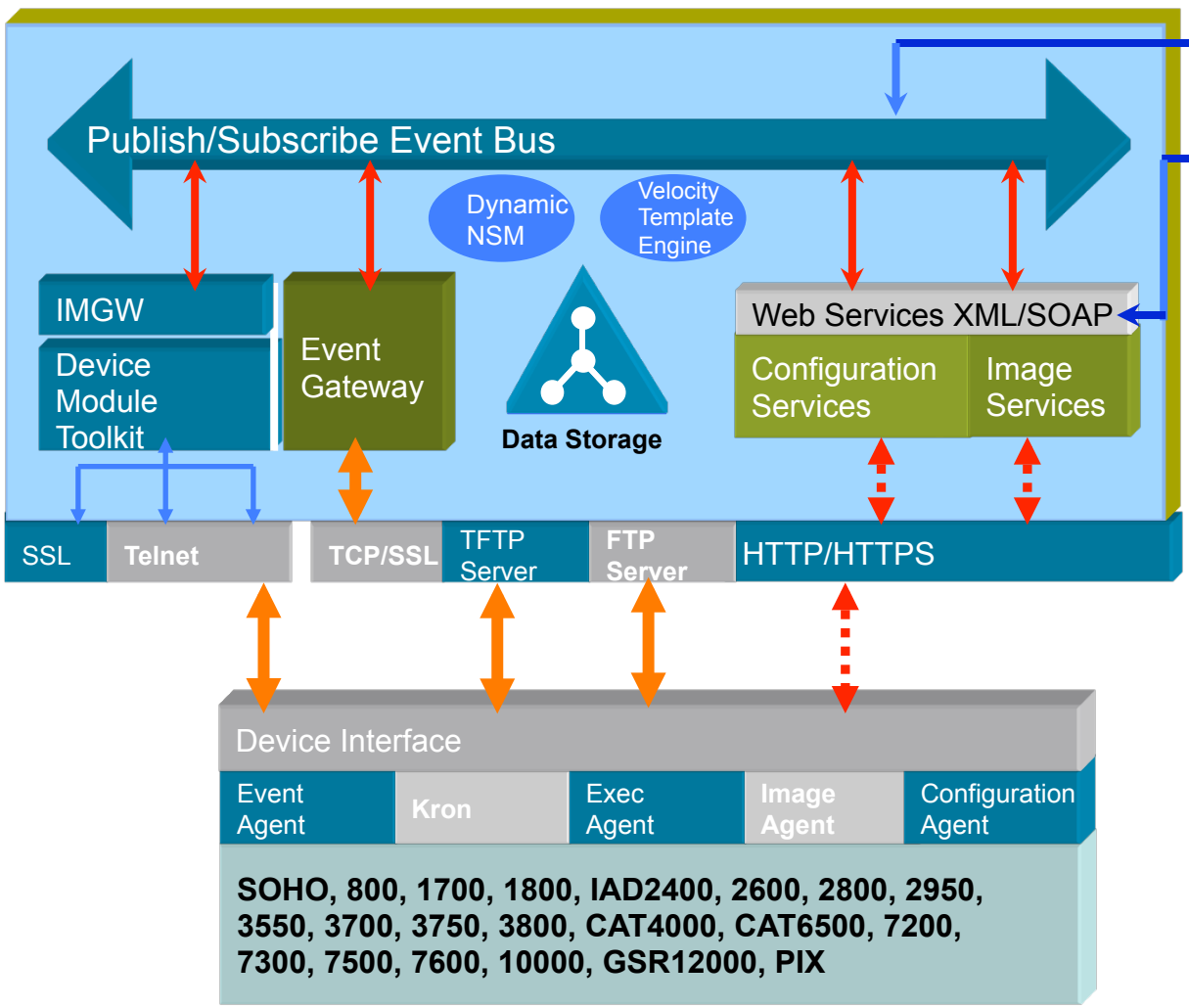
Cisco Config Engine



Zero Touch Provisioning —

Automated Ordering, Configuration and Service Turn-Up

Config Engine Architecture



Configuration Service

- Delivers initial (or partial) configuration

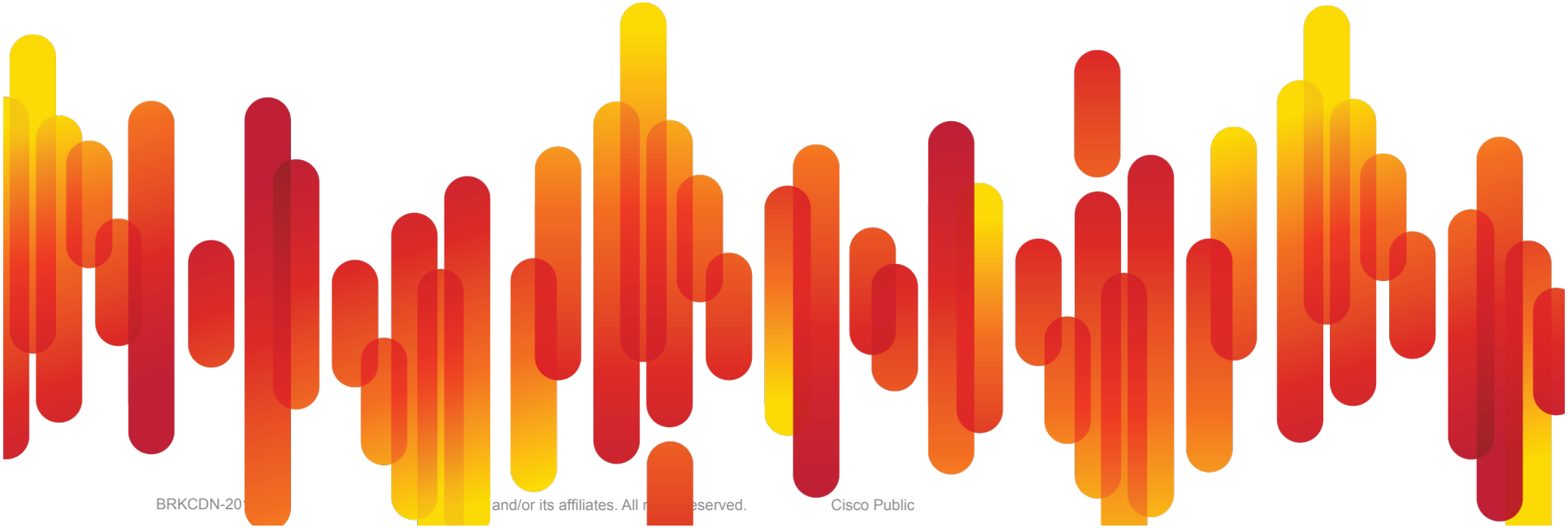
Image Service

- Distributes and activate software image to Cisco devices

Event Gateway

- Acts as an interface between the devices and the event bus

In-House Zero Touch



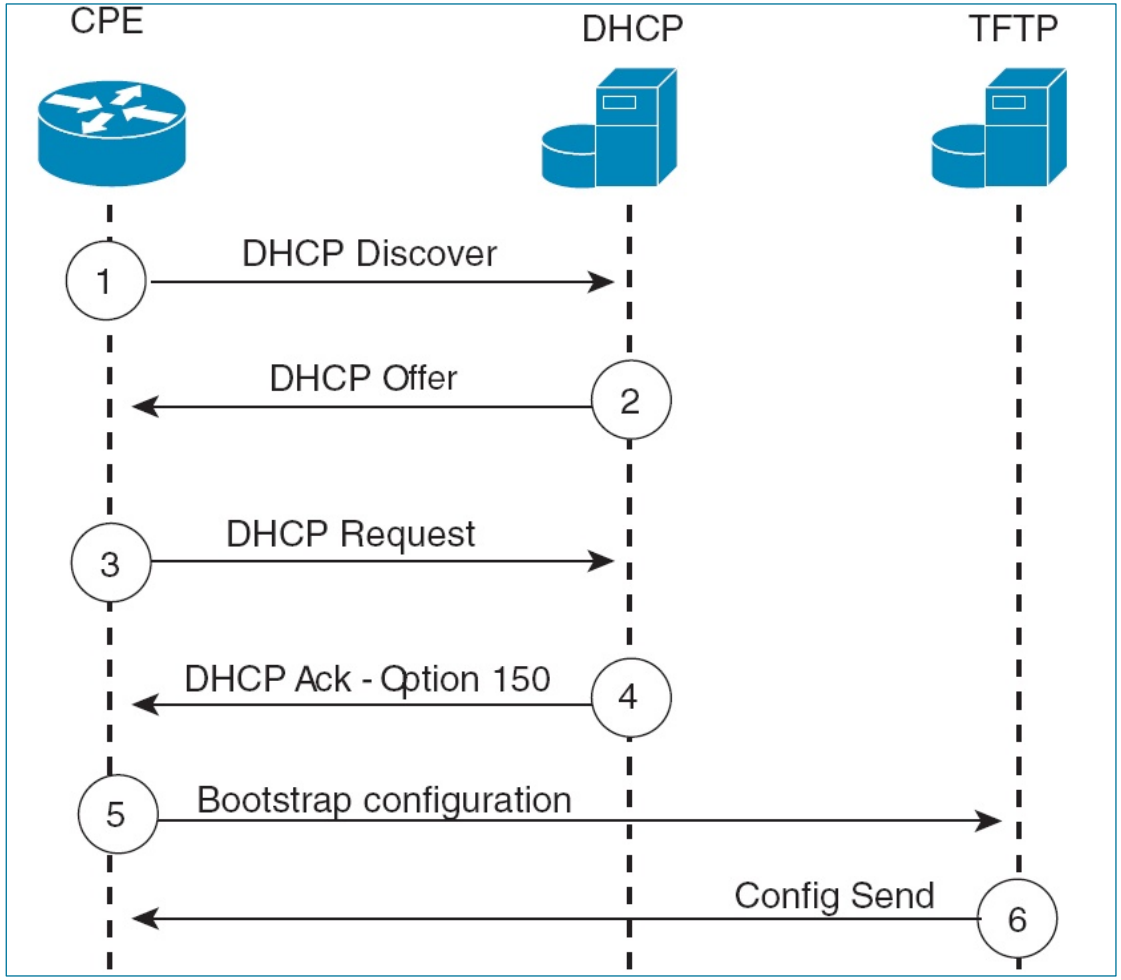
Bare Metal Boot

- All versions of IOS can obtain a bootstrap configuration using IOS Autoinstall
- Programmatic code (scripts) can be embedded in the bootstrap configuration
- The code can adapt the device based on:
  - Place in the network
  - Type of device
  - Neighbors
  - Interface speed
  - etc

What Pieces do I Need?

