

Authentication with 802.1x and EAP Across Congested WAN Links

Overview

Cisco has supported 802.1x authentication for 802.11 LANs since November 2000 with the introduction of the Lightweight Extensible Authentication Protocol (LEAP) algorithm. Cisco 802.1x/LEAP provides user-based, centralized authentication, as well as per-user wired equivalent privacy (WEP) session keys. Wireless LAN network administrators have been taking advantage of the simplified user and security administration that LEAP provides. Cisco support for 802.1x includes support for most EAP authentication types. With the introduction of Windows XP, Cisco supports the Transport Layer Security (TLS) EAP subtype, EAP-TLS, as well. As wireless LANs become more prevalent in enterprise networks, they are also extending into the enterprise branch office (Figure 1).

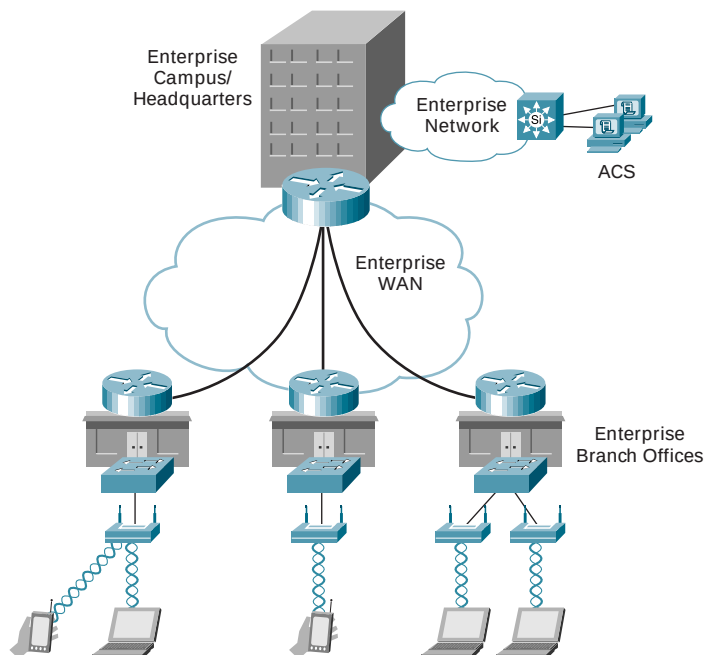
Cisco Aironet® deployments in the branch office may send authentication requests back to the authentication server (access control server [ACS] or Remote Access Dial-In User Service [RADIUS] server) across a WAN link. The 802.1x framework uses RADIUS messages for communications between the access point and the authentication server. RADIUS messages use User Datagram Protocol (UDP) and are connectionless, so it is possible during WAN link congestion for RADIUS packets to be delayed or dropped. This can cause delays or authentication timeouts to users attempting to authenticate to an access point, or when roaming to a different access point.

This issue is overcome by giving the RADIUS packets priority on transmissions both from the access point to the RADIUS server and from the RADIUS server to the access point. When priority is given to the RADIUS packets, the WAN routers service them before lower-priority traffic. The end result is that LEAP clients can authenticate successfully during times of WAN link congestion.

This document discusses the requirements and prerequisites for classifying and marking RADIUS packets using the Cisco Modular QoS Command Line (MQC), a methodology to determine the appropriate queue size for the 802.1x/RADIUS packets, and to determine how to enable queuing on router interfaces to provide priority for the RADIUS packets during network congestion. Although this paper is targeted for any 802.1x authentication type, Cisco LEAP is used in the examples. The methodology in prioritizing traffic can be applied to other algorithms as well.



Figure 1 Enterprise Branch Office



Prerequisites

- Router requirements—Refer to <http://cco/warp/public/732/Tech/qos/> for Cisco IOS® platform requirements
- Access point requirements—Minimum access point firmware of 11.06 for LEAP Draft 10, recommended 11.10T
- Client requirements—ACU 4.15.006, Drivers 6.97, and firmware of 4.25.10 (LEAP Draft 10), recommended ACU 5.01, Drivers 8.01.06, and firmware of 4.25.23

This document assumes that 802.1x authentication is already configured on the access point, client, and ACS.

