Whitepaper: 802.1X und WAC

Offene Besprechungsräume, leere Büros und überall Netzwerkdosen, die den ungehinderten Zugriff auf das Firmennetz freigeben. Das ist die Realität in vielen Firmen. Wenn dann noch ein DHCP Server freigiebig IP-Adressen verteilt steht einem ungehinderten Zugriff auf die Netzwerkinfrastruktur nichts mehr im Wege. Die dadurch auftretenden Risiken sind hoch. Unerlaubt an das Netzwerk angeschlossene Komponenten können dessen Stabilität schwächen. Angreifer können zunächst den Netzwerkverkehr mitschneiden, analysieren und danach gezielte Angriffe fahren. Ebenso können sensible Daten gelesen werden, ohne dass es überhaupt bemerkt wird.

Diese Risiken gilt es zu minimieren. Es bestehen unterschiedliche Möglichkeiten, dies zu tun. Unbenutzte Anschlüsse im Büro können ungepatcht bleiben. Das bedeutet, sie werden im Technikraum nicht auf einen Port am Netzwerk-Switch aufgelegt. Steckt sich nun ein Anwender auf einen dieser Anschlüsse, so bekommt er gar keine physikalische Verbindung. Das bedeutet aber auch, das mitunter ein Mehraufwand an Patchungen entsteht, da bei der Anforderung für neu zu verwendende Anschlüsse diese erst gepatcht werden müssen. Um diesen Aufwand auf eine Konfiguration zu reduzieren (um nicht vor Ort zu müssen) können gepatchte Ports, die ungenutzt sind, in ein isoliertes VLAN konfiguriert werden. Dieses VLAN wird ausschließlich auf ungenutzten User Ports konfiguriert. Auf Verbindungen zwischen den Switchen wird dieses VLAN nicht verwendet. Steckt sich nun ein User auf einen dieser Anschlüsse, so bekommt er zwar einen Link, ist aber in einem isolierten VLAN Segment, welches keine Verbindung zum internen Firmennetzwerk hat.

Die oben beschriebenen Maßnahmen haben den Vorteil, dass sie ohne weitere Konfigurationsmaßnahmen und unabhängig vom eingesetzten Client (Notebook, PC, Netzwerkdrucker usw.) funktionieren. Allerdings haben sie auch zwei gravierende Nachteile. Zum einen sind diese Konfigurationen statisch. Veränderungen in der Physik (Umzug, neuer Mitarbeiter usw.) bedingen immer eine aktive Konfigurationsänderung, ggf. sogar zusammen mit einer physikalischen Patchung. Zum anderen schützen diese Maßnahmen nicht vor unberechtigtem Zugriff auf das Netzwerk. Vorhandene, genutzte Anschlüsse können als Zugang missbraucht werden. Dies kann auch vom eigentlichen Nutzer unbemerkt über einen zusätzlich vorgeschalteten Mini-Switch geschehen.

Um unberechtigte Zugriffe auf Ihr Netzwerk wirksam zu verhindern, gleichzeitig aber auch die Administration gering und flexibel zu halten, ist es notwendig, Anmeldevorgänge am Netzwerk automatisiert ablaufen zu lassen. Anhand dieser Anmeldung bekommt der Anwendern Zugriff auf das Netz freigeschaltet. Im Umfeld der Server und Domänen wird dies bereits mit Username / Password Kombination sehr häufig eingesetzt. Der eigentliche Zugang zum Netzwerk wird hierüber aber nicht reglementiert. Dies bietet das standardisierte Protokoll 802.1X, welches zusammen mit dem Netzwerkswitch den Zugang zum Netzwerk steuert. Es kann in Kombination mit der Domainanmeldung verwendet werden und ermöglicht so die Verwendung von nur einer Username/Password Kombination, welches der Akzeptanz durch den Endanwender sehr zugute kommt.

