Avaya Solution & Interoperability Test Lab

Application Notes for DHCP Configuration with Infoblox DNS One Appliances and Avaya IP Telephones - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring the Infoblox DNS One to provide DHCP services to Avaya IP Telephones. During compliance testing, the Infoblox DNS One successfully assigned IP and Avaya-specific parameters to Avaya IP Telephones in both VLAN and non-VLAN network configurations. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe a compliance-tested configuration comprising of Avaya IP telephones and the Infoblox DNS One appliance. The DNS One is a network identity appliance that provides Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) services. It may be used as an integrated DNS/DHCP server, external authoritative name server, forwarder, secondary server, caching-only name server, or DHCP-only server. Since Avaya IP telephones do not require DNS services, these Application Notes pertain only to situations where Avaya IP telephones require DHCP services from the DNS One.

Configuration of the DNS One is done through a web-based user interface (UI). From the DNS One's UI, the network administrator may specify DHCP address scopes and any associated DHCP options. If redundant DNS One configurations are desired, the network administrator may also configure High Availability (HA) and DHCP-Failover modes through the UI. HA and DHCP-Failover configurations are not covered in these Application Notes.

Figure 1 shows a sample network configuration consisting of Avaya IP telephones, an Avaya P333R Multilayer Stackable Switch, Infoblox DNS One appliances, PCs, and other Avaya infrastructure components. The other infrastructure components, namely the Avaya P333T-PWR switches, Avaya S8300 Media Server, and Avaya G350 Media Gateway support the verification and illustration of the Avaya/Infoblox solution. The configuration of the infrastructure components are not the focus of these Application Notes and are thus not described here. Note that actual network configurations may vary.

