**CS - 590 PROJECT**

**REMOTE MANAGEMENT OF SYSTEM**

**BY**

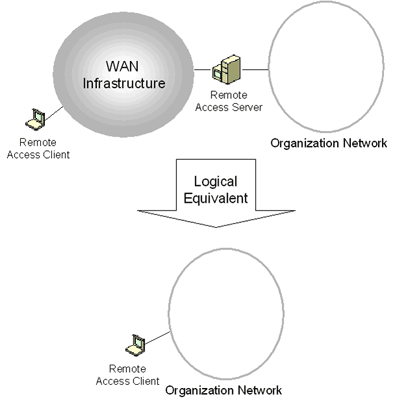
**Alekhya Vanga**

* **INTRODUCTION:**

Remote networking management is a process in which network Administrators have remote control of systems, thereby allows users with remote computers to create a logical connection to an organization network or the Internet. In our case study, which would base on Microsoft and Cisco networks. Microsoft operating system have sets of applications which enables remote access and security features that an administrator should need in his daily routing. We would explain the necessary operating system used in achieving a stable network.

Users run remote access client software and initiate a connection to a remote access server. The remote access server authenticates users and services sessions until terminated by the user or a network administrator. All services typically available to a LAN-connected user (including file and print sharing, Web server access, and messaging) are enabled by means of the remote access connection.

Remote access clients use standard tools to access resources. For example, on a computer running Windows 2000, clients can use Windows Explorer to make drive connections and to connect to printers. Connections are persistent: Users do not need to reconnect to network resources during their remote sessions. Because drive letters and universal naming convention (UNC) names are fully supported by remote access, most commercial and custom applications work without modification.



The above figure means that it is the logical equivalent for a remote access client when connected to a remote access server.

Remote access provides two different types of remote access connectivity:

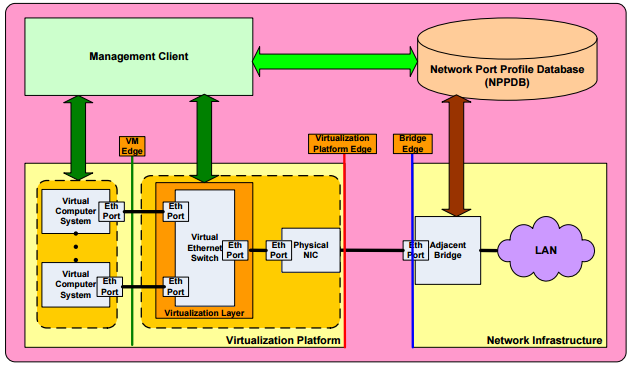
* **DIAL-UP REMOTE ACCESS:**

With dial-up remote access, a remote access client uses the telecommunications infrastructure (typically an analog phone line) to create a temporary physical circuit or a virtual circuit to a port on a remote access server. Once the physical or virtual circuit is created, the rest of the connection parameters can be negotiated.

* **VIRTUAL PRIVATE NETWORK (VPN) REMOTE ACCESS:**

With virtual private network, remote access, a VPN client uses an IP network to create a virtual point-to-point connection with a remote access server acting as the VPN server. Once the virtual point-to-point connection is created, the rest of the connection parameters can be negotiated.

* **COMPONENTS OF REMOTE MANAGEMENT SYSTEM:**



**FIG: REMOTE NETWORKING MANAGEMENT MODEL COMPONENTS**

* From the diagram above we can see how virtual system is used in managing a client system, there various steps which are in place for it to work smoothly.

**1**. Virtualization Platform (virtual computer systems, virtualization layer, and physical NICs)

**2**. Attached Bridge

**3**. Management Client

**4**. Network Port Profile Database (NPPDB)

1. **VIRTUALIZATION PLATFORM:**

The virtualization Platform consists of emulators and hypervisors that emulate whole physical computer machine providing multiple virtual machines on one physical platform. Emulation is the process of virtualizing a computer which is out of network. Virtual computer is an emulation of a computer system based on computer architectures providing functionality of a physical computer with specialized hardware, software, or both. Platform virtualization refers to the creation of a virtual machine that acts like a real computer with an operating system. Software executed on these virtual machines is separated from the underlying hardware resources. Network Interface Controller (NIC) is one of the components in the virtualization platform. Network Interface Controller is a computer hardware component that connects a computer to a computer network. Modern NICs provides advanced features such as interrupt and DMA interfaces to the host processors, support for multiple receive and transmit queues, partitioning into multiple logical interfaces, and on-controller network traffic processing such as the TCP offload engine

1. **ATTACHED BRIDGE:**

Attached Bridge is a direct attachment of the virtual machine's NIC to the given physical interface of the host physical machine. Packets whose destination is on the same host physical machine as where they originate from are directly delivered to the target device. Both origin and destination devices need to be in bridged mode for direct delivery. If either one of them is in Virtual Ethernet Port Aggregator (VEPA)mode, a VEPA capable bridge is required. A VEPA will be collecting every bit of traffic processed from virtual machines on a server and sends it to the external network switch. The external network switch provides some connectivity in between the virtual machines on the same physical server.

