

## Modul 145: Netzwerk betreiben und erweitern

Einführung in das FCAPS-Netzwerkmanagement mit  
Praxisbeispielen, Repetitionsfragen und Antworten

Attila Mathé und Johannes Scheuring

## **Modul 145: Netzwerk betreiben und erweitern**

---

Einführung in das FCAPS-Netzwerkmanagement mit  
Praxisbeispielen, Repetitionsfragen und Antworten

---

Attila Mathé und Johannes Scheuring

---

Modul 145: Netzwerk betreiben und erweitern

Einführung in das FCAPS-Netzwerkmanagement mit Praxisbeispielen, Repetitionsfragen und Antworten

Attila Mathé und Johannes Scheuring

Grafisches Konzept: dezember und juli, Wernetshausen

Satz und Layout, Korrektorat: Mediengestaltung, Compendio Bildungsmedien AG

Illustrationen: Oliver Lüde, Winterthur

Druck: Edubook AG, Merenschwand

Redaktion und didaktische Bearbeitung: Johannes Scheuring

Artikelnummer: 12953

ISBN: 978-3-7155-7066-2

Auflage: 4., überarbeitete Auflage 2015

Ausgabe: U1085

Sprache: DE

Code: ICTW 041

Alle Rechte, insbesondere die Übersetzung in fremde Sprachen, vorbehalten. Der Inhalt des vorliegenden Buchs ist nach dem Urheberrechtsgesetz eine geistige Schöpfung und damit geschützt.

Die Nutzung des Inhalts für den Unterricht ist nach Gesetz an strenge Regeln gebunden. Aus veröffentlichten Lehrmitteln dürfen blosse Ausschnitte, nicht aber ganze Kapitel oder gar das ganze Buch fotokopiert, digital gespeichert in internen Netzwerken der Schule für den Unterricht in der Klasse als Information und Dokumentation verwendet werden. Die Weitergabe von Ausschnitten an Dritte ausserhalb dieses Kreises ist untersagt, verletzt Rechte der Urheber und Urheberinnen sowie des Verlags und wird geahndet.

Die ganze oder teilweise Weitergabe des Werks ausserhalb des Unterrichts in fotokopierter, digital gespeicherter oder anderer Form ohne schriftliche Einwilligung von Compendio Bildungsmedien AG ist untersagt.

Copyright © 2005, Compendio Bildungsmedien AG, Zürich

Dieses Buch ist klimaneutral in der Schweiz gedruckt worden. Die Druckerei Edubook AG hat sich einer Klimaprüfung unterzogen, die primär die Vermeidung und Reduzierung des CO<sub>2</sub>-Ausstosses verfolgt. Verbleibende Emissionen kompensiert das Unternehmen durch den Erwerb von CO<sub>2</sub>-Zertifikaten eines Schweizer Klimaschutzprojekts.

Mehr zum Umweltbekenntnis von Compendio Bildungsmedien finden Sie unter: [www.compendio.ch/Umwelt](http://www.compendio.ch/Umwelt)

## Inhaltsverzeichnis

---

<b>Vorwort</b>	<b>5</b>
<b>Über dieses Lehrmittel</b>	<b>7</b>
<b>Teil A Grundlagen des Netzwerkmanagements</b>	<b>9</b>
<b>Einleitung, Lernziele und Schlüsselbegriffe</b>	<b>10</b>
<b>1 Netzwerkmanagement nach FCAPS</b>	<b>11</b>
1.1 Grundlegende Begriffe und Anforderungen	12
1.2 Funktionsbereiche, Ziele und Aufgaben	13
1.3 Netzwerkdokumentation	14
1.4 Netzwerkdarstellung	15
<b>Repetitionsfragen</b>	<b>20</b>
<b>2 Configuration Management</b>	<b>21</b>
2.1 Ziele und Aufgaben	21
2.2 Aufbau und Betrieb	22
<b>Repetitionsfragen</b>	<b>29</b>
<b>3 Fault Management</b>	<b>30</b>
3.1 Zweck und Aufgaben	30
3.2 Instrumente und Massnahmen	31
3.3 Fehlersuche und -analyse	39
<b>Repetitionsfragen</b>	<b>49</b>
<b>Teil B Netzwerk funktionssicher betreiben</b>	<b>51</b>
<b>Einleitung, Lernziele und Schlüsselbegriffe</b>	<b>52</b>
<b>4 Performance Management</b>	<b>54</b>
4.1 Voraussetzungen für ein effizientes Performance Management	54
4.2 Leistungsdaten mittels SNMP erheben	55
4.3 Messwerte darstellen und auswerten	60
4.4 Performanceprobleme lokalisieren	64
4.5 Massnahmen gegen Performanceprobleme	67
<b>Repetitionsfragen</b>	<b>80</b>
<b>5 Sicherheitsmanagement</b>	<b>82</b>
5.1 Ziele und Aufgaben	82
5.2 Massnahmen für die Netzwerksicherheit	83
<b>Repetitionsfragen</b>	<b>93</b>
<b>Teil C Netzwerk um WLAN erweitern</b>	<b>95</b>
<b>Einleitung, Lernziele und Schlüsselbegriffe</b>	<b>96</b>
<b>6 Funknetzwerke planen und sicher betreiben</b>	<b>97</b>
6.1 IEEE-Standards	97
6.2 Komponenten und Antennen	102
6.3 WLANs sicher betreiben	107
<b>Repetitionsfragen</b>	<b>116</b>
<b>7 Lokale Netze über das Internet sicher verbinden</b>	<b>117</b>
7.1 Virtual Private Network (VPN)	117
7.2 Sicheres Internetprotokoll (IPSec)	119
7.3 Praktische Anwendungen eines VPN	122
<b>Repetitionsfragen</b>	<b>126</b>

Teil D	Anhang	
	<b>Gesamtzusammenfassung</b>	<b>128</b>
	<b>Antworten zu den Repetitionsfragen</b>	<b>132</b>
	<b>Glossar</b>	<b>137</b>
	<b>Stichwortverzeichnis</b>	<b>142</b>

## Vorwort

---

### Liebe Leserin, lieber Leser

Vorweg schon einmal herzliche Gratulation! Sie haben sich für den Einsatz eines der aktuellsten Lehrmittel der Informatikausbildung entschlossen.

### An wen richtet sich die Lernwelt «Informatik»?

Die Lernwelt «Informatik» ist ausgerichtet auf die gültigen Modulbeschreibungen für die Informatik-Grund- und -Weiterbildung. Mit diesem Grundlagenbuch wenden wir uns deshalb an Auszubildende und Unterrichtende

- einer Informatiklehre,
- der Informatikmittelschulen,
- der höheren Berufsbildung und
- von Ausbildungsgängen und Schulungen in der Erwachsenenbildung.

Dank zahlreicher Beispiele, Grafiken, Abbildungen und Übungen mit kommentierten Lösungen eignet sich die Lernwelt «Informatik» auch für das Selbststudium.

### Wie Sie mit diesem Lehrmittel arbeiten

Dieses Arbeitsbuch bietet Ihnen mehr als nur einen Lerntext. Deshalb weisen unsere Bildungsmedien eine Reihe von Charakteristiken auf, die Ihnen Ihre Arbeit erleichtern:

- Das **Inhaltsverzeichnis** dient Ihnen als Orientierungshilfe und als Lernrepetition. Fragen Sie sich, was Sie von jedem Kapitel erwarten, und überprüfen Sie anschliessend an das Bearbeiten des Lerntexts, was Sie jetzt zu den einzelnen Teilen wissen.
- Wissen Sie gerne im Voraus, wofür Sie Ihre kostbare Zeit einsetzen? Kein Problem, lesen Sie die **Lernziele** vor der Lektüre des entsprechenden Teils. An gleicher Stelle finden Sie auch eine Auflistung der **Schlüsselbegriffe**.
- Die einzelnen Lerneinheiten werden durch eine **Zusammenfassung** abgeschlossen. Sie greift die wichtigsten Punkte des vorangegangenen Texts nochmals auf und stellt sie in den richtigen Zusammenhang.
- Nach dem Durcharbeiten der einzelnen Lerneinheiten können Sie anhand der **Repetitionsfragen** überprüfen, ob Sie das Gelernte verstanden haben. Die **Lösungen** zu diesen Repetitionsfragen finden Sie im Anhang des Buchs. Bitte beachten Sie, dass die Übungen nicht fortlaufend nummeriert sind; die Nummern dienen lediglich zum Auffinden der Lösung.
- Nutzen Sie das **Glossar**; schlagen Sie dort nach, wenn Sie einen Begriff nicht verstehen.
- Das **Stichwortverzeichnis** beschliesst das Lehrmittel. Sie können es benutzen, wenn Sie einzelne Abschnitte zu bestimmten Schlagwörtern nachlesen wollen.

### Wer steht hinter der Lernwelt «Informatik»?

Die erfahrenen Lehrmittelentwickler von Compendio Bildungsmedien haben die Lernwelt «Informatik» zusammen mit ausgewiesenen Fachleuten und Kennern der Informatikausbildung konzipiert und realisiert.

Dank gebührt allen, die trotz grossem Zeitdruck mit Rat und Tat am Konzept und an der Ausarbeitung mitgewirkt haben. Speziell möchten wir uns bedanken bei Emanuel Duss, der für das Fachlektorat verantwortlich war.

**In eigener Sache**

Haben Sie Fragen oder Anregungen zu diesem Lehrmittel? Sind Ihnen Fehler aufgefallen?  
Über unsere E-Mail-Adresse [postfach@compendio.ch](mailto:postfach@compendio.ch) können Sie uns diese gerne mitteilen.

Wir wünschen Ihnen mit diesem Lehrmittel viel Spass und Erfolg.

Zürich, im August 2015

Attila Mathé, Autor

Emanuel Duss, Fachlektor

Johannes Scheuring, Redaktor

**Anmerkung zur 4. Auflage 2015**

Änderungen gegenüber der 3. Auflage beruhen auf der aktualisierten Modulidentifikation  
der ICT-Berufsbildung (Stand 14.01.2014, ICT-Modulbaukasten, Release 6).

## Über dieses Lehrmittel

### Inhalt und Aufbau dieses Lehrmittels

Dieses Lehrmittel vermittelt Kenntnisse, wie die Performance und die Verfügbarkeit eines Netzwerks gemessen, interpretiert und verbessert werden können, wie ein Netzwerk nach Vorgabe um WLAN / VLAN erweitert kann und wie entfernte Netzwerke miteinander sicher verbunden werden können. Dabei lernen Sie, mit welchen Problemen und Aufgaben ein **Netzwerkadministrator** bei der Überwachung, Wartung und Erweiterung **eines lokalen Netzwerks (LAN)** typischerweise konfrontiert wird. Anhand praktischer Beispiele sehen Sie, welche Prozesse und Aktivitäten auf der Basis des **OSI-Management-Framework-Standards** aufgesetzt werden können, um ein möglichst effizientes und effektives Netzwerkmanagement sicherzustellen.

Das Lehrmittel ist wie folgt aufgebaut:

- **Teil A** verschafft Ihnen zunächst einen Überblick über die Begriffe, Anforderungen, Funktionsbereiche, Ziele und Aufgaben eines zeitgemäßen Netzwerkmanagements. Dabei erfahren Sie auch, was bei der Dokumentation und Darstellung eines Netzwerks generell zu beachten ist. Danach erhalten Sie eine Einführung in die beiden Funktionsbereiche Network Configuration Management und Network Fault Management.
- In **Teil B** werden die beiden Funktionsbereiche Network Performance Management und Network Security Management näher vorgestellt. Beim Performance Management wird aufgezeigt, welche Voraussetzungen und Arbeitsschritte notwendig sind, um Leistungsprobleme in einem Netzwerk zu lokalisieren und angemessene Massnahmen zu ergreifen. Beim Security Management werden die Ziele und Aufgaben sowie geeignete Massnahmen vorgestellt, um die Sicherheit eines Firmennetzwerks zu verbessern.
- **Teil C** befasst sich mit der Planung und dem Betrieb von sicheren Funknetzwerken und gibt nützliche Hinweise, um die Leistungsfähigkeit und Sicherheit solcher Netzwerke zu gewährleisten. Abschliessend werden Möglichkeiten gezeigt, um sichere Übertragungswege über das Internet aufzubauen und den Benutzern sichere Zugriffsmöglichkeiten auf das Firmennetzwerk zu bieten.

### Dieses Lehrmittel liefert die Grundlagen für den Erwerb folgender Kompetenzen

1. Dokumentation eines Netzwerks interpretieren und nachführen.
2. Performance und Verfügbarkeit des Netzes mit Tools überwachen (Netzwerkmanagement-System), entsprechende Auswertungen und Logfiles interpretieren.
3. Bei Störungen Fehlersymptome und -meldungen systematisch erfassen. Ursachen von Störungen mit Tools ermitteln und beheben.
4. Netzwerke in VLANs aufteilen und konfigurieren.
5. Netzwerke um WLANs erweitern und mit gesichertem Zugang konfigurieren.
6. Entfernte lokale Netze sicher verbinden.

### Methodische und technische Voraussetzungen

Für die Bearbeitung dieses Lehrmittels werden keine methodischen Voraussetzungen verlangt. Als technische Voraussetzung empfiehlt sich der Einsatz eines vernetzten PCs unter MS Windows oder Linux, um die Beispiele und Fragen besser nachvollziehen zu können.

## Für die Bearbeitung dieses Lehrmittels werden folgende Kenntnisse und Fähigkeiten vorausgesetzt

Für die Bearbeitung dieses Lehrmittels werden grundlegende Kenntnisse über die Einrichtung, Wartung und Erweiterung eines lokalen Netzwerks (LAN) empfohlen. Der Umfang dieser Kenntnisse entspricht den Inhalten der Module 117, 129 und 146 gemäss ICT-Berufsbildung. Vergleichen Sie dazu das nachfolgende Literaturverzeichnis.

### Nützliche Links zum Thema

Thema	URL	Beschreibung
Network-Management-Informationen und -Tools	<a href="http://www.cacti.net">www.cacti.net</a> <a href="http://www.nagios.org">www.nagios.org</a>	<ul style="list-style-type: none"> <li>Visualisierungslösung (Open Source)</li> <li>Eine Lösung zur Realisierung der Überwachung von Systemkomponenten (Open Source)</li> </ul>
Netzwerksymbole	<a href="http://www.cisco.com/web/about/ac50/ac47/2.html">www.cisco.com/web/about/ac50/ac47/2.html</a>	Kostenloser Bezug der Cisco-Netzwerk-symbole und -Icons
Überwachungsprogramme	<a href="http://www.whatsupgold.com">www.whatsupgold.com</a> <a href="http://www.zabbix.com">www.zabbix.com</a> <a href="http://www.opennms.org">www.opennms.org</a>	<ul style="list-style-type: none"> <li>WhatsUp Gold</li> <li>ZABBIX (Open Source)</li> <li>OpenNMS (Open Source)</li> </ul>
WLAN-Standards und Informationen	<a href="http://www.ieee.org">www.ieee.org</a> <a href="http://www.wi-fi.org">www.wi-fi.org</a>	<ul style="list-style-type: none"> <li>Infos zu allen IEEE-Standards</li> <li>Nützliche Infos für Endverbraucher</li> </ul>
Zeichenprogramme	<a href="http://www.microsoft.com">www.microsoft.com</a> <a href="http://www.smartdraw.com">www.smartdraw.com</a> <a href="http://www.dia-installer.de">www.dia-installer.de</a>	<ul style="list-style-type: none"> <li>MS Visio Standard</li> <li>SmartDraw Standard</li> <li>Dia (Open Source)</li> </ul>

### Nützliche Literatur zum Thema

Autor	Titel	ISBN	Jahr
Becker, Thomas; Dammer, Ingo; Howaldt, Jürgen; Loose, Achim	Netzwerkmanagement	978-3-642-19333-0	2011
Mathé, Attila; Roggeli, Simon	Modul 117: Informatik und Netzwerkinfrastruktur für ein kleines Unternehmen realisieren	978-3-7155-9943-4	2014
Aversa, Domenico; Meier, Jonas	LAN-Komponenten in Betrieb nehmen	978-3-7155-7021-1	2014
Hochstrasser, Heike; Bonfranchi Renzo	Modul 146: Internetanbindung für ein Unternehmen realisieren	978-3-7155-7037-2	2015

## **Teil A Grundlagen des Netzwerkmanagements**

---

## Einleitung, Lernziele und Schlüsselbegriffe

---

### Einleitung

---

Mit der zunehmenden Grösse eines Netzwerks wird der reibungslose Betrieb einer solchen Infrastruktur nicht nur aufwendiger, sondern auch anspruchsvoller. Das **Netzwerkmanagement** soll einen stabilen und effizienten Netzbetrieb sicherstellen. In diesem Teil des Lehrmittels werden die Grundlagen des Netzwerkmanagements gelegt. Dabei lernen Sie wichtige Begriffe, Aufgabenbereiche und Ziele eines modernen Netzmanagements kennen und erfahren, welche Unterlagen dafür benötigt werden.

### Lernziele und Lernschritte

---

Lernziele	Lernschritte
<input type="checkbox"/> Sie können mögliche Datenquellen (Netzwerkkomponenten und angeschlossene Endsysteme) für die Überwachung eines Netzwerks nennen und beschreiben.	<ul style="list-style-type: none"> <li>• Netzwerkmanagement nach FCAPS</li> <li>• Configuration Management</li> <li>• Fault Management</li> </ul>
<input type="checkbox"/> Sie können den Aufbau und den Inhalt einer Netzwerkdokumentation erklären.	<ul style="list-style-type: none"> <li>• Netzwerkmanagement nach FCAPS</li> <li>• Configuration Management</li> </ul>
<input type="checkbox"/> Sie können gängige Darstellungsarten und Symbole für Netzwerkpläne unterscheiden und korrekt interpretieren.	<ul style="list-style-type: none"> <li>• Netzwerkmanagement nach FCAPS</li> </ul>
<input type="checkbox"/> Sie können geeignete Tools zur Überwachung von Netzwerken nennen und charakterisieren.	<ul style="list-style-type: none"> <li>• Configuration Management</li> <li>• Fault Management</li> </ul>
<input type="checkbox"/> Sie können die wichtigsten Darstellungsarten für die erhobenen Daten unterscheiden und korrekt interpretieren.	<ul style="list-style-type: none"> <li>• Configuration Management</li> <li>• Fault Management</li> </ul>
<input type="checkbox"/> Sie können die wichtigsten Indizien / Symptome erläutern, die auf Störungen hinsichtlich der Verfügbarkeit und Performance hinweisen.	<ul style="list-style-type: none"> <li>• Fault Management</li> </ul>
<input type="checkbox"/> Sie können Methoden aufzeigen, um Störungen systematisch zu ermitteln und zu beheben.	<ul style="list-style-type: none"> <li>• Fault Management</li> </ul>

### Schlüsselbegriffe

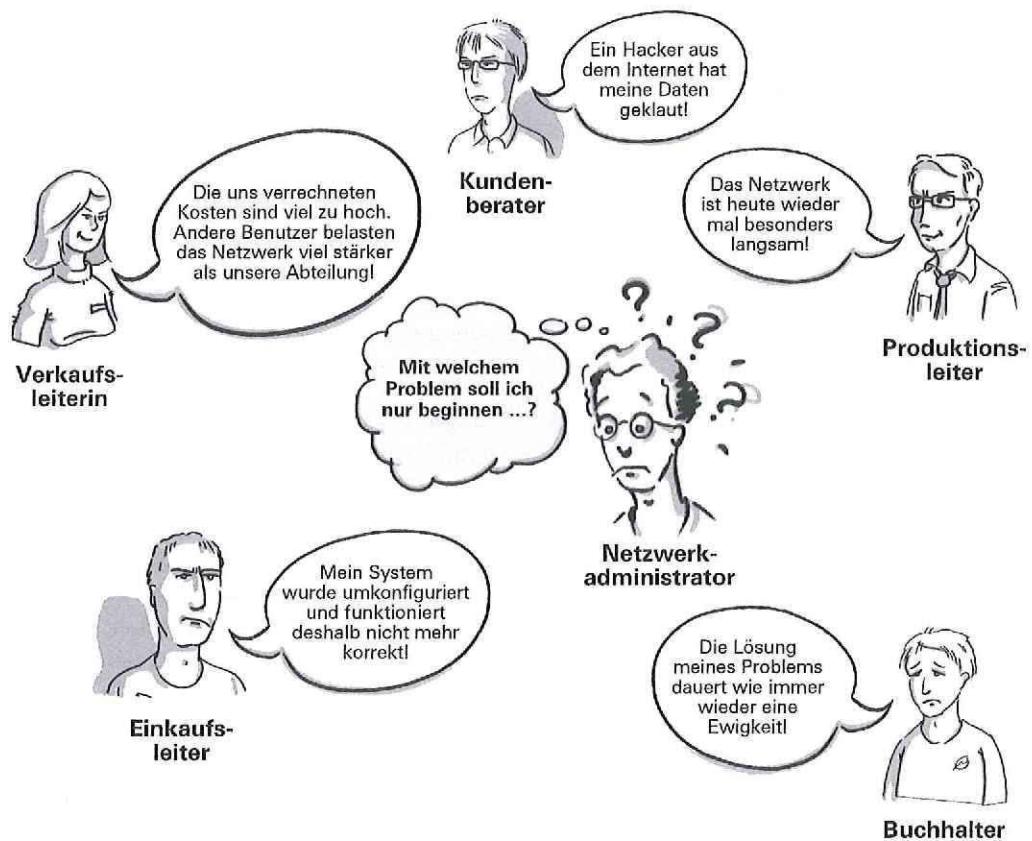
---

Netzwerkmanagement, Netzwerkinfrastruktur, Skalierbarkeit, Verfügbarkeit, Stabilität, Performance, Vertraulichkeit, FCAPS-MF, Fault Management, Configuration Management, Accounting Management, Performance Management, Security Management, Netzwerkdokumentation, Netzwerkdigramm, Netzwerksymbole, Verkabelungsplan, NCM, Inventarliste, Konfigurationsdatei, Fault Management, Syslog-Server, Network Monitoring Tool, Fehlersuche, Fehleranalyse, Portscan

## 1 Netzwerkmanagement nach FCAPS

Ist die Netzwerkinfrastruktur in einem Unternehmen gestört, stehen immer mehr Geschäftsprozesse still. Deshalb hat die Bedeutung des betrieblichen Netzwerkmanagements in den letzten Jahren stark zugenommen. Doch ein effektives und effizientes Netzwerkmanagement ist keine simple Angelegenheit, denn diese Aufgabe muss verschiedene Anforderungen erfüllen und umfasst zahlreiche Tätigkeiten. So erstaunt es nicht, dass die Herausforderungen des Netzwerkadministrators mit der Grösse und Komplexität der Netzwerkinfrastruktur immer mehr zunehmen und oft mehrere Probleme gleichzeitig gelöst werden müssen.

[1-1] Typische Herausforderungen des Netzwerkadministrators



Die meisten solcher Probleme lassen sich durch ein systematisches Netzwerkmanagement zeitnah lösen und oft sogar proaktiv<sup>[1]</sup> verhindern. Dies erhöht nicht nur die Zufriedenheit der Netzwerkbenutzer, sondern fördert auch die Produktivität des Unternehmens bzw. stellt diese sicher. Nachfolgend lernen Sie zunächst grundlegende Begriffe und Anforderungen zum Netzwerkmanagement kennen. Danach erfahren Sie mehr über die Aufgaben, Ziele, Tätigkeiten und Dokumente eines Netzwerkmanagements, das nach einem praxiserprobten Standardmodell organisiert wird. Dabei erfahren Sie viel Wissenswertes über die Zusammenhänge zwischen den einzelnen Aufgabenbereichen und Aktivitäten dieses Modells. Als System- bzw. Netzwerkadministrator können Sie dieses Wissen einsetzen, um die betriebliche Netzwerkinfrastruktur möglichst effektiv und effizient zu organisieren.

[1] Initiatives, vorausschauendes Handeln, d. h., nicht warten, bis ein Fehler auftritt (im Gegensatz zu «reakтив»).

## 1.1 Grundlegende Begriffe und Anforderungen

Unter **Netzwerkmanagement** versteht man die Verwaltung, die Kontrolle und den Betrieb eines Computernetzwerks. Das Netzwerkmanagement stellt den anforderungsgerechten Betrieb der entsprechenden Netzwerkinfrastruktur sicher. Zur **Netzwerkinfrastruktur** werden im Allgemeinen folgende **Komponenten** gezählt:

- **Netzwerkverkabelung** bei einem lokalen Netz (LAN)
- **Funkbereich** in einem Funknetz (WLAN)
- **Netzwerkgeräte** wie z. B. Switches, Access Points, Routers
- **Netzwerkdienste** wie z. B. Firewalls, Proxydienste<sup>[1]</sup> und Loadbalancers<sup>[2]</sup>
- **Öffentliche Übertragungsdienste** für den Zugriff auf externe, entfernte Netze bzw. Dienste

In grossen Unternehmen ist es möglich, dass diese Komponenten durch unterschiedliche Abteilungen oder mehrere Teams «gemanagt» werden. In einem KMU ist es nicht ungewöhnlich, wenn das Netzwerkmanagement durch die gleiche Person wahrgenommen wird, die auch für die Verwaltung der Server und PCs zuständig ist (z. B. durch den Systemadministrator).

Ein Netzwerkadministrator muss den anforderungsgerechten Betrieb der Netzwerkinfrastruktur im Unternehmen gewährleisten. Doch was bedeutet das konkret? Schauen wir uns zuerst die Anforderungen an, die heute an eine Netzwerkinfrastruktur gestellt werden. Das Netzwerkmanagement muss sicherstellen, dass folgende **Anforderungen** erfüllt werden:

- **Skalierbarkeit:** Mit Skalierbarkeit ist die Möglichkeit, sprich die «Fähigkeit» des Netzwerks gemeint, auch neue Anforderungen zu erfüllen, ohne dass deshalb das gesamte Netzwerk bzw. grössere Teile davon vollständig ersetzt werden müssen. So ist z. B. bei der Planung und Realisation eines Netzwerks darauf zu achten, dass das verlegte Netzwerkkabel nicht nur die aktuelle Übertragungsrate von 1-Gigabit-Ethernet erfüllt. Das verwendete Übertragungsmedium sollte idealerweise auch in der Lage sein, Datenraten von 10- oder 40-Gigabit-Ethernet zu übertragen.
- **Verfügbarkeit / Stabilität:** Mit der Verfügbarkeit ist die Eigenschaft hinsichtlich der Stabilität eines Netzwerks gemeint. Da ein Netzwerk für den reibungslosen Betrieb innerhalb einer Firma eine äusserst wichtige Rolle spielt, sollte dieses Netz natürlich sehr stabil laufen, sprich eine möglichst hohe Verfügbarkeit aufweisen. IT-Anwender benötigen zur Erledigung ihrer Arbeiten also möglichst stabile Netzwerke, die nie oder nur selten ausfallen. Die Verfügbarkeit wird mittels %-Angaben definiert. So entspricht eine Verfügbarkeit von 99% einer Gesamtausfallzeit innerhalb eines Jahres von knapp 4 Tagen, genauer gesagt von 3 Tagen 15 Stunden 40 Minuten.
- **Leistungsfähigkeit / Performance:** Die Leistungsfähigkeit eines Netzwerks ist dessen Eigenschaft, alle Datenübertragungen den Anforderungen entsprechend abzuwickeln. Dies bedeutet, dass auch wenn zeitweise ein sehr hohes Datenaufkommen im Netzwerk vorherrscht, die zu übertragenden Daten trotzdem ohne negative Effekte wie z. B. Latenzen<sup>[3]</sup> oder Verluste von Datenpaketen übertragen werden. In Netzwerken mit zu geringer Leistung, sprich Performance, sinkt die Übertragungsqualität infolge der Aus-

[1] Englisch für: Stellvertreter. Im Netzwerk fungiert ein Proxy als «Vermittlerdienst» zur Leistungssteigerung oder Erhöhung der Sicherheit.

[2] Englisch für: Lastenverteiler. Dieser Dienst verteilt die Arbeitslast auf mehrere Rechner (z. B. bei einer grossen Anzahl von Webzugriffen auf mehrere Webserver).

[3] Zeitliche Verzögerungen, hervorgerufen durch Signallaufzeiten und Verarbeitungszeiten aller beteiligten Netzwerkkomponenten.

wirkungen der erwähnten negativen Effekte. In solchen Netzwerken bzw. Situationen ist die Quality of Service (QoS), zu Deutsch «Dienstgüte», nicht gegeben.

- **Vertraulichkeit:** Die Netze bzw. die Dienste, die heute genutzt werden, beschränken sich nicht auf die eigenen, lokalen Systeme eines Unternehmens. Ein Grossteil der Datenübertragungen wird über Netzwerke abgewickelt, bei denen man weder Kontrolle hat hinsichtlich der Übertragung seiner Daten noch weiss, wer überhaupt diese Netze betreibt. Deshalb spielt bei der Übertragung vertraulicher oder schützenswerter Daten die Vertraulichkeit eine grosse Rolle. Diese Anforderung soll verhindern, dass Unbefugte bei der Übertragung über unsichere Netze wie z. B. das Internet vertrauliche Daten einsehen können.

## 1.2 Funktionsbereiche, Ziele und Aufgaben

Das Netzwerkmanagement lässt sich in fünf Funktionsbereiche gliedern, wobei jeder eigene Ziele verfolgt und eigene Aufgaben beinhaltet. Zusammen bilden diese Funktionsbereiche den sogenannten **FCAPS-Rahmen** bzw. das **FCAPS Management Framework**. Dieses wurde früher auch als OSI Management Framework (OSI-MF) bezeichnet, mittlerweile hat sich FCAPS als Synonym für ein systematisches Netzwerkmanagement etabliert. FCAPS umfasst folgende Funktionsbereiche, Ziele und Aufgaben:

Funktionsbereiche	Ziele	Aufgaben
<b>Fault Management (Fehlermanagement)</b>	Gewährleistung der Verfügbarkeit / Stabilität des Netzwerks, damit ein fehler- und unterbruchsfreier Netzwerkbetrieb gewährleistet ist. Im Fall einer Störung hat die rasche Wiederherstellung des normalen Netzbetriebs erste Priorität. In einem zweiten Schritt wird dann die nachhaltige Beseitigung der Problemursache angegangen.	<ul style="list-style-type: none"> <li>• Störungen / Netzwerkausfälle erkennen und beheben</li> <li>• Proaktive Massnahmen zur Verhinderung von Störungen / Netzwerkausfällen definieren</li> </ul>
<b>Configuration Management (Konfigurationsmanagement)</b>	Dokumentation und Aktualisierung der Konfigurationen aller Netzwerkkomponenten. Konfigurationsänderungen dürfen nur unter Einhaltung definierter Regeln erfolgen.	<ul style="list-style-type: none"> <li>• Bestehende Konfiguration ermitteln und abspeichern</li> <li>• Neue Konfigurationen in Kraft setzen</li> </ul>
<b>Accounting<sup>[1]</sup> Management (Abrechnungsmanagement)</b>	Bereitstellung statistischer Informationen über den Verbrauch von Netzwerkressourcen. Anhand dieser Informationen kann eine aufwandsorientierte Verrechnung der benutzten Netzwerkressourcen vorgenommen werden oder mittels Quoten eine Beschränkung der zur Verfügung stehenden Netzwerkressourcen definiert werden.	<ul style="list-style-type: none"> <li>• Statistiken über die Verwendung der Netzwerkressourcen erstellen</li> <li>• Benutzer über verbrauchte Netzwerkressourcen informieren</li> <li>• Verbrauchte Netzwerkressourcen abrechnen</li> <li>• Quoten für den überplanmässigen Verbrauch bestimmter Netzwerkressourcen definieren</li> </ul>
<b>Performance Management (Leistungsmanagement)</b>	Sicherstellung der Leistungsfähigkeit des Netzwerks mittels kontinuierlich erhobener Leistungsdaten von den Netzwerkkomponenten. Durch das Erkennen bestimmter Trends sollen Probleme erkannt werden, noch bevor diese zu Engpässen oder gar Ausfällen in Teilen des Netzes führen.	<ul style="list-style-type: none"> <li>• Leistungsdaten erheben und auswerten</li> <li>• Analysen bzw. Messungen durchführen, um leistungsrelevante Ereignisse abzuklären</li> <li>• Massnahmen zur Sicherstellung oder Steigerung der Netzwerkleistung vorschlagen</li> </ul>

Funktionsbereiche	Ziele	Aufgaben
<b>Security Management (Sicherheitsmanagement)</b>	Gewährleistung der Netzwerksicherheit entsprechend den unternehmerischen Vorgaben mithilfe von Massnahmen, die sicherheitsrelevante Funktionen der Netzwerkkomponenten überwachen.	<ul style="list-style-type: none"> <li>• Systemmeldungen auf sicherheitsrelevante Vorkommnisse hin untersuchen</li> <li>• Datenströme auf unerlaubte und schädliche Aktivitäten hin analysieren</li> <li>• Bei Erkennung unerlaubter und schädlicher Aktivitäten Sofortmassnahmen ergreifen</li> <li>• Sicherheitsvorkehrungen aufgrund der aktuellen Bedrohungslage überprüfen und anpassen</li> </ul>

[1] Dieser Aufgabenbereich wird im vorliegenden Lehrmittel nicht näher behandelt.

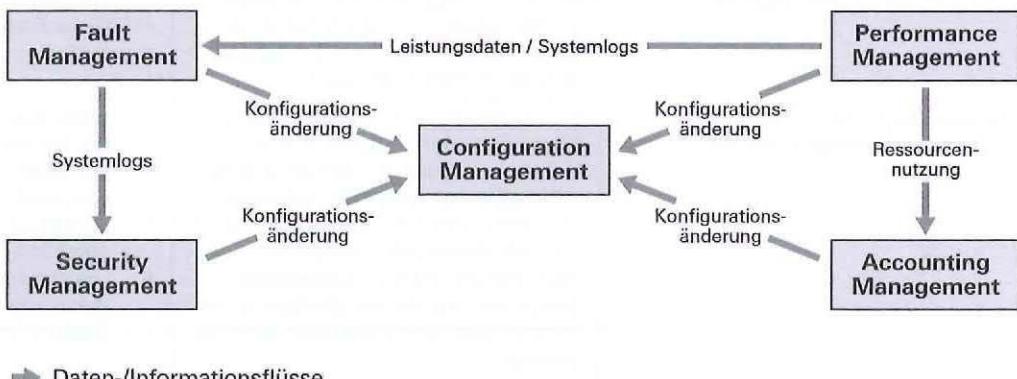
Die oben aufgeführten Funktionsbereiche bilden gemeinsam das **FCAPS Management Framework (FCAPS-MF)**. Dieses hilft Ihnen, unterschiedliche Ziele und Aufgaben des unternehmerischen Netzwerkmanagements zu definieren und aufeinander abzustimmen. Die einzelnen Funktionsbereiche sind eng miteinander verbunden und können daher nicht isoliert voneinander betrachtet werden.

### Beispiel

Anhand von Leistungsdaten aus dem Performance Management lässt sich erkennen, ob die Konfiguration(en) bestimmter Netzwerkkomponenten angepasst bzw. geändert werden muss. Diese Konfigurationsänderungen werden nach den Vorgaben des Configuration Management vorgenommen und müssen für jede Komponente dokumentiert werden.

Erst durch das Zusammenspiel der einzelnen Funktionsbereiche wird ein effektives und effizientes Netzwerkmanagement überhaupt möglich. Folgende Grafik zeigt die wichtigsten **Einflussgrößen** und **Wechselwirkungen** in diesem Zusammenspiel:

[1-2] Zusammenspiel der Funktionsbereiche des FCAPS Management Framework



### 1.3 Netzwerkdokumentation

Obwohl das Netzwerkmanagement mithilfe bestimmter Komponenten und Applikationen automatisiert werden kann, braucht man für den Aufbau und Betrieb einer solchen Lösung zwingend detaillierte Informationen über die bestehende Netzwerkinfrastruktur. Diese Informationen finden Sie normalerweise in einer **Netzwerkdokumentation**. Im Folgenden erfahren Sie mehr über die Ziele und Inhalte einer solchen Dokumentation und bekommen typische Beispieldokumente zu Gesicht.

### 1.3.1 Ziele und Inhalte

---

Eine Netzwerkdokumentation, die ein effektives und effizientes Netzwerkmanagement unterstützen soll, muss folgende **Ziele** erfüllen:

- **Visualisierung der aktuellen Netzwerkstruktur**, um einen raschen Überblick über ggf. komplexe Netzwerke zu erhalten bzw. zu gewährleisten
- **Dokumentierung wichtiger Betriebsinformationen** zur Unterstützung der Fehlersuche, zur Abklärung von Ereignissen bzw. Vorfällen, zur Planung von Anpassungen oder Erweiterungen etc.

Eine solche Netzwerkdokumentation muss folgende Informationen liefern bzw. **Inhalte** umfassen:

- Informationen über die Struktur des gesamten Netzwerks (ggf. gegliedert in einzelne Teilnetze)
- Informationen über öffentliche Netzanbindungen / Verbindungsstrecken
- Informationen über die interne Netzstruktur (LAN)
- Informationen über die eingesetzte Netzwerkadressierung in allen Netzbereichen
- Informationen zur Identifikation der aktiven Netzwerkkomponenten
- Informationen über spezielle Funktionen bzw. Dienste innerhalb des Netzwerks

Aus Sicht des Netzwerkmanagements gehören folgende Informationen **nicht** zwingend in eine Netzwerkdokumentation; sie werden von Vorteil an anderer Stelle dokumentiert (z. B. in der Systemdokumentation, im Hardware-/Software-Inventar oder im Systemhandbuch):

- System- und Inventurdaten über Server, Arbeitsplatzrechner, Drucker und Applikationen (Software)
- Informationen für den Zugriff auf Netzwerkkomponenten bzw. -dienste (Log-in, Passwörter)
- Informationen über Lieferanten von Hardware und Software (Preise, Konditionen)

### 1.3.2 Beispieldokumente

---

Am Beispiel des fiktiven Unternehmens **Caprez Ingenieure AG** werden im Folgenden ein paar Dokumente vorgestellt, die in einer Netzwerkdokumentation enthalten sein sollten. Die Firma Caprez Ingenieure AG betreibt neben ihrem Hauptsitz in Chur zwei weitere Standorte in Samedan und Bellinzona. Insgesamt arbeiten 45 Mitarbeitende in den Bereichen Tiefbau, Strassenbau, Wasserbau und Schutzbauten für diese Unternehmen. Ein funktionierendes und performantes Netzwerk ist für die Caprez Ingenieure AG äusserst wichtig, da ein Grossteil der Mitarbeitenden oft auswärts auf Baustellen arbeitet und von dort auf Firmendaten zugreifen muss. Alle wichtigen Firmendaten sind zentral am Hauptsitz abrufbar bzw. gespeichert.

## 1.4 Netzwerkdarstellung

---

Das **Netzwerkdigramm** ist eine grafische Darstellung mit allen wichtigen Informationen, die eine rasche Analyse und Behebung von Netzwerkstörungen erlaubt. Dazu gehören etwa die Adressen, Strukturen, Komponenten und die Organisation des unternehmerischen Netzwerks. Doch aufgepasst: Zu viele Informationen im Netzwerkdigramm können das Gegenteil bewirken und der Betrachter sieht «vor lauter Bäumen den Wald nicht mehr»! Daher sollten Sie sich genau überlegen, welche Informationen in diesem Dokument ausgewiesen werden.

In der folgenden Tabelle sind alle Sachverhalte aufgeführt, die in einem Netzwerkdigramm enthalten sein können. Aus Sicht des Netzwerkmanagements lassen sie sich in die Kategorien **Muss-Informationen** und **Kann-Informationen** einteilen:

Netzwerkadressen und -struktur		
Informationen	Typ	Beschreibungen
<b>IP-Adressen</b>	Muss	Zwingend sind die IP-Adressen zentraler Dienste und Funktionen (z. B. DHCP-Server, Proxydienste, öffentliche IPs). Achtung: Angabe der Subnetzmaske (CIDR) nicht vergessen!
<b>MAC-Adressen</b>	Kann	Nur wenn unbedingt nötig, ansonsten zum besseren Verständnis weglassen.
<b>Port-Nummern</b>	Kann	Nur wenn der Dienst nicht auf dem Standard-Port läuft, sondern angepasst wurde (z. B. HTTPS nicht auf tcp/443, sondern auf tcp/57612).
<b>VLAN-Infos</b>	Muss	Zwingend bei der Verwendung von VLAN. Dabei am besten auch den VLAN-Typ angeben (z. B. portbasierend, tagged).
<b>Netzwerkdienste</b>	Muss	Zwingend für Dienste, die für einen reibungslosen Netzbetrieb notwendig sind (z. B. DNS, DHCP, Proxydienste).
Netzwerkkomponenten		
<b>Gerätesymbole</b>	Muss	Die Funktion einer Netzwerkkomponente muss zwingend aus einem Diagramm ersichtlich sein.
<b>Modellbezeichnungen</b>	Muss	Aus einem Diagramm sollte klar ersichtlich sein, um welche Netzwerkkomponente und um welches spezifische Modell (Produkt) es sich handelt.
<b>Funktionsmodi</b>	Muss	Wenn Komponenten in einem speziellen Modus betrieben werden, wie z. B., ein Router läuft als «Bridge», der NAT-Modus ist aktiviert etc., sollte dies ersichtlich sein.
<b>Schnittstelleninfos</b>	Kann	Schnittstellenbezeichnungen wie z. B. eth1, fa0/1 o. Ä. nur wenn notwendig, ansonsten besser weglassen.
Netzwerkorganisation		
<b>Serviceinformationen</b>	Kann	Informationen, die bekannt sein müssen, um externen Support zu erhalten, müssen ersichtlich sein, wie z. B. Telefonnummern Hotlines, Supportzeiten, Kundennummer, zuständige Personen / Abteilungen / Firmen etc. Vertrauliche Informationen wie Log-in-Name / Passwörter sollten nie im Netzdigramm vorhanden sein.
<b>Datum / Ersteller</b>	Muss	Das Erstellungsdatum oder Angaben über den Zeichner eines Netzdigramms sollten ersichtlich sein. Diagramme, die über mehrere Jahre nicht aktualisiert wurden, sollten mit einer gewissen Vorsicht benutzt werden.

Für die grafische Darstellung einer Netzwerkkomponente werden meist standardisierte **Netzwerksymbole** verwendet. Oft kommen dabei die **Icons<sup>[1]</sup>** von **Cisco**, einem weltweit führenden Anbieter von Netzwerklösungen, zum Einsatz:

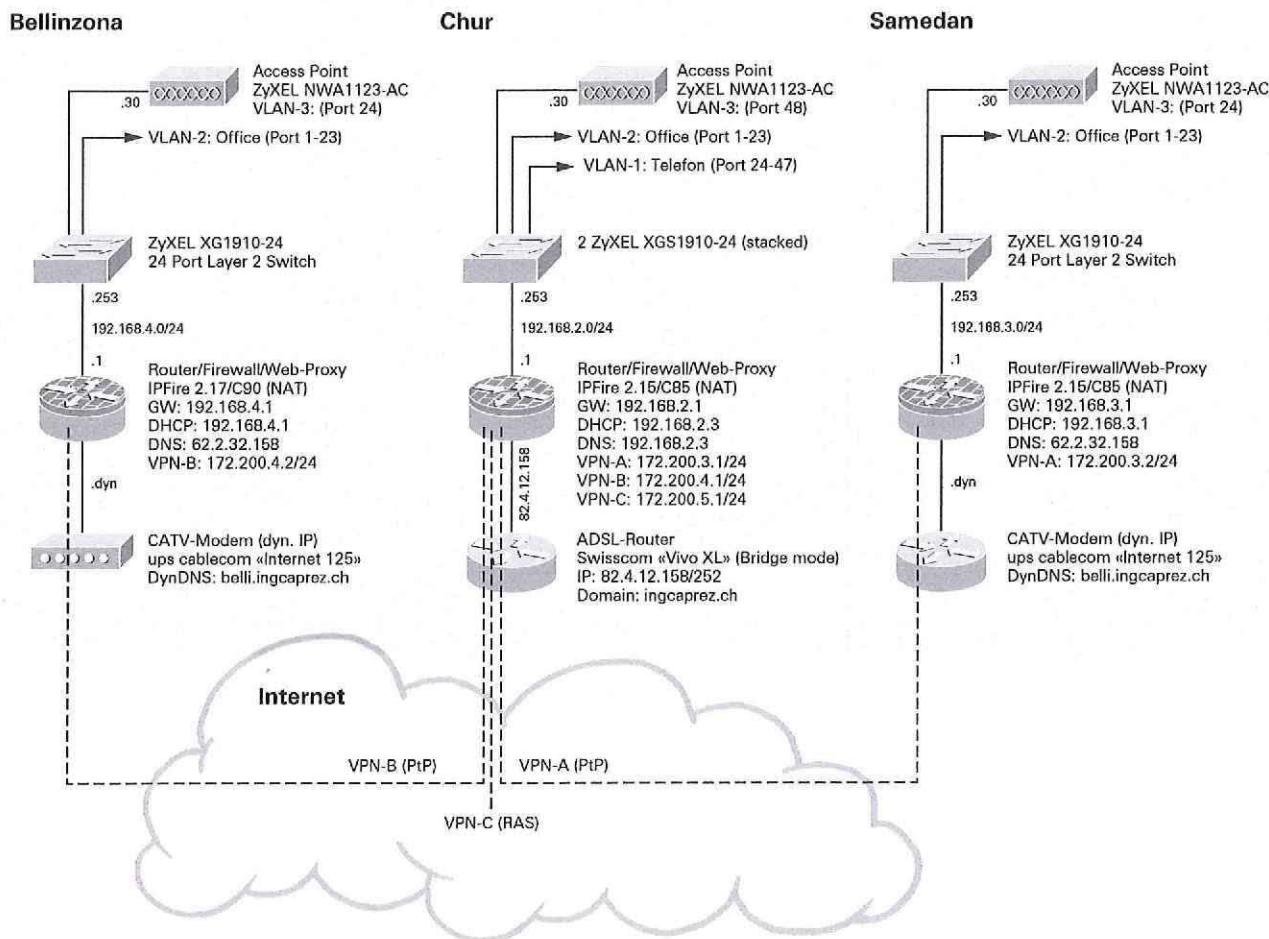
#### [1-3] Netzwerksymbole (Beispiele)

Router		Wireless Router		IP-Telefon		Firewall
Router mit Firewall		Switch		Access Point		

[1] Diese können unter folgender URL heruntergeladen werden: <http://www.cisco.com/web/about/ac50/ac47/2.html>.

Für unser Beispielunternehmen sieht das Netzwerkdiagramm wie folgt aus:

[1-4] Netzwerkdiagramm der Firma Caprez Ingenieure AG



PtP = Point-to-Point

RAS = Remote Access

,<Nr> = zugewiesene IP

.dyn = dynamische IP

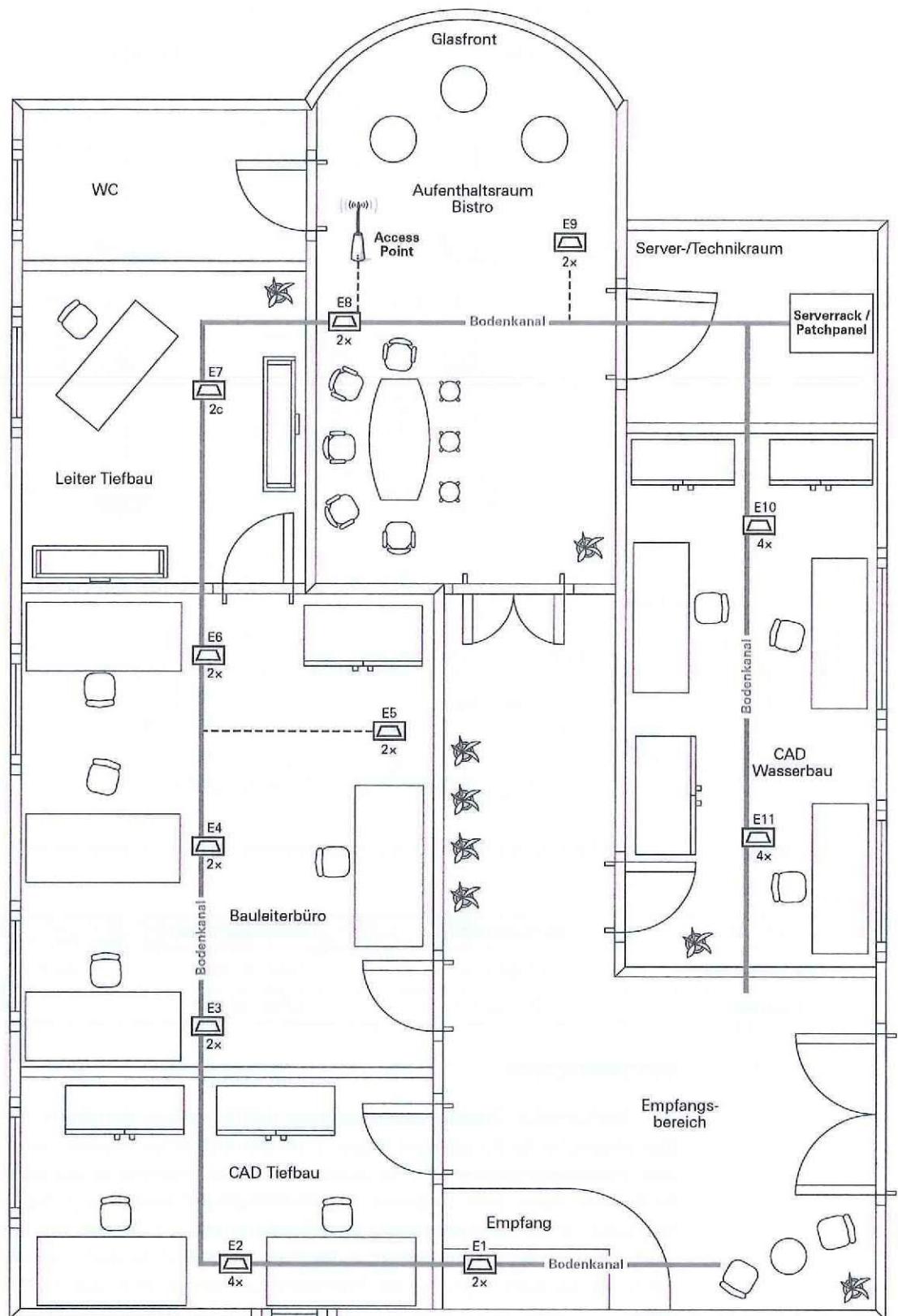
#### Support:

Lieferant	Kundennummer	Telefonnummer	Zeiten
upc cablecom	4000731-3	0800 66 88 66	Mo-Fr 08-22, Sa/Su 10-18
Swisscom	09341223-4	0800 800 800	Mo-So 0-24

#### Verkabelungsplan

Die «**Universelle Gebäudeverkabelung» (UGV)** enthält detaillierte Informationen über das physikalische Fundament (Layer 1 im OSI-Schichten-Modell) eines Netzwerks. Aus dem **Verkabelungsplan** sind die Standorte der Netzwerkanschlüsse eingezeichnet und oft findet man darin auch Angaben zur tatsächlichen Kabelführung. Neben dem Verkabelungsplan ist die **Belegungsliste des Patchpanels** von Bedeutung. Gemeinsam zeigen diese Dokumente, welche Netzwerkdosen an welchem Standort noch frei sind. Eine aktuelle Kopie der Belegungsliste des Patchpanels gehört daher immer zur Netzwerkdokumentation.

