project documentation

EATL Network as Built Documentation

EAST AFRICA TERMINAL LIMITED

28 January 2015
Version 0.01

Sammy Luvinzu (KE)
Tel: 020 499 3000
Mobile: 0723845993
Email: sammy.luvinzu@dimensiondata.com

Dimension Data Contact Details

We welcome any enquiries regarding this document, its content, structure or scope. Please contact:

Sammy Luvinzu (KE) - Network Engineer, Mobile: 0723845993

Dimension Data Solutions Ltd
Landmark Plaza,
3rd Floor,
Argwings Kodhek Road,
Nairobi

☏ 020 499 3000
✉ sammy.luvinzu@dimensiondata.com

Please quote reference in any correspondence or order.

Confidentiality

Contents

List of Figures

List of Tables

About This Design Document

1.1. Document Purpose

The purpose of this document is to provide in detail the implementation documentation for the EATL network. This document provides details on the physical and logical information that was implemented in the EATL network deployment.

This document provides sufficient detail required to service and maintain the network.

1.2. Intended Audience

The intended audience of this document are EATL / Dimension Data technical staff who was maintaining and operating the new network.

1.3. Document Usage Guidelines

The document should be used as a guideline for carrying out various maintenance and operational tasks and any network troubleshooting.

2. Project Scope

2.1. Detailed Project Scope

- Supply and installation of one (1) Cisco 2911 Integrated Services Router.
- Supply and installation of two (2) Cisco 3750X 24port Switches.
- Supply and installation of one (1) Cisco ASA 5515 firewall.
- Supply and installation of two (2) Cisco 2960 48port switches.
- Supply and installation of four (4) Cisco 2960 24port switches.
- Implementation of virtual LANs (VLANs) for data on the core switch and all access layers switches at the EATL Office.
- Implementation of inter-VLAN routing to achieve full IP connectivity.
- Optimization of spanning-tree protocol (STP) on all LAN switches for fast network recovery following a network outage, and optimal, deterministic path selection.
- Documentation of the project.
- Project sign off.

3. Network Architecture

3.1. Network Topology

The overall network topology will include a collapsed backbone design for the LAN at the EATL Office, as illustrated in figure 1 below.

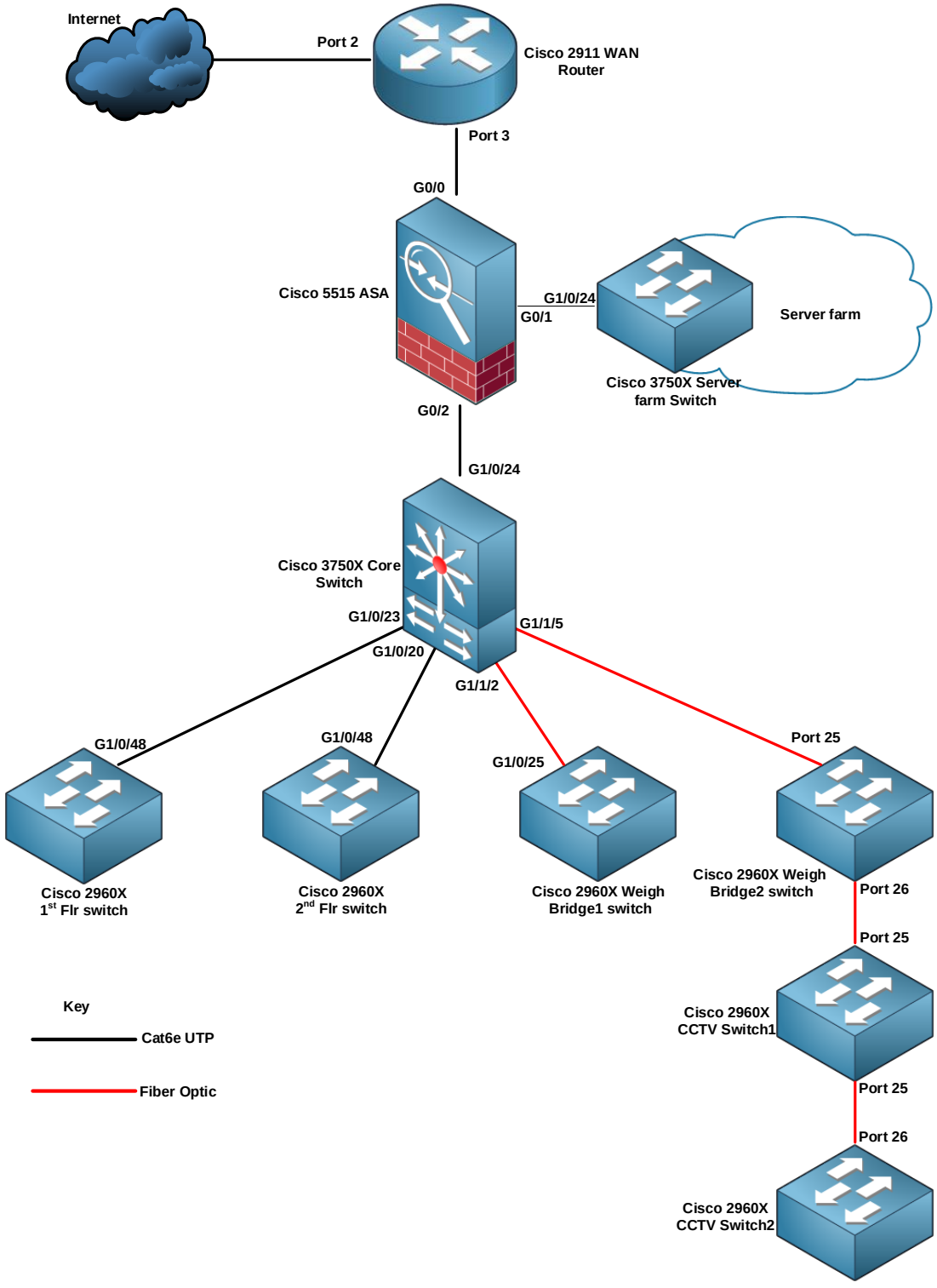

Figure 1EATL Overall Network Design

3.2. Naming Convention for Devices

The purpose of a hostname is to identify a device. Hostnames should be constructed so that anyone with little knowledge of the network can determine the devices' functions. Hostnames should be easy to remember. When a hostname is harder to remember than an IP address, using one is counterproductive. The following device naming has been used based on the best practices.

Table 1Device Names

Hostname	Platform	Device Role	Management IP Address
EATL_WAN_Route	Cisco 2911	WAN Router	
EATL_FW_ASA	Cisco ASA 5515-X	Internet Firewall	10.135.2.145
EATL_ASA_CX	Cisco ASA 5515-X	Internet Firewall CX	10.135.2.148
EATL_CORE_SW	Cisco 3750X	Core Switch	10.135.2.131
EATL_DMZ_SW	Cisco 3750X	Server farm Switch	10.135.2.254
EATL_1FL_SW	Cisco 2960X	1st Floor Access	10.135.2.133
EATL_2FL_SW	Cisco 2960X	2nd Floor Access	10.135.2.134
EATL_WEIGHBRIDGE_SW1	Cisco 2960X	Weigh Bridge 1 Access Switch	10.135.2.135
EATL_WEIGHBRIDGE_SW2	Cisco 2960X	Weigh Bridge 2 Access Switch	10.135.2.136
EATL_CCTV1_SW	Cisco 2960X	CCTV 1 Access Switch	10.135.2.137
EATL_CCTV2_SW	Cisco 2960X	CCTV 2 Access Switch	10.135.2.138

4. Physical Network Design

The physical network design at the EATL office included one cisco 3750X catalyst switch that acts as the core switch, interconnected to the access switches at Weigh Bridge 1 and Weigh Bridge 2 through optic fiber cable. The optic fiber link terminates on SC connectors on the Cisco Core switch. The firewall was connected between the core switch, router and server farm switch.

Connectivity from the core switch to access switches at 1st floor, 2nd floor and the internet router is through cat6e UTP. The server farm switch was connected to the firewall.

UTP was also used for connectivity to all network servers e.g. core application servers in the server room.

5. Logical Network Design

5.1. VLAN Trunking Protocol

VLAN Trunking protocol (VTP) is used on Cisco switches for centralized creation of VLANs. It is ideal for a network using dynamic VLANs, to accommodate mobile workers with no fixed workstations. This was not the case with the network in EATL where departments are situated in fixed geographic locations.

The use of VTP requires that the central switch be configured to operate in VTP server mode, while the rest of the switches are configured to operate in VTP client mode. All VLANs are then created on the central switch, which distributes this information to the rest of the switches. Since the VLANs span the whole network, it is difficult to isolate faults. It is also easy to accidentally delete VLANs with the introduction of a new switch configured as a VTP server (default mode). This strategy is therefore best avoided.

To disable VTP on the network, all switches in EATL were configured to operate in ***VTP transparent mode***.

5.2. VLANs and IP Subnets

A VLAN can be used to logically associate a user community with a common access policy as defined by access control lists (ACLs). Similarly, VLANs can be used within a server farm to associate a group of servers with a common access policy as defined by ACLs. An IP subnet is the logical Layer 3 equivalent of the VLAN at Layer 2, and therefore maps to a VLAN.

5.2.1. Data VLANs & IP Subnets

Consultations with EATL's technical staff determined the need to establish the set of Data VLANs and IP subnets, based on user communities and network services, as listed in table 2 below.

