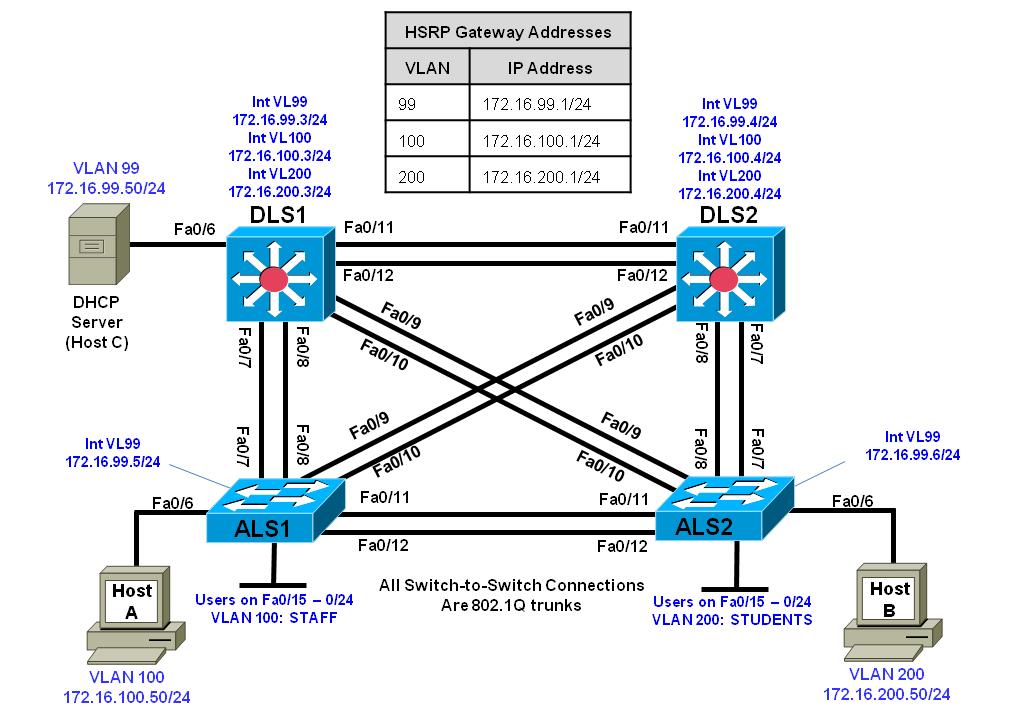
CCNPv7.1 SWITCH

Chapter 10 Lab 10-1, Securing Layer 2 Switches

Topology



Objectives

* Prepare the Network.
* Implement Layer 2 network security features.
* Prevent DHCP spoofing attacks.
* Prevent unauthorized access to the network using AAA.

Background

A fellow network engineer that you have known and trusted for many years has invited you to lunch this week. At lunch, he brings up the subject of network security and how two of his former co-workers had been arrested for using different Layer 2 attack techniques to gather data from other users in the office for their own personal gain in their careers and finances. The story shocks you because you have always known your friend to be very cautious with security on his network. His story makes you realize that your business network has been cautious with external threats, Layer 3–7 security, firewalls at the borders, and so on, but insufficient at Layer 2 security and protection inside the local network.

When you get back to the office, you meet with your boss to discuss your concerns. After reviewing the company’s security policies, you begin to work on a Layer 2 security policy.

First, you establish which network threats you are concerned about and then put together an action plan to mitigate these threats. While researching these threats, you learn about other potential threats to Layer 2 switches that might not be malicious but could threaten network stability. You decide to include these threats in the policies as well.

Other security measures need to be put in place to further secure the network, but you begin with configuring the switches against a few specific types of attacks, including MAC flood attacks, DHCP spoofing attacks, and unauthorized access to the local network. You plan to test the configurations in a lab environment before placing them into production.

Note: This lab uses Cisco Catalyst 3560 and 2960 switches running Cisco IOS 15.0(2) IP Services and LAN Base images, respectively. The 3560 and 2960 switches are configured with the SDM templates “dual-ipv4-and-ipv6 routing” and “lanbase-routing”, respectively. Depending on the switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab. Catalyst 3650 switches (running any Cisco IOS XE release) and Catalyst 2960-Plus switches (running any supported Cisco IOS image) can be used in place of the Catalyst 3560 switches and the Catalyst 2960 switches.

**Note:** This lab uses the Cisco WS-C2960-24TT-L switch with the Cisco IOS image c2960-lanbasek9-mz.150-2.SE6.bin and the Catalyst 3560V2-24PS switch with the Cisco IOS image c3560-ipservicesk9-mz.150-2.SE6.bin. Other switches and Cisco IOS Software versions can be used if they have comparable capabilities and features. Depending on the switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

Required Resources

* 2 switches (Cisco 2960 with the Cisco IOS Release 15.0(2)SE6 C2960-LANBASEK9-M image or comparable).
* 1 switches (Cisco 3560 with the Cisco IOS Release 15.0(2)SE6 C3560-ipservicesK9-M image or comparable).
* 3 PC’s with Windows OS. One of the PCs should be equipped Wireshark, WinRadius, and Tftpd32 software.
* Ethernet and console cables

1. Prepare for the Lab
   1. Prepare the switches for the lab

Use the **reset.tcl** script you created in Lab 1 “Preparing the Switch” to set your switches up for this lab. Then load the file BASE.CFG into the running-config with the command **copy flash:BASE.CFG running-config**.

* 1. Configure basic switch parameters.
     1. Loading BASE.CFG should have set the hostname, IP domain name, and shut down all of the interfaces on each switch.
     2. Configure enable secret, and VTY passwords. As with previous labs, if NETLAB compatibility is required, use **class** as the enable secret and **cisco** as the VTY password.
     3. Configure interface VLAN 99 on each switch with the management IP address shown in the topology diagram.
     4. Configure the access layer switches (ALS1 and ALS2) to use a default gateway IP address of 172.16.99.1.
     5. Configure basic (unauthenticated) NTP in the network. Use DLS1 as the NTP master and have DLS2, ALS1, and ALS2 synchronize to 172.16.99.3.
     6. Configure 802.1q trunking between the switches according to the diagram (Note that there are no EtherChannels in this topology). Create and then use VLAN 666 as the native VLAN for all trunks. Also turn off switchport negotiation on all trunks.

