Lucent Technologies
Bell Labs Innovations

VitalQIP Integration with Windows 2000

White Paper
Document ID # WP07991-0902

Abstract

VitalQIP provides support for the Microsoft® Windows® 2000 Server network operating system in various ways including the porting of the VitalQIP system to Microsoft Windows 2000, and the management of Microsoft Windows 2000 DHCP and DNS servers. In addition, integration to Active Directory also occurs at various points. This white paper will outline the operation of VitalQIP within a Microsoft Windows 2000 environment, as well as detail the integration that exists between VitalQIP and the Microsoft Windows 2000 components.

Note: This documentation outlines an integration and implementation strategy and plans for software that is currently under development. It is meant to accompany software that is still in development. Some of the information in this documentation may be inaccurate or may not be an accurate representation of the functionality of the final retail product. Some of the information in this documentation may be inaccurate or may not be an accurate representation of the functionality of the final retail Lucent products. Lucent assumes no responsibility for any damages that might occur either directly or indirectly from these inaccuracies.

© 1999 Lucent Technologies. All rights reserved.

The information contained in this document represents the current view of Lucent Technologies with respect to the technology being discussed as of the date of this publication. Because Lucent Technologies must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Lucent Technologies, and Lucent cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. LUCENT TECHNOLOGIES MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft, Windows, Windows NT, Windows 2000, Windows 95, and Windows 98 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Netscape is a registered trademark of Netscape Communications Corporation.

Novell is a registered trademark of Novell, Inc.

Oracle is a registered trademark of Oracle Corporation.

Sybase is a registered trademark of Sybase, Inc.

UNIX is a registered trademark of the Open Group.

Other products or company names mentioned herein may be the trademarks of their respective owners.

Lucent Technologies • 400 Lapp Road• Malvern, PA 19355 • USA

September 27, 2002

CONTENTS

INTRODUCTION 1

A PORT OF VITALQIP TO THE MICROSOFT® WINDOWS® 2000 OPERATING SYSTEM 2

VitalQIP Enterprise Server running Sybase or Oracle 2
VitalQIP Remote Servers 2
VitalQIP Administrative Client 2
VitalQIP Web Client 2

VITALQIP AND WINDOWS 2000 DHCP INTEGRATION 3

Ability for VitalQIP to create Microsoft DHCP Server configuration 3
Ability for DHCP Active Lease information to be displayed within VitalQIP 3
Ability for DHCP binding changes to be captured and sent to VitalQIP and DNS 3
New features of Windows 2000 DHCP Servers 3
Integration of DHCP and DNS – Option 81 3
Enhanced Monitoring and Statistical Reporting for DHCP Servers 5
New Vendor-specific Options and Vendor Class Support 5
User Class Support 6
Multicast Address Allocation 6
Unauthorized DHCP Server Detection 7
Protecting Against Unauthorized DHCP Servers 7
Protecting Against Improper Use of Workgroup DHCP Servers 8

VITALQIP AND WINDOWS 2000 DNS INTEGRATION 9

New features of Windows 2000 DNS Servers 9
Integration of DHCP and DNS 9
Support for the Service Locator record type 9
Active Directory Integration 10
Secure DNS Support 11
Multi-master DNS Support 11

VITALQIP SUPPORT OF SITES AND SUBNETS 13

SUMMARY 14

For More Information 14
Reference Material 14
Additional Reading 14

INTRODUCTION

The Microsoft Windows 2000 Server network operating system has made the move from WINS to DNS as the primary naming service on the network. This reliance on DNS has opened up new opportunities for VitalQIP to assist in management of the name and address space in a Windows 2000 environment. In addition to the new role DNS plays, Windows 2000 has added a number of new DNS and DHCP features as well as new services such as Active Directory that VitalQIP can leverage in its management of the IP space. In this paper, we will discuss the integration points between VitalQIP and Windows 2000, the new features VitalQIP has implemented to assist in this integration, and the plans for future enhancements to VitalQIP that affect this integration.