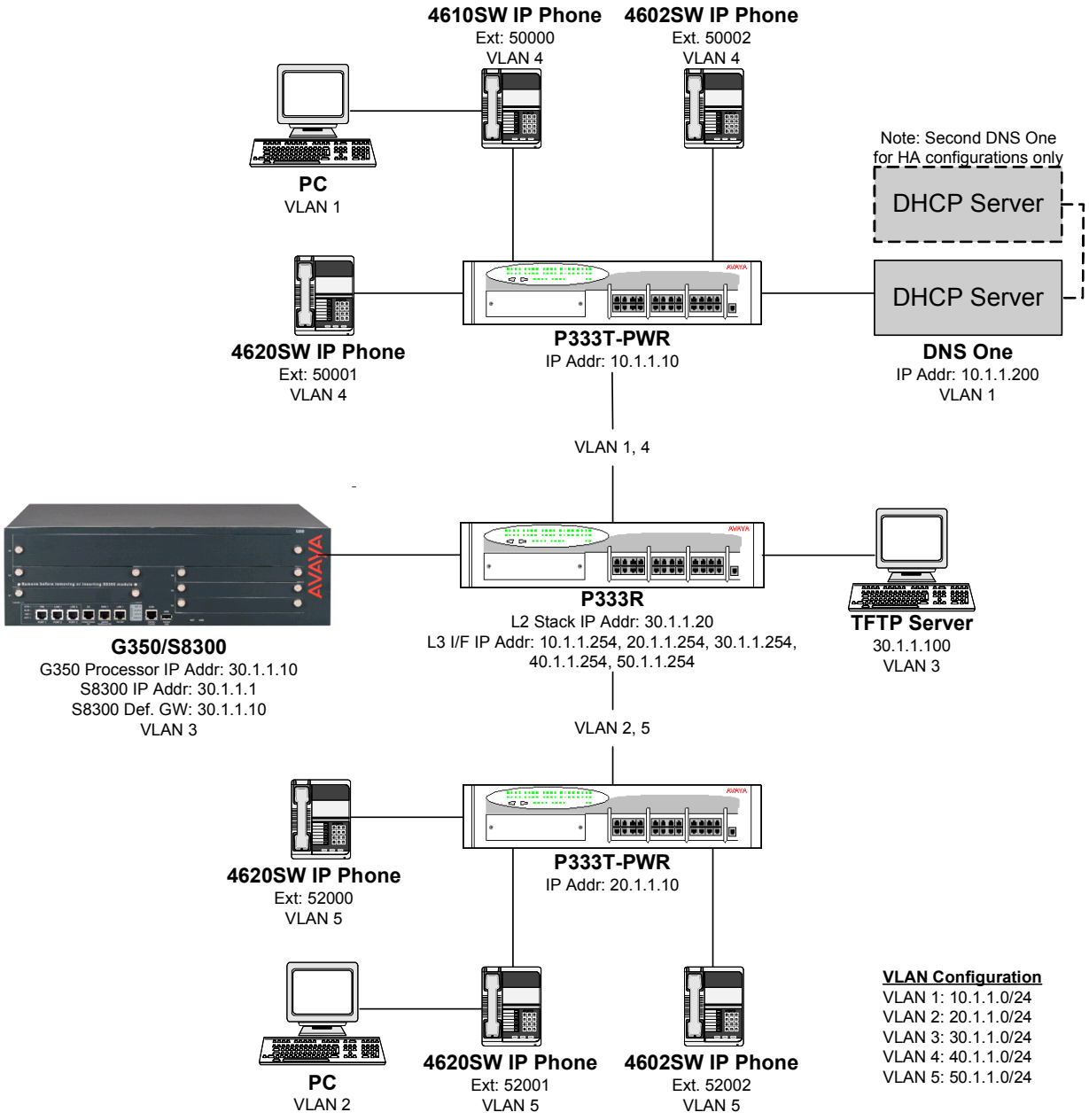


Figure 1: Sample Network Configuration for DHCP Interoperability

In **Figure 1**, the DNS One serves as the DHCP server in a network where PCs and Avaya IP telephones reside on separate VLANs and the Avaya P333R performs the BOOTP/DHCP relay function. VLANs 1 and 2 are the native (untagged) VLANs while VLANs 4 and 5 are the tagged VLANs in their respective domains. The PCs transmit and receive untagged frames on the native VLANs, and the Avaya IP telephones primarily transmit and receive tagged frames on the tagged VLANs. However, when the IP telephone requests new DHCP parameters, it first uses the untagged VLAN to exchange DHCP messages with the DNS One. From this initial

exchange, the IP telephone leases an IP address and more importantly, learns of the actual tagged VLAN (i.e., VLAN 4 or 5) that it is supposed to use. The IP telephone then releases the leased IP address, and issues a new DHCP request on the tagged VLAN. From this second exchange, the IP telephone receives IP address information valid for the tagged VLAN, as well as call server and TFTP server information.

2. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya 4600 Series IP Phones	1.8.1 (4602SW) 2.0.1 (4610SW) 2.0.1 (4620SW)
Avaya P333T-PWR Power over Ethernet Stackable Ethernet Switch	4.0.17
Avaya P333R Multilayer Stackable Switch	4.0.9
Avaya G350 Media Gateway	21.22.0
Avaya S8300 Media Server	R012x.00.1.221.1
Infoblox DNS One	2.4.0-patch6
PCs	Windows 2000 Professional SP4
SolarWinds.Net TFTP Server (running on Windows 2000 PC)	5.5

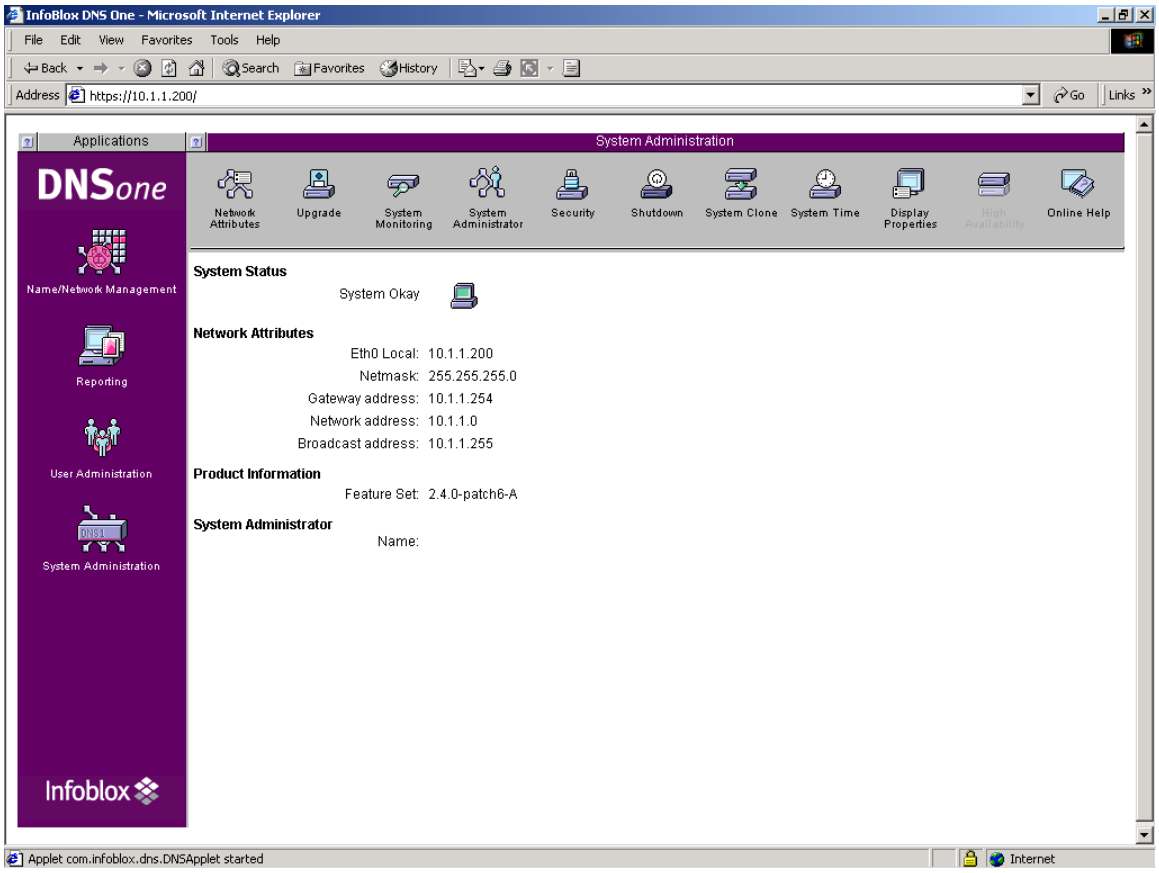
3. Configure the Infoblox DNS One

This section describes the steps for configuring DHCP server functionality on the DNS One. It assumes that the DNS One has already been configured with the appropriate IP network settings.

