



Cisco Collaborative Customer Experience—Digital Image Management

Cisco Validated Design

Version 1.1, September 3, 2008

Solution Overview

Executive Summary

Cisco Collaborative Customer Experience—Digital Image Management (Cisco CCE—Digital Image Management) optimizes the institution's current WAN connection so as to avoid a network upgrade after deploying Check 21 functionality. By adding Unified Communications, security, a redundant network connection and Wide Area Application Services, the institution will be able to increase service offerings, increase the amount of application traffic, provide high availability for the network at a lower cost, and obtain more throughput across the network without upgrading the existing connection.

Challenges Experienced in Branch Retail Banks

In today's competitive marketplace, one of the main business drivers in bank operating plans is cost reduction. However financial institutions no longer assess IT investments simply in terms of cost. Instead, there is a shift towards achieving better alignment between the key business goals and the capabilities of the underpinning IT to enable future agility. While lean/thin client computing can be demonstrably justified by return on investment and total cost of ownership analysis alone, the case for deployment becomes even more compelling when its contribution to the primary business drivers is measured by:

- Customer retention—Competition has led to the introduction of many new financial providers offering a wide range of products and services. Loyalty to traditional providers is declining, making customer retention a highly-valued strategy. The point at which customer and supplier meet, and therefore a major source of competitive differentiation, is the delivery of the core customer applications that set the scene for the relationship. Innovative, rapid, and consistent customer



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

experience has been identified as key to improving retention levels. Older network infrastructures, with their limited bandwidth, do not allow banks to implement the more advanced teller and platform functionality that they are seeking to enable more effective servicing and selling to customers.

- **Operational excellence**—This is not measured by cost alone. Institutions also have to balance their need for future agility, ensuring they are positioned to take rapid and effective steps to grow revenue, launch new products and services, and introduce new processes, either proactively or in response to trends and competition. With many institutions having large distributive branch networks, optimizing the way in which highly available core services are delivered, configured, and managed, plays a big part in meeting this challenge. Traditional client/server architectures are both costly and highly inefficient, requiring not just new applications to be rolled out manually in each additional branch, but also on-site maintenance and support.
- **Productivity**—Working practices in financial services are changing to reflect staff levels, the need for tasking flexibility, outsourcing, and the drive for better utilization of people and space. To some extent, institutions have been limited in their ability to address this issue by the lack of agility in their traditional IT environment and architecture. Flexibility in the delivery of applications is essential to take advantage of the changes that, when properly addressed, yield significant benefits in productivity and utilization.
- **Compliance and security**—Intense scrutiny of governance from national and international regulators requires process compliance along with traceable and retrievable audit trails. Expansion into new geographic markets and cross-selling of services highlights the need for rapid rollout of consistent, high-quality applications to branches that can reflect local conditions.

Solution Description

Cisco CCE—Digital Image Management is based upon Cisco and partner technologies to provide an enhanced solution for retail bank branches. The addition of check image capture to the existing Argo Platform Branch application is more bandwidth intensive than originally anticipated. Cisco CCE—Digital Image Management is being developed to accelerate the existing WAN so that it can accommodate the additional bandwidth requirements of check image capture as well as additional features/functions/services without a network upgrade. Additionally, Cisco CCE—Digital Image Management provides the base architecture for enhanced functionality and services in future releases.

Cisco CCE—Digital Image Management includes data center, MAN/WAN, and branch technologies and network connectivity is enhanced to provide an always-on connection, increasing reliability and reducing costs over existing technologies currently deployed.

Solution Benefits

Retail banking branch optimization has two main drivers:

- The need to streamline internal processes for cost efficiency.
- The mandate to differentiate customer-facing processes to achieve the highest quality of customer service and interaction.

Cisco CCE—Digital Image Management is purpose-built to specifically resolve these needs.

Cisco's core message to the financial services marketplace is that the Cisco CCE—Digital Image Management solution, which is part of its Customer Collaborative Experience initiative, supports the key elements of efficiency and customer satisfaction that are so crucial to continued organic growth and profitability.

The Cisco CCE—Digital Image Management solution offers a compelling opportunity to reduce the total cost of ownership of branch networks. Significant savings are made possible via reduction in costs associated with hardware acquisition, software, and ongoing support and maintenance. Taking guidance from industry studies conducted by Gartner (2004) and IDC (2005), TCO reductions in excess of 40% can be expected.

Cisco CCE—Digital Image Management increases network manageability, security, administrative control, and system uptime while significantly reducing branch capital and operational expenditures. Cisco CCE—Digital Image Management also facilitates ease of application upgrades. Finally, Cisco CCE—Digital Image Management is part of an institution's "green initiative," reducing the branch carbon footprint by reducing energy consumption.

Cisco CCE—Digital Image Management offers a broad range of values to our target market. Retail banks must grow, must respond to competition, and must satisfy customers who have become accustomed to a very high standard of service and consideration. In pursuit of these objectives, banks will find that Cisco CCE—Digital Image Management:

- Offers secure connectivity that provides secure transfer of sensitive information across open networks.
- Implements threat defense that provides dedicated security to networking devices and appliances, proactively defending the Institutions against known and emerging threats.
- Increases an institution's operational efficiency and reduces expenses.
- Increases effectiveness of existing employees.
- Decreases operational costs by building a common platform to launch current and future services.
- Enables trust and identity management by providing best-in-class capabilities to enforce Institution-wide security policies.

Solution Scope

The overall scope of the Collaborative Customer Experience Architecture is to provide a reference architecture that supports the aggregation of voice, video, and data across the Wide Area Network for retail branch banks.

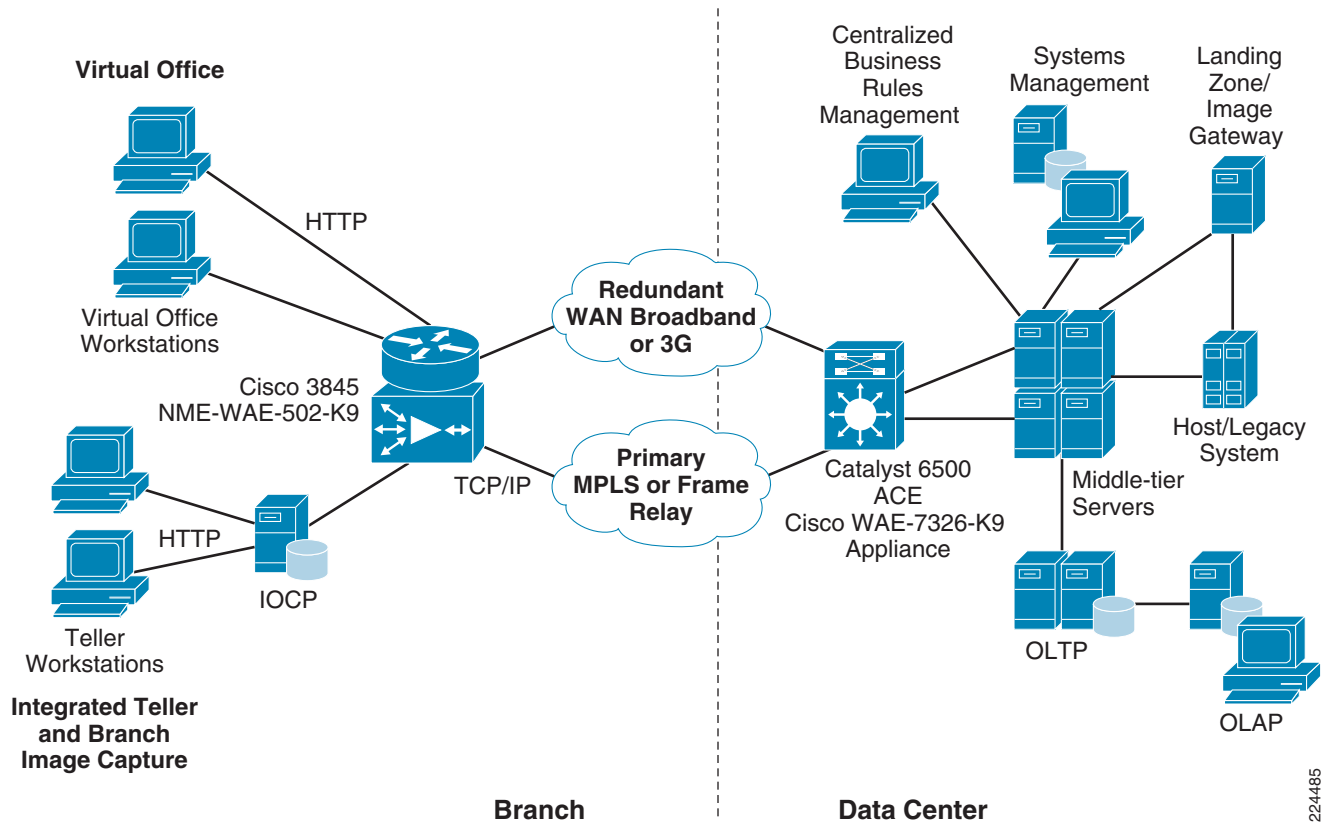
The scope of the Cisco CCE—Digital Image Management solution is limited to:

- WAN optimization
- Quality of Service (QoS)
- Redundant connectivity
- Security best practices

The devices used in this solution represent what was required to perform only functional testing. Any implementation of this solution would require proper sizing of the various devices based on the individual needs of the customer.