Table 2Data Vlan and IP Subnet

Vlan ID	Vlan name	Subnet	Valid Hosts		Subnet mask
10	Data	10.135.2.0	10.135.2.1	10.135.2.126	255.255.255.128
5	Servers	10.135.2.224	10.135.2.225	10.135.2.254	255.255.255.224
2	CCTV	10.135.2.192	10.135.2.193	10.135.2.222	255.255.255.224

Vlan ID	Vlan name	Subnet	Valid Hosts		Subnet mask
N/A	P2P BTWN CSW & ASA	10.135.2.152	10.135.2.153	10.135.2.158	255.255.255.248
N/A	P2P BTWN RTR & ASA	10.135.2.144	10.135.2.145	10.135.2.150	255.255.255.248
8	Management	10.135.2.128	10.135.2.129	10.135.2.142	255.255.255.240

5.2.2. VLANs per Switch

The above VLAN was implemented statically on the individual switches, as shown in table 3 below.

Table 3VLAN Locations

Device Name	Location	VLAN
EATL_Core_Switch	Server room	2, 4, 8, 10
EATL_DMZ_Switch	Server room	
EATL_1stFloor_Switch	Server room	8, 10
EATL_1stFloor_Switch	2nd Floor	8, 10
EATL_WeighBridge1_Switch	Weigh bridge 1	2,8,10
EATL_WeighBridge2_Switch	Weigh bridge 2	2,8,10
EATL_CCTV1_Switch	CCTV 1	2,8
EATL_CCTV2_Switch	CCTV 2	2,8

5.3. Access Ports

Switch ports where user hosts, servers, routers, firewalls, printers and other non-switch devices are connected are called access ports, and are generally allocated VLAN membership. All access ports was optimized to operate in VLAN access mode, to eliminate the possibility of a workstation negotiating to form a VLAN trunk with the switch, and reduce the time user ports take to become active when a workstation is connected.

5.4. Trunk Ports

Switch-to-switch links are typically configured as trunk ports, and not allocated VLAN membership, since they carry traffic from multiple VLANs using VLAN trunking protocols. The Cisco switches provided in this project support two VLAN trunking

protocols i.e. Inter-Switch Link (ISL), a Cisco proprietary protocol, and IEEE802.1Q, a standards-based protocol. By default, Cisco switch ports dynamically negotiate trunking, a process that introduces some latency before the ports become active.

All trunk ports in EATL Network were explicitly configured to operate as IEEE802.1Q VLAN trunks, to eliminate dynamic trunking negotiation, thereby reducing the time the trunks take to become active.

5.5. Spanning Tree Protocol (STP)

Ethernet switching is prone to bridging loops when physical loops are introduced, a situation which effectively shuts the network down. Spanning tree protocol (STP) addresses this problem by creating a loop-free topology. A downside to STP is its long convergence time (up to 50s), during topology changes, or when switches are first powered.

A relatively new standard, Rapid STP (RSTP), which eliminates this latency, is available on Cisco switches.

All the new Cisco switches in EATL network was configured to use RSTP. The core switch will then be configured to serve the role of RSTP root for all VLANs.

Other STP optimizations that was implemented include:

- **Portfast**, a feature for rapidly transitioning switch access ports to forwarding state, thus minimizing the long delay typically experience with STP.
- **Bpduguard**, a security feature for ensuring the switch does not receive STP traffic on access ports, and shuts down such interfaces upon receiving STP traffic.
- **Errordisable recovery bpduguard**, a feature that will ensure ports that are automatically shut down due to the bpduguard feature will also be automatically re-enabled after a certain time elapses.

5.6. IP Configurations

5.6.1. IP Addressing

User and Server VLANs was allocated the IP subnets indicated in table 2.

5.6.2. DHCP

User nodes (desktops) in Data VLAN was allocated addresses from the Core switch, using DHCP scopes with address ranges from 10.135.2.21 to 10.135.2.100. Address 10.135.2.1 – 20 was reserved for the default gateway and network printers

Nodes in VLAN 2, 8 and the Server Subnet were allocated IP addresses statically, instead of through DHCP, since they consist of servers and network devices.

5.7. IP Routing on LAN

Static routing was used for communication with the extranet networks, while a default route was used for communication to the Internet. The Core Switch and the internet router were therefore configured accordingly.

WAN Router

Core Switch

5.8. Perimeter Firewall

The information that follows will detail how the Cisco ASA 5515-X firewall appliance was used to secure the network perimeter for East Africa Terminal Limited.

The perimeter security solution was built to provide a single-tier security solution. Behind the firewall is the existing core switch at EATL Mombasa. The firewall acts as the default gateway of the core switch and DMZ servers.

5.8.1. Implemented

The following items were implemented for the perimeter securityt:

Cisco ASA 5515-X Firewall with a CX module:

- Basic configuration of a single Cisco ASA NGFW 5515-X Firewall with no redundancy
- Deployment of the Firewall to interconnect the LAN, DMZ and the Internet Router (Cisco 2911)
- Connecting the Outside interface of the Firewall to the Cisco 2911 Router.
- Connection of the internal interface of the Firewall to the Core Switch and a DMZ switch (Server Farm Switch).
- Configuration of VLANs and routing in the ASA firewall to interconnect various subnets in the network.

- Botnet traffic filter configuration with a Cisco Dynamic Database with reputation of various websites and internet application to monitor, log and/or block malware from entering the EATL network. The Database contains categories of known malware sites, known allowed websites, ambiguous addresses, etc.
- ASA Context Awaness (CX) Module Configuration:
    - Application Visibility and Control (AVC) Software module configuration to monitor and control usage of internet applications such as instant messaging and media streaming applications.
    - Web Security Essentials (WSE) software module configuration to monitor and control access to and usage of web categories such as business sites, gaming sites, proxy, and torrent sites.

5.8.2. Design

The diagram below shows the implemented topology of the EATL Perimeter Security Solution.

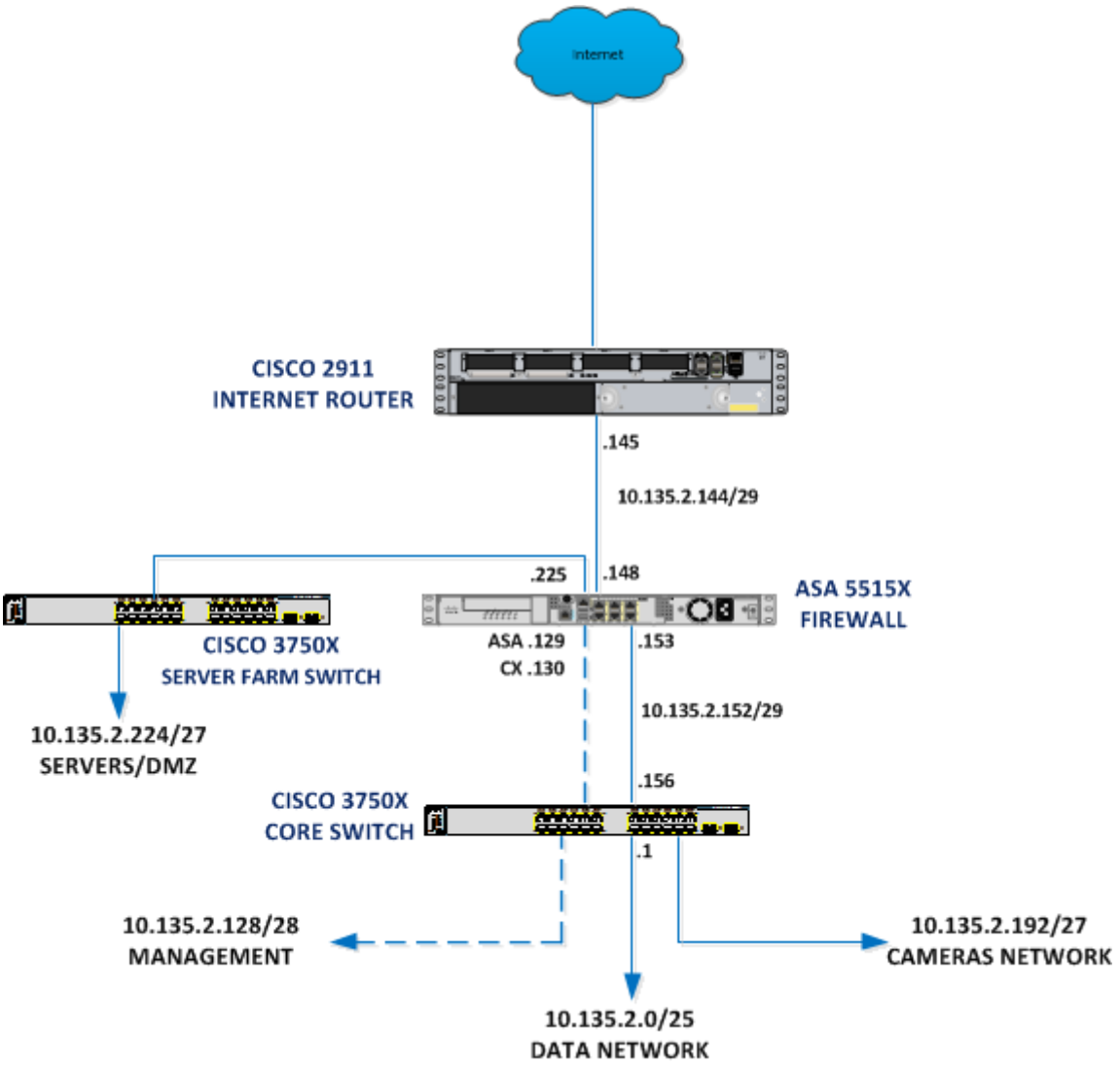

Figure 2 Implemented Physical Topology

The diagram below shows the logical design. The Management interfaces of both ASA Firewalls need to be in an UP state for the CX modules to be reachable over the network.

