

Virtuelle LANs am Arbeitsplatz bringen keine Sicherheit Kommunikationssicherheit auf dem Irrweg

von Dr. Behrooz Moayeri



Im Netzwerk Insider vom Juli/August 2007 wies der Autor darauf hin, dass Kommunikationssicherheit letztendlich immer mit Verschlüsselung einhergeht.

Dies leuchtet insbesondere dann ein, wenn man bedenkt, unter welchen Bedingungen man von einem „vertrauenswürdigen“ Netz sprechen kann. Ein IP-Netz ist nur dann vertrauenswürdig, wenn alle an dieses Netz angeschlossenen Systeme

me als vertrauenswürdig eingestuft werden können. Und dies wiederum setzt voraus, dass alle diejenigen Personen, die auf irgendwelche dieser Systeme uneingeschränkten Zugriff (zum Beispiel Administrationsrechte) haben, vertrauenswürdig sind. Kaum ein IP-Netz würde diese Bedingungen erfüllen.

Also bleibt zum Erreichen der Kommunikationssicherheit kein anderer Weg als

Ende-zu-Ende-Verschlüsselung. Wie im genannten Beitrag dargestellt, ist das auch der Weg, den man geht, wenn man zum Beispiel eine Banktransaktionen über das Internet durchführen muss. Es muss eine Ende-zu-Ende-Verschlüsselung geben, und die beiden Enden der Kommunikation müssen vertrauenswürdig sein, d.h. sowohl die involvierten Personen als auch die Endsysteme.

Schwerpunktthema

Virtuelle LANs am Arbeitsplatz bringen keine Sicherheit - Kommunikationssicherheit auf dem Irrweg



Dr. Behrooz Moayeri gehört der Geschäftsleitung der ComConsult Beratung und Planung GmbH an und beschäftigt sich seit ca. 15 Jahren mit Kommunikationssicherheit.

VLAN am Arbeitsplatz: warum und wie?

Virtuelle LANs sind keine neue Erfindung. Sie wurden in den 1990er Jahren dazu erfunden, Broadcast-Domänen in einer Layer-2-Struktur voneinander zu trennen. Die Technik wurde im Rahmen des Standards IEEE 802.1Q standardisiert. Mittels VLANs können mehrere logische Layer-2-Strukturen auf die selbe physikalische Struktur abgebildet werden (siehe Abbildung 1).

Die verschiedenen VLANs sind eigenständige Broadcast-Domänen, die untereinander nicht kommunizieren können, es sei denn, zwei oder mehr VLANs werden außerhalb der Layer-2-Struktur über einen anderen Switch, Router, Gateway, Firewall etc. miteinander verbunden. Aus der Sicht jedes der in der Abbildung 1 dargestellten VLANs handelt es sich bei der Layer-2-Struktur um ein „privates“ Netz; die anderen VLANs sind nicht sichtbar.

Die Voraussetzungen dafür, dass es so bleibt, dass also die verschiedenen VLANs tatsächlich „private“ Netze bleiben und von keinem VLAN aus auf ein anderes VLAN zugegriffen werden kann, sind wie folgt:

- Der Zugriff auf den Layer-2-Switch, der die VLANs voneinander trennt, über den aber Verkehrsströme aller VLANs übertragen werden, bleibt Personen vorenthalten, die aus der Sicht jeder Benutzergruppe vertrauenswürdig sind, ungefähr vergleichbar mit dem Service Provider, der die Daten verschiedener Kunden über die eigene Infrastruktur überträgt und insofern aus der Sicht aller Kunden vertrauenswürdig sein muss.
- Der Layer-2-Switch ist resistent gegen Angriffe, die auf die Aufhebung der Grenzen zwischen den VLANs abzielen, zum Beispiel einen Angriff namens MAC Flooding, der Pakete mit so vielen verschiedenen Source-Adressen an einen Switch sendet, dass dieser gemäß dem Standard IEEE 802.1D Pakete fluten muss. Wenn der Switch diese Paketflutung ohne Rücksicht auf VLAN-Grenzen durchführt, ist der Angreifer am Ziel.
- Die verschiedenen VLANs sind in den beiden Bereichen, in denen nicht vertrauenswürdige Personen präsent sind, auch physikalisch voneinander getrennt. Zum Beispiel darf kein dem

Der Benutzer muss zu seinem eigenen Endgerät Vertrauen haben, damit auch zu allen Personen mit administrativem Zugriff auf das Endgerät, und er muss sicherstellen können, dass es sich zum Beispiel bei dem anderen Ende des Kommunikationspfades um den Webserver seiner Bank handelt. Dies wird durch Authentifizierung mittels einer Public Key Infrastructure (PKI) erreicht.

Aber diese fundamentalen Erkenntnisse scheinen in der Kommunikationswelt nicht überall angekommen zu sein. Sonst wäre nicht zu erklären, warum statt der Ende-zu-Ende-Verschlüsselung häufig andere Wege zum Erreichen einer sicheren Kommunikation beschritten werden. Dabei handelt es sich teilweise um Irrwege.

Der vorliegende Beitrag geht auf diese Irrwege ein. Konkret wird begründet, warum Virtual Local Area Networks (VLANs) am Arbeitsplatz keine Sicherheit bringen. Genau dieser Weg, nämlich die Bildung verschiedener VLANs am Arbeitsplatz, wird häufig als eine Methode dargestellt, die Sicherheit der einen vor der anderen Anwendung oder des einen Endgeräts vor den anderen zu erreichen.

Zunächst werden die Konzepte kurz vorgestellt, die mittels VLANs am Arbeitsplatz angeblich für mehr Sicherheit sorgen. Anschließend wird begründet, warum diese Konzepte ohne eine Authentifizierung der Endgeräte im Netz inkonsequent und lückenhaft bleiben. Es folgt eine Darstellung der fundamentalen Schwächen einer reinen Geräteauthentifizierung ohne Verschlüsselung oder zumindest Paketauthentifizierung. Dann wird darauf eingegangen, ob und wie diese Schwächen behoben werden können.

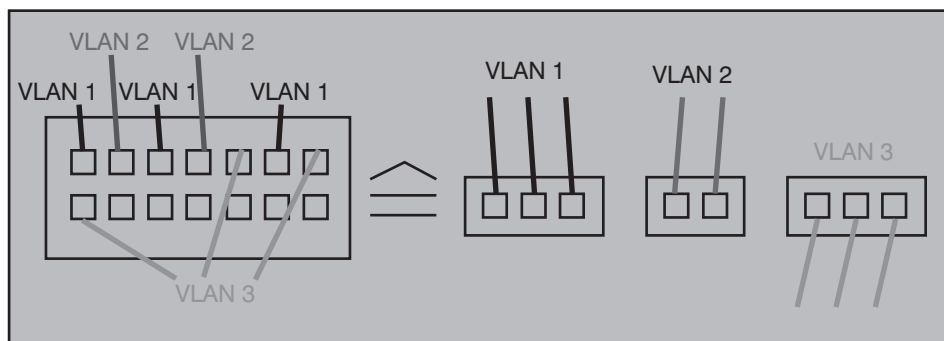


Abbildung 1: Abbildung mehrerer VLANs auf eine Layer-2-Struktur

Virtuelle LANs am Arbeitsplatz bringen keine Sicherheit - Kommunikationssicherheit auf dem Irrweg

VLAN 1 zugeordnetes Endgerät bzw. Anwendung durch einfaches Umstecken eines Kabels, Manipulation eines VLAN Tags gemäß IEEE 802.1Q etc. in die Lage versetzt werden können, Zugriff auf VLAN 2 zu erlangen.

Diese Voraussetzungen sind ungefähr mit den Bedingungen vergleichbar, unter denen Service Provider Virtual Private Networks (VPNs) implementieren und ihren Kunden anbieten. Der Kunde A ist über eine dedizierte Leitung mit einem Provider Edge (PE) Router verbunden, der auch andere Kunden bedient. Administrativen Zugriff auf den PE Router hat nur der Service Provider als vertrauenswürdige Instanz für alle Kunden. Die LANs der Kunden sind physikalisch voneinander getrennt, d.h. kein Kunde hat physikalischen Zugriff auf das LAN eines anderen Kunden. Der PE Router und alle anderen Komponenten, welche gemischte Datenströme verschiedener Kunden übertragen, widersteht Angriffen mit dem Ziel des Durchbruchs durch die Grenzen zwischen den VPN.

Ein Service Provider kann nach dem selben Modell auch VPNs aufbauen, die auf VLAN-Technik basieren: Die beiden Kunden A und B unterhalten getrennte physikalische Infrastrukturen, die aber beide mit einem Layer-2-Switch des Providers verbunden sind, allerdings mit verschiedenen VLANs auf diesem Switch. Wenn die o.g. Voraussetzungen erfüllt sind, gelten die VLANs als VPNs.

Aber in den letzten Jahren ist eine etwas andere Nutzung von VLANs als „Sicherheitsmechanismus“ üblich geworden, vor allem mit der Einführung der IP-Telefonie. Dieses Modell basiert darauf, dass verschiedene VLANs bis zu jedem Arbeitsplatz verlängert werden. Dieses Modell ist in drei verschiedenen Varianten in der Abbildung 2 dargestellt.

In allen dargestellten drei Varianten sind der Computer und das IP-Telefon verschiedenen VLANs zugeordnet. In den meisten Fällen befinden sich ein Computer und ein Telefon im selben Raum und werden von der selben Person genutzt. Insofern wird das Prinzip der physikalischen Trennung zwischen den VLANs nicht mehr eingehalten. Der Benutzer könnte seinen PC an das VLAN 1 (das dem Telefon vorenthalte VLAN) anschließen und umgekehrt. Unter solchen Bedingungen lassen sich die VLAN-Grenzen technisch nicht erzwingen. Die VLAN-Trennung bringt also keine Sicherheit.

Die drei Szenarien unterscheiden sich in den Details. In dem ersten Szenario, das

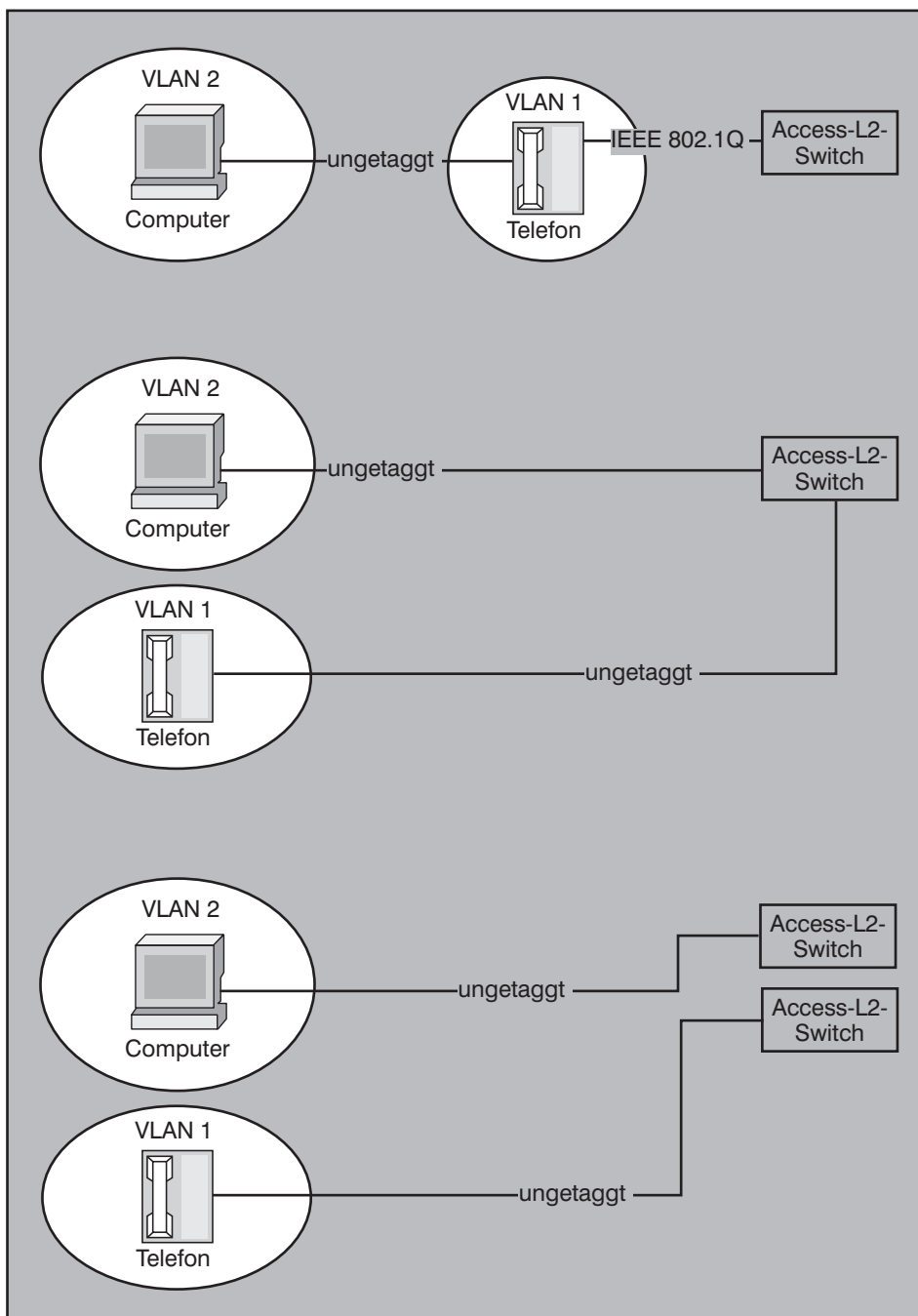


Abbildung 2: VLANs am Arbeitsplatz

im oberen Teil der Abbildung 2 dargestellt ist, und das in den meisten Unternehmen aus Kostengründen (zur Einsparung von Access Switch Ports und Kabeln) angewandt wird, ist der PC an einen Miniswitch im Telefon angeschlossen. Dieser Miniswitch leitet zum Beispiel in einer gängigen Konfiguration die Pakete des PCs ohne einen VLAN Tag gemäß IEEE 802.1Q weiter, während die Pakete des Telefons selbst mit einem IEEE 802.1Q Tag versehen werden, der die VLAN ID für das „Voice VLAN“ enthält (siehe Abbildung 3).