Configure all four switches. An example of DLS1 and ALS1 configuration follows:

DLS1# **clock set 14:55:00 3 August 2015**

DLS1# **config t**

DLS1(config)# **clock timezone CST -6**

DLS1(config)# **clock summer-time CDT recurring**

DLS1(config)# **ntp master 10**

DLS1(config)# **enable secret class**

DLS1(config)# **enable secret class**

DLS1(config)# **line vty 0 15**

DLS1(config-line)# **password cisco**

DLS1(config-line)# **login**

DLS1(config-line)# **exit**

DLS1(config)# **interface vlan 99**

DLS1(config-if)# **ip address 172.16.99.3 255.255.255.0**

DLS1(config-if)# **no shutdown**

DLS1(config-if)# **exit**

DLS1(config)# **vlan 666**

DLS1(config-vlan)# **name NATIVE\_DO\_NOT\_USE**

DLS1(config-vlan)# **exit**

DLS1(config)# **interface range fastethernet 0/7 - 12**

DLS1(config-if-range)# **switchport trunk encapsulation dot1q**

DLS1(config-if-range)# **switchport mode trunk**

DLS1(config-if-range)# **switchport trunk native vlan 666**

DLS1(config-if-range)# **switchport nonegotiate**

DLS1(config-if-range)# **no shut**

DLS1(config-if-range)# **exit**

ALS1(config)# **enable secret class**

ALS1(config)# **line vty 0 15**

ALS1(config-line)# **password cisco**

ALS1(config-line)# **login**

ALS1(config-line)# **exit**

ALS1(config)# **interface vlan 99**

ALS1(config-if)# **ip address 172.16.99.5 255.255.255.0**

ALS1(config-if)# **no shutdown**

ALS1(config-if)# **exit**

ALS1(config)# **ip default-gateway 172.16.99.1**

ALS1(config)# **ntp server 172.16.99.3**

ALS1(config)# **clock timezone CST -6**

ALS1(config)# **clock summer-time CDT recurring**

ALS1(config)# **vlan 666**

ALS1(config-vlan)# **name NATIVE\_DO\_NOT\_USE**

ALS1(config-vlan)# **exit**

ALS1(config)# **interface range fastethernet 0/7 - 12**

ALS1(config-if-range)# **switchport mode trunk**

ALS1(config-if-range)# **switchport trunk native vlan 666**

ALS1(config-if-range)# **switchport nonegotiate**

ALS1(config-if-range)# **no shut**

ALS1(config-if-range)# **exit**

* + 1. Verify trunking and spanning-tree operations using the show interfaces trunk and show spanning-tree commands. Which switch is the root bridge?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. For ALS1 and ALS2, which trunks have a role of designated (Desg), Alternate (Altn), and Root?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Step 3: Configure VTP on DLS2, ALS1, and ALS2.

* + 1. Change the VTP mode of ALS1 and ALS2 to client. An example from ALS1:

ALS1(config)# **vtp mode client**

Setting device to VTP CLIENT mode.

* + 1. Change the VTP mode of DLS2 to server with no further configuration:

DLS2(config)# **vtp mode server**

Setting device to VTP SERVER mode.

* 1. Configure VTP on DLS1.

Create the VTP domain on DLS1, and create VLANs 99, 100, and 200 for the domain.

DLS1(config)# **vtp domain SWPOD**

DLS1(config)# **vtp version 2**

DLS1(config)# **vlan 99**

DLS1(config-vlan)# **name Management**

DLS1(config-vlan)# **vlan 100**

DLS1(config-vlan)# **name STAFF**

DLS1(config-vlan)# **vlan 200**

DLS1(config-vlan)# **name STUDENTS**

DLS1(config-vlan)# **exit**

DLS1(config)#

* 1. Configure host PCs.

Configure PCs Host A, B, and C with the IP address and subnet mask shown in the topology. Host A is in VLAN 100 with a default gateway of 172.16.100.1. Host B is in VLAN 200 with a default gateway of 172.16.200.1. Host C is in VLAN 99 with a default gateway of 172.16.99.1.

* 1. Configure access ports.

Configure the host ports for the appropriate VLANs according to the diagram. Configure this on DLS1, ALS1, and ALS2. An example from ALS1 is below (all ports on ALS1 should be in VLAN 100, all ports on ALS2 should be in VLAN 200):

ALS1(config)# **interface range fa0/6, fa0/15 - 24**

ALS1(config-if-range)# **switchport mode access**

ALS1(config-if-range)# **switchport access vlan 100**

ALS1(config-if-range)# **spanning-tree portfast**

ALS1(config-if-range)# **no shut**

%Warning: portfast should only be enabled on ports connected to a single

host. Connecting hubs, concentrators, switches, bridges, etc... to this

interface when portfast is enabled, can cause temporary bridging loops.

Use with CAUTION

%Portfast will be configured in 10 interfaces due to the range command

but will only have effect when the interfaces are in a non-trunking mode.

* 1. Configure Spanning-Tree Root switches

Configure DLS1 to be the primary root for VLANs 99 and 100 and secondary root for VLAN 200. Configure DLS2 to be the primary root for VLAN 200 and the secondary root for VLANs 99 and 100.

DLS1(config)# **spanning-tree vlan 99,100 root primary**

DLS1(config)# **spanning-tree vlan 200 root secondary**

DLS2(config)# **spanning-tree vlan 99,100 root secondary**

DLS2(config)# **spanning-tree vlan 200 root primary**

* 1. Configure Routing and HSRP on DLS1 and DLS2.