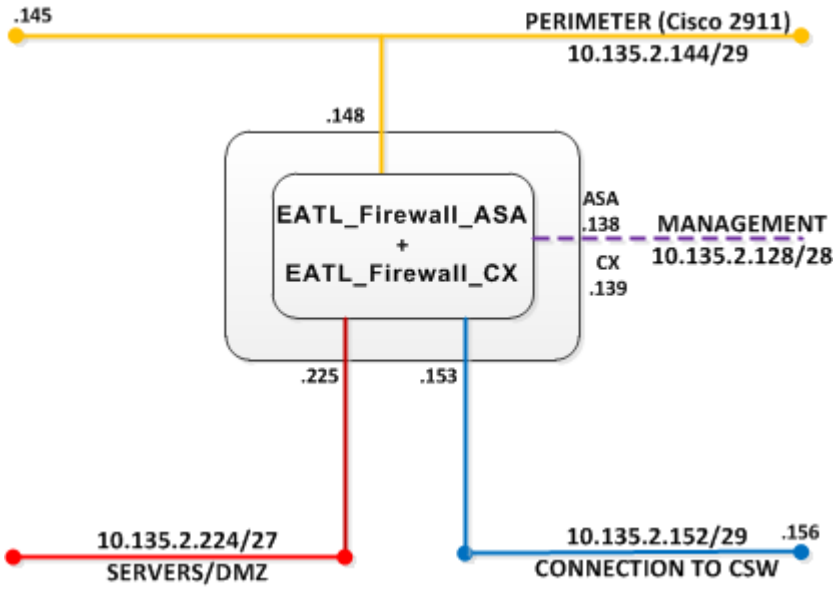

Figure 3 Implemented Logical Design

5.8.2.1. Interfaces

The Gigabit Ethernet interfaces were configured as follows in the EATL ASA Firewalls:

1. GigabitEthernet 0/0 – Outside interface (Cisco 2911 Router)
2. GigabitEthernet 0/1 – DMZ interface
3. GigabitEthernet 0/2 – LAN/Inside interface
4. GigabitEthernet 0/3-5 – Not in use
5. Management 0/0 – CX Management (Needed to be in UP state to allow reachability of CX module)

Each of the interfaces was configured with the following requirements where possible. The Management interface will not be named to allow the CX modules to be in the INSIDE network even though they rely on the Management Interfaces to be in an UP state.

- Description
- Interface name
- Security Levels
- IP address

ASA Firewalls Interface Configuration

PASTE CONFIGS IN HERE!!!!!!!!!!!!!!!!!!!!!!!!

5.8.2.2. **IP Routing**

The ASA appliance needs to know where to send traffic destined for both the inside and outside networks. To do so, static routing was enabled on the ASA appliance. A static route is a way of configuring path selection of routing devices in computer networks without communication between the devices regarding the current topology of the network. This is achieved by manually adding routes to the devices in order to enable it route packets to various destinations.

Dynamic routing, on the other hand, enables the ASA to learn about networks from neighbours participating in the same routing process.

Outside Networks

A static route was defined to direct traffic destined for outside the EATL network. On the Internet Router, we will not allow WAN routes to be NATTED to the Public IP on the external interface of the router. This will ensure that only traffic destined for the Internet get NATTED to the Public IP defined on the Router. To achieve this, the NAT Access Control List will contain deny statements for the WAN networks.

The following routing configurations was made to enable this:

```
PASTE OUTSIDE ROUTING CONFIGS HERE
```

Inside Networks

Static routes was configured pointing to the internal networks via the Core Switch as the Gateway. This is to enable the ASA Firewall to direct returning traffic to the device that made the traffic request and also VPN connections to the internal networks.

ASA Internal Routing Configuration

```
!
route INSIDE 10.135.2.0 255.255.255.0 10.135.2.153 1
!
```

Security Policy

Network Objects and Network Object Groups

```
!
object network DATA_NETWORK
 subnet 10.135.2.0 255.255.255.128
!
object network SERVERS_DMZ_NETWORK
 subnet 10.135.2.224 255.255.255.224
!
object-group network LAN_NETWORKS
 network-object object DATA_NETWORK
!
```

Objects are in use and was configured for ease of reference from Access rules.

Service Objects and Service Object Groups

Service objects are individual ports that make up the source and /or destination services through which applications, websites, servers and other remote resources on a network/Internet are accessed, e.g. web ports such as http and https.

A service object group, much like network object groups, combines several service objects into one unit that can be subjected to the same policies or rules.

```
!
object-group service WEB_ACCESS tcp
 port-object eq www
 port-object eq https
!
object-group service MAIL_ACCESS tcp
 port-object eq imap4
 port-object eq pop3
 port-object eq 465
 port-object eq 587
 port-object eq 993
 port-object eq 995
!
object-group service VPN_SERVICES udp
```

```
 port-object eq 4500
 port-object eq isakmp
!
object-group network DNS_SERVERS
 network-object host <Public_DNS_1>
 network-object host <Public_DNS_2>
!
```

Service Policy

This policy is for protocol application inspection and CX processing redirection. The following class maps, policy maps and service policies were configured on the ASA Firewall.

```
!
class-map dynamic-filter_snoop_class
 match port udp eq domain
class-map inspection_default
 match default-inspection-traffic
class-map default
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
```

```
 inspect sip
 inspect netbios
 inspect tftp
 inspect ip-options
 inspect icmp
class class-default
 cxsc fail-open auth-proxy
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map dynamic-filter_snoop_policy
 class dynamic-filter_snoop_class
  inspect dns preset_dns_map dynamic-filter-snoop
policy-map map
!
service-policy global_policy global
service-policy dynamic-filter_snoop_policy interface OUTSIDE
!
```

Firewall Rule Base

ASA Firewalls allow the definition of rules based on source IP and destination IP addresses. These are represented by the network objects and object groups defined earlier.

The proposed rules below was applied on the INSIDE interface

```
!
access-list LAN_ACCESS_INTERNET extended permit tcp object-group LAN_NETWORKS any object-group WEB_ACCESS log


access-list LAN_ACCESS_INTERNET extended permit tcp object-group LAN_NETWORKS any object-group MAIL_ACCESS log


access-list LAN_ACCESS_INTERNET extended permit udp host 10.135.2.241 object-group DNS_SERVERS eq domain


access-list p extended permit udp object-group LAN_NETWORKS any object-group VPN_SERVICES log
```

!

The EATL administrators should build on the proposed rule base after implementation as part of the day to day firewall administration.

Botnet Traffic Filtering

Malware that attempts network activity such as sending private data (passwords, credit card numbers, key strokes, or proprietary data) can be detected by the Botnet Traffic Filter when the malware starts a connection to a known bad IP address. The Botnet Traffic Filter checks incoming and outgoing connections against a dynamic database of known bad domain names and IP addresses (the blacklist), and then logs or blocks any suspicious activity.

The following Botnet configurations was made on the ASA Firewalls:

- **Dynamic Database –** This enables database updates from the Cisco update server, and also enables use of the downloaded dynamic database by the ASA.

```
dynamic-filter updater-client enable
dynamic-filter use-database
```

- **DNS Snooping** – This enables inspection of DNS packets, compares the domain name with those in the dynamic database or the static database (when a DNS server for the ASA is unavailable), and adds the name and IP address to the DNS reverse lookup cache.

```
class-map dynamic-filter_snoop_class
match port udp eq domain
policy-map dynamic-filter_snoop_policy
class dynamic-filter_snoop_class
inspect dns preset_dns_map dynamic-filter-snoop
service-policy dynamic-filter_snoop_policy interface OUTSIDE
```

Enabling traffic classification and actions for the Botnet Traffic Filter – This enables the Botnet Traffic Filter, which compares the source and destination IP address in each initial connection packet to the IP addresses in the dynamic database, static database, DNS reverse lookup cache, and DNS host cache, and sends a syslog message or drops any matching tra ffic.

The following configured commands monitor all traffic on the outside interface and drop all traffic at a threat level of moderate or higher:

```
dynamic-filter enable interface OUTSIDE
```

5.8.3. ASA CX Module Access Policies

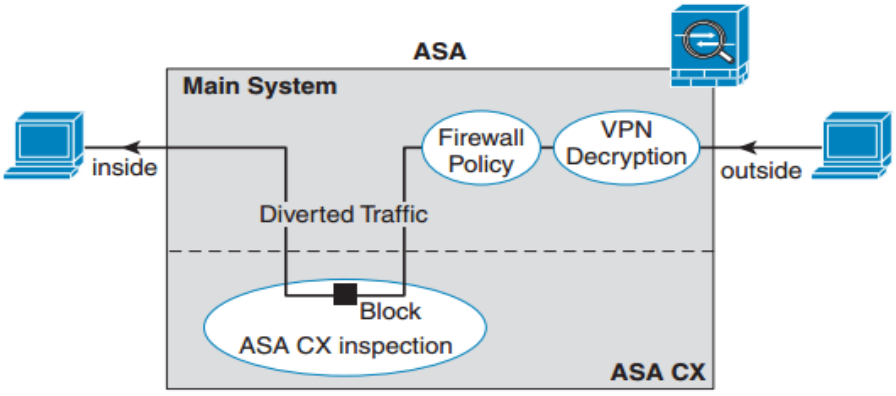

Figure 4 ASA CX Basic Traffic Flow

The following access policies was defined on the CX modules:

Rule 1 (Application Control): This rule denies access to Applications such as Online Games, Facebook Games and Google+ Games.

