

- Richten Sie die VLANs ein und konfigurieren Sie die Ports entsprechend ihren Erfordernissen. Sichern Sie die Switches durch Zugangs-Passwörter ab, deaktivieren Sie den Telnet-Zugang und aktivieren Sie den SSH-Zugang. Die Konfigurationsdateien können Sie beispielsweise auf einem TFTP-Server sichern.
- Die Vergabe der IP-Konfigurationen für die Netzwerkgeräte, Server und Clients in den VLANs erfolgt statisch gemäß ihren Erfordernissen.
- Verbinden Sie ihr Netzwerk über einen NAT-Router¹ mit dem neuen Provider (hier: EST 10.3.102.x²). Richten Sie am Router ein Inter-VLAN-Routing ein, damit zwischen den VLANs kommuniziert werden kann. Sichern Sie den Router durch Zugangs-Passwörter ab und speichern Sie die Konfigurationsdatei über einen TFTP-Server.
- Einigen Sie sich innerhalb der Klasse bzgl. der SSID(s) und der verwendeten Funk-Kanäle, damit es im Laborraum nicht zu unnötigen Störungen kommt.
- Konfigurieren Sie über das CLI eine passende IP-Adresse für den Access-Point Cisco Aironet. Führen Sie die weiteren Konfigurationsschritte dann über den Web-Browser durch.
- Realisieren Sie auf den WLAN-Komponenten folgende Sicherheitseinstellungen:
 - SSH-Zugang
 - gesicherter Browserzugang (https)
 - Zugangs-Passwörter (auch auf Konsole)
- Richten Sie auf dem Access-Point die notwendigen VLANs ein.
- WLAN mit WPA2 im PSK-Mode (Personal Mode) absichern. Vergewissern Sie sich, dass die Erreichbarkeit der Systeme auch jetzt noch gegeben ist.
- In der Firma TSE betreibt ein Intranet bestehend aus zwei Web-Servern. Installieren Sie hierfür zwei Webserver (z.B. AIDeX Mini-Webserver) in virtuellen Maschinen, die am Switch_B angeschlossen werden (vgl. Abb. 1).
- Sichern Sie das Netzwerk mit geeigneten ACLs ab:
 - Alle Netzwerkgeräte dürfen nur aus VLAN99 (Netzwerkverwalter) erreichbar sein.
 - Rechner aus dem VLAN10 (Firmennetzwerk) haben Internetzugang und dürfen auf den Intranet-Webserver "Firma" zugreifen. Zugriffe auf Rechner der Firmenleitung (VLAN20) und den Intranet-Webserver "Leitung" sind nicht erlaubt.
 - Rechner aus dem VLAN 20 (Firmenleitung) haben Internetzugriff und können auf beide Intranet-Webserver zugreifen.
 - Das Firmennetzwerk soll vom Internet aus nicht erreichbar sein. Ping-Kommandos aus dem Firmennetzwerk ins Internet sind aber zulässig. Es sollen nur etablierte TCP-Verbindungen zugelassen werden.

Wichtige Hinweise zur Bearbeitung und Durchführung:

- Setzen Sie die Access-Points vor Beginn ihrer Arbeit sicherheitshalber auf Werkseinstellungen zurück.
- Reduzieren Sie die Sendeleistung aller WLAN-Komponenten auf das Minimum (1 mW bzw. 10 mW).
- Deaktivieren Sie gegebenenfalls die Firewall von Windows XP.
- Realisieren Sie alle Verbindungen zunächst ohne Sicherheitsmechanismen (VLAN, SSH, https, Verschlüsselung, etc). Testen Sie ihre Konfiguration, ob die Verbindungen erfolgreich hergestellt werden können und richten Sie erst dann schrittweise die gewünschten Sicherheitsmechanismen ein!

2.2 Optionale technische Zusatzaufgaben

Wenn Sie noch freie Zeitressourcen haben, können Sie folgende Aufgaben zusätzlich bearbeiten:

- Authentifizierung der WLAN-Clients über den RADIUS-Server der Cisco-Aironet APs (Enterprise Mode) anstelle des PSK-Modes (Personal Modes).

¹ vgl. CCNA Semester 4, Kapitel 7

² Eine freie IP-Adresse aus dem Schulnetz erhalten Sie vom Lehrer!