On the DLS switches, create the SVIs for VLANs 100 and 200 using the addresses specified in the topology diagram. Further, configure HSRP with preemption on all three networks. Configure DLS1 with a priority of 150 for VLAN 99 and 100, and DLS2 with a priority of 150 for VLAN 200. Configure this on DLS1 and DLS2. An example from DLS1 is below:

DLS1(config)# **ip routing**

DLS1(config)# **interface vlan 100**

DLS1(config-if)# **ip address 172.16.100.3 255.255.255.0**

DLS1(config-if)# **standby 100 ip 172.16.100.1**

DLS1(config-if)# **standby 100 priority 150**

DLS1(config-if)# **standby 100 preempt**

DLS1(config-if)# **exit**

DLS1(config)# **interface vlan 200**

DLS1(config-if)# **ip address 172.16.200.3 255.255.255.0**

DLS1(config-if)# **standby 200 ip 172.16.200.1**

DLS1(config-if)# **standby 200 preempt**

DLS1(config-if)# **exit**

DLS1(config)# **interface vlan 99**

DLS1(config-if)# **standby 99 ip 172.16.99.1**

DLS1(config-if)# **standby 99 priority 150**

DLS1(config-if)# **standby 99 preempt**

DLS1(config-if)# **exit**

Verify the configuration using the show vlan brief, show vtp status, show standby brief, and show ip route command on DLS1. Output from DLS1 is shown here.

DLS1# **show vlan brief**

VLAN Name Status Ports

---- ------------------------------ --------- -------------------------------

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/6, Fa0/13, Fa0/14

Fa0/15, Fa0/16, Fa0/17, Fa0/18

Fa0/19, Fa0/20, Fa0/21, Fa0/22

Fa0/23, Fa0/24, Gi0/1, Gi0/2

100 staff active

200 Student active

1002 fddi-default act/unsup

1003 trcrf-default act/unsup

1004 fddinet-default act/unsup

1005 trbrf-default act/unsup

How many VLANs are active in the VTP domain?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

DLS1# **show vtp status**

VTP Version capable : 1 to 3

VTP version running : 1

VTP Domain Name : SWLAB

VTP Pruning Mode : Disabled

VTP Traps Generation : Disabled

Device ID : e840.406f.7280

Configuration last modified by 0.0.0.0 at 8-3-15 14:56:12

Local updater ID is 172.16.99.3 on interface Vl99 (lowest numbered VLAN interface found)

Feature VLAN:

--------------

VTP Operating Mode : Server

Maximum VLANs supported locally : 1005

Number of existing VLANs : 9

Configuration Revision : 3

MD5 digest : 0xE2 0x62 0xBC 0xCE 0x16 0xF3 0xBC 0x0C

0x6D 0x84 0x63 0xF2 0x38 0x55 0xB9 0xB7

DLS1# **show standby brief**

P indicates configured to preempt.

|

Interface Grp Pri P State Active Standby Virtual IP

Vl99 99 150 Active local 172.16.99.4 172.16.99.1

Vl100 100 150 P Active local 172.16.100.4 172.16.100.1

Vl200 200 100 P Standby 172.16.200.4 local 172.16.200.1

What is the active router for VLANs 1 and 100? What is the active router for VLAN 200?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

DLS1# **show ip route | begin Gateway**

Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks

C 172.16.99.0/24 is directly connected, Vlan99

L 172.16.99.3/32 is directly connected, Vlan99

C 172.16.100.0/24 is directly connected, Vlan100

L 172.16.100.3/32 is directly connected, Vlan100

C 172.16.200.0/24 is directly connected, Vlan200

L 172.16.200.3/32 is directly connected, Vlan200

What would be the effect on virtual interface VLAN 100 if VLAN 100 had not been created?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Part 2: Implement Layer 2 network security features.

Specify verification methods and mitigation techniques for attack types.

Complete the following table with the appropriate verification methods and mitigation approaches for the attack types specified in the left column.

|  |  |  |
| --- | --- | --- |
| **Attack Type** | **Verification** | **Mitigation** |
| MAC address spoofing or flooding |  |  |
| DHCP spoofing |  |  |
| Unauthorized LAN access |  |  |

* 1. Storm Prevention

When packets flood the local area network, a traffic storm occurs. This could degrade network performance. Storm control features help to protect against such an attack. Storm control is typically implemented at the access layer switch ports to mitigate the effects of a traffic storm before propagating to the network. Storm control can also be implemented on trunk interfaces, including port-channel interfaces, to protect distribution-layer devices from traffic saturation, which could have a much broader impact on the network.

Storm control can detect and mitigate storms of broadcast, unicast, or multicast traffic. As a part of the configuration, you must specify what qualifies as a storm; either a rising and falling threshold based on the percentage of an interface's bandwidth used (the storm is recognized when X% of the interface bandwidth is used, and seen to be abated when Y% of the interface bandwidth is used), or based on rising and falling thresholds measured in either bits-per-second (bps) or packets-per-second (pps).

|  |  |  |  |
| --- | --- | --- | --- |
| **Storm Control Command Options** | | | |
| storm-control [unicast | broadcast | multicast ] level | 0-100  *Rising Threshold* | 0-100  *Falling Threshold* | ***Omitt Falling and Rising is the high/low mark*** |
| bps | 0-10,000,000,000 [k|m|g] *Rising Threshold* | 0-10,000,000,000 [k|m|g] *Falling Threshold* |
| pps | 0-10,000,000,000 [k|m|g] *Rising Threshold* | 0-10,000,000,000 [k|m|g] *Falling Threshold* |

To accurately configure these levels, you must know the amount of these traffic types flowing in your network during peak hours.

When a traffic storm is detected and storm control is configured, the default response is to silently filter the traffic. Storm control can optionally be configured to either shutdown the interface receiving the traffic storm or to send an SNMP trap to the NMS.