In der anderen Richtung versieht der Access Switch alle für das Telefon bestimmten Pakete mit der VLAN ID für Voice und lässt die Pakete an den PC ungetaggt. Damit diese Konfiguration funktioniert, muss das IP-Telefon die VLAN ID für Voice kennen. Dies kann durch verschiedene Verfahren sichergestellt werden:

- Das aufwändigste Verfahren besteht darin, dass die Voice VLAN ID manuell an jedem IP-Telefon konfiguriert wird. Dies bedeutet, dass bei jenen Umzügen, in denen sich die zu nutzende

Virtuelle LANs am Arbeitsplatz bringen keine Sicherheit - Kommunikationssicherheit auf dem Irrweg

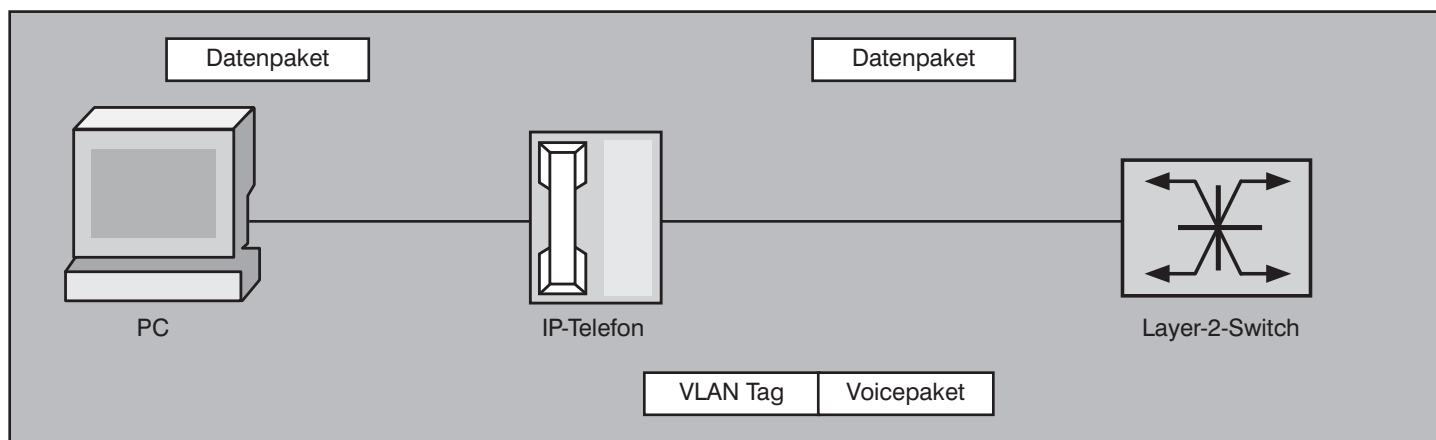


Abbildung 3: Tagging durch das Telefon

Voice VLAN ID ändert, eine Änderung am Telefon erforderlich ist. Im laufenden Betrieb kann dies mit zwei wesentlichen Nachteilen verbunden sein: mit erhöhtem Betriebsaufwand und mit längeren Wartezeiten von Benutzern, bevor sie nach Umzügen arbeitsfähig sind.

- Ein anderes Verfahren, dass von einigen Herstellern von IP-Telefonen angewandt wird, besteht darin, dass das Telefon zunächst im gleichen VLAN wie der PC bootet und ungetaggt kommuniziert. Das Telefon erhält temporär eine IP-Adresse aus dem Adressbereich für PCs. Gleichzeitig bekommt das Telefon auch eine VLAN ID für Voice zugewiesen. Dann schaltet das Telefon auf das Voice VLAN um und beantragt in diesem VLAN mit der richtigen VLAN ID eine neue IP-Adresse.
- Das dritte Verfahren besteht darin, dass das IP-Telefon und der Access Switch miteinander über ein Protokoll der Schicht 2 kommunizieren, das vor der IP-Konfiguration des Telefons diesem die Möglichkeit gibt, die passende Voice VLAN ID vom Access Switch in Erfahrung zu bringen. Ein solches Protokoll gab es zunächst nur als das proprietäres Cisco Discovery Protocol (CDP). Diejenigen Unternehmen, die sich für die Konfiguration der Voice VLAN ID mittels CDP entschieden haben, haben zugleich eine Konstellation geschaffen, in der sowohl der Access Switch als auch das Telefon von Cisco stammen müssen. Man kann dann ohne Umstellung des Netzes keine anderen Telefone einsetzen und umgekehrt, was eine wesentliche Abhängigkeit von einem Hersteller bedeutet. Seit 2005 gibt es aber auch den Standard IEEE 802.1AB mit dem Titel „Station and Media Access Control Connectivity Discovery“, in dem das Link Layer Discovery Protocol (LLDP) spezifiziert

ist. Dieses Protokoll soll ein standardisiertes Pendant zu CDP darstellen. In jüngster Zeit sind Switches und IP-Telefone auf den Markt gekommen, die angeblich LLDP unterstützen. Der Autor hat bisher jedoch keine funktionierende Abstimmung der Voice VLAN ID zwischen einem Telefon und einem Switch auf der Basis von LLDP gesehen. Hinzu kommt, dass CDP (und künftig auch LLDP) aus dem Blickwinkel der Informationssicherheit kritisch gesehen wird. Nicht ohne Grund ist ein Bestandteil vieler Sicherheitsaudits in Cisco-Umgebungen die Empfehlung, CDP abzuschalten. Darüber kann nämlich ein Angreifer wertvolle Informationen über das Netz in Erfahrung bringen. CDP und LLDP sind durch keinerlei Sicherheitsmechanismus geschützt.

Die anderen beiden in der Abbildung 2 dargestellten Varianten sind etwas einfacher als die oberste Variante. Die zweite Variante sieht die Verwendung unterschiedlicher Ports und die dritte sogar die Verwendung unterschiedlicher Switches für PC und Telefon vor. Die Notwendigkeit von VLAN Tagging bis zum Arbeitsplatz entfällt somit. Verschiedene VLANs nutzen verschiedene Kabel und Dosen am Arbeitsplatz.

Allen drei Varianten ist jedoch gemeinsam, dass die VLAN-Trennung auf das Wohlverhalten aller beteiligten Personen angewiesen ist. In keiner Variante kann technisch verhindert werden, dass ein Telefon an das PC-VLAN angeschlossen wird oder umgekehrt. Dazu bedarf es mehr, nämlich der fälschungssicheren Authentifizierung

Jetzt Leser werden

Der Netzwerk Insider

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.



Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:

<http://www.comconsult-akademie.de/de/Registrierung.php>

Virtuelle LANs am Arbeitsplatz bringen keine Sicherheit - Kommunikationssicherheit auf dem Irrweg

von Endgeräten und der Zuweisung dieser zum richtigen VLAN.

Authentifizierung und VLAN-Zuweisung

Erst dann, wenn technisch verhindert werden kann, dass ein Endgerät an das falsche VLAN angeschlossen wird, gilt die VLAN-Trennung als wirklicher Sicherheitsmechanismus. Deshalb ist die VLAN-Trennung am Arbeitsplatz unweigerlich mit der Authentifizierung von Endgeräten verbunden.

Seit 2004 gibt es nämlich den Standard IEEE 802.1X mit dem Titel Port-Based Network Access Control. Ohne Port-basierende Authentifizierung erlauben Netze gemäß den Standards der Standardfamilie IEEE 802 (LAN) auch nicht autorisierten Geräten bzw. Benutzern den Zugriff auf die LAN-Infrastruktur. Die Authentifizierung eines Benutzers erfolgt üblicherweise über ein Network Operating System (NOS) auf der Ebene höherer OSI-Schichten (5-7). Die Infrastruktur-Komponenten eines LANs (OSI-Layer 2) sind an diesem Anmeldeprozess in der Regel nicht betei-

ligt. Die Identifizierung des Benutzers ist eine NOS- oder Sicherheitsfunktion und nicht Bestandteil der Aufgaben des Netzes selbst.

Aus diesen Gründen wurde die Idee von IEEE 802.1X geboren, nämlich die Idee der Port-basierten Netzzugangskontrolle. Unter Ausnutzung der physikalischen Besonderheiten des Netzzugriffs in einem LAN werden gemäß IEEE 802.1X Authentifizierungsvorrichtungen an den LAN-Ports bereitgestellt. Unter Ports werden dabei Ports von MAC Bridges gemäß IEEE 802.1D (d.h. Layer-2-Switches), von Routern und Access-Points in einem Wireless LAN nach IEEE 802.11 verstanden. Ziel ist die Bereitstellung einer zusätzlichen Systemfunktion auf OSI-Layer 2, um den unautorisierten Zugang zum System oder zu einem Dienst des Systems zu unterbinden. Dabei werden die beim Remote Access Service (RAS) auf genutzten Authentifizierungsmechanismen auf das LAN übertragen.

Gemäß IEEE 802.1X können einem Port zwei unterschiedliche Rollen zugeordnet werden:

- Authenticator: Dieser Port verlangt eine Authentifizierung, bevor er den Zugang zu einem Dienst erlaubt, der über diesen Port erreicht werden kann.
- Supplicant: Dieser Port möchte den Zugang zu einem Dienst erlangen, der vom System des Authenticators angeboten wird.

Um einen vollständigen Authentifizierungsablauf zu ermöglichen, wird schließlich noch ein Authentication Server benötigt. Der Authentication Server bietet für den Authenticator die notwendige Authentifizierungsfunktion an, um die Login-Daten des Supplicants zu überprüfen. Der Server überprüft, ob der Supplicant autorisiert ist, Zugang zu dem über den Authenticator angebotenen Dienst zu erlangen.

