

Switched Network Services

User Manual Release 4.1



SwitchExpertSM Service Programs: An Alcatel service agreement brings your company the assurance of 7x24 no-excuses technical support. You'll also receive regular software updates to maintain and maximize your Alcatel product's features and functionality and on-site hardware replacement through our global network of highly qualified service delivery partners. Additionally, with 24-hour-a-day access to Alcatel's Service and Support web page, you'll be able to view and update any case (open or closed) that you have reported to Alcatel's technical support, open a new case or access helpful release notes, technical bulletins, and manuals. For more information on Alcatel's Service Programs, see our web page at www.ind.alcatel.com, call us at 1-800-995-2696, or email us at switchexpert@ind.alcatel.com.

**This Manual documents Release 4.1 Switched Network Services software.
This Manual is an addition to the 4.1 OmniSwitch and Omni Switch/Router User Manual.
The functionality described in this Manual is subject to change without notice.**

Copyright© 2000 by Alcatel Internetworking, Inc. All rights reserved. This document may not be reproduced in whole or in part without the express written permission of Alcatel Internetworking, Inc.

Alcatel® and the Alcatel logo are registered trademarks of Alcatel. Xylan®, OmniSwitch®, PizzaSwitch® and OmniStack® are registered trademarks of Alcatel Internetworking, Inc. X-Cell™, Omni Switch/Router™, PizzaPort™, X-Vision™, AutoTracker™, SwitchManager™, SwitchStart™, SwitchExpertSM, WebView™, X-WebVision™, PolicyView™ and the Xylan logo are trademarks of Alcatel Internetworking, Inc. All other brand and product names are trademarks of their respective companies.



26801 West Agoura Road
Calabasas, CA 91301
(818) 880-3500 FAX (818) 880-3505
info@ind.alcatel.com
US Customer Support-(800) 995-2696
International Customer Support-(818) 878-4507
Internet-<http://www.ind.alcatel.com>

Warning

This equipment has been tested and found to comply with the limits for Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions in this guide, may cause interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user will be required to correct the interference at his own expense.

The user is cautioned that changes and modifications made to the equipment without approval of the manufacturer could void the user's authority to operate this equipment. It is suggested that the user use only shielded and grounded cables to ensure compliance with FCC Rules.

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus out in the radio interference regulations of the Canadian department of communications.

Le present appareil numerique n'emet pas de bruits radioelectriques depassant les limites applicables aux appareils numeriques de la Class A prescrites dans le reglement sur le brouillage radioelectrique edicte par le ministere des communications du Canada.

Table of Contents

1 Authentication Services	1-1
Introduction	1-1
Components of an Authenticated Network	1-3
Configuration Overview	1-6
Application Example	1-8
Physical View	1-8
Logical Group View	1-9
How to Set Up this Network	1-10
Configuring Authenticated Groups	1-12
Creating an Authenticated Group	1-12
Modifying an Existing Group for Authentication	1-12
Specifying a Protocol	1-12
Viewing Current Authenticated Groups	1-13
Modifying an Authenticated Group	1-13
User Authentication UI Commands	1-15
Security Menu Commands	1-15
Managing Authentication Clients	1-17
Creating the Authentication Client Banner	1-17
Viewing the Current Authentication Client Banner	1-18
Configuring Authenticated Ports	1-18
Viewing Current Authenticated Ports	1-18
Installing AV-Clients	1-19
Loading the Microsoft DLC Protocol Stack	1-19
Windows 95 Stations	1-19
Windows 98 and Windows NT Stations	1-20
Loading AV-Client Software	1-21
Using the AV-Client Configuration Utility	1-24
Enabling/disabling the AV-Client at Startup	1-24
Configuring AV-Client DHCP Parameters	1-25
Logging Into the Network Through an AV-Client	1-26
Setting Up Telnet Clients	1-27
Defining Telnet Authentication Addresses	1-27
Viewing Current Telnet Authentication Addresses	1-27
Configuring an Authentication Host Name	1-28
Disabling an Authentication Host Name	1-28
Viewing the Current Authentication Host Name	1-28
Setting a Web Path Restriction	1-29
Viewing a Web Path Restriction	1-29