High Level Architecture

Figure 1 Cisco CCE—Digital Image Management High Level Architecture



224485

Solution Services

Cisco CCE—Digital Image Management Services

WAN Optimization

The Cisco Wide Area Application Services (WAAS) system consists of a set of devices called wide area application engines (WAE) that work together to optimize TCP traffic over the WAN. The WAEs examine the traffic and use built-in application policies to determine whether to optimize the traffic or allow it to pass through the WAN un-optimized. WAAS not only reduces latency, but also reduces the amount of traffic carried over the WAN links. Cisco WAAS deployments are transparent to the network and the applications running on them. The applications do not need to be aware of the added functionalities and continue to work as-is. In addition, common TCP ports are already configured in the built-in application policies; no further configuration in the Cisco WAE is necessary unless the application requires ports that are not part of the default application profile.

With the recommended design of Cisco WAAS at the WAN edge, client data only traverses the Cisco WAEs once, at the ingress and egress of the data center. Further application communication between the Web servers, application servers, and database servers are within the data center and are not affected by Cisco WAAS.

Transport Flow Optimization (TFO), Data Redundancy Elimination (DRE), and Lempel-Ziv (LZ)-compression, the three key technologies of Cisco WAAS, are enabled by default. You can enable them one by one to see which technology plays a significant role in optimizing a particular application.

Cisco uses disk encryption to ensure that data at rest stored on the WAE is secure. Encryption of all optimized data on the remote Cisco Wide Area Application Engine (WAE) Appliance or network module prevents unauthorized data access or theft. Federal Information Processing Standard (FIPS) 197 approved technologies and Advanced Encryption Standard (AES) 256-bit encryption are used to encrypt data on the Cisco WAE disk drives. The automated centralized key management service, integrated within the Cisco WAAS Central Manager, simplifies management of encryption keys, provides centralized failover capability for high availability, and supports backup and restoration of keys to offline vaults for disaster recovery purposes.

VPN

Assuming a frame relay WAN is used, each bank branch must have secure connectivity to the data center over the Internet Redundant connection. For this purpose, each branch is deployed with a VPN tunnel that terminates at the edge router at the branch as well as at the WAN aggregation mid-range router at the data center. The choice of a VPN protocol (direct IPSec, IPSec-Protected GRE, Point-to-Point GRE, DMVPN, WebVPN, etc.) should be made during the design and deployment phase of any implementation. The following branch reference design guides may be used to make that determination:

- [Enterprise Branch Security Design Guide](#)
- [Business Ready Branch Solutions for Enterprise and Small Offices—Reference Design Guide](#)

When choosing the tunneling protocol, some of the questions you should consider include:

- Whether IP multicast needs to be supported
- Whether the branch office must support more than a few subnets
- Whether non-IP protocol traffic is carried across the WAN
- Whether there are future requirements for spoke-to-spoke dynamic VPN tunnels

DMVPN was chosen for this solution for its support of hub-and-spoke deployments as well as for its ease of configuration. Depending on the deployment, multipoint or point-to-point GRE tunneling can be used. For further information on the DMVPN deployment options best for a specific environment, consult the “[Dynamic Multipoint VPN \(DMVPN\) Design Guide](#).”

Redundant Network Connectivity

Each bank branch has a redundant network connection over a simulated Internet to the data center. The WAN edge router is configured with two links, frame relay over the enterprise WAN and representative DSL over the simulated Internet, which consists of a single router. The solution may require that an MPLS WAN be included. Dynamic routing is configured to have weighted routes for the primary and backup links to force redirection of traffic to the backup when the primary is unavailable.

Baseline setting and performance testing of a single branch across its primary WAN link to the datacenter uses the Application Network Services (ANSWER) setup, which makes use of the Pageant WAN simulator to introduce the appropriate latency and packet loss.

Validation of the redundant network connectivity to prove that stateful failover is supported also includes the ANSwer setup with the Pageant WAN simulator used to enforce the appropriate delays on both links.

Voice Services

Branch office locations support integrated voice functions. With Cisco Unified Communication Manager and IP phones, employees at a branch can make calls over the WAN and hence save cost.

The branch router uses an IOS image that contains communication manager express (CME). If the headquarters has CUCM, but the WAN link between the headquarter and the branch is down, IP phones can fall back to the branch router to obtain basic telephony services, such as off-net calls to 911, calls within a branch office, or calls between branch offices through the public switched telephone network (PSTN). This feature is called Cisco Unified Survivable Remote Site Telephony (SRST). A branch can choose either Cisco Unified SRST or Cisco Unified CME in SRST fallback mode to provide survivability when the WAN link fails.

With a foreign exchange station (FXS) voice interface card, or a T1 card, a branch can use existing PBX as backup or load sharing. These interface cards enable employees at the branch to call local customers who use regular phones.

A retail bank branch typically has ten employees and about half of them are tellers. A 2-port or 4-port FXS card can be used. For a branch with large number of employees, a T1 card can be used. A T1 card can support 24 calls at the same time.

While FXS or T1 is used to connect IP phone to private branch exchange (PBX), a foreign exchange office (FXO) voice interface card is used to connect analog telephone handsets, fax machines, and (analog) modems.

Load Balancing

There are two types of load balancing being performed:

- Cisco Application Control Engine (ACE)—ACE is used for the connection requests and performs the primary load balancing. It decides which Request Manager gets the connection request from a client (branch). As a request comes in, the ACE engine determines the least used Request Manager and directs the connection request to that server.
- ARGO Request Manager —Request Manager handles the load balancing between the Request Manager and Application Servers. It decides which application server services the application request. The Request Manager uses a proprietary algorithm to balance the load to the application servers. It takes a connection request, queues it, and then distributes to the application server that is available to handle the request. The Request Manager uses a round robin scheme based on how servers are configured. It monitors the number of active threads and available processes on the application servers to determine which server gets the application request.

Quality of Service

Quality of Service (QoS) classifies network traffic into different classes and then gives them different treatment. Different types of traffic have different levels of importance. Routing protocols and Layer 2 control packets are critical for a router to perform well. For example, if a router does not respond to a Layer 2 keepalive message, its peer may think that it has gone down. In contrast, if a router drops traffic generated during teller training when the network is congested, the teller training can be done at a later time when network is not busy.

To use QoS, we first identify different types of traffic and then decide how to treat them in the QoS hierarchy. In a typical branch store, you would see the following types of traffic:

- Routing protocol and Layer 2 control packets
- Voice and video
- Production System interactive traffic
- Check image traffic
- Test System interactive traffic
- Additional application platform traffic

The network must ensure that the video and data transmission reach their destinations in a timely manner, with minimal loss and delay. The network engineer can instruct the network to treat voice and video with priority, i.e., transport voice and video traffic as soon as they arrive.

If the network is congested, we should guarantee the transport of transaction data by allocating a fixed percentage of bandwidth to it. For traffic generated during teller training, we do not allocate a fixed bandwidth to it and transport only when the network does not have more important traffic to transport.

The following policy map shows how this could be done:

```
Policy-map p0
  Class-map voice
    Priority 10 percent
  Class-map video
    Priority 20 percent
  Class-map control_traffic
    Bandwidth 2 percent
  Class-map transaction_data
    Bandwidth 20 percent
  Class-map check_images
    Bandwidth 10 percent
  Class-map teller_training
    Shape average 10 percent
```

With the above policy, if the network is busy, teller_training traffic is not transported. Of course, if the network is not busy, teller_training traffic is transported. If customers want, they can specify teller training traffic not to exceed 10 percent of the WAN link even if the network is not busy.

