IEEE 802.1x, Dynamic ARP Inspection und DHCP Snooping

von Thorsten Dahm
08.06.2006
t.dahm@resolution.de

1) Was Euch hier erwartet

1) Was ist 802.1x
   - Wozu braucht man's?
   - Möglichkeiten
   - Artenreichtum: Authentifizierung
   - Diverse Features
2) Dynamic ARP Inspection, DHCP Snooping
   - Funktionsweise
   - Trusts

1) Was ist 802.1x überhaupt?

- Methode zur Authentifizierung in Netzwerken (Port-basierend)
- User- und Maschinen-Authentifizierung möglich
- Identifizierung mittels Zertifikat oder Passwort

1) 802.1x: Wozu braucht man's?

- Kontrolle der Netzwerk-Zugriffe in Office-Netzwerken
- Einfache Identifizierung von externen Mitarbeitern
- Verhindern, dass externes Equipment (z.B. Laptops) ins interne Netz gelangen
- Roaming im Office für alle User möglich (z.B. in Konferenzräumen)

1) Eingesetzte Hard- und Software

- Cisco-Switche (2950, 4507 & 6509)
- Clients: WindowsXP, MacOS X und diverse Linux-Distributionen
- Cisco-RADIUS-Server
- Active Directory für die Computerkonten

1) 802.1x: Möglichkeiten

- Zuweisen von VLANs zu Usern/Rechnern beim Anmelden
- Wenn Authentifizierung fehlschlägt, zuweisen von „Authentication-failed-VLAN“
- Dauerndes Patchen in Serverräumen wird überflüssig
- Identifizierung des RADIUS-Servers per Zertifikat
- Keine PKI-Infrastruktur notwendig

1) 802.1x: Arten der Authentifizierung

- MD5
- EAP (Extensible Authentication Protocol)
- P-EAP (Protected EAP)
- EAP-TLS
- Viele weitere EAP-Verfahren, siehe RFC 3748

... Vor- und Nachteile von MD5

- einfache Inbetriebnahme: Keine Zertifikate auf dem RADIUS-Server nötig
- Keine automatische Anmeldung am Netzwerk möglich
- Keine Verschlüsselung der Anmeldedaten (nur CHAP)
- Identität des Rechners und RADIUS-Servers kann nicht sichergestellt werden

... Vorteile von P-EAP

- Verschlüsselte Kommunikation zwischen Workstation und RADIUS
- Automatische Anmeldung der Workstation per 802.1x

... Nachteile von P-EAP

- Zertifikat auf dem RADIUS-Server notwendig
- Benutzername wird im Klartext gesendet (in Phase 1, vor Initialisierung des SSL-Tunnels)

