

## Implementazione 802.1X

*Prevenzione dei conflitti di autenticazione 802.1X nelle reti cablate*

Grazie ai vantaggi che offre riguardo la sicurezza, il protocollo di autenticazione 802.1X è stato ampiamente implementato nell'ambiente wireless per molti anni. Supporta gli amministratori di rete nel mantenere la sicurezza garantendo o negando l'accesso ai servizi di rete in base a credenziali del client. Poiché l'esigenza di sicurezza è aumentata anche sulle reti cablate, gli amministratori stanno adottando sempre più la tecnologia 802.1X nelle reti di quel tipo, assegnando credenziali e fornendo autenticazione alle diverse periferiche collegate alle porte LAN.

La modifica della rete per fornire un livello di sicurezza 802.1X sulle porte non è di poco conto. 802.1X richiede che i dispositivi inviino le informazioni di autenticazione a un server RADIUS tramite un "richiedente" con credenziali appropriate per poter accedere alla rete. Per evitare problemi di connettività dovuti a conflitti 802.1X, è importante convalidare l'autenticazione prima di installare nuovi dispositivi. I nuovi strumenti di rete portatili con supporto 802.1X possono essere d'aiuto in questa convalida. Di seguito sono elencate alcune semplici procedure da seguire:

### 1: Configurazione del richiedente 802.1x

Individuare le porte nella rete dove le nuove macchine o i nuovi dispositivi devono essere aggiunti, spostati o modificati. Collegare il tester direttamente alla porta da convalidare e stabilire un collegamento di rete. Nella maggior parte delle implementazioni 802.1X, lo switch invia una query di autenticazione allo strumento richiedendone l'autenticazione nella rete. Lo strumento visualizza se questa comunicazione iniziale tramite il processo 802.1X è riuscita o meno. Se lo strumento non è riuscito a completare il processo di autenticazione 802.1X,

verificare per prima cosa la configurazione dello switch. Quindi controllare le credenziali configurate sullo strumento. Potrebbero essere state immesse in modo scorretto. Infine, controllare il server RADIUS per assicurarsi che lo strumento invii la richiesta di autenticazione utilizzando le credenziali esistenti.

### 2: Connessione alla rete e autenticazione

Individuare le porte nella rete dove le nuove macchine o i nuovi dispositivi devono essere aggiunti, spostati o modificati. Collegare il tester direttamente alla porta da convalidare e stabilire un collegamento di rete. Nella maggior parte delle implementazioni 802.1X, lo switch invia una query di autenticazione allo strumento richiedendone l'autenticazione nella rete. Lo strumento visualizza se questa comunicazione iniziale tramite il processo 802.1X è riuscita o meno. Se lo strumento non è riuscito a completare il processo di autenticazione 802.1X, verificare per prima cosa la configurazione dello switch. Quindi controllare le credenziali configurate sullo strumento. Potrebbero essere state immesse in modo scorretto. Infine, controllare il server RADIUS per assicurarsi che lo strumento invii la richiesta di autenticazione utilizzando le credenziali esistenti.

### 3: Richiesta di un indirizzo DHCP e Contact Key Services

Una volta che lo strumento è stato autenticato e connesso in modo appropriato utilizzando il client 802.1X, utilizzarlo per richiedere un indirizzo nella rete alla quale ora ha accesso. È quindi possibile configurare la porta dello switch per qualsiasi delle diverse VLAN. Controllare l'indirizzo concesso allo strumento, verificando che si trovi nella sottorete appropriata per le credenziali indicate durante il processo di



# AREA CULTURALE

# Cabling

autenticazione. Quindi effettuare il ping dei servizi chiave sulla rete per controllare che siano accessibili da quella posizione con quell'indirizzo. Verificare il collegamento ai server di applicazioni, e-mail e DNS. Uno

strumento con software adeguato consente di risparmiare tempo e semplificare le procedure durante la configurazione di servizi, dispositivi o URL multipli.



IntelliTone Pro



MicroScanner<sup>2</sup>



LinkRunner Pro



CableIQ



NetTool Series II

Implementazione 802.1X	Discreto	Discreto	Scelta ottimale 	Discreto	Discreto
<b>Risoluzione dei problemi sui cavi</b>					
Mappatura/lunghezza cavo	●	●	●	●	●
Distanza da Interruzioni o cortocircuiti	●	●	●	●	●
Individuare guasti crosstalk	●	●	●	●	●
Individuare guasti a livello di Impedenza	●	●	●	●	●
<b>Risoluzione dei problemi di collegamento</b>					
Velocità dispositivo (fino a Gig)	●	●	●	●	●
Collegamenti a 10/100/Gig	●	●	●	●	●
Richiedi l'indirizzo IP	●	●	DHCP/Manuale	●	DHCP/Manuale
Ping dei dispositivi chiave	●	●	●	●	●
Identificazione sottorete	●	●	●	●	●
CDP/EDP/LLDP	●	●	●	●	●
Coppie/voltaggio PoE	●	●	●	●	●
<b>Configurazione sicurezza</b>					
Autenticazione con 802.1x	●	●	●	●	●
Selezione tipo EAP	●	●	●	●	●
Immissione certificati/password	●	●	●	●	●
<b>Documentazione del test</b>					
Software di creazione report	●	●	●	●	●

Last Modified: 4/20/07