[1-5] Verkabelungsplan der Firma Caprez Ingenieure AG (Erdgeschoss am Hauptsitz in Chur)

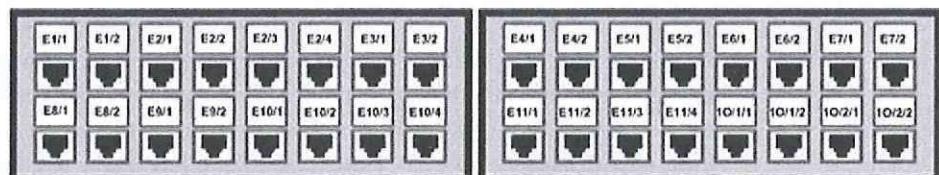


— Bodenkanal

- - - Stichleitung STP Kat. 6

■ RJ45-Mehrgefachnetzdosens (R&M, Typ 6)

[1-6] Patchpanel der Firma Caprez Ingenieure AG (am Hauptsitz in Chur)



[1-7] Belegungsliste des Patchpanels der Firma Caprez Ingenieure AG (am Hauptsitz)

Anschl.	Lokation	Status	Beschreibung	Datum	Von
E1/1	Empfang EG	Belegt	Arbeitsplatz-PC	29.11.13	rsauter
E1/2	Empfang EG	Belegt	VoIP-Telefon	18.05.14	abisang
E2/1	CAD Tiefbau	Belegt	CAD Workstation	13.08.13	rsauter
E2/2	CAD Tiefbau				
E2/3	CAD Tiefbau	Belegt	VoIP-Telefon	19.05.14	abisang
E2/4	CAD Tiefbau	Belegt	Plotter	04.03.14	blaeuchli
E3/1	Bauleiterbüro				
E3/2	Bauleiterbüro	Belegt	MF-Kopierer	11.10.13	rsauter
E4/1	Bauleiterbüro	Belegt	VoIP-Telefon	19.05.14	abisang
E4/2	Bauleiterbüro	Belegt	Arbeitsplatz-PC	11.10.13	rkundert
E5/1	Bauleiterbüro	Belegt	Arbeitsplatz-PC	11.10.13	rkundert
E5/2	Bauleiterbüro	Belegt	VoIP-Telefon	20.05.14	abisang
E6/1	Bauleiterbüro	Belegt	Arbeitsplatz-PC	28.01.14	blaeuchli
...	...	...	...	...	...

Bemerkung: wenn Statusfeld = leer, dann Anschluss = frei / verfügbar. Stand: 5.1.14

## Hilfsmittel

Es gibt zahlreiche **Zeichenprogramme**, mit denen Sie Netzwerkdokumentationen, Verkabelungspläne und andere grafische Darstellungen für Ihre Netzwerkdokumentation erstellen können. Nachfolgend sind drei Programmpakete aufgeführt, die sich besonders dafür eignen.

- **MS Visio 2013:** Die Visio-Grafikprogramme sind sicherlich eines der meistverwendeten Zeichenwerkzeuge zum Erstellen von Netzwerkdokumentationen. MS Visio ist bestens geeignet zum Erstellen von Zeichnungen aller Art, aber auch für Netzwerkdigramme. Visio verfügt über eine grosse Anzahl von Zeichenvorlagen und Icons, auch Shapes genannt. Dank der grossen Verbreitung von Visio bieten Firmen auch Kurse im Umgang mit Visio an. Es gibt unterschiedliche Visio-Editionen, die Standard- und die Professional-Edition. Für das Erstellen von Netzwerkdigrammen reicht die Standard-Edition vollständig aus.
- **SmartDraw Standard:** Eine gute Alternative zu MS Visio. Auch professionelles Zeichenprogramm zum Erstellen von Netzwerklayouts, Büroplänen und vielem mehr. Der Funktionsumfang ist vergleichbar mit dem von Visio Standard, übertrifft aber die Auswahl von speziellen Icons und Netzwerksymbolen im Vergleich zu Visio bei Weitem. Bestehende Visio-Dateien können problemlos von SmartDraw gelesen und weiterbearbeitet werden. Alle SmartDraw-Produkte können direkt via Internet gekauft (heruntergeladen) werden. Unter [www.smartdraw.com](http://www.smartdraw.com) kann eine kostenlose 30-Tage-Testversion von SmartDraw heruntergeladen werden.

- **Calligra Suite:** Bildet eine echte Alternative zu den beiden vorher genannten, proprietären Zeichenprogrammen. Innerhalb von Calligra gibt es das Modul «Flow» zum Erstellen von Diagrammen. Calligra ist ein Open-Source-Paket und kann im Internet kostenlos heruntergeladen werden. Calligra läuft auf MS-Windows-, Unix-/Linux- sowie auf Mac-OS-X-Systemen. Mit Calligra «Flow» lassen sich alle gängigen Diagrammtypen, also auch Netzwerdiagramme, einfach erstellen. Calligra «Flow» verfügt auch über eine grosse Anzahl von Icons und Shapes inklusive der Cisco-Netzwerksymbole. Für den Austausch von Diagrammen, die mit anderen Zeichenprogrammen erstellt wurden, stellt Calligra «Flow» diverse Import- und Exportfilter zur Verfügung. Weitere Informationen zu Calligra und der Download dieses Pakets unter folgender URL<sup>[1]</sup>: <https://www.calligra.org/>.

Für einen möglichst reibungslosen Betrieb eines Computernetzwerks muss dieses überwacht und betreut werden. Die dazugehörigen Aufgaben werden unter dem Begriff **Netzwerkmanagement** zusammengefasst. Das **FCAPS Management Framework** beschreibt die Funktionsbereiche, Ziele und Aufgaben für ein möglichst effizientes und effektives Netzwerkmanagement im Unternehmen. FCAPS umfasst folgende Funktionsbereiche, denen jeweils spezifische Ziele und Aufgaben zugeordnet sind:

- Fault Management
- Configuration Management
- Accounting Management
- Performance Management
- Security Management

Die **Netzwerkdokumentation** ist ein wichtiges Hilfsmittel für das operative Netzwerkmanagement und sollte deshalb folgende Elemente enthalten:

- **Netzwerdiagramm**, das grafisch die Struktur und die Komponenten der Netzwerkinfrastruktur aufzeigt
- **Verkabelungsplan**, aus dem die vorhandenen Netzwerkanschlüsse und deren Belegung / Verfügbarkeit in Erfahrung gebracht werden können

## Repetitionsfragen

- 
- 4 Welche allgemeinen Anforderungen werden an das Netzwerkmanagement gerichtet?
- 
- 21 Nennen Sie die fünf Funktionsbereiche des FCAPS Management Framework.
- 
- 11 Was sollte bei der Verwendung grafischer Symbole für Netzwerkkomponenten beachtet werden?
- 
- 30 Welche Dokumente gehören in eine Netzwerkdokumentation?
- 

[1] Abkürzung für: Uniform Resource Locator. Englisch für: einheitlicher Ressourcenanzeiger. Identifiziert in einem Computernetzwerk die Ressourcen (z. B. eine Website), auf die zugegriffen wird.

## 2 Configuration Management

Netzwerkinfrastrukturen besitzen eine eigene Dynamik, weil sie ständigen Veränderungen unterworfen sind. Typische Beispiele für solche Veränderungen sind:

- Netzwerkgeräte hinzufügen oder neu konfigurieren
- VLANs hinzufügen oder entfernen
- Firewall-Regeln anpassen

Die entsprechenden Netzwerkkomponenten müssen also fortlaufend angepasst werden. Das **Network Configuration Management (NCM)** dient dazu, solche Veränderungen kontrolliert und systematisch durchzuführen. Im Folgenden erfahren Sie mehr über die Ziele und Aufgaben sowie über den Aufbau und Betrieb eines NCM.

### 2.1 Ziele und Aufgaben

Das Network Configuration Management muss alle relevanten Informationen über die Konfigurationen der Netzwerkgeräte möglichst vollständig und aktuell zur Verfügung stellen. Unter dem Begriff Konfiguration sind in diesem Lehrmittel die **Einstellungen eines aktiven Netzwerkgeräts** wie z. B. eines Routers, eines Switches oder einer Firewall gemeint, mit denen bestimmte Funktionen dieses Geräts gesteuert werden können. Wenn also zwei identische Netzwerkgeräte über die gleiche Konfiguration verfügen, sollten sie auch identisch funktionieren («arbeiten»).

#### Hinweis

- ▷ Die Ziele des Network Configuration Management sind nicht identisch mit den Zielen des (Service) Configuration Management nach ITIL<sup>[1]</sup>. So ist beim FCAPS-Netzwerkmanagement beispielsweise die Definition der CMDB/CMS<sup>[2]</sup>-Struktur oder der zu verwaltenden CI<sup>[3]</sup> keine zwingende Vorgabe.

Um die oben genannten Ziele zu erreichen, müssen folgende **Aufgaben** erledigt werden:

- Aktive Netzwerkgeräte identifizieren und erfassen
- Aktuelle Konfigurationen speichern
- Alte Konfigurationen archivieren
- Zugriff auf die aktuellen Konfigurationen regeln

Auf diese Weise kann sichergestellt werden, dass alle benötigten **Konfigurationsinformationen** allen Funktionsbereichen des FCAPS-Netzwerkmanagements zur Verfügung stehen. Der Nutzen dabei ist:

- Der Netzwerkadministrator hat jederzeit den Überblick über die aktiven Netzwerkgeräte.
- Der Netzwerkadministrator hat jederzeit den Überblick über die aktuellen Geräteeinstellungen.
- Bei der Störung oder Wartung eines Netzwerkgeräts kann die ursprüngliche bzw. letztmalige Konfiguration rasch wiederhergestellt werden.

[1] Abkürzung für: IT Infrastructure Library. De-facto-Standard zur Umsetzung des IT Service Management in einem Unternehmen.

[2] Abkürzung für: Configuration-Management-Datenbank / Configuration-Management-System: Datenbank(system) zur Verwaltung von Konfigurationselementen.

[3] Abkürzung für: Configuration Item. Einzelnes Konfigurationselement wie z. B. ein PC, ein Server, eine Applikation oder ein Dienst.

## 2.2 Aufbau und Betrieb

Damit Sie die Komponenten bzw. Geräte eines Netzwerks systematisch verwalten können, muss zunächst geklärt werden, welche Informationen überhaupt verwaltet werden sollen. Auf dieser Basis kann danach ein manuelles oder automatisches NCM aufgebaut werden. Im Folgenden erfahren Sie mehr darüber.

### 2.2.1 Zu verwaltende Komponenten und Informationen definieren

Das **FCAPS Configuration Management** verwaltet alle Geräte oder Komponenten einer Netzwerkinfrastruktur, die individuell angepasst (konfiguriert) werden können. Haben solche Geräte bzw. Komponenten keine Konfigurationsmöglichkeit, handelt es sich um «Plug-and-Play»-Geräte oder um «unmanaged» Komponenten. Diese werden nicht durch das Network Configuration Management, sondern durch das **Asset<sup>[1]</sup> Management** erfasst und verwaltet und im sogenannten Netzwerkinventar aufgeführt. Informationen über Netzwerkschnittstellen (z. B. Netzwerkkarten für Dateiserver, PCs und Drucker) werden nicht durch das Network Configuration Management, sondern durch das **Configuration Management nach ITIL** verwaltet. Folgende Grafik soll diese Abgrenzung bzw. Aufgabenaufteilung verdeutlichen:

[2-1] FCAPS Configuration Management, Asset Management und ITIL Configuration Management im Vergleich



Das FCAPS Configuration Management benötigt insbesondere folgende **Informationen**:

- Eine **Inventarliste** mit allen Netzwerkgeräten und Informationen zur eindeutigen Identifikation (z. B. Hostname, Seriennummer, IP-Adresse). Bei grossen Netzwerkinfrastrukturen erleichtern Zusatzinformationen wie z. B. Standort und Beschreibungen der Geräte den Überblick.
- Die **Konfigurationseinstellungen** der Netzwerkgeräte, wobei für jedes Gerät eine eigene **Konfigurationsdatei** geführt wird. Diese erlauben es, jedes Netzwerkgerät rasch in die Originalkonfiguration bzw. in den Originalzustand zurückzusetzen.

[1] Englisch für: Vermögensgegenstand, Vermögenswert, Aktivposten.

Hier ein Beispiel für eine **Inventarliste**:

Inventarliste Netzwerkgeräte			
Hostname	Standort	IP-Adresse	Gerätebeschreibung
switch-1-chur	Chur	192.168.2.253	ZyXEL XGS-1910-24, 48 Ports (2 x 24 Stack)
switch-1-sam	Samedan	192.168.3.253	ZyXEL XGS-1910-24, 24 Ports
switch-1-bell	Bellinzona	192.168.4.253	ZyXEL XGS-1910-24, 24 Ports
router-fw-1-chur	Chur	192.168.2.1	IPFire Router / FW
router-fw-1-sam	Samedan	192.168.3.1	IPFire Router / FW
...	...	...	...

Im obigen Beispiel dient der Hostname der eindeutigen Identifikation eines Netzwerkgeräts. Jedes physische Gerät wird mit einem entsprechenden Label gekennzeichnet.

#### [2-2] Beschriftung eines Switches (Beispiel)



#### 2.2.2 Manuelles NCM einrichten

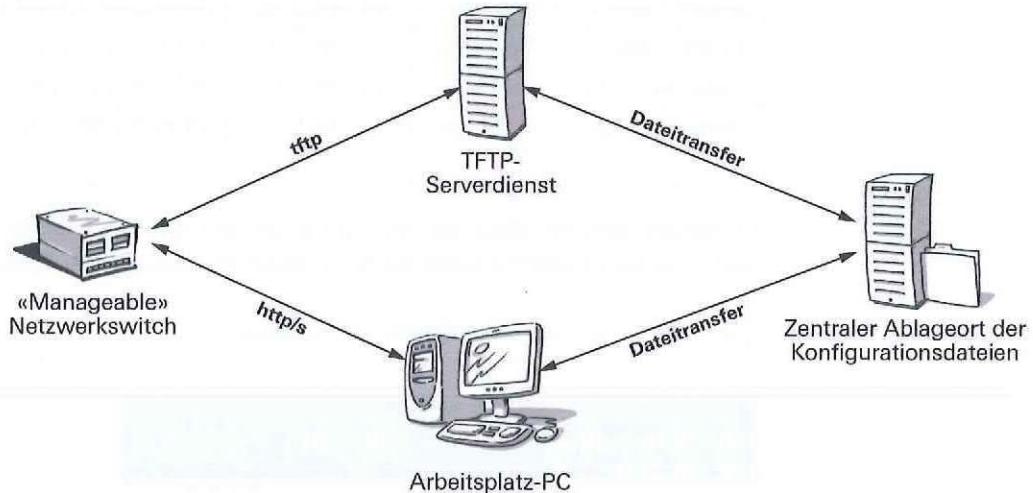
In einem KMU mit einer begrenzten Anzahl von Netzwerkgeräten wird das NCM oft manuell durchgeführt. Folgende Voraussetzungen bzw. Komponenten sind dafür notwendig:

- **TFTP<sup>[1]</sup>-Serverdienst:** Dieses Netzwerkprotokoll dient zum Hoch- und Herunterladen von Konfigurationsdateien der Netzwerkgeräte während des laufenden Systembetriebs. Werden Netzwerkgeräte mit einem Webbrowser verwaltet, können Konfigurationsdateien auch via HTTP / HTTPS direkt auf den lokalen PC heruntergeladen werden.
- **Zentraler Ablageort der Konfigurationsdateien:** Ein geeigneter Ablageort befindet sich z. B. auf einem Dateiserver, dessen Dateien regelmäßig gesichert werden und wo Zugriffe eingeschränkt werden können, weil Konfigurationsdateien schützenswerte Daten wie z. B. Log-ins und Passwörter enthalten können. TFTP-Server erfüllen diese Voraussetzung i. d. R. nicht.

[1] Abkürzung für: Trivial File Transfer Protocol.

Folgende Grafik zeigt die Komponenten und Informationsflüsse einer manuellen NCM-Lösung:

[2-3] Manuelle NCM-Lösung: Aufbau und Funktionsprinzip



Die **Verzeichnisstruktur** zur Speicherung bzw. Archivierung der Konfigurationsdateien sollte selbsterklärend sein. In unserem Fallbeispiel könnte der entsprechende Ablageort etwa wie folgt gegliedert sein:

[2-4] Verzeichnisstruktur für die Ablage von Konfigurationsdateien (Beispiel)

- NCM-Daten
  - Caprez Ingenieure AG
    - Bellinzona
      - Router-FW
      - Switches
      - WLAN
    - Chur
      - NAS
      - Router-FW
      - Switches
      - WLAN
    - Samedan
      - Router-FW
      - Switches
      - WLAN

Die **manuelle Sicherung der Konfigurationsdateien** kann mittels Webbrowser oder TFTP-Server durchgeführt werden. Womit die Gerätekonfigurationen im Einzelfall gesichert werden, ist vom Netzwerkgerät selbst abhängig bzw. davon, welche Möglichkeiten dieses unterstützt. Beim **Up- und Downloaden von Konfigurationsdateien** und beim **Fernzugriff** auf Netzwerkgeräte muss darauf geachtet werden, dass nur verschlüsselte Übertragungsprotokolle zum Einsatz kommen (z. B. https, ssh, sftp). Erfolgt der Fernzugriff über Internet, müssen zwingend verschlüsselte Übertragungsprotokolle verwendet werden.

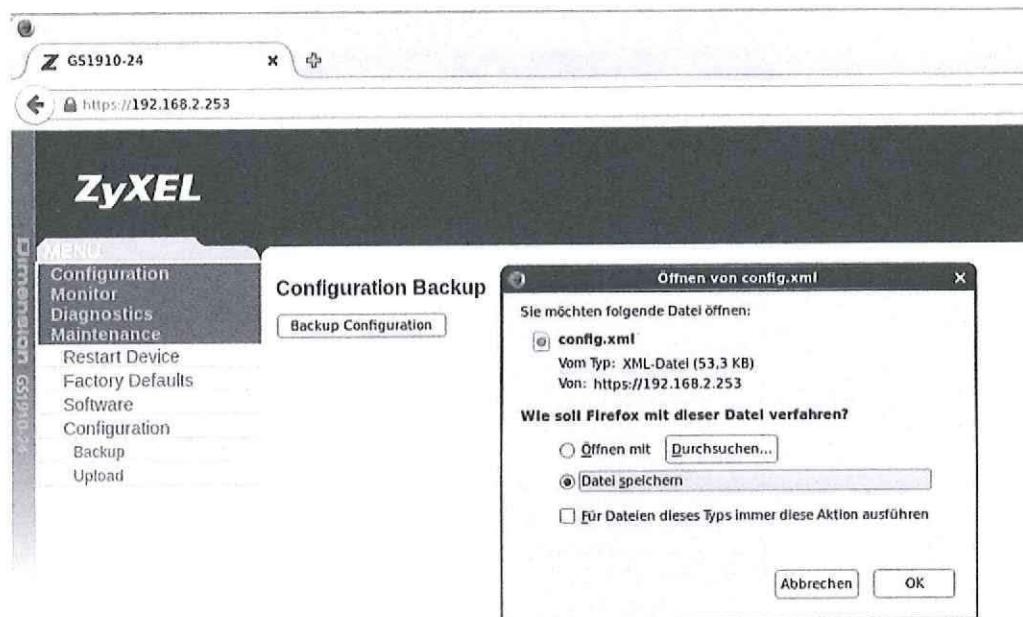
#### Gerätekonfiguration mittels Webbrowser sichern

Die Konfiguration eines Switches kann **via Webbrowser** wie folgt gesichert werden:

1. Tragen Sie als URL die IP-Adresse des Switches ein.
2. Geben Sie Ihren Log-in-Namen und Ihr Passwort ein.
3. Wählen Sie über das Auswahlmenü «Maintenance → Configuration → Backup → Backup Configuration».

Nun erscheint das folgende Dialogfenster:

[2-5] Sicherung einer Gerätekonfiguration mittels Mozilla Firefox (Beispiel)



4. Wählen Sie hier die Option «Datei speichern» aus und klicken Sie danach auf [OK]. In der Folge wird die aktuelle Konfiguration des Geräts (hier ZyXEL GS1910-24) in die Datei **config.xml** geschrieben und im Downloadverzeichnis des lokalen PCs abgespeichert.
5. Versehen Sie diese Konfigurationsdatei mit einer aussagekräftigen, eindeutigen Bezeichnung. Der Dateiname **switch-1-chur-17072015.xml** enthält beispielsweise den Hostnamen des Switches sowie das Erstellungsdatum der Konfigurationsdatei. Anstelle des Erstellungsdatums können Sie auch eine fortlaufende Versionsnummer verwenden.
6. Verschieben Sie abschliessend die Sicherungsdatei mit den Konfigurationsdaten vom lokalen Downloadverzeichnis in den zentralen Ablageort (z. B. **\NCM-Daten\Caprez Ingenieure AG\Chur\Switches**).

#### Hinweis

- ▷ Es empfiehlt sich, auch ältere Konfigurationsdateien aufzubewahren bzw. zu archivieren (z. B. mittels Backup), damit Sie den Verlauf der letzten Änderungen bei Bedarf nachvollziehen können.

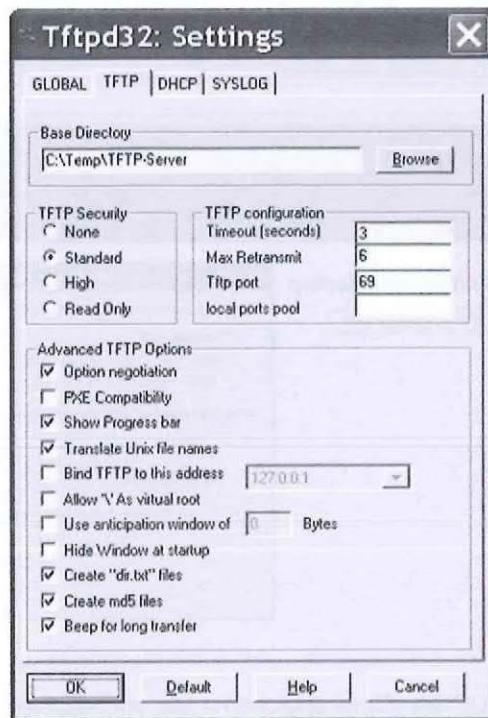
#### Gerätekonfiguration mittels TFTP sichern

Wenn noch kein TFTP-Serverdienst im Netzwerk vorhanden ist, können Sie diesen wie folgt einrichten:

1. Laden Sie das Programm für den TFTP-Serverdienst von <http://tftpd32.jounin.net/> herunter.
2. Führen Sie die heruntergeladene Installationsdatei **Tftpd64-4.50-setup.exe** aus.

Nun erscheint das folgende Dialogfenster:

[2-6] Einstellungen für den TFTP-Serverdienst (Beispiel)



3. Tragen Sie im Eingabefeld «Base Directory» das Verzeichnis ein, in dem die Konfigurationsdateien standardmäßig abgespeichert werden sollen. Die weiteren Angaben entsprechen den Default-Einstellungen des Programms.
4. Stellen Sie sicher, dass der TFTP-Serverdienst gestartet wurde.
5. Melden Sie sich mittels SSH (oder ggf. Telnet) beim Switch an, dessen Konfigurationsdatei gesichert werden soll.

#### Hinweis

- ▷ Verwenden Sie Telnet aus Sicherheitsgründen nur in lokalen Netzwerken.
- 6. Geben Sie nach dem Log-in den **CLI<sup>[1]</sup>-Befehl** ein, der für die Sicherung der aktuellen Konfigurationsdaten auf einen TFTP-Server vorgesehen ist.

#### Hinweis

- ▷ Üblicherweise werden auf der CLI bzw. Konsole eines Netzwerkgeräts nach der Eingabe von ?, help oder show alle verfügbaren Befehle angezeigt.

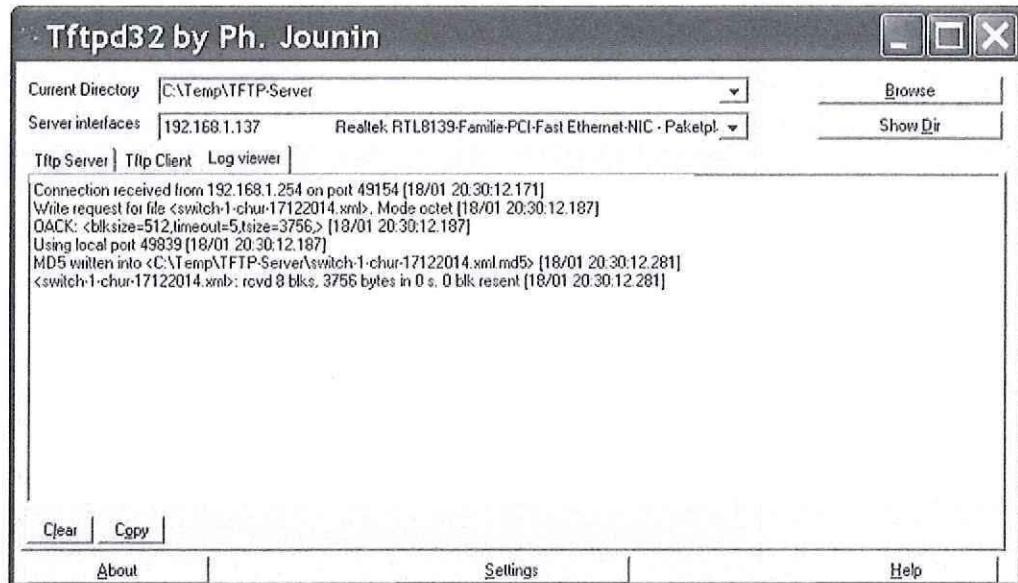
Für den D-Link Switch (Model DGS-1210-24) sieht die entsprechende Ein- und Ausgabe z. B. wie folgt aus:

```
DGS-1210-24> upload cfg_toTFTP tftp://192.168.1.137/switch-1-chur-17122014.xml
% Configuration backup successfully
DGS-1210-24>
```

[1] Abkürzung für: Command Line Interface. Englisch für: Kommandozeilenschnittstelle (wörtl.). Konsole für die direkte Befehlseingabe.

In der Folge wird die gesicherte Konfigurationsdatei im Logfile des TFTP-Servers wie folgt angezeigt:

[2-7] Sicherung der Gerätekonfiguration und Bestätigung unter TFTP



### Hinweis

- ▷ TFTP überträgt immer im Klartext (unverschlüsselt). Aus diesem Grund dürfen Sie Konfigurationsdaten, die mittels TFTP gesichert werden, nie via Internet übertragen. Beim Einsatz von TFTP in einem internen Netzwerk (LAN) ist dies weniger problematisch, solange die auf den TFTP-Server heruntergeladenen Konfigurationsdateien rasch in das dafür eingerichtete Verzeichnis auf dem Dateiserver verschoben werden.

### 2.2.3 Automatisches NCM einrichten

Die Konfigurationsdaten der Netzwerkgeräte lassen sich auch automatisch sichern. Dafür gibt es zahlreiche Softwarelösungen auf dem Markt. Eine automatische NCM-Lösung, die sich für Netzwerke mit Hunderten von Netzwerkgeräten eignet und auf Open Source basiert, heißt **rConfig**. Dieses Produkt bietet folgende Funktionen:

- Zentrale Erfassung und Abfrage der Gerätekonfigurationen via Webbrowser
- Automatische, zeitgesteuerte Abfrage und Archivierung von Gerätekonfigurationen
- Vielseitige Suchfunktionen nach bestimmten Konfigurationen oder spezifischen Einstellungen
- E-Mail-Benachrichtigung bei einer Änderung an einer Gerätekonfiguration
- Benutzerverwaltung zur Definition spezifischer Zugriffsberechtigungen
- Definition und Generierung spezifischer Reports über Gerätekonfigurationen

Die Hauptseite von rConfig sieht wie folgt aus:

[2-8] «Dashboard» für ein automatisches NCM (Beispiel)

The screenshot shows the rConfig dashboard in Mozilla Firefox. The title bar reads "rConfig - Configuration Management - Mozilla Firefox". The address bar shows the URL "rconfig/dashboard.php". The top right corner indicates "Logged In as admin Account | Help | Logout" with a gear icon. The main header "rConfig - Configuration Management" has a gear icon next to it. Below the header is a navigation menu with links: Home, Devices, Scheduled Tasks, Configuration Tools, Compliance, Settings, and a dropdown menu. The IP address "localhost.localdomain:192.168.2.100" is also displayed. The main content area is titled "Dashboard" and contains two sections: "Server Information" and "Last 5 devices added".

Server Information		
Servername	Date Added	Added By
localhost.localdomain	2014-05-19	admin
IP Address	192.168.2.100	
DNS	62.2.24.162	
Addresses		
Internet IP	82.4.12.158	
Disk Free Space	25.83 GiB	

Last 5 devices added		
Device Name	Date Added	Added By
switch-2-chur	2014-05-19	admin
switch-1-chur	2014-06-11	admin
switch-1-same	2014-01-16	admin
switch-1-hell	2014-01-09	admin
router-fw-chur	2014-01-10	admin

### Hinweise

- ▷ rConfig kann unter [www.rconfig.com](http://www.rconfig.com) kostenlos heruntergeladen und unter Linux OS einfach installiert werden.
- ▷ Wird eine NCM-Lösung für Netzwerke mit Tausenden von Netzwerkgeräten benötigt, bietet sich die Open-Source-Lösung **RANCID** an. Dieses Produkt kann kostenlos von [www.shrubbery.net](http://www.shrubbery.net) heruntergeladen werden, wobei die Installation unter Linux OS ziemlich aufwendig ist, weil die Konfigurationsdaten auf einem SQL-Server abgelegt werden müssen.

Beim **Network Configuration Management (NCM)** werden aktive Netzwerkgeräte wie z. B. Router, Switch, Firewalls und Access Points entsprechend den unternehmerischen Anforderungen konfiguriert und die Konfigurationseinstellungen systematisch und zentral verwaltet. Ziel des NCM ist es, Konfigurationsänderungen problemlos nachvollziehen und im Fall einer Netzwerk- oder Systemstörung rasch wieder rückgängig machen zu können.

Ein NCM lässt sich relativ einfach implementieren und betreiben:

- Für **kleine bis mittlere Netzwerke** reicht i. d. R. ein manuell betriebenes NCM aus.
- Für **mittlere bis grosse Netzwerke** sind professionelle Lösungen erhältlich, deren Funktionen sich meist automatisieren lassen. Neben proprietären und kommerziellen Lösungen gibt es auch Open-Source-Lösungen, die z. T. gratis zur Verfügung stehen.

## Repetitionsfragen

---

- 25 Welches Ziel wird beim Network Configuration Management verfolgt?
- 
- 3 Nennen Sie einen allgemeinen Unterschied zwischen NCM und ITIL Configuration Management.
- 
- 19 Was müssen Sie beachten, wenn Konfigurationsdaten mittels TFTP via Internet übertragen werden?
-

## 3 Fault Management

Das **Fault Management** soll die vereinbarte Verfügbarkeit eines Netzwerks sicherstellen und kümmert sich entsprechend um Fehler, die Netzwerkprobleme wie Störungen oder Unterbrüche verursachen (können).

### Hinweis

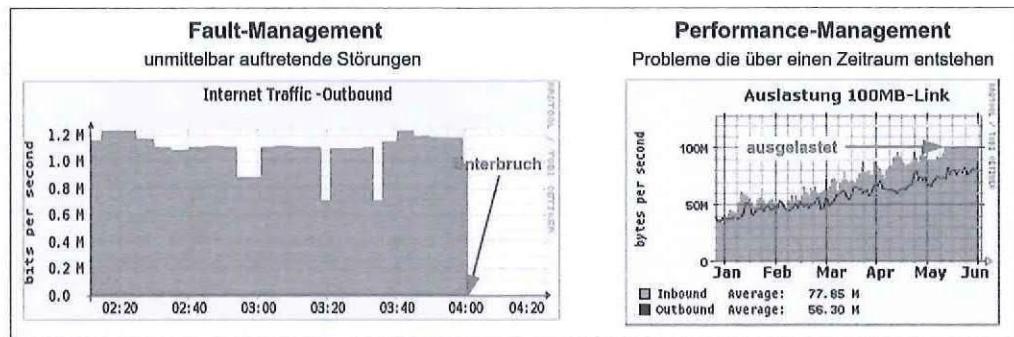
▷ Idealerweise werden Fehler in einem Netzwerk erkannt, bevor sie den Geschäftsbetrieb behindern oder vollständig unterbrechen. Denn solche Fehler kosten die Unternehmen am wenigsten. Je grösser und komplexer eine Netzwerkinfrastruktur aber ist, desto aufwendiger wird es, Fehlersymptome und Fehlerursachen zu finden oder diese sogar proaktiv anzugehen.

Nicht nur das Fault Management, sondern auch das Performance Management kümmert sich um Netzwerkprobleme. Der Unterschied lässt sich wie folgt beschreiben:

- Das Fault Management befasst sich in erster Linie um plötzlich auftretende Störungen, die zum Ausfall eines Netzwerkgeräts, eines Teilnetzes oder des gesamten Netzwerks führen (können).
- Das Performance Management befasst sich hauptsächlich mit Problemen, die über einen längeren Zeitraum entstehen und dazu führen können, dass bestimmte Dienste oder Funktionalitäten eines Netzwerks nur noch eingeschränkt oder gar nicht mehr benutzt werden können.

Folgende Grafik soll diese Unterscheidung verdeutlichen:

[3-1] Fault Management und Performance Management im Vergleich



Im Folgenden lernen Sie das Hauptziel und die Aufgaben eines Fault Management sowie geeignete Instrumente und Massnahmen für diese Aufgaben kennen.

### 3.1 Zweck und Aufgaben

Das **Fault Management** soll einen unterbruchsfreien Betrieb der Netzwerkinfrastruktur gewährleisten und plötzlich auftretende Störungen möglichst rasch und nachhaltig beheben. Um dies zu erreichen, müssen folgende **Aufgaben** erledigt werden:

- Systemmeldungen der Netzwerkgeräte sammeln und analysieren
- Störungen im Netzwerk möglichst rasch erkennen
- Fehler innerhalb der Netzwerkinfrastruktur eingrenzen
- Störungen im Netzwerk möglichst rasch beheben

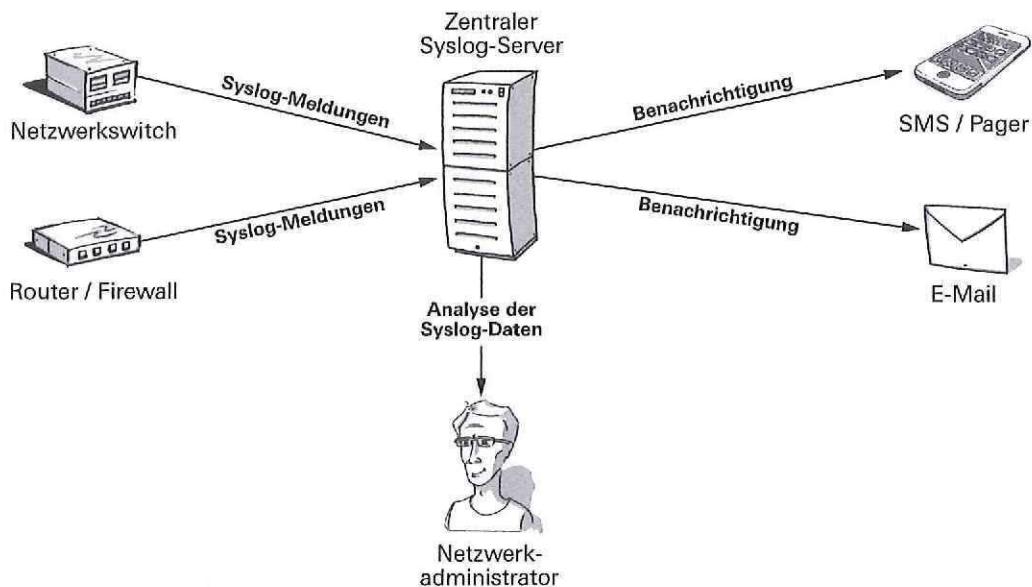
## 3.2 Instrumente und Massnahmen

Bestimmte Fehler wie z. B. Hardwaredefekte lassen sich bereits erkennen, bevor ein Netzwerk vollständig ausfällt. Entsprechende Anzeichen müssen aber frühzeitig erkannt und richtig interpretiert werden. Erste Anzeichen für ein sich anbahnendes Problem finden Sie häufig im **Systemlog** eines Rechnersystems oder eines Netzwerkgeräts. Darin werden Meldungen über Ereignisse<sup>[1]</sup> gespeichert, die Hardware- und Softwarekomponenten während des Systembetriebs erzeugen. So übermittelt etwa eine Festplatte bereits längere Zeit vor einem Totalausfall Fehlermeldungen wie z. B. «Bad-Block»-Events an das Systemlog. Auch verwaltbare Netzwerkgeräte verfügen über ein solches Systemlog. Für eine effiziente Analyse der abgesetzten Systemmeldungen ist es wichtig, dass die verteilten Netzwerkgeräte ihre Meldungen an einen Syslog-Server weiterversenden («forwarden»).

### 3.2.1 Syslog-Server

Ein **Syslog-Server** ist ein zentraler Server(dienst), der Systemmeldungen empfangen und speichern kann. Dies hat den Vorteil, dass Meldungen in einem Netzwerk nicht auf jedem einzelnen, verteilten Netzwerkgerät analysiert werden müssen, sondern an einem zentralen Ort zur Verfügung stehen und sich dadurch viel einfacher analysieren lassen. Folgende Grafik zeigt die Komponenten und Informationsflüsse einer solchen Lösung:

[3-2] Syslog-Server-Lösung: Aufbau und Funktionsprinzip



Ein Syslog-Server sollte mindestens über folgende **Funktionen** verfügen:

- Systemmeldungen filtern bzw. kategorisieren
- Automatische Benachrichtigung<sup>[3]</sup> des Netzwerkadministrators bei bestimmten Ereignissen

[1] Englischer Fachbegriff: Incidents, Events.

[2] Englisch für: defekter Datenblock. Unbrauchbar gewordene Speicherstelle auf einer magnetischen Festplatte.

[3] Englischer Fachbegriff: Notification.

Die Funktionen und Eigenschaften eines Syslog-Servers wurden im RFC 3164 standardisiert: Die Netzwerkgeräte senden ihre Logdaten mittels **UDP<sup>[1]</sup>** an die Port-Nummer 514 des Syslog-Servers und die **Datenpakete** sind wie folgt aufgebaut:

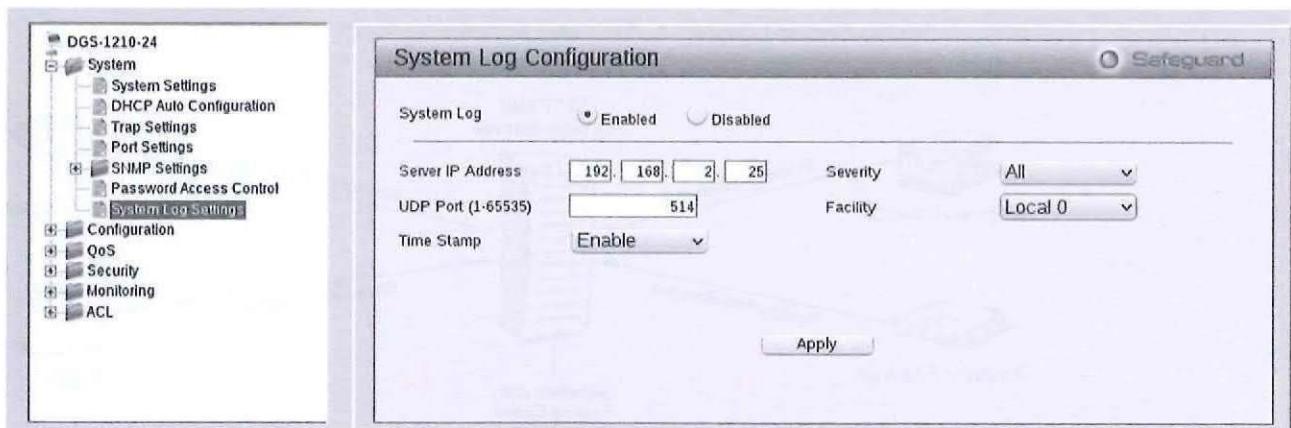
### [3-3] Syslog-Datenpakete: Struktur und Bedeutung

Timestamp	Facility	-	Severity (0–7)	-	Mnemonic	Message Text
00:30:39	%SYS	-	5	-	CONFIG_I:	Configured from Console by Console

Bei der **Konfiguration eines Syslog-Servers** ist zu beachten, dass eingehende Meldungen mit einem Zeitstempel<sup>[2]</sup> versehen werden, der es erlaubt, den genauen Zeitpunkt eines Ereignisses nachzuvollziehen. Aus diesem Grund müssen Sie sicherstellen, dass die Zeit bei jedem überwachten Netzwerkgerät korrekt eingestellt ist. Dies geschieht, indem Sie den **NTP<sup>[3]</sup>-Dienst** aktivieren.

Die Weiterleitung der **Systemmeldungen eines Switches** an den Syslog-Server kann unter «**System Log Settings**» eingestellt werden. Hier das entsprechende Dialogfenster:

### [3-4] Systemmeldungen an Syslog-Server weiterleiten



In kleinen bis mittelgrossen Netzwerken mit bis zu hundert Netzwerkgeräten sollten Sie beim Auswahlfeld «**Severity**»<sup>[4]</sup> die Option [All] festlegen. Dadurch werden alle lokal generierten Systemmeldungen an den zentralen Syslog-Server gesendet. Die Filterung der wirklich relevanten bzw. benötigten Systemmeldungen geschieht dann auf dem Syslog-Server. Die «**Severity-Werte**» wurden in RFC 3195, 5424 und 5426 wie folgt standardisiert:

- 0 = emergency: Notfall, höchste Dringlichkeit
- 1 = alert: Alarm, hohe Dringlichkeit
- 2 = critical: kritisch, mittlere Dringlichkeit
- 3 = error: Fehler, geringe Dringlichkeit
- 4 = warning: Warnung, unkritisch
- 5 = notice: Mitteilung, unkritisch
- 6 = information: Information, unkritisch
- 7 = debug: Detailinformation, unkritisch

[1] Abkürzung für: User Datagram Protocol. Ein einfaches, verbindungsloses Übertragungsprotokoll.

[2] Englischer Fachbegriff: Time Stamp.

[3] Abkürzung für: Network Time Protocol. Netzwerkdienst zur Synchronisation der Uhren von IT-Systemen aller Art.

[4] Englisch für: Schweregrad (einer Systemmeldung/-störung bzw. eines Fehlers).

In **grossen bis sehr grossen Netzwerken** mit Hunderten oder Tausenden von Netzwerkgeräten sollten Sie die Anzahl der generierten Systemmeldungen bereits lokal (auf dem jeweiligen Netzwerkgerät) begrenzen und dort die gewünschte «Severity-Option» einstellen. Auf diese Weise verhindern Sie eine unnötige Belastung des Netzwerks durch den Versand massenhafter Systemmeldungen.

Beim Auswahlfeld «**Facility**»<sup>[1]</sup> können Sie definieren, welche Funktion (Nachrichtenkanal) Systemmeldungen erzeugen und an den Syslog-Server senden soll. In unserem Beispiel bedeutet die Einstellung [Local 0], dass alle lokal generierten Systemmeldungen an den Server weitergeleitet werden.

#### Hinweis

- ▷ Konsultieren Sie im Zweifelsfall die Benutzeranleitung des jeweiligen Netzwerkgeräts, um die korrekten Einstellungen vorzunehmen.

Nachfolgend sehen Sie beispielhaft einen Auszug mit Systemmeldungen, die der Syslog-Server von einem Switch (192.168.1.254) empfangen hat:

[3-5] Meldungen an einen Syslog-Server (Ansicht einer PRTG<sup>[2]</sup>-Monitoring-Lösung)

SYSLOG MESSAGES							
Datum Zeit	Source	Message	Hostname	Timestamp (Device)	Severity	Tag	Facility
25.01.2015 18:43:34	192.168.1.254	Jan 25 18:43:35 2015:WEB-6:Logout through Web(SSL) ( IP: 192.168.1.156 )			6	22	
25.01.2015 20:15:12	192.168.1.254	Jan 25 20:15:13 2015:WEB-6:Successful login through Web(SSL) ( IP: 192.168.1.156 )			6	22	
25.01.2015 20:22:27	192.168.1.254	Jan 25 20:22:27 2015:LinkStatus-6:port 9 link down			6	17	
25.01.2015 20:22:28	192.168.1.254	Jan 25 20:22:29 2015:LinkStatus-6:port 13 link down			6	17	
25.01.2015 20:22:31	192.168.1.254	Jan 25 20:22:32 2015:LinkStatus-6:Port 9 link up, 1Gbps FULL duplex			6	17	
25.01.2015 20:23:57	192.168.1.254	Jan 25 20:23:58 2015:LinkStatus-6:Port 13 link up, 1Gbps FULL duplex			6	17	
25.01.2015 20:24:16	192.168.1.254	Jan 25 20:24:17 2015:WEB-6:Successful login through Web(SSL) ( IP: 192.168.1.156 )			6	17	
25.01.2015 20:33:45	192.168.1.254	Jan 25 20:33:46 2015:WEB-6:Logout through Web(SSL)( IP: 192.168.1.156 )			6	17	
25.01.2015 20:34:11	192.168.1.254	Jan 25 20:34:11 2015:WEB-4:Login failed through Web(SSL) ( IP: 192.168.1.156 )			4	17	
25.01.2015 20:34:38	192.168.1.254	Jan 25 20:34:38 2015:WEB-4:Login failed through Web(SSL) ( IP: 192.168.1.156 )			4	17	

Informationen welche sich gut zum Filtern eignen

Wenn Sie nur Informationen über bestimmte Ereignisse benötigen, können Sie diese aus den übrigen Systemmeldungen herausfiltern. Die oben angezeigten Meldungen lassen sich etwa anhand der Einträge in den Spalten «Severity» und «Facility» oder «Message» weiter eingrenzen und abspeichern. In unserer **PRTG-Monitoring-Lösung** können Sie z. B. folgende **Filtereinstellungen** setzen:

[1] Englisch für: Einrichtung, Standort, Funktionsbereich.

[2] Abkürzung für: Paessler Real Time Grapher. Monitoring-Tool für Netzwerke.

[3-6] Filteroptionen eines Syslog-Servers (Ansicht einer PRTG-Monitoring-Lösung)

FILTER EINSTELLUNGEN FÜR SYSLOG

Filter sind Formeln, die AND , OR , NOT , Klammern und die folgenden Felder verwenden:

Feld	Parameter	Beispiele
source[IP]	Geben Sie UDP-QuellIP, IP-Bereich oder IP-Maske ein	source[10.0.23.50], source[10.0.23.10-50], source[10.0.23.10/255]
facility[Denumerativer]	Geben Sie eine einzelne Zahl oder einen Bereich für den Facility-Code zwischen 0 und 23 ein	facility[2], facility[5-7]
severity[Zahl]	Geben Sie eine einzelne Zahl oder einen Bereich für den Severity-Code zwischen 0 (Emergency) und 7 (Debug) ein	severity[4], severity[1-3]
hostname[Text]	Geben Sie den zu findenden Hostnamen ein (Exakte Suche, Groß-/Kleinschreibung wichtig)	hostname[www.paessler.com]
tag[Text]	Geben Sie das zu findende Tag ein (Exakte Suche, Groß-/Kleinschreibung wichtig)	tag[lu]
appname[Text]	Geben Sie den zu findenden Appnamen ein (Exakte Suche, Groß-/Kleinschreibung wichtig)	appname[mynproc]
procid[Text]	Geben Sie die zu findende Prozess-ID ein (Exakte Suche, Groß-/Kleinschreibung wichtig)	procid[6710]
msgid[Text]	Geben Sie die zu findende Message ID ein (Exakte Suche, Groß-/Kleinschreibung wichtig)	msgid[1047]
message[TeileText]	Geben Sie den im Messagefeld zu findenden Teiltext ein (Teilweise Suche, Groß-/Kleinschreibung unwichtig)	message[Error]
data[TeileText]	Geben Sie den in strukturierten Daten wie in der Tabelle angezeigt zu findenden Teiltext ein (Teilweise Suche, Groß-/Kleinschreibung unwichtig); oder geben Sie eine ID und einen Parameter (Kommagetrennt) ein, um das Vorhandensein des Parameters in der ID zu überprüfen; oder geben Sie eine ID, einen Parameter und einen Wert (Kommagetrennt) ein, um mit einem strukturierten Datenwert zu vergleichen (RFC 5424)	data@exampleSDID@32473
data[ID,Param]	Überprüfen, ob der Param in der angegebenen ID existiert	data@exampleSDID@32473.eventSource
data[ID,Param,Wert]	Suche nach strukturierten Datenwerten (RFC5424)	data@exampleSDID@32473.eventSources.Application

Impliziter Gerätefilter

Dieser Sensor übermittelt einen impliziten Filter über die IP-Adresse des übergeordneten Geräts

Einschließen-Filter

severity[0-4] AND facility[16-23]

Einstellungen zum Filtern bestimmter Systemmeldungen

OK

Abbrechen

Erläuterungen zum obigen Screenshot:

- Durch die Filteroption severity [0-4] werden nur Systemmeldungen der Schweregrade 0 bis 4 angezeigt, also Meldungen, die auf ein Problem hinweisen.
- Durch die Filteroption facility [16-23] werden nur bestimmte funktionsbezogene Systemmeldungen eines Netzwerkgeräts angezeigt. Sollen z.B. nur fehlgeschlagene Log-in-Versuche aufgezeichnet werden, müssen Sie hier die Filteroption data [WEB-4 : Login failed through] verwenden.