* + 1. Enable broadcast storm control on ports 0/6 and 0/15 - 0/24 on ALS1 with the parameters listed below. If any storm is detected, an SNMP trap will be sent.
       1. Unicast storms will be noted at 65% bandwidth usage, and abated at 35% bandwidth
       2. Broadcast storms will be noted at 1000 pps and abated at 300pps
       3. Multicast storms will be noted at 40% bandwidth usage and abated at 25% bandwidth

ALS1(config)# interface range FastEthernet 0/6, f0/15-24

ALS1(config-if-range)# storm-control unicast level 65 35

ALS1(config-if-range)# storm-control broadcast level pps 1k 300

ALS1(config-if-range)# storm-control multicast level 40 25

ALS1(config-if-range)# storm-control action trap

* + 1. Verify the configuration with the **show storm-control** command. The output below is showing the information for just f0/6; leaving the interface designation off would show configuration information for all storm-control configured interfaces.

ALS1# **show storm-control f0/6 unicast**

Interface Filter State Upper Lower Current

--------- ------------- ----------- ----------- ----------

Fa0/6 Forwarding 65.00% 35.00% 0.00%

ALS1# **show storm-control f0/6 broadcast**

Interface Filter State Upper Lower Current

--------- ------------- ----------- ----------- ----------

Fa0/6 Forwarding 1k pps 300 pps 0 pps

ALS1# **show storm-control f0/6 multicast**

Interface Filter State Upper Lower Current

--------- ------------- ----------- ----------- ----------

Fa0/6 Forwarding 40.00% 25.00% 0.00%

ALS1#

* 1. Demonstrate Storm Control Operation

To demonstrate the effects of storm control, configure unicast storm control on DLS1 interfaces F0/7 and F0/8 with purposely low numbers and then generate traffic from ALS1 that will cause the threshold to be exceeded.

* + 1. At DLS1, configure F0/7 and F0/8 with the following:

DLS1(config)#**int ran f0/7-8**

DLS1(config-if-range)#**storm-control unicast level bps 750 300**

DLS1(config-if-range)#**storm-control action shut**

DLS1(config-if-range)#**exit**

* + 1. At ALS1, issue the command **ping 172.16.99.3 repeat 1000.**
    2. Within a few seconds you will see a SYSLOG message on DLS1 indicating that a storm had been detected and the interfaces shut down.

Aug 3 15:44:38.333: %PM-4-ERR\_DISABLE: storm-control error detected on Fa0/7, putting Fa0/7 in err-disable state

Aug 3 15:44:38.358: %STORM\_CONTROL-3-SHUTDOWN: A packet storm was detected on Fa0/7. The interface has been disabled.

Aug 3 15:44:39.339: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down

Aug 3 15:44:40.363: %LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to down

Aug 3 15:45:09.572: %PM-4-ERR\_DISABLE: storm-control error detected on Fa0/8, putting Fa0/8 in err-disable state

Aug 3 15:45:09.597: %STORM\_CONTROL-3-SHUTDOWN: A packet storm was detected on Fa0/8. The interface has been disabled.

Aug 3 15:45:10.579: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to down

Aug 3 15:45:11.602: %LINK-3-UPDOWN: Interface FastEthernet0/8, changed state to down

* + 1. Reset the storm control configuration on DLS1 F0/7 and F0/8. Because the interfaces are now shutdown due to an ERR-DISABLE, you have to manually reset them by issuing the shutdown and no shutdown commands. While you do this, remove the storm control from the interfaces.

DLS1(config)#**int ran f0/7-8**

DLS1(config-if-range)#**shutdown**

DLS1(config-if-range)#**no storm-control unicast level bps 750 300**

DLS1(config-if-range)#**no storm-control action shut**

DLS1(config-if-range)#**no shutdown**

DLS1(config-if-range)#**exit**

* 1. Configure Basic Port Security.

To protect against MAC flooding or spoofing attacks, configure port security on the VLAN 100 and 200 access ports. Because the two VLANs serve different purposes—one for staff and one for students—configure the ports to meet the different requirements.

The student VLAN must allow MAC addresses assigned to a port to change, because most of the students use laptops and move around within the network. Set up port security so that only one MAC address is allowed on a port at a given time. This type of configuration does not work on ports that need to service IP phones with PCs attached or PC’s running virtual machines. In this case, there would be two allowed MAC addresses. To enable security on a port, you must first issue the switchport port-security command by itself.

The staff MAC addresses do not change often, because the staff uses desktop workstations provided by the IT department. In this case, you can configure the staff VLAN so that the MAC address learned on a port is added to the configuration on the switch as if the MAC address were configured using the switchport port-security mac-address command. This feature, which is called sticky learning, is available on some switch platforms. It combines the features of dynamically learned and statically configured addresses. The staff ports also allow for a maximum of two MAC addresses to be dynamically learned per port.

* + 1. Enter the configuration for the student access ports on ALS2. To enable basic port security, issue the switchport port-security command.

**Note**: By default, issuing the switchport port-security command by itself sets the maximum number of MAC addresses to 1**,** and the violation mode to shutdown. It is not necessary to specify the maximum number of addresses, unless it is greater than 1.

ALS2(config)# **interface range fastethernet 0/6, f0/15 - 24**

ALS2(config-if-range)# **switchport port-security**

* + 1. Verify the configuration for ALS2 using the show port-security interface command.

ALS2# **show port-security interface f0/6**

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 1

Total MAC Addresses : 1

Configured MAC Addresses : 0

Sticky MAC Addresses : 0

Last Source Address:Vlan : 000c.2911.a33a:200

Security Violation Count : 0

* 1. Configure Additional Port Security Parameters.
     1. Enter the configuration of the staff ports on ALS1. First, enable port security with the switchport port-security command. Use the switchport port-security maximum #\_of\_MAC\_addresses command to change the maximum number of MAC addresses to 2, and use the **switchport port-security mac-address sticky** command to allow the two dynamically learned addresses to be added to the running configuration.

