



Ministry Of Culture Qatar

Low Level Design Document – Network Infrastructure

Version-0.1
Date - 15 Aug. 2010



Table of Contents

<i>Review and Distribution</i>	4
<i>Modification History</i>	4
<i>Audience</i>	5
<i>Scope and Requirements</i>	5
<i>Assumptions</i>	5
<i>Core</i>	8
<i>Access</i>	8
<i>Datacenter</i>	9
<i>Wireless LAN</i>	9
<i>WAN/Internet</i>	10
<i>Security</i>	11
<i>NMS</i>	12
<i>Physical Network Design</i>	13
Physical Components	
3	1
Redundancy and Availability	
4	1
Bandwidth Oversubscription	
4	1
<i>Naming Convention</i>	15
Device Role	
5	1
Iteration	
5	1
Floor numbering	
6	1
Network Device Layout and Port Allocations	
6	1
Domain name	
2	2
<i>Layer 2 design</i>	23
<i>Nexus 7000 virtual Port Channel (vPC)</i>	23
Virtual Device Contexts (VDC)	
3	2
vPC architecture	
4	2
vPC Concepts	
5	2
Interface specific settings	
1	3

Spanning Tree Protocol (STP)	3
1	
UDLD	3
9	
STP Features PIN Summary	4
0	
EtherChannel.....	40
LACP	4
0	
Load-Balancing algorithm	4
1	
<i>VLAN Trunking protocol (VTP)</i>	44
<i>VLAN, Trunks and Access ports</i>	45
<i>Layer 3 Network Design</i>	47
Design Overview	4
7	
Configuring WCCPv2 in Nexus7000	5
2	
<i>Quality of Service</i>	56
Nexus 7000	5
6	
Access Switches	6
2	
<i>Network Device Hardening</i>	66
Operating System Hardening	6
6	

Device Management and controlling device access	7
2	
Control plane protection (CoPP)	8
2	
<i>Internet/Security Infrastructure</i>	90
<i>Internet Segment</i>	90
Detailed Internet Edge Design	9
1	
Traffic Flows	9
2	
Firewall Key Concepts	9
5	
ASA Security Levels	9
7	
ASA Network Address Translation (NAT)	9
8	
Routing	10
3	
Firewall High Availability	10
3	
<i>IronPort E-Mail Security</i>	11
1	
Register the IronPort Appliance in DNS	11
1	
Using the System Setup Wizard	11
2	
<i>IronPort Web Security Appliance</i>	12
3	
Web Proxy	12
3	
Mode of Deployment	12
3	
SYSTEM SETUP WIZARD	12
4	
Proxy Authentication	13
4	
<i>Cisco Secure ACS</i>	13
9	
Initial Configuration of ACS	13
9	

Adding local user account in ACS.	14
2	
Group Setup	14
6	
Network Configuration	14
7	
System Configuration	14
8	
Adding AAA Clients on ACS	14
9	
Configure Remote Agent	15
1	
External Database Configuration	15
5	
Database Group Mapping	15
7	
ACS Configuration for Wireless User Authentication	16
1	
<i>LAN Management Solution</i>	17
2	
<i>WIRELESS INFRASTRUCTURE</i>	17
8	
Wireless Network Requirements	17
8	
Overview of the wireless network	17
8	
NAC Guest Server	18
1	
AP Groups Vlan	18
2	
Detailed Design	18
2	
Controller Configuration	18
6	
ACS Configuration For PEAP Authentication	19
8	
Guest Access	20
2	
WCS (Wireless Control System)	21
7	

DOCUMENT INFORMATION

Author: Engineers, Mannai Cooperation
Change Authority: Mannai Cooperation
Change Forecast: Medium

Review and Distribution

Organization	Name	Title
Mannai Corporation	T. Senthilkumar	Snr. Engineer
Mannai Corporation	Harindha Fernando	Tech. Lead
Mannai Corporation	Riju Thomas	Tech. Lead
Mannai Corporation	Arun Mathew	Snr. Engineer
Mannai Corporation	Anthic Joshep	Engineer
MoC	Abdelmonem Mosehli	
MoC	Mr. Sameh Khedar	

Modification History

Rev	Date	Originator	Status	Comment
0.1	15-Aug-10	Senthilkumar, Arun Mathew, Anthic Joshep	Draft	Initial Version

INTRODUCTION

Audience

This document is intended for use by:

- 1)** Mannai engineering Team
- 2)** MOC IT

Scope and Requirements

The scope of this document will cover the following Infrastructure elements:

- 1)** N7K
- 2)** 3750E-PD
- 3)** ASA5550
- 4)** Iron-Port Mail/Web security
- 5)** LAP1142
- 6)** WLC4404
- 7)** C4948
- 8)** ACS-1120
- 9)** CISCO3845
- 10)** C2960G
- 11)** LMS and WCS

Assumptions

Assumptions made in this document are as follows:

- [1]** This document covers the complete Low Level Design for MOC new tower
- [2]** All the IP addressing plan is done by customer

Network Overview

The objective of MOC network is to provide the following services in a secure manner:

Unified Communications (Voice, Contact-center, Meeting Express, DMS)

Cooperate service access to wired and wireless users

Internet access for wired and wireless users

The IT needs from a Mannai solution perspective are covered using following technologies:

Network

Infrastructure

Wireless

Security

Unified

Communications

Network Management

Logically, the network is divided into various zones; these logical blocks can be described as follows:

The Core Zone consists of Nexus7K configured as a Core block for redundancy and high availability. This zone provides the core connectivity for all the other zones. Co-operate Wireless controller and Web Security devices are connected to this zone.

A WAN zone that provides connectivity with Qtel for Internet access, as well as natting and firewalling capabilities. Additionally Qtel Cooperate VPN provides the connectivity to remote locations.

A DMZ zone wireless access for Guest user and provides mail security

Access Zone that serves as a distribution layer for wired & wireless corporate as well as wireless GUEST access. The access zone provides Cisco3750E-48PD access layer. The wireless access points connect to this zone.

A Data Center Zone that utilizes a pair of Cisco4948 as aggregating DCN devices connecting to the overall MOC network core. The DCN zone has connectivity for NMS cooperate servers

The following table gives the type of users that access the MOC network.

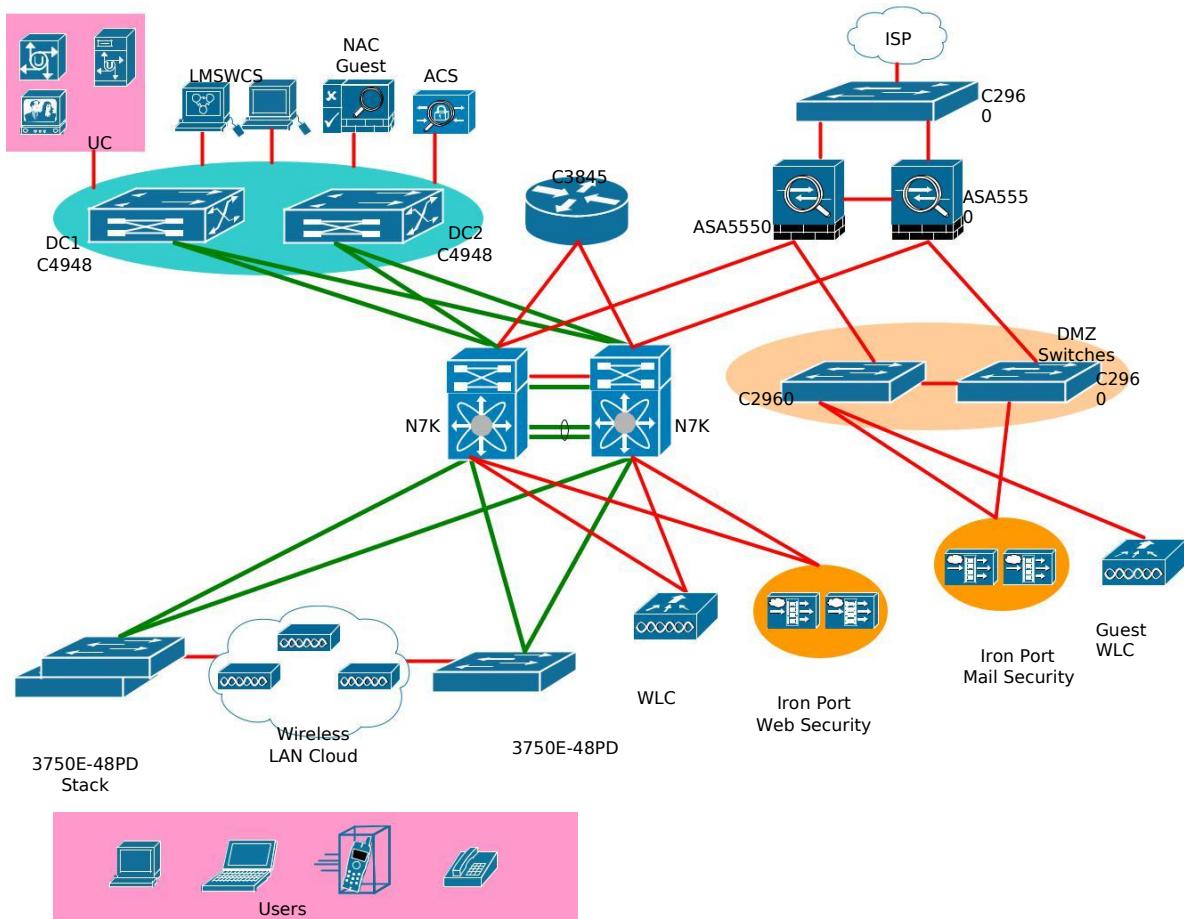
Customer	Connecting Zone	Wired/Wireless
Cooperate User	Access Zone	Wired and Wireless
Guest User	Access Zone	Wireless
Contractor	Access Zone	Wireless

Network Layout

The layout of the network is envisioned for connectivity and high availability. The infrastructure consists of a campus network in a 3 Tier model, Core, Distribution and Access layers. Core and Distribution layers are converged to single hardware.

The following topology represents an overview of the network layout.

Figure 1 MOC Network Topology Overview



The core of the network is the Dual Nexus7K providing connectivity to all the individual zones.

Bill of Material

This section gives the list of network active equipments used in the MOC project.

Core

Product	Description	Quantity
N7K-C7010	10 Slot Chassis, No Power Supplies, Fans Included	2
N7KS1K9-41	Nexus 7000 Release 4.1	2
N7K-LAN1K9	Nexus 7000 LAN Enterprise License (L3 protocols)	2
N7K-M148GT-11	Nexus 7000 - 48 Port 10/100/1000, RJ-45	2
N7K-M132XP-12	Nexus 7000 - 32 Port 10GbE, 80G Fabric (req. SFP+)	2
SFP-10G-SR	10GBASE-SR SFP Module	50
N7K-M132XP-12	Nexus 7000 - 32 Port 10GbE, 80G Fabric (req. SFP+)	2
SFP-10G-SR	10GBASE-SR SFP Module	50
N7K-SUP1	Nexus 7000 - Supervisor, Includes External 8GB Log Flash	2
N7K-CPF-2GB	Nexus Compact Flash Memory 2GB (Expansion Flash - Slot 0)	2
N7K-C7010-FAB-1	Nexus 7000 - 10 Slot Chassis - 46Gbps/Slot Fabric Module	6
N7K-AC-6.0KW	Nexus 7000 - 6.0KW AC Power Supply Module	6
CAB-AC-2500W-INT	Power Cord, 250Vac 16A, INTL	12
N7K-C7010-AFLT	Nexus 7010 Air Filter	2
N7K-C7010-FD-MB	Nexus 7010 Front Door Kit	2
CON-CSSPD-C7010	SHARED SUPP SDS 10 Slot Chassis, No Power Supplies, Fans	6
CON-CSSPD-N7FAB	SHARED SUPP SDS Nexus 7000 - 10 Slot Chassis	18
CON-CSSPD-N7LAN	SHARED SUPP SDS Nexus 7000 LAN Enterprise Lic	6
CON-CSSPD-N732XP	SHARED SUPP SDS Nexus 7000 - 32 Port 10GbE, 80G Fabric	6
CON-CSSPD-N732XP	SHARED SUPP SDS Nexus 7000 - 32 Port 10GbE, 80G Fabric	6
CON-CSSPD-N748G	SHARED SUPP SDS Nexus 7000 - 48 Port 10/100/1000, RJ-45	6
CON-CSSPD-N7SUP1	SHARED SUPP SDS Nexus 7000 - Supervisor, Includes Ext	6
Total	B.Core Switches Nexus 7K	

Access

Product	Description	Quantity
WS-C3750E-48PD-SF	Catalyst 3750E 48 10/100/1000 PoE+2*10GE(X2),1150W,IPB s/w	45
S3750EVT-12235SE	CAT 3750E IOS UNIVERSAL W/O CRYPTO WITH WEB BASED	45
CAB-STACK-50CM	Cisco StackWise 50CM Stacking Cable	45
CAB-ACU	Power Cord UK	45
CVR-X2-SFP	Cisco TwinGig Converter Module	45
CVR-X2-SFP-2	Two (2) Cisco TwinGig Converter Module	45
X2-10GB-SR=	10GBASE-SR X2 Module	90
CON-CSSPD-3750E4PT	SHARED SUPP SDS WS-C3750E-48PD-SF	135
Total	A.48x 10/100/1000 Switches	

Datacenter

Product	Description	Quantity
WS-C4948-10GE-S	Catalyst 4948, IPB s/w, 48*10/100/1000+2*10GE(X2), 1 AC p/s	2
CAB-BS1363-C15-UK	BS-1363 to IEC-C15 8ft UK	4
PWR-C49-300AC/2	Catalyst 4948 300-Watt AC Power Supply Redundant	2
X2-10GB-SR	10GBASE-SR X2 Module	2
PWR-C49-300AC	Catalyst 4948 300-Watt AC Power Supply	2
S49IPB-12246SG	Cisco CAT4900 IOS IP BASE W/O CRYPTO	2
CON-CSSPD-C4948GES	SHARED SUPP SDS 4948, IPB s/w 4810/100/1K 2 10GE	6
Total		

Wireless LAN

Product	Description	Quantity
AIR-LAP1142N-E-K9	802.11a/g/n Fixed Unified AP; Int Ant; ETSI Cfg	90
S114RK9W-12418JA	Cisco 1140 Series IOS WIRELESS LAN LWAPP RECOVERY	90
CON-CSSPD-LAP1142E	SHARED SUPP SDS 802.11a/g/n Fixed Unified AP; ETSI	270
Total	A.Wireless Access Point	

Product	Description	Quantity
AIR-WLC4404-100-K9	4400 Series WLAN Controller for up to 100 Lightweight APs	1
AIR-PWR-CORD-UK	AIR Line Cord United Kingdom	1
SWLC4400K9-52	WLAN Controller SW for 4400 - ED	1
SWLC4400K9-52-ER	WLAN Controller Emergency SW for 4400 - ED	1
CON-CSSPD-WC440410	SHARED SUPP SDS 4404-100 WLAN Controller	3
GLC-T	1000BASE-T SFP	2
Total	B.Wireless Controllers for LAN Segment	

WAN/Internet

Product	Description	Quantity
CISCO3845-HSEC/K9	3845 Bund. w/ AIM-VPN/SSL-3, Adv. IP Serv, 25 SSL lic, 128F/512D	1
PWR-3845-AC-IP	Cisco 3845 AC-IP factory upgrade option power supply	1
PWR-3845-AC-IP/2	Cisco 3845 redundant AC/IP power supply	1
CAB-ACU	Power Cord UK	2
S384AISK9-12415T	Cisco 3845 ADVANCED IP SERVICES	1
MEM3800-256U512D	256 to 512MB DRAM (single DIMM) Factory upgrade for 3800	1
MEM3800-64U128CF	64 to 128 MB CF Factory Upgrade for Cisco 3800 Series	1
AIM-VPN/SSL-3	DES/3DES/AES/SSL VPN Encryption/Compression	1
ROUTER-SDM-CD	CD for SDM software	1
CON-CSSPD-3845HSEC	SHARED SUPP SDS 3845 Security Bundle	3
HWIC-2FE	HWIC two routed port	1
Total	A. Internet VPN Gateway	

Product	Description	Quantity
WS-C2960G-8TC-L	Catalyst 2960 7 10/100/1000 + 1 T/SFP LAN Base	1
CAB-ACU-RA	Power Cord UK, Right Angle	1
CON-CSSPD-C2960G8C	SHARED SUPP SDS Catalyst 2960 7 10/1	3
Total	B. Outside L2 Switch	

Product	Description	Quantity
WS-C2960G-8TC-L	Catalyst 2960 7 10/100/1000 + 1 T/SFP LAN Base	2
CAB-ACU-RA	Power Cord UK, Right Angle	2
CON-CSSPD-C2960G8C	SHARED SUPP SDS Catalyst 2960 7 10/1	6
Total	C. DMZ L2 Switch	

Product	Description	Quantity
ASA5550-K8	ASA 5550 Appliance with SW, HA, 8GE+1FE, DES	2
CAB-ACU	Power Cord UK	2
SF-ASA-8.0-K8	ASA 5500 Series Software v8.0	2
ASA-VPN-CLNT-K9	Cisco VPN Client Software (Windows, Solaris, Linux, Mac)	2
ASA-180W-PWR-AC	ASA 180W AC Power Supply	2
ASA-ANYCONN-CSD-K9	ASA 5500 AnyConnect Client + Cisco Security Desktop Software	2
ASA5500-ENCR-K8	ASA 5500 Base Encryption Level (DES)	2
SSM-4GE-INC	SSM-4GE embedded within ASA 5550 systems	2
CON-CSSPD-AS5550K8	SHARED SUPP SDS ASA5550 w/ SW, HA, 8GE+1FE, DES	6
Total	D. Internet Firewall	

Product	Description	Quantity
AIR-WLC4402-12-K9	4400 Series WLAN Controller for up to 12 Lightweight APs	1
AIR-PWR-CORD-UK	AIR Line Cord United Kingdom	1
SWLC4400K9-52	WLAN Controller SW for 4400 - ED	1
SWLC4400K9-52-ER	WLAN Controller Emergency SW for 4400 - ED	1
CON-CSSPD-WC440212	SHARED SUPP SDS 4402-12 WLAN Controller	3
GLC-T	1000BASE-T SFP	2
Total	E.Wireless DMZ Controller	

Security

Product	Description	Quantity
CSACS-1120-K9	ACS 1120 Appliance.Supports ACS 4.2 and ACS 5.0 SW	1
CSACS-5-BASE-LIC	Cisco Secure ACS 5 Base License	1
CAB-ACU	AC Power Cord (UK), C13, BS 1363, 2.5m	1
CSACS-5.0-SW-K9	Config Option: ACS 5.0 software loaded on 1120	1
CON-CSSPD-CS1120K9	SHARED SUPP SDS Cisco 1120 Secure ACS Appliance with 5.0	3
CON-SAS-CSAS5W9	SW APP SUPP Config Option: ACS	3
Total	A.AAA Server	

Product	Description	Quantity
EBUN-2A-GV-SQRT-3Y-INT	Dual C360, 3 Year IPAS, 3 Year Sophos, 3 Years Virus Outbreak Filters, 3 Years Encryption and 3 Years Platinum Support	1000
WBUN-1A-GV-ABC-3Y	Dual Appliance Bundle.S160, 3 years URL Filtering, 3 Years Anti Virus, 3 Years Anti Malware and 3 Years platinum support	500
Total	B.Email & Web Security	

Product	Description	Quantity
NAC3310-GUEST-K9	NAC Guest Server	1
NAC3310-GUEST	NAC Appliance 3310 Guest Hardware	1
CAB-ACU	AC Power Cord (UK), C13, BS 1363, 2.5m	1
NAC-GUEST-10-K9	NAC Appliance Guest Release 1.0	1
CON-CSSPD-NACGUEST	SHARED SUPP SDS NAC Guest Server	3
Total	C.NAC Guest	

NMS

Product	Description	Quantity
CWLMS-3.1-300-K9	LMS 3.1 Small Enterprise I, networks of 100 to 300 devices	1
CON-SAS-LMS3300	SW APP SUPP LMS3.1 Sm Ent I Ntwrk of 100 to 300 Dev	3
Total	A.LAN Management	

Product	Description	Quantity
WCS-STANDARD-K9	WCS Top Level SKU for AP capacity options.	1
WCS-PLUS-500	Cisco WCS with PLUS License for 500 APs, Windows/Linux	1
CON-SAU-WCSP500	SW APP SUPP + UPGR Cisco WCS with PLUS	3
CON-SAU-WCSSTDK9	SW APP SUPP + UPGR WCS Top Level SKU for AP capacity option	3
Total	B.Wireless Management	

Design Considerations

The objective is to provide a highly available IP network interconnecting various MOC zones and services. The network is targeted to offer services like Wired, wireless, unified communications and internet access. Key factors in design include the ability to provide IP connectivity to all users, have a redundant and fault tolerant network with ability to react to various changes (link failure, node failure etc.) in the network. Network will also provide quality of service as permitted by architecture of the platform being used.

Physical Network Design

Physical Components

Following are the main components used in MOC physical infrastructure:

MOC Core network consists of Nexus7K and following cards for mentioned purpose,

- 1)** N7K-M132XP-12 (Nexus 7000 - 32 Port 10GbE) for connecting Access switches from every floor.
- 2)** N7K-M148GT-11(Nexus 7000 - 48 Port 10/100/1000, RJ-45) – for connecting service appliances

Each floor consists of two IDFs where floor wired users and wireless access points are terminated. Access zone consists of one WS-C3750E-48PD-SF switch per IDF and dual uplinked to Nexus7K core using 10G links.

WAN zone connects the external ip entities. Qtel Internet link is terminated via Cisco 2950-8TC to redundant ASA5550. ASA5550 is configured in active-failover mode. QCB connects to its remote location via Cisco3845 where Qtel cooperative MPLS VPN link is terminated.

DMZ zone hosts Guest WLC and Ironport Mail Security appliance.

MOC Datacenter zone consists of dual Cisco4948 switch uplinked to Core switches. All the MOC application servers, Unified Communication servers, NAC guest, LMS, WCS and ACS servers are connected to DC switches.

Redundancy and Availability

Redundancy and High Availability in MOC network is provided by ensuring the following:

Utilize Redundant Paths in the network and avoid single point of failure. Oversubscription on physical ports is avoided wherever possible

Use routers as redundant pairs in all zones

Use VPC architecture on N7Ks, VPC is discussed in detailed in later sections of this document.

Additionally, protocol level redundancy will be enabled HSRP. Physical redundancy at the router and line card level will be augmented by Quality of Service features to ensure availability of mission critical applications like Voice, Video and Telepresence.

Bandwidth Oversubscription

The ports can be configured on a 10GbE line card (N7K-M132XP-12) such that 10G of bandwidth is dedicated to one port or shared by four ports in the same port group. The two modes are referred to as Dedicated Mode vs. Shared Mode.

When dedicating the bandwidth to one port, other three ports in the same port group goes to disable mode.

Following table depicts the port groups, enabled dedicated ports and disabled ports.

Table 1 Port Groups for dedicated modes on Nexus7000

Port Group	Enabled Interface	Disabled Interfaces
1, 3, 5, 7	1	3, 5, 7
2, 4, 6, 8	2	4, 6, 8
9, 11, 13, 15	9	11, 13, 15
10, 12, 14, 16	10	12, 14, 16
17, 19, 21, 23	17	19, 21, 23
18, 20, 22, 24	18	20, 22 24
25, 27, 29, 31	25	27, 29, 31
26, 28, 30, 32	26	28, 30, 32

To avoid oversubscription wherever we need it is suggested to utilize dedicated ports.

Naming Convention

The following will be used as the naming convention for all devices within the MOC project.

Figure 2 Naming Convention

<device role><iteration>-<floor number>

The following sections further clarify the fields used in the naming convention

Device Role

Table 2 Network devices and its respective roles

Device Role	Abbreviation
Core Switch N7K	cs
Access Switch(3750)	as
Wireless Access Points	wap
Cooperate Wireless Controller	cwc
WAN ASA Firewall	wf
Ironport Mail Security	ims
Ironport Web Security	iws
Guest Wireless Controller	gwc
DMZ switches	dmzs
WAN Switch	ws
WAN router	wr
Datacenter switch	dcs
NAC Guest Controller	ngc
Cisco ACS	acs
LAN Management System	lms
Wireless Control system	wcs

The VoIP phones and Digital Media Players (DMP) do not require names.

Iteration

The following points further explain the iteration numbering:

- The iteration would at a minimum consist of two digits.
- The first unique device on that building floor occupies the number 01 with the second device numbered as 02 etc regardless of zone.
- If it is known there are more than 99 of a particular device then the iteration numbering will begin with 001 with the second device numbered as 002 etc

Floor numbering

Basement and Ground floor will have abbreviation as b and g respectively. The digit representing the other floor is an alphanumeric digit which has a range of the 1 - 21. For example first floor will have abbreviation as 1.

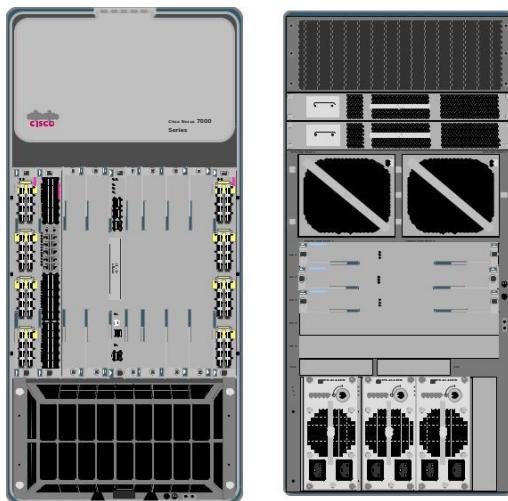
Each floor has two IDF and Datacenter is at 16th floor.

Network Device Layout and Port Allocations

Core router

Following diagram depicts the module used in the Nexus7K.

Figure 3 Nexus7010 front and back view



The line card placement for the Nexus 7K at the MOC is given below:

The single supervisors in the Nexus 7000 switches shall be placed in slots 5 of the chassis.

The 2 x N7K-M132XP-12 (10GbE Modules), shall be placed in slots 1 and 10. Slot 2 shall be occupied by N7K-M142GS-11 (10/100/1000 Module)

Other devices used in MOC project are single units.

Table 3 cs1-16 port connectivity

Device	Local port	Remote port	Link speed	Connected Device	Comments
cs1-16	E1/1	E1/1	10G	cs2-16	Layer2 vPC peer link
	E10/1	E10/1	10G	cs2-16	Layer2 vPC peer link
	E2/1	E2/1	1G	cs2-16	Layer 3, peer keepalive
	E1/9	E1/9	10G	cs2-16	Layer 3, peer keepalive
	E1/10	Tengi1/0/49	10G	as1-g	Downlink to Access sw
	E1/11	Tengi1/0/49	10G	as1-1	Downlink to Access sw
	E1/12	Tengi1/0/49	10G	as1-2	Downlink to Access sw
	E1/13	Tengi1/0/49	10G	as1-3	Downlink to Access sw
	E1/14	Tengi1/0/49	10G	as1-4	Downlink to Access sw
	E1/15	Tengi1/0/49	10G	as1-5	Downlink to Access sw
	E1/16	Tengi1/0/49	10G	as1-6	Downlink to Access sw
	E1/17	Tengi1/0/49	10G	as1-7	Downlink to Access sw
	E1/18	Tengi1/0/49	10G	as1-8	Downlink to Access sw
	E1/19	Tengi1/0/49	10G	as1-9	Downlink to Access sw
	E1/20	Tengi1/0/49	10G	as1-10	Downlink to Access sw
	E1/21	Tengi1/0/49	10G	as1-11	Downlink to Access sw
	E1/22	Tengi1/0/49	10G	as1-12	Downlink to Access sw
	E1/23	Tengi1/0/49	10G	as1-13	Downlink to Access sw
	E1/24	Tengi1/0/49	10G	as1-14	Downlink to Access sw
	E1/25	Tengi1/0/49	10G	as1-15	Downlink to Access sw
	E1/26	Tengi1/0/49	10G	as1-16	Downlink to Access sw
	E1/27	Tengi1/0/49	10G	as1-17	Downlink to Access sw
	E1/28	Tengi1/0/49	10G	as1-18	Downlink to Access sw
	E1/29	Tengi1/0/49	10G	as1-19	Downlink to Access sw
	E1/30	Tengi1/0/49	10G	as1-20	Downlink to Access sw
	E1/31	Tengi1/0/49	10G	as1-21	Downlink to Access sw
	E1/5	G1/49	10G	dcs1-16	To DC switch 1
	E10/10	Tengi1/0/49	10G	as2-g	Downlink to Access sw
	E10/11	Tengi1/0/49	10G	as2-1	Downlink to Access sw
	E10/12	Tengi1/0/49	10G	as2-2	Downlink to Access sw
	E10/13	Tengi1/0/49	10G	as2-3	Downlink to Access sw
	E10/14	Tengi1/0/49	10G	as2-4	Downlink to Access sw
	E10/15	Tengi1/0/49	10G	as2-5	Downlink to Access sw
	E10/16	Tengi1/0/49	10G	as2-6	Downlink to Access sw
	E10/17	Tengi1/0/49	10G	as2-7	Downlink to Access sw
	E10/18	Tengi1/0/49	10G	as2-8	Downlink to Access sw
	E10/19	Tengi1/0/49	10G	as2-9	Downlink to Access sw
	E10/20	Tengi1/0/49	10G	as2-10	Downlink to Access sw
	E10/21	Tengi1/0/49	10G	as2-11	Downlink to Access sw

MOC Low Level Design

E10/22	Tengi1/0/49	10G	as2-12	Downlink to Access sw
E10/23	Tengi1/0/49	10G	as2-13	Downlink to Access sw
E10/24	Tengi1/0/49	10G	as2-14	Downlink to Access sw
E10/25	Tengi1/0/49	10G	as2-15	Downlink to Access sw
E10/26	Tengi1/0/49	10G	as2-16	Downlink to Access sw
E10/27	Tengi1/0/49	10G	as2-17	Downlink to Access sw
E10/28	Tengi1/0/49	10G	as2-18	Downlink to Access sw
E10/29	Tengi1/0/49	10G	as2-19	Downlink to Access sw
E10/30	Tengi1/0/49	10G	as2-20	Downlink to Access sw
E10/31	Tengi1/0/49	10G	as2-21	Downlink to Access sw
E10/5	Gi1/49	10G	dcs2-16	To DC switch 2
E2/2	F0/0	1G	wrl-16	To WAN router 3845
E2/3	Port1	1G	cwc1-16	To Co-WC
E2/4	Port1	1G	iws1-16	To Ironport web app
E2/5	Gi0/0	1G	wf1-16	To WAN ASA firewall1

Table 4 cs2-16 port connectivity

Device	Local port	Remote port	Link speed	Connected Device	Comments
cs2-16	E1/1	E1/1	10G	cs1-16	Layer2 vPC peer link
	E10/1	E10/1	10G	cs1-16	Layer2 vPC peer link
	E2/1	E2/1	1G	cs1-16	Layer 3, peer keepalive
	E1/9	E1/9	10G	cs1-16	Layer 3, peer keepalive
	E1/10	Tengi1/0/50	10G	as1-g	Downlink to Access sw
	E1/11	Tengi1/0/50	10G	as1-1	Downlink to Access sw
	E1/12	Tengi1/0/50	10G	as1-2	Downlink to Access sw
	E1/13	Tengi1/0/50	10G	as1-3	Downlink to Access sw
	E1/14	Tengi1/0/50	10G	as1-4	Downlink to Access sw

E1/15	Tengi1/0/50	10G	as1-5	Downlink to Access sw
E1/16	Tengi1/0/50	10G	as1-6	Downlink to Access sw
E1/17	Tengi1/0/50	10G	as1-7	Downlink to Access sw
E1/18	Tengi1/0/50	10G	as1-8	Downlink to Access sw
E1/19	Tengi1/0/50	10G	as1-9	Downlink to Access sw
E1/20	Tengi1/0/50	10G	as1-10	Downlink to Access sw
E1/21	Tengi1/0/50	10G	as1-11	Downlink to Access sw
E1/22	Tengi1/0/50	10G	as1-12	Downlink to Access sw
E1/23	Tengi1/0/50	10G	as1-13	Downlink to Access sw
E1/24	Tengi1/0/50	10G	as1-14	Downlink to Access sw
E1/25	Tengi1/0/50	10G	as1-15	Downlink to Access sw
E1/26	Tengi1/0/50	10G	as1-16	Downlink to Access sw
E1/27	Tengi1/0/50	10G	as1-17	Downlink to Access sw
E1/28	Tengi1/0/50	10G	as1-18	Downlink to Access sw
E1/29	Tengi1/0/50	10G	as1-19	Downlink to Access sw

MOC Low Level Design

E1/30	Tengi1/0/50	10G	as1-20	Downlink to Access sw
E1/31	Tengi1/0/50	10G	as1-21	Downlink to Access sw
E1/5	Gi1/50	10G	dcs1-16	To DC switch 1
E10/10	Tengi1/0/50	10G	as2-g	Downlink to Access sw
E10/11	Tengi1/0/50	10G	as2-1	Downlink to Access sw
E10/12	Tengi1/0/50	10G	as2-2	Downlink to Access sw
E10/13	Tengi1/0/50	10G	as2-3	Downlink to Access sw
E10/14	Tengi1/0/50	10G	as2-4	Downlink to Access sw
E10/15	Tengi1/0/50	10G	as2-5	Downlink to Access sw
E10/16	Tengi1/0/50	10G	as2-6	Downlink to Access sw
E10/17	Tengi1/0/50	10G	as2-7	Downlink to Access sw
E10/18	Tengi1/0/50	10G	as2-8	Downlink to Access sw
E10/19	Tengi1/0/50	10G	as2-9	Downlink to Access sw
E10/20	Tengi1/0/50	10G	as2-10	Downlink to Access sw
E10/21	Tengi1/0/50	10G	as2-11	Downlink to Access sw
E10/22	Tengi1/0/50	10G	as2-12	Downlink to Access sw
E10/23	Tengi1/0/50	10G	as2-13	Downlink to Access sw
E10/24	Tengi1/0/50	10G	as2-14	Downlink to Access sw
E10/25	Tengi1/0/50	10G	as2-15	Downlink to Access sw
E10/26	Tengi1/0/50	10G	as2-16	Downlink to Access sw
E10/27	Tengi1/0/50	10G	as2-17	Downlink to Access sw
E10/28	Tengi1/0/50	10G	as2-18	Downlink to Access sw
E10/29	Tengi1/0/50	10G	as2-19	Downlink to Access sw
E10/30	Tengi1/0/50	10G	as2-20	Downlink to Access sw
E10/31	Tengi1/0/50	10G	as2-21	Downlink to Access sw
E10/5	Gi1/50	10G	dcs2-16	To DC switch 2
E2/2	F1/0/0	1G	wrl-16	To WAN router 3845
E2/3	Port2	1G	cwc1-16	To Co-WC
E2/4	Port1	1G	iws2-16	To Ironport web app
E2/5	Gi0/0	1G	wf2-16	To WAN ASA firewall2

Table 5 as1-g port connectivity

Device	Local port	Remote port	Link speed	Connected Device	Comments
as1-g	Tengig1/0/49	E1/10	10G	cs1-16	Uplink to Core
	Tengig1/0/50	E1/10	10G	cs2-16	Uplink to Core

Table 6 as2-g port connectivity

Device	Local port	Remote port	Link speed	Connected Device	Comments
as2-g	Tengig1/0/49	E10/10	10G	cs1-16	Uplink to Core
	Tengig1/0/50	E10/10	10G	cs2-16	Uplink to Core

Table 7 as1-x port connectivity

Device	Local port	Remote port	Link speed	Connected Device	Comments
as1-x	Tengig1/0/49	E1/10+x	10G	cs1-16	Uplink to Core
	Tengig1/0/50	E1/10+x	10G	cs2-16	Uplink to Core

Where x = 1-21

Table 8 as2-x port connectivity

Device	Local port	Remote port	Link speed	Connected Device	Comments
as2-x	Tengig1/0/49	E10/10+x	10G	cs1-16	Uplink to Core
	Tengig1/0/50	E10/10+x	10G	cs2-16	Uplink to Core

Where x = 1-21

Table 9 cwc1-16 port connectivity

Device	Local port	Remote port	Link speed	Connected Device	Comments
cwc1-16	Port1	E2/3	1G	cs1-16	Uplink to Core
	Port2	E2/3	1G	cs2-16	Uplink to Core

Table 10 iws1-16 port connectivity

Device	Local port	Remote port	Link speed	Connected Device	Comments
iws1-16	Port1	E2/4	1G	cs1-16	Uplink to Core

Table 11 iws2-16 port connectivity

Device	Local port	Remote port	Link speed	Connected Device	Comments
iws2-16	Port1	E2/4	1G	cs2-16	Uplink to Core

Table 12 ims1-16 port connectivity

Device	Local port	Remote port	Link speed	Connected Device	Comments
ims1-16	Port1	Gi0/3	1G	dmzs1-16	To DMZ switch

Table 13 ims2-16 port connectivity

Device	Local port	Remote port	Link speed	Connected Device	Comments
ims2-16	Port1	Gi0/3	1G	dmzs2-16	To DMZ switch

Table 14 gwcl1-16 port connectivity

Device	Local port	Remote port	Link speed	Connected Device	Comments
gwcl1-16	Port1	GO/2	1G	dmzs1-16	To DMZ switch

Table 15 dmzs1-16 port connectivity

Device	Local port	Remote port	Link speed	Connected Device	Comments
dmzs1-16	Gi0/1	Gi0/1	1G	wf1-16	To WAN ASA FW1
	Gi0/2	Port1	1G	gwcl1-16	To Guest WLC
	GO/3	Port1	1G	ims1-16	Ironport Mail Sec

Table 16 dmzs2-16 port connectivity

Device	Local port	Remote port	Link speed	Connected Device	Comments
dmzs2-16	Gi0/1	Gi0/1	1G	wf2-16	To WAN ASA FW1
	GO/3	Port1	1G	ims2-16	Ironport Mail Sec

Table 17 wf1-16 port connectivity

Device	Local port	Remote port	Link speed	Connected Device	Comments
wf1-16	Gi0/0	E2/5	1G	cs1-16	To Core switch1
	GO/1	Gi0/1	1G	dmzs1-16	To DMZ switch1
	GO/2	Gi0/1	1G	ws1-16	To WAN switch
	GO/3	GO/3	1G	wf2-16	To ASA FW2

Table 18 wf2-16 port connectivity

Device	Local port	Remote port	Link speed	Connected Device	Comments
wf2-16	Gi0/0	E2/5	1G	cs2-16	To Core switch 2
	Go/1	Gi0/1	1G	dmzs2-16	To DMZ switch2
	Go/2	Gi0/2	1G	ws1-16	To WAN switch
	Go/3	Gi0/3	1G	wf1-16	To ASA FW1

Table 19 ws1-16 port connectivity

Device	Local port	Remote port	Link speed	Connected Device	Comments
ws1-16	Gi0/1	Gi0/1	1G	wf1-16	To WAN ASA FW 1
	Go/2	Gi0/1	1G	wf2-16	To WAN ASA FW 2
	Go/3				To Qtel Internet link

Table 20 wr1-16 port connectivity

Device	Local port	Remote port	Link speed	Connected Device	Comments
wr1-16	F0/0	E2/2	1G	cs1-16	To Core switch
	F1/0/0	E2/2	1G	cs2-16	To core switch

Table 21 dcs1-16 port connectivity

Device	Local port	Remote port	Link speed	Connected Device	Comments
dcs1-16	Gi1/49	E1/5	1G	cs1-16	To Core switch
	Gi1/50	E1/5	1G	cs2-16	To core switch

Table 22 dcs2-16 port connectivity

Device	Local port	Remote port	Link speed	Connected Device	Comments
dcs2-16	Gi1/49	E10/5	1G	cs1-16	To Core switch
	Gi1/50	E10/5	1G	cs2-16	To core switch

Domain name

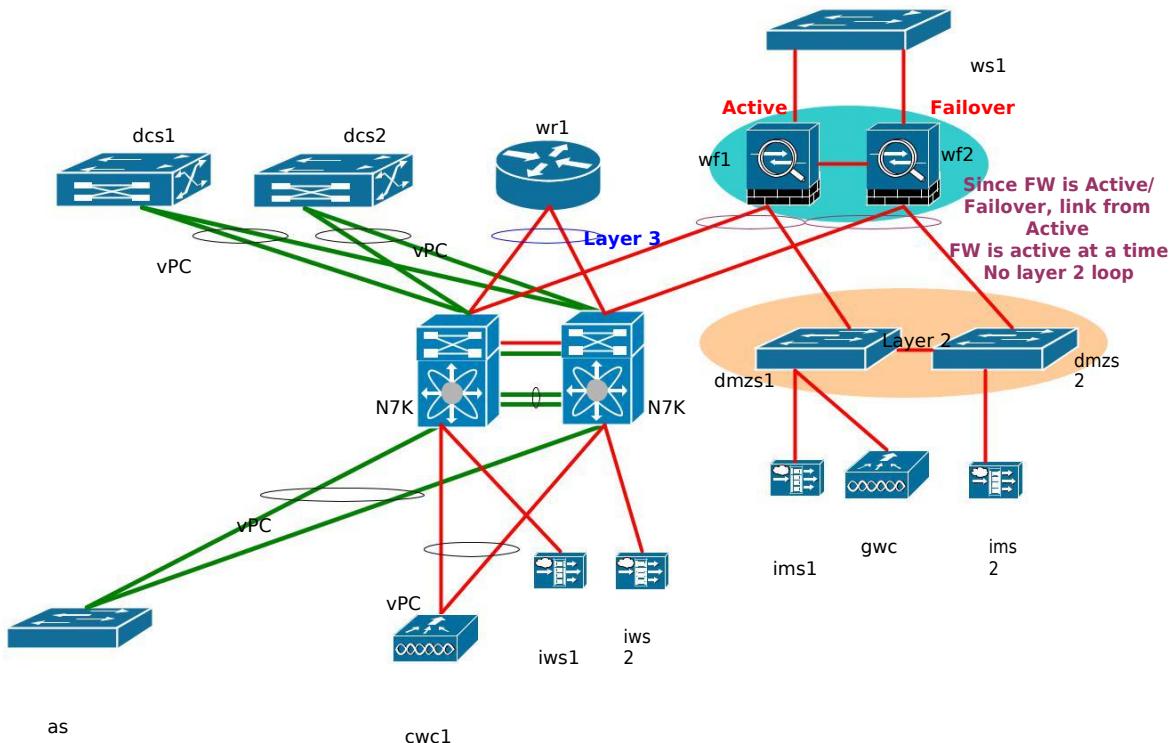
MOC domain name is moc.gov.qa.

Logical Network Design

Layer 2 design

The layer 2 topology for the MOC network is broadly based on the vPC technology, which is aimed at providing a more efficient utilization of the available ports, by eliminating the STP blocked interfaces. This will allow the infrastructure to use all available uplink interfaces and bandwidth between the various network tiers.

Figure 4 Layer 2 logical design



Nexus 7000 virtual Port Channel (vPC)

Virtual Device Contexts (VDC)

Cisco Nexus 7000 Series switches can be segmented into virtual devices based on business need. VDCs deliver true segmentation of network traffic, context-level fault isolation, and management through the creation of independent hardware and software partitions. Each VDC appears as a unique device to the connected users. A VDC runs as a separate logical entity within the physical device, maintains its own unique set of running software processes, has its own configuration, and can be managed by a separate administrator.

The physical device N7K always has one VDC, the default VDC (VDC 1). When you first log in to a new NX-OS device, you begin in the default VDC.

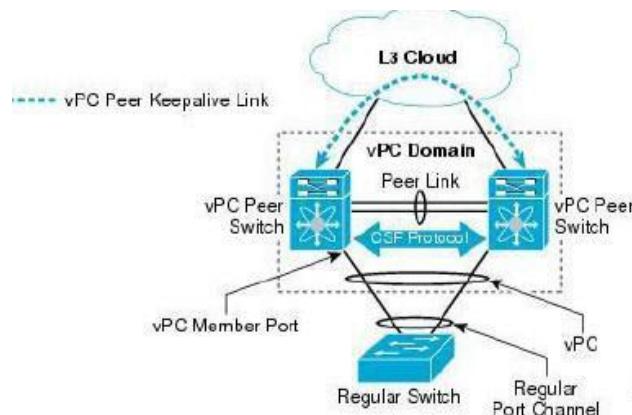
You must be in the default VDC to create, change attributes for, or delete a nondefault VDC. The NX-OS software can support up to four VDCs, including the default VDC, which means that you can create up to three VDCs.

MOC network does not require VDC separation and will be configured on default VDC.

vPC architecture

A virtual port channel (vPC) allows links that are physically connected to two different Cisco Nexus 7000 Series devices to appear as a single port channel by a third device as shown in the figure below. The third device can be a switch, server, or any other networking device. A vPC can provide Layer 2 multipathing, which allows you to create redundancy by increasing bisectional bandwidth by enabling multiple parallel paths between nodes and load balancing traffic where alternative paths exist.

Figure 5 vPC concepts and components



You can use only Layer 2 port channels in the vPC. A vPC domain is associated to a single VDC, so all vPC interfaces belonging to a given vPC domain must be defined in the same VDC. You must have a separate vPC peer-link and peer-keepalive link infrastructure for each VDC deployed. Consolidating a vPC pair (two vPC peer devices of the same domain) in two VDCs of the same physical device is not supported. The vPC peer link must use 10-Gigabit Ethernet ports for both ends of the link or the link will not form.

Cisco recommends that configure the vPC peer links on dedicated ports of different N7K-M132XP-12 modules to reduce the possibility of a failure. Configuring all the vPC peer links and core-facing interfaces on a single N7K-M132XP-12 module may

introduce a single point of failure in your network. For the best resiliency scenario, use at least two N7K-M132XP-12 modules.

vPC Concepts

Virtual Port Channel Domain

A vPC domain is group of two vPC peers switches running vPC so that they can build a L2 loop-free topology and provide multipathing. The domain has a unique identifier from 1 to 1000.

The vPC peer devices use the vPC domain ID that you configure to automatically assign a unique vPC system MAC address. Each vPC domain has a unique MAC address that is used as a unique identifier for the specific vPC-related operations, although the devices use the vPC system MAC addresses only for link-scope operations, such as LACP. We recommend that you create each vPC domain within the contiguous Layer 2 network with a unique domain ID. You can also configure a specific MAC address for the vPC domain, rather than having the Cisco NX-OS software assign the address.

As shown below, first enable the vPC feature, then will be able enter vPC domain mode.

Figure 6 configuring vPC domain

```
feature vpc  
vpc domain domain-id  
    system-priority priority  
    role priority priority
```

Virtual Port Channel Peer Switches

The two switches that are aggregated by the vPC feature as the end of a distributed channel. Only two switches can be part of this peer relationship.

Virtual Port Channel Peer Link

This is the link between the vPC peer switches. The whole architecture relies heavily on the availability of this link, so it is recommended to configure it as a port channel with members spread across different line cards. That aside, the peer link is just a regular interface with the ability to tag packets as having originated on the local peer.

When configuring the vPC peer link, the vPC peer devices negotiate that one of the connected devices is the primary device and the other connected device is the secondary device. It is recommended to manually configure the primary and secondary role by changing the default priority of 32767 coded on 16 bits integer to a lower value for the primary (lowest priority wins). The Cisco NX-OS software uses the lowest MAC address to elect the primary device. Beware that changing the priority of the vPC peer devices can cause the interfaces in your network to go up and down. Some feature, like STP root, HSRP should be consistent with the vPC role priority.

You must ensure that the two devices connected by the vPC peer link have certain identical operational and configuration parameters. The following command is useful to check them:

show vpc consistency-parameters {global | interface port-channel channel-number}

To configure a port-channel, first apply the same configuration steps of a classical L2 port-channel and declare it as a vPC peer-link.

Figure 7 Configuring vPC Peer link

```
vpc domain domain-id
system-priority priority
role priority priority

interface port-channel channel-number
vpc peer-link
```

Virtual Port Channel Peer Keepalive Link

When the vPC peer link is down, it is important to differentiate between the failure of the vPC peer link alone and the failure of the directly attached vPC peer as a whole. The peer-keepalive link allows the vPC peers to exchange heartbeat messages without using the peer-link. This mechanism is critical to prevent dual-active scenarios in case of peer-link failure.

Cisco recommends that the peer-link to be on a dedicated link on Layer 3 dense networks. Since MOC network has small layer 3 part, the keepalive link will go over the back-to-back layer 3 links between N7K.

Figure 8 vPC peer link configuration

```

vrf context peer-link-name
    interface type slot/port
    vrf member peer-link-name
    ip address address/mask

vpc domain domain-id
    peer-keepalive      destination      ipaddress
                        [hold-timeout   secs      | interval
                         msecs]
    {timeout secs} | {precedence {prec-value | network | internet | critical | flash-
override | flash | immediate | priority | routine}} | {tos {tos-value | max-
reliability | max-throughput | min-delay | min-monetary-cost | normal}} |
    tos-byte tos-byte-value} | source ipaddress | udp-port number | vrf {name |
    management | vpc-keepalive}]

```

Virtual Port Channel (vPC)

A vPC is port channel with at least one end distributed across two vPC peer switches.

To connect to the downstream device, you create a port channel from the downstream device to the primary vPC peer device and you create another port channel from the downstream device to the secondary peer device. Finally, working on each vPC peer device, you assign a vPC number (between 1 and 4096) to the port channel that connects to the downstream device with the following command:

Figure 9 Assigning vPC Member

```

interface port-channel channel-number
    vpc number

```

A good practice is to use the same id for port-channel-id and vpc number.

Always double attach devices to vPC system to avoid isolation in case of vPC peer-link failure and optimize traffic flows though the vPC system. In case of vPC failure, all vPC ports on vPC standby will be shutdown isolating single attached devices.

Virtual Port Channel Member Port

A vPC member port is a physical port on a vPC member that is associated to a vPC.

Cisco Fabric Services (CFS) Protocol

The CFS protocol is a reliable messaging protocol designed to support rapid stateful configuration message passing and synchronization. The vPC uses CFS to transfer a copy of the system configuration for a comparison process, and to synchronize protocol state information between the two vPC peer switches.

CFS is transported directly over Ethernet using the native VLAN of the peer link. Therefore, the native VLAN on the peer link should be dedicated.

vPC Interaction with Other Features

vPC and LACP

LACP uses the system MAC address of the vPC domain to form the LACP Aggregation Group (LAG) ID for the vPC.

You can use LACP on all the vPC port channels, including those channels from the downstream device. We recommend that you configure LACP with active mode on the interfaces on each port channel on the vPC peer devices. This configuration allows you to more easily detect compatibility between devices, unidirectional links, and multihop connection, and provides dynamic reaction to run-time changes and link failures.

We recommend that manually configure the system priority on the vPC peer-link devices to ensure that the vPC peer-link devices have a higher LACP priority than the downstream connected devices. A lower numerical value system priority means a higher LACP priority. These values must be the same on each VPC peers otherwise the vPC will not come up.

Figure 10 Configuring System Priority on vPC Peer-Link

```
vpc domain domain-id
system-priority priority
```

vPC Peer Links and STP

STP is distributed; that is, the protocol continues running on both vPC peer devices. However, the configuration on the vPC peer device elected as the primary device controls the STP process for the vPC interfaces on the secondary vPC peer device.

Cisco recommends that you configure the primary vPC peer device as the highest STP root priority, and configure the secondary device with a lower root priority.

If the primary vPC peer device fails over to the secondary vPC peer device, there is no change in the STP topology.

Configure both ends of vPC peer link with the identical STP configuration for the following parameters:

STP global settings:

STP mode

STP region configuration for MST

Enable/disable state per VLAN

Bridge Assurance setting

Port type setting—It is recommended that you set all vPC peer link ports as network ports.