Zudem können Sie auf dem Syslog-Server einstellen, welche Ereignisse bzw. Meldungen über welche **Kommunikationskanäle** an den Netzwerkadministrator geschickt werden. Nachfolgend sehen Sie beispielhaft eine entsprechende **Benachrichtigung**<sup>[1]</sup> per E-Mail:

[3-7] E-Mail Notification eines Syslog-Servers (Beispiel)

```

- Warning: Login failed on switch-1-chur (192.168.1.254)
Absender Attila Methé Datum 2015-01-25 23:55
This email was sent to administrator@ingcaprez.ch by your
network monitoring system mgmt-syst-1.ingcaprez.ch
=====
E-Mail gesendet an: administrator@ingcaprez.ch
E-Mail gesendet um: 25/01/2015 / 23:53:51
E-Mail gesendet von: mgmt-syst-1.ingcaprez.ch
=====
```

[1] Englisch: Notification.

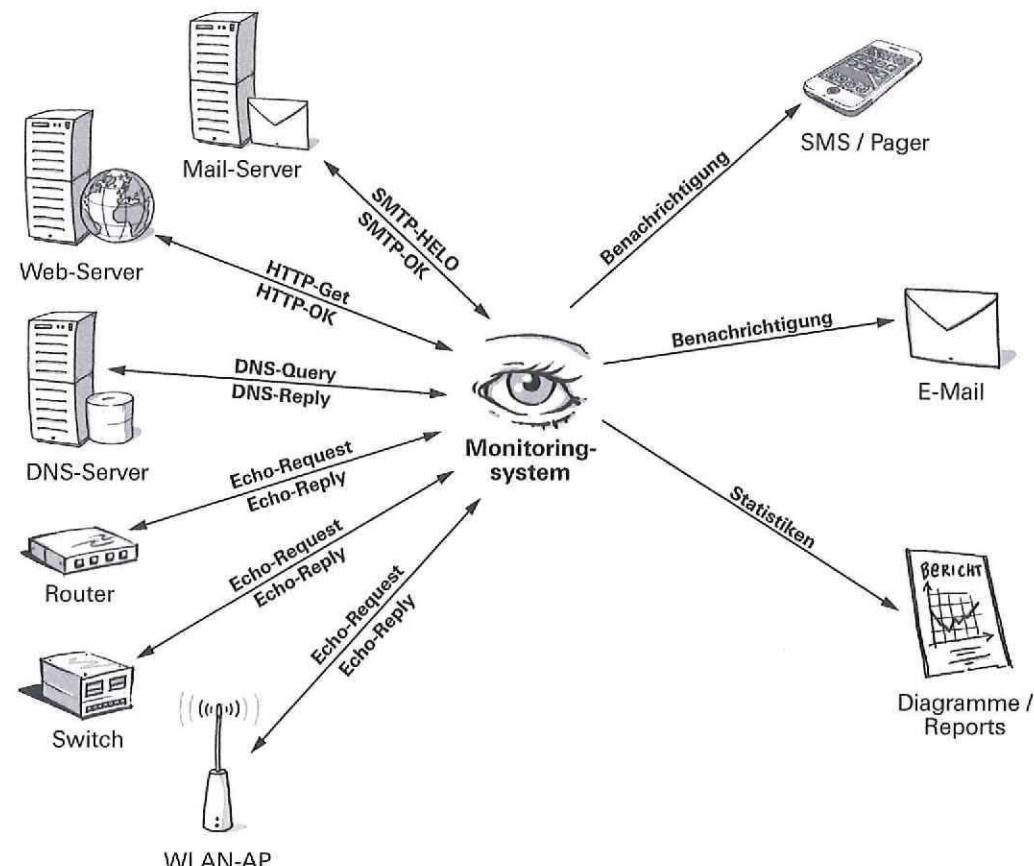
### 3.2.2 Network-Monitoring-Tools

Es kann passieren, dass ein Netzwerkgerät ohne vorherige Warnzeichen plötzlich ausfällt und nicht mehr erreichbar ist. Die Gründe dafür liegen oft in fehlerhaften Hardwarekomponenten. Erfahrungsgemäß sind häufige Ursachen für solche Ausfälle ein defektes Netzteil bzw. eine unterbrochene Netzwerkanbindung. Als Netzwerkadministrator dürfen Sie von solchen Ereignissen nicht erst von den Benutzern erfahren, sondern müssen sofort und automatisch bei Ereigniseintritt darüber informiert werden. Für solche Zwecke stehen ausgereifte **Network-Monitoring-Tools** zur Verfügung, die folgende Funktionen bieten:

- Automatische Überwachung der Netzwerkgeräte (z. B. Switch, Router etc.) und Netzwerkdienste (z. B. E-Mail, WWW, DNS etc.)
- Automatische Alarmierung bei definierten Ereignissen (z. B. Probleme) über definierte Kanäle (z. B. per E-Mail, SMS / Pagerfunktion, Pop-up-Meldung am Bildschirm)
- Automatische Dokumentation der definierten Ereignisse (z. B. Eintrag im Systemlog)
- Skriptausführung, d. h. Start und «Abarbeitung» einer bestimmter Systemroutine bei einem bestimmten Ereignis mithilfe eines vorgefertigten Batchfiles
- Bereitstellung statistischer Informationen (z. B. bezüglich der Verfügbarkeit eines Netzwerkgeräts)

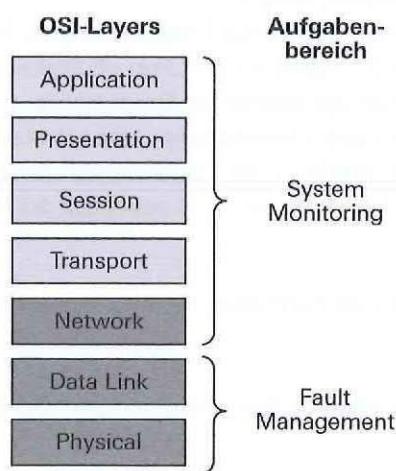
Folgende Grafik zeigt die typischen Komponenten und Informationsflüsse eines solchen Monitoring-Systems:

[3-8] Network-Monitoring-System: Aufbau und Funktionsprinzip



Als Netzwerkadministrator überwachen Sie mit einem solchen System hauptsächlich die **Netzwerkverbindungen** und stellen sicher, dass diese funktionieren. Im Fokus des Fault Management stehen also **Layer 1** (Bitübertagungsschicht bzw. Physical Layer) und **Layer 2** (Sicherungsschicht bzw. Data Link Layer) des OSI-Schichten-Modells. Die Gewährleistung des **ordnungsgemäßen Systembetriebs** ist dagegen Aufgabe des System-administrators bzw. des System Management. Hier stehen höhere Layers des OSI-Schichten-Modells im Zentrum des Interesses. Diese Abgrenzung lässt sich wie folgt veranschaulichen:

[3-9] Fault Management und System Management im Vergleich

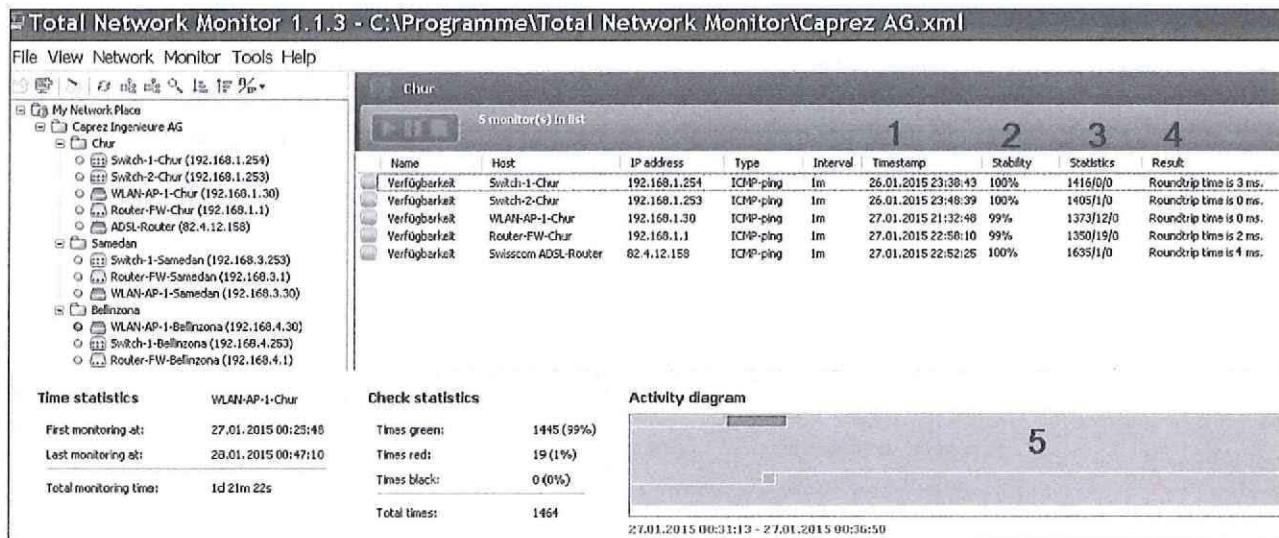


**Hinweis**

- ▷ Für ihre Überwachungsaufgaben greifen das Network Management und das System Management oft auf ähnliche oder gleiche Informationen zurück (z. B. IP-Adressen, TCP/UDP-Ports). Aus diesem Grund setzen viele Unternehmen für das Network-Monitoring und das System-Monitoring das gleiche Monitoring-Tool ein.

In unserem Fallbeispiel wird **Total Network Monitor** als Werkzeug für das Fault Management verwendet. Dieses Tool kann von [www.softinventive.com/products/total-network-monitor/](http://www.softinventive.com/products/total-network-monitor/) kostenlos heruntergeladen werden und eignet sich gut für die Überwachung wichtiger Netzwerkgeräte und -dienste in kleinen bis mittelgrossen Netzwerken. Das entsprechende Hauptmenü sieht wie folgt aus:

## [3-10] Total Network Monitor bei Caprez AG Ingenieure AG (Beispiel)



Wie Sie erkennen können, überwacht die Firma Caprez Ingenieure AG mit diesem Network-Monitoring-Tool die **Verfügbarkeit** der Router bzw. Firewalls, Switches und WLAN Access Points der Standorte Chur, Samedan und Bellinzona. Dabei werden folgende **Informationen** angezeigt:

- Timestamp:** letzter Zeitpunkt, zu dem sich der Verfügbarkeitsstatus eines Netzwerkgeräts geändert hat.
- Stability:** durchschnittliche Verfügbarkeit eines Netzwerkgeräts in Prozent (%). Wird anhand der Werte dieser Spalte über einen bestimmten Zeitraum hinweg berechnet. Je mehr Antworten auf Ping-Anfragen ausbleiben, desto instabiler bzw. desto weniger verfügbar (< 100%) scheint ein überwachtes Netzwerkgerät zu sein.
- Statistics:** Summen folgender Werte: Anzahl der beantworteten und unbeantworteten Anfragen, Anzahl der Zeitintervalle, zu denen der Sensor<sup>[1]</sup> deaktiviert war.
- Result:** durchschnittliche Übertragungsdauer einer Ping-Anfrage vom Sender zum Empfänger und wieder zurück.
- Activity Diagram:** Übersicht über die Zeitintervalle, zu denen das ausgewählte Netzwerkgerät (WLAN-AP-1-Chur) verfügbar (grün) bzw. nicht verfügbar war (rot). Durch Anklicken eines Zeitintervalls werden unten die zugehörigen Detailinformationen angegeben (Datum, Uhrzeit).

Für das **Monitoring** wurden diese Einstellungen vorgenommen bzw. Optionen definiert:

- An jedes überwachte Netzwerkgerät wird im Intervall von einer Minute via ICMP<sup>[2]</sup> eine **Ping<sup>[3]</sup>-Anfrage** gesendet (genauer gesagt sind es jeweils drei Pings pro Intervall, falls ein Ping-Paket verloren geht).
- Wenn ein Netzwerkgerät während dreier Intervalle hintereinander nicht auf eine Anfrage reagiert bzw. antwortet, wird der Netzwerkadministrator mittels Pop-up-Meldung auf dem Bildschirm und per E-Mail darüber informiert.

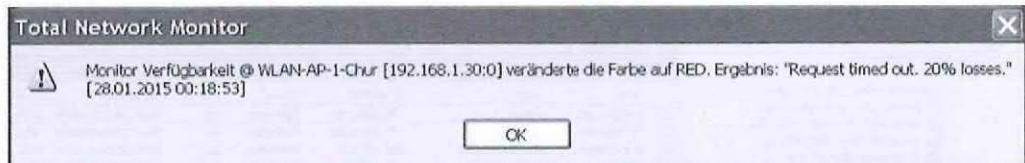
[1] Als Sensor wird jede eingerichtete Messung bezeichnet, die einen Host überwacht. In unserem Beispiel sind fünf Sensoren vorhanden.

[2] Abkürzung für: Internet Control Message Protocol. Spezifisches IP-Protokoll (IPv4) für den Austausch von Informationen und Fehlermeldungen in einem Computernetzwerk.

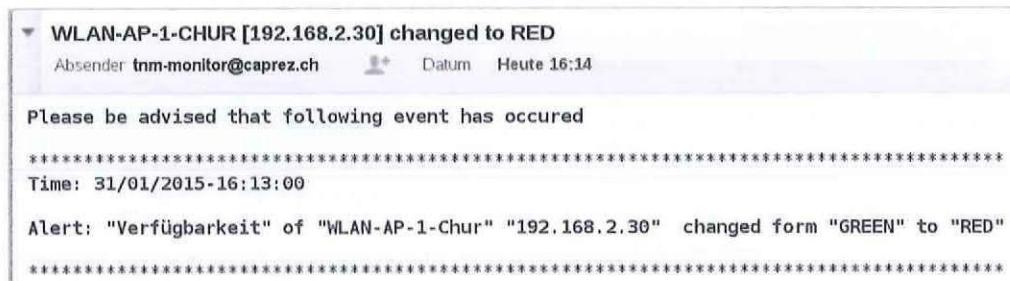
[3] Diagnose-Tool zur Überprüfung der Verfügbarkeit eines entfernten Hosts in einem IP-Netzwerk.

In unserem Fallbeispiel sehen diese Meldungen etwa wie folgt aus:

[3-11] Pop-up-Meldung (Beispiel)



[3-12] Notification per E-Mail (Beispiel)



Bei Netzwerkgeräten wie **Router oder Switches** reichen Ping-Anfragen für ein Monitoring meistens aus, da primär die Verbindungen getestet werden (müssen). Bei einem **Webserver, Mailserver oder DNS-Server** liefert eine Ping-Anfrage aber keinen Aufschluss darüber, ob ein bestimmter Dienst auf diesem System tatsächlich läuft. Aus diesem Grund werden an solche Systeme zusätzlich zu den Pings gezielt **Dienstanfragen** gesendet.

### 3.2.3 Organisatorische Massnahmen

Mithilfe eines Network-Monitoring-Tools können Netzwerkstörungen und Geräteausfälle zwar schnell erkannt, aber nicht behoben werden. Um bei solchen Störungen bzw. Ausfällen möglichst rasch reagieren zu können, lohnt es sich, weitere Vorkehrungen zu treffen. Dazu gehören vor allem folgende **organisatorische Massnahmen**:

- **Verantwortlichkeiten klären:** An wen können bzw. müssen sich die Benutzer im Falle einer Netzwerkstörung bzw. eines Netzerkausfalls wenden, um Unterstützung zu erhalten? Wer ist für den Ersatz eines defekten Netzwerkgeräts zuständig? Wer muss solche Ersatzbeschaffungen genehmigen?
- **Wartungsverträge abschliessen:** Wartungsverträge lohnen sich besonders für Netzwerke bzw. Systeme, deren Ausfall weitreichende Folgen für ein Unternehmen haben können. Dazu gehören in erster Linie Netzwerke, die **wichtige Dienste und Daten** bereitstellen oder verarbeiten und mit einem **SPOF<sup>[1]</sup>-Risiko** behaftet sind. Hier kann ein Wartungsvertrag die notwendige Absicherung bieten und das Unternehmen kann auf fachliche Hilfe seitens des Herstellers oder Lieferanten zurückgreifen.

[1] Abkürzung für: Single Point of Failure. Vergleichen Sie dazu auch das Lehrmittel zum Modul 117.

- **Ersatzmaterial:** Für Ersatzbeschaffungen der wichtigsten Netzwerkgeräte zwecks Überbrückung des Ausfalls eines zentralen Netzwerkgeräts, bei denen die Wiederbeschaffung mehrere Tage in Anspruch nehmen kann, sollte ein Ersatzgerät zur Verfügung stehen. Oft benötigt man zur raschen Überbrückung nicht zwingend das gleiche Modell wie das des defekten Geräts. Beim Ausfall eines «managed» Switch kann oft auch mit einem kostengünstigeren «unmanaged» Switch ein Teil der Grundfunktionen wiederhergestellt werden. Dabei sollte allerdings beachtet werden, dass durch eine solche temporäre Umgehungslösung keine unerwünschten Nebeneffekte wie z. B. Sicherheitslöcher entstehen.

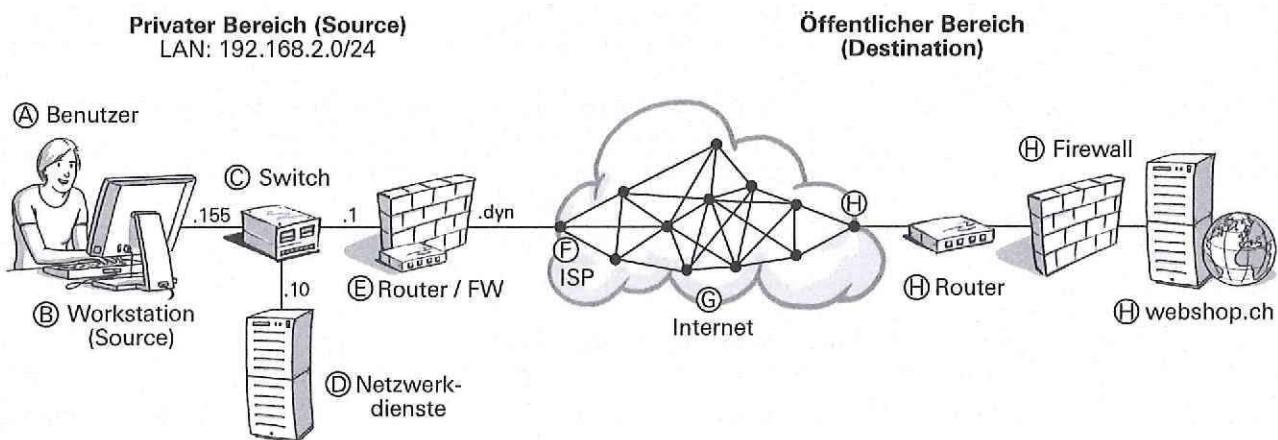
### 3.3 Fehlersuche und -analyse

Erfahrene Netzwerkadministratoren kennen «typische Fehler», die immer wieder zu Störungen oder Ausfällen «ihres» Netzwerks führen, und meist können sie diese auch rasch beheben. Wenn aber der Grund für Störungen oder Ausfällen unbekannt ist, muss der Fehler systematisch gesucht und analysiert werden. Nachfolgend werden grundsätzliche Überlegungen, wichtige Hilfsmittel und ein mögliches Vorgehen für eine systematische Fehlersuche und -analyse vorgestellt.

#### 3.3.1 Überlegungen und Hilfsmittel

Als Netzwerkadministrator haben Sie uneingeschränkten Zugriff auf die Netzwerkkomponenten und -geräte im LAN. Entsprechend ist der **private Bereich** auch die Systemumgebung, in der Sie uneingeschränkt nach Fehlern suchen können. Im **öffentlichen Bereich** haben Sie dagegen nur eingeschränkte Möglichkeiten, um einen Fehler zu lokalisieren. Folgende Grafik soll dies verdeutlichen:

[3-13] Privater und öffentlicher Netzwerkbereich



Die Buchstaben A bis E kennzeichnen Komponenten bzw. Geräte im privaten Bereich, die Netzwerkstörungen oder -ausfälle verursachen können. Die Buchstaben F bis H kennzeichnen Komponenten bzw. Geräte im öffentlichen Bereich, die Netzwerkstörungen oder -ausfälle verursachen können. Je besser Sie den Aufbau des privaten Bereichs kennen, desto schneller können Sie **Fehler im LAN eingrenzen und finden**.

Die **Fehlersuche** kann durch folgende **Aktivitäten** beschleunigt werden:

Aktivitäten	Fragen	Erkenntnisgewinn
<b>Abklärungen beim Benutzer</b>	<ul style="list-style-type: none"> <li>• Seit wann genau funktioniert die Verbindung nicht mehr?</li> <li>• Wurde eine Fehlermeldung ausgegeben?</li> <li>• Kann Ihr Arbeitskollege auf die gewünschte Webpage zugreifen?</li> </ul>	<ul style="list-style-type: none"> <li>• Informationen über die Störung</li> <li>• Informationen über die aktuelle Situation</li> <li>• Informationen über die Situation vor der Störung</li> </ul>
<b>Visuelle bzw. physische Kontrolle</b>	<ul style="list-style-type: none"> <li>• Ist das Netzwerkkabel korrekt angeschlossen?</li> <li>• Ist das Gerät eingeschaltet?</li> <li>• Leuchtet eine bestimmte LED?</li> </ul>	<ul style="list-style-type: none"> <li>• Informationen darüber, ob überhaupt ein Fehler vorliegt</li> <li>• Informationen darüber, welche Art von Fehler wahrscheinlich vorliegt (Verbindungs-, Hardware-, Softwarefehler)</li> </ul>

Als **technische Hilfsmittel für die Fehlersuche** reichen sogenannte **Bordmittel** meistens aus. Dabei handelt es sich um Tools, die im Lieferumfang eines Betriebssystems enthalten sind und sich einfach installieren und bedienen lassen. In der folgenden Tabelle werden solche **Tools<sup>[1]</sup>** beschrieben, die für die **Fehlersuche unter MS Windows** und Linux eingesetzt werden können:

Windows-Befehl	Linux-Befehl	Funktion
arp	(arp)	Überprüft die Zuweisung der IP-Adresse (OSI Layer 2) zur MAC-Adresse (OSI Layer 3)
ipconfig -all	(ifconfig) -all	Überprüft die IP-Konfiguration eines Systems oder einer Netzwerkschnittstelle
ping	(ping)	Überprüft die Verfügbarkeit eines Hosts oder eines anderen Systems auf IP-Basis (OSI Layer 3) und gibt die Latenzzeit sowie die Anzahl der erfolgreichen und verloren gegangenen Ping-Antworten an
netstat -es	(netstat) -es	Überprüft Ethernet auf bestimmte Netzwerkfehler und gibt eine detaillierte Übertragungsstatistik aus (OSI Layer 2 bis 4)
netstat -ab	(netstat) -ab	Zeigt die aktiven TCP/UDP-Verbindungen eines Rechners an (inklusive Port-Nummern, Gegenstelle, Verbindungsstatus und Programm, das diese Verbindung nutzt [OSI Layer 4 und 7])
tracert	(traceroute)	Überprüft und zeigt den gesamten Übertragungspfad an und gibt alle Router zwischen dem Sender und dem Empfänger eines IP-Datenpakets aus (OSI Layer 3)
nslookup	(nslookup)	Überprüft die Antwort eines DNS-Servers auf die DNS-Anfrage eines bestimmten Hosts oder einer IP-Adresse (OSI Layer 5)
nmap zenmap	(nmap)	Überprüft die Verfügbarkeit bestimmter Netzwerkdienste auf einem entfernten Rechner (OSI Layer 4)
	(whois)	Überprüft den Eigentümer einer bestimmten Domain bzw. einer öffentlichen IP-Adresse (OSI Layer 5)

MIB Browser

### 3.3.2 Praktisches Vorgehen (Beispiel)

Im Folgenden wird anhand eines typischen Problems aus der Praxis ein **Beispielvorgehen für die Fehlersuche und -analyse** demonstriert. Es soll aufzeigen, dass je nach Bedarf an Informationen (Erkenntnisgewinn) unterschiedliche Überlegungen, Aktivitäten und Tools zur Anwendung kommen. Die Buchstaben verweisen auf die Abbildung 3-13, S. 39.

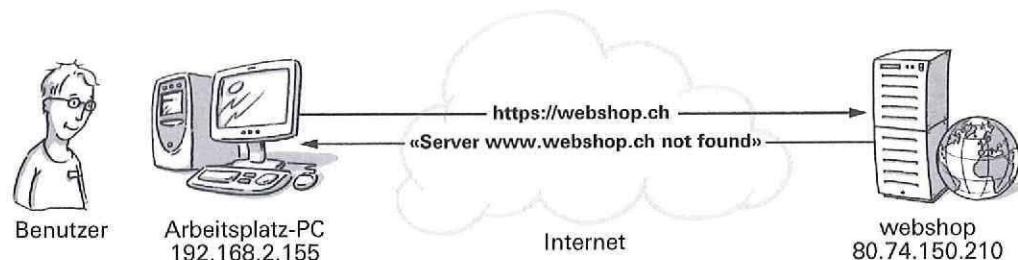
#### Hinweis

- ▷ Sämtliche Beispiele können sowohl unter Windows als auch unter Linux durchgeführt werden. Bei Ausnahmen wird speziell darauf hingewiesen.

[1] Die letzten beiden Tools sind standardmäßig keine Bordmittel und müssen bei Bedarf zusätzlich installiert werden.

Stellen Sie sich folgende **Ausgangssituation** vor: Ein Benutzer versucht über WWW auf den Webserver webshop.ch im Internet zuzugreifen. Nach längerer Wartezeit kommt folgende Fehlermeldung zurück: «Server www.webshop.ch not found».

[3-14] Fehlermeldung nach Zugriff auf Server im Internet



Der Webserver ist also nicht verfügbar. Doch wo genau liegt das Problem? Bei der Fehler-suche und -analyse gehen wir in folgenden Schritten vor:

### 1. Fehler reproduzieren

Vorliegende Information(en): URL des Webservers webshop.de

- Überlegung: Kann ich als Netzwerkadministrator auf diese Website zugreifen?
- Vorgang: Netzwerkadministrator → Fehler reproduzieren.
- Aktion: Aufruf der Website <http://webshop.de> auf dem eigenen Rechner.
- Fazit: Falls der Zugriff auf die Webseite funktioniert, hat der Benutzer die URL vermutlich falsch eingegeben.

Resultat: Der Netzwerkadministrator kann auch nicht auf die Website zugreifen. Da er aber noch nie auf diese Website zugreifen musste, fährt er mit der Fehlersuche bzw. -analyse direkt beim betroffenen Benutzer weiter.

### 2. Details beim Benutzer abklären (A)

Vorliegende Information(en): keine

- Überlegung: Wann hat der Zugriff auf die Website zuletzt geklappt? Handelt es sich um ein lokales Problem?
- Vorgang: Supportmitarbeiter → Abklärungen beim Benutzer (A).
- Aktion: Wann hat der Zugriff auf diese Website zuletzt geklappt? Seit wann genau besteht das Problem? Kann ein anderer Mitarbeiter auf diese Website zugreifen?
- Fazit: Wurde etwas im Netzwerk verändert oder handelt es sich um ein lokales Problem auf dem Rechner des Benutzers?

Resultat: Der letzte erfolgreiche Zugriff des Benutzers auf diese Website war gestern Vormittag. Der Arbeitskollege bestätigt, dass auch er seit gestern nicht mehr auf die Website zugreifen kann.

### 3. Netzwerkkonfiguration des Benutzerrechners überprüfen (B)

Vorliegende Information(en): IP-Adressen, die dem Client vom DHCP-Server zugewiesen worden sind

- Überlegung: Verfügt der Rechner über eine korrekte IP-Adresskonfiguration?
- Vorgang: Supportmitarbeiter → Überprüfen der Netzwerkkonfiguration beim Rechner des Benutzers.
- Aktion / Tool: Ausführen des Befehl `ipconfig /all`.

Die korrekte Konfiguration der IP-Adresse für diesen Rechner sieht z. B. wie folgt aus:

[3-15] Ausgabe des ipconfig-Befehls auf dem Benutzerrechner (Beispiel)

```
C:\WINDOWS\system32\cmd.exe
C:\>ipconfig /all
Windows-IP-Konfiguration

Host Name . . . . . : kvm-xp-1
Primäres DNS-Suffix . . . . . :
Knotentyp . . . . . : Gemischt
IP-Routing aktiviert . . . . . : Nein
WINS-Proxy aktiviert . . . . . : Nein

Ethernetadapter LAN-Verbindung:
  Verbindungsspezifisches DNS-Suffix: Realtek RTL8139-Familie-PCI-Fast Ethernet-NIC
  Beschreibung . . . . . : Realtek RTL8139-Familie-PCI-Fast Ethernet-NIC
  Physische Adresse . . . . . : 52-54-00-6B-58-A7
  DHCP aktiviert . . . . . : Ja
  Autokonfiguration aktiviert . . . . . : Ja
  IP-Adresse . . . . . : 192.168.2.155
  Subnetzmaske . . . . . : 255.255.255.0
  Standardgateway . . . . . : 192.168.2.1
  DHCP-Server . . . . . : 192.168.2.3
  DNS-Server . . . . . : 62.2.24.162
  Lease erhalten . . . . . : Sonntag, 1. Februar 2015 20:07:31
  Lease läuft ab . . . . . : Montag, 2. Februar 2015 02:07:31
```

Resultat: Die obigen IP-Adressen sind gültig, d. h., die IP-Konfiguration sieht korrekt aus. Ob die Verbindungen zum aufgelisteten Gateway, DHCP und DNS aber effektiv funktionieren, muss einzeln überprüft und ggf. analysiert werden. Bestimmte IP-Adressen deuten auf ein mögliches Netzwerkproblem hin. So gibt etwa eine IP-Adresse in der Form 169.254.x.x Hinweise auf ein Problem mit dem DHCP-Server.

#### Hinweis

- ▷ Wurde einem Rechner mit aktiviertem DHCP eine **APIPA<sup>[1]</sup>-Adresse** zugewiesen, weist dies darauf hin, dass entweder der DHCP-Dienst nicht korrekt funktioniert oder die Verbindung zum DHCP-Server unterbrochen ist.

### 4. Verbindungen zu wichtigen Netzwerkdiensten überprüfen (D, E, F)

Vorliegende Information(en): aktuelle IP-Adresskonfiguration vom DHCP-Server erhalten

- Überlegung: Stehen die erforderlichen Netzwerkdienste überhaupt zur Verfügung?
- Vorgang: Supportmitarbeiter → Überprüfung der Verbindung zu wichtigen Netzwerkdiensten.
- Aktion / Tool: Ping auf die beiden Netzwerkdienste Standard-Gateway und DNS-Server.
- Fazit: Antworten die angepingten Netzwerkdienste, funktionieren die Verbindungen.

[1] Abkürzung für: Automatic Private IP Addressing. Englisch für: automatische Zuweisung einer IP-Adresse (ohne Hilfe eines DHCP-Servers).

Hier das Ergebnis eines erfolgreichen Pings auf die IP-Adresse des Standard-Gateways:

[3-16] Funktionierende Verbindung zum Standard-Gateway (Beispiel)

```
C:\>ping 192.168.2.1
Ping wird ausgeführt für 192.168.2.1 mit 32 Bytes Daten:
Antwort von 192.168.2.1: Bytes=32 Zeit<1ms TTL=64

Ping-Statistik für 192.168.2.1:
Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms
```

**Hinweis**

- ▷ Ein erfolgreicher Ping auf den Domänennamen eines Webservers liefert in einem einzigen Arbeitsschritt folgende Informationen: DNS, Standard-Gateway und Internetanschluss funktionieren korrekt.

Hier das Ergebnis eines erfolgreichen Pings auf die Domäne «webshop.ch»:

[3-17] Funktionierende Verbindung zur Domäne (Beispiel)

```
C:\>ping webshop.ch
Ping webshop.ch [80.74.150.210] mit 32 Bytes Daten:
Antwort von 80.74.150.210: Bytes=32 Zeit=9ms TTL=57
Antwort von 80.74.150.210: Bytes=32 Zeit=8ms TTL=57
Antwort von 80.74.150.210: Bytes=32 Zeit=8ms TTL=57
Antwort von 80.74.150.210: Bytes=32 Zeit=10ms TTL=57

Ping-Statistik für 80.74.150.210:
Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust)
Ca. Zeitangaben in Millisek.:
Minimum = 8ms, Maximum = 10ms, Mittelwert = 8ms
```

Resultat: Obwohl der Zugriff ins Internet funktioniert und auch die Namensauflösung via DNS ordnungsgemäss läuft, kann immer noch nicht auf die Website zugegriffen werden. Mehrere Benutzer bestätigen aber, dass der Zugriff auf die Website «webshop.ch» gestern noch möglich war.

## 5. Dienste des entfernten Webserver überprüfen (H)

Vorliegende Information(en): IP-Adresse / Domainname des gewünschten Webservers

- Überlegung: Kann der Webserver erreicht werden? Sind die notwendigen Dienste auf dem entfernten System überhaupt verfügbar?
- Vorgang: Supportmitarbeiter → Laufende Dienste auf dem entfernten Webserver überprüfen.
- Aktion: Verfügbare Dienste auf dem entfernten System mittels Portscan überprüfen.<sup>[1]</sup>
- Fazit: Ist das entfernte System via IP erreichbar (OSI Layer 3), kommt als Ursache z. B. die Filterung der Ports 80/443 in der lokalen Firewall oder in der entfernten Firewall in Frage. Daneben ist es auch möglich, dass die notwendigen Dienste oder das gesamte System bei «webshop.ch» nicht ordnungsgemäss laufen.

Hier das Ergebnis des Portscans auf den Webserver «webshop.ch»:

[3-18] Fehlende Verbindung zum entfernten Webserver (Beispiel)

The screenshot shows a command prompt window titled 'C:\WINDOWS\system32\cmd.exe'. The command entered is 'C:\>nmap webshop.ch'. The output of the Nmap scan is as follows:

```
Nmap 5.51 ( http://nmap.org ) at 2015-02-02 22:40 Westeuropäische Normalzeit
Nmap scan report for webshop.ch (80.74.150.210)
Host is up (0.0036s latency).
rDNS record for 80.74.150.210: inn.host.ch
Not shown: 974 filtered ports
PORT      STATE SERVICE
20/tcp    closed  ftp-data
21/tcp    open   ftp
25/tcp    open   smtp
53/tcp    open   domain
80/tcp    closed  http
106/tcp   open   pop3pw
110/tcp   open   pop3
143/tcp   open   imap
443/tcp   closed  https
465/tcp   open   smtps
587/tcp   open   submission
993/tcp   open   imaps
995/tcp   open   pop3s
2121/tcp  open   cccproxy-ftp
3306/tcp  open   mysql
8443/tcp  open   https-alt

Nmap done: 1 IP address (1 host up) scanned in 5.78 seconds
```

Resultat: Der erfolglose Zugriff auf den Webserver wird durch die Protokolle http und https verursacht, die nicht verfügbar sind bzw. gesperrt wurden. Ob eine Firewall diese Protokolle sperrt oder ob der Webserverdienst auf dem entfernten System IP 80.74.150.210 deaktiviert worden ist, können wir nicht sagen.

Lösungsmöglichkeiten: Um diese Frage zu klären, kommen folgende Optionen in Frage:

- Der Benutzer wartet, bis der Webdienst wieder gestartet bzw. bis die Sperre der beiden Protokolle aufgehoben ist und der Zugriff auf die gewünschte Website wieder funktioniert.
- Sie kennen eine Ansprechperson in der Firma, die den Server «webshop.ch» betreibt, und versuchen, diese zu kontaktieren, um die Ursache des Problems herauszufinden.
- Sie ermitteln die Adressdaten des zugehörigen Domänenhalters via CLI oder über einen «Whois»-Dienst im Internet (z. B. <https://www.switchplus.ch/whois>).

Im folgenden Screenshot sehen Sie exemplarisch die «Whois»-Angaben zum Halter der Domäne «webshop.ch»:

[1] Vergleichen Sie zum Portscan das Kapitel 3.3.3, S. 45.

**[3-19] Informationen über den Halter der Domäne «webshop.ch»**

```
Wer ist der Halter der DOMAIN (Whois)
Query: webshop.ch
Registry: whois.nic.ch
Results:
whois: This information is subject to an Acceptable Use Policy.
See http://www.nic.ch/terms/aup.html
Domain name:
webshop.ch

Holder of domain name:
MS Mail Service AG
Müller Christine
Buchhaltung
Fürstenlandstrasse 35
CH-9001 St. Gallen
Switzerland
Contractual Language: German

Technical contact:
mhs internet AG
Hertzog Matthias
http://www.mhs.ch
Zürcher Strasse 204
CH-9014 St. Gallen
Switzerland

Registrar:
mhs @ internet AG

First registration date:
1997-06-19

DNSSEC:N

Name servers:
ns.ch-inter.net
ns2.ch-inter.net
```

### 3.3.3 Weitere Möglichkeiten

Im Folgenden werden zusätzliche oder ergänzende Überlegungen, Aktivitäten und Tools vorgestellt, die je nach Situation bei der Fehlersuche und -analyse nützlich sein können.

#### Portscans durchführen (B und H)

Anstatt alle Ports eines Systems zu scannen, können Sie auch gezielt nach dem Zustand (Status) eines Ports oder die Erreichbarkeit eines Diensts überprüfen.

##### Beispiel

```
nmap webshop.ch -p 80,443
```

Mittels Eingabe von `nmap webshop -p 80:443` beim Nmap-Portscanner werden gezielt die Status der TCP-Ports 80 und 443 abgefragt.

##### Hinweis

- ▷ Mehrfache bzw. regelmässige Portscans auf fremde Systeme können von deren Betreiber als Vorbereitung (Ausspionieren, Informationsbeschaffung) für eine Attacke betrachtet werden. Daher sollten Sie Portscans möglichst auf eigene Systeme begrenzen und bei fremden Systemen nur zurückhaltend anwenden.

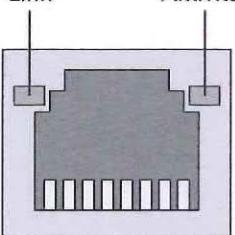
#### Verbindung zwischen Rechner und Switch überprüfen (B und C)

Der **Status einer Netzwerkschnittstelle** (OSI Layer 1 und 2) lässt sich auf verschiedene Weise überprüfen. Im Folgenden werden drei Optionen näher vorgestellt.

## 1. Schnittstelle visuell kontrollieren

Die meisten Netzwerkschnittstellen von Rechnern verfügen über zwei **LED<sup>[1]</sup>-Lämpchen**, die Auskunft über den Portstatus geben.

[3-20] Visuelle Kontrolle der Verbindung

	<b>Link On:</b> Verbindung zwischen Rechner und Switch aktiv <b>Link Off:</b> Verbindung zwischen Rechner und Switch nicht aktiv <b>Aktivität:</b> Blinkt, wenn Daten über diese Schnittstelle gesendet werden (Information nicht für die Fehlersuche und -analyse geeignet)
---	--

### Hinweis

- ▷ Welche LED welche Information liefert, kann im Zweifelsfall im Handbuch oder im Online-Hilfesystem des betreffenden Rechners nachgelesen werden.

Mögliche Ursachen für eine **inaktive Verbindung** sind:

- Die Netzwerkabnehmer sind nicht korrekt eingesteckt.
- Der Switchport wurde deaktiviert (disabled).
- Der Switchport ist einem anderen VLAN zugeordnet.
- Der Treiber für die Netzwerkschnittstelle konnte nicht geladen werden.
- Die Übertragungsmodi des Senders und des Empfängers sind nicht aufeinander abgestimmt.

## 2. Switchport via CLI überprüfen

Auf einem «managed» Switch empfiehlt es sich, den Portstatus direkt über die CLI zu prüfen. Der folgende Screenshot zeigt die Statusinformationen einiger Ports auf einem Cisco Catalyst 4500 Series Switches. Der Gigabitport Gi1/3 ist deaktiviert und kann nur vom Netzwerkadministrator reaktiviert werden.

[3-21] Statusprüfung via CLI (Cisco Catalyst 4500)

Switch# show interfaces status						
Port	Name	Status	Vlan	Duplex	Speed	Type
Gi1/1		connected	1	a-full	auto	10/100/1000-TX
Gi1/2		connected	1	auto	auto	10/100BaseTX
Gi1/3	Down (Administratively down)	disabled		auto	auto	10/100/1000-TX
Gi1/4		connected	1	a-full	auto	10/100/1000-TX
Gi1/5		connected	1	auto	auto	10/100/1000-TX

[1] Abkürzung für: Light-emitting Diode. Englisch für: Leuchtdiode.

### 3. Switchport via Webinterface überprüfen

Hier werden die aktuellen Porteinstellungen mittels eines Webbrowsers überprüft.

[3-22] Statusprüfung via Webinterface (D-Link DGS 1210-24)

The screenshot shows a 'Port Settings' window with the following configuration:

Port	Link Status	Speed	MDI/MDIX	Flow Control
1	100M Full	Auto	AUTO	Disabled
2	100M Full	Auto	AUTO	Disabled
3	Down	Auto	AUTO	Disabled
4	Down	Auto	AUTO	Disabled
5	Down	Auto	AUTO	Disabled
6	Down	Auto	AUTO	Disabled
7	Down	Auto	AUTO	Disabled
8	Down	Auto	AUTO	Disabled
9	1000M Full	Auto	AUTO	Disabled
10	Down	Auto	AUTO	Disabled
11	Down	Auto	AUTO	Disabled
12	Down	Auto	AUTO	Disabled
13	1000M Full	Auto	AUTO	Disabled
14	1000M Full	Auto	AUTO	Disabled
15	Down	Auto	AUTO	Disabled

### Übertragungsweg zwischen Sender und Empfänger prüfen (H)

In manchen Situationen hilft es zu wissen, welchen **Weg die Datenpakete** zwischen dem eigenen System und einem entfernten System zurücklegen müssen. Bei langen Antwortzeiten können Sie anhand dieser Information evtl. Rückschlüsse auf Verbindungsprobleme ziehen. Lassen Sie sich zu diesem Zweck mittels Befehl tracert alle Router zeigen, die ein Datenpaket zwischen Sender und Empfänger passieren muss. Dabei werden auch Informationen über die Latenzzeit zwischen den einzelnen Routern angezeigt. Im folgenden Screenshot können Sie etwa die **Route zum Webserver «webshop.ch»** verfolgen:

[3-23] Route zum Webserver (Beispiel)

```
C:\>tracert webshop.ch
Routenverfolgung zu webshop.ch [80.74.150.210] über maximal 30 Abschnitte:
 1 <1 ms <1 ms <1 ms 192.168.2.3
 2 9 ms 7 ms 9 ms 80-218-244-1.dclient.hispeed.ch [80.218.244.1]
 3 8 ms 7 ms 8 ms 217-168-57-209.static.cablecom.ch [217.168.57.209]
 4 10 ms 10 ms 9 ms 84.116.200.237
 5 10 ms 7 ms 9 ms ch-zrh01b-ra1-ae1.aorta.net [84.116.134.142]
 6 8 ms 11 ms 8 ms lg-g100-cr1.ch-meta.net [80.74.134.13]
 7 8 ms 9 ms 9 ms inn.host.ch [80.74.150.210]

Ablaufverfolgung beendet.
```

### Hinweis

- ▷ Für eine gezielte Routenprüfung können Sie die Befehle tracert (unter MS Windows) bzw. traceroute (unter Linux) um diverse Optionen erweitern. Die weiteren Optionen des tracert-Tools können Sie sich mithilfe der Hilfeoption tracert -? anzeigen lassen.

### Probleme mit der Namensauflösung analysieren

Bei der **Namensauflösung** werden die Namen der Domänen und Hosts vom DNS in die zugehörigen IP-Adressen verwandelt. Mit dem Befehl nslookup können Sie überprüfen, welche IP-Adresse das DNS einem bestimmten Domänen- bzw. Hostnamen zugeordnet hat. Für unseren Webshop sieht die entsprechende Zuordnung etwa wie folgt aus:

[3-24] Namensauflösung der Domäne «webshop.ch»

The screenshot shows a Windows Command Prompt window titled 'C:\WINDOWS\system32\cmd.exe'. The command entered is 'nslookup webshop.ch'. The output shows two entries: one from a server named 'ns5.cablecom.net' with the address '62.2.24.162', and another 'Nicht autorisierte Antwort' (unauthorized answer) from a different server with the name 'webshop.ch' and the address '80.74.150.210'.

```
C:\>nslookup webshop.ch
Server: ns5.cablecom.net
Address: 62.2.24.162

Nicht autorisierte Antwort:
Name: webshop.ch
Address: 80.74.150.210
```

Beachten Sie in diesem Zusammenhang folgende Aspekte:

- Bei einigen Betriebssystemen werden die vom DNS-Server gesendeten Daten auf dem Client zwischengespeichert («gecached»). Um sicherzustellen, dass die Informationen zur Namensauflösung aktuell sind (d. h. direkt vom DNS-Server stammen und nicht aus dem lokalen DNS-Cache), können Sie den Zwischenspeicher des Clients mit dem Befehl ipconfig /flushdns (unter MS Windows) löschen. Dieser wird danach automatisch sukzessive wieder «aufgefüllt».
- Bei der Namensauflösung schaut das DNS immer zuerst in der lokalen Datei **hosts** nach, ob die gewünschte Information verfügbar ist. Aus diesem Grund sollten Sie sicherstellen, dass in dieser Datei keine falschen Einträge vorhanden sind. Ansonsten werden die hier gefundenen Informationen ohne weitere Überprüfung verwendet.

#### Hinweise

- ▷ Bei MS Windows befindet sich die Datei hosts im Verzeichnis %SystemRoot%\system32\drivers\etc.
- ▷ Bei Linux befindet sich die Datei hosts im Verzeichnis /etc.

Das **Fault Management** befasst sich hauptsächlich mit plötzlich auftretenden Störungen. Dabei kommt ein zentraler **Syslog-Server** zum Einsatz, der alle Meldungen analysiert, die von **verwalteten (managed) Netzwerkgeräten** generiert und übermittelt werden. Beim Auftreten bestimmter Ereignisse benachrichtigt dieser Server den Netzwerkadministrator via Mail oder über einen anderen Informationskanal. Mithilfe einer solch automatischen Benachrichtigung können bei einem Störfall Fehler rasch entdeckt und behoben werden, am besten noch, bevor die Benutzer etwas vom Fehler bemerken.

Für die Auswertung von Systemmeldungen und die Erkennung von Netzwerkstörungen kommen sogenannte **Network-Monitoring-Tools** oder **System-Monitore** zum Einsatz. Diese verschicken in regelmässigen Zeitabständen Anfragen an ein Netzwerkgerät, um zu prüfen, ob dieses Gerät noch antwortet. Dabei ist es möglich, für verschiedene Netzwerkdienste spezifische Anfragen zu senden. Antwortet ein Netzwerkgerät nicht innerhalb des definierten Zeitraums, wird der Netzwerkadministrator via E-Mail oder über einen anderen Informationskanal davon in Kenntnis gesetzt.

Neben technischen Hilfsmitteln sind auch **organisatorische Massnahmen** erforderlich, um Netzwerkstörungen möglichst rasch zu beheben. Dazu gehören etwa:

- Eindeutige Verantwortlichkeiten und Kompetenzen des Netzwerkadministrators.
- Klärung der Unterstützung bei grösseren Problemen oder im Notfall: Wer muss informiert werden und wie bzw. von wem kann Unterstützung angefordert werden? Eventuell muss ein Wartungsvertrag abgeschlossen werden.
- Anschaffung von Ersatzgeräten und -materialien: Wichtige, aber anfällige oder schwer zu beschaffende Komponenten sollten vorkonfiguriert bereitgehalten werden.

Die **Eingrenzung und Behebung von Netzwerkfehlern** hängt von diesen Faktoren ab:

- **Klare Vorgehensstrategie**
  - Mittels gezielter Fragen den Untersuchungsbereich ein- bzw. abgrenzen
  - Fehlersymptome mögliche Fehlerursachen gegenüberstellen
  - Naheliegende Lösungsschritte zuerst durchführen
- **Einsatz geeigneter Tools**
  - Einsatz einfacher, leicht bedienbarer Tools, z. B. die «Bordmittel» eines Systems
  - Kenntnis über die Wirkung der eingesetzten Tools, sprich Erfahrung in der Fehlerbehebung

## Repetitionsfragen

- 
- 2 Im Fault Management sowie im Performance Management geht es hauptsächlich um die Beseitigung bzw. Vermeidung bestimmter Fehlersituationen. Doch worin besteht der Unterschied zwischen diesen beiden Aufgabenbereichen?
- 
- 20 Ping-Anfragen (ICMP, Echo-Requests) eignen sich gut zur Überprüfung der Verfügbarkeit eines Netzwerkgeräts. Dennoch liefern solche Anfragen bei der Überprüfung z. B. eines Mailservers nicht immer zuverlässige Rückmeldungen.
- A] Weshalb ist eine Ping-Anfrage nicht immer die zuverlässigste Methode, die Verfügbarkeit eines bestimmten Systems bzw. Diensts wie z. B. Webserver oder Mailserver zu überprüfen?
- B] Wie kann die Überprüfung z. B. eines Mailservers zuverlässiger durchgeführt werden als «nur» mit einer Ping-Abfrage?
- 
- 5 Welcher IP-Adressbereich ist für APIPA-Adressen reserviert und welche Rückschlüsse können Sie daraus ziehen, wenn einem System eine APIPA-Adresse zugewiesen wurde?
- 
- 18 Nennen Sie zwei organisatorische Massnahmen, die sicherstellen sollen, dass trotz dem Defekt eines Netzwerkgeräts der normale Betrieb in einem Unternehmen möglichst schnell wiederhergestellt wird.
- 
- 31 Nennen Sie zwei mögliche Ursachen, weshalb sich die IP-Adresse eines Hosts via DNS nicht auflösen lässt bzw. eine ungültige IP-Adresse zurückgegeben wird.
- 
- 15 Welche Vorteile hat die Verwendung eines Syslog-Servers?



## **Teil B Netzwerk funktionssicher betreiben**

---

## Einleitung, Lernziele und Schlüsselbegriffe

### Einleitung

Neue Technologien und Betriebsformen der IT wie z. B. Systemvirtualisierung, Speicher-konsolidierung, Cloud Computing oder Unified Communication and Collaboration (UCC) haben das Datenvolumen in den Netzwerken weiter anwachsen lassen. Diese Entwicklung erhöht nochmals die Anforderungen an die Leistungsfähigkeit, die Sicherheit und die Zuverlässigkeit dieser Netze.

Anders als im Fault Management, wo es um Probleme geht, die Netzwerke zum völligen Stillstand bringen können, befasst sich das **Performance Management** mit Netzwerkproblemen, die sich nicht immer eindeutig erkennen lassen. Mit diesen oft diffusen Problemstellungen und deren Behebung befasst sich dieser Teil des Lehrmittels. Zu Beginn werden die Grundlagen des Performance Management näher vorgestellt. Danach wird anhand von Beispielen aus der Praxis aufgezeigt, welche Möglichkeiten zur Verfügung stehen, die Ursachen zu erkennen, die die Leistungsfähigkeit bzw. Performance eines Netzwerks negativ beeinflussen. Auch mögliche Massnahmen und Hilfsmittel werden vorgestellt, mit denen effizient gegen diese negativen Ursachen vorgegangen werden kann.

