Dyport mit 802.1x

04.07.2025 08:09:45

FAQ-Artikel-Ausdruck

Kategorie:	Datennetz::Netz-Anbindung	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	de	**Letzte Aktualisierung:**	13:44:32 - 19.03.2025

Schlüsselwörter

Dyport Netzwerk 802.1x

Lösung (öffentlich)

Netzzugang mit 802.1x an Dyport-Anschlüssen

An Dyport-Anschlüssen ist die Anmeldung mit 802.1x die bevorzugte Variante.
Im Vergleich zur Netzzuordnung mit MAC-Adresse über das Dyport-Portal (MAB) wird eine bessere Sicherheit erreicht. Die Netzzuordnung erfolgt schneller. Es wird nur das in 802.1x konfigurierte VLAN zugeordnet, alternative Netze wie bei MAB werden nicht vergeben - ist das in 802.1x konfigurierte VLAN am Switch nicht vorhanden, erfolgt keine Netzzuordnung. Bei MAB erfolgt ein Rückfall in andere Netze, z. B. in ein allgemeines Mitarbeiternetz oder Gastnetz.
Im [1]Dyport-Portal können die zum Login verfügbaren VLANs angezeigt werden. Unter "Gerät hinzufügen" kann bei "VLAN:" die Liste aufgeklappt werden.
Prinzipiell können mit 802.1x verschiedene Netze ausgewählt und auch im Betrieb umgeschaltet werden. Der in Windows enthaltene Supplicant eignet sich jedoch mangels Umschaltfunktion nur für eine statische Netzzuordnung.
Mit dem NAM-Modul zum AnyConnect-Client von Cisco oder dem Geant-Supplicanten ist eine Umschaltung möglich. Bei Linux ist ein geeigneter Networkmanager in der Regel bereits aktiv oder kann über die Paketverwaltung installiert werden.

Windows 10 mit integriertem Supplicanten

Dieser Supplicant ist für eine statische Netzzuordnung geeignet.
Da die netsh Profile keine Credentials enthalten, ist eine Umschaltung über netsh-Aufrufe mit erneuter Passworteingabe verbunden. Die Passworteingabe ist zeitkritisch, da der 802.1x-Prozess für die Passworteingabe stehen bleibt und dadurch missglückte Anmeldungen entstehen können.
Start -> Computerverwaltung tippen/öffnen -> Dienste und Anwendungen aufklappen -> Dienste ->
Dienst "Automatische Konfiguration (verkabelt)" Doppelklick -> Dienstname: dot3svc, Starttyp: Automatisch, Dienststatus: Starten
Start -> Windows-Einstellungen -> Netzwerk und Internet -> Ethernet -> Adapteroptionen ändern -> Eigenschaften von z.B. Ethernet2 ->
  Eigenschaften von Ethernet2: 2.Tab Auth.:
    IEE 802.1x-Auth. aktivieren
    Microsoft: EAP-TTLS wählen, Haken bei Anmeldeinfo für jede Anmeldung speichern
  Einstellungen:
    Identitätsschutz: meinlogin@mein-vlan
    Verbindung Server: radius-tud.zih.tu-dresden.de
    Vertrauenswürdige Stamm...: COMODO RSA Cert Auth
    Clientauthentifizierung / EAP-fremde Authentifizierungsmethode auswählen: Unverschlüsseltes Kennwort (PAP) [OK]
    Zusätzliche Einstellungen ...
      Haken bei Authentifizierungsmodus angeben, Benutzerauthentifizierung
        Anmeldeinformation speichern (angeben/ersetzen)
          Benutzername: meinlogin@mein-vlan
          PW: vomLogin [OK]
  Bei dem Nutzername/Passwort-Popup gibt es 12 Sekunden für die Eingabe
    Beim 1. Versuch bis zu 12 Sekunden: Auth erfolgreich
    Beim 1. Versuch 12 bis zu 60 Sekunden: Auth nicht erfolgreich, 2. Popup erscheint
    Beim 1. Versuch über 60 Sekunden: Auth erfolgreich
    Beim 2. Versuch zeitunabhängig: Auth erfolgreich
  Beim PC-Start wird das Netz mit den vorherigen Credentials bereits vor dem Login aktiviert.
  Mit netsh sind Profile speicherbar und wiederherstellbar aber ohne die Credentials (erfordert Adminrechte):
    netsh lan export profile folder=. Interface="Ethernet 2"
    netsh lan add profile filename="C:\Users\meinlogin\dot1x_G_zih-ma-admin.xml" Interface="Ethernet 2"

Windows 10 mit Cisco AnyConnect NAM-Modul

Im Cisco AnyConnect kann mit dem NAM-Modul vergleichsweise einfach die Umschaltung und Konfiguration von verschiedenen Netzen erfolgen.
Die Installation und Nutzung sind im [2]FAQ-Artikel "Cisco Secure Client (AnyConnect) - NAM-Modul installieren" beschrieben.
Standardmäßig wird auch das WLAN vom NAM-Modul verwaltet. Soll Windows weiterhin das WLAN verwalten, muss mit einem leeren Profil "NoWifi" begonnen werden.
Beim PC-Start wird das oberste Profil in der Auswahlliste aktiviert. Falls an oberster Stelle das "Wired"-Profil (MAB, kein 802.1x) nicht verschoben oder entfernt werden kann, muss mit einem leeren Profil "NoWired" begonnen werden.