Loop Guard
settings STP interface
settings:

Port type setting

Loop Guard

Root Guard

vPC Multicast—PIM, IGMP, and IGMP Snooping

The software keeps the multicast forwarding state synchronized on both of the vPC peer devices. The IGMP snooping process on a vPC peer device shares the learned Group information with the other vPC peer device through the vPC peer link; the multicast states are always synchronized on both vPC peer devices. The PIM process in vPC mode ensures that only one of the vPC peer devices forwards the multicast traffic to the receivers.

vPC Peer Links and Routing

The First Hop Redundancy Protocols (FHRP) interoperate with vPCs. The Hot Standby Routing Protocol (HSRP), Gateway Load Balancing Protocol (GLBP), and Virtual Router Redundancy Protocol (VRRP) all interoperate with vPCs. The primary FHRP device responds to ARP requests, even though the secondary vPC device forwards the data traffic. In the case of HSRP, the improvement was made to the forwarding engine specifically to allow local Layer 3 forwarding at both the "active" HSRP peer and at the "standby" HSRP peer. This provides in effect an Active/Active HSRP configuration with no changes to current HSRP configuration recommendations or best practices and no changes to the HSRP protocol either. The HSRP control protocol still acts like an Active/Standby pair, such that only the active device responds to ARP requests, but a packet destined to the shared HSRP MAC address is accepted as local on either the active or standby HSRP device.

To simplify initial configuration verification and vPC/HSRP troubleshooting, configure the primary vPC peer device with the FHRP active router highest priority. Aggressive timers are recommended to achieve better convergence. The timer values can be 300 ms for Hellos and 900 ms for Hold Interval.

CFSoE

The Cisco Fabric Services over Ethernet (CFSoE) is a reliable state transport mechanism that is used to synchronize the actions of the vPC peer devices. CFSoE carries messages and packets for many features linked with vPC, such as STP and ICMP. Information is carried in CFS/CFSoE protocol data units (PDUs).

When enable the vPC feature, the device automatically enables CFSoE, and you do not have to configure anything. CFSoE distributions for vPCs do not need the capabilities to distribute over IP or the CFS regions. No need to configure anything for the CFSoE feature to work correctly on vPCs.

vPC failure recovery

Member port failure is perhaps the most likely scenario, where a member port from an adjacent access switch has a failure. When the vPC peer determines that a member port has failed (and there are no other local member-ports for that vPC), the peer with the failed vPC member port notifies the remote peer of the fact that it no longer has an active member port for a configured vPC. The remote peer will then enable forwarding on that vPC for packets that traverse the peer-link. This mechanism assures reachability, and at the same time provides loop management.

In the highly unlikely case that both ports and line cards in the peer-link fail (being that two ports on two different line cards are the recommended minimum for the peer-link) or if the CFS messaging infrastructure fails to communicate across the peer-link, the vPC management system will look to the peer-keepalive interface to determine if the failure is a link level failure or if in fact the remote peer has failed entirely. In the case that the remote peer is still alive (peer-keepalive messages are still being received), the vPC secondary switch will disable its vPC member ports and any Layer 3 interfaces attached to a vPC associated VLAN. If the peer-keepalive messages are not being received, then the peer continues to forward traffic as it is then assuming that it is the last device available in the network. In either case, on recovery of the peer-link, or re-establishment of CFS message forwarding, the systems will re-synchronize any MAC addresses learned while communications was disrupted, and the system will continue forwarding normally.

In this last case of failure, the access switch receives BPDU from both vPC systems carrying different inconsistent information which trigger a

protection consisting in disabling the port-channel. To avoid this behavior on IOS platform (disabled by default on NX-OS), disable the check:

Figure 11 Disabling Guard Check

```
no spanning-tree etherchannel guard misconfig
```

Interface specific settings

L2/L3 interfaces

By default, all interfaces on Nexus 7000 are L3. To change the default interface mode for the system from Layer 3 routing to Layer 2 switching use the system default switchport command. To return the system to Layer 3 routing default interface mode, use the no form of this command.

Figure 12 Changing Default Interface Mode to L2

```
System default switchport [switchport]
```

You can configure a L2 interface into a L3 interface using,

Figure 13 Configuring L3 Port

```
interface Ethernet [slot/port | port-channel id]
```

```
no switchport
```

For MOC network all the interfaces should be kept as Layer 2 default.

Link Debounce

The debounce timer delays notification of a link change, which can decrease traffic loss due to network reconfiguration. You can configure the debounce timer separately for each Ethernet port and specify the delay time in milliseconds. By default, this parameter is set for 100 milliseconds.

To accelerate propagation of loss and improve convergence time, debounce timer should be configured to 1ms between Nexus 7000 and other Nexus 7000. All other link remains at default value.

Figure 14 link debounce

```
Link debounce time milliseconds
```

Spanning Tree Protocol (STP)

STP mode selection

Although the universal use of vPC throughout the network means there is no requirement for STP to block redundant links, it is still however recommended practice to enable it in a deterministic fashion. Still we need to have STP between DMZ switches.

A robust, reliable network needs to transfer traffic efficiently, providing redundancy and recovering quickly from faults. In a Layer 2 network, where routing protocols are not available, Spanning Tree protocol offers redundant connections and eliminates the danger of data traffic loops by building a loop-free logical forwarding topology from a meshed physical topology.

The Spanning Tree Protocol, as originally specified in the IEEE 802.1D standard, typically recovers a link failure within 50 seconds [convergence time = $(2 \times \text{Forward_Delay}) + \text{Max_Age}$]. While such outage may be adequate for data applications, currently many mission-critical applications require faster network convergence and address scalability limitations related to Spanning Tree and Vlan interaction, the IEEE committee developed two new standards, Rapid Spanning-Tree Protocol (RSTP) defined in IEEE 802.1w and Multiple Spanning-Tree Protocol (MST) defined in IEEE 802.1s.

There are a number of Spanning Tree protocols, and it is important to understand the differences of each, before making a choice as to which one is most appropriate. They are listed here:

Common Spanning-Tree (CST) assumes one spanning-tree instance for the entire bridged network, regardless of the number of VLANs. This implementation reduces CPU load since only one Spanning Tree instance is maintained for the entire network. This implementation can be used when only one Layer 2 topology is needed in the network.

Per-VLAN Spanning Tree (PVST) maintains a Spanning Tree instance for each VLAN configured in the network. It uses ISL Trunking and allows a VLAN trunk to be forwarding for some VLANs while blocking for other VLANs. Since PVST treats each VLAN as a separate network, it has the ability to load balance traffic (at layer-2) by forwarding some VLANs on one trunk and other VLANs on another trunk without causing a Spanning Tree loop.

Per VLAN Spanning Tree Plus (PVST+) provides the same functionality as PVST using 802.1Q trunking technology rather than ISL. PVST+ is an enhancement to the 802.1Q specification and is not supported on non-Cisco devices.

Rapid Spanning Tree Protocol (RSTP) / 802.1w is an evolution of the Spanning Tree Protocol (802.1D standard) and provides for faster Spanning

Tree convergence after a topology change, by relying on an active bridge-to-bridge handshake mechanism rather than depending on network-wide timers specified by the root bridge. The standard also includes features equivalent to Cisco PortFast, UplinkFast and BackboneFast for faster network reconvergence.

Rapid Per Vlan Spanning Tree Plus (RPVST+) uses the existing configuration for PVST+ and improves it by using rapid convergence based on the IEEE 802.1w standard. In RPVST+ mode, each Vlan runs its own spanning tree instance up to the maximum supported on the platform.

Multiple Spanning Tree (MST) / 802.1s is an IEEE standard inspired from the Cisco proprietary Multiple Instances Spanning Tree Protocol (MISTP) implementation which allows several VLANs to be mapped to a reduced number of spanning-tree instances. This is possible since most networks do not need more than a few logical topologies. Each instance handles multiple VLANs that have the same Layer 2 topology.

The two main choices in today's networks are RPVST+ and MST

The advantages of MST over Rapid-PVST are as follows:

MST is an IEEE standard.

MST is more resource efficient. In particular, the number of BPDUs transmitted by MST does not depend on number of VLANs, as in Rapid-PVST.

Fault isolation (when regions are defined).

The advantages of Rapid-PVST over MST are as follows:

MST introduces some administrative overhead: a consistent configuration has to be strictly enforced across the domain in order to benefit from the load balancing.

MST does not interact seamlessly with service appliances/service modules in transparent mode.

Easier interoperability with PVST domain as interconnection between MST and PVST requires bridge root to be placed inside the MST domain.

The default mode of NX-OS and IOS is Rapid-PVST, thus configuration command is not required.

Pathcost Method

The STP BPDUs carry a 32-bit field representing the cost to reach the root bridge. The initial implementation of STP, however, was only using 16 bits out of those 32 available, allowing a cost in the range of 0 to 65535. The spanning tree privilege links

with the least cost to the root bridge, it is incremented by the cost of the links traversed on the path to the root. By default, the cost is tied to the bandwidth of a link. Encoded over 16-bit, the cost was not granular enough for modern networks and IEEE decided to update the protocol so that it takes full advantage of the 32 bits reserved for the cost in the BPDU.

It is recommended to use pathcost method long in the STP domain.

Figure 15 Configuring Spanning Tree Pathcost Method Long

```
spanning-tree pathcost method long
```

Root Priority & STP Topology

Spanning Tree Protocol will compute a topology centered on the root bridge, meaning that the ports that are kept forwarding in the final topology are the ones with the best path (evaluated with a metric depending on the bandwidth) to the root bridge. In the data center, Layer 2 is used for its flexibility and mainly bridges frames for Layer 3 traffic between some hosts and their default gateway. Locating the root bridge as close as possible to this default gateway is enough to get STP to compute the optimal topology for the network in a single command.

The root bridge is the bridge with the smallest bridge ID in the network. The most significant 16 bits of the bridge ID can be set using the priority command. The last 48 bits of the bridge ID are MAC address from the switch chassis, so that a root bridge can always be elected in a deterministic way, even in the case when the best priority in the network is configured on several bridges. By locating the bridge with the second best priority in the network very close to the root bridge, the failure of the root bridge will have minimal impact on the overall network topology.

The default priority is set to 32768 on NX-OS/IOS and can be modified by using one of two available methods:

- Manually configuring the priority
- Using the macro available for setting the priority

Figure 16 Configuring STP Root Priority - Manual Method

```
spanning-tree vlan vlan-range priority value
```


Figure 17 Configuring STP Root Priority - Macro

```
spanning-tree vlan vlan-range root primary [diameter dia [hello-time hello-time]]
```

```
spanning-tree vlan vlan-range root secondary [diameter dia [hello-time hello-time]]
```

Extended system-ID

Strictly speaking required only when high numerical Vlan id_s are used. For switches configured with extended system-id running Rapid PVST+ the Vlan id_s are carried inside the BPDU and for that to be supported the amount of bits (16) providing the bridge priority value is decreased to 4 and 12 additional bits are now freed up to determine the Vlanid.

Extended system-id is enabled by default on NX-OS/IOS.

Bridge Assurance

Bridge Assurance (BA) is used to protect against problems that can cause bridging loops in the network. Specifically, to protect against a unidirectional link failure or other software failures that can erroneously instruct a device to forward data traffic on a link that should have been blocked by spanning-tree under normal switch operations. With BA enabled all interfaces including STP blocked ports send and receive BPDUs to ensure bi-directional communication of BPDUs on all the links.

Bridge Assurance is globally enabled by default in NX-OS. This feature is not available

Figure 18 Enabling Bridge Assurance Globally

```
spanning-tree bridge assurance
```

Figure 19 Enabling Bridge Assurance on Interface Level

```
spanning-tree port type network
```

In spanning-tree protocol —fail-open mean if a bridge stop sending BPDUs, the receiving port can transition from blocking to forwarding and can cause loops in the network. With Bridge Assurance enabled BPDUs would be sent on all the BA enabled bridge-to-bridge ports, not just the designated ports. If BPDUs are not received on BA enabled bridge-to-bridge port then the port would be blocked.

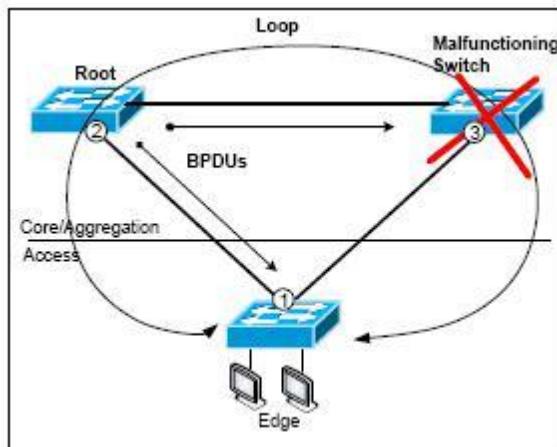
Bridge assurance is enabled globally by default. The feature will become operational only on network ports that are configured as type network. For

BA feature to function properly, both ends of the link must have BA enabled.
If the device on one

side of the link has Bridge Assurance enabled and the device on the other side either does not support BA or has not enabled Bridge Assurance feature, the connecting port is put into bridge inconsistent state (blocked).

The Figure below demonstrates a potential network problem when the device fails and you are not running Bridge Assurance.

Figure 20 Layer 2 Loop Without Bridge Assurance



In normal STP operation without Bridge Assurance feature BPDUs will not be send out by blocked ports only it will receive and process the BPDUs. In the above figure due to some software failure or a unidirectional link Switch 3 will not send any BPDUs to Switch 1. So Switch 1 will move the port connected to the Switch 3 from blocking to forwarding state it may lead to a Layer 2 loop as shown in the figure.

Cisco's recommendation is to configure all switch to switch Layer 2 links as port type network with Bridge Assurance enabled globally.

STP Port Types

The spanning-tree port type designation depends on the device the port is connected to.

Edge Port

Edge ports are connected to Layer 2 hosts and can be either an access port or a trunk port. The edge port interface immediately transitions to the forwarding state, without moving through the listening or learning states. This immediate transition was previously configured as the Cisco proprietary feature PortFast.

Network Port

Network ports are connected only to Layer 2 switches or bridges.

Normal Port

Normal ports are neither edge ports nor network ports; they are normal spanning-tree ports these ports can be connected to any device.

Port types can be configured either globally or per interface. By default, the spanning tree port type on Nexus is normal.

Figure 21 Configuring STP Port Types Globally

```
spanning-tree port type edge default  
spanning-tree port type network default
```

Figure 22 Configuring STP Port Types on Interface Level

```
#Edge port configuration on access port  
spanning-tree port type edge  
  
#Edge port configuration on trunk port  
spanning-tree port type edge trunk  
  
#Network port configuration  
spanning-tree port type network
```

The global configuration of edge port type will not affect the interfaces operating in trunk mode and it will make all ports as edge port type. The network port type global configuration will make all L2 ports as type network.

It is important to understand many STP enhancements work together with the spanning-tree port type, including PortFast, BPDU-Guard, Portfast, BPDU-Filter and Bridge Assurance.

Cisco AS does not recommend configure default port type globally. Instead, it is recommended to configure the STP port type on individual interfaces. All host side network interfaces should be configured as spanning-tree port type edge. This includes both access and trunk host ports.

Cisco's recommendation is to configure all Layer 2 switch to switch (Nexus-to-Nexus) interfaces with spanning-tree port type network to leverage Nexus Bridge Assurance capabilities.

BPDU Guard

BPDU Guard is an STP enhancement that is used to protect Layer 2 STP domain from rogue spanning-tree BPDUs. Once BPDU Guard is enabled it shuts down a port that receives a BPDU on the particular interface.

Figure 23 Configuring BPDU-Guard Globally - NX-OS only

```
spanning-tree port type edge bpduguard default
```

Figure 24 Configuring BPDU Guard on Interface Level

```
spanning-tree bpduguard enable
```

When BPDU Guard is configured globally it is only effective on ports that are operational port type edge state. In a valid configuration host interfaces do not receive BPDUs. Reception of a BPDU by a host port signals an invalid configuration, such as connection of an unauthorized device. BPDU Guard provides a secure response to invalid configurations, because the administrator must manually put the Layer 2 LAN interface back in service.

BPDU Guard can be configured at the interface level. When configured at the interface level, BPDU Guard shuts the port down as soon as the port receives the BPDU, regardless of the port type configuration.

Cisco's recommendation is to enable BPDU Guard for all host facing interfaces.

BPDU Filtering

BPDU Filter is used to prevent the device from sending or even receiving BPDUs on specified ports.

Figure 25 Configuring BPDU Filtering Globally

```
spanning-tree port type edge bpdufilter default
```

Figure 26 Configuring BDDP Filtering on Interface Level

```
spanning-tree bpdufilter enable
```

BPDU Filter allows the administrator to prevent the system from sending or receiving BPDUs on specified ports. BPDU Filter configured globally applies to all operational port type edge ports. Ports in an operational portfast state are supposed to be connected to hosts, which typically do not transmit or receive BPDUs. If an operational portfast port receives a BPDU, it immediately loses its operational portfast status. In that case BPDU Filtering is disabled on this port and STP resumes sending BPDUs on this port.

BPDU Filter can also be configured on a per-port basis, if it explicitly configured on a port, it does not send any BPDUs and drop all BPDUs it receives.

Cisco's recommendation is to configure BPDU Filter on a per interface level for all ports that will be connected to end stations.

UDLD

The Cisco-proprietary UDLD protocol allows devices connected through fiber-optic or copper Ethernet cables connected to LAN ports to monitor the physical configuration or connectivity of the cables and detect when a unidirectional link exists.

Figure 27 Configuring UDLD - Global Configuring

```
feature udld          - only in Nexus  
udld aggressive
```

Figure 28 Configuring UDLD on Interface Level

```
udld enable  
udld aggressive
```

Unidirectional link can cause a variety of problems, including spanning tree topology loops. When a unidirectional link is detected, UDLD shuts down the affected LAN port and alerts the user.

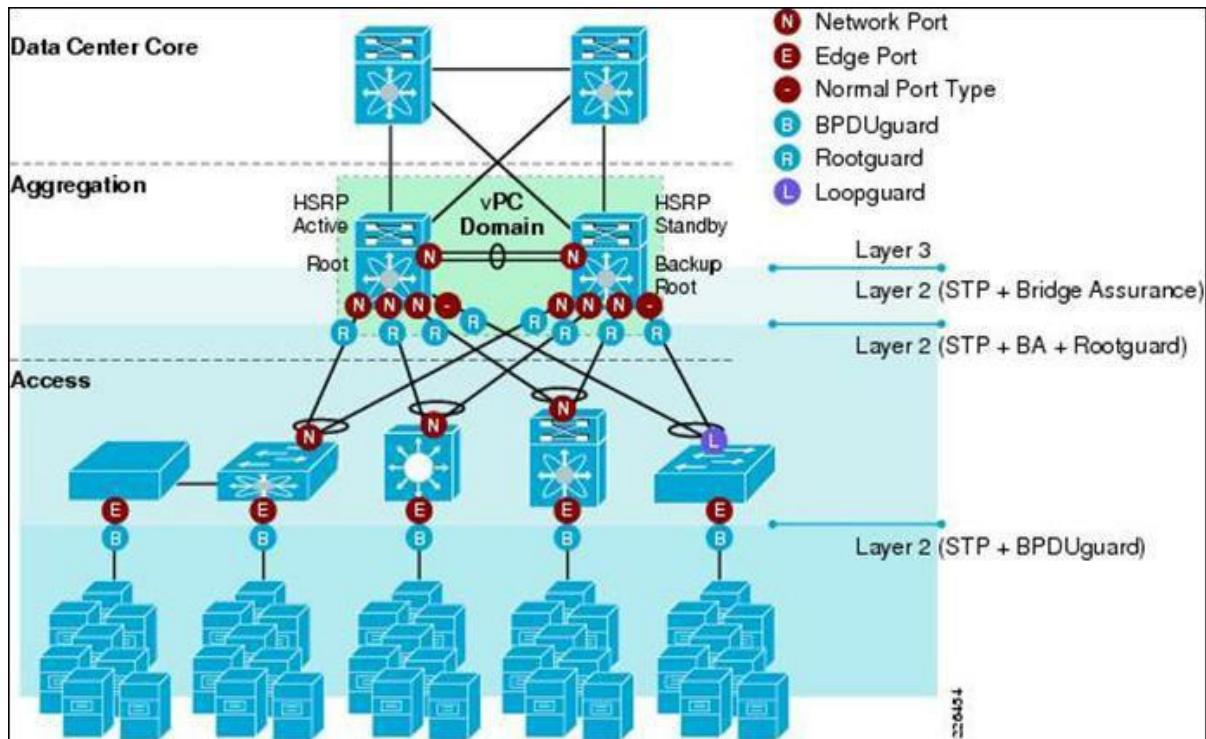
UDLD is a conditional feature in Nexus 7000 so it must be enabled before UDLD configuration. After enabling UDLD feature, UDLD normal mode is enabled by default for all fiber ports on Nexus 7000. The global normal mode is not configurable on the NX-OS. Once UDLD aggressive mode is configured globally, it will be operational on all fiber ports in the chassis. UDLD aggressive mode needs to be enabled manually per port on Ethernet interfaces.

Cisco's recommendation is to use Bridge Assurance as a primary mechanism for detecting a unidirectional link and use UDLD aggressive mode as a failsafe mechanism. UDLD is also recommended to be used between Nexus and devices that do not support BA. This includes both Cisco and non-Cisco products.

STP Features PIN Summary

The following figure summarizes the place in network of various STP features:

Figure 29 STP Feature PIN Summary



EtherChannel

LACP

Link Aggregation Control Protocol (LACP) introduced by IEEE 802.3ad is a standards-based mechanism for two switches to negotiate the building of these bundled links. Many Cisco products also support the use of Port Aggregation Protocol (PAgP) to provide this function. NX-OS does not currently support PAgP. The use of LACP is the recommended solution for configuration of port channel interfaces to the Nexus 7000 over static configuration as it provides configuration sanity check and monitoring of the health of the channel. LACP is configured using the keywords active and passive in the interface configuration. At least one end of the port channel connection must be placed in active mode for channel negotiation to occur.

The use of LACP is beneficial to the stability of the Layer 2 network. LACP enforces some consistency checks (locally and between peers) and has the final word as to which physical link will join the channel. It also monitors the health of the individual

members. Both ends of a port channel can be configured as LACP active for the sake of simplicity.

In NX-OS, LACP is disabled by default; you must enable LACP before you begin LACP configuration.

Figure 30 Enabling LACP

```
feature lacp
```

only in Nexus7000

Port-Channel interfaces are created and configured as shown in the following

Figure 31 Creating Port-Channel

```
interface port-channel channel-number
```

```
description description
```

```
logging event port link-status
```

```
logging event port trunk-status
```

Configuration of link status logging provides UP/DOWN and CHANGE messages in the logs for the case that logging for those types of events has not been enabled globally.

Interfaces are assigned to Port-Channels by configuring:

Figure 32 Mapping Interface to Port-Channel

```
interface type slot/port
```

```
channel-group channel-number [force] [mode {on|active|passive}]
```

The number of EtherChannels is limited to 1 – 48 on Catalyst 3750 series switches.

Load-Balancing algorithm

Hashing algorithms are configured on a per-hop basis, and do not need to match on both sides of a portchannel.

Nexus 7000

Load-Balancing can be performed by one of the following criteria:

Destination IP address and L4 port

Destination IP address, L4 port and VLAN
Destination IP address and VLAN
Destination MAC address
Destination L4 port
Source & Destination IP address and L4 port
Source & Destination IP address, L4 port and VLAN
Source & Destination IP address and VLAN
Source & Destination MAC address
Source & Destination L4 port
Source IP address and L4 port
Source IP address, L4 port and VLAN
Source IP address and VLAN
Source MAC address
Source L4 port

You can configure the load-balancing mode to apply to all port channels that are configured on the entire device or on specified modules. The per-module configuration takes precedence over the load- balancing configuration for the entire device. You can configure one load-balancing mode for the entire device, a different mode for specified modules, and another mode for the other specified modules. You cannot configure the load-balancing method per port channel.

You cannot configure load balancing using port channels per VDC. You must be in the default VDC to configure this feature; if you attempt to configure this feature from another VDC, the system displays an error.

By default Layer 3 IP packets use Source & Destination IP address and VLAN information for load-balancing. The source & destination L4 ports VLAN algorithm offers a better granularity by combining source and destination MAC, VLAN; IP addresses and TCP/UDP ports.

Figure 33 Port-Channel Load Balancing on Nexus 7000

```
port-channel load-balance ethernet {dest-ip-port | dest-ip-port-vlan | destination-ip-vlan | destination-mac | destination-port | source- dest-ip-port | source-dest-ip-port-vlan | source-dest-ip-vlan | source-dest-mac | source-dest-port | source-ip-port | source-ip-port- vlan | source-ip-vlan | source-mac | source-port}[module-number]
```

In case the module-number keyword is used, then the configuration is applied to this module, otherwise, the configuration applies to the entire default VDC.

The load-balancing algorithms that use port channels do not apply to multicast traffic. Regardless of the load-balancing algorithm you have configured, multicast traffic uses the following methods for load balancing with port channels:

Multicast traffic with Layer 4 information—Source IP address, source port, destination IP address, destination port

Multicast traffic without Layer 4 information—Source IP address, destination IP address

Non-IP multicast traffic—Source MAC address, destination MAC address

The behavior of the port ASICs of member ports upon the failure of a single member is handled by the so called adaptive port channel hash-distribution algorithm. While this functionality had to be enabled in IOS explicitly, the Nexus 7000 performs this optimization by default, and does not require this configuration command.

Switches running on IOS

You can configure the switch to use one of the following methods to load balance across the EtherChannel:

Destination MAC address

Source MAC address

Source and destination MAC address

Destination IP address

Source IP address

Source and destination IP address

EtherChannels provide load balancing by default and the basic configuration uses the following criteria to select the link:

For a Layer 2 frame, it uses the source and destination MAC addresses.

For a Layer 3 frame, it uses the source and destination MAC addresses and the source and destination IP addresses.

Figure 34 Port-Channel Load Balancing on IOS switches

```
port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip  
| src-mac}
```

Different load-balancing methods have different advantages, and the choice of a particular load-balancing method should be based on the position of the switch in the network and the kind of traffic that needs to be load-distributed.

By default in switches layer 2 load balance is based on source-destination-mac.

VLAN Trunking protocol (VTP)

Virtual Trunking Protocol (VTP) is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of the VLANs on a network-wide basis within a VTP Domain. A VTP domain is made up of one or more network devices that share the same VTP domain name that are interconnected with trunks.

When configure the switch as VTP transparent (also referred as disabled), VTP passes through the switch: a VTP transparent switch does not send VTP updates and does not act on VTP updates that are received from other switches. So one can create and modify VLANs but the changes affect only the individual switch.

When disabled (also referred as off), the switch does not process any VTP packets and does not even forward them.

There are pros and cons to VTP's ability to make changes easily on a network. Many enterprises prefer a cautious approach of using VTP transparent mode for the following reasons:

It encourages good change control practice, as the requirement to modify a Vlan on a switch or trunk port has to be considered one switch at a time.

It limits the risk of an administrator error, such as deleting a Vlan accidentally and thus impacting the entire domain.

On IOS platforms, the extended Vlan range in numbers 1025-4094, can only be configured in this way

There is no risk from a new switch being introduced into the network with a higher VTP revision number and overwriting the entire domain's Vlan configuration.

It encourages VLAN to be pruned from trunks running to switches that do not have ports in that Vlan, thus making frame flooding more bandwidth-efficient. Manual pruning also has the benefit of reducing the spanning tree diameter.

Unnecessary STP instances are removed, which reduces CPU utilization and thereby improving overall scalability

Cisco recommends that VTP mode is disabled or at least transparent. On NX-OS, VTP is disabled by default on the device and the device does not relay any VTP protocol packets. But in IOS switch it has to be configured as transparent.

VLAN, Trunks and Access ports

Nexus 7000 supports up to 4094 VLANs, this is in accordance with the IEEE 802.1Q standard in each VDC as normal IOS switches.

Figure 35 Configuring VLAN

```
vlan {vlan-id | vlan-range}
      name vlan-name
```

Cisco recommends that you don't use VLAN 1 for any purpose for security reasons.

Figure 36 VLAN Ranges

VLAN Number	Range	Usage
1	Normal	Cisco Default. You can use this VLAN, but you cannot modify or delete it.
2 – 1005	Normal	You can create, use, modify and delete these VLANs
1006-3967 & 4048-4093	Extended	You can create, name, and use these VLANs. You cannot change the following parameters: <ul style="list-style-type: none"> The state is always active. The VLAN is always enabled. You cannot shut down these VLANs.
3968 – 4047 & 4094	Internal	These 80 VLANs, and VLAN 4094, are allocated for internal device use. You cannot create, delete, or modify any VLANs within the block reserved for internal use.

Figure 37 Proposed VLAN range

Valn range	Purpose
100-200	Wired and wireless users
200-250	DataCenter
250-300	WAN and DMZ
300-350	Appliance directly connected to Core
999	Native vlan

Figure 38 Proposed VLANs

Vlan	Used for
100	Wired user
110	Wireless cooperate user
120	Wireless guest user
200	Server farm of MOC
205	UC components
210	DMS Components
215	NMS and other servers
250	ASA outside
255	ASA DMZ
260	ASA inside
261	ASA state

262	ASA failover
265	Guest WLC Management
266	Guest WLC
300	WAN router
305	WLC Mgmt
306	WLC Cooperate user
307	WLC Guest user
310	Ironport Web security Appliance
999	Native vlan

Trunks

Some recommendations should be applied concerning VLAN native on trunks to mitigate security attacks like VLAN hopping:

Clear the native VLAN from all 802.1Q trunks (or set them to 802.1q-all-tagged mode).

In cases where the native VLAN cannot be cleared, use an unused VLAN as the native VLAN for all trunks (don't use this VLAN for any other purpose). Protocols like STP, DTP, etc. should be the only rightful users of the native VLAN and their traffic should be completely isolated from any data packets.

On NX-OS, the default is to allow all VLANs on the trunk interface: 1 to 3967 and 4048 to 4094. VLANs 3968 to 4047 are the default VLANs reserved for internal use by default; this group of VLANs is configurable.

Cisco recommends to explicitly defining VLANs allowed on a trunk.

Figure 39 Allowing VLANs on Trunk

```
interface {type slot/port | port-channel number}
switchport mode trunk
switchport trunk allowed vlan {vlan-list all | none [add |except | none | remove {vlan-list}]}
switchport trunk native vlan 999
```

Access port

The following commands configure an access port.

Figure 40 Configuring Access Port

```
interface {type slot/port | port-channel  
number} switchport mode access  
switchport access vlan vlan-id
```

Layer 3 Network Design

Design Overview

The Layer 3 infrastructure at the MOC would be based mainly on the following:

L3 interfaces for the server farms shall terminate on the Core Nexus7000. HSRP will be running for the servers with redundancy OSPF shall be utilized as the routing protocol between the WAN router and the Core router.

There will be a static default route pointing to the ASA cluster

Common VLAN and HSRP to be created between the ASAs and the Nexus 7000s for routing purposes in case of Failover.

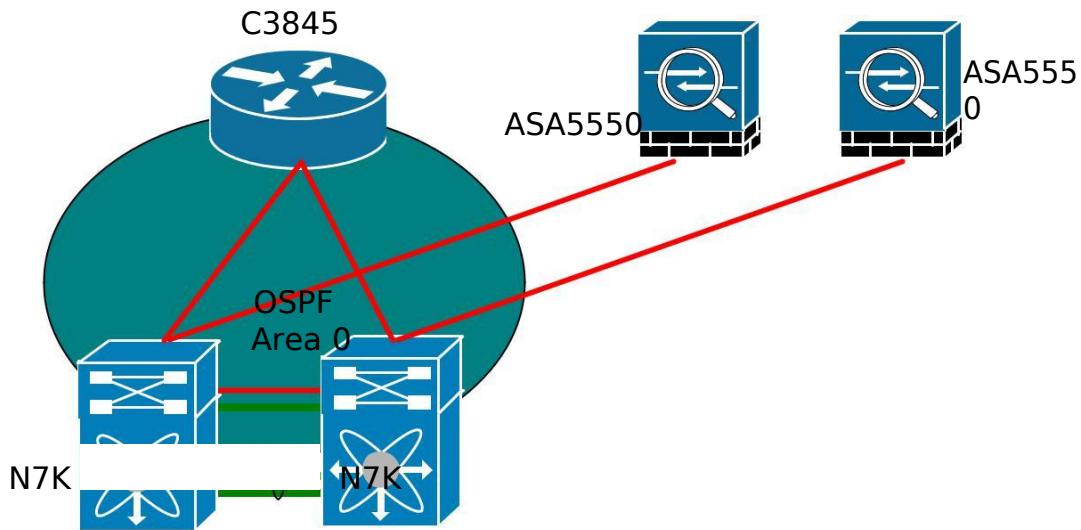
HSRP will be configured on the SVIs for the user VLANs (wired, voice and wireless) on the Nexus 7000.

The above mentioned static routes shall be redistributed into OSPF by the Nexus 7000 switches.

HSRP will be configured on a SVI for WLC on the both Nexus 7000.

HSRP will be configured on a SVI for the Ironport web security appliance on both Nexus 7000.

Gateway ip address of Ironport Mail security appliance and Guest WLC will be configured on DMZ interface of the ASAs.

Figure 41 Layer 3 logical overview diagram

Layer 3 Interfaces for Routing

There will be a common VLAN between Nexus 7000 and the WAN. This will be used for routing remote location subnets. The IP Addresses shall be advertised into OSPF for achieving network reachability. All the other VLAN will be configured as Gateway interface of connected device with the use of HSRP running between Nexus7000.

Figure 42 Configuring L3 Interfaces on N7K

```
interface vlan vlan-id
ip address ip-address/prefix
```

HSRP

The HSRP protocol protects against the failure of the first-hop router. HSRP uses a monitoring function to determine the status of primary and standby router interfaces.

Cisco NX-OS supports HSRP version 1 by default. You can configure an interface to use HSRP version 2. HSRP version 2 has the following enhancements to HSRP version 1:

Expands the group number range. HSRP version 1 supports group numbers from 0 to 255. HSRP version 2 supports group numbers from 0 to 4095.

Uses the new IP multicast address 224.0.0.102 to send hello packets instead of the multicast address of 224.0.0.2, which is used by HSRP version 1.

Uses the MAC address range from 0000.0C9F.F000 to 0000.0C9F.FFFF. HSRP version 1 uses the MAC address range 0000.0C07.AC00 to 0000.0C07.ACFF.

Adds support for MD5 authentication.

When you change the HSRP version, Cisco NX-OS reinitializes the group because it now has a new virtual MAC address.

HSRP version 2 shall be configured on the devices at the MOC network.

The use of HSRP in the context of vPC does not require any special configuration. With vPC, only the active HSRP interface answers ARP requests, but both HSRP interfaces (active and standby) can forward traffic.

If an ARP request coming from a server arrives on the secondary HSRP device, it is forwarded to the active HSRP device via the peer link.

The primary vPC peer should be configured as the HSRP active peer for all VLANs. The HSRP behaviour has been modified when vPC is in use to allow the secondary HSRP peer to actively forward traffic, thereby allowing for an active / active forwarding model. Note that only the active HSRP peer responds to ARP requests.

The HSRP feature must be enabled in NX-OS (HSRP requires no license), before HSRP can be configured.

Figure 43 Enabling HSRP on Nexus 7000

```
feature hsrp
```

The basic configuration for HSRP on the L3 interfaces is given below:

Figure 44 Configuring HSRP on L3 Interfaces

```
interface type slot/port
ip address ip-address/prefix
hsrp group-number
ip virtual-ip-address
```

Figure 45 Configuring the HSRP Version

```
hsrp version 1/2
```


You can configure the HSRP priority on an interface. HSRP uses the priority to determine which HSRP group member acts as the active router.

Figure 46 Configuring HSRP Priority

```
priority level
```

Figure 47 Configuring HSRP timers

```
timers msec hello time msec hold time
```

The HSRP priority and timers are configured from within the HSRP group menu in NX-OS.

Default Gateway

All the servers within a VLAN would have a default gateway and this would be the IP address on the respective VLAN created on the Nexus7000.

The user devices would have a default gateway and this would be the ip address on a SVI created on the Nexus 7000.

Ironport Web security appliance and WLC would have their respective gateways on their SVIs configured on the Nexus 7000.

Ironport Mail security appliance and Guest WLC would have their gateways on the ASA DMZ interface.

IGP Routing – OSPF

IGP is needed to make sure that all networks within a zone are accessible to other zone and also to the outside world and vice versa. OSPF has been chosen as the protocol of choice. The decision to choose OSPF was primarily driven by the following;

Performance and
Scalability Vendor
Compatibility

The OSPF Configuration for the MOC can be summarized as given below:

OSPF Adjacencies to be established between Core N7K and WAN router OSPF Area 0 to be used for the configuration.

The neighbour relationship would be established over the point-to-point L3 links between the devices

OSPF Configuration

The OSPF configuration on Nexus Platform is the same to that on an IOS device with a few minor differences. The configuration steps are given below:

Figure 48 Enabling OSPF on Nexus 7000

```
feature ospf
```

Figure 49 Configuring OSPF Instance and Router-id on Nexus 7000

```
router ospf instance-tag
router-id ip-address
```

Networks are advertised into OSPF on Nexus Platform by configuring the relevant interfaces for routing.

Figure 50 Advertising Network into OSPF

```
interface interface-type slot/port
ip address ip-prefix/length
ip router ospf instance-tag area area-id
```

Figure 51 Configuring OSPF Instance and Router-id on C3845

```
router ospf process-id
router-id ip-address
```

Networks are advertised into OSPF on router by configuring the relevant interfaces for routing.

Figure 52 Advertising Network into OSPF

```
interface interface-type slot/port
ip address ip-prefix/length
ip ospf network point-to-point
```

```
router ospf process-id  
network ip-prefix/wildcast mask area 0
```

OSPF is not enabled on an interface till it is configured with a valid IP Address and mask.

Configuring WCCPv2 in Nexus7000

Web Cache Communication Protocol version 2 (WCCPv2) specifies interactions between one or more Cisco NX-OS routers and one or more cache engines. WCCPv2 transparently redirects selected types of traffic through a group of routers. The selected traffic is redirected to a group of cache engines to optimize resource usage and lower response times.

WCCPv2 enables the Cisco NX-OS router to transparently redirect packets to cache engines. WCCPv2 does not interfere with normal router operations. Using WCCPv2, the router can redirect requests on configured interfaces to cache engines rather than to intended host sites. With WCCPv2, the router can balance traffic loads across a cluster of cache engines (cache cluster) and ensure fault-tolerant and fail-safe operation in the cluster. As you add or delete cache engines from a cache cluster, WCCPv2 dynamically redirects the packets to the currently available cache engines.

WCCPv2 accepts the traffic at the cache engine and establishes the connection with the traffic originator (the client). The cache engine acts as if it were the original destination server. If the requested object is not available on the cache engine, the cache engine then establishes its own connection out to the original destination server to retrieve the object.

WCCPv2 communicates between routers and cache engines on UDP port 2048.

WCCPv2 Service Types

A service is a defined traffic type that the router redirects to a cache engine with the WCCPv2 protocol.

You can configure the router to run one of the following cache-related services:

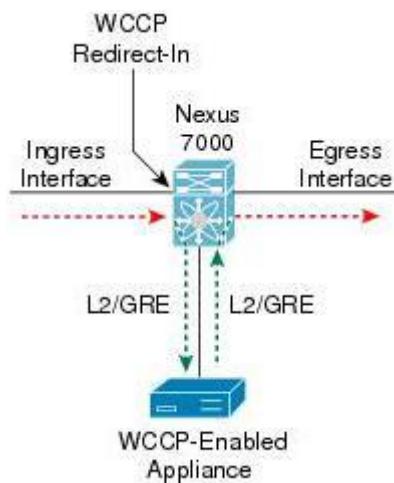
- Well-known —The router and the cache engine know the traffic type, for example the web cache service on TCP port 80 for HTTP.

- Dynamic service—A service in which the cache engine describes the type of redirected traffic to the router.

Redirection

You can use an IP access list as a redirect list to specify a subset of traffic to redirect with WCCPv2. You can apply this access list for ingress or egress traffic on an interface.

Figure 53 WCCP redirection



WCCPv2 Authentication

WCCPv2 can authenticate a device before it adds that device to the service group. Message Digest (MD5) authentication allows each WCCPv2 service group member to use a secret key to generate a keyed MD5 digest string that is part of the outgoing packet. At the receiving end, a keyed digest of an incoming packet is generated. If the MD5 digest within the incoming packet does not match the generated digest, WCCP ignores the packet.

WCCPv2 rejects packets in any of the following cases:

The authentication schemes differ on the router and in the incoming packet. The MD5 digests differ on the router and in the incoming packet.

Redirection Method

WCCPv2 negotiates the packet redirection method between the router and the cache engine. Cisco NX-OS uses this traffic redirection method for all cache engines in a service group.

WCCPv2 redirects packets using the following forwarding method:

Layer 2 Destination MAC rewrite—WCCPv2 replaces the destination MAC address of the packet with the MAC address of the cache engine that needs to handle the packet. The cache engine and the router must be Layer 2 adjacent.

You can also configure an access control list (ACL), called a redirect list, for a WCCPv2 service group. This ACL can either permit a packet to go through the WCCPv2 redirection process or deny the WCCP redirection and send the packet through the normal packet forwarding procedure.

Packet Return Method

WCCPv2 filters packets to determine which redirected packets have been returned from the cache engine and which packets have not. WCCPv2 does not redirect the returned packets, because the cache engine has determined that these packets should not be cached. WCCPv2 returns packets that the cache engine does not service to the router that transmitted them.

A cache engine may return a packet for one of the following reasons:

- The cache engine is overloaded and cannot service the packets.
- The cache engine is filtering certain conditions that make caching packets counterproductive, for example, when IP authentication has been turned on.

WCCPv2 negotiates the packet return method between the router and the cache engine. Cisco NX-OS uses this traffic return method for all cache engines in a service group.

WCCPv2 returns packets using the following forwarding method:

Destination MAC rewrite—WCCPv2 replaces the destination MAC address of the packet with the MAC address of the router that originally redirected the packet. The cache engine and the router must be Layer 2 adjacent.

High Availability for WCCPv2

WCCPv2 supports stateful restarts and stateful switchovers. A stateful restart occurs when the WCCPv2 process fails and is restarted. A stateful switchover occurs when the active supervisor switches to the standby supervisor. Cisco NX-OS applies the running configuration after a switchover.

Guidelines and Limitations for WCCPv2

WCCPv2 has the following guidelines and limitations:

WCCPv2 works with IPv4 networks only.

Do not configure policy-based routing and WCCPv2 on the same interface.

WCCP2 Configuration

To enable the WCCPv2 feature, use the following command in global configuration mode:

Figure 54 Enable WCCPv2

```
feature wccp
```

To configure a WCCPv2 service group, use the following command in global configuration mode:

Figure 55 WCCPv2 service group configuration

```
ip wccp {service-number | web-cache} [mode {open [redirect-list acl-name] | closed service-list acl-name}]] [password [0-7] pwstring]
```

To apply WCCPv2 redirection on an interface, use the following commands in interface configuration mode:

Figure 56 Applying WCCPv2 redirection to interface

```
interface interface-type slot/port
```

```
ip wccp {service-number | web-cache} redirect {in | out}
```


Quality of Service

Nexus 7000

Nexus 7000 Series switch uses modular QoS CLI (MQC) to apply queuing and traditional QOS policies. The default MQC object type is qos. Class maps are used to match the traffic, policy maps to define the actions to take on these classes, and service policy to tie the policy maps to an interface in the input and output directions. QoS policies include marking and policing features, while queuing policies include the queuing and scheduling features and a limited set of marking features.

QoS Hardware Design

As of NX-OS 4.2, Nexus 7000 Series switch supports a 32-port 10G line card (N7K-M132XP-12), a 48-port 1G copper line card (N7K-M148GT-11), and a 48-port 1G SFP line card (N7K-M148GS-11).

In the current solution, 48-port 1G cards are not used, hence the QoS architecture of these cards are not included here. The 32-port 10G card offers a flexible performance model where each group of four front panel ports can run in either shared mode or dedicated mode. Shared mode is the default operational mode of the module. This mode is typically used for connections to servers where a sustained rate of 10 Gbps is not a requirement. In shared mode, a group of four front panel ports share the 10G system bandwidth. The module can have all 32 ports running in the shared port mode. Dedicated mode offers sustained 10 Gbps connection; however, three ports on the port-groups are disabled so the remaining port has full access to the 10G system bandwidth. The 32-port 10G card can have up to eight ports in dedicated mode offering 80G of non-blocking access to the fabric. The dedicated mode ports are marked and highlighted in yellow to differentiate from the remaining front panel ports.

Port QoS on 32-Port 10G Module

The 32-port 10G module implements buffering, queuing, and scheduling in both ingress and egress direction. On ingress, the module uses a two-stage ingress buffering scheme, regardless of whether the port groups are configured in shared mode or dedicated mode. On the egress, the module implements a single of buffering.

In dedicated mode, the 10G port has a 1 MB ingress buffer with an additional 65 MB second-stage buffer and 80 MB egress buffer. The first-stage ingress buffer has eight queues with two tail-drop thresholds (8q2t). The second-stage buffer has two queues with a single tail-drop threshold (2q1t). The egress buffer on the 10G module has a strict- priority queue, along with seven additional queues with four tail-

drop/WRED thresholds (1p7q4t). At the port level, all eight CoS values can be mapped to individual queues in ingress and egress direction.

Fabric QoS

Nexus 7000 Series switch I/O modules use virtual output queuing (VOQ) to ensure fair access to fabric bandwidth for multiple ingress ports transmitting to one egress port. Access to the fabric bandwidth on ingress module is controlled by the central arbiter on the supervisor engine. Arbitration works on credit request and grant basis. All modules inform the central arbiter on egress buffer availability. A module that needs to send traffic over the fabric to a destination port requests credits from the supervisor. The supervisor grants credits based on egress fabric buffer availability for that destination port.

There are four classes of service available at the switch fabric level. The following table shows cos-to-queue mapping within the fabric:

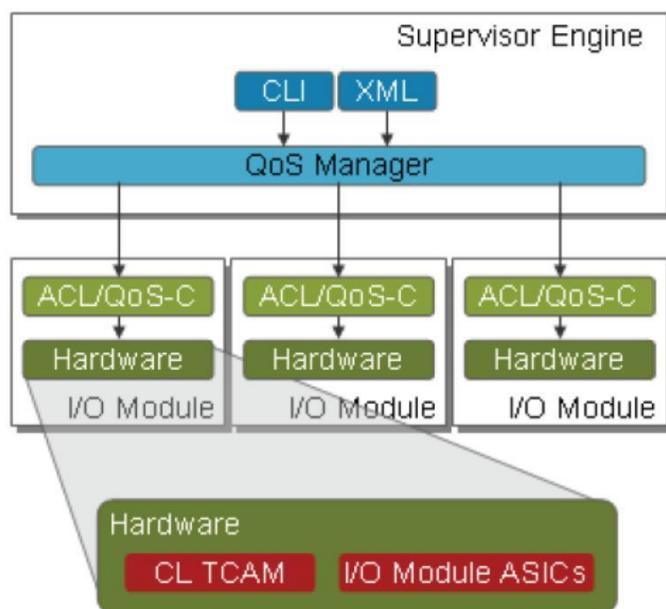
Figure 57 The cos-to-queue mapping within the switch fabric

Queue #	CoS
Q0 (SP)	5-6
Q1	3-4
Q2	2
Q3	0-1

Strict priority traffic takes precedence over best-effort traffic across the fabric. Non-strict priority queues are serviced equally, as they have the same DWRR weight.

QoS Detailed Design

Figure 58 QoS on Nexus 7000



The QoS manager running on the supervisor engine receives the service policy configuration in the command line or XML interface. QoS manager in turn distributes these policies to ACL/QoS client process running on the line cards. ACL/QoS clients perform ACL merge and program the classification TCAM or queuing ASICs on the line card depending on the type of policy.

Classification and Marking

Classification is used to partition traffic into classes based on port characteristics such as CoS field or packet header fields such as IP precedence, and DSCP. Classification is done using a match criterion. The packets that fail to match any class map are assigned to a default class called class-default. Marking is used to identify the traffic type for use in another QoS operation such as policing or queuing.

The Nexus 7000 Series switch in this design is a L2/L3 switch with no specific requirement to perform any QoS classification at ingress. By default, all ports on the Nexus 7000 Series switch are trusted ports. Hence, the DHCP/COS values are preserved during transit.

Following table provide the QoS Baseline Marking Recommendations:

Table 23 Qos Markings recommendation

Application	L3 Classification			L2 CoS
	IPP	PHB	DSCP	
Routing	6	CS6	48	6
Voice	5	EF	46	5
Video Conferencing	4	AF41	34	4
Streaming Video	4	CS4	32	4
Mission-Critical Data	3	AF31*	26	3
Call Signaling	3	CS3*	24	3
Transactional Data	2	AF21	18	2
Network Management	2	CS2	16	2
Bulk Data	1	AF11	10	1
Scavenger	1	CS1	8	1
Best Effort	0	0	0	0

Queuing, Scheduling, and Congestion Management

The queuing and scheduling process enables you to control the bandwidth allocated to traffic classes, so you achieve the desired trade-off between throughput and latency. Congestion management algorithm provides proactive queue management by dropping traffic based on the cos field. Weighted Random Early Detection (WRED) is used for congestion management at the ingress and egress modules.

By default, the Nexus 7000 Series switch enables a system default queuing policy on each port and port channel. When you configure and apply a new queuing policy to an interface, the new policy replaces the default queuing policy.

To change the default queuing behavior, configure the following:

- Configure class maps that define cos-to-queue mapping
- Configure queuing policy maps and define how each class is treated
- Apply queuing service policy to the physical or port-channel interface
- Default queue mapping at ingress and egress port is cos-to-queue. It cannot be changed.

Ingress queuing policy on a 10G module (N7K-M132XP-12) is applied only at the first-stage buffer (i.e., per-port buffer at 4:1 Mux chip). Second stage buffer behavior is fixed. In the current design, 10G modules are used in dedicated mode; hence no specific queuing policy is used in the ingress direction. Egress queuing policy on a 10G module (N7K-M132XP-12) is applied at the port ASIC level.

When egress queuing policy is applied on a 10G port on N7K-M132XP-12 module, the policy is propagated to the remaining ports in the port group even if only the first port of the port-group is used. Only the first port in the port-group is used in dedicated port mode.

Configuration Examples

```
! # Define cos to queue mapping using class-maps
class-map type queuing match-any VOICE
match dscp 46
class-map type queuing match-any BUSINESS
match dscp 26
```



```
class-map type queuing match-any
MGMT match dscp cs6,cs2
class-map type queuing match-any
SIGNALING match dscp 34,32
class-map type queuing match-any
DEFAULT match dscp 0
```

! # Define policy maps

```
policy-map type queuing qos-trunk-uplink-
policy-out class type queuing DEFAULT
bandwidth remaining percent 1
random-detect cos-based aggregate minimum-threshold percent 25
maximum-threshold percent 80
class type queuing SIGNALING
bandwidth remaining percent
10

class type queuing VOICE
bandwidth remaining percent
60 class type queuing
BUSINESS bandwidth
remaining percent 25
random-detect cos-based aggregate minimum-threshold percent 25
maximum-threshold percent 80
class type queuing MGMT
bandwidth remaining
percent 1
random-detect cos-based aggregate minimum-threshold percent 25
maximum-threshold percent 80
```

!


```
policy-map type queuing qos-trunk-downlink-
policy-out class type queuing DEFAULT
bandwidth remaining percent 1
random-detect cos-based aggregate minimum-threshold percent 25
maximum-threshold percent 80
class type queuing
SIGNALING bandwidth
remaining percent 10 class
type queuing VOICE
bandwidth remaining
percent 60 class type
queuing MGMT bandwidth
remaining percent 1
random-detect cos-based aggregate minimum-threshold percent 25
maximum-threshold percent 80
class type queuing BUSINESS
bandwidth remaining percent
25
random-detect cos-based aggregate minimum-threshold percent 25
maximum-threshold percent 80
! # Apply service policy to an
interface interface port-channel1
description vPC peerlink to NEXUS-7k
service-policy type queuing output qos-trunk-downlink-policy-out
!
interface port-channel101
description vPC link to IDF
SWs
service-policy type queuing output qos-trunk-downlink-policy-out
!
```

```
interface port-channel102
description vPC link to
WLC
service-policy type queueing output qos-trunk-uplink-policy-out
```

```
!
interface port-channel103
description vPC link to DC
switch
service-policy type queuing output qos-trunk-uplink-policy-out
!
interface
Ethernet2/x
description To ASA
service-policy type queuing output qos-trunk-uplink-policy-out

interface Ethernet2/y
description To Ironport Web
```

Sec

service-policy type queuing output qos-trunk-uplink-policy-out

Access Switches

All the access switches will be enabled with —mls qos|| and dscp will be trusted in trunk interfaces.