Damit eine Geräteauthentifizierung gemäß IEEE 802.1X funktioniert, müssen daher folgende Bedingungen erfüllt sein:

- Das Gerät, das authentifiziert und somit Zugang zum Netz erhalten soll (Supplicant), muss eine Authentifizierung

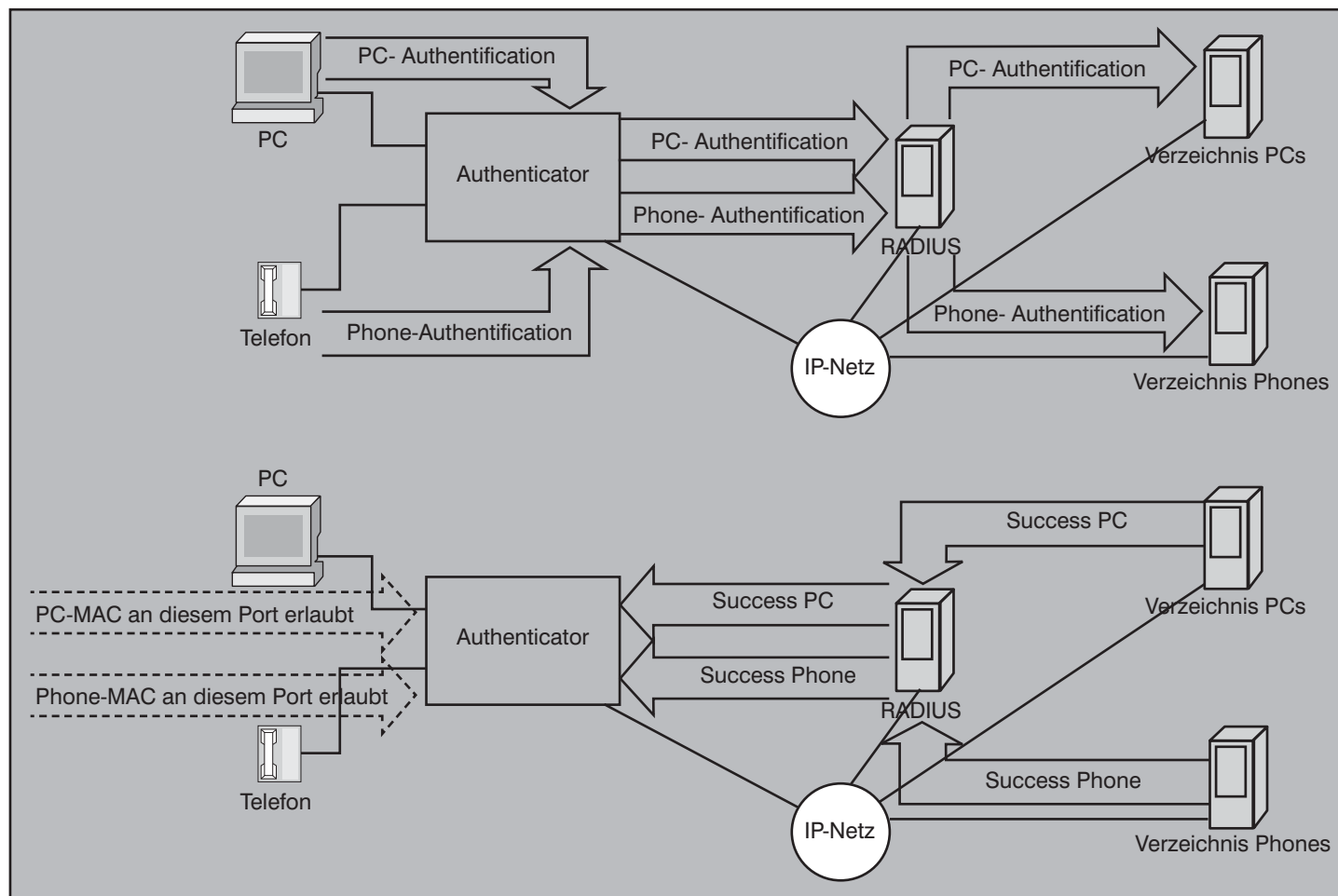


Abbildung 4: Authentifizierung von zwei Endgeräten an zwei verschiedenen Ports

Virtuelle LANs am Arbeitsplatz bringen keine Sicherheit - Kommunikationssicherheit auf dem Irrweg

gemäß dem im Standard IEEE 802.1X vorgesehenen Extensible Authentication Protocol Over LAN (EAPOL) unterstützen.

- Die Netzkomponente, die den Zugang des Endgerätes zum Netz sichern und prüfen soll, ob dazu die Bedingung der Authentifizierung erfüllt ist, muss die im Standard vorgesehene Rolle des Authenticators übernehmen.
- Im Hintergrund muss der Authenticator mit dem Authentifizierungsserver kommunizieren und die Daten, die der Supplicant zwecks Authentifizierung übergeben hat, an den Server weiterleiten, damit dieser die Berechtigung des Endgerätes für die Erlangung des Netzzugangs prüfen kann.
- Da es mehrere Methoden der Authentifizierung gibt, müssen der Supplicant und der Authentifizierungsserver mindestens eine gemeinsame Methode unterstützen, zum Beispiel die Verwendung von Zertifikaten gemäß dem Standard Transport Layer Security (TLS). In diesem Fall würde die Authentifizierungsmethode EAP-TLS heißen.

Eine Erweiterung der Vorgänge gemäß IEEE 802.1X besteht darin, abhängig vom Ergebnis der Authentifizierung eine Zuordnung des Endgerätes zu einem VLAN zu veranlassen. Dies erfolgt in der Regel durch eine Anweisung des Authentifizierungsservers an den Authenticator, zum Beispiel den LAN-Switch, das authentifizierte Endgerät einem bestimmten VLAN zuzuweisen. Somit ist auf den ersten Blick nicht nur für eine Authentifizierung der an das Netz angeschlossenen Endgeräte gesorgt, sondern darüber hinaus auch für ihre Zuordnung zum richtigen VLAN zu somit zur richtigen Vertrauensdomäne.

Die Abbildung 4 zeigt den Fall, dass zwei Endgeräte unterschiedlichen Typs an zwei verschiedene Ports eines LAN-Switches angeschlossen sind. Der PC und das IP-Telefon stellen jeweils einen Authentifizierungsrequest, der über den LAN-Switch (den Authenticator) an den Authentifizierungsserver, in der Regel einen Remote Access Dial-In User Service (RADIUS) weitergeleitet wird. Dieser kann die

Requests je nach Endgerätetyp an verschiedene nachgelagerte Authentifizierungsdienste übergeben, zum Beispiel Verzeichnisserver für PCs und Telefone. Diese überprüfen den Authentifizierungsrequest und beantworten ihn positiv, wenn die Bedingungen für die Authentifizierung erfüllt sind (zum Beispiel wenn ein Challenge-Response-Verfahren erfolgreich abgeschlossen wird). Danach lässt der LAN-Switch das authentifizierte Endgerät ins Netz und schaltet in der Regel die MAC-Adresse des Endgerätes an dem verwendeten Port frei.

Nicht nur die Authentifizierung eines Endgerätes, sondern auch dessen Zuordnung zu einem VLAN kann abhängig vom Ergebnis der Authentifizierung erfolgen. Wie in der Abbildung 5 dargestellt kann der Authentifizierungsserver zwischen verschiedenen Gruppen von Supplicants unterscheiden und bei Erkennung einer bestimmten Gruppe den Authenticator anweisen, das Endgerät einem bestimmten VLAN zuzuordnen. In der Abbildung 5 wird der PC dem VLAN 1 und das IP-Telefon dem VLAN 2 zugeordnet. Technisch

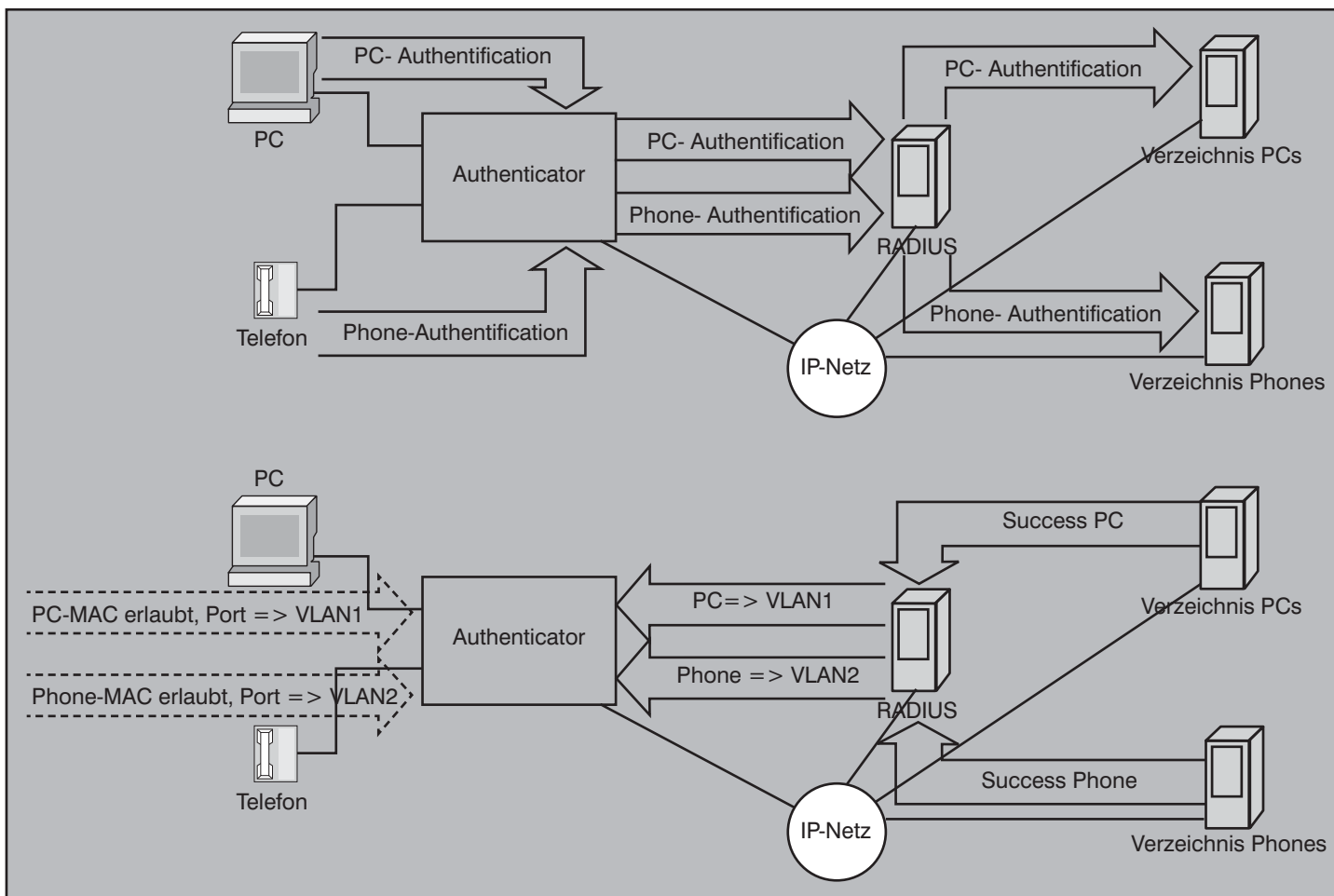


Abbildung 5: Dynamische VLAN-Zuweisung

Virtuelle LANs am Arbeitsplatz bringen keine Sicherheit - Kommunikationssicherheit auf dem Irrweg