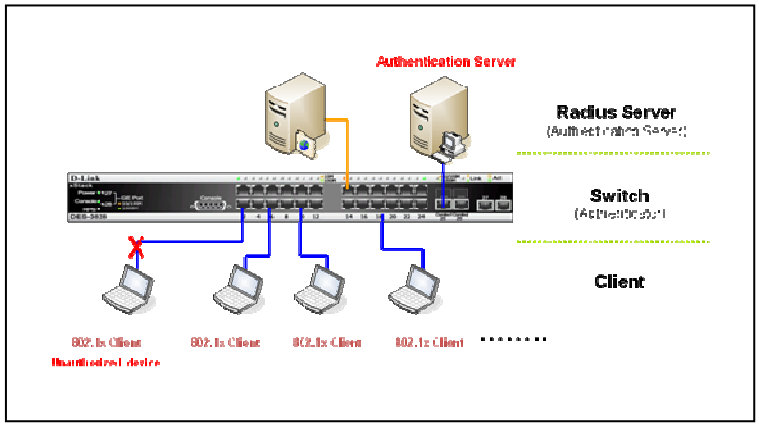
Whitepaper: 802.1X und WAC

802.1X – wie funktioniert das?

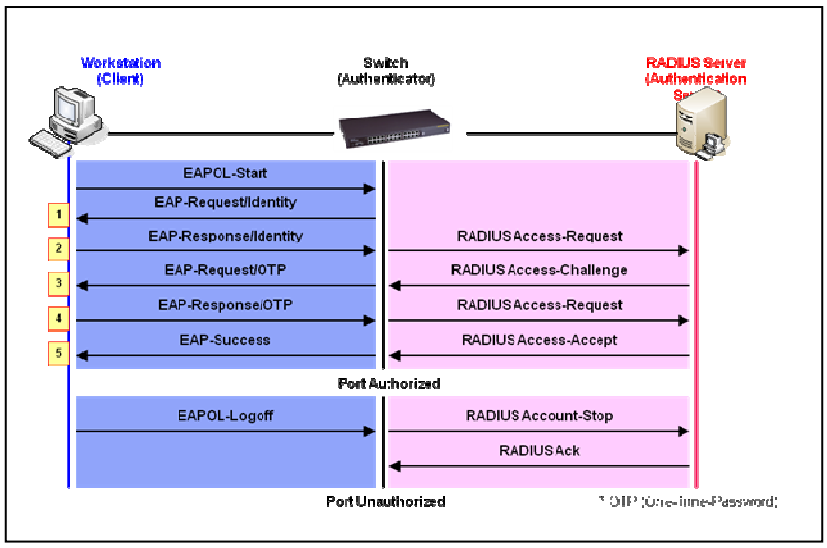
802.1X ist ein von der IEEE ratifiziertes Protokoll und ermöglicht die Authentifikation sowohl am verkabelten (wired) als auch im drahtlosen (wireless LAN oder WLAN) Netzwerk. Das Protokoll arbeitet mit Hilfe von drei Komponenten:

- **Authentication Server (RADIUS Server)**
  Der Authentication Server überprüft die Identität des Supplicants (Clients) und gibt danach eine entsprechende Meldung an den Switch weiter.
- **Authenticator (Switch)**
  Der Authenticator fordert die für die Anmeldung am Netzwerk erforderlichen Identifikationsdaten wie Username und Passwort vom Client, sendet diese Informationen weiter an den Authentication Server und gibt auch dessen Antwort an den Client weiter.
- **Supplicant (Client)**
  Ein PC, Laptop, Druckerserver o.ä., welcher Zugang zum Netzwerk benötigt. Auf dem Client wird eine entsprechende, 802.1X kompatible Software benötigt (diese ist z.B. bei Windows XP und Vista bereits enthalten).

Der Authentifizierungs-Prozess erfolgt vom Client aus über das Extensible Authentication Protocol (EAP) over LAN, kurz EAPoL. Das Protokoll stammt aus der Zeit, als Rechner noch direkt über je ein Modem und eine (Telefon-) Leitung miteinander verbunden waren und über das PPP-Protokoll (Point-to-Point Protocol) kommunizierten. Daher existiert EAPoL, um EAP auch für Local Area Networks verwenden zu können.