Security Services

Several security features are configured on the branch router to ensure that the Redundant Internet link is protected against untrusted access. Access control lists are configured on the router to allow only traffic between the branch and data center and explicitly deny traffic from any other source than the data center. The IOS Firewall on the branch router is configured to inspect standard application protocol traffic to ensure no malicious traffic gets through. Cisco IOS Firewall Application Inspection and Control minimizes threats on desirable network services, such as Web traffic and mail protocols, by enforcing protocol conformance and blocking unwanted application activity. Network bandwidth and employee time waste is limited by the Cisco IOS Firewall blocking unwanted applications, such as instant messaging traffic, peer-to-peer file-sharing traffic, and http-tunneling applications. In addition, as time permits, other security features like IOS Intrusion Protection Services and IOS Network Address Translation may be implemented to enhance perimeter security around the backup Internet connection.

In addition to protecting the perimeter, the edge router is configured with security measures to protect the device itself, according to the security best practices as described in the Enterprise Branch Security Design Guide and the reference guides referred to within that document. Such security measures include use of non-default login parameters, disabling unnecessary services, and ensuring that all management traffic to the device is over a secure protocol (e.g., SSH instead of Telnet).

Management Services

In a real-world deployment, hundreds to thousands of branches may need to be configured with the same type of policies for security, QoS, and application acceleration, to name a few.

For this solution, Cisco Security Manager can be used to manage security on the branch and data center infrastructure devices. While there is only one branch and one data center in this solution, the implementation and design guidance developed in this solution is applicable to larger-scale networks.

Cisco Security Manager is suitable for efficiently managing networks that range from a few devices to thousands of devices. Scalability is achieved through powerful policy-based management techniques, which allow settings to be defined once and then optionally assigning the settings to individual devices, groups of devices, or across the enterprise. When a setting is changed, Cisco Security Manager automatically applies the change to all affected network devices. The firewall or VPN policies are platform-neutral, and can be applied across different device platforms such as Cisco routers, security appliances, or services modules. Cisco Security Manager also provides flexible device-level overrides; this allows policy re-use and sharing while retaining the ability to customize device-specific settings as necessary.

While the deployment of Cisco Security Manager was outside the scope of solution validation, the following link provides more information on how to deploy the Cisco Security Manager for your network:

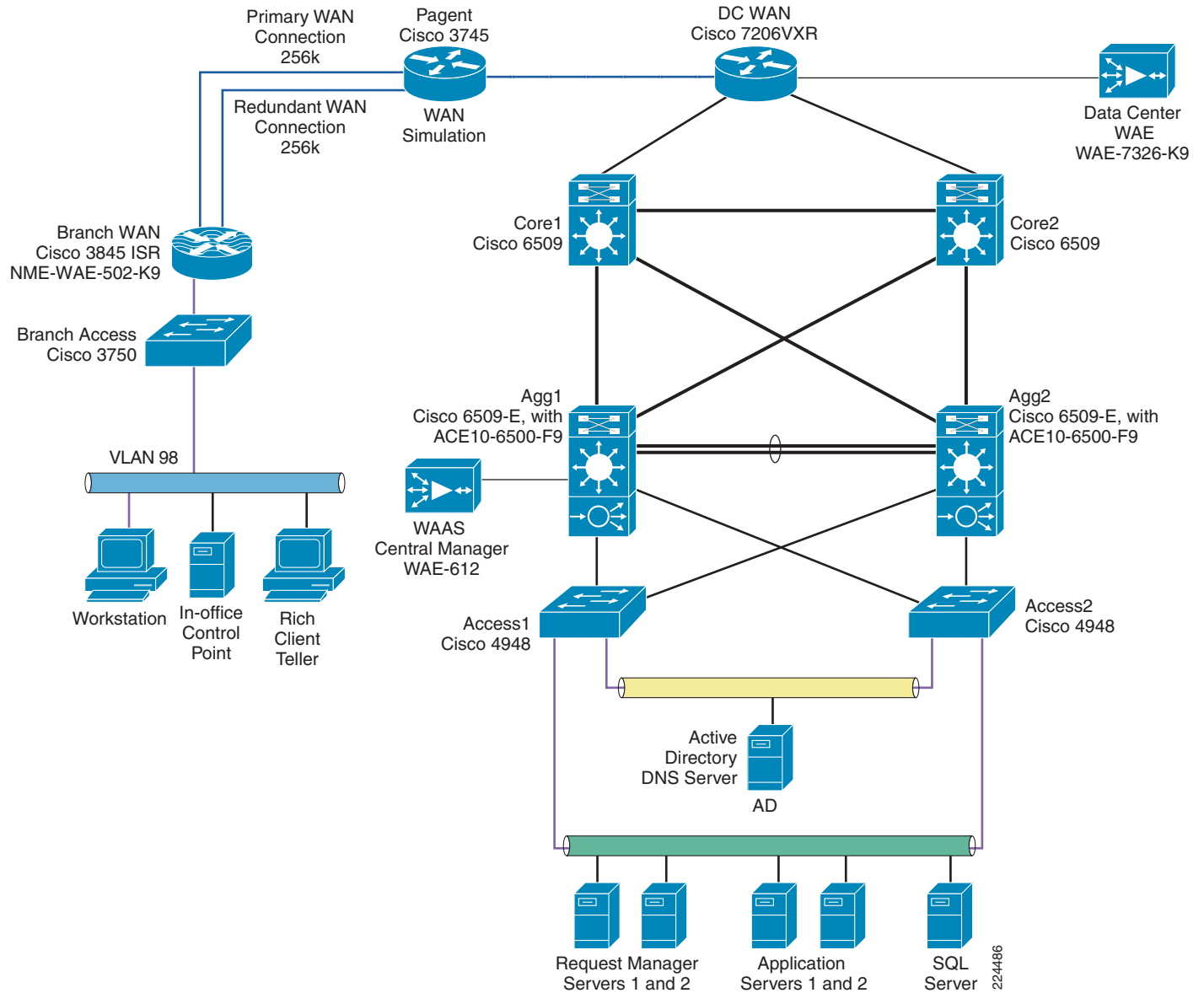
http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.1/user/guide/ug31.html

Solution Architecture

Cisco CCE—Digital Image Management Architecture

Figure 2 provides a high level overview of the network used to validate this design architecture.

Figure 2 Cisco CCE—Digital Image Management Architecture



ARGO Data Application Scope

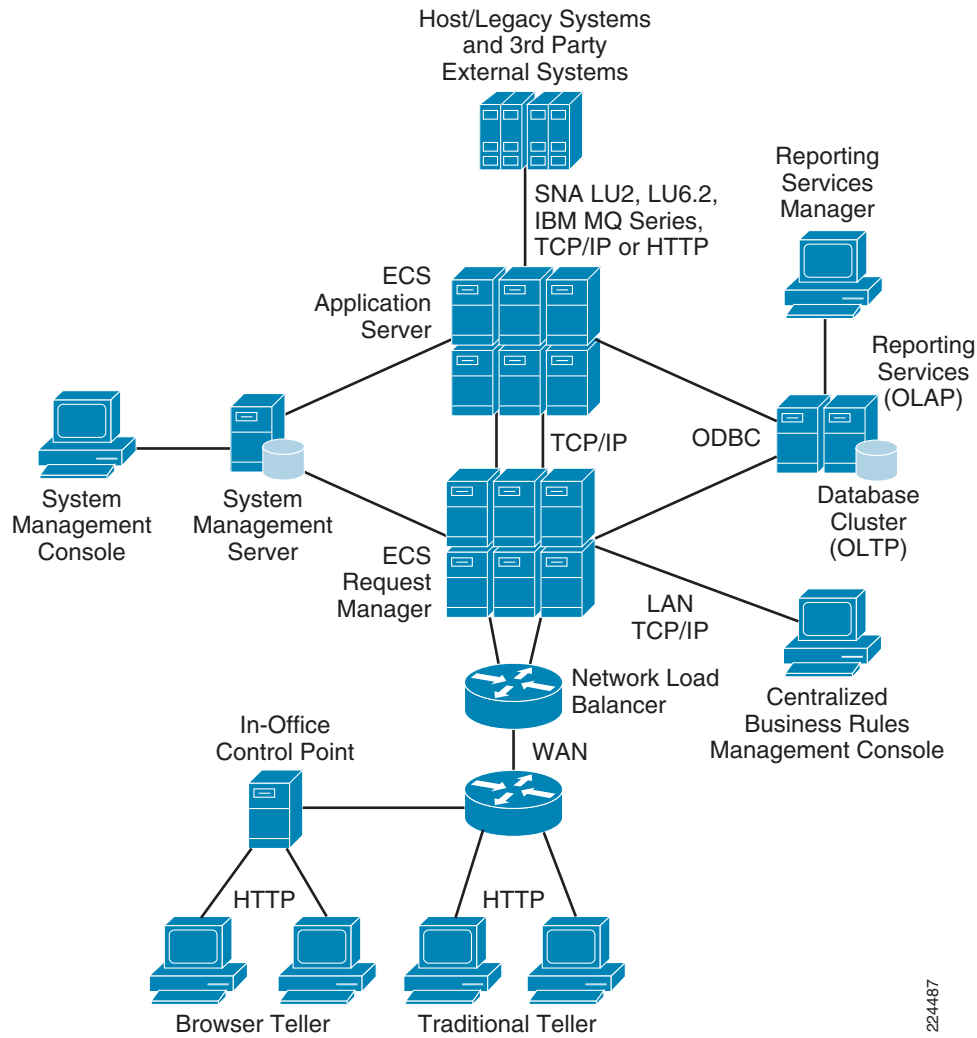
In April 2008, Argo Data acquired Gilson Information Systems to replace the existing check image capture software. As a result, BANKPRO Teller has been completely re-engineered and includes end-to-end payments processing. Teller transactions are streamlined and faster with the enhanced Branch Payments capability. Fewer keystrokes and reduced errors translates into improved customer service. Teller Payments is a complete teller and payments processing solution that completely replaces legacy payment processing systems and allows for straight through processing in seconds from presentment to posting.

