# Background Information for World-Wide Trading Company

World-Wide Trading (WWTC) is a large online broker firm in the Hong Kong. The trading company has a staff of 9,000 who are scattered around the globe. Due to aggressive growth in business, they want to establish a regional office in New York City. They leased the entire floor of a building on Wall Street. You were hired as the director of the IT Department. The President of the company asked you to set up the state of the art network by end of this year. He shared with you the organizational structure and a list of the staff. You hired a consultant to test the network infrastructure and power requirement at WWTC office space. The consultant reported that the network infrastructure is solid and gigabit network can be set up on existing network wiring. Also, the existing power supply will meet their current and future demand. The President has reiterated these business goals.

# Business and Technical Goals

* Increaserevenue from 10 billion to 40 billion in three to four years
* Reduce the operating cost from 30 to 15 percent in two to three years by using an automated system for buying and selling.
* Provide secure means of customer purchase and payment over Internet.
* Allow employee to attach their notebook computers to the WWTC network and Internet services.
* Provide state of the art VoIP and Data Network
* Provide faster Network services
* Provide fast and secure wireless services in the lobby and two large conference rooms (100x60)

On the basis of these business goals, you prepared a RFP to solicit a proposal for designing and implementing a fast, reliable and secure network.

The purpose of this Request for Proposal is to solicit from qualified vendors proposals for a

secure and fast network to ensure proper operation of the network.

To prepare a design for a state of the art network at the Wall Street location of World-Wide Trading.

Propose a Network design that solves the current security audit problems (see security sections), to meet business and technical goals.

Provide a modular, scalable and network.

Provide redundancy at building core layer and building distribution layer and access layer and at workstation level to avoid failure at one point. For Building Access layer provide redundant uplinks connection to Building Distribution layer.

Select appropriate Cisco switch model for each part of your enterprise campus model design from the Cisco Products Link, and use the following assumptions in your selection process.

**Selecting the Access layers switches:**

* 1. Provide one port to each device
  2. Make provision for 100% growth

**Server farm switches**

* Assume 6 NIC cards in each server and one NIC card uses one port of switch
* Dual processors and dual power supply

Propose an IP addressing redesign that optimizes IP addressing and IP routing (including the use of route summarization). Provide migration provision to IPv6 protocol in future.

Propose a High Level security plans to secure key applications and servers but encryption of all application is not acceptable. Develop security policy to stop sniffing and man-in-the-middle attack. Your security plan must be based on current industry standards. Multilayer security or defense-in-depth.

Integrate voice and data network to reduce cost. For dialing outside, the World-Wide Trading Company proposes a plan for 100% connectivity with a minimum number of outside lines. For telephone requirements, see the Organization Chart and Telephone Equipment Table.

Provide aggregate routing protocols with hierarchal IP scheme.

Centralize all services and servers to make the network easier to manage and more cost-effective.

Provide LAN speed minimum 100 MB and Internet speed minimum 54 MB.

Provide wireless network access to network users and guest users in limited area (Lobby and Conference room). In conference room and the lobby, the user will get a minimum 54 Mbps of bandwidth. (You can assume that site survey is done and no sources of interference or RF were discovered.)

Provide provisions for video conference and multicast services.

Standardize on TCP/IP protocols for the network. Macintoshes will be accessible only on guest notebook but must use TCP/IP protocols or the Apple Talk Filling Protocol (AFP) running on top of TCP.

Provide extra capacity at switches so authorized users can attach their notebook PCs to the network

Install DHCP software to support notebook PCs

The World-Wide Trading Company will use the following applications:

* Microsoft Office 2014
* Sending and receiving e-mail
* Surfing the Web using Netscape or Microsoft’s Internet Explorer applications to access information, participate in chat rooms, and use other typical Web services
* Accessing the library card-catalog
* File Server application.

Associate will use the following Custom Applications

* **Market Tracking Application**. This application will provide real-time status of stock and bond market to brokers and their clients.
* **Stock and Bond Analytical Application.** This application will provide analysis of stock and Bond to Brokers only.
* **On Line Trading.** The Company wishes to train new clients in online trading to attract new customer. The Company will sign up new client to receive **streaming video** and instructions

1. Assume any information (with proper justification) which you think is missing and critical to the development of the design.