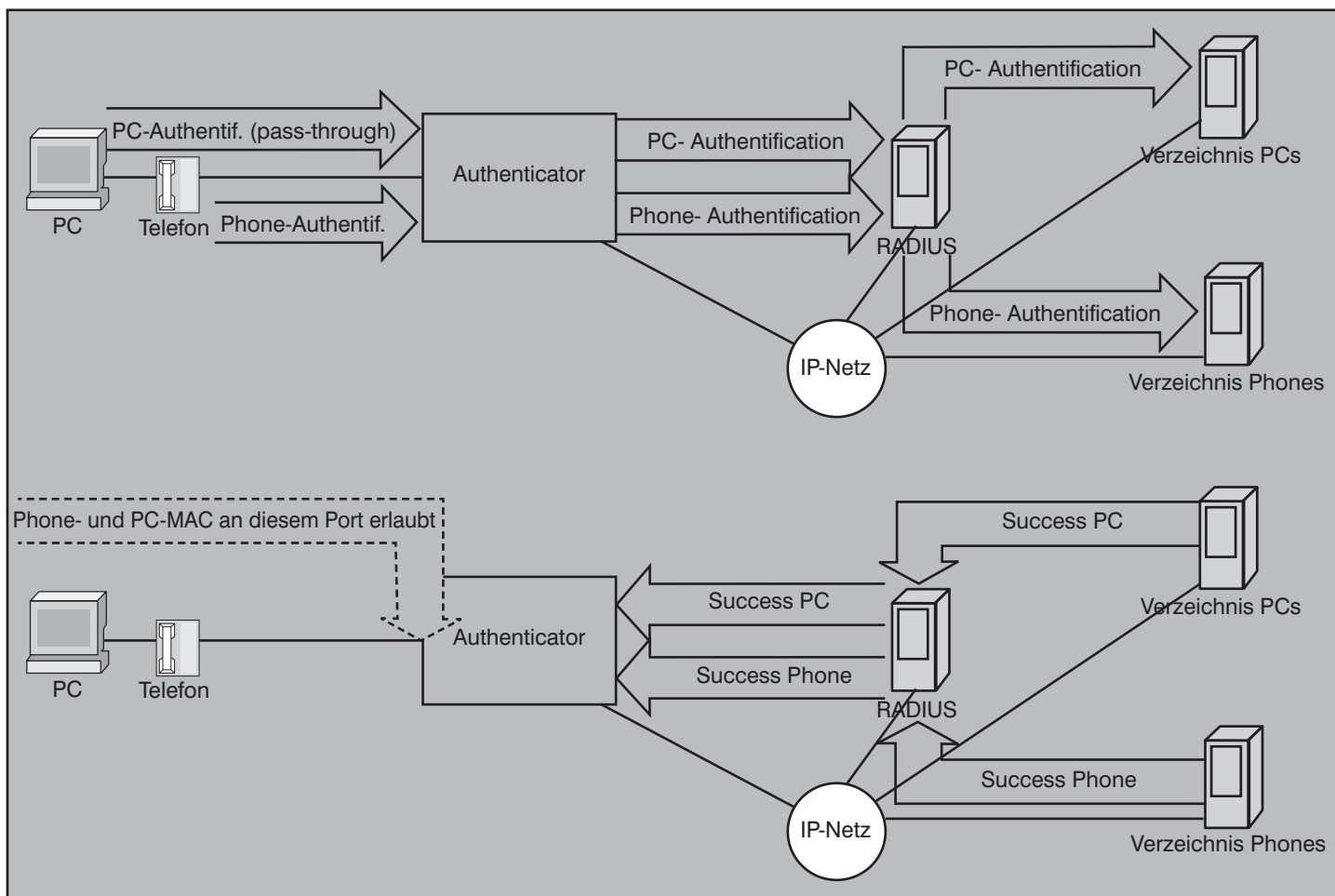


Abbildung 6: Authentifizierung von zwei Endgeräten an einem Port

erfolgt dies so, dass der LAN-Switch die beiden eigenen Ports, an die der PC bzw. das Telefon angeschlossen sind, mit dem VLAN 1 bzw. VLAN 2 verbindet.

Der Fall, dass zwei Endgeräte an ein und den selben Port des LAN-Switches angeschlossen werden, ist in der Abbildung 6 dargestellt. Ein gängiges Beispiel dafür ist die Kaskadierung eines PCs und eines Telefons, indem der PC mit dem so genannten PC-Port des Telefons verbunden wird. In vielen IP-Telefonen ist ein Mini-Switch integriert, der dazu verwendet wird, den selben Port am Switch und das selbe Kabel zwischen dem Arbeitsplatz und dem Verteilerraum zwei Endgeräten zur Verfügung zu stellen und Kosten für Switch Ports und Kabel einzusparen.

Wie aus der Abbildung 6 hervorgeht, erhält der LAN-Switch (Authenticator) am selben Port die Authentifizierungsrequests von zwei Endgeräten (PC und Telefon) und muss diese weiter leiten. Der LAN-Switch muss in der Lage sein, den Authentifizierungsstatus von mehr als einem Endgerät pro Port zu überwachen

und mehr als eine authentifizierte MAC-Adresse pro Port zuzulassen.

Damit der Authentifizierungsrequest des PCs den Authenticator erreicht, muss das IP-Telefon, das zwischen PC und LAN-Switch geschaltet ist, die Kommunikation zwischen PC und Authenticator unverändert weiter leiten, d.h. im so genannten Pass-Through-Modus arbeiten.

Dabei ist die Überwachung des Authentifizierungsstatus jedes Endgerätes von Bedeutung. Es muss verhindert werden, dass ein „Trittbrettfahrer“ eine bereits erfolgte Authentifizierung zum Eindringen in das Netz missbraucht. Abbildung 7 zeigt eine gängige Variante der Überwachung des Authentifizierungsstatus an einem Switch-Port. Die meisten Switches, die IEEE 802.1X unterstützen, überwachen den Status des physikalischen Links an einem Port. Der Wechsel dieses Status von aktiv (up) zu inaktiv (down) wird vom Switch (Authenticator) als ein Ereignis gewertet, welches den Status des bisher an den Port angeschlossenen Endgerätes von „authentifziert“ in „nicht authentifziert“

ändert. Das muss sein, weil sonst ein beliebiges Ersetzen authentifzierter Endgeräte durch andere Endgeräte möglich wäre. Überwacht der Switch den Status des Links, führt jede auch nur kurzzeitige Unterbrechung der Kabelverbindung zwischen Switch und Endgerät dazu, dass die Authentifizierung wiederholt werden muss.

Der Authenticator kann nur den Status jener physikalischen Verbindungen überwachen, die an seinen eigenen Ports terminiert werden. Dabei entsteht eine Sicherheitslücke, die in der Abbildung 8 dargestellt ist. Zwei Endgeräte sind an ein und dem selben Port eines Switches authentifziert, sodass die zu den beiden Endgeräten gehörenden MAC-Adressen an diesem Port zugelassen sind. Der Authenticator überwacht den Status der physikalischen Verbindung zum IP-Telefon. Aber nicht das Telefon, sondern der PC, der an den PC-Port des Telefons angeschlossen ist, wird durch ein anderes Endgerät ersetzt. Von diesem Wechsel der physikalischen Verbindung zwischen Telefon und PC in den inaktiven Status er-

Virtuelle LANs am Arbeitsplatz bringen keine Sicherheit - Kommunikationssicherheit auf dem Irrweg

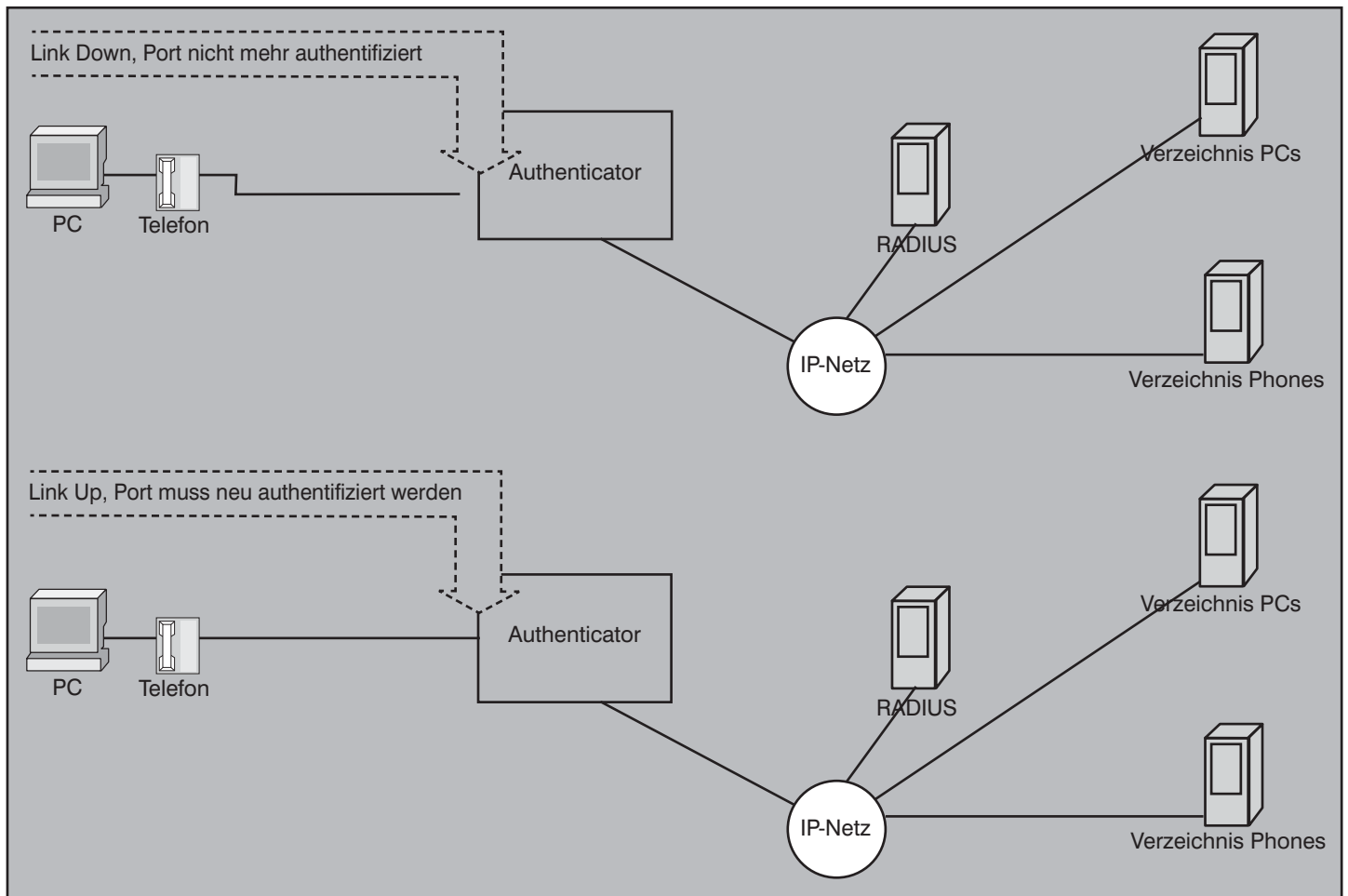


Abbildung 7: Überwachung des Link-Status

fährt der Authenticator nichts, weil er nur die direkt an den eigenen Ports endenden Verbindungen überwachen kann. So kann ein Endgerät lediglich durch Einstellung der MAC-Adresse des authentifizierten PCs den Zugang zum Netz erlangen, ohne die Bedingungen der Authentifizierung (Zertifikat etc.) erfüllen zu müssen.

Um die in der Abbildung 8 dargestellte Sicherheitslücke zu schließen, haben einige Hersteller von IP-Telefonen die so genannte Proxy-Logoff-Funktion in ihren IP-Telefonen implementiert. Wie in der Abbildung 9 dargestellt besteht diese Funktion darin, dass statt des LAN-Switches das IP-Telefon den Zustand des Links zwischen dem IP-Telefon und dem PC überwacht. Wechselt dieser Zustand von aktiv zu inaktiv, meldet das Telefon stellvertretend für den PC diesen beim Authenticator ab (daher die Bezeichnung Proxy Logoff). Beim erneuten Versuch des Zugriffs auf das Netz fordert der Authenticator von dem Endgerät, das an den PC-Port des Telefons angeschlossen ist, eine neue Authentifizierung. Ein Endgerät, das die Bedingungen der Authentifizierung nicht erfüllt, wird

Jetzt Leser werden

Der Netzwerk Insider

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.



Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:

<http://www.comconsult-akademie.de/de/Registrierung.php>

Virtuelle LANs am Arbeitsplatz bringen keine Sicherheit - Kommunikationssicherheit auf dem Irrweg

