



Technology Brief:

LDAP User Authentication

What it Means to You:

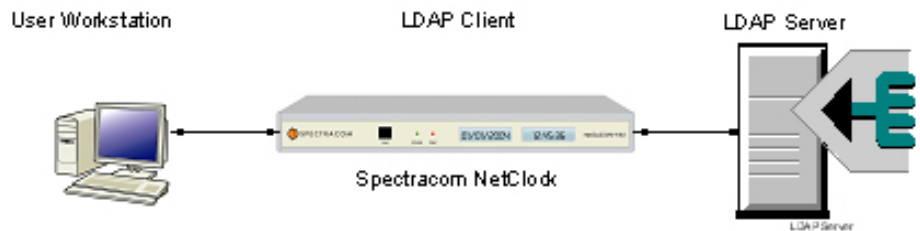
- Supports enterprise directory server
- Centralized user authentication and administration improves network management, regulatory compliance, and security

Why LDAP?

- Perhaps best known for its use with Windows Active Directory, LDAP also supports Linux.
- LDAP allows standards-based centralized authentication of users.
- LDAP is a connection-oriented, message-based protocol developed to support email directories on the Internet.
- Using LDAP improves IT security practices compared to administering passwords on each target system.

Introduction

Authentication of network device users is increasingly important to support IT security and regulatory compliance. Spectracom's products support up to 16 local user accounts and can, as a standard feature, also centrally authenticate to enterprise directory servers via Lightweight Directory Access Protocol (LDAP).



How Does NetClock Support LDAP?

- LDAP v3 (RFC 3377) or LDAP v2 (RFC 1777), both for Active Directory or openLDAP
- Simple authentication with or without SSL.
- User ID login stored in NetClock unit; password checked in LDAP server
- LDAP over SSL – LDAPS – TCP Port 636
- LDAP over TLS (RFC 2246), encrypted or non-encrypted
- Pluggable Authentication Module (PAM)-based interface
- Binding to directory server with or without credentials
- NetClock products support up to 5 LDAP servers (one master directory server and four replication directory servers – all on the same directory system)
- Login events are logged in the Auth Log; user activity is logged in the Journal Log

Applicable Products

- NetClock 9200 and 9300 Series
- SecureSync