1. **MANAGEMENT CLIENT:**

The main purpose of management client is that it delivers distributed endpoint management (mobile, laptop, desktop, and server), helping managers deliver great service to end-users giving minimizing cost, maintaining compliance, and reducing security risks. The other functions include making intelligent decisions like knowing the current state of database. And also pass software audits with ease and manage software and reduce vulnerability and financial risk through endpoint compliance and automated software patching. Automate system provisioning, application deployment, profile configuration from a single console. Seamlessly drive endpoint troubleshooting and management from BMC service management solutions. Must be available on-demand or on premises.

1. **NETWORK PORT PROFILE DATABASE (NPPDB):**

It has a set of networking attributes for virtual machines like MAC address, VLAN and also describes a specific configuration of network infrastructure on which virtual machine gets connected to. It also establishes consistent configuration among the bridges. Network port profile XML schema and OVF are some of the standards that provide an interoperable way of provisioning and deploying networks in virtualized.

* **REMOTE MANAGEMENT SYSTEMS IN CISCO AND MICROSOFT:**

The Cisco and Microsoft companies use almost the same architecture for the Remote Management Network. Below is the information about Cisco and Microsoft remote management systems.

* **CISCO’S APPROACH TO REMOTE MANAGEMENT SYSTEMS:**

CISCO used remote management model by software called Cisco Virtual Office which provided support for quality of service (QoS) for voice and video, and has flexible security options

* **CISCO REMOTE MANAGEMENT SYSTEM:**

CRMS enables organizations helps companies/organizations to target expertise at the point-of-need through immersive Cisco TelePresence, self-service “end-of-the-aisle” kiosks, and consumers directly from their homes. Firms can centralize specialist pools to provide maximum coverage, and still support “carbon neutral” environmental imperatives. With the CRMS can deliver a differentiated and compelling customer experience while reducing revenue leakage and travel expenses.

* **CISCO AGENT DESKTOP:**

Cisco Agent Desktop is computer telephony integration (CTI) solution for IP-based contact centers that allows contact center agents to use powerful tools that help increase agent and supervisor productivity, improve customer satisfaction, and reduce costs. In addition to traditional agent application support, the Premium version of the CAD application supports an integrated browser, which is required for use with Remote Expert Agent Desktop.

* **CISCO REMOTE EXPERT AGENT DESKTOP:**

The Cisco Remote Expert Agent Desktop (READ) is a browser-based application for experts, and it is provided either through CAD application’s integrated browser, or as a gadget in Cisco Finesse. READ allows experts to use powerful tools that help increase the expert’s productivity, improve customer satisfaction, and reduce costs. With READ, experts can:

* Selectively push videos to the customer
* Remotely print at branch site
* Share data (peer-to-peer) in conjunction with Direct Connect application
* Take notes (both private, visible only to the expert, and public, also visible to the customer)
* Access and use IEC connected peripherals such as a printer, scanner, document camera, card reader, and so on.
* **SOLUTION COMPONENTS:**

Cisco also offer solutions such as Interactive Experience Manager and Remote Expert Manager, the IEM is based on the configuration while the REM is based on total control of the system

* **CISCO INTERACTIVE EXPERIENCE MANAGER (IEM):**

The Interactive Experience Manager (IEM) allows configuration, control, and support of Interactive Experience Clients (IEC) 4600 series. Using the IEM, the system administrator can enable peripherals, apply policy on sessions, and generate logs and reports from the IEC.

* **CISCO REMOTE EXPERT MANAGER (REM):**

Remote Expert Manager (REM) is the core control system of the Remote Expert Solution, providing the collaboration features that make customer interactions with the expert simple and effective.REM implements the following administrative, control, and messaging functions:

* **RE ADMINISTRATOR CONSOLE (REAC):**

Web-based management interface to add, verify and update all necessary configurations that are needed for normal operation of REM platform

* **RE AGENT DESKTOP (READ):**

Web-based Expert desktop environment provides CRM, note taking, video streaming, application sharing and printing capabilities between the Expert and the Customer

* **RE INTERACTIVE APPLICATIONS CONTROLLER (REIC):**

Renders graphics, fonts and video on the touch screen located in the customer pod, render desktop applications shared by the expert, relays Customer touch inputs and facilitates customer control of the expert’s shared application.

* **RE SESSION CONTROLLER (RESC)**:

Provides session management to initiate and terminate RE video sessions, data sharing sessions, trigger Customer-side printing and control video streaming

* The REM relies on the following components for its functions:
* Interactive Experience Manager (IEM)
* Interactive Experience Client (IEC)
* Media Server (MS)
* **SECURITY FEATURES:**

Cisco provides security features such as 24x7 Threat Analysis and Management, Log Collection and Event Correlation, High Touch Management and Incident Support, Net flow and Metadata Extraction, Proactive Threat Hunting, Full Packet Capture.