Rule 2 (Application Control) – This rule explicitly allows access to Microsoft Exchange Mail services, Outlook Web Mail and Skype in the EATL network.

Rule 3 (Application Control): This rule allows access to Applications in the following categories: Media (Streaming Media), Social Networking and Instant Messaging Applications; but limits their bandwidth usage to a maximum 3Mbps out of the total 10Mbps available on the Liquid Telecom link.

Rule 4 (Web Usage Control): This rule denies access to Web Applications in the following categories:

Rule 5 (Application Control): - This rule denies access to a custom group called LIABILITY SITES that consists of the following URL categories: Proxies and File Sharing, with the exception of Storage/Cloud Backup applications such as DropBox and Google Drive.

5.8.4. Network Objects, Access Rules and Route Maps

Object IP	Subnet	Object Name
10.135.2.0	255.255.255.128	DATA_NETWORK
10.135.2.224	255.255.255.224	SERVERS_DMZ_NETWORK
10.135.2.192	255.255.255.224	CCTV_NETWORK

Table 4 Network Objects

Interface	Destination IP	Destination Subnet-mask	Gateway
outside	10.135.x.0	255.255.255.0	10.135.2.146
outside	0.0.0.0	0.0.0.0	10.135.2.146

Table 4 Routes

Source	Destination	Service	Interface	Action
DATA_NETWORK	any	icmp	outside	permit
DATA_NETWORK	any	WebAccess	outside	permit
DATA_NETWORK	any	NSLOOKUP	outside	permit
DATA_NETWORK	SERVERS_DMZ_NETWORK	ip	Inside	Permit
CCTV_NETWORK	SERVERS_DMZ_NETWORK	ip	Inside	Permit
CCTV_NETWORK	SERVERS_DMZ_NETWORK	ip	Dmz	Permit

Table 6 Access Rules

6. DEVICE CONFIGURATIONS

6.1. CISCO 2911 ROUTER: EATL-WAN-Router

```
Current configuration : 2274 bytes
!
! Last configuration change at 05:12:10 UTC Wed Jan 21 2015
! NVRAM config last updated at 05:12:12 UTC Wed Jan 21 2015
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname EATL-WAN-Router
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$9hZZ$35qC3irGkYO2XEzRIWJ95.
enable password cisco
!
no aaa new-model
!
no ipv6 cef
ip source-route
ip cef
!
!
!
!
!
ip domain name eatl.co.ke
ip name-server 41.222.10.26
ip name-server 196.201.225.19
ip name-server 8.8.8.8
```

```
multilink bundle-name authenticated
!
!
!
!
!
crypto pki token default removal timeout 0
!
!
voice-card 0
!
!
!
!
!
!
!
!
license udi pid CISCO2911/K9 sn FCZ183161E4
hw-module pvdm 0/0
!
!
!
username cisco privilege 15 password 0 cisco321
username soc privilege 15 password 0 W!M@x
!
redundancy
!
!
ip ssh version 2
!
!
!
!
interface GigabitEthernet0/0
 ip address 10.135.2.145 255.255.255.248
 ip nat inside
```

```
 ip virtual-reassembly in
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 description jtl-wan
 ip address 197.232.28.30 255.255.255.252
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 description lan
 ip address 10.135.2.2 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 shutdown
 duplex auto
 speed auto
!
ip local pool EAT_POOL_1 10.135.2.190 10.135.2.199
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip nat inside source list 1 interface GigabitEthernet0/1 overload
ip nat inside source static udp 10.135.2.148 500 197.232.28.30 500 extendable
ip nat inside source static tcp 10.135.2.148 4500 197.232.28.30 4500 extendable
ip nat inside source static udp 10.135.2.148 4500 197.232.28.30 4500 extendable
ip route 0.0.0.0 0.0.0.0 197.232.28.29
ip route 10.135.2.0 255.255.255.0 10.135.2.148
!
access-list 1 permit any
access-list 23 permit any
```

```
access-list 100 remark VPN-ACCESS
access-list 100 permit ip any any
!
!
!
control-plane
!
!
!
!
!
!
!
!
gatekeeper
 shutdown
!
!
line con 0
line aux 0
line vty 0 4
 password cisco123
 login
 transport input ssh
 transport output none
line vty 5 15
 password cisco321
 login local
 transport input telnet
!
scheduler allocate 20000 1000
end!
```