**WWTC Security:**

Although WTC has strong security requirements at other locations (see network diagram below), you will need to move to a significantly more secure network than WTC currently has available. At other places, lack of strong authentication, data confidentiality and separations between internal protected server and public server are principal areas that need to improve at this location.

Audit results of other locations identified the following problems

* E-mail had been inappropriately used at times to communicate Business sensitive information.
* Confidential business information and public data were connected to the same physical network.
* End users systems had inappropriately housed confidential data should have resided only on servers. In addition, some of the end-user systems were found to be laptops, which had left the facility in clear violation of security policies.
* Some logical control systems were found to rely on username and password combinations only.
* Some sensitive business information was found to be transmitted in clear text between server and client.



In order to address these audit findings, you decided to firm up security policies in these areas.

Internet Connectivity

Internet connectivity and any other unclassified network must be physically separate from the network

Classified Network

The classified network must be physically secure to prevent any access to the classified network’s data. Control should be put in place to prevent local users from removing data from the systems in any way. This includes removable media, AV recorders, pen and paper, and any form of printer.

All data transmitted on the classified network must be cryptographically protected throughout the network. All classified data must be centrally stored and secured in a physically separate area from the unclassified network.

WAN Connectivity

In addition to the cryptographic protections of the data within the classified network, all data crossing wide-area links should undergo another layer of cryptographic protection such as IPSec/VPN/SSL.

Public Servers

All public servers must configured HTTPS connections and accept all requests that are on valid IP addresses and pass through firewall. Server must ask some identity of the connecting party.

Site-to-site VPN tunnels

All devices must be mutually authenticated and cryptographic protection should be provided.

PSTN dial-up

Dial-up client must authenticate with username and OTP

User Education

All users should undergo periodic user awareness training program on network threats and good security practices.

**Deliverables**

These are only recommendations on the general approach you might take for this project.

1. Determine the most important assets of the company, which must be protected
2. Determine general security architecture for the company
3. Develop a list of 12specific policies that could be applied.
4. Write specific details along with the rationale for each policy
5. Integrate and write up the final version of the Security Policy Document for submittal
6. Develop a High availability secure design for this locations addressing above considerations and mitigating 4 primary networks attacks categories mentioned below.

The Four Primary Attack Categories:

* Reconnaissance attacks: An intruder attempts to discover and map systems, services, and vulnerabilities.
* Access attacks: An intruder attacks networks and systems to retrieve data, or gain access, or escalate access privileges
* Denial of Service attacks: An intruder attacks your network in a way that damages or corrupts your computer system or denies you and others access to your networks, system, or services.
* Worms, viruses, and Trojan horses: Malicious software is inserted onto a host in order to damage a system, corrupt a system, replicate itself, or deny services or access to networks, system or services.

The following are the guidelines for security policies.

**Security Policies:**

* Policies defining acceptable use
* Policies governing connections to remote network
* Polices outlining the sensitivity level of the various types of information held within an organization
* Policies protecting the privacy of the network’s user and any customer data
* Policies defining security baselines to be met by devices before connecting them to the network.
* Creates a basis for legal action if necessary.

The key components of security policies:

* Statement of authority and scope: Define the name of security authority and areas cover under that statement
* Identification and authentication policy
* Create Network access policy: How the user will use the company’s data infrastructure
* Remote access policy
* Incident handling policy: This topic specifies how the company will create an incident response team and the procedure to be used during and after an incident

**WWTC Active Directory Design**

WWTC office at New York is largely autonomous and few IT personnel to take care of day-to-day IT support activities such as password resets troubleshoot virus problems. You are concerned about sensitive data store in this location. You want to deploy a highly developed OU structure to implement security policies uniformly through GPO automatically at all domains, OU, and workstations.