Figure 59 Trust boundaries in Access switches

Uplinks to Nexus7K



Figure 60 Enable mls Qos

```
mls qos
```


Figure 61 Defining trust boundary

```
interface GigabitEthernet0/1-
48 mls qos trust device cisco-
phone
interface
```

```
TenGigabitEthernet0/49 mls
qos trust dscp
```

Figure 62 Modifies CoS-to-DSCP mapping to map CoS 5 to DSCP EF

```
CAT3750(config)#mls qos map cos-dscp 0 8 16 24 32 46 48 56
```

Following table depicts the Queuing design used in the access switches:

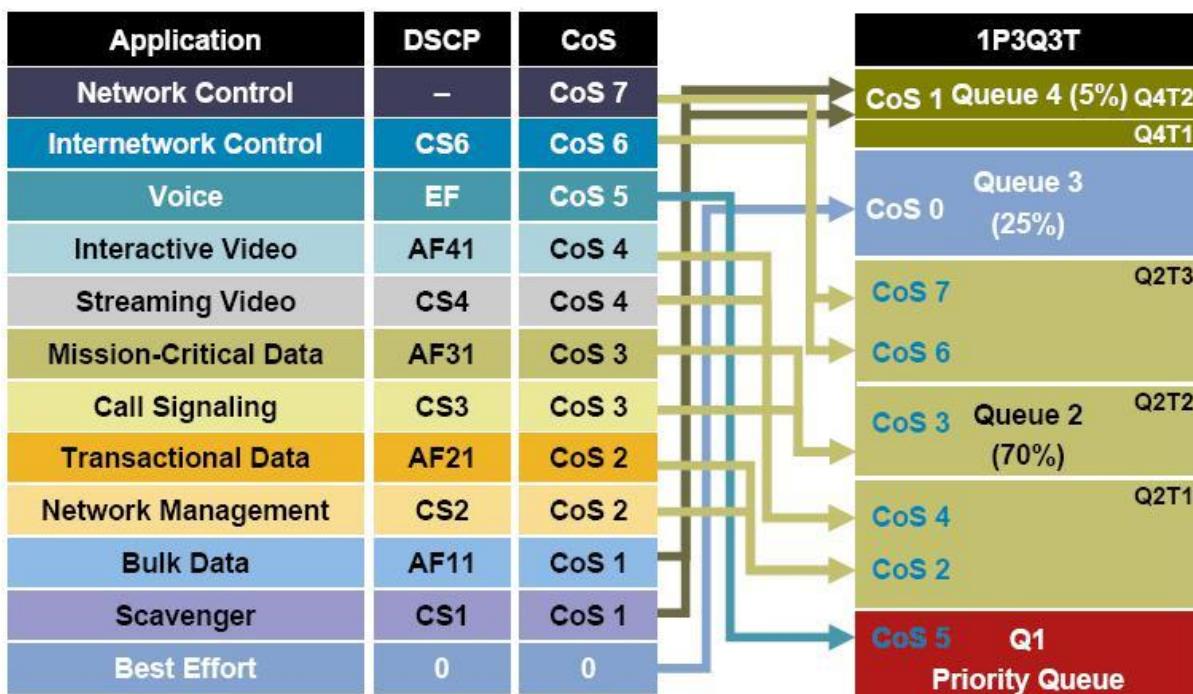
Table 24 Queue assignment in access switches

Figure 63 Access Switch QoS Configuration Example

```
CAT3750(config)#mls qos srr-queue output cos-map queue 1 threshold 3 5
! Maps CoS 5 to Queue 1 Threshold 3 (Voice gets all of Queue 1)

CAT3750(config)#mls qos srr-queue output cos-map queue 2 threshold 12 4
! Maps CoS 2 and CoS 4 to Queue 2 Threshold 1

CAT3750(config)#mls qos srr-queue output cos-map queue 2 threshold 2 3
! Maps CoS 3 to Queue 2 Threshold 2

CAT3750(config)#mls qos srr-queue output cos-map queue 2 threshold 3 6 7
! Maps CoS 6 and CoS 7 to Queue 2 Threshold 3

CAT3750(config)#mls qos srr-queue output cos-map queue 3 threshold 3 0
! Maps CoS 0 to Queue 3 Threshold 3 (Best Efforts gets all of Q3)

CAT3750(config)#mls qos srr-queue output cos-map queue 4 threshold 31
! Maps CoS1 to Queue 4 Threshold 3 (Scavenger/Bulk gets all of Q4)

CAT3750(config)#mls qos srr-queue output dscp-map queue 1 threshold 3 46
! Maps DSCP EF (Voice) to Queue 1 Threshold 3

CAT3750(config)#mls qos srr-queue output dscp-map queue 2 threshold 116
! Maps DSCP CS2 (Network Management) to Queue 2 Threshold 1

CAT3750(config)#mls qos srr-queue output dscp-map queue 2 threshold 118 20 22
! Maps DSCP AF21, AF22, AF23 (Transactional Data) to Queue 2 Threshold 1

CAT3750(config)#mls qos srr-queue output dscp-map queue 2 threshold 126
! Maps DSCP AF31 (Mission-Critical Data) to Queue 2 Threshold 1

CAT3750(config)#mls qos srr-queue output dscp-map queue 2 threshold 132
! Maps DSCP CS4 (Streaming Video) to Queue 2 Threshold 1

CAT3750(config)#mls qos srr-queue output dscp-map queue 2 threshold 134 36 38
! Maps DSCP AF41, AF42, AF43 (Interactive-Video) to Queue 2 Threshold 1

CAT3750(config)#mls qos srr-queue output dscp-map queue 2 threshold 2 24
! Maps DSCP CS3 (Call-Signaling) to Queue 2 Threshold 2
```

```
CAT3750(config)#mls qos srr-queue output dscp-map queue 2 threshold 3  
48 56
```

! Maps DSCP CS6 and CS7 (Network/Internetwork) to Queue 2 Threshold 3

```
CAT3750(config)#mls qos srr-queue output dscp-map queue 3 threshold 3 0
```

! Maps DSCP 0 (Best Effort) to Queue 3 Threshold 3

```
CAT3750(config)#mls qos srr-queue output dscp-map queue 4 threshold 1 8
```

! Maps DSCP CS1 (Scavenger) to Queue 4 Threshold 1

```
CAT3750(config)#mls qos srr-queue output dscp-map queue 4 threshold 3  
10 12 14
```

! Maps DSCP AF11, AF12, AF13 (Bulk Data) to Queue 4 Threshold 3

```
CAT3750(config)#mls qos queue-set output 1 threshold 2 70 80 100 100
```

! Sets Q2 Threshold 1 to 70% and Q2 Threshold 2 to 80%

```
CAT3750(config)#mls qos queue-set output 1 threshold 4 40 100 100 100
```

! Sets Q4 Threshold 1 to 40% and Q4 Threshold 2 to 100%

```
CAT3750(config)#
```

```
CAT3750(config)#interface range
```

```
GigabitEthernet0/1 - 48 CAT3750(config-if-range)#
```

```
queue-set 1
```

! Assigns interface to Queue-Set 1 (default)

```
CAT3750(config-if-range)# srr-queue bandwidth share 1 70 25 5
```

! Q2 gets 70% of remaining BW; Q3 gets 25% and Q4 gets 5%

```
CAT3750(config-if-range)# srr-queue bandwidth shape 3 0 0 0
```

! Q1 is limited to 30% of the total available BW

```
CAT3750(config-if-range)# priority-queue out
```

! Q1 is enabled as a PQ

```
CAT3750(config-if-range)#end
```


Network Device Hardening

Network device hardening design covers the following aspects of device hardening:

Device physical security. We assume that physical security of the DC equipment is taken care of, and proper controls (i.e. secure room, physical access control, video surveillance, etc.) are in place to protect all DC devices and their interconnecting links.

Use of secure software, where care must be taken that software running on a device does not contain any known vulnerabilities, or that temporarily workarounds are in place to make these vulnerabilities unexploitable.

Design of device operating system hardening, where the device OS is hardened to resist attacks and minimize the chance of unauthorized access.

Design of a local access control model, where user authentication and authorization method can control administrators _ access to device resources and configuration.

Design of a local security auditing system, where an audit subsystem accounts for local resource use, and allows for detection of unauthorized activity.

Design of local resource protection, which uses controls that limit the use of critical resources, such as device CPU or memory to avoid denial of service

Design of secure remote management channels, which prevent attacks against remote management interfaces by limiting access and providing secure management paths.

Operating System Hardening

Disabling of DHCP services

All unnecessary services on the switches should be disabled. This will be implemented using the following configuration:

Figure 64 Disabling the DHCP service

```
no service dhcp
```

Disable Small Servers

Small services, such as echo, chargen, daytime and discard can be used to launch DoS and other attacks that would otherwise be prevented using packet filtering. As these services are rarely used they should be disabled.

Figure 65 Disabling small servers

```
no service tcp-small-servers
```

```
no service udp-small-servers
```

Disable Finger Service

Cisco routers provide an implementation of the —finger|| service, which is used to

discover the users that are logged into a device. The information it provides could be useful to an attacker. The service is enabled by default, and if not required should be disabled using the following commands:

Figure 66 Disabling Finger Serv

```
no ip finger
```

```
no service finger
```

Disable Configuration Auto-loading Service

Routers can be configured to load their startup-config from a network server as well as their local memory. Loading router configurations across a network can be dangerous and should only be used in fully trusted network situations. The service is disabled by default.

Figure 67 Disabling Auto-config

```
no service config
```

Disable Bootp Server

Bootp is a UDP based service that allows Cisco routers to obtain copies of IOS from other routers also running the bootp service. In reality, the service is rarely used and

could be used by an attacker to download a copy of a router's IOS. The service is

enabled by default, and can be disabled using the following command:

Figure 68 Disabling Bootp service

```
no ip bootp server
```

Disable IP Source Routing

IP source routing enables the sender of a datagram to specify the route the datagram will take on route to its destination, and generally the route that any reply will take

when returning to the originator. Although enabled by default, source routing is rarely used and could be used by an attacker. If a network does not require source routing, it should be disabled using the following command:

Figure 69 Disabling IP Source-route Feature

```
no ip source-route
```

This will cause the router to drop any IP packet that carries a source route option.

Disable TFTP Server

It is recommended to have a central storage location for IOS images and restrict access to only the loopback ip address of the routers and switches on the network. It is therefore recommended to disable the local tftp servers running on the network and to put all the images needed for the operation of the network on a dedicated server inside the NOC with strict ACLs that only allow tftp traffic inside, if sourced from the loopback ip addresses of the routers or switches on the network. The following command will disable the tftp-server:

```
no tftp-server
```

Disable IP Directed Broadcasts

An IP directed broadcast is a datagram sent to the broadcast address of a subnet to which the sending device is not directly attached. The directed broadcast is routed through the network as a unicast packet until it arrives at the target subnet, where it is converted into a data-link-layer broadcast.

Directed broadcasts are rarely used for legitimate purposes, and are utilised in the

—SMURF|| and other related attacks. The following interface command will cause

directed broadcasts to be dropped instead turned into data-link-layer broadcasts:

```
no ip directed-broadcast
```

As only the last router in the chain of routers that the packet passes through can recognize that the packet is a directed-broadcast, the above command must be configured on every interface that could be a target. It is not sufficient to configure only the first Layer3 routers.

Disable IP Redirects

ICMP redirect messages are enabled by default, and instruct an end device to use a specific router in its path to a destination. By design, a router will send redirects only to hosts on its local subnet, no end device will ever send a redirect, and no redirect will be sent more than one network hop away. However, an attacker may violate these rules to launch an attack on a network. If not required, ICMP redirect messages can be disabled using the following interface command:

```
no ip redirects
```

It is also possible to filter out ICMP redirect messages using ACLs on routers located at the edge of the network. This will prevent redirect attacks launched by remote attackers.

Disable IP Mask Replies

Mask replies are disabled by default, but if enabled, the router responds to ICMP mask requests with ICMP mask replies, which could provide an attacker with important network information. Mask replies should be disabled on all interfaces, especially those at the edge of a network, using the following command:

```
no ip mask-reply
```

Disable Unused Router Interfaces

If an attacker has physical access to a router, any un-used interface could be used to gain access to the router and the network. All un-used interfaces on a router should be disabled in the configuration using the shutdown command.

Disable PAD Service

Security Audit disables all packet assembler/dissembler (PAD) commands and connections between PAD devices and access servers whenever possible. The command to disable PAD is as follows.

```
no service pad
```

Disable Proxy Arp

Proxy ARP is the technique in which one host, usually a router, answers ARP requests intended for another machine. By "faking" its identity, the router

accepts responsibility for routing packets to the "real" destination. Proxy ARP can help

machines on a subnet reach remote subnets without the need to configure routing or a default gateway. This feature is not required in MOC network and can be disabled.

```
interface gig x/y/z
```

```
  no ip proxy-arp
```

Configuration Summary to disable unneeded services

Following is the configuration summary to disable the above mentioned services.

Global configuration mode:

```
no service tcp-small-
servers no service udp-
small-servers no ip finger
no service finger
no service config
no ip bootp
server no ip
source-route no
tftp-server
```

```
no service pad
```

Interface Configuration Mode:

```
no ip directed-broadcast
no ip redirects
no ip mask-reply
no ip proxy-arp
```

Enable Protection Services

Cisco routers and switches support a number of services that can be enabled on a device to improve the overall security of a network. Before any of these services are enabled, they should be reviewed in the context of the network to ensure that they will not effect the current operation of the network.

Enable TCP Keepalive Feature

Idle logged-in user sessions can be susceptible to unauthorized access and hijacking attacks. By default, Cisco routers do not continually test whether a previously connected TCP endpoint is still reachable. If one end of a TCP connection idles out or terminates abnormally (for example, crashes or reloads), the opposite end of the

connection may still believe the session is available. These —orphaned|| sessions use

up valuable router resources. Attackers can take advantage of this weakness to attack devices.

To mitigate this problem, Cisco routers can be configured to send periodic keepalive messages to ensure that the remote end of a session is still available. If the remote device fails to respond to the keepalive message, the sending router will clear the connection. This immediately frees router resources for other more important tasks.

The following IOS commands enable the tcp-keepalive feature:

```
service tcp-keepalives-in  
service tcp-keepalives-out
```

Set TCP Synwait Time

The TCP synwait time is a value that is useful in mitigating SYN flooding attacks, a form of Denial-of-Service (DoS) attack. It is possible to set the amount of time the Cisco IOS software will wait to attempt to establish a TCP connection. Because the connection attempt time is a host parameter, it does not pertain to traffic going through the device, just to traffic originated at the device. To set the TCP connection attempt time, use the ip tcp synwait-time command in global configuration mode. The default is 30 seconds.

Setting the TCP synwait time to 10 seconds causes the router to shut down an incomplete connection after 10 seconds, preventing the buildup of incomplete connections at the host. Following command is used for changing default tcp synwait-time.

```
ip tcp synwait-time 10
```


Device Management and controlling device access

Simple Network Management Protocol

The use of SNMP to collect management data, and in some circumstances to configure network devices, is essential to running an IP network effectively.

The following configuration provides a baseline for an SNMP polling configuration as a starting point:

Figure 70 SNMP community setting

```
snmp-server community <community_string> ro <acl_no>
snmp-server contact noc@moc.gov.qa
access-list <acl_no> permit <NMS subnet> <mask>
```

SNMP Trap Settings

SNMP Traps allow a device to send pro-active notifications of issue via SNMP to the NMS; instead of waiting to be polled for the date. As a bare minimum traps should be used to track major events on Cisco routers & switches. There are many traps which can be enabled in IOS. Their use should be carefully considered as the intention should not be to overwhelm the NOC staff with too much information; rather provide them with useful information.

Following traps can be enabled on routers & switches. All the traps can be sent to a server which could represent the traps by means of alarms.

Figure 71 SNMP trap Setting

```
snmp-server host <ip address> snmp-
server trap-source loopback 0 snmp-
server trap authentication acl-failure
snmp-server trap link switchover
snmp-server enable traps snmp
snmp-server enable traps config
snmp-server enable traps envmon
snmp-server enable traps bgp snmp-
server enable traps mpls ldp snmp-
server enable traps mpls vpn
```



```
snmp-server enable traps mvpn
snmp-server enable traps isis snmp-
server enable traps alarms snmp-
server enable traps bridge snmp-
server enable traps c6kxbar swbus
snmp-server enable traps chassis
snmp-server enable traps config-
copy snmp-server enable traps
entity

snmp-server enable traps envmon fan shutdown supply
temperature status snmp-server enable traps event-manager
snmp-server enable traps flash snmp-
server enable traps fru-ctrl snmp-
server enable traps hsrp snmp-server
enable traps ipmulticast snmp-server
enable traps mac-notification snmp-
server enable traps module
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-
pim-message snmp-server enable traps rf
snmp-server enable traps rtr
snmp-server enable traps snmp authentication linkdown linkup coldstart
warmstart snmp-server enable traps stpx
snmp-server enable traps syslog
snmp-server enable traps
transceiver all snmp-server enable
traps tty snmp-server enable traps
vlan-mac-limit snmp-server enable
traps vlancreate snmp-server enable
traps vlandelete snmp-server enable
traps vtp
```

Also, port traps for key ports, such as infrastructure links to routers and switches, and key server ports should be enabled. Enablement is not necessary for other ports,

such as host ports or access ports. Issue the following command in the interface mode in order to configure the port and enable link up/down notification:

Figure 72 SNMP interface trap setting

```
snmp trap link-status
```

The SNMP ifIndex persistence provides an interface index (ifIndex) value that is retained and used when the router or switch reboots. The ifIndex value is a unique identifying number associated with a physical or logical interface.

SNMP ifIndex persistence is disabled by default and can be enabled globally by using following command:

```
snmp-server ifindex persist
```

Further CPU Threshold Notification feature notifies users when a predefined threshold of CPU usage is crossed by generating a Simple Network Management Protocol (SNMP) trap message for the top users of the CPU.

A rising and a falling CPU threshold notification can be configured as well. In the following configuration, a CPU threshold notification is send if the CPU utilization rises above 50 percent for a period of 5 seconds or longer and falling threshold is send if the CPU utilization falls below 30 percent for a period of 5 seconds or longer.

```
snmp-server enable traps cpu threshold
```

```
process cpu threshold type total rising 50 interval 5 falling 30 interval 5
```

SNMP traps should be sent with a DSCP value of 16(CS2) so that traps are not lost when there is congestion in the network.

```
snmp-server ip dscp 16
```

Logging

Logging of events on a network is an important part of any network security policy. The logging of events assists problem troubleshooting and security investigations.

Cisco routers can log information regarding configuration changes, ACL violations, interface status changes and many other types of events.

Logging messages can be directed to several different locations

Console – used when modifying or testing the device while connected to the console.

Terminal lines – enabled EXEC sessions can be configured to receive log messages on any terminal lines.

Memory buffer – the device can be directed to store log messages in the local memory.

SNMP traps – certain router events may be processed by the router SNMP agent and forwarded as SNMP traps to an external SNMP host.

Syslog – Cisco devices can be configured to forward log messages to an external Syslog service.

When logging, it is important to capture the necessary amount of information. The granularity of detail in logging information can also be configured to one of eight levels, as shown below:

Table 25 Severity Levels

Level	Name	Description
0	Emergencies	Router unusable
1	Alerts	Immediate action required
2	Critical	Condition is critical
3	Errors	Error condition
4	Warnings	Warning condition
5	Notifications	Normal, but important event
6	Informational	Informational message
7	Debugging	Debug message

The following are best practices for logging on IOS devices:

Cisco devices can send their log messages to a Syslog service. A Syslog service accepts messages and stores them in a file. This form of logging is highly recommended, as it provides protected, long-term storage for logs. The following command enables logging:

```
logging on
logging <Syslog_server>
```

Timestamps should be enabled for log and debug messages, which will facilitate interpretation of the messages for troubleshooting and investigating network attacks. This is enabled using the following command:

```
service timestamps log datetime show-timezone msec
service timestamps debug datetime show-timezone msec
```

Timezone has to be changed to GMT+3 to match the Qatar Standard Time. This is enabled by the following command.

```
clock timezone QST +3
```

Sequence numbers indicate the sequence in which messages that have identical time stamps were generated. Knowing the timing and sequence that messages are generated is an important tool in diagnosing potential attacks. This is enabled using following command.

```
service sequence-numbers
```

Enable Buffered Logging - Cisco devices can store log messages in memory. The buffered data is available only from an exec or enabled exec session, and it is cleared when the device reboots. This form of logging is useful, even though it does not offer enough long-term protection for the logs. To enable buffered logging:

```
logging buffered
```

Disable Logging to the Console - Limit the severity level of messages sent to the console or disable logging to the console. This form of logging is not persistent; the device does not store messages printed to the console. Although useful for troubleshooting from the console port, it is possible that excessive log messages on the console could make it impossible to manage the device, even from the console. Console logging can be disabled using the following command:

```
no Logging console
```

Set trap level – Determine the severity of messages that will generate a trap. The following command sets the trap level:

```
logging trap 5
```

To specify the logging facility used for messages sent to system message servers, use the logging facility command in global configuration mode.

```
logging facility local7
```

Set loopback as source of logging – If the loopback interface is not available then a suitable interface should be used, such as the management VLAN.

```
logging source-interface loopback0
```

Logging for the link status has to be enabled on interfaces so that a log is generated whenever there is a link flap on the interface.

```
interface gig x/y/z
```

```
  logging event link-status
```

Physical access

Physical access to devices should be limited, e.g. locked cabinets, restricted access to equipment rooms, etc.

Strong password

To prevent dictionary attacks on network passwords, strong passwords should be used. Passwords should be chosen that contain letters and numbers, as well as special characters (e.g. \$pecial\$ - —specials|| where the s has been replaced by \$ and l with 1).

One Time password

Password sniffing can be mitigated via the use of One Time Passwords (OTPs). For increased security, two-factor authentication via a One-Time Password Server should be used. Two-factor authentication involves using —something you have|| combined with —something you know||. When snuffed, passwords will reveal useless information because of the one-time password environment.

Secure access to the console and Aux ports

Console access requires a minimum level of security both physically and logically. An individual that gains console access to a system will gain the ability to recover or reset the system enable password, giving them the ability to bypass all other security implemented on that system. Consequently it is imperative to secure access to the console.

Alternatively, the console login can be protected using AAA authentication.

```
line con 0
login
password <password>
login authentication <AAAlistName> !If AAA authentication list is used
```

Enable Secret

The enable secret command is used to set the password that grants enable access to the IOS system. The enable secret command replaces the older enable password command as the standard method of configuring the system's privileged mode password. The new method employs a more secure method of encryption than the older command.

All systems should be configured with an enable secret password. Additionally, since the enable secret command simply implements an MD5 hash on the configured password, strong passwords should be chosen to prevent dictionary attacks.

```
enable secret <password>
```

It is also possible to use same encryption with user passwords using the following command:

```
Username <username> secret <password>
```

Service password-encryption

With the exception of the enable secret password, all IOS device passwords are by default stored in clear text form within the device configuration. These passwords can be clearly seen by performing a show running-config command.

The service password-encryption command directs the IOS software to encrypt the passwords, CHAP secrets, and similar data that are saved in its configuration file. This is useful for preventing casual observers from reading passwords, for example, when they happen to look at the screen over an administrator's shoulder.

The algorithm used by service password-encryption is considered relatively weak, and was not designed to protect configuration files against serious analysis, and should not be used for this purpose. Any Cisco configuration file that contains encrypted passwords should be treated with the same care used for a clear text list of those same passwords. It is important to use a

protected link, when accessing the router config using the console, or when TFTP'ing config files. Command:

service password-encryption

Set Authentication Failure Rate to Less Than 3 Retries

One method of cracking passwords, called the "dictionary" attack, is to use software that attempts to log in using every word in a dictionary. This configuration causes access to the router to be locked for a period of 15 seconds after three unsuccessful login attempts, disabling the dictionary method of attack. In addition to locking access to the router, this configuration causes a log message to be generated after three unsuccessful login attempts, warning the administrator of the unsuccessful login attempts.

The command used to lock router access after three unsuccessful login attempts is:

security authentication failure rate 3

Secure access to Mgt port, CMP and VTYs

In a similar manner to console access, remote access via VTYs requires a minimum level of security. The minimum recommended security that should be implemented is as follows:

- Configure a line password for all configured VTYs.
- Apply a basic ACL for inbound access to all VTYs.
- If telnet is the only protocol being used, then permit only telnet transport.

Alternatively, the VTY lines can be protected using AAA authentication which will be discussed later in this section.

```
access-list <acl_no> permit <ip address> <subnet mask>
line vty 0 4
access-class <acl_no> in
login authentication <AAAlistName> !If AAA authentication list is used
```

Login Banners

For both legal and administrative purposes, configuring a system-warning banner to display prior to login is a convenient and effective way of

reinforcing security and general usage policies. By clearly stating the ownership, usage, access, and

protection policies prior to a login, future potential prosecution becomes a more solidly backed case.

MOC is advised to configure a login banner on every device stating that access is restricted, and with the NOC contact details. Of course, no one but authorized MOC staff should be accessing the devices but this is a common best practice.

```
banner login ^C
```

```
-----+
+   Authorized Users Only. Unauthorized Users will be
|   prosecuted.                                |
| This system is the property of Ministry Of Culture |
-----+
+   ^C
```

CLI Management Authentication & Logging (AAA)

It is strongly advised to utilize either TACACS+ or RADIUS to authenticate users accessing network equipment. In addition, accounting may be used to keep a record of each command entered by a user. A sample configuration for TACACS+ is given below. Actual configuration is dependent on MOC's security policies and Cisco Secure ACS server configuration.

```
username moc privilege 15 secret moc123
! A local username and password is set so that the device can be accessed AAA
server is not reachable

aaa new-model
!
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 7 default start-stop group
tacacs+ aaa accounting commands 15 default start-stop
group tacacs+ aaa accounting system default start-stop
group tacacs+
aaa authentication login default group tacacs+
local aaa authentication enable default group
```

```
tacacs+ enable aaa authorization exec default
```

```
group tacacs+ local
```

```
aaa authorization commands 7 default group tacacs+
local aaa authorization commands 15 default group
tacacs+ local
!
```

```
tacacs-server host <ip address of
ACS> tacacs-server key
```

```
<secret_key>
```

```
ip tacacs source-interface loopback0 The access switches will uses mgmt VLAN
```

HTTP Server

Cisco IOS has an inbuilt HTTP service to allow management from a GUI front-end. Most people manage their routers & switches using the CLI, most customers keep this service shutdown as part of security practice. To confirm that service is indeed turned off use the following command in global config mode.

```
no ip http server
```

Network Time Protocol

Network Time Protocol (NTP) is used to synchronize the clocks of various devices across a network. The local NTP client, which runs on the device, accepts time information from other remote time-servers and adjusts its clock accordingly. Synchronization of the clocks within a network is critical for the correct interpretation of events within Syslog data. The following should be considered when deploying NTP:

Define a trusted time source and configure all devices as part of an NTP hierarchy.

Use proper authentication of NTP messages. Version 3 and above of NTP supports a cryptographic authentication mechanism between peers.

ACLs should be used to specify which network devices are allowed to synchronize with which other network devices.

Disable NTP messages on interfaces that are connected to un-trusted interfaces (ntp disable command). If NTP messages have been disabled on an interface of a router, the router could still receive and process NTP messages on another interface. ACLs could also be used to drop NTP messages.

In MOC Network, both the Core Switches (N7K) will be the NTP servers and other network elements will synchronize with Core switches for Network Time.

Following is a sample configuration for NTP Server.

```
clock calendar-valid  
ntp authentication-key 10 md5  
<password> ntp authenticate  
ntp trusted-key 10  
ntp source  
loopback 0 ntp  
master 3
```

```
ntp update-calendar
```

Configuration of NTP Client:

```
ntp authentication-key 10 md5  
<password> ntp authenticate  
ntp trusted-key 10  
ntp source  
loopback 0  
ntp server << IP Address –  
1 >> ntp server << IP Address
```

```
– 2 >> ntp update-calendar
```

Control plane protection (CoPP)

The supervisor module divides the traffic that it manages into three functional components or planes:

Data plane - Handles all the data traffic. The basic functionality of a NX-OS device is to forward packets from one interface to another. The packets that are not meant for the switch itself are called the transit packets. These packets are handled by the data plane.

Control plane - Handles all routing protocol control traffic. These protocols, such as the Border Gateway Protocol (BGP), Open Shortest Path First (OSPF) Protocol, and Protocol Independent Multicast (PIM) Protocol, send control packets between devices. These packets are destined to router addresses and are called control plane packets.

Management plane - Runs the components meant for NX-OS device management purposes such as the command-line interface (CLI) and Simple Network Management Protocol (SNMP).

The supervisor module has both the management plane and control plane and is critical to the operation of the network. Any disruption or attacks to the supervisor module will result in serious network outages.

The NX-OS device supports only hardware-based CoPP which does not support the management interface (mgmt0). The out-of-band mgmt0 interface connects directly to the CPU and do not pass through the in-band traffic hardware where CoPP is implemented. To limit traffic on the mgmt0 interface, use ACLs.

The following protocols are taken into account: IGMP, SNMP, OSPF, PIM, HSRP, GLBP, VRRP, TACACS, TELNET, SSH, SFTP, FTP, NTP, ICMP.

The default CoPP Policy on Nexus 7000 is given below:

Figure 73 Default CPP in Nexus7000

```
ip access-list copp-system-acl-
bgp 10 permit tcp any gt 1024 any
eq bgp 20 permit tcp any eq bgp
any gt 1024 ipv6 access-list copp-
system-acl-bgp6 10 permit tcp
any gt 1024 any eq bgp 20 permit
tcp any eq bgp any gt 1024 ip
access-list copp-system-acl-eigrp
10 permit eigrp any any
ip access-list copp-system-
acl-ftp 10 permit tcp any any
eq ftp-data 20 permit tcp any
any eq ftp
30 permit tcp any eq ftp-data any
40 permit tcp any eq ftp any
ip access-list copp-system-acl-glbp
10 permit udp any eq 3222 224.0.0.0/24 eq
3222 ip access-list copp-system-acl-hsrp
10 permit udp any 224.0.0.0/24 eq
1985 ip access-list copp-system-acl-
icmp
```

10 permit icmp any any echo

20 permit icmp any any echo-reply

```
ipv6 access-list copp-system-acl-
icmp6 10 permit icmp any any
echo-request 20 permit icmp any
any echo-reply
ipv6 access-list copp-system-acl-icmp6-
msgs 10 permit icmp any any router-
advertisement 20 permit icmp any any
router-solicitation
30 permit icmp any any nd-na
40 permit icmp any any nd-ns
50 permit icmp any any mld-query
60 permit icmp any any mld-report
70 permit icmp any any mld-
reduction ip access-list copp-
system-acl-igmp
10 permit igmp any 224.0.0.0/3
ip access-list copp-system-acl-
msdp 10 permit tcp any gt 1024
any eq 639 20 permit tcp any eq
639 any gt 1024 ip access-list
copp-system-acl-ntp 10 permit
udp any any eq ntp
20 permit udp any eq ntp any
ipv6 access-list copp-system-acl-
ntp6 10 permit udp any any eq
ntp
20 permit udp any eq ntp any
ip access-list copp-system-acl-
ospf 10 permit ospf any any
ipv6 access-list copp-system-acl-
ospf6 10 permit 89 any any
```

```
ip access-list copp-system-acl  
pim 10 permit pim any  
224.0.0.0/24  
20 permit udp any any eq pim-auto-  
rp ip access-list copp-system-acl  
pim-reg
```

```
10 permit pim any any
ipv6 access-list copp-system-acl-
pim6 10 permit 103 any ff02::d/128
20 permit udp any any eq pim-
auto-rp ip access-list copp-system-
acl-radius 10 permit udp any any
eq 1812
20 permit udp any any eq 1813
30 permit udp any any eq 1645
40 permit udp any any eq 1646
50 permit udp any eq 1812 any
60 permit udp any eq 1813 any
70 permit udp any eq 1645 any
80 permit udp any eq 1646 any
ipv6 access-list copp-system-acl-
radius6 10 permit udp any any eq
1812
20 permit udp any any eq 1813
30 permit udp any any eq 1645
40 permit udp any any eq 1646
50 permit udp any eq 1812 any
60 permit udp any eq 1813 any
70 permit udp any eq 1645 any
80 permit udp any eq 1646 any
ip access-list copp-system-acl-
rip
10 permit udp any 224.0.0.0/24 eq
rip ip access-list copp-system-acl-
sftp
10 permit tcp any any eq 115
20 permit tcp any eq 115 any
```

```
ip access-list copp-system-acl-
snmp 10 permit udp any any eq
snmp
20 permit udp any any eq snmptrap
```

```
ip access-list copp-system-
acl-ssh 10 permit tcp any any
eq 22
20 permit tcp any eq 22 any
ipv6 access-list copp-system-acl-
ssh6 10 permit tcp any any eq 22
20 permit tcp any eq 22 any
ip access-list copp-system-acl-
tacacs 10 permit tcp any any eq
tacacs
20 permit tcp any eq tacacs any
ipv6 access-list copp-system-acl-
tacacs6 10 permit tcp any any eq
tacacs
20 permit tcp any eq tacacs any
ip access-list copp-system-acl-
telnet 10 permit tcp any any eq
telnet
20 permit tcp any any eq 107
30 permit tcp any eq telnet any
40 permit tcp any eq 107 any
ipv6 access-list copp-system-acl-
telnet6 10 permit tcp any any eq
telnet
20 permit tcp any any eq 107
30 permit tcp any eq telnet any
40 permit tcp any eq 107 any
ip access-list copp-system-acl-
tftp 10 permit udp any any eq
tftp
20 permit udp any any eq 1758
30 permit udp any eq tftp any
```

```
40 permit udp any eq 1758 any  
ipv6 access-list copp-system-acl-  
tftp6 10 permit udp any any eq  
tftp  
20 permit udp any any eq 1758
```

```
30 permit udp any eq tftp any
40 permit udp any eq 1758 any
ip access-list copp-system-acl-
traceroute 10 permit icmp any any
ttl-exceeded
20 permit icmp any any port-
unreachable ip access-list copp-
system-acl-undesirable 10 permit udp
any any eq 1434
ip access-list copp-system-acl-
vpc 10 permit udp any any eq
3200
ip access-list copp-system-acl-
vrrp 10 permit 112 any
224.0.0.0/24
class-map type control-plane match-any copp-system-
class-critical match access-group name copp-system-acl-
bgp
match access-group name copp-system-
acl-bgp6 match access-group name copp-
system-acl-eigrp match access-group name
copp-system-acl-igmp match access-group
name copp-system-acl-msdp match
access-group name copp-system-acl-ospf
match access-group name copp-system-
acl-ospf6 match access-group name copp-
system-acl-pim match access-group name
copp-system-acl-pim6 match access-group
name copp-system-acl-rip match access-
group name copp-system-acl-vpc
class-map type control-plane match-any copp-system-class-
exception match exception ip option
```

```
match exception ip icmp  
unreachable match exception  
ipv6 option  
match exception ipv6 icmp unreachable  
class-map type control-plane match-any copp-system-class-  
important match access-group name copp-system-acl-glbp
```

```
match access-group name copp-system-acl-
hsrp match access-group name copp-
system-acl-vrrp
match access-group name copp-system-acl-
icmp6-msgs match access-group name copp-
system-acl-pim-reg
class-map type control-plane match-any copp-system-class-
management match access-group name copp-system-acl-ftp
match access-group name copp-system-acl-
ntp match access-group name copp-system-
acl-ntp6 match access-group name copp-
system-acl-radius match access-group name
copp-system-acl-sftp match access-group
name copp-system-acl-snmp match access-
group name copp-system-acl-ssh match
access-group name copp-system-acl-ssh6
match access-group name copp-system-acl-
tacacs match access-group name copp-
system-acl-telnet match access-group name
copp-system-acl-tftp match access-group
name copp-system-acl-tftp6 match access-
group name copp-system-acl-radius6 match
access-group name copp-system-acl-tacacs6
match access-group name copp-system-acl-
telnet6
class-map type control-plane match-any copp-system-class-
monitoring match access-group name copp-system-acl-icmp
match access-group name copp-system-acl-
icmp6 match access-group name copp-system-
acl-traceroute
class-map type control-plane match-any copp-system-class-
normal match protocol arp
```

```
class-map type control-plane match-any copp-system-class-
redirect match redirect dhcp-snoop
match redirect arp-inspect
class-map type control-plane match-any copp-system-class-undesirable
```

```
match access-group name copp-system-acl-
undesirable policy-map type control-plane copp-
system-policy class copp-system-class-critical
police cir 39600 kbps bc 250 ms conform transmit
violate drop class copp-system-class-important
police cir 1060 kbps bc 1000 ms conform transmit
violate drop class copp-system-class-management
police cir 10000 kbps bc 250 ms conform transmit
violate drop class copp-system-class-normal
police cir 680 kbps bc 250 ms conform transmit
violate drop class copp-system-class-redirect
police cir 280 kbps bc 250 ms conform transmit
violate drop class copp-system-class-monitoring
police cir 130 kbps bc 1000 ms conform transmit
violate drop class copp-system-class-exception
police cir 360 kbps bc 250 ms conform transmit
violate drop class copp-system-class-undesirable
police cir 32 kbps bc 250 ms conform drop violate
drop class class-default
police cir 100 kbps bc 250 ms conform transmit
violate drop control-plane
service-policy input copp-system-policy
```

Internet/Security Infrastructure

Internet Segment

IT often needs to satisfy the conflicting demands of end users, business leaders and the risk management team, providing seamless, secure access to applications, a consistent user experience and high-performance and availability for users everywhere. MOC security architectures are pairing the application performance as well as network security as a natural cost effective solution. This Cisco recommended security system consists of many components. Ideally, all components work together, which minimizes maintenance and improves security.

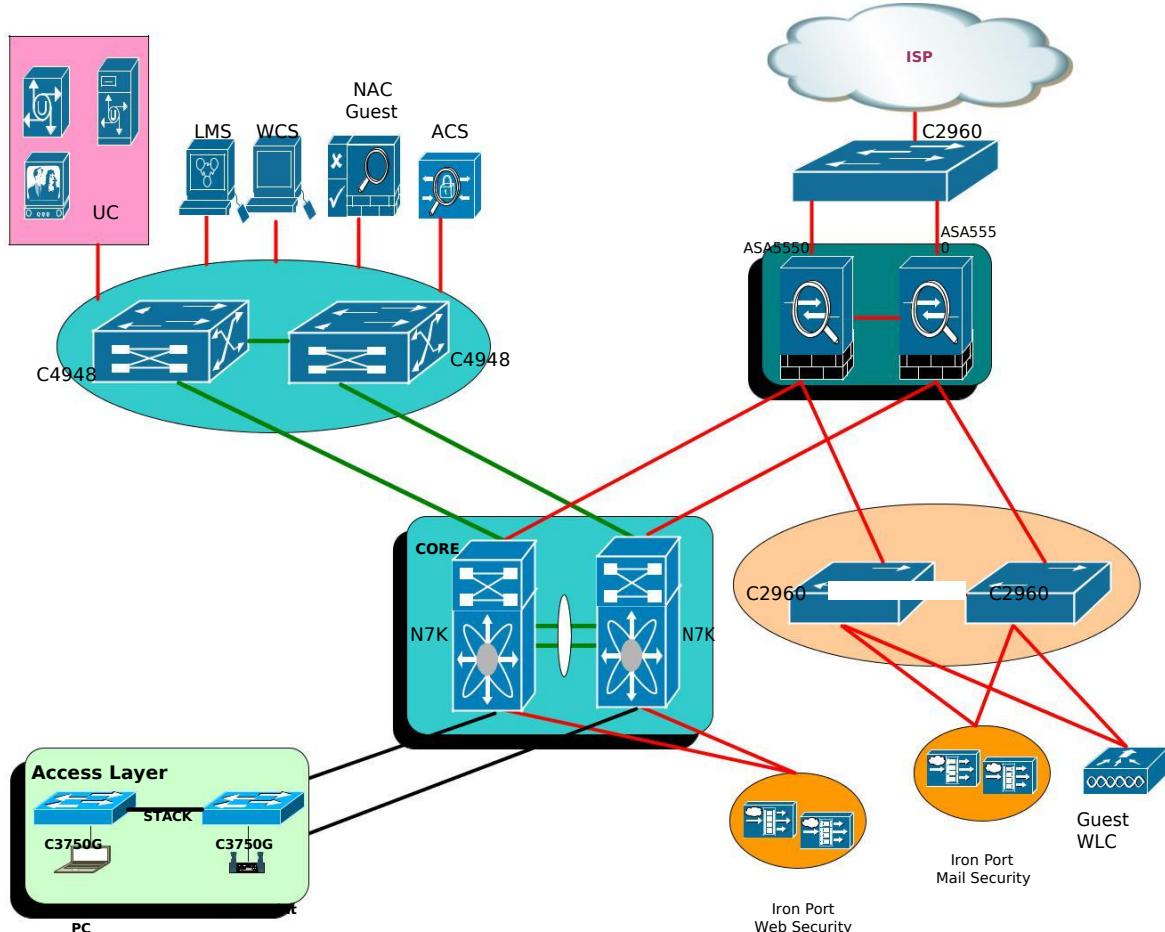
Network security components include:

- ❖ Anti-virus and anti-spyware
- ❖ Firewall, to block unauthorized access to the network
- ❖ Virtual Private Networks (VPNs), to provide secure remote access

This security solution should be able to accommodate increased network traffic or advanced applications without disrupting service.

Detailed Internet Edge Design

Figure 74 INTERNET LOGICAL



This section focuses on the overall design of the Internet edge module.

A pair of firewalls provide stateful access control and deep packet inspection. These firewalls are deployed to protect the organization's internal resources and data from external threats by preventing incoming access from the Internet; to protect public resources served by the DMZ by restricting incoming access to the public services and by limiting outbound access from DMZ resources out to the Internet; and to control user's Internet-bound traffic. To that end, firewalls are configured to enforce access policies, keep track of connection status, and inspect packet payloads. The firewalls are configured in active/standby mode for redundancy purposes. The DMZ hosts services such as the E-mail Security Appliance, HTTP, Domain Name System (DNS), and FTP. IronPort Email Security Appliance (ESA) may be deployed at the DMZ to protect email communications.

Another essential function of the Internet-edge module is to provide secure access to remote workers. Many different approaches can be taken, depending on particular requirements and policies within the enterprise. Full client remote access will be configured and in which clients have full access to all services within the enterprise and experience the same level of service as internal corporate users.

Traffic Flows

This section presents a high-level overview of expected traffic flows in the planned MOC network.

Based on discussions with the customer, the following is expected to traverse the ASA:

- 1.** Traffic between the Internet and the DMZ applications.
- 2.** Traffic between servers in the Datacenter network and the DMZ applications.
- 3.** Traffic between users in the corporate network and internet or DMZ applications.
- 4.** Traffic between users in the remote network and internet or DMZ applications.
- 5.** Traffic from user to Datacenter network will not pass through any security appliance

Access lists will be configured to implement the security policies based on the application / port details provided by the customer.

Moreover all internet traffic will be forwarded via Ironport mail security appliance for web filtering and all the SMTP traffic from the SMTP server to internet will be forwarded via Ironport Mail security appliance for the filtering. Filtering policy will be configured as per the customer requirement.

Figure 75 Traffic flow from DMZ server farm and DC server farm

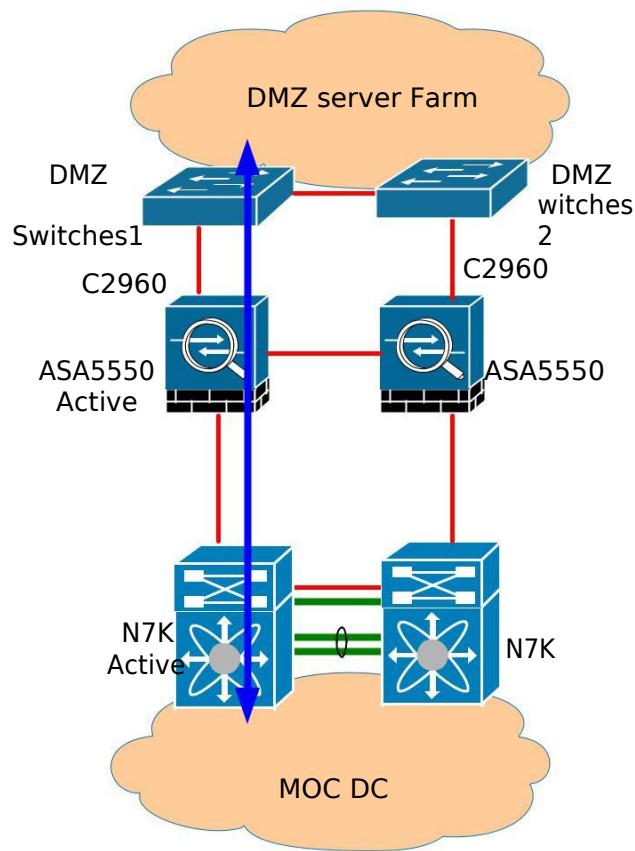


Figure 76 Traffic flow from User segment to DMZ server farm

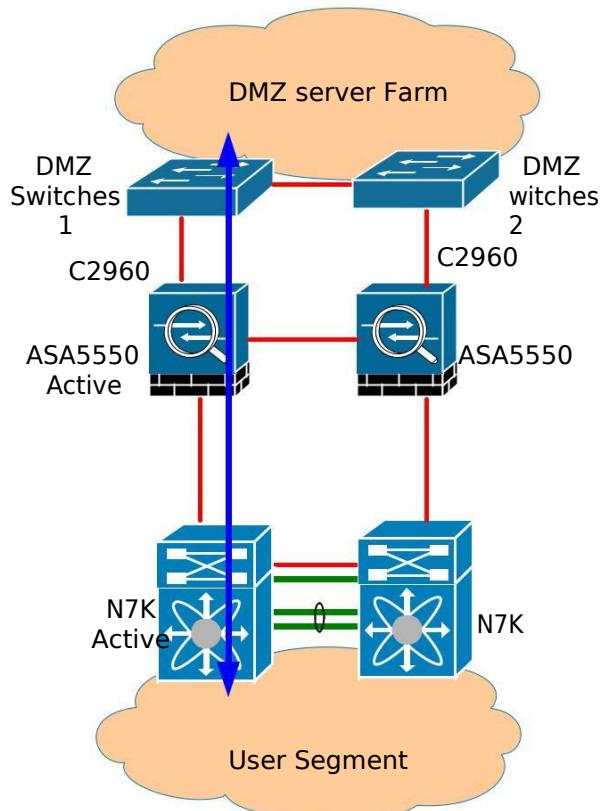


Figure 77 Web traffic from User to internet

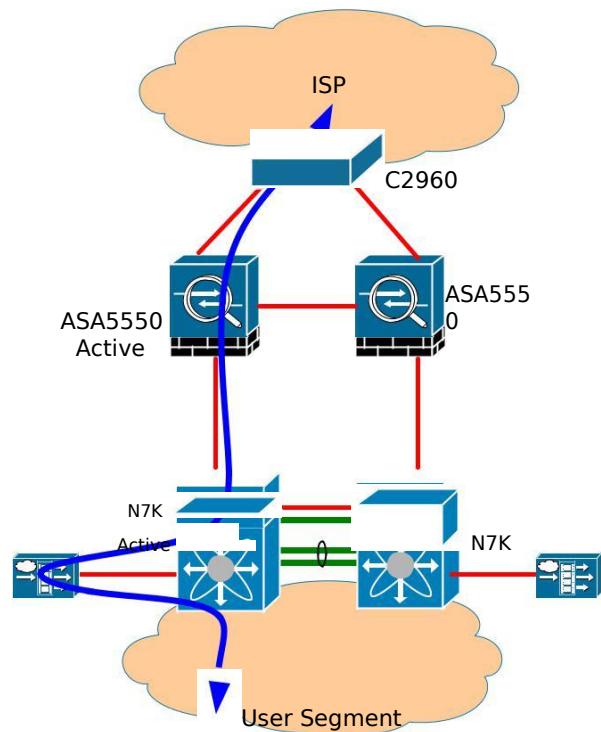


Figure 78 User mail traffic to internet

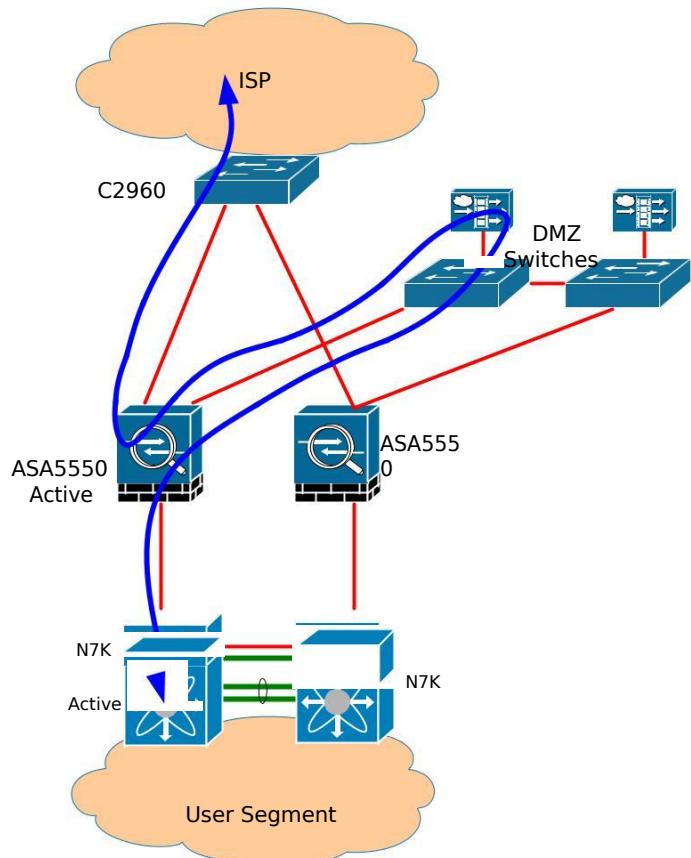
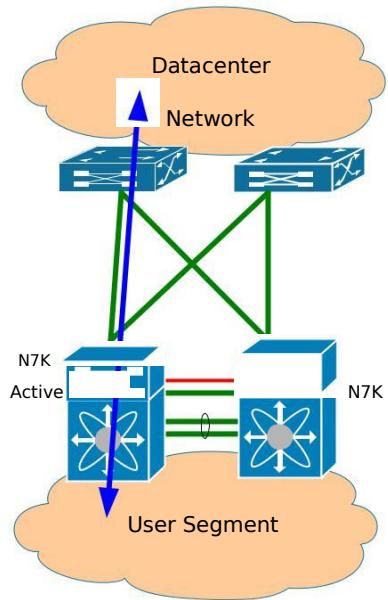


Figure 79 Traffic between user and DC application



Firewall Key Concepts

Overview

Firewalls protect —inside|| networks from unauthorized access by users on an outside

network. The firewall can also protect inside networks from each other, for example, by keeping a human resources network separate from a user network. If network resources need to be available to an outside user, such as a web or FTP server, these resources can be placed on a separate network behind the firewall, called a demilitarized zone (DMZ). The firewall allows limited access to the DMZ, but because the DMZ only includes the public servers, an attack there only affects the servers and does not affect the other inside networks.

Firewalls can also be used to **control inside users' access to outside networks** (for example, access to the Internet), by allowing only certain addresses out, by requiring authentication or authorization, or by coordinating with an external URL filtering server.

Figure 80 ASA5550 image



The Cisco ASA 5550 Adaptive Security Appliance delivers gigabit-class security services with Active/Active high availability and fiber and Gigabit Ethernet

connectivity for large enterprise and service-provider networks in a reliable, 1-rack-unit form factor. Using its eight Gigabit Ethernet interfaces, four Small Form-Factor Pluggable (SFP) fiber interfaces*, and support for up to 200 VLANs, businesses can segment their network into numerous high-performance zones for improved security.

