



Cisco Virtual Workspace (VXI) Smart Solution As-Built Reference Guide

April 2, 2013



Contents

Goal	4
Audience	4
Objectives	4
Design Overview	2
Data Center Compute and Storage Components	9
Cisco Unified Computing System	9
Cisco UCS 6248UP Fabric Interconnect.....	10
Cisco UCSM Configuration	10
UCS 6248UP Uplink Storage Configurations.....	12
Fibre Channel Storage Components	12
NFS Storage Components.....	13
Cisco Nexus 1000v	13
Hypervisor Installation and Configuration.....	14
VMware ESX/ESXi	14
Desktop Virtualization Software Installation and Configuration	14
VMware View Configuration	14
Citrix XenDesktop Configuration	14
Data Center Networking Infrastructure.....	15
Cisco Nexus 5548 Access Layer Switch	15
Cisco Nexus 7010.....	16
Cisco Application Control Engine (ACE4710)	16
Cisco Adaptive Security Appliance (ASA5580)	17
Cisco WAN Acceleration Engine (WAE-512)	20
Campus Network.....	20
Cisco Catalyst 6504E (CAT6504E)	20
Cisco 7206VXR Router.....	21
Cisco WAN Acceleration (WAE-674).....	21
Cisco Adaptive Security Appliance (ASA5540)	21
Cisco Catalyst 4500E (Campus Access CAT4500E)	21
Cisco Catalyst 4507E (Campus Access CAT4507E)	21
Contact Center	22
VXC-6215.....	23
CUCM Config.....	23
Dual VLAN config	24
Remote ASA config	24
WebAuth	25
MediaNet.....	26
Appendix 1 - Endpoint security 802.1x, MacSec, MAB, ACS.....	27
Appendix 2 – QOS settings in Cisco Virtual Workspace (VXI) Smart Solution	31
Appendix 3 – Jabber and Deskphone control.....	35
Appendix 4 – Netflow and Energywise	42



Figures

Figure 1: Test Configuration.....	2
Figure 2: Network Map showing IP addresses	4
Figure 3: Virtual Infrastructure.....	5
Figure 4: Server Configuration.....	9
Figure 6: Complete UCS System Block	10
Figure 7: UCS 6248 Uplink Storage Connectivity	12
Figure 8: Data Center Network Components.....	15
Figure 9: Campus Network Components	20

Tables

Table 1: Data Center Compute Components.....	6
Table 2: Data Center Storage Components.....	6
Table 3: Data Center Network Components	6
Table 4: Campus Network Components	7
Table 5: Supporting Application Services	7
Table 6: 3rd Party Products	8



Goal

This document reports the tested configuration for the Cisco Virtual Workspace (VXI) Smart Solution Release 2.7 architecture. It includes specific device configurations and diagrams showing interconnections.

Audience

This document is intended to assist solution architects, sales engineers, field engineers and consultants in planning, design and deployment of Cisco Virtual Workspace (VXI) Smart Solution. This document assumes the reader has an architectural understanding of the Cisco Virtual Workspace (VXI) Smart Solution and has reviewed the CVDs for Citrix XenDesktop and VMware View.

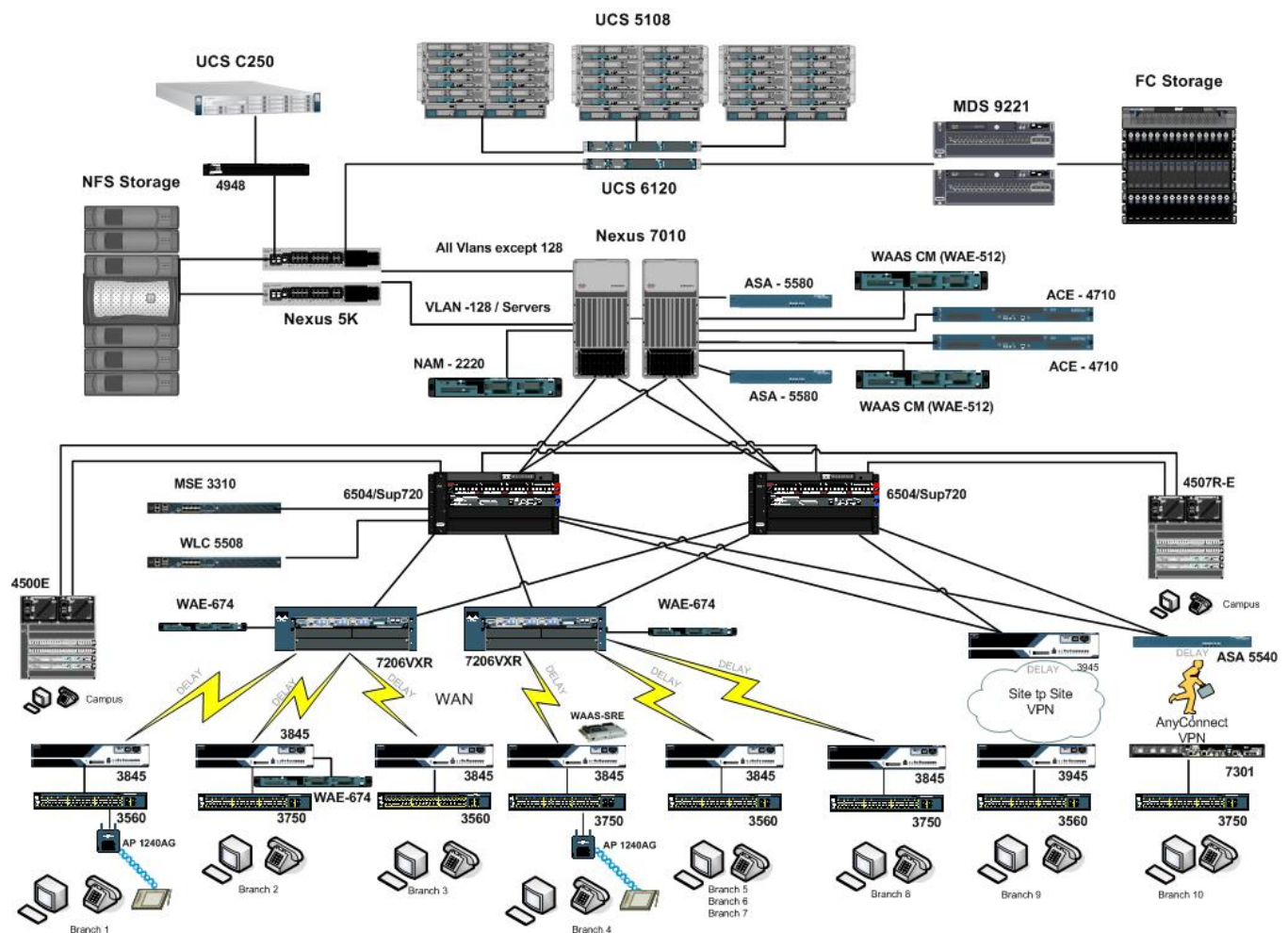
Objectives

This document is intended to articulate the overall design and specific configurations of the tested architecture called out in the Cisco Virtual Workspace (VXI) Smart Solution Release 2.7 CVDs for Citrix XenDesktop and VMWare View.

Design Overview

The design for the Cisco Virtual Workspace (VXI) Smart Solution replicates a customer's network, end-to-end, from the datacenter to the endpoints installed either in the campus or branch environment. Figure 1 shows the complete system test setup. Discussion for each of the sections are shown as follows.

Figure 1: Test Configuration



Release 2.7 of the Cisco Virtual Workspace (VXI) Smart Solution is based on equipment from both Cisco and its eco-system partners. Where possible the preferred operating mode and configuration was used, unless specific changes yielded improvements or enhancements to the Desktop Virtualization (DV) experience.



Due to the number of devices in the Cisco Virtual Workspace (VXI) Smart Solution test setup, the configuration files for each device are included as hyperlink references throughout the document. Refer to the Appendix section of this document for guidance on completing specific use cases.