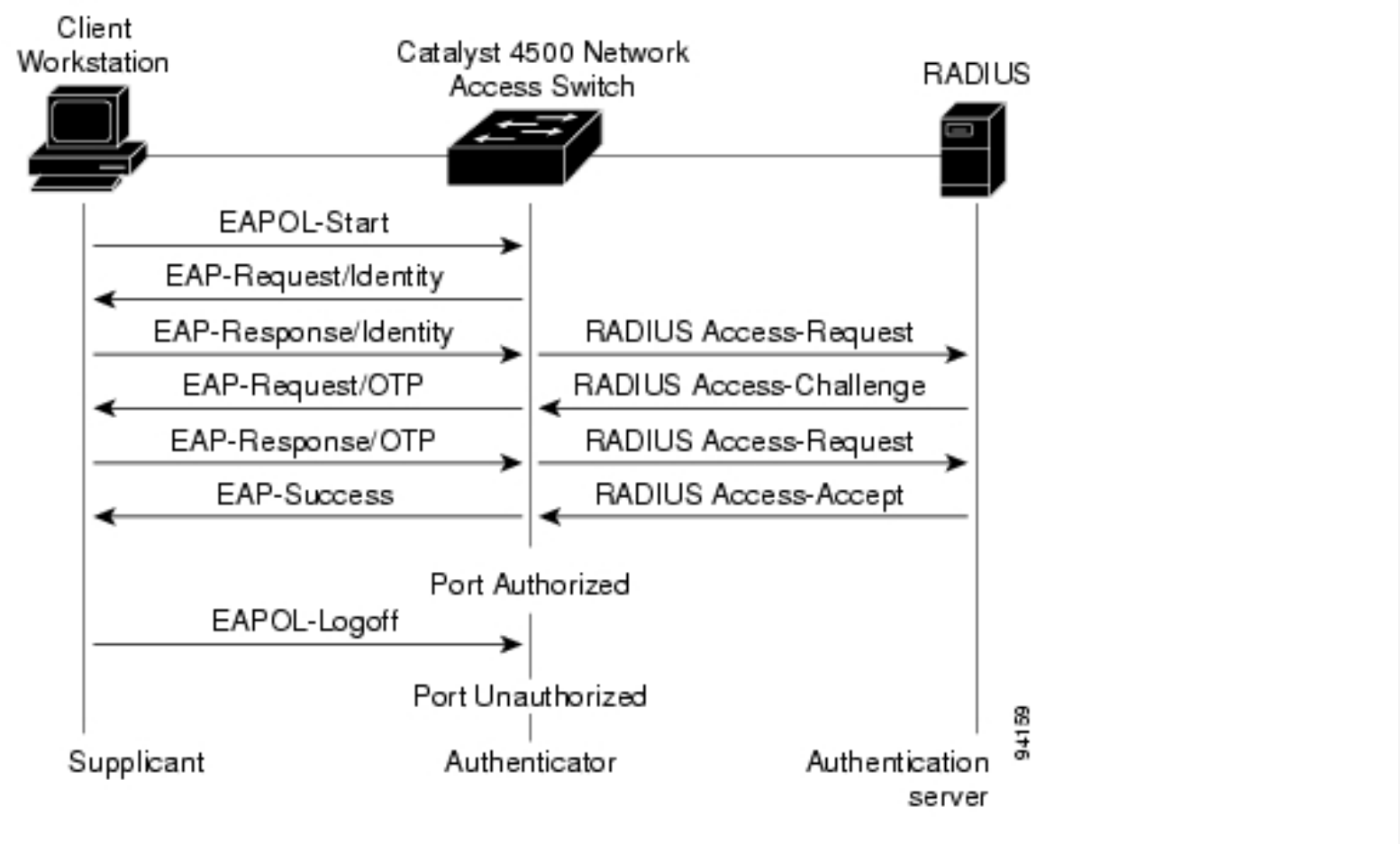
... Vorteile von EAP-TLS

- Verschlüsselte Kommunikation zwischen Workstation und RADIUS-Server
- Automatische Anmeldung der Workstation am Netz per 802.1x
- Identifizierung der Workstation und des RADIUS-Servers per Zertifikat.
- Ohne Zertifikat: Keine Anmeldung am Netzwerk möglich