At this location Windows Server 2014 is required providing the following AD features:

* Use BitLocker encryption technology for devices (server and Work station) disc space and volume.
* Enables a BitLocker system on a wired network to automatically unlock the system volume during boot (on capable Windows Server 2014 networks), reducing internal help desk call volumes for lost PINs.
* Create group policies settings to enforce that either Used Disk Space Only or Full Encryption is used when BitLocker is enabled on a drive.
* Enable BranchCache in Windows Server 2014 for substantial performance, manageability, scalability, and availability improvements
* **Implement Cache Encryption to store encrypted data by default.**  This allows you to ensure data security without using drive encryption technologies.
* Implement Failover cluster services
* Implement File classification infrastructure feature to provide automatic classification process.
* IP Address Management (IPAM) is an entirely new feature in Windows Server 2012 that provides highly customizable administrative and monitoring capabilities for the IP address infrastructure on a corporate network.
* Smart cards and their associated personal identification numbers (PINs) are an increasingly popular, reliable, and cost-effective form of two-factor authentication. With the right controls in place, a user must have the smart card and know the PIN to gain access to network resources.
* Implement Windows Deployment Services to enables you to remotely deploy Windows operating systems. You can use it to set up new computers by using a network-based installation.

Deliverables

Deliverables

* Create Active directory infrastructure to include recommended features
* Create OU level for users and devices in their respective OU
* Create Global, Universal, Local group.. Each global group will contain all users in the corresponding department. Membership in the universal group is restrictive and membership can be assigned on the basis of least privileged principle. (For design purpose, you can assume that WTC as a Single Forest with multiple domains).
* Create appropriate GPO and GPO policies and determine where they will be applied.

**Reference:**

**WWTC Organization Chart**



VP OPR, VP NW USA, VP SW USA, VP NE USA, VP SE USA, VP M USA

Table:-1 Equipment Inventory

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subnet | Offices | Telephone | Devices | Comment |
| VP OPR | VP OPR Office | 2 | 1 | Work Stations |
| CEO IT | 2 | 1 | Work Stations |
| CEO FIN | 2 | 1 | Work Stations |
| CEO HR | 2 | 1 | Work Stations |
| CEO IT’s Staff | 2 | 1 | Work Stations |
| CEO FIN’s Staff | 2 | 1 | Work Stations |
| CEO HR’s Staff | 2 | 1 | Work Stations |
|  |  |  |  |
| VP NW USA, | VP Office | 2 | 2 | Work Stations |
|  | Manager 1 | 2 | 2 | Work Stations |
| Manager 2 | 2 | 2 | Work Stations |
| Broker 1 | 2 | 2 | Work Stations |
| Broker 2 | 2 | 2 | Work Stations |
| Broker 3 | 2 | 2 | Work Stations |
| Broker 4 | 2 | 2 | Work Stations |
| Staff | 2 | 2 | Work Stations |
|  |  |  |  |
| VP SW USA | VP SW Office | 2 | 2 | Work Stations |
|  | Manager 1 | 2 | 2 | Work Stations |
| Manager 2 | 2 | 2 | Work Stations |
| Broker 1 | 2 | 2 | Work Stations |
| Broker 2 | 2 | 2 | Work Stations |
| Broker 3 | 2 | 2 | Work Stations |
| Broker 4 | 2 | 2 | Work Stations |
| Staff | 2 | 2 | Work Stations |
|  |  |  |  |
|  |  |  |  |  |
| VP NE USA | VP NE Office | 2 | 2 | Work Stations |
|  | Manager 1 | 2 | 2 | Work Stations |
| Manager 2 | 2 | 2 | Work Stations |
| Broker 1 | 2 | 2 | Work Stations |
| Broker 2 | 2 | 2 | Work Stations |
| Broker 3 | 2 | 2 | Work Stations |
| Broker 4 | 2 | 2 | Work Stations |
| Staff | 2 | 2 | Work Stations |
|  |  |  |  |
| VP SE USA | VP SE Office | 2 | 2 | Work Stations |
|  | Manager 1 | 2 | 2 | Work Stations |
| Manager 2 | 2 | 2 | Work Stations |
| Broker 1 | 2 | 2 | Work Stations |
| Broker 2 | 2 | 2 | Work Stations |
| Broker 3 | 2 | 2 | Work Stations |
| Broker 4 | 2 | 2 | Work Stations |
| Staff | 2 | 2 | Work Stations |
|  |  |  |  |
|  |  |  |  |
| VP M USA | VP M Offices | 2 | 2 | Work Stations |
|  | Manager 1 | 2 | 2 | Work Stations |
| Manager 2 | 2 | 2 | Work Stations |
| Broker 1 | 2 | 2 | Work Stations |
| Broker 2 | 2 | 2 | Work Stations |
| Broker 3 | 2 | 2 | Work Stations |
| Broker 4 | 2 | 2 | Work Stations |
| Staff | 2 | 2 | Work Stations |
|  |  |  |  |
|  | Printer |  | 20 | At various offices. Exact location to be determined. |
|  | Server |  | 40 | These does not include DNS, DHCP, Domain Controller. Need to be determined by designer |
|  |  |  |  |  |