For details on configuring LEAP, refer to: http://www.cisco.com/warp/customer/cc/pd/witc/ao350ap/prodlit/salep_an.htm

This document assumes a basic understanding of quality of service (QoS) and differentiated services (DiffServ) technology and techniques. For more information, refer to: http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iowft/prodlit/difse_wp.htm



Client Authentication Overview

This document focuses on prioritizing RADIUS packets from the access point to the RADIUS server and from the RADIUS server to the access point across congested WAN links. In order to provide the appropriate perspective on the authentication messages, this section reviews the 802.1x standard for the wireless authentication process.

Cisco LEAP, like many EAP variants used for wireless LAN authentication, is an authentication algorithm that utilizes the 802.1x authentication framework. The 802.1x standard is the messaging between a LEAP-enabled RADIUS server, 802.1x authenticator (the access point), and a LEAP-enabled client (the wireless station).

Understanding the 802.1x message flow provides the necessary insight into LEAP for the purposes of this paper.

Authentication with 802.1x

The client becomes active on the medium and associates to the access point. The access point detects the client association and enables the client's port. It forces the port into an unauthorized state, so only 802.1x traffic is forwarded. Traffic such as Dynamic Host Configuration Protocol (DHCP), Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Message Transfer Protocol (SMTP), Post Office Protocol 3 (POP3), and so on is blocked. The client can send an EAP-Start message, although client initiation is not required (Figure 2).

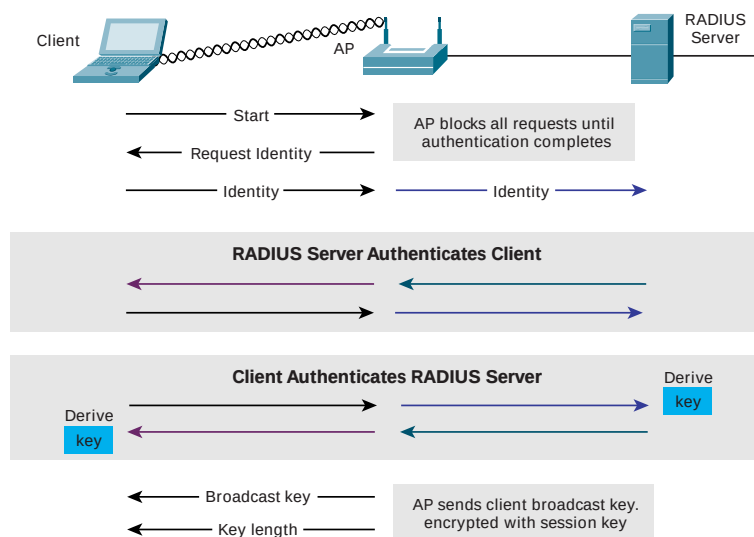
The access point replies with an EAP-Request Identity message back to the client to obtain the client's identity. The client's EAP-Response packet containing the client's identity is forwarded to the authentication server.

The authentication server is configured to authenticate clients with a specific authentication algorithm. Currently, 802.1x for 802.11 LANs does not stipulate a specific algorithm to use, but because we are focusing on LEAP, the assumption is that LEAP credential verification takes place.

The end result is an ACCEPT or REJECT packet from the authentication server to the access point.

Upon receiving the ACCEPT packet, the access point transitions the clients port to an authorized state, and traffic is forwarded.