The areas of integration between VitalQIP and Windows 2000 include the following:

- A port of the current VitalQIP system to the Windows 2000 operating system
- Ability for VitalQIP to manage Windows 2000 DHCP servers including authorization in Active Directory
- New DHCP Options – Vendor class, user class, option 81
- Multicast address allocation
- Windows 2000 DHCP client support
- Ability for VitalQIP to manage Windows 2000 DNS servers including Active Directory integrated DNS zones
- Ability for VitalQIP to support SRV resource records
- Flexible Dynamic DNS Update Support
- Secure DNS support
- Multi-master DNS support
- VitalQIP's management of sites and subnets

These features, together with the robust functionality inherited from previous versions of Lucent's VitalQIP system, make it a compelling solution to the networking needs of corporations today. In addition, VitalQIP provides an invaluable tool to help network administrators migrate to the Windows 2000 operating system, or utilize components of the Windows 2000 operating system, within their existing DHCP and DNS deployments.

A PORT OF VITALQIP TO THE MICROSOFT® WINDOWS® 2000 OPERATING SYSTEM

VitalQIP has been ported to the Microsoft Windows 2000 operating system and is treated as a standard VitalQIP supported platform. This includes the ability to have some, or all of the components of VitalQIP running on the Microsoft Windows 2000 operating system including:

- VitalQIP Enterprise Server running Sybase or Oracle
- VitalQIP Remote Servers including:
  - Lucent DHCP Server
  - Lucent DNS Server
- VitalQIP Administrative Client
- VitalQIP Web Client

VitalQIP Enterprise Server running Sybase or Oracle

The VitalQIP Enterprise server is capable of being hosted on the Microsoft Windows 2000 operating system. This includes support for Sybase, Oracle, and all corresponding VitalQIP Enterprise Server services.

VitalQIP Remote Servers

The VitalQIP Remote server is capable of being hosted on the Microsoft Windows 2000 operating system. This includes support for the Lucent DHCP Server, Lucent DNS Server, and all corresponding VitalQIP Remote services. The services operate in the same manner and configuration that is available today on the Windows NT 4.0 operating system.

VitalQIP Administrative Client

The VitalQIP Administrative Client is capable of being hosted on the Microsoft Windows 2000 operating system. This includes full support for all administrative functions that are available today with the Microsoft 95/98/NT VitalQIP Administrative Client.

VitalQIP Web Client

The VitalQIP Web Client will be capable of being hosted on the Microsoft Windows 2000 operating system. This includes full support for all administrative functions that are available today with the VitalQIP Web Client. The Microsoft Internet Information HTTP Web server that ships with Microsoft Windows 2000 is fully supported.

VITALQIP AND WINDOWS 2000 DHCP INTEGRATION

VitalQIP supports the ability to centrally manage Microsoft DHCP servers running under Microsoft NT 4.0 and 2000.

Ability for VitalQIP to create Microsoft DHCP Server configuration

In 5.2 and above, VitalQIP has the ability to create Microsoft Windows 2000 DHCP Server configuration information, providing an alternative management console that can be used enterprise wide for DHCP configuration. Dynamic objects can be defined within VitalQIP and then "pushed" to the remote Microsoft® Windows® 2000 DHCP Server using the standard Network Services – DHCP Generation menu option. The update to the Windows 2000 DHCP server is accomplished using supplied command line utilities from Microsoft.

Ability for DHCP Active Lease information to be displayed within VitalQIP

VitalQIP has the ability to display all active lease information from Microsoft Windows 2000 DHCP Servers using supplied command line utilities from Microsoft.

Ability for DHCP binding changes to be captured and sent to VitalQIP and DNS

VitalQIP has the ability to capture DHCP binding changes (events such as DHCP Grants, or Renews) that occur with the Microsoft Windows 2000 DHCP Server. The VitalQIP MS DHCP Monitor service captures the events, and sends them to the VitalQIP message transport system, where they are reliably delivered to the VitalQIP Enterprise Server. Additionally, the VitalQIP DNS Update Service (via the Message Service) can be configured to forward the updates to all DNS servers that are either primary or secondary for the DHCP client's domain. This capability includes the name collision management feature of the first-in/last-in policy provided in VitalQIP.