- DHCP servers – get IP address, mask, DNS, etc
- TFTP server – get bootstrap config
- EEM – launch and schedule
- Install script (applet or IOS.sh) – fine tune the config
- Tcl program, WSMA, perl – optional advanced configuration

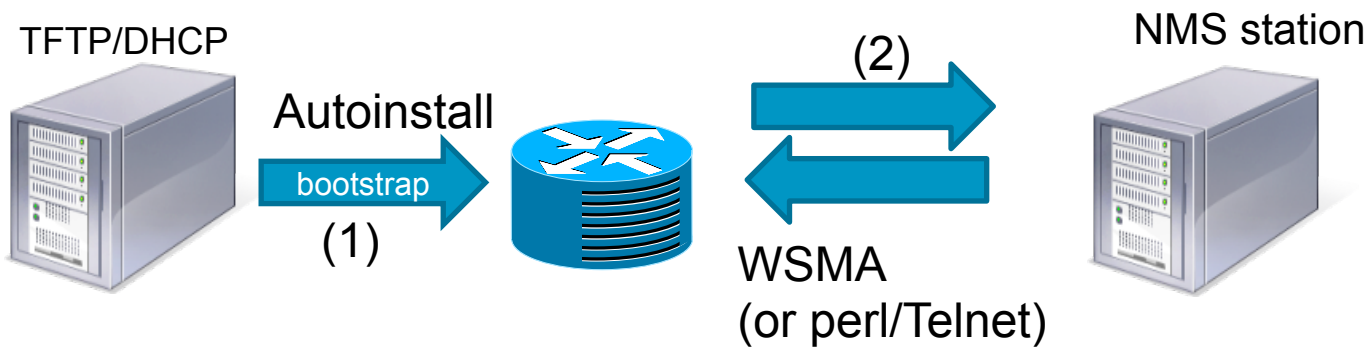
AutoInstall Dialog



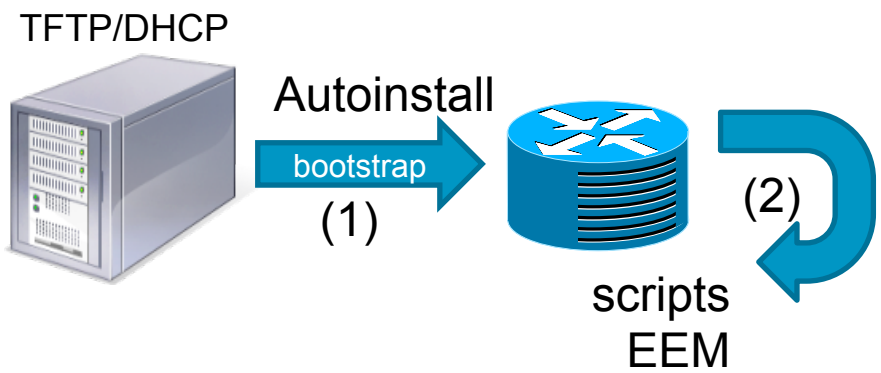
In-house ZTP

Centralized vs Autonomous

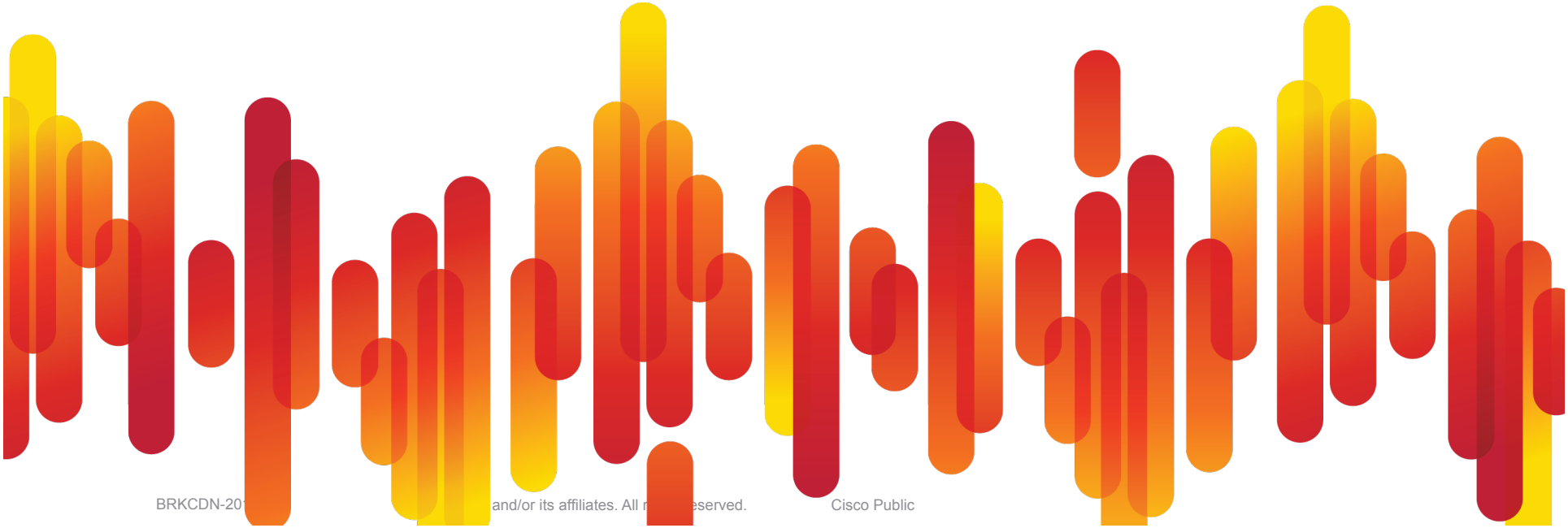
1. Centralized



2. Autonomous



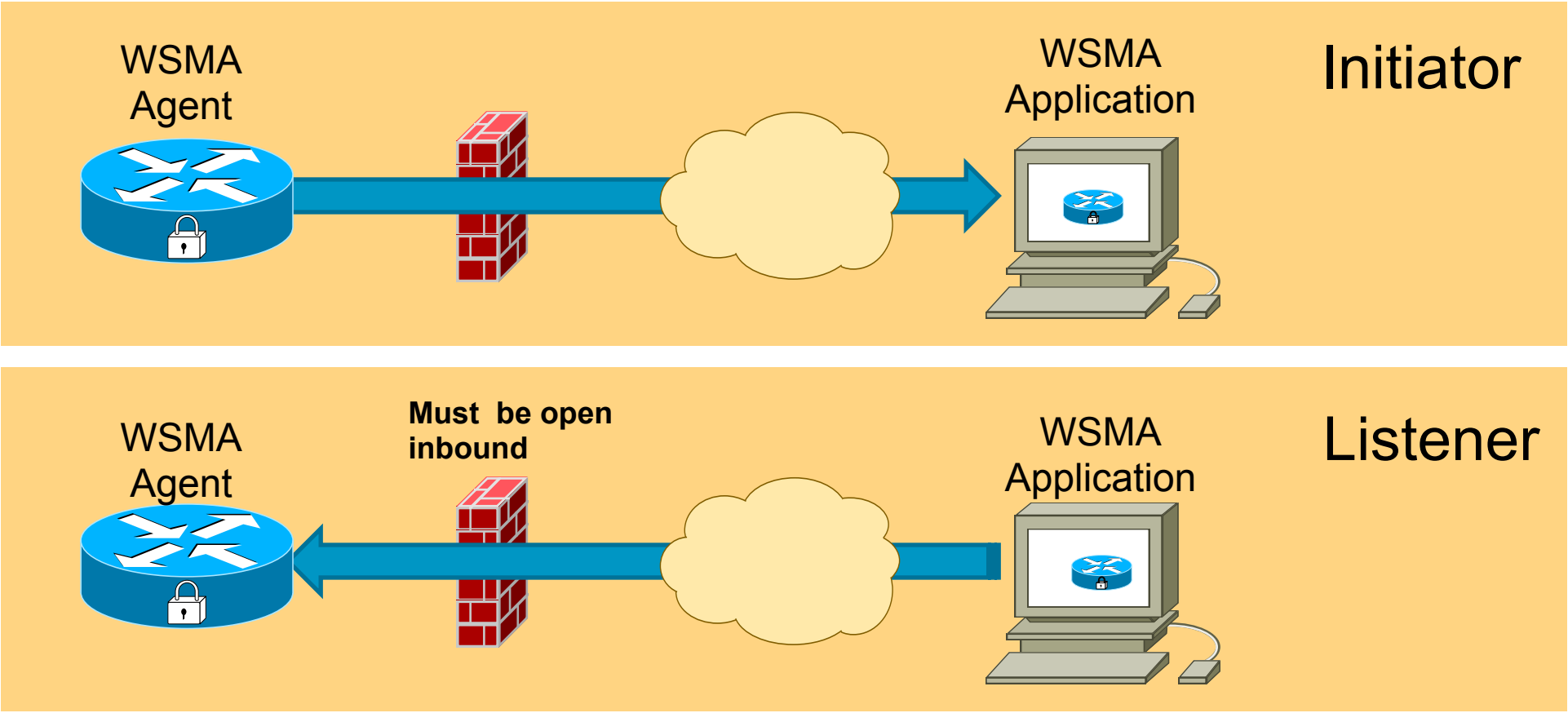
Zero Touch Provisioning With WSMA



Web Services Overview

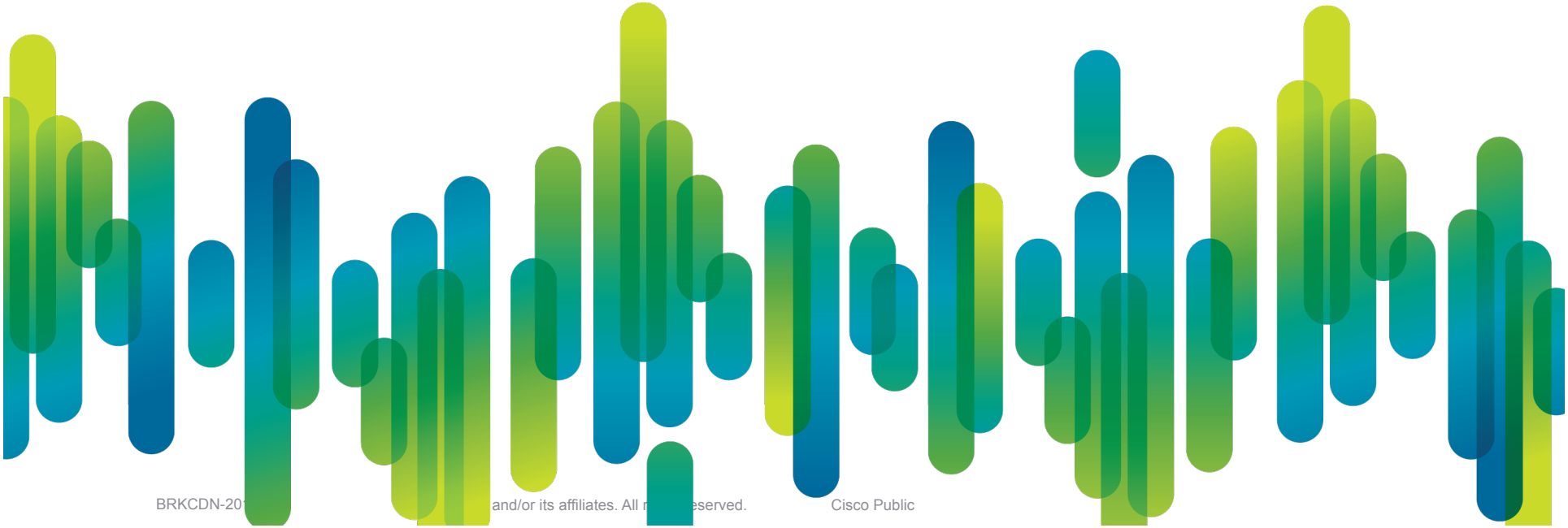
- Embedded Web Server in IOS is called Web Services Management Agent (WSMA)
- Four Web Services – Config, Exec, File System and Notify
- Each web service conforms to a schema published and maintained by Cisco
- A device can get all it's boot and WSMA configuration from a DHCP server using option 43.