Branches 1 - 4

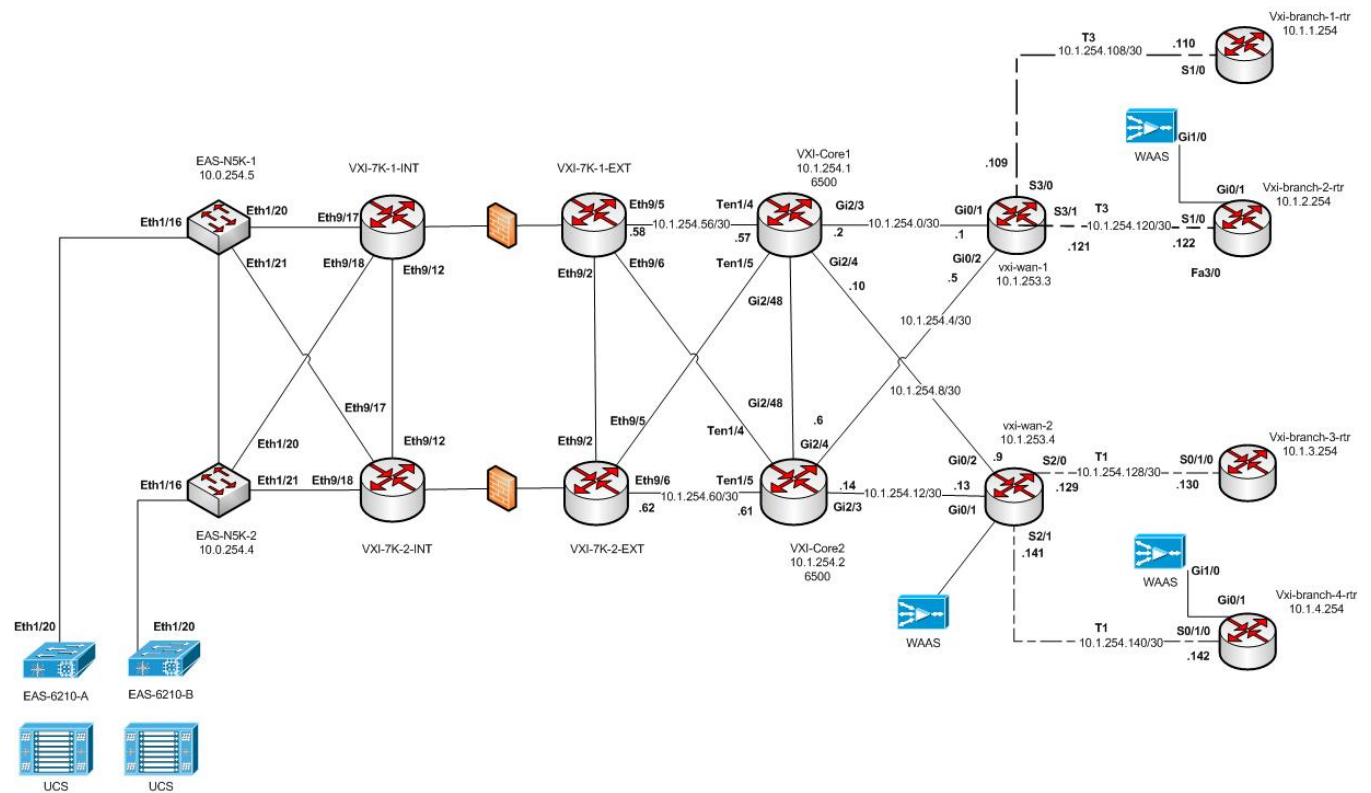
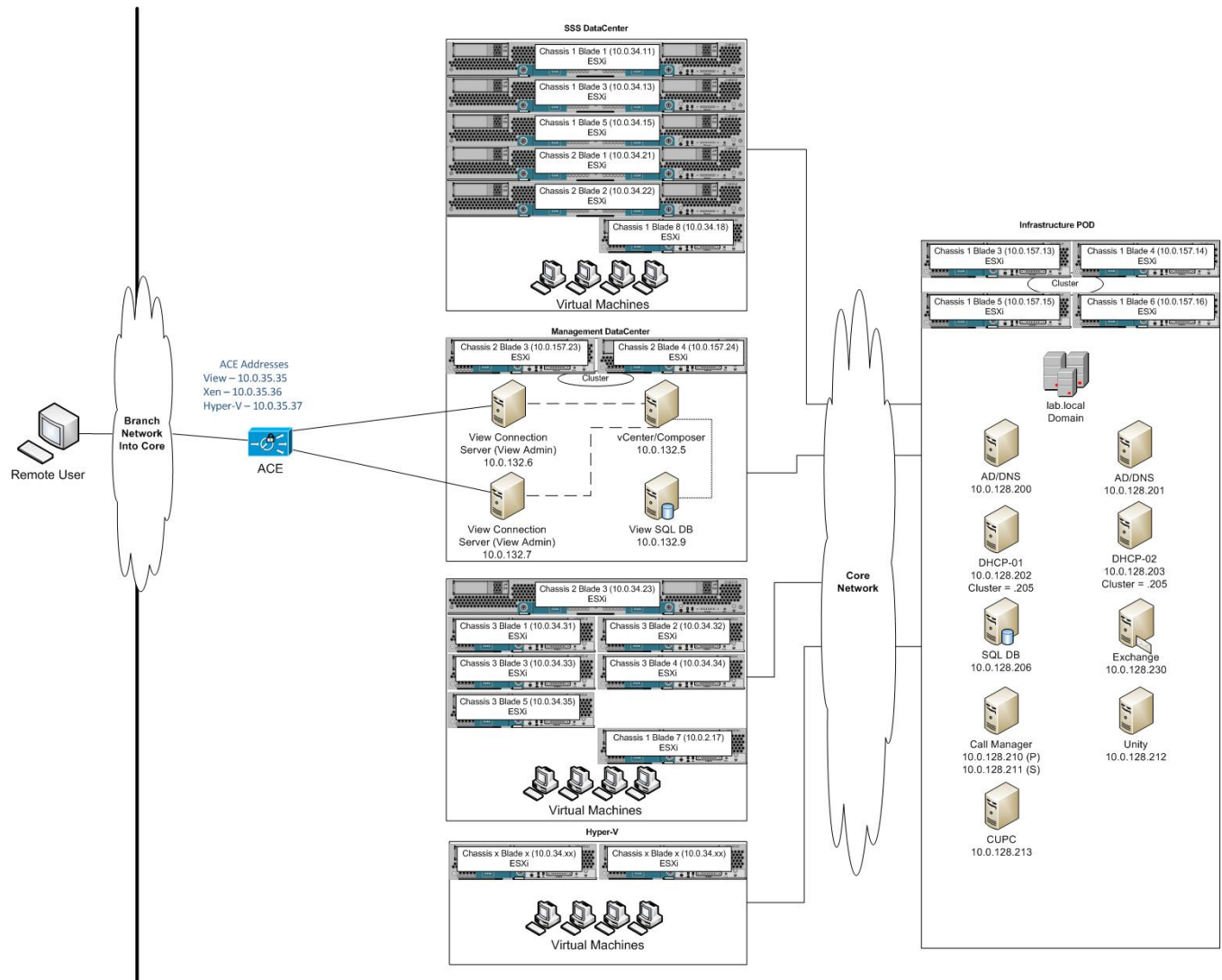


Figure 3: Virtual Infrastructure



**Table 1: Data Center Compute Components**

Component	Software Release
Cisco Unified Computing System: <ul style="list-style-type: none">• UCS 5108• B200 M1 / M2 / M3• B250M2• B230 M1 / M2• UCS 6248UP Fabric Interconnect• UCS Manager	2.1.1a

Table 2: Data Center Storage Components

Component	Software Release
Cisco MDS 9506 Cisco MDS 9134	5.2(6a)

Table 3: Data Center Network Components

Component	Software Release
Cisco Nexus 1000v	4.2(1)SV2.(1.1a)
Cisco Nexus 5000	5.2(1)N1(3)
Cisco Nexus 7010	NxOS 6.1(2)
Cisco Application Control Engine (ACE) 4710	5(1.1)
Cisco ACE Device Manager	5(1.1)
Cisco Adaptive Security Appliance (ASA) 5580	8.3(1)4
Cisco Adaptive Security Device Manager (ASDM)	6.3(1)
Cisco WAAS central manager	5.1.1 build b16

**Table 4: Campus Network Components**

Component	Software Release
Cisco Catalyst 6504-Sup720	12.2(33)SX15
Cisco 7206VXR NPE-G1	15.2(4)S1
Cisco Catalyst 4507R-E	122-54.SG
Cisco WAE 674	5.1.1 build b16
Cisco Adaptive Security Appliance (ASA) 5540	9.0
Cisco ISR 3945 G2	15.2(3)T
Cisco Aironet Access Point	7.0.116.0
Cisco 5508 Wireless Controller	7.0.116.0
Cisco Wireless Control System	7.0.172.0
Cisco Mobility Services Engine	7.0.201.0
Cisco Identify Services Engine	1.1.1

Table 5: Supporting Application Services

Component	Software Release
Cisco Unified Communication Manager	9.1.1
Cisco Unity Connection	9.0.1ES
Cisco Unified Presence Server (CUP)	9.0.1
Cisco Jabber	9.1.3.13181
Cisco AnyConnect	3.1



Table 6:3rd Party Products

Component	Software Release
VMware ESXi /ESX	5.1a
VMware vSphere/vCenter	5.1a
VMware View Connection Server	5.1.2-928164
VMware View Composer	3.0.0.691993
VMware View Agent	5.1.2-928164
Citrix XenDesktop	5.6 FP1
Citrix PVS	6.1.17
Citrix XenApp	6.5 HRP1
Microsoft AD Domain Controllers	Win 2008 R2
Microsoft DNS	Win 2008 R2
Microsoft DHCP	Win 2008 R2
Microsoft Windows	7 SP1
Apple iPad	iPAD 3
EMC Unisphere	05.31.000.5.509
NetApp FAS 3170	8.1.2 7-mode
NetApp Mgmt. Software	2.1

Data Center Compute and Storage Components

This section describes the Data Center infrastructure components used in the configuration.

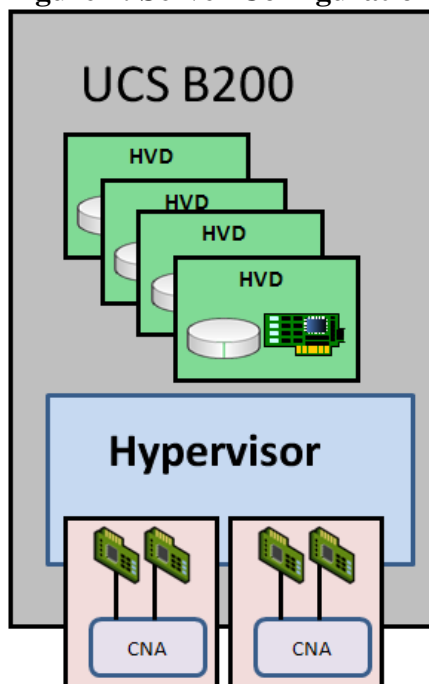
The design for the data center uses guide lines from the Data Center 3.0 CVD available on the Cisco Design Zone. It deploys the standard three tier model: Access, Aggregation, and Core. Service Appliances are connected to the Aggregation Layer and are covered in this section.

Cisco Unified Computing System

The Cisco Unified Computing System is used to host the virtual desktops. Three Cisco UCS 5108 Blade enclosures were used for the test. Two enclosures contain eight half width Cisco UCS B200 blade servers each and one enclosure contains four full width UCS B250 blade servers. The Desktop Virtualization (DV) machines are distributed across all three enclosures.

The Cisco UCS VIC1240 Converged Network Adapter (CNA) mezzanine card was used for this test. It provides virtual 40 Gigabit Ethernet NICs and virtual Fibre Channel HBAs combining them into Fibre Channel over Ethernet (FCoE) interfaces. The hypervisor will map these interfaces to the various VLANs needed to support the DV environment.

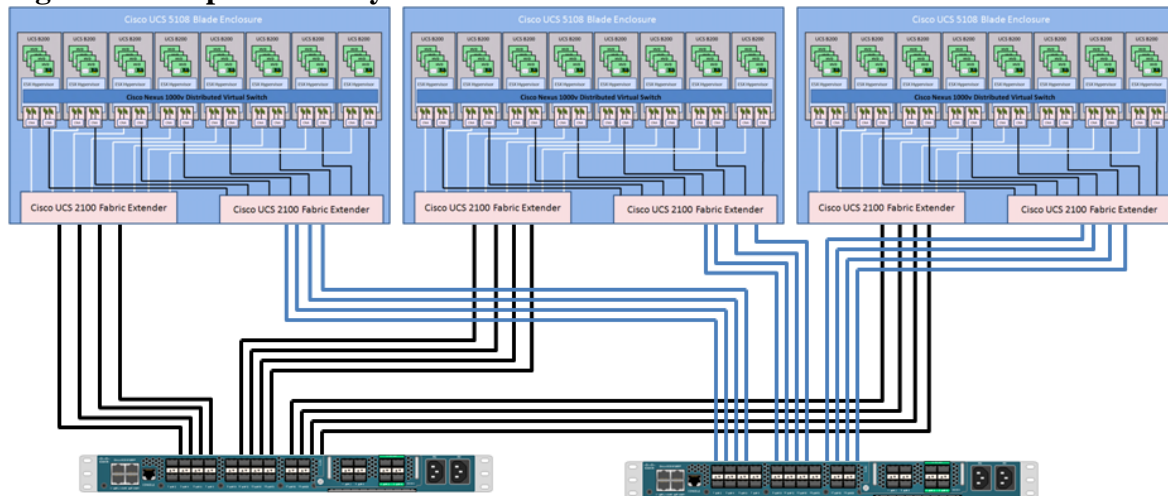
Figure 4: Server Configuration



Cisco UCS 6248UP Fabric Interconnect

The Cisco UCS 6248 Series Fabric Interconnects are a core part of the Cisco Unified Computing System, providing both network connectivity and management capabilities for the system.

Figure 5: Complete UCS System Block



Cisco UCSM Configuration

The converged fabric (FC and Ethernet) is managed by the pair of UCS 6248UP switches. The Ethernet and FC traffic is broken up and placed onto separate sets of interfaces. Each UCS 6248UP has a unique IP address. Each switch contains the Unified Computing System Manager (UCSM). A virtual IP address is created to link the two switches together and provide a single point of management. The UCSM is accessed via a browser.