New features of Windows 2000 DHCP Servers

In order to completely understand the interface between the Microsoft Windows 2000 DHCP service and VitalQIP, it is important to understand the new features that Microsoft offers with this version of the server. New features include:

- Integration of DHCP and DNS – Option 81
- Enhanced monitoring and statistical reporting for DHCP servers
- New DHCP vendor-specific and class ID option support
- Multicast address allocation
- Rogue DHCP Server detection

Integration of DHCP and DNS – Option 81

Microsoft has enhanced the Windows 2000 DHCP Server to include the capability to perform Dynamic DNS (DDNS) via the IETF RFC2136 protocol. For older Microsoft DHCP clients such as Windows 95/98, and NT 4.0, the DHCP server will send both the A and the PTR records to DNS, acting as a proxy for the client, for the purpose of DDNS registration. This is similar to the current operation of VitalQIP. For newer DHCP clients such as Windows 2000 DHCP clients, the

DHCP client by default will send an A record update to DNS, and request that the DHCP server perform the PTR record update. This option is configured via the DHCP client GUI.

The specifications of the proposed implementation of DHCP-DNS interaction are described in RFC draft documents (http://www.ietf.org/internet-drafts/draft-ietf-dhc-fqdn-option-01.txt , http://www.ietf.org/internet-drafts/draft-ietf-dhc-ddns-resolution-01.txt). These IETF drafts specify how a DHCP server may register and update pointer (PTR) and address (A) resource records on behalf of its DHCP-enabled clients. It also specifies how to assign an additional DHCP option code (option code 81) that enables the return of a client's fully qualified domain name (FQDN) to the DHCP server. If implemented, this option is then interpreted by the DHCP server, which can then initiate further interaction and updating by using dynamic DNS (DDNS) to modify an individual host's resource records with a dynamic DNS server. [1] Microsoft has implemented an earlier incarnation of these drafts before they were split into two separate documents (draft-ietf-dhc-dhcp-dns-08.txt)

The DHCP server can differentiate between Windows 2000 Professional and other clients. This DHCP option permits the DHCP server the following possible interactions for processing DNS information on behalf of DHCP clients:

- The DHCP server always registers the DHCP client for both the forward (A-type records) and reverse lookups (PTR-type records) with DNS. [1]
- The DHCP server never registers the name-to-address (A-type records) for DHCP clients. [1]
- The DHCP server registers the DHCP client for both forward (A-type records) and reverse lookups (PTR-type records) only when requested to by the client. [1]

Note that the DHCP client must support option 81, and be able to pass the option to the DHCP server. Currently, the Windows 2000 DHCP client is the only DHCP client that supports this option. Older DHCP clients such as Windows 95/98/NT do not support this option. Option 81 is configured on the Windows 2000 DHCP client, as well as can be enabled/disabled by the DHCP server. [1]

VitalQIP can create the policy that governs how the Microsoft DHCP Server supports the option to perform Dynamic DNS updates. The Microsoft DHCP Server can be configured to honor, or not honor the requested Dynamic DNS update options that are sent from the DHCP client via option 81. This functionality is first supported in the VitalQIP 5.2 release. In the Windows 2000 DHCP server profile in VitalQIP, use the additional policies section to enter the "netsh dhcp set dnsconfig [*flags*]" command to modify the option 81 setting of the DHCP server. See the Microsoft documentation for information on the netsh command settings.

The Lucent DHCP server has also been modified to honor option 81. Lucent DHCP now fully supports this option. Option 81 can be configured in VitalQIP in the Lucent DHCP server profile by using the Option81Support policy setting. A setting of 'suppress' causes the server to ignore the client FQDN option 81 packet, and

update VitalQIP/DNS with the hostname in option 12 of the client's request and the domain name configured for the scope from which the server issued a lease. A setting of 'client' will cause the server to honor the client FQDN option 81, meaning that if instructed by the client, the server will update only the client's PTR record in DNS (via Message Service or Update Service), using the FQDN contained in option 81. A setting of 'server' will cause the server to perform both the A and PTR record updates, using the FQDN contained in option 81. If the server is configured to accept option 81 from the client, the domain name information can be passed into VitalQIP and only accepted if it is listed as one of the valid domain names for the subnet on which the client is trying to get a lease. This check for a valid domain name in VitalQIP can also be set to predate the name being entered into DNS. This way the DNS update will be dependant upon the domain the client has picked being an acceptable name according to VitalQIP.