6.2. CISCO ASA5515 FIREWALL: EATL-FW-ASA

```
ASA Version 9.1(2)
!
hostname EATL-FW-ASA
domain-name eatl.co.ke
enable password pgVOsZPlgsvFroEa encrypted
names
ip local pool VPNPOOL 192.168.30.1-192.168.30.254 mask 255.255.255.0
!
interface GigabitEthernet0/0
 description == Connection to Internet Router (Cisco 2911) ==
 nameif OUTSIDE
 security-level 0
 ip address 10.135.2.148 255.255.255.248
!
interface GigabitEthernet0/1
 description == Connection to DMZ Server Farm Switch ==
 nameif DMZ
 security-level 50
 ip address 10.135.2.225 255.255.255.224
!
interface GigabitEthernet0/2
 description == Connection to LAN/Inside ==
 nameif INSIDE
 security-level 100
 ip address 10.135.2.153 255.255.255.248
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 shutdown
 no nameif
```

```
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 description == Device Management Interface ==
 management-only
 nameif management
 security-level 100
 ip address 10.135.2.129 255.255.255.240
!
banner login UNAUTHORISED ACCESS TO THIS NETWORK RESOURCE IS STRICTLY PROHIBITED!
boot system disk0:/asa912-smp-k8.bin
ftp mode passive
clock timezone EAT 3
dns domain-lookup OUTSIDE
dns server-group DefaultDNS
 name-server 41.222.10.26
 name-server 8.8.8.8
 name-server 196.201.225.1
 domain-name eatl.co.ke
object network DATA_NETWORK
 subnet 10.135.2.0 255.255.255.128
object network SERVERS_DMZ_NETWORK
 subnet 10.135.2.224 255.255.255.224
object service RDC
 service tcp destination eq 3389
object network NTP_SERVER
 host 41.79.80.34
object network CORE-SW
```

```
 host 10.135.2.1
object network MANAGEMENT_NETWORK
 subnet 10.135.2.128 255.255.255.240
object-group network LAN_NETWORKS
 network-object object DATA_NETWORK
 network-object object MANAGEMENT_NETWORK
object-group service MAIL_ACCESS tcp
 port-object eq imap4
 port-object eq pop3
 port-object eq 465
 port-object eq 587
 port-object eq 993
 port-object eq 995
object-group service VPN_SERVICES udp
 port-object eq 4500
 port-object eq isakmp
object-group network DNS_SERVERS
 network-object host 8.8.8.8
 network-object host 196.201.225.19
 network-object host 41.222.10.26
object-group service WEB_ACCESS tcp
 port-object eq www
 port-object eq https
object-group service DM_INLINE_SERVICE_1
 service-object object RDC
 service-object tcp destination eq ssh
object-group network DM_INLINE_NETWORK_1
 network-object object NTP_SERVER
 network-object object SERVERS_DMZ_NETWORK
object-group service DM_INLINE_SERVICE_2
 service-object tcp destination eq ssh
 service-object udp destination eq ntp
access-list LAN_ACCESS_INTERNET extended permit tcp object-group LAN_NETWORKS
any object-group WEB_ACCESS log
access-list LAN_ACCESS_INTERNET extended permit tcp object-group LAN_NETWORKS
any object-group MAIL_ACCESS log
access-list LAN_ACCESS_INTERNET remark Allow NTP Access
```

```
access-list LAN_ACCESS_INTERNET extended permit udp object CORE-SW object-group DM_INLINE_NETWORK_1 eq ntp
access-list LAN_ACCESS_INTERNET extended permit udp object-group LAN_NETWORKS object-group DNS_SERVERS eq domain
access-list LAN_ACCESS_INTERNET extended permit udp object-group LAN_NETWORKS any object-group VPN_SERVICES log
access-list LAN_ACCESS_INTERNET remark ICMP Allow
access-list LAN_ACCESS_INTERNET extended permit icmp any4 any4 log
access-list LAN_ACCESS_INTERNET remark Remote Desktop, SSH
access-list LAN_ACCESS_INTERNET extended permit object-group DM_INLINE_SERVICE_1 object DATA_NETWORK 10.135.2.224 255.255.255.224
access-list LAN_ACCESS_INTERNET extended permit ip 10.135.2.0 255.255.255.128 host 10.135.2.241
access-list LAN_ACCESS_INTERNET extended permit tcp host 10.135.2.10 host 10.135.2.240
access-list LAN_ACCESS_INTERNET extended permit udp host 10.135.2.10 host 10.135.2.240
access-list DMZ_access_in remark ICMP Allow
access-list DMZ_access_in extended permit icmp any4 any4 log
access-list DMZ_access_in remark PRINTER ACCESS
access-list DMZ_access_in extended permit ip host 10.135.2.240 host 10.135.2.10
access-list DMZ_access_in extended permit ip 10.135.2.224 255.255.255.224 object-group DNS_SERVERS
access-list DMZ_access_in remark NTP,SSH ACCESS
access-list DMZ_access_in extended permit object-group DM_INLINE_SERVICE_2 10.135.2.224 255.255.255.224 object CORE-SW
access-list splitACL standard permit 10.135.2.0 255.255.255.0
access-list OUTSIDE_ACCESS_IN extended permit tcp any interface OUTSIDE eq 4500
access-list OUTSIDE_ACCESS_IN extended permit udp any interface OUTSIDE eq 4500
access-list OUTSIDE_ACCESS_IN extended permit udp any interface OUTSIDE eq isakmp
access-list OUTSIDE_ACCESS_IN extended permit tcp any interface OUTSIDE eq ssh
access-list OUTSIDE_ACCESS_IN extended permit ip object-group LAN_NETWORKS host 10.135.2.241
access-list OUTSIDE_ACCESS_IN extended permit ip 192.168.30.0 255.255.255.0 10.135.2.0 255.255.255.0
pager lines 24
logging enable
logging buffered informational
```

```
logging asdm informational
mtu OUTSIDE 1500
mtu DMZ 1500
mtu INSIDE 1500
mtu management 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
icmp permit any OUTSIDE
icmp permit any DMZ
icmp permit any INSIDE
asdm image disk0:/asdm-713.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group OUTSIDE_ACCESS_IN in interface OUTSIDE
access-group DMZ_access_in in interface DMZ
access-group LAN_ACCESS_INTERNET in interface INSIDE
route OUTSIDE 0.0.0.0 0.0.0.0 10.135.2.145 1
route INSIDE 10.135.2.0 255.255.255.128 10.135.2.156 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
http server enable
http 10.135.2.128 255.255.255.240 management
http 0.0.0.0 0.0.0.0 INSIDE
http 0.0.0.0 0.0.0.0 OUTSIDE
no snmp-server location
no snmp-server contact
```

```
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map EATL_DYN_MAP 65535 set pfs group1
crypto dynamic-map EATL_DYN_MAP 65535 set ikev1 transform-set ESP-AES-128-SHA
ESP-AES-256-SHA
crypto map EATL_MAP 65535 ipsec-isakmp dynamic EATL_DYN_MAP
crypto map EATL_MAP interface OUTSIDE
crypto ca trustpool policy
crypto ikev1 enable OUTSIDE
crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 14400
crypto ikev1 policy 20
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 14400
telnet timeout 5
ssh 0.0.0.0 0.0.0.0 OUTSIDE
ssh 0.0.0.0 0.0.0.0 INSIDE
ssh timeout 5
ssh version 2
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics
threat-detection statistics tcp-intercept rate-interval 30 burst-rate 400 average-rate 200
dynamic-filter updater-client enable
dynamic-filter use-database
dynamic-filter enable
```

```
dynamic-filter drop blacklist
ntp server 10.135.2.1
ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1
group-policy EATL-IPSEC-VPN internal
group-policy EATL-IPSEC-VPN attributes
 dns-server value 196.201.225.19 10.135.2.241
 vpn-tunnel-protocol ikev1
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value splitACL
 default-domain value eatl.co.ke
username eatlremote password 9.OTpQ0M19nEc8Xv encrypted privilege 15
username eatlremote attributes
 service-type remote-access
username admin password 6LKCEw6MG6.GJyTH encrypted
tunnel-group EATL-IPSEC-VPN type remote-access
tunnel-group EATL-IPSEC-VPN general-attributes
 address-pool VPNPOOL
 default-group-policy EATL-IPSEC-VPN
tunnel-group EATL-IPSEC-VPN ipsec-attributes
 ikev1 pre-shared-key *****
!
class-map global-class
 match any
class-map dynamic-filter_snoop_class
 match port udp eq domain
class-map inspection_default
 match default-inspection-traffic
class-map default
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 description ASA CX Module Inspection
```

```
class inspection_default
 inspect dns preset_dns_map
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect rsh
 inspect rtsp
 inspect esmtp
 inspect sqlnet
 inspect skinny
 inspect sunrpc
 inspect xdmcp
 inspect sip
 inspect netbios
 inspect tftp
 inspect ip-options
 inspect icmp
 inspect icmp error
class global-class
 cxsc fail-open
class class-default
 user-statistics accounting
policy-map dynamic-filter_snoop_policy
 class dynamic-filter_snoop_class
  inspect dns preset_dns_map dynamic-filter-snoop
policy-map map
!
service-policy global_policy global
service-policy dynamic-filter_snoop_policy interface OUTSIDE
prompt hostname context
no call-home reporting anonymous
hpm topN enable
Cryptochecksum:c10b61bc81127806da7ba16221c0b522
: end
```

6.3. CISCO 3750 CORE SWITCH: EATL-CORE-SW

```
Current configuration : 7688 bytes
!
! Last configuration change at 15:21:28 EAT Fri Feb 6 2015 by admin
! NVRAM config last updated at 11:05:11 EAT Fri Feb 6 2015 by admin
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec show-timezone
service password-encryption
!
hostname EATL-CORE-SW
!
boot-start-marker
boot-end-marker
!
!
logging buffered informational
no logging console
no logging monitor
enable secret 5 $1$MdLV$ybqfEJ0QARNwLNoWRtk9H0
!
username admin password 7 13003706075F567B
no aaa new-model
clock timezone EAT 3 0
switch 1 provision ws-c3750x-24s
system mtu routing 1500
ip routing
!
ip dhcp excluded-address 10.135.2.1 10.135.2.20
!
ip dhcp pool EATL_DATA_POOL
 network 10.135.2.0 255.255.255.128
 domain-name eatl.co.ke
 dns-server 41.222.10.26 8.8.8.8 196.201.225.19
```

```
 default-router 10.135.2.1
 lease 7
!
!
ip domain-name eatl.co.ke
ip name-server 41.222.10.26
ip name-server 196.201.225.19
ip name-server 8.8.8.8
vtp mode transparent
!
!
crypto pki trustpoint TP-self-signed-3463894016
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3463894016
 revocation-check none
 rsakeypair TP-self-signed-3463894016
!
!
crypto pki certificate chain TP-self-signed-3463894016
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33343633 38393430 3136301E 170D3131 30333330 30313330
  31365A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 34363338
  39343031 3630819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  810090FC ECF4D0AD C05C7713 FD4E4A85 70379494 B53E5851 E3F32C29 AA13321D
  B1B69164 5150CEB6 0A9A8103 CC14CD4B D8A2B052 72E33A68 4C5AC03A 0924501E
  BAE8EC5C 3289F60F D98DD3E6 A3D39A4E 241A0A20 20BEBD1F E67B0252 9C555049
  F44E54E4 FDBA2394 3BFDA0D1 EAE387A4 1E0397E3 E218686B 8279E4E8 7930BEE0
  145F0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
  551D2304 18301680 14BDBC70 BF79DF9D D02116D6 B4EDD994 1F67B659 0B301D06
  03551D0E 04160414 BDBC70BF 79DF9DD0 2116D6B4 EDD9941F 67B6590B 300D0609
  2A864886 F70D0101 05050003 8181002D F250BCAA 445DA211 B11152B4 2A9A4C54
  B7D47D24 2CB90A10 3CF539CF 672EB2C3 01AEA9FA DFD43CDC 856F0FDA A8EF7AF9
  49C1E669 AC547EE8 F8405D9E C13BC6D0 9E3F7907 27BA7F0D 581F187C 3ED12C24
```

```
  326BE462 224ECC34 D92F9B69 FEE0FA8F 042CE511 59E74DCB B6C2D8DE 2BBB693D
  4F832C81 032206F2 91AF6077 184F58
        quit
archive
 log config
  logging enable
  logging size 200
  hidekeys
 path flash:archived.config
!
!
!
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
!
!
!
!
!
!
!
!
vlan internal allocation policy ascending
!
vlan 2,8,10
!
ip ssh time-out 60
ip ssh version 2
!
!
!
!
!
```

```
!
!
!
!
!
!
interface FastEthernet0
 no ip address
 no ip route-cache
!
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/4
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/5
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/6
```

```
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/7
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/8
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/9
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/10
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/11
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/12
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/13
 switchport trunk encapsulation dot1q
```

```
 switchport trunk allowed vlan 2,4,8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/14
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/15
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/16
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/17
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/18
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/19
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/20
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
```

```
 switchport mode trunk
!
interface GigabitEthernet1/0/21
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/22
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/23
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/24
 no switchport
 ip address 10.135.2.156 255.255.255.248
!
interface GigabitEthernet1/1/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode access
!
interface GigabitEthernet1/1/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
!
interface GigabitEthernet1/1/3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode access
!
interface GigabitEthernet1/1/4
```

```
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,4,8,10
 switchport mode access
!
interface TenGigabitEthernet1/1/1
!
interface TenGigabitEthernet1/1/2
!
interface Vlan1
 no ip address
!
interface Vlan4
 no ip address
!
interface Vlan5
 ip address 10.135.2.230 255.255.255.224
!
interface Vlan8
 ip address 10.135.2.131 255.255.255.240
!
interface Vlan10
 description == Data VLAN ==
 ip address 10.135.2.1 255.255.255.128
!
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.135.2.153
ip route 10.135.2.0 255.255.255.128 Vlan10
ip route 10.135.2.144 255.255.255.248 10.135.2.153
ip route 10.135.2.224 255.255.255.224 10.135.2.153
!
!
!
!
```

```
banner motd ^C
==================================================================
UNAUTHORISED ACCESS TO THIS NETWORK RESOURCE IS STRICTLY PROHIBITED!
==================================================================
^C
!
line con 0
 logging synchronous
 login local
line vty 0 4
 logging synchronous
 login local
 transport input ssh
line vty 5 15
 login local
 transport input none
!
ntp server 41.79.80.34 source Vlan10
end
```