Figure 2 Authentication Process with 802.1x

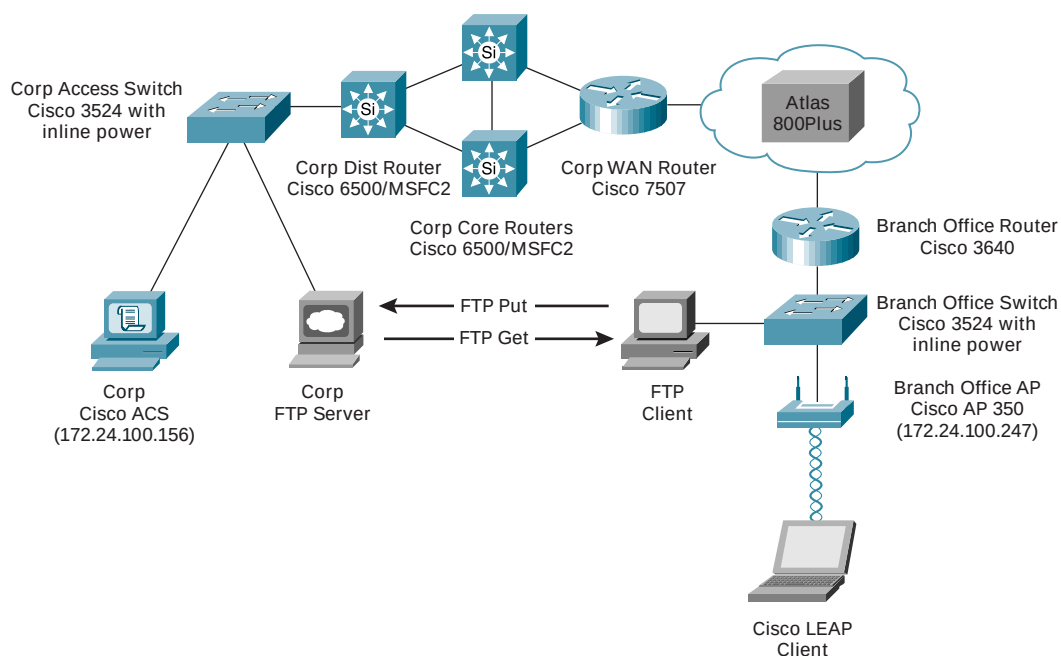




Lab Setup

Figure 3 shows the test network used to simulate the branch office connectivity to the central ACS.

Figure 3 Testbed Setup



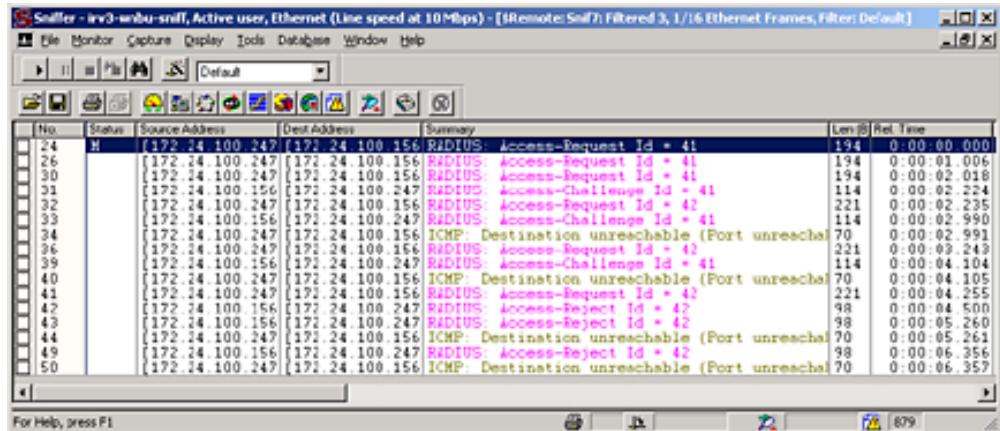
The WAN is simulated using an Adtran Atlas 800Plus WAN circuit emulator. A T1 is provisioned for use between the main WAN router and the branch office router. To simplify the testing, only one 64-kbps channel is enabled on the routers.

To generate the congestion, two FTP file transfers are initiated by a wired client on the branch office side of the network to a server on the other side of the WAN link. To saturate both directions of the link, one FTP is a PUT sending a large file to the server, while the other is a GET, receiving a large file from the server.

When the transfers are under way, the wireless client attempts to LEAP authenticate. With no QoS in place, the authentication will fail. A packet trace illustrates the failure (Figure 4):



Figure 4 Trace of LEAP Timeout



The access point, with IP address 172.24.100.247, is attempting to reach RADIUS server 172.24.100.156. The first Access-Request message (ID = 41) is received, and 172.24.100.156 responds back to the access point. The second Access-Request message (ID = 42) does not receive a response, so the access point issues an Internet Control Message Protocol (ICMP) destination unreachable message, indicating that the host is not responding.

