Einrichtung der IP-Adresse des Xerox Secure Access Unified ID System®

Weißbuch

Version 1.5, Juni 2009

Inhalt

Einrichtung der IP-Adresse des Xerox Secure Access Unified ID System

Inhalt dieses Kapitels:

1. Zielsetzung

Das hier vorgestellte Verfahren ist eine Zusammenfassung des bootp-Prozesses an einem für Modus 2 (Office-Umgebung) konfigurierten Terminal. Zur einwandfreien Kommunikation zwischen Authentifizierungsgeräten und DCE-Server ist eine ordnungsgemäße IP-Adressvergabe erforderlich.

2. Allgemeiner Startvorgang

Zur Kommunikation zwischen XSA-Authentifizierungsgerät und DCE-Server sind folgende Netzwerkdaten erforderlich:

1. IP-Adresse des Authentifizierungsgeräts
2. IP-Adresse des DCE-Servers
3. Subnetzmaske
4. Standardgateway

Die IP-Adresse der Authentifizierungsgeräte kann auf zweierlei Weise konfiguriert werden:

1. Eingabe statischer IP-Adressen
2. Verwendung von DHCP

Bei Verwendung statischer IP-Adressen werden diese und sämtliche künftigen Änderungen im EEPROM gespeichert. Bei Verwendung von DHCP ist dies nicht der Fall. Dies muss berücksichtigt werden, da Authentifizierungsgeräte im DHCP-Modus unter bestimmten Bedingungen Werte aus dem EEPROM verwenden.

XSA-Modus - Web-Admin-Seite

Die im EEPROM gespeicherten Werte können sowohl bei Verwendung statischer Adressen als auch von DHCP über die Admin-Seite des Authentifizierungsgeräts vorgegeben werden. Im DHCP-Modus werden IP-Adresse, Subnetzmaske und Gateway unabhängig vom spezifizierten Modus nicht gespeichert. Die Serveradresse wird immer gespeichert.

XSA-Authentifizierungsgerät konfigurieren	
Adressvergabe	Static IP
IP-Adresse	192.168.92.88
Subnetzmaske	255.255.255.000
Gateway	192.168.092.001
HID-Entschlüsselung	☐

Server einrichten	
Server-IP-Adresse	192.168.092.045

3. Statische IP-Adressen

Dies ist die einfachste Methode. Die in Abschnitt 2 angegebenen IP-Adressen werden manuell in den Authentifizierungsgeräten eingegeben. Danach werden die Werte im EEPROM gespeichert und treten bei späteren Geräteneustarts in Kraft. Informationen zum Gerätestart sind Abschnitt 6 zu entnehmen.

4. DHCP

Die Vergabe statischer IP-Adressen ist zwar relativ unkompliziert, nimmt jedoch, wenn zahlreiche Authentifizierungsgeräte verwendet werden, viel Zeit in Anspruch.

In diesem Fall kann DHCP zur dynamischen Vergabe von IP-Adressen, Subnetzmaske und Standardgateway eingesetzt werden. Zudem kann die Adresse des DCE-Servers, sofern sie auf dem DHCP-Server eingerichtet ist, verwendet werden (s. Option 230 weiter unten).

DHCP-Adressverhandlung schlägt fehl

Schlägt die Adressvergabe über DHCP fehl, erhält das Authentifizierungsgerät folgende IP-Einstellungen:

1. IP-Addresse = 192.168.2.1 (fest programmiert)
2. Subnetzmaske = 255.255.0.0 (fest programmiert)
3. Gateway-IP-Adresse = im EEPROM gespeicherter Wert
4. Server-IP-Adresse = im EEPROM gespeicherter Wert

Gibt es mehrere Authentifizierungsgeräte, und die DHCP-Verhandlung schlägt fehl, erhalten alle Geräte dieselbe IP-Adresse (192.168.2.1).

DHCP-Adressverhandlung erfolgreich

Bei erfolgreicher DHCP-Verhandlung werden die vom DHCP-Server vergebenen Werte (IP-Adresse, Subnetzmaske und Gateway) verwendet.

Hinweis: Vom DHCP-Server vergebene Werte werden nicht im EEPROM gespeichert.

Option 230

Der Administrator kann Option 230 auf dem DHCP-Server zur Konfigurierung des Serverfelds auf dem Authentifizierungsgerät einstellen.

EQ;A;<IP-Adresse des DCE-Servers>

<IP-Adresse des DCE-Servers> = IP-Adresse in Acht-Bit-Format, z. B. 192.168.1.23.

Bei erfolgreichem Parsing der Zeichenfolge wird die Server-IP-Adresse wie spezifiziert eingestellt, schlägt das Parsing fehl, wird die Adresse auf 0.0.0.0 gesetzt. Erhält der Server die IP-Adresse 0.0.0.0, gibt das Authentifizierungsgerät eine Broadcast-bootp-Anforderung aus (s. Abschnitt 6).