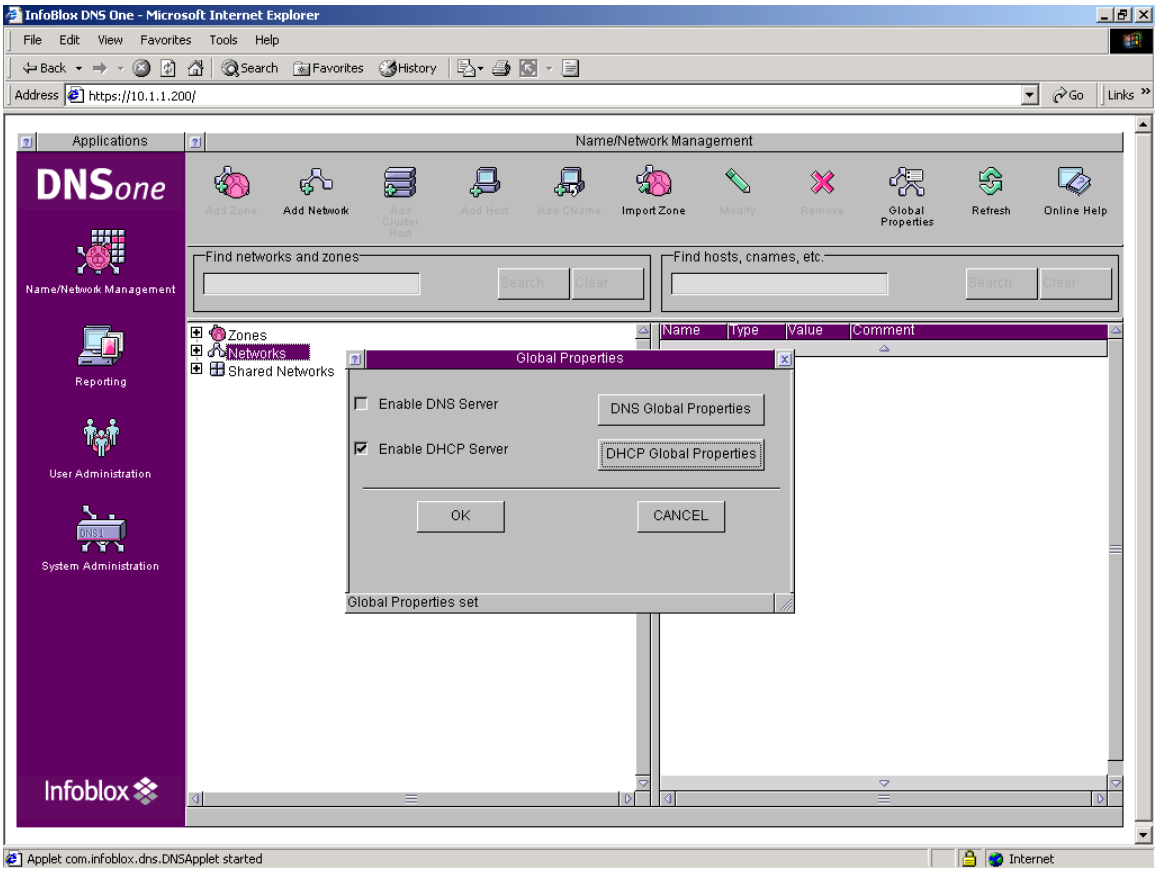
3.1. Configuring Global DHCP Settings

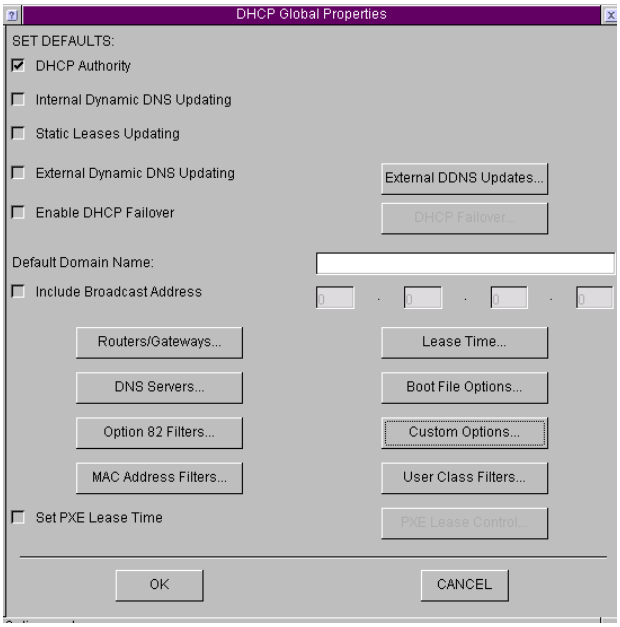
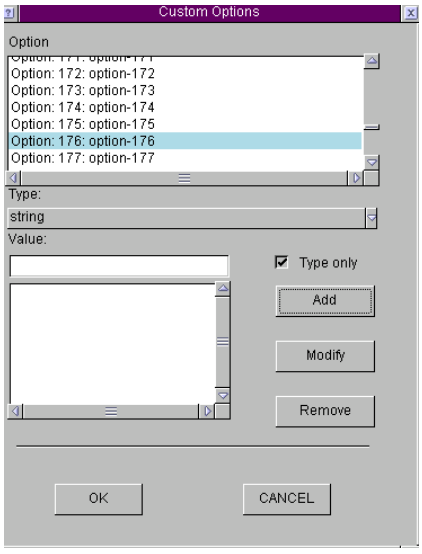
Global DHCP settings apply to all address scopes configured on the DNS One, though certain settings may be overridden in each address scope. The settings described below apply globally.