The Cisco ASA 5550 Adaptive Security Appliance scales with businesses as their network security requirements grow, delivering exceptional investment protection and services scalability. Businesses can scale their SSL and IPsec VPN capacity to support a larger number of mobile workers, remote sites, and business partners. Businesses can scale up to 5000 SSL VPN peers on each Cisco ASA 5550 by installing an SSL VPN upgrade license; 5000 IPsec VPN peers are supported on the base platform. VPN capacity and resiliency can also be increased by taking advantage of the Cisco ASA 5550's integrated VPN clustering and load-balancing capabilities. The Cisco ASA 5550 supports up to 10 appliances in a cluster, supporting a maximum of 50,000 SSL VPN peers or 50,000 IPsec VPN peers per cluster. For business continuity and event planning, the ASA 5550 can also benefit from the Cisco VPN FLEX licenses, which enable administrators to react to or plan for short-term bursts of concurrent SSL VPN remote-access users, for up to a 2-month period.

Using the optional security context capabilities of the Cisco ASA 5550 Adaptive Security Appliance, businesses can deploy up to 50 virtual firewalls within an appliance to enable compartmentalized control of security policies on a per-department or per-customer basis, and deliver reduced overall management and support costs.

The system provides a total of 12 Gigabit Ethernet ports, of which only 8 can be in service at any time. Businesses can choose between copper or fiber connectivity, providing flexibility for data center, campus, or enterprise edge connectivity.

Table 26 ASA5550 platform capability

Feature	Description
Firewall Throughput	Up to 1.2 Gbps
VPN Throughput	Up to 425 Mbps
Concurrent Sessions	650,000
IPsec VPN Peers	5000
SSL VPN Peer License Levels*	2,10, 25, 50, 100, 250, 500, 750, 1000, 2500, and 5000
Security Contexts	Up to 50*(license required)
Interfaces	8 Gigabit Ethernet ports, 4 SFP fiber ports, and 1 Fast Ethernet port
Virtual Interfaces (VLANs)	250

Scalability	VPN clustering and load balancing
High Availability	Active/Active**, Active/Standby

[ASA Security Levels](#)

Each interface on the ASA must have a security level from 0 (lowest) to 100 (highest). The most secure network, such as the inside host network, should be assigned level 100; while the least secure network, such as the outside network connected to the Internet should be assigned level 0. Other networks, such as DMZs can be in between.

The security level controls the following behavior:

Network access - By default, there is an implicit permit from a higher security interface to a lower security interface (outbound). Hosts on the higher security interface can access any host on a lower security interface. Access can be limited by applying an access list to the interface.

Inspection engines - Some application inspection engines are dependent on the security level:

NetBIOS inspection engine—Applied only for outbound connections.

SQL*Net inspection engine—if a control connection for the SQL*Net (formerly OraServ) port exists between a pair of hosts, then only is an inbound data connection permitted through the security appliance.

Filtering - HTTP(S) and FTP filtering applies only for outbound connections (from a higher level to a lower level).

NAT control - When NAT control is enabled, NAT must be configured for hosts on a higher security interface (inside) when they access hosts on a lower security interface (outside). Without NAT control, NAT can be used between any interface, or cannot be used at all, as required.

Established command - This command allows return connections from a lower security host to a higher security host if there is already an established connection from the higher level host to the lower level host.

[IP Address and Security Level Assignment](#)

The following table shows the IP addresses and security levels assigned to the firewalls each zone. Private addressing will be used on all the local interfaces however public addressing could also be used on the public DMZ's and Internet facing interfaces such as in WAN zone.

Interface name	Subnet	Primary ip address	Secondary ip address	Security level
Outside	/29			0
Inside	/29			100
DMZ				50
State	/29			-
Failover	/29			-

ASA Network Address Translation (NAT)

Address translation substitutes the real address in a packet with a mapped address that is routable on the destination network. NAT is composed of two steps: the process by which a real address is translated into a mapped address, and the process to undo translation for returning traffic. When describing NAT, the terms inside and outside represent the security relationship between any two interfaces. The higher security level is inside and the lower security level is outside.

The ASA translates an address when a NAT rule matches the traffic. If no NAT rule matches, processing for the packet continues. The exception is when NAT control is enabled.

NAT control requires that packets traversing from a higher security interface (inside) to a lower security interface (outside) match a NAT rule, or processing for the packet stops.

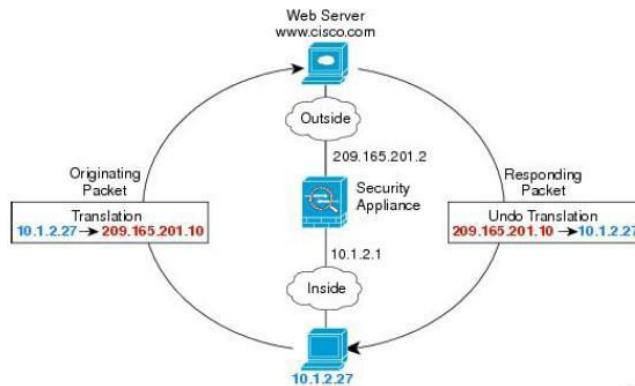
Some of benefits of NAT are as follows:

- Private addresses, which are not routable on the Internet can be used on the inside networks.

- NAT hides the real addresses from other networks, so attackers cannot learn the real address of a host.

- NAT can be used to resolve IP routing problems such as overlapping addresses.

The figure below shows a typical NAT scenario in routed mode, with a private network on the inside. When the inside host with IP address 10.1.2.27 sends a packet to a web server, the local/real source address of the packet (10.1.2.27) is changed to a routable global address (209.165.201.10). When the server responds, it sends the response to the global address (209.165.201.10), and the ASA receives the packet. The ASA then translates the global address (209.165.201.10) back to the real address (10.1.2.27) before sending it on to the host.

Figure 81 Typical NAT in Routed Mode

The following commands would be used on the ASA to produce this translation using dynamic NAT:

Figure 82 NAT configuration example

```
nat (inside) 1 10.1.2.0 255.255.255.0
global (outside) 1 209.165.201.1-209.165.201.15
```

NAT Types

There are a number of ways in which address translation can be implemented: dynamic NAT, Port Address Translation (PAT), static NAT, static PAT or as a mix of these types. It is also possible to bypass NAT, if NAT control has been enabled. These methods are detailed below: Dynamic NAT translates a group of real addresses to a pool of mapped addresses that are routable on the destination network. The mapped pool may include fewer addresses than the real group. When a local host needs to access the destination network, the ASA assigns the host an IP address from the mapped pool. The translation is added only when the local host initiates the connection. The translation is in place only for the duration of the connection, and a given user does not keep the same IP address after the translation times out.

Dynamic NAT is configured using the nat and global commands:

Figure 83 Configuring Dynamic NAT

```
nat (localInterface) <natId> <localIp> <mask> [options...]
global (globalInterface) <natId> {globalIp[-globalIp] / interface}
```

The nat and global statements are linked via the natId.

PAT translates multiple real addresses to a single mapped IP address. Specifically, the ASA translates the real address and source port (real socket) to the mapped address and a unique port above 1024 (mapped socket). Each host receives the same IP address, but because the source port numbers are unique, the responding traffic, which includes the IP address and port number as the destination, can be sent to the correct host. PAT allows the use a single global address, thus conserving routable addresses. However, PAT does not work with some multimedia applications that have a data stream that is different from the control path.

Static NAT creates a fixed translation between real addresses and mapped address.

With dynamic NAT and PAT, each host uses a different address or port after the translation times out. Because the mapped address is the same for each consecutive connection with static NAT, and a persistent translation rule exists, static NAT allows hosts on the destination network to initiate traffic to a translated host (if an access list exists that allows it).

The command to configure static NAT is as follows:

Figure 84 Configuring Static NAT

```
static (localInterface, globalInterface) <globalIp> <localIp> [netmask  
mask] [options]
```

Appropriate values for the max number of TCP, UDP and embryonic options for a translation can be set at the end of the static command. The default values are 0, which means unlimited connections.

Bypassing NAT - By default NAT control is disabled on the ASA. If NAT control is enabled, inside hosts must match a NAT rule when accessing outside hosts. If NAT is not required for certain hosts, NAT control can be disabled, or NAT can be bypassed using a number of methods such as Identity NAT (nat 0 command), Static Identity NAT (static command) or NAT Exemption (nat 0 access-list command).

ASA Policies

A security policy determines which traffic is allowed to pass through the firewall to access another network. Policies are implemented on the ASA using Access Control Lists (ACLs), which are applied to interfaces, thus defining the traffic that is allowed and disallowed to traverse an interface.

Access List Overview

Access lists are made up of one or more Access Control Entries (ACEs). An ACE is a single entry in an access list that specifies a permit or deny rule, and is applied to a protocol, a source and destination IP address or network, and optionally the source and destination ports. The order of ACEs is important. When the ASA decides whether to forward or drop a packet, the security appliance tests the packet against each ACE in the order in which the entries are listed. After a match is found, no further ACEs are checked. Access lists have an implicit deny at the end of the list, so unless it is explicitly permitted, traffic cannot pass.

For TCP and UDP connections it is not necessary to create an access list to allow returning traffic, because the security appliance allows all returning traffic for established, bidirectional connections. For connectionless protocols such as ICMP, however, the security appliance establishes unidirectional sessions, so ICMP needs to be permitted in both directions, or the ICMP inspection engine needs to be enabled, which treats ICMP sessions as bidirectional connections. One access list can be applied to each direction of an interface.

The same access list can be applied to multiple interfaces. When an access-list command is entered for a given access list name, the ACE is added to the end of the access list unless the line number is specified. The following command creates an ACE:

Figure 85 Configuring ACL

```
access-list <ACLname> {deny | permit} <protocol> <sourceAdd> <mask>
[<operator> <port>] <destAdd> <mask> [<operator> <port>]
```

Names and Object Groups

The name command can be used to associate an IP address with a name. The name will be used, wherever that address is referenced in the rest of the configuration, which makes the configuration more readable. The command to define a name is as follows:

Figure 86 Name configuration in ASA

```
name <ipAddress> <name>
```

Using name is however not recommended since no network mask is associated to the named object. For that specific reason, Cisco Security Manager cannot discover

these particular commands. This point may be of particular concern as later phase of this project involves setting up CSM to manage the firewalls.

Using network-object and object-group would be a preferred way of achieving the same objective. Object groups can be used to group like-objects together, so that security policies and rules can be applied to the whole group. This feature can be used to simplify ACLs by reducing the number of entries, and making the ACL more readable by naming groups of objects.

The following lists the object types that can be grouped together, along with the related commands:

Figure 87 Object-group configuration for protocol

```
object-group protocol <name>
  protocol-object <protocol>
```

Figure 88 Object-group configuration for Network

```
object-group network <name>
  network-object {host <IPAddress> | <IPAddress> <mask>}
```

Figure 89 Object-group configuration for Service

```
object-group service <name> {tcp | udp | tcp-udp}
  port-object {eq <port> | range <beginPort> <endPort>}
```

Figure 90 Object-group configuration for ICMP type

```
object-group icmp-type <name>
  icmp-object <icmpType>
```

The name defined in the object-group is used in the relevant position of the ACE, as in the following example:

Figure 91 Usage of an object-group in an ACE

```
object-group network
  SalesServers network-object
  host 10.1.50.1 network-object
  host 10.1.50.2 network-object
  host 10.1.50.3

access-list OUTSIDE-IN extended permit tcp any object-group SalesServers
```

Following command is used to bind the ACL to its respective interface,

```
accessgroup <ACL-name> {in/out} interface <interface-name>
```

Routing

Routing used on the firewall devices will be based on the following considerations:

- Firewall will be L3 aware and operating as a L3 entity.
- Only static routing will be used.
- A default route will be used to provide overall network reach-ability.

The default route for the WAN zone firewall will point to the upstream next-hop ip address as the default gateway which is Qtel ip address. In addition there will be one summarized route that will point to the downstream next-hop router's address for MOC corporate and guest network.

WAN Zone:

```
!default route  
route outside 0 0 <Qtel_Public_HSRP_IP>
```

Firewall High Availability

Overview

Failover allows a standby firewall to take over the functionality of a failed firewall. Failover is compatible with both routed and transparent firewall modes, and with single and multiple context modes. When the active firewall fails, it changes to the standby state, while the standby firewall changes to the active state.

The failover configuration requires two identical firewalls connected to each other through a dedicated failover link and, optionally, a state link. The health of the active interfaces and units is monitored to determine if specific failover conditions are met. If those conditions are met, failover occurs.

The firewall unit that becomes active takes over the active firewall's IP addresses (or, for transparent firewall, the management IP address) and MAC address, and it begins passing traffic. The firewall has one MAC address for all interfaces. The firewall that was active and is now in standby state takes over the standby IP addresses and MAC address. Because network devices see no

change in the MAC to IP address pairing, failover is unnoticed by the rest of the network.

The standby firewall unit can effectively take over as the active firewall unit because it has the same configuration, and it is assigned the same VLANs from the switch.

[Failover Prerequisites](#)

Failover prerequisites are

1. A pair of redundant firewall must run the exact same software image
2. A pair of redundant firewall must have the exact same number of interfaces and/or VLANs
3. A pair of redundant firewall must be Layer-2 adjacent on all their interfaces; in other words all interfaces must be capable of exchanging Layer-2 broadcast packets (ARP, etc.) between each other; failover protocol packets cannot be routed
4. Both firewall must run in the same mode; a single mode unit cannot be paired with a multiple mode unit
5. Both firewalls must agree on operating either as routed or transparent

[Failover Modes](#)

Cisco firewalls supports two failover configurations, Active/Active failover and Active/Standby failover. Each failover configuration has its own method for determining and performing failover.

Active/Standby — this type of failover lets you use a standby firewall to take over the functionality of a failed unit. When the active unit fails, it changes to the standby state while the standby unit changes to the active state. The unit that becomes active assumes the IP addresses (or, for transparent firewall, the management IP address) and the MAC address of the failed unit and begins passing traffic. The unit that is now in standby state takes over the standby IP addresses and MAC address. Because network devices see no change in the MAC to IP address pairing, no ARP entries change or time out anywhere on the network.

The main difference between the two units in a failover pair is related to which unit is active and which unit is standby, namely which IP addresses to use and which unit actively passes traffic.

Active/Active — this failover is only available to firewalls in multiple context mode. In an Active/Active failover configuration, both firewalls can pass network traffic however you divide the security contexts on firewalls into failover groups. A failover group is simply a logical group of one or more security contexts.

For MOC network, the firewalls will be deployed in Active/Standby failover mode.

The firewall module supports two types of failover:

Regular failover — when a failover occurs, all active connections are dropped and clients need to re-establish connections when the new active module takes over.

Stateful failover — during normal operation, the active module continually passes per-connection stateful information (for each context) to the standby module.

For MOC network, the firewalls will be deployed in Active/Standby mode with stateful failover configuration.

After a failover occurs, the same connection information is available at the new active module. Supported end-user applications are not required to reconnect to keep the same communication session.

The state information passed to the standby module includes the following data:

NAT translation
table TCP
connection states
UDP connection states (for connections lasting at least 15 seconds)
HTTP connection states (Optional)
H.323, SIP, and MGCP UDP media connections
ARP table

[Failover Link](#)

The two units in failover pair constantly communicate over a failover link to determine the operating status of each module. Communications over the failover link include the following data:

The unit state (active or standby) Hello messages (keep-alives)
MAC address exchange Network link status
Configuration synchronization between the two modules

A separate interface/VLAN should be configured for the failover link.

[State Link](#)

To use stateful failover, a state link needs to be configured to pass all state information. This link can be the same as the failover link, but it is recommended that a separate VLAN and IP address is assigned for the state

link. The state traffic can be large, and performance is improved with separate links.

For Cisco ASA 5550 adaptive security appliances, stateful link speed can be 1 Gigabit interface, but only non-management ports should be used for the stateful link.

A separate interface/VLAN is recommended and should be configured for the State Link.

It is recommended to use a failover key to secure the communication between the two firewalls as by default the communication over failover and state link is in clear text.

[Failover Options](#)

There are 2 options on how the firewalls can be used for Failover:

Intra-Chassis (Only for FWSM and not used within MOC network)
Inter-Chassis

Inter-Chassis Failover

For the firewall appliances, the stateful and failover interfaces would be connected between the two firewalls via switches however it could also directly connected using the two 1 gigabit interface with a cross over cable to provide inter-chassis failover however all other firewalled data VLANs should be trunked via the dedicated etherchannel between the two distribution multi-layer switches.

It is recommended that a dedicated failover interface should be used for firewall stateful failover link.

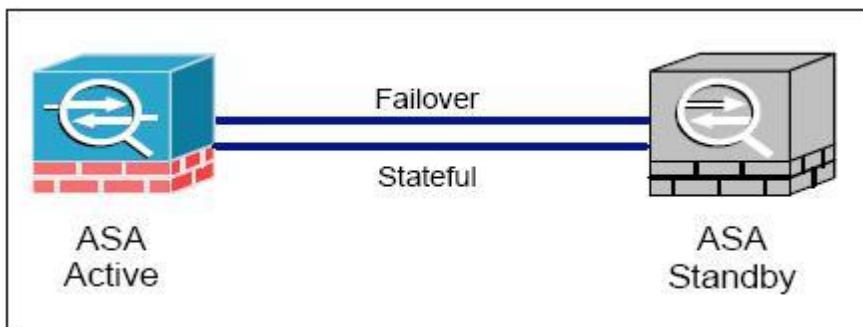
If a single trunk is used between the switches to carry all traffic, the following should be considered:

The trunk must carry all firewalled VLANs, including the failover and state VLANs.

The trunk between the two devices needs to include at least 1 Gbps for the data plus the other firewall traffic.

The trunk should have QoS enabled so that failover VLAN packets, which have the CoS value of 5 (higher priority), are treated with higher priority in these ports.

The below figures shows a high level view of the failover concept used in the MOC firewall failover deployment:

Figure 92 ASA Inter-chassis Failover concept using cross cables

Configuration Replication

The two firewalls share an almost identical configuration, as both configurations include the active and standby IP addresses. When a firewall unit is active, it uses the active IP addresses; when a firewall unit is standby, it uses the standby IP addresses. Because the configuration is the same on both firewall units, the host names, usernames, and passwords are also the same.

The only difference in the configuration is the primary and secondary designation, although the failover link must also be pre-configured on the secondary unit before the firewalls can communicate. All other configuration is automatically replicated from the active to the standby unit.

The active unit sends the configuration in running memory to the standby unit. On the standby unit, the configuration exists only in running memory. Configuration replication from the active unit to the standby unit occurs in the following circumstances:

When the standby unit completes its initial start-up, it clears its running configuration (except for the failover commands that must be pre-configured and are not replicated), and the active unit sends its entire configuration to the standby unit.

As commands are entered on the active unit, they are sent across the failover link to the standby unit.

If the write standby command is entered on the active unit, the standby unit clears its running configuration (except for the failover commands that must be pre-configured and are not replicated), and the active unit sends its entire configuration to the standby unit.

Failover Triggers

The firewall can fail if one of the following events occurs:

The firewall has a hardware failure or a power failure. The firewall has a software failure.

Too many monitored interfaces fail.

The no failover active command is entered on the active unit or the failover active command is entered on the standby unit.

Unit Health Monitoring

The firewall determines the health of the other unit by monitoring the failover link. When a firewall unit does not receive hello messages on the failover link, the firewall unit sends an ARP request on all interfaces, including the failover interface. The firewall unit retries a user-configurable number of times.

The action the firewall takes depends on the response from the other firewall unit. The following are possible actions:

If firewall module receives a response on any interface, then it does not fail over.

If the firewall appliance receives a response on the failover interface, then it does not fail over.

If the firewall does not receive a response on any interface, then the standby unit switches to active mode and classifies the other unit as failed.

If the firewall does not receive a response on the failover link, but receives a response on another interface, then the unit does not failover. The failover link is marked as failed. The failover link should be restored as soon as possible because the unit cannot fail over to the standby while the failover link is down.

Interface Monitoring

By default, monitoring physical interfaces is enabled and monitoring subinterfaces is disabled. You can monitor up to 250 interfaces on a unit. You can control which interfaces affect your failover policy by disabling the monitoring of specific interfaces and enabling the monitoring of others. You should monitor important interfaces and this lets you exclude interfaces attached to less critical networks from affecting your failover policy.

When a firewall unit does not receive hello messages on a monitored interface, it runs the following tests:

Link Up/Down test - test of the Interface/VLAN status. If the Link Up/Down test indicates that the Interface is operational, the firewall performs network tests. The purpose of these tests is to generate network traffic to determine which (if either) the unit has failed. If neither firewall unit has received traffic, then the next test is used.

Network Activity test - A received network activity test. The firewall unit counts all received packets for up to 5 seconds. If any packets are received at any time during

this interval, the interface is considered operational and testing stops. If no traffic is received, the ARP test begins.

ARP test - A reading of the module ARP cache for the 2 most recently acquired entries. One at a time, the firewall unit sends ARP requests to these machines, attempting to stimulate network traffic. After each request, the firewall unit counts all received traffic for up to 5 seconds. If traffic is received, the interface is considered operational. If no traffic is received, an ARP request is sent to the next machine. If at the end of the list no traffic has been received, the ping test begins.

Broadcast Ping test - A ping test that consists of sending out a broadcast ping request. The firewall unit then counts all received packets for up to 5 seconds. If any packets are received at any time during this interval, the interface is considered operational and testing stops.

If all network tests fail for an interface, but this interface on the other firewall unit continues to successfully pass traffic, then the interface is considered to be failed. If the threshold for failed interfaces is met, then a failover occurs. If the other firewall unit interface also fails all the network tests, then both interfaces go into the "Unknown" state and do not count towards the failover limit.

An interface becomes operational again if it receives any traffic. A failed firewall unit returns to standby mode if the interface failure threshold is no longer met.

Figure 93 Monitoring the interface

```
hostname(config)# monitor interface if_name
```

Configuring Active/Standy Inter-Chassis Failover

To configure the primary unit in an Active/Standby failover configuration, perform the following steps:

Figure 94 State-failover configuration

```
Primary Unit:
```

```
failover lan unit primary
```

```
failover lan interface failover_intf_name physical_intf
```

```
failover interface ip failover_intf_name ip_address mask standby
```

```
ip_address failover link state_<intf_name physical_intf
```

```
failover interface ip state_intf_name ip_address mask standby ip_address
```



```
interface physical_intf
no shutdown
failover
Secondary Unit:
failover lan unit secondary
failover lan interface failover_intf_name physical_intf
failover interface ip failover_intf_name ip_address mask standby ip_address
failover
```

Enabling HTTP Replication with Stateful Failover

To allow HTTP connections to be included in the state information replication, you need to enable HTTP replication. Because HTTP connections are typically short-lived, and because HTTP clients typically retry failed connection attempts, HTTP connections are not automatically included in the replicated state information.

To enable HTTP state replication for a failover group, enter the following command. This command only affects the failover group in which it was configured. To enable HTTP state replication for both failover groups, you must enter this command in each group. This command should be entered in the system execution space:

Figure 95 http replication

```
failover replication http
```

Enabling Secure Failover Communication

To secure the failover communications enter the following command on the unit that has failover group 1 in the active state of an Active/Active failover pair:

Figure 96 Secure Failover Communication

```
failover key {secret | hex key}
```


IronPort E-Mail Security

The IronPort® C360™ is an accurate, affordable and easy to use all-in-one appliance

— purpose-built for email security. Designed to meet the needs of small and medium enterprises, the IronPort C360 is built on the same robust platform that protects the email infrastructures of major Global 2000 companies. The IronPort C360 is designed and built not only for power and ease of use, but also for affordability. This innovative technology provides a comprehensive solution to ensure the availability and security of your email infrastructure— implemented in a manner that makes it cost-effective for companies of all sizes. The IronPort C360 uses the industry's most advanced technology to stop spam, viruses and anomalies in a fully automated manner. This allows highly skilled IT staff to focus on other problems, and leave the email issues to IronPort.

The following part of this document is the initial configuration for Ironport E-mail security appliance in MOC network.

Register the IronPort Appliance in DNS

Malicious email senders actively search public DNS records to hunt for new victims. We need to ensure that the IronPort appliance is registered in DNS to utilize the full capabilities of IronPort Anti-Spam, Brightmail Anti-Spam, Virus Outbreak Filters, McAfee Antivirus and Sophos Anti-Virus. To register the IronPort appliance in DNS, create an A record that maps **the appliance's hostname to its IP address, and an MX**

record that maps MOC public domain to the appliance's hostname. It must specify a

priority for the MX record to advertise the IronPort appliance as either a primary or backup MTA for the domain.

The following figure shows the typical placement of the IronPort appliance in MOC network environment:

Figure 97 IRON PORT



In this scenario, the IronPort appliance resides inside the network —DMZ,|| in which

case an additional firewall sits between the IronPort appliance and the groupware server.

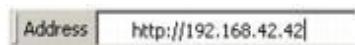
Using the System Setup Wizard

The IronPort AsyncOS operating system provides a browser-based System Setup Wizard to guide through the five step process of system configuration. Also included is a command line interface (CLI) version of the System Setup Wizard.

WARNING: The System Setup Wizard will completely reconfigure the system. It should only use the System Setup Wizard the very first time we install the appliance, or if we want to completely overwrite your existing configuration.

WARNING: The IronPort appliance ships with a default IP address of 192.168.42.42 on the e Data 1 port of C10/100 systems. Before connecting the IronPort appliance to the network, ensure that no other device's IP address conflicts with this factory default setting.

To access the web-based Graphical User Interface (GUI), open your web browser and point it to 192.168.42.42.



The login screen is displayed:

A screenshot of the IronPort AsyncOS Login screen. The screen has a purple header with the word "Welcome". Below the header is a "Login" form. The form has two input fields: "Username:" containing "admin" and "Password:" containing masked text. At the bottom left is the text "v4.5.0-606" and at the bottom right is a blue "Login" button.

Log in to the appliance by entering the username and password below.

- Username: admin
- Password: ironport

Step 1: Start

Begin by reading the license agreement. Once we have read and agreed to the license agreement, check the box indicating that you agree and then click Begin Setup to proceed.



Step 2: System

Setting the Hostname

Define the fully-qualified hostname for the IronPort appliance. This name should be assigned by the network administrator.

Configuring System Alerts

IronPort AsyncOS sends alert messages via email if there is a system error that requires the user's intervention. Enter the email address (or addresses) to which to send those alerts.

We must add at least one email address to which to send System Alerts. Enter an email address, or separate multiple addresses with commas. The email addresses entered will initially receive all types of alerts at all levels. You can add more granularity to the alert configuration later.

Configuring Report Delivery

Enter the address to which to send the default scheduled reports. If we leave this value blank, the scheduled reports are still run. They will be archived on the appliance rather than delivered.

Setting the Time

Set the time zone on the IronPort appliance so that timestamps in message headers and log files are correct. Use the drop-down menus to locate time zone or to define the time zone via GMT offset.

We can set the system clock time manually later, or can use the Network Time Protocol (NTP) to synchronize time with other servers on network or the Internet. By default, one entry to the IronPort Systems time servers (time.ironport.com) to synchronize the time on IronPort appliance is already configured.

Setting the Password

Set the password for the admin account. This is a required step. When changing the password for IronPort AsyncOS admin account, the new password must be six characters or longer. Be sure to keep the password in a secure location.

Participating in SenderBase Network

SenderBase is an email reputation service designed to help email administrators research senders, identify legitimate sources of email, and block spammers.

If we agree to participate in the SenderBase Network, IronPort will collect aggregated email traffic statistics about the organization. This includes only summary data on message attributes and information on how different types of messages were handled by IronPort appliances.

To participate in the SenderBase Network, check the box next to —Allow IronPort to

gather anonymous statistics on email and report them to SenderBase in order to identify and stop email-based threats|| and click Accept.

Enabling AutoSupport

The IronPort AutoSupport feature (enabled by default) keeps the IronPort Customer Support team aware of issues with IronPort appliance so that they can provide better support.

System Configuration

Before you enter your System and Network settings:

- Choose a configuration that best matches your network infrastructure
- Determine network and IP address assignments
- Gather information about your system setup

System Settings	
Default System Hostname:	<input type="text" value="smtp.ironport.com.qa"/> example: ironport-C60.example.com
Email System Alerts To:	<input type="text" value="example: admin@company.com"/>
Deliver Scheduled Reports To:	<input type="text"/> example: admin@company.com. Leave blank to only archive reports on-box.
Time Zone:	Region: <input type="button" value="GMT Offset"/> Country: <input type="button" value="GMT"/> Time Zone / GMT Offset <input type="button" value="GMT"/>
NTP Server:	<input type="text" value="time.ironport.com"/>
Administrator Password:	Password: <input type="password"/> Must be 6 or more characters. Confirm Password: <input type="password"/>
SenderBase Network Participation:	<input checked="" type="checkbox"/> Allow IronPort to gather anonymous statistics on email and report them to SenderBase in order to identify and stop email-based threats. Learn what information is shared...
AutoSupport:	<input checked="" type="checkbox"/> Send system alerts and weekly status reports to IronPort Customer Support

[Cancel](#)

[Next >](#)

Click Next to continue

Step 3: Network

In Step 3, we will define the default router (gateway) and configure the DNS settings, and then set up the appliance to receive and or relay email by configuring the Data1 interfaces.

Type the IP address of the default router (gateway) on the network.

Next, configure the DNS (Domain Name Service) settings. IronPort AsyncOS contains a high-performance internal DNS resolver/cache that can query the Internet's root servers directly, or the system can use DNS servers we specify.

Configuring Network Interfaces

The following information is required:

The IP address assigned by network administrator.

The netmask of the interface.

The netmask can be in standard dotted decimal form or hexadecimal form.

(optional) A fully-qualified hostname for the IP address

Note — IP addresses within the same subnet cannot be configured on separate physical Ethernet interfaces.

Accepting Mail

When configuring your interfaces to accept mail, you define:

the domain for which to accept mail

destination (SMTP Route) for each domain, this is optional

Mark the checkbox for Accept Incoming Mail to configure the interface to accept mail. Enter the name of the domain for which to accept mail.

Enter the Destination. This is the SMTP Route or name of the machine(s) where we would like to route email for the domains specified.

This is the first SMTP Routes entry. The SMTP Routes table allows redirecting all email for each domain (also known as a Recipient Access Table (RAT) entry) we enter to a specific mail exchange (MX) host. In typical installations, the SMTP Routes table defines the specific groupware (for example, Microsoft Exchange) server or the

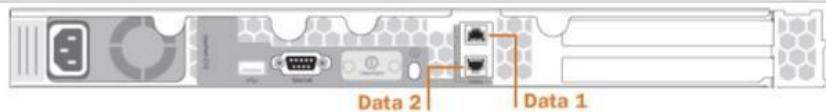
—next hop|| in the email delivery for our infrastructure.

Relaying Mail

When configuring the interfaces to relay mail, we define the systems allowed to relay email through the appliance. These are entries in the RELAYLIST of the Host Access Table for a listener. Mark the checkbox for Relay Outgoing Mail to configure the interface to relay mail. Enter the hosts that may relay mail through the appliance.

Interfaces

You must set up at least 1 interface and 1 interface must be configured to accept mail from the Internet.



Enable Data 2 Interface

This interface is typically used to accept and relay mail.

IP Address:	192.168.1.1									
Network Mask:	255.255.255.0									
Fully Qualified Hostname:	mail3.example.com <small>Fully qualified hostname for this appliance</small>									
Accept Incoming Mail:	<input checked="" type="checkbox"/> Accept mail on this interface									
<table border="1"> <thead> <tr> <th>Domain ?</th> <th>Destination</th> <th>Add Row</th> </tr> </thead> <tbody> <tr> <td>.example.com</td> <td>exchange.example.com</td> <td></td> </tr> <tr> <td>example: company.com</td> <td>i.e. An Exchange or Notes server</td> <td></td> </tr> </tbody> </table>		Domain ?	Destination	Add Row	.example.com	exchange.example.com		example: company.com	i.e. An Exchange or Notes server	
Domain ?	Destination	Add Row								
.example.com	exchange.example.com									
example: company.com	i.e. An Exchange or Notes server									
Relay Outgoing Mail:	<input checked="" type="checkbox"/> Relay mail on this interface									
<table border="1"> <thead> <tr> <th>System ?</th> <th>Add Row</th> </tr> </thead> <tbody> <tr> <td>exchange.example.com</td> <td></td> </tr> <tr> <td>example: company.com</td> <td></td> </tr> </tbody> </table>		System ?	Add Row	exchange.example.com		example: company.com				
System ?	Add Row									
exchange.example.com										
example: company.com										

Enable Data 1 Interface

This interface is typically used for system administration. (You are currently connected to this interface.)

IP Address:	192.168.42.42
Network Mask:	255.255.255.0
Fully Qualified Hostname:	mail.example.com <small>Fully qualified hostname for this appliance</small>
Accept Incoming Mail:	<input type="checkbox"/> Accept mail on this interface
Relay Outgoing Mail:	<input type="checkbox"/> Relay mail on this interface

Click Next to continue.

Step 4: Security

In step 4, you configure anti-spam and anti-virus settings. The anti-spam options include SenderBase Reputation Filtering and selecting an anti-spam scanning engine. For anti-virus, you can enable Virus Outbreak Filters and Sophos or McAfee anti-virus scanning.



Message Security

Your IronPort appliance uses message security to protect your email infrastructure from security threats. The security solutions are applied in the order depicted below. Each module reduces the overall volume of email sent to your infrastructure.



Anti-Spam	
SenderBase Reputation Filtering	<p><i>SenderBase Reputation Filtering provides a "first line of defense" against incoming spam by restricting access to your email infrastructure based on senders' trustworthiness as determined by their SenderBase Reputation Score (SBRS). More about SBRS...</i></p> <p><input checked="" type="checkbox"/> Enable SenderBase Reputation Filtering</p>
Anti-Spam Scanning	<p>Select the anti-spam engine to use for the default incoming mail policy:</p> <p><input type="radio"/> None <input checked="" type="radio"/> IronPort Anti-Spam <input type="radio"/> Symantec Brightmail</p>
Anti-Virus	
Sophos Anti-Virus Scanning:	<p><i>Sophos Anti-Virus provides best-of-breed anti-virus protection.</i></p> <p><input checked="" type="checkbox"/> Enable Sophos Anti-Virus Scanning</p>
Virus Outbreak Filters	<p><i>Virus Outbreak Filters quarantine suspicious messages even before traditional anti-virus security services have provided a signature file. More about Virus Outbreak Filters...</i></p> <p><input checked="" type="checkbox"/> Enable Virus Outbreak Filters</p>

[« Previous](#) [Cancel](#)

[Next »](#)

Click Next to continue.

Step 5: Review

A summary of the configuration information is displayed. You can edit the System Settings, Network Integration, and Message Security information by clicking the previous button or by clicking the corresponding Edit link in the upper-right of each section.



The IronPort appliance is now ready to send email.

Note — Clicking Install will cause the connection to the current URL (<http://192.168.42.42>) to be lost if you changed the IP address of the interface we used to connect to the appliance.

Review Your Configuration[Printable Page](#)

Please review your configuration. If you need to make changes, click the Edit button to return to the page you'd like to edit.

System Settings		Edit
Default System Hostname:	example.com	
Email System Alerts To:	admin@example.com	
Time Zone:	America/Los_Angeles	
NTP Server:	time.ironport.com	
Admin Password:	(hidden)	
SenderBase Network Participation:	Enabled	
AutoSupport:	Enabled	

Network Integration		Edit
Gateway:	192.168.0.1	
DNS:	Use the Internet's Root DNS servers	
Interfaces		
Data 1 Port		
IP Address:	192.168.1.1	
Network Mask:	255.255.255.0	
Fully Qualified Hostname:	mail3.example.com	
Accept Incoming Mail:	Domain .example.com	Destination exchange.example.com
Data 2 Port		
IP Address:	192.168.2.1	
Network Mask:	255.255.255.0	
Fully Qualified Hostname:	mail.example.com	
Relay Outgoing Mail:	System exchange.example.com	
Management Port		
IP Address:	192.168.42.42	
Network Mask:	255.255.255.0	
Fully Qualified Hostname:	mail.example.com	

Message Security		Edit
SenderBase Reputation Filtering:	Enabled	
Default Incoming Mail Anti-Spam Engine:	IronPort Anti-Spam	
Sophos Anti-Virus:	Enabled	
Virus Outbreak Filters:	Enabled	

[« Previous](#) [Cancel](#)[Install This Configuration](#)

Once you are satisfied with the information displayed click Install This Configuration. A confirmation dialog is displayed. Click Install to install the new configuration.

LDAP Integration

We must create an LDAP server profile to store the information about your LDAP server. To create an LDAP server profile,

1. On the System Administration > LDAP page, click Add LDAP Server Profile The Add LDAP Server Profile page is displayed:

LDAP Server Settings	
Server Attributes	
LDAP Server Configuration Name:	<input type="text"/>
Host Name(s):	<input type="text"/> <small>Separate multiple entries with commas.</small>
	Maximum number of simultaneous connections for all hosts: <input type="text" value="10"/> Multiple host options: <input checked="" type="radio"/> Load-balance connections among all hosts listed <input type="radio"/> Failover connections in the order listed
Port: <small>(?)</small>	<input type="text" value="3268"/>
Connection Protocol:	<input type="checkbox"/> Use SSL
Base DN: <small>(?)</small>	<input type="text"/>
Cache TTL (time-to-live):	<input type="text" value="900"/> Seconds
Maximum Retained Cache Entries:	<input type="text" value="10000"/>
Authentication Method:	<input checked="" type="radio"/> Anonymous <input type="radio"/> Use Password Username: <input type="text"/> Password: <input type="password"/>
Accept Query	
Not configured	
Routing Query	
Not configured	
Masquerade Query	
Not configured	
Group Query	
Not configured	
SMTP Authentication Query	
Not configured	

2. Enter a name for the server profile.
3. Enter the host name(s) for the LDAP server. We can enter multiple host names if we want to configure the LDAP servers for failover or load-balancing. Separate multiple entries with commas.
4. Enter a maximum number of simultaneous connections. If you configure the LDAP Profile for load-balancing, these connections are distributed among the listed LDAP servers (host names).
5. Enter a port number, and select whether to use SSL when communicating with the LDAP server. The default port is 3268. This is the default port for Active Directory that enables it to access the global catalog in a multi-server environment.
6. Enter a Base DN (distinguishing name) for the LDAP server and select an authentication method. If you authenticate with a user name and a password, the user name must include the full DN to the entry that contains the

password. For example, a user is a member of the marketing group with an email address of joe@MOC.gov.qa the entry for this user would look like the following entry:

dc=MOC dc=gov.qa

7. Enter cache time-to-live. This value represents the amount of time to retain caches.
8. Enter maximum retained cache entries.
9. Enter an authentication method. It should authenticate with AD username and password.

NOTE: The profile for this account must be created as no-expired password.

10. Click **Submit**. Click the **Commit Changes** button, add an optional comment if necessary, and then click **Commit Changes** to finish creating the LDAP server profile.

Important Note: This example uses the dummy information to configure. Please use the original credentials once we configure the box in live network.

IronPort Web Security Appliance

The Web Security appliance (WSA) is a robust, secure, efficient device that protects corporate networks against web-based malware and spyware programs that can compromise corporate security and expose intellectual property. The Web Security **appliance extends IronPort's SMTP security applications to include** protection for standard communication protocols such as HTTP, HTTPS, and FTP.

Malware (—malicious software||) is software designed to infiltrate or damage a computer system without the owner's consent. It can be any kind of hostile,

intrusive, or annoying software or program code. Web-based malware includes spyware, system monitors, adware, phishing and pharming techniques, keystroke (key) loggers, browser hijackers, trojan horses, and more.

Web-based malware is a rapidly growing threat, responsible for significant corporate downtime, productivity losses and major strains on IT resources. Additionally, companies run the risk of violating compliance and data privacy regulations if their networks become compromised by malware. Companies run the risk of expensive legal costs and exposure of intellectual property.

The best place to stop these threats from entering the network is right at the gateway. The Web Security appliance provides deep application content inspection, by offering a web proxy service and by monitoring layer 4 traffic. The Web Proxy and Layer 4 Traffic Monitor allow organizations to ensure breadth of coverage within their networks. The Web Security appliance provides a powerful web security platform to protect the organization against malware that is optimized for performance and efficacy.

Web Proxy

The S-Series Web Proxy supports the following security features:

- **Policy groups** — Policy groups allow administrators to create groups of users and apply different levels of category-based access control to each group.
- **IronPort URL Filtering Categories** — IronPort URL Filters allow we to configure how the appliance handles each Web transaction based on the URL category of a particular HTTP request.
- **Web Reputation Filters** — Reputation filters analyze web server behavior and characteristics to identify suspicious activity and protect against URL-based malware threats.
- **Anti-Malware Services** — **The IronPort DVS™ engine in combination with the Webroot™ and McAfee scanning engines identify and stop a broad range of web-based malware threats.**

Mode of Deployment

We can deploy the WSA in network in two different ways.

1. Explicit Forward Proxy. Client applications, such as web browsers, are aware of the Web Proxy and must be configured to point to a single Web Security appliance. This deployment requires a connection to a standard network switch. When we deploy the Web Proxy in explicit forward mode, we can place it anywhere in the network.

2. Transparent Proxy. Clients applications are unaware of the Web Proxy and do not have to be configured to connect to the proxy. This deployment requires an L4 switch or a WCCP v2 router.

MOC will deploy Transparent Proxy mode.

SYSTEM SETUP WIZARD

The IronPort AsyncOS for Web operating system provides a browser-based wizard to guide through initial system configuration. This System Setup Wizard prompts basic initial configuration, such as network configuration and security settings. The System Setup Wizard is located on the System Administration tab.

We must run the System Setup Wizard when we first install the Web Security appliance. After finish the System Setup Wizard, the appliance is ready to monitor web traffic. However, we may want to make more custom configurations to the appliance that the System Setup Wizard does not cover

Accessing the System Setup Wizard

To access the System Setup Wizard, open a browser and enter the IP address of the Web Security appliance. The first time we run the System Setup Wizard, use the default IP address:

<http://192.168.42.42>

The appliance login screen appears. Enter the username and password to access the appliance. By default, the appliance ships with the following username and password:

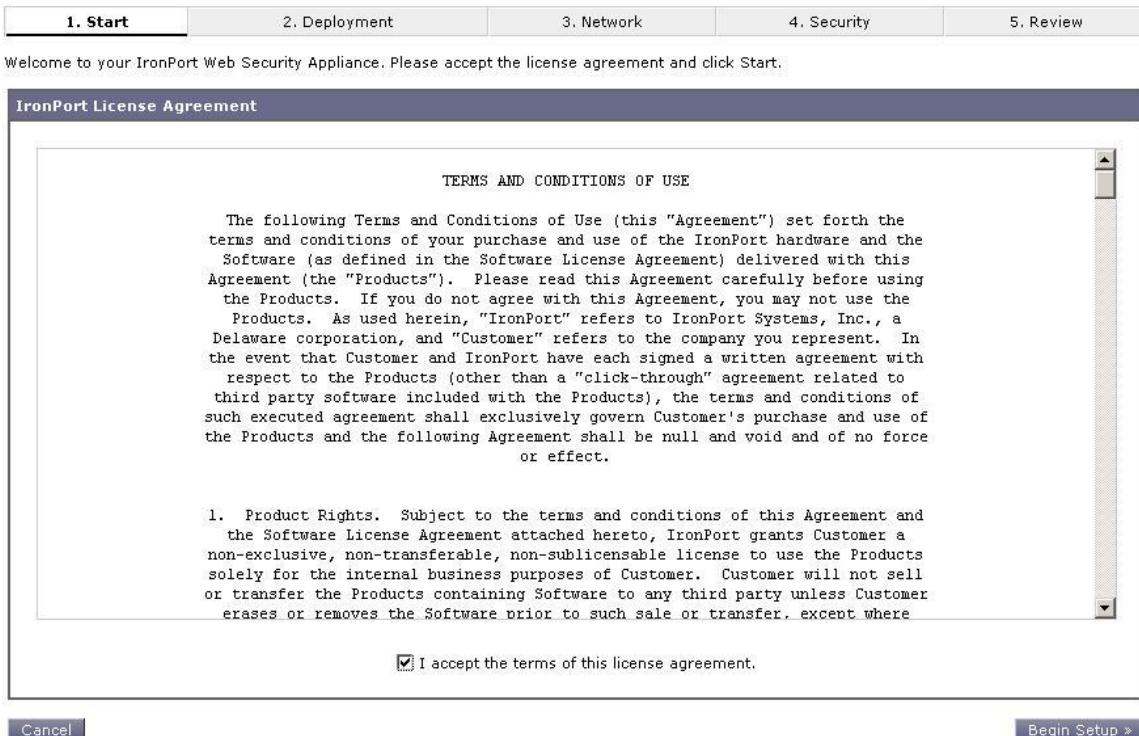
- Username: **admin**
- Password: **ironport**

Note — Wer session will time out if it is idle for over 30 minutes or if we close wer browser without logging out. If this happens, we must re-enter the username and password.

Step 1. Start

When we first start the System Setup Wizard, it displays an end user license agreement.

- Accept the terms of the agreement by clicking the check box at the bottom of the page.

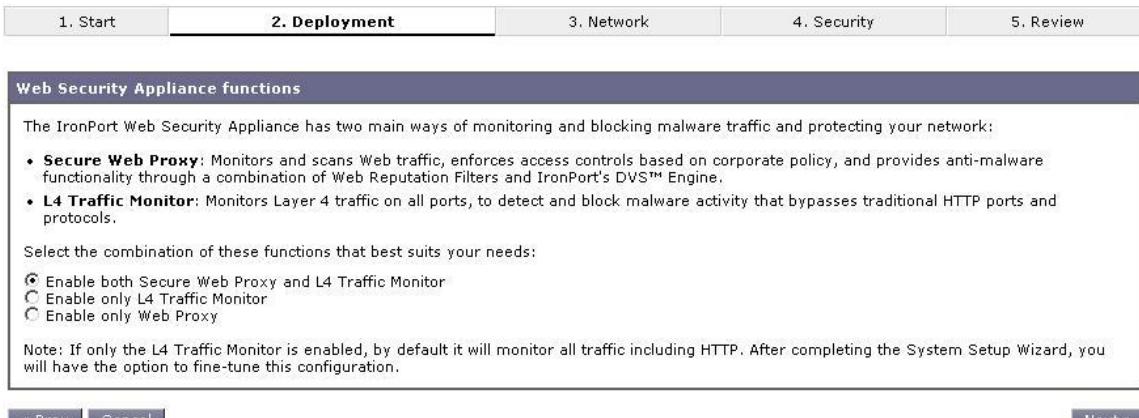


- Click Begin Setup to continue. The Deployment tab appears.

Step 2. Deployment

The System Setup Wizard continues to the Deployment tab. The Deployment tab contains multiple pages that prompt us to enter information.

- Verify that the Web Security Appliance Functions page appears.



- Choose the Web Security Appliance Functions options.

- 3.** Click Next.
- 4.** The Network Context page appears.

1. Start **2. Deployment** 3. Network 4. Security 5. Review

Network Context

Is there another web proxy in your network?

No other proxy
 Other proxy in Transparent mode
 Other proxy in Forward mode

Address: [] Port: [3128]

If another web proxy is present, the IronPort Web Security Appliance must be placed downstream of the existing proxy (closer to the client), as illustrated below:

Note: When another web proxy is present, the IronPort Web Security Appliance cannot be configured to perform authentication.

< Prev Cancel [Next >](#)

- 5.** Configure the Network Context options.

Note — When we use the Web Security appliance in a network that contains another proxy server, we must place the Web Security appliance downstream from the proxy server, closer to the clients.

- 6.** Click Next.

If we configured the Web Security appliance as a web proxy on the Web Security Appliance Functions page, then the Proxy Mode page appears

1. Start **2. Deployment** 3. Network 4. Security 5. Review

Proxy Mode

The following configurations can be used in your network context. Please select the option that best meets your needs:

IronPort Web Security Appliance in Transparent mode This configuration requires no changes to clients or the existing proxy. Use either a Layer 4 switch or a WCCP v2 Router to connect the IronPort Web Security Appliance to your network.

IronPort Web Security Appliance in Forward mode Use this configuration if you prefer to enable the IronPort Web Security Appliance selectively for specific clients. In a Forward mode deployment, you may also configure all clients through a client auto script.

< Prev Cancel [Next >](#)

- 7.** Configure the Proxy Mode options. As per the deployment scenario configure the proxy either in transparent mode or Forward mode.

- 8.** Click Next.

The Deployment Summary page appears.

1. Start	2. Deployment	3. Network	4. Security	5. Review
----------	----------------------	------------	-------------	-----------

Deployment Summary

You have selected the following deployment options for the IronPort Web Security Appliance:

**Secure Web Proxy and L4 Traffic Monitor
Transparent Mode**

To change the selected deployment options, use the Previous button to return to the applicable page. To proceed to network configuration, select Next.

[« Prev](#) [Cancel](#) [Next »](#)

8. Verify that the Deployment options are correct, and click **Next**. The Network tab appears.

Step 3. Network

On the Network tab, we can configure appliance system properties, such as the appliance hostname and time zone. The first page of the Network tab is the System Configuration page.

1. Verify that we are viewing the System Configuration page

1. Start	2. Deployment	3. Network	4. Security	5. Review
----------	---------------	-------------------	-------------	-----------

System Configuration

System Settings

Default System Hostname: ?	<input type="text" value="vmw-wsa06.qb"/> <small>e.g., proxy.company.com</small>
DNS Server(s):	<input type="radio"/> Use the Internet's Root DNS Servers <input checked="" type="radio"/> Use these DNS Servers: <input type="text" value="192.168.1.500"/> <small>(optional)</small> <input type="text"/> <small>(optional)</small>
NTP Server:	<input type="text" value="time.ironport.com"/>
Time Zone:	Region: <input type="button" value="GMT Offset"/> Country: <input type="button" value="GMT"/> Time Zone / GMT Offset: <input type="button" value="GMT"/>

[« Prev](#) [Cancel](#) [Next »](#)

2. Configure the System Configuration options. These options are Hostname, DNS servers IP address and NTP server or Time zone information
3. Click Next.
4. The Network Interfaces and Wiring page appears.
5. The Web Security appliance has network interfaces that are associated with the physical ports on the machine.

1. Start 2. Deployment **3. Network** 4. Security 5. Review

Network Interfaces and Wiring

Note: If the Management and Data interfaces are both configured, they must be assigned IP addresses on different subnets.

Management	Data	L4 Traffic Monitor
This interface is used to manage the appliance. Optionally, this interface may also handle Web Proxy monitoring and optional L4 Traffic Monitor blocking.	This interface may be used for Web Proxy monitoring and optional L4 Traffic Monitor blocking.	These interfaces are used for L4 Traffic Monitor data.
Ethernet Port: M1	Ethernet Port: P1	In Duplex mode, T1 receives incoming and outgoing traffic. In Simplex mode, T1 receives outgoing traffic and T2 receives incoming traffic.
IP Address: 192.168.1.115	IP Address: []	The L4 Traffic Monitor should always be deployed inside the firewall (before NAT) to capture real client IP addresses.
Network Mask: 255.255.255.0	Network Mask: []	Wiring Type: <input checked="" type="radio"/> Duplex TAP: T1 (In/Out)
Hostname: wsa01-vmw1-tpub.qa (e.g. wsa.example.com)	Hostname: [] (e.g. data.example.com)	<input type="radio"/> Simplex TAP: T1 (In) and T2 (Out)
<input type="checkbox"/> Use M1 port for management only		

« Prev Cancel Next »

6. Configure the Network Interfaces and Wiring options. Configure the M1 interface for monitoring the traffic and managing the device. According to the design perspective 10.3.180.49/28 and 10.3.180.50/28 are the IP address for two web proxies in MOC network.

7. Click Next.

The Routes for Management and Data Traffic page appears.