WSMA Modes

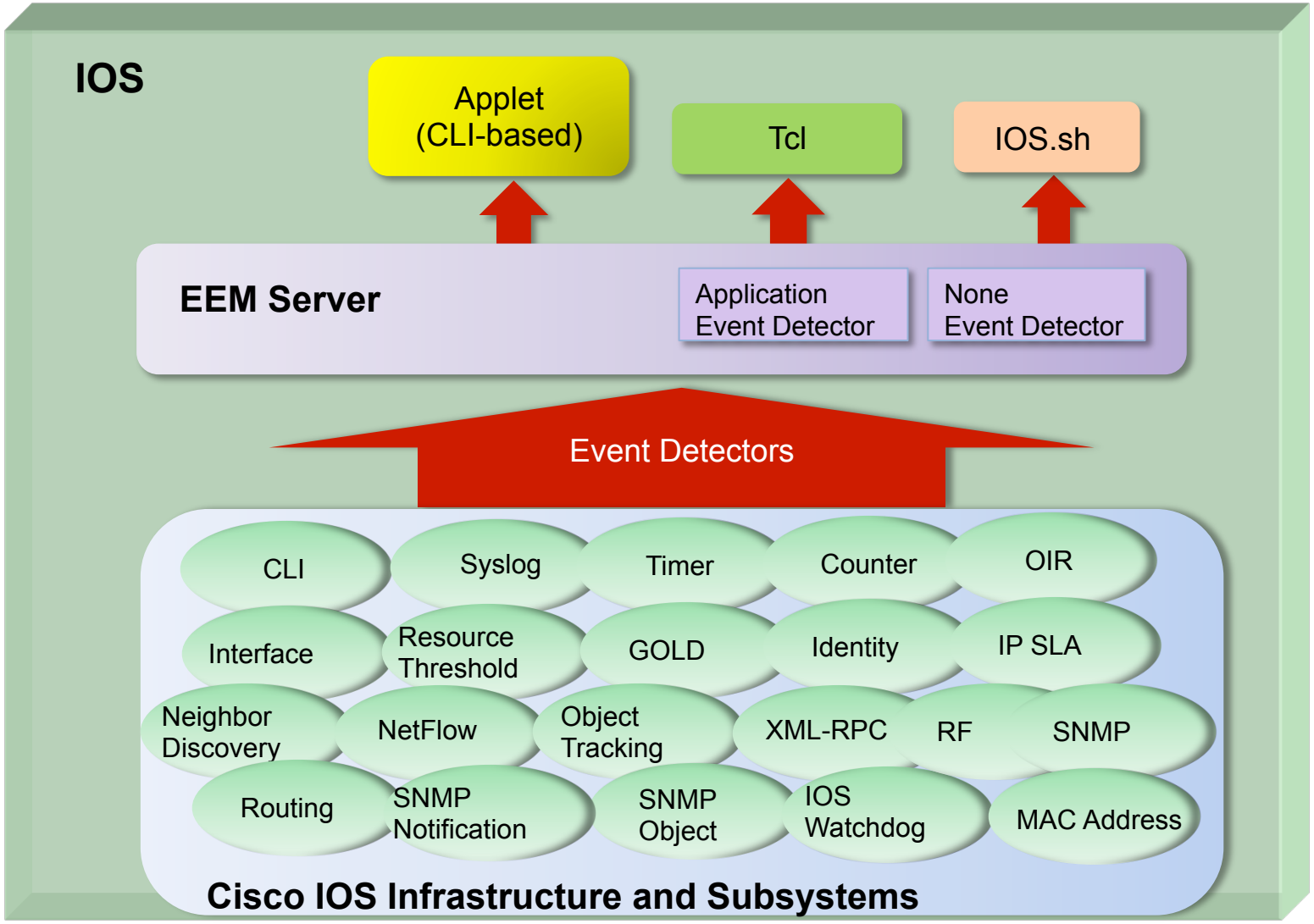


- Listener is good for traditional Web Services methods
- Initiator is good for situations needing to traverse firewall and NAT

Provisioning with EEM & IOS.sh



What is EEM?



Need more EEM Info?

1. What problem are you solving?
2. Which event detector and action do you need?

   Upgrade to the right IOS image

   Use `show event manager detector <detector-type> detailed`
3. Check whether a suitable script/applet is available already

   http://www.cisco.com/go/ciscobeyond

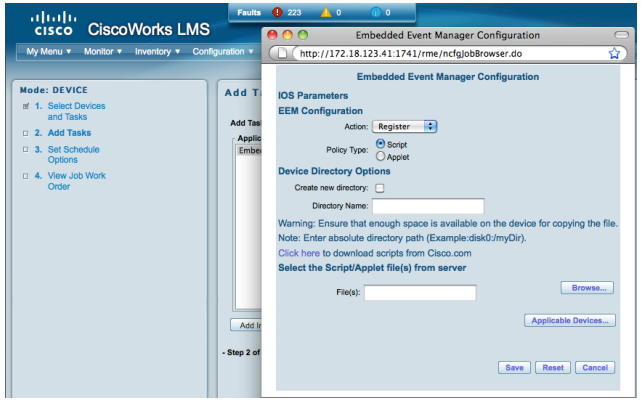
   http://www.cisco.com/go/eem

   https://supportforums.cisco.com/community/netpro/network-infrastructure/network-management

   Use third party EEM tools

   Davra Networks EEMLive: http://www.davranetworks.com

   Progrizon script generator: http://www.progrizon.com/



4. Deploy and Monitor via CiscoWorks

   Yes, LMS 3.1 adds support for EEM in RME
   http://www.cisco.com/go/lms
5. If customization/new development/testing is required

   CA EEM Developer Support Practice

What is IOS.sh?

- “bash-like” shell in IOS
- Automates repetitive tasks
- Familiar scripting environment
- Integrated into IOS CLI
- “fast fingers” – automates what you would have typed manually
- Low-risk automation

What can I do with IOS.sh?

- Built into IOS Parser - available in all modes and submodes
- Can run from a file or from CLI command line interactively
- Shell variable substitution ($name) and user environment variables (name=value)
- System variables: `` `interfaces` `` is a list of all interfaces
- Pipe and redirection (| and >)
- Conditional tests (if/then/elif/fi) & loops (while/do, case, for/until)

```
router# for x in `interfaces`
do interface $x
description This is interface $x
done
```

```
if [ $interface == "FastEthernet 0/0" ]
```

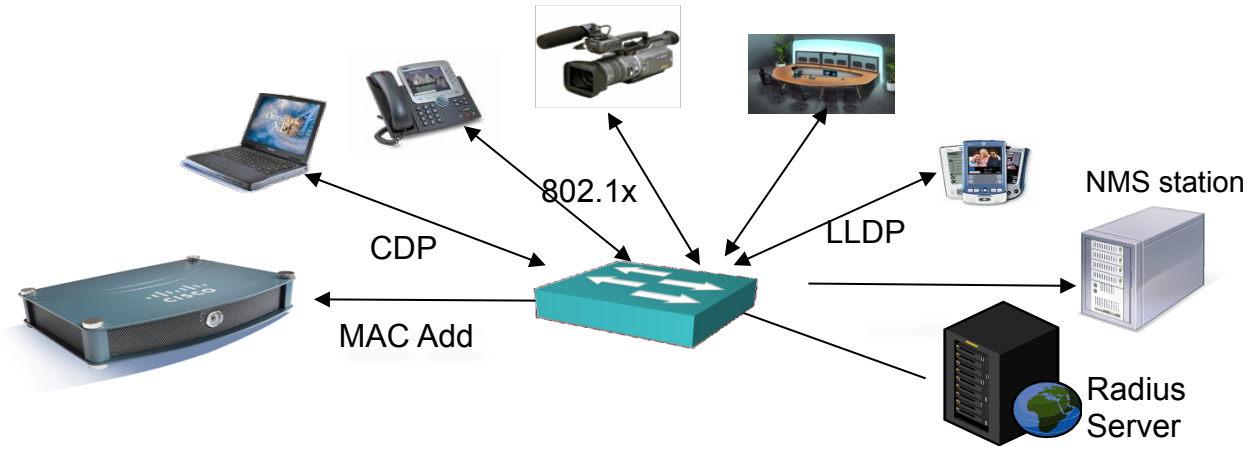
- Regular express pattern matching

```
router# name=SFrCisco
router# if [[ $name =~ "^[A-Z].*F.+[Cc].?sco$" ]]; then
          echo yes; else echo no; fi
yes
```

How “Linux-like” is IOS.sh?

```
cat             output data from a pipe or file to the terminal
cut             edit piped output
echo            echo arguments to the terminal
false           return false in while or if expressions, and set the result
fetch           return values from the configuration database
grep            search for regular expressions in piped output or files
head            print the first lines in the input
interface       print interfaces that match the argument
let             evaluate a numeric expression, and set the result
man             print information for builtins
more            page piped output to the terminal
nl              number the lines in the input
null            ignore the input
printf          output formatted data to the terminal
read            read input into variables
set_oper        set operational values
sleep           pause execution of the terminal
sort            sort the input
tail            print the tail of the input
true            return true in while or if expressions, and set the result
uname           print system information
```

ZTP Use Case – Switch Ports



- Pre-build port configuration templates for various devices simplify user experience and minimize configuration error
- Automatic event detection (CDP/LLDP/MAC) triggers auto configuration
- Authentication (802.1x, MAB) and authorization can be conducted before port configuration applied
- Automatic notification can be sent to NMS system to help with asset tracking
- Sample solution: Auto Smartports, Medianet Autoconfig Solution