Neben der Leistung eines Netzwerks spielt auch die Sicherheit im Netzwerk eine grosse Rolle. Da i. d. R. alle IT-Systeme vernetzt sind, können sich die Auswirkungen von böswilligen Angriffen schnell auf weitere IT-Systeme ausbreiten. Im Kapitel **Sicherheitsmanagement** lernen Sie die wichtigsten operativen Sicherheitsvorkehrungen kennen.

### Lernziele und Lernschritte

Lernziele	Lernschritte
<input type="checkbox"/> Sie können mögliche Datenquellen (Netzwerkkomponenten und angeschlossene Endsysteme) für die Überwachung eines Netzwerks nennen und beschreiben.	<ul style="list-style-type: none"><li>• Performance Management</li></ul>
<input type="checkbox"/> Sie können geeignete Tools zur Überwachung von Netzwerken nennen und charakterisieren.	<ul style="list-style-type: none"><li>• Performance Management</li><li>• Sicherheitsmanagement</li></ul>
<input type="checkbox"/> Sie können die relevanten Parameter zur Auswertung der Performance und Verfügbarkeit nennen.	<ul style="list-style-type: none"><li>• Performance Management</li></ul>
<input type="checkbox"/> Sie können die wichtigsten Darstellungsarten für die erhobenen Daten unterscheiden und korrekt interpretieren.	<ul style="list-style-type: none"><li>• Performance Management</li></ul>
<input type="checkbox"/> Sie können die wichtigsten Indizien / Symptome erläutern, die auf Störungen hinsichtlich der Verfügbarkeit und Performance hinweisen.	<ul style="list-style-type: none"><li>• Performance Management</li><li>• Sicherheitsmanagement</li></ul>
<input type="checkbox"/> Sie können die Möglichkeiten zur physikalischen und logischen Gliederung eines Netzwerks und ihre Auswirkungen auf die Performance und Verfügbarkeit erläutern.	<ul style="list-style-type: none"><li>• Performance Management</li></ul>
<input type="checkbox"/> Sie können VLAN-Typen unterscheiden und typische Konfigurationen der Geräte nennen.	<ul style="list-style-type: none"><li>• Performance Management</li></ul>
<input type="checkbox"/> Sie können Methoden aufzeigen, um Störungen systematisch zu ermitteln und zu beheben.	<ul style="list-style-type: none"><li>• Sicherheitsmanagement</li></ul>

## Schlüsselbegriffe

---

Servicequalität, QoS-Parameter, SNMP-Agent, SNMP-Manager, SNMP-Protokoll, Management Information Base, Portstatistik, NetFlow-Messung, Bandbreitenprobleme, Übertragungsprobleme, Segmentierung, Tagging, Netzwerkkarte, CoS/ToS-Bits, Netzwerksicherheit, Schutzziele, Firewall, trusted / untrusted Network, Verarbeitungslinien, DOS-Attacke, Datenfilterung, Stateful Packet Inspection, Application Layer Firewall, Authentifizierung, DMZ, IPS, IDS, MITM-Attacke

## 4 Performance Management

---

Eine schlechte Netzwerkperformance wird von Benutzerseite meist als ein «langsam»es Netzwerk bemängelt. Obwohl bei einer solchen Reklamation meist klar ist, was den Benutzer stört, ist es für einen Netzwerkadministrator genauso unklar, zu erkennen, was ein Benutzer als «langsam» einstuft. Dauert etwa das Herunterladen einer Datei wirklich zu lange oder ist die Antwortzeit von drei Sekunden beim Laden einer Website aus dem Internet wirklich unzumutbar? Um in solchen Problemsituationen gezielt und nachhaltig helfen zu können, muss man die notwendigen Voraussetzungen und Aufgaben für ein **operatives Performance Management** kennen.

### 4.1 Voraussetzungen für ein effizientes Performance Management

---

Um bestimmen zu können, ob bei einem Problem überhaupt Handlungsbedarf besteht, muss vorgängig bekannt sein, was ein Netzwerk generell leisten muss. Bei dieser Frage geht es nicht darum, Störungsmeldungen von Benutzer-/Kundenseite abzuwimmeln. Es geht vielmehr darum, zu verstehen, ob die vereinbarte **Servicequalität** wirklich die Anforderungen der Benutzer erfüllt. Eine solche Vereinbarung nennt man SLA<sup>[1]</sup>. Ein **SLA** regelt üblicherweise folgende Aspekte des Netzwerkbetriebs:

- **Verfügbarkeit des Netzwerks:** Hier wird definiert, zu welchen Zeiten das Netzwerk den Benutzern zur Verfügung steht. Hierbei sollte man zwei Zeitspannen unterscheiden. Zuerst die Zeitspanne, in der das Netzwerk den Benutzern quasi uneingeschränkt zur Verfügung steht, die genannten «business hours». Danach sollte auch die Zeitspanne bekannt sein, in der das Netzwerk auch für Wartungsarbeiten der IT-Abteilung wie z. B. Backup-Jobs o. Ä. zur Verfügung steht. Diese zweite Zeitspanne wird auch «off business hours» genannt.
- **Ansprechpersonen/-stellen:** Hier wird definiert, an wen sich ein Benutzer bei Fragen oder im Falle einer Störung im Netzwerk wenden kann / muss sowie wann und wie diese Stellen erreichbar sind.
- **Lösungszeiten im Störungsfall:** Hier wird definiert, wie lange es dauern darf, bis eine bestimmte Störung behoben wird. Oft werden deshalb Störungen einer bestimmten Kategorie zugeordnet, die einer bestimmten Priorität entspricht. Unterschiedliche Prioritätsklassen erhalten meist unterschiedliche Lösungszeiten zugewiesen. In der Regel gilt: Je höher die Priorität, desto schneller muss das Problem gelöst werden.

#### 4.1.1 Netzqualität festlegen und messen

---

Die in einem Netzwerk-SLA definierten Anforderungen sind meistens zu allgemein gefasst, um Netzdienste anhand dieser Vorgaben beurteilen zu können. Doch mithilfe der **QoS<sup>[2]</sup>-Parameter** lassen sich diese Anforderungen genau beschreiben und auch messen. Folgende QoS-Parameter sind in IP-Netzwerken gebräuchlich:

[1] Abkürzung für: Service Level Agreement. Englisch für: Dienstleistungsvereinbarung.

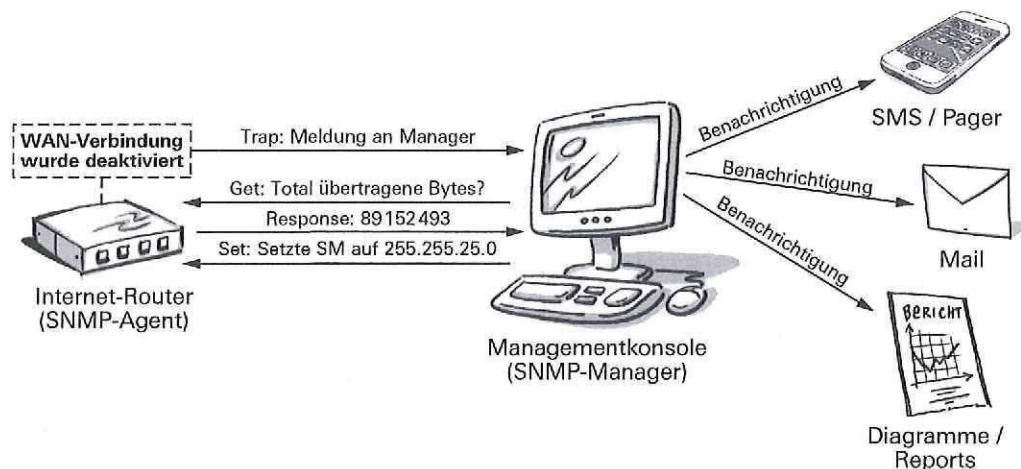
[2] Abkürzung für: Quality of Service. Englisch für: Güte eines Kommunikationsdiensts in Bezug auf die zu erfüllenden Anforderungen.

- **Latenzzeit:** Zeitdauer (Verzögerung in Millisekunden, ms), die ein Datenpaket für die Übertragung vom Sender zum Empfänger benötigt. Wird dabei der Weg des Datenpaketes vom Empfänger zurück zum Sender ebenfalls gemessen, spricht man von der «Round Trip Time» (RTT) eines Datenpaketes.
- **Datendurchsatz:** durchschnittlich pro Zeiteinheit übertragene Datenmenge (Kilo-, Mega- oder Gigabit/Sekunde, Kbps, Mbit/s oder Gbps).
- **Paketverlustrate:** maximale Anzahl von Paketen, die während einer Übertragung verloren gehen dürfen (z. B. 10 von 10<sup>-6</sup> bedeutet, max. 10 Pakete gehen bei 1 Million übertragener Pakete verloren).
- **Jitter:** Abweichung der Latenzzeit von ihrem Mittelwert (in Millisekunden, ms).

## 4.2 Leistungsdaten mittels SNMP erheben

«Managed» Netzwerkgeräte sammeln laufend Leistungsdaten, die für das Performance Management benötigt werden. Auf einem Netzwerkgerät arbeitet ein sogenannter **SNMP-Agent**, ein kleines Programm, das laufend die Daten und Status der verschiedenen internen Komponenten wie z. B. Netzwerkports, CPU, RAM etc. abfragt und lokal speichert. Der lokale Speicherplatz eines SNMP-Agent ist i. d. R. sehr begrenzt. Wenn kein Speicherplatz mehr vorhanden ist, werden die am längsten gespeicherten Daten durch die neuesten Daten ersetzt. Diese Art der Speicherverwaltung funktioniert nach dem **FIFO<sup>[1]</sup>-Prinzip**. Damit keine Daten verloren gehen, ruft die Managementkonsole in festgelegten Zeitintervallen die Daten auf dem SNMP-Agent ab und speichert diese zentral auf der Managementkonsole, dem **SNMP-Manager**. Dieser kann den Netzwerkadministrator bei definierten Ereignissen automatisch benachrichtigen und ist in der Lage, die Daten der überwachten Netzwerkgeräte in Statistiken und Berichte aufzubereiten.

[4-1] Kommunikationsflüsse beim SNMP-Management



[1] Abkürzung für: «First in, first out». Wird auch FCFS-Prinzip genannt (Abk. für: «First come, first served»).

#### 4.2.1 SNMP-Protokoll

Im Jahr 1990 wurde unter der Bezeichnung «SNMPv1» (RFC 1157) dieses Managementprotokoll erstmals standardisiert. Die aktuelle Version SNMPv3 stammt aus dem Jahr 2002 (RFC 3418). SNMP wird nicht ohne Grund **Simple Network Management Protocol** genannt. Die Kommunikation zwischen den Agents und der Managementkonsole ist sehr einfach gehalten. **SNMP** kennt lediglich sechs verschiedene Nachrichtentypen, die zwischen einem Agent und der Managementkonsole ausgetauscht werden können:

Nachrichtentyp	Aktion
<b>get</b>	Abfrage eines bestimmten Datensatzes
<b>getnext</b>	Abfragen des nächsten Datensatzes
<b>getbulk</b>	Abfragen mehrerer Datensätze / Tabellen
<b>response</b>	Antwort auf eine vorangegangene Abfrage
<b>set</b>	Änderung eines Datensatzes (ermöglicht Konfigurationsänderungen)
<b>trap</b>	Direkte, unaufgeforderte Nachricht vom Agent an den Manager. Wird bei einem bestimmten Ereignis ausgelöst, wenn diese Information ohne Zeitverzögerung an den Manager gelangen muss.

Alle Nachrichtentypen außer trap werden mittels UDP über Port 161 versendet. Traps werden mittels UDP über Port 162 verschickt.

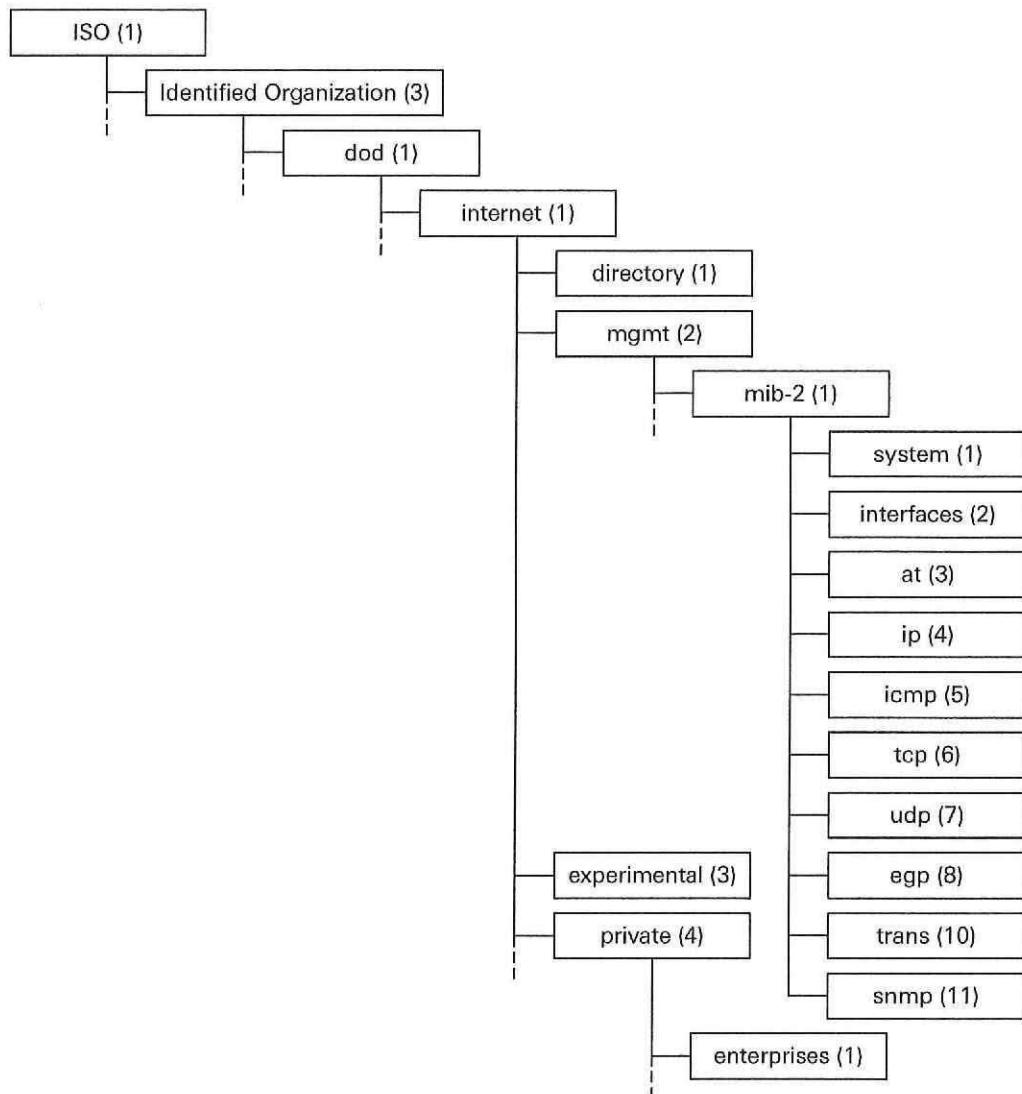
#### 4.2.2 Datenablage des SNMP-Agent

Der SNMP-Agent speichert die erfassten Daten in seiner **Management Information Base (MIB)**. In der MIB werden die Daten bzw. Informationen abgelegt werden, die der SNMP-Agent des Netzwerkgeräts laufend abruft. Die MIB wird meistens vom Hersteller des Netzwerkgeräts zur Verfügung gestellt. Deshalb ist eine MIB i. d. R. produktspezifisch. Es gibt aber auch offizielle MIBs für Netzwerkgeräte, die Standardattribute enthalten. Die einzelnen Datensätze in einer MIB werden mittels der entsprechenden **OID (Object Identifier)** angesprochen. Die OID ist die genaue Speicheradresse oder der genaue Pfad, wo eine spezifische Information (Attribut) innerhalb der MIB abgelegt ist. Anbei einige Beispiele von häufig abgerufenen OIDs:

Gewünschte Information	OID innerhalb der MIB-Struktur
<b>Hostname</b> (Gerätename oder Systembeschreibung)	.1.3.6.1.2.1.1.1.0
<b>SysUpTime</b> (Gesamtaufzeit des Systems)	.1.3.6.1.2.1.1.3.0
<b>Status Eth0</b> (Status der 1. Netzwerkschnittstelle)	.1.3.6.1.2.1.2.2.1.2.2.1.7.1

Die **Struktur der MIB** ist baumartig aufgebaut. Die MIB eines Netzwerkgeräts enthält normalerweise nicht die gesamte MIB-Baumstruktur, sondern nur diejenigen «Zweige» (engl. Branches) bzw. Informationen, die ein Gerät zur Verfügung stellen kann. Folgende Abbildung zeigt die Struktur einer solchen MIB (v2):

## [4-2] MIB-Baumstruktur (Teilansicht)



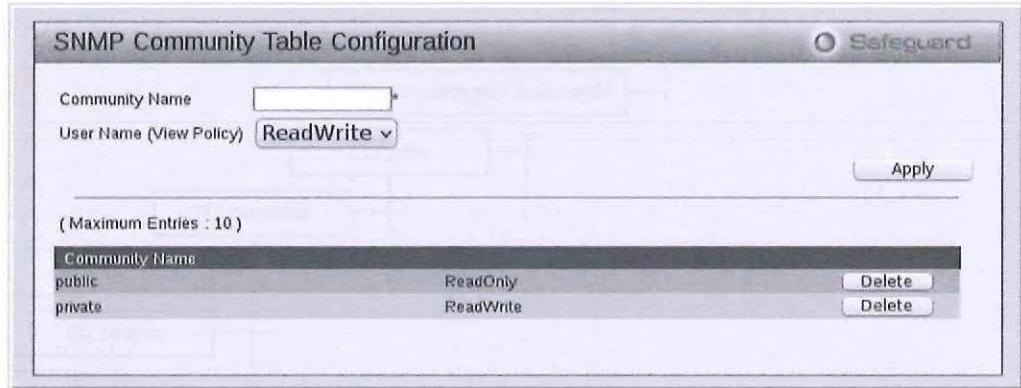
## 4.2.3 SNMP-Agent konfigurieren

Bei der **Konfiguration des SNMP-Agent** eines Netzwerkeräts gilt es einiges zu beachten. Besonderes Augenmerk sollte man vor allem auf die **Sicherheitseinstellungen** legen. SNMP kennt folgende Möglichkeiten hinsichtlich Sicherheit:

**SNMPv1**

Steuert den primären Zugriff auf einen SNMP-Agent über sogenannte Community Names oder Community Strings. Der **Community Name / String** ist eine normale Textbezeichnung und wird bei jeder Abfrage mitgesendet. Nur wenn der Community Name / String korrekt ist, kann auf den entsprechenden Agent zugegriffen werden. Dieser primäre Zugriff kann zusätzlich durch die Zuweisung des Access Mode weiter eingeschränkt werden. Der **Access Mode** kontrolliert, ob der Zugriff mit Lese- oder Schreibrechten geschieht. Generell stehen zwei Access Modes zur Verfügung, der **ReadOnly Mode** und der **ReadWrite Mode**. Im **ReadOnly Mode** hat der **set**-Befehl keine Wirkung. Per Default wird die «public»-Community auf **ReadOnly** gesetzt, die «private»-Community dagegen auf **ReadWrite**. Da alle Abfragen und Daten im Klartext über das Netzwerk versendet werden, bieten diese Sicherheitsoptionen keinen Schutz für den Agent und seine Daten.

[4-3] Zugriffssteuerung mittels Community Names (Switch D-Link DGS-1210)



**Hinweis**

- ▷ Jeder, der den Community Name «public» oder «private» kennt, kann mit einem entsprechenden Tool (z. B. MIB-Browser) auf den SNMP-Agent zugreifen. Ob SNMP auf einem Netzwerkgerät aktiviert ist, können Sie einfach mithilfe eines Portscanners (z. B. nmap) feststellen. Mittels Zugriff auf die «private»-Community könnte ein Angreifer sogar Änderungen an der Konfiguration vornehmen.

[4-4] Zugriffssteuerung mittels «View-Tabellen» (Switch Cisco SG 300-28P)

SNMP Management Station	Community Type	Community String	Access Mode	View Name
192.168.2.253	Basic	switch-1-chur	Read Only	Default

Object ID Subtree	Object ID Subtree View
1	Included
1.3.6.1.6.3.13	Excluded
1.3.6.1.6.3.16	Included
1.3.6.1.6.3.18	Excluded
1.3.6.1.6.3.12.1.2	Excluded
1.3.6.1.6.3.12.1.3	Excluded
1.3.6.1.6.3.15.1.2	Included

Einige SNMP-Agents verfügen über die Möglichkeit, den Zugriff nur auf bestimmte OIDs zu gestatten (include) bzw. diesen exizit zu verweigern (exclude). Im obigen Beispiel wird dies mit der Funktion «View Table» realisiert.

### SNMPv2c

Mit dieser Version wurde die Zugriffssteuerung anhand der Community Names mit der Möglichkeit ergänzt, Benutzerkonten auf dem Agent zu erstellen. Es lassen sich neu **lokale Benutzer** definieren und diesen Lese- (ReadOnly) oder Schreibrechte (ReadWrite) auf eine Community zuteilen. Das Setzen eines Passworts ist in dieser Version nicht möglich. Daneben wurden unter **SNMPv2c** auch einige Änderungen bei den SNMP-Befehlen vorgenommen. So wurde z. B. der getbulk-Befehl neu zum Protokoll hinzugefügt. Da die Kommunikation noch immer unverschlüsselt abläuft, gilt auch SNMPv2c als unsicher.

[4-5] Zugriffssteuerung unter SNMPv2c (Switch D-Link DGS-1210)

User Name	Group Name	SNMP Version	Auth Protocol	Priv Protocol	
ReadOnly	ReadOnly	v2c	None	None	<input type="button" value="Delete"/>
ReadWrite	ReadWrite	v2c	None	None	<input type="button" value="Delete"/>
snmpadmin	ReadWrite	v2c	None	None	<input type="button" value="Delete"/>

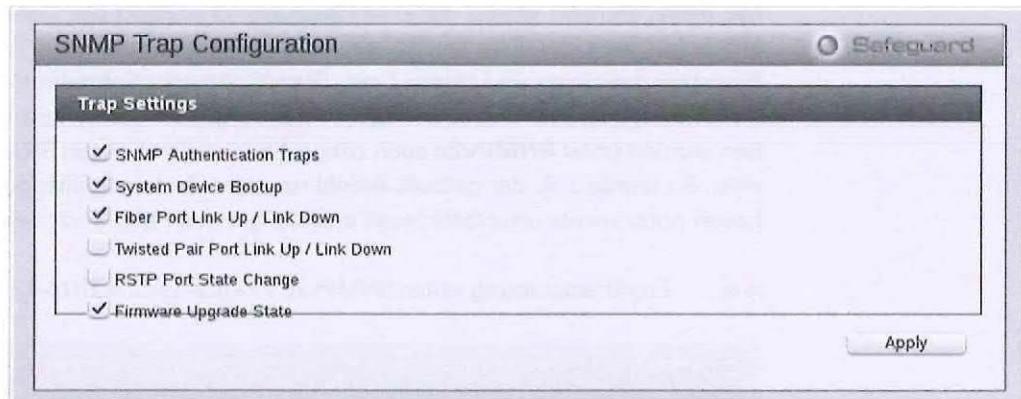
### SNMPv3

Erst mit dieser Version wurde der Sicherheit etwas mehr Aufmerksamkeit geschenkt. Zusätzlich kann nun dem Benutzer auch ein **Passwort** zugewiesen werden, das verschlüsselt auf dem Agent abgelegt werden kann. Dies ermöglicht nun eine bessere Authentifizierung des Zugriffs auf den Agent. Auch wurden die **Zugriffsberechtigungen** mittels spezieller **Gruppenrechte** etwas erweitert. Mit diesen Änderungen erfüllt SNMPv3 zumindest minimale Anforderungen hinsichtlich der IT-Sicherheit.

[4-6] Zugriffssteuerung unter SNMPv3 (Switch D-Link DGS-1210)

User Name	Group Name	SNMP Version	Auth Protocol	Priv Protocol	
snmpadmin	ReadWrite	v3	MD5	DES_CBC	<input type="button" value="Delete"/>

## [4-7] Konfiguration von Trap-Events (Switch D-Link DGS-1210)

**Hinweis**

▷ Man tut gut daran, sich genau zu überlegen, welche Ereignisse automatisch einen «Trap» auslösen sollen. Nicht jedes Ereignis ist wirklich von Bedeutung. Normalerweise sind es sicherheitsrelevante Ereignisse wie z.B. der Restart eines Netzwerkgeräts, die Versionsänderung einer Firmware oder der Ausfall einer wichtigen Komponente / Funktion, die dem Netzwerkadministrator möglichst rasch gemeldet werden sollten.

**Abfrage einiger gebräuchlicher OIDs auf dem Kommandoprompt mittels der SNMP-Tools unter Linux**

Abfrage der Systembeschreibung (Hostname)

```
snmpget -v1 -c public 192.168.2.253 .1.3.6.1.2.1.1.1.0
SNMPv2-MIB::sysDescr.0 = STRING: DGS-1210-24      2.02.002
```

Abfrage nach der SysUpTime

```
snmpget -v1 -c public 192.168.2.253 .1.3.6.1.2.1.1.3.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (409518593) 47 days, 9:33:05.93
```

Abfrage nach dem Status der 1. Ethernet-Schnittstelle

```
snmpget -v1 -c public 192.168.2.253 .1.3.6.1.2.1.2.2.1.7.1
IF-MIB::ifAdminStatus.1 = INTEGER: up(1)
```

**4.3 Messwerte darstellen und auswerten**

Dank SNMP können kontinuierlich Informationen über den Zustand und die Leistung eines Netzwerkgeräts abgefragt werden. Diese Informationen sollten so aufbereitet sein, dass diese möglichst einfach dem Betrachter einen Anhaltspunkt geben, wo allenfalls ein Problem vorhanden ist. Die **Portstatistik eines Netzwerkswitches** gibt zwar exakt die aktuellen Werte wieder, ist aber (bei einer Darstellung wie im nachstehenden «Zahlenfriedhof») bei der Problemsuche kaum von grossem Nutzen.

## [4-8] Portstatistik eines Netzwerkswitches (Beispielansicht)

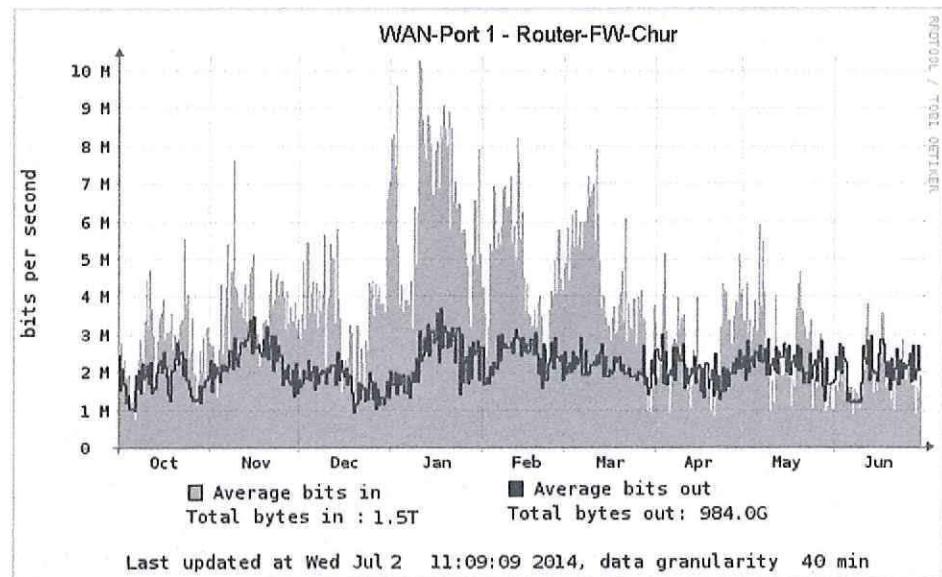
## Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	160055167	103493327	198367956793	36041375596	26	0	36280	0	2
2	364367	356778	340568967	246023218	0	0	0	0	16
3	834803	1744654	201462712	908779873	0	0	0	0	155
4	27321305	55737209	5685864244	66179606494	2	0	0	0	191
5	18640602	31581916	6267953979	29037319053	0	0	0	0	667
6	0	0	0	0	0	0	0	0	0
7	8732762	16429363	4290774368	14116026228	0	0	45	0	206
8	7115918	15992880	1846108686	14263900531	0	0	0	0	83
9	0	0	0	0	0	0	0	0	0
10	3888679	3949813	3100085915	4261418975	0	0	43	0	655
11	9350184	20055180	2429915514	20374515357	0	0	9	0	75
12	3967143	11154396	759350518	6562477136	0	0	0	0	167
13	20772213	39851320	10869163599	45629749497	8	0	69	0	64
14	115908	153993	88541388	92757822	0	0	0	0	80
15	0	0	0	0	0	0	0	0	0

## 4.3.1 Messwerte darstellen

Unterschiedliche Informationsbedürfnisse erfordern oft unterschiedliche **Darstellungsarten von Messwerten**. Nachfolgend werden einige Darstellungsarten vorgestellt, mit denen bestimmte Sachverhalte aussagekräftig dargestellt werden können. Die grafische Darstellung ist sicher die am häufigsten verwendete Methode, um Messwerte aussagekräftig darzustellen bzw. zu visualisieren. Eine geeignete Darstellungsart ist ein sogenanntes **Histogramm**. Ein Histogramm ist i. d. R. ein Koordinatensystem mit zwei Achsen, der x- und der y-Achse. Ein Histogramm eignet sich besonders zur Visualisierung von Messwerten über einen längeren Zeitraum (Zeitreihen).

## [4-9] Histogramm der Auslastung einer Verbindungsleitung (Beispiel)



Beim Performance Management benötigen Sie ggf. genauere Informationen darüber, welches System welchen Anteil an einer Netzwerkressource «konsumiert» hat. Normalerweise wird diese Information mithilfe eines **Kuchendiagramms**<sup>[1]</sup> dargestellt. Für unsere Zwecke eignet sich ein **Balkendiagramm** aber besser, da sich mithilfe von absteigenden

[1] Englisch: Pie Chart.

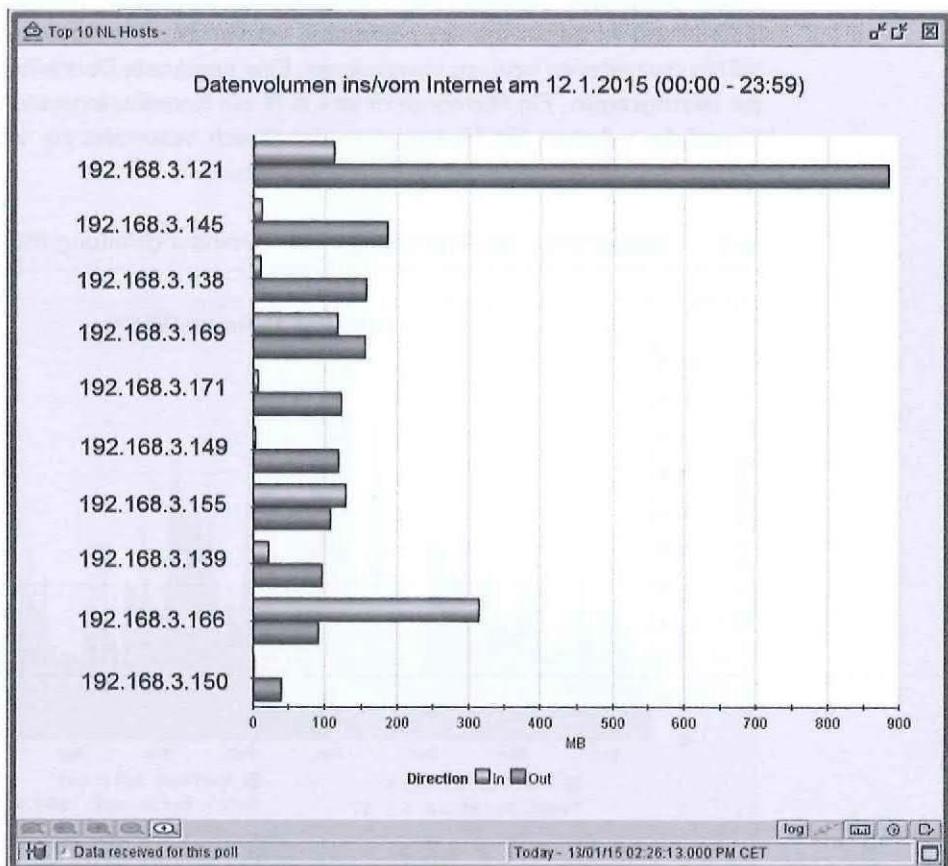
Balken bzw. Werten eine Art von Rangliste<sup>[1]</sup> darstellen lässt. Diese Form der Darstellung wird im Performance Management häufig angewendet und «Top-Talker-Liste» genannt. Damit sieht man auf einen Blick, welches System welchen Anteil am Gesamtverbrauch einer Netzwerkressource hat. Im Folgenden sehen Sie zwei verschiedene Möglichkeiten für die Aufbereitung solcher Informationen:

[4-10] Top-Talker-Informationen (Darstellungsbeispiel 1)

Adresse IP	Port	Trafic	Ratio global	Ratio
192.168.2.0/24		895.93M	100%	
192.168.2.240	tcp/8080	352.40M	41.24%	
192.168.2.217	tcp/8080	150.16M	17.57%	
192.168.2.213	tcp/8080	66.43M	7.78%	
192.168.2.157	tcp/8080	43.52M	5.09%	
192.168.2.248	tcp/39058	29.74M	3.48%	
192.168.2.153	tcp/39058	29.74M	3.48%	
192.168.2.152	tcp/8080	27.17M	3.18%	
192.168.2.158	tcp/55161	16.03M	1.88%	
192.168.2.210	tcp/55161	16.03M	1.88%	
192.168.2.201	tcp/8080	16.01M	1.87%	
192.168.2.245	tcp/443	12.01M	1.41%	
192.168.2.151	tcp/35292	9.84M	1.15%	
192.168.2.217	tcp/35292	9.84M	1.15%	
192.168.2.249	tcp/39062	9.82M	1.15%	
192.168.2.150	tcp/39062	9.82M	1.15%	
192.168.2.245	tcp/143	8.52M	1.00%	
192.168.2.247	tcp/35291	3.08M	0.66%	

"Rangliste"

[4-11] Top-Talker-Informationen (Darstellungsbeispiel 2)



[1] Englisch: Ranking.

### 4.3.2 Aussagekraft der Netzwerkinformationen erhöhen

Die oben vorgestellten Darstellungsarten haben einen entscheidenden Nachteil. Die Beantwortung der Fragen «Wann war die Leitung komplett ausgelastet?» und «Wer hat den Traffic bzw. Netzwerkverkehr generiert?» setzt zwei getrennte Messungen voraus und die Messresultate werden auch getrennt dargestellt. Es wird also etwas getrennt, was in Wirklichkeit zusammengehört. Um aussagekräftigere Messresultate zu erhalten, benötigen wir Netzwerkgeräte, die neben SNMP auch **NetFlow** und / oder **sFlow** unterstützen.

Wie reicht SNMP nicht aus? Der Datenverkehr in einem Netzwerk ist mit einem Fluss (Flow) vergleichbar. Alle übertragenen Daten haben einen bestimmten Ursprung (Quelle) und werden an ein bestimmtes Ziel (Senke) gesendet. Systeme bzw. Applikationen schicken diese Daten zu einer bestimmten Zeit auf die Reise. NetFlow und sFlow machen es möglich, diese Informationen aus einem Datenstrom herauszufiltern und sich ein genaueres Bild über die Vorgänge bzw. **Datenströme in einem Netzwerk** zu machen. In der folgenden Tabelle werden wichtige Eigenschaften von NetFlow und sFlow zusammengefasst:

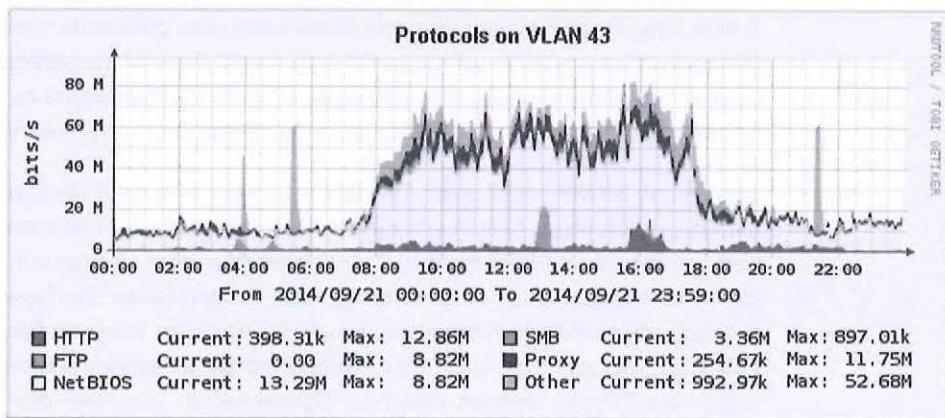
Merkmale	NetFlow	sFlow
<b>Entwicklung / Version</b>	Ursprünglich von der Firma Cisco entwickelt, mittlerweile unter RFC 3954. Aktuelle Version 9, wobei Version 5 am häufigsten eingesetzt wird.	Wurde ursprünglich in einer Zusammenarbeit der Firma HP und der Universität Genf entwickelt, mittlerweile unter RFC 3176. Aktuelle Version 5.
<b>Informationen</b>	Kann u. a. folgende Informationen erheben: <ul style="list-style-type: none"> <li>• Zeitstempel</li> <li>• Byte- und Paketzähler (Counter)</li> <li>• IP: Quell- und Ziel-Adressen (IPv6 nur mit V.9)</li> <li>• IP: Quell- und Ziel-Ports</li> <li>• ToS-Informationen</li> <li>• TCP-Flags</li> <li>• Protokolltypen (ICMP, TCP und UDP)</li> </ul>	Kann u. a. folgende Informationen erheben: <ul style="list-style-type: none"> <li>• Zeitstempel</li> <li>• Ethernet (Framesize/-count, VLAN, 802.1Q)</li> <li>• Byte- und Paketzähler (Counter)</li> <li>• IP: Quell- und Ziel-Adressen (IPv4/v6)</li> <li>• IP: Quell- und Ziel-Ports</li> <li>• ToS<sup>[1]</sup>-Informationen</li> <li>• TCP-Flags</li> <li>• Protokolltypen (ICMP, TCP und UDP)</li> </ul>
<b>Vor- und Nachteile</b>	NetFlow-Funktionen sind SW-Erweiterungen und müssen daher vom Betriebssystem unterstützt werden. Die Performance von NetFlow ist stark abhängig vom eingesetzten Netzwerkgerät. Das Betriebssystem IOS der Firma Cisco unterstützt primär NetFlow. Bestimmte Cisco-Gerätemodelle unterstützen auch sFlow.	sFlow ist in der Lage, auch Layer-2-Informationen zu erheben. Die sFlow-Funktionen werden i. d. R. in einer eigenen CPU (ASIC <sup>[2]</sup> ) ausgeführt. Somit wird die eigentliche CPU des Netzwerkgeräts von dieser Aufgabe entlastet, was sich vorteilhaft auf die Gesamtleistung des Netzwerkgeräts auswirkt.

[1] Abkürzung für: Type of Service. 8-Bit-Feld im IP-Header. Dient zur Prioritätsangabe (Markierung) des IP-Pakets.

[2] Abkürzung für: Application Specific Integrated Circuit. CPU, die nur für eine bestimmte Funktion / Applikation verwendet wird.

Nachfolgend sehen Sie die Resultate einer **NetFlow-Messung** während 24 Stunden:

[4-12] Ergebnisse einer Messung mit NetFlow (Beispiel)



Der Vorteil gegenüber einer SNMP-Messung besteht darin, dass bei der Ermittlung und Darstellung des kumulierten Datenvolumens verschiedene Protokolle berücksichtigt werden können. Ohne NetFlow bzw. sFlow wären dafür mehrere getrennte Messungen und Auswertungen nötig.

Für die Durchführung von **NetFlow- bzw. sFlow-Messungen** werden folgende **Komponenten** vorausgesetzt:

- **NetFlow / sFlow Exporter:** Netzwerkgerät (Router, Switch, Server etc.), das NetFlow bzw. sFlow unterstützt. Weitere Infos dazu finden Sie unter: [sflow.org/products/network.php](http://sflow.org/products/network.php).
- **NetFlow / sFlow Collector:** System (meist eine SW-Applikation), das die Messdaten empfängt, speichert und visualisiert. Eine verbreitete Open-Source-Lösung heißt NfSen. Weitere Infos dazu finden Sie unter: [sflow.org/products/collectors.php](http://sflow.org/products/collectors.php).

#### Hinweis

- ▷ NetFlow / sFlow wird noch nicht von allen «managed» Netzwerkgeräten unterstützt.

Für die Visualisierung der mittels SNMP oder NetFlow / sFlow erfassten Messwerte eignen sich folgende **Open-Source-Programme**:

- **Cacti:** häufig eingesetzte Anwendung für Linux und MS Windows, Infos und Download unter: [cacti.net](http://cacti.net)
- **ntop:** Netzwerk-Monitoring-Lösung für Linux, MS Windows und Mac OS X, erlaubt umfangreiche Auswertungen und Darstellungen der Messdaten. Infos und Download unter: [ntop.org](http://ntop.org)

## 4.4 Performanceprobleme lokalisieren

Probleme hinsichtlich der Netzwerkperformance lassen sich einfach feststellen, da die Symptome meist klar in Erscheinung treten. Wer hat es nicht schon selber bemerkt und sich ggf. auch darüber beschwert, wenn das Netzwerk (wieder mal) langsam arbeitet. Dies kann ein erster Hinweis auf ein tatsächliches Performanceproblem sein. Doch das Lokalisieren und Beheben der Ursachen eines Performanceproblems ist oft alles andere als einfach. Nachfolgend erhalten Sie einige Anhaltspunkte, weshalb es in einem Netzwerk zu Performanceproblemen kommen kann.

#### 4.4.1 Häufige Ursachen für Performanceprobleme

Performanceprobleme in Netzwerken lassen sich meist auf folgende **Ursachen** zurückführen:

Problem	Symptome	Mögliche Ursachen
<b>Fehlende Bandbreite</b>	<ul style="list-style-type: none"> <li>• Lange Antwortzeiten einer Applikation</li> <li>• Fehlermeldung von der betroffenen Applikation infolge Verbindungsabbruch (Session Timeout / Termination)</li> </ul>	<ul style="list-style-type: none"> <li>• Ständig mehr Datenvolumen als Übertragungskapazität vorhanden (exhausted line capacity)</li> <li>• Zeitweise mehr Datenvolumen als Übertragungskapazität vorhanden (bulky traffic)</li> </ul>
<b>Viele Übertragungsfehler</b>	<ul style="list-style-type: none"> <li>• Lange Antwortzeiten einer Applikation</li> <li>• Fehlermeldung von der betroffenen Applikation infolge Verbindungsabbruch (Session Timeout / Termination)</li> <li>• Zufällige, unkontrollierte Programmabstürze</li> </ul>	<ul style="list-style-type: none"> <li>• Unpassende Konfiguration des Übertragungsprotokolls, z. B. TCP-Options</li> <li>• Zu hohe Latenzen bei einer Netzkomponente im Übertragungspfad zwischen dem Sender und dem Empfänger</li> </ul>

#### 4.4.2 Bandbreitenprobleme erkennen

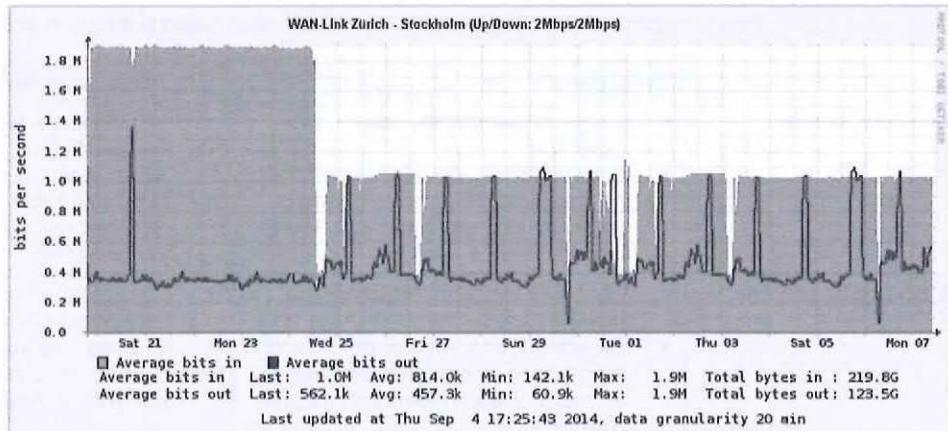
Das einzige Problem bezüglich der Bandbreite ist, dass unter Umständen zu wenig Bandbreite zur Verfügung steht. Zu viel Bandbreite bzw. eine unvollständig genutzte Bandbreite verursacht keine technischen Probleme, sondern hat höchstens finanzielle Auswirkungen.

Wie können Sie erkennen, ob die **Bandbreite einer Übertragungsstrecke** ausgelastet ist? Am besten anhand einer längeren Messung und grafischen Darstellung der übertragenen Datenvolumen. Eine solche Messreihe sollte Messwerte von mehreren Stunden bis einigen Tagen umfassen. Kurze Messungen von einer Stunde oder weniger bergen die Gefahr, dass lediglich eine «Momentaufnahme» vorliegt, die keine Hinweise für das weitere Vorgehen erlaubt.

##### Auslastung einer Netzwerkverbindung über mehrere Tage messen

Stellen Sie sich folgende Ausgangslage vor: Die Mitarbeitenden der Niederlassung in Stockholm melden, dass der Zugriff auf den Hauptsitz in Zürich seit Mittwoch, dem 25. August, extrem langsam ist. Dieser Zugriff war zwar schon früher langsam, aber jetzt ist fast kein Arbeiten mehr möglich. Als Netzwerkadministrator stellen Sie fest, dass die Bandbreite des WAN-Links normalerweise 2 Mbit/s beträgt. Seit dem 25. August beträgt der Maximaldurchsatz allerdings nur noch ca. 1 Mbit/s, also 50% weniger. Sie vermuten, dass ein Provider oder ein Router die Bandbreite auf maximal 1 Mbit/s reduziert. Zudem lässt sich bestätigen, dass diese Verbindung schon vorher extrem ausgelastet war. Die entsprechende grafische Auswertung sieht wie folgt aus:

[4-13] Auslastung des WAN-Links während 18 Tagen (Beispiel)



Die obigen Daten bzw. Informationen bezüglich der Auslastung lassen sich via SNMP vom WAN-Port des Routers abgreifen und mit einem geeigneten Visualisierungsprogramm (Cacti, ntop) darstellen. Sie zeigen, dass seit dem 25. August nur noch die Hälfte der üblichen Bandbreite von 2 Mbit/s zur Verfügung steht. Dass die Verbindung bereits vorher völlig ausgelastet war, ist zwar auch eine wichtige Information, erklärt aber die Reduktion der Bandbreite seit diesem Datum nicht. Der klare Schnitt der Bandbreite<sup>[1]</sup> an einem bestimmten Tag deutet auf eine gesteuerte bzw. kontrollierte Begrenzung des Datenverkehrs hin.

#### Maximale Bandbreite einer Datenverbindung ermitteln

Die **Bandbreite einer Internetverbindung** lässt sich relativ einfach ermitteln bzw. überprüfen, indem Sie einen **Online-Speedtest** wie z. B. [www.speedtest.net/de](http://www.speedtest.net/de) aufrufen. Wenn Sie die **Bandbreite einer LAN-Verbindung** ermitteln bzw. überprüfen möchten (z. B. die Verbindung zwischen Client-PC und Server im eigenen Netzwerk), brauchen Sie dafür ein spezielles Tool.

Mit dem Open-Source-Tool **Iperf** können beliebige Netzwerkverbindungen einem **Belastungstest** unterzogen werden. Um festzustellen, wie hoch die maximale Bandbreite ist, versucht dieses Tool, die betreffende Netzwerkverbindung vollständig auszulasten. Beachten Sie dabei folgende Punkte:

- Für einen **Iperf**-Test werden zwei Rechner benötigt; der eine fungiert als Client und der andere als Server. Während des Belastungstests ist die Verbindung zwischen Client und Server vollständig ausgelastet.
- **Iperf** kann Daten sowohl via UDP als auch via TCP übertragen. Weil im Netzwerk die Daten vornehmlich via TCP übertragen werden, empfiehlt es sich, den Belastungstest ebenfalls mittels TCP durchzuführen.
- **Iperf** läuft unter Linux, MS Windows und Mac OS X und kann von der Website [www.iperf.fr](http://www.iperf.fr) heruntergeladen werden.

Die Belastung der Netzwerkverbindung zwischen zwei Rechnern (über das Internet) kann mit diesem Tool wie folgt getestet werden.

#### 1. iperf-Server starten

[1] Englisch: Cut of Bandwidth.

Geben Sie folgenden Befehl ein:

```
[atmat@PC-1] > iperf -s -p 36773
-----
Server listening on TCP port 36773
TCP window size: 85.3 KByte (default)
```

## 2. iperf-Client starten

```
Geben Sie folgenden Befehl ein:
[user1@PC-2] > iperf -p 36773 -c 178.83.75.196 -t 30 -P 3
-----
Client connecting to 178.83.75.196, TCP port 36773
TCP window size: 19.3 KByte (default)
-----
[ 5] local 192.168.2.3 port 55865 connected with 178.83.75.196 port 36773
[ 4] local 192.168.2.3 port 55864 connected with 178.83.75.196 port 36773
[ 3] local 192.168.2.3 port 55863 connected with 178.83.75.196 port 36773
[ DJ] Interval      Transfer      Bandwidth
[ 4]   0.0-30.2 sec   17.0 MBytes   4.73 Mbits/sec
[ 5]   0.0-30.3 sec   18.9 MBytes   5.22 Mbits/sec
[ 3]   0.0-30.4 sec   18.8 MBytes   5.17 Mbits/sec
[SUM]   0.0-30.4 sec   54.6 MBytes   15.1 Mbits/sec
```

Im oben dargestellten Beispiel ergibt der Belastungstest eine durchschnittliche Bandbreite von 15.1 Mbit/s. Dabei wurden Daten im Umfang von 54.6 MBytes vom Client zum Server gesendet. Dieser Wert stellt deshalb die **Upload-Bandbreite** dar.