**Note: WWTC is opening an office only at New York location. Please do not confuse Office holder’s title (VP NW USA) with the location.**

**WLC and AP ordering Guide**

**Table 4.** Ordering Information for Cisco Wireless LAN Controllers

|  |  |  |  |
| --- | --- | --- | --- |
| **Product** | **Features** | **Customer Requirements** | **Part Number** |
| Wireless LAN Controllers | | | |
| Cisco 4400 Series Wireless LAN Controller | • Modular support of 12, 25, 50, or 100 Cisco Aironet access points  • The Cisco 4402 with 2 Gigabit Ethernet ports supports configurations for 12, 25, and 50 access points  • The Cisco 4404 with 4 Gigabit Ethernet ports supports configurations for 100 access points  • IEEE 802.1D Spanning Tree Protocol for higher availability  • IPSec encryption  • Industrial-grade resistance to electromagnetic interferences (EMI) | • For midsize to large deployments  • High availability | • AIR-WLC4402-12-K9  • AIR-WLC4402-25-K9  • AIR-WLC4402-50-K9  • AIR-WLC4404-100-K9  See the [Cisco Wireless LAN Controllers Data Sheet](http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps6307/product_data_sheet0900aecd802570b0_ps6308_Products_Data_Sheet.html) for more information. |
| Cisco 2100 Series Wireless LAN Controller | • Supports up to 6, 12 or 25 Cisco Aironet access points  • Eight Ethernet ports, two of which can provide power directly to Cisco APs  • Desk mountable | • For retail, enterprise branch offices, or SMB deployments | • AIR-WLC2106-K9  • AIR-WLC2112-K9  • AIR-WLC2125-K9  See the [Cisco 2106 Wireless LAN Controller Data Sheet](http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps7206/ps7221/product_data_sheet0900aecd805aaab9.html) for more information. |
| Cisco Catalyst**®** 6500 Series /7600 Series Wireless Services Module (WiSM) | • Wireless LAN Controller for Cisco Catalyst 6500 or Cisco 7600 Series Router  • Supports 300 Cisco Aironet access points  • IPSec encryption  • Industrial-grade resistance to electromagnetic interferences (EMI)  • Intrachassis and interchassis failover  • Interoperable with Cisco Catalyst 6500 Series Firewall and IDS services modules | • Embedded system for the Cisco Catalyst 6500 Series and Cisco 7600 Series Router infrastructure  • For large-scale deployments  • High availability | • WS-SVC-WISM-1-K9  • WS-SVC-WISM-1-K9= (spare)  See the [Cisco Catalyst Wireless Services Module Data Sheet](http://www.cisco.com/en/US/prod/collateral/modules/ps2706/ps6526/product_data_sheet0900aecd80364340.html) for more information. |
| Cisco Catalyst 3750G Integrated WLAN Controller | • Cisco Catalyst 3750G Series Switch with wireless LAN controller capabilities  • Modular support of 25 or 50 Cisco Aironet access points per switch (and up to 200 access points per stack\*)  • IPSec encryption  • Industrial-grade resistance to electromagnetic interferences (EMI) | • For midsize to large deployments  • High availability | • WS-C3750G-24WS-S25  • WS-C3750G-24WS-S50  See the [Cisco Catalyst 3750G Integrated Wireless LAN Controller Data Sheet](http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps7185/ps6915/product_data_sheet0900aecd804b0879.html) for more information. |
| Cisco Wireless LAN Controller Module for Cisco Integrated Services Routers | • Wireless LAN controller integrated into Cisco integrated services routers  • Supports 6, 8, 12, or 25 Cisco Aironet access points | • Embedded system for Cisco 2800/3800 Series and Cisco 3700 Series routers  • For retail, small to medium-sized deployments or branch offices | • NME-AIR-WLC6-K9  • NME-AIR-WLC6-K9= (spare)  • NME-AIR-WLC8-K9  • NME-AIR-WLC8-K9= (spare)  • NME-AIR-WLC12-K9  • NME-AIR-WLC12-K9= (spare)  • NME-AIR-WLC25-K9  • NME-AIR-WLC25-K9= (spare)  See the [Cisco WLAN Controller Modules Data Sheet](http://www.cisco.com/en/US/prod/collateral/modules/ps2797/ps6730/product_data_sheet0900aecd80364432.html) for more information. |

