Lucent Technologies
Bell Labs Innovations

QIP® Integration with Microsoft® Windows® 2000

Frequently Asked Questions

Q: Does Active Directory provide the same functionality as QIP?

A: Active Directory does not provide the same functionality as QIP. QIP is an IP Management tool, not a directory service. QIP provides the ability to:

- Manage your IP Address space holistically
- Manage networks centrally or in a distributed fashion
- Manage subnets and IP addresses
- Manage DNS servers and DHCP servers from a central location, regardless of the vendor or platform.
- Provide reporting and auditing capability
- Manage at a very granular level, administrators and their capabilities
- Define policies to ensure consistency throughout your network
- Operate in a mixed platform environment
- Give error checking to ensure networks and servers are properly defined and overlapping scopes are not present

Active Directory was never designed to be an IP Management tool. Rather, it is a directory server that provides data storage.

Q: Why use QIP with Windows 2000?

A: It is quite important to have a holistic view of the networks, subnets, domains, and the IP object space. Windows 2000 offers only the view of individual servers in your environment. With QIP you have a central place to manage your whole IP space for your entire network, not just one server. Windows 2000 allows you to configure a server. QIP allows you to manage your network. QIP is more than just DNS and DHCP. QIP is a tool to manage your entire IP infrastructure. It handles inventory and contact information, networks, subnets, OSPF areas, scheduled IP network changes, IP address reclaim utilities, and more.

Q: Windows 2000 clients can dynamically update their own DNS information, but if I open my Lucent DNS server up to let anyone update the zone, how do I keep my DNS secure? Won't I be risking a malicious client clobbering the DNS name of my important servers?

A: The way QIP has been handling dynamic DNS updates for DHCP clients in the past is still valid in a Windows 2000 environment. One way of handling this is to configure the system as follows. The DNS servers would be configured to only allow dynamic updates from the enterprise server. The QIP services would then be configured such that, when the DHCP server gives out a lease, it passes the lease information to the update service on the enterprise server. The update service then checks the QIP database to see if that name belongs to a static client or another dynamic client. If conflicts occur, there are polices that can be set to configure different ways for the system to resolve the conflicts. Using this scheme you keep your DNS space secure since every client update gets validated with the QIP database before updating DNS and only the enterprise server has the ability to make those updates.

Q: What about SRV records? How do we get them into QIP since they are dynamically generated from domain controllers? We don't want to register SRVs by hand, that would be far too much work.

A: Understandable. We don't expect you to actually enter the SRV records into QIP. We would expect that you would define the domain controllers as static objects in QIP and manage them as you would any other IP resource in your network. You would need to define an ACL for the DNS server that allows the domain controllers generating the SRV records to update that zone. The SRV records will be automatically be updated within QIP when they are obtained from the DNS server via the Dynamic DNS Monitor Agent (DDMA). This service can be run manually, or can be scheduled, to point to a DNS server and/or zone and get any dynamically added SRV records.

Q: What about securing the SRV records that are entered into DNS? What is to stop another device from overwriting an SRV record that already exists (it's registered dynamically earlier)? This would cause big problems for a Windows 2000 domain controller. Another case could be a bogus SRV record; a machine says (illegally) that it is a domain controller but it isn't.

A: If you are using the approach described in the previous question, both of these situations are secure. For the first case, this would be controlled using the access control list (ACL) which is defined for the server/zone and specifies which hosts are allowed to send dynamic updates to the server for that zone. In this case, the known domain controllers would be specified in an ACL along with the QIP Enterprise server, thus defining the hosts that are allowed to send dynamic DNS updates. A rogue server would not have access to overwrite SRV records. Only the servers that you have specified as legal servers for that domain in the ACL could update the domain. For the second case, this ACL approach would deal with this situation as well and prevent rogue clients from entering malicious information in DNS.

Q: Will I be able to set up a QIP DHCP Server or template to accept domain name in addition to host name from DHCP Client?

A: Yes, for newer DHCP clients that support DHCP Option 81 (i.e. Windows 2000 DHCP clients). Note that older DHCP clients (Windows 95,98, or NT) do not support this option. Option 81 specifies that the client can pass its hostname and domain name to the server. QIP will support the ability to accept the domain name from the client via this option. You are required to define valid domains for a subnet within the subnet profile. This provides a way to limit which domains could be accepted by QIP for a specific subnet.