* **MICROSOFT’S APPROACH TO REMOTE MANAGEMENT SYSTEMS:**

Microsoft operating systems have sets of applications which enable remote access and security features that an administrator should need in his daily routing. It’s the implementation of WS-Management Protocol, which was developed to remotely manage any system that protocol. It provides a common way for systems to access and exchange management information across the IT infrastructure. There are software’s in which Microsoft uses for remote management of data from systems remotely or locally, these software’s are scripting objects, the WinRM command-line tool, the Windows Remote Shell command line tool WinRS. If the computer runs a Windows-based operating system version that includes WinRM, the management data is supplied by Windows Management Instrumentation (WMI).

* **MICROSOFT REMOTE MANAGEMENT SYSTEM PROTOCOL:**

The Microsoft Remote Management System Protocol (RMSP) provides remote display and input capabilities over network connections for Windows-based applications running on a server. RMSP is designed to support different types of network topologies and multiple LAN protocols.

* **FEATURES:**

Microsoft RMSP includes the following features and capabilities:

* **ENCRYPTION:**

RMSP uses RSA Security's Rivest Cipher 4 (RC4) cipher, a stream cipher designed to efficiently encrypt small amounts of data. RC4 is designed for secure communications over networks. Administrators can choose to encrypt data by using a 56- or 128-bit key.

* **BANDWIDTH REDUCTION FEATURES:**

RMSP supports various mechanisms to reduce the amount of data transmitted over a network connection. Mechanisms include data compression, persistent caching of bitmaps, and caching of glyphs and fragments in RAM. The persistent bitmap cache can provide a substantial improvement in performance over low-bandwidth connections, especially when running applications that make extensive use of large bitmaps.

* **ROAMING DISCONNECT:**

A user can manually disconnect from a remote desktop session without logging off. The user is automatically reconnected to their disconnected session when he or she logs back onto the system, either from the same device or a different device. When a user's session is unexpectedly terminated by a network or client failure, the user is disconnected but not logged off.

* **CLIPBOARD MAPPING:**

Users can delete, copy, and paste text and graphics between applications running on the local computer and those running in a remote desktop session, and between sessions.

* **PRINT REDIRECTION:**

Applications running within a remote desktop session can print to a printer attached to the client device.

* **VIRTUAL CHANNELS:**

By using RMSP virtual channel architecture, existing applications can be augmented and new applications can be developed to add features that require communications between the client device and an application running in a remote desktop session.

* **REMOTE CONTROL:**

Computer support staff can view and control a remote desktop session. Sharing input and display graphics between two remote desktop sessions gives a support person the ability to diagnose and resolve problems remotely.

* **NETWORK LOAD BALANCING:**

RMSP takes advantage of network load balancing (NLB), where available.

In addition, RMSP contains the following features:

* Support for 24-bit colour.
* Improved performance over low-speed dial-up connections through reduced bandwidth.
* Smart Card authentication through Remote Desktop Services.
* Keyboard hooking. The ability to direct, special Windows key combinations, in full-screen mode, to the local computer or to a remote computer.
* Sound, drive, port, and network printer redirection. Sounds that occur on the remote computer can be heard on the client computer running the RDC client, and local client drives will be visible to the remote desktop session.
* **SECURITY FEATURES:**

Microsoft has security features such as Authentication and authorization, Secure user authentication, Extensible Authentication Protocol, Data encryption, Caller ID, Remote access account lockout, Remote access policy profile packet filtering, Packet filtering for VPN remote access.

* **PROBLEM STATEMENT:**

Due to the changes and advancement in modern day technology, remote network management are no longer made up of only routers and switches and firewalls alone. Technologies such as WAN optimization voice/video over IP, WLAN Application based policy control have all become an important to network element which oversees the effectiveness on Remote Network Management. Microsoft and Cisco offer various software and hardware tool to enable the effectiveness of an administrator. Some of the challenges are: Complexity, Cost, Resourcing, Reliability and others.

* **COMPLEXITY:** Disparate network elements from multiple vendors need to be managed, along with secure policies, application performance and service levels.
* **COST:** Networking and communications costs are a perennial concern for organisations and one of the most important factors in implementing new services.
* **RESOURCING:** technical expertise could be better used to progress business projects, rather than manage network monitoring and availability issues.
* **RELIABILITY:** Critical business applications and processes are impacted by unpredictable network availability.
* Lack of common configuration information that may be referenced by the virtualization ecosystem management entities.
* Disparity between the capabilities of embedded bridges in the virtualization hosts and the capabilities of bridges in the attached network.
* **CONCLUSION:-**
* We have discussed about:
* Introduction
* Components for efficient functioning of Remote Management
* Security Features of Microsoft and Cisco Remote Management
* Problems
* Challenges
* Solutions
* **REFERENCES:-**
* <http://www-01.ibm.com/common/ssi/rep_ca/5/616/ENUSA313-035/IBM_Network_Managed_Services_-_Untangling_the_Complexity.pdf>
* <https://technet.microsoft.com/en-us/library/cc754263(v=ws.11).aspx>
* <https://msdn.microsoft.com/en-us/library/bb742490.aspx>
* <https://msdn.microsoft.com/en-us/library/aa384426(v=vs.85).aspx>