Sample EEM IOS.sh Policy - Discovery

```
##::cisco::eem::event_register_neighbor_discovery interface .* cdp update link-
   event
if [[ $_nd_notification =~ "cdp-update|cdp-add" ]]; then
    if [[ $_nd_cdp_capabilities_bit_4 -eq YES ]]; then
        if [[ $_nd_cdp_platform =~ "^((Cisco IP Phone)|(Cisco IP Confe))" ]]; then
            fetch CONFIGD /config/interface{$_nd_local_intf_name}/description
            if [[ $CONFIGD -eq "" ]]; then
                # Add the config
                conf t
                    interface  $_nd_local_intf_name
                        description YES
                        switchport access vlan 1
                        switchport mode accessswitchport block unicast
                        switchport voice vlan 10
                        switchport port-security maximum 3
                        switchport port-security maximum 2 vlan access
                        switchport port-security
                        switchport port-security aging time 1
                        switchport port-security violation restrict
                        switchport port-security aging type inactivity
```

EEM Policy Registration

Built-in Variables

Apply Predefined Port Configuration

Sample EEM IOS.sh Policy - Removal

```
if [[ $_nd_notification -eq "link" ]]; then
    if [[ $_nd_intf_linkstatus =~ down ]]; then
        if [[ $_nd_intf_linestatus -eq down ]]; then
            fetch CONFIGD /config/interface{$_nd_local_intf_name}/description
            if [[ $CONFIGD -eq "YES" ]]; then
                # Remove the config
                conf t
                    interface $_nd_local_intf_name
                        no description
                        no switchport port-security
                        no switchport access vlan 1
                        no switchport block unicast
                        no switchport port-security maximum
                        no switchport port-security maximum 2 vlan access
                        no switchport port-security aging time 1
                        no switchport port-security violation restrict
                        no switchport port-security aging type inactivity
…..
```

Remove Predefined Port Configuration

EEM Auto-Configuration

Step1:

EEM IOS.sh-based policy registered listening for CDP event,
Interface is down and no configuration available
No CDP neighbor detected

```
Cat3750e-2#show event manager policy registered
No.  Class     Type    Event Type          Trap  Time Registered          Name
1    shell     user    neighbor-discovery  Off   Mon Mar 1 12:15:17 1993   autoconf.sh
 interface (.*) cdp update link-event
 nice 0 queue-priority normal maxrun 0.000

Client Policies
No.  Class     Type    Event Type          Trap  Time Registered          Name
Cat3750e-2#show run interface gigabitEthernet1/0/5
Building configuration...

Current configuration : 48 bytes
!
interface GigabitEthernet1/0/5
 shutdown
end

Cat3750e-2#show cdp neighbors gigabitEthernet 1/0/5
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Cat3750e-2#
```

Step2:

Interface turned on and CDP neighbor detected

```
Cat3750e-2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Cat3750e-2(config)#interface gigabitethernet1/0/5
Cat3750e-2(config-if)#no shut
Cat3750e-2(config-if)#end
Cat3750e-2#
Enter configuration commands, one per line.  End with CNTL/Z.
*Mar  1 12:19:40.885: %SYS-5-CONFIG_I: Configured from console by console
*Mar  1 12:19:42.244: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/5, changed state to up
*Mar  1 12:19:42.454: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/5, changed state to up
*Mar  1 12:19:43.419: %SYS-5-CONFIG_I: Configured from console by console
Cat3750e-2#show cdp neighbors gigabitEthernet 1/0/5
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
SEP0002B9EB0883  Gig 1/0/5         167               H    IP Phone  Port 1
```

EEM Auto-Configuration (Cont.)

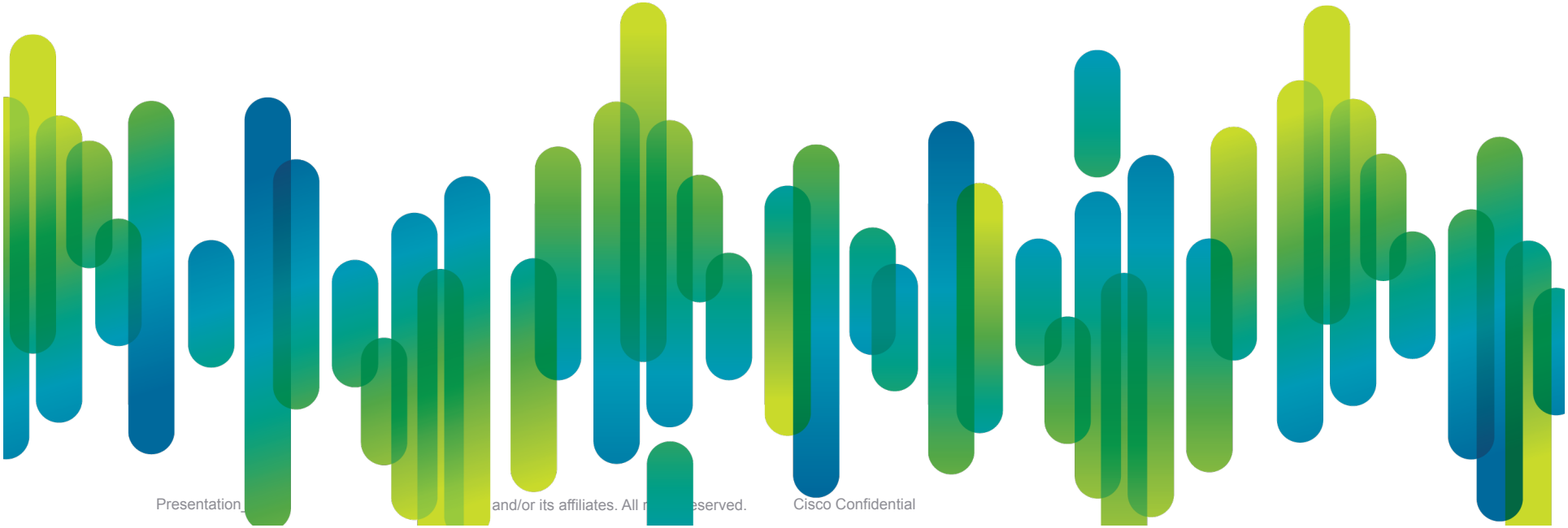
Step3:
EEM IOS.sh-based policy triggered and configuration applied to the port

```
Cat3750e-2#show run interface gigabitEthernet1/0/5
Building configuration...

Current configuration : 657 bytes
!
interface GigabitEthernet1/0/5
 description YES
 switchport mode access
 switchport block unicast
 switchport voice vlan 10
 switchport port-security maximum 3
 switchport port-security maximum 2 vlan access
 switchport port-security
 switchport port-security aging time 1
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 load-interval 30
 priority-queue out
 mls qos trust device cisco-phone
 mls qos vlan-based
 storm-control broadcast level pps 1k
 storm-control multicast level pps 2k
 storm-control action trap
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 15
end

Cat3750e-2#
```

Step4:
Interface shutdown, EEM policy triggered and configuration removed from the port

```
Cat3750e-2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Cat3750e-2(config)#interface gigabitethernet1/0/5
Cat3750e-2(config-if)#shut
Cat3750e-2(config-if)#e
Enter configuration commands, one per line.  End with CNTL/Z.nd
Cat3750e-2#
*Mar  1 12:21:32.462: %LINK-5-CHANGED: Interface GigabitEthernet1/0/5, changed state to administratively down
*Mar  1 12:21:32.647: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/5, changed state to down
*Mar  1 12:21:32.789: %SYS-5-CONFIG_I: Configured from console by console
*Mar  1 12:21:33.301: %SYS-5-CONFIG_I: Configured from console by console
Cat3750e-2#show cdp neighbors gigabitEthernet 1/0/5
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Cat3750e-2#show run interface gigabitEthernet1/0/5
Building configuration...

Current configuration : 48 bytes
!
interface GigabitEthernet1/0/5
 shutdown
end

Cat3750e-2#
```