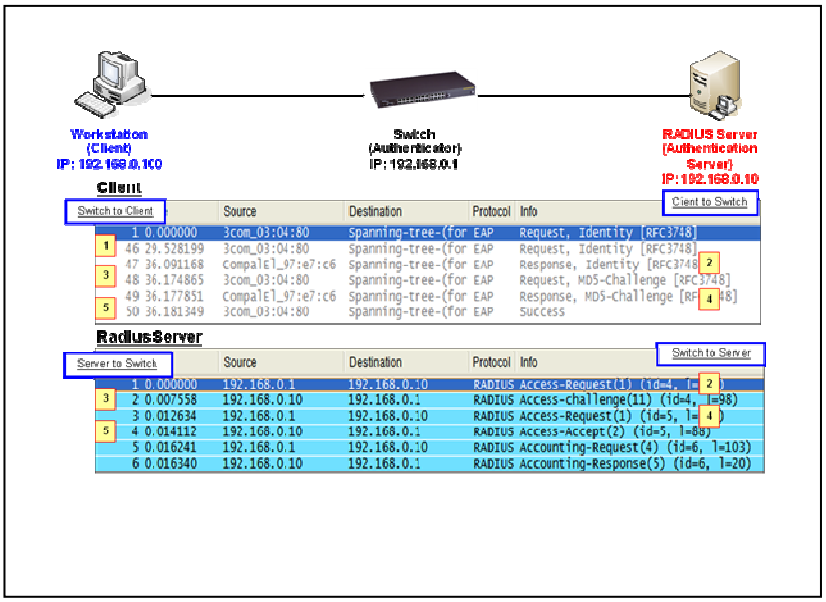
Der Authenticator (Switch) setzt die EAPoL Authentifizierung in eine RADIUS Anfrage um und sendet diese an den Authentication Server. Der Authentifizierungsprozess läuft bei einer Anmeldung eines Clients über 802.1X in fünf Schritten ab (siehe nebenstehendes Diagramm).



Hierbei wird die Anmeldung des Clients über eine EAPoL

Session, klassischerweise mit Username/Passwort z.B. der Windows Anmeldung, vom Authenticator (dem Switch) als RADIUS Access-Request an den Authentication Server (z.B. dem im Windows Server 2003/2008 integrierten Radius Server) weitergegeben. Dieser überprüft die Identität des Clients und gibt eine RADIUS-Accept Meldung an den Switch, der diese wiederum als EAP-Success Meldung an den Clients übermittelt. Gleichzeitig schaltet er den Switchport, an welchem der Client angeschlossen ist, für den Netzwerkverkehr frei.

Am Mitschnitt des Netzwerkverkehrs kann sehr gut die Umsetzung der EAPoL Kommunikation des Clients auf die RADIUS Kommunikation des Switches zum Server erkannt werden.



Dynamische VLAN Zuweisung

Über zusätzliche Parameter, welche der Authentication Server über RADIUS an den Switch meldet, kann z.B. das VLAN, in welches der Client verbunden werden soll, mitgegeben werden. Der Switch konfiguriert dann den Port, an welchem der Client angeschlossen ist, mit dem entsprechenden VLAN.

Port oder MAC-Adresse

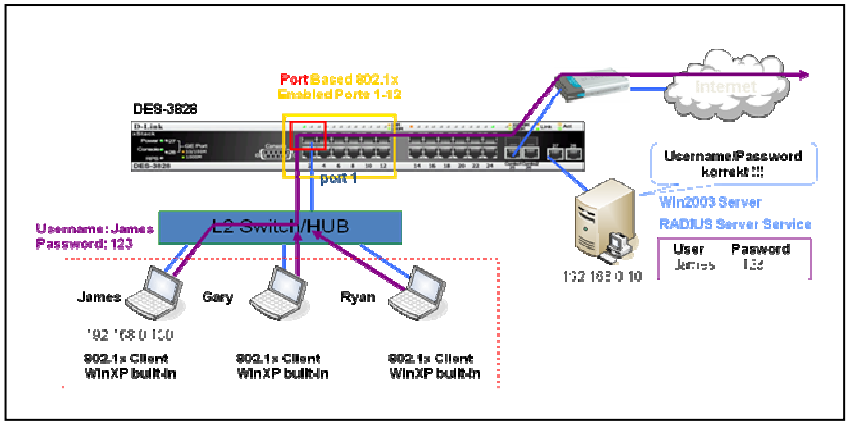
Port basierte Authentifizierung

Die standardmäßige Hardware-Konfiguration sieht einen Rechner an einem Switchport vor. Dieser Rechner authentifiziert sich über 802.1X und schaltet den Port frei. Diese Art der Authentifizierung nennt sich „Port basiert". In Ermangelung freier Netzwerkdosen kommt es aber immer wieder vor, dass in einem Büro ein kleiner Miniswitch installiert wird, um den Nutzern zusätzliche Netzwerkanschlüsse zur Verfügung zu stellen.