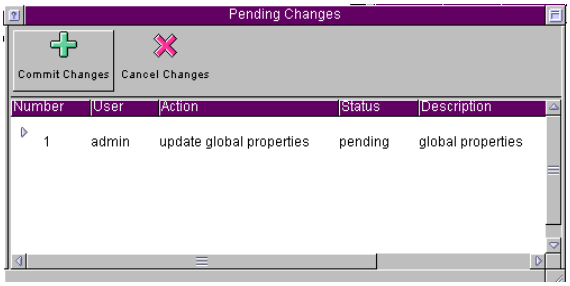
Step	Description
1.	Open a browser and enter the DNS One's IP address in the URL and log in with the appropriate credentials.



Step	Description
2.	Click on the **Name/Network Management** icon on the left pane and then the **Global Properties** icon at the top of the **Name/Network Management** window. In the **Global Properties** dialog box, check **Enable DHCP Server** and click on the **DHCP Global Properties** button.



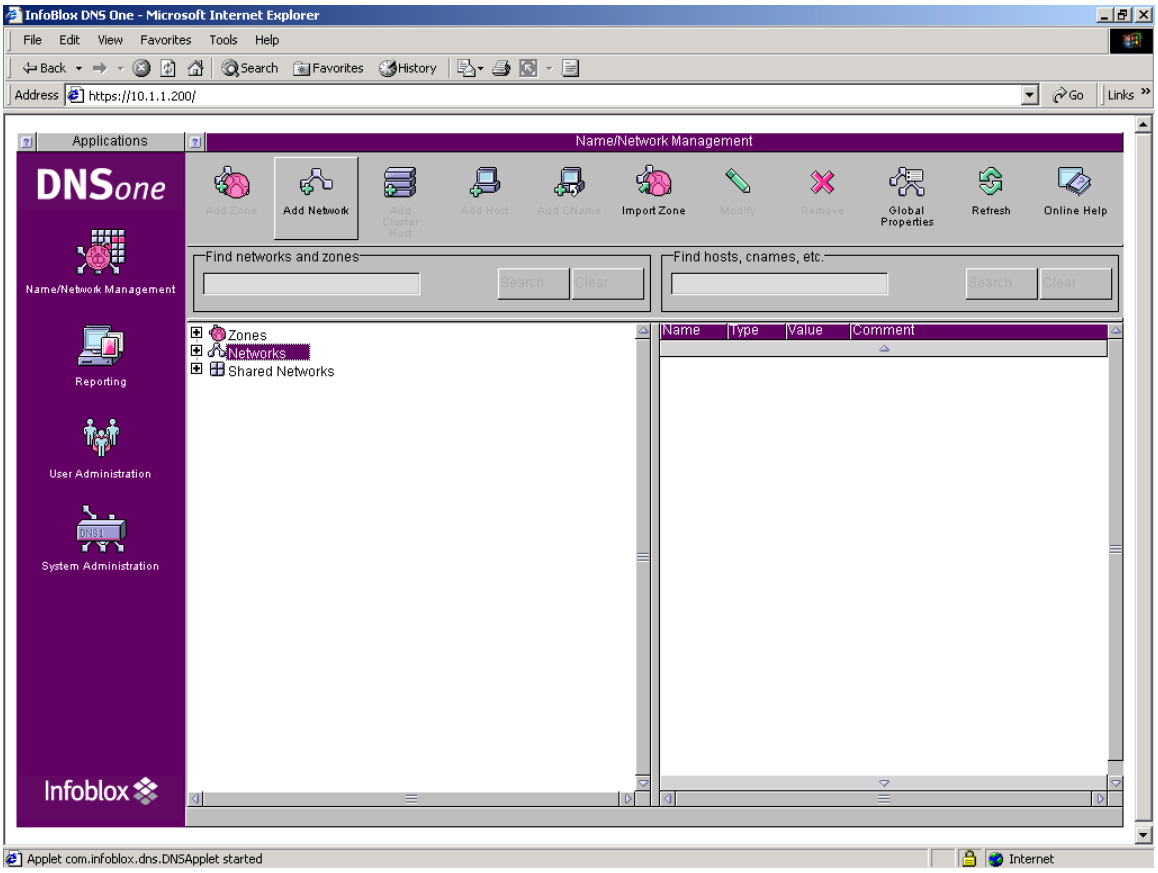
Step	Description
3.	In the **DHCP Global Properties** dialog box, check the **DHCP Authority** checkbox and click on the **Custom Options** button. 
4.	In the **Custom Options** dialog box, select **Option 176**, select **String** as the **Type**, check the **Type Only** checkbox, and click on the **Add** button. 
5.	Click on the **OK** buttons in the **Custom Options**, **DHCP Global Properties**, and **Global Properties** dialog boxes.