This phase of the solution was tested using the new BANKPRO Teller with check image capture.

The scope of the Argo system deployed in this solution consists of the minimal installation of the thin-client, middle-tier servers, back-end servers, and database required to generate enough standard teller transactions and check-imaging traffic to simulate the traffic types and amount of load expected from a typical branch with 3-5 tellers. While the thick client is installed on the teller client, whether it is tested depends on available time, as the highest priority is testing the thin-client with IOCP.

Application Architecture

Figure 3 ARGO Data Application Architecture



224487

Banking System Components

This section describes the Argo products that make up the retail banking system included in this solution and explains the functionality of each. The following client and servers compose the Argo banking system in this solution.

Teller Client

The teller client can be either thick or thin-client. The thin-client uses Internet Explorer as the user interface. Teller transactions as well as check image transfers are sent from the teller client across the WAN to the data center.

In-Office Control Point

The In-Office Control Point (IOCP) allows operations at the branch office to continue in spite of a WAN outage. Teller transactions as well as check image transfers are handled by the IOCP in this case. Under normal operation when the WAN is available, the IOCP processes the teller transaction and queues up those transactions to be transferred over the WAN to the data center. The check images, however, bypass the IOCP and are sent directly to the branch edge router for forwarding across the WAN.

Request Manager

Request Manager Servers are used to control and process in-coming requests and subsequent responses from and to the IOCP/Teller Clients. Business function requests are sent to the ECS Request Manager from the branch and back office workstations. There are a minimum of two request managers in the data center for redundancy and load-balancing.

The functions provided by the Request Manager Servers include:

- Request distribution—Request Managers automatically distribute messages to Application Servers based on the type of function requested. Business components are hosted by Application Servers, while also providing core services like host communication, security, office administration, electronic journal, and store and forward processing. Multiple Application Server processes are configured across multiple physical clustered servers to avoid any single point of failure.
- Load balancing—When multiple Application Server processes are available to service a request, the Request Managers distribute requests across the multiple process instances. The number of requests distributed to an instance is based on its inherent processing capability. All applications take advantage of SMP (Symmetric Multi-Processing) hardware configurations, which also has a direct impact on improving processing capability.
- Failover processing—When a request manager cannot communicate to an Application Server application instance, it automatically distributes requests to remaining instances. Request manager periodically polls the application instance for availability and as soon as it is available, starts distributing requests to that process.
- Tiered network—All clients communicate to Application Servers through request managers. This considerably reduces the number of network connections, increases system availability, and reduces complexity through consolidation of network traffic. Application requests have redundant paths to request managers, thus providing reliable, fault-tolerant communications.
- Context management—ECS Application Servers do not maintain request states. Session states are maintained in context records by the Request Managers. The type of client determines session duration. For example, for customer requests through a browser, the session duration is from customer logon to customer logoff. Keeping session state external of the application server process allows request managers to provide load balancing and fail-over processing.

Application Server

The Application Servers provide business logic processing for transaction requests received from the workstations via the ECS Request Managers. In addition, the application servers provide the integration point for third-party systems such as mainframe data, check order vendors, and valuation sources. Requests to the Application Server are load-balanced by the Request Manager. There is a single persistent TCP session between each Request Manager and each Application Server and the Application Server makes ODBC connections to the SQL database. There are a minimum of two application servers in the datacenter for redundancy and load-balancing.

Services provided by the application servers include:

- **Office control**—Office Control provides the office administration information necessary to operate the office. Office Control interfaces with the client workstations as well as with the security, totals, and electronic journal server functions. Office Control is also used to define an office. This information contains the office address and processing time. In addition to the office information, the office holidays (non-processing days), terminals, and operators are defined. The complete office information defines the office operating hours and days, which can access the office and on what terminals.
- **Security**—Security provides user authentication and transaction level security for applications. Each user is assigned a security profile at login, consisting of functional access, limits, and override authority.

ARGO's security can also be integrated with host security systems such as RACF and Top Secret.

- **Host communications**—ARGO's Host Communication provides the ability to communicate with multiple host types, using multiple message formats over multiple communication protocols.
- **Store and forward**—Store & Forward Service provides the ability to queue host communication transaction requests when the host is unavailable or off-line. Store & Forward maintains a "heart beat" with the host and attempts to send any transactions in its queue to the host. This support allows transactions performing host updates to be processed even when the host system is unavailable. Additionally, by using the "Send to Store & Forward" service, transactions can be routed directly to the Store & Forward queue, to enable the scheduling of less critical host transmission when the host is not heavily used.

Store & Forward is automatically invoked when host connectivity is lost, which ensures transactions are uploaded to the host. Store & Forward transactions are stored in the middle tier and are forwarded to the host asynchronously. Store and Forward systematically checks for host availability and subsequently paces transactions once the host is available. Configurable pacing parameters are available to avoid host overload. These pacing parameters include the frequency at which to check for host availability, inter-transaction delay, and time of day.

- **Electronic journal**—Electronic journal provides the ability to maintain an electronic journal of the activities performed by an operator. The Electronic Journal maintains cashbox activity associated with each operator, cash dispenser, vault, and ATM. Functionality to perform teller transaction corrections and reversals are available within the Electronic Journal.
- **Totals**—Totals provides the ability to maintain application totals, cashbox totals, and batch details. Totals are tracked by cashbox. Branch and region level totals are generated from these totals. Totals are also maintained by AM, PM, calendar day, business day, month-to-date, and year-to-date.

SQL Database

The online transaction processing (OLTP) SQL database is used to store configuration, event, operational, and security profiles and limits as well as Check 21 images. For example, data such as an Electronic Journal of all of the teller’s activities, the cashbox position for every teller in the enterprise, and the name and number of threads configured for the server are all stored in the SQL database.

Testing Results

Figure 4 shows the results of the testing that was performed for the solution. For the scope of the testing completed, the test setup used a 256k WAN link that simulated 0.1% packet loss and 100ms latency.

The Argo teller application was used for the interactive traffic and the digital check images were simulated.