### Hinweis

- ▷ Auch hier gilt: Um genauere Informationen über die Bandbreite einer Verbindung zu erhalten, sollten Sie den Belastungstest zu unterschiedlichen Zeitpunkten wiederholen.

## 4.5 Massnahmen gegen Performanceprobleme

Zu wenig Bandbreite bzw. Übertragungskapazität kann sowohl bei Verbindungen in einem lokalen Netzwerk (LAN) als auch bei Verbindungen über öffentliche Netzwerke (WAN-Verbindungen, Internet) Probleme bereiten. Die einfachste Lösung wäre wohl eine **Erhöhung der Bandbreite**. Dies kann bei einer WAN-Verbindung aber recht teuer zu stehen kommen. Immer wieder wird auch die Erfahrung gemacht, dass eine erhöhte Bandbreite eine «flüchtige» Ressource ist, die innert kurzer Zeit wieder «aufgebraucht» wird. Mehr Bandbreite ohne flankierende Massnahmen ist daher weder zielführend noch nachhaltig.

Besser ist es, die vorhandene Übertragungskapazität im Rahmen eines **Bandbreitemanagements** proaktiv zu steuern und allen Diensten bzw. Applikationen genau diejenige Bandbreite zuzuweisen, die sie für den optimalen Betrieb benötigen. Während ausgefahrene oder defekte Netzwerkverbindungen im Rahmen des Fault Management behandelt werden, kümmert sich das Bandbreitemanagement also um Netzwerkverbindungen mit einer (sehr) hohen Auslastung, wobei das primäre Ziel in der Sicherstellung der **Quality of Services (QoS)** besteht. Nachfolgend erfahren Sie mehr über die Aufgaben eines so verstandenen Bandbreitemanagements.

#### 4.5.1 Datenströme analysieren und gruppieren

Hier geht es darum, die **Anforderungen verschiedener Datenströme (Flows)** zu identifizieren und **ähnliche Datenströme in Gruppen** zusammenzufassen. Der Ursprung eines Datenstroms liegt bei einer Applikation und jede Applikation hat spezifische Anforderungen an die Datenübertragung. Diese müssen gemeinsam mit den jeweiligen Benutzern und Verantwortlichen ermittelt bzw. definiert werden. Danach können ähnliche Anforderungen in Gruppen zusammengefasst werden. Jede Gruppe repräsentiert somit bestimmte Eigenschaften eines Datenstroms. Das Resultat einer solchen **Gruppierung** könnte z. B. so aussehen:

Gruppe	Beschreibung	Applikationen
<b>Businesskritisch</b> (keine Alternativen verfügbar)	<b>Höchste Priorität.</b> Fehler oder Unterbrechungen haben sofortige Auswirkungen auf viele Applikationen. Die Zahl betroffener Benutzer kann sehr hoch sein, im Extremfall die gesamte Belegschaft einer Firma.	<ul style="list-style-type: none"> <li>• Zugriffe auf zentrale Datenspeicher wie SAN/NAS</li> <li>• 7 x 24-Stunden-Applikationen wie z. B. Reservationssysteme, Produktionssteuerungen, Terminaldienste etc.</li> </ul>
<b>Zeitkritisch</b> (Alternativen nur begrenzt verfügbar)	<b>Hohe Priorität.</b> Fehler oder Unterbrechungen können Auswirkungen auf mehrere Applikationen haben. Die Zahl betroffener Benutzer kann hoch sein, im Extremfall ganze Abteilungen betreffen.	<ul style="list-style-type: none"> <li>• VoIP, Multimedia</li> <li>• Wertschriften- oder Devisenhandel</li> <li>• Intranet-Applikationen</li> </ul>
<b>Unkritisch</b> (Alternativen verfügbar oder unnötig)	<b>Mittlere Priorität.</b> Fehler oder Unterbrechungen haben kaum direkte negative Auswirkungen auf Applikationen. Nur einzelne Benutzer sind im Problemfall betroffen. Oft wird dieses Problem kaum wahrgenommen.	<ul style="list-style-type: none"> <li>• Druckaufträge</li> <li>• E-Mail-Versand/-Empfang</li> <li>• Zugang ins Internet</li> </ul>

Erläuterungen zur Tabelle:

- Mit «Alternativen» sind die verfügbaren Möglichkeiten gemeint, falls ein Datenstrom dieser Gruppe nicht übertragen werden kann.
- Mehr als vier Gruppen sind für die Charakterisierung von Datenströmen i. d. R. nicht sinnvoll, da die Unterscheidungsmerkmale ansonsten unklar bzw. zu gering werden. Für die meisten Unternehmen sind drei Gruppen völlig ausreichend.

#### 4.5.2 Datennetze segmentieren

In jedem Netzwerk werden neben den **Nutzdaten** auch **Verwaltungs- oder Dienstdaten** ausgetauscht. Diese können als «Overhead»<sup>[1]</sup> betrachtet werden, den die Systeme im Netzwerk benötigen, damit sie ordnungsgemäß am Netzwerkbetrieb teilnehmen können (z. B. ARP-Broadcasts, DNS-Queries, Updates von Routing- oder Bridgetabellen). Solange in einem Netzwerk kein grosser Datenverkehr herrscht, sind solche Dienstdaten unproblematisch. Bei einem hohen Datenaufkommen kann der «Overhead» aber dazu beitragen, dass es vermehrt zu **Übertragungsproblemen** kommt.

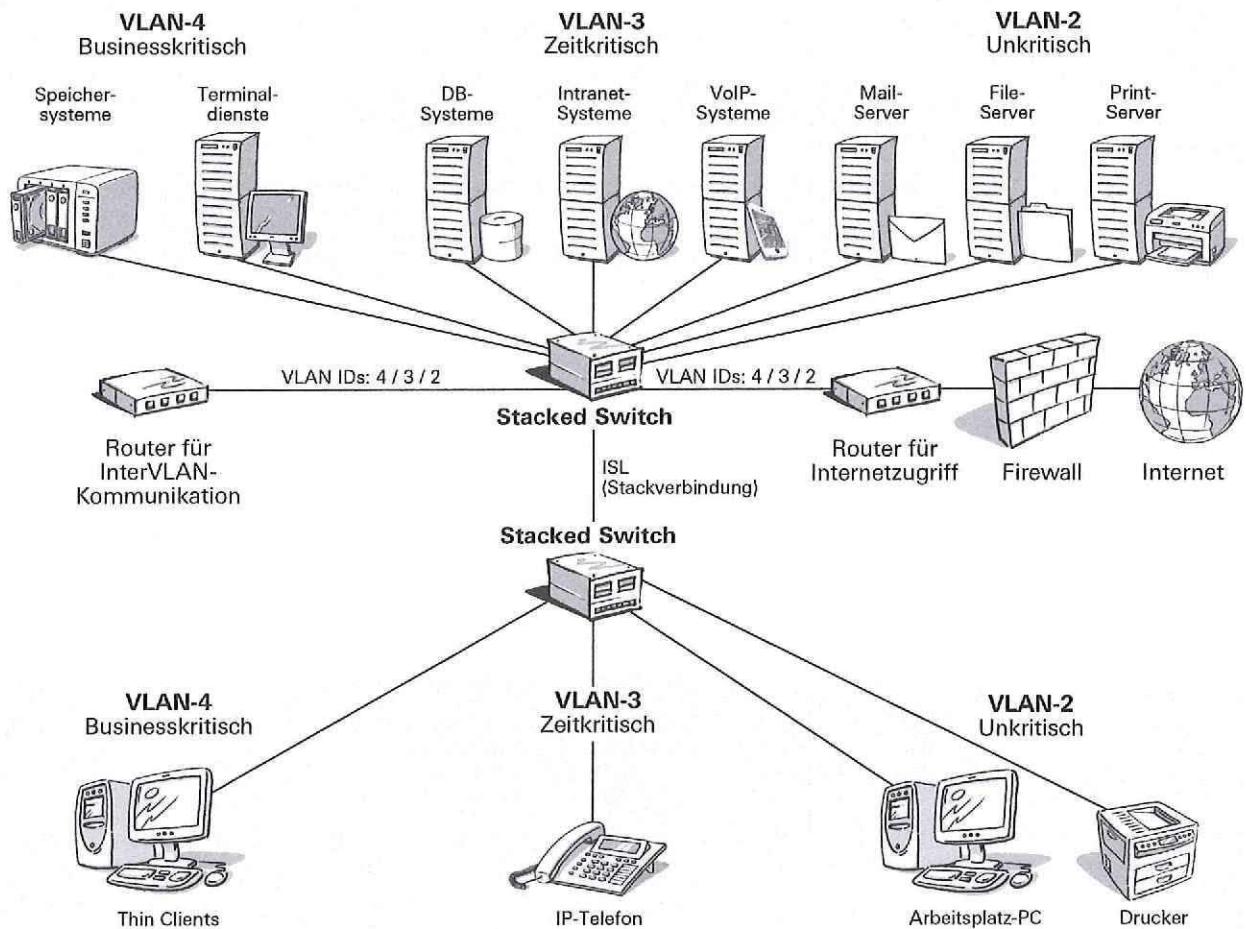
Ganz auf Dienstdaten zu verzichten, ist nicht möglich, da sie für die Steuerung des Netzwerkbetriebs notwendig sind. Sie können aber die Verbreitung solcher Daten im Netz einschränken, indem Sie das Netzwerk in verschiedene Bereiche aufteilen. Diese **Segmentierung** geschieht durch virtuelle LANs (VLANs), die mithilfe eines Switches eingerichtet werden können. Systeme zwischen zwei verschiedenen VLANs sind komplett voneinander getrennt, da die Trennung auf Layer 2 des OSI-Modells vollzogen wird. Daher «kennen» sich diese Systeme nicht und können auch keine Daten austauschen. Dies gilt auch für die

[1] Englisch für: Betriebslasten, Betriebskosten, zusätzlicher Aufwand.

Verwaltungs- und Dienstdaten. Der Overhead eines VLANs kann sich also nicht auf ein anderes VLAN «ausbreiten».

Aufgrund der weiter oben vorgenommenen Gruppierung der Datenströme wird das LAN also in drei verschiedene VLANs segmentiert. Die entsprechende **Netzwerkstruktur** kann z. B. wie folgt aussehen:

[4-14] Segmentierung eines LANs gemäss Datenklassifizierung (Beispiel)



Obwohl sich diese Trennung auswirkt, als ob die Netzwerksegmente **physisch** voneinander getrennt wären, erfolgt lediglich eine **logische Trennung** der Datenströme auf den Netzwerkswitches. Ein Datenaustausch zwischen den einzelnen VLANs nur dann möglich, wenn diese mittels Router über OSI Layer 3 miteinander verbunden werden. Und weil ein Router generell Broadcasts sperrt, bleiben die **Dienstdaten** im jeweiligen VLAN.

Ein **Switchport** kann unterschiedlichen VLANs zugewiesen werden. Häufig werden folgende Zuweisungsmöglichkeiten genutzt:

- **Untagged:** Hier wird der Switchport keinem VLAN zugeordnet. «Untagged» Switchports sind aber immer automatisch Mitglied (Member) des «Default-VLANs». Ein «untagged» Port wird i. d. R. mit VLAN-ID 1 bezeichnet. Die folgenden Switchports sind alle «untagged», da sie nur Mitglied des Default-VLANs (VID 1) sind:

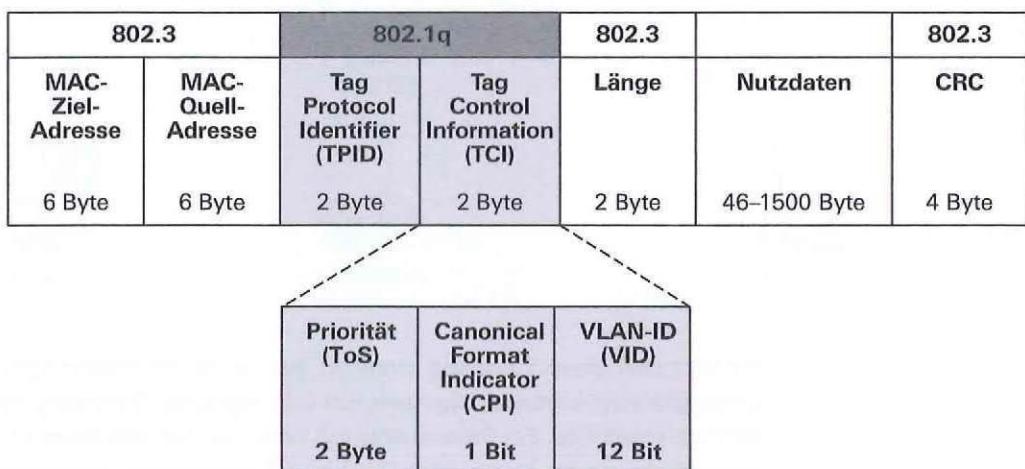
[4-15] VLAN-Zuweisungen auf einem 24 Port Switch (ZyXEL GS1910-24)

VLAN Membership Status																									Port Members
VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	Port Members
1	<input checked="" type="checkbox"/>																								

- **Tagged:** Hier entnimmt der Switchport die Information, für welches VLAN die Daten bestimmt sind, direkt aus dem Ethernet-Frame. Gemäß IEEE 802.1Q stehen 12 Bits für die VID-Definition (VLAN Identifier) zur Verfügung. Theoretisch können also 212, d. h. 4 096 unterschiedliche VLANs adressiert werden. Da aber die beiden VLAN-IDs 0 und 1 reserviert sind, können maximal 4 094 VLANs adressiert werden. Ein «tagged» Port gehört i. d. R. mehreren VLANs an. Wenn ein Switchport mehreren VLANs zugewiesen wird, muss der entsprechende Port zwingend «tagged» sein.

Gemäß IEEE 802.1Q bedeutet **Tagging**, einem Ethernet-Frame zusätzliche Informationen hinzuzufügen. Dies geschieht mithilfe von **Tags**<sup>[1]</sup>. Innerhalb eines Tags (2 Bytes) finden sich Informationen über VLANs und Prioritäten:

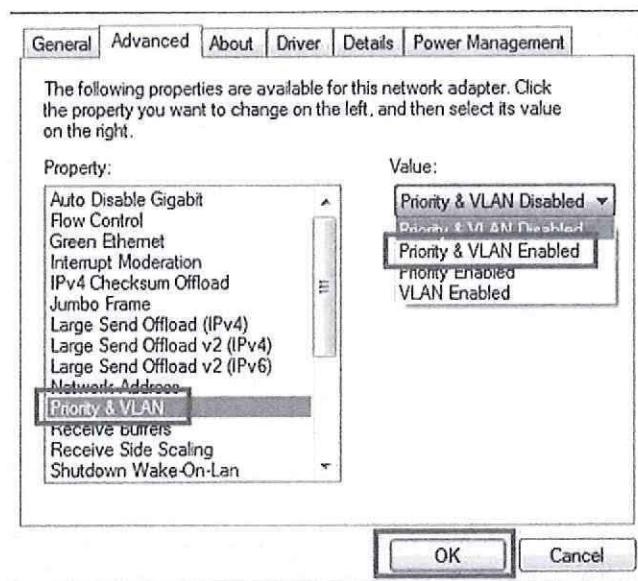
[4-16] «Tagged» Ethernet-Frame nach IEEE 802.1Q



In diesem Zusammenhang muss beachtet werden, dass eine **Netzwerkkarte** auch in der Lage sein muss, Tagging-Informationen zu verarbeiten. Die **Netzwerkschnittstelle** muss also 802.1Q-kompatibel sein. Unter MS Windows kann die entsprechende Einstellung z. B. wie folgt vorgenommen werden:

[1] Englisch für: Kennzeichen, Etikett, Anhänger, Schildchen.

## [4-17] 802.1Q auf Netzwerkkarte aktivieren (Beispiel)



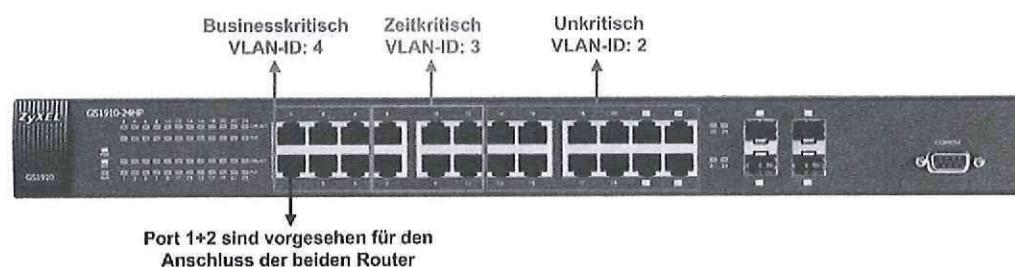
**Portbasiert:** Hier wird der Switchport einem oder mehreren VLANs fix zugewiesen. Diese Option hat also eine statische Zuweisung zur Folge. Als Netzwerkadministrator müssen Sie beim «Patchen»<sup>[1]</sup> eines Systems an einen freien Switchport genau wissen, welche VLANs welchem Switchport zugewiesen wurden. Für die gruppierten Datenströme wurden folgende Zuweisungen vorgenommen:

## [4-18] VLANs und Portzuweisungen (Beispiel)

		VLAN Membership Status																							
VLAN ID	VLAN Name	Port Members																							
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	default	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2	noncritical	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>									
3	timecritical	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
4	businesscritical	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>											

Im oben angezeigten Beispiel sind die Ports 1 und 2 «tagged», da sie Mitglied mehrerer VLANs sind. Mittels Tagging werden entsprechende Informationen in das Ethernet-Frame eingebettet. An diese Ports werden später die Router für die VLAN-Kommunikation und für den Internetzugriff angeschlossen. Die restlichen Ports (3 bis 24) sind «untagged». Falls ein Ethernet-Frame keine VLAN-IDs enthält (also «untagged» ist), wird es automatisch dem Native- oder Default-VLAN (VLAN-ID 1) zugeteilt. In unserem Fall möchten wir die Ports 3 bis 24 auf verschiedene VLANs verteilen. Folgende Abbildung zeigt die Frontansicht eines Switches mit der entsprechenden VLAN-Zuteilung:

## [4-19] Portbasierte VLAN-Zuteilung (ZyXEL GS1910-24)



[1] Englisch für: Anschließen.

### Hinweis

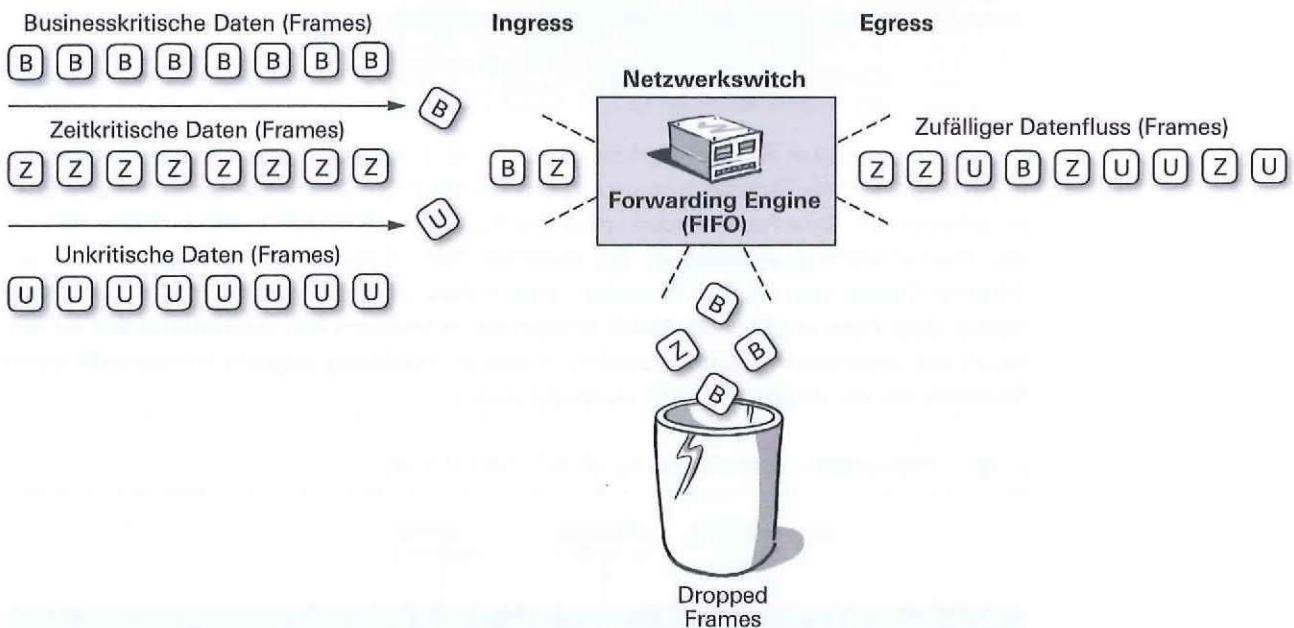
▷ Wenn ankommende Ethernet-Frames (Ingress<sup>[1]</sup>) mit VLAN-Tags an einen weiteren Switch geleitet werden, muss der entsprechende Switchport (Egress<sup>[2]</sup>) im «tagged»-Modus arbeiten. Ansonsten kann es sein, dass die Tags bei der Weiterleitung gelöscht werden. Dasselbe muss auch bei der Weiterleitung solcher Frames an einen Endknoten (z. B. Server) beachtet werden. Bei der Virtualisierung werden die Netzwerkkarten eines Host-Systems von mehreren virtuellen Maschinen (VM) benutzt. In solchen Fällen ist es üblich, dass eine VM einer spezifischen VLAN zugeordnet ist.

### 4.5.3 Datenströme priorisieren

Die Steuerung der Datenströme wird i. d. R. ebenfalls auf einem Netzwerkswitch durchgeführt. Ohne diese Steuerung würden alle ankommenden Frames nach dem FCFS<sup>[3]</sup>-Prinzip weitergeleitet. Mit anderen Worten: «Wer zuerst kommt, mahlt zuerst.»

Solange im Netzwerk nur ein schwaches bis mittleres Datenaufkommen herrscht, besteht kein Problem mit diesem Prinzip. Sobald aber hohe Netzlasten zu bewältigen sind und ein Switch mehr Daten verarbeiten muss, als er kann, beginnt er damit, einzelne Frames fallen zu lassen bzw. zu verwerfen. Diese Tatsache an sich ist schon problematisch. Im Extremfall können sogar Frames verworfen werden, die aus businesskritischen Datenströmen stammen, was das Problem weiter verschärft. Hinzu kommt, dass die von einem Switch abgehenden Daten (Egress) in einer zufälligen Reihenfolge (nach dem FCFS-Prinzip) weitergeleitet werden, was je nach Situation auch nicht unseren Anforderungen an die Datenströme entspricht. Dieser **ungesteuerte Datentransport** lässt sich wie folgt veranschaulichen:

[4-20] Frame Forwarding eines Switches ohne Priorisierung



[1] Englischer Fachbegriff für: ankommender, eingehender Datenverkehr.

[2] Englischer Fachbegriff für: ab- bzw. ausgehender Datenverkehr.

[3] Abkürzung für: «First come, first served».

Um solche Probleme zu vermeiden, können Sie dem Netzwerkswitch Vorgaben bezüglich der Weiterleitung von Frames machen. Sie können z. B. verschiedene **Queues**<sup>[1]</sup> für die **Priorisierung der Datentransporte** definieren und entsprechende Bandbreiten reservieren:

[4-21] Queues definieren (Cisco SG 300-28P)

Queue	Scheduling Method			
	Strict Priority	WRR	WRR Weight	% of WRR Bandwidth
1	<input type="radio"/>	<input checked="" type="radio"/>	1	14.29
2	<input type="radio"/>	<input checked="" type="radio"/>	2	28.57
3	<input type="radio"/>	<input checked="" type="radio"/>	4	57.14
4	<input checked="" type="radio"/>	<input type="radio"/>	8	

Queue 1 has the lowest priority, queue 4 has the highest priority.

Buttons: Apply, Cancel

Erläuterungen zum Screenshot:

- In der obigen Grafik sind drei von vier **Priorisierungsoptionen** aktiviert, d. h., es stehen drei Verarbeitungslinien mit unterschiedlichen Prioritäten zur Verfügung.
- Die Priorisierung basiert auf dem **WRR<sup>[2]</sup>-Mechanismus**. Dieser Mechanismus weist jeder Verarbeitungslinie einen bestimmten Anteil der gesamten Weiterleitungskapazität des Switches zu.

Im obigen Beispiel wurden den Verarbeitungslinien folgende Prioritäten zugeordnet:

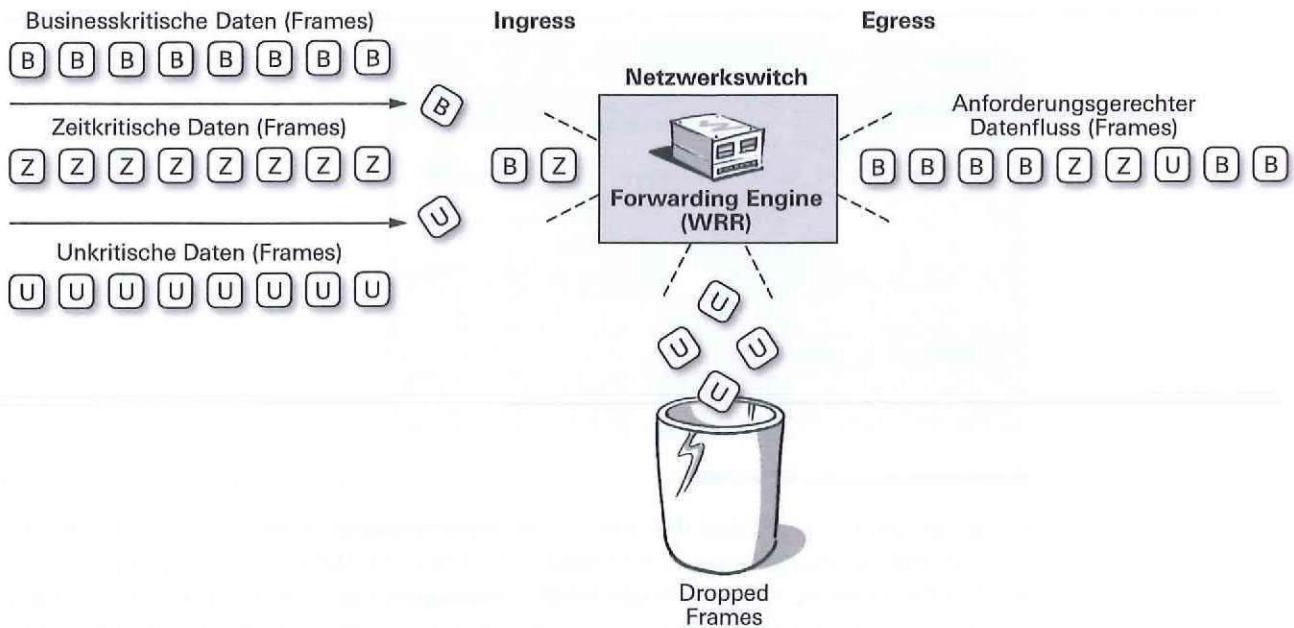
- **Queue 1** erhält 1/7 (ca. 14.3%) der gesamten Weiterleitungskapazität des Switches zugewiesen und ist für unkritische Datenströme geeignet.
- **Queue 2** erhält 2/7 (ca. 28.6%) der gesamten Switching-Kapazität zugewiesen und ist für zeitkritische Datenströme geeignet.
- **Queue 3** erhält 4/7 (ca. 57.1%) der gesamten Switching-Kapazität zugewiesen und ist für businesskritische Datenströme geeignet.

[1] Englisch für: Warteschlangen, Verarbeitungslinien.

[2] Abkürzung für: Weighted Round Robin. Englisch für: gewichteter Ring-/Kreisbetrieb. Nach Prioritäten gesteuerter Datenumlauf.

Die oben vorgenommenen Einstellungen wirken sich wie folgt auf die Weiterleitung von Frames aus:

[4-22] Frame Forwarding eines Switches mit WRR-Priorisierung



Auch wenn Datenströme priorisiert werden, kann es zu Situationen kommen, in denen ein Netzwerk überlastet ist und ein Switch ggf. Frames verwerfen muss. Mit der beschriebenen Priorisierung können Sie die Wahrscheinlichkeit aber gering halten, dass zeit- oder businesskritische Frames davon betroffen sind. Der Grund: Wegen der «bevorzugten Behandlung» der Frames in den Queues 2 und 3 sind mehrheitlich die Frames in der Queue 1 noch nicht verarbeitet und können deshalb (statistisch gesehen) auch mehrheitlich verworfen werden.

#### 4.5.4 Prioritätsstufen festlegen und anwenden

Damit Datenströme gemäss den festgelegten Regeln verarbeitet werden, müssen Sie auf den Switchports festlegen, mit welcher Priorität ankommende und abgehende Frames zu verarbeiten sind. Die Definition verschiedener **Prioritätsstufen** geschieht mithilfe sogenannter **CoS<sup>[1]</sup>-Bits** bzw. **ToS<sup>[2]</sup>-Bits**. Die drei Bits eines CoS/ToS-Felds ermöglichen es, acht (2<sup>3</sup>) unterschiedliche Prioritätsstufen zu definieren. Im Standard IEEE 802.1p werden folgende Stufen vorgeschlagen:

[1] Abkürzung für: Class of Service.

[2] Abkürzung für: Type of Service.

[4-23] Prioritätsstufen gemäss Empfehlung IEEE (Bezeichnung 802.1Q-2005)

PCP <sup>[1]</sup> -Bit	Prioritätsstufe	Kürzel	Eignung (Traffic-Eigenschaften)
1	0 (tiefste)	BK	Hintergrund (Background)
0	1	BE	Best Effort
2	2	EE	Excellent Effort
3	3	CA	Kritische Anwendungen (Critical Applications)
4	4	VI	Video, < 100 ms Verzögerung (Latenz)
5	5	VO	Sprache (Voice), < 10 ms Verzögerung (Latenz)
6	6	IC	Internet Control (Netzwerkmanagement)
7	7 (höchste)	NC	Network Control (Netzwerkmanagement)

[1] Abkürzung für: Priority Code Point.

#### CoS/ToS-Bits den Forwarding-Queues zuweisen

Damit die ankommenden Daten auf einem Switch gemäss den betrieblichen Anforderungen verarbeitet werden können, müssen Sie die CoS/ToS-Bits auf dem Switch den angelegten Queues zuweisen. Für unseren Fall werden folgende Zuweisungen getroffen:

PCP-Bit	Queue	Gruppe	Zuweisung (Mapping)																				
0 bis 2	1	Unkritisch																					
3 bis 5	2	Zeitkritisch																					
6 bis 7	3	Business-kritisch	<p><b>Cos/802.1p to Queue</b></p> <table border="1"> <thead> <tr> <th colspan="2">Cos/802.1p to Queue Table</th> </tr> <tr> <th>802.1p</th> <th>Output Queue</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>1</td> </tr> <tr> <td>1</td> <td>1</td> </tr> <tr> <td>2</td> <td>1</td> </tr> <tr> <td>3</td> <td>2</td> </tr> <tr> <td>4</td> <td>2</td> </tr> <tr> <td>5</td> <td>2</td> </tr> <tr> <td>6</td> <td>3</td> </tr> <tr> <td>7</td> <td>3</td> </tr> </tbody> </table> <p>Queue 1 has the lowest priority, queue 4 has the highest priority.</p>	Cos/802.1p to Queue Table		802.1p	Output Queue	0	1	1	1	2	1	3	2	4	2	5	2	6	3	7	3
Cos/802.1p to Queue Table																							
802.1p	Output Queue																						
0	1																						
1	1																						
2	1																						
3	2																						
4	2																						
5	2																						
6	3																						
7	3																						

**Prioritätsstufen auf Portebene zuweisen**

Abschliessend müssen Sie festlegen, in welcher Priorität die ausgehenden Daten weiterzuleiten sind. Zu diesem Zweck können Sie jedem Switchport einen **Default-CoS/ToS** zuordnen. Am jeweiligen Wert erkennt ein Port, welcher Queue er die Frames übergeben muss. Für unseren Fall werden folgende Zuweisungen getroffen:

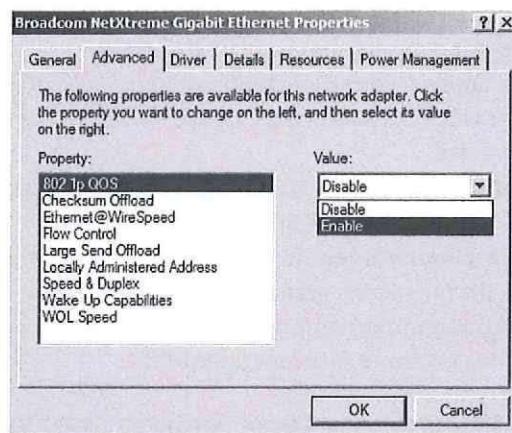
[4-24] Prioritätsstufen auf Portebene zuweisen

QoS Configuration Table			
	Entry No.	Interface	Default CoS
	1	GE1	7
	2	GE2	7
	3	GE3	7
	4	GE4	7
	5	GE5	7
	6	GE6	7
	7	GE7	5
	8	GE8	5
	9	GE9	5
	10	GE10	5
	11	GE11	5
	12	GE12	5
	13	GE13	2
	14	GE14	2
	15	GE15	2
	16	GE16	2
	17	GE17	2
	18	GE18	2

### QoS-Funktion auf Netzwerkkarte aktivieren

Wie beim Tagging nach 802.1Q muss auch eine **Priorisierung nach 802.1p** von der Netzwerkschnittstelle unterstützt werden. Ist eine **Netzwerkkarte (NIC)** mit diesem Standard nicht kompatibel oder wurde die entsprechende **QoS-Funktion** nicht aktiviert, werden die CoS/ToS-Bits i. d. R. verworfen oder ignoriert. Die entsprechende Einstellung einer Netzwerkkarte unter MS Windows sieht wie folgt aus:

[4-25] QoS-Funktion nach 802.1p aktivieren



### Prioritätsstufen auf Applikationsebene zuweisen

CoS/ToS-Bits können auch Applikationen zugewiesen werden. Damit haben Sie die Möglichkeit, die Priorität eines Datenstroms direkt beim Ursprung zu steuern. Dies hat aber nur dann die erhoffte Wirkung, wenn alle Netzwerkkomponenten auf dem Übertragungsweg zwischen einem Sender und Empfänger mit dem Standard 802.1p kompatibel sind.

#### Hinweis

- ▷ Eine Übersteuerung der CoS/ToS-Werte eines empfangenden Switchports ist auch durch direkte «Einbettung» des gewünschten CoS/ToS-Werts beim Sender nicht möglich. Wird z. B. vonseiten einer Applikation der CoS/ToS-Wert 6 vorgegeben und hat der empfangende Switchport «nur» den CoS/ToS-Wert 2 eingestellt, wird der Datenstrom gemäss den Einstellungen des Ports weiterverarbeitet.

### Weitere QoS-Massnahmen

Die bisher aufgezeigten QoS-Massnahmen beziehen sich auf Layer 2 des OSI-Modells, d. h., die Informationen zur Steuerung der Servicequalität stammen aus den Ethernet-Frames. Eine weitere Möglichkeit zur Steuerung der Servicequalität bietet der sogenannte DSCP<sup>[1]</sup>. DSCP ist unter RFC 2474 und 3260 standardisiert und erlaubt eine Priorisierung des Datenverkehrs anhand von QoS-Informationen innerhalb des IP-Datenpakets, also auf Layer 3 des OSI-Modells.

[1] Abkürzung für: Differentiated Services Code Point.

#### 4.5.5 Datenflüsse in öffentliche Netzwerke steuern

Nachdem Sie die nötigen Massnahmen ergriffen haben, um die Datenströme im lokalen Netzwerk gemäss den betrieblichen Anforderungen zu steuern, soll abschliessend sicher gestellt werden, dass ein **bedarfsgerechter Internetanschluss** zur Verfügung steht. Entsprechende Massnahmen basieren mehrheitlich auf Layer 4 des OSI-Modells.

Für die **Steuerung der Datenflüsse in öffentliche Netzwerke** ist folgendes Vorgehen zu empfehlen:

1. **Problem analysieren:** Hier ist abzuklären, ob ein bzw. welches Performanceproblem im Zusammenhang mit dem Internetanschluss besteht.
2. **Internetanschluss analysieren:** Hier ist abzuklären, welche technischen Eigenschaften der Internetanschluss aufweist und wie dieser in die bestehende Netzwerkinfrastruktur eingebunden ist.
3. **Massnahmen evaluieren:** Hier ist zu ermitteln, welche Massnahmen grundsätzlich für die Lösung des Problems infrage kommen.
4. **Lösungsvariante implementieren:** Ist die am besten geeignete Massnahme erkannt und bewilligt, kann sie umgesetzt werden.
5. **Wirksamkeit der Lösung überprüfen:** Hier wird die Effektivität der umgesetzten Lösung in Bezug auf das erkannte Problem überprüft.

Nachfolgend werden die **Ergebnisse dieser Vorgehensschritte** für unser Fallbeispiel zusammengefasst:

Problemanalyse				
Rückmeldungen der Benutzer:				
<ul style="list-style-type: none"> <li>• Viele Benutzer beklagen sich, dass der Zugriff auf bestimmte Websites manchmal sehr lange dauert (&gt; 5 Sek.). Häufig besuchte Websites sind: tagesanzeiger.ch, nzz.ch, wikipedia.org, facebook.com, 20min.ch.</li> <li>• Der Versand / Empfang von E-Mails funktioniert problemlos.</li> <li>• Der externe Zugriff bzw. die Synchronisation der E-Mail-Daten hat bis anhin immer problemlos funktioniert.</li> <li>• Beim Telefonieren kommt es in letzter Zeit immer wieder zu Aussetzern. Diese treten völlig zufällig auf. Manchmal mehrmals pro Tag, danach gibt es aber auch wieder Tage ohne jegliche Probleme.</li> </ul>				
Analyse Internetanschluss				
<ul style="list-style-type: none"> <li>• Provider: upc cablecom</li> <li>• Abo / Package: internet 125, Up-/Download: 10/125 Mbit/s</li> <li>• Volumeninfo: keine monatliche Volumenbeschränkung (Flatrate)</li> <li>• Addressinfo: dynamische IP</li> <li>• Zusatzdienste: nur Internzugang, Webmail / Mailboxen nicht genutzt</li> <li>• VoIP: Abonnement für 5 Telefonlinien bei sipcall.ch</li> </ul>				
Mögliche Massnahmen				
Aus den Rückmeldungen der Benutzer kann kein gravierendes Performanceproblem abgeleitet werden. Die Aussagen betreffend die VoIP-Telefonie weist zeitweise auf eine grosse Auslastung bzw. Überlastung der Bandbreite ins Internet hin. Als mögliche Massnahme wird eine Langzeitmessung der Datenübertragungen des Internetanschlusses (Up- und Download) ins Auge gefasst. Die Resultate einer solchen Messung sollte Flow-basierend sein. Als Sofortmassnahme bietet sich an, die QoS-Funktion beim Router für den Zugang ins Internet zu aktivieren. Folgende Regeln scheinen dabei sinnvoll zu sein:				
IP-Telefonie / VoIP	Protokoll/Port:	TCP&UDP/50605080	Richtung: Up&Down	Priorität: Hoch
Internet HTTP	Protokoll/Port:	TCP/80	Richtung: Up	Priorität: Mittel
Internet HTTPS	Protokoll/Port:	TCP/443	Richtung: Up	Priorität: Mittel
FTP	Protokoll/Port:	TCP/20-21	Richtung: Up	Priorität: Normal
SMTP	Protokoll/Port:	TCP/25	Richtung: Up	Priorität: Tief
Restlicher Traffic	Protokoll/Port:	TCP&UDP/*	Richtung: Up	Priorität: Tief
Restlicher Traffic	Protokoll/Port:	TCP&UDP/*	Richtung: Down	Priorität: Normal

**Umgesetzte Lösung**

Beim betreffenden Gerät können für das Bandbreitenmanagement folgende Prioritätsstufen vergeben werden:

- High = 4
- Medium = 3
- Normal = 2
- Low = 1

Für unser Fallbeispiel wurden folgende Regeln für den Router definiert:

Bandwidth				
The Maximum Bandwidth provided by ISP				
Bandwidth Table				
Interface	Upstream (Kbit/Sec)	Downstream (Kbit/Sec)		
WAN	10000	125000		

Bandwidth Priority Table				
Enable	Service	Direction	Priority	
✓	Voice(SIP)[TCP & UDP/5060~5080]	Upstream	High	
✓	Voice(SIP)[TCP & UDP/5060~5080]	Downstream	High	
✓	HTTP[TCP/80~80]	Upstream	Medium	
✓	HTTPS[TCP/443~443]	Upstream	Medium	
✓	FTP[TCP/20~21]	Upstream	Normal	
✓	SMTP[TCP/25~25]	Upstream	Low	
✓	All Traffic[All]	Upstream	Low	
✓	All Traffic[All]	Downstream	Normal	

Erläuterungen zu den Einstellungen:

- **Voice(SIP):** Hier sollte darauf geachtet werden, dass dieser zeitkritische Dienst eine hohe Priorität erhält und dass der Portrange genug gross ist, damit die Vorgaben auch bei mehreren gleichzeitigen Anrufen noch wirkt. Diese Regel sollte für beide Richtungen gelten (Up / Down).
- **HTTP:** Dass dies das meistverwendete Protokoll ist, sollte vor allem in Richtung Up eine gewisse (minimale) Bandbreite zur Verfügung stehen. In Richtung Down ist das unproblematischer, da die Bandbreite in diese Richtung viel grösser ist. Dasselbe gilt übrigens auch für HTTPS.
- **FTP:** Sollte zumindest in Richtung Up etwas gedrosselt werden, damit bei einem grösseren Datenversand nicht alle anderen Übertragungen (Flows) in Mitleidenschaft gezogen werden.
- **SMTP:** Ähnliche Einstellung wie bei FTP, da E-Mails immer öfters umfangreiche Anhänge besitzen. Die Priorität Low wurde darum gewählt, da Mailverkehr eine Stop-&-Forward-Übertragung ist und dadurch auch mit weniger Bandbreite problemlos funktioniert.
- **All Traffic:** Bei diesem Router bedeutet «All» alle restlichen Datenübertragungen, die nicht in der Regelliste aufgeführt sind. In Richtung Up wurde Low deshalb gewählt, da die Upload-Bandbreite im Vergleich zu Download um ein Vielfaches geringer ist und wir die verwendeten Übertragungsprotokolle nicht kennen mit Ausnahme von denen, die wir bei den Regeln angegeben haben. In Richtung Down wurde eine etwas höhere Priorität zugelassen (Normal), da die Bandbreite in diese Richtung wie bereits erwähnt wesentlich höher ist. Versuchshalber kann nach einer gewissen Zeit diese Priorität auch auf Medium erhöht werden, falls keine Probleme mehr auftreten.

**Hinweis**

- ▷ Eine zurückhaltende Vergabe der Prioritätsstufen lässt Spielraum für spätere Anpassungen offen.

Damit ein **Performance Management** betrieben werden kann, muss bekannt sein, welche Leistung bzw. Performance das Netzwerk überhaupt haben muss. Ist dieser Punkt geklärt, kann man damit beginnen, Leistungsdaten zu sammeln und auszuwerten.

Mithilfe von **SNMP** können auf einfache Weise die auf «managed» Netzwerkgeräten erhobenen Leistungsdaten abgerufen werden. Die Konfiguration eines SNMP-Agent auf einem Netzwerkgerät gestaltet sich recht einfach, doch hinsichtlich der Sicherung von vertraulichen Daten verfügt SNMP über einige Lücken. Nur SNMPv3 kann minimale Anforderungen an die Sicherheit erfüllen.

Neben SNMP etablieren sich immer mehr **NetFlow** und **sFlow** als eine zeitgemässere Art, Leistungsdaten auszuwerten. Daten basierend auf NetFlow und sFlow beinhalten neben dem bisher «reinen» Ressourcenverbrauch auch Angaben, wann und von wem diese Ressourcen verbraucht worden sind. Anhand dieser mehrstufigen Informationen lässt sich das Netzwerkperformancemanagement viel effizienter durchführen. Die gesammelten Leistungsdaten lassen sich meist durch deren grafische Darstellung einfacher analysieren. Hier muss darauf geachtet werden, dass eine geeignete **Darstellungsmethode** gewählt wird. Bei der grafischen Darstellung von Zeitreihen, das sind Daten über einen längeren Zeitraum, werden i. d. R. Histogramme dazu verwendet.

Damit die benötigte Performance eines Netzwerks besser eingeschätzt werden kann, sollten die anfallenden Datenströme gemäss deren Anforderungen charakterisiert werden. Eine solche Charakterisierung bildet die Grundlage dafür, dass man eine Priorisierung, also eine «Bevorzugung» gewisser Daten bzw. Applikationen, beim Transport durchs Netzwerk vornehmen kann. Zur **Priorisierung der Weiterleitung von Datenströmen** stehen verschiedene standardisierte Verfahren zur Verfügung. Mit IEEE 802.1Q ist es möglich, ein Netzwerk in verschiedene **virtuelle Netzwerke (VLANs)** aufzuteilen. Dies hat den Vorteil, dass sich der Netzwerkverkehr unterschiedlicher VLANs nicht gegenseitig negativ beeinflusst. Mit IEEE 802.1p lassen sich acht verschiedene Prioritätsstufen (CoS) auf Layer 2 definieren, mit deren Hilfe ein Ethernet-Frame eines entsprechenden Datenstroms gesteuert bzw. priorisiert weitergeleitet werden kann. Die meisten Netzwerkgeräte wie Switches, Router und Access Points unterstützen diese QoS-Mechanismen.

## Repetitionsfragen

---

**17**

SNMPv3 erfüllt zwar minimale Voraussetzungen hinsichtlich der IT-Sicherheit, gilt aber immer noch als ein unsicheres Protokoll. Was müsste SNMP zusätzlich erfüllen, damit es als «sicher» eingestuft werden kann?

---

**24**

Wann wählen Sie ein «Ranking» und wann wählen Sie ein «Histogramm» zur Darstellung von Messwerten?

---

**28**

Welchen Vorteil ergibt sich aus dem Einsatz von NetFlow-/sFlow-fähigen Netzwerkgeräten gegenüber der Nutzung von SNMP?

---

**9**

Nennen Sie zwei Situationen, die zu Problemen hinsichtlich der Netzwerkperformance führen können, und nennen Sie zu jedem Problem eine mögliche Ursache.

- 
- 13 Welche standardisierten Verfahren stehen zur Verfügung, um den Netzwerkverkehr auf OSI Layer 2 zu steuern?
- 
- 23 Nennen Sie die Schritte, die notwendig sind, um einen «problematischen» Internetzugang mittels Bandbreitenmanagement zu verbessern.
- 
- 14 Was müssen Sie bei der Konfiguration des SNMP-Agent in Bezug auf die Sicherheit beachten?
-

## 5 Sicherheitsmanagement

---

Da fast alle Systeme innerhalb einer IT-Infrastruktur vernetzt sind, muss dem Thema Sicherheit die nötige Beachtung geschenkt werden. Man kann zu Recht sagen, dass das Netzwerk eines der «Haupteinfallstore» für Angriffe auf die IT-Systeme eines Unternehmens sind. Aus diesem Grund müssen spezielle Massnahmen implementiert werden, damit vonseiten des Netzwerks Angriffe auf die Systeme und Informationen erfolgreich abgewehrt werden können. In diesem Kapitel werden die gängigsten **Sicherheitsmaßnahmen** aufgezeigt, die speziell innerhalb des Netzwerks zum Einsatz kommen.

### 5.1 Ziele und Aufgaben

---

Das generelle Ziel des FCAPS-Sicherheitsmanagements ist es, innerhalb der Netzwerkinfrastruktur **Sicherheitsrisiken** zu identifizieren und mithilfe geeigneter Massnahmen zu minimieren. Im Folgenden werden die übergeordneten **Schutzziele der IT-Sicherheit** sowie typische Aufgaben eines Netzwerkadministrators beim Management der **Netzwerksicherheit** dargelegt.

#### 5.1.1 Schutzziele der IT-Sicherheit

---

Die **IT-Sicherheit** umfasst folgende **Schutzziele**:

Schutzziele	Beschreibung
<b>Verfügbarkeit</b>	Der Zugriff auf die Daten und Applikationen des Unternehmens muss innerhalb eines vereinbarten Zeitraums jederzeit gewährleistet sein. Ein Systemausfall muss wirksam verhindert werden.
<b>Integrität</b>	Die Daten des Unternehmens sind korrekt und vertrauenswürdig. Datenänderungen müssen nachvollziehbar sein.
<b>Vertraulichkeit</b>	Die Daten des Unternehmens dürfen nur von berechtigten Personen bzw. Mitarbeitenden eingesehen und bearbeitet werden. Entsprechend müssen der Zugriff auf solche Daten und deren Übertragung sicher sein.
<b>Authentizität</b>	Die Identität der Personen bzw. Mitarbeitenden, die auf die Daten und Applikationen des Unternehmens zugreifen, muss echt sein und wird überprüft.
<b>Verbindlichkeit</b>	Eine Handlung innerhalb des Netzwerks wie z. B. die Einsichtnahme und Bearbeitung von Daten kann eindeutig nachgewiesen werden. Das Abstreiten solcher Handlungen ist nicht möglich.
<b>Zurechenbarkeit</b>	Eine Handlung innerhalb des Netzwerks kann einer bestimmten Person bzw. einem bestimmten Mitarbeiter eindeutig zugeordnet werden.