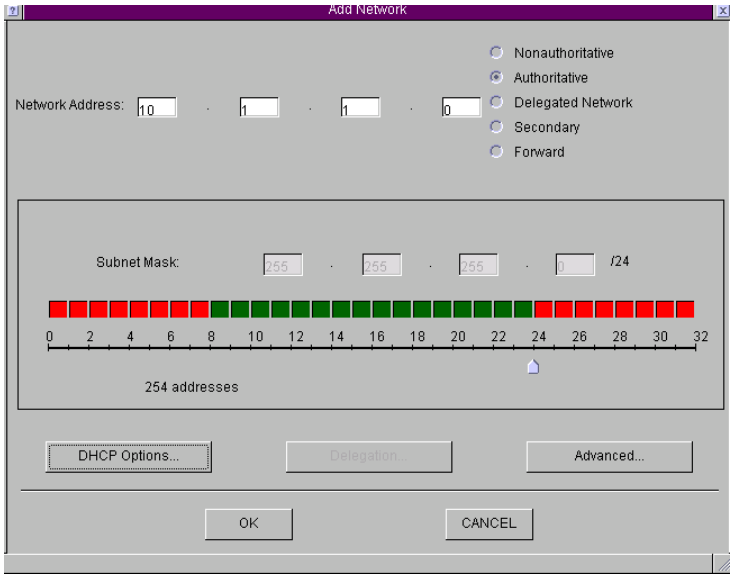
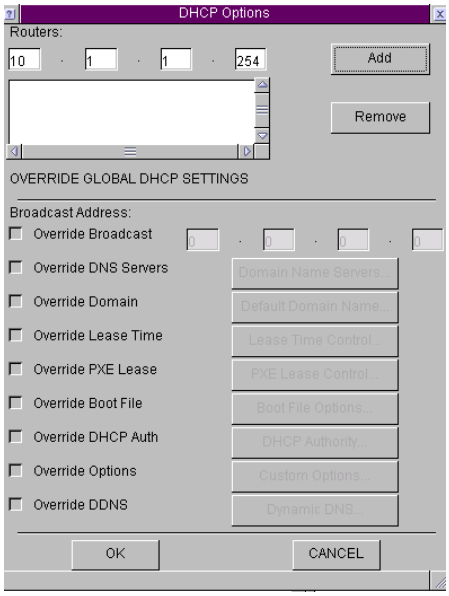
Step	Description
6.	The DNS One then prompts for confirmation of the changes. In the **Pending Changes** window, click on the **Commit Changes** icon. 

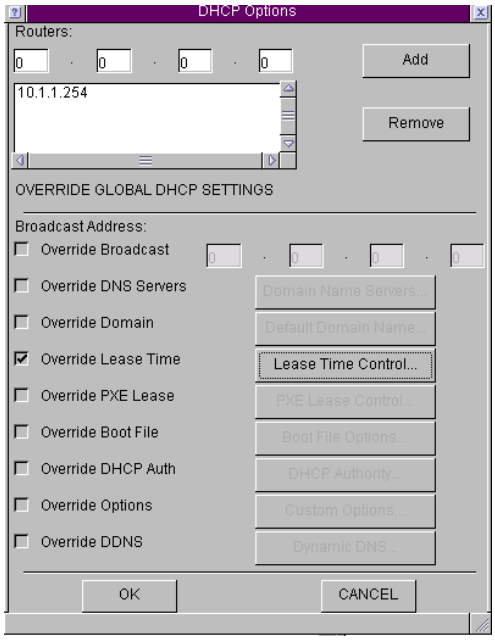
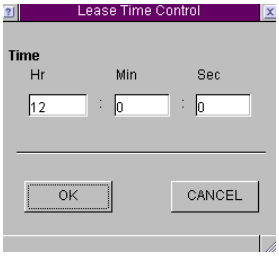
3.2. Adding Address Scopes