Enhanced Monitoring and Statistical Reporting for DHCP Servers

Enhanced monitoring and statistical reporting has been added to the DHCP server for Windows 2000 via SNMP. SNMP traps can be generated when IP addresses are running below a user-defined threshold. For example, an alert could be triggered when 90 percent of IP addresses assigned for a particular scope have been assigned. A second alert can be triggered when the pool of IP addresses is exhausted. To alert network managers, the icon is changed to yellow on the remaining addresses falling below the defined level. The icon is changed to red if the addresses are completely depleted. [1]

The DHCP manager, which supports Simple Network Management Protocol (SNMP) and Management Information Bases (MIBs), provides graphical display of statistical data. This helps administrators monitor system status, such as the number of available versus depleted addresses, or the number of leases being processed per second. Additional statistical information includes the number of messages and offers processed, as well as the number of requests, acknowledgements, declines, negative status acknowledgment messages (Nacks), and releases received. [1]

Also viewable are the total number of scopes and addresses on the server, the number used, and the number available. These statistics can be provided for a particular scope, or at the server level, which shows the aggregate of all scopes managed by that server. [1]

VitalQIP provides management and reporting information of network services via the "Services Manager" add-on product, which will be enhanced to provide support for the Windows 2000 DHCP Server. Note that custom "Services Manager Displays" will need to be developed that will display the information that is available from the DHCP server. The data this is currently provided from the Microsoft DHCP Server is a subset of the data that is provided by the Lucent DHCP Server.

New Vendor-specific Options and Vendor Class Support

The DHCP server for Windows 2000 now provides support for the vendor-specific

options 43 and 60 defined in RFC2132. It allows for vendor-specific options to be defined, as an alternative to the potentially lengthy process of obtaining IETF approval for a new standard option. These vendor options are defined by specific vendors, and are triggered by data bits that determine whether a given option class is standard or vendor-specific. Once identified as vendor-specific, DHCP looks up the configuration as specified for the specific vendor. The vendor class and vendor options are described in RFC 2132.

VitalQIP and Lucent DHCP currently support the vendor specific and class id options 43 and 60 defined by RFC2132.

User Class Support

Microsoft has added the capability for DHCP clients to differentiate themselves to the DHCP server via a user class option 77. This allows for pools of dynamic addresses to be configured with specific options, and assigned a specific user class. [1]

User classes allow DHCP clients to differentiate themselves by specifying what type of client they are, such as a desktop or laptop, for example. An administrator can then configure the DHCP server to assign different options, depending on the type of client receiving them. For example, shorter leases could be assigned to laptop clients. Desktop clients on the same network may require special settings, such as computer-aided design (CAD) platforms. These variations could include lease length, WINS and DNS settings, and all others allowed by DHCP options. This feature gives administrators greater flexibility in configuring clients. If client class options are unused, default settings are assigned. [1]

User class(es) are defined on the DHCP server, and attached to specific set of DHCP options. A single user class is defined on the DHCP client, using the ipconfig utility supplied with Windows 2000. [1]

Older DHCP clients such as Microsoft 95/98/Ntclients, do not support this option. [1]

VitalQIP provides the capability to define User Classes within the VitalQIP administrative user interface. The Lucent DHCP Server fully supports the User Class option 77.

Multicast Address Allocation

The Microsoft DHCP server has been extended to allow the assignment of multicast addresses, in addition to unicast addresses. The multicast address range is from 224.0.0.0 to 239.255.255.255. A proposed IETF standard defines multicast address allocation. The proposed standard benefits network administrators by allowing multicast addresses to be assigned in the same fashion as unicast addresses, allowing complete utilization of the existing infrastructure. [1]

Typical applications for multicast are conferencing or audio, which usually require users to specially configure multicast addresses. Unlike IP broadcasts, which must be readable by all computers on the network, a multicast address is a group of computers, using the concept of a group membership to identify those to whom the

message is to be sent. [1]

The multicast address allocation feature has two parts. The server side implementation to hand out multicast addresses and the client side APIs that applications can use to request, renew, and release multicast addresses. To use this feature, the administrator first configures the multicast scopes and the corresponding multicast IP ranges on the server. The multicast addresses are then managed like normal IP addresses. The client can call the APIs to request a multicast address from a scope. The underlying implementation uses DHCP protocol–style packet formats between client and the server. [1]

VitalQIP 5.2 and above supports defining multicast scopes in the address range from 224.0.0.0 to 239.255.255.255. You can then assign the appropriate multicast options such as scope life, lease duration, and multicast TTL (number of router hops) to the scope and assign the multicast scope to a Windows 2000 DHCP server. When you generate the configuration for the server, VitalQIP recognizes this special address space, and will generate the multicast information in order to configure the server to hand out multicast addresses.