Apply QoS to the 802.1x RADIUS Packets

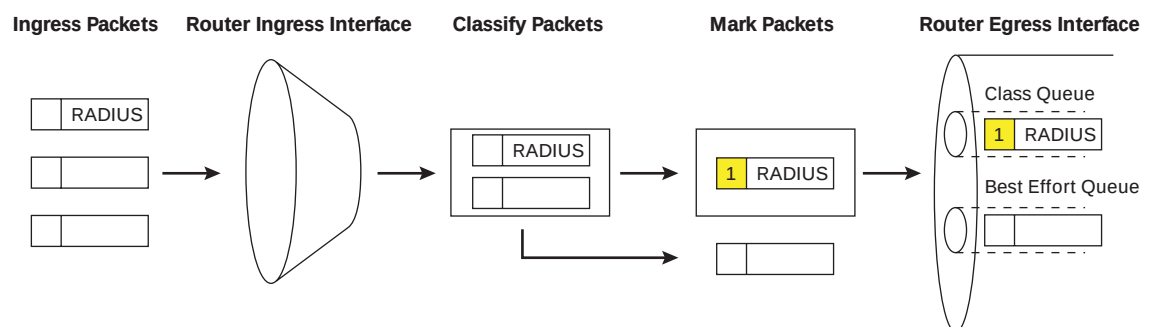
Because every network implementation is different, no QoS configuration will meet the needs of every implementation. This document assumes that no other traffic requires prioritization. In actual implementations, prioritizing 802.1x/LEAP RADIUS packets can be done while maintaining voice and video, or any other application priority.

To give LEAP RADIUS packets priority, three things must happen to the packets:

1. The packets are classified as they enter the router ingress interface.
2. The classified packets are marked with a differentiated service code point (DSCP) or IP Precedence value.
3. The classified packets are placed in a priority transmit queue.

Figure 5 shows the packet classification and marking process in the router.

Figure 5 Classification, Marking, and Queuing of Packets





Classify the LEAP RADIUS packets

Note: For full details on packet classification and marking, refer to: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt8/qcfmcli2.htm

To classify the packets, a simple ACL is needed to “catch” only RADIUS packets that are destined or sourced from the authentication server.

On the branch office router in our testbed, the following ACL was used:

```
ip access-list extended LEAP
  permit udp any host 172.24.100.156 eq 1645
```

The ACL permits UDP traffic from any source address to the destination address of 172.24.100.156 and a destination port of 1645 (the IP address and port of the ACS).

The ACL used on the main office router is slightly different:

```
ip access-list extended LEAP
  permit udp host 172.24.100.156 eq 1645 any
```

This main office router ACL permits any UDP traffic from host 172.24.100.156 where the source port is 1645 to any destination address.

Note: Refer to Appendix A for the full router configurations.

Note: In the testbed, the only RADIUS traffic is 802.1x/LEAP authentication messages. In an actual implementation, the RADIUS traffic may include non-LEAP messages, which would be incorrectly prioritized. If that happens, the ACL can be made more granular by including the IP addresses of the access points in the ACLs.

With the ACLs granular enough to catch the RADIUS packets, yet broad enough to scale to handle multiple access points, the next step is to create the classifications. This is accomplished using the class-map Cisco IOS command. The class-map command enables the router to use the ACL to classify the traffic.

The command as implemented on both the branch office and corporate WAN routers follows:

```
class-map match-any LEAP
  match access-group name LEAP
```

The commands create a class map called “LEAP” that classifies traffic that matches the access list named “LEAP.”

Classifying the traffic has made the router aware that the traffic is “interesting.” The traffic has no marking applied to it yet, nor has any queuing been configured to prioritize it with respect to normal traffic.

Mark the LEAP RADIUS Packets

Note: For full details on packet classification and marking, refer to: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt8/qcfmcli2.htm

Marking the LEAP RADIUS packets is the next step. Marking modifies the three type of service (ToS) bits (Figure 6) or six DSCP bits in the IP header (Figure 7). DSCP values are used in the testbed network, because DSCP is the latest and best classification and marking framework to date, although IP Precedence works as well.