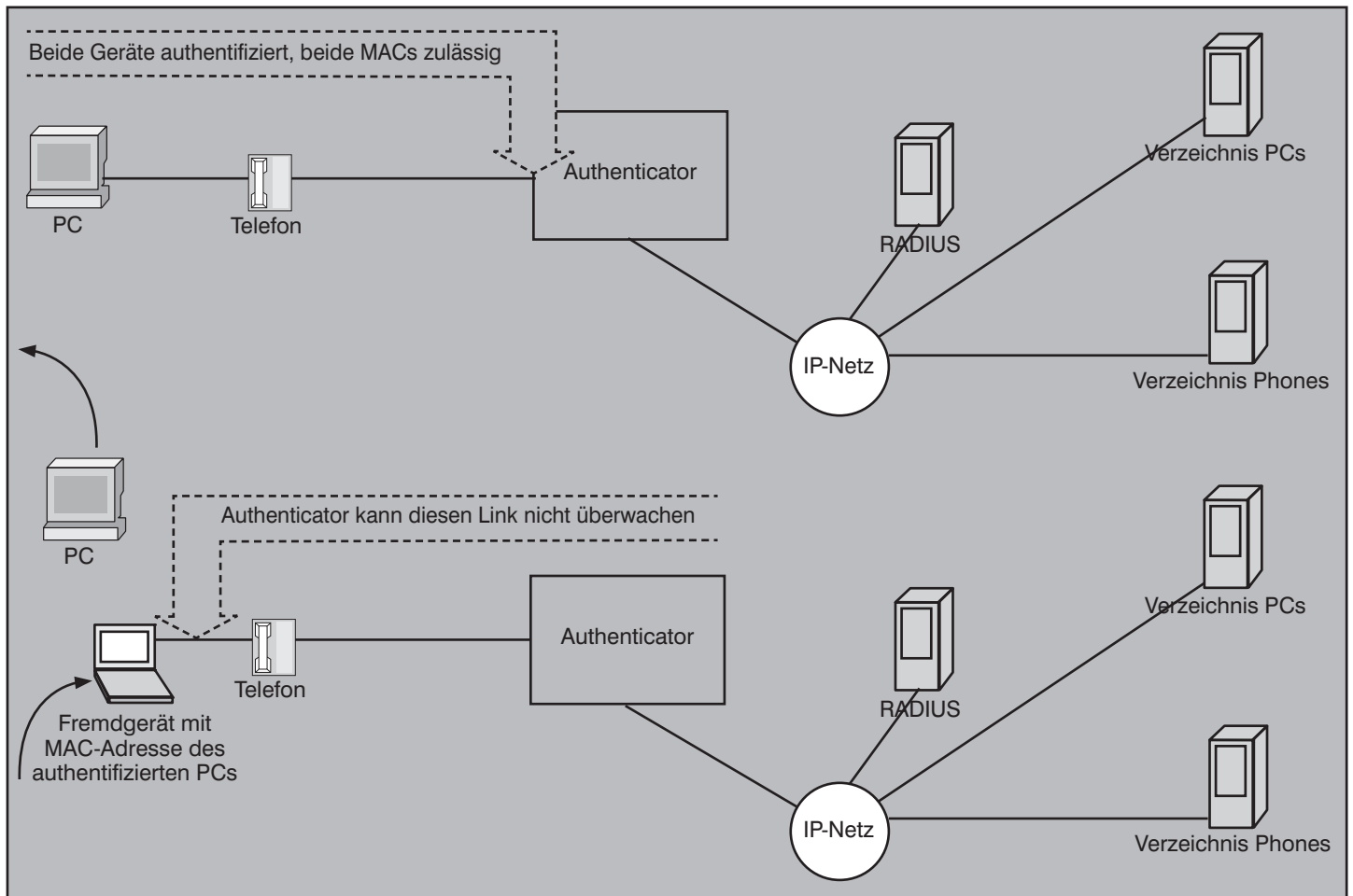


Abbildung 8: Authenticator kann Link zwischen Telefon und PC nicht überwachen

nicht in das Netz gelassen.

Unabhängig davon, ob das IP-Telefon im Pass-Through- oder Proxy-Logoff-Modus arbeitet, ist bei Anschluss eines PCs an den PC-Port des Telefons die dynamische Zuordnung der beiden Endgeräte zu verschiedenen VLANs komplexer als bei Verwendung von zwei verschiedenen Ports des LAN-Switches durch die beiden Endgeräte. Wie aus der Abbildung 10 hervorgeht, bedarf es dazu nicht nur einer Anweisung an den LAN-Switch, die Pakete von Telefon und PC verschiedenen VLANs zuzuordnen, sondern auch einer dynamischen VLAN-Zuordnung auf dem Telefon selbst. Ist diese dynamische VLAN-Zuordnung mit einem Protokoll wie Cisco Discovery Protocol (CDP) bzw. Link Layer Discovery Protocol (LLDP) sichergestellt, kann sie nicht vom Ergebnis einer Authentifizierung gemäß IEEE 802.1X abhängig gemacht werden, denn CDP bzw. LLDP sind in der Regel unabhängig von einem Authentifizierungsprozess. Bei diesen Protokollen handelt es sich um Kommunikationsbeziehungen, die auf eine physikalische Verbindung begrenzt sind.

Jetzt Leser werden

Der Netzwerk Insider

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.



Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:

<http://www.comconsult-akademie.de/de/Registrierung.php>

Virtuelle LANs am Arbeitsplatz bringen keine Sicherheit - Kommunikationssicherheit auf dem Irrweg

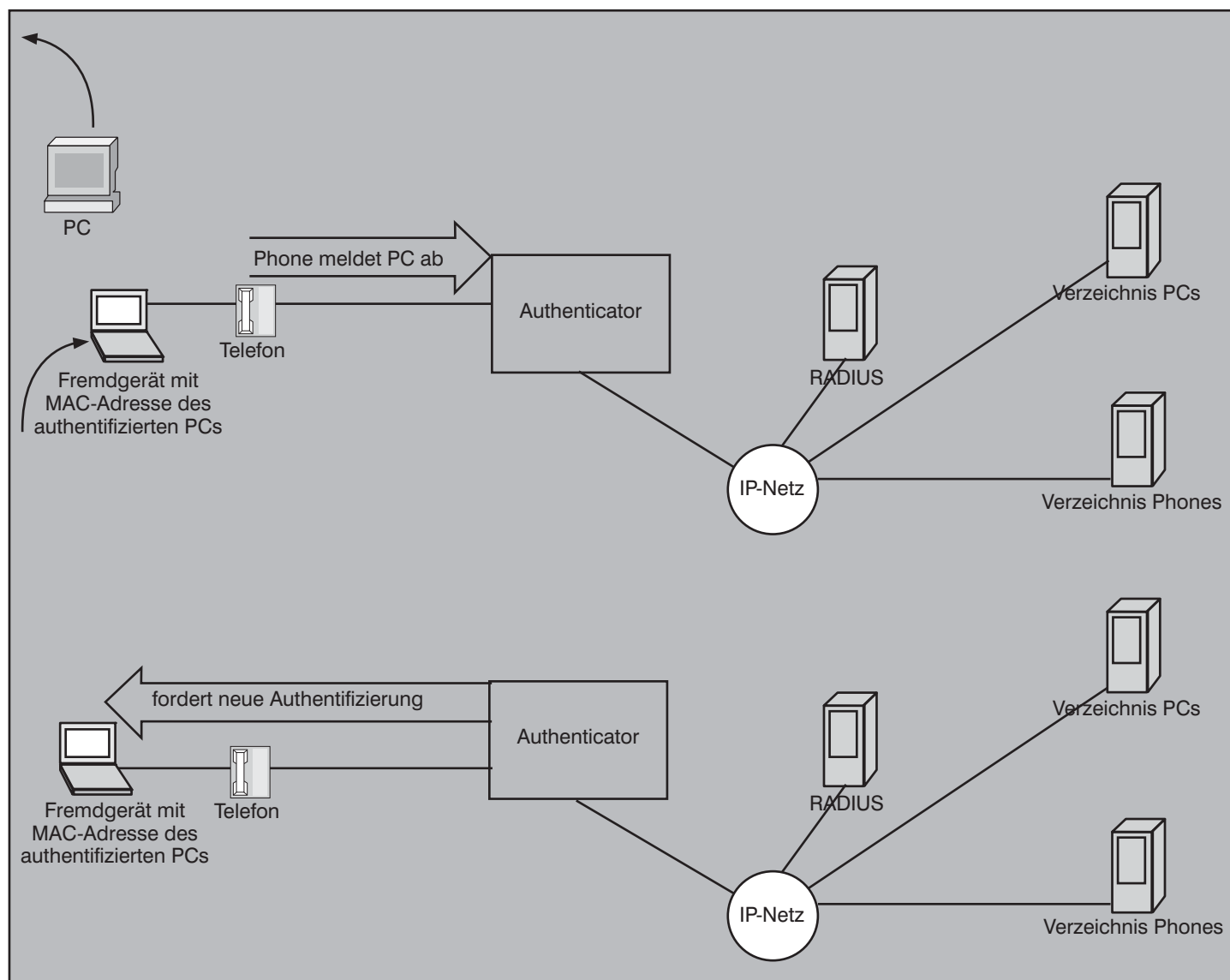


Abbildung 9: Proxy Logoff

Außerdem unterstützen viele LAN-Switches die dynamische VLAN-Zuweisung nur bei Ports, die nicht als so genannte Trunk Ports konfiguriert sind, sondern Pakete ohne VLAN-Zuordnung übertragen.

Aber selbst wenn die dargestellten Probleme auf Umwegen wie zum Beispiel mehrstufige DHCP-Kommunikation gelöst werden, bleiben, wie der nächste Abschnitt zeigen wird, wesentliche Sicherheitslücken.

Grenzen der reinen Geräteauthentifizierung

Der Standard IEEE 802.1X beschreibt eine reine Geräteauthentifizierung, ohne dass nach der Authentifizierung des Gerätes dessen Pakete ebenfalls authentifiziert werden. Hier kommt es zu einem Problem,

das bei jedem Szenario der reinen Geräteauthentifizierung am Anfang einer Verbindung entsteht, nämlich zu dem Problem, dass eine einmal erfolgreiche Authentifizierung von einem „Trittbrettfahrer“ missbraucht werden kann.

Die Abbildung 11 zeigt dieses prinzipielle Problem bei IEEE 802.1X. Ist das Endgerät mit der MAC-Adresse A an einem Switch authentifiziert, kann diese Authentifizierung von jedem Endgerät missbraucht werden, dass die MAC-Adresse A verwendet. Der Angreifer kann nämlich zwischen dem Supplicant und dem Authenticator einen Hub einsetzen. Der Authenticator kann nach dieser Aktion zwar die erneute Authentifizierung des Gerätes mit der MAC-Adresse A erzwingen, aber nicht mehr kontrollieren, ob außer dem authentifizierten Endgerät nicht auch noch ein anderes Endgerät

die MAC-Adresse A verwendet. Das kann durchaus der Fall sein, nämlich wenn an den zwischen Supplicant und Authenticator eingesetzten Hub ein weiteres Gerät angeschlossen wird, an dem die MAC-Adresse A eingestellt ist. Auch wenn die Authentifizierung periodisch wiederholt wird, hat sie nur das Ergebnis, eine bestimmte MAC-Adresse an einem Port des Switches freizugeben. Da die Pakete des authentifizierten Endgerätes nicht einzeln authentifiziert werden, kann der Authenticator nicht zwischen den Paketen des authentifizierten Endgerätes und den anderen Paketen unterscheiden, die als Source-Adresse die MAC-Adresse A tragen.

Da der Hub alle empfangenen Pakete auf alle Ports flutet, findet an keiner Stelle eine Prüfung statt, ob das an den Hub angeschlossene Endgerät die MAC-Adresse A

Virtuelle LANs am Arbeitsplatz bringen keine Sicherheit - Kommunikationssicherheit auf dem Irrweg