Unauthorized DHCP Server Detection

The Microsoft DHCP Server for Windows 2000 is designed to prevent unauthorized DHCP servers from creating address assignment conflicts. This solves problems that could otherwise occur if naïve users created unauthorized DHCP servers that could assign improper or unintended IP addresses to clients elsewhere on the network. For example, a user could create what was intended to be a local DHCP server, using non-unique Net 10 addresses that could lease the addresses to unintended clients requesting addresses from elsewhere on the network. [1]

This is one reason to keep the number of DHCP servers deployed at a minimum, as described in Best Practices, below. However, most of these events are accidental, where a second DHCP server is installed by someone who is unaware of other DHCP servers already active on the network. [1]

The DHCP server for Windows 2000 has management features to prevent unauthorized deployments and to detect existing unauthorized DHCP servers. In the past, anyone could bring up a DHCP server on a network. Today, an authorization step is required. These authorized personnel are usually the administrator of the domain that the Windows 2000 Server platform belongs to or someone to whom they have delegated the task of managing the DHCP servers. [1]

Protecting Against Unauthorized DHCP Servers

Active Directory is now used to store records of authorized DHCP servers. When a DHCP server comes up, the directory can now be used to verify the status of that server. If that server is unauthorized, no response is returned to DHCP requests. The domain administrator can assign access to the DHCP folder holding configuration data, to allow only authorized personnel to add DHCP servers to the approved list. [1]

In VitalQIP, the Active Directory server can be specified in VitalQIP's Windows 2000 DHCP server profile. With this information, when VitalQIP generates the configuration for a Windows 2000 DHCP server it will connect to Active directory and authorize the DHCP server.

Protecting Against Improper Use of Workgroup DHCP Servers

When a DHCP server that is not a member server of the domain (such as a member of a workgroup) comes up, the following happens: The server broadcasts a DHCPINFORM message on the network. Any other server that receives this message responds with DHCPACK message and provides the name of the directory domain it is part of. If a workgroup DHCP server detects another member DHCP server of a domain on the network, the workgroup DHCP server assumes that it is unauthorized on that network and does not service requests. If the workgroup DHCP server detects the presence of another workgroup server, it ignores it; this means that there can be multiple workgroup servers active at the same time, as long as there is no directory service. [1]

Even when a workgroup server comes up and finds itself allowed to run (because no other domain member server or workgroup server is on the network), it continues to probe DHCPINFORM every five minutes. If an authorized domain member DHCP server comes up later, the workgroup server becomes unauthorized and stops servicing. [1]

If no Active Directory server is specified in VitalQIP's Windows 2000 DHCP server profile, VitalQIP will not attempt to authorize the DHCP server. Thus workgroup servers can be configured through the VitalQIP GUI as well.

When VitalQIP is used to manage Microsoft Windows 2000 DHCP servers, VitalQIP becomes "authoritative" for the addressing and the Windows 2000 "DHCP Manager" is not required. VitalQIP replaces the need to use the Windows 2000 "DHCP Manager".

VITALQIP AND WINDOWS 2000 DNS INTEGRATION

VitalQIP currently supports the ability to centrally manage Microsoft DNS servers running under Microsoft Windows NT and 2000.

New features of Windows 2000 DNS Servers

In order to completely understand the interface between the Microsoft Windows 2000 DNS Server and VitalQIP, it is important to understand the new features that Microsoft offers with this version of the DNS server. New features include:

- Integration of DHCP and DNS
- Support for SRV resource records (RFC2052)
- Active Directory Integration
- Secure DNS support
- Multi-master DNS support

Integration of DHCP and DNS

Microsoft has enhanced the Windows 2000 DHCP Server to include the capability to perform Dynamic DNS (DDNS) via the IETF RFC2136 protocol. In addition, the Windows 2000 DHCP clients can optionally send dynamic updates to DNS directly. Dynamic updates either from the Windows 2000 DHCP Server or the Windows 2000 DHCP clients follow the IETF RFC2136 protocol that has been defined. See the Option 81 section for more information about configuring DHCP to interact with DNS.