#### 5.1.2 Aufgaben des Netzwerkadministrators

---

Bei der **Netzwerksicherheit** geht es darum, die übergeordneten Schutzziele der IT-Sicherheit zu gewährleisten und unerwünschte Sicherheitsrisiken wie z. B. Angriffsmöglichkeiten über das Netzwerk einzuschränken. Folgende **Sicherheitsaufgaben** fallen in den Bereich des Netzwerkadministrators:

- Datenströme filtern
- Systeme und Benutzer authentifizieren
- Gefährdete Netzwerkbereiche abschotten
- Sicherheitsrelevante Aktivitäten erkennen und stoppen

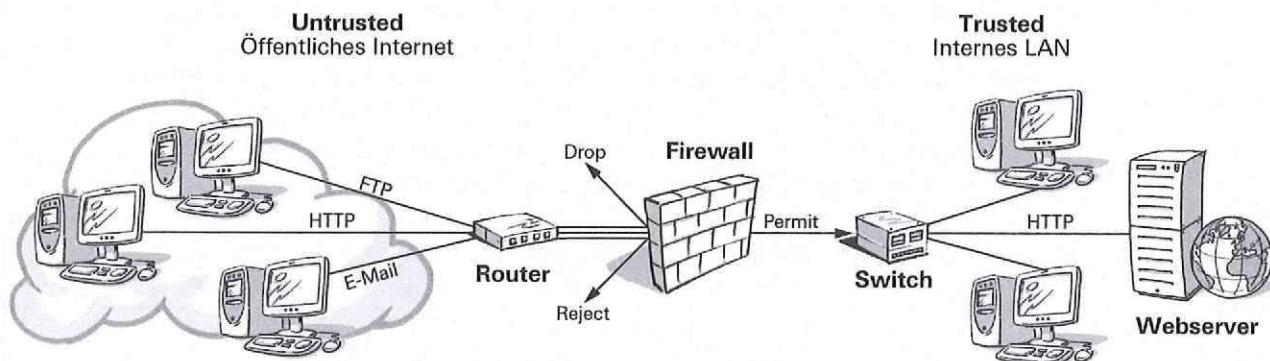
## 5.2 Massnahmen für die Netzwerksicherheit

Im Folgenden werden typische Massnahmen vorgestellt, die für die Erfüllung dieser Aufgaben infrage kommen. Dabei ist zu beachten, dass ggf. erst die Kombination mehrerer Massnahmen die gewünschte Wirkung erzielt. Je nach Situation bzw. Bedarf reicht es also nicht aus, eine bestimmte Massnahme isoliert umzusetzen.

### 5.2.1 Datenströme filtern

Eine Filterung der Datenströme auf **maliziöse<sup>[1]</sup> Inhalte** geschieht üblicherweise mithilfe einer **Firewall**<sup>[2]</sup>. Dies ist eine Netzwerkkomponente, die sich zwischen einem sicheren Netzwerk (**trusted Network**) und einem unsicheren Netzwerk (**untrusted Network**) befindet und die zwischen diesen Netzwerken ausgetauschte Datenpakete anhand vorgegebener Regeln bearbeitet.

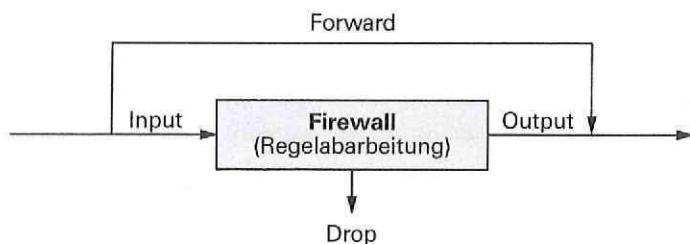
[5-1] Positionierung einer Firewall



### Arbeitsprinzip einer Firewall

Eine Firewall kann Datenpakete oder Netzwerkanfragen anhand definierter Regeln filtern und verfügt normalerweise über drei verschiedene **Verarbeitungslinien**: die **Input-Queue**, die **Forward-Queue** und die **Output-Queue**. Die definierten **Firewall-Regeln** bilden eine Art Stapel, der jeweils von oben nach unten abgearbeitet wird. Passt die Anweisung der ersten Regel nicht auf ein Datenpaket bzw. eine Netzwerkanfrage, wird die nächste Regel angewendet. Dieser Prozess wird so lange fortgeführt, bis die letzte Regel abgearbeitet worden ist. Kann keine Regel bzw. keine Anweisung angewendet werden, wird das Paket bzw. die Anfrage verworfen (**dropped**). Folgende Grafik soll dieses Prinzip veranschaulichen:

[5-2] Verarbeitungslinien einer Firewall



[1] Fremdwort für: boshaft, arglistig, böswillig.

[2] Englisch für: Brandschutzmauer (wörtl.).

Bei der Regeldefinition kommen üblicherweise folgende **Grundoperationen** zum Einsatz:

Operation / Anweisung	Aktion
<b>DROP oder DENY</b>	Das Datenpaket bzw. die Netzwerkanfrage wird verworfen, also gesperrt, ohne den Sender des Pakets darüber zu informieren.
<b>REJECT</b>	Das Datenpaket bzw. die Netzwerkanfrage wird zurückgewiesen und der Sender des Pakets darüber informiert.
<b>FORWARD oder PERMIT</b>	Das Datenpaket bzw. die Netzwerkanfrage wird erlaubt, d. h., das Paket wird durchgelassen bzw. weitergeleitet.

Zusätzlich zu diesen Operationen bzw. Anweisungen gibt es **erweiterte Möglichkeiten**, die Datenfilterung zu regeln. So könnte ein Angreifer etwa eine **DoS<sup>[1]</sup>-Attacke** starten, um die Webseiten eines Unternehmens durch unzählige Verbindungsanfragen zu blockieren. Dies lässt sich verhindern, indem von einer bestimmten IP-Adresse während einer bestimmten Zeitspanne nur eine begrenzte Anzahl von externen Verbindungen zugelassen wird.

#### Beispiel für eine Regeldefinition

Ein kleines Dienstleistungsunternehmen möchte, dass Personen von extern via Internet auf den Webserver im LAN zugreifen können. Die IP-Adresse des Webservers lautet 192.168.5.10. Der Internet-Router der Firma soll für Überwachungszwecke «gepingt» werden können. Die öffentliche IP-Adresse (WAN-Anschluss) des Unternehmens lautet 167.12.9.53. Alle Benutzer sollen auf das Internet zugreifen können. Der Router mit Firewall verfügt über einen ADSL- und einen Ethernet-Port. Um die gewünschten Datenverbindungen zu ermöglichen, werden auf der Firewall folgende Regeln definiert und aktiviert:

Pos.	Regel	Auswirkung / Beschreibung
1	DROP Input	Sperrt alle direkten Verbindungsanfragen aus dem Internet.
2	DROP Forward	Erlaubt keine Weiterleitungen.
3	PERMIT -prot icmp -dest 167.12.9.53 icmp echo-request	Ping-Aufrufe an den Internet-Router (Destination IP 167.12.9.53) werden beantwortet, jedoch nur Ping-Anfragen an einen anderen Host.
4	INPUT -p tcp -dport 80;443 -limit 20/minute -limit-max 100	Es werden höchstens 20 Verbindungsanfragen pro Minute auf die TCP-Ziel-Ports des Webservers (80 und 443) zugelassen. Insgesamt sind maximal 100 Verbindungen (Sessions) erlaubt.
5	FORWARD -p tcp -d 167.12.9.53 -dport 80;443 -to 192.168.5.10	Leitet alle TCP-Datenpakete mit der Ziel-IP 167.12.9.53 und den Ziel-Ports 80+443 direkt an die interne LAN-IP 192.168.5.10 (Webserver) weiter.
6	PERMIT Output	Direkte Datenverbindungen vom LAN ins Internet sind uneingeschränkt erlaubt. Das bedeutet, dass auch alle Antworten durchgelassen werden, da Firewalls normalerweise nur direkte Verbindungsaufrufe sperren.
7	DROP ALL	Alle übrigen (undefinierten) Datenpakete werden verworfen.

#### Hinweis

▷ Beachten Sie, dass obige Regeln nicht unbedingt die korrekte Schreibweise bzw. Syntax einer Firewall wiedergeben. Ziehen Sie für die Regeldefinition jeweils die spezifischen Vorgaben des Routers bzw. der Firewall zurate.

Je nach **Art der Datenfilterung** lassen sich unterschiedliche **Firewall-Typen** unterscheiden, die nachfolgend näher vorgestellt werden:

[1] Abkürzung für: Denial of Service. Englisch für: Dienstblockade eines überlasteten Systems.

## Paketfilter

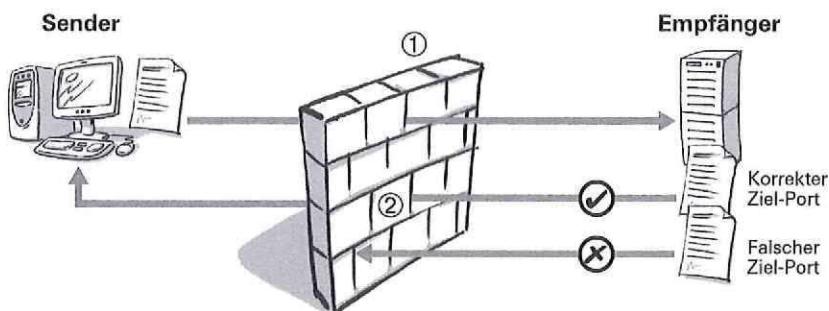
Dieser Firewall-Typ filtert Datenpakete anhand folgender Informationen:

- Layer 2: MAC-Adressen, VLAN-ID, CoS-Typ etc.
- Layer 3: Quell- und Ziel-IP-Adresse, Protokolle TCP, UDP etc.
- Layer 4: Quell- und Ziel-Ports, TCP SYN-Flag, ICMP-Typen etc.

## Stateful Packet Inspection (SPI)

Dieser Firewall-Typ filtert Datenpakete anhand einer zustandsorientierten Analyse der Datenverbindung. Dabei wird jedes Datenpaket einer spezifischen **Verbindung (Session)** zugeordnet. Jede Verbindung besitzt immer auch einen bestimmten **Zustand (State)**. Ein solcher Zustand ist z. B. der Quell-Port (Source) des Systems, das eine Verbindung initiiert. Entsprechend müssen die Datenpakete, die der Empfänger dem Sender als Antwort zurückschickt, als Ziel-Port (Destination) jeweils die Port-Nummer der Quelle enthalten. Folgende Grafik soll die Prüfung dieser Informationen verdeutlichen:

[5-3] Prinzip einer Stateful Packet Inspection



- ① Speicherung der Daten in der Statustabelle  
② Vergleich der Daten mit der Statustabelle

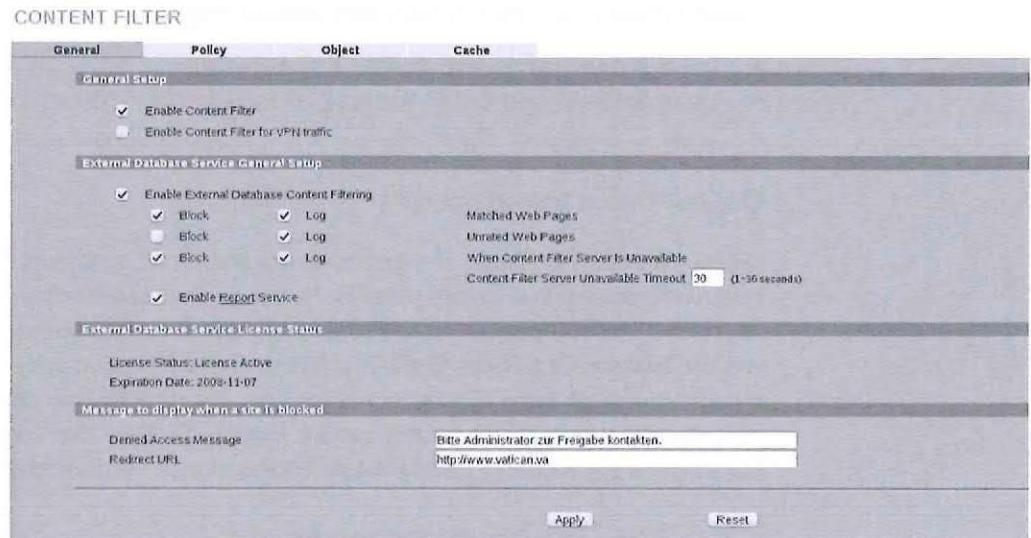
## Application Layer Firewall (ALF)

Dieser Firewall-Typ lässt keine direkte Kommunikation zwischen einem externen Netzwerk (Internet) und einem internen Netzwerk (LAN) zu. Zusätzlich zu den bereits erwähnten Informationen werden hier auch die **Nutzdaten (Payload)** eines Datenpakets untersucht. Dabei stehen folgende **Ziele** im Vordergrund:

- Unerlaubte Funktionsaufrufe bei Applikationsdaten erkennen und verhindern
- Schädliche Programmcodes bei Applikationsdaten erkennen und verhindern
- Zugriff auf unerwünschte (verbogene) Inhalte aus dem Internet erkennen und verhindern
- In Datenströme eingebettete Schadprogramme (Viren, Trojaner etc.) erkennen
- Datenübertragung durch eine Zwischenspeicherung (Caching) mehrfach abgerufener (identischer) Daten beschleunigen

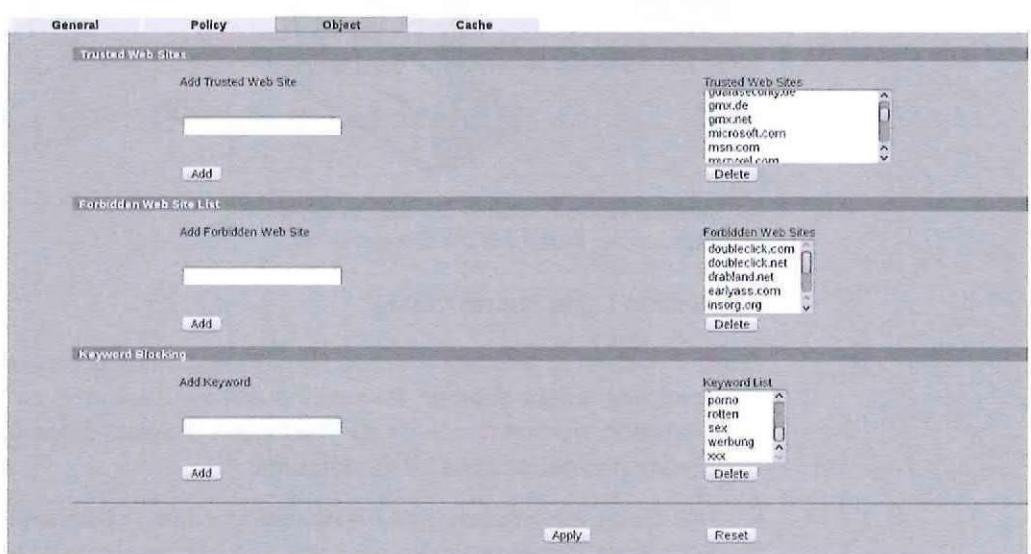
Entsprechend wird diese Art der Filterung auch **Content Filtering** genannt. Dabei werden auch die Daten der OSI Layer 5 bis 7 analysiert. Folgende Abbildung zeigt beispielhaft die Konfiguration und Aktivierung des URL-Filters (http-Proxy) auf einer Firewall (ZyWALL 35):

[5-4] Content Filter konfigurieren und aktivieren (Beispiel)



Und der folgende Screenshot zeigt beispielhaft die Definition der verbotenen Websites und Ausdrücke sowie möglicher Ausnahmen auf einer Firewall (ZyWALL 35):

[5-5] Unerwünschte bzw. verbotene Inhalte definieren (Beispiel)

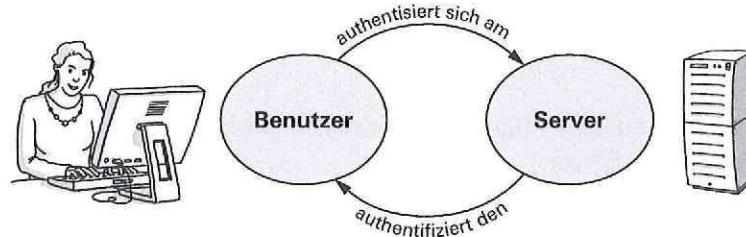


### 5.2.2 Systeme und Benutzer authentifizieren

Als Netzwerkadministrator möchten Sie nicht nur die übertragenen Datenpakete kontrollieren, sondern auch die Benutzer und Systeme identifizieren, die auf Ihr Netzwerk zugreifen. Für die **Authentifizierung der Benutzer und Systeme** können Sie das speziell dafür entwickelte, standardisierte Protokoll **IEEE 802.1X** sowie einen **RADIUS<sup>[1]</sup>-Server** einsetzen. Damit sind Sie in der Lage, den Zugriff eines Benutzers oder eines Systems an bestimmte Bedingungen zu knüpfen und den Zugriff auf das Netzwerk zu erlauben oder zu verweigern.

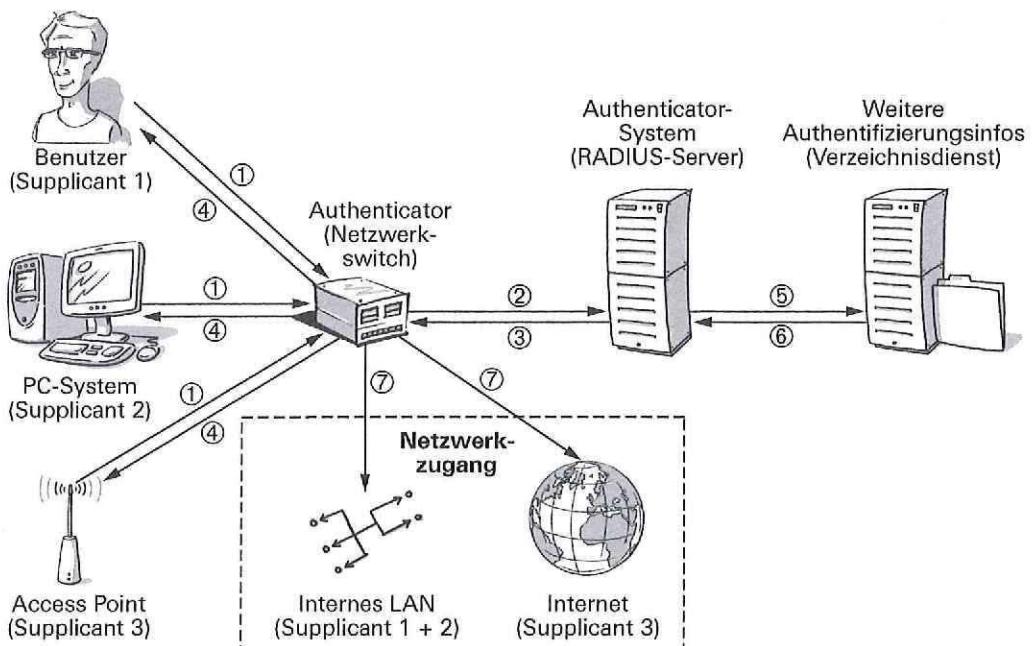
Bei der **Authentifizierung nach IEEE 802.1X** erfolgt die Kontrolle direkt beim Zugang zum Netzwerk auf Layer 2, also noch bevor ein Benutzer oder ein System Zugriff auf eine Ressource innerhalb dieses Netzwerks hat. Dabei wird sichergestellt, dass nur diejenigen Benutzer und Systeme Zugang zum Netzwerk erhalten, die bekannt sind bzw. die Erlaubnis dafür haben. Folgende Grafik soll das zugrunde liegende Prinzip veranschaulichen:

[5-6] Prinzip der Authentifizierung nach 802.1X



Voraussetzung für diese **Authentifizierungsmethode** ist, dass die eingesetzten Netzwerkgeräte «802.1X-kompatibel» sind. Eine Authentifizierungslösung nach diesem Standard beinhaltet folgende Komponenten und Funktionen:

[5-7] IT-Infrastruktur einer Authentifizierungslösung nach 802.1X



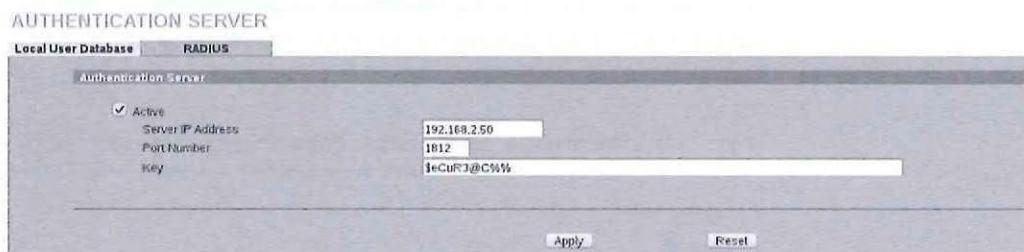
[1] Abkürzung für: Remote Authentication Dial-In User Service. Englisch für: Authentifizierungsserver für Fernzugriffe.

Erläuterungen zur obigen Abbildung:

- **Supplicant:** Der Supplicant (Antragssteller) meldet sich beim Authenticator (1) und erfordert den Zugang zum Netzwerk. Der Supplicant kann ein Benutzer, ein System, ein Netzwerkgerät oder eine Applikation sein. Die Antwort, ob ein Zugang erteilt oder abgelehnt wird (4), erhält der Supplicant direkt vom Authenticator.
- **Authenticator:** Der Authenticator (Antragsprüfer) erfüllt die Funktion eines Pfortners oder Türstehers und leitet die Zugangsanfragen (2) an das zentrale Authentication-System weiter. Der Authenticator ist ein Netzwerkgerät (i. d. R. ein Netzwerkswitch oder ein WLAN Access Point), das auf Layer 2 arbeitet.
- **Authentication-System:** Das Authentication-System ist eine zentrale Authentifizierungsstelle (z. B. RADIUS-Server), die die Zugangsanfragen der Supplikanten prüft und den Authenticator anweisen kann (3), den Zugang zum Netzwerk zu erteilen oder zu verweigern.
- **Weitere Authentifizierungsdienste:** Die zentrale Authentifizierungsstelle kann bei Bedarf auf weitere Authentifizierungssysteme zurückgreifen (5 und 6). Dies ist z. B. dann notwendig, wenn die Passwörter der Benutzer zentral in einem Verzeichnisdienst und nicht auf der zentralen Authentifizierungsstelle gespeichert werden.
- **Netzwerzugang:** Gemäß Anweisung der zentralen Authentifizierungsstelle erteilt der Authenticator den Supplikanten Zugang zu den entsprechenden Netzwerkbereichen (7).

Nachfolgend sehen Sie eine Beispielkonfiguration für die Authentifizierung nach 802.1X via RADIUS-Server:

#### [5-8] Einstellungen bei einem Authentifizierungsserver (ZyAIR WLAN-AP)



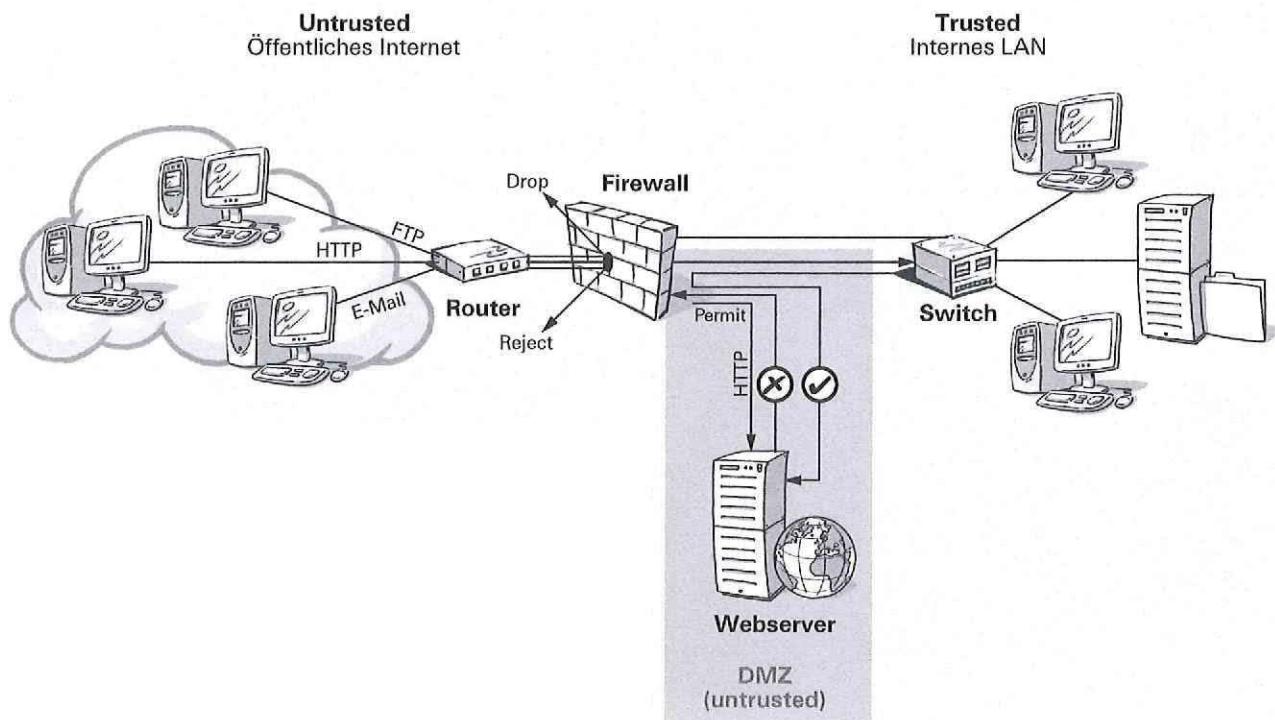
#### Hinweis

- ▷ Bei der obigen Server-IP-Adresse handelt es sich um die IP-Adresse des Authentication-Servers, da der Access Point die Funktion des Authenticators übernimmt.

#### 5.2.3 Gefährdete Netzwerkbereiche abschotten

Auch wenn Sie mehrere sinnvolle Massnahmen umsetzen und aufeinander abstimmen, gibt es keine Garantie für absolute Netzwerksicherheit. Aus diesem Grund empfiehlt es sich, besonders gefährdete Systeme von besonders schützenswerten Netzwerkbereichen abzuschotten. Dabei werden vor allem öffentlich zugängliche Systeme wie z. B. Web- oder Mailserver in einer sogenannten **Demilitarisierten Zone (DMZ)** platziert. Ein Angreifer kann auch bei einem erfolgreichen Angriff innerhalb der DMZ nur minimalen Schaden anrichten, weil sich hier keine besonders schützenswerten Systeme befinden und ein direkter Zugriff von einem System in der DMZ (untrusted) auf das LAN (trusted) nicht möglich ist. Folgende Grafik soll diese Trennung verdeutlichen:

[5-9] Prinzip eines abgeschotteten Netzwerkbereichs (internes LAN)

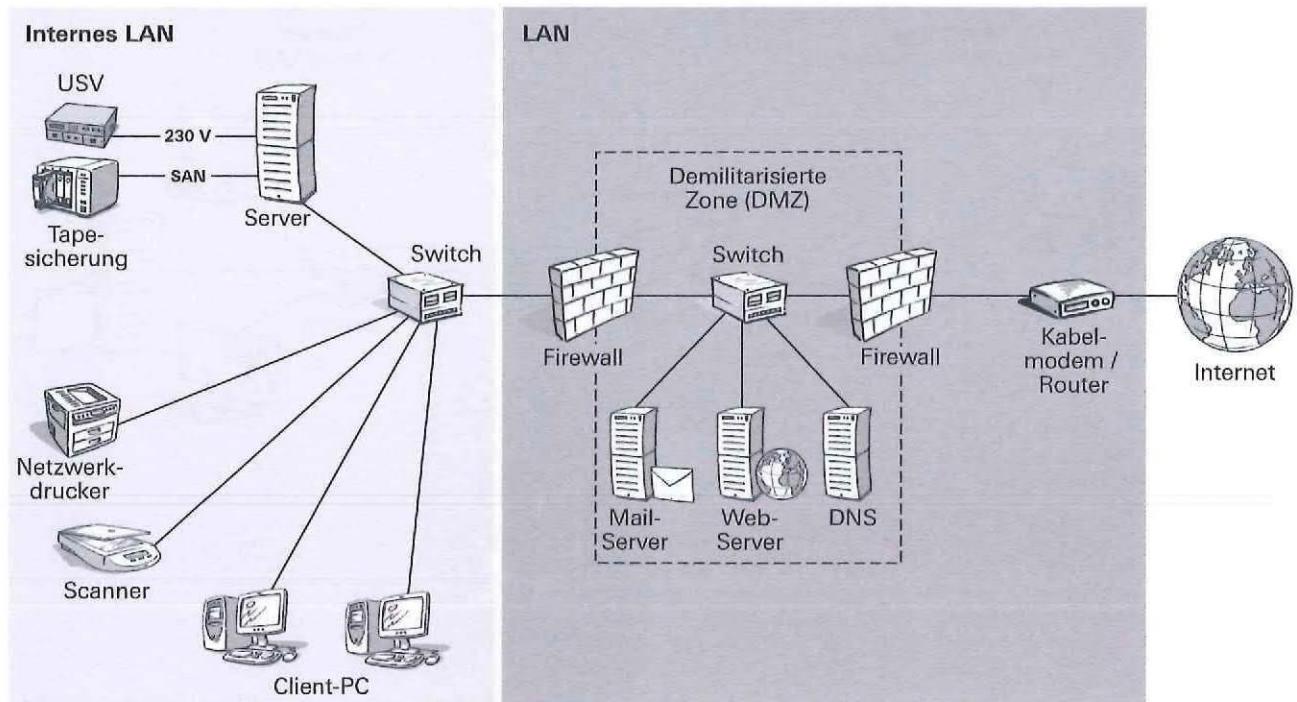


Erläuterungen zur Grafik:

Das obige Netzwerkschema zeigt ein **1-stufiges Firewall-Konzept**. Systeme aus dem internen LAN (trusted) können Anfragen direkt an den Webserver in der DMZ richten. Die Firewall sendet nur Datenpakete ins interne LAN zurück, die auf solche direkte Anfragen antworten. Direkte Anfragen aus der DMZ ins interne LAN dagegen werden von der Firewall abgeblockt. Durch diesen Filtermechanismus ist es für Angreifer besonders schwierig, auf das interne LAN (trusted) zuzugreifen, auch wenn sie ein System innerhalb der DMZ vollständig kontrollieren können.

Für eine noch wirkungsvollere Abschottung kann ein **2-stufiges Firewall-Konzept** realisiert werden. Das entsprechende Netzwerkschema sieht wie folgt aus:

[5-10] Prinzip eines 2-stufigen Firewall-Konzepts



**Hinweis**

- ▷ Ein 2-stufiges Firewall-Konzept kommt für die meisten KMUs aus Kostengründen nicht infrage.

**5.2.4 Sicherheitsrelevante Aktivitäten erkennen und stoppen**

Es muss nicht unbedingt sein, dass ein Angreifer von aussen in das Netzwerk eines Unternehmens eindringt. Oft werden Angriffe auch von Mitarbeitenden ausgeführt, die sich bereits im internen LAN, also im trusted Netzwerkbereich, befinden. In solchen Situationen helfen die bisher aufgeführten Massnahmen nicht weiter.

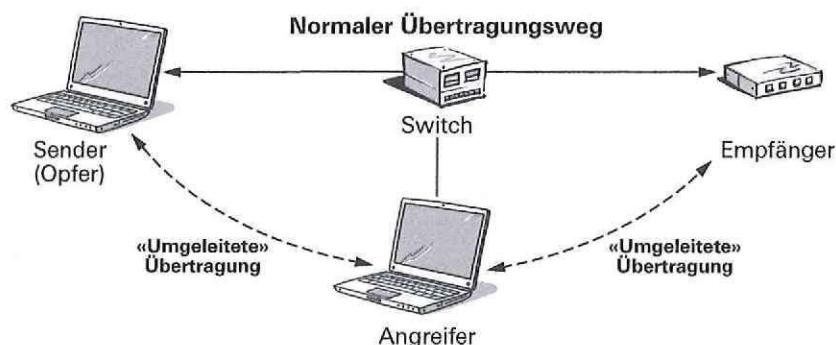
Jede Handlung<sup>[1]</sup> in einem Netzwerk löst spezifische Aktivitäten aus, die sich in einem bestimmten Muster (Pattern) des Datenstroms niederschlagen. Bei der Suche nach einer maliziösen Handlung geht es darum, Muster innerhalb der Datenströme zu erkennen, die darauf hinweisen. Diese Suche kann von einem sogenannten **Intrusion Prevention System (IPS)** oder **Intrusion Detection System (IDS)** übernommen werden. Ein solches System überwacht den Datenverkehr im Netzwerk und sucht dabei nach spezifischen Mustern. Sobald ein bestimmtes Muster erkannt ist, wird automatisch eine dafür hinterlegte (definierte) Aktion ausgelöst.

[1] Unabhängig davon, ob es eine erlaubte oder unerlaubte, eine interne oder externe Handlung ist.

## MITM-Attacke

Bei einer «**Man in the middle**»-Attacke klinkt sich ein Angreifer in die Übertragung zwischen Sender und Empfänger ein. Damit dies gelingt, sendet der Angreifer dem Sender, also dem Opfer, gefälschte **ARP<sup>[1]</sup>-Nachrichten**. In diesen Nachrichten wird dem Opfer mitgeteilt, dass die MAC-Adresse des lokalen Gateways geändert habe. Natürlich handelt es sich bei dieser geänderten MAC-Adresse nicht um die tatsächliche MAC-Adresse des Gateways, sondern um die MAC-Adresse des Angreifers. Da ARP-Nachrichten nicht verifiziert werden, ändert das Opfer «gutgläubig» den entsprechenden Eintrag in seiner lokalen ARP-Tabelle. Das Ändern einer **ARP-Tabelle** mit der Absicht, sich unerlaubt in eine Kommunikation einzuklinken, wird auch «**ARP-Poisoning**» genannt, also das «**Vergiften**» der ARP-Tabelle. Ab diesem Zeitpunkt läuft der gesamte Datenverkehr des Opfers über das System des Angreifers. Dieser kann nun den Datenstrom aufzeichnen oder direkt nach bestimmten Informationen analysieren. Das Opfer merkt nichts von diesem Vorgang, da es alle angeforderten Daten erhält trotz der bestehenden «Umleitung». Damit diese Umleitung aufrechterhalten bleibt, muss der Angreifer laufend ARP-Nachrichten an das Opfer senden, um zu verhindern, dass die ARP-Tabelle des Opfers zufällig durch eine korrekte ARP-Nachricht wieder geändert wird. Und genau dieser stetige Versand von ARP-Nachrichten kann von einem IPS erkannt und als Angriff taxiert werden. In diesem Fall könnte z. B. das IPS eine Meldung an den RADIUS-Server schicken mit der Anweisung, den Switchport des Angreifers zu deaktivieren.

[5-11] Schematischer Ablauf einer «Man in the middle»-Attacke (MITM)

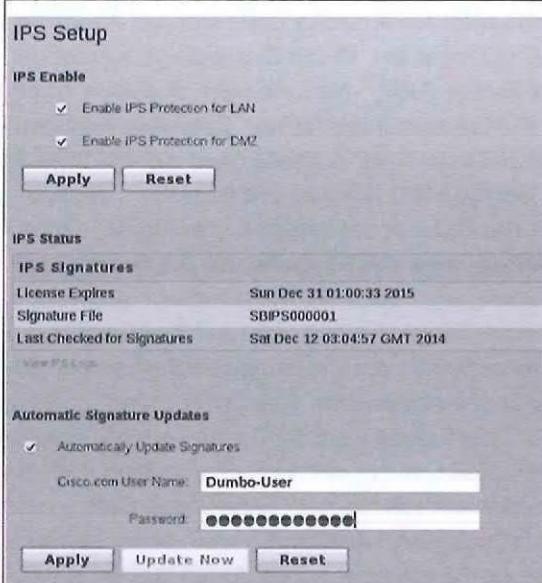
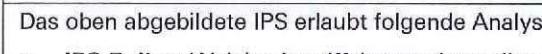


## Grundkonfiguration einer IPS / IDS

In KMUs wird ein IPS bzw. IDS i. d. R. direkt in den Datenstrom zwischen dem Internet und den internen Netzwerkbereichen wie DMZ und internes LAN geschaltet. So besteht die Möglichkeit, den gesamten ein- und ausgehenden Datenstrom bei Bedarf auf unerlaubte Netzaktivitäten hin zu analysieren. Dabei ist aber zu beachten, dass diese Analysen eine gewisse **Latenz** verursachen. Je mehr Analysefunktionen aktiviert werden, desto grösser wird auch die dadurch verursachte Verzögerung bei der Datenübertragung. Aus diesem Grund sollten Sie sich gut überlegen, welche Analysen wirklich unbedingt vorgenommen werden müssen. Ist es beispielsweise sinnvoll, dass das IPS bzw. IDS nach Viren und Spammails sucht, wenn alle Clients und Server mit einem Virenschanner ausgerüstet worden sind und beim Mailserver ein wirkungsvoller Spamfilter installiert wurde? Nachfolgend sehen Sie ein Beispiel für die Definition und Aktivierung der zu überwachenden Objekte in einem IPS.

[1] Abkürzung für: Address Resolution Protocol. Weist einer IP-Adresse die MAC-Adresse der Netzwerkschnittstelle zu.

## [5-12] Einstellungen bei einem IPS (Cisco SA520W)

 <p>The screenshot shows the 'IPS Setup' configuration page. In the 'IPS Enable' section, two checkboxes are checked: 'Enable IPS Protection for LAN' and 'Enable iIPS Protection for DMZ'. Below this are 'Apply' and 'Reset' buttons. The 'IPS Status' section displays the following information:</p> <table border="1"> <tr><td>License Expires</td><td>Sun Dec 31 01:00:33 2015</td></tr> <tr><td>Signature File</td><td>SBIPS00001</td></tr> <tr><td>Last Checked for Signatures</td><td>Sat Dec 12 03:04:57 GMT 2014</td></tr> </table> <p>Below the status is a link to 'View Log'.</p>	License Expires	Sun Dec 31 01:00:33 2015	Signature File	SBIPS00001	Last Checked for Signatures	Sat Dec 12 03:04:57 GMT 2014	<p><b>Überwachte Netzwerkbereiche</b> Bei diesem IPS wird der Datenverkehr vom Internet (WAN) zur DMZ und zum LAN analysiert.</p>
License Expires	Sun Dec 31 01:00:33 2015						
Signature File	SBIPS00001						
Last Checked for Signatures	Sat Dec 12 03:04:57 GMT 2014						
 <p>The screenshot shows the 'Automatic Signature Updates' section. A checkbox is checked for 'Automatically Update Signatures'. Below it is a form for 'Cisco.com User Name' containing 'Dumbo-User' and a password field with masked input. Below the form are 'Apply', 'Update Now', and 'Reset' buttons.</p>	<p><b>Updates der Angriffsmuster</b> Damit die IPS immer über die neuesten Angriffsmuster (Patterns) verfügt, muss die interne Muster-DB regelmäßig aktualisiert werden. Dieser Vorgang ist vergleichbar mit der Aktualisierung der Viren-Muster bei einem Antivirenskanner. Dieser Updateservice ist i. d. R. kostenpflichtig.</p>						
	<p><b>Automatisieren der Musterupdates</b> Am besten aktiviert man die automatische Aktualisierung der Muster-DB, damit dies nicht vergessen geht. Nur mit aktuellen Mustern lassen sich aktuelle, bekannte Angriffe erkennen und abwehren.</p>						

Das oben abgebildete IPS erlaubt folgende Analysemöglichkeiten:

- **IPS Policy:** Welche Angriffskategorien sollen überwacht werden?
- **Protocol Inspection:** Welche Netzwerkprotokolle sollen zusätzlich auf maliziöse oder ungewöhnliche Inhalte wie z. B. eingebetteter, «protokollfremder» Code / Befehle untersucht werden? Zum Beispiel könnten dies SQL-Befehle innerhalb von HTTP-Daten sein, sogenannte «SQL Injections».
- **IM and P2P Blocking:** Welche unerlaubten Netzwerkfunktionen wie z. B. Peer-to-Peer-Aktivitäten (P2P) mittels bestimmter Filesharing-SW oder der Nachrichtenversand (Instant Messaging, IM) über bestimmte Nachrichtendienste sollen blockiert werden?

Die Thematik **Netzwerksicherheit** ist ein Teilbereich innerhalb der IT-Sicherheit. Die Schutzziele der Netzwerksicherheit decken sich mehrheitlich mit denen der IT-Sicherheit. Doch bei der Netzwerksicherheit liegt der Fokus hauptsächlich auf der Erkennung und Verhinderung der Übertragung von maliziösen Daten über das Netzwerk. Dazu sind folgende Aktivitäten nötig:

- **Analysieren und Filtern der Datenströme** auf maliziöse Inhalte
- **Authentifizierung von Systemen / Benutzern** beim Netzzugang
- **Abschottung gefährdeter Netzwerkbereiche** für bestimmte Systeme und Funktionen
- **Erkennen und Stoppen** von unerlaubten Netzaktivitäten

Mit den folgenden technischen Massnahmen werden die oben aufgeführten Aktivitäten durchgeführt:

- **Firewalls** für das Filtern und Analysieren der Datenströme
- **Einsatz von 802.1X** zur Authentifizierung beim Netzzugang
- **Realisieren einer DMZ** zur Trennung von «trusted» und «untrusted» Netzwerkbereichen
- **Einsatz eines Intrusion Prevention System IPS** zum Aufspüren und Unterbinden von unerlaubten Netzaktivitäten

## Repetitionsfragen

---

- 6 Welche unterschiedlichen Firewall-Arten gibt es?
- 
- 12 Wozu wird eine DMZ eingerichtet und was versucht man damit zu erreichen?
- 
- 26 Die Netzzugangsauthentifizierung gemäss 802.1X basiert bekanntlich auf dem OSI Layer 2, Angriffe via Internet basieren aber mehrheitlich auf Layer 3 bis 7. Aus welchem Grund ist es trotzdem sinnvoll, IEEE 802.1X in schützenswerten Netzwerkbereichen einzusetzen?
- 
- 10 Nennen Sie drei unterschiedliche Zielobjekte, nach denen ein Intrusion Prevention System (IPS) Datenpakete analysiert.
-



## **Teil C Netzwerk um WLAN erweitern**

---

## Einleitung, Lernziele und Schlüsselbegriffe

---

### Einleitung

---

**Funknetzwerke** bzw. **Wireless LANs (WLAN)** haben sich in den letzten Jahren rasant weiterentwickelt und verbreitet. Gründe dafür: Sowohl bezüglich der Leistungsfähigkeit und Sicherheit als auch bezüglich der Einsatzmöglichkeiten und Kosten wurden grosse Verbesserungen erzielt. In diesem Teil des Lehrmittels lernen Sie zunächst wichtige Standards, Betriebsarten und Komponenten eines WLANs kennen. Danach erfahren Sie mehr darüber, was beim Betrieb eines **sicheren Funknetzwerks** zu beachten ist. Ein eigenes Unterkapitel befasst sich mit Möglichkeiten und Techniken, um sichere (trusted) Netzwerke über das unsichere (untrusted) Internet zu verbinden.

Auch der sichere Fernzugriff auf ein LAN sowie der sichere Zusammenschluss lokaler Netzwerke über das Internet **mittels VPN (virtuelles privates Netzwerk)** sind für viele Unternehmen aktuelle Themen. Entsprechend wird abschliessend aufgezeigt, wie sichere Verbindungs- und Zugriffsmöglichkeiten auf das Firmennetzwerk von ausserhalb ermöglicht werden können.

### Lernziele und Lernschritte

---

Lernziele	Lernschritte
<input type="checkbox"/> Sie können wichtige WLAN-Standards und Antennenarten nennen sowie deren Einsatzgebiete, Vor- und Nachteile beschreiben.	• Funknetzwerke planen und sicher betreiben
<input type="checkbox"/> Sie können wesentliche WLAN-Sicherheitsmaßnahmen erläutern.	• Funknetzwerke planen und sicher betreiben
<input type="checkbox"/> Sie können Möglichkeiten und typische Einsatzgebiete für eine sichere Verbindung entfernter LANs aufzeigen.	• Lokale Netzwerke über das Internet sicher verbinden
<input type="checkbox"/> Sie können die Vorteile und Nachteile von VPN-Technologien für eine sichere Verbindung nennen.	• Lokale Netzwerke über das Internet sicher verbinden
<input type="checkbox"/> Sie können den prinzipiellen Unterschied zwischen WAN Access, WAN-Core-Netzwerk und VPN-Verbindungen darlegen.	• Lokale Netzwerke über das Internet sicher verbinden

### Schlüsselbegriffe

---

IEEE-Standards, Datenübertragungsrate, Ad-hoc-Modus, Infrastruktur-Modus, WLAN-Roaming-Modus, WDS-Repeating-Modus, Access Point, WLAN-NIC, Repeater, Sendeleistung, Rundstrahl-Antenne, MIMO-Technik, Dämpfung, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Rogue Access Point, Hardening, SSID-Broadcast, Virtual Private Network (VPN), Site-to-Site, End-to-Site, End-to-End, IPsec, Authentication Header (AH), Encapsulated Security Payload (ESP), Internet Key Exchange (IKE), SSL-VPN

## 6 Funknetzwerke planen und sicher betreiben

Grundlegende Voraussetzung für die Planung und Umsetzung eines Funknetzwerks sind gute Kenntnisse über die Standards und Betriebsarten kabelloser Netzwerke.

### 6.1 IEEE-Standards

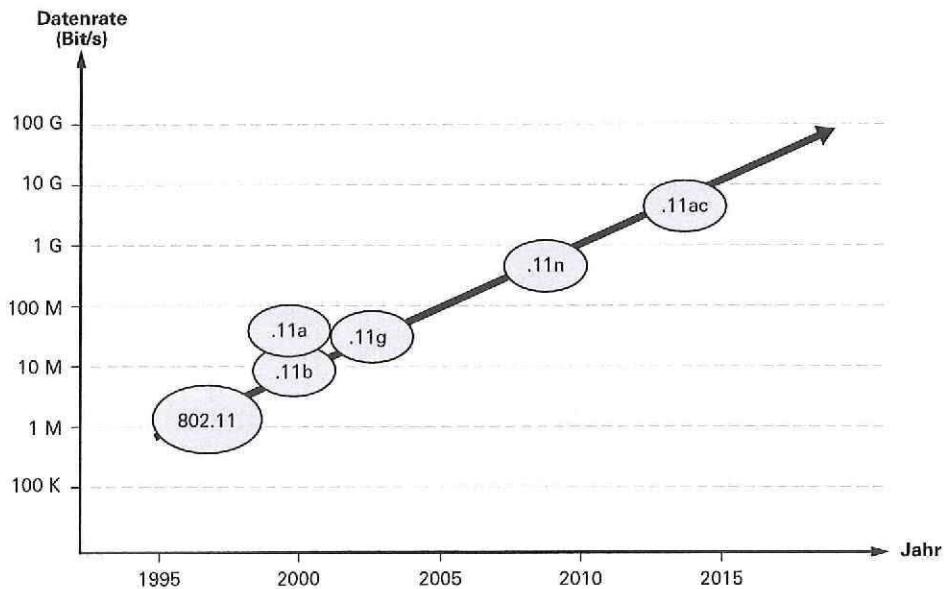
Während die IEEE-Standards der Reihe 802.3 verbindliche Vorgaben für kabelgebundene lokale Netzwerke (LAN) machen, definieren die **IEEE-Standards der Reihe 802.11** verbindliche Vorgaben für kabellose lokale Netzwerke (WLAN). Folgende Grafik fasst die IEEE-Standards im Bereich «Internet Working»<sup>[1]</sup> zusammen und zeigt deren Zuordnung zu den Layern 1 und 2 des OSI-Schichten-Modells:

[6-1] IEEE-Standards 802.1 (Übersicht)

2	802.1	802.2 Logical Link Control (LLC)			
		802.1 Media Access Control (MAC)			
1		802.3	802.4	802.5	802.11 Wireless LAN
		Ethernet	Token-Bus	Token-Ring	Wireless LAN

In den letzten beiden Jahrzehnten wurden die **IEEE-Standards für WLANs** laufend weiterentwickelt, wobei die **Datenübertragungsraten** markant zugenommen haben.

[6-2] Entwicklung der WLAN-Standards IEEE 802.11



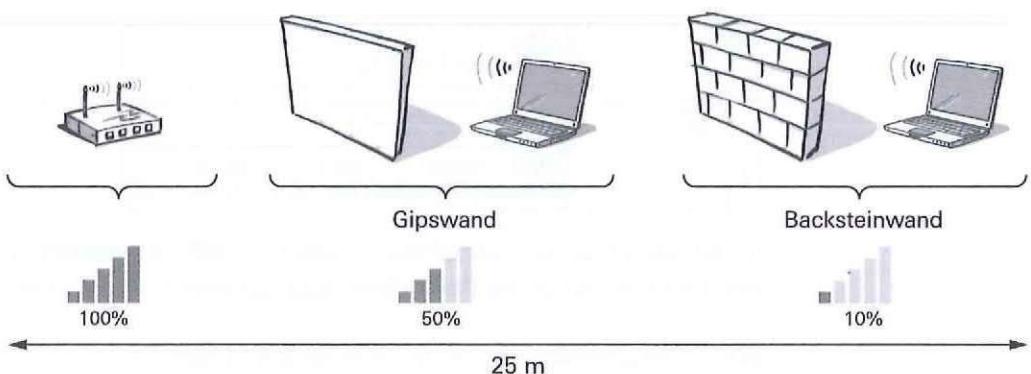
[1] Datenaustausch mittels Vernetzung zwischen unterschiedlichen Systemen.

Folgende Tabelle zeigt die in Europa gängigen **WLAN-Standards** mit den wichtigsten Merkmalen auf:

WLAN-Standard	802.11	802.11b	802.11a	802.11g	802.11n	802.11ac
<b>Frequenzbereich</b>	2.4 GHz	2.4 GHz	5 GHz	2.4 GHz	2.4 und 5 GHz	5 GHz
<b>Übertragungsrate (brutto)</b>	2 Mbps	11 Mbps	54 Mbps	54 Mbps	150–600 Mbps	1.3 Gbps
<b>Übertragungsrate (netto)</b>	≤ 1 Mbps	1–5 Mbps	≤ 32 Mbps	2–16 Mbps	≤ 200 Mbps	≤ 400 Mbps

Bezüglich der **Datenübertragungsrate** ist zu beachten, dass Hersteller i. d. R. den **Bruttodatendurchsatz** ausweisen, der einen theoretischen Wert darstellt. Die tatsächliche Übertragungsrate entspricht dem **Nettodataendurchsatz** und ist um einiges geringer. Zum einen können **Hindernisse und Entfernung** zwischen dem Sender und dem Empfänger das Funksignal reduzieren, sodass als Folge davon die Datenrate deutlich abnimmt:

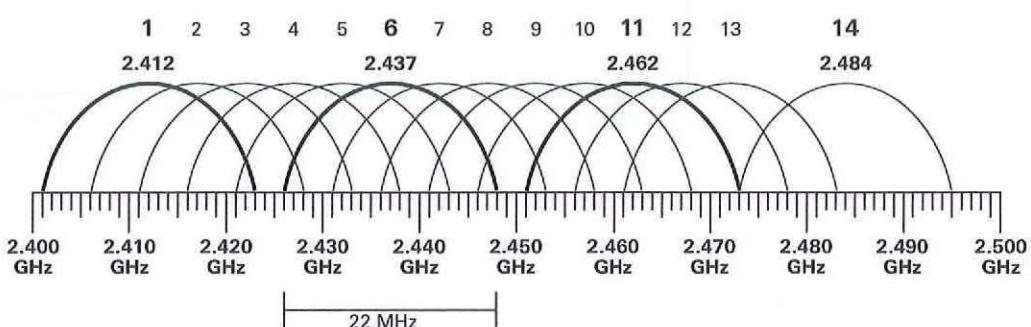
[6-3] Signalverlust infolge von Hindernissen und Entfernung



Zum anderen werden für die Datenübertragung verschiedene **Funkkanäle** verwendet, die unter den WLAN-Benutzern aufgeteilt werden. Das bedeutet, dass den einzelnen Benutzern nur ein Teil der theoretisch vorhandenen Übertragungskapazität zur Verfügung steht. So ist beispielsweise das **2.4-GHz-Frequenzband** in Europa in **13 Funkkanäle** aufgeteilt,<sup>[1]</sup> wobei der **Frequenzbereich (Kanalbreite)** jeweils 22 MHz beträgt und WLAN-Komponenten mit einer **Leistung** von höchstens 100 mW senden dürfen.