Real-world Use Case



Demo Objectives

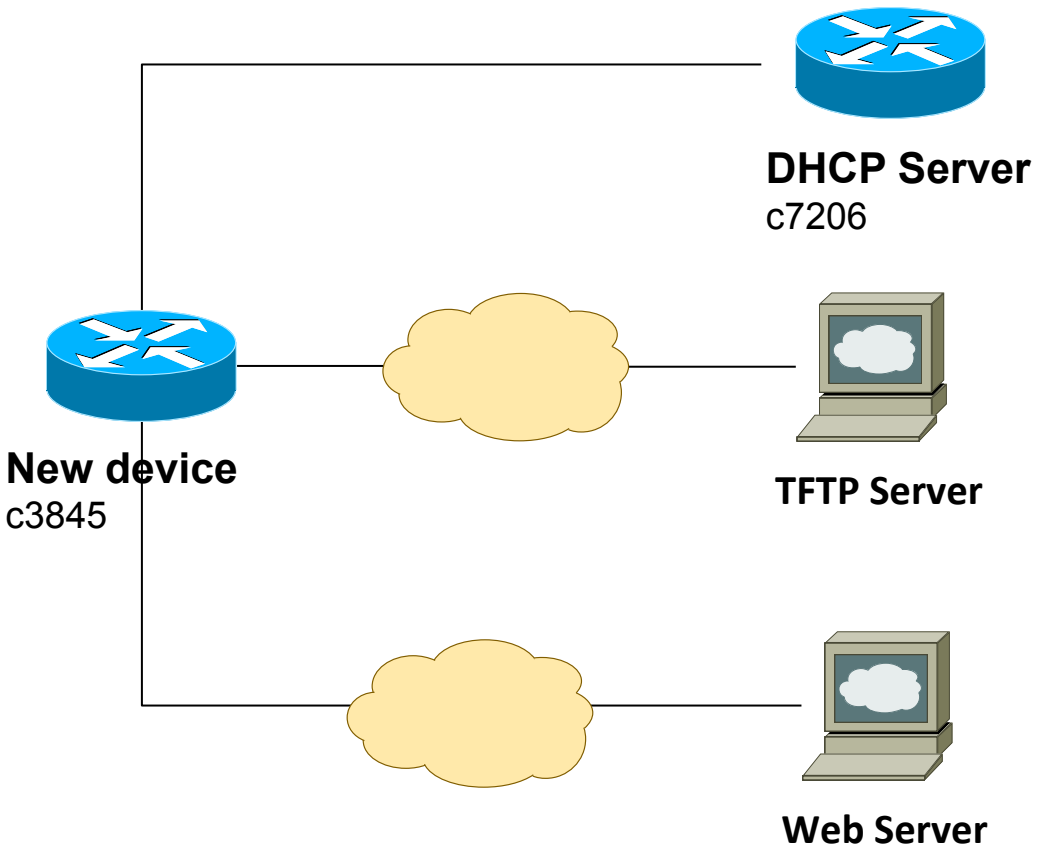
Showcase a custom built ZTD solution

- Based on EEM & Auto-Install

Demonstrate the power of on-the-box scripting

Integration with external in-house systems

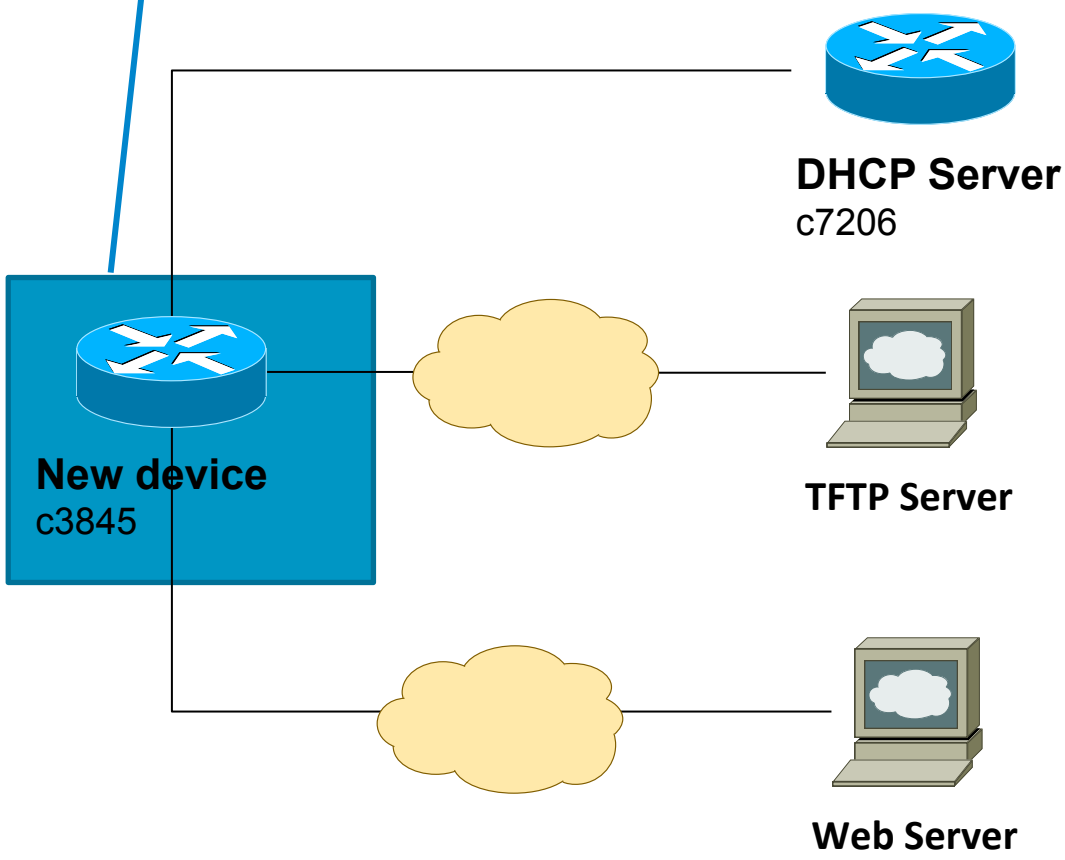
Setup



DEMO GOALS

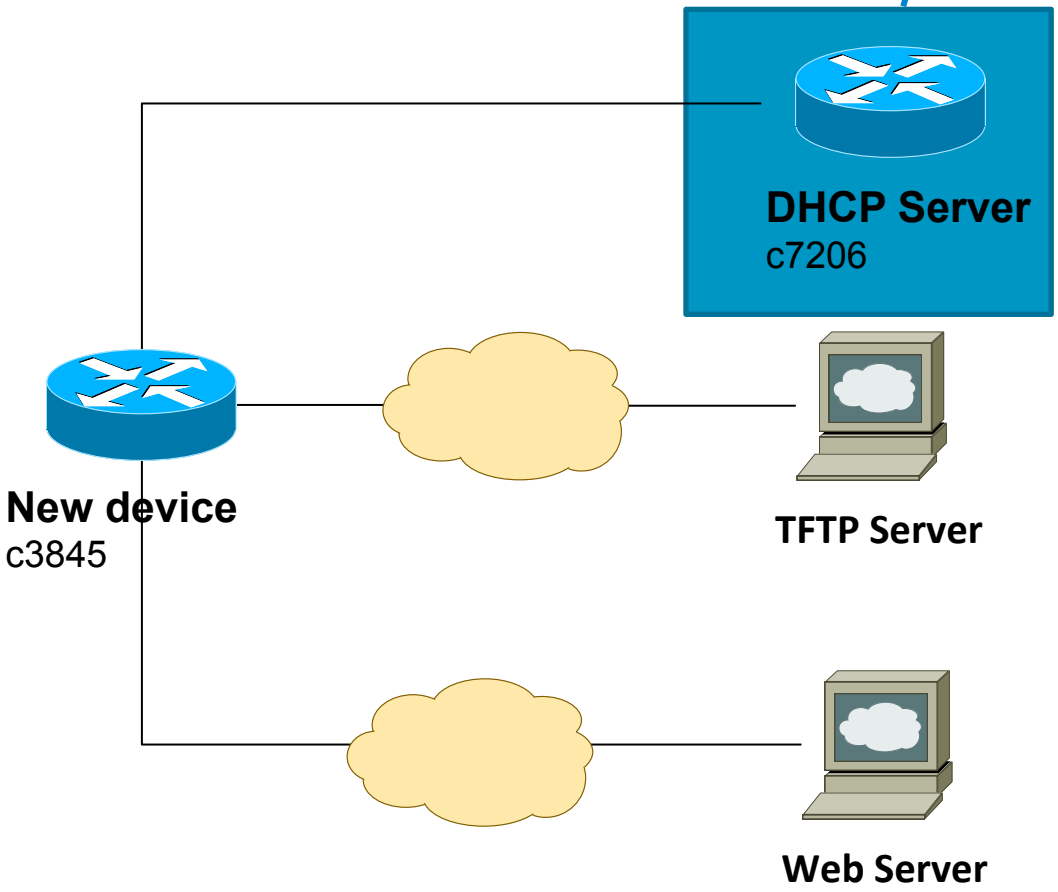
- **Zero Touch Provision new device**
  - ✓ Get image name & configuration file from Web server
  - ✓ Download the image and configuration file from TFTP server
  - ✓ Necessary configuration changes and reload

Setup



- Brand new device from Cisco manufacturing
  - No image on it
  - No configuration on it
- Will be powered on after plugging into a network that has a DHCP server

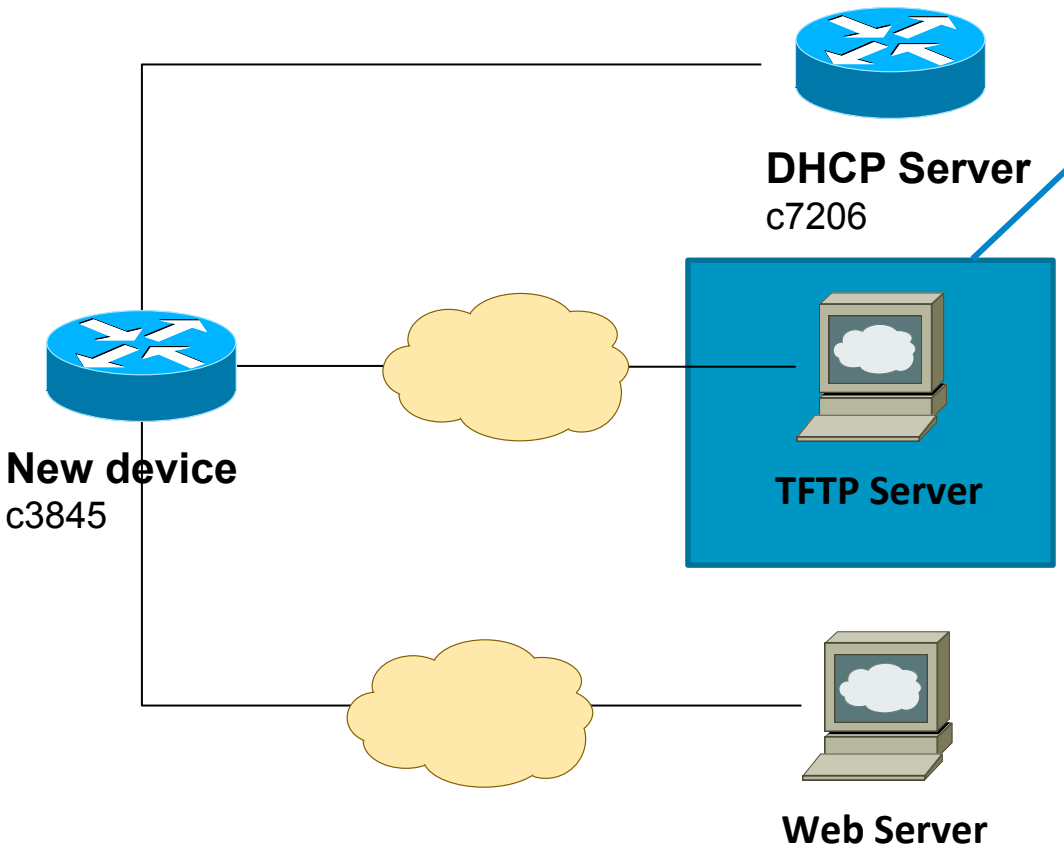
Setup



- Present in the same LAN as the new device
- Has DHCP option 150 configured on it

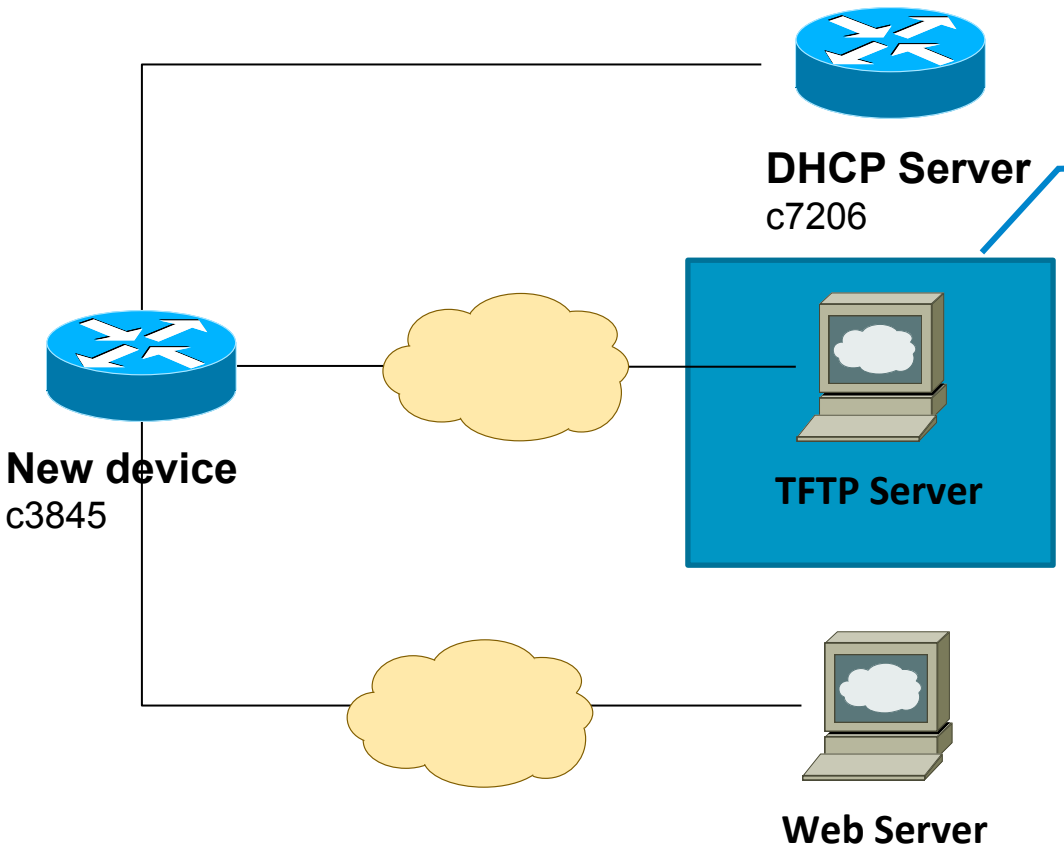
```
bootfile jpfeifer/initial-
   config

option 150 ip 171.69.1.129
```