... Nachteile von EAP-TLS

- Zertifikat auf RADIUS-Server und Workstation nötig
- PKI-Infrastruktur nötig

Der Authentifizierungsprozess

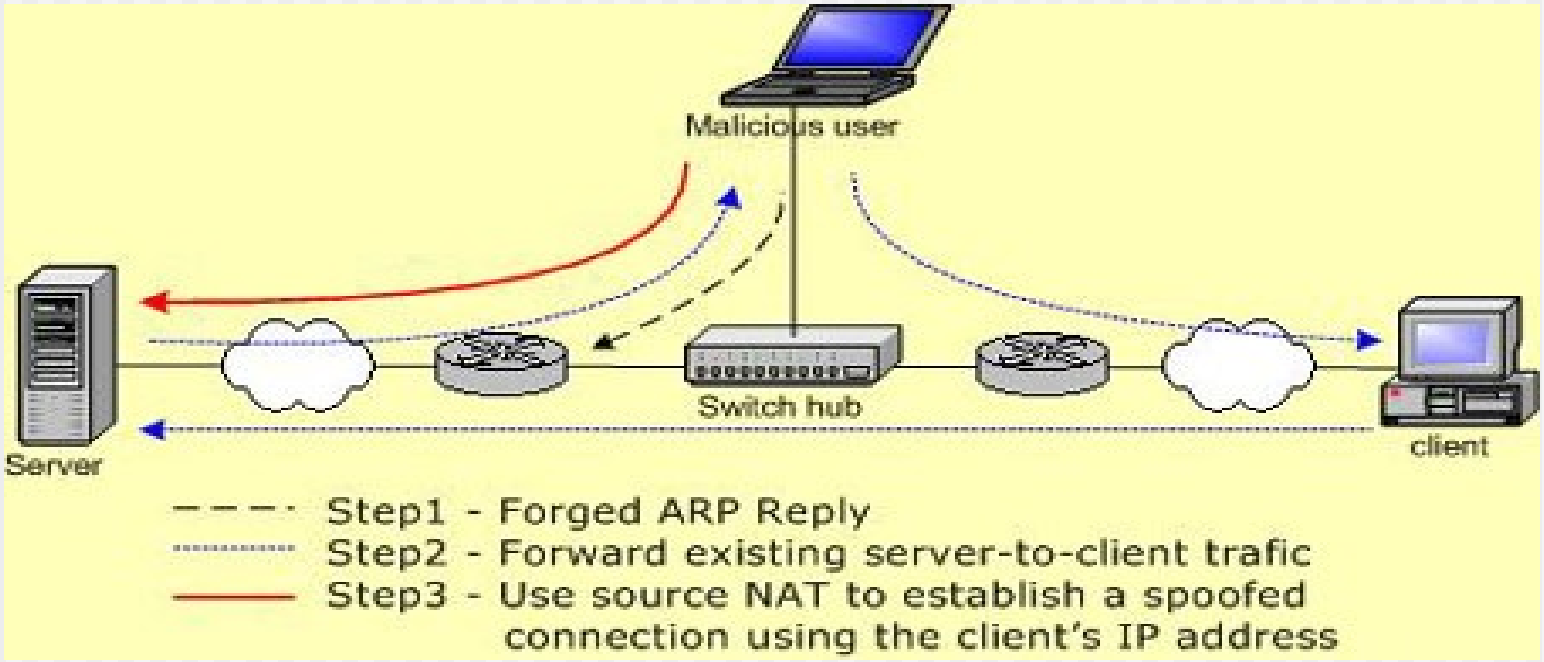


Features von 802.1x

- Guest-VLAN / Authentication-Failure-VLAN:
  Geht Authentifizierung schief, bleibt der Port nicht „down“, sondern kann in ein spezielles VLAN fallen
- Mehrere Geräte an einem Netzwerkport können erlaubt/nicht erlaubt werden

2) Dynamic ARP Inspection (DAI) & DHCP Snooping

- Dient zur Verhinderung von ARP cache poisoning und Spoofing Attacken (Man-in-the-middle)
- DAI fängt ARP-Pakete ab, loggt und verwirft Pakete mit unkorrekten IP-to-MAC-Zuordnungen



... Funktionsweise von DAI

- Switch fängt alle ARP-Anfragen + Antworten auf Untrusted Ports ab
- Er überprüft, ob abgefangenen Pakete eine gültige IP-to-MAC-Zuordnung haben, bevor er seinen ARP-Cache auffrischt und Pakete weiterleitet
- Er verwirft ungültige ARP-Pakete
- Einschränken der Durchsatzrate eingehender ARP-Pakete zur Verhinderung von DoS
- Dafür: „dhcp snooping binding database“

... DHCP Snooping Bindings

- Population der Snooping Binding Tabelle mit Hilfe der DHCP-Requests
- Switch liest DHCP-Requests mit und merkt sich Antwort des DHCP-Servers. Er kennt somit die jeweils gültige Zuordnung IP-Adresse <-> MAC-Adresse

Aufbau der DHCP Snooping Bindings Tabelle

- Der Switch erkennt DHCP-Requests
- Der Broadcast wird in einen Unicast umgewandelt (somit können keine „fremden“ DHCP-Server mehr Adressen verteilen)
- Die Antworten des DHCP-Servers werden in eine Tabelle eingetragen

... Trusts

- Es ist möglich, ein Interface auf *trust* zu setzen, damit wird die ARP-Inspection umgangen (z.B. Uplinks der Switche)
- DAI kann ARP-Pakete gegen ACLs testen und erlauben (z.B. für Hosts mit fest konfigurierter IP)
- Alle „untrusted Interfaces“ müssen ARP-Inspection-Prozedur durchlaufen

Alternativen / wie es früher war

- Port Security:
- Switch lernt die erste MAC-Adresse
- Kann “sticky” gehalten werden (übersteht reboot)
- Verhalten bei falscher MAC konfigurierbar (meist: Switchport shutdown bis der Admin ihn wieder freigibt)
- Syslog-Eintrag wird erzeugt, somit einfach zu monitoren
- Gilt auch für 802.1x / ARP Inspection / DHCP Snooping

Ende ;-)

Macht‘s gut, und danke für den Fisch.

Fragen?