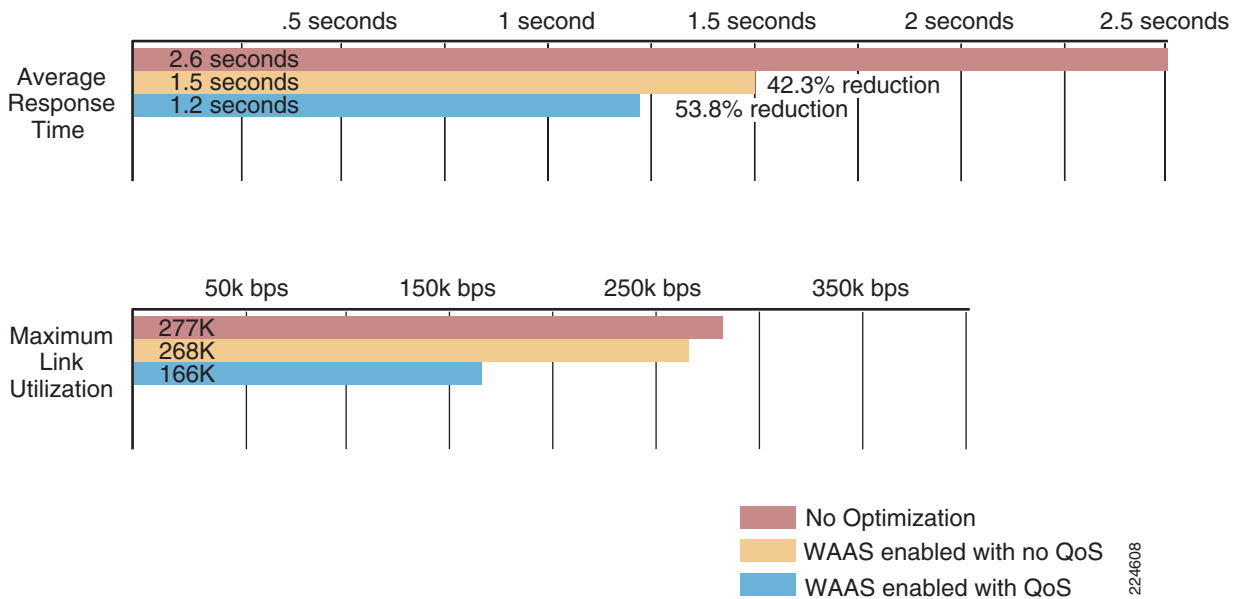
The test consisted of 152 individual transactions which resulted in 712 unique requests. The check image traffic was queued up for the test and consisted of 234 unique check images.

Note in Figure 4 that the addition of QoS did not have any effect on the test results because we did not generate enough traffic to saturate the link and, as a result, no QoS was applied. Additional testing on this will be performed in future phases.

What testing demonstrates is that by implementing WAAS on the WAN, bandwidth consumption can be reduced significantly, which allows for the addition of other IP-based services, such as voice, video, Web, etc. The addition of QoS lets you deploy these additional services and still be able to guarantee your SLAs on the interactive traffic.

Figure 4 Testing Results

Tests performed over 256k link, 0.1% packet loss and 100ms latency
 152 transactions/712 Requests and 59.4mb of check images



224608

Solution Components

The solution components required for Cisco CCE—Digital Image Management span across several key technologies. These technologies, used in combination, address the requirements to improve communication flow between a retail branch store and the data center.

Data Center Components

Table 1 **Data Center Components**

Component	Description	Lab Configuration
Cisco Catalyst 6500	Core routers and aggregation routers	s72033-adventerprisek9_wan-mz.122-18.SXF10.bin, i.e., 12.2(18)SXF10
ACE10-6500-K9	Application Control Engine Module	c6ace-t1k9-mz.A2_1.bin
7206VXR	Data center WAN router	c7200p-advipservicesk9-mz.124-15.T1.bin
WAE-612	WAAS Central Manager	oe612-4.0.13.12
WAE-7326	Data center WAE appliance	oe7326-4.0.13.12
Cisco Catalyst 4948	Data center access switch	cat4000-i9s-mz.122-25.EWA11.bin

Branch Components

Table 2 **Branch Components**

Component	Description	Lab Configuration
Cisco WS-C3750G-48PS	Cisco 48 port switch	c3750-ipservices-mz.122-25.SEE2.bin
Cisco 3845	Cisco Integrated Services Router (ISR)	c3845-adventerprisek9-mz.124-15.T3
Cisco NM-WAE-502-K9	Cisco WAAS network module	nme-wae-502-4.0.7.46

Partner Components

Table 3 Partner Components

Component	Recommended	Lab Configuration
Teller Workstation	Single 32-bit – 3.2 GHz processor	Cisco 7845
IOCP	1024 MB memory	2 x Dual core Xeon 3.4Ghz processors
	36 GB Disk Space	3.5 GB memory
	1024x768 display resolution	70GB Disk (Raid 5)
	Windows XP Professional	
Request Managers	Two-way 32-bit Intel Xeon 3.0 GHz	Cisco 7845
Application Servers	Dual-core	2 x Dual core Xeon 3.4Ghz processors
Database Server	2 GB memory	3.5 GB memory
Load Generator	RAID 1: Two 72 GB Disk drives	70GB Disk (Raid 5)
	Windows Server 2003	

Reference Design Guides

The Digital Image Management solution is layered on several foundational design guidelines which are often referred to as places in the network (PINS). The PINs that should be followed are listed in [Table 4](#).

Table 4 PINS and Design Guides

PIN	Links
Branch Design Guides	http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a00807593b6.pdf
	http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns656/net_design_guidance0900aec80488134.pdf
	http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a00807593b6.pdf
	http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a00807593b7.pdf
Data Center Design Guides	http://cisco.com/application/pdf/en/us/guest/netsol/ns107/c649/ccmigration_09186a008073377d.pdf
Next Gen Metro and WAN Design	http://www.cisco.com/application/pdf/en/us/guest/netsol/ns264/c649/ccmigration_09186a00808c77d9.pdf

Designing the Solution

WAN Optimization

WAAS optimizes performance of any TCP-based application in a WAN or MAN environment. A typical bank branch has a private WAN link of 256 Kbps or 512 Kbps. Optimizing the traffic over WAN enables banks to do more with their WAN link. WAAS consists of the following hardware components:

- **Application Accelerators**—An application accelerator is deployed on each side of the optimized connection. Upon discovery of the device on each end of the connection, the application accelerators exchange information pertaining to the TCP flow and their capabilities to optimize it. When placed within the data center, the WAE is the TCP optimizer for the origin servers. When placed at the branch, the WAE is the main TCP optimization and caching proxy for branch clients. With WAAS, the TCP headers are fully preserved.
- **WAAS Central Manager (CM)**—Provides management, configuration, and monitoring of all the WAEs in the deployment. Using the CM, one can apply a unified configuration of application policies to the WAEs, collect health and performance information, and view performance statistics. The WAAS CM usually resides within the data center, although it can be physically placed anywhere provided that there is a communications path to all the managed WAEs.

In this design, two WAEs are installed on the branch side and data center side respectively. Cisco NM-WAE is placed at the branch; Cisco high-end WAE appliance WAE-7326 is placed at the data center/WAN edge for aggregation of WAAS services. Install the WAE at the WAN edge to increase optimization coverage to all hosts in the network. In addition, placing data center WAE at the WAN edge would relieve the WAE from the internal traffic of the data center.

One CM is installed to configure the WAE via the Web interface and obtain centralized reporting, such as total traffic reduction, application mix, and pass-through traffic. WAAS continues to function in the event of CM failure, but configuration changes via the CM are prohibited.

Optimizations are performed between the branch WAE and the data center WAE after configuring interceptions on routers and application policies on WAEs:

1. Configure routers to intercept packets. The WAN/branch router intercepts the packets from the client and data center servers. Data is transferred between the clients and servers transparently, without knowing that the traffic flow is optimized through the WAEs. Web Cache Communications Protocol version 2 (WCCPv2) is used for interception since WCCPv2 provides more high availability and scalability features and is also easier to configure. Use **show ip wccp** for verification.
2. Through WAAS Central Manager GUI, configure WAEs to optimize for a particular TCP traffic (this step is often not needed because the default policies on a WAE cover common type of TCP traffic).

For ARGO teller application, check images use TCP port 9311 and transaction data use TCP port 5008. To check if the port is already configured in the default policy, type **show run | in <port>**.

```
ANS-CoreWAE#sh run | in 9311
```

```
ANS-CoreWAE#sh run | in 5008
```

No output from the commands indicates that neither port 9311 nor port 5008 are defined.

When you choose a TCP port for customized application, avoid using a well-known port. For example, the default policies on a WAE includes “for traffic destined to port 5007, let it pass through.” If you use port 5007 and modify default policy to “for traffic destined to port 5007, use full optimization,” then the original application with port 5007 would be changed to use optimization.

We need to configure “for traffic destined to port 9311, apply full optimization” as well as “for traffic destined to port 5008, apply full optimization” through WAAS CM.

Use **show tfo conn summary** for verification.

```
WAE-ARGO#sh tfo conn sum
Optimized Connection List
Policy summary order: Our's, Peer's, Negotiated, Applied
F: Full optimization, D: DRE only, L: LZ Compression, T: TCP Optimization
Local-IP:Port      Remote-IP:Port      ConId  PeerId      Policy
11.1.1.2:1447      10.1.190.10:5008    7      00:14:5e:a4:52:34 F,F,F,F
11.1.1.2:1450      11.1.2.6:9311      9      00:14:5e:a4:52:34 F,F,F,F
```

Use **show stat tfo** to see percentage improvement or check stats through central manager.