Setup



- Hosts the following files
  - initial-config
  - autoconf.tcl
  - final-config
  - c3845-entservices-mz.124-24.T

Setup

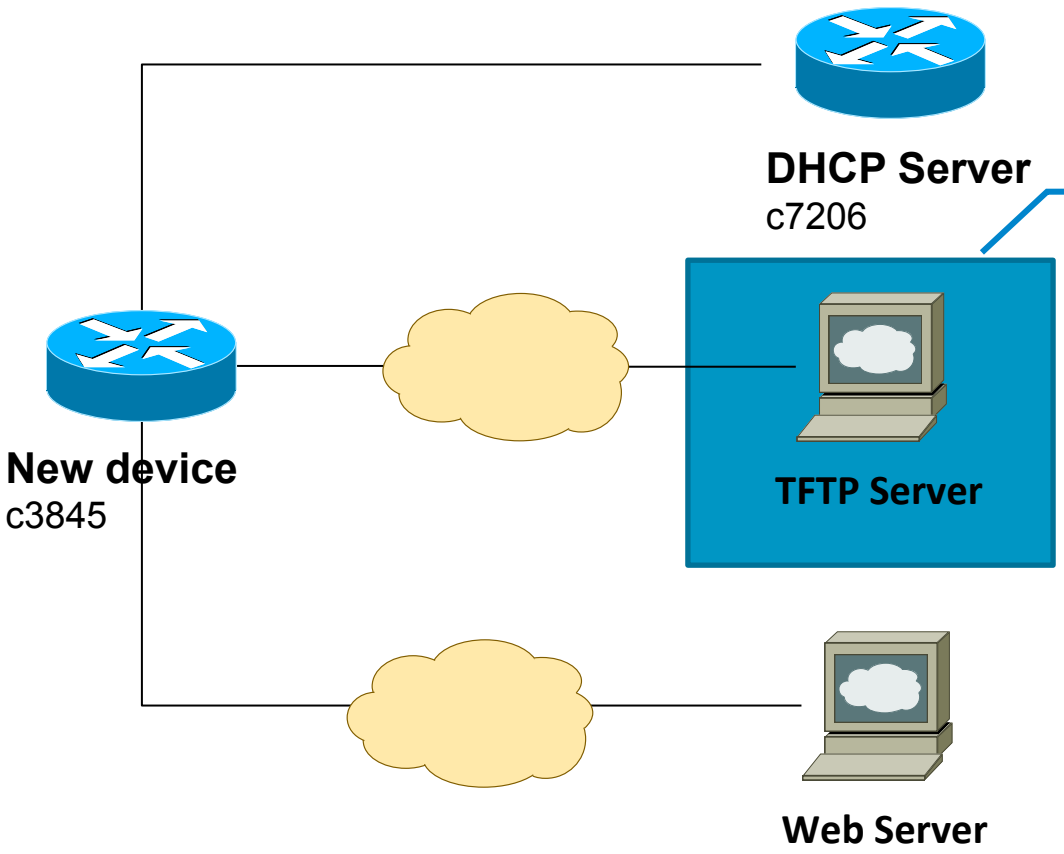


initial-config

- Triggers timer based EEM policy
  - ✓Copies EEM Tcl policy from TFTP
  - ✓Registers EEM Tcl policy
  - ✓Enables debugging

```
event manager applet copy_script
event timer countdown name 40second time 40
    maxrun 900
action 01.0 cli command "enable“
action 02.0 cli command "config t“
action 03.0 cli command "file prompt quiet“
action 05.0 cli command "copy tftp://
    171.69.1.129/jpfeifer/autoconf.Tcl flash:“
action 09.0 cli command "event manager
    directory user policy flash:“
action 0a.0 cli command "event manager policy
    autoconf.Tcl“
action 0c.0 cli command "no event manager
    applet copy_script“
action 0d.0 cli command "end“
action 0e.0 cli command "wr“
```

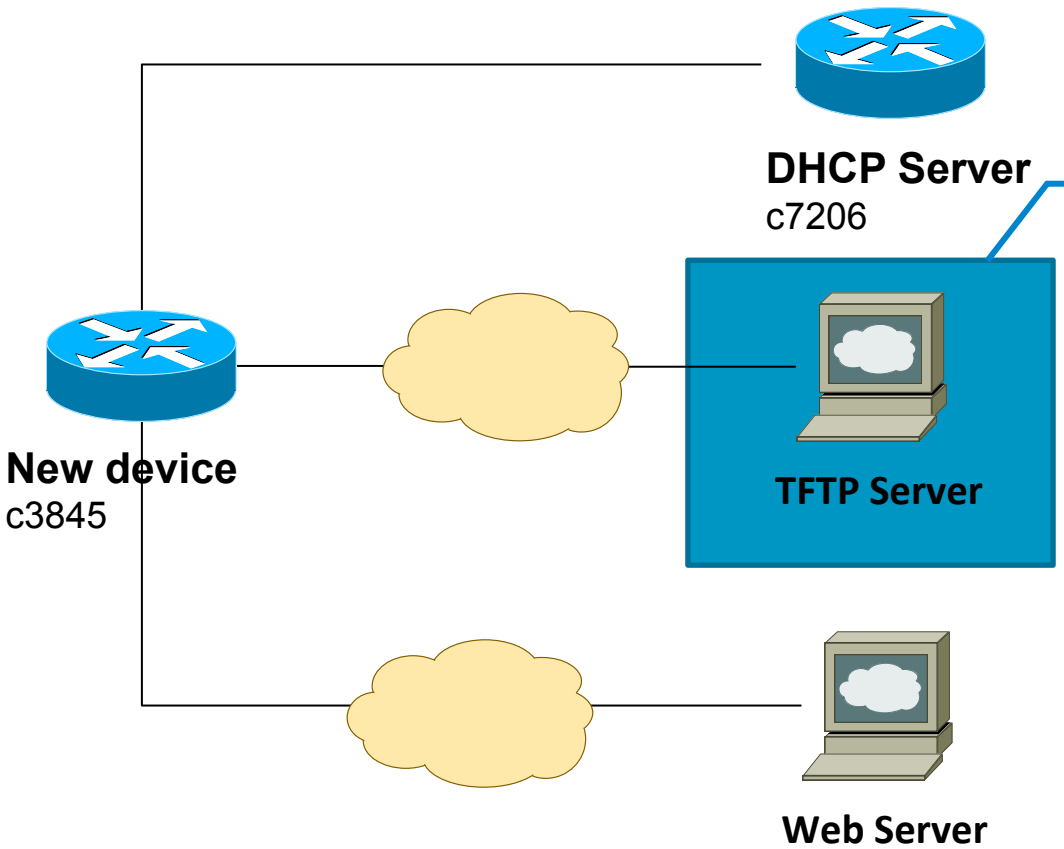
Setup



autoconf.tcl

- Triggered by timer based EEM policy.
- Collects the following info and sends to webserver
  - ✓IP address of active interface
  - ✓Image version running
  - ✓File system contents
- Receives the following from webserver
  - ✓Action (none or load or copy of image)
  - ✓TFTP server address
  - ✓Image name
  - ✓Config file name
- Performs the necessary action
  - ✓None – does nothing
  - ✓Load – boots to a different image
  - ✓Copy – copies a new image from tftp server and boots to it
- Copies final config from tftp and merges it to running-config

