CHAPTER 5

Configuring a LAN with DHCP and VLANs

The Cisco 1800 series integrated services fixed-configuration routers support clients on both physical LANs and virtual LANs (VLANs). The routers can use the Dynamic Host Configuration Protocol (DHCP) to enable automatic assignment of IP configurations for nodes on these networks. Other interfaces and configurations of the VLANs are described in the "Switch Port Configurations" section on page 5-7.

1	Fast Ethernet LAN (with multiple networked devices)
2	Router and DHCP server—Cisco 1800 series integrated services router—connected to the Internet
3	VLAN 1
4	VLAN 2

DHCP

DHCP, which is described in RFC 2131, uses a client/server model for address allocation. As an administrator, you can configure your Cisco 1800 integrated services fixed-configuration router to act as a DHCP server, providing IP address assignment and other TCP/IP-oriented configuration information to your workstations. DHCP frees you from having to manually assign an IP address to each client.

When you configure a DHCP server, you must configure the server properties, policies, and DHCP options.

Note Whenever you change server properties, you must reload the server with the configuration data from the Network Registrar database.

VLANs

The Cisco 1800 series integrated services routers (fixed) support eight Fast Ethernet ports on which you can configure VLANs. See the "Switch Port Configurations" section on page 5-7 for a description of the interfaces and features that can be configured on the switch ports and a link to a document containing the configuration procedures.

VLANs enable networks to be segmented and formed into logical groups of users, regardless of the user's physical location or LAN connection.

Configuration Tasks

Perform the following tasks to configure this network scenario:

- Configure DHCP

- Configure VLANs

Note The procedures in this chapter assume you have already configured basic router features as well as PPPoE or PPPoA with NAT. If you have not performed these configurations tasks, see Chapter 1, "Basic Router Configuration," Chapter 3, "Configuring PPP over Ethernet with NAT," and Chapter 4, "Configuring PPP over ATM with NAT" as appropriate for your router. See the *Cisco IOS IP Configuration Guide* to assign an IP address to the ports.

Configure DHCP

Perform these steps to configure your router for DHCP operation, beginning in global configuration mode:

	Command	Purpose

Step 1	**ip domain name** *name*
	
	Example:
	`Router(config)# ip domain name smallbiz.com`
	`Router(config)#`
		Identifies the default domain that the router uses to complete unqualified hostnames (names without a dotted-decimal domain name).

Step 2	**ip name-server** *server-address1 [server-address2...server-address6]*
	
	Example:
	`Router(config)# ip name-server 192.168.11.12`
	`Router(config)#`
		Specifies the address of one or more Domain Name System (DNS) servers to use for name and address resolution.

Step 3	**ip dhcp excluded-address** *low-address [high-address]* **Example:** `Router(config)# ip dhcp excluded-address 192.168.9.0`	Specifies IP addresses that the DHCP server should not assign to DHCP clients. In this example, we are excluding the router address.

Step 4	**ip dhcp pool** *name*
	
	Example:
	`Router(config)# ip dhcp pool dpool1`
	`Router(config-dhcp)#`
		Creates a DHCP address pool on the router and enters DHCP pool configuration mode. The *name* argument can be a string or an integer.

Step 5	**network** *network-number* [*mask* | *prefix-length*]
	
	Example:
	`Router(config-dhcp)# network 10.10.0.0 255.255.255.0`
	`Router(config-dhcp)#`
		Defines subnet number (IP) address for the DHCP address pool, optionally including the mask.

	Command	Purpose

Step 6	**import all**
	
	Example:
	`Router(config-dhcp)# import all`
	`Router(config-dhcp)#`
		Imports DHCP option parameters into the DHCP portion of the router database.

Step 7	**default-router** *address* [*address2...address8*]
	
	Example:
	`Router(config-dhcp)# default-router 10.1.1.1`
	`Router(config-dhcp)#`
		Specifies up to 8 default routers for a DHCP client.

Step 8	**dns-server** *address* [*address2...address8*]
	
	Example:
	`Router(config-dhcp)# dns-server 192.168.35.2`
	`Router(config-dhcp)#`
		Specifies up to 8 DNS servers available to a DHCP client.