1. Start 2. Deployment **3. Network** 4. Security 5. Review

Routes for Management Traffic (Interface M1: 192.168.1.115)

Default Gateway: 192.168.1.1			
Static Routes Table			
Optionally, add static routes for Management access to the IronPort Web Security Appliance.			
Name	Destination Network	Gateway	<input type="button" value="Delete"/>
[]	[]	[]	<input type="button" value="Delete"/>
Identifying name for route	IP Address (such as 10.1.1.10) or CIDR (such as 10.1.1.0/24)	IP Address	<input type="button" value="Add Route"/>

Routes for Data Traffic (Interface P1: 192.168.2.115)

Default Gateway: 192.168.2.1			
Static Routes Table			
Optionally, add static routes for Data traffic. Depending on the appliance functions you enable, these routes will be used for monitoring by the Secure Web Proxy and optional blocking by the L4 Traffic Monitor.			
Name	Destination Network	Gateway	<input type="button" value="Delete"/>
[]	[]	[]	<input type="button" value="Delete"/>
Identifying name for route	IP Address (such as 10.1.1.10) or CIDR (such as 10.1.1.0/24)	IP Address	<input type="button" value="Add Route"/>

« Prev Cancel Next »

8. Configure the default gateway to routes the Management and Data Traffic. Here default gateway is 10.3.180.51/28 as SVI interface in Core switch.

9. Click Next.

When we configure the Web Security appliance as a web proxy in transparent mode and non-inline, we must connect it to a Layer 4 switch or a version 2 WCCP router. The Switch or Router Settings page appears.

When we configure the Web Security appliance as a web proxy in forward mode, the Switch or Router Settings page does not appear.

1. Start	2. Deployment	3. Network	4. Security	5. Review
----------	---------------	-------------------	-------------	-----------

Transparent Redirection Device Settings

When the IronPort Web Security Appliance is in transparent mode and non-inline, it must be connected via a Layer 4 switch or WCCP router.

Transparent Redirection Device:	<input type="radio"/> Layer 4 Switch <input checked="" type="radio"/> WCCP v2 Router
Note: If using a WCCP router, WCCP services must be configured after completing the System Setup Wizard (see Network > Transparent Redirection).	

[« Prev](#) [Cancel](#) [Next »](#)

8. Specify whether the appliance is connected to a Layer 4 switch or a version 2 WCCP router.

Note — If we connect the appliance to a version 2 WCCP router, we must configure the Web Security appliance to create WCCP services after running the System Setup Wizard.

9. Click Next.

The Administrative Settings page appears.

1. Start	2. Deployment	3. Network	4. Security	5. Review
----------	---------------	-------------------	-------------	-----------

Administrative Settings

Administrator Password:	Password: <input type="password"/> <small>***** Must be 6 or more characters</small> Confirm Password: <input type="password"/> <small>*****</small>
Email system alerts to:	<input type="text"/> admin@example.com <small>e.g. admin@company.com</small>
Send Email via SMTP Relay Host (optional): <small>(?)</small>	<input type="text"/> <small>i.e., smtp.example.com, 10.0.0.3</small> Port: <input type="text"/> <small>(?) optional</small>
AutoSupport:	<input checked="" type="checkbox"/> Send system alerts and weekly status reports to IronPort Customer Support

[« Prev](#) [Cancel](#) [Next »](#)

10. Configure the Administrative Settings options.

Option	Description
Administrator Password	Enter a password to access the Web Security appliance. The password must be six characters or more.
Email System Alerts To	Enter an email address for the account to which the appliance sends alerts.
Send Email via SMTP	We can enter a host name or address for an SMTP relay host that AsyncOS uses for sending system

generated

Mannai Confidential

Page
129

Relay Host	email messages. Optionally, we can enter the port number, too. If no port number is defined, AsyncOS uses port 25. If no SMTP relay host is defined, AsyncOS uses the mail servers listed in the MX record.
AutoSupport	Choose whether or not the appliance sends system alerts and weekly status report to IronPort Customer Support

11. Click **Next**.
The Security tab appears.

Step 4. Security

On the Security tab, we can configure which security services to enable, such as whether to block or monitor certain components. The Security tab contains one page.

- 1.** Verify that we are viewing the Security tab.

1. Start	2. Deployment	3. Network	4. Security	5. Review
----------	---------------	------------	--------------------	-----------

Security Services

Web Proxy

IP Spoofing: **Enable**
If an upstream proxy requires client IP addresses (for IP-based authentication or access control), enable IP spoofing. If using a WCCP router, configure an additional service to redirect based on source port (return path).

L4 Traffic Monitor

Action: **Monitor only**
 Block

URL Filtering

IronPort URL Filtering: **Enable**
The Global Web Filtering Policy will be initially configured to monitor all pre-defined categories.

Web Reputation

Web Reputation Filters: **Enable**
The Global Web Filtering Policy will be initially configured to use Web Reputation Filtering.

IronPort DVS™ Engine

Malware and Spyware Scanning: **Enable Webroot** **Enable McAfee**
The Global Web Filtering Policy will be initially configured to apply the actions configured below.

Action for Detected Malware: **Monitor only**
 Block

Action for Unscannable Transactions: **Monitor only**
 Block

SenderBase Network Participation

Network Participation: **Allow IronPort to gather anonymous statistics on HTTP requests and report them to IronPort in order to identify and stop web-based threats.**

Participation Level: **Limited - Summary URL information.**
 Standard - Full URL information. (Recommended)

Learn what information is shared...

2. Choose the Security Services options.

Option	Description
Web Proxy	<p>Choose whether or not to enable IP spoofing. Enable this option when a proxy server upstream in the network requires client IP addresses. This option only appears when on the Network Context page we specify that the network has an existing proxy. If we connect the appliance to a WCCP v2 router, we must create at least one WCCP service that redirects traffic based on the source port.</p>
L4 Traffic Monitor	<p>Choose whether the Layer-4 Traffic Monitor should monitor or block level 4 traffic. The L4 Traffic Monitor detects rogue traffic across all network ports and stops malware attempts to bypass port 80. We might choose to monitor traffic when we evaluate the Web Security appliance, and block traffic when we purchase and use the appliance.</p>
URL Filtering	<p>Choose whether or not to enable URL filtering. IronPort URL Filters allow us to control user access based on the category of a particular HTTP request. Enable this option when we want to restrict users from accessing particular types of websites.</p>
Web Reputation	<p>Choose whether or not to enable Web Reputation filtering for the Global Policy Group. When we create custom web access policy groups, we can choose whether or not to enable Web Reputation filtering. IronPort Web Reputation Filters is a security feature that analyzes web server behavior and assigns a reputation score to a URL to determine the likelihood that it contains URL-based malware. Enable this option when</p>

	we want to identify suspicious activity and stop malware attacks before they occur.
IronPort DVS Engine	Choose whether or not to enable malware and spyware scanning using Webroot or McAfee. If enabled, also choose whether to monitor or block detected malware, and whether to monitor or block unscannable transactions. We might choose to monitor malware and/or

	unscannable transactions when we evaluate the Web Security appliance, and block them when we purchase and use the appliance. We can further configure malware scanning after we finish the System Setup Wizard
SenderBase Network Participation	Choose whether or not to participate in the SenderBase Network. If we participate, we can configure limited or full participation. The SenderBase Network is a threat management database that tracks millions of domains around the world and maintains a global watch list for Internet traffic. When we enable SenderBase Network Participation, the Web Security appliance sends anonymous statistics about HTTP requests to IronPort to increase the value of SenderBase Network data.

3. Click Next.
The Review tab appears.

Step 5. Review

The last tab of the System Setup Wizard displays a summary of the configuration information we chose. We can edit any of the configuration options, such as Network Settings or Deployment, by clicking the **Edit** button for each section.

1. Verify that we are viewing the Review tab.

Mannai Confidential
132

Page

1. Start

2. Deployment

3. Network

4. Security

5. Review**Review Your Configuration**[Printable Page](#)

Please review your configuration. If you need to make changes, click the Previous button to return to the previous page.

Deployment[Edit](#)

Web Security Appliance Functions:	L4 Traffic Monitor and Secure Web Proxy
Network Context:	No upstream proxy
Secure Web Proxy Mode:	Transparent

Network Settings[Edit](#)

Default System Hostname:	wsa01-vmw1-tpub.qa
DNS Servers:	192.168.1.500
Network Time Protocol (NTP):	time.ironport.com
Time Zone:	Etc/GMT-8

Interfaces[Edit](#)**Management (M1)**

IP Address:	192.168.1.115
Network Mask:	255.255.255.0
Hostname:	wsa01-vmw1-tpub.qa
Use M1 port for management only:	No

L4 Traffic Monitor:

Wiring Type:	Duplex TAP: T1 (In/Out)
--------------	-------------------------

Routes[Edit](#)

Default Gateway:	192.168.1.1
Static Routes:	No static routes have been defined.

Transparent Redirection[Edit](#)

Transparent Redirection Device Type:	WCCP v2 Router Note: WCCP services must be configured after completing the System Setup Wizard (see Network > Transparent Redirection)
--------------------------------------	--

Administrative Settings[Edit](#)

Administrator Password:	(hidden)
Email System Alerts To:	admin@example.com
Internal SMTP Relay Hosts:	No internal relay host is defined
AutoSupport:	Yes

Security Services[Edit](#)

Secure Web Proxy:	IP spoofing not enabled
L4 Traffic Monitor:	Monitoring
URL Filtering:	Enabled
Web Reputation Filters:	Enabled
IronPort DVS™ Engine:	Webroot: Enabled McAfee: Enabled
SenderBase Network Participation:	Yes

[« Previous](#)[Cancel](#)[Install This Configuration](#)

2. Review the configuration information. If we need to change an option, click the **Edit** button for that section.

3. Click **Install This Configuration** after we confirm the configuration is correct. The Web Security appliance applies the configuration options we selected.

If we changed the Management interface IP address from the current value, then clicking **Install This Configuration** will cause the connection to the current URL to be lost.

Proxy Authentication

The Web Security appliance integrates web access with an authentication framework. When we enable authentication, the Web Security appliance authenticates clients on the network before allowing them to connect to a destination server.

The Web Security appliance supports the following authentication protocols:

- **Lightweight Directory Access Protocol (LDAP).** The appliance supports standard LDAP server authentication and secure LDAP authentication. We can use a Basic authentication scheme
- **NT Lan Manager (NTLM).** The appliance supports NTLM to enable authentication

between the appliance and a Microsoft Windows domain controller. We can use either NTLMSSP or Basic authentication schemes

To enable authentication, we must create at least one authentication realm.

An authentication realm is a set of authentication servers (or a single server) supporting a single authentication protocol with a particular configuration

When we create more than one realm, we can group the realms into an authentication sequence. An authentication sequence is a group of authentication realms listed in the order the Web Security appliance uses for authenticating clients. By creating authentication realms and sequences, we can configure the Web Security appliance to use one or more authentication servers for authenticating clients on the network.

After creating an authentication realm and possibly a sequence, too, we can create or edit policy groups based on authentication realms or sequences. Note, however, that if we delete an authentication realm or sequence, any policy group that depends on the deleted realm or sequence becomes disabled

WORKING WITH AUTHENTICATION REALMS

We create, edit, and delete authentication realms on the Network > Authentication page under the Authentication Realms section

Authentication

The screenshot shows the 'Authentication Realms' configuration page. At the top, there is a button labeled 'Add Realm...'. Below it, a message states 'No authentication realms have been defined.' In the center, there is a table titled 'Global Settings' with the following rows:

Global Settings	
Transparent Authentication Type:	Cookie
Authentication Timeout:	300 seconds
Action if Authentication Service Unavailable:	Block all traffic if authentication fails
Authentication Cache (Basic Only):	Cache TTL: 3600 seconds Cache Size: 8192 entries

At the bottom right of the table, there is a link labeled 'Edit Global Settings...'.

AUTHENTICATING USING NTLM

The NT Lan Manager (NTLM) authenticates users with an encrypted challenge-response sequence that occurs between the appliance and a Microsoft Windows domain controller. The NTLM challenge-response handshake occurs when a web browser attempts to connect to the appliance, and before data is delivered.

When we configure an NTLM authentication realm, we do not specify the authentication scheme. Instead, we choose the scheme at the web access policy group level when we configure the policy member definition. This allows us to choose different schemes for different policy groups. When we create or edit the policy group, we can choose one of the following schemes:

- Use NTLMSSP
 - Use Basic or NTLMSSP
 - Use Basic
-

NTLM Authentication Settings

The following table describes the authentication settings we define when we choose NTLM authentication.

Setting	Description
Active Directory Server	<p>Enter the Active Directory server IP address or host name. We can specify up to three servers. The hostname must be a fully-qualified domain name. For example, ntlm.MOC.com.qa An IP address is required only if the DNS servers configured on the appliance cannot resolve the Active Directory server hostname.</p> <p>Note: When multiple authentication servers are configured in the realm, the appliance attempts to authorize with up to three authentication servers before failing to authorize the transaction within this realm.</p>
Active Directory Account	<p>Enter the following Active Directory account information:</p> <ul style="list-style-type: none"> · Active Directory server domain name. · NetBIOS domain name. · Computer account location. <p>Note: We must click Join Domain to enter an Active Directory username and password.</p>
(Active Directory User)	<p>When we click Join Domain, enter the name and password for the Active Directory user. If the appliance and the Active Directory server are in the same domain, any valid user that is a member of User Domain is allowed. However, depending on the Active Directory server configuration, this user might need Domain Admin Group or Enterprise Admin Group credentials. For example:</p> <ul style="list-style-type: none"> · If the appliance and the Active Directory server are not in the same domain, the Active Directory user must be a member of the DomainAdmin Group.

	<ul style="list-style-type: none"> If the Active Directory server configuration is a forest, the Active Directory user must be a member of the Enterprise Admin Group.
Network Security	Configure whether or not the Active Directory server is configured to require signing. When we enable this check box, the appliance uses Transport Layer Security (TLS) when communicating with the Active Directory server.

Edit Realm

NTLM Authentication Realm

Realm Name:	ad2
Authentication Protocol and Scheme(s): NTLM (NTLMSSP or Basic Authentication)	
NTLM Authentication	
Active Directory Server:	Specify up to three Active Directory servers: example.com [empty field] [empty field] hostname or IP address
Active Directory Account:	Active Directory Domain: ? WSA NetBIOS Domain: ? WSA Computer Account ? Location: Computers (Example: Computers/BusinessUnit/Department/Servers) <i>Status: Computer account wsa01-vmw1-tpub\$ not yet created.</i>
Network Security:	<input type="checkbox"/> Client Signing Required
Test Current Settings	
Test Authentication Realm Settings:	<input type="button" value="Start Test"/>

When we click **Join Domain**, we are prompted to enter login credentials for the Active Directory server. The login information is used only to create the Active Directory computer account and is not saved. Enter the login information and click

Create Account.

Note — We must enter the sAMAccountName user name for the Active Directory user. Also, verify that users enter their sAMAccountName user name when they log in to their computers. Once an account is created, the status of the account creation is displayed below the Join Domain button. If the account creation fails, the status and reason for error is displayed. Also, when we view all realms on the Network > Authentication page, the appliance displays warning text in red saying that the domain was not joined for any realm that did not create a computer account.

Authentication

Authentication Realms

Authentication Realms					
<input type="button" value="Add Realm..."/>					
Realm Name	Protocol	Scheme(s)	Servers	Base DN or NetBIOS Domain	Delete
ad2	NTLM	NTLMSSP or Basic	ad2.wga	Domain WGA not joined	
sunone	LDAP	Basic	sunone.qa	ou=raptor-qa,dc=qa	

Note — AsyncOS only creates an Active Directory computer account when we edit the authentication realm Active Directory information or when the appliance reboots.

Cisco Secure ACS

Initial Configuration of ACS

Connect a console to the serial console port on the back panel: (Attach a DB-9 to RJ-45 adapter (provided) to the serial port of the console).

Power on ACS SE and the console, and open the terminal emulation communication software with following settings:

Baud = 115200

Databits = 8

Parity = N

Stops = 1

Flow control = None

Terminal emulation type =

ANSI The login prompt will appear.

(We need to configure the ACS SE when we boot the system for the first time, and whenever we re-image the system.)

Step 1 Establish a serial console connection to the ACS SE; for details see [establishing a Serial Console Connection](#).

Step 2 Confirm that the following information appears above the login prompt [Cisco Secure ACS: \[version number\]](#)

[Appliance Management Software: \[version number\]](#) [Appliance Base Image: \[version number\]](#)

[SA builds \[version number\]: \(Patch: \[version number\]\)](#) [Status: Appliance is functioning properly](#)

[The ACS Appliance has not been configured.](#)

[Logon as "Administrator" with password "setup" to configure appliance.](#)

Step 3 login: Administrator

Step 4 password:

[setup Initialize](#)

[Appliance.](#)

Machine will be rebooted after initialization.

Entering Ctrl-C before setting appliance name will shutdown the appliance

Step 5 ACS Appliance name [deliverance1]: moc-

acs-01 ACS Appliance name is set to moc-acs-01.

Step 6 DNS domain []:

moc.gov.qa DNS name is set to

moc.com.qa

You need to set the administrator account name and password.

Step 7 Enter new account name: acsadmin

Step 8 Enter new password:cisco@moc

Step 9 Enter new password again:

cisco@moc Password is set successfully.

Administrator name is set to acsadmin.

Step 10 The following prompt appears for the new database

password: Please enter the Encryption Password for the

Configuration Store.

Please note this is different from the administrator account, it is used to encrypt the Database.

Step 11 Enter new password: cisco123

Step 12 Enter new password

again:cisco123 Password is set

successfully

Step 13 would you like to add GUI Administrator

now? : Y Enter new GUI administrator name:

webadmin

Enter new password: cisco@moc

Enter new password again:

cisco@moc GUI Administrator

added successfully.

Step 14 Use Static IP Address [Yes]: Y

IP Address [xx.xx.xx.xx]: 10.200.0.11

Subnet Mask [xx.xx.xx.xx]:

255.255.255.192 Default Gateway

[xx.xx.xx.xx]: 10.200.0.1

DNS Servers [xx.xx.xx.xx]: 10.200.1.6

10.200.1.7 IP Address is reconfigured.

Confirm the changes? [Yes]: Y

New ip address is set to

10.200.0.11 Default gateway is

set to 10.200.0.1

DNS servers are set to: 10.200.1.6

10.200.1.7 Accept network setting: Y

The IP address for the appliance will be

set. Test network connectivity [Yes]: Y

Enter hostname or IP address: Enter the IP address of the WLC and Active Directory to

verify the connectivity.

If successful, the system displays the ping statistics and displays the Test network connectivity prompt.

If you don't want to continue the ping test Enter (Test network connectivity [Yes]: N)

Step 15 If the settings appear correctly, Accept network setting

[Yes]: Y. Current Date Time Setting:

Time Zone: (GMT -xx:xx) XXX Time

Date and Time: mm/dd/yyyy

NTP Server(s): NTP Synchronization Disabled.

Step 16 To set the time and date of the ACS SE, at the Change Date & Time Setting [N]:

prompt, enter Y, and press Enter

The console displays a numbered list of time zones.

Step 17 At the Enter desired time zone index (0 for more choices): prompt, enter the

index number of the appropriate time zone for your geography and, press Enter.

The console displays the new time zone.

Step 20 At the Synchronize with NTP server? [N]: prompt, do one of the following:

To set the time manually, enter N, and press Enter.

Step 21 At the Enter date [mm/dd/yyyy]: prompt, enter the date in the given format, and

press Enter.

Step 22 At the Enter time [hh:mm:ss]: prompt, enter the current time in the given format,

and press Enter.

Initial configuration is successful. Appliance will now reboot.

The system reboots.

After the above mentioned configuration steps, system will be rebooted and will be ready for service provisioning. Login to the ACS GUI through a web browser with the URL <http://<ACS IP Address>:2002>.

Adding local user account in ACS.

Click User Setup tab and fill the user account details

MOC Low Level Design

CiscoSecure ACS - Microsoft Internet Explorer

User Setup

User: acstest

Account Disabled

Supplementary User Info

Real Name
Description acs local user

User Setup

Password Authentication: ACS Internal Database
CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password Confirm Password
 Separate (CHAP/MS-CHAP/ARAP)

Submit Delete Cancel

Help

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

Account Disabled Status

http://192.168.200.195:23672/users/sh_edit_help_page.htm#Advanced_Settings

CiscoSecure ACS - Microsoft Internet Explorer

User Setup

Separate (CHAP/MS-CHAP/ARAP)
Password Confirm Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned: ACS Network Group

Callback

Use group setting
 No callback allowed
 Callback using this number
 Dialup client specifies callback number
 Use Windows Database callback settings

Client IP Address Assignment

Use group settings
 No IP address assignment

Submit Delete Cancel

Help

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

Account Disabled Status

Applet dialup_filter started

MOC Low Level Design

Select the ACS group which user belongs to.

CiscoSecure ACS - Microsoft Internet Explorer

User Setup

Use group settings
No IP address assignment
Assigned by dialup client
Assign static IP address []
Assigned by AAA client pool
[]

Advanced Settings

Network Access Restrictions (NAR)

Shared Network Access Restrictions
Only Allow network access when
All selected NARs result in permit
Any one selected NAR results in permit

NARs Selected NARs
[] []
[>>] [>] [<] [<<]
Submit Delete Cancel

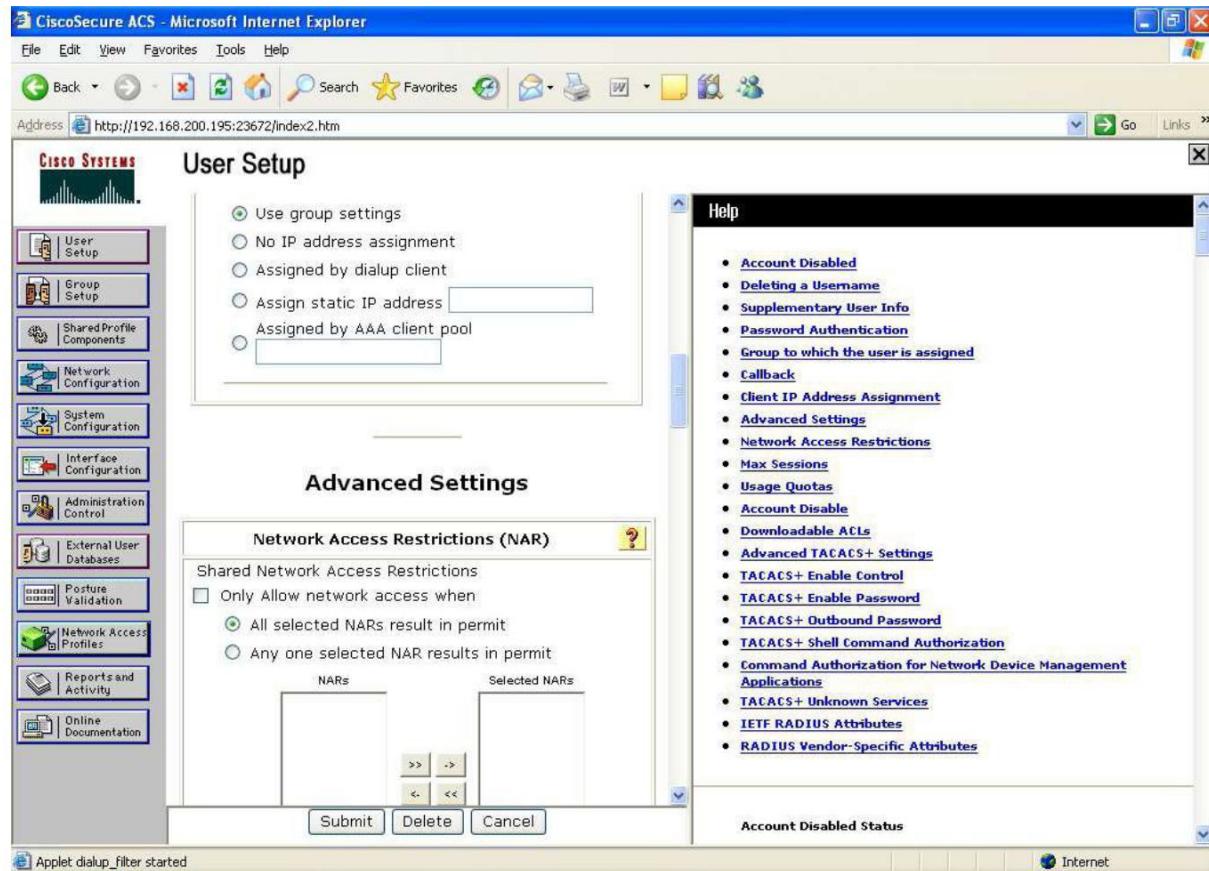
Help

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

Account Disabled Status

Applet dialup_filter started

Internet



CiscoSecure ACS - Microsoft Internet Explorer

User Setup

Max Sessions

Sessions available to user
Unlimited
1
Use group setting

User Usage Quotas

Use group settings
Use these settings
Limit user to [] hours of online time per Day
Limit user to [] sessions per Day

Current Usage

	Day	Week	Month	Absolute
Online time	00:00	00:04	00:04	00:04
Sessions	0	3	3	3

[] On submit reset all usage counters

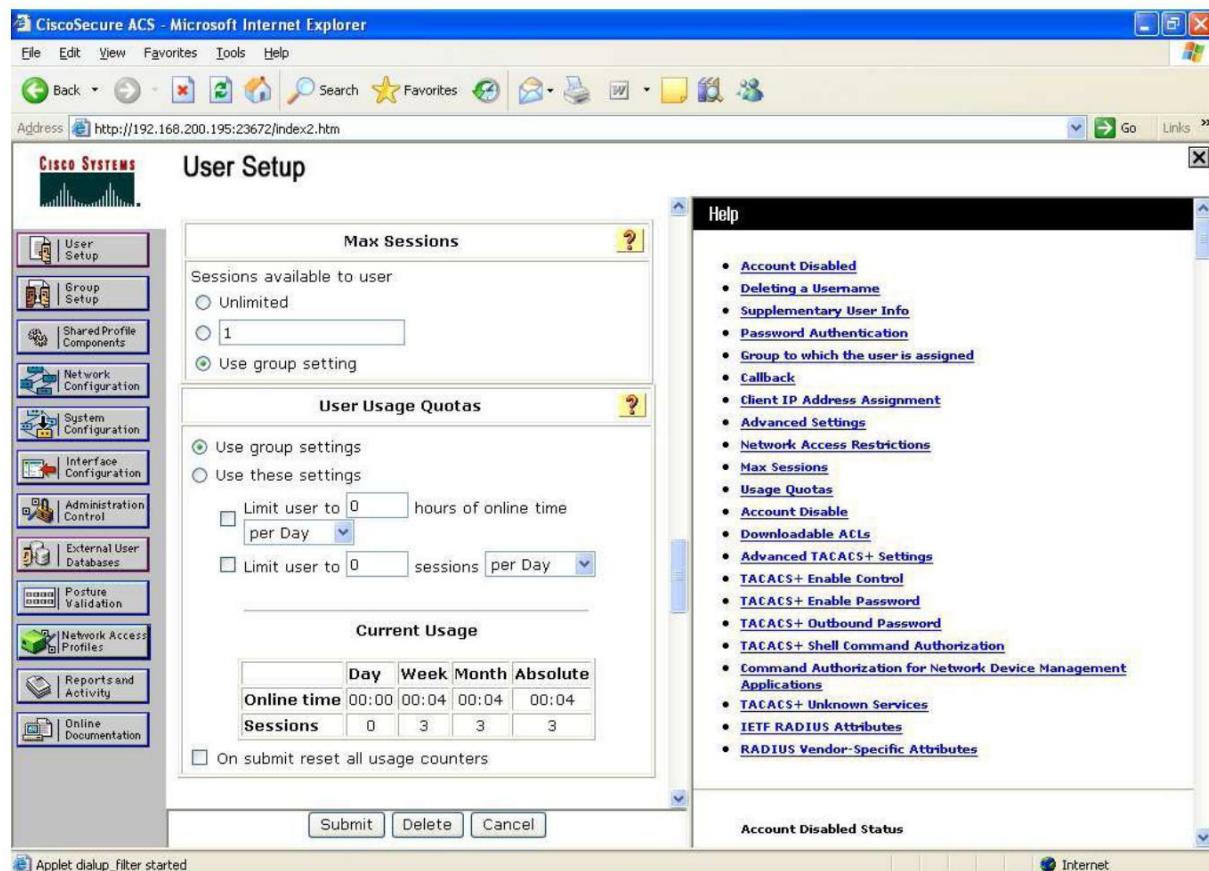
Help

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

Account Disabled Status

Applet dialup_filter started

Internet



You can configure the above settings for individual user or allow inheriting from the group settings as above.

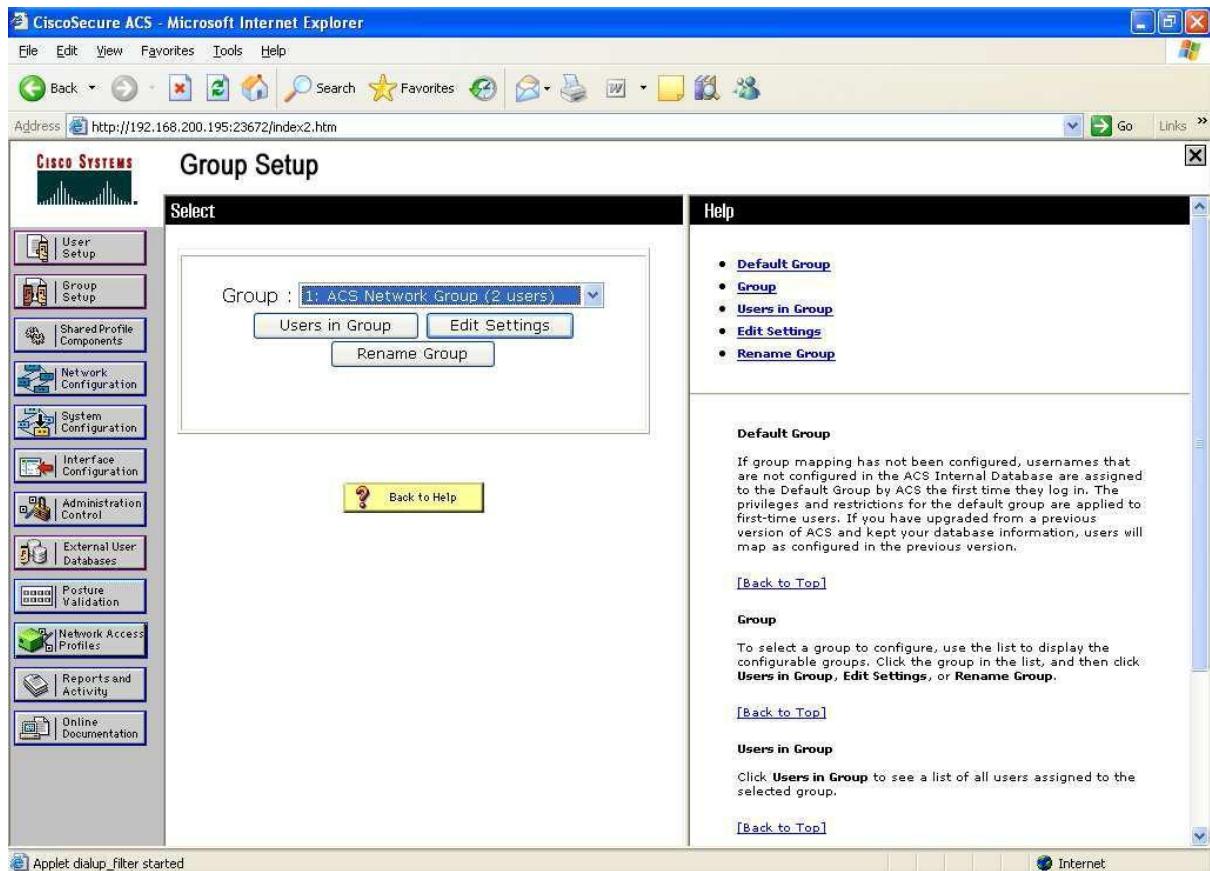
If we need MAC address based authentication for wireless users, we need to create user accounts with username=MAC address and password=MAC address. This is illustrated in below screen captures.

The screenshot shows the 'User Setup' page in Mozilla Firefox. The URL is <http://192.168.200.3:14234/index2.htm>. The left sidebar has a 'User Setup' icon. The main area shows a search bar with 'User: 001dfd5c390e' and buttons for 'Find' and 'Add/Edit'. Below it is a list titled 'List users beginning with letter/number:' with a grid of letters and numbers. Buttons for 'List all users' and 'Remove Dynamic Users' are at the bottom. A 'Back to Help' link is at the bottom right. The right panel contains a 'Help' section with links for 'User Setup and Internal User Databases' and 'External User Databases'.

The screenshot shows the 'User Setup' page in Mozilla Firefox, specifically the 'Edit' screen for a user account. The URL is <http://192.168.200.3:14234/index2.htm>. The left sidebar has a 'User Setup' icon. The main area shows a 'User: 001dfd5c390e' header with an 'Account Disabled' checkbox. Below it is a 'Supplementary User Info' section with fields for 'Real Name', 'Person's name', 'Description', and 'Model'. The 'Person's name' field is highlighted with a red oval. The right panel contains a 'Help' section with a large list of configuration options under 'User Setup'.

Group Setup

Click on ‘Group Setup’ tab and selects ‘Edit Settings’ option (to change the name of the group use Rename Group tab)



Leave the default settings if there is no specify settings required.

Network Configuration

Create a Network Device Group and give a name

The screenshot shows a Microsoft Internet Explorer window titled "CiscoSecure ACS - Microsoft Internet Explorer". The address bar shows the URL <http://192.168.200.195:4572/index2.htm>. The main content area is titled "Network Configuration" and "Select". A sub-section titled "New Network Device Group" is displayed. It contains fields for "Network Device Group Name" (set to "QG2-TSF") and "Shared Secret" (set to "XXXXX"). Below this, a section titled "RADIUS Key Wrap" is shown with fields for "Key Encryption Key" and "Message Authenticator Code Key". The "Key Input Format" is set to "ASCII". At the bottom are "Submit" and "Cancel" buttons, and a "Back to Help" link.

Network Configuration

Select

New Network Device Group

Network Device Group Name: QG2-TSF

Shared Secret: XXXXX

RADIUS Key Wrap

RADIUS Key Wrap

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format: ASCII Hexadecimal

Submit Cancel

Back to Help

Click Add Entry button under Network Device Group to add new device group.

System Configuration

Click on System Configuration tab and make sure that host name, domain name and time zone settings are configured correctly.

Appliance Configuration

Name Configuration

The Name and Domain values will only be updated if reboot is selected

Host Name: c1113_scas2
Domain Name: qatargas.com.qa

Local Date/Time Configuration

Time Zone: (GMT+03:00) Kuwait, Riyadh

Time: 16:18:12
Day: 19
Month: November
Year: 2007

NTP Synchronization Enabled
NTP Server(s): 192.168.200.2

Submit, Reboot, Shutdown, Cancel

Help

- [Name Configuration](#)
- [Local Date/Time Configuration](#)
- [Cisco Secure Agent](#)
- [SNMP Agent](#)
- [Reboot](#)
- [Shutdown](#)

This page enables you to configure name, domain, date, and time settings and the SNMP Agent settings for the ACS Solution Engine.

Name Configuration

You can specify the hostname of the ACS Solution Engine and the domain to which it belongs. If you change either of these options, you must reboot the ACS Solution Engine.

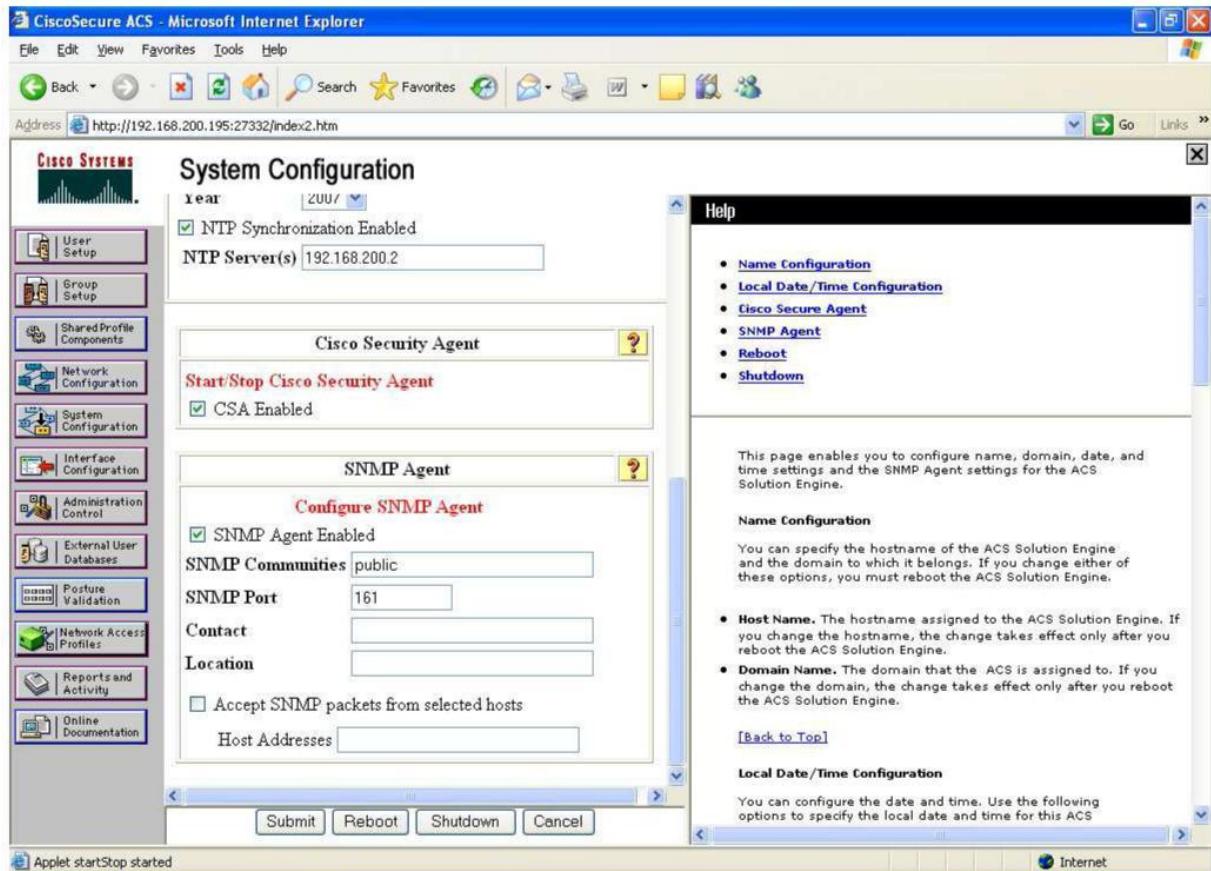
- Host Name.** The hostname assigned to the ACS Solution Engine. If you change the hostname, the change takes effect only after you reboot the ACS Solution Engine.
- Domain Name.** The domain that the ACS is assigned to. If you change the domain, the change takes effect only after you reboot the ACS Solution Engine.

[\[Back to Top\]](#)

Local Date/Time Configuration

You can configure the date and time. Use the following options to specify the local date and time for this ACS

Give the NTP server details.



Adding AAA Clients on ACS

In order to authenticate users on your network device, the device has to be added as AAA client and required AAA commands to be added on the devices and ACS has to be added as RADIUS or TACACAS+ protocol with pre-shared key. Following steps explain adding network device as AAA client.

1. Create a Network Device Group

Network Configuration _ Click Add Entry under Network Device Group

New Network Device Group

RADIUS Key Wrap

Network Device Group Name

To add a new Network Device Group (NDG), enter a name for the group and a shared secret. You can also enter shared keys for EAP-TLS authentication; then click Submit. Names can consist of any combination of numbers, letters, or symbols. You can also assign users to an NDG at the group level.

Shared Secret

Enter a shared secret key for the Network Device Group. Each device that is assigned to the Network Device Group, will use the shared key entered here. The key that was assigned to the device when it was added to the system is ignored. If the key entry is null, the AAA client key is used. This feature simplifies key management for devices. Maximum length for the NDG key is 32 characters.

RADIUS Key Wrap

Enter the shared secret keys for RADIUS Key Wrap in EAP-TLS authentications. Each key must be unique, and must also be distinct from the RADUIS shared key. These shared keys are configurable for each AAA Client, as well as for each NDG. The NDG

2. Add network device as AAA client

Network Configuration _ Click the Network Device Group name Network Device Groups

Network Configuration

Help

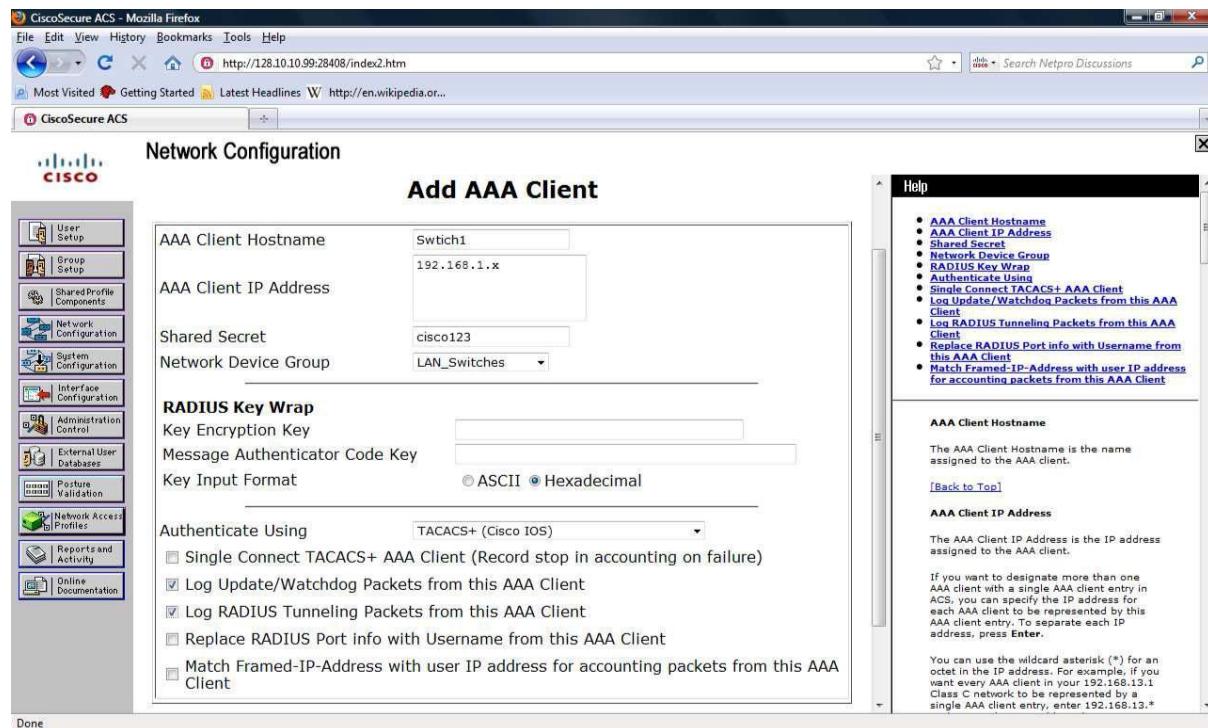
- Network Device Groups
- Adding a Network Device Group
- Renaming a Network Device Group
- Deleting a Network Device Group
- Searching for Network Devices
- AAA Clients
- Adding a AAA Client
- Editing a AAA Client
- Deleting a AAA Client
- AAA Servers
- Adding a AAA Server
- Editing a AAA Server
- Deleting a AAA Server
- Remote Agents
- Adding a Remote Agent
- Editing a Remote Agent
- Deleting a Remote Agent
- Proxy Distribution Table
- Adding a Proxy Distribution Table Entry
- Sorting Proxy Distribution Table Entries
- Editing a Proxy Distribution Table Entry
- Deleting a Proxy Distribution Table Entry

Note: This page changes depending your interface configuration. If you are using Network Device Groups (NDGs), after you click Network Configuration in the navigation bar, only the Network Device Groups table and Proxy Distribution Table information appear. In this case, site notes using NDGs, the AAA Clients table and the AAA Servers table appear in place of the Network Device Groups table.

Network Device Groups

Network device groups are collections of AAA clients and AAA servers. You can assign AAA clients and AAA servers to the network device groups you create. AAA clients and AAA servers not assigned to a particular NDG are, by default, assigned to the hot

3. Click Add Entry under LAN Switches AAA Client give the Client Hostname, IP address and Shared secret key and select your device group in the Network Device Group



Configure Remote Agent

Cisco ACS Solution Engine (SE) requires to add Remote Agent in the ACS SE in order to integrate with external database. The Remote Agent has to be installed on one of the member servers or Domain Controller and required to do the necessary setting in order to pass the user request to Active Directory. Following URL explains the required configuration on member server or domain controller that you install CRA.

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_se/r_for_solution_engine/4.2/installation/guide/remote_agent/rawi.html

Please make sure to install the correct CRA according to the ACS software version. Following steps explain on adding CRA on ACS.

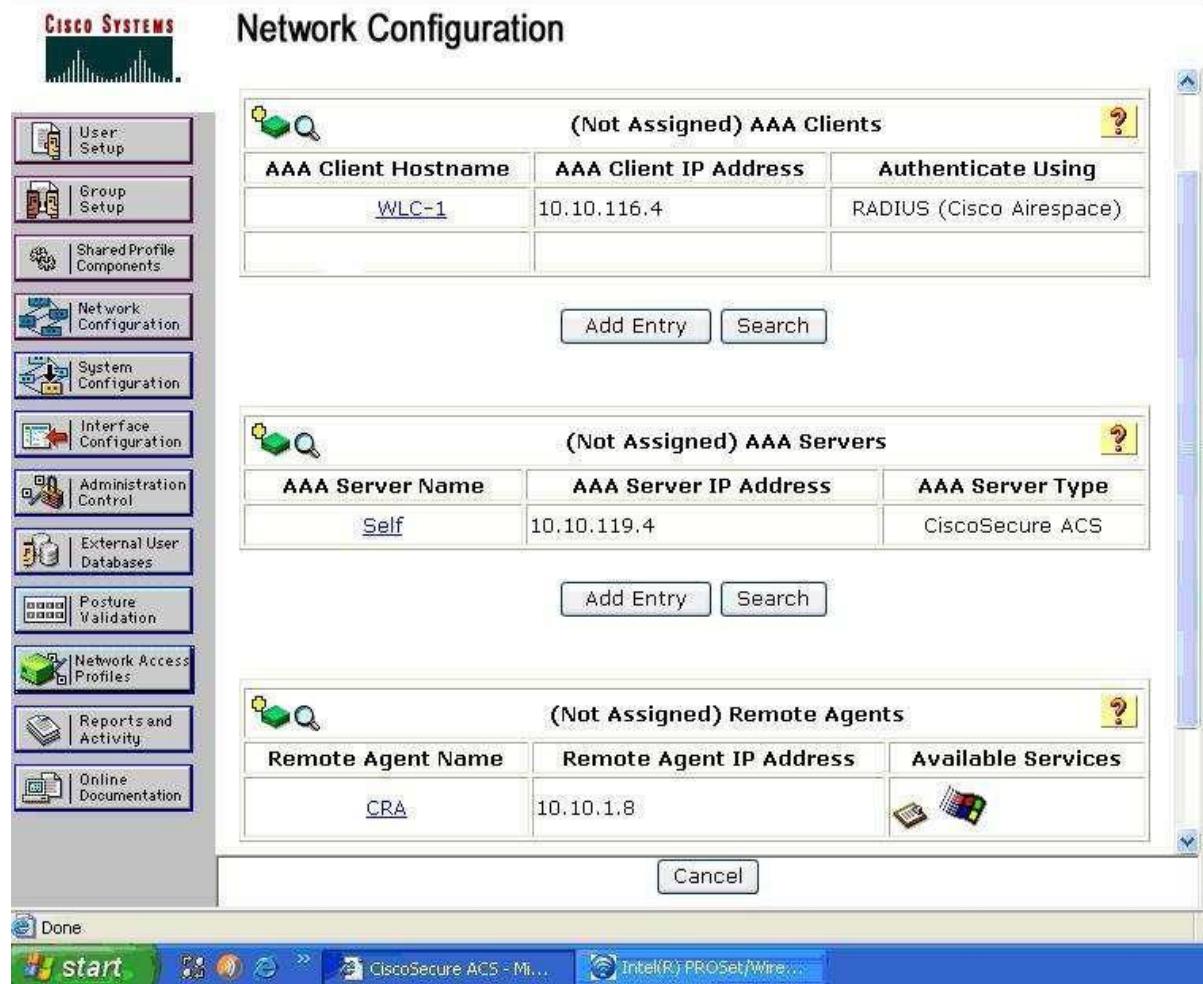
1. Click Network Configuration _ Select any Network Device Group and click Add Entry under Remote Agent section.

The screenshot shows the CiscoSecure ACS - Mozilla Firefox interface. The main window displays three tables under the 'Network Configuration' section:

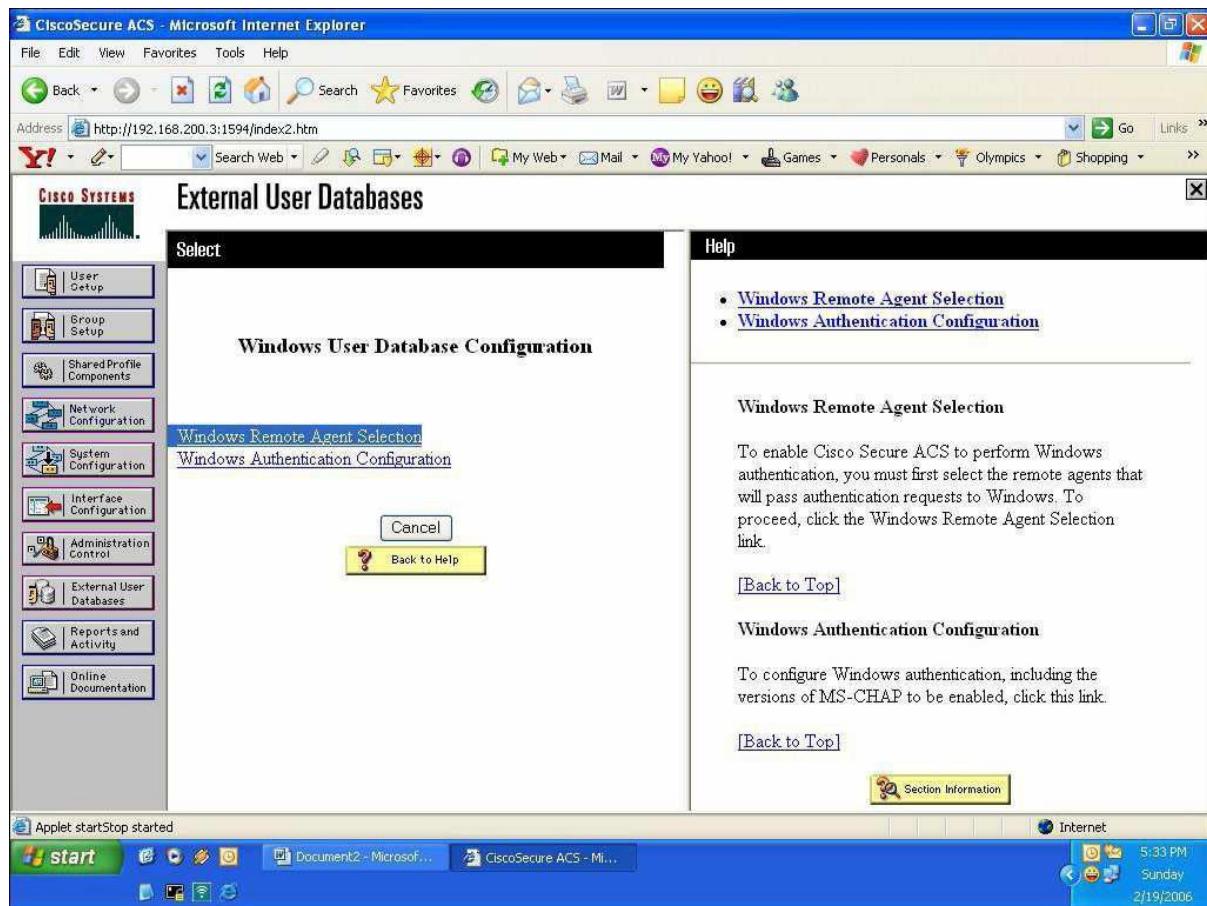
- (Not Assigned) AAA Clients:** Columns: AAA Client Hostname, AAA Client IP Address, Authenticate Using. Row: None Defined.
- (Not Assigned) AAA Servers:** Columns: AAA Server Name, AAA Server IP Address, AAA Server Type. Row: Self, 127.0.0.1, CiscoSecure ACS.
- (Not Assigned) Remote Agents:** Columns: Remote Agent Name, Remote Agent IP Address, Available Services. Row: None Defined.

