



Exam	CCIE – LABS - Cisco Certified Internetworking Expert
Title	Access Lists: Tricks of the Trade
Updated	01/03/2011
Product Type	Demo File = Become premium member to view complete file

Access Lists: Tricks of the Trade

Access lists are a general Cisco mechanism that allows you to be selective in the traffic you forward -- more selective than routing alone. They operate on individual packets, which distinguishes them from the new techniques of traffic engineering. Access lists (and their more powerful cousins, such as route maps) are designed to let you specify selective handling for certain traffic, beyond the rules established by traditional destination-based forwarding.

Access Lists Lab Scenario

Introduction

As network administrator for Galaxy One Inc., you are responsible for all routers and switches in the internetwork. The internetwork consists of four sites: Dallas, Tulsa, Las Vegas, and Phoenix. A drawing of the network is shown below. You must install all the network devices, configure them, and maintain them. It is also

your responsibility to maintain connectivity across the corporate WAN and properly secure the network. Securing the network is one task that never seems to end.

Much of the work involved in securing the network stems from the ever-changing threat from entities outside

your network, as well as the constantly changing political climate within your own organization. Now, management is at it again. They have decided that they are no longer satisfied with allowing full access to objects within the corporate network to all subjects within the internal organization. They have decided that certain objects should have controlled access, even for subjects that are known to be within the organization. Specifically, they have decided that the resources in the accounting department, located at the Las Vegas site,

should be off limits to all other organizations within the company, with the exception of the Time and Attendance application that every employee must access. Employees enter their timesheets electronically, and

this information is transferred across the network to a database server in the accounting department. The client/server application that handles this operates over TCP using port 2200. Accounting staff members that are

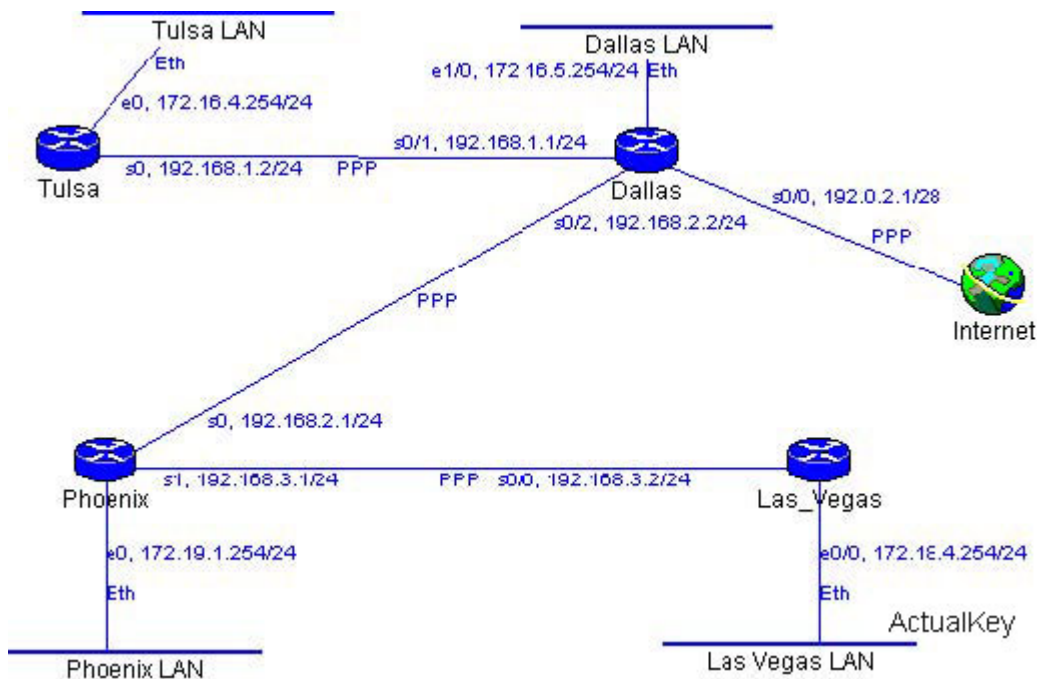
located outside Las Vegas, as well as system administrators, need full access to all of the resources in the Las

Vegas site. These users all reside on the 172.16.4.0/24 network in Tulsa.

You decide to take this opportunity to control access to the router terminal lines, as well, in order to ensure that

only designated administrators can gain remote access to the routers. You also want to implement a security measure that can prevent users from outside the organization from knowing that you have access control lists in place.

Network Diagram



Lab Objectives

1. Configure an access list to allow all users in the enterprise to access the Time and Attendance application on TCP port 2200.
2. Configure an access list to allow administrators full access to the Las Vegas site.
3. Configure an access list to restrict all other access to the Las Vegas site.
4. Configure access control for the terminal lines on all routers.
5. Configure an access list to prevent ICMP "administratively prohibited" messages from being sent to hosts outside the corporate network.

Solution

1. Configure an extended IP access list on the Las Vegas router. The list should contain the following entry to allow access to the Time and Attendance application:
 2. access-list 101 permit tcp any 172.16.4.0 0.0.0.255 eq 2200
 - 3.
 4. Add another entry to access list 101 on the Las Vegas router. The following entry will allow the administrators and accounting staff in Tulsa full access to the Las Vegas network:
 5. access-list 101 permit ip 172.16.4.0 0.0.0.255 any
 - 6.
 7. Without any additional entries, all other access to the Las Vegas site will be restricted by the implicit deny all at the end of access list 101. Apply this list as an incoming access control list on the Las Vegas router interface s0/0 using the following command:
 8. Las_Vegas(config-int)#ip access-group 101 in
 - 9.
 10. All administrators are located in Tulsa on network 172.16.4.0/24. Configure a Standard IP access list to allow access to the terminal lines only to that network:
 11. access-list 10 permit 172.16.4.0 0.0.0.255
 - 12.
- Apply this list to all terminal lines using the following commands on each router:
- Tulsa(config)#line vty 0 4

Tulsa(config-line)access-class 10 in

13. Create an Extended IP access list on the Dallas router that prevents ICMP "administratively prohibited" messages from being sent out over the connection to the Internet:

14. access-list 102 deny icmp any any 3 9

15. access-list 102 deny icmp any any 3 10

16. access-list 102 permit ip any any

17.

Apply access list 102 as an outbound access control list to the Dallas router interface s0/0 with the following command:

Dallas(config-int)#ip access-group 102 out

Dallas(config-int)#ip access-group 102 out