Setup

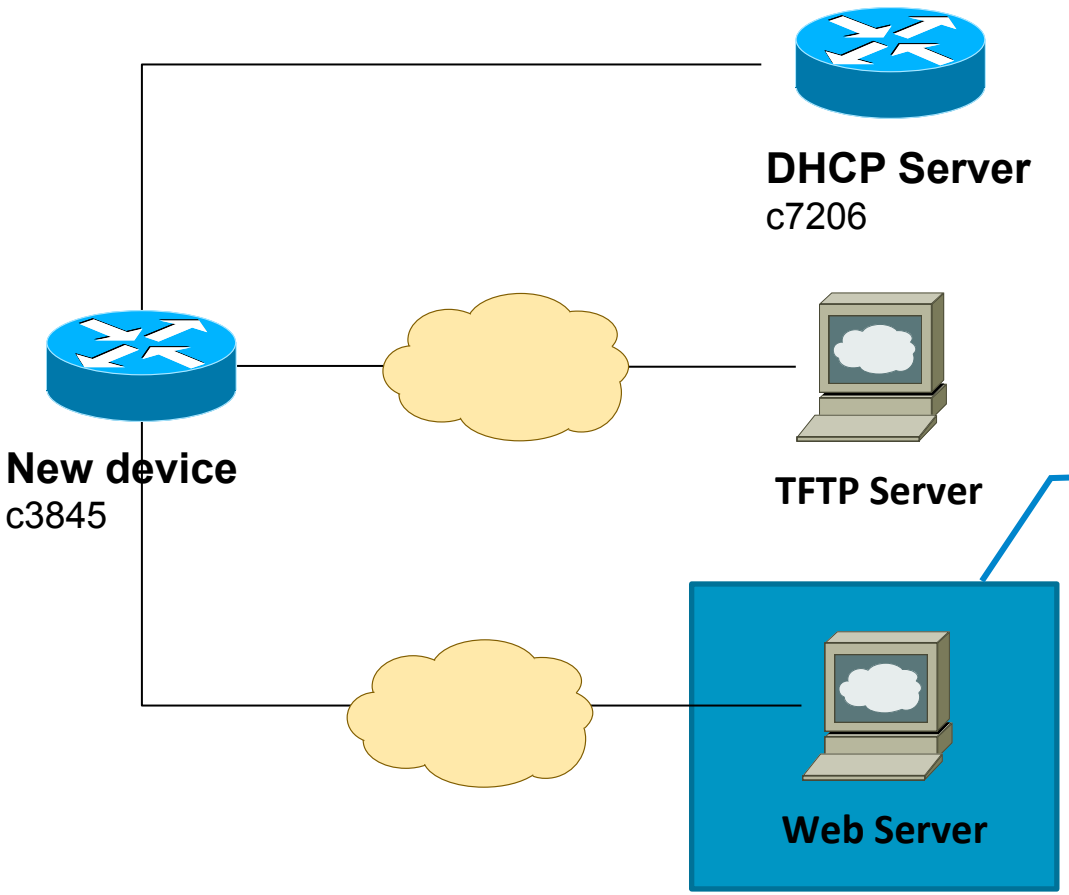


final-config

- Device specific configuration file

```
hostname configured3845

end
```

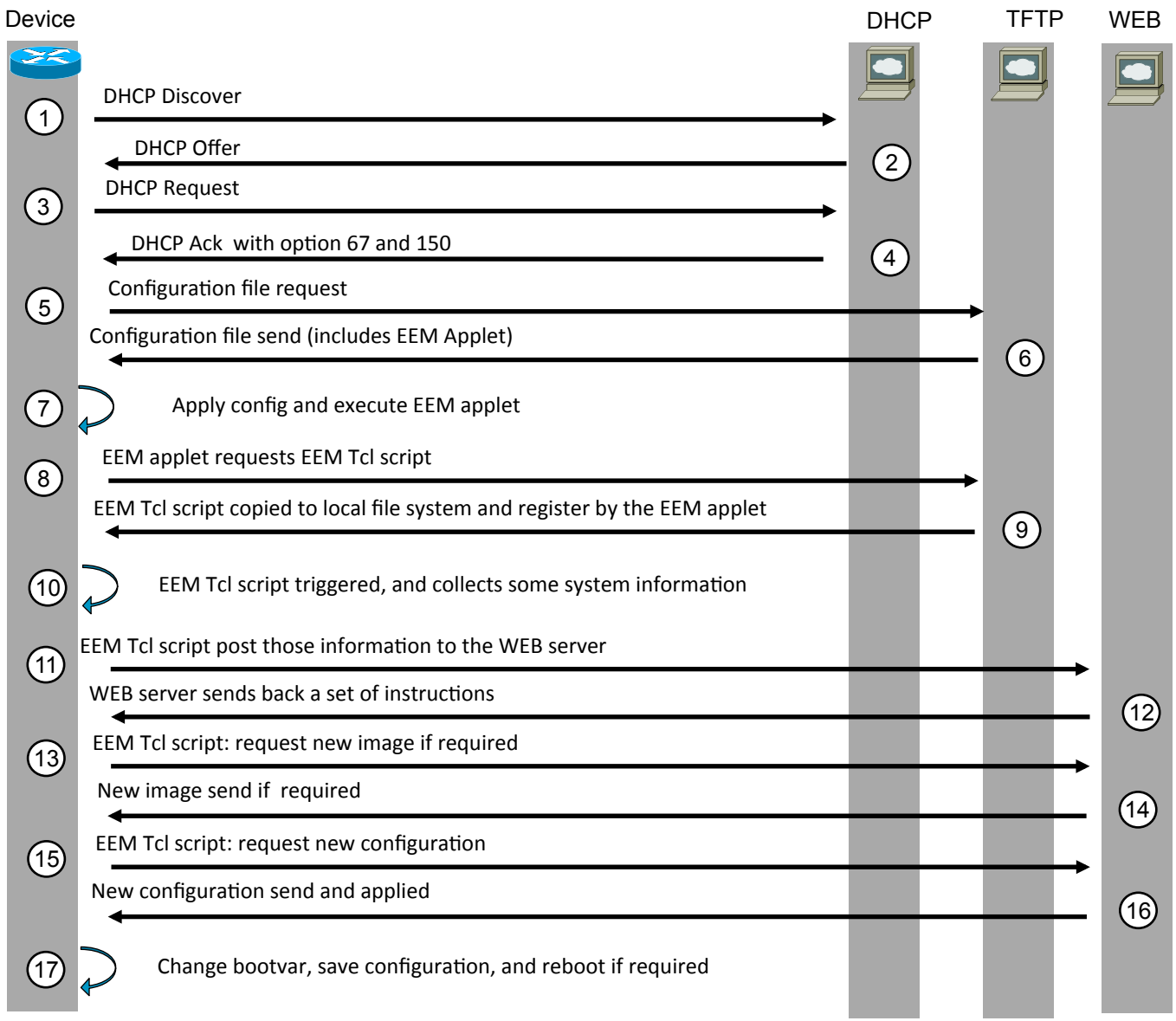
Setup



autoconf.cgi

- Perl script.
- Receives the following from the device
  - ✓IP address of active interface
  - ✓Image version running
  - ✓File system contents
- Processes the info from the device and does device specific decisions
- Sends the following back to the device
  - ✓Action (none or load or copy of image)
  - ✓TFTP server address
  - ✓Image name (c3845-entservices-mz.124-24.T)
  - ✓Config file name

Pulling it all together



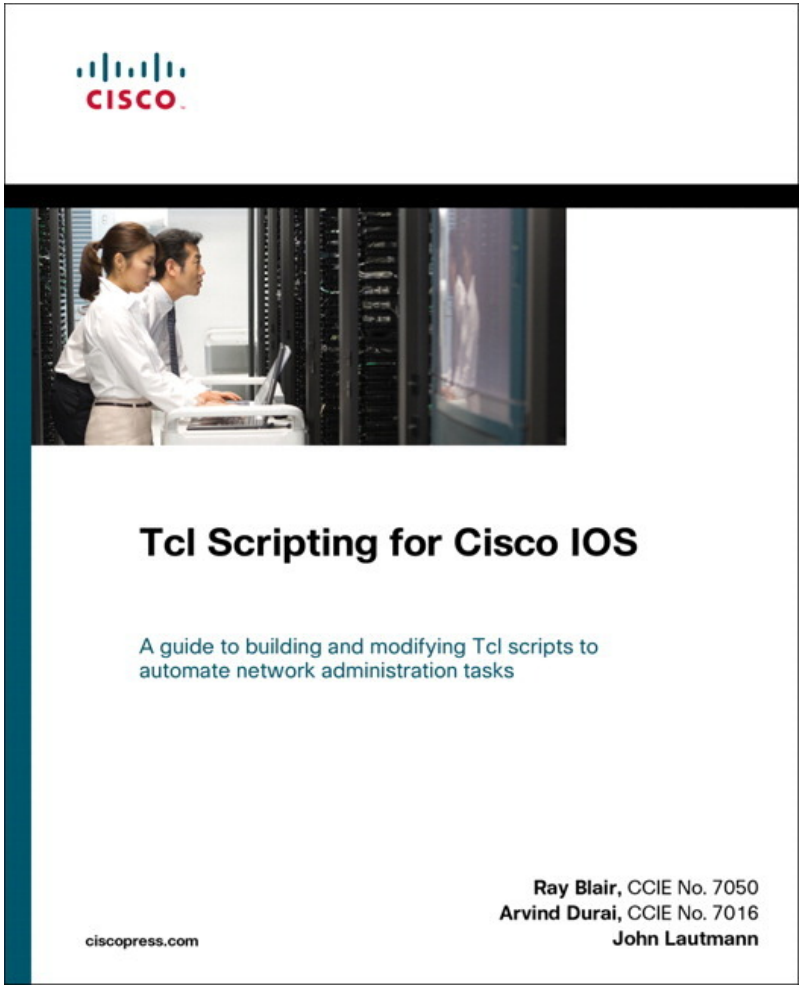
Remember

The next time you manually configure a Cisco device,

you already have everything you need to zero touch provision that device.

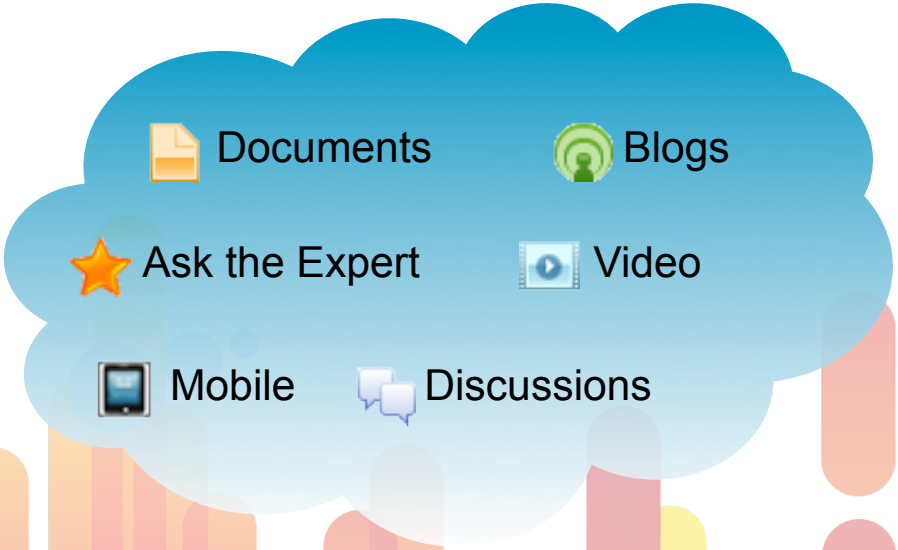
BRKCDN-2010

Recommended Reading



Join Cisco Support Communities!

- **Free** for anyone with Cisco.com registration
- Get **timely** answers to your technical questions
- Find **relevant** technical documentation
- Engage with over 200,000 **top technical experts**
- **Seamless** transition from discussion to TAC Service Request *(Cisco customers and partners only)*
- Visit the Cisco Support Community booth in the World of Solutions for more information



supportforums.cisco.com
supportforums.cisco.mobi

The Cisco Support Community is your one-stop community destination from Cisco for sharing current, real-world technical support knowledge with peers and experts.