6.4. CISCO 3750 SERVER FARM SWITCH: EATL-DMZ-SW

```
Current configuration : 6262 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec show-timezone
service password-encryption
no service dhcp
!
hostname EATL-DMZ-SW
!
boot-start-marker
boot-end-marker
!
!
logging buffered informational
no logging console
no logging monitor
enable secret 5 $1$F6y1$8A5gFvYShbMe2vd6hguWw/
!
username admin password 7 104B290D0944405A
no aaa new-model
clock timezone EAT 3 0
switch 1 provision ws-c3750x-24
system mtu routing 1500
!
!
!
no ip domain-lookup
ip domain-name eatl.co.ke
!
!
crypto pki trustpoint TP-self-signed-2294405120
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2294405120
```

```
 revocation-check none
 rsakeypair TP-self-signed-2294405120
!
!
crypto pki certificate chain TP-self-signed-2294405120
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32323934 34303531 3230301E 170D3131 30333330 30313239
  31355A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 32393434
  30353132 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100AD3E 088CBD28 36044ACC C9D3D6B8 76F075D1 F9524DCD 2997C004 9A15BD22
  B9591264 EC9C9E5F E4A1AF9E 5BE62881 D348F35F 1AABD221 8CB71D7F AC34959B
  247DF874 B7CE854A 45D57C69 3A469102 2D522CC7 D969533E CF347BAD A7810644
  B8953C7E B9D5AB33 A446000D E9311377 0904F149 E06E7BE5 6AF03355 636784A1
  2F7F0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
  551D2304 18301680 1424B847 14E49325 96F63958 B73742B7 8B76CFDB D3301D06
  03551D0E 04160414 24B84714 E4932596 F63958B7 3742B78B 76CFDBD3 300D0609
  2A864886 F70D0101 05050003 81810002 0FF64431 17C1AAB1 A68A7932 0E5B258E
  C8669294 FF7E0E5C 7E1C4FD3 7BCD9A5B CA6BF08B E8CE2917 6B72C95A E51DC85D
  6E321EAC AEA28A09 B540FEB8 4B3B6369 8FF9818E 07C0714B 63E6FE28 130FB937
  B8B8E7FA 3249F062 0FD01968 6D31A0C7 308924C9 45554939 B98A29DC A9054818
  876D54D8 C6C34D43 4AF00D45 B7060D
       quit
archive
 log config
  logging enable
  logging size 200
  hidekeys
 path flash:archived-config
 maximum 14
 write-memory
 time-period 1440
!
!
```

```
!
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
!
!
!
!
!
!
!
!
vlan internal allocation policy ascending
!
ip ssh time-out 60
ip ssh version 2
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0
 no ip address
 no ip route-cache
!
interface GigabitEthernet1/0/1
 switchport access vlan 5
 switchport mode access
```

```
 switchport port-security
!
interface GigabitEthernet1/0/2
 switchport access vlan 5
 switchport mode access
 switchport port-security
!
interface GigabitEthernet1/0/3
 switchport access vlan 5
 switchport mode access
 switchport port-security
!
interface GigabitEthernet1/0/4
 switchport access vlan 5
 switchport mode access
 switchport port-security
!
interface GigabitEthernet1/0/5
 switchport access vlan 5
 switchport mode access
 switchport port-security
!
interface GigabitEthernet1/0/6
 switchport access vlan 5
 switchport mode access
 switchport port-security
!
interface GigabitEthernet1/0/7
 switchport access vlan 5
 switchport mode access
 switchport port-security
!
interface GigabitEthernet1/0/8
 switchport access vlan 5
 switchport mode access
 switchport port-security
```

```
!
interface GigabitEthernet1/0/9
 switchport access vlan 5
 switchport mode access
 switchport port-security
!
interface GigabitEthernet1/0/10
 switchport access vlan 5
 switchport mode access
 switchport port-security
!
interface GigabitEthernet1/0/11
 switchport access vlan 5
 switchport mode access
 switchport port-security
!
interface GigabitEthernet1/0/12
 switchport access vlan 5
 switchport mode access
 switchport port-security
!
interface GigabitEthernet1/0/13
 switchport access vlan 5
 switchport mode access
 switchport port-security
!
interface GigabitEthernet1/0/14
 switchport access vlan 5
 switchport mode access
 switchport port-security
!
interface GigabitEthernet1/0/15
 switchport access vlan 5
 switchport mode access
 switchport port-security
!
```

```
interface GigabitEthernet1/0/16
 switchport access vlan 5
 switchport mode access
 switchport port-security
!
interface GigabitEthernet1/0/17
 switchport access vlan 5
 switchport mode access
 switchport port-security
!
interface GigabitEthernet1/0/18
 switchport access vlan 5
 switchport mode access
 switchport port-security
!
interface GigabitEthernet1/0/19
 switchport access vlan 5
 switchport mode access
 switchport port-security
!
interface GigabitEthernet1/0/20
 switchport access vlan 5
 switchport mode access
 switchport port-security
!
interface GigabitEthernet1/0/21
 switchport access vlan 5
 switchport mode access
 switchport port-security
!
interface GigabitEthernet1/0/22
 switchport access vlan 5
 switchport mode access
 switchport port-security
!
interface GigabitEthernet1/0/23
```

```
 switchport access vlan 5
 switchport mode access
 switchport port-security
!
interface GigabitEthernet1/0/24
 switchport access vlan 5
 switchport mode access
 switchport port-security
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface TenGigabitEthernet1/1/1
!
interface TenGigabitEthernet1/1/2
!
interface Vlan1
 ip address 10.135.2.132 255.255.255.240
 no ip route-cache
 shutdown
!
interface Vlan5
 ip address 10.135.2.254 255.255.255.224
 no ip route-cache
!
interface Vlan8
 ip address 10.135.2.132 255.255.255.240
 no ip route-cache
!
ip default-gateway 10.135.2.225
!
```

```
no ip http server
no ip http secure-server
!
!
!
!
!
banner motd ^C
==========================================================================
UNAUTHORISED ACCESS TO THIS NETWORK RESOURCE IS STRICTLY PROHIBITED!
==========================================================================
^C
!
line con 0
 logging synchronous
 login local
line vty 0 4
 logging synchronous
 login local
 transport input ssh
line vty 5 15
 login local
 transport input none
!
end
```

6.5. CISCO2960 1st FLOOR SWITCH: EATL-1FL-SW

```
Current configuration : 7553 bytes
!
! Last configuration change at 10:38:04 EAT Fri Feb 6 2015 by admin
! NVRAM config last updated at 10:38:08 EAT Fri Feb 6 2015 by admin
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec show-timezone
service password-encryption
no service dhcp
!
hostname EATL-1FL-SW
!
boot-start-marker
boot-end-marker
!
logging buffered informational
no logging console
no logging monitor
enable secret 5 $1$F9Pc$bxzuMIZ4wJbV3mcuik12L.
!
username admin password 7 050E261B2D1F1C58
username administrator privilege 15 password 7 020D015512074C701E1D48
no aaa new-model
clock timezone EAT 3 0
switch 1 provision ws-c2960x-48fps-l
!
!
no ip domain-lookup
ip domain-name eatl.co.ke
!
!
crypto pki trustpoint TP-self-signed-2802730880
 enrollment selfsigned
```

```
 subject-name cn=IOS-Self-Signed-Certificate-2802730880
 revocation-check none
 rsakeypair TP-self-signed-2802730880
!
!
crypto pki certificate chain TP-self-signed-2802730880
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32383032 37333038 3830301E 170D3135 30313235 31313232
  30395A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 38303237
  33303838 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100A159 09A3A71F EE5FE97E F34B1AE8 345C990B A2731C4A F4898EB9 9E07E86F
  9EA98C83 59DE8A52 AF054986 442FBFE4 73F468E8 CCA00799 6B1EA351 9AC2D649
  414AF14C 7A07A2CB 66BC2A3E 377A7B12 93675276 D06AA2F7 F946BD17 8E7FE023
  4F450931 EB3A0AD9 8D2EF0CF 0F6AC040 EBF2EABD 9D037190 5295B7A1 808493E3
  0C850203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
  551D2304 18301680 14844DC1 D22AFD04 88702B87 C7567E7C 97A7D3F7 96301D06
  03551D0E 04160414 844DC1D2 2AFD0488 702B87C7 567E7C97 A7D3F796 300D0609
  2A864886 F70D0101 05050003 81810019 613BF5E1 999953C6 B6AB81AE C816C3E9
  70707A1B D1361AF1 221411E1 F3639B84 55C73EDE F56340C6 1EA03A16 1794F567
  449D68B9 E6937709 E34C9C4E 3BC0A6F4 AF2BE89D 13712F09 BD95BCD6 9C597C2F
  B960F8A5 354A7182 3C01033E 8EBA8C53 48D19FE7 A9E1DFEA 57D66BFF E4B52EA0
  21670E94 5B0CB26B 32637ABD A48564
       quit
archive
 log config
  logging enable
  logging size 200
  hidekeys
 path flash:archived-config
 maximum 14
 write-memory
 time-period 1440
!
```

```
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
!
!
!
!
!
vlan internal allocation policy ascending
!
ip ssh time-out 60
ip ssh version 2
!
!
!
!
!
interface Loopback0
 no ip address
!
interface FastEthernet0
 no ip address
!
interface GigabitEthernet1/0/1
 switchport access vlan 8
 switchport mode access
!
interface GigabitEthernet1/0/2
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/3
 switchport access vlan 10
 switchport mode access
!
```

```
interface GigabitEthernet1/0/4
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/5
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/6
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/7
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/8
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/9
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/10
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/11
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/12
 switchport access vlan 10
 switchport mode access
!
```

```
interface GigabitEthernet1/0/13
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/14
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/15
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/16
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/17
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/18
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/19
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/20
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/21
 switchport access vlan 10
 switchport mode access
!
```

```
interface GigabitEthernet1/0/22
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/23
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/24
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/25
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/26
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/27
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/28
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/29
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/30
 switchport access vlan 10
 switchport mode access
!
```

```
interface GigabitEthernet1/0/31
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/32
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/33
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/34
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/35
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/36
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/37
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/38
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/39
 switchport access vlan 10
 switchport mode access
!
```

```
interface GigabitEthernet1/0/40
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/41
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/42
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/43
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/44
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/45
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/46
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/47
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/48
 switchport trunk allowed vlan 8,10
 switchport mode trunk
!
```

```
interface GigabitEthernet1/0/49
!
interface GigabitEthernet1/0/50
!
interface GigabitEthernet1/0/51
!
interface GigabitEthernet1/0/52
!
interface Vlan1
 ip address 10.135.2.5 255.255.255.0
 shutdown
!
interface Vlan8
 ip address 10.135.2.133 255.255.255.240
!
ip default-gateway 10.135.2.131
no ip http server
no ip http secure-server
!
!
!
banner motd ^C
======================================================================
UNAUTHORISED ACCESS TO THIS NETWORK RESOURCE IS STRICTLY PROHIBITED!
======================================================================
^C
!
line con 0
 logging synchronous
 login local
line vty 0 4
 logging synchronous
 login local
 transport input ssh
line vty 5 15
 login local
```

```
!
ntp server 10.135.2.1
end
```