Please refer to the [Cisco Wireless LAN Controller Ordering Guide supplement](http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps6366/data_sheet_c78-501742.html) to learn when to add the following SKUs to track the deployment of voice and context-aware mobility applications.

**Table 2.** Cisco Aironet Indoor Rugged, Indoor, Wireless Mesh, and Outdoor Rugged Access Points

|  |  |  |  |
| --- | --- | --- | --- |
| **Product** | **Features** | **Customer Requirements** | **Part Number** |
| Indoor Rugged Access Points | | | |
| Cisco Aironet 1250 Series | • Industry's first business-class access point based on the IEEE 802.11n draft 2.0 standard  • Provides reliable and predictable WLAN coverage to improve the end-user experience for both existing 802.11a/b/g clients and new 802.11n clients  • Offers combined data rates of up to 600 Mbps to meet the most rigorous bandwidth requirements | • Designed for both office and challenging RF environments  • Especially beneficial for environments with the following characteristics:  • Challenging RF environments (for example, manufacturing plants, warehouses, clinical environments)  • Bandwidth-intensive applications (for example, digital imaging, file transfers, network backup)  • Real-time, latency-sensitive applications such as voice and video  • Need to support existing 802.11a/b/g and new 802.11n wireless clients | Access point platform with pre-installed radio modules:  • AIR-AP1252AG-x-K9: 802.11a/g/n-draft 2.0 2.4/5-GHz Modular Autonomous Access Point; 6 RP-TNC  • AIR-AP1252G-x-K9: 802.11g/n-draft 2.0 2.4-GHz Modular Autonomous Access Point; 3 RP-TNC  • AIR-LAP1252AG-x-K9: 802.11a/g/n-draft 2.0 2.4/5-GHz Modular Unified Access Point; 6 RP-TNC  • AIR-LAP1252G-x-K9: 802.11g/n-draft 2.0 2.4-GHz Modular Unified Access Point; 3 RP-TNC  See the [Cisco Aironet 1250 Series Ordering Guide](http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6973/ps8382/product_data_sheet0900aecd806b7c6d.html) for more information. |
| Cisco Aironet 1240AG Series | • Second-generation 802.11a/g dual-band indoor rugged access point  • 2.4-GHz and 5-GHz antenna connectors for greater range or coverage versatility and more flexible installation options using the broad selection of Cisco antennas available | • Ideal for challenging indoor RF environments  • Recommended for offices and similar environments  • Ideal for deployments above suspended ceilings  • Recommended for outdoors when deployed in a weatherproof NEMA-rated enclosure | • AIR-AP1242AG-x-K9: 802.11a/g Nonmodular Cisco IOS Software- Based Access Point; RP-TNC  • AIR-LAP1242AG-x-K9: 802.11a/g Nonmodular LWAPP Access Point; RP-TNC  See the [Cisco Aironet 1240AG Series 802.11a/b/g Data Sheet](http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6521/product_data_sheet0900aecd8031c844.html) for more information. |
| Indoor Access Points | | | |
| Cisco Aironet 1130AG Series | Low-profile, enterprise-class 802.11a/g access point with integrated antennas for easy deployment in offices and similar RF environments | Ideal for offices and similar environments | • AIR-AP1131AG-\*X-K9  See the [Cisco Aironet 1130AG Series Ordering Guide](http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6087/product_data_sheet0900aecd801b901c.html) for more information. |
| Wireless Mesh Access Points | | | |