Virtual Private Network Services

The recommended configuration is to use 802.1x key management. This mandates the use of an external RADIUS server to authenticate end user devices. By using Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), unlike Lightweight Extensible Authentication Protocol (LEAP) authentication, the entire authentication stream is encrypted end-to-end. This approach provides a high level of security across the wireless network during the authentication process.

Redundant Network Connectivity

The recommended configuration is to use 802.1x key management. This mandates the use of an external RADIUS server to authenticate end user devices. By using Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), unlike Lightweight Extensible Authentication Protocol (LEAP) authentication, the entire authentication stream is encrypted end-to-end. This approach provides a high level of security across the wireless network during the authentication process.

Voice Services

Voice services were not tested with this version of the solution. However, we chose an IOS image for the 3845 that has been tested to support voice services. Refer to Services Ready Large Branch Foundation CVD (currently in draft format).

Quality of Service

Quality of Service (QoS) policies are similar to rules for balancing work and life. While humans set up a rule to balance work and life, such as “spend 8 hours at work and 8 hours for personal life,” QoS enables a router to act according to a policy when it can not transport everything it receives, such as “allocate 30% of capacity on transaction data; allocate 20% of capacity on check images.”

We need to consider three things when designing quality of service:

1. Where is the congestion point from end to end?

In a typical branch and data center design, congestion usually happens at the branch WAN router because of the limited capacity of WAN link. A bank branch usually has a 256K or 512K private WAN link. So we need to instruct branch WAN router what to do when traffic is larger than the link capacity. We also need to apply QoS among the routers inside the wide area network.

2. How to identify the traffic in the system?

There are three types of traffic in this phase I design:

- Routing protocol and Layer 2 control packets
- Transaction data
- Check images

We can identify transaction data and check imaging through TCP ports. Transaction data uses TCP port 5008 and check imaging uses TCP port 9311. After identifying or classifying traffic, we often mark them by setting the type of service (ToS) byte in a packet so downstream routers can identify them by looking at the ToS byte in a packet.

3. How do you treat them differently during congestion?

There are three kinds of treatment:

- Congestion avoidance—Congestion avoidance drops packets randomly to signal upper layer protocol to slow down traffic. The most used one is weighted random early detect.
- Congestion management—Congestion management, also known as queuing, buffers traffic in queues and then decides which queue of traffic to transmit first. Queuing packets is similar to putting tasks into several to-do lists then performing a task from one of the to-do lists. The most used ones are low-latency queuing and class-based weighted fair queuing.
- Traffic conditioning—Traffic conditioning limits traffic to a specific rate through traffic policing or traffic shaping.

For an in-depth design guide on QoS, refer to <http://www.cisco.com/go/srnd>. This publicly available Web site provides excellent Solution Reference Network Design material.

- [Enterprise QoS Solution Reference Network Design Guide Version 3.3](#)

High Availability (HA) Considerations

The goal of a highly-available system is to eliminate and automate as much as possible all aspects of the solution. A signal point of failure anywhere in the system can lead to unscheduled outages as well as possibly sporadic availability. Monitoring of the overall system end-to-end is also a critical component to determine just how available the system is. Since there are a number of different technologies used in the solution, we break down each component part to identify possible HA architectures. For each major grouping of components, we also include suggested monitoring systems and techniques that can be employed in order to validate the availability.

Application Load Balancing

The Cisco Application Control Engine (ACE) is a service module that provides advanced load balancing and protocol control for data center applications. It scales up to 16 Gbps and four million concurrent TCP connections. In addition to performing Layer 3, 4-7 load balancing, SSL off-load, and deep packet inspection, ACE can be partitioned to multiple contexts, with each context acting like an independent ACE.

We can create one context “argo” to load balance for teller application; select one request manager to process transaction data entered by tellers. We can create another context “users” to load balance traffic for customer access; select one Web server to process online banking requests. These two contexts are independent. Modifying one does not affect the other. For example, we can configure the “users” context with deep packet inspection (possible because ACE contexts are placed outside the WAAS optimization path.)

The ARGO browser teller application establishes a connection from each branch, regardless of how many tellers are in the branch. ACE load balances on a per-connection basis. For ARGO transaction data, we configure ACE to perform Layer 4 load balancing, identifying traffic through the unique TCP port number. ACE supports multiple load balancing algorithms. We selected the “Least connections” algorithm for this design.

Refer to [Figure 2](#). A pagent router simulates a WAN. Branch devices are on the left side of the pagent router and data center devices are on the right side of the pagent router. ACE is a module in the aggregation router in the data center.

If the teller workstation sends a request to the address of request manager 1, ACE lets the traffic go through without taking any action. For ACE to do load balancing, there are two requirements:

- Client machines send traffic to a virtual IP address.
- We configure a policy on the ACE. If traffic is destined to a virtual IP address, we load balance by selecting one of the servers in the server farm.

For the ARGO teller application, we configured the following policy: for TCP traffic destined to VIP address with port 5008, forward it to request manager 1 or request manager 2, depending on which server has the least number of connections.

For example, when five branches sent traffic to data center, **show rserver** displays that ACE sends connections from three branches to request manager 1 and sends connections from the other two branches to request manager 2.

```
ACE1-Slot3/argo# sh rserver
```

```
rserver          : RM1, type: HOST
state            : OPERATIONAL (verified by arp response)
-----
```

real	weight	state	connections	
			current	total
serverfarm: ARGO_FARM				
11.1.2.2:0	8	OPERATIONAL	3	106

```
rserver          : RM2, type: HOST
state            : OPERATIONAL (verified by arp response)
-----
```

real	weight	state	connections	
			current	total
serverfarm: ARGO_FARM				
11.1.2.3:0	8	OPERATIONAL	2	5

Cisco Infrastructure

The Cisco infrastructure required to deliver the Cisco CCE—Digital Image Management solution can be broken down into a number of horizontal technologies which are described in the subsections below. It is beyond the scope of this document to describe in detail the various high availability aspects of each technology used. For an in-depth discussion, it is recommended that the Solution Reference Network Designs and Cisco Validated Designs (CVDs) be referenced. The SRND and CVDs can be downloaded from <http://www.cisco.com/go/srnd> and <http://www.cisco.com/go/cvd> respectively.

In summary, the overall availability of Cisco CCE—Digital Image Management depends upon the infrastructure on which it is deployed. Items that should be considered in the high availability planning process include:

- Network core, distribution, and access

- Diverse power sources for each component comprising a pair of redundant devices or servers
- Redundant Active Directory, DNS, and DHCP servers
- Redundant Unified Communications components
 - Call Manager Clusters with redundant TFTP servers activated
 - ISR Voice Gateways
 - Server Load Balancing SLB for XML service redundancy
- Redundant paths between core, distribution, access, and wireless layers
- Validated Layer 2 and Layer 3 routing protocols for rapid convergence
- Dual-homed servers utilizing Fast Etherchannel on separate switch fabrics (ACS, DNS, DHCP, Active Directory, etc.)
- Cold spared hardware for core, distribution, access, wireless controllers, access points, servers, etc.
- Each redundant component should be on a separate maintenance, upgrade, and outage schedule.

Although only a summary, this lists items that must be considered during the GAP analysis phase.

Network Components

The network components include the Layer 2 and Layer 3 devices that compose the campus network and specifically include access, distribution, and core layers. There are a number of Solution Reference Network Design guides (SRNDs) available. The key documentation that is recommended for Cisco CCE—Digital Image Management include:

- Designing a Campus Network for High Availability
- Campus Network Multilayer Architecture and Design Guidelines
- Deploying a Fully Routed Enterprise Campus Network
- Campus Design: Analyzing the Impact of Emerging Technologies on Campus Design

After reviewing these SRNDs, it is recommended that a GAP analysis or readiness check be performed. To help facilitate this step, it may be helpful to engage a third-party Cisco Certified implementation partner for each of the areas where a GAP was identified. In general, and in line with eliminating all single points of failure in the design, the following are mandatory for achieving a highly available network architecture which is capable of delivering between 99.99% and 99.999% availability. These levels of availability represent between 52.33 and 5.35 minutes of downtime per year, a goal that is highly desirable for any network delivering critical services such as those found in Cisco CCE—Digital Image Management.

Security

General Notes/Best Practices for the Integrated Service Router

In addition to configuring the edge router to secure the network perimeter, there are several device-hardening measures that can be taken on an ISR to minimize the risk of illegitimate access to the device.

The following are general best practices for configuration of the ISR router for perimeter security:

- Firewall rule sets must adhere to a “least amount of access necessary” policy. Rules must be defined by specific source/destination addressing and TCP/UDP ports required for the cardholder data environment on the point-of-sale networks.
- Ensure that inspection rules are enabled on the ISR router so that the firewall maintains state (none are enabled by default).