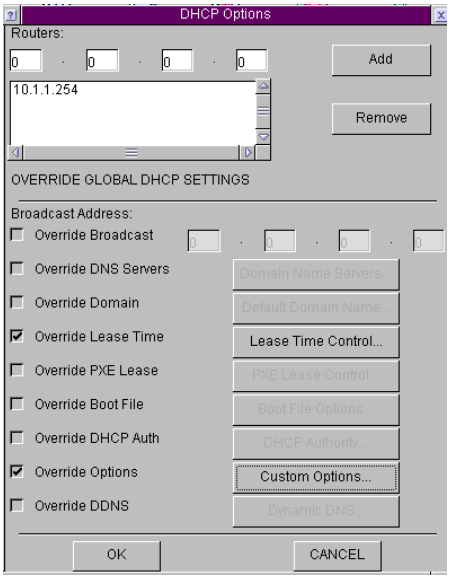
An address scope needs to be defined for each subnet/VLAN that obtains DHCP services from the DNS One. Each address scope includes the subnet/VLAN's IP information (network address, subnet mask, and router addresses), as well as any DHCP options to be applied to the subnet/VLAN. Specifically, DHCP Option 176 must be specified in the address scopes for both the untagged VLANs ("data" VLANs) and the tagged VLANs ("voice" VLANs). For the "data" VLANs, DHCP Option 176 is used to instruct Avaya IP telephones to turn tagging on and inform them of the "voice" VLAN ID. PCs and other DHCP clients ignore DHCP Option 176. For the "voice" VLANs, DHCP Option 176 is used to pass media server, VLAN, and TFTP server information to the Avaya IP telephones.

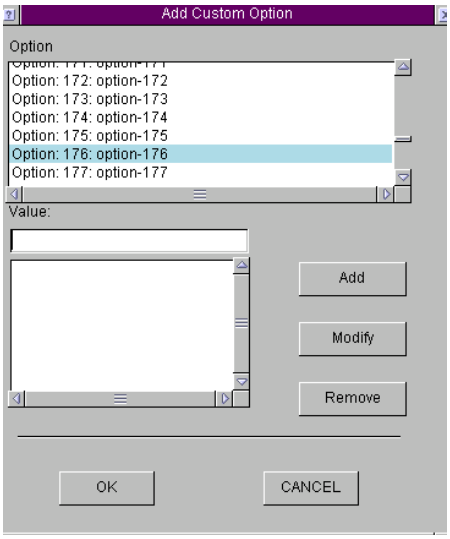
Step	Description
1.	In the **Name/Network Management** window, select **Networks** and click on the **Add Network** icon.



Step	Description
2.	In the **Add Network** dialog box, enter the **Network Address** of the address scope, select the **Authoritative** radio button, and adjust the **Subnet Mask** slider to the desired value. Click on the **DHCP Options** button. 
3.	In the **DHCP Options** dialog box, enter a default router for the address scope and click on the **Add** button. Repeat for additional routers if necessary. 

Step	Description
4.	Check the **Override Lease Time** checkbox and click on the **Lease Time Control** button. 
5.	In the **Lease Time** Control dialog box, specify the lease time and click on the **OK** button. 

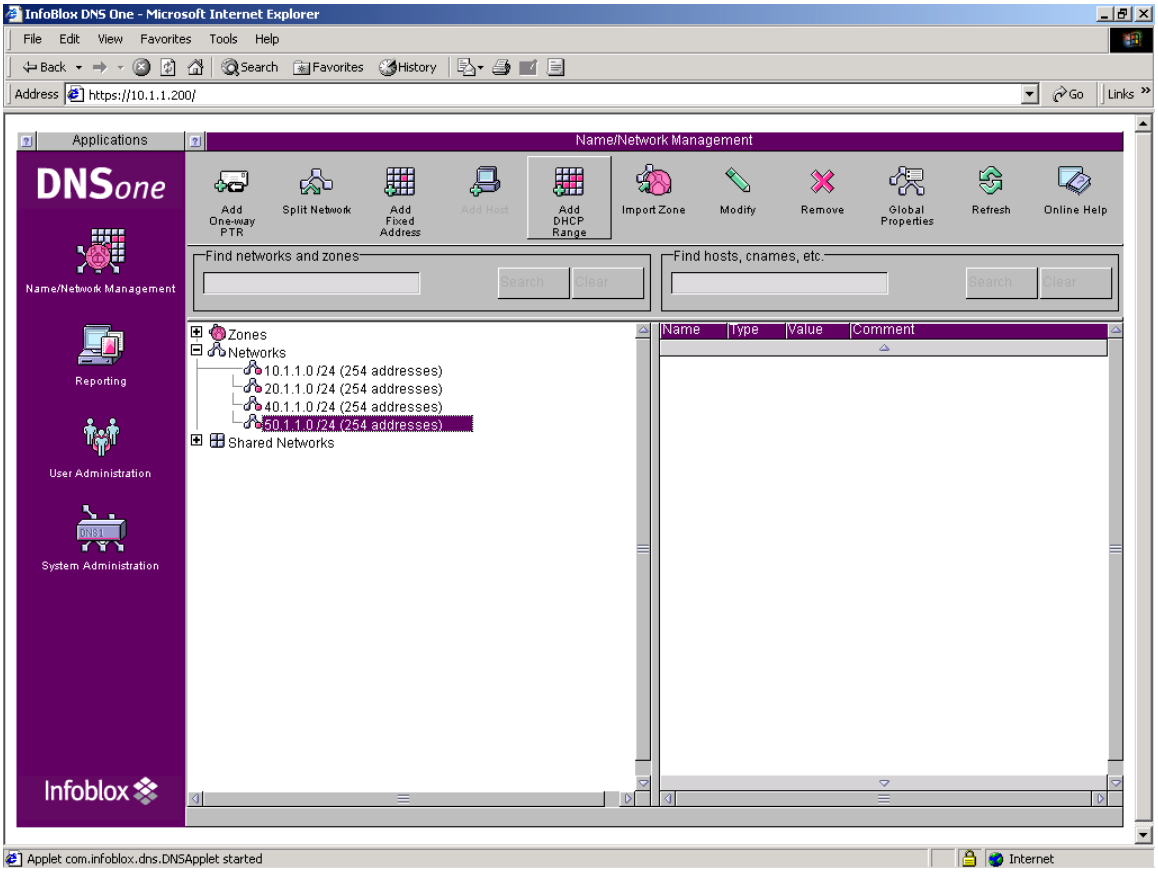
Step	Description
6.	In the **DHCP Options** dialog box, check the **Override Options** checkbox and click on the **Custom Options** button. 