Figure 6 IP Precedence in an IPv4 Header

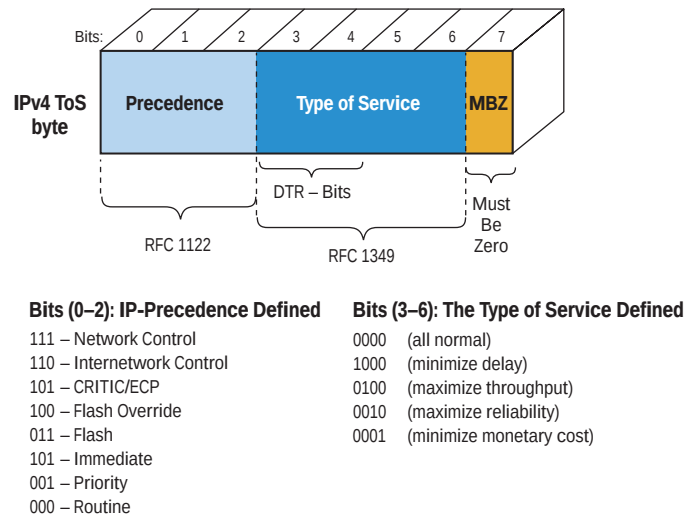
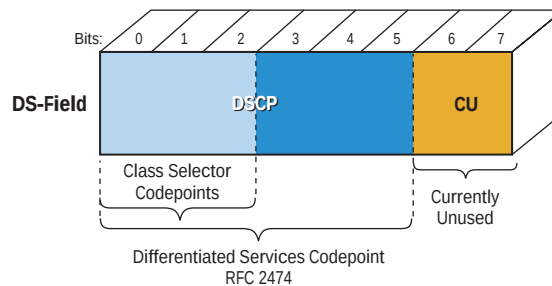


Figure 7 DSCP in an IPv4 Header



Standard 802.1x RADIUS packets are considered network control packets, so to maintain consistency with other Cisco products and standards, 802.1x RADIUS frames are marked as DSCP value AF31. For some perspective, the AF31 marking places 802.1x RADIUS frames in the same class as voice over IP (VoIP) call control packets.

The packets are marked using the policy-group Cisco IOS command. The policy-group command marks packets based on the classifications defined with the class-map command.

The command as implemented on both the branch office and corporate WAN routers follows:

```
class-map match-any LEAP
  match access-group name LEAP
!
policy-map mark
  class LEAP
    set ip dscp 26
```



The policy group called “mark” marks all LEAP classified traffic and sets the DSCP value in the packet to a DSCP 26 or AF31 (refer to http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iofwft/prodlit/difse_wp.htm for details on DSCP values).

To start marking packets, the policy-group mark needs to be applied to the ingress interface of the router. The service-policy Cisco IOS command applies a policy group to an interface.

```
interface FastEthernet0/0.100
 encapsulation dot1Q 100
 ip address 172.24.100.242 255.255.255.240
 ip helper-address 172.24.100.156
 service-policy input mark
 standby 100 ip 172.24.100.241
 standby 100 priority 105
 standby 100 preempt
```

The service-policy command is entered at the interface level; it specifies whether a configured policy group will analyze and mark inbound or outbound traffic. In the example above, policy-group “mark” is applied to FastEthernet0/0.100, and it classifies and marks inbound traffic.

Verify Classification and Marking

The LEAP RADIUS traffic is now classified and marked. The show policy-group interface Cisco IOS command is used to verify that LEAP RADIUS packets are being properly marked. The output is as follows:

```
irv3-wnbu-mmbo1#show policy-map interface f0/0.100
FastEthernet0/0.100
```

Service-policy input: mark

```
Class-map: LEAP(match-any)
  63 packets, 13641 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: access-group name LEAP
    63 packets, 13641 bytes
    5 minute rate 0 bps
  QoS Set
    ip dscp 26
  Packets marked 63
```

```
Class-map: class-default (match-any)
  6300 packets, 4011799 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any
irv3-wnbu-mmbo1#
```




The output of the EXEC command reveals that 63 packets have been classified since the last router reboot. The class map used to classify the traffic is called “LEAP,” and it matches traffic based on the ACL called “LEAP.”

The last line of output shows that 63 classified packets have been marked with a DSCP value of 26.

The 802.1x/LEAP RADIUS traffic is now classified and marked for priority. The traffic is still forwarded as normal traffic, so the last step is to prioritize the LEAP RADIUS traffic.

Determine Queuing Method and Queue Size

Before router configuration takes place, a few queuing decisions need to be made:

1. Is the 802.1x/LEAP traffic the only traffic that needs to be prioritized (voice traffic may be present and require QoS)?
2. What queuing algorithm will be used?
3. What is the minimum bandwidth guaranteed required for the priority queue?