ALS1(config)# **interface range fastethernet f0/6, f0/15 - 24**

ALS1(config-if-range)# **switchport port-security**

ALS1(config-if-range)# **switchport port-security maximum 2**

ALS1(config-if-range)# **switchport port-security mac-address sticky**

This time two MAC addresses are allowed. Both will be dynamically learned and then added to the running configuration.

* + 1. Verify the configuration using the show port-security interface command.

ALS1#**sho port-security int f0/6**

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 2

Total MAC Addresses : 1

Configured MAC Addresses : 0

Sticky MAC Addresses : 1

Last Source Address:Vlan : 000c.2915.ab9d:100

Security Violation Count : 0

* 1. Configure Error Disabled Port Automatic Recovery

Once a violation occurs on a port, the port will transition to an error disabled state. The only way to clear a port that has been error disabled is to perform a **shutdown** command and then a **no shutdown** on the interface. This method, of course, requires manual intervention by an administrator.

Error disabled ports can be configured to automatically recover from port security violations with the use of the **errdisable recovery cause** command. An interval can be configured so that after a specified time the port will automatically clear the violation.

The command to verify the error disable configuration is the **show errdisable recovery**.

Configure the switch to automatically recover an error disabled port caused from a port security violation. Notice there are many different options for which you can configure error disable recovery. However, we will configure it only for port-security violation.

ALS1(config)# **errdisable recovery cause ?**

all Enable timer to recover from all error causes

arp-inspection Enable timer to recover from arp inspection error

disable state

bpduguard Enable timer to recover from BPDU Guard error

channel-misconfig (STP) Enable timer to recover from channel misconfig error

dhcp-rate-limit Enable timer to recover from dhcp-rate-limit error

dtp-flap Enable timer to recover from dtp-flap error

gbic-invalid Enable timer to recover from invalid GBIC error

inline-power Enable timer to recover from inline-power error

link-flap Enable timer to recover from link-flap error

loopback Enable timer to recover from loopback error

mac-limit Enable timer to recover from mac limit disable state

pagp-flap Enable timer to recover from pagp-flap error

port-mode-failure Enable timer to recover from port mode change

failure

pppoe-ia-rate-limit Enable timer to recover from PPPoE IA rate-limit

error

psecure-violation Enable timer to recover from psecure violation error

psp Enable timer to recover from psp

security-violation Enable timer to recover from 802.1x violation error

sfp-config-mismatch Enable timer to recover from SFP config mismatch

error

small-frame Enable timer to recover from small frame error

storm-control Enable timer to recover from storm-control error

udld Enable timer to recover from udld error

vmps Enable timer to recover from vmps shutdown error

ALS1(config)# **errdisable recover cause psecure-violation**

Configure the recovery interval for 30 seconds. If no recovery interval is specified, the recovery time defaults to 300 seconds.

ALS1(config)# **errdisable recovery interval ?**

<30-86400> timer-interval (sec)

ALS1(config)# **errdisable recovery interval 30**

Use the **show errdisable recovery** command to view the configuration.

ALS1# **show errdisable recovery**

ErrDisable Reason Timer Status

----------------- --------------

arp-inspection Disabled

bpduguard Disabled

channel-misconfig (STP) Disabled

dhcp-rate-limit Disabled

dtp-flap Disabled

gbic-invalid Disabled

inline-power Disabled

link-flap Disabled

mac-limit Disabled

loopback Disabled

pagp-flap Disabled

port-mode-failure Disabled

pppoe-ia-rate-limit Disabled

psecure-violation Enabled

security-violation Disabled

sfp-config-mismatch Disabled

small-frame Disabled

storm-control Disabled

udld Disabled

vmps Disabled

psp Disabled

Timer interval: 30 seconds

Interfaces that will be enabled at the next timeout:

1. Configure IPv4 DHCP snooping

DHCP spoofing is a type of attack primarily where an unauthorized device assigns IP addressing and configuration information to hosts on the network.

IPv4 DHCP servers reply to DHCPDISCOVER frames. These frames are generally BROADCAST, which means they are seen all over the network. The attacker replies to a DHCP request, claiming to have valid gateway and DNS information. A valid DHCP server might also reply to the request, but if the attacker’s reply reaches the requestor first, the invalid information from the attacker is used. This can lead to a denial of service or traffic interception.

The process we will use to see this work is to first verify that the DHCP DISCOVER is broadcast everywhere, and then enable DHCP snooping to see this being stopped.

To do this, we will use Tftpd32's DHCP server function.

* 1. Verify DHCP Broadcast Operation

|  |  |
| --- | --- |
| On Host C, configure the DHCP server settings in Tftpd32 to support DHCP for VLAN 200. The screenshot details the settings: |  |

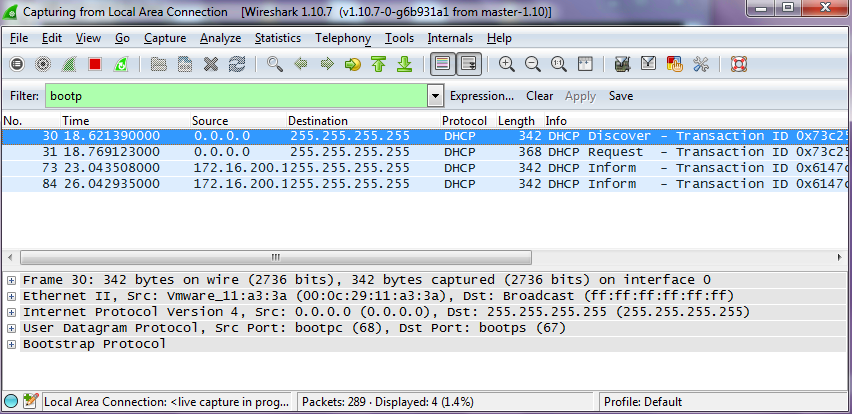
* + 1. On DLS1, issue the ip helper-address 172.16.99.50 command under interface VLAN 200.
    2. Reassign interface f0/6 on ALS1 to VLAN 200.
    3. On Host A, run Wireshark and have it collect on its ethernet interface. In the filter bar, type **bootp** and press enter (this filters the output to show only packets related to DHCP).