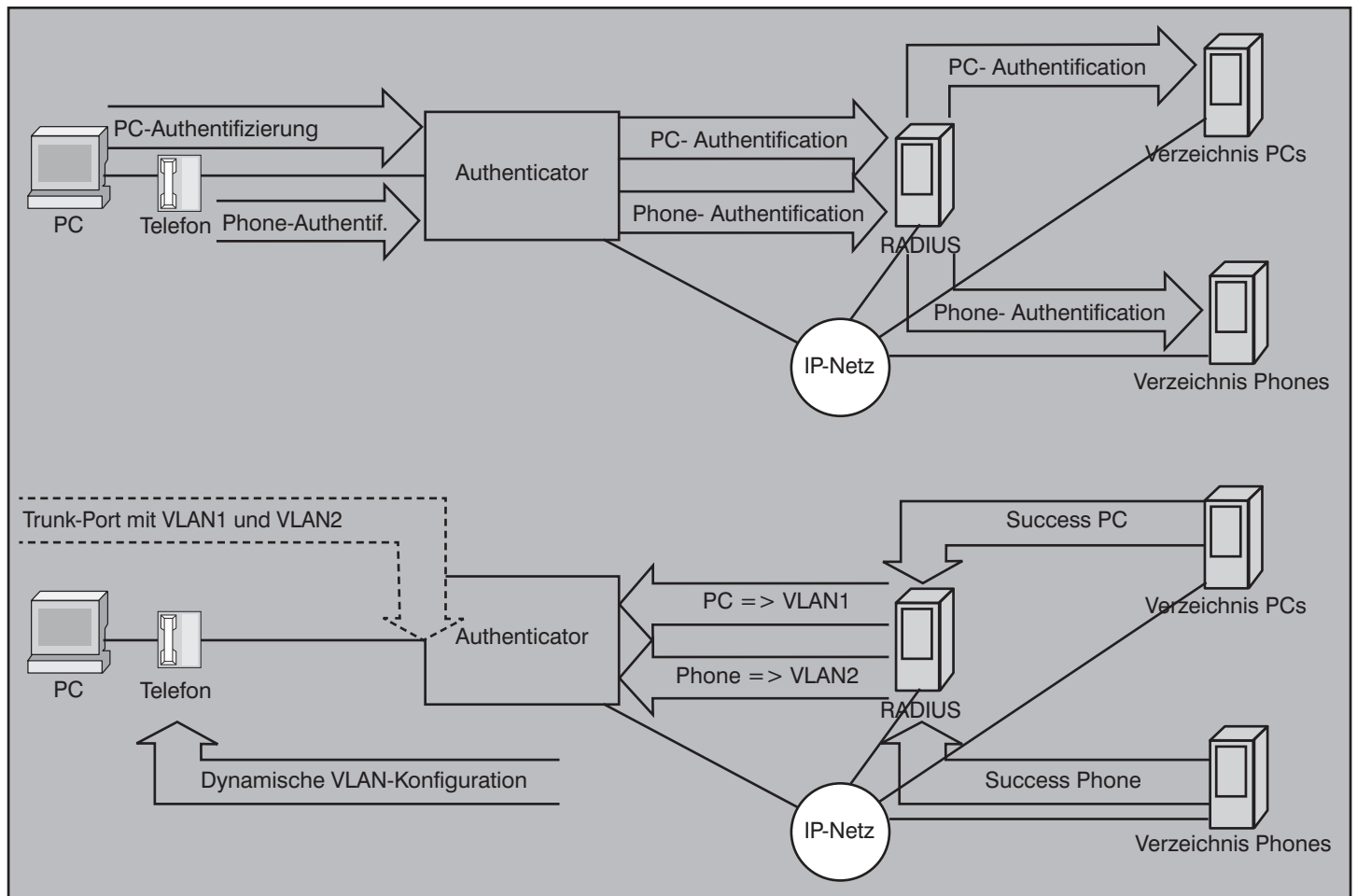


Abbildung 10: Dynamische VLAN-Zuordnung bei Kaskadierung von PC und Telefon

fälscht. Lediglich der authentifizierte PC mit der selben MAC-Adresse könnte erkennen, dass ein anderes Endgerät diese Adresse auch verwendet. Selbst wenn man auf allen Endgeräten einen Mechanismus implementieren würde, der bei einem solchen Ereignis Alarm schlägt (was bei den gängigen Endgerätetypen nicht möglich ist), kann der Angreifer leicht solche Alarmmeldungen am Hub blockieren. Er könnte darüber hinaus dafür sorgen, dass die Pakete des zusätzlich hinzugefügten Endgerätes nicht an das Endgerät weiter geleitet wird, das die MAC-Adresse A legitim besitzt. Dazu könnte zum Beispiel statt eines Hubs ein Switch eingesetzt werden, der mittels eines Filters alle Pakete mit der Source-Adresse A an dem zum authentifzierten PC gerichteten Port blockiert.

Das Problem ist grundsätzlich auf die folgenlose Anfangsauthentifizierung zurückzuführen. Zwar wird das Endgerät am Anfang authentifiziert, aber die darauf folgende Kommunikation wird nicht mehr überprüft. Dies öffnet Trittbrettfahrern Tür und Tor. Aus diesem Grund wurde die Authentifizierung gemäß IEEE 802.1X bei Wireless LAN anders angewandt und mit weiteren Verfahren kombiniert. Bei WLAN war der Leidensdruck groß, nachdem offensichtlich geworden war, dass der im Standard IEEE 802.11 vorgesehene Mechanismus WEP (Wired Equivalent Privacy) große Sicherheitslücken hat. Das Medium WLAN bietet anders als kabelgebundene Netze auch Angreifern außerhalb der Gebäude des Netzbetreibers die Möglichkeit, auf das Netz zuzugreifen. Deshalb musste WEP durch ein sicheres Verfahren ersetzt werden. Bei diesem zweiten Versuch hat man es dann gründlich gemacht. Die Anfangsauthentifizierung gemäß IEEE 802.1X wurde eingesetzt, aber gleichzeitig dazu genutzt, um ein Schlüsselmanagement direkt mit der Authentifizierung einzuleiten. Mit dem Schlüsselaustausch wurde auch der Aufbau einer sicheren Kommunikationsbeziehung zwischen zwei WLAN-Partnern ermöglicht. Sämtliche Pakete, die in einem sicheren WLAN zum Beispiel gemäß dem Standard IEEE 802.11i ausgetauscht werden, werden von den Kommunikationspartnern authentifiziert und verschlüsselt. Ein Angreifer kann zwar das Shared Medi-

um WLAN nutzen und Pakete an beliebige Kommunikationspartner senden, aber diese sind in der Lage zu erkennen, ob diese Pakete wirklich von dem authentifzierten Partner stammen. Darüber hinaus werden die Pakete verschlüsselt. Das Schlüsselmaterial dazu ist ja vorhanden.

Dass eine solche sichere Kommunikation mit Authentifizierung und Verschlüsselung aller Pakete möglich ist und keine unlösbaren Probleme und keine zu hohe Belastung für die Hardware der angeschlossenen Endgeräte schafft, hat die Praxis der sicheren WLANs in den letzten Jahren bewiesen. WLANs sind somit hinsichtlich Sicherheit weiter als die kabelgebundenen LANs, was plausibel ist, weil bei WLANs der größere Leidensdruck die Implementierung einer lückenlosen Sicherheit erforderlich gemacht hat. In sicheren WLANs wird keine Scheinsicherheit durch Hinzufügen eines leicht zu verfälschenden VLAN Tags genutzt, sondern eine Verschlüsselung, die erst auf zwei als vertrauenswürdige eingestuft Geräte aufgehoben wird: WLAN Access Point einerseits und WLAN-Endgerät andererseits. Der WLAN Access

um WLAN nutzen und Pakete an beliebige Kommunikationspartner senden, aber diese sind in der Lage zu erkennen, ob diese Pakete wirklich von dem authentifzierten Partner stammen. Darüber hinaus werden die Pakete verschlüsselt. Das Schlüsselmaterial dazu ist ja vorhanden.

Dass eine solche sichere Kommunikation mit Authentifizierung und Verschlüsselung aller Pakete möglich ist und keine unlösbaren Probleme und keine zu hohe Belastung für die Hardware der angeschlossenen Endgeräte schafft, hat die Praxis der sicheren WLANs in den letzten Jahren bewiesen. WLANs sind somit hinsichtlich Sicherheit weiter als die kabelgebundenen LANs, was plausibel ist, weil bei WLANs der größere Leidensdruck die Implementierung einer lückenlosen Sicherheit erforderlich gemacht hat. In sicheren WLANs wird keine Scheinsicherheit durch Hinzufügen eines leicht zu verfälschenden VLAN Tags genutzt, sondern eine Verschlüsselung, die erst auf zwei als vertrauenswürdige eingestuft Geräte aufgehoben wird: WLAN Access Point einerseits und WLAN-Endgerät andererseits. Der WLAN Access

Virtuelle LANs am Arbeitsplatz bringen keine Sicherheit - Kommunikationssicherheit auf dem Irrweg

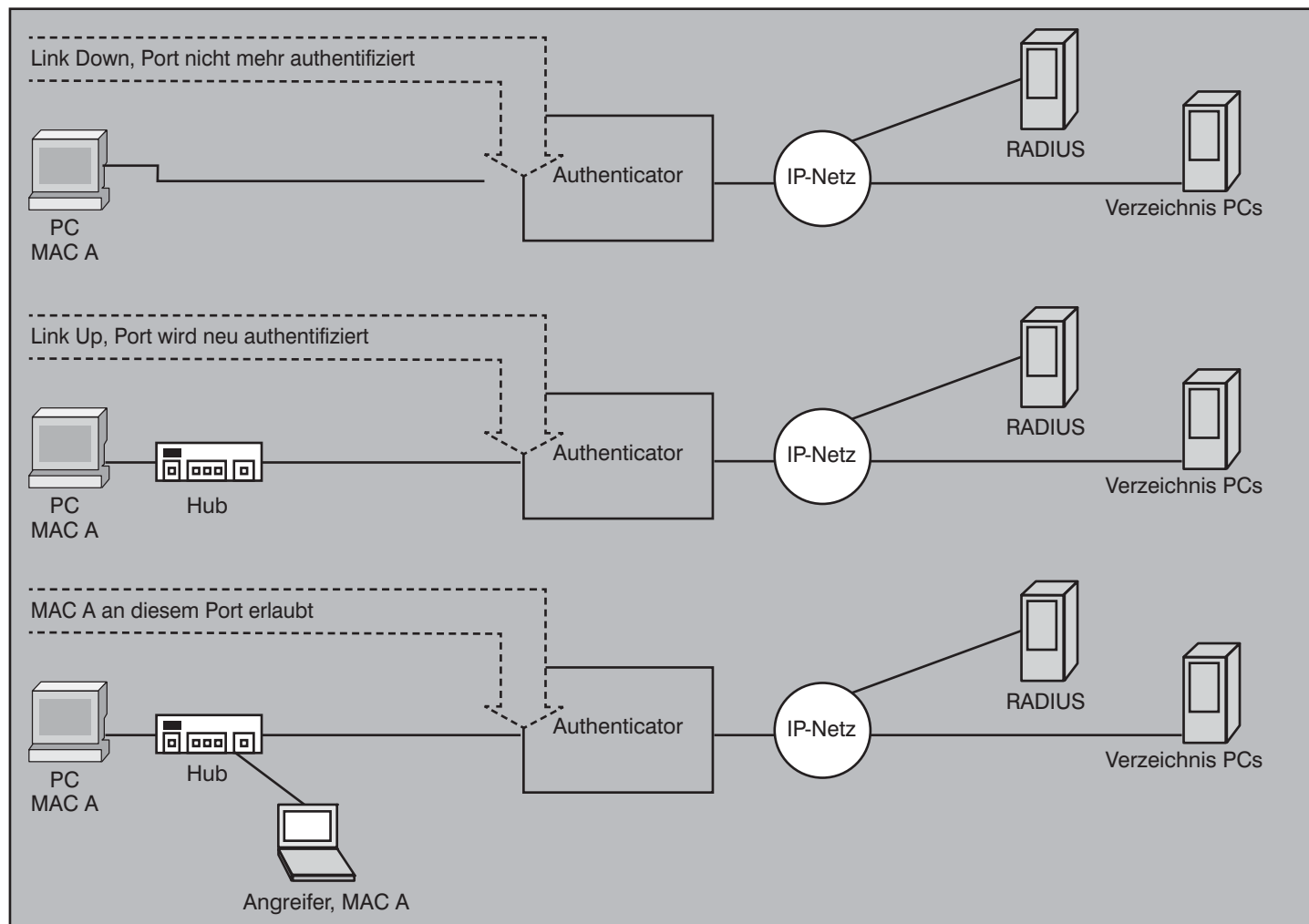


Abbildung 11: Sicherheitslücke bei IEEE 802.1X

Point wird von einem Netzbetreiber administriert. Ist die physikalische Sicherheit des AP gewährleistet (was nicht immer leicht zu bewerkstelligen ist), und ist der Netzbetreiber als vertrauenswürdig eingestuft, kann der Nutzer jedes Endgerätes in einem sicheren WLAN davon ausgehen, dass die Kommunikation im WLAN von Dritten weder abgehört noch manipuliert oder gefälscht werden kann. Mittel dazu ist die Verschlüsselung. Ohne Verschlüsselung ist die anfängliche Authentifizierung wertlos.

MACsec gemäß IEEE 802.1AE

Die Grenzen der reinen Geräteauthentifizierung sind natürlich auch den Gremien klar, die für die Standardisierung von LAN-Sicherheit zuständig sind. Deshalb gibt es seit August 2006 den Standard IEEE 802.1AE mit dem Titel Media Access Control (MAC) Security. Bei diesem Standard geht es darum, in einem Medium, das Zugriffsmechanismen gemäß den Standards der IEEE-Standardfamilie 802 verwendet

und auf der Ebene der Schicht 2 Media Access Control (MAC) einsetzt, vor allem in einem Ethernet, auf der Ebene der Schicht 2 (MAC) vor Angriffen zu schützen. Der Standard IEEE 802.1AE beschreibt Mechanismen, die unter dem Oberbegriff MAC Security (MACsec) die Vertraulichkeit der ausgetauschten MAC-Rahmen sicherstellen sowie dafür sorgen, dass die Integrität dieser Rahmen gewahrt bleibt und dass überprüfbar ist, ob ein Paket wirklich von dem Kommunikationspartner stammt, dessen Identität im Frame Header als Source-Adresse angegeben ist.

MACsec gemäß IEEE 802.1AE ist ausdrücklich nicht für ein WLAN gedacht, denn für Wireless LANs hat der Standard IEEE 802.11i von 2004 bereits die Grundlagen zum Erreichen der selben Ziele geschaffen, die mit dem Standard IEEE 802.1AE für kabelgebundene LANs angestrebt werden.