Support for the Service Locator record type

Because each Windows Domain now has a corresponding DNS domain representation, DNS is used to locate the Active Directory Servers. Windows 2000 requires a DNS server that supports the service locator record type RFC2052 (SRV Records). SRV records let a server advertise a service to the network. Microsoft is using SRV records to advertise a number of services including the following:

- Advertisement of Domain Controllers
- Advertisement of the Global Catalog
- Advertisement of special services such as Kerberos and Active Directory

By default, domain controllers will try to dynamically update these resource records in DNS via the protocol described in RFC2136. The domain controllers also create a file called netlogon.dns that contains all of the service related resource records that they wish to add to DNS.

VitalQIP supports the dynamic creation of SRV records to be placed into a zone as described below.

If an administrator wants to support the dynamic creation of the SRV records by the Domain Controllers, the DNS server can be configured to accept dynamic updates from the domain controllers. Since the domain controllers directly update DNS

without informing VitalQIP, the External Dynamic Update Propagation feature must be employed. This feature has the ability to track and capture dynamic changes to DNS and store this information in QIP. There are two models that can be used to get dynamic updates from external sources into QIP.

The first is the polling model. The polling model depends on the periodic execution of the qip-syncexternal CLI. This CLI will capture a DNS server's current zone information and update the VitalQIP database with any new or changed resource records. The polling model is restricted to capturing resource records that may have been added to DNS by a Windows operating system. This model may be used with all VitalQIP managed DNS servers that support the AXFR DNS protocol such as any BIND 8.x or 9.x based, or Windows 2000 DNS server. Prior to VitalQIP release 6.0, the qip-syncexternal CLI was named the qip-miniddma CLI.

The second model is the continuous model. In the continuous model, VitalQIP is continuously being updated with external DNS information. The continuous model is not restricted to capturing resource records from Windows 2000 sources. Currently, only the Lucent DNS Service (version 3.1 or above) supports the continuous model. With the continuous model, the Lucent DNS server can be configured to forward dynamic updates to VitalQIP and to all other DNS servers authoritative for the zone that are managed by VitalQIP. The Lucent DNS server can be configured to propagate these dynamic updates based upon which zone the update belongs to and what record type the update is affecting (A, CNAME, PTR, or SRV). The continuous model is available in VitalQIP 6.0 and above.

It is recommended that customers have the DHCP remote server forward the new binding information to VitalQIP when a DHCP lease is given out. Once those updates have been authorized by VitalQIP (to make sure that the DHCP client is not trying to overwrite a static server's name), then the update is forwarded to DNS. Static addresses will be managed from the VitalQIP GUI and entered into DNS through the normal VitalQIP mechanisms.

If administrators do not wish to turn on dynamic update in their environment, they can use they netlogon.dns file created by the domain controller and manually enter the needed resource records in VitalQIP.

Active Directory Integration

The Microsoft 2000 DNS Server has been modified to optionally store zone information in the Active Directory. The server can run in three modes of operation, either disk based, registry based, or directory based. Running in a directory based mode of operation provides the capability for multiple DNS servers to share zone files, thus eliminating the need for zone transfers to take place, and eliminating the concept of a DNS server being Primary vs. Secondary for a zone. All DNS servers become primary for a specific zone that is located in the Active Directory. The Active Directory replication facility will replicate this data to other Active Directory Servers that are in the network.

VitalQIP 5.2 and above can create Microsoft Windows 2000 DNS Server

configuration information, providing an alternative management console that can be used enterprise wide for DNS configuration. Objects can be defined within VitalQIP and then “pushed” to the remote Microsoft Windows 2000 DNS Server using the standard QIP Network Services – DNS Generation menu option. VitalQIP can generate traditional boot and zone file configuration files for a Windows 2000 DNS server as well as directory integrated zone information. The VitalQIP DNS generation logic utilizes the dnscmd tool provided in the support tools package on the Windows 2000 installation disk to generate the configuration information. You must have the support tools installed for VitalQIP’s management of Windows 2000 DNS servers to function.

VitalQIP currently cannot generate configuration information for secure DNS zones on a Windows 2000 DNS server. This functionality is planned to be supported in a future release.

Secure DNS Support

The Windows 2000 DNS server has implemented secure dynamic updates. The algorithm used to negotiate these updates is based on the Internet Draft “GSS Algorithm for TSIG (GSS-TSIG)”. This algorithm is based on the Generic Security Service Application Program Interface (GSS-API) specified in RFC 2078 that provides security services independently of the security mechanism. It is planned, in a future release, for VitalQIP to be able to manage a Windows 2000 DNS server hosting secure zones.