Step 9	**domain-name** *domain*
	
	Example:
	`Router(config-dhcp)# domain-name cisco.com`
	`Router(config-dhcp)#`
		Specifies the domain name for a DHCP client.

Step 10	**exit**
	
	Example:
	`Router(config-dhcp)# exit`
	`Router(config)#`
		Exits DHCP configuration mode, and enters global configuration mode.

Configuration Example

The following configuration example shows a portion of the configuration file for the DCHP configuration described in this chapter.

```
ip dhcp excluded-address 192.168.9.0
!
ip dhcp pool dpool1
   import all
   network 10.10.0.0 255.255.255.0
   default-router 10.10.10.10
   dns-server 192.168.35.2
   domain-name cisco.com
!
ip domain name smallbiz.com
ip name-server 192.168.11.12
```

Verify Your DHCP Configuration

Use the following commands to view your DHCP configuration.

- **show ip dhcp import**—Displays the optional parameters imported into the DHCP server database.
- **show ip dhcp pool**—Displays information about the DHCP address pools.
- **show ip dhcp server statistics**—Displays the DHCP server statistics, such as the number of address pools, bindings, and so forth.

```
Router# show ip dhcp import

Address Pool Name: dpool1

Router# show ip dhcp pool

Pool dpool1 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 10.10.0.1            10.10.0.1        - 10.10.0.254       0

Router# show ip dhcp server statistics
Memory usage         15419
Address pools        1
Database agents      0
Automatic bindings   0
Manual bindings      0
Expired bindings     0
Malformed messages   0
Secure arp entries   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         0
DHCPREQUEST          0
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            0
DHCPACK              0
DHCPNAK              0
Router#
```

Configure VLANs

Perform these steps to configure VLANs on your router, beginning in global configuration mode:

	Command	Purpose

Step 1	**vlan ?**
	Example:
	`Router# config t`
	`Router(config)#vlan ?`
	
	`WORD  ISL VLAN IDs 1-4094`
	`accounting  VLAN accounting configuration`
	`ifdescr  VLAN subinterface ifDescr`
	
	`Router(config)#vlan`
		Enters VLAN configuration mode.

Step 2	*ISL VLAN ID*
	Example:
	`Router(config)#vlan 2`
	`Router(config-vlan)#`
		Adds VLANs, with identifiers ranging from 1- 4094.
		For details about this command and additional parameters that can be set, see the *Cisco IOS Switching Services Command Reference*.

Step 3	**exit**
	Example:
	`Router(config-vlan)#exit`
	`Router(config)#`
		Updates the VLAN database, propagates it throughout the administrative domain, and returns to global configuration mode.

Verify Your VLAN Configuration

Use the following commands to view your VLAN configuration.

- **show**—Entered from VLAN database mode. Displays summary configuration information for all configured VLANs.
- **show vlan-switch**—Entered from privileged EXEC mode. Displays detailed configuration information for all configured VLANs.