The UCSM configuration screenshots can be found here : [UCS Manager Configuration](#).

The configuration file for the UCS6248 was captured by using SSH to get access to the CLI and issuing the command: `show config >> sftp://<host>/<path>/<dest_filename>`

The complete configuration for the UCS6248 can be found here : [UCS 6248 Configuration](#).



NOTE

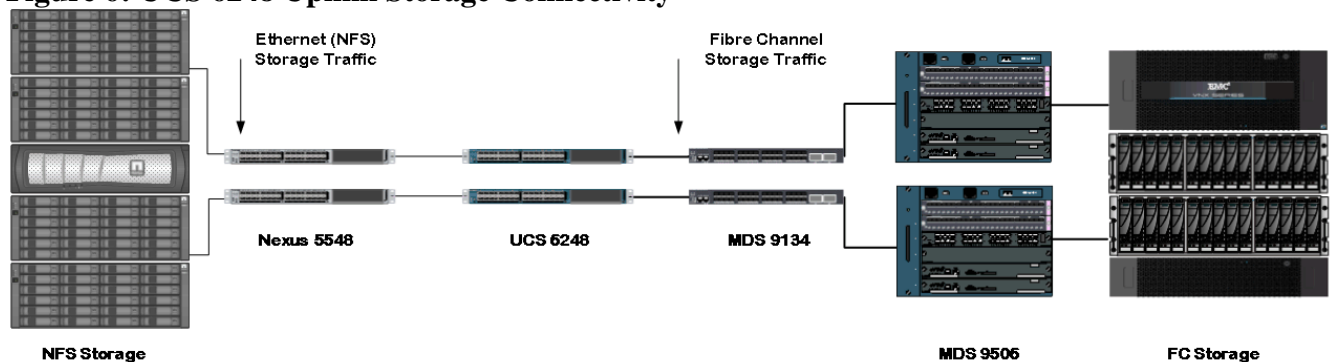
To enable Jumbo Frames for both NFS and FC storage, use the QOS configuration on the Cisco Unified Computing System Manager.

Configure platinum policy by checking the Platinum policy box and if you want jumbo frames enabled change MTU from normal to 9000. Use the option to set no packet drop policy during this configuration.

UCS 6248UP Uplink Storage Configurations

Two sets of uplinks are provided on the UCS 6248UP. One set is used for Fibre Channel (FC) connectivity to FC based storage. These uplinks are located on the module slot. The second set is used for Ethernet connectivity including access to NFS storage. Ethernet ports on the module slot or from the built-in ones can be used for this purpose. Figure 6 shows this portion of the system configuration.

Figure 6: UCS 6248 Uplink Storage Connectivity



Fibre Channel Storage Components

A pair of MDS 9134 series was used in the configuration to connect to the FC port of the Cisco UCS Fabric Interconnect FC expansion module ports to a pair of MDS 9506 for aggregation. The MDS9506 then connects to the Fibre Channel Storage array. The MDS SAN fabrics were predominantly used for configuring boot from SAN of the UCS server blades.

The uplink FC ports on the UCS 6248 operate in N-Port Virtualization (NPV) mode. The uplink ports operate in a similar mode to host ports (referred to as N-Ports in the FC world). To support NPV on the UCS 6248, the N-Port ID Virtualization (NPIV) feature must be enabled on the MDS 9134 Switch.

```
# show feature | grep npiv
npiv 1 enabled
# show interface br
```

```
-----
Interface Vsan Admin Admin Status SFP Oper Oper Port
          Mode Trunk Mode Speed Channel
          Mode (Gbps)
-----
```

```
fc1/1 1 auto on up swl F 4 --
fc1/2 1 auto on up swl F 4 --
fc1/3 1 auto on up swl F 4 --
fc1/4 1 auto on up swl F 4 --
```

The VSANs must be consistent on the ESX/ESXi host, UCS, MDS, and the FC storage array. VSAN configuration can be done either in the MDS switches' CLI or the Cisco MDS Device



manager. Cisco Fabric Manager can also be used for managing of the SAN configuration and zoning information.

The complete MDS 9506 configuration can be found here : [MDS9506 Configuration](#).

The complete MDS 9134 configuration can be found here : [MDS9134 Configuration](#)

See your FC storage array manufacturer's instructions for configuration details.

Refer to EMC documentation for specific configuration guidance on provisioning EMC Unified Storage in virtual desktop environment :

<http://www.emc.com/collateral/solutions/reference-architecture/h8020-virtual-desktops-celerra-vmware-citrix-ra.pdf>

<http://www.emc.com/collateral/software/technical-documentation/h6082-deploying-vmware-view-manager-celerra-unified-storage-plaform-solution-guide.pdf>

NFS Storage Components

As shown in Figure 5 above, the NFS based storage array is connected to the Cisco Nexus 5548. The array needs to have L2 adjacency to the hypervisors. If the array is on another L2 segment then special routes will need to be manually added to both the array and the hypervisor connections. The NFS array can be connected to another Cisco Nexus 5548 or the Cisco Nexus 7010 as long as the L2 adjacency is maintained. Jumbo Frames need to be configured on all the Ethernet switches that make up the pathway between the hypervisors and the NFS storage array.

See your NFS based storage storage array manufacturer's instructions for configuration details.

Cisco Nexus 1000v

The Cisco Nexus 1000V was overlaid across all the servers in each of the Blade enclosures. The Nexus 1000V provides the distributed virtual switch with Layer 2 intelligent edge features such as QoS and Security. Cisco Nexus 1000V Series is software switch implementation for VMware vSphere environments running the Cisco NX-OS Software operating system.

The following changes were made on the Nexus 1000v port profile configuration to forward virtual desktop traffic to the VSG and vWAAS virtual appliance hosted services using vPath :

```
port-profile type vethernet VM-60-WebVSG
  vmware port-group
  switchport mode access
  switchport access vlan 60
  org root/Sit_ORT
  ip verify source dhcp-snooping-vlan
  vn-service ip-address 10.0.46.5 vlan 46 fail open security-profile SP_HVD
```




```
no shutdown
max-ports 1024
state enabled
port-profile type vethernet VM-60-View-VM-vWAAS
vmware port-group
switchport mode access
switchport access vlan 60
vn-service ip-address 10.0.132.40 vlan 132 fail open
no shutdown
state enabled
```

The complete Nexus 1000v configuration can be found here : [Nexus1000v Configuration](#).

Hypervisor Installation and Configuration

VMware ESX/ESXi

In this test The VMware ESX/ESXi hypervisor was installed on the servers. Version 5.1a was tested. The vSphere/vCenter was used to manage the hypervisor.

The ESX/ESXi and vCenter configuration screenshots can be found here : [vSphere configuration](#).

Desktop Virtualization Software Installation and Configuration

VMware View Configuration

In this test VMware View 5.1.2 was installed to provide DV services to end users. The VMware View Composer 3.0 was used to provision the hosted virtual desktop pools.

The VMware View configuration screenshots can be found here : [VMWare View Configuration](#).

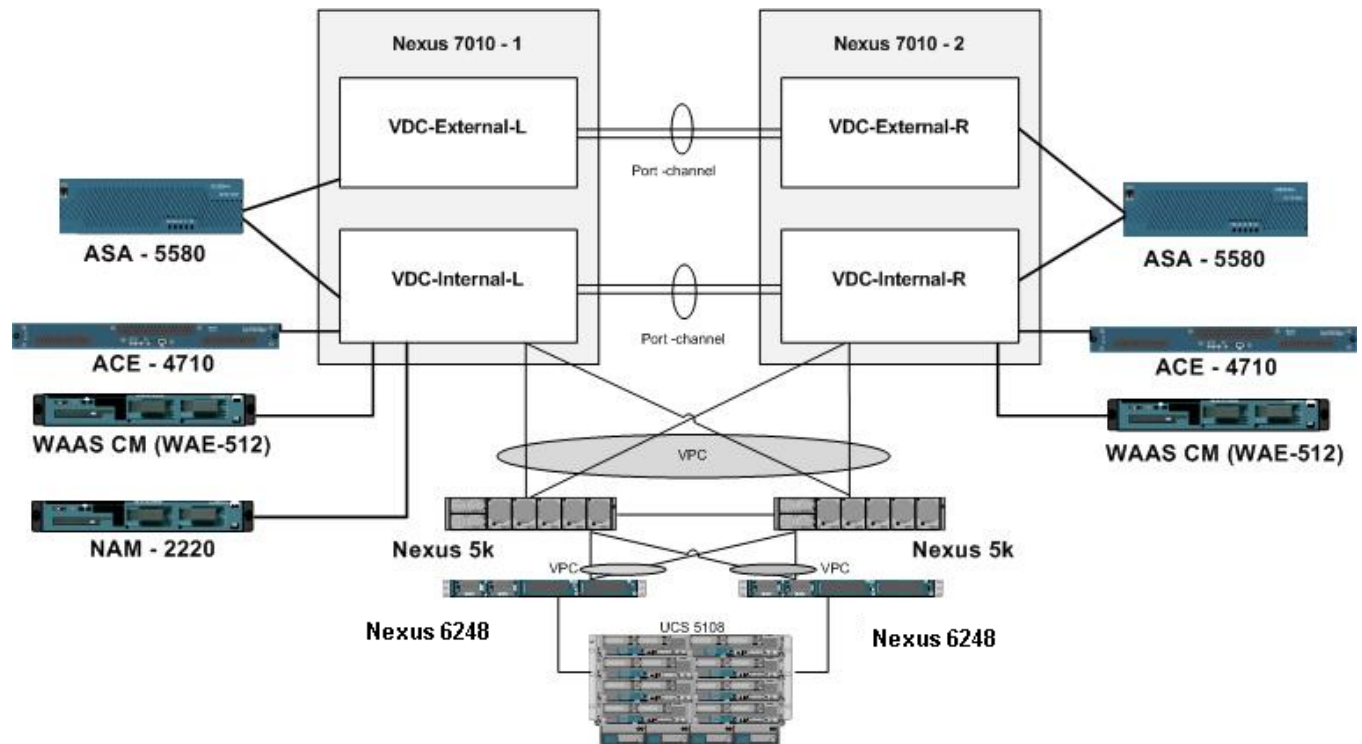
Citrix XenDesktop Configuration

In this test Citrix XenDesktop 5.6 FP1 was installed to provide DV services to end users. The Citrix Desktop Studio was used to provision the hosted virtual desktop pools.

The Citrix XenDesktop configuration screenshots can be found here : [Citrix XenDesktop Configuration](#).

Data Center Networking Infrastructure

Figure 7: Data Center Network Components



Cisco Nexus 5548 Access Layer Switch

The Cisco Nexus 5548P is a 1RU 10Gbps switch offering up to 960 Gbps throughput and up to 48 ports. It offers 32, 1/10 Gbps fixed SFP+ unified Ethernet/FCoE ports and one expansion slot. The expansion modules include a 16-port 10 Gbps SFP+ Ethernet/FCoE and a 8-port 10 Gbps SFP+ Ethernet/FCoE, plus 8-port 1/2/4/8Gbps Native FC.