* + 1. On Host B, reconfigure the network interface to use DHCP. You should see that Host B receives an IP address and other DHCP information.

|  |
| --- |
| Ethernet adapter Local Area Connection:  Connection-specific DNS Suffix . : GOOD-DHCP.SRV  Link-local IPv6 Address . . . . . : fe80::b8ee:7ffd:e885:8423%10  IPv4 Address. . . . . . . . . . . : 172.16.200.150  Subnet Mask . . . . . . . . . . . : 255.255.255.0  Default Gateway . . . . . . . . . : 172.16.200.1 |

* + 1. Return to Host A and you should see the DHCP traffic in the capture window.



If Host A were an attacker, it could craft DHCP server OFFER messages or other DHCP sever messages to respond to Host B’ s DHCP request.

To help protect the network from such an attack, you can use DHCP snooping.

* 1. Configure DHCP Snooping

DHCP snooping is a Cisco Catalyst feature that determines which switch ports are allowed to respond to DHCP requests. Ports are identified as trusted or untrusted. Trusted ports permit all DHCP messages, while untrusted ports permit (ingress) DHCP requests only. Trusted ports can host a DHCP server or can be an uplink toward a DHCP server. If a rogue device on an untrusted port attempts to send a DHCP response packet into the network, the port is disabled. From a DHCP snooping perspective, untrusted access ports should not send any DHCP server responses, such as a DHCPOFFER, DHCPACK, or DHCPNAK.

Configuring DHCP Snooping on a single switch is very simple. There are additional considerations when configuring DHCP Snooping at the access layer of a multi-layer enterprise network. By default switches that pass DHCP requests on to another switch will insert option-82 information, which can be used for various management functions.

When a switch receives a DHCP frame that has option-82 information on an untrusted interface, the frame will be dropped. The **ip dhcp relay information trust-all** command is one way to work around this default behavior. It is not necessary to enable DHCP snooping on the distribution layer switches, although this would allow DLS1 and DLS2 to trust ALS1 and ALS2 as relay agents.

* + 1. Configure DLS1 and DLS2 to trust relayed DHCP requests (Option 82 preset with giaddr field equal to 0.0.0.0). Configure this on DLS1 and DLS2. An example from DLS1 is below:

DLS1(config)# **ip dhcp relay information trust-all**

* + 1. Configure ALS1 and ALS2 to trust DHCP information on the trunk ports only, and limit the rate that requests are received on the access ports. Configuring DHCP snooping on the access layer switches involves the following steps:
* Turn snooping on globally using the ip dhcp snooping command.
* Configure the trusted interfaces with the ip dhcp snooping trust command. By default, all ports are considered untrusted unless statically configured to be trusted. \* Very Important \* : The topology used for this lab is not using EtherChannels. Remember that when an EtherChannel created, the virtual port channel interface is used by the switch to pass traffic; the physical interfaces (and importantly their configuration) is not referenced by the switch. Therefore, if this topology was using EtherChannels, the **ip dhcp snooping trust** command would need to be applied to the Port Channel interfaces and not to the physical interfaces that make up the bundle.
* Configure a DHCP request rate limit on the user access ports to limit the number of DHCP requests that are allowed per second. This is configured using the ip dhcp snooping limit rate rate\_in\_pps. This command prevents DHCP starvation attacks by limiting the rate of the DHCP requests on untrusted ports.
* Configure the VLANs that will use DHCP snooping. In this scenario, DHCP snooping will be used on both the student and staff VLANs.

Configure this on ALS1 and ALS2. An example from ALS1 is below:

ALS1(config)# **ip dhcp snooping**

ALS1(config)# **interface range fastethernet 0/7 - 12**

ALS1(config-if-range)# **ip dhcp snooping trust**

ALS1(config-if-range)# **exit**

ALS1(config)# **interface range fastethernet 0/6, f0/15 - 24**

ALS1(config-if-range)# **ip dhcp snooping limit rate 20**

ALS1(config-if-range)# **exit**

ALS1(config)# **ip dhcp snooping vlan 100,200**

* + 1. Verify the configurations on ALS1 and ALS2 using the show ip dhcp snooping command.

ALS2# **show ip dhcp snooping**

Switch DHCP snooping is enabled

DHCP snooping is configured on following VLANs:

100,200

DHCP snooping is operational on following VLANs:

100,200

DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled

circuit-id default format: vlan-mod-port

remote-id: 5017.ff84.0a80 (MAC)

Option 82 on untrusted port is not allowed

Verification of hwaddr field is enabled

Verification of giaddr field is enabled

DHCP snooping trust/rate is configured on the following Interfaces:

Interface Trusted Allow option Rate limit (pps)

----------------------- ------- ------------ ----------------

FastEthernet0/6 no no 20

Custom circuit-ids:

FastEthernet0/7 yes yes unlimited

Custom circuit-ids:

FastEthernet0/8 yes yes unlimited

Custom circuit-ids:

Interface Trusted Allow option Rate limit (pps)

----------------------- ------- ------------ ----------------

FastEthernet0/9 yes yes unlimited

Custom circuit-ids:

FastEthernet0/10 yes yes unlimited

Custom circuit-ids:

FastEthernet0/11 yes yes unlimited

Custom circuit-ids:

FastEthernet0/12 yes yes unlimited

Custom circuit-ids:

<...OUTPUT OMITTED...>

* 1. Verify IPv4 DHCP Snooping Operation

To verify DHCP Snooping is working, re-run the test conducted to observe DHCP operation without DHCP snooping configured. Ensure WIRESHARK is still running on HOST\_A. Issue the ipconfig /renew command on HOST\_B. In this case, the DHCPDISCOVER should NOT be seen at HOST\_A.