Durch diese **Kanalaufteilung** wird sichergestellt, dass mehrere Benutzer im gleichen WLAN parallel arbeiten können. Werden bei der Datenübertragung Funkkanäle verwendet, deren Frequenzbereiche sich überschneiden, nimmt die Übertragungsleistung deutlich ab. Sehen Sie sich dazu folgende Grafik an:

[6-4] Kanalaufteilung im 2.4-GHz-Frequenzband

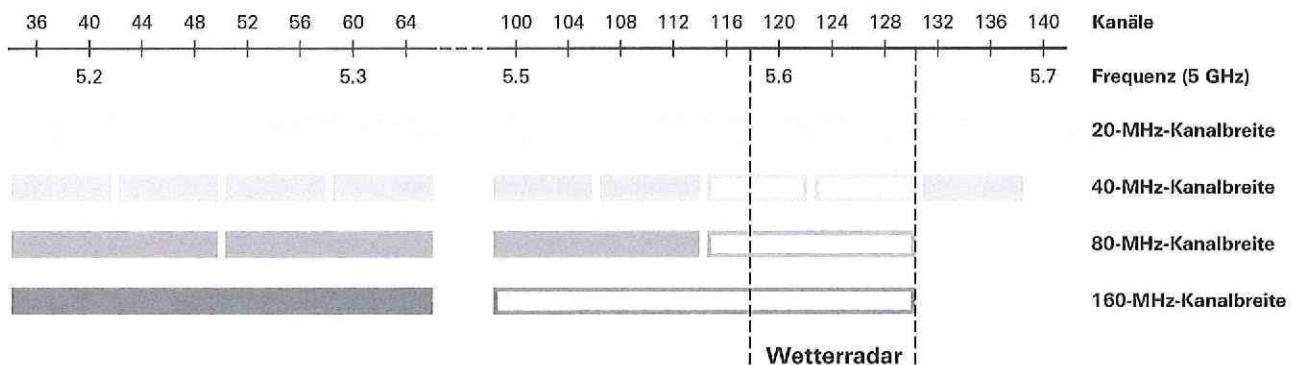


[1] In den USA und Japan sind es 14 Funkkanäle.

Im obigen Frequenzband gibt es nur drei **überlappungsfreie Kanäle** (1, 6 und 11). Alle anderen Kanäle (2 bis 5; 7 bis 10; 12 und 13) überschneiden sich. Wenn Sie allen Arbeitsstationen in einem WLAN einen überlappungsfreien Kanal zuweisen können, erzielen Sie jeweils die beste (höchste) Übertragungsleistung.

In einem **5-GHz-Frequenzband** kommen mehrere Kanäle mit unterschiedlichen Kanalbreiten zwischen 20 MHz und 160 MHz zum Einsatz. Durch diese Aufteilung wird eine höhere Übertragungskapazität erreicht. Damit eine WLAN-Komponente hier die zur Verfügung stehenden Kanäle nutzen kann, muss sie mit einer sogenannten **MIMO-Antenne** ausgerüstet sein. Vergleichen Sie dazu das Kapitel 6.2.2, S. 104.

[6-5] Kanalaufteilung im 5-GHz-Frequenzband



Quelle: elektronik-kompendium.de

### Hinweis

- ▷ Die Sendeleistung in den verschiedenen Kanälen des 5-GHz-Frequenzbands beträgt in Europa mehrheitlich 200 mW.

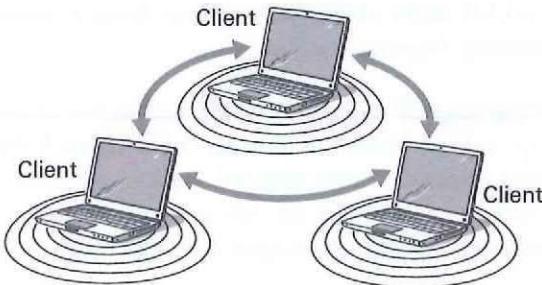
#### 6.1.1 Betriebsarten

Die Stationen in einem Funknetzwerk lassen sich auf verschiedene Arten zu einer sogenannten **Funkzelle** verbinden. Es lassen sich folgende **Betriebsarten** unterscheiden:

- **Ad-hoc<sup>[1]</sup>-Modus:** Bei diesem Modus kommunizieren die einzelnen WLAN-Stationen direkt miteinander, wobei jede Station einer Ad-hoc-Funkzelle selbstständig steuert, wer wie auf ihre Ressourcen zugreifen darf. Dieser Modus ist also mit einem Peer-to-Peer-Netzwerk vergleichbar. Der Ad-hoc-Modus empfiehlt sich vor allem für kleine (temporäre) Arbeitsgruppen und für Kleinstbetriebe mit zwei bis drei Mitarbeitenden ohne zentrale IT-Ressourcen. Für die Identifikation bzw. als Zellen-ID besitzt jede Ad-hoc-Funkzelle einen sogenannten **Independent Basic Service Set (IBSS)**.

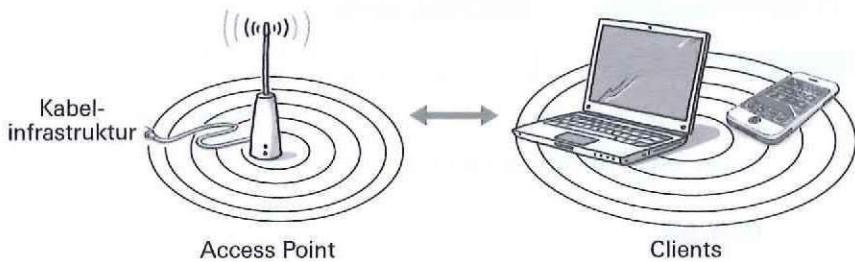
[1] Aus dem Lateinischen für: spontan, aus einer Situation heraus, aus dem Stegreif, nur für diesen Augenblick, nur für diese Gelegenheit.

[6-6] Ad-hoc-Funkzelle mit drei Teilnehmern



- **Infrastruktur-Modus:** Über diesen Modus wird eine Funkzelle mit der bestehenden Netzwerkinfrastruktur (Kabelnetzwerk) gekoppelt, wobei zur Koppelung jeweils **Access Point (AP)** eingesetzt wird. Der AP dient als Zugangspunkt zur «Kabelinfrastruktur» und hat somit für die einzelnen WLAN-Teilnehmer eine Brückenfunktion. Für die Identifikation bzw. als Zellen-ID besitzt jede Infrastruktur-Funkzelle einen sogenannten **Basic Service Set (BSS)** bzw. **Service Set Identifier (SSID)**.

[6-7] Infrastruktur-Funkzelle mit einem Access Point



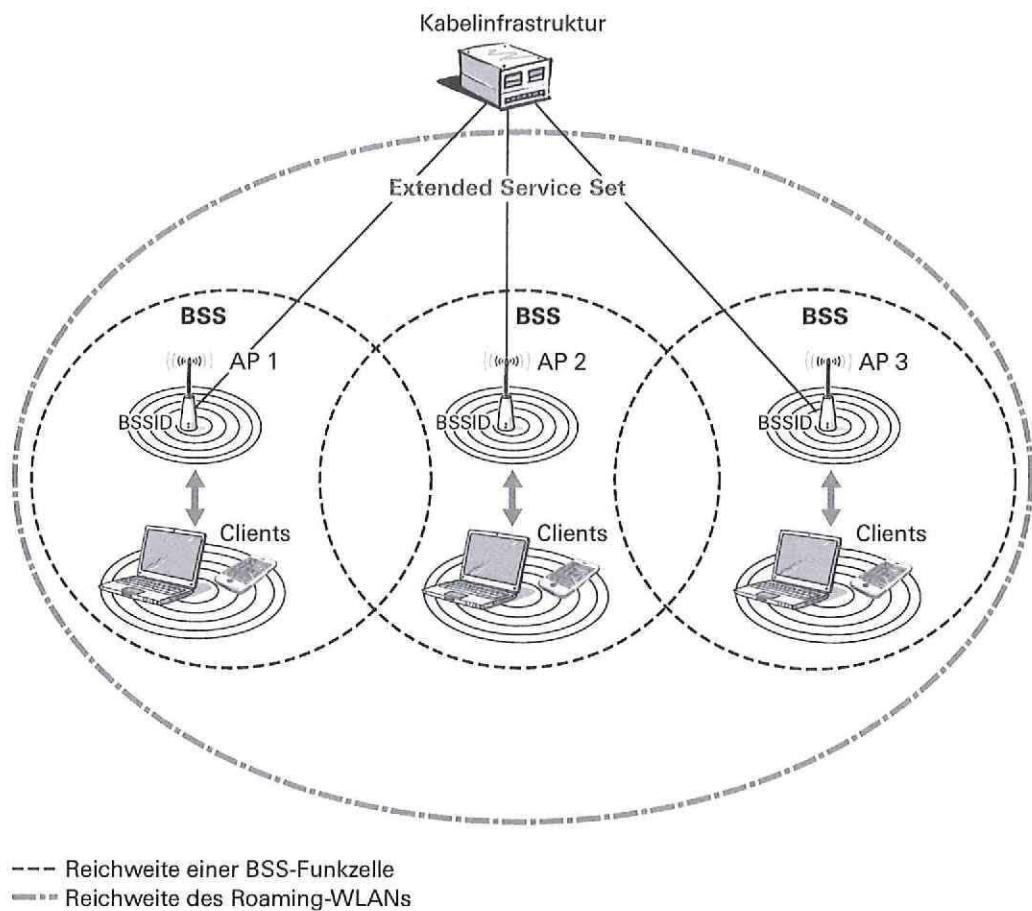
- **WLAN-Roaming<sup>[1]</sup>-Modus:** Muss ein Funknetzwerk grössere Flächen bzw. Räume abdecken (z. B. mehrere Stockwerke in einem Gebäude), können mehrere Access Points mit diesem Modus zu einem einheitlichen WLAN zusammengeschlossen werden. Der Vorteil einer solchen Infrastruktur besteht darin, dass sich WLAN-Teilnehmer innerhalb des **Roaming-Netzes** frei bewegen können. Im Grunde kommt beim Roaming also das gleiche Prinzip wie beim Mobiltelefon zum Tragen. Nimmt die Signalstärke der Funkzelle ab, in der sich ein Teilnehmer gerade befindet, versucht die WLAN-Station automatisch, eine Verbindung zur benachbarten Zelle mit einem stärkeren Funksignal herzustellen. Von diesem «**Hand over**»<sup>[2]</sup> sollte der Benutzer nichts mitbekommen. Der Roaming-Modus funktioniert nur dann, wenn sich die einzelnen Funkzellen genügend überlappen, sodass ein «**Hand over**» problemlos durchgeführt werden kann. Diese Betriebsart ist häufig an öffentlich zugänglichen Orten wie Hotels, Bahnhöfen oder Flughäfen anzutreffen. Die Zellen-ID eines Roaming-Netzes heisst **Extended Service Set (ESS)**, und diese umfasst immer mehrere BSS. Damit ein AP über die Kabelinfrastruktur angesprochen werden kann, muss dessen **Basic Service Set Identifier (BSSID)**<sup>[3]</sup> bekannt sein.

[1] Englisch für: streunen, herumwandern, herumstreifen, durchwandern, durchleiten.

[2] Englisch für: Übergabe an die nächste Funkzelle.

[3] Die BSSID entspricht der MAC-Adresse eines Access Point.

## [6-8] WLAN-Roaming mit drei Access Points

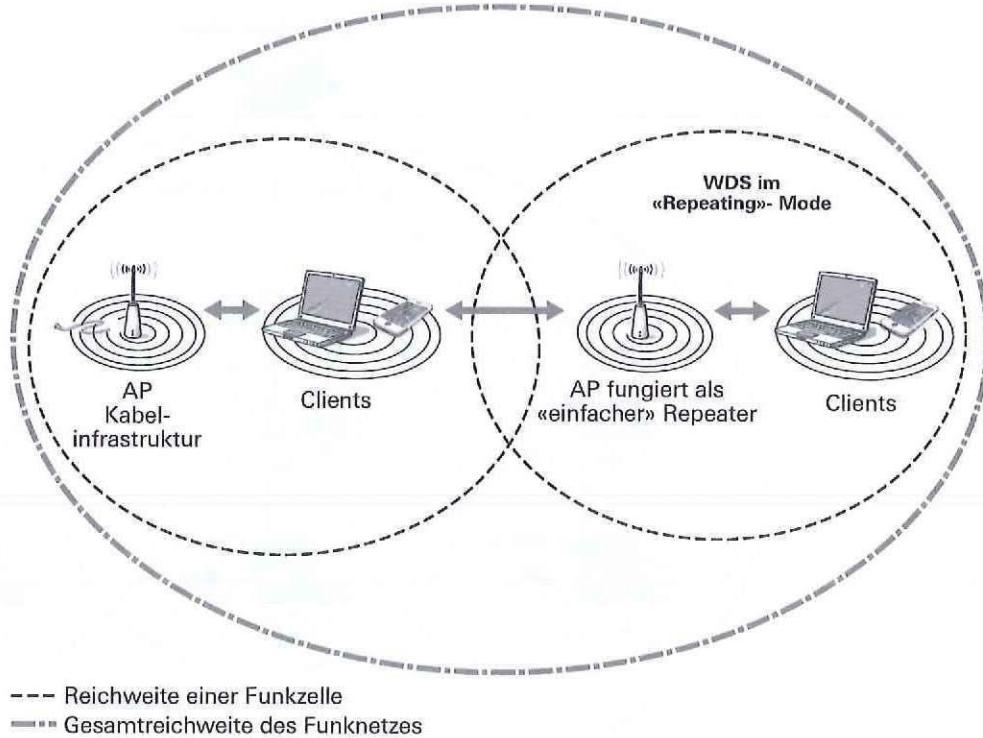
**Hinweis**

- ▷ Beim Aufbau eines Roaming-Funknetzwerks empfiehlt es sich, jeweils Access Points vom gleichen Typ und vom gleichen Hersteller zu verwenden. Der Grund: Häufig werden proprietäre Funktionen implementiert (z. B. zur Leistungssteigerung), die die Interoperabilität<sup>[1]</sup> zwischen WLAN-Komponenten unterschiedlicher Hersteller erschweren oder sogar verunmöglichen.
- **WDS<sup>[2]</sup>-Repeating-Modus:** Reicht die Signalstärke einer Funkzelle nicht aus, um alle Clients zu erreichen, kann ein WLAN mithilfe dieser Betriebsart relativ einfach erweitert werden. Diverse WLAN-Komponenten lassen sich in diesem Modus betreiben, wobei die betreffende Komponente dann «nur» noch als **Repeater** arbeitet. Wird z. B. ein Access Point im Repeating-Modus betrieben, kann sich kein WLAN-Client mehr bei diesem anmelden. Die einzige Funktion des AP in dieser Situation ist die Weiterleitung der Datenpakete von einer Funkzelle zur anderen Funkzelle.

[1] Fremdwort für: Fähigkeit zur Zusammenarbeit.

[2] Abkürzung für: Wireless Distribution System. Englisch für: drahtloses Verteilsystem (wörtl.).

## [6-9] Erweiterte Funkzelle mittels WDS-Repeater



## 6.2 Komponenten und Antennen

Im Folgenden lernen Sie gängige Komponenten und Antennen für das WLAN sowie deren Einsatzmöglichkeiten kennen. Je nachdem, welches Gerät Sie auswählen bzw. einsetzen, wirkt sich dies auf die Effizienz und Leistung des Funknetzes aus.

### 6.2.1 WLAN-Komponenten und Funktionen

Im Folgenden werden die wichtigsten **WLAN-Komponenten** mit ihren **Hauptaufgaben** näher vorgestellt:

- **Access Point:** Ein WLAN-AP gewährleistet den zentralen Verbindungspunkt den Zugang der WLAN-Clients in eine kabelbasierte Netzwerkinfrastruktur. Dieses Gerät stellt somit das Pendant zum Switch innerhalb eines Kabelnetzwerks dar und bietet üblicherweise folgende Funktionen:
  - Authentifizierung der Zugriffe auf die Kabelinfrastruktur mittels IEEE 802.1X und RADIUS
  - Weitere Sicherheitsüberprüfungen wie z. B. die Zugangsprüfung anhand der MAC-Adresse eines Systems
  - Zuteilung von IP-Adressen an die WLAN-Clients mittels integrierten DHCP-Servers
  - Verschlüsselung des Datenaustauschs zwischen AP und WLAN-Clients mittels kryptografischer Funktionen
  - Bereitstellung unterschiedlicher Betriebsarten. Vergleichen Sie dazu das Kapitel 6.1.1, S. 99

[6-10] Access Point (Beispiel mit MIMO-Antenne)



- **Netzwerkkarte:** Eine **WLAN-Netzwerkkarte (WLAN-NIC)** dient zur Übertragung der Daten mittels Funk. Bei der Beschaffung einer WLAN-NIC muss darauf geachtet werden, dass die Netzwerkkarte die Standards des betreffenden Access Point unterstützt. Nachfolgend sehen Sie verschiedene Bauformen solcher Netzwerkkarten:

[6-11] WLAN-Netzwerkkarten



Quelle: [dlink.com](http://dlink.com)

- **Repeater:** Ein WLAN-Repeater dient zur Erweiterung der Funkzelle eines WLANs. Zu diesem Zweck leitet er die von einem WLAN-Client empfangenen Daten an den Access Point weiter. Auch diese sind in verschiedenen Bauformen erhältlich:

[6-12] WLAN-Repeater

Quelle: [avm.de](http://avm.de)Quelle: [netgear.com](http://netgear.com)

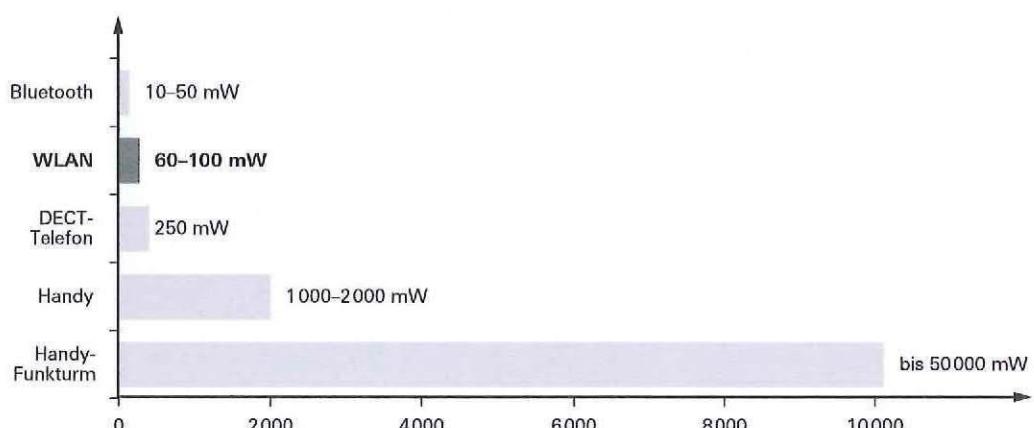
### 6.2.2 WLAN-Antennen und Sendeleistung

Die Auswahl an Antennen für WLAN-Komponenten ist riesig. Doch bei aller Vielfalt an Bauformen und Leistungen stehen bei jeder **Funkantenne** folgende **Ziele** im Vordergrund:

- Hohe Reichweite der Funksignale gewährleisten
- Hohe Abdeckungsgenauigkeit der Funksignale gewährleisten

Je mehr **Sendeleistung** zur Verfügung steht, desto höher ist generell auch die Reichweite der gesendeten Funksignale. Dennoch haben die WLAN-Komponenten nur eine beschränkte Sendeleistung. Der Grund: Wären in den frei zugänglichen Frequenzbereichen unbeschränkte Sendeleistungen erlaubt, würde dies zwar für einige Funknetzwerke hohe Reichweiten bedeuten, aber nur wenige Benutzer könnten überhaupt ein WLAN betreiben, da es an freien Sendeplätzen mangelt. In der folgenden Grafik sehen Sie die maximale Sendeleistung von WLAN-Komponenten im Vergleich zu anderen Funksystemen.

[6-13] Maximal erlaubte Sendeleistungen für verschiedene Funksysteme

Quelle: [hrz.tu-darmstadt.de](http://hrz.tu-darmstadt.de)

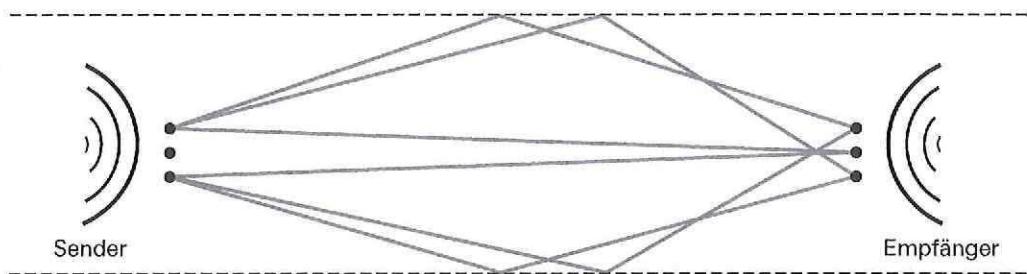
## Rundstrahl-Antenne

Damit trotz dieser Beschränkung eine möglichst hohe Reichweite erzielt werden kann, werden WLAN-Systeme häufig mit einer **Rundstrahl-Antenne**<sup>[1]</sup> aus- bzw. nachgerüstet, mit der sich die Sendeleistung erheblich steigern lässt. Eine reguläre Rundstrahl-Antenne erlaubt z. B. eine Verdoppelung der Sendeleistung einer WLAN-Komponente.

## MIMO-Technik

Bei der **MIMO**<sup>[2]</sup>-Technik werden mehrere Sende- und Empfangsantennen genutzt, um höhere Datenübertragungsraten als herkömmliche WLAN-Systeme zu erreichen. Das bedeutet, dass durch mehrere Sende- und Empfangsantennen die Übertragungsleistung dank der gleichzeitigen, parallelen Übertragung auf verschiedenen Frequenzen deutlich gesteigert werden kann. Folgende Grafik soll diesen Sachverhalt verdeutlichen:

[6-14] MIMO-Technik (Funktionsprinzip)



## Dämpfung durch Widerstand

Neben der Art und Anzahl der eingesetzten WLAN-Antennen spielen bezüglich der Sendeleistung auch das Kabel und der Stecker eine wichtige Rolle, mit denen ein Access Point angeschlossen wird. Jeder Leiter weist einen elektrischen Widerstand<sup>[3]</sup> auf, der von dessen Material, Durchmesser, Länge, Temperatur und anderen Faktoren abhängt. Der Widerstand der verwendeten **Kabel- und Steckverbindungen** dämpft (verringert) die Sendeleistung in einem WLAN-System. Im Extremfall kann diese Dämpfung bis zu –0.5 db Leistungsverlust pro Meter Kabellänge bedeuten. Deshalb ist es von grosser Bedeutung, welche Antennenkabel und welche Stecker für die Verbindung zwischen dem Access Point und der Antenne eingesetzt werden.

[1] Auch: Omni-Antenne bzw. Omni-Strahler.

[2] Abkürzung für: Multiple Input, Multiple Output. Englisch für: mehrfacher (Signal)eingang, mehrfacher (Signal)ausgang.

[3] Fachbegriff: Ohmscher Widerstand.

### 6.2.3 Positionierung

Bei der Installation von Funkantennen und Access Points müssen diese so positioniert werden, dass sich die ausgestrahlten Signale möglichst ohne Hindernisse ausbreiten können. Weiter sollten Sie darauf achten, dass nur derjenige Raum «ausgeleuchtet» bzw. diejenige Fläche abgedeckt wird, die vom WLAN wirklich beansprucht wird. Dies ist keine einfache Aufgabe, da sich einmal ausgesendete Funksignale nicht (um)lenken lassen. Beachten Sie daher bei der **Positionierung** von Sendeanlagen und Access Points folgende **Regeln**:

- **Sicherheit gewährleisten:** Die von einer Funkantenne gesendete Energie sollte in das Innere eines Raums bzw. Gebäudes gerichtet werden. Der Grund: Nach innen gerichtete Signale werden i. d. R. rasch absorbiert. Ungerichtete Funksignale können dagegen bei ungünstigen Bedingungen im Umkreis von mehreren Hundert Metern außerhalb eines Raums bzw. Gebäudes noch empfangen werden, da sie sich unkontrolliert ausbreiten.
- **Funkstörungen und Interferenzen vermeiden:** Um eine freie Ausbreitung und einen freien Empfang der Funksignale zu ermöglichen, sollten Sie einen AP möglichst hoch installieren (z. B. an der Wand oder an der Decke). Werden im gleichen Raum weitere elektronische Geräte genutzt, müssen Sie die Gefahr von Interferenzen<sup>[1]</sup> berücksichtigen. Stellen Sie daher eine Funkantenne oder einen AP nie direkt neben ein Schnurloses Telefon, neben ein Radio oder neben bzw. auf einen Lautsprecher. Vermeiden Sie auch Installationen auf metallischen Oberflächen oder in der Nähe von Mikrowellengeräten. Wandantennen mit einer Richtwirkung von höchstens 160 Grad können dagegen auch auf metallischen Oberflächen installiert werden, da die Sendeleistung nur nach vorne abgegeben wird.

#### Hinweis

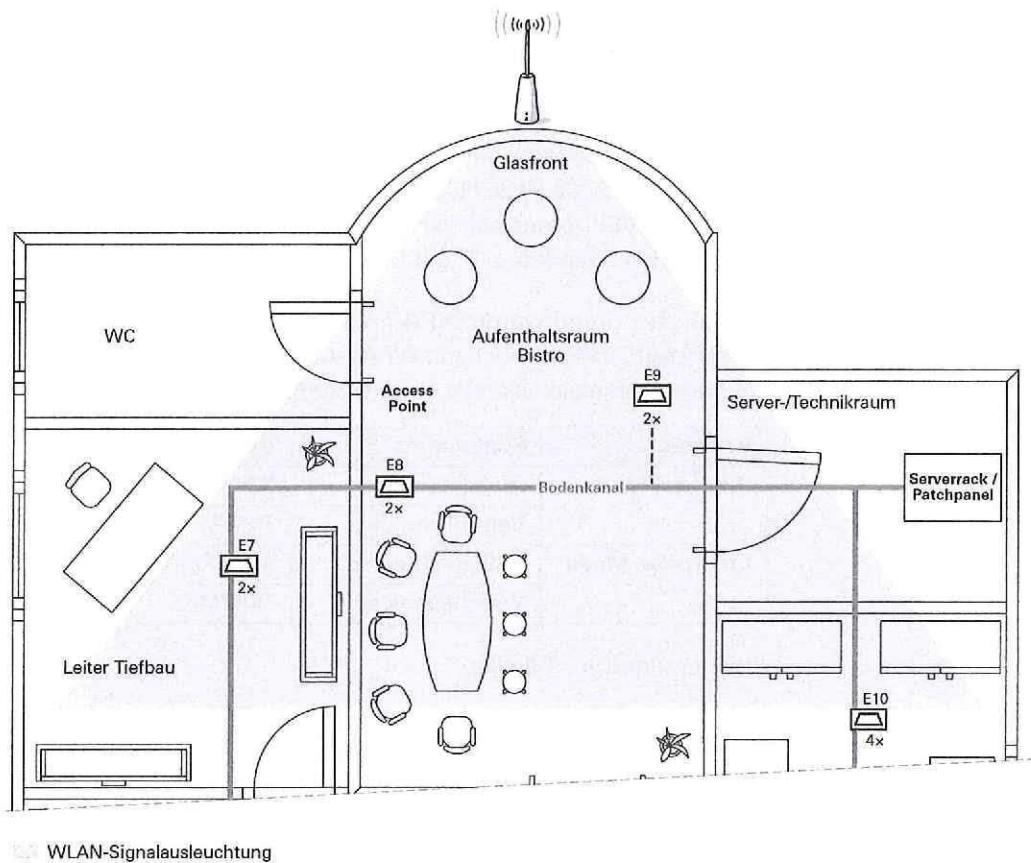
- ▷ Bei komplexeren WLAN-Installationen leisten geeignete Werkzeuge nützliche Dienste. Mit dem Gratis-Tool «HeatMapper» können Sie z. B. herausfinden, an welchem Standort ein WLAN-Router die beste Leistung bringt. Vergleichen Sie dazu: [www.ekahau.com](http://www.ekahau.com).

Im Fallbeispiel der Firma Caprez AG wird am Hauptsitz in Chur der obere Bereich der Glasfront als optimale Position für den Access Point bestimmt. Um eine optimale «Signalausleuchtung» zu erreichen, kommt ein AP mit einer gerichteten Indoor-Wandantenne und einem Abstrahlwinkel<sup>[2]</sup> von 120 Grad zum Einsatz. Mit dieser Positionierung und Ausstattung wird sichergestellt, dass kaum Funksignale nach aussen gelangen.

[1] Überlagerungsscheinungen, die beim Zusammentreffen elektromagnetischer Wellen auftreten können.

[2] Horizontal und vertikal.

[6-15] Positionierung des Access Point (Beispiel)



### 6.3 WLANs sicher betreiben

Das Thema **Sicherheit bei Funknetzwerken** ist besonders brisant, weil zum Abhören der Datenübertragung lediglich Funksignale empfangen werden müssen. Ein unerwünschter Mithörer oder ein unberechtigter Eindringling kann sich also einfach in den Empfangsbereich eines WLAN begeben und dort sein Empfangsgerät einschalten. Ein betriebliches WLAN muss daher gegenüber folgenden **Sicherheitsrisiken** geschützt werden:

- Unerlaubtes Abhören der Datenübertragung innerhalb des WLANs
- Unerlaubter Zugriff auf die IT-Systeme des Unternehmens mithilfe des WLANs

Um diese Risiken zu reduzieren, können Sie diverse **Sicherheitsmaßnahmen** ergreifen, die im Folgenden ausführlicher beschrieben werden.

### 6.3.1 Datenverkehr verschlüsseln

Zu Beginn dieses Jahrhunderts wurde noch weitgehend **Wired Equivalent Privacy (WEP)** eingesetzt, um den Datenverkehr in WLANs zu verschlüsseln. Inzwischen gilt WEP als unsichere Verschlüsselungsmethode und sollte nicht mehr eingesetzt werden. Seit dem Jahr 2013 wird WEP auch nicht mehr in WLAN-Komponenten integriert. IEEE entwickelte daher zusammen mit Wi-Fi Alliance<sup>[1]</sup> den Sicherheitsstandard 802.11i. Zuvor hatte Wi-Fi Alliance bereits die Verschlüsselungsmethode **Wi-Fi Protected Access (WPA)** als Nachfolger von WEP vorgestellt. WPA erfüllte aber der Vorgaben des Standards 802.11i nur teilweise und verwendete z. B. mit RC4<sup>[2]</sup> die gleiche Verschlüsselungsroutine wie WEP.

Aus diesem Grund wurde **WPA** im Jahr 2006 durch **WPA2** abgelöst und Access Points werden seit 2014 nur noch mit WPA2-AES ausgeliefert. In der folgenden Tabelle finden Sie wichtige Merkmale einander gegenübergestellt:

Variante	Funktion	WPA	WPA2
<b>Personal Mode</b>	Authentifizierung	PSK	PSK
	Verschlüsselung	TKIP/MIC	AES-CCMP
<b>Enterprise Mode</b>	Authentifizierung	802.1X/EAP	802.1X/EAP
	Verschlüsselung	TKIP/MIC	AES-CCMP

Erläuterungen zur Tabelle:

- **Personal Mode:** geeignet für kleinere Installationen bzw. Umgebungen mit wenigen WLAN-Systemen.
- **Enterprise Mode:** geeignet für grosse WLAN-Infrastrukturen mit zahlreichen WLAN-Systemen.
- **PSK:** Abkürzung für: Pre-Shared Key. Vordefinierter Schlüssel zur Authentifizierung der WLAN-Benutzer.
- **TKIP:** Abkürzung für: Temporal Key Integrity Protocol. Sicherheitsprotokoll mit dem (veralteten) Verschlüsselungsalgorithmus RC4. Wird seit 2011 in Access Points nicht mehr unterstützt.
- **MIC:** Abkürzung für: Message Integrity Check. Verfahren zur Prüfung der Datenintegrität. Analysiert, ob eine Nachricht von Unbefugten verändert wurde.
- **AES:** Abkürzung für: Advanced Encryption Standard. Gilt zurzeit als eine der sichersten, frei erhältlichen Verschlüsselungsroutinen. Ermöglicht Schlüssellängen von 128, 192 und 256 Bit. 192-Bit-Schlüssel werden von US-amerikanischen Regierungsbehörden als Standardverschlüsselung vorgeschrieben.
- **CCMP:** Abkürzung für: Counter Mode with Cipher Block Chaining Message Authentication Code Protocol. Auf AES basierendes Authentifizierungs- und Verschlüsselungsprotokoll mit 128-Bit-Schlüssel-Länge.
- **EAP:** Abkürzung für: Extensible Authentication Protocol. Ein von IETF<sup>[3]</sup> entwickeltes Authentifizierungsprotokoll (RFC 3748).

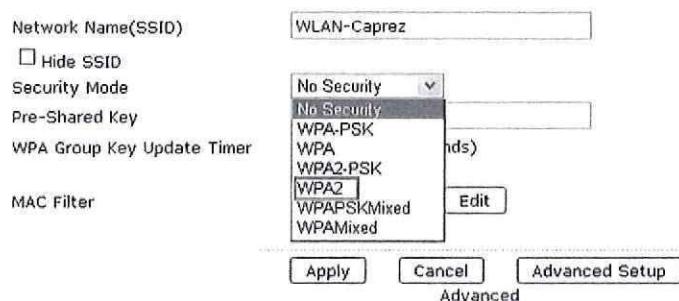
Die nachfolgenden Konfigurationseinstellungen beziehen sich auf den im obigen Verkabelungsplan eingezeichneten Access Point. Über diesen AP im Aufenthaltsraum Bistro sollen Mitarbeitende und Gäste der Firma Caprez Ingenieure AG **direkten Zugriff auf das (untrusted) Internet**, jedoch **keinen Zugriff auf das (trusted) LAN** des Unternehmens erhalten.

[1] Internationale Non-Profit-Organisation zur Förderung und Standardisierung drahtloser Netzwerke (gegründet 1999).

[2] Veralteter Verschlüsselungsstandard, der heute als unsicher gilt und nicht mehr verwendet wird.

[3] Abkürzung für: Internet Engineering Task Force. Arbeitsgruppe zur Weiterentwicklung der Internetprotokolle.

## [6-16] Einstellung des Security Mode bei Zyxel NWA1100-N (Beispiel)



In unserem Fallbeispiel wird mit der Option «WPA2» im Auswahlfeld «**Security Mode**» die höchste Sicherheitsstufe erreicht. Unter Umständen unterstützen ältere WLAN-fähige PCs noch nicht WPA2, sondern nur WPA. Dies betrifft vor allem PCs, WLAN-APs und WLAN-Karten, die vor dem Jahr 2007 hergestellt wurden. WLAN-Komponenten ab dem Jahr 2010 sollten alle WPA2 unterstützen.

**Hinweis**

- ▷ Ändern Sie die Default-Werte (Standardeinstellungen) der Sicherheitskonfiguration nur dann, wenn Sie die Auswirkungen einer Änderung genau kennen. Ziehen Sie in Zweifelsfällen die technische Dokumentation des AP zurate.

### 6.3.2 Benutzer und Systeme authentifizieren

Der Access Point nimmt eine erste Authentifizierung der Benutzer bzw. Systeme mittels PSK vor. Um sicherzustellen, dass nur bestimmte Benutzer bzw. Systeme auf ein WLAN zugreifen können, stellen die meisten Access Points zusätzlich folgende **Optionen** bereit:

- **Authentifizierung mittels 802.1X:** Diese Option erlaubt eine zuverlässige und bequeme Authentifizierung auf der Basis von IEEE 802.1X und mittels eines RADIUS-Servers. Die Vorteile: Der Verschlüsselungsstandard kennt bezüglich der Anzahl der Objekte (Benutzer bzw. Systeme) kaum Grenzen, gewährleistet eine sichere Datenübertragung und kann auf Benutzerinformationen aus anderen Systemen zurückgreifen.
- **Authentifizierung mittels MAC-Filter:** Für die Nutzung dieser Option müssen Sie beim Access Point MAC-Adressen für die Authentifizierung hinterlegen. Dabei ist zu beachten, dass die Anzahl der möglichen Einträge in den Filtertabellen auf den handelsüblichen Access Points relativ gering ist. Zudem kann die Verwaltung der MAC-Adressen schnell aufwendig werden, wenn viele Benutzer bzw. Systeme zu erfassen sind. Als Netzwerkadministrator müssen Sie laufend darüber informiert sein, welches System ausgewechselt oder neu in Betrieb genommen wird. Ein weiterer Nachteil dieser Funktion besteht darin, dass ein Angreifer innerhalb kurzer Zeit eine gültige MAC-Adresse ausfindig machen kann, da diese Information unverschlüsselt versendet wird. Aus diesen Gründen ist es fraglich, ob diese Option den gewünschten Sicherheitsgewinn bringt.
- **Authentifizierung mittels lokaler Benutzerkonten:** Für die Nutzung dieser Option müssen Sie beim Access Point lokale Benutzerkonten für die Authentifizierung hinterlegen. In der Folge müssen sich die betreffenden Benutzer beim Zugriff auf das WLAN mittels Kennwort und Passwort anmelden. Ein solches WLAN-Log-in beim AP ist allerdings nur in kleinen Netzwerken sinnvoll, da Benutzerkonten i. d. R. bereits beim Verzeichnisdienst eingerichtet werden. Als Netzwerkadministrator sind Sie daran interessiert, den Verwaltungsaufwand möglichst gering zu halten und Benutzerkonten an einem zentralen Ort zu pflegen.

[6-17] Authentifizierung mittels MAC-Filter (links) und lokaler Benutzerkonten (rechts)

Wireless LAN- MAC-Filter			Wireless LAN - LAN-Benutzer				
Aktiviert	Ja	Aktion	Zuordnung ermöglichen	#	Aktiviert	Benutzername	Kennwort
MAC-Adresse							
1	00:60:b3:66:07:f4	2	00:60:b3:74:ba:b8	1	✓	BigBoss	oooooooooo
3	00:60:b3:73:3b:fb	4	00:a0:c5:40:62:eb	2	✓	LittleBoss	oooooooooo
5	00:ba:be:fa:ce:00	6	7a:09:65:2d:01:aa	3	✓	Lehrling	oooooooooo
7	00:00:00:00:00:00	8	00:00:00:00:00:00	4	✓	Prokurist	oooooooooo
9	00:00:00:00:00:00	10	00:00:00:00:00:00	5	✓	Marketing	oooooooooo
11	00:00:00:00:00:00	12	00:00:00:00:00:00	6			
13	00:00:00:00:00:00	14	00:00:00:00:00:00	7			
15	00:00:00:00:00:00	16	00:00:00:00:00:00	8			
17	00:00:00:00:00:00	18	00:00:00:00:00:00	9			
19	00:00:00:00:00:00	20	00:00:00:00:00:00	10			
21	00:00:00:00:00:00	22	00:00:00:00:00:00	11			
23	00:00:00:00:00:00	24	00:00:00:00:00:00	12			
25	00:00:00:00:00:00	26	00:00:00:00:00:00	13			
27	00:00:00:00:00:00	28	00:00:00:00:00:00	14			
29	00:00:00:00:00:00	30	00:00:00:00:00:00	15			
31	00:00:00:00:00:00	32	00:00:00:00:00:00	16			
Zurück Anwenden Abbrechen				Zurück Anwenden Abbrechen			

- Authentifizierung mittels Pre-Shared Key (PSK): In vielen Fällen wird mittels PSK überprüft, ob ein Benutzer oder ein System auf das WLAN zugreifen darf. Wenn der Zugriff auf das WLAN nicht nur den Mitarbeitenden, sondern auch den Gästen einer Firma erlaubt werden soll, können Sie auf die Definition eines PSK verzichten. Für unser Fallbeispiel könnten die entsprechenden Einstellungen so aussehen:

[6-18] PSK-Einstellung für Gäste und Mitarbeitende (links) sowie nur für Mitarbeitende (rechts)

Security Mode	WPA2-PSK	Security Mode	WPA2-PSK
Pre-Shared Key	Internet-Caprez	Pre-Shared Key	PoB\$Y%AQ?cV-
WPA Group Key Update Timer	1800 (In Seconds)	WPA Group Key Update Timer	1800 (In Seconds)

### Hinweis

▷ Unter bestimmten Umständen kann ein PSK auch unter WPA2 «ausgespäht», d. h. während der Datenübertragung abgefangen werden. Ein PSK sollte daher möglichst schwierig zu «knacken» sein. Dabei gelten die gleichen Faustregeln wie beim Passwort: Definieren Sie einen PSK, der möglichst nicht zu erraten ist, und verwenden Sie dafür eine Kombination aus Buchstaben, Sonderzeichen und Ziffern. Sie können die Sicherheit eines PSK ggf. mithilfe des Passwortcheck-Tools des Datenschutzbeauftragten des Kantons Zürich<sup>[1]</sup> überprüfen.

### 6.3.3 Gefährliche Access Points blockieren

Ein «Rogue<sup>[2]</sup> Access Point» ist ein gefährlicher AP, der ohne explizite Bewilligung des Netzwerkadministrators in ein sicheres Firmennetzwerk eingebunden oder speziell dafür eingerichtet wurde, Man-in-the-middle-Attacken durchzuführen.<sup>[3]</sup> Ein solcher Access Point kann die Kommunikation eines WLAN-Clients (Opfer) auf einen anderen, bösartigen

[1] Vergleichen Sie dazu: <https://www.passwortcheck.ch>.

[2] Englisch für: Schurke, Schlingel, aggressiver Einzelgänger.

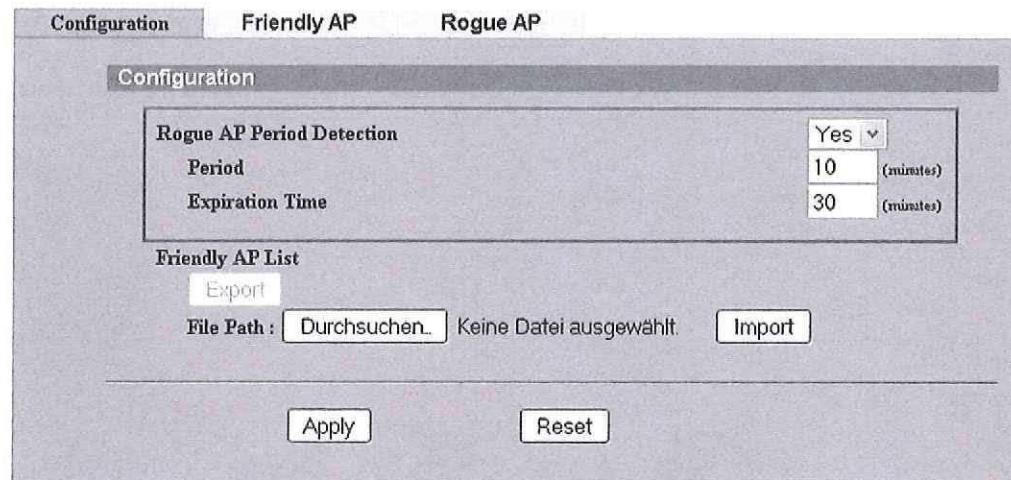
[3] Vergleichen Sie zu MITM-Attacken das Kapitel 5.2.4, S. 90.

Access Point (Angreifer) umleiten und stellt für Unternehmen eine grosse Sicherheitsbedrohung dar.

Acess Points können aber auch erkennen, ob die empfangenen Funksignale direkt von einem WLAN-Client stammen oder über einen anderen, ggf. bösartigen AP umgeleitet worden sind. Zur Aufdeckung eines Rouge Access Point muss allerdings die entsprechende **Abwehrfunktion** aktiviert werden. Hier entsprechendes Konfigurationsbeispiel:

[6-19] Funktion zur Erkennung eines Rogue AP (Zyxel NWA-3165-N)

## ROGUE AP DETECTION



Erläuterungen zum Screenshot:

- Im Eingabefeld «**Period**» können Sie festlegen, in welchen Zeitabständen der Datenstrom automatisch nach einem Rogue AP untersucht werden soll. Da solche Analysen die Rechenkapazität eines AP stark belasten, sollten die Intervalle nicht zu kurz ausfallen. Bedenken Sie, dass die Prozessoren der meisten APs eine geringere Leistungsfähigkeit aufweisen als die CPUs eines PCs oder Servers.
- Im Eingabefeld «**Expiration Time**» können Sie festlegen, wie lange ein entdeckter Rogue AP als WLAN-Client geblockt werden soll. Üblicherweise wird diese Zeitspanne in Minuten eingegeben. Auch wenn eine Blockierung über mehrere Tage oder Wochen möglich ist, sollten Sie hier zurückhaltend sein und bedenken, dass auch ein Fehlalarm<sup>[1]</sup> vorkommen kann und der Ausschluss eines sicheren WLAN-Clients über einen längeren Zeitraum in solchen Fällen nicht wünschenswert ist. Begrenzen Sie die Blockade also auf ein vernünftiges Mass.
- Unter dem Register «**Friendly AP**» können Sie die APs erfassen, die zum WLAN der Firma gehören und autorisiert worden sind, WLAN-Datenpakete weiterzuleiten.
- Unter dem Register «**Rogue AP**» werden die APs aufgeführt, die als bösartig entdeckt bzw. eingestuft wurden.

### 6.3.4 Ein WLAN vom restlichen Netzwerk abgrenzen

Eine wirksame Sicherheitsmaßnahme besteht darin, risikobehaftete Bereiche des Firmennetzwerks von vertrauenswürdigen oder sensitiven Netzwerkbereichen zu trennen. Überlegen Sie daher immer, inwiefern das WLAN für Ihre Firma ein Sicherheitsrisiko darstellt.

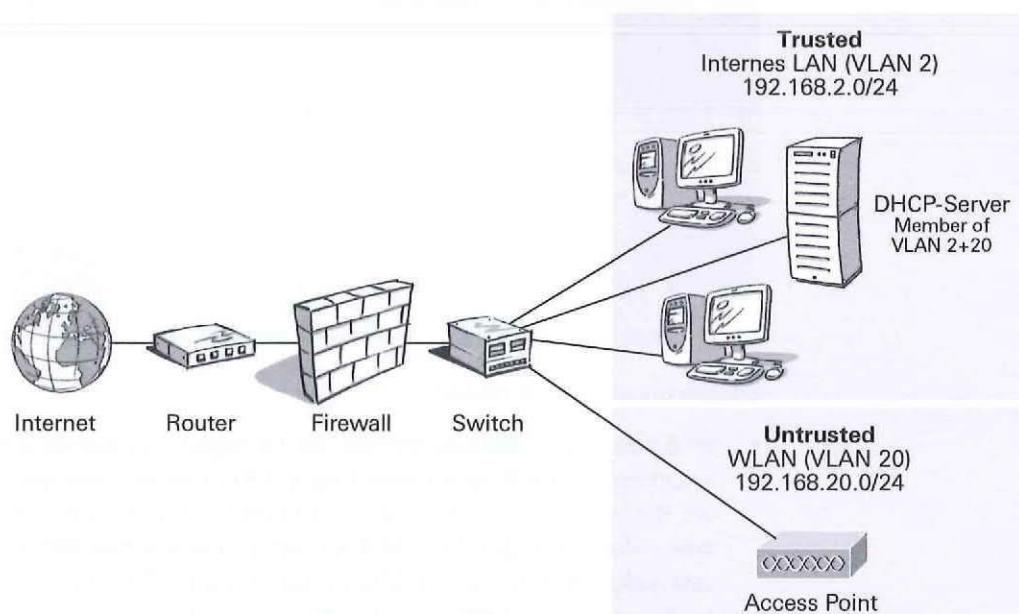
[1] Englischer Fachbegriff: False Positives.

**Beispiel**

In unserem Fallbeispiel sollen nicht nur die Mitarbeitenden der Firma Caprez Ingenieure AG über das WLAN auf das Internet zugreifen können, sondern auch die Gäste und Besucher bzw. deren Systeme wie z. B. deren Notebooks, Laptops, Tablet-PCs oder Smartphones. Da Sie als Netzwerkadministrator i. d. R. keine Kenntnisse über den Sicherheitsstandard solcher «Fremdsysteme» haben, müssen Sie das WLAN generell als «untrusted» (nicht vertrauenswürdig) einstufen. Oft wissen nicht einmal die Benutzer selbst, ob ihr System vertrauenswürdig ist oder schädliche Software wie z. B. Viren oder Hackerprogramme beinhaltet.

Handeln Sie also konsequent nach dem Motto «Vertrauen ist gut, Kontrolle ist besser» und grenzen Sie das WLAN vom restlichen Netzwerk der Firma ab. Dies geschieht am einfachsten mithilfe eines separaten **VLANs für das WLAN**, das einen sicheren Internetzugang ermöglicht. Folgende Grafik soll den Aufbau eines solchen Netzwerks veranschaulichen:

[6-20] WLAN mittels VLAN vom LAN abgrenzen (Prinzipschema)



### 6.3.5 Dienste und Funktionen deaktivieren

Eine weitere hilfreiche Sicherheitsmaßnahme besteht darin, ungenutzte Dienste und unnötige Funktionen zu deaktivieren. Die Entfernung aller Softwarekomponenten, die zur Erfüllung der vorgesehenen Aufgaben bzw. Geschäftsprozesse nicht zwingend notwendig sind, wird als **Hardening**<sup>[1]</sup> bezeichnet. Ob genutzt oder ungenutzt – Dienste und Funktionen bergen immer ein gewisses Sicherheitsrisiko, insbesondere für externe Angriffe.