Logging Into the Network Through a Telnet Client	1-30
Authentication Clients and DHCP	1-31
AV-Client and DHCP	1-31
Telnet Client and DHCP	1-31
BOOTP Relay for Telnet Authentication	1-32
Viewing the Current Status of the BOOTP Relay	1-32
Configuring AMC Authentication	1-33
Disabling AMC Authentication	1-36
Moving an Authenticated Client Back to the Default Group	1-36
Troubleshooting Instructions	1-37
2 RADIUS Authentication	2-1
RADIUS Server Attributes	2-1
General Attributes	2-1
Vendor Specific Attributes (VSAs)	2-3
RADIUS Accounting Server Attributes	2-4
Enabling RADIUS Authentication	2-5
RADIUS Authentication UI	2-6
Configuring the Authority Mode	2-7
Viewing the Current Mode	2-9
Changing the Authority Mode	2-9
Adding RADIUS Servers	2-9
Adding a RADIUS Server in Single Authority Mode	2-9
Adding a RADIUS Server in Multiple Authority Mode	2-10
Displaying the Authority Chain	2-12
Removing RADIUS Servers from a Chain	2-13
Removing a Server in Single Authority Mode	2-13
Removing a Server in Multiple Authority Mode	2-13
Modifying the RADIUS Configuration	2-14
Configuring RADIUS Agent Prompts/Messages	2-14
Displaying the Current Prompts/Messages	2-15
Setting the Timeout for Authentication Attempts	2-15
Displaying the Current Timeout for Authentication Attempts	2-15
Setting the Number of Retries	2-15
Displaying the Number of Retries	2-16
Setting the Timeout for Replies	2-16
Displaying the Timeout for Replies	2-16
Removing a User from an Authenticated Group	2-16
Displaying the Authentication Version	2-16
RADIUS Accounting	2-17
Deleting a RADIUS Accounting Server	2-18
Displaying RADIUS Accounting Servers	2-19

3	LDAP Authentication	3-1
	Introduction	3-1
	General Assumptions and Recommendations	3-1
	Authentication Network Services Overview	3-3
	Authentication Clients	3-3
	Authentication Agent	3-4
	Authentication Servers	3-4
	Modes of Operation for Authentication Services	3-4
	Configuring the Authority Mode	3-4
	Single Authority Mode	3-5
	Multiple Authority Mode	3-6
	Logging and Accounting Features	3-7
	Directory Server Schema for LDAP Authentication	3-9
	Password Policies and Directory Servers	3-9
	Schema Extensions for LDAP Authentication	3-10
	Unique User Identifiers	3-10
	Schema Extensions by Directory Service	3-11
	Enabling LDAP Authentication	3-12
	LDAP Authentication UI Commands	3-13
	Authentication Mode and Prompts	3-14
	Viewing the Current Mode	3-14
	Changing the Authority Mode	3-14
	Configuring Directory Servers	3-14
	Configuring Host Client Prompts/Messages	3-14
	Displaying the Current Prompts/Messages	3-15
	Setting the Timeout for User Authentication Attempts	3-15
	Displaying the Current Timeout for User Authentication Attempts	3-15
	Adding, Viewing and Removing Directory Servers	3-16
	Adding Directory Servers (Single or Multiple Authority Mode)	3-16
	Viewing the Server Authority Chain (Single or Multiple Authority Mode)	3-18
	Displaying the Authentication Version	3-18
4	IP FireWall	4-1
	Introduction	4-1
	Components of the IP Firewall	4-1
	Configuration Overview	4-3
	Interaction with Authentication Services	4-3
	Firewall and the HRE or HRE-X	4-3
	Firewall Software	4-4
	Installing the Firewall Software	4-4
	Configuring the Firewall Software	4-5
	Disabling the Firewall	4-9
	Troubleshooting Instructions	4-10
	EMC Licensing Issues	4-10