The following are general best practices for securing management access to the ISR router itself:

- Disable the HTTP server service on the router and enable the HTTP secure server.
- Configure the session-timeout and exec-timeout commands to 15 minutes or less on the console, aux, VTY, and line interfaces on the router.
- Configure appropriate banner messages on login, incoming, and exec modes of the router. The login banner warning should not reveal the identity of the company that owns or manages the router. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the router to be directed to the access control server (ACS). Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the router itself in the event of a WAN or ACS failure.
- Use the no service password-recovery command in conjunction with the service password encryption command to prevent password theft by physical compromise of the router.
- Change default passwords and community strings to appropriate complexity.

Cisco CCE—Digital Image Management Implementation

This section provides implementation details for the services enabled by Cisco CCE—Digital Image Management and includes configuration examples. This section describes the steps required to configure features across the components to enable the services. Some design concepts and limitations are provided that you should keep in mind during implementation.

Test Method

Configuration and testing was conducted in this order:

1. Network connectivity
2. ACE load balancing
3. WAAS
4. QoS
5. Redundant WAN connectivity

The primary link is 256Kbps. WAN simulation is 0.1% packet loss and 100ms latency.

Data Center

Data Center Servers

Data center servers and their IP addresses:

- Request manager 1: 11.1.2.2
- Request manager 2: 11.1.2.3
- Application server 1: 11.1.2.5
- Application server 2: 11.1.2.6
- Database server: 11.1.2.7
- BPU LOAD: 11.1.2.4

Each server has two network connections. Local Area Connection is used for remote desktop access and Local Area Connection 2 connects to the c4948. For these servers, set default gateway 11.1.2.1 on Local Area Connection 2.

Access Router C4948

The access router connects to the aggregation router through a trunk port and connects to a data center server through an access port.

The connection between c4948 and aggregation router 1:

c4948 (TenGigabitEthernet1/49) --- (TenGigabitEthernet4/6) aggregation router 1

Step 1 Configure trunk port:

```
int TenGigabitEthernet1/49
description this goes to aggregation router 1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 191
switchport mode trunk
```

```
conf t
vlan 191
```

Step 2 Configure access port (do this for each port which connects to a server). For example:

```
interface GigabitEthernet1/1
switchport access vlan 191
switchport mode access
```

Aggregation Router 1 (C6509)

On its ACE module, create an argo context. On the argo context, server side VLAN 191 is Layer 2 and client side VLAN 190 is Layer 3. On the MSFC console, create interface VLAN 190 so the ACE argo context and MSFC can route.

The connections of the aggregation router:

Core router --- MSFC of aggregation router --- ACE (vlan 191) --- branch access router

On the MSFC, configure 10.1.3.2 as the IP address of the interface connecting to the core router.

Also configure an IP address for connecting to ACE: int VLAN 190, 10.1.190.2.

On the ACE, configure: int VLAN 190, 10.1.190.4.

Also configure an IP address for connecting to branch access router: VLAN 191, 11.1.2.4.

Step 1 Configure the port that connects to the access router:

```
interface TenGigabitEthernet4/6
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 190,191
 switchport mode trunk
 no ip address
 rmon collection stats 6054 owner monitor
```

Step 2 Configure VLANs, then configure the VLAN group then assign it to the ACE:

```
svclc module 3 vlan-group 1
svclc vlan-group 1 190,191
vlan 190
name argo-client
vlan 191
name argo-server
```

Step 3 Configure ACE client side:

```
interface Vlan190
 description ARGO Testing - ACE client side connection
 ip address 10.1.190.2 255.255.255.0
 ip nat inside
```

Step 4 Configure routing:

```
router eigrp 10
 network 10.0.40.0 0.0.0.255
 network 10.1.2.0 0.0.0.255
 network 10.1.3.0 0.0.0.255
 network 10.1.7.0 0.0.0.255
 network 10.1.21.0 0.0.0.255 ! for WAAS central manager
 network 10.1.40.0 0.0.0.255
 network 10.1.50.0 0.0.0.255
 network 10.1.100.0 0.0.0.255
 network 10.1.190.0 0.0.0.255
 no auto-summary
```

Step 5 Configure default route:

```
ip route 11.1.2.0 255.255.255.0 10.1.190.4
```

Step 6 Allow VLANs in port channel:

```
interface Port-channel1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 190,191,220,221,230,231,240,241
 switchport mode trunk
 no ip address
 spanning-tree guard loop
!
interface TenGigabitEthernet4/1
 description To ANS1-AGG-2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 190,191,220,221,230,231,240,241
 switchport mode trunk
 no ip address
 rmon collection stats 6049 owner monitor
 channel-protocol lacp
 channel-group 1 mode active
```

```

interface TenGigabitEthernet4/2
description To ANS1-AGG-2
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 190,191,220,221,230,231,240,241
switchport mode trunk
no ip address
rmon collection stats 6050 owner monitor
channel-protocol lacp
channel-group 1 mode active
!
```

Step 7 Add configuration to support WAAS central manager:

```

ip nat inside source static 10.1.21.2 172.28.196.251
ntp master
interface GigabitEthernet2/3
description to WAAS Central Manager
switchport
switchport access vlan 21
switchport mode access
no ip address
speed 1000
duplex full
rmon collection stats 6002 owner monitor
spanning-tree portfast
end

interface Vlan21
description to WAAS Central Manager
ip address 10.1.21.1 255.255.255.0
ip nat inside
end
```

Step 8 Configure Admin context to include argo context:

```

context argo
description financial services application
allocate-interface vlan 82
allocate-interface vlan 190-191
member Gold
```

Step 9 Configure argo context:

```

access-list ANYONE line 10 extended permit ip any any
access-list ANYONE line 20 extended permit icmp any any
```

```

probe icmp PING
interval 5
passdetect interval 2
passdetect count 1
probe tcp PROBE-TCP
port 5007
interval 2
faildetect 2
passdetect interval 10
passdetect count 2

rserver host RM1
ip address 11.1.2.2
inservice
rserver host RM2
ip address 11.1.2.3
inservice
```

```

serverfarm host ARGO_FARM
  predictor leastconns
probe PING
probe PROBE-TCP
  rserver RM1
  inservice
  rserver RM2
  inservice

class-map type management match-any REMOTE-MANAGEMENT
  2 match protocol telnet any
  3 match protocol icmp any
  4 match protocol ssh any
  5 match protocol snmp any
  6 match protocol http any
  7 match protocol https any
class-map match-any VIP-TCP
  2 match virtual-address 10.1.190.10 tcp eq 5007
  3 match virtual-address 10.1.190.10 tcp eq 4098

policy-map type management first-match REMOTE-MANAGEMENT
  class REMOTE-MANAGEMENT
    permit

policy-map type loadbalance first-match VIP-POLICY-10
  class class-default
    serverfarm ARGO_FARM

policy-map multi-match LB-VIP
  class VIP-TCP
    loadbalance vip inservice
    loadbalance policy VIP-POLICY-10
    loadbalance vip icmp-reply

! peer ip address refers to the address of the other ACE
! when access ACE, we use alias address which includes addresses for both ACEs
interface vlan 190
  description Client side vlan
  ip address 10.1.190.4 255.255.255.0
  access-group input ANYONE
  service-policy input LB-VIP
  service-policy input REMOTE-MANAGEMENT
  no shutdown
interface vlan 191
  description Server side vlan
  ip address 11.1.2.1 255.255.255.0
  access-group input ANYONE
  service-policy input REMOTE-MANAGEMENT
  no shutdown

```

The default route on the argo context should point to the addr of int VLAN 190 on the MSFC:

```
ip route 0.0.0.0 0.0.0.0 10.1.190.2
```

WAAS Central Manager (WAE-612)

Every WAAS device uses ntp server 10.1.3.2 (IP address on aggregation router 1).

```
device mode central-manager
```

```

primary-interface GigabitEthernet 1/0
interface GigabitEthernet 1/0
 ip address 10.1.21.2 255.255.255.0
 exit
ip default-gateway 10.1.21.1
cms enable

```

Core Router 1 (C6509)

Configure router:

```

router eigrp 10
 network 10.1.190.0 0.0.0.255

ip route 11.1.2.0 255.255.255.0 10.1.190.4
ip route 10.1.191.0 255.255.255.0 10.1.190.4