| Cisco Aironet 1520 Series | • Next-generation outdoor wireless mesh access point  • Integrated dual band 802.11 a/b/g radios, Ethernet, fiber and cable modem interface  • Provides easy and flexible deployments for outdoor wireless network  • Available in a lightweight version only | • Ideal for outdoors  • Recommended for industrial deployments and local government, public safety, and transit agencies | • AIR-LAP1522AG-X\*-K9:  See the [Cisco Aironet 1520 Series Lightweight Outdoor Mesh Access Point Ordering Guide](http://www.cisco.com/en/US/products/ps8368/products_data_sheet0900aecd8066a157.html) for more information. |
| Cisco Aironet 1500 Series | • Mesh access point that enables cost-effective, scalable deployment of secure outdoor wireless LANs for metropolitan networks or enterprise campuses  • Available in a lightweight version only | • Ideal for outdoors  • Recommended for providing wireless services and applications to local government, public safety, and transit agencies | • AIR-LAP1510AG-\*X-K9:  • Cisco Aironet 1510AG Lightweight Outdoor Mesh Access Point, FCC configuration  See the [Cisco Aironet 1500 Series Ordering Guide](http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps6548/product_data_sheet0900aecd80364a54.html) for more information. |
| Outdoor Rugged Access Points | | | |
| Cisco Aironet 1400 Series | • High-speed, high-performance outdoor bridging solution for line-of-sight applications  • Offers affordable alternative to leased-line services  • Available in a standalone version only | • High-speed building-to-building or campus connectivity  • Share LAN/Internet access between two or more sites  • Fast installation | • AIR-BR1410A-\*X-K9: With integrated antenna  • AIR-BR1410A-A-K9-N: With N-Type connector for use with external antennas  See the [Cisco Aironet 1400 Series Bridge Data Sheet](http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5279/ps5285/product_data_sheet09186a008018495c.html) for more information. |
| Cisco Aironet 1300 Series | Outdoor access point/bridge offers high-speed and cost-effective wireless connectivity between multiple fixed or mobile networks and clients | Ideal for outdoor areas, network connections within a campus area, temporary networks for portable or military operations, or outdoor infrastructure for mobile networks | ● AIR-BR1310G-X-K9: With integrated antenna  ● AIR-BR1310G-X-K9-R: With RP-TNC connector for use with external antennas  ● AIR-BR1310G-A-K9-T: For transportation applications  See the [Cisco Aironet 1300 Series Ordering Guide](http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet09186a008022198b.html) for more information. |

\*X = regulatory domain

(Source: Curtsy Cisco Web site

<http://cisco.com/en/US/prod/collateral/wireless/ps5679/ps6548/prod_brochure0900aecd80565e00_ps2706_Products_Brochure.html>)

**WLC and AP Placement Templates**

Suggested Placement Table Wireless Network

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Building | Access Point  Requirements | Wireless LAN Controller  Requirements | Total AP | Total WLC |
| Building |  | | | |
| Lobby |  |  |  |  |
| Cafeteria |  |  |  |  |
| Conference room |  |  |  |  |
|  |  | | | |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Suggested Product Table (WLC)

|  |  |  |  |
| --- | --- | --- | --- |
| WLC | Cisco Part Number | Quantity | Cost |
| Cisco 2100 Series Wireless LAN Controller | AIR-WLC2106-K9 | 2 |  |
|  |  |  |  |
|  |  |  |  |

Suggested Product Table (AP)

|  |  |  |  |
| --- | --- | --- | --- |
| AP | Cisco Part Number | Quantity | Cost |
| Cisco Aironet 1250 Series | AIR-AP1252AG-x-K9: 802.11a/g/n-draft 2.0 2.4/5-GHz Modular Autonomous Access Point; 6 RP-TNC | 20 |  |
|  |  |  |  |
|  |  |  |  |