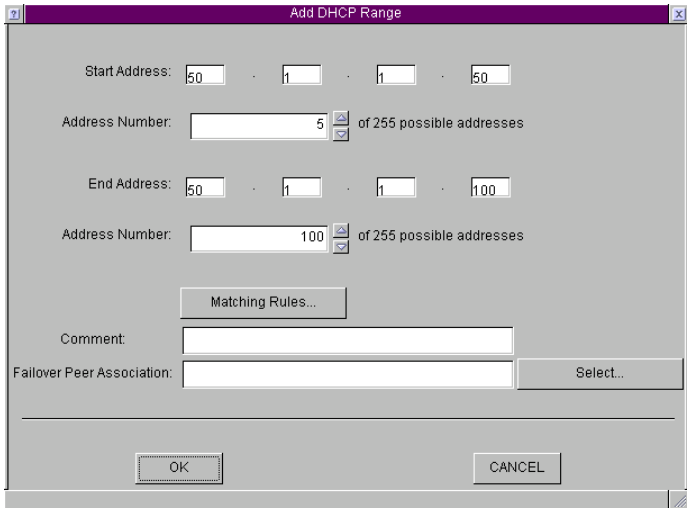
Step	Description
7.	In the **Add Custom** Options dialog box, select **Option 176** from the **Option** list.  Enter one of the following in the **Value** field: 1) For an address scope for a "data" (untagged) VLAN, specify the Layer 2 tagging setting (L2Q) and the VLAN ID (L2QVLAN) values of the "voice" (tagged) VLAN. PCs and other DHCP clients will ignore those values, but the Avaya IP telephones will accept the L2Q and L2QVLAN values. For example, for the VLAN 1 and VLAN 2 address scopes in the sample configuration, enter **L2Q=1,L2QVLAN=4** and **L2Q=1,L2QVLAN=5**, respectively, and click on the **Add** button. 2) For an address scope for a "voice" (tagged) VLAN, specify the Avaya Media Server IP address (MCIPADD), Avaya Media Server Port (MCPORT), and TFTP server IP address (TFTPSRVR). For example, for the VLAN 4 and VLAN 5 address scopes in the sample configuration, enter **MCIPADD=30.1.1.1,MCPORT=1719,TFTPSRVR=30.1.1.100** and click on the **Add** button.
8.	Click on the **OK** buttons in the **Add Custom Option**, **DHCP Options**, and **Add Network** dialog boxes and commit the changes.
9.	Repeat steps 1 through 8 for each address scope to be added.

3.3. Specifying Address Pools for Address Scopes

An address pool defines the IP addresses that the DNS One may lease to DHCP clients. One or multiple address pools may be specified for each address scope.

Step	Description
1.	In the **Name/Network Management** window, expand **Networks**, and select an address scope. Click on the **Add DHCP Range** icon at the top of the window.



Step	Description
2.	In the **Add DHCP Range** dialog box, enter the **Start Address** and **End Address** for the address scope and click on the **OK** button. 
3.	Commit the changes.
4.	Repeat steps 1 through 3 for each additional address pool in the address scope.
5.	Repeat steps 1 through 4 for the other address scopes.

4. Configure the Avaya P333R

The Avaya P333R must be configured as BOOTP/DHCP relay agent to forward DHCP broadcast requests from subnets/VLANs without DHCP servers to VLANs with DHCP servers. When a DHCP client requests an IP address, it broadcasts DHCP requests to find a DHCP server. If there is no DHCP server on the broadcast domain, then the DHCP messages needs to be forwarded by a BOOTP/DHCP relay agent to a DHCP server.

Note: The following steps assume that the VLAN Layer 3 interfaces have been previously provisioned.

Step	Description
1.	Log into the P333R with the appropriate credentials via the console port or a telnet session.