-

Umbenennen von C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml in configuration-xml.ori

-

Ablegen eines der configuration-Anhänge (rechts im zweiten Frame) configuration_NoWifi_xml oder configuration_NoWired_xml unter C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\

-

Umbenennen von configuration_NoWifi_xml oder configuration_NoWired_xml in configuration.xml

-

den Rechner neu starten

-

die benötigten Netzeinträge wieder erstellen

Windows 10 mit dem Geant-Supplicanten

Dieser Supplicant ist zusätzlich zu einer statischen Netzzuordnung auch zum Umschalten über netsh-scripte geeignet, da die netsh Profile auch Credentials enthalten.
Die letzte Version des [3]Geant-Supplicanten ist 1.3g (03.10.2022). Die [4]X86-Installationsdatei herunterladen und installieren.
Start -> Computerverwaltung tippen/öffnen -> Dienste und Anwendungen aufklappen -> Dienste ->
Dienst "Automatische Konfiguration (verkabelt)" Doppelklick -> Dienstname: dot3svc, Starttyp: Automatisch, Dienststatus: Starten
Start -> Windows-Einstellungen -> Netzwerk und Internet -> Ethernet -> Adapteroptionen ändern -> Eigenschaften von z.B. Ethernet2 ->
  Eigenschaften von Ethernet: 2.Tab Authentifizierung.:
    IEE 802.1x-Auth. aktivieren
    GEANTlink:EAP-TTLS wählen
  Einstellungen von "GEANTLink:EAP-TTLS"
  Unverschlüsselte Anmeldungsphase
    Abweichende Identität: meinlogin@mein-vlan
    herunterladen von comodo-root-ca.pem -> rechts im zweiten Frame
    CA aus einer Datei hinzufügen... : comodo-root-ca.pem (aus Downloads)
    unter Vertrauenseinstellungen (CAs) wird angezeigt: AAA Certificate Services (Details mit Doppelklick prüfbar - Aussteller: Comodo CA Limited)
    Akzeptable Servernamen: radius-tud.zih.tu-dresden.de
    Benutzer-Zertifikat: Profilkonfig: (keine)
  Verschlüsselte Anmeldungsphase
    PAP: Profilkonfig
      Benutzername: meinlogin@mein-vlan
      PW: vomLogin
    [+] / Fortgeschritten...
    Hier sind zwar Profile konfigurierbar, aber es ist kein Nutzerfrontend zur Profilauswahl enthalten.
GEANTlink EAP-TTLS mit [OK] beenden
zurück zu Eigenschaften von Ethernet: 2.Tab Authentifizierung.: Zusätzliche Einstellungen
 [x] Authentifizierungsmodus angeben:
    * Computerauthentifizierung (Beim PC-Start wird das Netz wird mit den vorherigen Credentials bereits vor dem Login aktiviert.)
    * Benutzerauthentifizierung (Beim PC-Start wird das Netz wird mit den vorherigen Credentials erst nach dem Login aktiviert.)
    * [OK]
Eigenschaften von Ethernet: 2.Tab Authentifizierung mit [OK] übernehmen. Jetzt wird das Netz mit den gewählten Einstellungen umgeschaltet.
Profile erstellen und aufrufen:
  Mit netsh sind Profile speicherbar und wiederherstellbar inklusive der Credentials (erfordert Adminrechte):
    netsh lan export profile folder=. Interface="Ethernet 2"
    netsh lan add profile filename="C:\Users\fleck\dot1x_G_zih-ma-admin.xml" Interface="Ethernet 2"
  Um von dot1x wieder auf MAB zu wechseln, muss zusätzlich zur Profilwiederherstellung der Ethernetadapter getoggelt werden:
    netsh interface set Interface="Ethernet 2" disabled
    netsh interface set Interface="Ethernet 2" enabled
  Mit bginfo kann die aktuelle Einstellung auf dem Hintergrund angezeigt werden.
  Für jedes Profil kann ein eigenes cmd-script erstellt werden.
  Auf dem Desktop können Verknüpfungen zu den Scripten abgelegt werden
  Ein Verzeichnis mit Links zu den Scripten kann als "Neue Symbolleiste" neben dem Systray ein Auswahlmenü ermöglichen.

MacOS

802.1x ist unter MacOS unterstützt inkl. Umschaltung zwischen verschiedenen Netzen. Um unter MacOS 802.1x nutzen zu können, laden Sie zunächst eines der an diesen Artikel angehängten Konfigurationsprofile (profilX.mobileconfig) herunter.