Join the Cisco Developer Network

Accelerate your development efforts

Technical Enablement*

Cisco Developer Community

- Low-cost developer kits
- Blogs, wikis, forums
- Cisco SMEs

Technical Support

Interoperability Labs

Marketing Enablement*

Developer Logos

Cisco Compatible

Cisco Developer Preferred Solution

- Promote relationship
- Promote interoperability
- Leverage Cisco brand

Solutions Catalog

Marketing Tools

Sales Enablement*

Cisco Events

- Showcase at Cisco Live
- Trade show collaboration
- Local events

Field Engagement

- Access to Cisco sales
- Access to Cisco channels

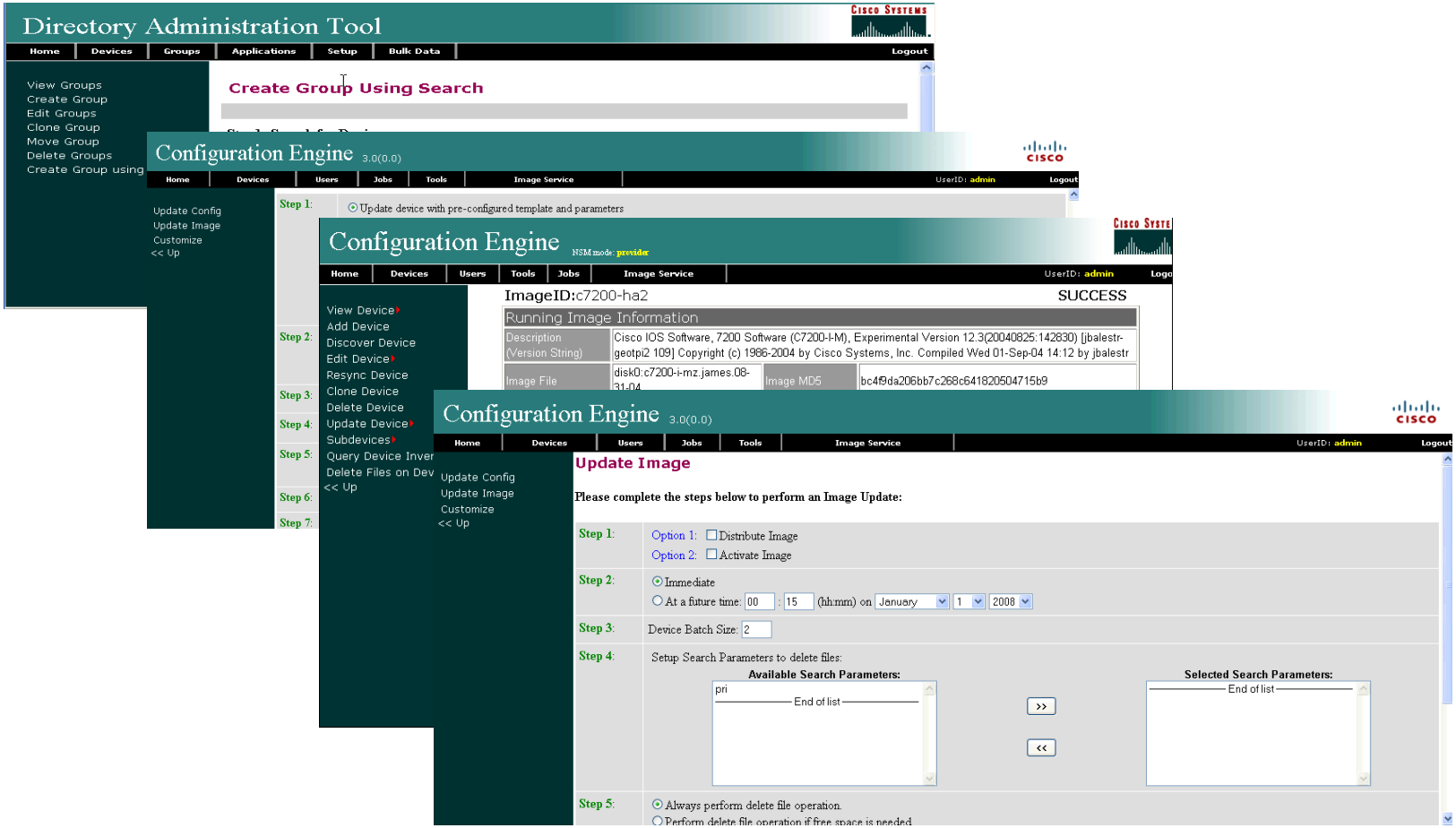
GTM Programs

- STI Program
- Solutions Plus Program
- Solution Incentive Program

developer.cisco.com

CISCO

Configuration Engine Screen Sample



Device Inventory

Configuration Engine NSM mode: provider

Home | Devices | Users | Tools | Jobs | Image Service | UserID: admin | Logo

- View Device
- Add Device
- Discover Device
- Edit Device
- Resync Device
- Clone Device
- Delete Device
- Update Device
- Subdevices
- Query Device Inventory
- Delete Files on Devices
- << Up

ImageID:c7200-ha2 SUCCESS

Running Image Information

Description (Version String)	Cisco IOS Software, 7200 Software (C7200-I-M), Experimental Version 12.3(20040825:142830) [jbalestr-geotpi2 109] Copyright (c) 1986-2004 by Cisco Systems, Inc. Compiled Wed 01-Sep-04 14:12 by jbalestr				
Image File	disk0:c7200-i-mz.james.08-31-04	Image MD5	bc4f9da206bb7c268c641820504715b9		
Config Variable		Config Reg	0x2102	Config Reg Next Boot	
Boot Variable	disk0:/c7200-i-mz.image6,1;	BootIdr Variable		Return To ROM Reason	reload
Return To ROM Time		Started At			

Hardware Information

Vendor	Cisco	Platform Name	7204	Hardware Revision	A
Processor Type	NPE225	Main Mem Size	117440512	IO Mem Size	16777216
Hardware Serial #	16068814	MidPlane Version	4 slot midplane, Version 1.0		
Processor Rev	R527x CPU at 262MHz, Implementation 40, Rev 10.0, 2048KB L2 Cache				
Hardware Rework					

File System List

	[FileSys name=[nvram], type=[nvram], size=[129016], freespace=[123370], readable=[true],
	File 0 under Directory[/]: name=[startup-config],

Configuration Enablers

- CLI Enhancements

  Rollback/replace – unwind CLI configs

  Parser return codes – well-defined success and error codes

  Syntax check – check a command before applying it

  Config change notification – accurate before/after of configuration changes

  Config diff – context sensitive comparison

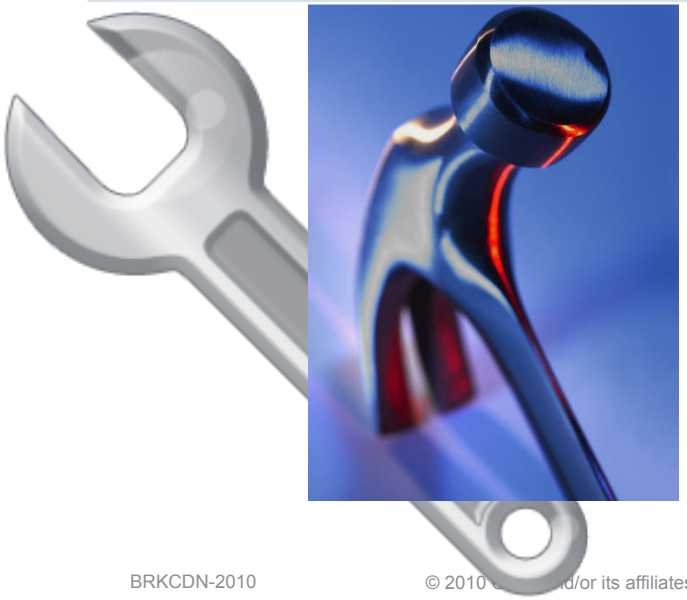
  Config tracking ID – unique identifier for each config

Configuration Enablers (Cont.)

- Release/documentation Management
  - Syslog Usability Tool
  - MIB release
- Next Generation XML Access
  - Fully tagged show output
  - Bulk config commands and atomic rollback
  - Leverages existing Web Services tools and expertise
  - Allows “phone home” to eliminate all inbound ports
  - Fully encrypted and authenticated

Should I Build or Buy?

In-house	Commercial Off the Shelf
Requires development and test effort	Ready to use
Can be tailored to exactly what the business needed	Not always aligned with business
Can take longer to deploy and rollout	Usually quicker to deploy and use
Inexpensive capital $$	Upfront investment plus ongoing support cost
Requires ongoing care and feeding	Support contracts and consulting



Why Web Services?

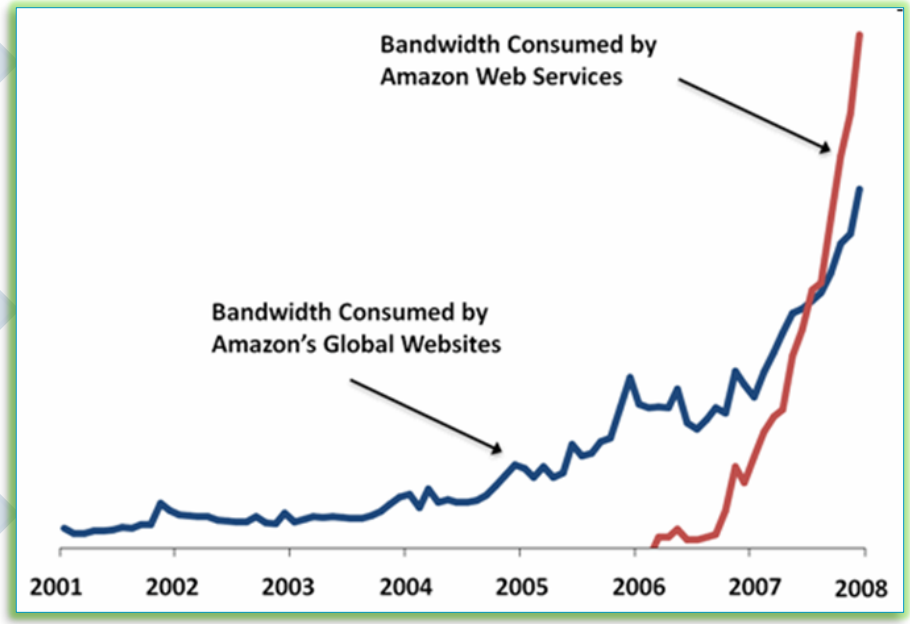
Open
- W3C/OASIS
- SOAP4J
- XERCES
- Apache Axis
- HTTP/REST

Industrial Strength
- WebSphere
- BEA WebLogix
- Microsoft .NET

Self-describing
- WSDL
- UDDI
- Google…

Simple
- XML
- SAX
- Expat
- DOM

Secure
- SSH
- TLS
- HTTPs/SSL



WSMA - Configuration Web Service

- Validate and apply configuration commands in IOS
- Support for three types of data models
  - **Block** – Tag block of commands
  - **Cmd** – line by line tagging
  - **Edi** – encoding C2X, X2C
- Support for three types of config requests
  - **Config Test** – Validate the configuration but do not apply to running config
  - **Config Apply** – Modify running configuration with supplied config data
  - **Config Persist** – Copy to startup configuration
- Action on fail config request options:
  - **Stop** – Stop execution on the first error but preserve the system state. Configuration could be partially applied
  - **Continue** – Just ignore the errors and keep going to the end
  - **Rollback** – Abort at the first error and restore the configuration to the state before any configuration applied
- Option to report back on error details
  - **Brief, Errors, All**
- ResultEntry – Detailed log of every line of CLI
  - **Success, Failure, Invalid, Not Executed**

WSMA - Execute Web Service

- Exec WS support handling of exec-mode commands such as show and other diagnostic commands
- Support for all Exec commands
- Interactive command support
- Max Bytes and Max Time Termination
- Show output can be tagged in XML seamlessly using specfile to define XML to Text mapping
- Eliminates screen scrapping

WSMA - File System Web Service

- File System WS enables copying and validating files between local and remote file systems
- Support for IOS image management
- Directory listing support
- Additional validation info in requests
  - File size
  - MD5 Checksum
- Overwrite or erase existing files
- Delete Files