In dieser Konfiguration mit Port basierter Authentifizierung über 802.1X würde der erste Rechner, der sich erfolgreich am Netzwerk anmeldet, den Port auf dem Hauptswitch im Technikraum freischalten. Zusätzlich an dem Miniswitch angeschlossene Rechner sind somit ebenfalls für das Netzwerk „freigeschaltet" und benötigen keine eigene Authentifizierung. Dieses Verhalten öffnet auch bewussten Angriffen auf das Netzwerk die Türen, da Angreifer unbemerkt einen kleinen Switch im Büro installieren können und über die zusätzlichen Anschlüsse nach der Anmeldung des offiziellen Rechners problemlos Zugriff auf das Netzwerk erhalten.

Whitepaper: 802.1X und WAC

Zu sehen ist dieses am Beispiel auf der rechten Seite. Nur ein Nutzer (James) hat sich korrekt über 802.1X am Netzwerk angemeldet. Trotzdem können auch die anderen, an dem Miniswitch angeschlossenen Teilnehmer auf das Netzwerk zugreifen.

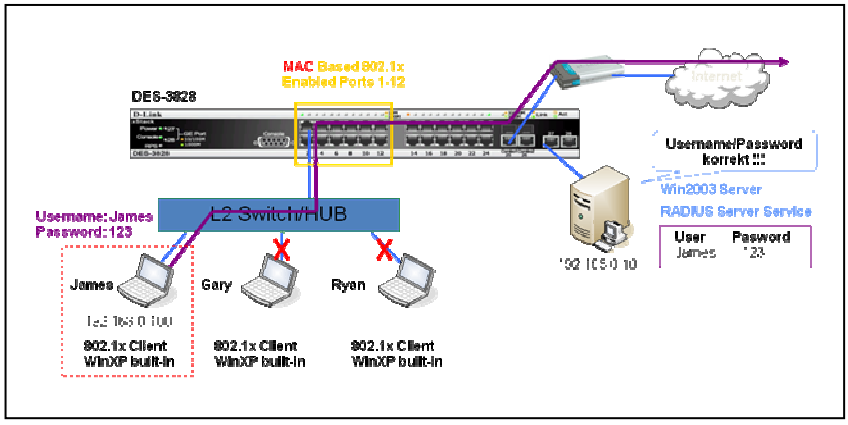


Um dieses Sicherheitsleck zu schließen ist die sogenannte MAC-basierte Authentifizierung zwingend erforderlich.

MAC basierte Authentifizierung

Bei dieser Authentifizierung berücksichtigt der Authenticator (Switch) ebenfalls die von dem Client verwendete MAC-Adresse. Über diese Funktionalität wird sichergestellt, dass sich jeder an dem Miniswitch angeschlossene Client einzeln am Authentication Server authentifizieren muss, um Zugang zum Netzwerk zu erhalten.

Auf dem rechts dargestellten Beispiel ist zu erkennen, dass dieses Mal nur der korrekt angemeldete Client (James) Zugriff auf das Netzwerk erhält.

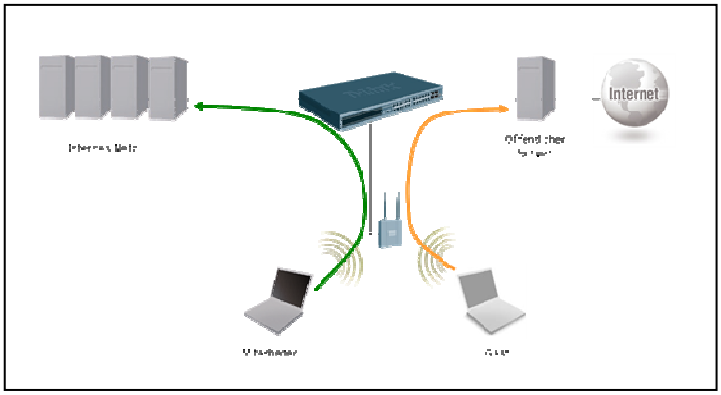


Die zwei anderen Rechner bekommen über den Hauptswitch hinweg keinen Zugriff.