Below these tables are 'Add Entry' and 'Search' buttons. To the right of the tables is a 'Help' sidebar with a list of network configuration tasks and a note about interface changes if NDGs are used. At the bottom are 'Back to Help' and 'Cancel' buttons.

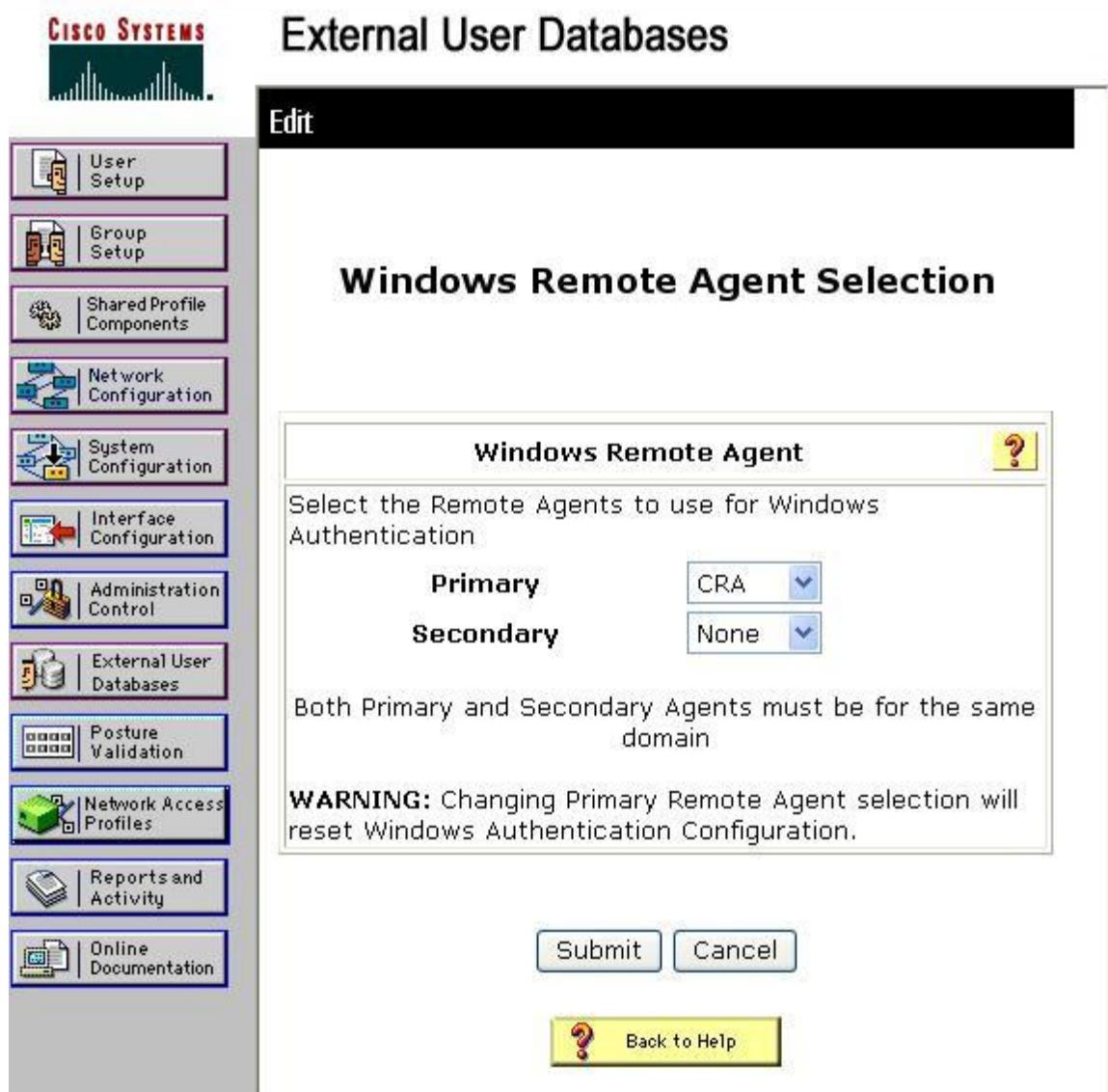
2. Ensure that the windows symbol appears in the available services indicating that the service is up



3. Go to External User Database _ Database configuration _ Windows Database then click Configure button and select Windows Remote Agent option.



4. Select the remote agent you created in the 'primary' part and then click submit.



External Database Configuration

User authentication can be done either using ACS internal database users (creating users locally on ACS) or redirect the request to external database such as Windows Database or LDAP. Following steps explain the configuring ACS for external database. Make sure you have completed the Adding Remote Agent part before configuring external database.

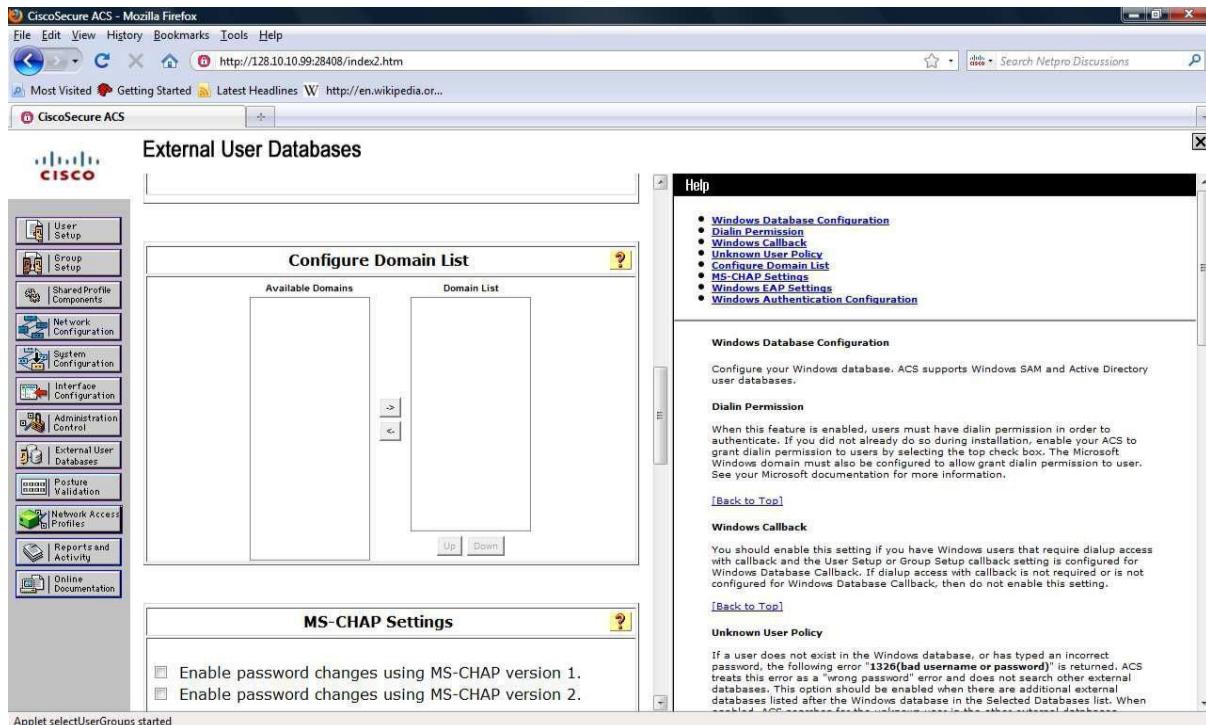
1. Click the External User Database button at the left side and select Database Configuration option

<http://128.10.99.28408/index2.htm>

2. Select Windows Database and click Configure button

<http://128.10.99.28408/index2.htm>

3. Select Windows Authentication Configuration and select the under Available domains in the Configure Domain lists section. You can select the Domain and click the Right arrow button to go to Domain list box

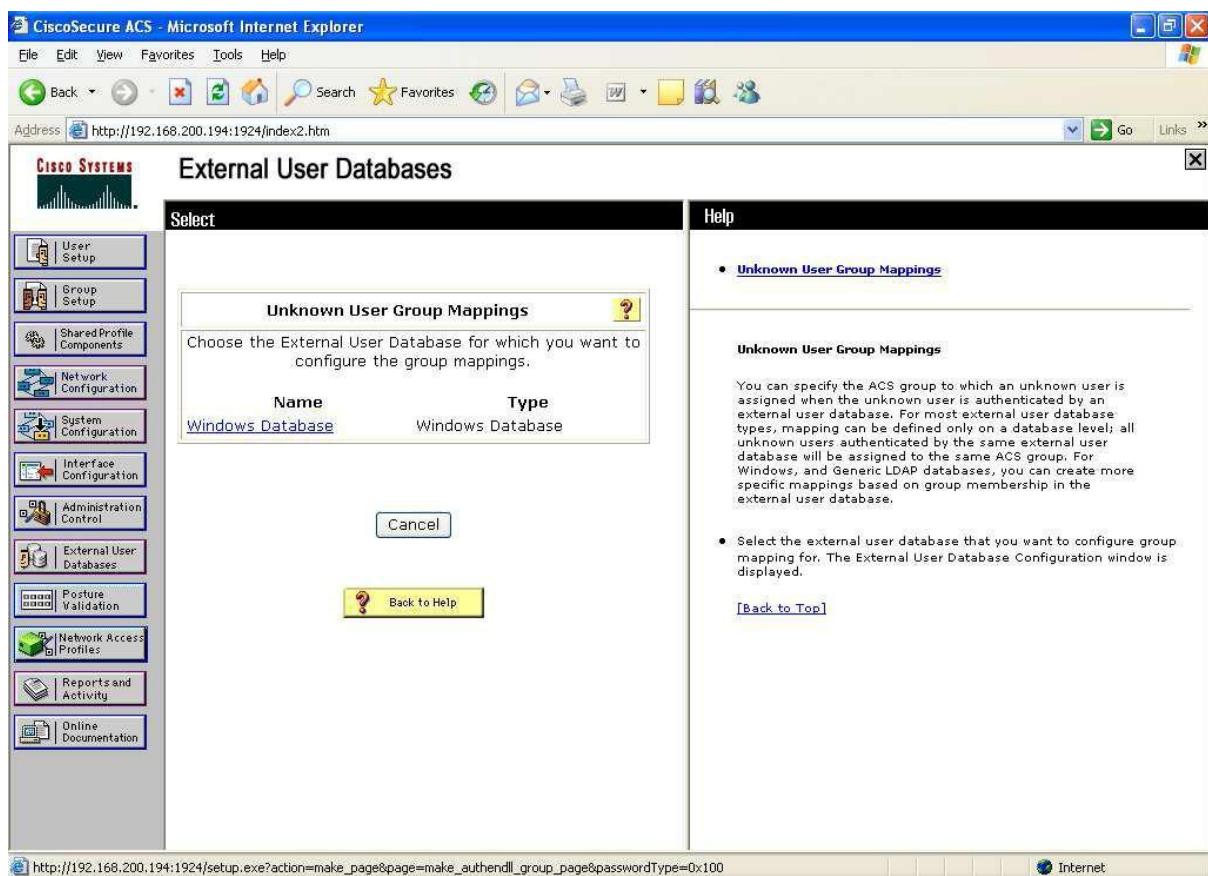


Database Group Mapping

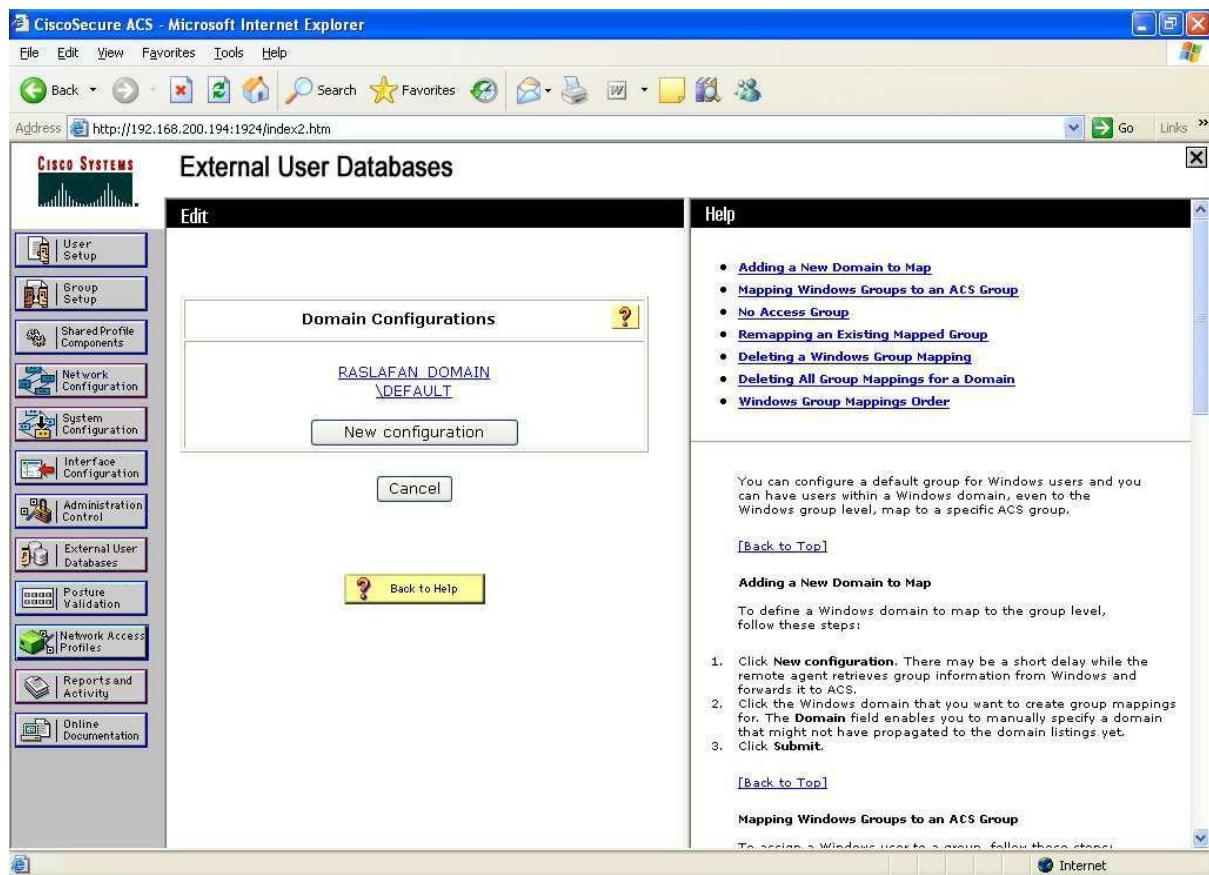
You can use the Database Group Mapping feature in the External User Databases section to associate unknown users with an ACS group for the purpose of assigning authorization profiles. For external user databases from which ACS can derive group information, you can associate the group memberships, which are defined for the users in the external user database, to specific ACS groups. For Windows user databases, group mapping is further specified by domain; because each domain maintains its own user database.

Following steps explain the procedure for mapping ACS groups with Active Directory groups (domain groups)

1. Go to External Users Database _ click Database Group mapping _ click the Windows Database



2. Click New Configuration tab and Select the Domain Name



3. Click Add mapping tab

External User Databases

Edit

Group Mappings for Domain : RASLAFAN_DOMAIN

NT groups **ACS group**
Network Services, * ACS Network Group

Add mapping Add manual mapping

Delete Configuration

Cancel

Back to Help

Help

- [Adding a New Domain to Map](#)
- [Mapping Windows Groups to an ACS Group](#)
- [No Access Group](#)
- [Remapping an Existing Mapped Group](#)
- [Deleting a Windows Group Mapping](#)
- [Deleting All Group Mappings for a Domain](#)
- [Windows Group Mappings Order](#)

You can configure a default group for Windows users and you can have users within a Windows domain, even to the Windows group level, map to a specific ACS group.

[Back to Top]

Adding a New Domain to Map

To define a Windows domain to map to the group level, follow these steps:

1. Click **New configuration**. There may be a short delay while the remote agent retrieves group information from Windows and forwards it to ACS.
2. Click the **Windows domain** that you want to create group mappings for. The **Domain** field enables you to manually specify a domain that might not have propagated to the domain listings yet.
3. Click **Submit**.

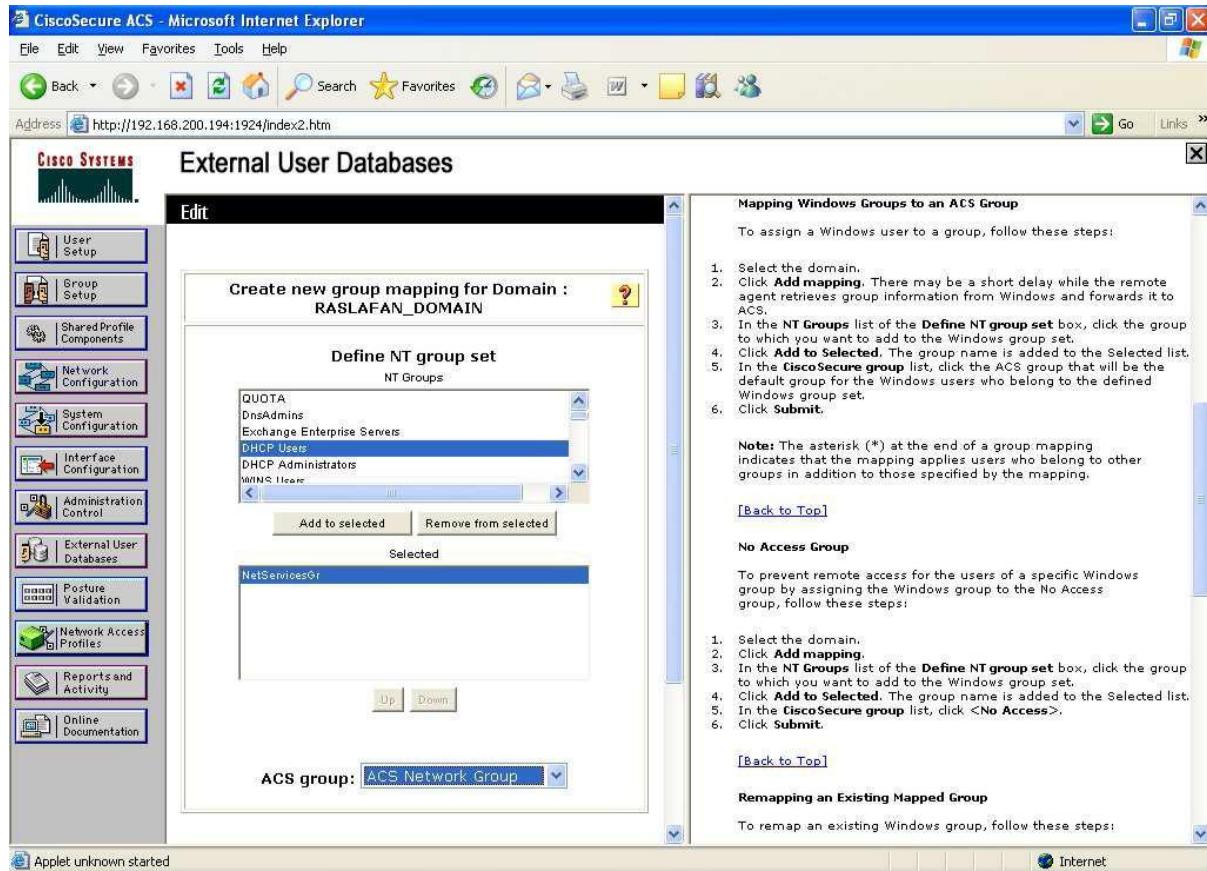
[Back to Top]

Mapping Windows Groups to an ACS Group

To assign a Windows user to a group, follow these steps:

4. Select the Active Directory group name under Define NT Group set and Click Add to selected tab.

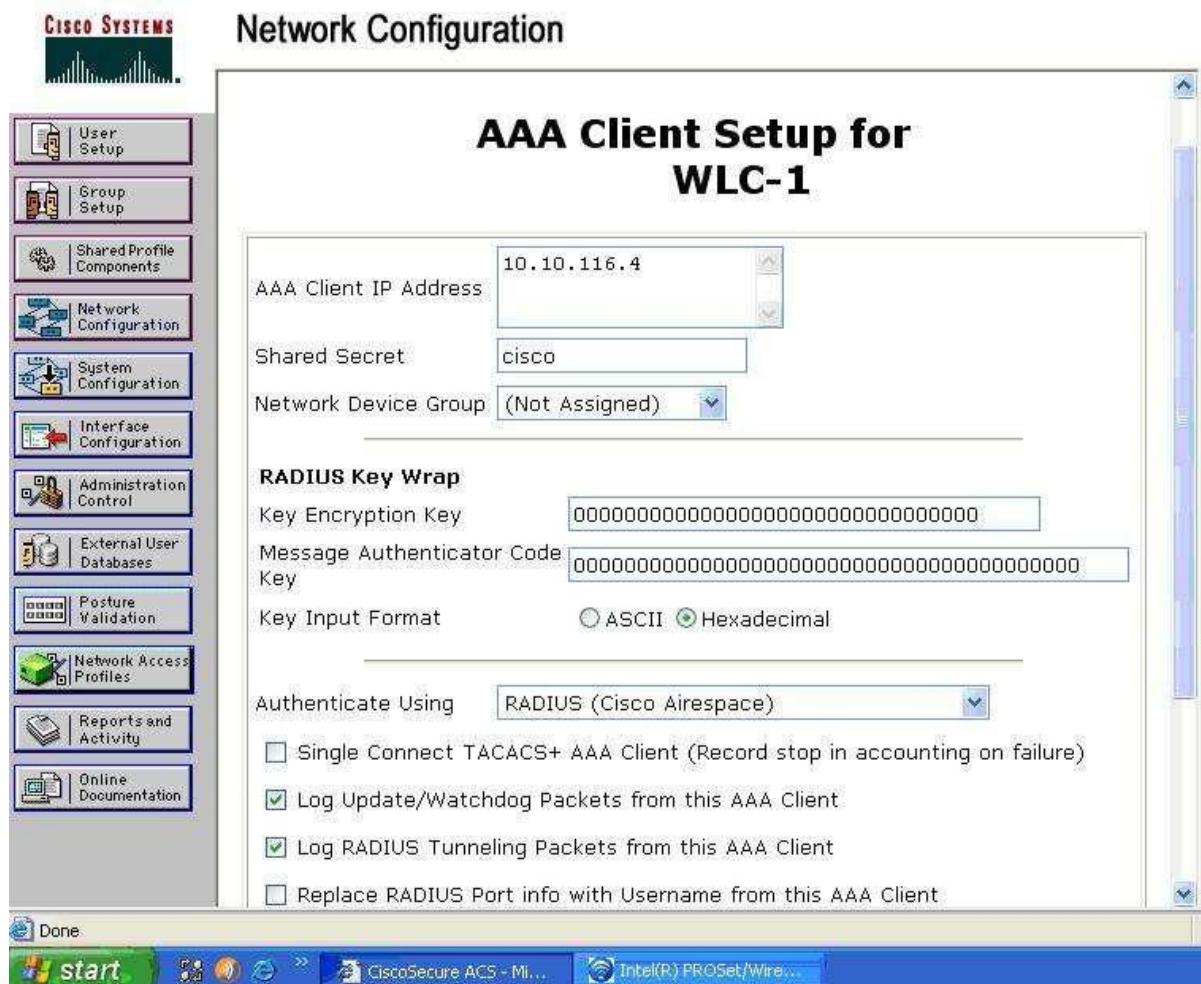
Select ACS group name from the ACS group drop down menu



ACS Configuration for Wireless User Authentication

As a part of MOC wireless implementation, ACS plays a vital role in providing authentication for wireless users. Following steps explain the configuration settings required for adding WLC, generating certificate and PEAP settings.

1. Log in to the ACS and click 'Network Configuration' in the main tab and go to the 'not assigned' group to add the Wireless LAN controller.



CiscoSecure ACS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://192.168.200.3:2988/index2.htm

External User Databases

Select

Windows User Database Configuration

Windows Remote Agent Selection Windows Authentication Configuration

Cancel Back to Help

Help

- Windows Remote Agent Selection
- Windows Authentication Configuration

Windows Remote Agent Selection

To enable Cisco Secure ACS to perform Windows authentication, you must first select the remote agents that will pass authentication requests to Windows. To proceed, click the Windows Remote Agent Selection link.

[Back to Top]

Windows Authentication Configuration

To configure Windows authentication, including the versions of MS-CHAP to be enabled, click this link.

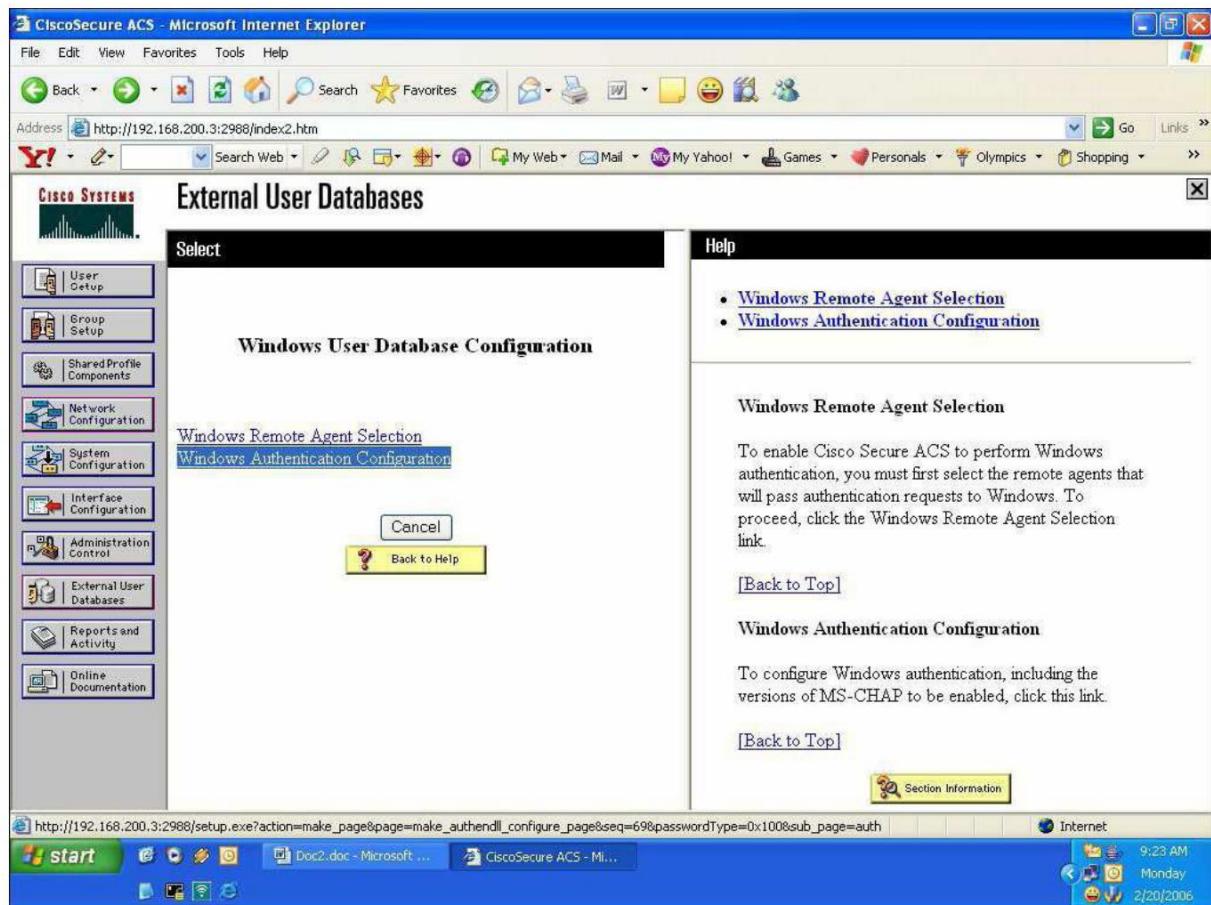
[Back to Top]

Section Information

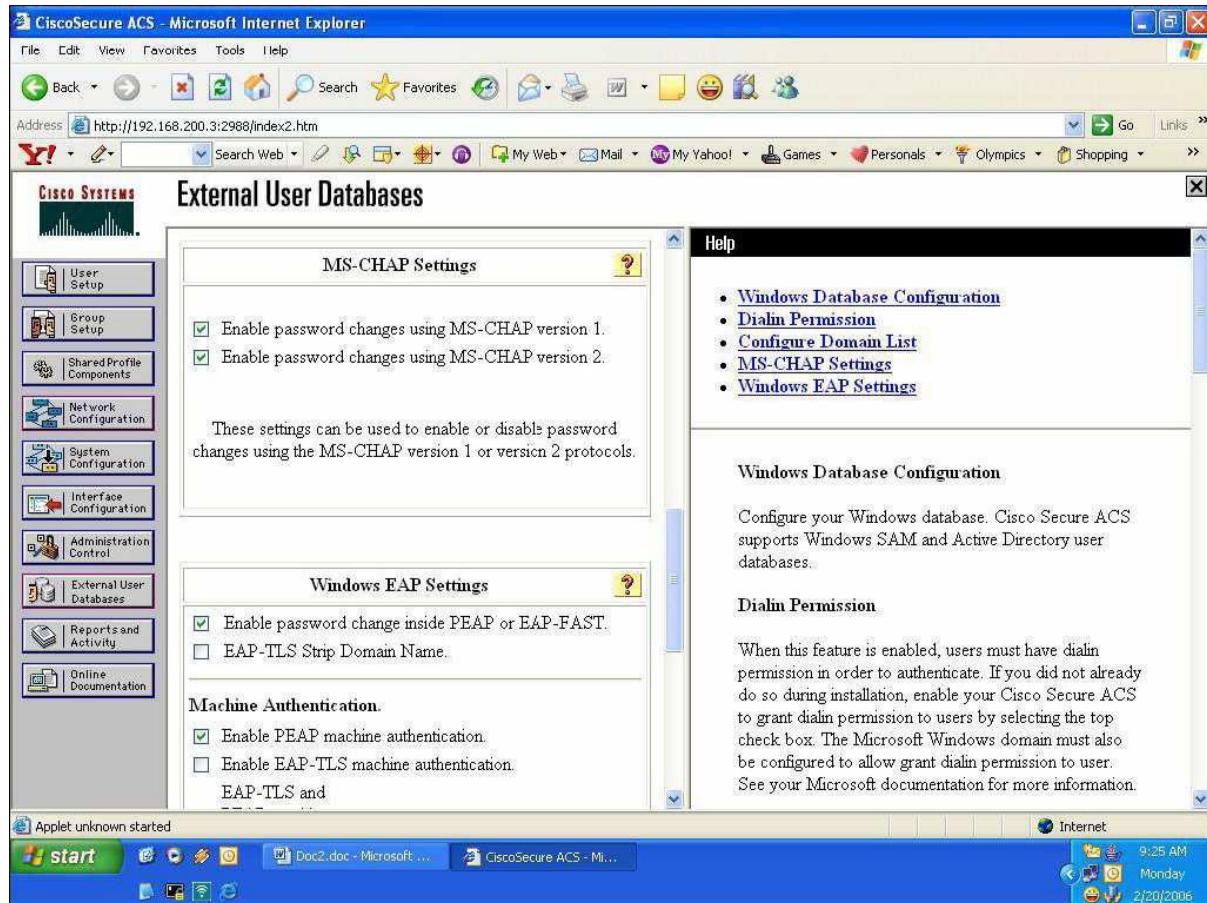
http://192.168.200.3:2988/setup.exe?action=make_page&page=make_authendl_configure_page&seq=69&passwordType=0x100&sub_page=auth

Internet

start Doc2.doc - Microsoft ... CiscoSecure ACS - Mi... 9:23 AM Monday 2/20/2006

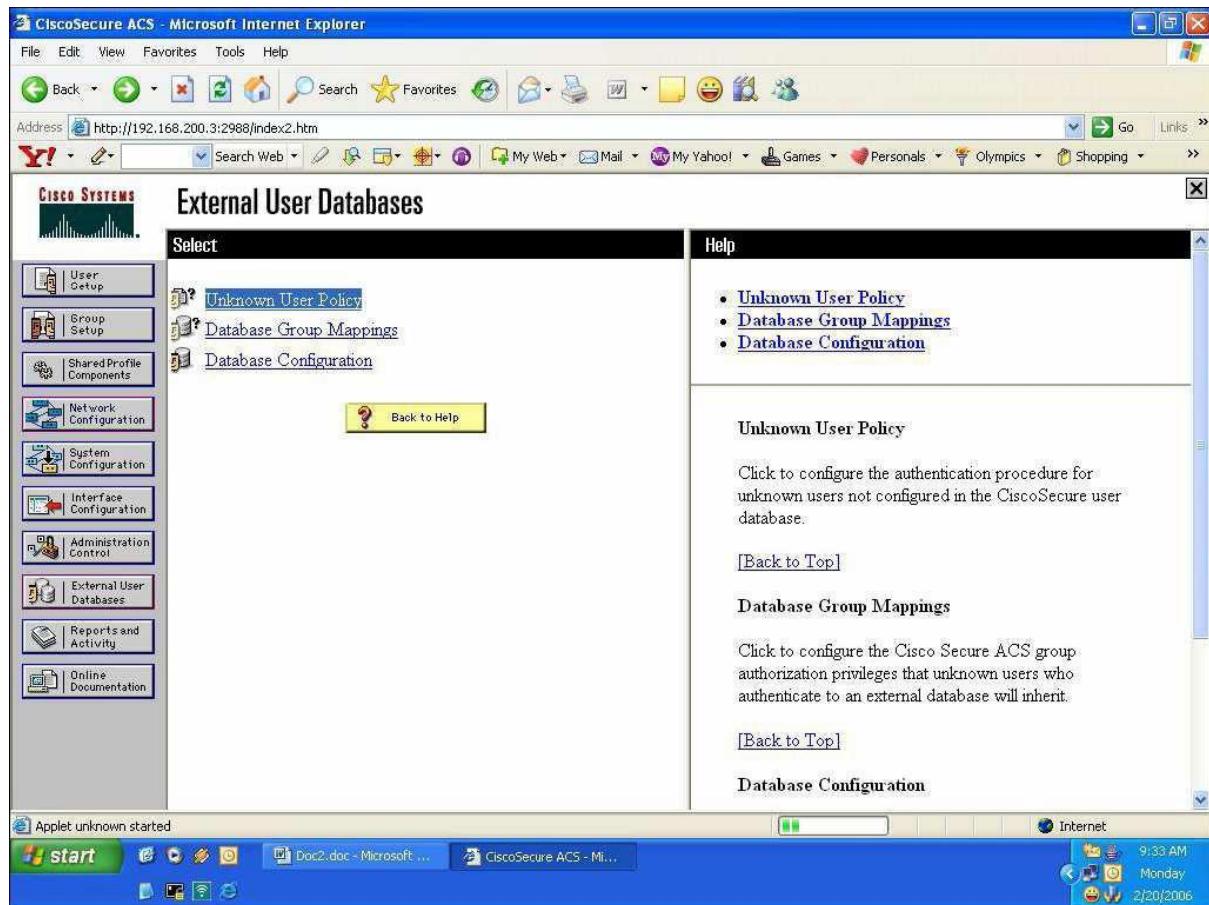


2. Click 'Windows authentication configuration'. From the list select the appropriate domain.

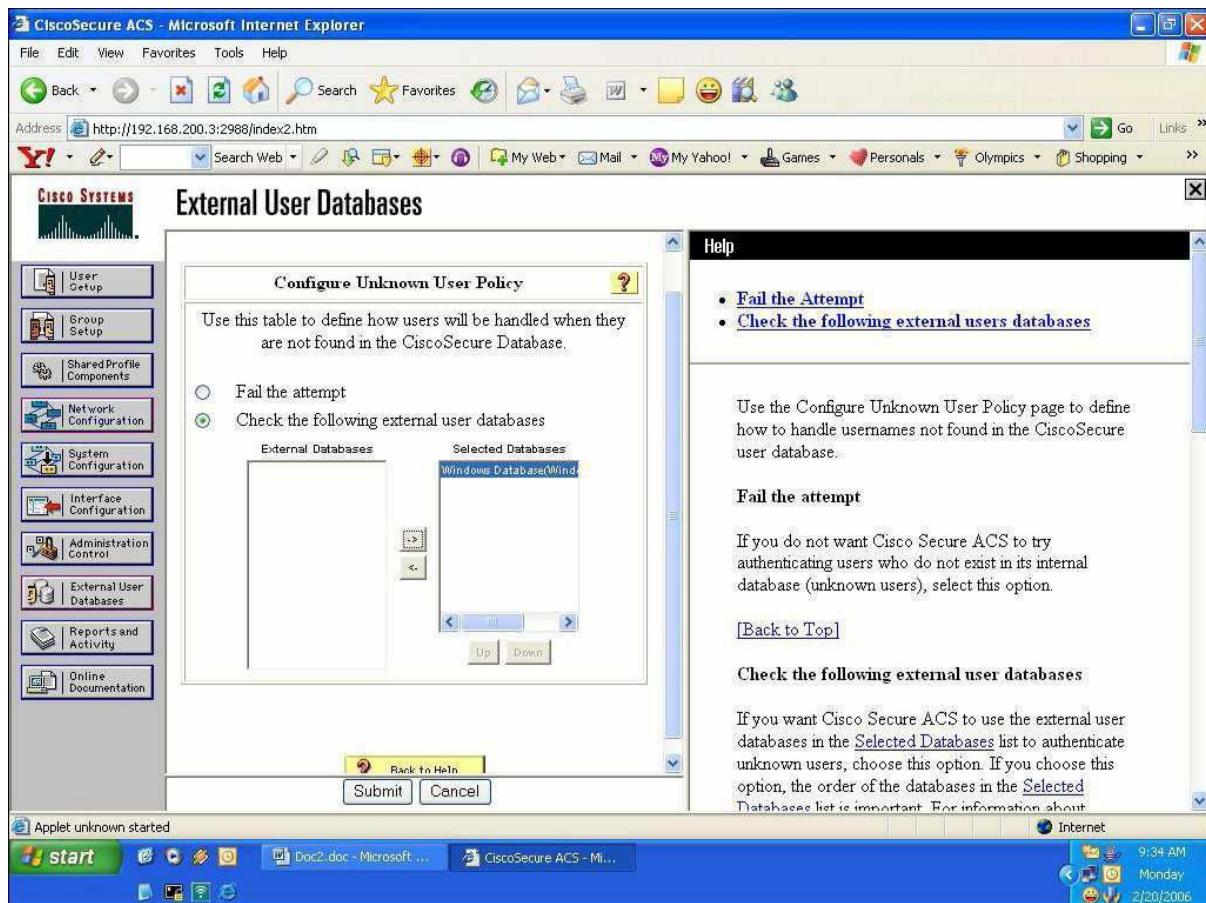


Scroll down and ensure above shown options are checked. Click submit at the end.

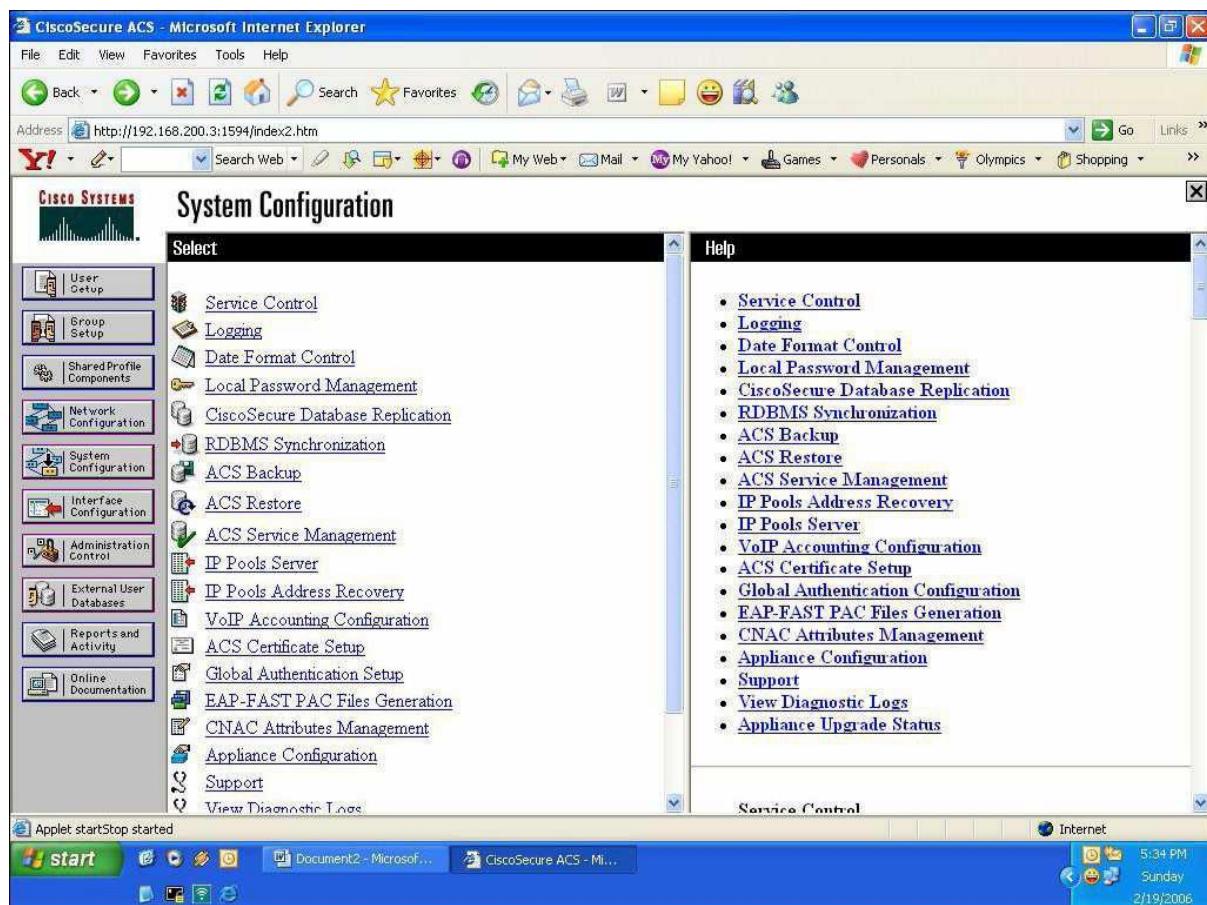
3. Click 'unknown user policy' present in the 'external user database' main tab.



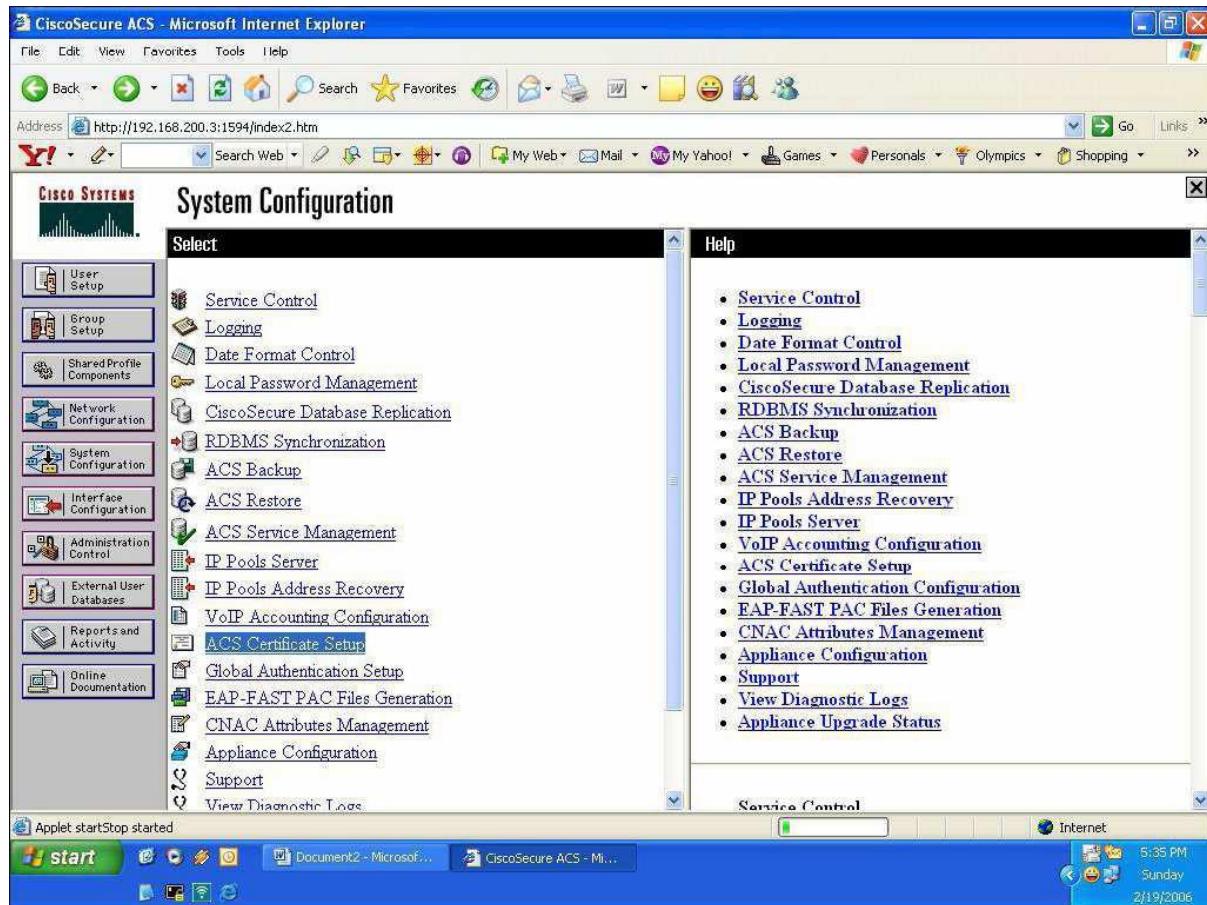
4. Move the windows database to the selected databases from the external databases and then click submit.



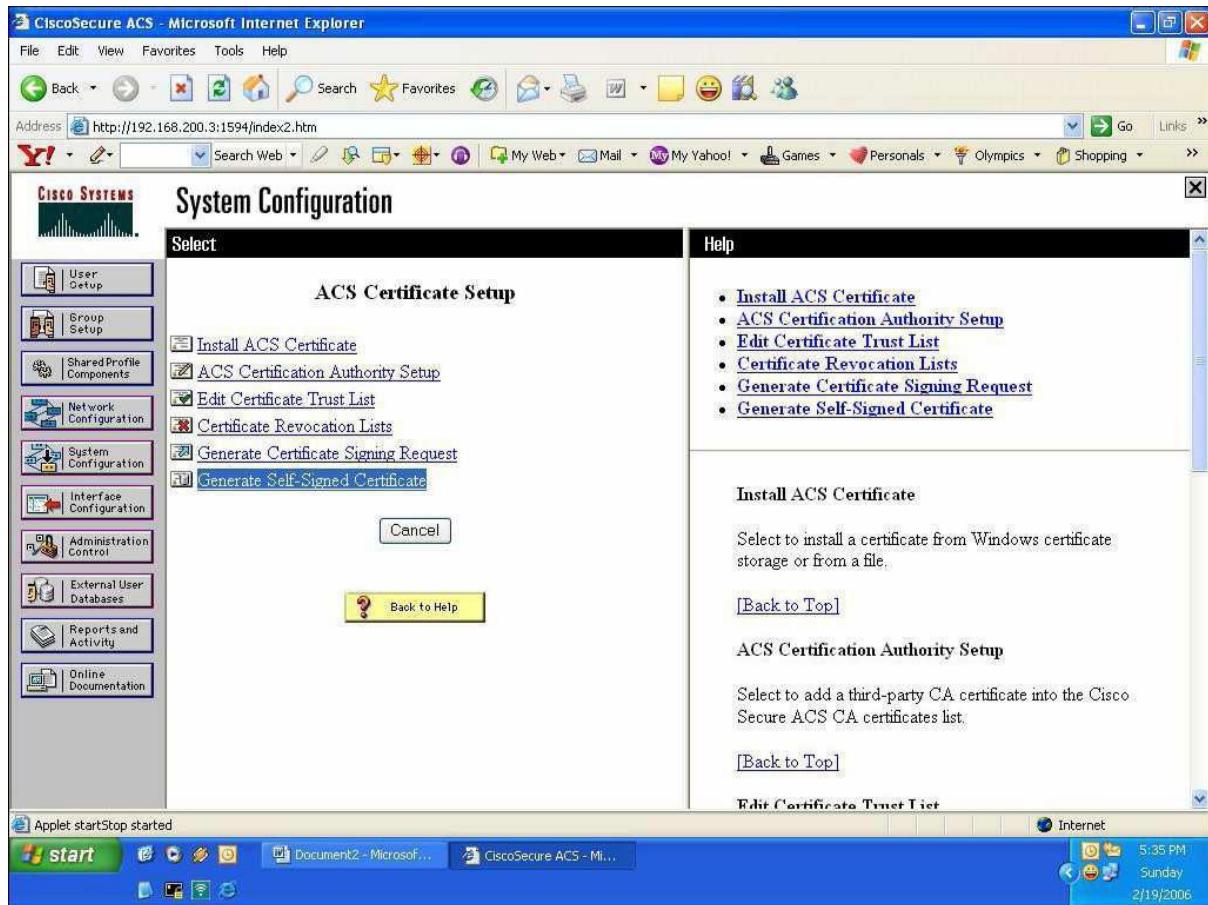
5. Click 'system configuration' in the main tab section (this is to create the self signed certificate which will be used for PEAP)



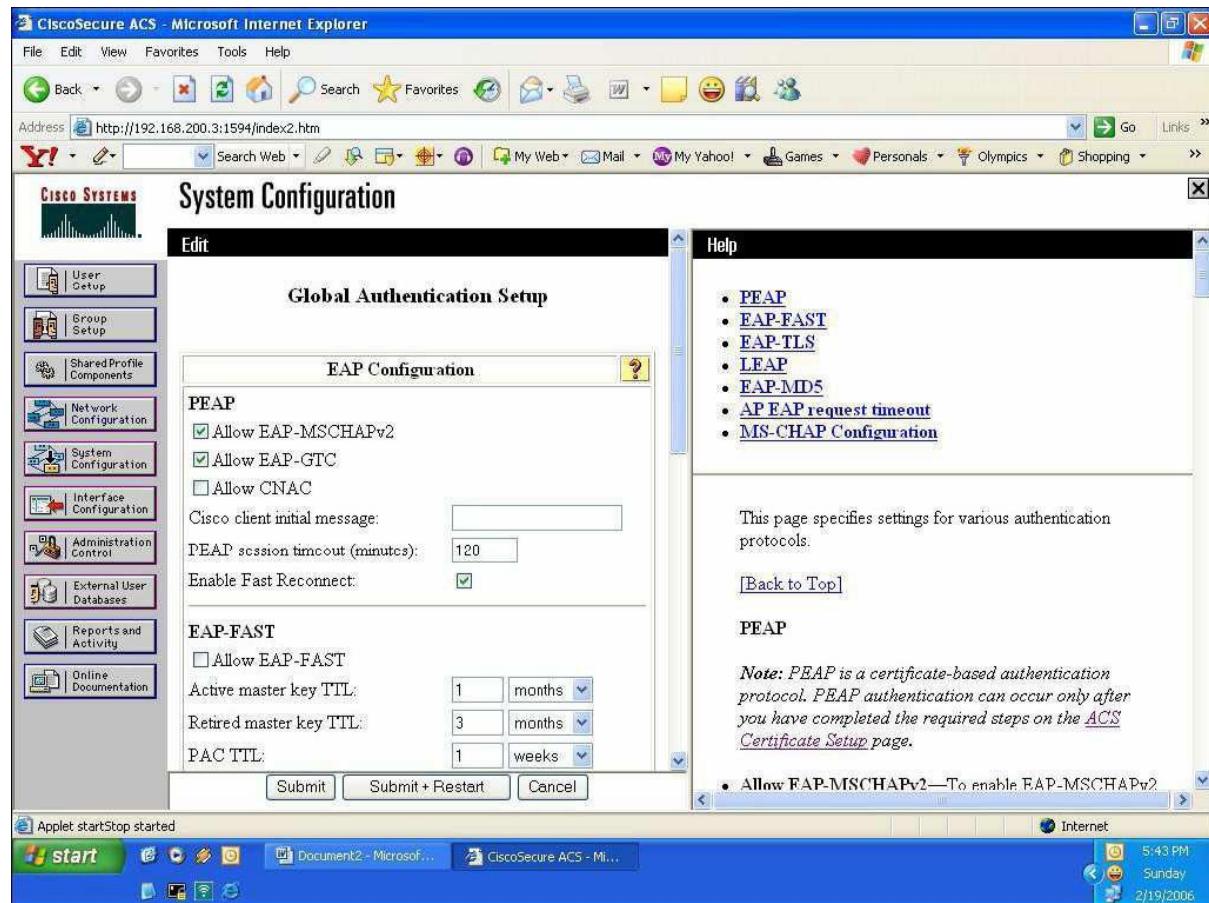
6. Select ACS certificate setup.