The Cisco Nexus 5548, in combination with the Cisco Nexus 1000v, provides the functions for the Data Center Access Layer. This test configuration consists of a pair of Cisco Nexus 5548. Four 10 GE uplinks are configured on each of the Cisco UCS Fabric interconnect and are connected to each Nexus 5548 in parallel. The upstream interfaces are connected to ports that belong to the Internal Virtual Device Contexts (VDCs) on the Cisco Nexus 7010.

The complete Nexus 5548 configuration can be found here : [Nexus 5548 Configuration](#).



Cisco Nexus 7010

The Cisco Nexus 7010 Switch is used in the collapsed module for both the Data Center Aggregation and Core layers. This is done by creating two Virtual Device Contexts (VDCs): Internal (connected to Hosted Desktops, Application Servers) and External (connected to Enterprise Core switches). The Internal VDC acts as the Aggregation layer. The External VDC acts like the Core Layer. Each VDC is isolated from the other for increased availability. Should one VDC encounter an error or crash, the other is not affected. The Nexus 7010s are installed as a redundant pair.

The complete Nexus 7010 configuration can be found here: [Nexus 7010 Internal Device Context Configuration](#) and [Nexus 7010 External Device Context Configuration](#).

Cisco Application Control Engine (ACE4710)

The Cisco Application Control Engine (ACE4710) is used in the Cisco Virtual Workspace (VXI) Smart Solution environment to provide load balancing functions for the DV Connection Brokers. They are connected in a redundant pair to the Internal VDC on the Cisco Nexus 7010. Virtual contexts are created on the ACE for different test environments and each context included server farms for VMware View Desktops, the Citrix XenDesktops, and Microsoft Remote Desktops.

The following configurations on the ACE implement health monitoring probes for the View Manager and XenDesktop Controller:

```
probe https View-Web
  interval 15
  faildetect 1
  passdetect interval 30
  passdetect count 2
  receive 2
  ssl version all
  expect status 200 200
  open 1
probe http Xen-Web
  interval 15
  faildetect 1
  passdetect interval 15
  passdetect count 2
  receive 2
  expect status 200 200
  open 1
```

The following configurations on the ACE setup the XenDesktop Controller server farm:

```
rserver host XenCM1
  ip address 10.0.132.11
  inservice
rserver host XenCM2
  ip address 10.0.132.24
  inservice
```



```
serverfarm host XenCM
  probe Ping
  probe Xen-Web
  fail-on-all
  rserver XenCM1
  inservice
  rserver XenCM2
  inservice

sticky ip-netmask 255.255.255.255 address source StickyXen
  timeout 5
  serverfarm XenCM

class-map match-all Xen-VIP
  2 match virtual-address 10.0.60.36 any

policy-map type loadbalance first-match Xen-LB
  class class-default
  sticky-serverfarm StickyXen

policy-map multi-match Xen
  class Xen-VIP
  loadbalance vip inservice
  loadbalance policy Xen-LB
  loadbalance vip icmp-reply
  nat dynamic 1 vlan 132

interface vlan 60
  service-policy input Xen
  no shutdown
```

The complete Cisco ACE4710 configuration can be found here: [ACE Configuration](#).

Cisco Adaptive Security Appliance (ASA5580)

The Cisco Adaptive Security Appliance installed in the Data Center provides firewall services to isolate and protect the various compute resources from both external traditional desktop users as well as the DV users installed in the data Center. Two virtual contexts are used on the ASA : Non Server (connected to VRF for Hosted Desktops) and Server (connected to VRF for Application Servers). The ASA5580s are deployed as a redundant pair (configured in active-active mode) and are connected to the Internal VDC and External VDC on the Cisco Nexus 7010.

Use the ASDM or the ASA CLI to provision security services on the ASA. The following configuration on the ASA provisions services (UC and Virtual Desktop services) and hosts to be allowed through the firewall :

```
object-group service UC-SERVICES
  group-object JABBER
  group-object RTP
  group-object SCCP
  group-object SIP
  group-object WEB-SERVICES
  service-object tcp destination range 1101 1129
  service-object tcp destination eq 2444
  service-object tcp destination eq 2749
```



```
service-object tcp destination eq 3223
service-object tcp destination eq 3224
service-object tcp destination eq 3804
service-object tcp destination eq 4321
service-object tcp destination eq 61441
service-object tcp destination eq 8007
service-object tcp destination eq 8009
service-object tcp destination eq 8111
service-object tcp destination eq 8222
service-object tcp destination eq 8333
service-object tcp destination eq 8404
service-object tcp destination eq 8444
service-object tcp destination eq 8555
service-object tcp destination eq 8998
service-object tcp destination eq 9007
service-object tcp destination eq 9009
service-object tcp destination eq ctigbe
group-object LDAP
group-object TFTP
group-object IMAP

object-group service ICA - desktop protocols
service-object tcp destination eq 1604
service-object tcp destination eq 2598
service-object tcp destination eq citrix-ica
object-group service PCOIP
service-object tcp destination eq 32111
service-object tcp destination eq 4172
service-object tcp destination eq 50002
service-object udp destination eq 50002
service-object udp destination eq 4172
object-group service RDP
service-object tcp destination eq 3389
object-group service DESKTOP-SERVICES
group-object ICA
group-object RDP
group-object PCOIP

access-list allowall extended permit object-group UC-SERVICES object-group ALL-HOSTED-DESKTOPS object-group UC-SERVERS
```

Similarly, hosts and services in the network like hypervisor managers and desktop connection managers should also be provisioned.

Use the following configuration on the ASA to enable jumbo frames :

```
mtu outside 9216 Used for Jumbo Frames
mtu inside 9216
```

Configure the global policy to enable application layer inspection by the ASA :

```
policy-map global_policy
class inspection_default
inspect waas
```

It is important to add 'inspect waas' to allow vWAAS traffic through the ASA. Otherwise vWAAS traffic will be blocked going through the ASA.



The complete Cisco ASA 5580 configuration can be found here : [ASA Server Configuration](#) and [ASA Non Server Configuration](#).

Cisco WAN Acceleration Engine (WAE-512)

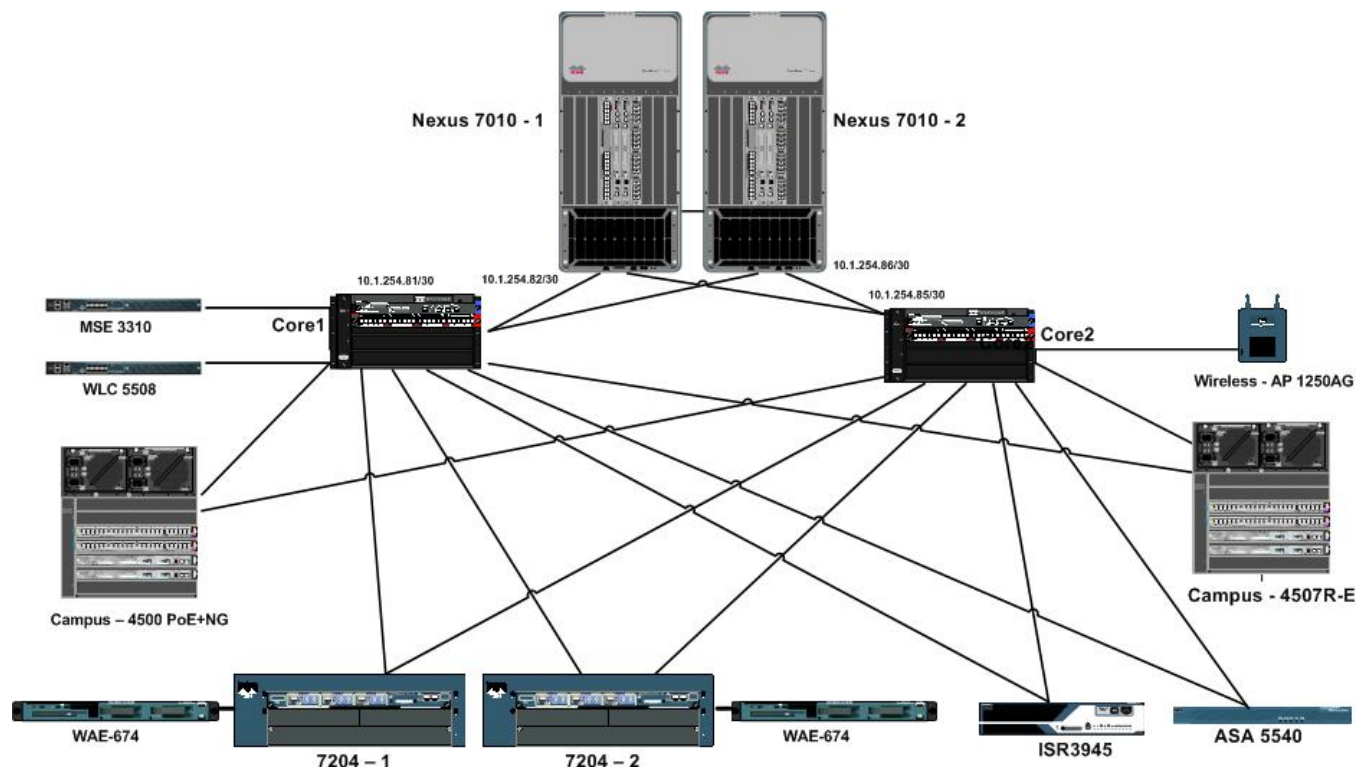
The WAE-512s installed in the data center are the controllers for the other WAAS appliances installed. They are installed as a redundant pair. They also have QoS and Citrix Multi-Stream ICA enabled.

The complete Cisco WAE-512 configuration can be found here : [WAAS Controller Configuration](#).

Campus Network

The campus network is composed of two redundant Catalyst 6504E switches, Branch Connectivity routers, internet access routers, WAN accelerators, and Firewall Appliances. It also contains equipment for local campus access.

Figure 8: Campus Network Components



Cisco Catalyst 6504E (CAT6504E)

The Cisco CAT6504E switches are used for the core and distribution layer functions for the campus network. They are installed uplinked to the data center Nexus 7010 which provides the data center core functions. These switches are installed as a redundant pair.



The complete Cisco CAT6504E configuration file can be found here : [Catalyst 6504 configuration](#).

Cisco 7206VXR Router

The Cisco 7206VXR routers are used to provide branch connections that do not require VPN services.

The complete Cisco 7206VXR configuration can be found here : [7206VXR Configuration](#).

Cisco WAN Acceleration (WAE-674)

The Cisco WAE-674s installed in the campus network provide the campus-side termination of the WAAS tunnels from the branch WAE appliances.

The complete Cisco WAE-674 configuration file can be found here : [WAE-674 Configuration](#).

Cisco Adaptive Security Appliance (ASA5540)

The Campus Cisco ASA5540 network provides a VPN concentrator for the Cisco AnyConnect Clients.

The complete Cisco ASA 5580 configuration can be found here : [ASA Configuration](#).

Cisco Catalyst 4500E (Campus Access CAT4500E)

This Catalyst 4500E provides the campus user access to the network with PoE+ It contains the L2 edge features such as QoS, Security, and Energywise.

The complete Catalyst 4500E configuration file can be found here : [Catalyst4500E Configuration](#).