Step	Description

2.	Enter into router configuration mode:
	
	`Cajun_P330-1(super)# configure`
	`Cajun_P330-1(configure)#`
	
	`Cajun_P330-1(configure)# session router`
	`Router-1(configure)#`

3.	Enable relaying of DHCP requests to the DHCP server:
	
	`Router-1(configure)# ip bootp-dhcp relay`
	`Done!`

4.	For each interface that connects to DHCP clients, specify the IP address of the DHCP server that will handle the DHCP requests received on the interface:
	
	`Router-1(configure)# interface net20`
	`Done!`
	`Router-1(config-if:net20)# ip bootp-dhcp server 10.1.1.200`
	`Done!`
	`Router-1(config-if:net20)# exit`
	`Router-1(configure)#`
	
	`Router-1(configure)# interface net40`
	`Done!`
	`Router-1(config-if:net40)# ip bootp-dhcp server 10.1.1.200`
	`Done!`
	`Router-1(config-if:net40)# exit`
	`Router-1(configure)#`
	
	`Router-1(configure)# interface net50`
	`Done!`
	`Router-1(config-if:net50)# ip bootp-dhcp server 10.1.1.200`
	`Done!`
	`Router-1(config-if:net50)# exit`
	`Router-1(configure)#`
	
	Notes:
	1. In this example, the interface names “net10”, “net20”, “net30”, “net40”, and “net50” correspond to the router interfaces 10.1.1.254, 20.1.1.254, 30.1.1.254, 40.1.1.254, and 50.1.1.254, respectively.
	2. For an interface that connects to a DHCP server, i.e. “net10” in this example, specifying that DHCP server’s IP address on the interface is not necessary.
	3. For an interface that does not have DHCP clients, i.e. “net30” in this example, specifying a DHCP server on the interface is not necessary.
	4. Up to two DHCP server IP addresses may be specified for each interface.

5. Configure the Avaya IP Telephones

Step	Description
1.	With the telephone powered on and on-hook (idle), press the **MUTE** button and then press the following keys in sequence on the dialpad: **73738#** (**RESET#**).
2.	When prompted to "**Reset Values?**", press the **#** key. This will reset any previously assigned values. When prompted to "**Restart Phone?**", press the # key.

6. Interoperability Compliance Testing

The interoperability compliance testing included feature functionality, serviceability and redundancy testing. The feature functionality testing evaluated the DNS One's capabilities to provide the following to the Avaya IP telephones in network configurations with and without VLANs:

- IP address, subnet mask, and router IP address
- H.323 gatekeeper (Avaya Media Server) IP address and TCP port
- TFTP server IP address
- Layer 2 tagging and VLAN information

The serviceability testing introduced failure scenarios and examined the DNS One's ability to correctly assign DHCP parameters to the Avaya IP telephones after failure recovery. The redundancy testing put two DNS One appliances in HA and DHCP-Failover modes, and evaluated DHCP functionality and serviceability after the active/primary DNS One failed.

6.1. General Test Approach

All tests were performed manually primarily from the user's perspective. The main objectives were to verify that:

- The DNS One provides correct IP and Avaya-specific information to Avaya IP telephones configured as DHCP clients on different subnets and VLANs.
- Avaya IP telephones successfully renew their leases from the DNS One after lease expiration.
- Avaya IP telephones successfully obtain new DHCP information from the DNS One after moving to a different subnet or VLAN.
- The DNS One continues to provide DHCP services after recovery from failures such as cable pulls and server (DNS One) and telephone resets.

- When two DNS One appliances are configured in HA or DHCP-Failover mode, the active/primary DNS One provides correct IP and Avaya-specific information to Avaya IP telephones, and the passive/secondary DNS One continues to do so even after the active/primary DNS One fails.

6.2. Test Results

All test cases completed successfully. The DNS One was able to provide correct IP and Avaya-specific information to the Avaya IP telephones in network configurations with and without VLANs under normal conditions and after failure recovery. In addition, in the redundancy testing, the passive/secondary DNS One correctly provided DHCP services after a failure of the active/primary DNS One.

7. Verification Steps

The following steps may be used to verify communication between the DNS One and the Avaya IP telephones, and checking the configurations of the Avaya IP telephones.

1. From each subnet/VLAN, ping the DNS One, Avaya Media Server, and TFTP server and verify connectivity.

2. In the DNS One UI, verify that the address scopes and their associated address ranges and options are specified correctly.

3. After the Avaya IP telephone acquires configuration information, enter the extension and password when prompted. After the telephone comes up, press the **MUTE** button followed by **2337#** (**ADDR#**), and verify that the assigned IP address, subnet mask, call server IP address and port, 802.1q tagging setting, and VLAN ID are correct. Repeat this step for each Avaya IP telephone.

4. Verify the leased IP addresses in the DNS One UI.

5. Verify that calls can be made to and from each Avaya IP telephone.

8. Support

For technical support on the Infoblox DNS One, consult the Infoblox Support Center (ID and password required) at http://www.infoblox.com/support or contact Infoblox Technical Support at:

- E-mail: support@infoblox.com

- Phone: 888-463-6259 or 408-716-4300 ext. 1

9. Conclusion

These Application Notes illustrate the procedures necessary for configuring the Infoblox DNS One to provide DHCP services to Avaya IP telephones. The DNS One and Avaya IP telephones were successfully compliance-tested in the converged voice/data network configurations described in these Application Notes. The DNS One was able to assign correct IP, VLAN, and Avaya-specific information to the Avaya IP telephones.

10. Additional References

Product documentation for Avaya IP telephones may be found at http://support.avaya.com.

Product information for the Infoblox DNS One may be found at http://www.infoblox.com/products/dnsone_overview.cfm.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at devconnect@avaya.com.