With VitalQIP 6.0, Lucent DNS servers have implemented the GSS-TSIG security mechanism for dynamic update. They are able to respond to any Windows 2000 DNS clients attempting to make a secure update. The Lucent DNS server is compatible with the Windows 2000 DNS clients. Thus, Lucent DNS servers are able to accept secure dynamic updates coming from Windows 2000 machines including Windows 2000 clients and domain controllers.

Multi-master DNS Support

The Microsoft 2000 DNS Server has been modified to optionally store zone information in the Active Directory. Running in a directory based mode of operation provides the capability for multiple DNS servers to share zone information in the directory, thus eliminating the need for zone transfers to take place and eliminating the concept of a DNS server being Primary vs. Secondary for a zone. All DNS servers become primary for a specific zone that is located in the Active Directory. The Active Directory replication facility will replicate this data to other Active Directory Servers that are in the network.

Windows 2000 DNS servers that are Active Directory integrated can be managed from VitalQIP. In a multi-master environment, the qip-syncexternal CLI should be run against only one of the DNS servers in order to keep a consistent view of changing data. All changes to DNS information will be replicated via Active Directory to all AD integrated masters for that zone, so running qip-syncexternal against only one of these servers is sufficient for retrieving changes made on any of

the masters.

With the continuous model of propagation of dynamic external updates, multiple Lucent DNS servers can be specified as masters for a zone. All master servers will be able to accept dynamic updates. When a domain controller updates its SRV information, it will update one of the master servers. That Lucent DNS server will then immediately forward the update information to VitalQIP and all other authoritative servers. The qip-syncexternal CLI will not need to be run in this environment since the updates are automatically forwarded to VitalQIP.

VITALQIP SUPPORT OF SITES AND SUBNETS

Windows 2000 stores information about the physical infrastructure of the network in Active Directory. Active Directory contains information about the subnets in your network as well as how well connected they are. This connection information is stored as sites. Sites are considered to be sets of well-connected subnets. VitalQIP manages much of this same information. The VitalQIP management interface has been modified to allow for synchronizing of this information with Windows 2000.

VitalQIP currently manages information about subnets and subnet organizations. The subnet organizations can be used to model Windows 2000 sites. That is, they can be used to depict a set of well-connected subnets. Since VitalQIP already manages this information, we would like to avoid the tedious and error prone task of having the user reenter that information into the Windows 2000 management console. Thus, VitalQIP provides a mechanism for having the subnet and subnet organization information exported from VitalQIP and imported into Windows 2000 Active Directory as subnets and sites. Site link information will not be created as that information is not managed by VitalQIP. A utility to have this information exported from Active Directory and imported into VitalQIP is also provided.

SUMMARY

The support for Windows 2000 outlined in this white paper by the VitalQIP product line builds on a long history of support for flexible, scalable, and manageable, network management tools. These features allow network administrators to deploy robust, high-performance, scalable, and easily configurable networks. In addition, VitalQIP provides network administrators with deployment options, by adhering to open standards, and providing product support across many different operating system platforms.

VitalQIP partnered with the Windows 2000 operating system provides yet another tool that the network administrators can use to deploy mission critical network services across the enterprise.

For More Information

For the latest information on VitalQIP, visit our Web site at:
http://www.qip.lucent.com

For more information regarding DHCP, visit the dhcp.org web site at:
http://www.dhcp.org

Reference Material

[1] Microsoft, “Dynamic Host Configuration Protocol for Windows 2000”, White Paper, March 1999

Additional Reading

P. Vixie, S. Thomson, Y. Rekhter, and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE) ", RFC2136, April 1997.

Yakov Rekhter and Mark Stapp, “Interaction between DHCP and DNS“, Internet Draft draft-ietf-dhc-dhcp-dns-10, June 1999.

Microsoft, “Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services”, White Paper, July 1997

Microsoft, “Planning Microsoft Windows NT Server 4.0 Deployment with Microsoft Windows 2000 Server in Mind”, White Paper, January 1998

Microsoft, “Migrating from Microsoft Windows NT Server 4.0 to Windows NT Server 5.0”, White Paper, September 1997

Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC2132, March 1997.