7. Select generate self signed certificate Enter the required fields. (certificate subject: cn=ASHGHAL) then Go to the install ACS certificate to verify the certificate generated



8. Click 'global authentication setup' in the system configuration setup in order to setup the PEAP.



9. Ensure the following options are ticked for PEAP configuration:

The screenshot shows the 'System Configuration' page of CiscoSecure ACS. On the left, there's a sidebar with various icons for User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled 'System Configuration'. It has sections for 'Client initial message', 'Authority ID Info', 'Allow automatic PAC provisioning' (unchecked), 'EAP-FAST master server' (checked), and 'Actual EAP-FAST server status: Master'. Below these are sections for 'EAP-TLS' (with 'Allow EAP-TLS' checked), 'Select one or more of the following options' (with 'Certificate SAN comparison' unchecked, 'Certificate CN comparison' checked, and 'Certificate Binary comparison' unchecked), and 'EAP-TLS session timeout (minutes): 120'. There are also sections for 'LEAP' (with 'Allow LEAP (For Aironet only)' checked) and 'EAP-MD5' (with 'Allow EAP-MD5' checked). At the bottom, there are 'Submit', 'Submit + Restart', and 'Cancel' buttons. To the right of the main content is a 'Help' panel with a list of links: PEAP, EAP-FAST, EAP-TLS, LEAP, EAP-MD5, AP EAP request timeout, and MS-CHAP Configuration. Below the help panel is a note: 'This page specifies settings for various authentication protocols.' and a link to '[Back to Top]'. Under the 'PEAP' section, there's a note: 'Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have completed the required steps on the ACS Certificate Setup page.' At the very bottom, there's a note: '• Allow EAP-MSCHAPv2—To enable EAP-MSCHAPv2.' The status bar at the bottom shows 'Applet startStop started', the Windows taskbar with 'start', 'Document2 - Microsoft...', 'CiscoSecure ACS - Mi...', and the system tray with the date '2/19/2006', time '5:44 PM', and day 'Sunday'.

10. Click Submit + Restart at the end.

LAN Management Solution

As per the design, MOC network will have the Cisco LAN management version 3.1 as management software. CiscoWorks LAN Management Solution (LMS) is a suite of management tools that simplify the configuration, administration, monitoring, and troubleshooting of Cisco Switches and Routers. CiscoWorks LMS provides:

- A centralized system for sharing device information across all LAN management applications, improving manageability, and increasing systemwide awareness of network changes
- Network discovery, topology views, end-station tracking, and VLAN management
- Real-time network fault analysis with easy-to-deploy, device-specific, best-practice templates
- Hardware and software inventory management, centralized configuration tools, and syslog monitoring
- Monitoring and tracking of network response time and availability
- Real-time device and link management, as well as port traffic management, analysis, and reporting
- A flexible Web portal for launching and navigating network management functionality
- A workflow engine that provides step-by-step wizards for system setup and device troubleshooting
- Support for network virtualization through configuration, reporting, monitoring and troubleshooting for VRFLite networks

The CiscoWorks LMS application versions are as follows:

- CiscoWorks Device Fault Manager (DFM) 3.1
- CiscoWorks Campus Manager 5.1
- CiscoWorks Resource Manager Essentials (RME) 4.2
- CiscoWorks Internetwork Performance Monitor (IPM) 4.1
- CiscoWorks CiscoView 6.1.8
- CiscoWorks Common Services 3.2
- CiscoWorks LMS Portal 1.1
- CiscoWorks Assistant 1.1

The function of each application is described as depicted in the table.

Applications	Description
CiscoWorks Device Fault Manager	Real-time fault detection, analysis, and reporting using device knowledge and fault rules based on Cisco best practices for each device.
CiscoWorks Campus Manager	A robust set of Layer 2 tools for device and connectivity discovery, detailed topology views,, end-station tracking, network discrepancies
CiscoWorks Resource Manager Essentials	Tools for managing Cisco devices using inventory- and devicechange management, network-configuration and software-image management, network availability, and syslog analysis.
CiscoWorks CiscoView	GUI providing back- and front-panel displays of devices in a dynamic, color-coded graphical display. Simplifies device-status monitoring, device-specific component diagnostics, and application launching.
CiscoWorks Internetwork Performance Monitor	A network response-time and availability troubleshooting application. This tool empowers network engineers to proactively troubleshoot performance issues using real-time and historical reports.
CiscoWorks Common Services	Provides the infrastructure for a common management desktop experience and the services for securing access to all CiscoWorks applications. Includes a common device and credentials repository for all applications

as it

populates the repository after running discovery over the managed network. Facilities include a foundation for integrating with other Cisco and third party applications.

LMS will be managing all the devices in MOC and the number of devices can be increased at any point of time up to 300 devices.

DMZ and Internet Edge switches cannot be managed by LMS as the SNMP traffic will not be permitted through the ASA.

Installation of LMS can be done using the DVD that comprises of all the applications specified above. After the installation the configuration has to be done after which we can manage all the devices. The Configuration will be done as follows.

1. Device Discovery
2. Data Collection
3. Providing Device Credentials to LMS
4. Device Update in RME
5. Automatic Configuration Backup in RME
6. Device Update in DFM
7. Notification Services configuration in DFM.

Device Discovery: Device Discovery will be the basic step to configure LMS. All the devices that should be managed by LMS should be discovered by the application. The Device discovery option is available in the common services application.

To enable device discovery, SNMP credentials are mandatory. Apart from this, we can choose either CDP, ARP table, OSPF table or Routing table or all.

In MOC LMS, SNMP and CDP will be used for device discovery. A Sample screenshot containing the device discovery settings is as follows.

The screenshot shows a Microsoft Internet Explorer window titled "srplmssfnoc - Discovery Settings Summary - Microsoft Internet Explorer". The address bar shows the URL: "http://172.25.54.13:1741/cwhp/discovery.settingssummary.do". The page header includes the Cisco logo and navigation links for Home, Server, Software Center, Device and Credentials, Groups, Device Discovery, Device Management, Auto Update Server Management, Reports, Device Selector Settings, Admin, and Help.

The main content area is titled "Discovery Settings Summary". On the left, there is a "TOC" sidebar with links to "Discovery Settings", "Discovery Schedule", "Discovery Logging", and "Configuration". The main panel displays a table of discovery settings:

Discovery Settings Summary	
Module Settings:	Configure
Seed Device Settings:	Configure
SNMP Settings:	Configure
Filter Settings:	Configure
Global Settings:	Configure
Modules Selected:	CDP
Use DCR as Seed List:	No
Preferred Management IP:	Resolve by Name
Preferred DCR Display Name:	Host Name
Update DCR Display Name:	Yes
Use DCR Default Credentials:	No
E-mail:	
Add Discovered Devices to a Group:	No
Selected Group Name:	

At the bottom right of the main panel are two buttons: "Configure" and "Start Discovery".

Data Collection: The Data collection of all the reachable devices that are discovered should be done using the Data collection option available with the Campus Manager application.

The data collection will collect all details pertaining to a single device and will enable LMS to provide a complete view of the device. The Data collection should be done as per the following screenshot.

This screenshot shows the Cisco Campus Manager Home page. At the top, there's a navigation bar with links for Home, User Tracking, Visualization, Configuration, Reports, Job Mgmt, and Admin. Below the navigation bar, it says "Version : 5.1.0" and "Last Updated: 04 Jun 2009, 17:54:15 GMT+03:00". The main content area includes sections for System Status, Best Practices Deviation and Discrepancies, Application Setup Tasks, Operational Tasks, Network Reports, and Advanced Reports. The "System Status" section shows two entries: "Data Collection" (Idle) and "User Tracking Acquisition" (Running). The "Best Practices Deviation and Discrepancies" section shows a table with one row. The "Application Setup Tasks" and "Operational Tasks" sections list various configuration items. The "Network Reports" and "Advanced Reports" sections also list several report types. A message "No records found." is displayed in the "Recently Completed Jobs" section.

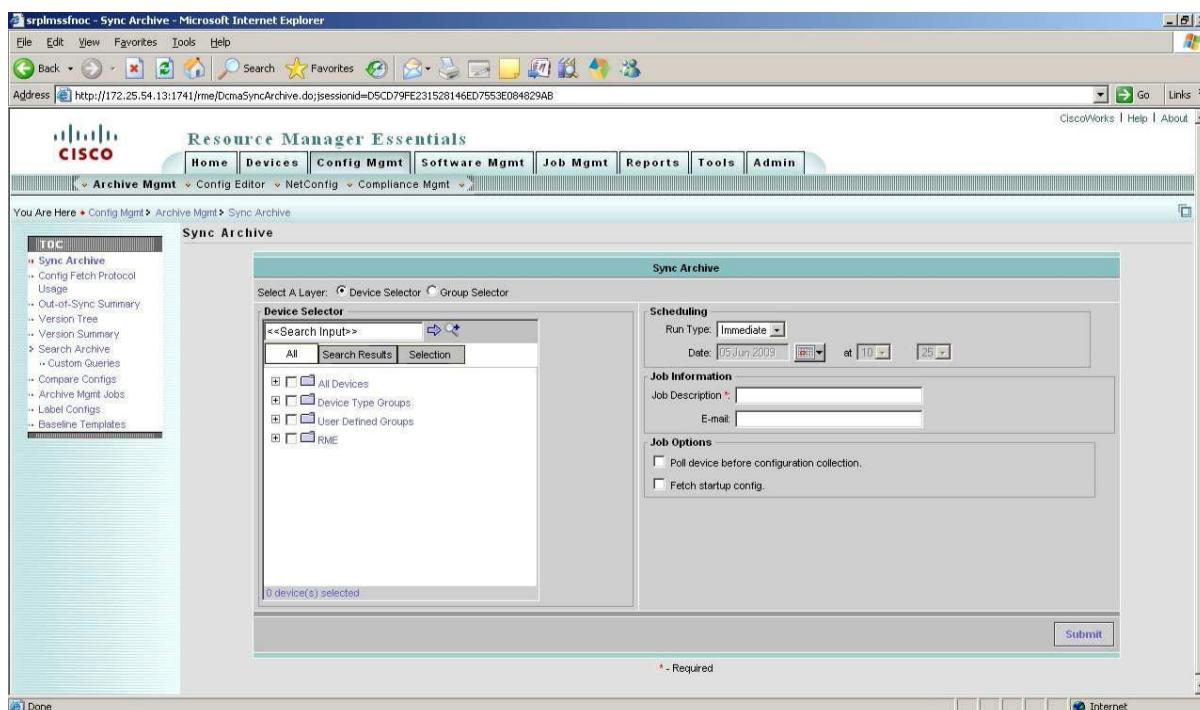
Device Credentials in LMS: The Device credentials like the Username and password for Telnet /SSH can be provided in the LMS as follows.

This screenshot shows the Cisco Device Management - Device Summary page. At the top, there's a navigation bar with links for Home, Server, Software Center, Device and Credentials, Groups, and Admin. Below the navigation bar, it says "Device Discovery > Device Management > Auto Update Server Management > Reports > Device Selector Settings > Admin". The main content area is titled "Device Summary" and contains a search input field and a list of selection options: All Devices, Device Type Groups, and User Defined Groups. Below the list, it says "0 device(s) selected". At the bottom, there are buttons for Edit Identity, Edit Credentials, Delete, View, Add, Bulk Import, Export, and Exclude.

The Device credentials will be required for the automatic configuration backup, Configuration editing of the devices and also for the software upgrade of the devices.

Device Update in RME: RME (Resource Manager Essential) is the application that will be used for the configuration backup, Editing Configuration and IOS Update. The application will not have the devices by default. After the Device discovery and Data collection, the devices should be updated in RME.

Automatic configuration Backup in RME: The Best feature of LMS is the configuration backup of the Devices. The configuration backup can be scheduled daily, weekly or hourly basis. The Configuration backup will be maintained in LMS Server for a maximum of 6 months which can also be extended to any number of days. The Configuration will be stored in Binary format. The Configuration backup will be scheduled in the following screen.



Device Update in DFM: DFM (Device Fault Manager) is the application which receives the SNMP traps from all the devices and sends alerts to the LMS screen and also notifies these alerts via e-mail to the configured e-mail. This application will also have no devices at the startup. The Devices has to be updated from the Data collection.

Notification Services in DFM: DFM receives the SNMP alerts from all the devices. The SNMP alerts will be converted to error messages by DFM. These error messages will be classified as High Severity like High CPU utilization, Interface flaps, Unreachable and Low severity as configuration changes. The High severity error messages can be notified to the Network Administrators.

WIRELESS INFRASTRUCTURE

This Section will cover all the aspects of proposed wireless network infrastructure for MOC. It will provide detailed Information on how the Wired and Wireless infrastructure will integrate with each other. The security issues specific to wireless networks and the proposed solution will also be discussed.

Wireless Network Requirements

Wireless coverage needs to be provided for all the floors at the MOC building. The following are the requirements from MOC.

- 1.** Internet & Intranet Access to Corporate users.
- 2.** Internet (only) for Guest users.
- 3.** Support for 802.11n
- 4.** Uses off multiple SSID's – SSID for Guest access and SSID for corporate access.
- 5.** Use of ACS radius server for corporate users authentication via Active Directory
- 6.** Use of NAC Guest Server for Guest Users authentication

Overview of the wireless network

The proposed wireless network for MOC is basically to meet requirements like Internet access to Guest Users coming in frequently and Internet and intranet access to the corporate users. The proposed network shall generate temporary usernames and passwords for the Guest Users from the Cisco NAC Guest server as on when required basis. The User (Corporate/Guest) shall first connect to the Controller over a tunnel called CAPWAPP tunnel and from there the guest will connect to the Anchor controller via EoIP Tunnel.

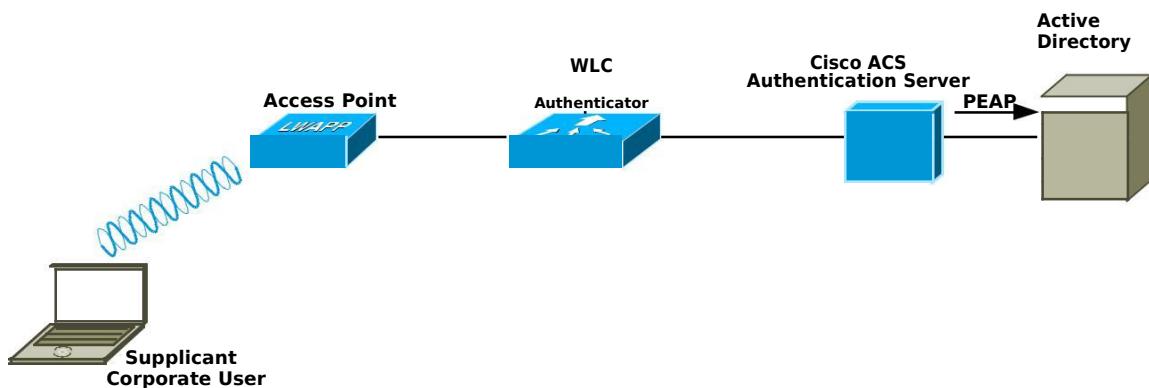
Considering the Guest Users as security vulnerability to the Intranet and to the important information available within the network, one Guest controller has been considered connecting to the firewall on the DMZ segment and all the Guest users shall directly terminate on the Outside controller connected to the Firewall. In the design 4402 series controller is considered as the Guest controller.

Corporate users shall directly connect to the controller (Cisco 4404), which is inside the network connected to both the Core switch (N7K). These users shall securely connect to both Intranet and Internet simultaneously via PEAP Authentication. For corporate users we are creating one vlan which will be mapped to the Corp SSID.

Protected EAP (PEAP)

The IEEE 802.1x is a protocol standard framework for wired and wireless LANs that authenticates users or network devices and policy enforcement to provide MOC secure network access control. It involves communications between a supplicant, authenticator, and authentication server. The supplicant is often software on a client device, such as a laptop/desktop, the authenticator is wireless lan controller, and an authentication server is generally a radius server such as Cisco ACS. With 802.1X authentication, the supplicant provides credentials, such as user name / password, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the credentials are valid (in the authentication server database), the supplicant (client device) is allowed to access resources located on the protected side of the network.

Dot1x Authentication for Corporate Users



The 802.1X specification requires that we use an Extensible Authentication Protocol (EAP)-based method for authentication. There are two popular EAP-based methods: EAP-Transport Layer Secured (EAP-TLS) and Protected EAP (PEAP) with Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2).

PEAP is generally selected because of its simplicity, interoperability and high security.

Further, it does not require public key infrastructure (PKI) and client certificates, therefore it is easier to manage compared to EAP-TLS.

Guest Tunnelling

Guest tunneling provides additional security for guest-user access to the corporate wireless network, helping to ensure that guest users are unable to access the corporate network without first passing through the corporate firewall. Instead extending the DMZ VLAN to each wireless LAN controller on the network, a Wireless controller can be used to terminate traffic from the remote controller. When a user associates with a SSID (Service Set Identifier) that is designed as the guest

SSID, the user's traffic is tunneled to the DMZ Anchor controller or guest controller which can route the traffic to the DMZ network outside of the corporate firewall.

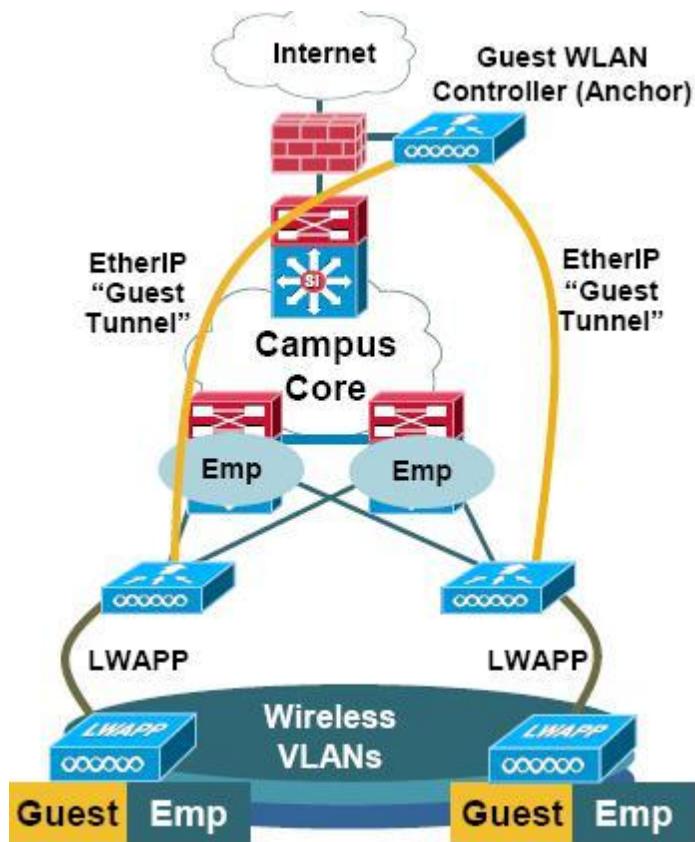
In guest tunneling scenarios:

The user's IP address is administered from the DMZ anchor controller/guest controller which has dedicated VLAN for guest users.

All user traffic is transported over Ethernet over IP (EoIP) tunnel between the primary wireless LAN controller and the DMZ anchor wireless LAN controller/guest controller.

Mobility is supported as a client device roams between wireless LAN controllers.

Each DMZ anchor controller/guest controller can support 40 tunnels from various 'inside' controllers. These tunnels are established from each controller for each SSID utilizing mobility anchor feature, meaning that many wireless clients can ride the tunnel.

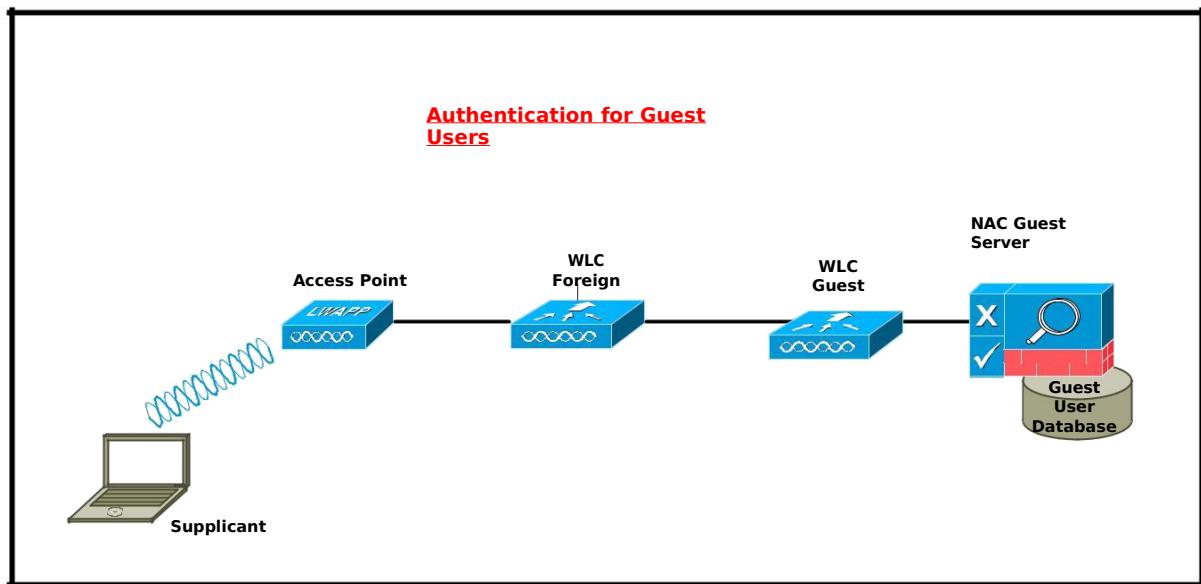
Figure 98 Guest Traffic Flow

NAC Guest Server

For Guest users, the NAC Guest server can generate the username and passwords. The NAC guest server can be integrated with the active directory. So the person with the active directory username and password can login to the NAC Guest server and can create the user name and password for his guests.

For creating guest users, there is an option to create a user called Sponsor user account who can manage guest account creation and deletion. The Sponsor user account is not allowed to view or modify other settings of the NAC Guest Server.

Sponsor user account privilege can be given to helpdesk where they can manage guest accounts.



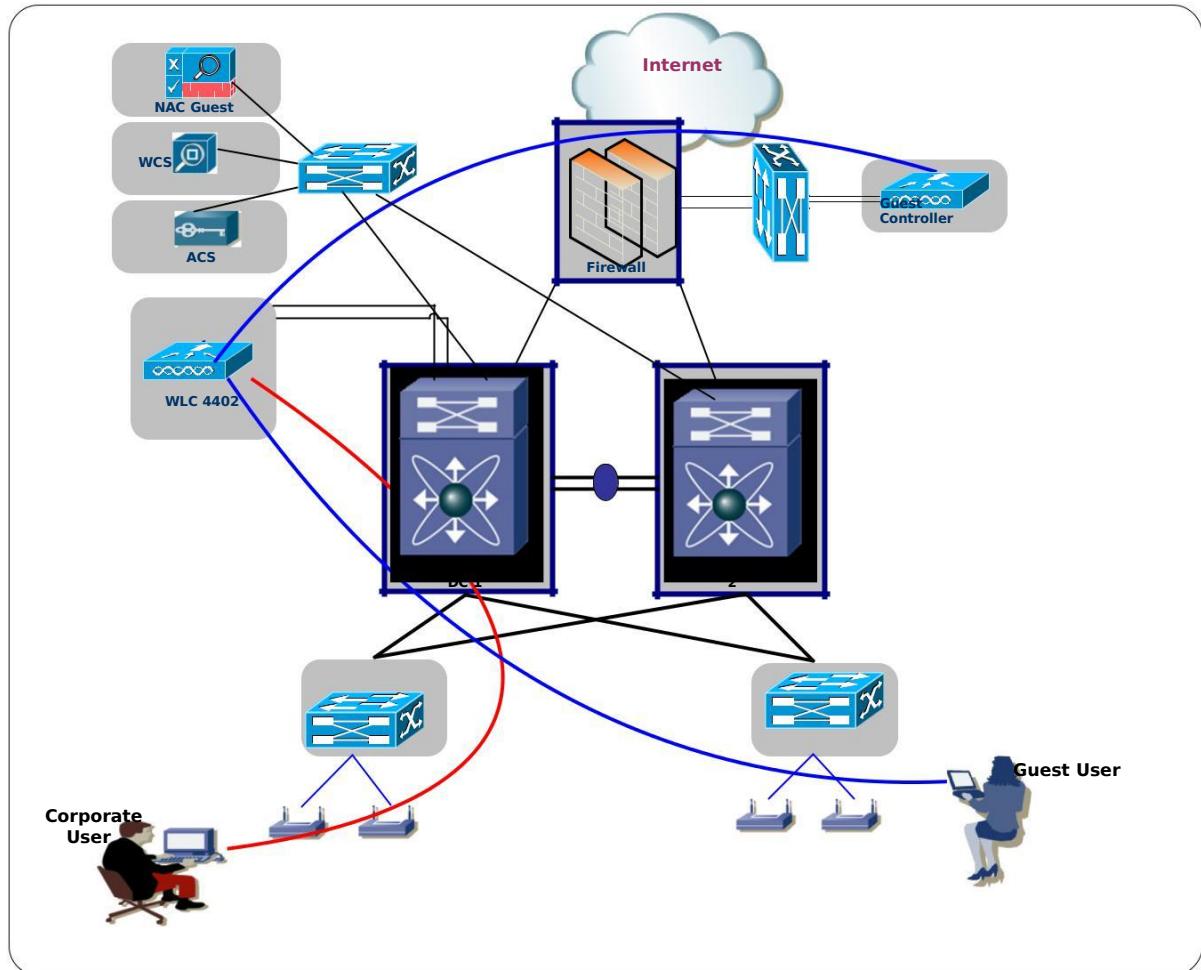
AP Groups Vlan

The AP Grouping feature of the WLC allows a single WLAN to be supported across multiple dynamic interface of the controller. This will help us to maintain a single SSID for the corporate users even if they are associated to different vlans.

Detailed Design

The Wireless network will provide access to the wireless users (Corporate and Guest). Corporate users will have access to both the Intranet and Internet and with Secured connection (PEAP). For Guest users, the access will be restricted to basic Internet usage upon permission and the availability of 'username' and 'password' from the local Administrator or the Lobby Receptionist (Helpdesk) of MOC.

The local controller shall connect to both the Core switches. Wireless guest controller (WLC-4402) will be connected to DMZ zone of the firewall.

Figure 99 Wireless Network Diagram

As shown in the figure WLC is connected to one of the Core switches. The link has to be configured as a trunk link to pass multiple wireless LANs. Further the trunk link is configured not to pass all vlans but only the wireless vlans. Guest controller is connected to the ASA. WLC form an EOIP tunnel to the Guest controller for the guest users.

If one of the controllers fails, the access points associate to the working wireless LAN controller, but the limitation is that it can only handle only 50 access points.

The access points are connected to the access switches. The link connecting the access point to the access switch is configured as an access link.

The Wireless network will provide access to the wireless users (Employees and Guests). To achieve this, two SSID (logical wireless networks) are created namely,

MOC_CORP

MOC_GUEST

Employee Access

There is a dedicated SSID for employees. It is broadcasted to avoid Windows XP connectivity problems. Employees will have full access to corporate network upon successful authentication. The Secured for employees will be based on Wireless Protected Access (WPA) standard. Basically, WPA includes 802.1X authentication and encryption. Advanced Encryption Standard (AES) or TKIP has been chosen as the encryption protocol to encrypt the wireless employee data because of its high encryption strength. Further, 802.1X authentication is integrated with active directory to provide a single sign-on to the user. PEAP authentication is used for staffs.

The DHCP service to MOC_CORP is provided by the DHCP sever.

For successful authentication the employee must have

Valid Active directory Username/Password

Corporate Users Authentication Process

Assuming that wired network is Server/Client or transparent architecture, the new VLANS created for Wireless Management and Wireless Corporate, shall be broadcasted all over the Edge switches/Access Switches. All the Access are capable of PoE.

Figure 100 Core Config FOR WIRELESS

CORE SWITCH

Vlan xxx

Name WLC-MGMT

Vlan yyy

Name AP-MGMT

Creating The DHCP Scope for Wireless Access

Points ip dhcp pool AP_MGMT

network <network address>

<Mask> default-router <i.p

address>

option 43 ascii <controller ip

address option 60 ascii "Cisco AP

c1142"


```
!  
Sample Interface vlan  
configuration Interface vlan <vlan  
id>  
Description Wireless Corporate  
users Ip helper-address <ip of dhcp  
server> Ip address <svi ip>  
No shut  
  
Interface GigabitEthernet x/x/x  
Description Connected to WLC  
Switchport trunk encapsulation dot1q  
Switchport mode trunk  
Switchport trunk native vlan <vlan id>  
Switchport trunk allowed vlan <vlan id>  
No shut
```

Access Switch configuration

Access point shall be connected to the access switches which have the capability of providing PoE to the access point

The following template is a sample configuration of an access port in an edge switch:

Figure 101 ACCESS SWITCH FOR WIRELESS

```
Interface GigabitEthernet x/x  
description *** Connected to the Access point ***  
switchport  
switchport mode access  
switchport access vlan <vlan id of AP-MGMT>  
no shutdown
```


Controller Configuration

Initial configuration of the controller is via console and will be edited later accessing via GUI (Graphical User Interface).

Figure 102 Initial Configuration on WLC1

```
Welcome to the Cisco Wizard Configuration  
Tool Use the '-' character to backup  
Would you like to terminate autoinstall? [yes]: yes  
System Name [Cisco_36:7c:e3] (31 characters max): MOC-  
WLC AUTO-INSTALL: process terminated -- no  
configuration loaded Enter Administrative User Name (24  
characters max): cisco Enter Administrative Password (24  
characters max): cisco Re-enter Administrative Password  
cisco  
Service Interface IP Address Configuration [none][DHCP]:  
none Service Interface IP Address:  
Service Interface Netmask:  
Enable Link Aggregation (LAG) [yes][NO]:  
yes Management Interface IP Address:  
Management Interface Netmask:  
Management Interface Default Router:  
Management Interface VLAN Identifier (0 =  
untagged): 0 Management Interface DHCP Server  
IP Address:  
AP Manager Interface IP Address:  
AP Manager Interface DHCP  
Server: Virtual Gateway IP  
Address: Mobility/RF Group  
Name: MOC  
Enable Symmetric Mobility Tunneling [yes][NO]:  
YES Network Name (SSID): MOC  
Allow Static IP Addresses [YES][no]: NO  
Configure a RADIUS Server now? [YES][no]:  
no  
Warning! The default WLAN Secured policy requires a RADIUS  
server. Please see documentation for more details.
```

Enter Country Code list (enter 'help' for a list of countries)

[US]: GB Enable 802.11b Network [YES][no]: yes

Enable 802.11a Network [YES][no]:

Yes Enable 802.11g Network

[YES][no]: yes Enable Auto-RF

[YES][no]: yes

Configure a NTP server now? [YES][no]: no

Configure the system time now? [YES][no]: no

Warning! No AP will come up unless the time
is set. Please see documentation for more
details.

Configuration correct? If yes, system will save it and reset. [yes][NO]:

yes Configuration saved!

The following is just a sample of the procedure; however the initial configuration may vary due to the changing requirements of the project. The screen shots will be useful only for reference. The ip addressing scheme used in this screen shots will not reflect actual ip used.

Now we have to create the interfaces for the Vlans. First for the Secured (CORP) vlan.

Go to Controller Interfaces

The screenshot shows a Cisco Wireless Local Controller (WLC) interface. The URL in the browser is <https://192.168.1.1/screens/frameset.html>. The page title is "QAPCO_WLC - Windows Internet Explorer provided by Yahoo!". The navigation bar includes links for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The CONTROLLER tab is selected. On the left, a sidebar menu under "Controller" lists: General, Inventory, Interfaces (which is selected), Network Routes, Internal DHCP Server, Mobility Management (expanded to show Spanning Tree, Ports, Master Controller Mode, Network Time Protocol, QoS, and CDP), and CDP. The main content area is titled "Interfaces > New". It contains two input fields: "Interface Name" and "VLAN Id". Below these fields are "Back" and "Apply" buttons. At the bottom of the page, there are "Done", "Local intranet", and "100%" zoom controls.

Give Name for the interface. Give the vlan number you created in the core switch as the vlan Id. And apply.

It will redirect to another page. Here you can give the ip address for the interface followed by dhcp server ip. Apply settings.

The screenshot shows a web browser window titled "QAPCO_WLC - Windows Internet Explorer provided by Yahoo!". The URL is "https://192.168.1.1/screens/frameset.html". The browser toolbar includes "File", "Edit", "View", "Favorites", "Tools", and "Help". The menu bar includes "Web Search", "Bookmarks", "Settings", "Groups", "Mail", "My Yahoo!", "Answers", "Games", and "Anti-Spy". The search bar has "Search", "Images", "Weather", "News", "Highlight", "Resize", and "Pop-up Blocker". The address bar shows "QAPCO_WLC". The main content area is titled "Controller" and shows the "CONTROLLER" tab selected. On the left, a sidebar lists navigation options: General, Inventory, Interfaces, Network Routes, Internal DHCP Server, Mobility Management (selected), Spanning Tree, Ports, Master Controller Mode, Network Time Protocol, QoS, and CDP. The main panel displays several sections: "General Information" (Interface Name: 00:18:b9:ea:7d:e7, MAC Address: 00:18:b9:ea:7d:e7), "Interface Address" (VLAN Identifier, IP Address, Netmask, Gateway), "Physical Information" (The interface is attached to a LAG), "Configuration" (Quarantine checkbox), "DHCP Information" (Primary DHCP Server, Secondary DHCP Server), and "Access Control List". At the bottom right, there are links for "Save Configuration", "Ping", "Logout", and "Refresh". The status bar at the bottom shows "Done", "Local intranet", "100%", and a zoom control.

Similar way create the interface for all the vlans.

Finally you can verify the configuration. Go To Controller → Interfaces

The screenshot shows a Cisco QIB-LWLC web interface in Internet Explorer. The URL is <https://10.130.130.1/screens/frameset.html>. The page title is "QIB-LWLC - Windows Internet Explorer provided by Yahoo!". The main menu includes File, Edit, View, Favorites, Tools, Help, Web Search, Bookmarks, Settings, Groups, Mail, My Yahoo!, Answers, Games, and Anti-Spy. Below the menu is a toolbar with a search bar and a link to Ask.com.

The navigation bar at the top has links for Home, Feeds, Print, Page, and Tools. The main navigation bar below the title bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The CONTROLLER tab is selected.

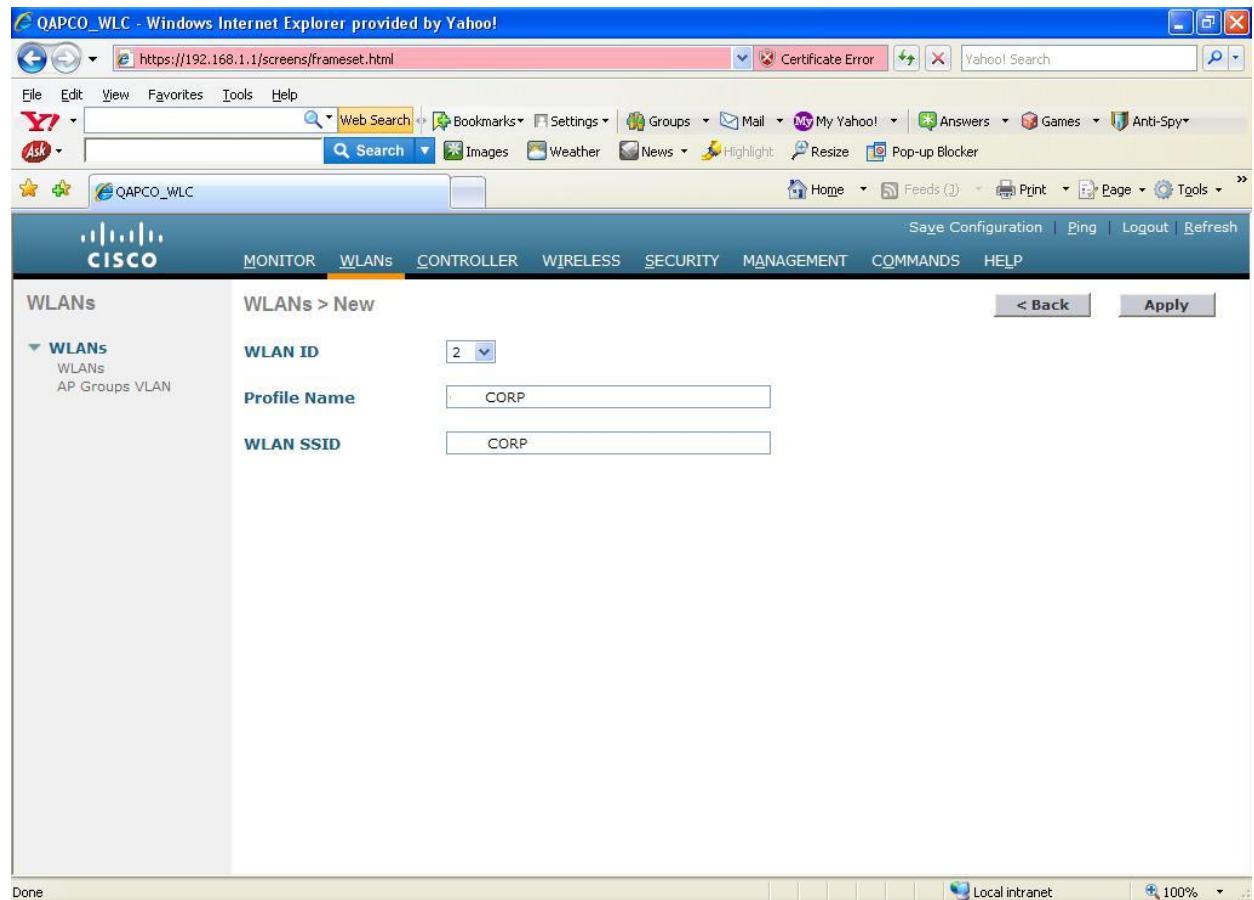
The left sidebar contains a tree view with nodes: Controller (General, Inventory, Interfaces, Multicast, Network Routes, Internal DHCP Server, Mobility Management (Ports, NTP, CDP, Advanced), and Advanced).

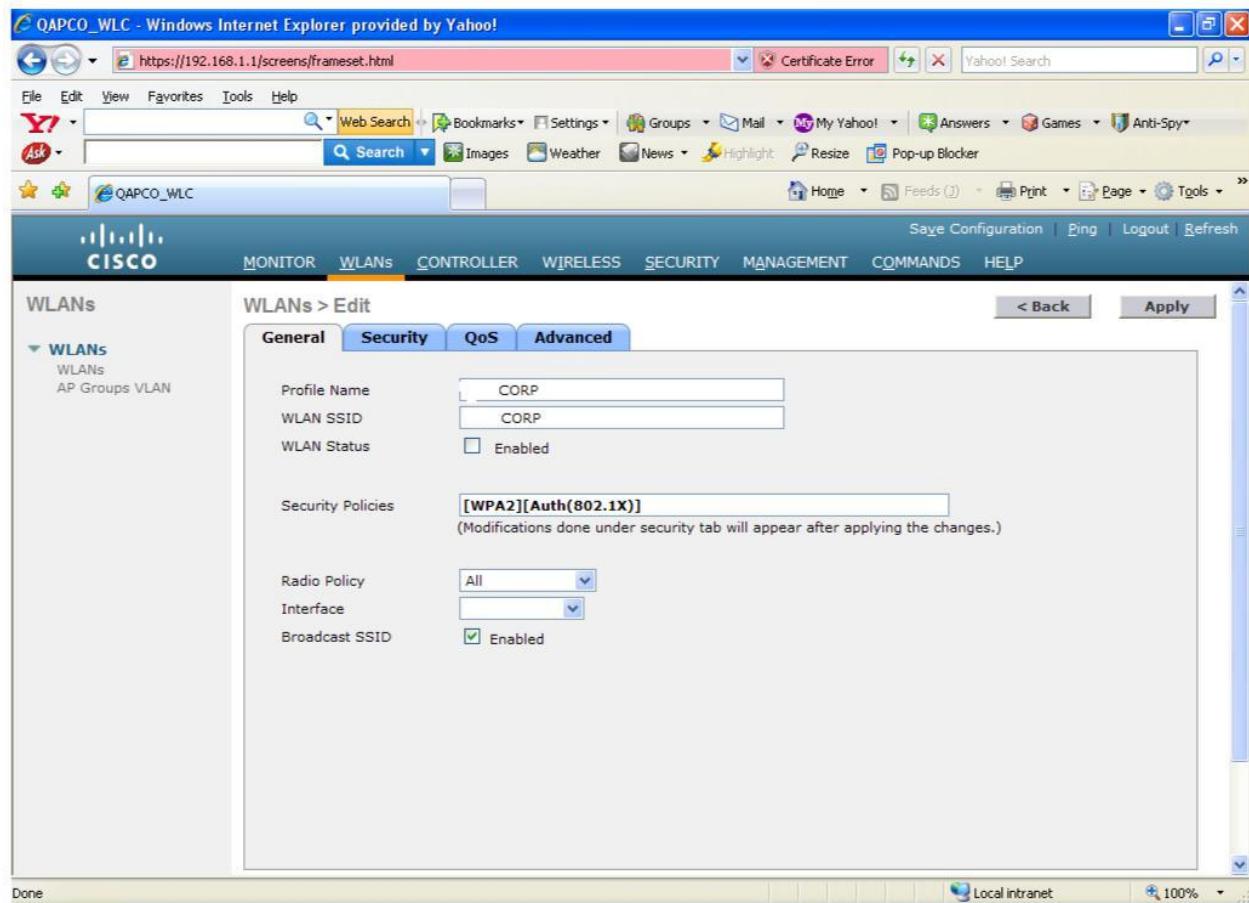
The right panel displays a table titled "Interfaces". The columns are: Interface Name, VLAN Identifier, IP Address, Interface Type, and Dynamic AP Management. The table lists the following interfaces:

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
ap-manager	untagged	10.130.130.2	Static	Enabled
management	untagged	10.130.130.1	Static	Not Supported
3rd_floor	433	10.130.133.1	Dynamic	Disabled
5th_floor	435	10.130.135.1	Dynamic	Disabled
6th_floor	436	10.130.136.1	Dynamic	Disabled
service-port	N/A	0.0.0.0	Static	Not Supported
virtual	N/A	1.1.1.1	Static	Not Supported

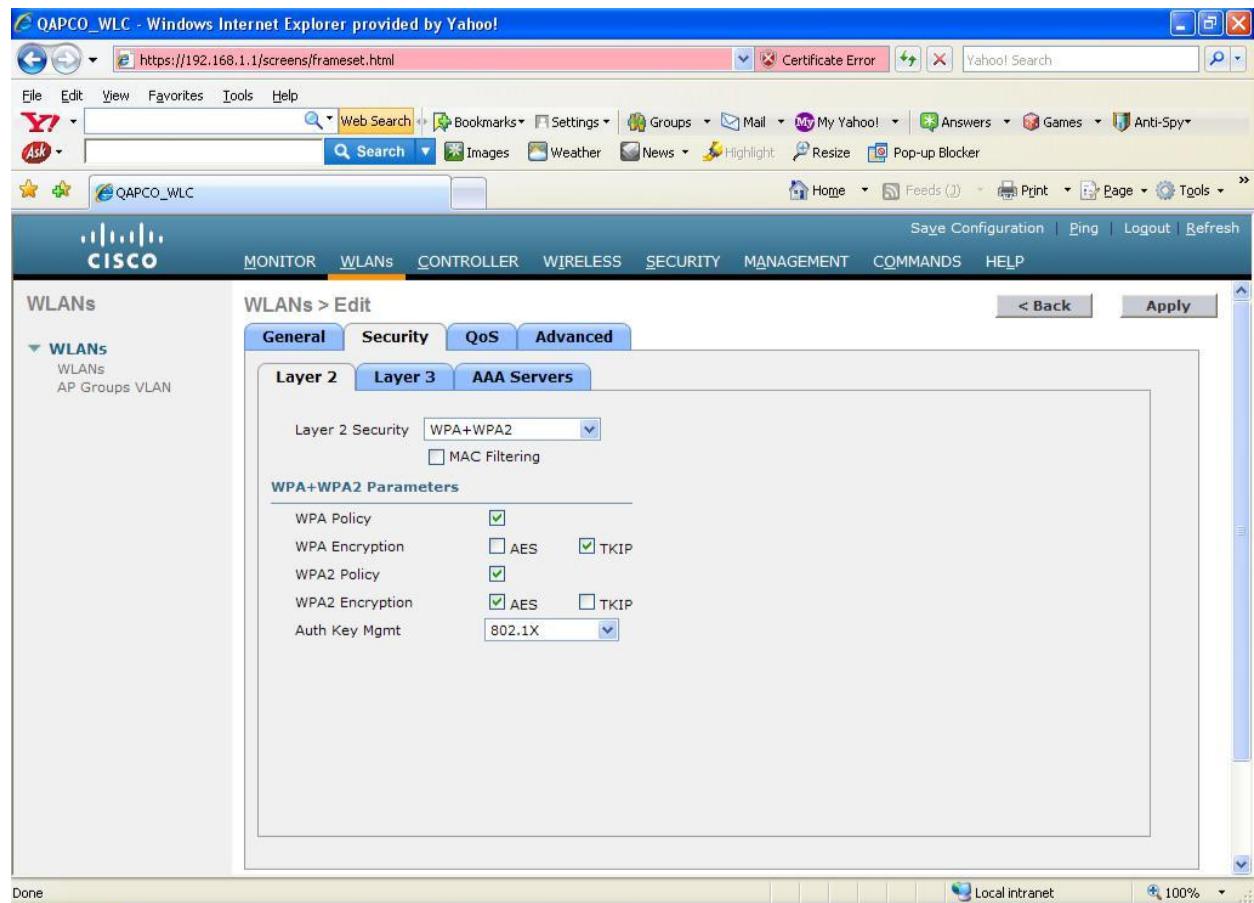
MOC Low Level Design

To create WLANS Go to WLANS, to create new WLAN select new. Then give any WLAN ID from the drop down menu and give a name for the SSID and select apply.





Enable the WLAN Status, Enable Broadcast SSID, and select the appropriate interface from the drop down menu.



Select Layer 2 Security as WPA+WPA2 and select the WPA policies and Encryption parameter as above. Make sure Auth Key Mgmt as 802.1X. Select Authentication and Accounting Server as ACS IP address which has already added as Radius servers under Security Menu.

MOC Low Level Design

The screenshot shows the Cisco Wireless Local Controller (WLC) web interface. The URL in the browser is <https://192.168.1.1/screens/frameset.html>. The page title is "QAPCO_WLC - Windows Internet Explorer provided by Yahoo!". The main menu includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The sub-menu under WLANs shows "WLANS" and "AP Groups VLAN". The current page is "WLANS > Edit" under the "Security" tab. The sub-tab "AAA Servers" is selected. The interface displays "Radius Servers" and "LDAP Servers" sections. Under Radius Servers, there are three servers: Server 1 (IP:10.129.9.151, Port:1812), Server 2 (None), and Server 3 (None). Under Accounting Servers, the "Enabled" checkbox is checked. Under LDAP Servers, all three servers (Server 1, Server 2, Server 3) are set to "None". A "Local EAP Authentication" section is also present with an "Enabled" checkbox. At the bottom right of the interface, there are buttons for "Save Configuration", "Ping", "Logout", and "Refresh".

Make sure to add the ACS as Radius server on the controller before configuring AAA servers for required SSID

Go to Secured AAA Radius Authentication.

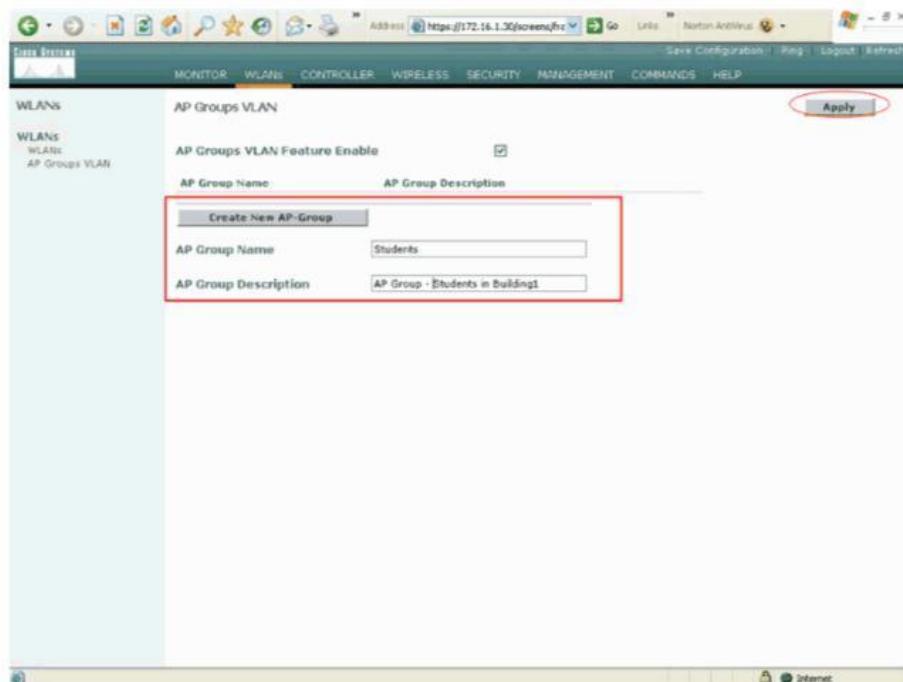
Add ACS as Authentication Server

The screenshot shows a Cisco Wireless LAN Controller (WLC) configuration page. The URL is <https://192.168.1.1/screens/frameset.html>. The main menu at the top includes MONITOR, WLANS, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The SECURITY tab is selected. On the left, a navigation tree shows sections like AAA, Local EAP, Priority Order, Access Control Lists, etc. The main panel displays the 'RADIUS Authentication Servers > New' configuration screen. The 'Server Index (Priority)' dropdown is set to 1. The 'Server IP Address' field contains 10.129.9.151. The 'Shared Secret Format' dropdown is set to ASCII, and the 'Shared Secret' field contains '*****'. The 'Confirm Shared Secret' field also contains '*****'. There is a note about 'Key Wrap' being designed for FIPS customers. Other fields include Port Number (1812), Server Status (Enabled), Support for RFC 3576 (Enabled), Retransmit Timeout (2 seconds), Network User (Enable checked), and Management (Enable checked). Buttons for 'Back', 'Apply', and 'Save Configuration' are visible.