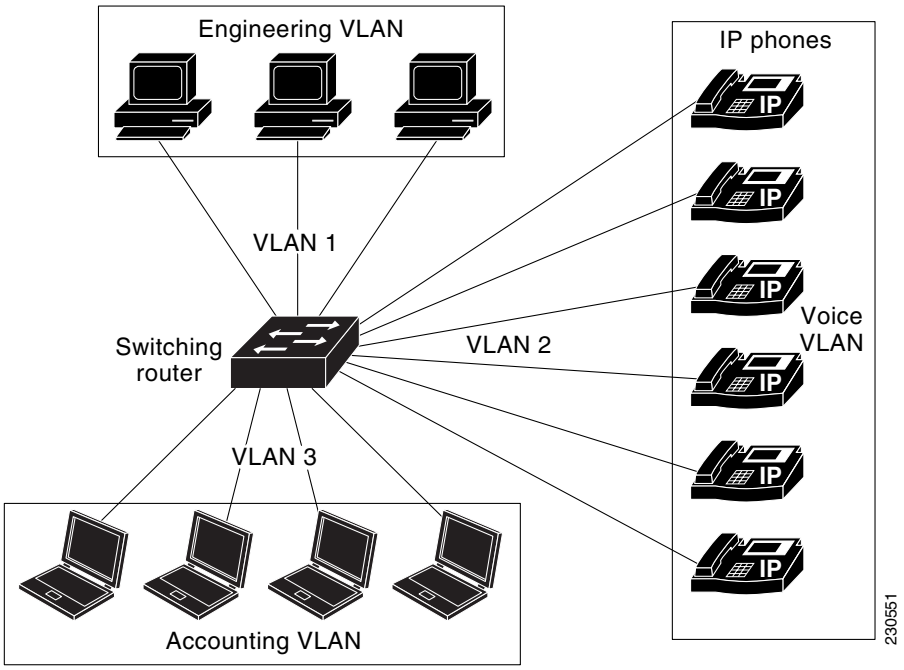
```
Router# vlan database
Router(vlan)# show
  VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Translational Bridged VLAN: 1002
    Translational Bridged VLAN: 1003

  VLAN ISL Id: 1002
    Name: fddi-default
    Media Type: FDDI
    VLAN 802.10 Id: 101002
    State: Operational
    MTU: 1500
    Bridge Type: SRB
```

```
    Translational Bridged VLAN: 1
    Translational Bridged VLAN: 1003

  VLAN ISL Id: 1003
    Name: token-ring-default
    Media Type: Token Ring
    VLAN 802.10 Id: 101003
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Ring Number: 0
    Bridge Number: 1
    Parent VLAN: 1005
    Maximum ARE Hop Count: 7
    Maximum STE Hop Count: 7
    Backup CRF Mode: Disabled
    Translational Bridged VLAN: 1
    Translational Bridged VLAN: 1002

  VLAN ISL Id: 1004
    Name: fddinet-default
    Media Type: FDDI Net
    VLAN 802.10 Id: 101004
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Bridge Number: 1
    STP Type: IBM

  VLAN ISL Id: 1005
    Name: trnet-default
    Media Type: Token Ring Net
    VLAN 802.10 Id: 101005
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Bridge Number: 1
    STP Type: IBM

Router# show vlan-switch

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0, Fa1, Fa2, Fa3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
1002 fddi  101002     1500  -      -      -        -    -        1      1003
1003 tr    101003     1500  1005   0      -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
Router#
```

Switch Port Configurations

The 8 high speed Ethernet ports on the Cisco 1800 (fixed) integrated router supports 8 VLANs per port. To configure and verify VLANs on the switch ports see the the "Configure VLANs" section on page 5-5 and the "Verify Your VLAN Configuration" section on page 5-5.

Figure 5-1 VLAN Configuration on the Cisco 1800 (Fixed) Router Showing Three VLAN Segments



Other procedures for configuring the switch ports, including configuration examples and information on the features and interfaces are in the *Cisco HWIC-4ESW and HWIC-9ESW EtherSwitch Interface Cards* document on Cisco.com. See this document to configure the switch ports. The configuration procedures described in this document are listed below.

- Configuring VLANs (required)
- Configuring VLAN Trunking Protocol (optional)
- Configuring 802.1x Authentication (required)
- Configuring Spanning Tree on a VLAN (required)
- Configuring Layer 2 Interfaces (required)
- Configuring MAC Table Manipulation (required)
- Configuring the Switched Port Analyzer (required)
- Configuring Power Management on the Interfaces (optional)
- IP Multicast Layer 3 Switching (required)
- Configuring Per-Port Storm Control (optional)
- Configuring Fallback Bridging (optional)
- Configuring Separate Voice and Data Submits (optional)
- Configuring IGMP Snooping (optional)

This section briefly describes the features and interfaces that can be configured on the VLANs assigned to the switch ports and any differences between the configurations for the HWIC-4ESW and HWIC-9ESW and the configuration of the switch ports.

VLAN Trunking Protocol (VTP)

VLAN Trunking Protocol(VTP) supports three types of VTP modes – server, client and transparent modes. In VTP server mode, you create, modify and delete VLANs and specify other configuration parameters such as the VTP version for the entire VTP domain. VTP clients behave the same way as VTP servers, but you cannot create, change or delete VLANs on a VTP client. A VTP transparent switch does not advertise its' VLAN configuration, and does not synchronize its VLAN configuration based on received advertisements.