Das Prinzip von MACsec ist in der Abbildung 12 dargestellt. Der Authentifizie-

rung folgt der Aufbau von Sicherheitsassoziationen auf der MAC-Ebene. Diese Sicherheitsassoziationen erlauben, alle ausgetauschten Pakete entweder nur zu authentifizieren oder auch noch zu verschlüsseln. Somit hätte ein Angreifer mit physikalischem Zugang zum Medium keine Chance, eigene Pakete für solche auszugeben, die von einem der authentifizierten Geräte stammen. Der Angreifer kann ebenso wenig die zwischen den Endgeräten ausgetauschten Pakete manipulieren. Und wenn die Pakete verschlüsselt sind, kann der Angreifer sie ebenso wenig abhören.

Der Standard MACsec befasst sich ausdrücklich nicht mit der Authentifizierung und Autorisierung von Endgeräten, sondern damit, wie bereits authentifizierte und autorisierte Endgeräte sicherstellen, dass die Vertraulichkeit, die Integrität und die Echtheit der ausgetauschten Pakete erreicht werden. Insofern ist MACsec ohne Kombination mit anderen Verfahren zur Authentifizierung meistens nicht sinn-

Virtuelle LANs am Arbeitsplatz bringen keine Sicherheit - Kommunikationssicherheit auf dem Irrweg

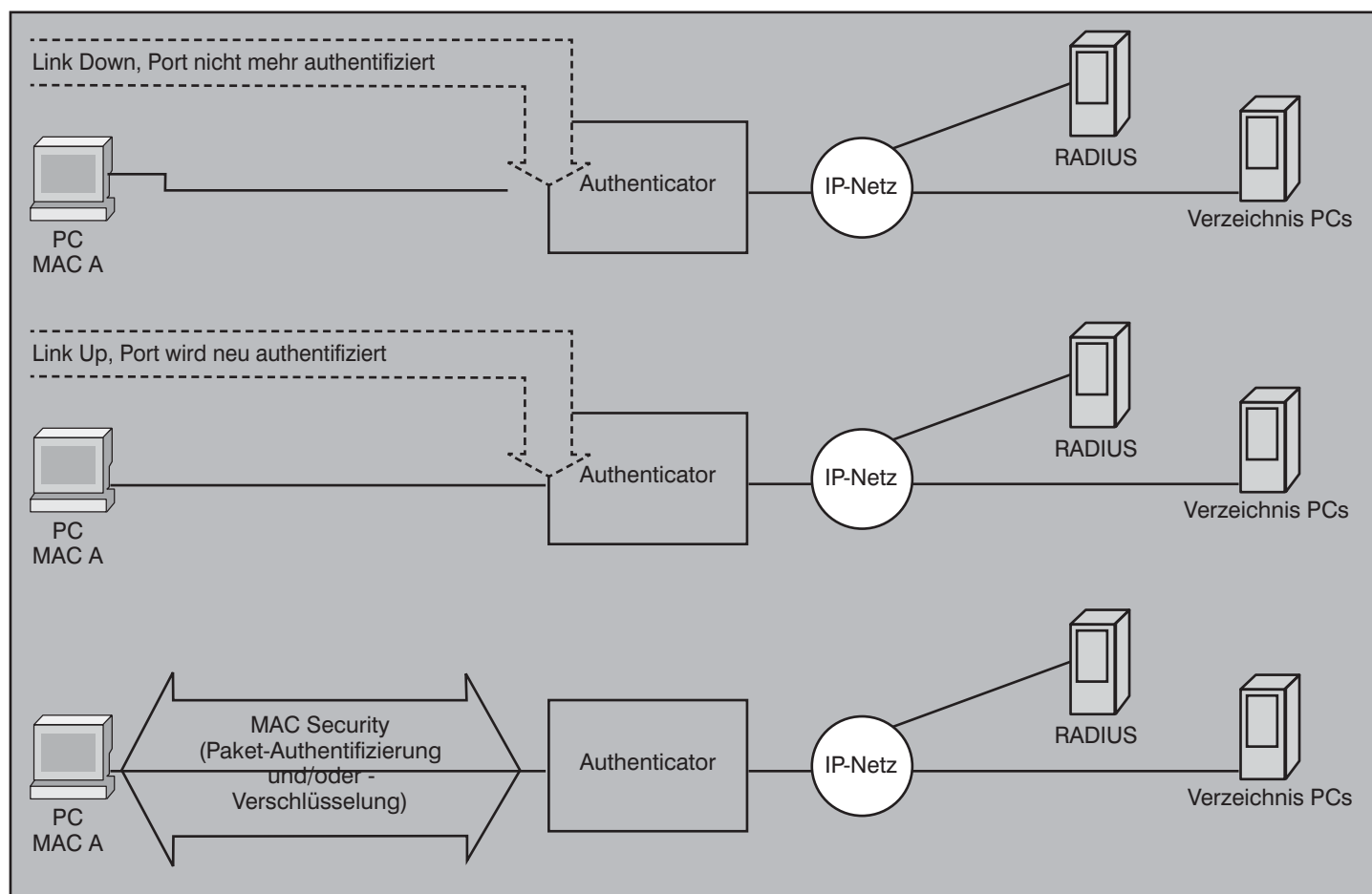


Abbildung 12: MAC Security (MACsec) gemäß dem Standard IEEE 802.1AE

voll. Das ist auch der Grund, dass bereits auf Seite 6 des Standardtextes von IEEE 802.1AE auf IEEE 802.1X hingewiesen wird und auch darauf, dass einer künftigen Ergänzung des Authentifizierungsstandards IEEE 802.1X, nämlich IEEE 802.1af, die Aufgabe vorenthalten bleibt, die beiden Standards für Authentifizierung (IEEE 802.1X) und MAC-Sicherheit (IEEE 802.1AE) miteinander zu kombinieren. Ergebnis wird dann ein sicheres LAN sein, in dem sich die angeschlossenen Geräte gegenseitig authentifizieren und darauf aufbauend auch die Vertraulichkeit, Integrität und Echtheit aller ausgetauschten Pakete sicherstellen können.

Aber auch ohne Authentifizierung gemäß IEEE 802.1X wären sinnvolle Einsätze der Mechanismen von MACsec denkbar, nämlich dann, wenn die Geräte auch ohne IEEE 802.1X sicher authentifiziert werden. Ein Beispiel dafür wären die Netzkomponenten selbst. Ein Netzbetreiber kann durch andere Mechanismen wie zum Beispiel sichere physikalische Aufstellung der Netzkomponenten dafür sorgen, dass diese Netzkomponenten nur dem Zugriff authentifizierter Personen ausgesetzt sind. Um die ausge-

tauschten Pakete vor Abhörscenarien sowie Manipulation und Fälschung auf dem Übertragungsweg zu schützen, kann MACsec eingesetzt werden. Dies ist vor allem dann sinnvoll, wenn zwar die Netzkomponenten und ihre physikalische Lokation, nicht aber das Medium dazwischen (das Kabel) als sicher eingestuft wird. Dann hilft MACsec, aus diesem nur teilweise sicheren Szenario ein sicheres zu machen. Ein typisches Einsatzszenario wäre die Verbindung von zwei Komponenten über eine physikalische Verbindung, die über öffentliches Gelände verläuft, zum Beispiel die Verbindung von zwei Ethernet-Switches über Dark Fiber.

Einige Hersteller haben die Unterstützung von MACsec von ihren Produkten schon angekündigt. Der erste Schritt wird sein, dass MACsec auf den Verbindungen zwischen den Netzkomponenten eingesetzt wird.

Ob das Verfahren MACsec auch bis zu den Endgeräten eingesetzt werden kann, hängt von den Herstellern von Chipsätzen und Treibern für die LAN Interfaces ab, die in den Endgeräten eingesetzt werden. Ein vollständiges MACsec-Szenario

im Access-Bereich ist erst dann möglich, wenn der Standard IEEE 802.1af vorliegt, wenn also MACsec mit der Authentifizierung gemäß IEEE 802.1X kombiniert werden kann. Vermutlich wird die Unterstützung von MACsec durch die Endgeräte erst nach der Verabschiedung von IEEE 802.1af kommen.

Verschlüsselung: segmentweise oder Ende zu Ende?

Es wird noch Jahre dauern, bis MACsec nicht nur in Form eines durchgängig standardisierten Ansatzes, sondern auch in der Gestalt von Geräten verfügbar sein wird, die keine Interoperabilitätsprobleme aufweisen. Wenn man bedenkt, dass fast vier Jahre nach der Verabschiedung des Standards IEEE 802.1X immer noch viele Endgeräte diesen Standard nicht unterstützen und selbst bei Endgeräten, die angeblich 1X-konform sind, die Interoperabilität mit Switches und Authentifizierungsservern keineswegs sichergestellt ist, und dass viele Probleme wie zum Beispiel die Behandlung von Kaskaden von Endgeräten existieren, fällt es schwer zu glauben, dass wir in diesem Jahrzehnt funktionieren-

 Virtuelle LANs am Arbeitsplatz bringen keine Sicherheit - Kommunikationssicherheit auf dem Irrweg

de MACsec-Umgebungen sehen werden. Davor werden noch einige Jahre vergehen.

Aber selbst wenn man optimistisch ist und glaubt, dass die Kombination von MACsec und Authentifizierung in wenigen Jahren in den Endgeräten implementiert sein wird, bleibt die Frage, was damit erreicht wird.

Mit der Kombination von Port-basierender Authentifizierung gemäß IEEE 802.1X und MACsec wird erreicht, dass eine bestimmte Kommunikationsbeziehung innerhalb eines Layer-2-Netzes gegen Abhören, Manipulation und Fälschung gesichert wird. Kommunikationsbeziehungen gehen aber fast immer über mehrere Layer-2-Netze. In jedem dieser Segmente müsste die Kombination aus MACsec und Authentifizierung implementiert werden. Außerdem muss den Betreibern aller dieser Layer-2-Netze Vertrauen entgegengebracht werden, denn diese Betreiber haben Zugriff auf Daten, die nicht gemäß MACsec verschlüsselt sind.

Dagegen ist heute schon bei vielen Kommunikationsbeziehungen eine Ende-zu-Ende-Verschlüsselung machbar. Diese Verschlüsselung erfolgt entweder auf der Ebene der Schicht 3 von IP-Endgerät zum IP-Endgerät mittels IP Security (IPsec), auf der Ebene der Schicht 4 durch Nutzung von Transport Layer Security (TLS) oder auf der Ebene der Schichten 5 bis 7 mithilfe von Verfahren wie E-Mail-Verschlüsselung, z.B. durch S/MIME, bzw. Secure Real-time Transport Protocol (SRTP) wie im Falle von Echtzeit-Audio bzw. Echtzeit-Video. Es ist fraglich, ob angesichts der zunehmenden Verfügbarkeit und Verbreitung der Ende-zu-Ende-Verschlüsselung die mühsam zusammengestellte Kombination von Verfahren, die für die Sicherheit auf der Ebene der Schicht 2 erforderlich ist, irgendeinen Vorteil bringen wird, wenn sie irgendwann einmal tatsächlich verfügbar und anwendbar ist.

Die Ende-zu-Ende-Verschlüsselung ist nämlich die vollständigste Art, eine Kommunikationsbeziehung zu schützen, die physikalische Medien mit anderen Kommunikationsbeziehungen teilen muss. Keine logische Netztrennung, keine segmentweise Verschlüsselung erreicht das Niveau an Sicherheit, das mit der Ende-zu-Ende-Verschlüsselung realisierbar ist. Nur mit der Ende-zu-Ende-Verschlüsselung wird eine universelle Kommunikationssicherheit möglich, die von den variierenden Kommunikationswegen und den Betreibern der verschiedenen Pfade des Kommunikationspfades unabhängig ist.

Dennoch die VLAN-Trennung am Arbeitsplatz?

In diesem Beitrag wurde begründet, warum die Zuordnung von Endgeräten zu verschiedenen VLANs die Authentifizierung von Endgeräten erfordert, die wiederum Sicherheitslücken aufweist, wenn sie eine reine Geräteauthentifizierung bleibt und nicht eine Authentifizierung jedes einzelnen Paketes zur Folge hat. Da für eine solche Authentifizierung die selben Mechanismen erforderlich sind für eine Verschlüsselung, wäre der Schritt zur Implementierung von MAC Security (MACsec) nicht weit. Im Moment fehlen dafür sowohl in der Standardisierung als auch bei den Produkten einige wesentliche Bausteine. Dagegen ist bei vielen Applikationen, u.a. bei Voice over IP, E-Mail und Web eine Ende-zu-Ende-Verschlüsselung verfügbar, die im Vergleich zu MACsec die ohnehin bessere Lösung darstellt.