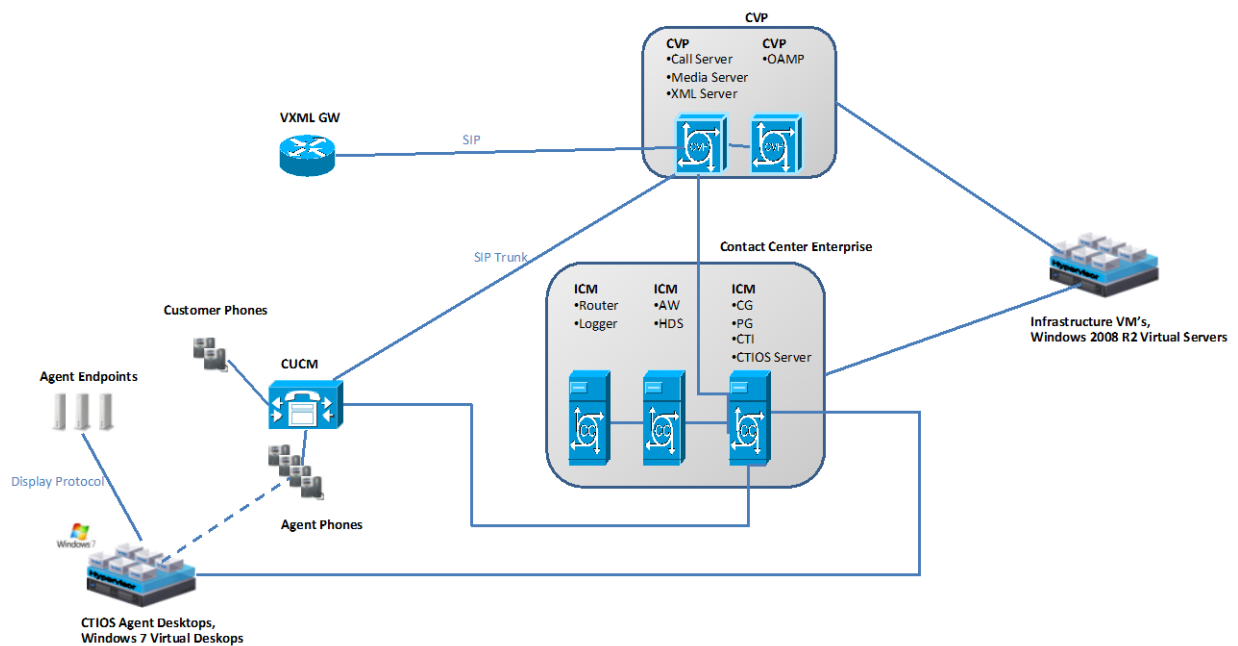
Cisco Catalyst 4507E (Campus Access CAT4507E)

The Catalyst 4507E provides alternate method for campus user access to the network. It contains the L2 edge features such as QoS and Security.

The complete Cisco Catalyst 4507E configuration can be found here : [Catalyst 4507E Configuration](#).

Contact Center

The following diagram illustrates the UCCE configuration. All of the UCCE servers run as virtual machines in the data center. CTI OS is installed on each agent's hosted virtual desktop. The contact center is setup as a comprehensive functional deployment model. This functional deployment model provides organizations with a mechanism to route and transfer calls across a VoIP network, to offer IVR services and to queue calls before being routed to a selected agent. This is typical of pure IP-based contact centers. Callers are provided IVR services initially and then are queued for treatment and then transferred to an agent.



Note: Phones and endpoints simulated by ScaPa for load and scale testing.

Figure 10 – UCCE Topology



VXC-6215

Both VMware View and Citrix solutions are tested on the VXC-6215. The VXC-6215 is configured with the following .ini file.

```
Update.Mode=both
Privilege=High
Autopower=yes
InstallAddons=vxme-9.0.0-298.sletc11sp2.rpm

DisbleVnc=no
VNCAuthTypes=none
VncPrompt=no
ICADenyUsb=class=01
VMWareViewExcludeUSBFamily=hid,keyboard,mouse,audio,video

CONNECT=BROWSER \
Description="SONC Citrix XenDesktop" \
URL=https://citrix-web-sonc.lab.local \
Resolution=FullScreen \
Mode=Normal \
autoconnect=yes


CONNECT=VMWARE_VIEWCLIENT \
Description="SONC View Connection Server" \
Host=vc50-sonc-conn.lab.local \
DomainName=LAB \
autoconnect=yes



ImportCerts=yes
Certs=lab-ca-root.pem
```

This .ini file provisions both a view client icon and a firefox icon (used for XenDesktop/XenApp) on the desktop.

CUCM Config

The CUCM config for the VXC-6215 is updated as of this release. The Product type is that of “Cisco Unified Client Services Framework (CSF) as shown below.

Status	
 Status: Ready	

Association Information	
Modify Button Items	
1	 Line [1] - 10001 (no partition)
----- Unassigned Associated Items -----	
2	 Line [2] - Add a new DN

Phone Type	
Product Type:	Cisco Unified Client Services Framework
Device Protocol:	SIP

Device Information	
Registration	Unknown
IP Address	Unknown
<input checked="" type="checkbox"/> Device is Active	
<input checked="" type="checkbox"/> Device is trusted	
Device Name*	<input type="text" value="CSFsituser1"/>



The corresponding end user must have the following permissions.

– Permissions Information

Groups	<div>Standard CCM Admin Users Standard CCM End Users Standard CTI Allow Control of Phones supporting C Standard CTI Enabled</div>	View Details
Roles	<div>Standard CCM Admin Users Standard CCM End Users Standard CCMUSER Administration Standard CTI Allow Control of Phones supporting C Standard CTI Enabled</div>	View Details

Dual VLAN config

The VXC-6215 contains two virtual MAC addresses that allow it to be placed in both a voice and data VLAN. A typical access switch config is shown as follows:

```
interface GigabitEthernet0/9
 switchport access vlan 20
 switchport mode access
 switchport voice vlan 25
 authentication host-mode multi-domain
 authentication port-control auto
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 2
 spanning-tree portfast
end
```

The VXC-6215 supports MAB authentication which is also shown in the configuration above.

Remote ASA config

The VXC-6215 ships with AnyConnect and may be used to connect via SSL VPN to an enterprise's corporate network. The corresponding ASA config is shown below.

```
ip local pool SSLClientPool 10.1.12.11-10.1.12.200 mask 255.255.255.0 ### Remote client
### address pool

ssl trust-point test outside
webvpn
 enable outside ### Enable SSL VPN on outside interface.
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-3.0.0629-k9.pkg 1 regex "Windows CE"
 anyconnect image disk0:/anyconnect-linux-2.5.2019-k9.pkg 2 regex "Linux"
 anyconnect enable
 tunnel-group-list enable
 group-policy SSLClient internal
 group-policy SSLClient attributes
 wins-server none
```



```
dns-server value 10.0.128.200
vpn-tunnel-protocol ssl-client ssl-clientless
default-domain value lab.local
webvpn
anyconnect ssl dtls enable
anyconnect ask enable default anyconnect timeout 10
tunnel-group SSLClient type remote-access
tunnel-group SSLClient general-attributes
default-group-policy SSLClient
dhcp-server 10.0.128.205
tunnel-group SSLClient webvpn-attributes
group-alias MY_RA enable
```

WebAuth

The switch configuration for web auth is as follows:

```
interface GigabitEthernet0/7
switchport access vlan 100
switchport mode access
ip access-group webauth in
authentication order mab
authentication priority mab
authentication port-control auto
mab
dot1x pae authenticator
spanning-tree portfast
end

ip access-list extended redirect
deny    udp any any eq domain
deny    ip any host 10.0.128.132    ### ISE server
deny    ip any host 10.0.128.27    ### VXC-M Server
permit tcp any any eq 443
permit tcp any any eq www

ip access-list extended webauth
permit ip any any
```

The ISE has the following authorization policies:

	2nd Auth	if Network Access:UseCase EQUALS Guest Flow	then PermitAccess
	is a guest	if AD1:ExternalGroups EQUALS lab.local/Users/SITUserGroup	then Re_Auth
	MAC not known	if Session:PostureStatus EQUALS Unknown	then Web_Auth

where the Web_Auth profile contains:

▼ Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=redirect
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa
cisco-av-pair = url-redirect=https://ip:8443/guestportal/gateway?sessionId=SessionIdValue&action=cwa
```

the Re-Auth profile contains:

▼ Attributes Details

```
Access Type = ACCESS_ACCEPT
Session-Timeout = 1
Termination-Action = Default
```

MediaNet

The access switch configuration for medianet contains:

metadata flow

```
interface GigabitEthernet5/1
  description fishbowl access port
  switchport access vlan 100
  switchport mode access
  metadata flow
  spanning-tree portfast
  service-policy input VXC-6215
```

```
class-map match-any CISCO-PHONE
  match application cisco-phone
```

```
policy-map VXC-6215
  class CISCO-PHONE
    set dscp ef
```

```
ip rsvp snooping vlan 100
```



Appendix 1 - Endpoint security 802.1x, MacSec, MAB, ACS

Configuration sequences below are built based on the discussion in Phase Cisco Virtual Workspace (VXI) Smart Solution CVD. Please see Deployment and Configuration best practices of Cisco Virtual Workspace (VXI) Smart Solution security components section under Anyconnect 3.0, Dot1x, MacSec and MAB along with ACS. The configuration sequence below is an sample scenario and not part of the validated architecture. It is presented here as a reference to understand configuration sequence of various elements involved in securing the Cisco Virtual Workspace (VXI) Smart Solution Access.

Following procedure should be used to setup Anyconnect, Dot1x, ACS5.2 and MacSec in Cisco Virtual Workspace (VXI) Smart Solution environment.

1. Any Connect 3.0 Network Access Manager (NAM) Configuration

In this section, the AnyConnect NAM Profile Editor is used to create an example wired 802.1x connection that is MACsec enabled. Before starting Launch the profile editor

Client Policy Configuration : Defines the options that govern the client policy.

-
- Step 1** From the left navigation menu, select Client Policy
 - Step 2** Select Enable for the Service Operation under Administrative Status.
 - Step 3** Select Attempt connection after user logon for Connection Settings
 - Step 4** Under Mediatecheck Allow Wired (802.1x) Media, and Allow user to disable client
-

Note MACsec is only supported on wired media.

Authentication Policy Configuration:

Define the global association and authentication policies. This policy controls what type of networks the end user may create using the AnyConnect UI. Launch the Network menu and enable all options. Depending on the enterprise policy some options may be disabled as needed.

Network Configuration:

AnyConnect 3.0 is configured for use on a wired network that supports 802.1x authentication and MACsec encryption. From the Anyconnect UI on the Anyconnect profile editor follow the procedure below. This is a onetime procedure for each type of profile and is recommended to be distributed via ASA.

-
- Step 1** Click Add.
 - Step 2** Enter a Name for the connection (MACsec for example) and select Wired (802.3) Network
 - Step 3** At the bottom of the window, click Next
 - Step 4** Under Security Level, select Authenticating Network
 - Step 5** Within the Security section, set Key Management to MKA and Encryption to MACsec AES-GCM-128
 - Step 6** Within the Port Authentication Exception Policy, select Dependent on 802.1x. In this example the switch is configured for 'must secure' so therefore none of the port exceptions under 'Dependent on 802.1x' need to be checked.
 - Step 7** Click Next
 - Step 8** Under Network Connection Type, select User Connection.
-

Note MACsec encryption is supported for Machine and User Connections. However, in this example only User Connection is selected

- Step 9** ClickNext



Step 10 Within EAP methods, select PEAP

Note In this example PEAP is used for authentication however MACsec encryption is supported with any EAP method that generates a Session-Id (See RFC5247) including EAP-TLS, EAP-PEAP, and EAP-FAST.

Step 11 Click Next

Step 12 Within User Credentials, select Prompt for Credentials

Step 13 Click Done.

Step 14 Navigate to the menu options in the upper left corner of the Profile Editor. Choose File -> Save. Save the file as "configuration.xml".

Deploy this profile via the ASA, please refer to Chapter 2, "Deploying the AnyConnect Secure Mobility Client", of the Cisco AnyConnect Secure Mobility Client Administrator Guide.

2. Configuring the 3750-X/3560-X switch with Dot1X and MacSec

Base AAA Configuration: Base configuration for AAA (RADIUS). The configuration described below is required to enable 802.1X authentication:

```
CTS-3750X(config)#aaa new-model
CTS-3750X(config)#aaa authentication dot1x default group radius
CTS-3750X(config)#aaa authorization network default group radius
CTS-3750X(config)#aaa accounting dot1x default start-stop group radius
CTS-3750X(config)#radius-server host <ip address> auth-port 1812 acct-port 1813 key cisco123
CTS-3750X(config)#radius-server vsa send authentication
CTS-3750X(config)#radius-server vsa send accounting
```

Note The command "aaa authorization network" is required for authorization methods such as dynamic VLAN assignment or downloadable ACL.

802.1x and MACsec Configuration:

Enable 802.1X in global configuration mode
CTS-3750X(config)#dot1x system-auth-control

Enable 802.1X on interface

```
CTS-3750X(config)#int gil/0/1
CTS-3750X(config-if)#switchport mode access
CTS-3750X(config-if)#authentication port-control auto
CTS-3750X(config-if)#dot1x pae authenticator
```

Enable MACsec on interface

```
CTS-3750X(config-if)#mka default-policy
CTS-3750X(config-if)#macsec
CTS-3750X(config-if)#authentication linksec policy
CTS-3750X(config-if)#authentication event linksec fail action next-method
CTS-3750X(config-if)#authentication event linksec fail action authorize VLAN
```

3. Configure 802.1x Components in ACS: 802.1x policy elements, Identity Stores, Access Services and Access Service Selection are configured on ACS.

Configuring Identity Stores and an Identity

Step 1 In the left column, under Users and Identity Stores, select Identity Store Sequences and select Create.



- Step 2** Enter a name (in this example the name is "802.1x Identities"). Select the check box for Password Based authentication method, and then add Internal Users to the Selected section. Click Submit.
- Step 3** In the left navigation column, under Users and Identity Stores, expand Internal Identity Stores, and select Users. Click Create.
- Step 4** Enter a username. Enter and confirm a password under Password Information. Click Submit when done.

Create an Authorization Profile: Creating a wired authorization profile. This profile is used to define users access to the network.

-
- Step 1** In the left navigation column, under Policy Elements, expand Authorization and Permissions. Then expand Network Access and select Authorization Profiles. Click Create.
 - Step 2** On the General tab, specify a name for this profile.
 - Step 3** Click on the Common Tasks tab. Navigate down to 802.1x-REV. Select a Static value of "must-secure".

Note This linksec policy will override the policy configured on the interface

- Step 4** Click Submit.

Create a 802.1x Access Service

-
- Step 1** In the left navigation column, under Access Policies, click Access Services.
 - Step 2** At the bottom of the resulting pane, click Create.
 - Step 3** Specify a name to for this service.
 - Step 4** Under Access Service Policy Structure, choose Based on service template, and then click Select.
 - Step 5** Choose Network Access-Simple and click OK. Then click Next at the bottom of the resulting window.
 - Step 6** No need to change any settings in this window*. * Click Finish. You will be prompted to modify the service selection policy. Click No.

Define the Authorization Policy: Here the authorization policy of the access service is defined.

In the left navigation column, under Access Policies navigate to the access service that was just created. (802.1x Service in this example).

-
- Step 1** Expand 802.1x Service and click Authorization. Click Create.
 - Step 2** Specify a name for the rule
 - Step 3** Under Conditions, choose NDG:Location and click Select. Set the value to All Locations.
 - Step 4** Scroll down to the Results section and click Select. An Authorization Profiles dialog box appears:
 - Step 5** Select the Finance 802.1x Authz profile that was created in Create an Authorization Profile section.
 - Step 6** Click OK. Click Save Changes.

Create a Service Selection Rule: Creating a service selection rule. This rule ensures the policies defined in an access service (802.1x Service in this example) are applied to 802.1x requests.



-
- Step 1** In the left navigation menu, under Access Policies, click Service Selection. At the bottom of the right pane, click Create.
- Step 2** Specify a name for the rule (Match 802.1x Requests is used here)
- Step 3** Select Protocol and match it with Radius.
- Step 4** Select Compound Condition. Under Condition, choose RADIUS-IETF for Dictionary and Service-Type for Attribute. For Value, select Framed and click Add to add the condition to the Current Condition Set.
- Step 5** Under Results, select the access service that was created in Create an 802.1x Access Service section. Click Ok. Click Save Changes.
- Step 6** Finally: Launch AnyConnect and get connected.

The following dot1x and MAB port configuration was found to provide a satisfactory experience with most thin clients:

```
interface GigabitEthernet0/10
switchport access vlan XX
switchport mode access
dot1x mac-auth-bypass
dot1x pae authenticator
dot1x port-control auto
dot1x timeout tx-period 2
spanning-tree portfast
```



Appendix 2 – QOS settings in Cisco Virtual Workspace (VXI) Smart Solution

Many applications do not mark traffic with DSCP values. For even those that do, the marking may not be appropriate for every enterprise's priority scheme. Therefore, you should perform hardware-based classification (using a Cisco Catalyst or Cisco Nexus Family switch) instead of software-based classification. In testing, the markings were implemented on a Cisco Nexus 1000V Switch whenever possible. See below for an configuration example used during testing of Cisco Virtual Workspace (VXI) Smart Solution system

Classification:

```
ip access-list RDP
  permit tcp any eq 3389 any
ip access-list PCoIP-UDP
  permit udp any eq 50002 any
ip access-list PCoIP-TCP
  permit tcp any eq 50002 any
ip access-list PCoIP-UDP-new
  permit udp any eq 4172 any
ip access-list PCoIP-TCP-new
  permit tcp any eq 4172 any
ip access-list ICA
  permit tcp any eq 1494 any

ip access-list View-USB
  permit tcp any eq 32111 any

ip access-list MMR
  permit tcp any eq 9427 any

ip access-list NetworkPrinter
  permit ip any host 10.1.128.10
  permit ip any host 10.1.2.201

ip access-list CUPCDesktopControl
  permit tcp any host 10.0.128.125 eq 2748
  permit tcp any host 10.0.128.123 eq 2748
```

Class-maps:

```
class-map type qos match-any CALL-SIGNALING
  match access-group name CUPCDesktopControl

class-map type qos match-any MULTIMEDIA-STREAMING
  match access-group name MMR

class-map type qos match-any TRANSACTIONAL-DATA
  match access-group name RDP
  match access-group name PCoIP-UDP
  match access-group name PCoIP-TCP
  match access-group name PCoIP-UDP-new
  match access-group name PCoIP-TCP-new

class-map type qos match-any BULK-DATA
  match access-group name View-USB
  match access-group name NetworkPrinter
```

Policy-map:

```
policy-map type qos pmap-HVDAccessPort
  class CALL-SIGNALING
    set cos 3
```



```
set dscp cs3
! dscp = 24
class MULTIMEDIA-STREAMING
set cos 4
set dscp af31
! dscp = 26
class TRANSACTIONAL-DATA
set cos 2
set dscp af21
! dscp = 18
class BULK-DATA
set cos 1
set dscp af11
! dscp = 10
```

Apply policy-map to the switch port to which the hosted virtual desktop (HVD) virtual machine connects:

```
port-profile type vethernet VM240
description Port profile for View HVD VM access
vmware port-group
switchport mode access
switchport access vlan 240
no shutdown
state enabled
system vlan 240
service-policy input pmap-HVDAccessPort
Nexus 1000v QoS information:
```

http://www.cisco.com/en/US/partner/docs/switches/datacenter/nexus1000/sw/4_0/qos/configuration/guide/qos_2cassification.html#wp1067764

Note These examples are meant to be guidelines for deploying QoS in a Cisco Virtual Workspace (VXI) Smart Solution network and should not be applied without consideration given to all traffic flows within the enterprise.

In a campus network, the bandwidth is high enough so that contention for the resources should be minimal. However, slower connections in a branch WAN router network need to be examined. Here at the egress point from the high-speed connections of the branch-office LAN to the slower-speed links of the WAN is where bandwidth contention is likely to occur. Service policies that constrain the amount of bandwidth that is dedicated to a given protocol are defined and applied at this point. These same queuing and bandwidth configurations can be placed anywhere there is a concentration of Cisco Virtual Workspace (VXI) Smart Solution endpoints, to enforce the appropriate response in case of traffic congestion. Below is an example of Bandwidth Services Policies used during Cisco Virtual Workspace (VXI) Smart Solution system testing.

Class Maps - defining the buckets:

```
class-map match-any BULK-DATA
match dscp af11 af12 af13
class-map match-all NETWORK-CONTROL
match dscp cs6
class-map match-all MULTIMEDIA-CONFERENCING
match dscp af41 af42 af43
class-map match-all VOICE
match dscp ef
class-map match-all SCAVENGER
match dscp cs1
class-map match-all CALL-SIGNALING
match dscp cs3
class-map match-all TRANSACTIONAL-DATA
match dscp af21 af22 af23
class-map match-any MULTIMEDIA-STREAMING
match dscp af31 af32 af33
```

**Policy Maps - Assigning the bandwidth per bucket:**

```
policy-map WAN-EDGE
  class VOICE
    priority percent 10
  class NETWORK-CONTROL
    bandwidth percent 2
  class CALL-SIGNALING
    bandwidth percent 5
  class MULTIMEDIA-CONFERENCING
    bandwidth percent 5
    random-detect dscp-based
  class MULTIMEDIA-STREAMING
    bandwidth percent 5
    random-detect dscp-based
  class TRANSACTIONAL-DATA
    bandwidth percent 65
    random-detect dscp-based
  class BULK-DATA
    bandwidth percent 4
    random-detect dscp-based
  class SCAVENGER
    bandwidth percent 1
  class class-default
    bandwidth percent 25
    random-detect
```

Cisco Virtual Workspace (VXI) Smart Solution thin-client endpoints do not typically provide the capability to mark the session traffic. Therefore, the same marking that was performed on the Cisco Nexus1000V in the data center for outbound desktop virtualization traffic must be performed at the branch office on behalf of the endpoints for the traffic returning to the data center virtual machine. Below is an example of a branch switch configuration used during Cisco Virtual Workspace (VXI) Smart Solution system testing.

Endpoint

Classification:

```
ip access-list RDP
  permit tcp any eq 3389 any
ip access-list PCoIP-UDP
  permit udp any eq 50002 any
ip access-list PCoIP-TCP
  permit tcp any eq 50002 any
ip access-list PCoIP-UDP-new
  permit udp any eq 4172 any
ip access-list PCoIP-TCP-new
  permit tcp any eq 4172 any
ip access-list ICA
  permit tcp any eq 1494 any

ip access-list View-USB
  permit tcp any eq 32111 any

ip access-list MMR
  permit tcp any eq 9427 any

ip access-list NetworkPrinter
  permit ip any host 10.1.128.10
  permit ip any host 10.1.2.201

ip access-list CUPCDesktopControl
  permit tcp any host 10.0.128.125 eq 2748
  permit tcp any host 10.0.128.123 eq 2748
```



Class-maps:

```
class-map type qos match-any CALL-SIGNALING
  match access-group name CUPCDesktopControl

class-map type qos match-any MULTIMEDIA-STREAMING
  match access-group name MMR

class-map type qos match-any TRANSACTIONAL-DATA
  match access-group name RDP
  match access-group name PCoIP-UDP
  match access-group name PCoIP-TCP
  match access-group name PCoIP-UDP-new
  match access-group name PCoIP-TCP-new

class-map type qos match-any BULK-DATA
  match access-group name View-USB
  match access-group name NetworkPrinter
```

Policy-map:

```
policy-map type qos pmap-HVDAccessPort
  class CALL-SIGNALING
    set cos 3
    set dscp cs3
    ! dscp = 24
  class MULTIMEDIA-STREAMING
    set cos 4
    set dscp af31
    ! dscp = 26
  class TRANSACTIONAL-DATA
    set cos 2
    set dscp af21
    ! dscp = 18
  class BULK-DATA
    set cos 1
    set dscp af11
    ! dscp = 10
```



Appendix 3 – Jabber and Deskphone control

How to deliver a UC video/voice call solution using deskphone control in a hosted virtual desktop environment

This section will describe the required components and necessary steps to achieve a basic Cisco Jabber environment (IM, directory lookup and voice/video calls) running in a Citrix XenDesktop hosted virtual desktop (HVD) deployment.

The required components are listed below:

- Cisco Unified Communications Manager (Cisco UCM) 7.1(5) or later
- Cisco Unified Presence Server 8.0 or later
- Cisco Jabber 9.0.5 or later
- Cisco IP phones 9971 or 9951 with USB video camera (Phone load <9-1-0VD-6>)
- VXC-2112 clients
- LDAP server (Microsoft Active Directory is used in this example)
- Citrix XenDesktop 5

Cisco Unified Communications Manager

Delivering the UC experience to XenDesktop HVD users can be accomplished on either virtualized Cisco UCM or MCS server based Cisco UCM deployments. For details on virtualizing your Cisco UCM see

http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/virtual/servers.html

Cisco UCM administration does not require any extra steps or upgrades to achieve UC with Citrix XenDesktop. The provisioning and assignment of users, devices and deskphone control remains the same as if the deployment of Cisco Jabber was installed on regular laptops, but instead the Cisco Jabber application will be installed on the users Hosted Virtual Desktop. Cisco UCM must be integrated to Cisco Unified Presence server (CUP) in order to deliver Cisco Jabber sign-in, instant message, directory look-up and deskphone control features. To integrate Cisco UCM to CUP follow the steps below:

- [User and Device Configuration on Cisco Unified Communications Manager](#)
http://www.cisco.com/en/US/docs/voice_ip_comm/cups/8_0/english/install_upgrade/deployment/guide/dgcucm.html#wp1099013
- [Configure the Presence Service Parameter](#)
http://www.cisco.com/en/US/docs/voice_ip_comm/cups/8_0/english/install_upgrade/deployment/guide/dgcucm.html#wp1063445
- [Configure the SIP Trunk on Cisco Unified Communications Manager](#)
http://www.cisco.com/en/US/docs/voice_ip_comm/cups/8_0/english/install_upgrade/deployment/guide/dgcucm.html#wp1063383
- [Configure the SIP Trunk Security Profile for Cisco Unified Presence](#)
http://www.cisco.com/en/US/docs/voice_ip_comm/cups/8_0/english/install_upgrade/deployment/guide/dgcucm.html#wp1050014
- [Configuring the SIP Trunk for Cisco Unified Presence](#)



http://www.cisco.com/en/US/docs/voice_ip_comm/cups/8_0/english/install_upgrade/deployment/guide/dgcucm.html#wp1063105

- Create Deskphone control application user as an application user on Cisco UCM (required for deskphone control)

This user is created on CUCM as a “Application User” and must match the settings on Cisco Jabber “Desk Phone Control→Settings”

The screenshot displays the Cisco Unified CM Administration web interface. The top navigation bar includes links for System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, and Bulk Administration. The main heading is "Application User Configuration". Below this, there are icons for Save, Delete, Copy, and Add New. The "Status" section shows "Status: Ready". The "Application User Information" section contains fields for User ID* (CtiGw), Password, Confirm Password, Digest Credentials, Confirm Digest Credentials, and Presence Group* (Standard Presence group). An "Edit Credential" button is present. A callout bubble indicates that the username and password must match the username password set in the CUP server. The "Permissions Information" section shows a list of Groups and Roles, both containing "Standard CTI Allow Control of All Devices" and "Standard CTI Enabled". Buttons for "Add to User Group" and "Remove from User Group" are visible. Callout bubbles indicate that these user groups must be assigned.

- [Verifying That the Required Services are Running on Cisco Unified Communications Manager](http://www.cisco.com/en/US/docs/voice_ip_comm/cups/8_0/english/install_upgrade/deployment/guide/dgcucm.html#wp1050114)

http://www.cisco.com/en/US/docs/voice_ip_comm/cups/8_0/english/install_upgrade/deployment/guide/dgcucm.html#wp1050114

For full details on how to configure Cisco Unified Communications Manager for Cisco Unified Presence see:

http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cups/8_0/english/install_upgrade/deployment/guide/dgcucm.html#wp1063445 (Section: [Configuring Cisco Unified Communications Manager for Integration with Cisco Unified Presence](#))



Each Cisco UCM end user that will use Cisco Jabber must be properly licensed. For instructions on how to license your Cisco Jabber users see:

http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cups/8_0/english/install_upgrade/deployment/guide/dglic.html#wp1081264

For all licensing requirements see:

http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cups/8_0/english/install_upgrade/deployment/guide/dglic.html#wp1081264

Cisco Unified Presence server

As with Cisco UCM the Cisco Unified Presence server can be installed on either a virtualized environment or MCS server based deployment. Also, CUP administration remains the same as if it were installed to service a laptop or desktop environment (non-hosted virtual desktop environment). To provision directory lookup a LDAP server is required and must integrate to the CUP server. For details on installing CUP server in a virtual environment see

http://www.cisco.com/en/US/docs/voice_ip_comm/cups/8_0/english/install_upgrade/installation/guide/cpinvmware.html

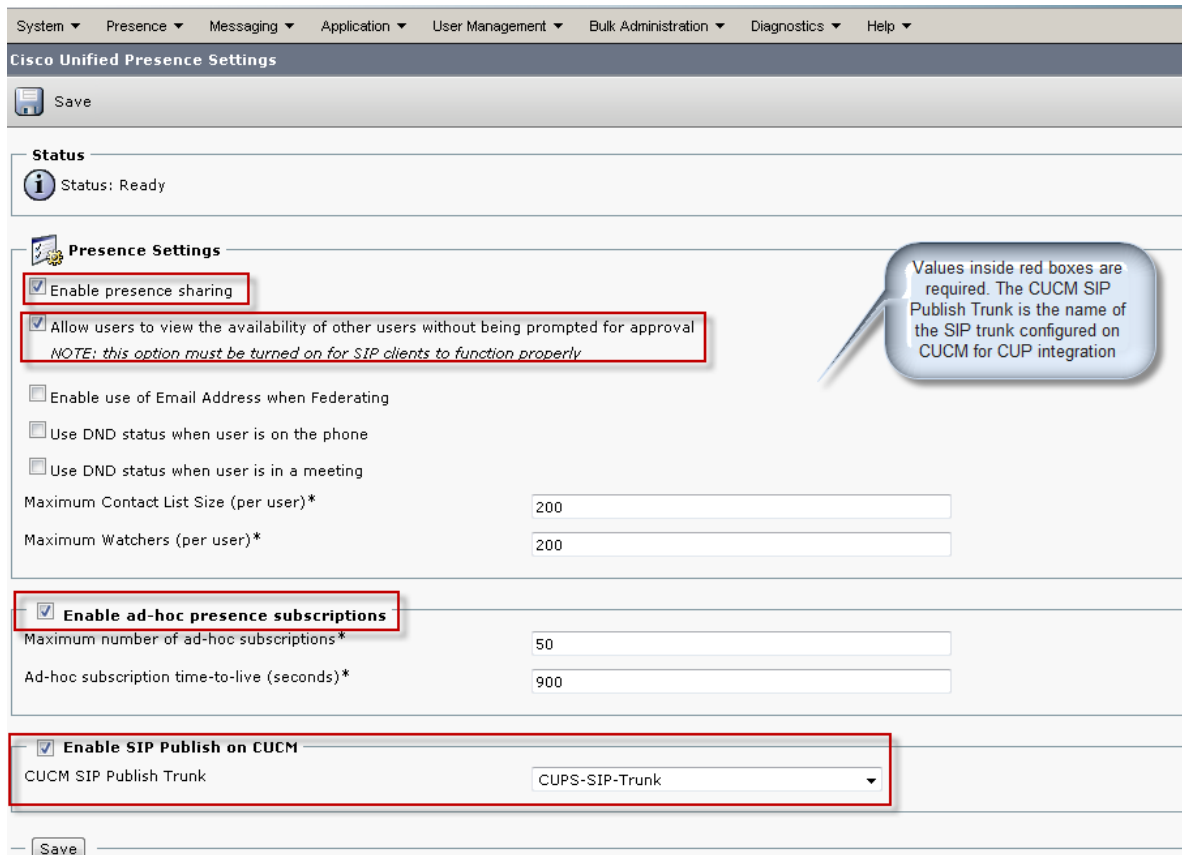
Note LDAP to CUP integration is used for directory lookup only, for user provisioning and user authentication the LDAP server must integrate to Cisco UCM. This is outside the scope of this document but information on how to integrate LDAP to Cisco Unified Communications Manager can be found here:
http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/admin/8_5_1/ccmcfg/bccm-851-cm.html

Follow the steps below to provision and assign features to CUPC/Jabber users:

- Configure CUCM Publisher


This value is configured during the Cisco Unified Presence installation process. If this field needs to be changed see:
http://www.cisco.com/en/US/docs/voice_ip_comm/cups/8_0/english/install_upgrade/installation/guide/cppostins.html#wp1075065

- Configure Cisco Unified Presence settings




System ▾ Presence ▾ Messaging ▾ Application ▾ User Management ▾ Bulk Administration ▾ Diagnostics ▾ Help ▾

Cisco Unified Presence Settings

 Save

Status

 Status: Ready

Presence Settings

☒ Enable presence sharing

☒ Allow users to view the availability of other users without being prompted for approval
NOTE: this option must be turned on for SIP clients to function properly

☐ Enable use of Email Address when Federating

☐ Use DND status when user is on the phone

☐ Use DND status when user is in a meeting

Maximum Contact List Size (per user)*

Maximum Watchers (per user)*


☒ **Enable ad-hoc presence subscriptions**

Maximum number of ad-hoc subscriptions*

Ad-hoc subscription time-to-live (seconds)*

☒ **Enable SIP Publish on CUCM**

CUCM SIP Publish Trunk

 Save

Values inside red boxes are required. The CUCM SIP Publish Trunk is the name of the SIP trunk configured on CUCM for CUP integration

- **Configure Presence Gateway**

You must configure Cisco Unified Communications Manager as a Presence Gateway on Cisco Unified Presence to enable the SIP connection that handles the availability information exchange between Cisco Unified Communications Manager and Cisco Unified Presence. The Cisco Unified Presence server sends SIP subscribe messages to Cisco Unified Communications Manager over a SIP trunk which allows the Cisco Unified Presence server to receive availability information (for example, phone on/off hook status). On how to configure the Presence gateway see:

http://www.cisco.com/en/US/docs/voice_ip_comm/cups/8_0/english/install_upgrade/deployment/guide/Deployment_Guide_Cisco_Unified_Presence_85_March16.pdf (search for “Presence gateway”)

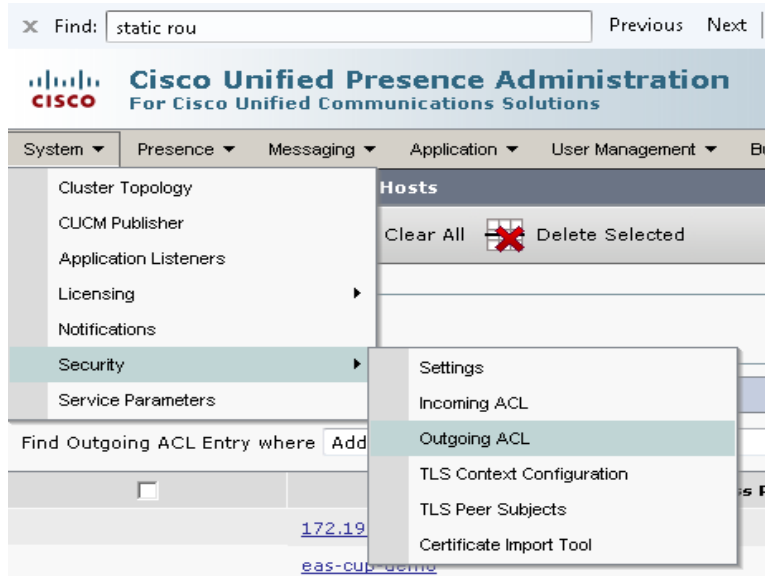
- **Enable Instant Messaging**

You can enable instant messaging on CUP server through Messaging → Settings menu. See :

http://www.cisco.com/en/US/docs/voice_ip_comm/cups/8_0/english/install_upgrade/deployment/guide/Deployment_Guide_Cisco_Unified_Presence_85_March16.pdf (search for “instant messaging”)

- **Create incoming and outgoing ACL (access list)**

Access-list for both incoming and outgoing communication between CUCM and CUP server must be configured. Either IP address or FQDN (if a DNS server is deployed) can be used. For Outgoing ACL configure the CUCM server only, for the incoming ACL configure both CUCM and CUP server. These values are typically automatically populated by the CUP server during install and integration to the CUCM, but if errors occur you must enter these values manually.



- Configure Unified Personal Communicator settings

TFTP and proxy settings must be configured under Applications → Cisco Unified Personal Communicator → Settings. The TFTP server will be your CUCM publisher (Or CUCM node handling CUPC application). See

http://www.cisco.com/en/US/docs/voice_ip_comm/cups/8_0/english/install_upgrade/deployment/guide/Deployment_Guide_Cisco_Unified_Presence_85_March16.pdf (search for “Configuring the Proxy Listener and TFTP Addresses”)

- Configure LDAP host and profile

LDAP user provisioning, user authentications and directory look-up are all supported. In order to support LDAP user provisioning and authentication the LDAP integration is done with Cisco Unified Communications Manager, for directory lookup services the LDAP integration is done on the Cisco Unified Presence server. For details see: http://www.cisco.com/en/US/docs/voice_ip_comm/cups/8_0/english/install_upgrade/deployment/guide/Deployment_Guide_Cisco_Unified_Presence_85_March16.pdf (for CUCM LDAP integration search for “LDAP integrations”) for LDAP to CUP integration search for “Creating LDAP Profiles and Adding Cisco Unified Personal Communicator Users to the Profile and Configuring LDAP Server Names and Addresses for Cisco Unified Personal Communicator”)

- Configure DeskPhone control settings

To configure deskphone control both the CUCM and CUP server must be configured to the CTI (Computer Telephony Integration) application. For details see:

http://www.cisco.com/en/US/docs/voice_ip_comm/cups/8_0/english/install_upgrade/deployment/guide/Deployment_Guide_Cisco_Unified_Presence_85_March16.pdf (search for “How to Configure CTI Gateway Settings for Desk-Phone Control on Cisco Unified Presence”)

- Assign desk phone control feature to users

Desk phone control privileges are easily assigned to users by using the CUP GUI interface



Find: static rou Previous Next Options

Cisco Unified Presence Administration
For Cisco Unified Communications Solutions

System Presence Messaging Application User Management Bulk Administration Diagnostics Help

LDAP Host Configuration

Save Delete Copy

Status
Status: Ready

Cisco Unified Personal Communicator
Desk Phone Control
IP Phone Messenger
Meeting Notification
Third-Party Clients
Plugins

Settings
User Assignment

System Presence Messaging Application User Management Bulk Administration Diagnostics Help

Find and List CUP Users

Select All Clear All Assign Selected Users

Status
10 records found

Desk Phone Control Usage
10 Desk phone control users assigned

CUP users (1 - 10 of 10)

Find CUP users where User ID begins with Find Clear Filter

	User ID	Last Name
<input type="checkbox"/>	pmccartney	McCartney
<input type="checkbox"/>	rstarr	Starr
<input type="checkbox"/>	gharrison	Harrison
<input checked="" type="checkbox"/>	jlennon	Lennon
<input type="checkbox"/>	epresley	Presley
<input type="checkbox"/>	lellison	Ellison
<input type="checkbox"/>	jcash	Cash

Desk Phone Control Assignment -- Webpage Dialog
https://172.19.239.99:8443/cupadmin/c Certificate Error

Desk Phone Control Assignment

Desk Phone Control Usage

1 Selected User(s)
☒ Enable Desk Phone Control

Assign Cancel

Internet | Protected Mode: Off



Citrix XenDesktop

To install Citrix XenDesktop you require virtual Windows server 2003 (XenDesktop 4) or Windows server 2008 (XenDesktop 5) for the Connection broker application (Controller). For the HVD images Windows 7 or Windows XP are supported and are installed with Citrix VDA agent. Citrix XenDesktop can be hosted by VMware ESX or ESXi, Citrix XenServer or Windows Hyper-V hypervisor environment. XenDesktop requires an Active Directory. For complete details on XenDesktop installation and configuration see <http://support.citrix.com/proddocs/index.jsp?topic=/xenapp5fp-w2k8/>



Appendix 4 – Netflow and Energywise

Cisco NetFlow provides statistics on packets flowing through network elements (routers and switches) and can be used to monitor traffic utilization. Netflow is supported on the following routing and switching platforms: Cisco ISR and 7200, 10000, 12000, CRS-1 Series Routers; Catalyst4k, Cat6500, and Nexus switches. Refer to the Cisco Virtual Workspace (VXI) Smart Solution CVD for guidelines on implementing Netflow.

Steps to enable Netflow:

1. Configure netflow on the network elements (router and switches)
Set the netflow collector IP address and the netflow export version.
Enable netflow on devices and interfaces
2. Install the netflow collector as the management station.
Provision the netflow collector with IP address and SNMP attributes of Netflow enabled routers and switches
3. Start the netflow collector to begin netflow data collection
4. Run a netflow analyzer report on the collected data

The following configuration implements Netflow Data Export (NDE) on the Catalyst 6504 campus core switch :