This document provides a methodology for prioritizing LEAP RADIUS traffic. What is critical is how LEAP RADIUS traffic relates to other priority traffic (such as voice, video, or application-specific traffic) and normal traffic.

In our testbed, the only traffic that requires priority is LEAP RADIUS traffic. Because the possibility of voice existing on a WAN is high, 802.1x traffic is not placed in a strict priority queue (assuming the use of low-latency queuing [LLQ] or IP Real-Time Transport Protocol [RTP] Priority Queuing). Class-Based Weighted Fair Queuing (CBWFQ) is used, and 802.1x RADIUS packets are placed in a class queue with a bandwidth guarantee. Unclassified data packets are placed in the best-effort queue.

The size of the 802.1x transactions will vary by EAP type. In the LEAP example, the size of each RADIUS packet requires approximately 1.5 kb of bandwidth. These values will vary, based on username length, network access server name, and other variable fields. To maintain simplicity, the bandwidth requirement should be symmetric in both directions; the corporate WAN router queue matches the remote branch office router queue.

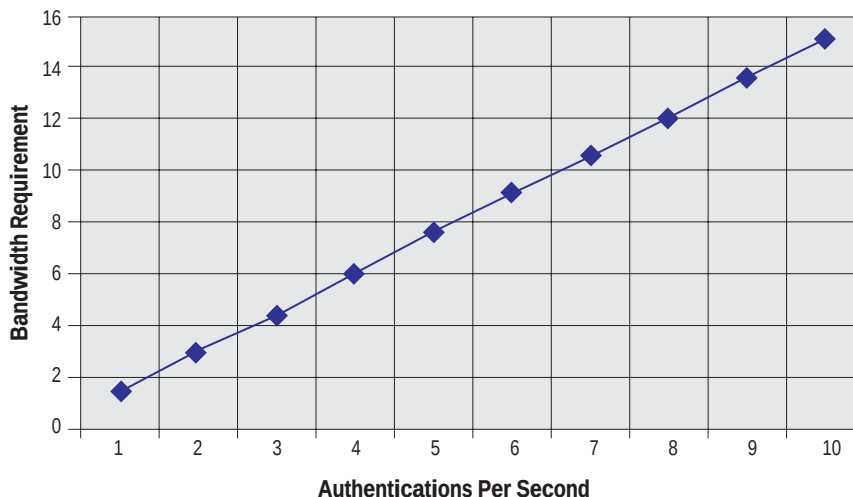
Given that the smallest bandwidth requirement configurable is 8 kb, approximately five authentications per second can be supported at any given time. The number of authentications per second in a wireless LAN depends on the number of users and the WEP key rekey interval.

Note: Refer to http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1515_pp.htm for information on how to determine optimal WEP rekey intervals.

An 8-kb queue can service up to five authentications per second and can scale to up 3000 users (at the rate of five authentications per second). As the number of authentications per second increases, the bandwidth requirement should increase (Figure 8).



Figure 8 Authentication Rate vs. Bandwidth Requirement



Prioritize 802.1x RADIUS Packets

Note: For full details on packet classification and marking, refer to: <http://www.cisco.com/warp/public/732/Tech/qos/techdoc/diffserv.shtml>

Prioritizing the LEAP RADIUS packets over normal traffic is the last step—it is also the most crucial step.

Placing the marked LEAP RADIUS packets into a prioritized queue and assigning a minimum bandwidth are accomplished with the same policy-group Cisco IOS command used to mark the classified packets. The configuration from the testbed follows:

```
policy-map queue
  class LEAP
    bandwidth 8
```

A policy map named “queue” is created. The policy map includes the bandwidth subcommand to specify the minimum bandwidth guarantee. Traffic classified from the class map “LEAP” is guaranteed a minimum bandwidth of 8 kbps on the link. This means that LEAP classified traffic is guaranteed up to 8 kbps of bandwidth, *if it needs it*. For example, if LEAP traffic requires only 3 kbps during network congestion, normal traffic will have full access to the remaining 5 kbps of traffic on the 64-kbps link.