Create all the interfaces for the corporate user vlans. Once all the interfaces are created bind all interfaces with a single SSID using the AP Group Vlan feature. To configure Ap group vlans, go to WLANS-> AP Group Vlan.

Give a name and description for the AP Group and then Apply.

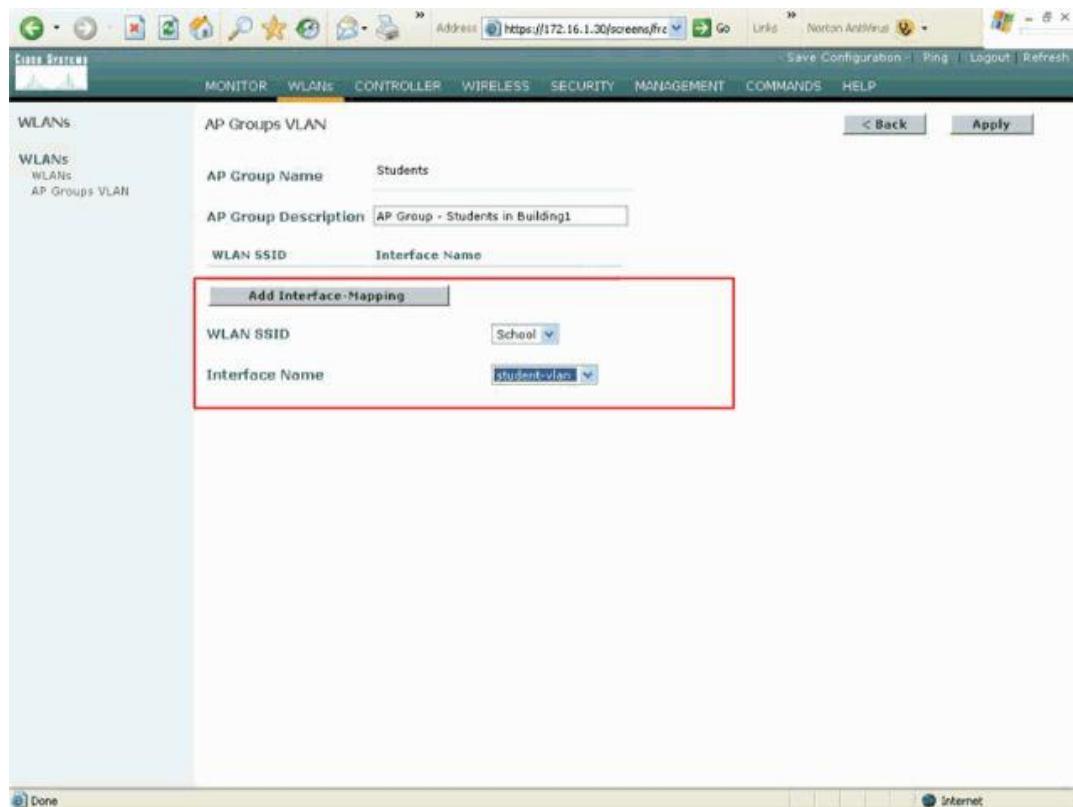
MOC Low Level Design



For a new AP group, click on **Detail**. Select the appropriate SSID from the WLAN

SSID pull-down menu and the interface with which you wish to map this AP group.

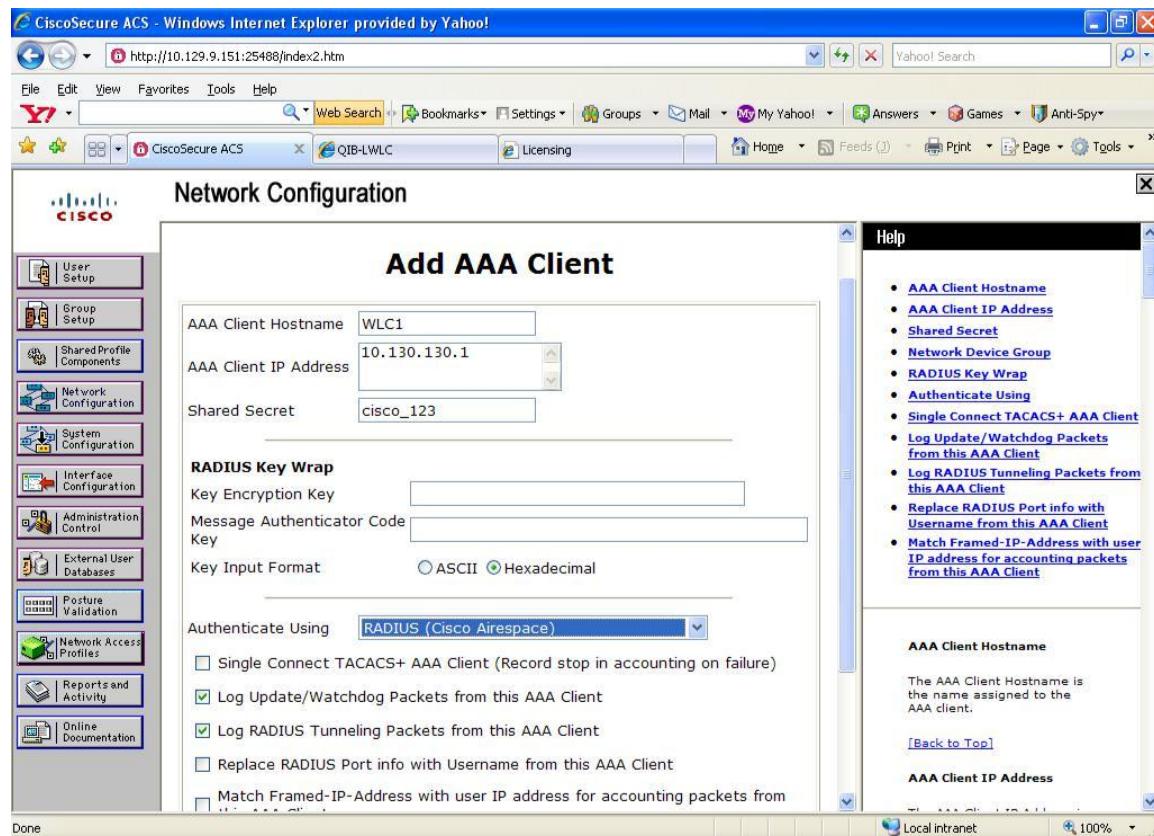
Then click on the add interface mapping. With this same procedure we can map all the interfaces to a single SSID called MOC_CORP.



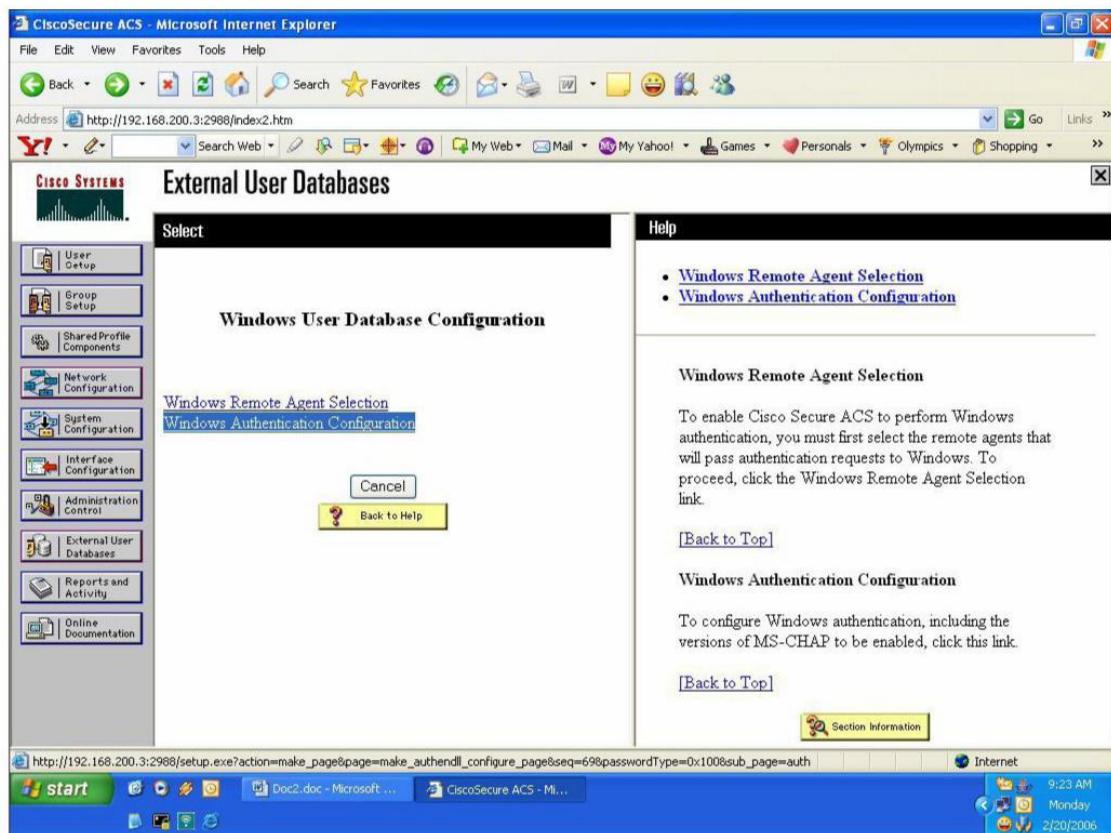
The final task is to assign the LAPs to the appropriate AP groups. To do this go to controller->wireless. Select one of the AP then click detail. Then Map the AP to the corresponding AP group from the drop down menu.

ACS Configuration For PEAP Authentication

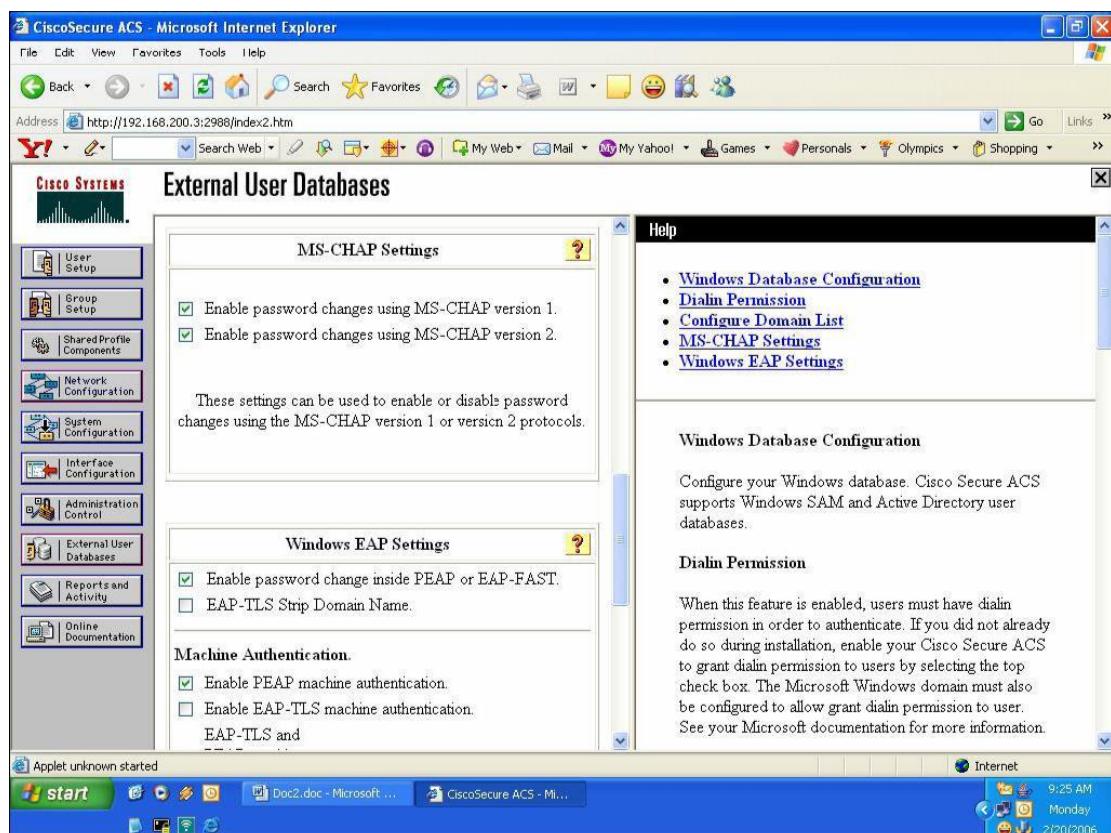
Log in to the ACS and click network configuration in the main tab and go to the not assigned group to add the Wireless lan controller.



Similarly add the second controller also. Then from the external user data bases select windows authentication configuration.

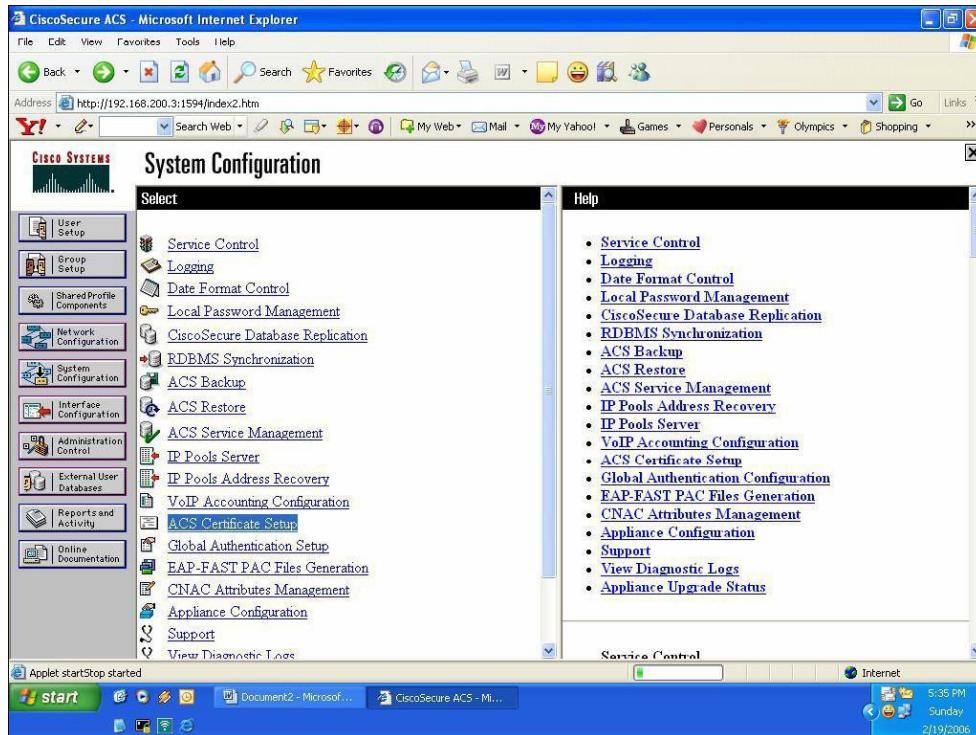


Click 'Windows authentication configuration'. From the list select the appropriate domain.

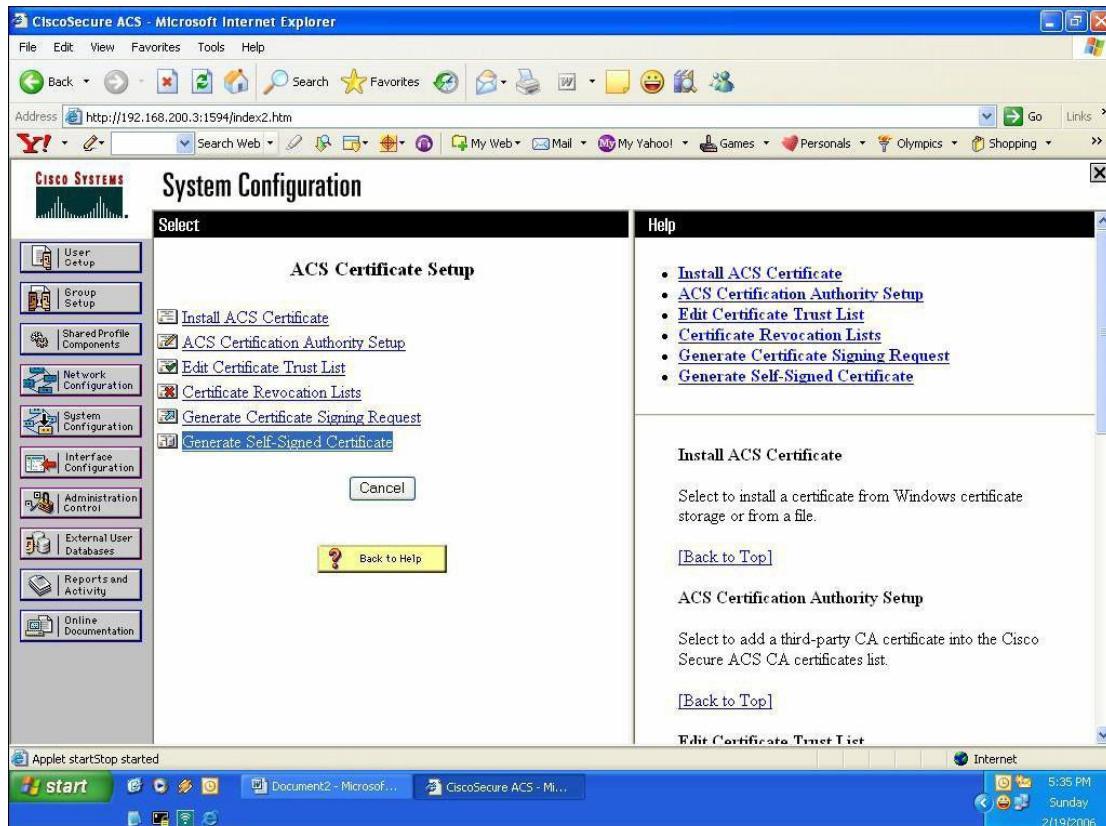


Scroll down and ensure these options are checked. Click submit at the end.

Click 'System configuration' in the main tab (this is to create the self signed certificate which will be used for PEAP)



Select 'ACS certificate setup'.



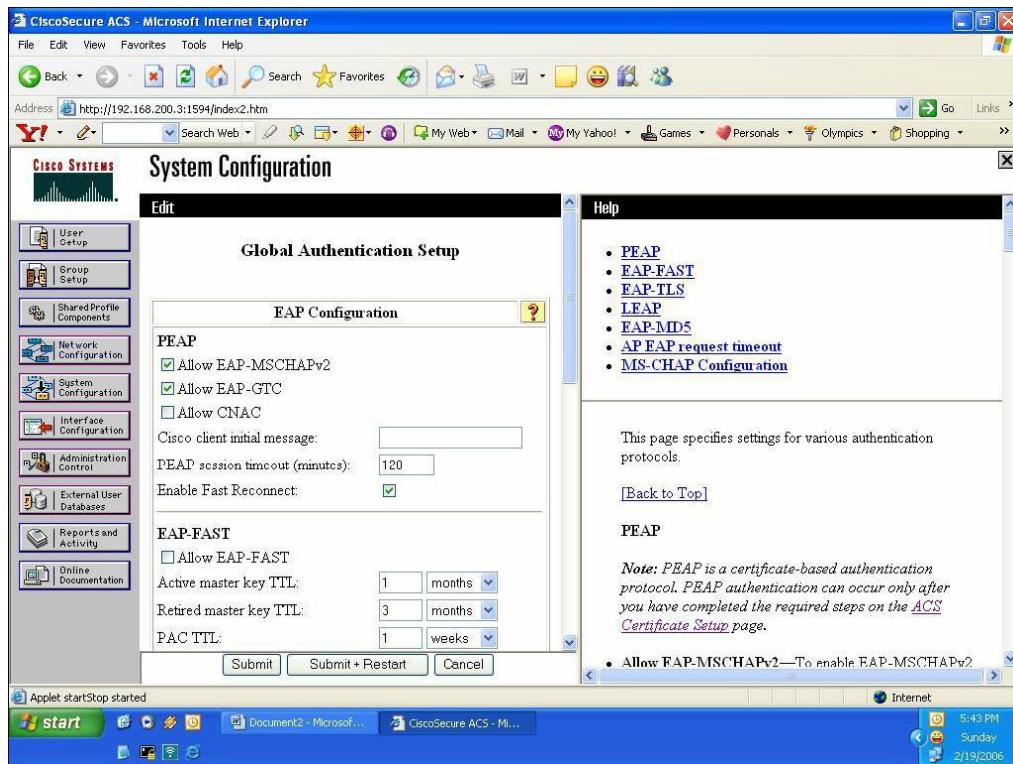
Select 'generate self signed certificate'

MOC Low Level Design

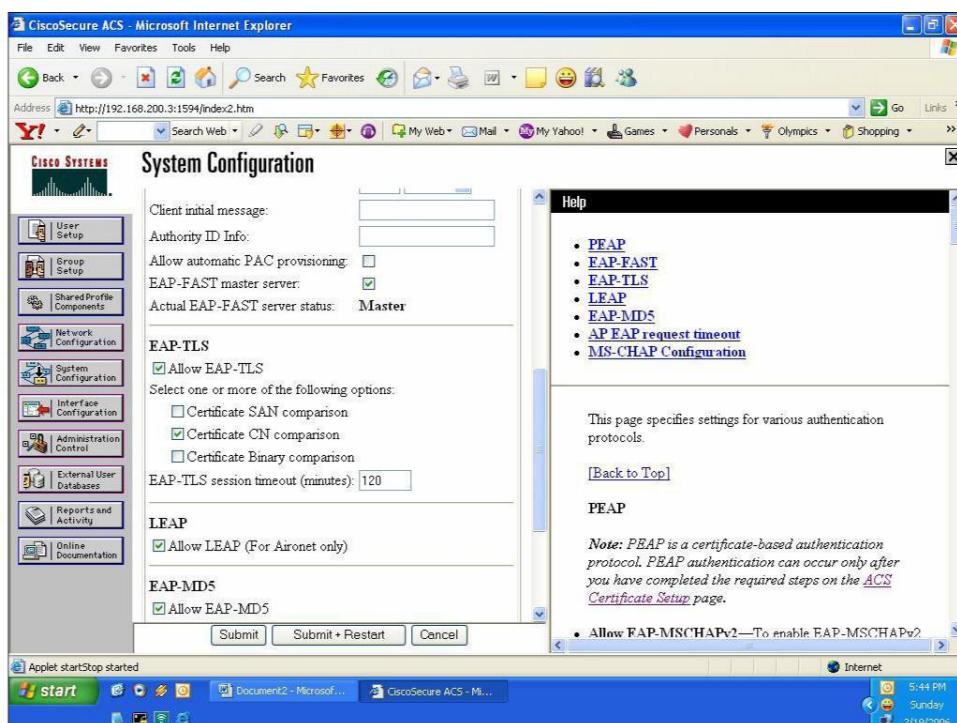
Enter the required fields. (certificate subject: cn=MOC)

Go to the 'install ACS certificate' to verify the certificate generated.

Click 'global authentication setup' in the system configuration setup in order to setup PEAP.



Ensure the following options are ticked for 'PEAP configuration':



Click submit + restart at the end.

Guest Access

There is a dedicated wireless guest SSID to isolate guest traffic from the corporate traffic. The guest SSID is a broadcast to facilitate the guests for easier connectivity. Guest authentication is provided through captive portal on the Guest controller. The user database resides on Cisco NAC Guest server and not local to the Guest controller. When the guest laptop connects to the wireless guest SSID and tries to browse the web, he will be automatically presented with a log-in screen. Guests will use the temporary time based accounts generated through NAC Guest server.

For creating guest users, there is an option to create a user called Sponsor user account who can manage guest account creation and deletion. The Sponsor user account is not allowed to view or modify other settings of the NAC Guest Server.

Sponsor user account privilege can be given to helpdesk where they can manage guest accounts.

Guest Users Authentication Process

The internal DHCP server in the Guest controller is utilized to provide IP Addresses to the guests. Guest tunneling provides additional Secured guest user access to the corporate wireless network,

helping to ensure that guest users are unable to access the corporate network without first passing through the corporate firewall.

This module will cover all the aspects of Wireless guest infrastructure in MOC. Wireless guest controller is connected to the DMZ zone. Wireless guest controller is providing the IP address to the guest user from the dhcp scope which is configured in the guest controller.

Configure Auto Anchor Mobility

The following is a step-by-step procedure to configure the Mobility Anchor Controller (Guest Controller):

- ✓ Create a mobility group in the LAN controller and guest controller.
 - ✓ Add the MAC address and IP address of the guest controller in the LAN controller as a mobility group member.
-

- ✓ Similarly add the MAC address and IP address of all the remote controllers/LAN controllers in the guest controller.
- ✓ Add the mobility anchor configuration on the guest' WLAN on the primary and guest controller.
- ✓ For connectivity testing **eping** and **mping** are tested, on a successful testing EoIP tunnel is established.

To create the mobility group, go to Controller → Mobility Groups. Once the controllers are configured to be part of the same mobility group, we can create the mobility anchor between the LAN controller and the guest controller. The mobility anchor feature is created on the controllers on a specific SSID basis. The guest SSID and its corresponding interface needs to be present in the DMZ guest controller where the Ethernet over IP (EoIP) tunnel is terminated.

The following ports should be open between Guest controller in the DMZ and local controller.

- UDP 16666 for tunnel control traffic
- UDP 16667 for encrypted traffic
- IP Protocol 97 for user data traffic
- UDP 161 and 162 for SNMP

To create the mobility group, go to Controller → Mobility Groups. Add the Guest Controller's MAC address with Management IP in Mobility Group Members Edit area. Make sure to provide mobility group name given for Guest controller along with MAC/IP address details as follow. Similarly add the mac address and ip address of the remoter controller in the guest controller.

QIB-LWLC - Windows Internet Explorer provided by Yahoo!

File Edit View Favorites Tools Help

Web Search Bookmarks Settings Groups Mail My Yahoo! > Ask Search Images Weather News Highlight Resize

QIB-LWLC Home Feeds Print Page Tools >

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Controller

Mobility Group Members > Edit All

< Back Apply Content

This page allows you to edit all mobility group members at once. Mobility group members are listed below, one per line. Each mobility group member is represented as a MAC address, IP address and group name(optional) separated by one or more spaces.

00:22:55:90:9f:c0	10.130.130.1
00:1e:4a:ff:21:e0	192.168.208.7

Done Local intranet 100%

QIB-LWLC - Windows Internet Explorer provided by Yahoo!

File Edit View Favorites Tools Help

Web Search Bookmarks Settings Groups Mail My Yahoo! > Ask Search Images Weather News Highlight Resize

QIB-LWLC Home Feeds Print Page Tools >

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Controller

Static Mobility Group Members

New... EditAll

Local Mobility Group

MAC Address	IP Address	Group Name
00:22:55:90:9f:c0	10.130.130.1	
00:1e:4a:ff:21:e0	192.168.208.7	

Done Local intranet 100%

Repeat the same for Guest controller

The screenshot shows a Cisco Wireless Controller interface in a web browser. The URL is <https://192.168.208.7/screens/frameset.html>. The browser title bar says "QIB-GWLC1 - Windows Internet Explorer provided by Yahoo!". The page header includes links for Save Configuration, Ping, Logout, and Refresh.

The main navigation menu at the top has tabs: MONITOR, WLANS, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The CONTROLLER tab is selected.

The left sidebar contains a tree view of configuration categories:

- Controller
- General
- Inventory
- Interfaces
- Multicast
- Network Routes
- Internal DHCP Server
- Mobility Management** (selected)
- Ports
- NTP
- CDP

The "Mobility Management" section contains three sub-links: Mobility Groups, Mobility Anchor Config, and Multicast Messaging.

The main content area is titled "Mobility Group Members > Edit All". It contains a description: "This page allows you to edit all mobility group members at once. Mobility group members are listed below, one per line. Each mobility group member is represented as a MAC address, IP address and group name(optional) separated by one or more spaces." Below this is a text input field containing two entries:

```
00:1e:4a:ff:21:e0 192.168.208.7
00:22:55:90:9f:c0 10.130.130.1
```


The screenshot shows a Cisco Mobility Controller interface in a web browser. The URL is <https://192.168.208.7/screens/frameset.html>. The browser title bar says "QIB-GWLC1 - Windows Internet Explorer provided by Yahoo!". The main menu includes File, Edit, View, Favorites, Tools, Help, and a toolbar with Web Search, Bookmarks, Settings, Groups, Mail, My Yahoo!, and other links.

The navigation bar at the top has icons for Home, Feeds, Print, Page, and Tools. Below the navigation bar, the Cisco logo is followed by tabs: MONITOR, WLANs, **CONTROLLER**, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The CONTROLLER tab is selected.

The left sidebar under "Controller" lists: General, Inventory, Interfaces, Multicast, Network Routes, Internal DHCP Server, **Mobility Management** (selected), Ports, NTP, and CDP. Under Mobility Management, there are sub-links: Mobility Groups, Mobility Anchor Config, and Multicast Messaging.

The main content area is titled "Static Mobility Group Members". It shows a table with one entry:

Local Mobility Group QIBG		
MAC Address	IP Address	Group Name
00:1e:4a:ff:21:e0	192.168.208.7	
00:22:55:90:9f:c0	10.130.130.1	

Buttons "New..." and "EditAll" are located above the table. The status bar at the bottom shows "Local intranet" and "100%".

Once the controllers are added to the same mobility group we can create the mobility anchor relationship between the local controller and the remote controller.

In the local controller select the IP of the Guest controller from the drop down menu and click mobility anchor create button.

The screenshot shows a Cisco Mobility Controller interface within a Windows Internet Explorer browser window. The URL is <https://172.18.136.12/screens/frameset.html>. The page title is "Cisco_1f:f8:83 - Windows Internet Explorer provided by Yahoo!". The main navigation menu includes MONITOR, WLANS, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The WLANS section is selected, and the sub-menu shows "WLANS" and "Advanced". The sub-sub-section "Mobility Anchors" is currently active. A table lists a single entry for "DT-Guest" with the following details:

WLAN SSID	DT-Guest	Data Path	Control Path
Switch IP Address (Anchor)	local 192.168.22.10	up down	up down

Below the table is a button labeled "Mobility Anchor Create". A dropdown menu labeled "Switch IP Address (Anchor)" is open. The status bar at the bottom indicates "Done" and "Internet".

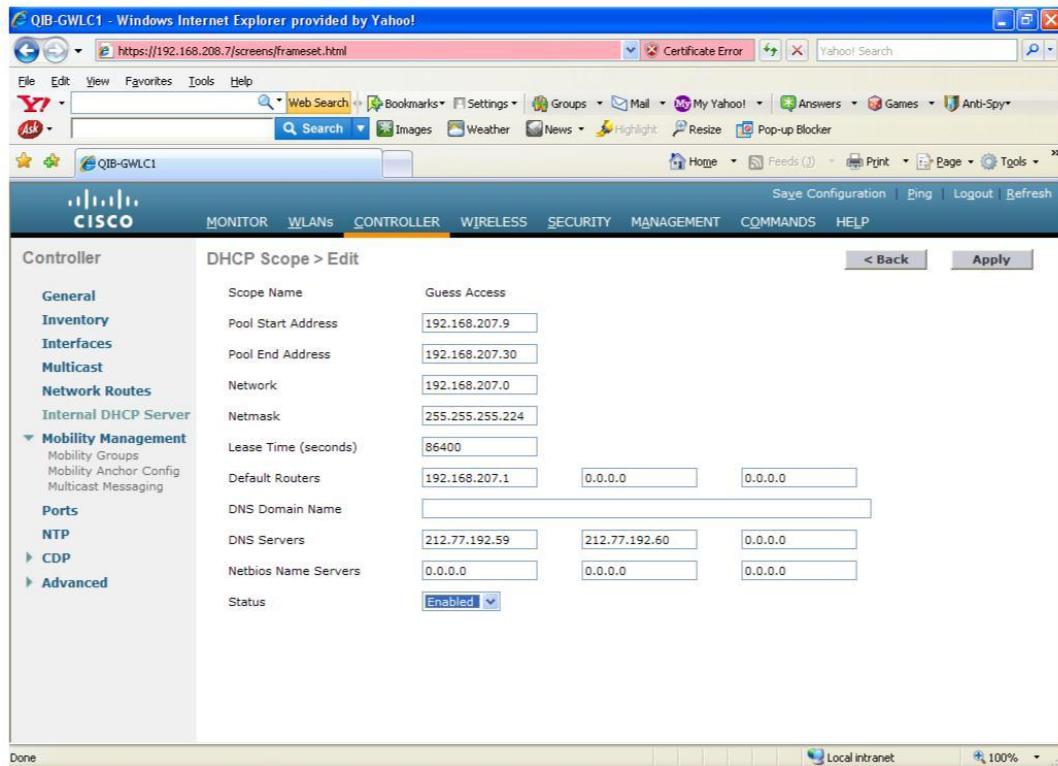
Similar manner, from the guest controller select the ip of the local controller and click the mobility anchor create button.

MOC Low Level Design

The screenshot shows a Cisco Wireless Local Controller (WLC) interface running on a Windows Internet Explorer browser. The URL is <https://192.168.22.10/screens/frameset.html>. The page title is "DT-WLC-GUEST - Windows Internet Explorer provided by Yahoo!". The navigation bar includes File, Edit, View, Favorites, Tools, Help, and a search bar. The main menu bar has links for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The current section is "WLANs". On the left, there's a sidebar with "WLANS" expanded, showing "WLANS" and "Advanced". The main content area is titled "Mobility Anchors" and shows a table for "DT-Guest". The table has columns for "WLAN SSID", "Switch IP Address (Anchor)", "Data Path", and "Control Path". It lists one entry: "local" with IP "172.18.136.12" and both Data and Control paths set to "up". There is also a "Mobility Anchor Create" button. Below the table is a dropdown menu labeled "Switch IP Address (Anchor)".

Once the mobility anchor is created we can test the tunnel by ping tests Create the DHCP scope in the Guest Controller for the guest users.

MOC Low Level Design



NAC Guest Server Configuration

Cisco NAC Guest Server allows any user with privileges to easily create temporary guest accounts and sponsor guests. Cisco NAC Guest Server performs full authentication of sponsors, the users who create guest accounts, and allows sponsors to provide account details to the guest by printout, email or SMS. The entire experience, from user account creation to guest network access, is stored for audit and reporting.

The Cisco NAC Guest Server provisions the guest account for the amount of time specified when the account is created.

Initial configuration of the NAC Server can be configured via CLI and rests of the configuration can be done via GUI by entering

Add a local user account in order to create guests users in the NAC Guest Server

MOC Low Level Design

Add a new Local User Account - Windows Internet Explorer provided by Yahoo!

https://10.129.9.152/admin/adduser.php

Cisco Add a Local User Account

Local User Accounts can create guest user accounts.

First Name: Lobby
Last Name: Ambassador

Username: mannal
Password: *****
Repeat Password: *****

Group: DEFAULT

Email Address:

Add User Reset Form

Main Home/Summary Logout

Authentication Local Users AD Authentication Admin Accounts User Groups

Guest Policy Username Policy Password Policy

Devices NAC Appliance Radius Clients Email Settings SMS Settings

User Interface Templates Mapping

Server Network Settings Date/Time Settings SSL Settings System Log

Done Local intranet 100%

The screenshot shows a web-based administration interface for a Cisco device. The main title is "Cisco Add a Local User Account". Below it, a note says "Local User Accounts can create guest user accounts.". The form contains fields for First Name ("Lobby"), Last Name ("Ambassador"), Username ("mannal"), Password (redacted), Repeat Password (redacted), Group ("DEFAULT"), and Email Address (empty). At the bottom are "Add User" and "Reset Form" buttons. On the left, a sidebar menu includes "Main", "Home/Summary", "Logout", "Authentication", "Guest Policy", "Devices", "User Interface", and "Server" sections. The "Authentication" section is expanded, showing "Local Users", "AD Authentication", "Admin Accounts", and "User Groups". The "Devices" section shows "NAC Appliance", "Radius Clients", "Email Settings", and "SMS Settings". The "User Interface" section shows "Templates" and "Mapping". The "Server" section shows "Network Settings", "Date/Time Settings", "SSL Settings", and "System Log". A "Done" button is at the bottom left, and a status bar at the bottom right shows "Local intranet" and "100%".

Integrate the Windows Active Directory with NAC Guest Server

The screenshot shows the Cisco Wireless Local Controller (WLC) interface. On the left, there's a vertical navigation menu with sections like Main, Authentication, Guest Policy, Devices, User Interface, and Server. The main content area is titled "Add Active Directory Domain Controller". It contains a form for "Active Directory Details" with fields for Server Name (HQ-dc01), User Account Suffix (with a note: "The User Account Suffix should start with @ such as @cisco.com"), Domain Controller IP Address (10.129.9.27), Base DN (DC=Prod,DC=loc), AD Username (CNAC), AD Password, and Confirm Password. At the bottom right of the form are "Add Domain Controller" and "Reset Form" buttons.

Once the user is associated to the Guest SSID in the WLC it passes the traffic to the GWLC through the EoIP tunnel. For Guest users we are using Web authentication. For the database we are using NAC Guest server. The NAC guest server is associated with the active directory. So an active directory user can generate the password for the guest users. Once it passed the authentication, the traffic will go to the internet directly through the firewall. So the guest user doesn't have access to the internal network.

MOC Low Level Design

Adding the NAC Guest server to the Controller

The screenshot shows the Cisco Wireless Controller (GWLC) configuration interface via a Microsoft Internet Explorer browser. The URL in the address bar is <https://10.88.68.1/screens/frameset.html>. The page title is "GWLC - Microsoft Internet Explorer". The navigation bar includes links for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The SECURITY tab is selected.

The main content area displays the "RADIUS Authentication Servers" configuration. On the left, a sidebar menu under the AAA section lists General, RADIUS (selected), Authentication, Accounting, TACACS+, LDAP, Local Net Users, MAC Filtering, Disabled Clients, User Login Policies, AP Policies, Local EAP, Priority Order, Access Control Lists, Wireless Protection Policies, Web Auth, and Advanced.

The "Call Station ID Type" dropdown is set to "IP Address". A checkbox for "Use AES Key Wrap" is checked, with a note: "(Designed for FIPS customers and requires a key wrap compliant RADIUS server)".

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	10.88.49.30	1812	Disabled	Enabled

The status bar at the bottom shows the Windows taskbar with icons for Start, Intel(R) PR..., Cisco Syste..., https://1.1...., GWLC - Mic..., gwlc8.JPG - ..., and a clock showing 4:11 PM.

Enable the Layer 3 Secured and Web authentication which shall be used for redirecting the page to the controller via the virtual IP address.

Similarly add the local controller in the NAC Guest server as a Radius Client as below

The screenshot shows the 'Add Radius Client' page in the Cisco NAC Appliance Admin interface. The URL in the browser is <https://10.129.9.152/admin/addradius.php>. The page displays a success message: 'Radius Client has been added. Changes will not take effect until Radius service has been restarted.' A form is present for adding a new Radius Client, with the following fields filled:

Name:	GWLC
IP Address:	192.168.208.7
Secret:	*****
Confirm Secret:	*****
Description:	Guest Controller

Below the form are two buttons: 'Add Radius Client' and 'Reset Form'. The left sidebar contains a navigation menu with categories like Main, Authentication, Guest Policy, Devices, User Interface, and Server, each with sub-options. The 'Devices' category is expanded, showing 'NAC Appliance', 'Radius Clients', 'Email Settings', and 'SMS Settings'. The 'Radius Clients' option is selected, indicated by a blue border around the 'Add Radius Client' button.

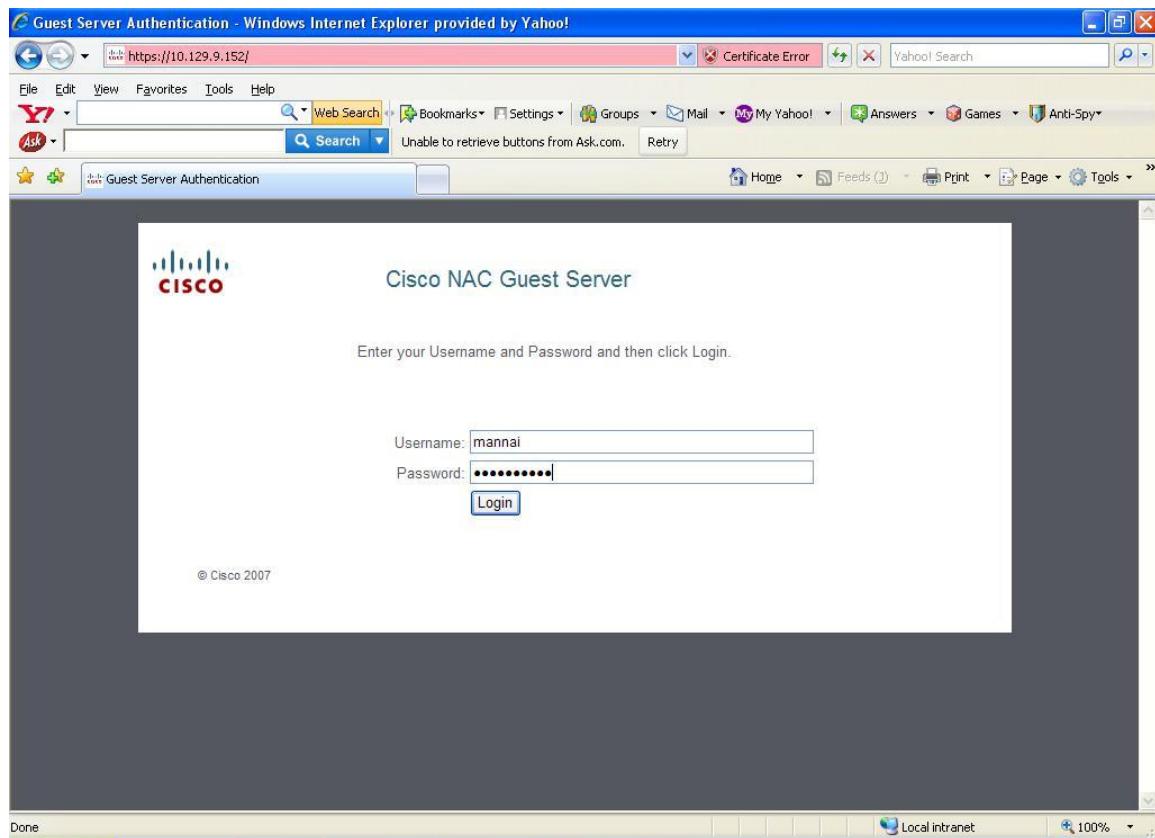
Add SMTP server and a username in order NAC Guest server to send the username/password by email.

The screenshot shows the Cisco NAC Guest server interface. On the left is a vertical navigation menu with sections: Main, Authentication, Guest Policy, Devices, User Interface, and Server. The 'Email Settings' page is currently active, indicated by a teal header bar. The main content area has two sections: 'Change the settings for sending email to guests' and 'Restart Sendmail'. In the first section, there is an 'Enable Email' checkbox (checked), an 'SMTP Server' input field containing '10.129.9.31', and a 'Sent From Email Address' input field. Below these are 'Save Settings' and 'Reset Form' buttons. In the second section, there is a note: 'After saving settings please click Restart to restart the mail component to apply the changes.' followed by a 'Restart' button.

© Cisco 2007 Version 1.0.0

Create a guest username and password by using Lobby administrator account.

- 1) Log into the NAC guest Server using Lobby Administrator username/password



2)Select create Guest User Account option

The screenshot shows a web browser window for the Cisco NAC Guest Server. The URL in the address bar is <https://10.129.9.152/main.php>. The page title is "Welcome to the Cisco NAC Guest Server". On the left, there is a sidebar with navigation links: Main (Home, Logout), User Accounts (Create, Edit, Suspend), and Reporting (Active Accounts, Full Reporting). The main content area displays a list titled "What would you like to do:" with the following options:

- Create a Guest User Account
- Edit Guest User Account end time
- Suspend Guest User Accounts
- View Active Guest User Accounts
- Report on Guest User accounts

3) Enter required information as bellow

The screenshot shows a web browser window titled "Create a Guest User Account - Windows Internet Explorer provided by Yahoo!". The URL in the address bar is <https://10.129.9.152/newuser.php>. The page itself is titled "Create a Guest User Account". On the left, there's a sidebar with navigation links: Main (Home, Logout), User Accounts (Create, Edit, Suspend), and Reporting (Active Accounts, Full Reporting). The main content area contains a form for entering guest user details. The fields include:

- First Name: [text input]
- Last Name: [text input]
- Company: [text input]
- Email Address: [text input]
- Account Start: Time [dropdowns for hours and minutes] : Date [dropdowns for day, month, year] [calendar icon]
- Account End: Time [dropdowns for hours and minutes] : Date [dropdowns for day, month, year] [calendar icon]
- Timezone: [dropdown menu showing "Asia/Bahrain"]

At the bottom of the form are two buttons: "Add User" and "Reset Form".

4) Click Add User. Now the user can access internet service with the username and password.

WCS (Wireless Control System)

WCS includes the same configuration, performance monitoring, Secured, fault management, and accounting options used at the controller level and adds a graphical view of multiple controllers and managed access points. WCS runs on Windows 2000, Windows 2003, and Red Hat Enterprise Linux ES 3 servers. On both Windows and Linux, WCS can run as a normal application or as a service, which runs continuously and resumes running after a reboot.

The WCS user interface enables operators to control all permitted Cisco Wireless LAN Solution

Configuration, monitoring, and control functions through Internet Explorer 6.0 or later. WCS uses the industry-standard SNMP protocol to communicate with the controllers.

A typical Cisco WCS user interface page consists of the following areas:

The screenshot displays the Cisco Wireless Control System (WCS) interface. At the top, there's a navigation bar with links like Home, Monitor, Reports, Configure, Mobility, Administration, Tools, and Help. Below the navigation is a sub-menu for 'WCS Home' with tabs for General, Client, Security, and Mesh. The main content area includes:

- Inventory Detail Status:** Shows 2 Controllers, 16 Radios, and 0 Location Servers. Each category has a large green circular icon.
- Client Count:** A line graph showing the number of clients over time. The x-axis ranges from 14:00 to 11:00, and the y-axis ranges from 0 to 3. The graph shows fluctuating client counts between 0 and 2.
- Coverage Areas:** A section for the site "QIB-HQ" showing coverage details. It lists Total APs (8), a/n Radios (8), b/g/n Radios (8), OOS Radios (0), and Clients (2). A message indicates "No Coverage Holes found".
- Recent Coverage Holes (0):** A table showing coverage hole statistics for QIB-HQ.
- Alarm Summary:** A table showing the count of various types of alarms. The table is as follows:

Category	Total	a/n	b/g/n	OOS	Clients
Malicious AP	0	0	0	0	0
Unclassified AP	0	0	0	0	0
Coverage Hole	0	0	0	0	0
Security	0	0	0	0	0
Controllers	3	0	0	2	0
Access Points	0	0	0	0	0
Location	0	0	0	0	0
Mesh Links	0	0	0	0	0

Now we have to add our WLC to the WCS. For that we need a license. We have to register our private key number with in the WCS package in the cisco site. Here we have to associate our PAK number to the WCS server hostname. If we change the hostname of the server after licensing it will not work. So associate the PAK with the correct hostname. Cisco will send the license key via mail. We can download and store the license file on the hard disk of theWCS server.

Cisco strongly recommends that you print the email, save the attachment to a removable media, and store both in a safe place for future use, if needed by either yourself or anyone in your organization.

Before you proceed, make sure that the WCS server software has been installed and configured on the server.

To install the WCS license, follow these steps:

Step 1 Save the license file ([.lic](#)) to a temporary directory on your hard drive.

Step 2 Open a supported version of the Internet Explorer browser.

Step 3 In the Location or Address field, enter the following URL, replacing IP address or host name of the WCS server: <https://<IP address>>.

Step 4 Log in to the WCS server as system administrator. User names and passwords are case-sensitive.

Step 5 From the Help menu, select [Licensing](#).

Step 6 On the Licensing page, from the Select a command drop-down menu, choose [Add License](#).

Step 7 On the Add License page, click Browse to navigate to the location where you saved the [.lic](#) file.

Step 8 Click [Upload](#).

The WCS server imports the license.

Now we can add the Controller, floor maps and Access points in the WCS.

Adding a controller to the WCS

Address  <https://172.18.4.80/webacs/switchListCommandAction.do>

Wireless Control System

Quick Search <IP, Name, SSID> **Go**

Search Controllers **New Search...**

Saved Searches **Edit** **--Select Search--**

Add Controllers

Add Format Type Device Info

IP Addresses 172.18.36.10 (comma-separated IP Addresses)

Network Mask 255.255.255.0

SNMP Parameters*

Version v2c

Retries 3

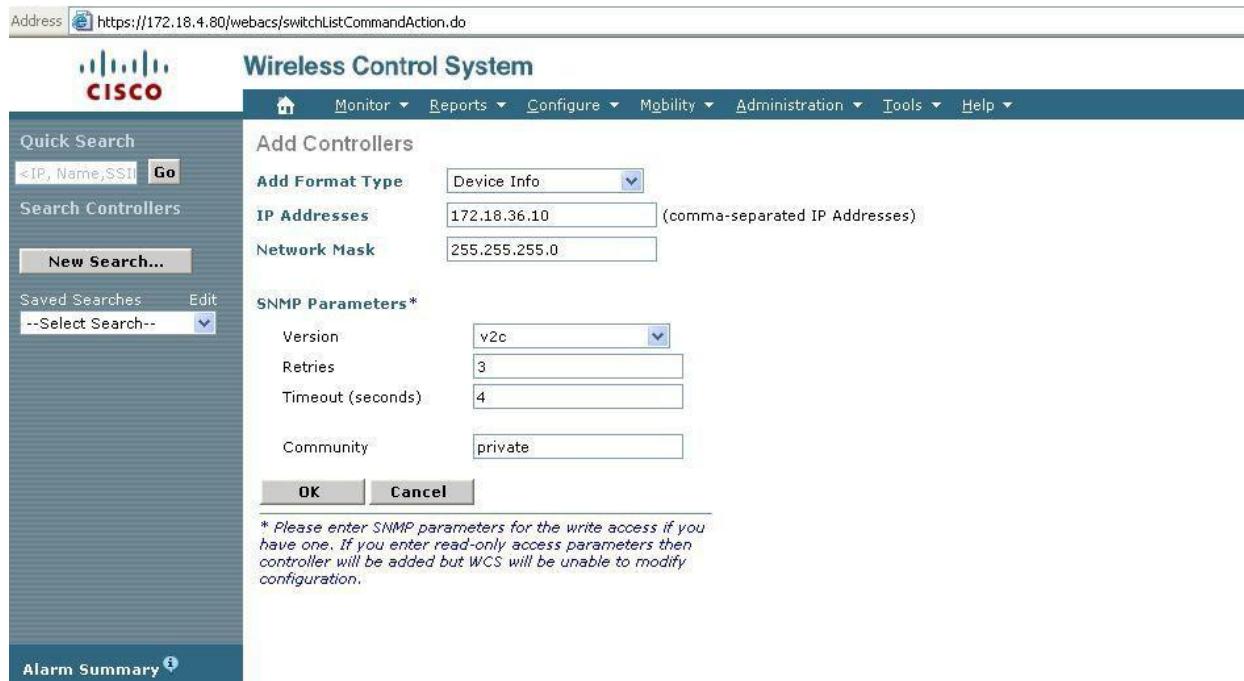
Timeout (seconds) 4

Community private

OK **Cancel**

* Please enter SNMP parameters for the write access if you have one. If you enter read-only access parameters then controller will be added but WCS will be unable to modify configuration.

Alarm Summary 



Document Acceptance Certificate

Title: MOC Network Low Level Design Document

Version: 1.0

Name <hr/>	Name <hr/>
Title <hr/>	Title <hr/>
Company <hr/>	Company <hr/>
Signature <hr/>	Signature <hr/>
Date <hr/>	Date <hr/>

Name <hr/>	Name <hr/>
Title <hr/>	Title <hr/>
Company <hr/>	Company <hr/>
Signature <hr/>	Signature <hr/>
Date <hr/>	Date <hr/>

Name <hr/>	Name <hr/>
Title <hr/>	Title <hr/>
Company <hr/>	Company <hr/>
Signature <hr/>	Signature <hr/>
Date <hr/>	Date <hr/>