Unterstützt ein Switch beide Arten der Authentifizierung (MAC- und Port-basiert), so ist auf jeden Fall die Verwendung der MAC-basierten Authentifizierung zu empfehlen, da niemals sicher ausgeschlossen werden kann, dass ein Miniswitch in einem Büro angesteckt wird.

Gäste willkommen

Wird ein Client an das Netzwerk angeschlossen, der keine gültige Identität im Authentication Server aufweisen kann, so bleibt dieser ausgeschlossen vom Netzwerk. Es kann aber gewollt sein, das solch ein Anwender einen speziellen, eingeschränkten Zugang zum Netzwerk

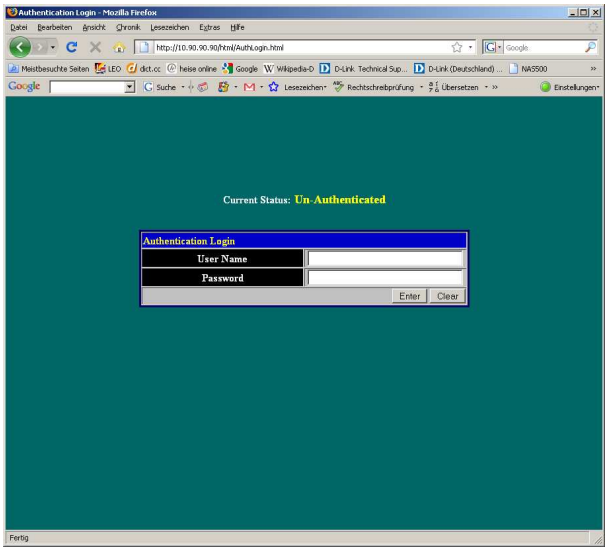


erhält. So kann z.B. Gästen oder externen Mitarbeitern ein Internetzugang ermöglicht oder ein Drucker zu Verfügung gestellt werden.

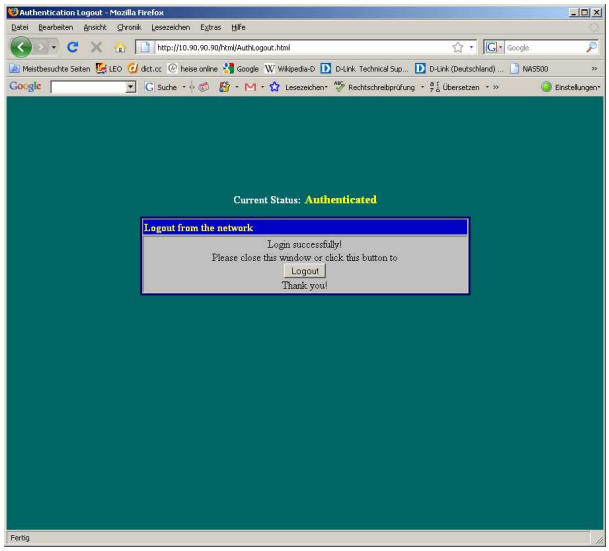
Diese Funktionalität stellt die 802.1X Guest VLAN Funktion bereit. Die dynamische Zuweisung eines VLANs durch den Authentication Server wird dazu verwendet, Clients ohne gültige Identifikation ein spezielles VLAN zuzuweisen. Dieses Gast-VLAN wird so konfiguriert, dass es keinen Zugang zum normalen internen Netzwerk erlaubt und nur sehr eingeschränkte Kommunikation zulässt.