Konfiguration
-

Nachdem das Herunterladen abgeschlossen ist, finden Sie die Profildatei in ihrem Download-Ordner.

  Screenshot MacOS: Download-Ordner
-

Öffnen Sie die Profildatei mit dem Programm TextEdit. Wählen Sie dazu die Datei mit einem Rechtsklick aus und wählen dann über "Öffnen mit" TextEdit aus.

  Screenshot MacOS: Datei öffnen mit

-

Der Texteditor öffnet sich.

Screenshot MacOS: Geöffneter Texteditor
-

Öffnen Sie nun die Suchfunktion über das Menü oder mit Hilfe der Tastenkombination "Cmd-F". Setzen Sie den Haken bei "Ersetzen" rechts neben der Suchleiste und geben Sie den Namen der Profildatei (profilX) in die Suche ein. In die Ersetzen-Leiste darunter geben Sie den Namen des VLANs, für das Sie den Zugang erstellen wollen ein (im dargestellten Beispiel maoffen6) und bestätigen Sie die Eingabe durch einen Klick auf die Schaltfläche "Alle".

Screenshot MacOS: Suchen und Ersetzen
-

Schließen Sie TextEdit. Sie können nun die Installation des Profils durch einen Doppelklick auf die Profildatei starten. Bestätigen Sie den Start der Installation durch die Auswahl von "Fortfahren" im sich öffnenden Bestätigungsdialog.

Screenshot MacOS: Installation starten
-

Bestätigen Sie nun auch die zweite Sicherheitsabfrage durch die Auswahl von "Installieren".

Screenshot MacOS: Installation bestätigen
-

Abhängig von den Sicherungseinstellungen Ihres Systems werden Sie dazu aufgefordert, den Vorgang noch einmal durch die Eingabe Ihres Passworts zu autorisieren.

Screenshot MacOS: Passwortabfrage
-

Das Profil ist nun installiert. Zur Bestätigung sehen Sie es in der Übersicht der installierten Geräteprofile.

Screenshot MacOS: Übersicht Geräteprofile

Beachten Sie bitte: Falls Sie mehrere VLANs konfigurieren möchten, müssen Sie dazu eine der anderen oben bereitgestellten Profildateien nutzen. Bei der Verwendung der gleichen Profildatei wird das vorher installierte Profil überschrieben.

Benutzung
-

Zur Verbindung mit einem zuvor konfigurierten VLAN öffnen Sie die Netzwerkoptionen in den Systemeinstellungen.

Screenshot MacOS: Netzwerkoptionen öffnen
-

Wählen Sie Ihre Netzwerkverbindung aus der Liste links aus und betätigen Sie die Schaltfläche "Trennen".

Screenshot MacOS: Netzwerkverbindung trennen
-

Neben dem Eintrag "802.1X:" können Sie nun Ihr gewünschtes VLAN aus dem Dropdown-Menü auswählen.

Screenshot MacOS: VLAN auswählen
-

Nach der Auswahl des gewünschten VLANs betätigen Sie die Schaltfläche "Verbinden".

Screenshot MacOS: Mit ausgewähltem VLAN verbinden
-

Beim ersten Verbinden werden Sie außerdem nach Ihrem Nutzernamen und Passwort gefragt. Der Nutzername ist Ihr ZIH-login + @ + der Name des VLANs (Beispiel im Bild anhand von maoffen6). Das Passwort ist Ihr ZIH-Passwort.

Screenshot MacOS: Passwortabfrage

Linux

802.1x ist in Linux unterstützt. Die Konfiguration und Umschaltung zwischen verschiedenen Netzen ist in der Regel im Networkmanager der unterschiedlichen Distributionen bereits enthalten.
Im Networkmanager sind folgende Werte einzutragen:
Legitimierung: Getunneltes TLS (TTLS oder EAP-TTLS)
äußere Identität (Anonymous Identity): login@vlan-name
Zertifikat: Comodo CA (comodo-root-ca.pem -> rechts im zweiten Frame)
Servernamen (Domain): radius-tud.zih.tu-dresden.de
innere Legitimierung: PAP
innere Identität (UserName): login@vlan-name
Bei Nutzung eines USB-C Docks von Lenovo musste für eine zuverlässige Anmeldung der Timeout auf z.B. 75s (802-1x.auth-timeout 75) erhöht werden.
Zum Umschalten zwischen Netzen sind die konfigurierten Netzprofile im Systray (Network) auswählbar.
Um von dot1x wieder auf MAB zu wechseln, muss zusätzlich der Ethernetadapter getoggelt werden.

[1] https://dyport.zih.tu-dresden.de/
[2] https://faq.tickets.tu-dresden.de/v/ItemID=595
[3] https://github.com/Amebis/GEANTLink/releases
[4] https://github.com/Amebis/GEANTLink/releases/download/1.3g/GEANTLink-x64.msi