Now that we have defined the queue and bandwidth guarantee for LEAP RADIUS packets, we apply the queuing to an interface. Using the service-policy command in the same manner used previously to mark traffic, the policy group “queue” is applied to the WAN interface. The following example illustrates the application of the command.

```
interface Serial3/0:0
  ip address 172.24.100.66 255.255.255.252
  load-interval 30
```



Service-Policy Output Queue

The service-policy command directs outbound packets on the link to conform to the policy group named “queue.” This is done on both WAN routers.

Verify LEAP RADIUS Priorities

To verify that the egress interface is giving the classified packets the correct priority, the show policy-group Cisco IOS command is used. The following is an example from the testbed:

```
irv3-wnbu-wan1#show policy-map interface s2/0/0:0
```

```
Serial2/0/0:0
```

```
service-policy output: queue
```

```
class-map: LEAP(match-all)
  20 packets, 2631 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  match: access-group LEAP
  queue size 0, queue limit 10
  packets output 20, packet drops 0
  tail/random drops 0, no buffer drops 0, other drops 0
  bandwidth: kbps 8, weight 62
```

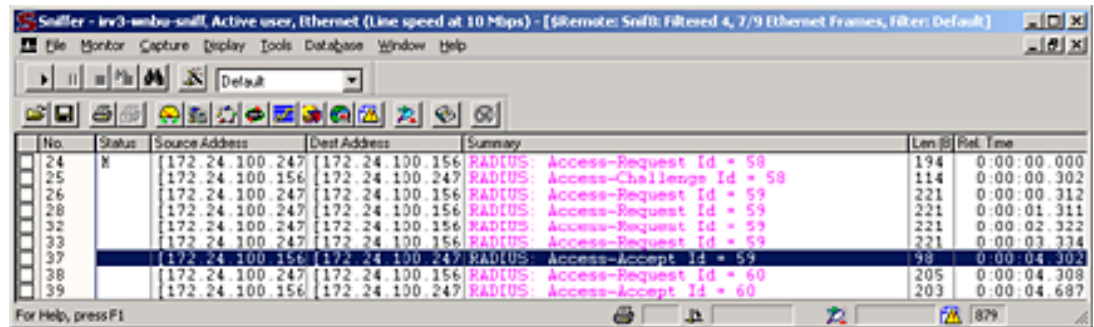
```
irv3-wnbu-wan1#
```

The output from the command reveals that 20 packets matched the ACL named “LEAP,” and those 20 packets were prioritized according to the settings in the policy group named “queue.” The 802.1x/LEAP RADIUS packets were successfully prioritized.

Referring back to the lab setup described earlier in Figure 3, the same congested WAN scenario is created, but this test has the QoS configuration in place. A sniffer trace of the RADIUS messages from the access point to the RADIUS server illustrates that the packet loss experienced without QoS is no longer an issue with QoS enabled. Figure 9 indicates that the access point with IP address 172.24.100.247 is successfully communicating with RADIUS server 172.24.100.156 with no packet loss.



Figure 9 Trace of LEAP Authentication with QoS Enabled



No.	Status	Source Address	Dest Address	Summary	Len	Rel. Time
24	M	172.24.100.247	172.24.100.156	RADIUS: Access-Request Id = 58	194	0:00:00.000
25		172.24.100.156	172.24.100.247	RADIUS: Access-Challenge Id = 58	114	0:00:00.302
26		172.24.100.247	172.24.100.156	RADIUS: Access-Request Id = 59	221	0:00:00.312
28		172.24.100.247	172.24.100.156	RADIUS: Access-Request Id = 59	221	0:00:01.311
32		172.24.100.247	172.24.100.156	RADIUS: Access-Request Id = 59	221	0:00:02.322
33		172.24.100.247	172.24.100.156	RADIUS: Access-Request Id = 59	221	0:00:03.334
37		172.24.100.156	172.24.100.247	RADIUS: Access-Accept Id = 59	98	0:00:04.302
38		172.24.100.247	172.24.100.156	RADIUS: Access-Request Id = 60	205	0:00:04.308
39		172.24.100.156	172.24.100.247	RADIUS: Access-Accept Id = 60	203	0:00:04.687

Providing End-to-End QoS for LEAP RADIUS Packets

Just as congestion can occur on a high-utilization WAN link, it can occur on LAN links as well. If necessary, the process for classifying and queuing high-priority traffic such as LEAP RADIUS packets can be done end to end from the first router hop from the access point to the last router before the ACS or RADIUS server. This requirement varies on a case-by-case basis, but the methodology for classifying, marking, and queuing packets is the same as that detailed for the WAN link in the testbed.