```

Data Center WAE (WAE-7326)

```

device mode application-accelerator
primary-interface GigabitEthernet 1/0
!
interface GigabitEthernet 1/0
 ip address 10.1.20.2 255.255.255.0
 exit
ip default-gateway 10.1.20.1
wccp router-list 1 10.1.20.1
wccp tcp-promiscuous router-list-num 1
wccp version 2
central-manager address 10.1.21.2
cms enable
flow monitor tcpstat-v1 host 10.1.70.11
flow monitor tcpstat-v1 enable
!
tfo tcp optimized-send-buffer 2048
tfo tcp optimized-receive-buffer 2048

```

DC WAN Router (C7206VXR)

Step 1 Configure interception:

```

ip wccp 61
ip wccp 62
ip wccp 61 redirect in

 ip wccp 62 redirect out

interface Serial1/2:1

ip wccp 61 redirect in

interface Gi0/1

ip wccp 62 redirect in

interface Gi0/2

ip wccp 62 redirect in

interface GigabitEthernet2/0

```

```

description to ANS Core WAE 7326
ip address 10.1.20.1 255.255.255.0
ip flow egress
negotiation auto
end

```

Step 2 Configure routing:

```

router eigrp 10
network 10.1.8.0 0.0.0.255 ! for core 1
network 10.1.9.0 0.0.0.255 ! for core 2
network 10.1.20.0 0.0.0.255 ! for data center WAE
network 12.1.1.0 0.0.0.255 ! for branch WAN route (go through L2 pagent)
no auto-summary

interface GigabitEthernet2/0
description to ANS Core WAE 7326
ip address 10.1.20.1 255.255.255.0
ip flow egress
negotiation auto

```

Step 3 Configure fractional T1:

```

dc_wan(config)#controller T1 1/2
dc_wan(config-controller)#channel-group 1 timeslots 1-4

```

pagent Router (C3745)

The pagent router is configured as a Layer 2 device (pass-through mode).

```

interface Serial0/0
description link to serial1/3:1 on DC WAN 7206 Router
no ip address
no keepalive
no fair-queue
service-module t1 timeslots 1-24
end

```

```

interface Serial0/1
description Link to FS-ISR-2 Branch 3845
no ip address
no keepalive
no fair-queue
service-module t1 timeslots 1-24
end

```

```

br3_pagent#pmod
br3_pag(PMOD:Vo0:0/0)#show config
br3_pag(PMOD:Vo0:0/0)#show interface

```

#	interface	admin state	operational state	filters created	PMOD state	PMOD peer
5	Vo0	up	up	0	inactive	
2	Se0/0	up	up	0	inactive	
4	Se0/1	up	up	0	inactive	
1	Fa0/0	up	down	0	inactive	
3	Fa0/1	up	down	0	inactive	

```

br3_pag(PMOD:Vo0:0/0)#se0/0
br3_pag(PMOD:Se0/0:0/0)#active
br3_pag(PMOD:Se0/0:0/0)#se0/1
br3_pag(PMOD:Se0/1:0/0)#active

```

```
***Interfaces Serial0/0 and Serial0/1
are now internally connected by Passthru Modify.
```

```
br3_pag(PMOD:OFF:Se0/1:0/0)#show interface
```

#	interface	admin state	operational state	filters created	PMOD state	PMOD peer
5	Vo0	up	up	0	inactive	
2	Se0/0	up	up	0	active	Se0/1
4	Se0/1	up	up	0	active	Se0/0
1	Fa0/0	up	down	0	inactive	
3	Fa0/1	up	down	0	inactive	

```
br3_pag(PMOD:OFF:Se0/1:0/0)#end
```

```
latency = 100ms, packet loss = 0.1%
```

```
br3_pag(PMOD:ON:Se0/1:0/0)#stop
br3_pag(PMOD:OFF:Se0/1:0/0)#delay on
br3_pag(PMOD:OFF:Se0/1:0/0)#delay duration 100
br3_pag(PMOD:OFF:Se0/1:0/0)#drop on
br3_pag(PMOD:OFF:Se0/1:0/0)#drop one-in 1000
br3_pag(PMOD:OFF:Se0/1:0/0)#start
```

Configure fractional T1:

```
br3_pagent(config)#interface Serial0/0
br3_pagent(config-if)#service-module t1 timeslots 1-4
br3_pagent(config-if)#interface Serial0/1
br3_pagent(config-if)#service-module t1 timeslots 1-4
```

Branch

The following represents portions of the code for the branch devices pertinent to this implementation and testing.

Branch WAN Router (C3845 ISR)

Step 1 Configure QoS (configure access-list to match on TCP destination port):

```
ip access-list extended data
permit tcp any any eq 5007
exit
ip access-list extended images
permit tcp any any eq 9311
exit

class-map transactions
match access-group name data
exit
class-map check_images
match access-group name images

policy-map p0
class transactions
bandwidth percent 80
class check_images
```

```

bandwidth percent 10
shape average percent 60

int Serial0/1/0:0
!by default the maximum reservable bandwidth on any interface is 75%
max-reserved-bandwidth 90
service-policy out p0

```

Step 2 Configure routing:

```

interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
media-type rj45
!
interface GigabitEthernet0/0.98
description ARGO data VLAN
encapsulation dot1Q 98
ip address 11.1.1.1 255.255.255.0

policy-map p0
class class-default
police 256000

interface Serial0/1/0:0
ip address 12.1.1.2 255.255.255.0
service-policy input p0
service-policy output p0

router eigrp 10
network 11.1.1.0 0.0.0.255
network 12.1.1.0 0.0.0.255
no auto-summary

```

Step 3 Configure interception:

```

ip wccp 61
ip wccp 62

interface Gi0/0.90

ip wccp 61 redirect in

interface se0/1/0:0

ip wccp 62 redirect in

```

Step 4 Configure fractional T1:

```

FS-ISR-branch(config)#controller T1 0/1/0
FS-ISR-branch(config-controller)#channel-group 0 timeslots 1-4

sh int Serial0/1/0:0
Serial0/1/0:0 is up, line protocol is up
...BW 256 Kbit

int Serial0/1/0:0
load-interval 30

```

Step 5 Configure the interface:

```

interface Integrated-Service-Engine2/0
description Branch WAAS module
ip address 11.1.10.1 255.255.255.0

```

```

no ip redirects
no ip unreachable
no ip proxy-arp
ip nbar protocol-discovery
ip route-cache flow
service-module ip address 11.1.10.3 255.255.255.0
service-module ip default-gateway 11.1.10.1
no keepalive

interface GigabitEthernet0/0.90
description WAAS module
encapsulation dot1Q 90
no ip redirects
no ip unreachable
no ip proxy-arp

interface GigabitEthernet0/0.98
description ARGO data VLAN
encapsulation dot1Q 98
ip address 11.1.1.1 255.255.255.0
no ip redirects
no ip unreachable
no ip proxy-arp

```

Step 6 Advertise to the other routers:

```

conf t
router eigrp 10
network 11.1.10.0 0.0.0.255
no auto-summary

```

WAE Module (NM-WAE-502-K9)

```

hostname WAE-ARGO
clock timezone US/Pacific -7 0
ip domain-name cisco.com
primary-interface GigabitEthernet 1/0
interface GigabitEthernet 1/0
ip address 11.1.10.3 255.255.255.0
no autosense
bandwidth 1000
full-duplex
exit
ip default-gateway 11.1.10.1
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
ntp server 10.1.3.2
!
!
wccp router-list 1 11.1.10.1
wccp tcp-promiscuous router-list-num 1
wccp version 2

central-manager address 10.1.21.2
cms enable

```

Branch Access Switch (C3750)

Interface gi1/0/13 connects to IOCP (IP address is 11.1.1.3).

```
interface GigabitEthernet1/0/48
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 98
  switchport mode trunk

interface GigabitEthernet1/0/13
  switchport access vlan 98
  switchport mode access
!
interface GigabitEthernet1/0/14
  switchport access vlan 98
  switchport mode access
```

Branch Client Machines (Windows-Based Workstations)

Branch client machines and their IP address are:

- Teller workstation: 11.1.1.2
- IOCP: 11.1.1.3

Each machine has two network connections. Local Area Connection is used for remote desktop access and Local Area Connection 2 connects to the branch access switch. For these machines, set default gateway 11.1.1.1 on Local Area Connection 2.

Partner Configuration Considerations

The changes in the ARGO Teller application for this deployment are minimal:

- ARGO can be configured to use a range of ports or a fixed port. Configure it to use port 5008 for transaction data.
- Instead of configuring requests go to one of request managers, configure them to go to a virtual IP address so ACE can load balance the connection requests.

Cisco Validated Design

The Cisco Validated Design Program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit:

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

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING,

WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.