```
mls netflow
mls netflow interface
mls flow ip interface-full
mls nde sender
!
interface TenGigabitEthernet1/4
 ip address 10.1.254.45 255.255.255.252
 ip flow ingress
 ip flow egress
!
interface TenGigabitEthernet1/5
 ip address 10.1.254.41 255.255.255.252
 ip flow ingress - enable netflow for inbound traffic
 ip flow egress - enable netflow for outbound traffic
!
ip flow-export version 9 - Netflow format version 9
ip flow-export destination 10.0.128.49 2055 - IP address of the Netflow collector
```

The following sample configuration implements Netflow data export on the 7206VXR campus edge router :

```
interface GigabitEthernet0/3
 ip flow ingress - enable netflow for inbound traffic
!
ip flow-export source GigabitEthernet0/1
ip flow-export version 9 - Netflow format version 9
ip flow-export destination 10.14.1.206 3000 - IP address of the Netflow collector
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
snmp-server ifindex persist
```

Cisco's Energywise Orchestrator can be used to monitor, control, and conserve power consumption on EnergyWise enabled network elements and endpoints. Cisco Virtual Workspace (VXI) Smart Solution desktop virtualization endpoints like thick PC's and thin clients running the Orchestrator Client can be managed directly by the Energywise Orchestrator. The power consumption on DV endpoints like VXC clients (zero clients) that use PoE can also be monitored and controlled by managing the attached port on an Energywise enabled switch. Refer to the Cisco Virtual Workspace (VXI) Smart Solution CVD, for guidelines on implementing Energywise.



Steps for integrating Energywise:

1. Configure EnergyWise on the domain members (router and switches)
 - Set the domain and management password on the domain members connected to the endpoints.
 - Configure energywise attributes on devices and interfaces connected to endpoints
2. Install the Orchestrator client on PC end points
3. Install the Orchestrator server (including the Proxy server) as the management station.
 - Provision the Proxy server with the domain, password, and IP address of the primary domain member
4. Start the Orchestrator server to begin discovery of EnergyWise devices and PCs

Here is a sample configuration that enables Energwise management of the PoE+ ports (connected to VXC clients) on the Catalyst 4500E campus access switch :

```
energywise domain Campus security shared-secret 0 cisco - sets up the domain
energywise importance 70 - set the devices priority
energywise name Campus_switch - sets device identity
energywise keywords Campus_switch - sets device identity
energywise role Campus_switch - sets the device function
energywise management security shared-secret 0 cisco - sets up management communications
!
interface GigabitEthernet0/3
  energywise importance 60 - sets the device priority
  energywise role vxc-client-1 - sets the device function
  energywise keywords Campus.switch2.port0/3 - sets the device locations
  energywise name vxc-client-1 - sets the device identity
```