EMC Registration Issues	4-10
EMC Setup and Configuration Issues	4-11
Unsupported Features of FireWall-1	4-14
5 The QoS Manager	5-1
QoS Overview	5-1
QoS and WAN Switching Modules (WSMs)	5-2
QoS Manager Overview	5-2
QoS Policy Decision	5-2
Provisioned and RSVP Traffic	5-3
Traffic Parameters for Provisioned Flows	5-4
QoS Policy Enforcement	5-4
Hardware/Software Requirements	5-5
Installing the QoS Manager	5-5
Configuring QoS	5-6
QoS Configuration Example	5-8
QoS Manager UI Commands	5-9
Modifying QoS Manager Parameters	5-10
Viewing QoS Manager Statistics	5-11
Configuring QoS Actions	5-12
Adding a New Action	5-14
Modifying an Action	5-14
Deleting an Action	5-14
Displaying QoS Actions	5-15
Configuring QoS Conditions	5-16
Adding a Condition	5-18
Modifying a Condition	5-19
Deleting a Condition	5-19
Displaying QoS Conditions	5-20
Mapper Submenu	5-21
Viewing Mapper Ports	5-21
Viewing Mapper Virtual Ports	5-22
Viewing Active Mapper Ports	5-22
Viewing Mapper Queues	5-23
Viewing Mapper Groups	5-24
6 Policy Manager	6-1
Introduction	6-1
Policy Manager General Description	6-1
Relationship between the QoS Manager and the Policy Manager	6-1
Policies and QoS	6-2
Policy Manager Operations	6-3
How the Policy Manager Works with the QoS Manager	6-3
Policy Manager Decisions	6-4

Policy Manager QoS Operations with LDAP	6-6
Traffic Flows and Policy Messages	6-7
RSVP Policy Messages for QoS Bandwidth Reservations	6-7
RSVP and the Policy Manager	6-8
Provisioned Notifications	6-9
Components of the QoS Policy Manager	6-10
Policy Manager Component Setup	6-11
Policy Manager Installation	6-12
PolicyView	6-16
PolicyView Menus	6-16
Using PolicyView to Create and Assign Policies	6-16
User Interface (UI) Commands	6-18
LDAP Configuration	6-18
LDAP Submenu	6-18
Displaying a List of Defined LDAP-enabled Servers	6-18
Displaying and Modifying a List of Parameters for LDAP-enabled Servers	6-20
Removing LDAP-enabled Server from Server List	6-22
Flushing Cached LDAP Data from the Switch	6-22
Manually Loading Policy Rules Set through PolicyView	6-22
Displaying Cached Policies	6-23
Monitoring General Performance	6-23
Policy Manager Configuration	6-24
Policy Submenu	6-24
Displaying a List of Policy-Based Flows	6-24
Defining RSVP Default Policy	6-24
Displaying a list of Provisioned QoS Default Policies	6-25
Assigning a Provisioned QoS Default Policy a Group ID	6-25
Deleting a Provisioned QoS Default Policy by Group ID	6-26
Showing Policy Events	6-26
7 Resource Reservation Protocol (RSVP)	7-1
Introduction	7-1
Path Messages and Reservations	7-1
Relationship to QoS Manager	7-2
Policies for RSVP	7-2
Software/Hardware Requirements	7-3
Installing RSVP	7-3
RSVP Configuration Overview	7-4
RSVP UI Commands	7-5
Displaying RSVP Sessions	7-5

8	IP Control	8-1
	Introduction	8-1
	How IP Control Works	8-1
	What is Communicated	8-3
	Components of the IP Control Feature	8-4
	IP Control Component Setup	8-5
	Pre-Installation Hardware Considerations	8-5
	IP Control Installation	8-5
	IP Control Menu Options	8-10
	User Interface (UI) Commands	8-12
	DHCP and DNS Server Configuration	8-12
	System Time Configuration for IP Control	8-14
	Component Descriptions	8-15
	IP Control Management Application	8-15
	LDAP (Lightweight Directory Access Protocol)	8-16
	LDAP Protocol Description	8-16
	LDAP Client	8-16
	LDAP-Enabled Directory Server	8-16
	LDAP Operations	8-20
	LDAP Sessions	8-20
	LDAP-Enabled Directory Searches	8-21
	LDAP-Enabled Directory Modifications	8-22
	Directory Compare and Sort	8-22
	The LDAP URL	8-22
	DHCP (Dynamic Host Configuration Protocol) and LDAP	8-24
	DHCP Protocol Description	8-24
	DHCP Server	8-24
	DHCP Configuration	8-24
	DNS (Domain Name System) and LDAP	8-26
	DNS Protocol Description	8-26
	DNS Server	8-26
	DNS Configuration	8-26
	Index	I-1