Authentifizierung auch ohne 802.1X

Die Verwendung von 802.1X bietet die komfortable Möglichkeit eine Authentifizierung durchzuführen, die für den Anwender vollkommen automatisiert erfolgt. Die Anmeldedaten an der Domäne können genutzt werden, um eine zusätzliche Eingabe von Username und Passwort möglichst zu vermeiden. Sie bedingt aber auch das Vorhandensein einer entsprechenden Software auf Seiten des Clients. Oft genug ist nun genau dies nicht möglich, trotzdem wird aber der Zugriff auf das Netzwerk benötigt.



Für diese Fälle hat D-Link die Möglichkeit der WEB based Authentication (WAC) entwickelt. Hierbei wird der Anwender bei der ersten Verwendung seines Webbrowsers per Anmeldemaske gebeten, seine Zugangsdaten einzugeben. Die Verifikation kann, wie bei 802.1X, über einen zentralen RADIUS Server erfolgen. Zusätzlich besteht auch die Möglichkeit einer Verifikation über eine interne User-Datenbank. Nach der erfolgreichen Authentifizierung ist der Anwender dann am Netzwerk angemeldet. Eine dynamische Zuweisung eines VLANs ist hierbei ebenfalls möglich.



Nach der Anmeldung muss das danach erscheinende Browserfenster geöffnet bleiben, bis kein Netzzugang mehr benötigt wird. Danach kann das Fenster geschlossen oder der Logout-Button betätigt werden.

Somit bietet WAC die komfortable Anmeldung am Netzwerk, auch ohne einen 802.1X Client. Voraussetzung hierfür ist lediglich das Vorhandensein eines WEB-Browsers.

Whitepaper: 802.1X und WAC

Sicherheit für Netzwerke, Daten und Anwendungen

Das Server und Rechner über Zugangsdaten geschützt werden ist uns bereits in Fleisch und Blut übergegangen. Wir haben erkannt, dass die Daten und Anwendungen geschützt werden müssen, um einen unberechtigten Zugriff zu vermeiden und die Produktivität zu sichern.

D-Link bietet über die Implementierung von 802.1X die Möglichkeit, auch das Netzwerk in den Kreis der gesicherten Systeme mit einzubinden. Unberechtigter Zugriff wird abgelehnt und somit die Analyse von Daten effektiv verhindert. Wo ein Client 802.1X nicht unterstützt, ermöglicht D-Link über WAC die komfortable Möglichkeit auch diesen Geräten einen authentifizierten Zugang zum Netzwerk zu ermöglichen. Zusätzlich bietet das Gast-VLAN Besuchern Zugriff auf z.B. E-Mail, Internet und Drucker, um auch abseits des eigenen Firmennetzes produktiv arbeiten zu können.

Aktuelle Themen im Rahmen					
Sicherheit	**Stabilität**	**Performance**	**Redundanz**	**Verwaltbarkeit**	**D-Link Lösung**
	Loop Connections				**Loopback–Detection**
	Mehrere DHCP Server				**DHCP Server Screening**
	Wurm Ausbrüche				**SafeguardEngine**
Wurm Ausbrüche					**Zonedefense**
ARP Spoofing					**IMPB v3**
Man in the Middle Attack					**IMPB v3**
Grundsätzlich geschützter Netzwerkzugriff					**ACL Liste Web based Access (WAC) 802.1x**
Erweiterter Netzwerkzugriff mit Policies					**Microsoft NAP**
		P2P Abusing			**Flow based Bandwidth Control**
			Chassis übergreifende Redundanz		**RERP (DES-7200)**
			Stacking		**Stacking auch über Glasfaser**
		Bandbreiten-erhöhung			**Stacking**
Überwachung / Konfigurations-rollout	Überwachung	Überwachung	Überwachung / Konfiguration	Einfache Administration	**D-View 6**

Whitepaper: 802.1X und WAC

Folgende Switch Serien unterstützen 802.1X und WAC:

- DES-1200 *)	**- DGS-1200 *)**	**- DES-3010/18/26 **)**	**- DES-3028/52 **)**
- DGS-3024/48 **)	**- DGS-3100 **)**	**- DGS-3200 ***)**	**- DES-3526/50 ***)**
- DES-3528/52 *)**	**- DES-3800 ***)**	**- DGS-3400 ***)**	**- DGS-3600 ***)**

***)** **802.1X nur Port based**
****)** **802.1X Port- und Host based**
*****)** **802.1X Port- und Host based und WAC**