Wird Option 230 verwendet, jedoch nicht für XSA, sondern für eine andere Anwendung, wird die Server-IP-Adresse auf 0.0.0.0 gesetzt, mit der Folge, dass eine Broadcast-bootp-Anforderung ausgegeben wird.

Gibt es mehrere Authentifizierungsgeräte, und der DHCP-Server kann Option 230 nicht verarbeiten, registriert der bootp-Prozess alle Geräte auf ALLEN, im Segment aktiven DCE-Servern. Es kann jedoch nur der erste DCE-Server, der mit dem Terminal Verbindung aufnimmt, mit diesem kommunizieren.

Option 230 fehlt

Fehlt Option 230, wird die im EEPROM gespeicherte Serveradresse verwendet.

5. Verfahren bei Rückstellung des Authentifizierungsgeräts

Wird der Rückstellschlüssel des Authentifizierungsgeräts gedreht, werden folgende Schritte durchgeführt:

1. Die Server-IP-Adresse wird auf 0.0.0.0 gesetzt und im EEPROM gespeichert.
2. Als IP-Adressvergabemethode wird DHCP aktiviert.
3. Das Kennwort wird auf “pc_passwd” gesetzt.
4. Die EDI-Einstellung wird auf die werkseitigen Vorgaben rückgesetzt.

6. Aufbau der Kommunikation zwischen Authentifizierungsgerät und DCE

Im Folgenden wird der Startablauf des Authentifizierungsgeräts beschrieben.

1. Verfügt das Authentifizierungsgerät über die IP-Adresse des Servers, sendet es eine bootp-Anforderung an diese Adresse. Andernfalls (d. h. wenn die IP-Adresse 0.0.0.0 lautet) sendet es eine Broadcast-bootp-Anforderung.

   Die bootp-Anforderung enthält folgende Daten:

   - IP-Adresse des Authentifizierungsgeräts
   - MAC-Adresse des Authentifizierungsgeräts
   - Terminaltyp = XSA-Modus Der DCE-Server ignoriert jegliche bootp-Anforderungen, die nicht die entsprechende Signatur enthalten. Die Signatur lautet: Xerox = ‘XEFB’
2. Das Authentifizierungsgerät wartet auf die bootp-Antwort. Diese muss an das Authentifizierungsgerät gerichtet sein.
3. Enthält das Gerät innerhalb von 10 Sekunden keine Antwort, schaltet es für ein bestimmtes Intervall in den Ruhezustand und sendet dann die bootp-Anforderung erneut. Dieser Vorgang kann sich bis zu drei Mal wiederholen, danach schaltet das Gerät offline.
   - Die Ruhezustand-Intervalle verlängern sich jedes Mal, das letzte dauert 22 Sekunden. Danach wird das Intervall wieder auf 0,15 Sekunden rückgesetzt.
   - Ruheintervalle in Sekunden: 0,15 -> 0,8 -> 2 -> 3,2 -> 5,6 -> 12 -> 22
4. Erhält das Authentifizierungsgerät eine bootp-Antwort, startet das Gerät am Socket-Server (TCP) und wartet auf die Verbindung mit einem (einzigen!) Client.
5. Wird innerhalb von vier Minuten keine Verbindung aufgebaut, wird das Authentifizierungsgerät zurückgesetzt, und der Startvorgang beginnt wieder mit Schritt 1.
6. Wenn eine Verbindung aufgebaut ist, wartet das Authentifizierungsgerät auf eine Anforderung vom DCE-Server, und der Startvorgang wird abgeschlossen.
7. Im Offlinemodus versuchen XSA-Geräte alle 30 Sekunden, über eine bootp-Anforderung eine Verbindung mit dem Server aufzubauen.

7. Hinweise zur Konfiguration

1. Werden mehrere DCE-Server betrieben, ist im DHCP-Modus Option 230 nicht zu verwenden. Stattdessen die Serveradresse über die Webseite des Authentifizierungsgeräts einrichten.
2. Wird nur ein DCE-Server betrieben, kann Option 230 eingesetzt werden. Es ist dann gewährleistet, dass die spezifizierte IP-Adresse des Servers verwendet wird, ohne dass eine Änderung der Adresse auf allen Webseiten des Authentifizierungsgeräts erforderlich ist.
3. DHCP ist in Umgebungen der Vorzug zu geben, in denen die IP-Adresse des Servers sich von Zeit zu Zeit ändert. Es ist dann allerdings wichtig, Option 230 zu verwenden, sodass die Serveradresse an alle Authentifizierungsgeräte ohne manuelle Konfiguration weitergegeben wird.