Und dennoch wird VLAN-Trennung am Arbeitsplatz angewandt. Neben den angeblichen Sicherheitsvorteilen wird auch geltend gemacht, dass eine solche VLAN-Trennung Vorteile für die Ausfallsicherheit der Applikationen habe. Um welche Vorteile geht es? Wann könnte sich eine VLAN-Trennung positiv auf die Verfügbarkeit von Applikationen auswirken?

Um diese Frage zu beantworten, muss man alle Szenarien betrachten, in denen die Verfügbarkeit eines VLANs trotz der gemeinsamen Nutzung eines physikalischen Netzes durch Fehler und Probleme in einem anderen VLAN nicht beeinträchtigt wird. Vorstellbar sind folgende Fälle:

- In einem VLAN kommt es zu einem Broadcast-Sturm. Die Broadcasts in einem VLAN breiten sich jedoch in den meisten Fällen nicht auf andere VLANs aus. Deshalb gilt die Eindämmung der Auswirkung von Broadcast-Stürmen als wesentliches Argument für die VLAN-Trennung. Grundsätzlich ist gegen die Verkleinerung von Broadcast-Domänen nichts einzuwenden, nur warum muss die Einteilung in verschiedene Broadcast-Domänen unbedingt anhand einer Kategorisierung von Endgeräten erfolgen?
- Eine häufige Ursache von Problemen ist die fehlerhafte Vergabe von IP-Adressen. Entweder durch eine falsche manuelle Konfiguration oder durch die Aktivierung eines DHCP-Servers, der falsche IP-Konfigurationen verteilt, kommt es hin und wieder dazu, dass Endgeräte in einer Broadcast-Domäne (Wirkungsfeld eines unerwünschten

DHCP-Servers) von der Kommunikation mit anderen Subnetzen abgeschnitten werden. Es ist verständlich, dass man IP-Telefone vor solchen Szenarien schützen will. Aber verdienen die anderen Clients keinen solchen Schutz? Ist es tolerierbar, wenn in einer Broadcast-Domäne Dutzende PCs nicht auf ERP-Anwendungen oder andere geschäftskritische Applikationen zugreifen können, weil sie von einem „wildem“ DHCP-Server eine falsche IP-Konfiguration erhalten haben?

- Die gezielte Manipulation der per Address Resolution Protocol ermittelten Zuordnung von IP- zu MAC-Adressen – als ARP Poisoning bekannt – ist immer nur in einer Broadcast-Domäne möglich. Je kleiner die Broadcast-Domäne, umso weniger die Kommunikationsbeziehungen, die mittels ARP Poisoning von einer Station aus abgehört werden können. Trennt man die VLANs für Voice und Data, können PCs keinen ARP-Posioning-Angriff mehr gegen IP-Telefone durchführen. Aber ist es tolerierbar, wenn mit solchen Angriffen Datenapplikationen ausspioniert werden? Sind Inhalte von übertragenen Dateien weniger kritisch und schützenswert als Telefongespräche?
- Probleme werden manchmal auch durch die Flutung von Paketen verursacht. Die Auswirkungen solcher Probleme bleiben in der Regel jedoch nicht auf eine Broadcast-Domäne beschränkt. Muss ein Layer-2-Switch in einem VLAN die Pakete fluten, weil zum Beispiel ein fehlerhafter Netzadapter zu viele MAC-Adressen als Source-Adressen von Paketen verwendet und so die MAC-Adresstabellen von Switches zum Überlauf bringt oder weil eine asymmetrische Verkehrsführung Pakete verursacht, dessen Ziel dem Layer-2-Switch unbekannt ist, steigt die Belastung des Switches insgesamt. Das wirkt sich auf die gesamte Switch-Leistung aus und nicht bloß in einem VLAN.
- Auch undefinierte Netzzustände und Spanning-Tree-Probleme wirken sich manchmal auf alle VLANs aus, sodass die VLAN-Trennung nicht immer die Eindämmung solcher Probleme bewirkt.
- Die VLAN-Trennung erleichtert die Zuordnung von separaten Adressbereichen zu verschiedenen Gerätetypen. Beim Betrieb des Netzes ist es hilfreich, Subnetze und somit IP-Adressen eindeutig einem der beiden Bereiche Daten oder Sprache zuzuordnen zu können.

Virtuelle LANs am Arbeitsplatz bringen keine Sicherheit - Kommunikationssicherheit auf dem Irrweg

Das gilt zum Beispiel für die Priorisierung von Voice in Weitverkehrsnetzen oder für die Implementierung von Access Control Lists (ACL), die dafür sorgen, dass bestimmte Kommunikationsbeziehungen zwischen dem Daten- und dem Voice-Bereich unterbunden oder nur namentlich eingestellte Kommunikationsbeziehungen zwischen den beiden Bereichen erlaubt werden. Aber auch ohne VLAN-Trennung lassen sich separate Adressbereiche für verschiedene Gerätetypen vergeben. Einige DHCP-Server unterstützen zum Beispiel die Vergabe von Adressen aus bestimmten Pools an Geräte, deren MAC-Adressen mit einer vorgegebenen Folge von Bytes (einer Herstellerkennung, Vendor ID) beginnen.

Insgesamt können also die technischen Argumente für eine VLAN-Trennung am Arbeitsplatz entkräftet werden.

Insbesondere Anbieter von IP-Telefonielösungen empfehlen dennoch ihren Kunden standardmäßig die Zuordnung von IP-Telefonen und PCs zu unterschiedlichen VLANs. Um Empfehlungen von Herstellern zu befolgen und diesen keinen Vorwand zu liefern, die technische Unterstützung insbesondere bei Problemen einzuschränken, lassen sich viele Unternehmen auf diese Art VLAN-Trennung am Arbeitsplatz ein. Der Beobachtung des Autors zufolge ist längst keine technisch nachvollziehbare Begründung mehr für diesen Schritt vorhanden, sondern lediglich der Hinweis auf die eine oder andere von wem auch immer dokumentierte „Best Practice“. Die Empfehlung der VLAN-Trennung zwischen Voice und Data wurde von White Paper zu White Paper, von Studie zu Studie übernommen und entwickelte eine Eigendynamik. Auf technische Diskussionen lässt man sich häufig nicht mehr ein. Dass die Argumente für eine VLAN-Trennung einer technischen Prüfung nicht standhalten, interessiert wenig.

Es wird übersehen, dass Voice nicht mehr und nicht weniger ist als eine Applikation im IP-Netz. Diese Applikation hinsichtlich der damit verbundenen Verkehrsströme anders zu behandeln als andere, ebenfalls geschäftskritische und in einigen Fällen sogar noch wichtigere Anwendungen ist langfristig nicht haltbar. Jedes Unternehmen nutzt eine Vielzahl von Applikationen, jede Applikation hat ihre Daseinsberechtigung, sonst würde sie ja nicht genutzt werden. Wo käme man denn hin, wenn man für jede Applikation ein separates logisches Netz fordern würde?

Dass die immer noch in vielen Fällen praktizierte VLAN-Trennung am Arbeitsplatz nicht mehr technisch begründet ist, sieht man am besten daran, dass in den allermeisten Fällen im Layer-2-Bereich zwar eine logische Netztrennung zwischen Voice und Data realisiert wird, gleichzeitig jedoch diese Trennung an der ersten Layer-3-Instanz aufhört. Mühsam getrennte VLANs für Sprache und Daten werden in über 90 % der Fälle auf der Ebene von Schicht 3 miteinander verbunden, ohne dass irgendein Sicherheitsmechanismus die Kommunikation zwischen diesen VLANs einschränken würde.

Dabei wäre nur jene VLAN-Trennung konsequent, die sich auf der Ebene der Schicht 3 fortsetzen würde. Die getrennten logischen Netze müssen logischerweise auch auf der Ebene der Schicht 3 getrennt gehalten werden. Die Verfahren dazu sind Multi-Protocol Label Switching (MPLS) oder Virtual Routing and Forwarding (VRF). Jedes Voice-VLAN muss demnach mit einer logischen Routing-Instanz verbunden werden, die einem MPLS-VPN oder einer VRF-Instanz für Voice zugeordnet ist, während die Daten-VLANs an das entsprechende MPLS-VPN bzw. VRF-Instanz für Daten angeschlossen werden.

Dass dadurch die Komplexität der Netzwerkstruktur steigt, steht außer Frage. Aber die Komplexität steigt schon mit der Einführung von getrennten VLANs am Arbeitsplatz. Die Trennung auf Layer 3 ist nur die logische Konsequenz der Netztrennung auf Layer 2.

Problematischer als die erhöhte Komplexität dürfte die immer noch fehlende Unterstützung von MPLS bzw. VRF durch die meisten Hersteller von LAN-Switches sein. Zwar ist MPLS- und VRF-Unterstützung bei WAN-Routern mittlerweile Standard, aber das lässt sich für LAN-Switches nicht sagen. Die meisten Layer-3-Switches unterstützen keine logische Trennung von Routing-Instanzen auf der Basis der selben Hardware. Nicht zuletzt deshalb belässt man es in den allermeisten Fällen bei getrennten VLANs für Voice und Daten, die an Layer-3-Switches verbunden werden.

In letzter Zeit ist in die Diskussion über VLAN-Trennung am Arbeitsplatz Bewegung gekommen, besonders seitdem neue Anbieter den Markt der Sprachkommunikation adressieren. Man nehme zum Beispiel Microsoft mit ihrem Office Communications Server (OCS). Der OCS ist die IP-basierende Kommunikationslösung von Microsoft, die bei den Clients keinen Unterschied mehr macht zwischen PC-basierenden und anderen Endgeräten.

Der zu bevorzugende Client ist sogar der PC mit dem Microsoft Office Communicator. Die ersten funktionierenden OCS-Umgebungen sehen den Einsatz von PC-basierenden Clients vor. Dass Microsoft mit dieser Lösung Marktanteile bei der Sprachkommunikation gewinnen will, steht außer Frage. Dass solche Lösungen keinen Raum mehr für die Zuordnung der Applikation Voice zu einem eigenen VLAN mehr lassen, kann ebenso wenig bezweifelt werden. Die Microsoft-Strategie gibt dem Einsatz von Softphones neuen Auftrieb, nachdem jahrelang weder die traditionellen Hersteller von TK-Lösungen noch die neuen Anbieter wie Cisco ein wirkliches Interesse an der Vermarktung von Softphones gezeigt haben. Dieses Desinteresse ist an der mangelhaften Qualität vieler Softphone-Implementierungen erkennbar. Teilweise sind die Funktionsdefizite von Softphones durch keinerlei technischen Zwang zu erklären. Warum unterstützen zum Beispiel viele Softphones keine Verschlüsselung, wenn es einen verhältnismäßig kleinen Aufwand bedeuten würde, die Softphones mit Funktionen in diesem Bereich zu erweitern? Es liegt der Verdacht nahe, dass viele Hersteller kein Interesse an der breiten Vermarktung von Softphones haben, weil sich mit Hardphones einfacher Geld verdienen lässt.

Jetzt ändert sich jedoch die Situation. Einerseits kommen Benutzer in das Berufsleben, die seit ihren sehr jungen Jahren den PC für sämtliche Kommunikationszwecke, auch für die Sprachübertragung, genutzt haben. Von diesem Anwenderkreis kommen weniger Bedenken gegen ein Telefon, das täglich erst einmal minutenlang booten muss. Andererseits betritt mit Microsoft ein Anbieter den Markt, für den das eigene Softphone der eigentliche strategische Client ist. Ein Softphone ist eine Applikation neben anderen auf dem PC. Das Softphone ist der Tod der VLAN-Trennung am Arbeitsplatz.

Fazit

Dass der Versuch zum Erreichen der Kommunikationssicherheit mit VLAN-Trennung am Arbeitsplatz ein Irrweg ist, wurde in diesem Beitrag damit begründet, dass diese Praxis einerseits die Netzbetreiber vor kaum lösbare Probleme stellt und andererseits angesichts der fehlenden Bausteine, die insgesamt für die Sicherheit auf der Ebene der Schicht 2 sorgen würden, praktisch keine Sicherheit bringt. Angesichts der verfügbaren Lösungen für Ende-zu-Ende-Verschlüsselung ist nämlich dieser Ansatz der zu bevorzugende Weg der Kommunikationssicherheit.