802.1x Authentication

The switch port determines whether a client is granted access to the network. In the default setting, the port is in the unauthorized state. While in this state, the port disallows all ingress and egress traffic except for 802.1x packets. When a client has successfully authenticated, the port changes to the authorized state, allowing all traffic for the client to flow normally.

If a client that does not support 802.1x is connected to an unauthorized 802.1x port, the switch requests the client's identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

The 802.1x protocol supports authentication and full authentication, authorization, and accounting [AAA] and RADIUS modes with port VLAN ID (PVID) and voice VLAN ID (VVID); and with VLAN assignment with guest VLAN single and multi-host support on the Cisco 1800 (fixed) Configuration Series.

Note These security features are not supported on the switch ports: Security Access Control Lists, IP Access Control Lists (IP- ACLs) for Layer 2 ports, and VLAN ACLs Virtual ACLs.

Layer 2 Interfaces

The integrated switch ports support Layer 2 switching across Ethernet ports based on Cisco IOS Catalyst Software. They support simultaneous, parallel connections between Layer 2 Ethernet segments. Switched connections between Ethernet segments last only for the duration of the packet. Different connections can be made for different segments for the next packet. You can configure a range of Layer 2 interfaces, define a range macro, set the interface speed, set the duplex mode, and add a description for the interface.

MAC Table Manipulation

The MAC table is configured to provide port security. The switch ports use the MAC address tables to forward traffic between the ports. All MAC addresses in the address table are associated with one or more ports. The MAC tables include the following types of addresses:

- Dynamic address–the source MAC address that the switch learns and then drops when not in use.
- Secure address–manually entered unicast address that is usually associated with a secured port. Secure addresses do not age.
- Static address–manually entered unicast or multicast address that does not age and that is not lost when the switch resets.

The Cisco 1800 (Fixed) Configuration Series supports 100 secure and static MAC addresses. General MAC addresses are supported for 50 users.

Maximum Switched Virtual Interfaces (SVIs)

A switch virtual interface (SVI) represents a VLAN of switch ports as one interface to the routing or bridging function in the router. Only one SVI can be associated with a VLAN; it is necessary to configure an SVI for a VLAN only when you wish to route between VLANs, when you wish to configure fallback-bridge nonroutable protocols between VLANs, or when you wish to provide IP host connectivity. Eight SVI interfaces are supported on each port of the fixed router

Switched Port Analyzer (SPAN)

You can configure SPAN sessions using parameters that specify the type of network traffic to monitor. SPAN sessions allow you to monitor traffic in one or more interfaces and allow you to send ingress traffic, egress traffic or both to one destination interface.

You can enable spanning tree on a per-VLAN basis and configure various spanning tree features. All frames have 802.1q tags.

IP Multicast Switching

Multicast switching is Layer 3 switching. To configure Multicast switching, the maximum number of configured VLANs must be less than or equal to 242. The maximum number of multicast groups is equal to to the maximum number of VLANs.

You can configure your router to enable multi-cast switching globally, enable IP Protocol Independent Multicast (PIM) on a Layer 3 interface, and verify the Multicast Layer 3 switching information.

Note Per-Port enabling and disabling of unknown multicast and unicast packets is not supported on the Cisco 1800 (Fixed) configuration router.

Per-Port Storm Control

You can use these per-port storm control techniques to block the forwarding of unnecessary, flooded traffic.

Fallback Bridging

With Fallback Bridging, the switch bridges together two or more VLANs or routed ports, essentially connecting multiple VLANs within one bridge domain.

To configure Fallback Bridging for a set of SVIs, the SVIs must be assigned to bridge groups. All bridges in the same group belong to the same bridge domain. Each SVI can be assigned to only one bridge group.

Separate Voice and Data Subnets

For ease of network administration and increased scalability, network managers can configure the switch ports to support Cisco IP phones such that the voice and data traffic reside on separate subnets.

IGMP Snooping

By default, IGMP Snooping is globally enabled on the switch ports. When globally enabled or disabled, it is also enabled or disabled on all VLAN interfaces. It can be enabled and disabled on a per-VLAN basis.

Note All of the procedures for configuring the switch ports, including configuration examples and information on the features and interfaces are in the *Cisco HWIC-4ESW and HWIC-9ESW EtherSwitch Interface Cards* document on Cisco.com. See this document to configure the switch ports.