Once validated, change ALS1 f0/6 back to VLAN 100 and make sure HOSTA and HOSTB have valid static IP addresses assigned.

Will DHCP replies be allowed to ingress access ports assigned to VLAN 200?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

How many DHCP packets will be allowed on Fast Ethernet 0/16 per second?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Configure AAA

AAA stands for Authentication, Authorization, and Accounting. The authentication portion of AAA is concerned with the user being positively identified. Authentication is configured by defining a list of authentication methods and applying that list to specific interfaces. If lists are not defined, a default list is used.

To demonstrate this we will use AAA to validate users attempting to log into the VTY lines of our network devices. The AAA server will be a radius server on Host C (172.16.99.50) connected to DLS1's F0/6 . There are many different radius server alternatives, but for this lab the program WinRadius is used.

* 1. Configure Switches to use AAA to secure VTY line access

As it stands, all of the switches should have a statically assigned password of cisco on the VTY lines. This is not a scalable configuration. It requires a single known password, and manual modification of each switch individually as well as controlled dissemination of that single known password. Using centralized authentication is a much simpler method, where each user uses their own unique username and password.

Ensure that Host C has connectivity to the gateway and all four switches.

Make the following configuration changes to all four switches:

* + 1. Issue the aaa new-model global configuration command to enable AAA

ALS1(config)# aaa new-model

* + 1. Configure a local user named lastditch with a privilege level of 15 and a password of $cisco123&

ALS1(config)# username lastditch privilege 15 password $cisco123&

* + 1. Configure the radius server to use authentication port 1812, accounting port 1813 and the shared key WinRadius

ALS1(config)# radius server RADIUS

ALS1(config-radius-server)# address ipv4 172.16.99.50 auth-port 1812 acct-port 1813

ALS1(config-radius-server)# key WinRadius

ALS1(config-radius-server)# exit

* + 1. Configure the AAA authentication method REMOTE-CONTROL to use the radius server and to fallback to the local database

ALS1(config)# aaa authentication login REMOTE-CONTROL group radius local

* + 1. Configure the VTY lines to use the REMOTE-CONTROL authentication method

ALS1(config)# line vty 0 4

ALS1(config-line)# login authentication REMOTE-CONTROL

ALS1(config-line)# exit

* 1. Configure WinRadius

Use the instructions in Appendix A to setup, test, and run WinRadius. As a part of the configuration, you should have the user account **remote** with the password **cisco123**.

* 1. Test centralized VTY line authentication

Now from a host on the network, attempt to telnet to one of the switches. You should be required to enter a username and password . Use the username of *remote* and the password of cisco123. Authentication should be successful.

* 1. End of Lab

Do not save your configurations. The equipment will be reset for the next lab.

**Appendix A—WinRadius Server Installation**

A WinRadius (or comparable) server should be installed on your host platform for this lab. If it is not, you can use the following procedure to download and install it. Check with your instructor if you have questions regarding the RADIUS server installation.

* 1. Download the WinRadius software.

A number of RADIUS servers are available, both freeware and for sale. This lab uses WinRadius, a freeware standards-based RADIUS server that runs on Windows 7 and most other Windows operating systems.

***Note:*** *The free version of the software can support only five usernames. These usernames are NOT retained over restarts, so try not to restart the PC for the duration of the lab!*

* 1. Install the WinRadius software.
     1. Create a folder named WinRadius on your desktop or other location in which to store the files.
     2. Search the web for **winradius** and download the latest version from a trusted website.

***Instructor note:*** *The instructions provided in this lab are for WinRadius 4.0. However, you can use another RADIUS server if one is available.*

* + 1. Save the downloaded zip file in the folder created in Step 2a, and extract the zipped files to the same folder. There is no installation setup. The extracted WinRadius.exe file is executable.
    2. Create a shortcut on your desktop for WinRadius.exe.
  1. Configure the WinRadius server database.
     1. Start the WinRadius.exe application. WinRadius uses a local database in which it stores user information. When the application is started for the first time, the following messages are displayed:

Please go to “Settings/Database and create the ODBC for your RADIUS database.

Launch ODBC failed.

* + 1. From the main menu, select **Settings > Database**.
    2. Click the **Configure ODBC automatically** button and then click **OK**. You should see a message that the ODBC was created successfully. Exit WinRadius and restart the application for the changes to take effect.
    3. When WinRadius starts again, you should see messages similar to the following:

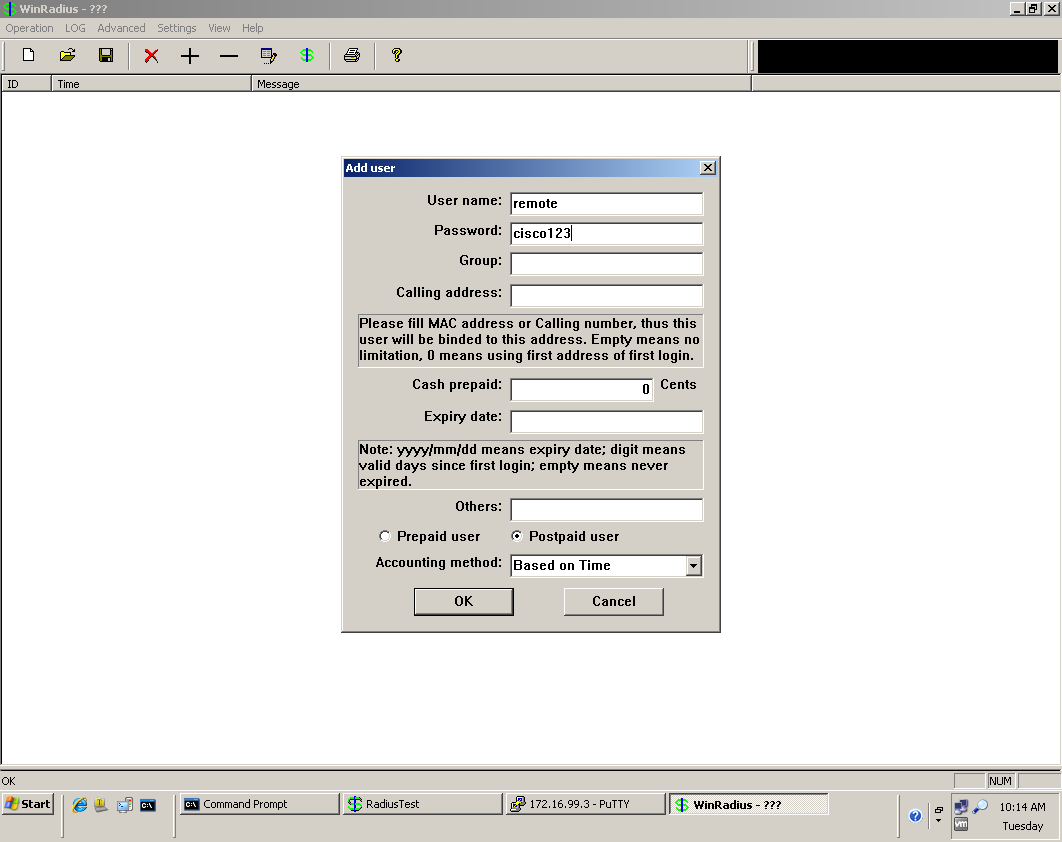


***Note:*** *WinRadius listens for authentication on port 1812 and accounting on port 1813.*

* 1. Configure users and passwords on the WinRadius server.

**Note:** The free version of WinRadius can support only five usernames at a time. The usernames are lost if you exit the application and restart it. Any usernames created in previous sessions must be recreated. The first message in the previous screen shows that zero users were loaded. No users had been created prior to this, but this message is displayed each time WinRadius is started, regardless of whether users were created or not.

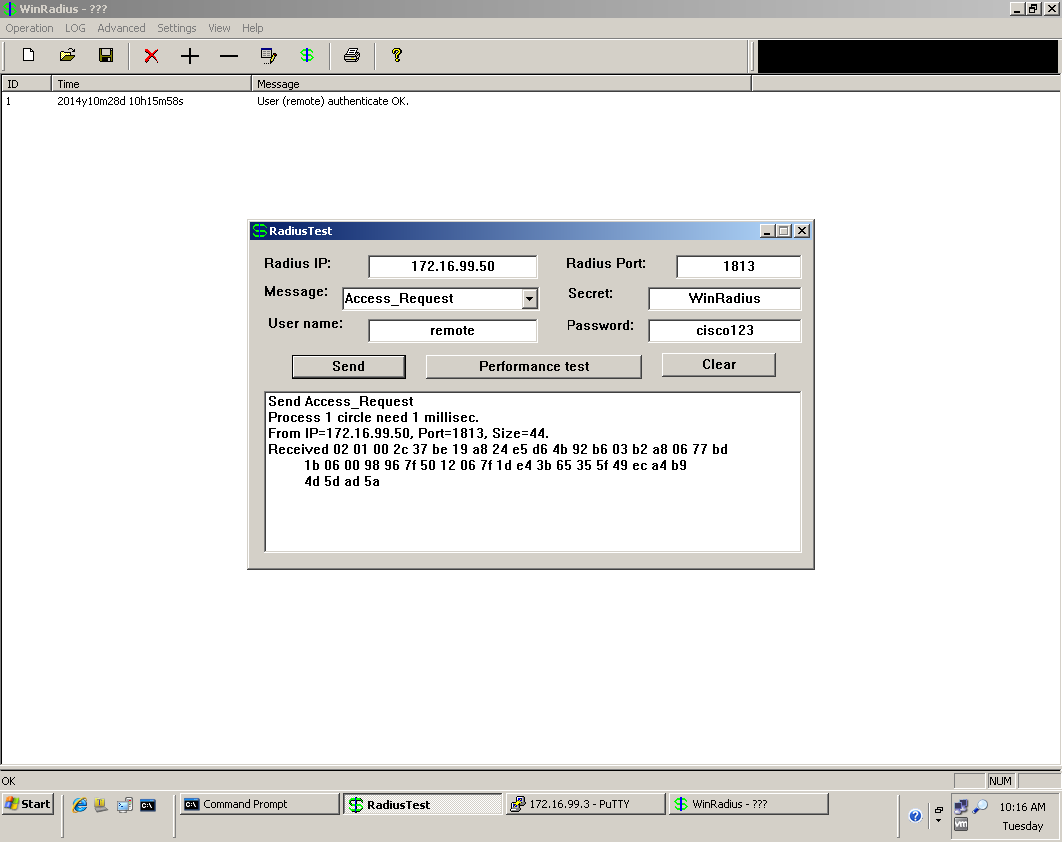
* + 1. From the main menu, select **Operation > Add User.**
    2. Enter the username **remote** with a password of **cisco123.**
    3. Click **OK**. You should see a message on the log screen that the user was added successfully.



* 1. Clear the log display.

From the main menu, select **Log > Clear**.

* 1. Test the new user added using the WinRadius test utility.
     1. a. A WinRadius testing utility is included in the downloaded zip file. Navigate to the folder where you unzipped the WinRadius.zip file and locate the file named RadiusTest.exe.
     2. b. Start the RadiusTest application, and enter the IP address of the RADIUS server. For this lab, the RADIUS server is SRV1, and the IP address is 172.16.99.50.
     3. c. Enter username **remote** and password cisco123. Do not change the default RADIUS port number of 1813 nor the RADIUS password of WinRadius.
     4. **Note:** Be sure to use the IP address of PC-C in this lab (172.16.99.50) when testing.
     5. d. Click **Send** and you should see a Send Access\_Request message indicating that the server at 172.16.99.50, port number 1813, received 44 hexadecimal characters. On the WinRadius log display, you should also see a message indicating that user *remote* was authenticated successfully.



* + 1. Close the WinRadius application.