6.6. CISCO 2960 2nd FLOOR SWITCH: EATL-2FL-SW

```
Current configuration : 5900 bytes
!
! Last configuration change at 10:44:14 EAT Fri Feb 6 2015 by admin
! NVRAM config last updated at 11:04:42 EAT Fri Feb 6 2015 by admin
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec show-timezone
service password-encryption
no service dhcp
!
hostname EATL-2FL-SW
!
boot-start-marker
boot-end-marker
!
logging buffered informational
no logging console
no logging monitor
enable secret 5 $1$F9Pc$bxzuMIZ4wJbV3mcuik12L.
!
username admin password 7 070A0158425A4B54
username administrator privilege 15 password 7 020D015512074C701E1D48
no aaa new-model
clock timezone EAT 3 0
switch 1 provision ws-c2960x-48fps-l
!
!
no ip domain-lookup
ip domain-name eatl.co.ke
!
!
crypto pki trustpoint TP-self-signed-2801802368
 enrollment selfsigned
```

```
 subject-name cn=IOS-Self-Signed-Certificate-2801802368
 revocation-check none
 rsakeypair TP-self-signed-2801802368
!
!
crypto pki certificate chain TP-self-signed-2801802368
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32383031 38303233 3638301E 170D3135 30313235 31313233
  35325A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 38303138
  30323336 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100CC03 112DCD47 B45238E8 5AD4316B 40768CBD 4FA9507D 2FC8ADE2 8B62617B
  076A939B D5450693 EC7C3B61 7117CDDF 53E95AFC B4224704 31DF57E4 E368AA57
  FDDFEBE7 B3442471 D6671038 8B9E79ED 52E2E32C 9B6AF5F0 2AF72694 CD601A7B
  4B0DE123 5C806BB6 D90482F1 8BA7D815 A7C5B19D BC44623E 78DC3B8E 3B9DFCC6
  0E210203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
  551D2304 18301680 14B5E3D7 D15D3D9C 84A49C2B 4819DA78 CF140838 F0301D06
  03551D0E 04160414 B5E3D7D1 5D3D9C84 A49C2B48 19DA78CF 140838F0 300D0609
  2A864886 F70D0101 05050003 818100B2 8DFC2E43 E2BEA9EC 6F87ADE8 E4224C0E
  D768CF5A C36E158B B7A53E25 158BEC2A C1B8FB14 77CAD761 B5E6EE63 7AC7BB63
  9DE3F78F 495A3F0A 59E36ECE 569FF3D1 ED7265A4 0678DFF4 7CEC1708 D1A9F561
  929CC4C6 B2051260 B82EB6BB 0CBC8C6A 1F487B21 E0409A1A 54E99635 559B15CA
  8466F6A6 A9FA98F5 BD342A9A 865506
        quit
archive
 log config
  logging enable
  logging size 200
  hidekeys
 path flash:archived-config
 maximum 14
 write-memory
 time-period 1440
!
```

```
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
!
!
!
!
!
vlan internal allocation policy ascending
!
ip ssh time-out 60
ip ssh version 2
!
!
!
!
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet1/0/1
 switchport access vlan 8
 switchport mode access
!
interface GigabitEthernet1/0/2
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/3
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/4
 switchport access vlan 10
```

```
 switchport mode access
!
interface GigabitEthernet1/0/5
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/6
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/7
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/8
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/9
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/10
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/11
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/12
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/13
 switchport access vlan 10
```

```
 switchport mode access
!
interface GigabitEthernet1/0/14
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/15
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/16
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/17
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/18
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/19
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/20
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/21
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/22
 switchport access vlan 10
```

```
 switchport mode access
!
interface GigabitEthernet1/0/23
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/24
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/25
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/26
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/27
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/28
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/29
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/30
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/31
 switchport access vlan 10
```

```
 switchport mode access
!
interface GigabitEthernet1/0/32
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/33
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/34
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/35
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/36
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/37
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/38
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/39
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/40
 switchport access vlan 10
```

```
 switchport mode access
!
interface GigabitEthernet1/0/41
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/42
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/43
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/44
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/45
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/46
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/47
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/48
 switchport trunk allowed vlan 8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/49
!
```

```
interface GigabitEthernet1/0/50
!
interface GigabitEthernet1/0/51
!
interface GigabitEthernet1/0/52
!
interface Vlan1
 no ip address
!
interface Vlan8
 ip address 10.135.2.134 255.255.255.240
!
ip default-gateway 10.135.2.131
no ip http server
no ip http secure-server
!
!
!
banner motd ^C
======================================================================
UNAUTHORISED ACCESS TO THIS NETWORK RESOURCE IS STRICTLY PROHIBITED!
======================================================================
^C
!
line con 0
 logging synchronous
line vty 0 4
 logging synchronous
 login local
 transport input ssh
line vty 5 15
 login local
!
ntp server 10.135.2.1
end
```

6.7. CISCO 3960 WEIGHBRIDGE SWITCH 1: EATL-WEIGHBRIDGE1-SW

```
Current configuration : 4009 bytes
!
! Last configuration change at 11:06:53 EAT Fri Feb 6 2015 by admin
! NVRAM config last updated at 11:03:28 EAT Fri Feb 6 2015 by admin
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec show-timezone
no service password-encryption
no service dhcp
!
hostname EATL-WEIGHBRIDGE1-SW
!
boot-start-marker
boot-end-marker
!
logging buffered informational
no logging console
no logging monitor
enable secret 5 $1$y7CC$nihEESlDTcDJdhhkxHfFJ0
!
no aaa new-model
clock timezone EAT 3 0
switch 1 provision ws-c2960x-24ps-l
!
!
no ip domain-lookup
ip domain-name eatl.co.ke
!
!
!
archive
 log config
  logging enable
```

```
 logging size 200
 hidekeys
 path flash:archived-config
 maximum 14
 write-memory
 time-period 1440
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
!
!
!
!
!
vlan internal allocation policy ascending
!
ip ssh time-out 60
ip ssh version 2
!
!
!
!
!
interface FastEthernet0
 no ip address
!
interface GigabitEthernet1/0/1
 switchport access vlan 8
 switchport mode access
!
interface GigabitEthernet1/0/2
 switchport access vlan 10
 switchport mode access
!
```

```
interface GigabitEthernet1/0/3
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/4
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/5
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/6
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/7
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/8
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/9
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/10
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/11
 switchport access vlan 10
 switchport mode access
!
```

```
interface GigabitEthernet1/0/12
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/13
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/14
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/15
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/16
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/17
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/18
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/19
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/20
 switchport access vlan 10
 switchport mode access
!
```

```
interface GigabitEthernet1/0/21
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/22
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/23
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/24
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/25
 switchport access vlan 10
 switchport trunk allowed vlan 8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/26
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/27
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/28
 switchport access vlan 10
 switchport mode access
!
interface Vlan1
 no ip address
!
```

```
interface Vlan8
 ip address 10.135.2.135 255.255.255.240
!
ip default-gateway 10.135.2.135
no ip http server
no ip http secure-server
!
!
!
banner motd ^C
==========================================================================
UNAUTHORISED ACCESS TO THIS NETWORK RESOURCE IS STRICTLY PROHIBITED!
==========================================================================
^C
!
line con 0
 logging synchronous
line vty 0 4
 logging synchronous
 login local
 transport input ssh
line vty 5 15
 login
!
ntp server 10.135.2.1
end
```