Scenarios for Local ACS or RADIUS Servers

This paper describes how to utilize Cisco MQC and robust QoS support to cost-effectively deploy secure wireless LANs to remote offices. The ACS server has a recommended limit of 40 authentications per second. It may be possible for a large number of remote users to place excessive strain on the ACS server, or possibly the WAN link. At some point, a local ACS server or dedicated ACS server for remote clients may be needed. The scenarios for this will vary on a case-by-case basis, but it is important not to discount the possibility of deploying a local or dedicated ACS server.



Appendix A: Testbed Router Configurations

Cisco 3640—Midmarket Branch Office Router

```
version 12.2
no parser cache
no service single-slot-reload-enable
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
service linenumber
!
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
ip rcmd rcp-enable
ip rcmd rsh-enable
!
!
ip domain-name cisco.com
ip name-server 171.70.168.183
ip name-server 171.68.226.120
!
ip cef
no ip dhcp-client network-discovery
!
class-map match-any LEAP
  match access-group name LEAP
!
!
policy-map mark
  class LEAP
    set ip dscp 36
policy-map queue
  class LEAP
    bandwidth 8
!
isdn switch-type basic-ni
call rsvp-sync
!
controller T1 3/0
```



```
framing esf
linecode b8zs
channel-group 0 timeslots 1 speed 64
!
controller T1 3/1
framing sf
linecode ami
!
interface FastEthernet0/0
ip address 172.24.100.225 255.255.255.248
duplex auto
speed auto
!
interface Serial3/0:0
ip address 172.24.100.66 255.255.255.252
load-interval 30
service-policy output queue
!
router ospf 500
log-adjacency-changes
network 172.24.100.64 0.0.0.3 area 1
network 172.24.100.88 0.0.0.3 area 1
!
ip classless
ip http server
!
ip access-list extended LEAP
permit udp any host 172.24.100.156 eq 1645
!
end
```



Cisco 7507—Corporate WAN Router

```
version 12.1
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
service linenumber
!
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
ip rcmd rcp-enable
ip rcmd rsh-enable
!
no ip finger
ip domain-name cisco.com
ip name-server 171.70.168.183
ip name-server 171.68.226.120
!
!
class-map match-all LEAP
  match access-group LEAP
!
!
policy-map mark
  class LEAP
    set ip dscp 36
policy-map queue
  class LEAP
    bandwidth 8
!
controller T1 2/0/0
  channel-group 0 timeslots 1
!
interface Serial2/0/0:0
  ip address 172.24.100.65 255.255.255.252
  no ip route-cache distributed
  service-policy output queue
!
router ospf 500
  log-adjacency-changes
```

```

network 172.24.100.48 0.0.0.3 area 0
network 172.24.100.52 0.0.0.3 area 0
network 172.24.100.64 0.0.0.3 area 1
network 172.24.100.88 0.0.0.3 area 1
!
ip classless

```

```

ip http server
ip ospf name-lookup
!
ip access-list extended LEAP
permit udp host 172.24.100.156 eq 1645 any
end

```



Corporate Headquarters
 Cisco Systems, Inc.
 170 West Tasman Drive
 San Jose, CA 95134-1706
 USA
www.cisco.com
 Tel: 408 526-4000
 800 553-NETS (6387)
 Fax: 408 526-4100

European Headquarters
 Cisco Systems Europe
 11, Rue Camille Desmoulins
 92782 Issy-les-Moulineaux
 Cedex 9
 France
www-europe.cisco.com
 Tel: 33 1 58 04 60 00
 Fax: 33 1 58 04 61 00

Americas Headquarters
 Cisco Systems, Inc.
 170 West Tasman Drive
 San Jose, CA 95134-1706
 USA
www.cisco.com
 Tel: 408 526-7660
 Fax: 408 527-0883

Asia Pacific Headquarters
 Cisco Systems, Inc.
 Capital Tower
 168 Robinson Road
 #22-01 to #29-01
 Singapore 068912
www.cisco.com
 Tel: 65 317 7777
 Fax: 65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
 Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
 Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
 Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
 Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Aironet, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0201R)