6.8. CISCO 3960 WEIGHBRIDGE SWITCH 1: EATL-WEIGHBRIDGE2-SW

```
Current configuration : 4026 bytes
!
! Last configuration change at 13:25:30 EAT Wed Feb 11 2015 by admin
! NVRAM config last updated at 13:25:27 EAT Wed Feb 11 2015 by admin
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec show-timezone
service password-encryption
no service dhcp
!
hostname EATL-WIGHBRIDGE2-SW
!
boot-start-marker
boot-end-marker
!
logging buffered informational
no logging console
no logging monitor
enable secret 5 $1$y7CC$nihEESlDTcDJdhhkxHfFJ0
!
username admin privilege 15 password 7 09496E1D15564543
no aaa new-model
clock timezone EAT 3 0
switch 1 provision ws-c2960x-24ps-l
!
!
no ip domain-lookup
ip domain-name eatl.co.ke
!
!
!
archive
 log config
```

```
 logging enable
 logging size 200
 hidekeys
 path flash:archived-config
 maximum 14
 write-memory
 time-period 1440
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
!
!
!
!
!
vlan internal allocation policy ascending
!
ip ssh time-out 60
ip ssh version 2
!
!
!
!
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet1/0/1
 switchport access vlan 8
 switchport mode access
!
interface GigabitEthernet1/0/2
 switchport access vlan 10
```

```
 switchport mode access
!
interface GigabitEthernet1/0/3
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/4
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/5
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/6
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/7
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/8
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/9
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/10
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/11
 switchport access vlan 10
```

```
 switchport mode access
!
interface GigabitEthernet1/0/12
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/13
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/14
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/15
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/16
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/17
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/18
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/19
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/20
 switchport access vlan 10
```

```
 switchport mode access
!
interface GigabitEthernet1/0/21
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/22
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/23
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/24
 switchport trunk allowed vlan 2,8
 switchport mode trunk
!
interface GigabitEthernet1/0/25
 switchport trunk allowed vlan 2,8,10
 switchport mode trunk
!
interface GigabitEthernet1/0/26
 switchport trunk allowed vlan 2,8
 switchport mode trunk
!
interface GigabitEthernet1/0/27
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/28
 switchport access vlan 10
 switchport mode access
!
interface Vlan1
 no ip address
```

```
 shutdown
!
interface Vlan8
 ip address 10.135.2.136 255.255.255.240
!
ip default-gateway 10.135.2.131
no ip http server
no ip http secure-server
!
!
!
banner motd ^CC
========================================================================
UNAUTHORISED ACCESS TO THIS NETWORK RESOURCE IS STRICTLY PROHIBITED!
========================================================================
^C
!
line con 0
 logging synchronous
line vty 0 4
 logging synchronous
 login local
 transport input ssh
line vty 5 15
 login
!
ntp server 10.135.2.1
end
```

6.9. CISCO 2960 CCTV SWITCH 1: EATL-CCTV-SW1

```
Current configuration : 3981 bytes
!
! Last configuration change at 13:28:02 EAT Wed Feb 11 2015 by admin
! NVRAM config last updated at 13:28:00 EAT Wed Feb 11 2015 by admin
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec show-timezone
service password-encryption
no service dhcp
!
hostname EATL-CCTV-SW1
!
boot-start-marker
boot-end-marker
!
logging buffered informational
no logging console
no logging monitor
enable secret 5 $1$y7CC$nihEESlDTcDJdhhkxHfFJ0
!
username admin privilege 15 password 7 050E261B2D1F1C58
no aaa new-model
clock timezone EAT 3 0
switch 1 provision ws-c2960x-24ps-l
!
!
no ip domain-lookup
ip domain-name eatl.co.ke
!
!
!
archive
 log config
```

```
 logging enable
 logging size 200
 hidekeys
path flash:archived-config
 maximum 14
 write-memory
 time-period 1440
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
!
!
!
!
!
vlan internal allocation policy ascending
!
ip ssh time-out 60
ip ssh version 2
!
!
!
!
!
interface FastEthernet0
 no ip address
!
interface GigabitEthernet1/0/1
 switchport access vlan 8
 switchport mode access
!
interface GigabitEthernet1/0/2
 switchport access vlan 2
 switchport mode access
```

```
!
interface GigabitEthernet1/0/3
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/4
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/5
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/6
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/7
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/8
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/9
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/10
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/11
 switchport access vlan 2
 switchport mode access
```

```
!
interface GigabitEthernet1/0/12
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/13
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/14
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/15
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/16
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/17
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/18
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/19
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/20
 switchport access vlan 2
 switchport mode access
```

```
!
interface GigabitEthernet1/0/21
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/22
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/23
 switchport trunk allowed vlan 2,8
 switchport mode trunk
!
interface GigabitEthernet1/0/24
 switchport trunk allowed vlan 2,8
 switchport mode trunk
!
interface GigabitEthernet1/0/25
 switchport trunk allowed vlan 2,8
 switchport mode trunk
!
interface GigabitEthernet1/0/26
 switchport trunk allowed vlan 2,8
 switchport mode trunk
!
interface GigabitEthernet1/0/27
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/28
 switchport access vlan 2
 switchport mode access
!
interface Vlan1
 no ip address
!
```

```
interface Vlan8
 ip address 10.135.2.137 255.255.255.240
!
ip default-gateway 10.135.2.131
no ip http server
no ip http secure-server
!
!
!
banner motd ^CC
========================================================================
UNAUTHORISED ACCESS TO THIS NETWORK RESOURCE IS STRICTLY PROHIBITED!
========================================================================
^C
!
line con 0
 logging synchronous
line vty 0 4
 logging synchronous
 login local
 transport input ssh
line vty 5 15
 login
!
ntp server 10.135.2.1
end
```

6.10. CISCO 2960 CCTV SWITCH 2: EATL-CCTV-SW2

```
Current configuration: 3802 bytes
!
! Last configuration change at 13:36:11 EAT Wed Feb 11 2015 by admin
! NVRAM config last updated at 13:35:36 EAT Wed Feb 11 2015
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec show-timezone
no service password-encryption
no service dhcp
!
hostname EATL-CCTV-SW2
!
boot-start-marker
boot-end-marker
!
logging buffered informational
no logging console
no logging monitor
enable secret 5 $1$y7CC$nihEESlDTcDJdhhkxHfFJ0
!
no aaa new-model
clock timezone EAT 3 0
switch 1 provision ws-c2960x-24ps-l
!
!
no ip domain-lookup
ip domain-name eatl.co.ke
!
!
!
archive
 log config
  logging enable
```

```
 logging size 200
 hidekeys
 path flash:archived-config
 maximum 14
 write-memory
 time-period 1440
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
!
!
!
!
!
vlan internal allocation policy ascending
!
ip ssh time-out 60
ip ssh version 2
!
!
!
!
!
interface FastEthernet0
 no ip address
!
interface GigabitEthernet1/0/1
 switchport access vlan 8
 switchport mode access
!
interface GigabitEthernet1/0/2
 switchport access vlan 2
 switchport mode access
!
```

```
interface GigabitEthernet1/0/3
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/4
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/5
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/6
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/7
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/8
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/9
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/10
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/11
 switchport access vlan 2
 switchport mode access
!
```

```
interface GigabitEthernet1/0/12
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/13
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/14
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/15
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/16
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/17
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/18
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet1/0/19
 switchport mode access
!
interface GigabitEthernet1/0/20
 switchport mode access
!
interface GigabitEthernet1/0/21
 switchport mode access
```

```
!
interface GigabitEthernet1/0/22
 switchport mode access
!
interface GigabitEthernet1/0/23
 switchport mode access
!
interface GigabitEthernet1/0/24
 switchport trunk allowed vlan 2,8
 switchport mode trunk
!
interface GigabitEthernet1/0/25
 switchport trunk allowed vlan 2,8
 switchport mode trunk
!
interface GigabitEthernet1/0/26
 switchport trunk allowed vlan 2,8
 switchport mode trunk
!
interface GigabitEthernet1/0/27
 switchport mode access
!
interface GigabitEthernet1/0/28
 switchport access vlan 2
 switchport mode access
!
interface Vlan1
 no ip address
!
interface Vlan8
 ip address 10.135.2.138 255.255.255.240
!
ip default-gateway 10.135.2.131
no ip http server
no ip http secure-server
!
```

```
!
!
banner motd ^CC
==========================================================================
UNAUTHORISED ACCESS TO THIS NETWORK RESOURCE IS STRICTLY PROHIBITED!
==========================================================================
^C
!
line con 0
 logging synchronous
line vty 0 4
 logging synchronous
 login local
 transport input ssh
line vty 5 15
 login
!
ntp server 10.135.2.1
end
```

Sign-off Certificate

Acceptance

The following signatories agree that the above mentioned project has been delivered by Dimension Data in full and that all outstanding payments may be invoiced by Dimension Data.

Client's Signature	Dimension Data PM's Signature
Print Name and Title	Print Name and Title
Date	Date