#### Dienste prüfen und ggf. deaktivieren

Diskutieren und entscheiden Sie zusammen mit Ihren Vorgesetzten, welche Dienste auf welcher WLAN-Komponente unbedingt notwendig sind und aktiv bleiben müssen. Alle anderen Dienste sollten Sie nach Möglichkeit deaktivieren. Nachfolgend werden wichtige **Netzwerkdienste** kurz beschrieben, die bei einem Access Point normalerweise aktiv sind:

[1] Englisch für: Härt(en).

- **DHCP (Dynamic Host Configuration Protocol):** automatische Zuweisung einer IP-Adresskonfiguration an ein vernetztes System. Ermöglicht die Zuordnung von IP-Adressen zu den WLAN-Clients. In unserem Fallbeispiel kann dieser Dienst ausgeschaltet werden, weil die WLAN-Clients ihre IP-Adressen vom internen DHCP-Server erhalten.
- **SNMP (Simple Network Management Protocol):** Netzwerkprotokoll zur Verwaltung und Überwachung von IT-Systemen. Vergleichen Sie dazu das Kapitel 4.2, S. 55.
- **SSH (Secure Shell):** Netzwerkprotokoll für den sicheren Zugriff auf ein entferntes System. Die gesamte Kommunikation über das Netzwerk wird verschlüsselt abgewickelt.
- **Telnet:** Vorgänger von SSH. Netzwerkprotokoll, das den Zugriff auf ein entferntes System erlaubt. Da bei Telnet die Datenübertragung nicht verschlüsselt wird, sollte nur noch SSH eingesetzt werden.
- **TFTP (Trivial File Transfer Protocol):** sehr einfach gehaltenes Netzwerkprotokoll für den Transfer von Dateien. Wird meist für den Versand von Konfigurations- und Systemdateien verwendet.
- **WWW (World Wide Web):** ermöglicht den Fernzugriff auf Systeme via Webbrowser für Administrationszwecke.

Nachfolgend sehen Sie beispielhaft, wie der interne Webserver eines Access Point für **Fernzugriffe über den Webbrowser konfiguriert** werden kann:

[6-21] Konfiguration des internen Webservers (Zyxel NWA-3165-N)

#### REMOTE MANAGEMENT

The screenshot shows the 'REMOTE MANAGEMENT' configuration page. It has tabs for TELNET, FTP, WWW (selected), and SNMP. Under the WWW tab, there are two sections: 'WWW' and 'HTTPS'. In the 'WWW' section, the 'Server Port' is set to 51080, 'Server Access' is LAN, and 'Secured Client IP Address' is 0.0.0.0. In the 'HTTPS' section, the 'Server Certificate' dropdown is set to 'auto-generated\_self\_signed\_cert' (See My Certificates). The 'Authenticate Client Certificates (See Trusted CAs)' checkbox is unchecked. The 'Server Port' is set to 51443, 'Server Access' is LAN, and 'Secured Client IP Address' is 0.0.0.0. At the bottom are 'Apply' and 'Reset' buttons.

Im obigen Beispiel wurden aus Sicherheitsgründen folgende Einstellungen vorgenommen:

- Die Standardkonfiguration<sup>[1]</sup> der **Server Ports** wurden geändert. Der ursprüngliche Wert im Bereich WWW (für http) wurde von 80 auf 51080 geändert. Der ursprüngliche Wert für https wurde von 443 auf 51443 geändert. Ein solches «Umlegen der Default-ports» auf andere Port-Nummern wird auch «Security through obscurity»<sup>[2]</sup> genannt.
- Unter «**Server Access**» wurde sowohl für **http** als auch für **https** festgelegt, dass nur vom LAN (in unserem Fall vom Subnetz 192.168.2.0 aus) auf den internen Webserver zugegriffen werden kann. Diese Einstellung sollte bei allen Netzwerkdiensten eines AP vorgenommen werden, um das Risiko externer Attacken zu senken.
- Unter «**Secured Client IP Address**» können Sie einschränkend festlegen, von welcher IP-Adresse bzw. von welchem System aus auf diesen AP zugegriffen werden darf.

[1] Synonyme: Standardeinstellungen, Default-Werte.

[2] Englisch für: Sicherheit durch Unklarheit, Verdunkelung, Vernebelung (wörtl.).

## Hinweis

- ▷ Da sich der LAN-Anschluss des AP bei der Firma Caprez Ingenieure AG im VLAN befindet und nur der DHCP-Server Mitglied in diesem VLAN ist, erübriggt sich eine Einschränkung in unserem Fall. Dies bedeutet aber auch, dass nur das System, das den DHCP-Dienst zur Verfügung stellt, auf den Webserver des AP zugreifen kann. Dies mag zwar ein wenig umständlich wirken, ist aber aus Gründen der Netzwerksicherheit erwünscht.

#### **Ausgehende Informationen prüfen**

Überprüfen Sie jede WLAN-Komponente daraufhin, welche Daten bzw. Informationen sie versendet. Dies lässt sich z. B. mittels **Portscan** auf die IP-Adresse der betreffenden WLAN-Komponente feststellen.

#### **Broadcast-Funktion deaktivieren**

Damit ein WLAN-Client erkennt, welche Funknetzwerke in seiner Nähe verfügbar sind, versendet Access Points automatisch sogenannte **SSID-Broadcasts**. Dabei handelt es sich um regelmäßige Rundfunksignale, die Daten bzw. Informationen über ein WLAN im sogenannten «**Beacon Frame**<sup>[1]</sup>-Format übermitteln. Diese Informationen kann ein potenzieller Angreifer u. U. dazu nutzen, um das betreffende WLAN «etwas genauer unter die Lupe zu nehmen». Ist der SSID-Broadcast in einem Firmennetzwerk nicht notwendig bzw. nicht erwünscht, sollte er auf den betreffenden APs deaktiviert werden.

Dabei ist aber zu beachten, dass auch versteckte WLANs mithilfe geeigneter **Scan-Tools** aufgesprt werden knnen. Das Deaktivieren des SSID-Broadcasts ist daher nicht unbedingt eine griffige Sicherheitsmaßnahme. Folgender Screenshot zeigt beispielhaft die Anzeige des WLAN-Scanners «Kismet»<sup>[2]</sup>.

## [6-22] Informationen über versteckte WLANs (Kismet)

Network List—(Packets desc)							Info	
	Name	T	W	On	Packets	Flags	IP Range	Rate
+	Grehouse-Steal-This	A	Y	008	1974	04	10.0.0.116	76
	2000-33-190-000-000-000	A	Y	008	1974	04	0.0.0.0.0	3785
+	! Hinetw	A	Y	011	464	0	0.0.0.0.0	Cryptd
	052405000094	A	Y	006	55	0	0.0.0.0.0	4
+	Josh Leibering	A	0	006	53	0	0.0.0.0.0	Weak
+	Probe networks	G	H	003	44	0	0.0.0.0.0	0
	<no ssid>	A	H	—	28	T4	192.168.10.113	Noise
	<no ssid>	A	H	—	12	04	10.107.167.122	133
	<no ssid>	A	H	—	4	04	10.0.0.116	Discard
+	Allinic networks	G	H	008	2	0	0.0.0.0.0	165
+	Beta networks	G	H	—	2	0	0.0.0.0.0	Bits/s
	<no ssid>	A	Y	—	1	0	0.0.0.0.0	42
	<no ssid>	A	H	—	1	0	0.0.0.0.0	Elapsed
	<no ssid>	A	Y	—	1	0	0.0.0.0.0	00:05:18
	<no ssid>	A	H	—	1	0	0.0.0.0.0	25% (+) Down

In unserem Fallbeispiel verzichten Sie nach Absprache mit Ihren Vorgesetzten bewusst auf ein Abschalten der Broadcast-Funktion, damit Gäste bzw. Besucher möglichst einfach auf das WLAN der Firma Caprez Ingenieure AG zugreifen können.

[1] Datenpaket mit Verwaltungsinformationen über das WLAN.

[2] Vergleichen Sie dazu [www.kismetwireless.net](http://www.kismetwireless.net).

### 6.3.6 Betriebszeiten einschränken

Bei einigen Access Points kann festgelegt werden, zu welchen Zeiten das Funknetzwerk aktiv sein soll. Wenn dies möglich ist, sollten Sie zusammen mit Ihren Vorgesetzten diskutieren und entscheiden, ob die **Betriebszeit des WLANs** beschränkt werden kann.

#### Beispiel

In unserem Fallbeispiel sollen sowohl Mitarbeitende als auch Gäste das WLAN der Firma benutzen können. Es handelt sich also quasi um ein «halböffentliches Funknetz». Normalerweise werden die Gäste bzw. Besucher aber nur während der üblichen Geschäftszeiten empfangen und jeder Mitarbeiter kann auch an seinem Arbeitsplatz auf das Internet zugreifen. Mit dem WLAN im Bistro am Hauptsitz der Firma Caprez Ingenieure AG haben die Mitarbeitenden zusätzlich die Möglichkeit, während der Arbeitspausen auf das Internet zuzugreifen. In dieser Situation ist gut zu überlegen, ob das Funknetzwerk wirklich durchgehend 7 × 24 Stunden in Betrieb sein muss. Aus Sicherheitsgründen entschliessen Sie sich dazu, das WLAN nur in folgenden Zeiten zu betreiben:

<b>WLAN aktiv:</b>	Von Montag bis Freitag von 07:00 Uhr bis 19:00 Uhr Samstag von 08:00 bis 16:00 Uhr
<b>WLAN inaktiv:</b>	Sonntag von 00:00 Uhr bis 23:59 Uhr

#### Hinweis

- ▷ Sorgen Sie dafür, dass alle Mitarbeitenden der Firma über die Betriebszeiten des WLANs informiert sind, und geben Sie es durch einen entsprechenden Aushang am WLAN-Standort auch den Gästen bzw. Besuchern bekannt.

Die Dynamik bei der Weiterentwicklung von Funknetzwerken hat in den letzten Jahren noch zugenommen. Daher ist es nicht immer einfach, den Überblick über Standards und Vorgaben innerhalb der **Standardgruppe 802.11** zu behalten.

Dank den verschiedenen **WLAN-Betriebsarten** kommen heutzutage Funknetzwerke in fast allen Bereichen einer Firma oder auch im privaten Umfeld zum Einsatz. Von Kleinstgruppen bis hin zu grossen Hotelkomplexen: WLANs sind aus den Alltag kaum mehr wegzudenken. Die Effizienz und Stabilität von WLANs ist die Summe aller eingesetzten Komponenten. Bei diesen spielen vor allem die eingesetzten Antennen eine wichtige Rolle, da diese das Fundament der Datenübertragung im Funknetzwerk bedeuten.

Trotz allen Fortschritten bei der Entwicklung von WLANs der letzten Jahre darf man nicht vergessen, dass Funknetzwerke im Vergleich mit kabelbasierenden Netzen ein grösseres Angriffspotenzial haben. Damit auch WLANs die hohen Sicherheitsanforderungen an Datennetze erfüllen, müssen in WLANs folgende **Sicherheitsmaßnahmen** implementiert werden:

- Verschlüsselung des Datenverkehrs innerhalb des WLANs
- Authentifizierung der WLAN-Benutzer/-Systeme
- Abgrenzung des WLANs von anderen Netzwerkbereichen
- Deaktivierung ungenutzter Dienste und Funktionen im WLAN

## Repetitionsfragen

- 
- 8** Die erlaubte Sendeleistung bei WLAN-Netzen ist im Vergleich zu anderen Funksystemen wie z. B. Mobiltelefon relativ gering. Weshalb ist bei WLAN-Netzen nur eine geringe Sendeleistung erlaubt und mit welchen erlaubten Mitteln lässt sich die Sendeleistung dennoch merklich steigern?
- 
- 29** WLANs unterstützen unterschiedliche Verschlüsselungs- und Authentifizierungsprotokolle. Welches dieser Protokolle sollte heutzutage in einem WLAN zum Einsatz kommen und welches dieser Protokolle sollte unter keinen Umständen eingesetzt werden?
- 
- 32** Sie müssen zwischen zwei Gebäuden, die ca. 500 Meter voneinander entfernt sind, eine Funkstrecke einrichten. Freie Sicht zwischen den Gebäuden ist gegeben. Was müssen Sie in dieser Situation besonders beachten und warum?
- 
- 16** Weshalb hat die Deaktivierung bzw. die Unterdrückung der SSID keinen grossen Einfluss auf die Sicherheit eines WLANs?
-

## 7 Lokale Netze über das Internet sicher verbinden

Bis in die 1990er-Jahre wurden hauptsächlich **Mietleitungen**<sup>[1]</sup> angeschafft, um zwei Netzwerke miteinander zu koppeln (verbinden). Neben den hohen Kosten stellte sich bei dieser Lösung aber der aufwendige Bestell- und Installationsprozess als nachteilig heraus. Die Ursachen dafür lagen vor allem in der monopolartigen Struktur der Telekom-Industrie. Mit dem Aufkommen des Internets gegen Ende der 1990er-Jahre ist die Zahl der **Service Provider** und der entsprechenden Angebote markant gestiegen. Dadurch hat sich die Situation grundlegend geändert. Heute spielen finanzielle und zeitliche Aspekte bei der Koppelung von Netzwerken eine eher untergeordnete Rolle; das Augenmerk liegt vielmehr auf den Bereichen Leistung und Sicherheit. Insbesondere die Verfügbarkeit und die Sicherheit der Firmendaten müssen gewährleistet sein. In diesem Kapitel erfahren Sie mehr zum Thema «**Sichere LAN-Koppelung**» auf der Basis von Netzwerksystemen, die eine gültige IP-Konfiguration aufweisen.

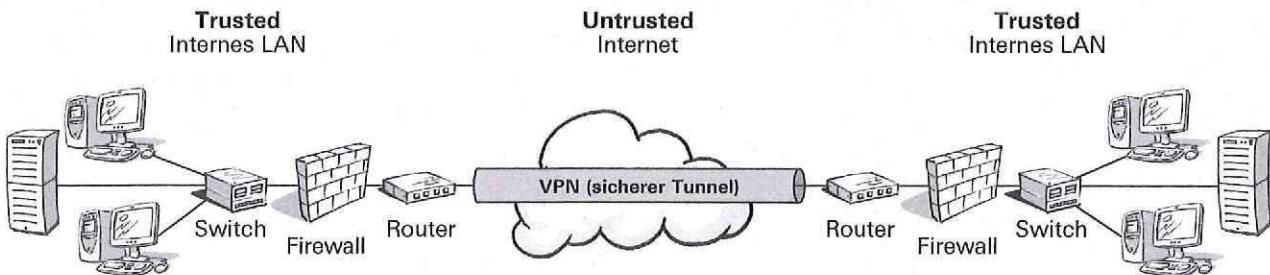
### 7.1 Virtual Private Network (VPN)

Für externe Zugriffe auf interne Firmennetzwerke über unsichere Verbindungen kommen heute meistens Virtual Private Networks zum Einsatz. Im Folgenden lernen Sie das Funktionsprinzip dieser Technik und verschiedene Verbindungsarten kennen.

#### 7.1.1 Funktionsprinzip

Ein **VPN** ist ein **virtuelles**<sup>[2]</sup> **Netzwerk**, das physisch nicht vorhanden ist, den Benutzern aber real erscheint, weil es funktional wirksam ist. **Privat** ist dieses Netzwerk insofern, als die übertragenen Daten nur vom **VPN-Betreiber**<sup>[3]</sup> genutzt werden können, d. h., nur dieser kann auf die Daten in ihrer ursprünglichen, unverschlüsselten Form zugreifen. Andere Personen oder Systeme sind möglicherweise auch in der Lage, auf die Daten im Tunnel zuzugreifen, können sie aber nicht nutzen, weil sie verschlüsselt und somit unkenntlich sind. Ein VPN kann also mit einem unsichtbaren Tunnel verglichen werden, der eine sichere Datenübertragung über unsichere Übertragungsstrecken (wie z. B. das öffentliche Internet) erlaubt. Folgende Grafik soll dieses Prinzip verdeutlichen:

[7-1] VPN-Prinzip: Tunnel für Datenübertragungen durch unsichere Netzwerkbereiche



[1] Englischer Fachbegriff: Leased Line.

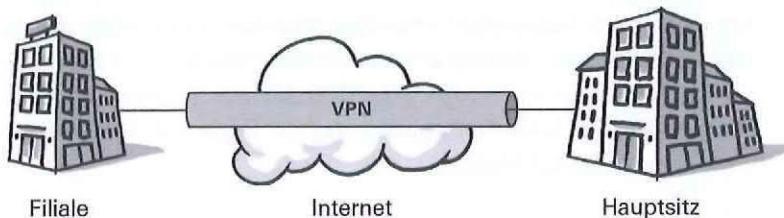
[2] Im Sinne von: nicht echt oder wirklich existierend, aber echt bzw. wirklich erscheinend.

[3] Der VPN-Betreiber ist die Stelle oder Person, die sicherstellen muss, dass die übertragenen Daten von Unbefugten nicht gelesen werden können.

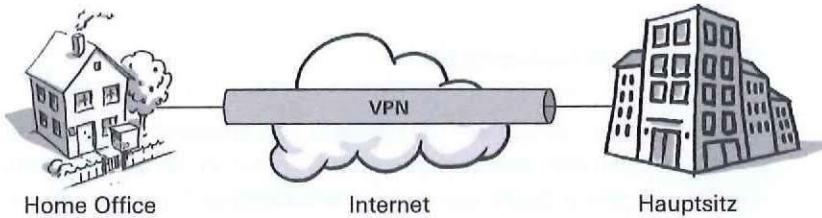
### 7.1.2 Verbindungsarten

Beim Einsatz eines VPN lassen sich folgende **Verbindungsarten** unterscheiden:

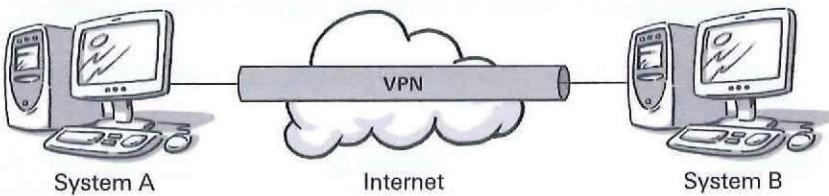
- **Site-to-Site:** Über diese Verbindungsart können getrennte Netzwerkbereiche bzw. Subnetze permanent miteinander verbunden werden (z. B. Koppelung des LANs einer Filiale mit dem Firmennetzwerk am Hauptsitz). Entsprechend wird diese Verbindungsart für die **Standortvernetzung** eingesetzt. Vergleichen Sie dazu auch das Kapitel 6.2.1, S. 102.



- **End-to-Site:** Über diese Verbindungsart können Benutzer von unterwegs oder von zu Hause aus auf die Daten und Applikationen der eigenen Firma zugreifen. Beispiel: Koppelung des WLANs beim Kunden oder des Home Office mit dem Firmennetzwerk am Hauptsitz. Diese Verbindungsart erlaubt also einen **Remote Access**<sup>[1]</sup>. Vergleichen Sie dazu auch das Kapitel 6.2.2, S. 104.



- **End-to-End:** Über diese Verbindungsart können zwei Rechnersysteme direkt miteinander verbunden werden, wobei keine zusätzlichen VPN-Komponenten wie z. B. Router benötigt werden. Die VPN-Clients (Software) auf den Endsystemen verwalten alle Funktionen selbstständig.



[1] Englisch für: Fernzugriff (autorisiert).

## 7.2 Sicherer Internetprotokoll (IPSec)

Die Datenübertragung im VPN basiert auf **IPsec**. Dieses Protokoll wurde von der Internet Engineering Task Force<sup>[1]</sup> (IETF) entwickelt, unter RFC 4301 (und weiteren RFCs) standardisiert und kann sämtliche Daten verschlüsseln, die über IPv4 oder IPv6 ausgetauscht werden. IPSec arbeitet auf Layer 3 des OSI-Modells und bietet gegenüber dem ursprünglichen **Internetprotokoll (IP)** zusätzlich folgende **Sicherheitsfunktionen**:

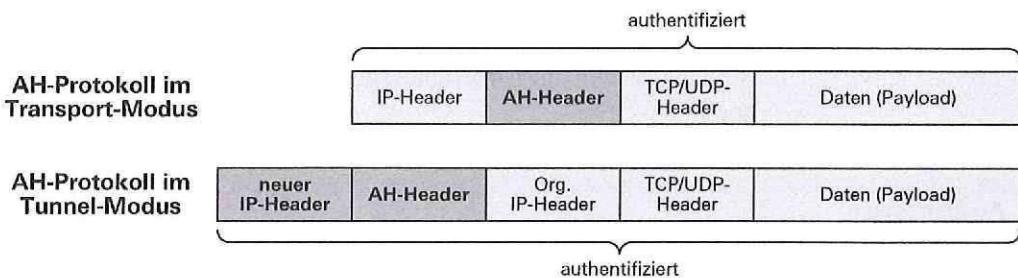
- **Authentisierung** zur Sicherstellung der Echtheit der Kommunikationspartner bzw. ausgetauschten Nachrichten
- **Datenverschlüsselung** zur Sicherstellung der Vertraulichkeit und Integrität der übermittelten Daten
- **Schlüsselverwaltung** zur Überwachung des Schlüsselaustauschs, Überprüfung der Gültigkeitsdauer eines Schlüssels und zur Verwaltung abgelaufener, ungültiger Keys

Im Folgenden werden die Techniken näher beschrieben, die IPsec zur Umsetzung dieser Funktionen anwendet.

### 7.2.1 Authentication Header (AH)

Um einen sicheren Datenaustausch zu gewährleisten, ergänzt IPsec die ursprünglichen IP-Pakete im Kopfbereich (Header der Frames) um sogenannte **Dienstdaten**. Je nachdem, welche **Übertragungsart** zum Einsatz kommt, sieht diese **Header-Erweiterung** unterschiedlich aus. Während im regulären **Transport-Modus** ein **Authentication Header (AH)** in die bestehenden IP-Header eingefügt wird, bleiben die bestehenden IP-Header im **Tunnel-Modus** unangetastet. Zusätzlich zum AH wird hier aber ein neuer IP-Header für die Dienstdaten von IPsec vorangestellt. Folgende Grafik soll diese Struktur verdeutlichen:

[7-2] AH-Protokoll im Transport- und Tunnel-Modus



Erläuterungen zur Grafik:

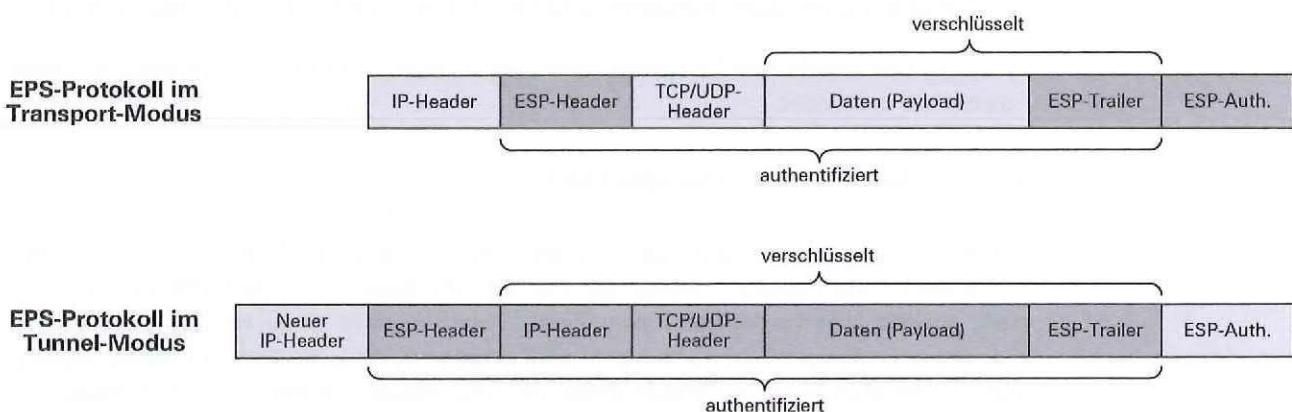
- Bei einem authentifizierten IP-Paket ist sichergestellt, dass die Daten des IP-Pakets während der Übertragung nicht verändert worden sind, bzw. eine Änderung der Daten wird erkannt. Das IP-Paket beim Empfänger ist identisch mit dem Paket, das der Sender abgeschickt hat. Das IP-Paket ist integer, also vertrauenswürdig.
- Bei VPN kommt immer der Tunnel-Modus zum Einsatz. Ein VPN hat zum Ziel, die übertragenen Daten «privat», also nicht jedermann, zugänglich zu machen. Nur der Tunnel-Modus verschlüsselt die übertragenen Daten.

[1] Arbeitsgruppe, die die Entwicklung neuer Protokolle sowie die Weiterentwicklung bzw. Anpassung bestehender IP-Protokolle bzw. Internet-Standards koordiniert.

## 7.2.2 Encapsulated Security Payload (ESP)

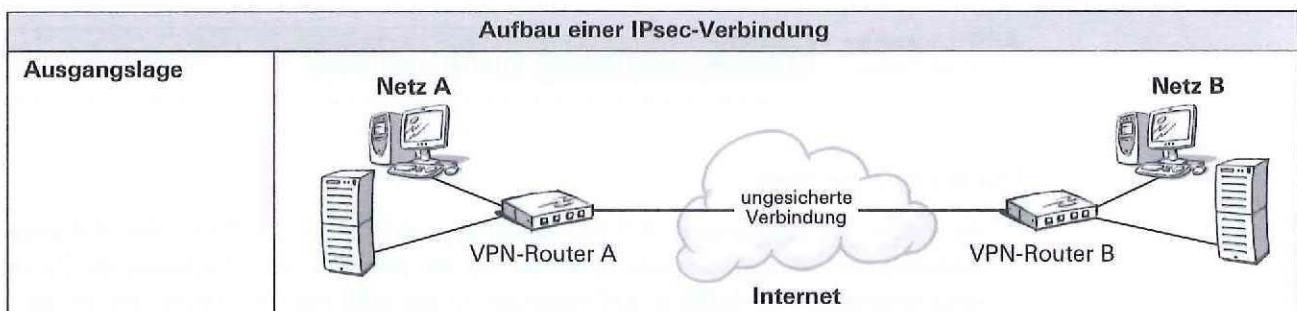
ESP basiert ebenfalls auf IP und verwendet die IP-Protokollnummer 50. Im Unterschied zum AH wird hier der Header eines IP-Pakets nicht überprüft, jedoch die Nutzdaten verschlüsselt übertragen, wobei alle gängigen Verschlüsselungsmethoden eingesetzt werden können. VPNs verwenden ESP, um die Vertraulichkeit der übertragenen Daten sicherzustellen. Wenn also zwei Standorte sicher vernetzt werden sollen (Site-to-Site), kommt ESP im **Tunnel-Modus** zur Anwendung. Für eine sichere Verbindung von zwei Rechnern (Host-to-Host) kommt grundsätzlich ESP im **Transport-Modus** zum Einsatz. Folgende Abbildung soll die entsprechenden Strukturen verdeutlichen:

[7-3] ESP-Protokoll im Transport- und Tunnel-Modus



## 7.2.3 Internet Key Exchange (IKE)

Bevor Daten über ein VPN übertragen werden können, muss eine **gesicherte Verbindung** zwischen den Kommunikationspartnern hergestellt werden. Zu diesem Zweck handeln die beteiligten Systeme Sicherheitsmodalitäten aus und vereinbaren z. B. die Methoden der Authentisierung und Verschlüsselung. Diese Aufgabe wird vom **IKE-Protokoll** übernommen.



Aufbau einer IPsec-Verbindung	
<b>Phase 1</b>	<p>VPN-Router A (Initiator) sendet der Gegenseite mehrere Vorschläge hinsichtlich der von ihm unterstützten Authentisierungs- und Verschlüsselungsalgorithmen.</p> <p>VPN-Router B (Responder) wählt die für ihn passenden Algorithmen aus und sendet diese Information an den Initiator.</p> <p>VPN-Router A sendet der Gegenseite den öffentlichen Bestandteil des Schlüssels nach Diffie-Hellman<sup>[1]</sup>. Dieser Teil besteht aus einer natürlichen und einer Primzahl. Daneben generiert der Router eine Zufallszahl, die er aber geheim hält.</p> <p>VPN-Router B sendet ebenfalls seinen öffentlichen Teil des Schlüssels an den Initiator und behält seine Zufallszahl geheim.</p> <p>Jede Seite berechnet nun mit dem gemeinsamen öffentlichen Teil und seiner geheimen Zahl einen eigenen Schlüssel, z. B. Key-A. Dieser Schlüssel Key-A wird der Gegenseite gesendet. Die Gegenseite verschlüsselt nun mit Key-A einige Informationen und sendet diese dem Initiator zurück. Kann der VPN-Router A diese Informationen entschlüsseln, hat er einerseits die Gegenseite erfolgreich authentifiziert, andererseits funktioniert auch die Verschlüsselung, da ja nur die jeweilige Seite eine Nachricht mit ihrer geheimen Zahl wieder entschlüsseln kann. Nun können die VPN-Router die Zertifikate und den Hashwert<sup>[2]</sup> des geheimen Schlüssels austauschen.</p>
<b>Zwischenresultat</b>	Die Kommunikationspartner sind identifiziert und die Schlüssel für die Datenverschlüsselung sind bekannt.
<b>Phase 2</b>	Anhand der Informationen aus der ersten Phase wird eine <b>Security Association (SA)</b> gebildet. Dies ist eine Vereinbarung zwischen zwei Kommunikationspartnern, die definiert, welche Dienste wie eingesetzt werden, um einen sicheren Datenaustausch zu gewährleisten. Eine SA beinhaltet u. a. einen <b>Security Protocol Identifier (SPI)</b> und die jeweilige Ziel-Adresse. Beim SPI handelt es sich um das zu verwendende Übertragungsverfahren von IPsec (z. B. AH oder ESP). Sobald die SA erfolgreich aufgebaut ist, steht eine gesicherte Übertragungsstrecke bzw. ein VPN zur Verfügung.
<b>Endresultat</b>	

[1] Verfahren für die Erzeugung und den Austausch eines geheimen Schlüssels zur Datenverschlüsselung.

[2] Prüfsumme zur Integritätsprüfung. Anhand des Hashwerts lässt sich die Originalinformation nicht rekonstruieren.

### Hinweise

- ▷ Für die erste IKE-Phase stehen i. d. R. die Optionen «Main Mode» und «Aggressive Mode» zur Auswahl. Im ersten Modus werden die ausgetauschten Daten (z. B. Authentisierungsangaben) verschlüsselt übertragen, im zweiten Modus dagegen im Klartext. Geben Sie wenn möglich dem «Main Mode» den Vorzug, falls die Gegenseite und die gewählte Verbindungsart dies zulässt.
- ▷ Mit IKEv1 und IKEv2 sind zwei unterschiedliche Versionen von IKE verfügbar. Verwenden Sie wenn möglich IKEv2, da diese Version zusätzlich dynamische IP-Adressen und NAT-Router unterstützt.

## 7.3 Praktische Anwendungen eines VPN

Nachfolgend werden wichtige Schritte und Einstellungen gezeigt, die beim Aufbau eines VPN in unserem Fallbeispiel vorzunehmen sind. Dabei kommen folgende Anwendungen zur Sprache:

- Aufbau eines Site-to-Site-VPN
- Aufbau eines End-to-Site-VPN
- Aufbau eines SSL-VPN

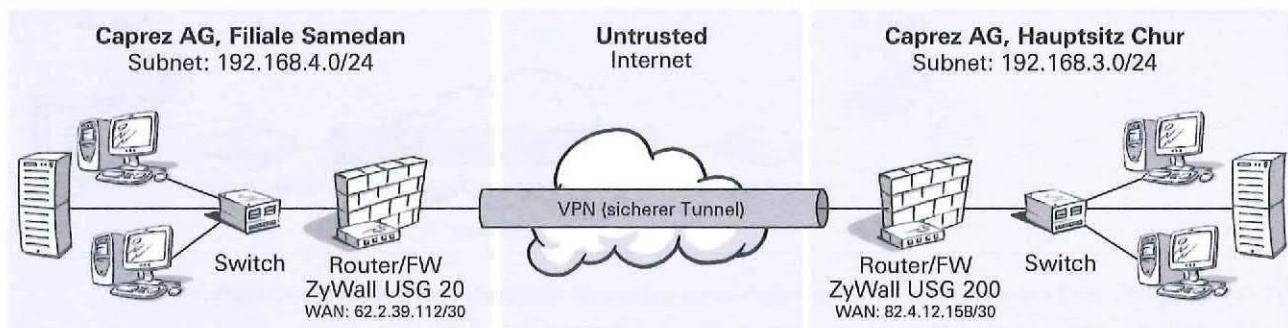
### Hinweis

▷ Auch wenn es inzwischen eine fast unüberschaubare Anzahl von Komponenten und Software für VPN gibt, sind die Konfigurationsschritte und -einstellungen bei den meisten Produkten ähnlich, da alle auf IPsec basieren.

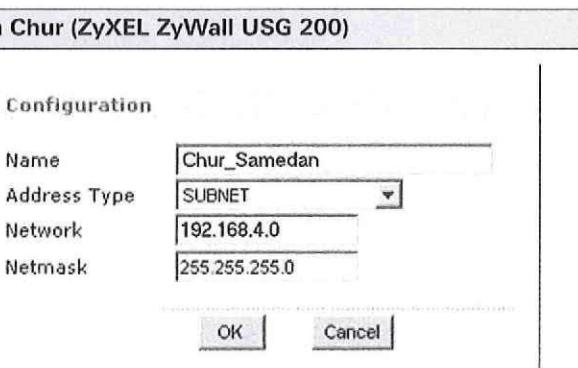
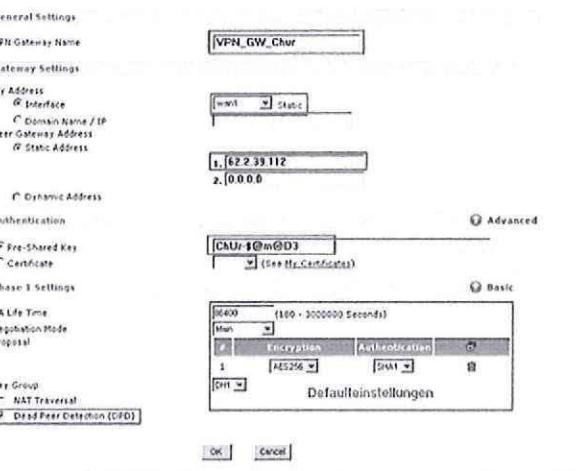
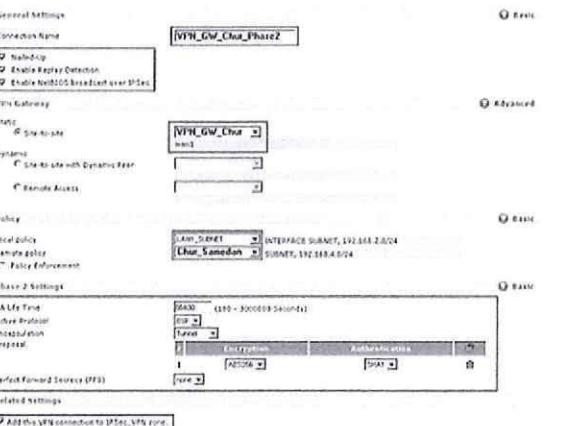
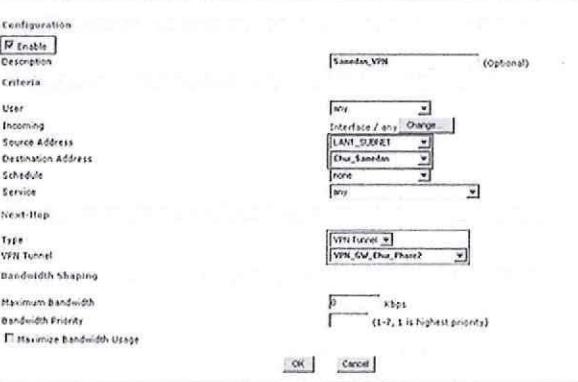
### 7.3.1 Site-to-Site-VPN einrichten

Zwischen dem Hauptsitz der Firma Caprez Ingenieure AG in Chur und der Filiale in Samedan soll ein Hardware-basierendes **Site-to-Site-VPN** eingerichtet werden. Das entsprechende Netzwerkschema kann vereinfacht wie folgt dargestellt werden:

[7-4] Site-to-Site-VPN (Beispielschema)



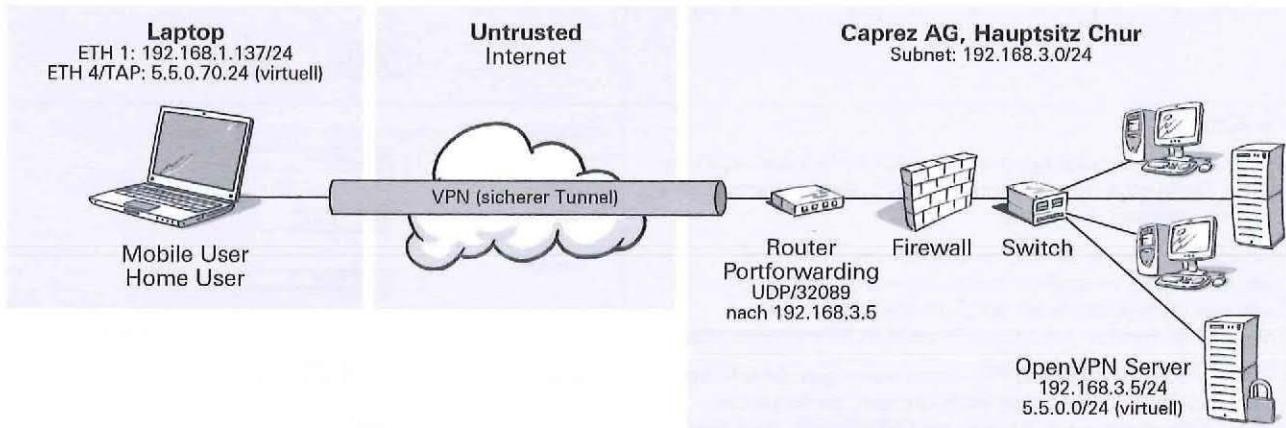
Die nachfolgend aufgezeigten Schritte und Einstellungen beziehen sich auf IKEv1:

Konfiguration auf dem VPN-Gateway in Chur (ZyXEL ZyWall USG 200)	
<b>1. Schritt:</b> Festlegen eines Namens für die neue VPN-Verbindung, der Art der Netzwerkverbindung (Subnet = Site-to-Site) und der IP-Adresse des entfernten Subnetzes (VPN-Gegenstelle).	 <p>Configuration</p> <p>Name: Chur_Samedan</p> <p>Address Type: SUBNET</p> <p>Network: 192.168.4.0</p> <p>Netmask: 255.255.255.0</p> <p>OK Cancel</p>
<b>2. Schritt:</b> Angaben der Bezeichnung des lokalen VPN-Systems (Gateway), Definieren des zu verwendenden Netzwerkinterfaces und von dessen IP-Adresse.  Danach Definieren eines Pre-Shared Key (PSK) und der Parameter bezüglich Verschlüsselung, Authentication und der Gültigkeitsdauer der Schlüssel. Nach Ablauf dieser Zeit werden automatisch neue Schlüssel vereinbart. «Dead Peer Detection» (DPD) muss wenn gewünscht auf beiden VPN-Komponenten aktiviert sein, da sonst die VPN-Verbindung nach Ablauf des DPD-Timers abgebaut wird.	 <p>General Settings</p> <p>VPN Gateway Name: VPN_GW_Chur</p> <p>My Address</p> <ul style="list-style-type: none"> <li>Interface: LAN1 Static</li> <li>Domain Name / IP: 1.62.2.39.112</li> <li>Peer Gateway Address: 2.0.0.0</li> </ul> <p>Peer Dynamic Address</p> <p>Authentication</p> <ul style="list-style-type: none"> <li>Pre-Shared Key: CHUR_123@03</li> <li>Certificate: (See My Certificate)</li> </ul> <p>Phase 1 Settings</p> <p>SA Life Time: 6000 (100 - 3000000 Seconds)</p> <p>Proposed: Encryption: AES256, Authentication: SHA1</p> <p>Key Group: 0 Dead Peer Detection (DPD)</p> <p>OK Cancel</p>
<b>3. Schritt:</b> Definieren, ob die VPN-Verbindung ständig online ist (Nailed-Up), also auch wenn keine Daten übertragen werden. Aktivieren des Schutzes gegen «Replay»-Attacken und Zulassen von Weiterleiten von NetBIOS-Broadcasts über die VPN-Strecke.  Angaben der gewünschten VPN-Typs (Site-to-Site), Festlegen der lokalen und der entfernten Richtlinien (Policies).  Nochmals Bestätigen der Parameter für die Verschlüsselung, der Authentication, der Gültigkeitsdauer und zusätzlich des IPsec-Protokolls (ESP im Tunnel-Modus).	 <p>General Settings</p> <p>Connector Name: VPN_GW_Chur_Phase2</p> <p>VPN Gateway</p> <ul style="list-style-type: none"> <li>State: Site-to-Site</li> <li>Dynamic: Site-to-site with Dynamic Peer</li> <li>Remote Access: 2</li> </ul> <p>Policy</p> <ul style="list-style-type: none"> <li>Local policy: LAN1_S2S (INTERFACE SUBNET, 192.168.2.0/24)</li> <li>Remote policy: Chur_Samedan (SUBNET, 192.168.4.0/24)</li> </ul> <p>Phase 2 Settings</p> <p>SA Life Time: 6000 (100 - 3000000 Seconds)</p> <p>Proposed: Encryption: AES256, Authentication: SHA1</p> <p>Perfect Forward Secrecy (PFS): None</p> <p>Related Settings</p> <p>Add this VPN connection to Samedan VPN zone.</p> <p>OK Cancel</p>
<b>4. Schritt:</b> Zum Schluss muss das Routing aktiviert und die benötigten Netzwerkinfos (Senden- und Ziel-IP-Adressen) angegeben werden. «Schedule none» bedeutet, dass diese Routestrecke 7 x 24 Stunden in Betrieb sein soll und für alle Dienste (Service = any). Zum Schluss wird nochmals der VPN-Typ (VPN Tunnel) bestätigt.	 <p>Configuration</p> <p>Enable: checked</p> <p>Description: Samedan_VPN (Optional)</p> <p>Criteria</p> <p>User: Any</p> <p>Incoming Source Address: LAN1_S2S/24</p> <p>Destination Address: Chur_Samedan</p> <p>Schedule: none</p> <p>Service: Any</p> <p>Next-Hop</p> <p>Type: VPN Tunnel</p> <p>Bandwidth Shaping: 1 Kbps (1-7, 1 is highest priority)</p> <p>Maximize Bandwidth Usage: checked</p> <p>OK Cancel</p>

### 7.3.2 End-to-Site-VPN einrichten

Zwischen dem Hauptsitz der Firma Caprez Ingenieure AG in Chur und den Mitarbeitenden, die zu Hause arbeiten (Home User) oder im Aussendienst tätig sind (Mobile User), soll ein Software-basierendes **End-to-Site-VPN** eingerichtet werden. Das Netzwerkschema auf der Basis von OpenVPN kann vereinfacht wie folgt dargestellt werden:

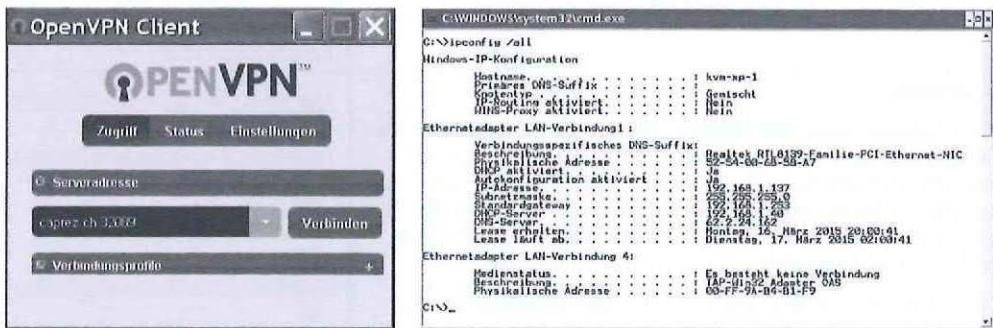
[7-5] End-to-Site-VPN (Beispielschema)



**OpenVPN** ist eine auf Open Source basierende Software für eine End-to-Site-Lösung, die ein Firmennetzwerk bis zum Rechner eines Benutzers erweitert. Dabei greift der **VPN-Client** nicht einfach via Remote Access auf das Zielnetzwerk zu, sondern wird als zusätzliches Subnetz in das Firmennetzwerk integriert.

Zu diesem Zweck wird der VPN-Client um ein sogenanntes **TAP<sup>[1]</sup>-Device** erweitert, das das OpenVPN-Subnetz bildet. Der **OpenVPN-Client** besitzt neben der physischen Netzwerkschnittstelle also auch eine virtuelle Netzwerkkarte. Der **OpenVPN-Server** routet die Daten der VPN-Clients nach ihrer Entschlüsselung in das LAN und auch in umgekehrter Richtung an den VPN-Client weiter. Folgende Screenshots zeigen den OpenVPN-Client (links) sowie die Netzwerkkonfiguration (rechts) jeweils vor dem Verbindungsaufbau mit dem OpenVPN-Server:

[7-6] Statusinformationen bei OpenVPN während der Verbindung (Beispiel)



Die Vorteile dieser VPN-Lösung bestehen u. a. darin, dass der Server einfach aufgesetzt werden kann, der Datenaustausch standardmäßig via UDP abgewickelt wird und OpenVPN somit auch bei VoIP- und Video-Streaming-Applikationen eingesetzt werden kann.

[1] Abkürzung für: Tunnel Adapter. Virtuelle Netzwerkschnittstelle, die mittels Software eine Netzwerkkarte simuliert.

VPN-Lösungen, die vornehmlich auf TCP basieren, eignen sich dagegen kaum für solche zeitkritischen Anwendungen.

#### Hinweise

- ▷ Der **OpenVPN-Server** läuft primär auf Linux, kann aber dank der virtuellen Appliances problemlos auch auf anderen Systemen wie z. B. VMware oder MS Windows Hyper-V eingesetzt werden.
- ▷ Die **OpenVPN-Client SW** gibt es für alle gängigen Betriebssysteme in Mac OS X und Android. OpenVPN findet sich oft als eine «embedded» Variante auf FW/Routern. Nähere Informationen über OpenVPN finden Sie unter [www.openvpn.net](http://www.openvpn.net).

### 7.3.3 SSL-VPN einsetzen

**SSL-VPNs** basieren auf den standardisierten Verschlüsselungstechniken **SSL<sup>[1]</sup>** bzw. **TLS<sup>[2]</sup>**. SSL-VPNs werden mehrheitlich als End-to-End-Lösung für **Fernzugriffe<sup>[3]</sup>** von Clients und weniger für die Kopplung von Netzwerken eingesetzt. Ein SSL-VPN kann mittels **Internetbrowser** aufgebaut werden. Dieser verfügt prinzipiell über alle Komponenten, die für eine **sichere Datenverbindung** benötigt werden.

SSL-VPNs bietet gegenüber anderen VPN-Techniken folgende **Vorteile**:

- Clientseitig muss i. d. R. keine zusätzliche Software installiert werden.
- Clientseitig ist i. d. R. kaum Administrationsaufwand erforderlich.
- Firewall-Regeln müssen i. d. R. nicht angepasst werden, da die Verschlüsselung auf den gleichen Routinen beruht, die bereits für die anderen Internetdienste zum Einsatz kommen (z. B. für das Onlinebanking).
- Bei Bedarf werden Softwarebibliotheken genutzt, die vom Browser während des Betriebs automatisch nachgeladen werden.

Demgegenüber ist der Einsatz von SSL-VPNs mit dem **Nachteil** verbunden, dass der vergleichsweise langsame Verbindungsaufbau und die i. d. R. benötigten Java-Applets oder Aktive-X-Komponenten meist höhere Anforderungen an die HW-Ausstattung der Rechner stellen.

Eine interessante **SSL-VPN-Lösung** auf Open-Source-Basis ist SoftEther VPN. Dieses Produkt wurde an der Tsukuba University in Japan entwickelt. Nähere Informationen darüber finden Sie unter: [www.softether.org](http://www.softether.org).

[1] Abkürzung für: Secure Socket Layer. Obwohl SSL heute unter dem Begriff TLS weiterentwickelt wird, ist die Bezeichnung SSL-VPN immer noch weitverbreitet.

[2] Abkürzung für: Transport Layer Security.

[3] Remote Access.

Mit dem Durchbruch des Internets sind auch die Anforderungen an die **Koppelung von Netzwerken** stark gestiegen. Als Antwort darauf werden heute häufig virtuelle private Netzwerke, sogenannte **VPNs**, verwendet. Diese kommen i. d. R. in folgenden Situationen zum Einsatz:

- **Site-to-Site-VPN:** Hier werden ganze Netzwerke miteinander verbunden.
- **End-to-Site-VPN:** Hier werden Fernzugriffe (Remote Access) auf Netzwerke möglich.
- **End-to-End-VPN:** Hier werden zwei Rechnersysteme miteinander verbunden.

VPN bietet folgende **Sicherheitsfunktionen**:

- Verschlüsselung der übertragenen Daten
- Authentisierung einer Nachricht auf dessen Echtheit bzw. Unverfälschtheit
- Authentisierung der Kommunikationspartner
- Verwaltung der verwendeten Schlüssel für die Verschlüsselung und Authentisierung

In einem VPN kommt i. d. R. das standardisierte Sicherheitsprotokoll **IPsec** zum Einsatz. Dieses bietet je nach Bedarf unterschiedliche Verschlüsselungsrouterien: Während für die Verschlüsselung der Daten der **Advanced Encryption Standard (AES)** zum Einsatz kommt, wird für den sicheren Austausch der Schlüssel zwischen zwei Kommunikationspartnern meistens das **Diffie-Hellman-Protokoll** eingesetzt. Für die Datenübertragung bietet IPsec zudem folgende Sicherheitsoptionen:

- **Authentication Header (AH)** gewährleistet die Authentizität und Integrität der Datenpakete.
- **Encapsulated Security Payload (ESP)** gewährleistet die Verschlüsselung der Datenpakete.

Die meisten VPNs laufen eingebettet auf einem Router und sind eng mit dem Hersteller und dem entsprechenden Produkt verzahnt. **OpenVPN** dagegen ist eine auf Open Source basierende Softwarelösung, die auf einem Rechner im Netzwerk betrieben werden kann.

## Repetitionsfragen

- 
- 1 Nennen Sie die drei Hauptaufgaben, die eine VPN-Lösung erfüllt.
- 
- 2 IPsec kennt die beiden Übertragungsprotokolle AH und ESP. Worin besteht der Unterschied zwischen diesen beiden Protokollen?
- 
- 7 IPsec kennt folgende zwei Übertragungsmodi, nämlich Transport- und Tunnel-Modus. Worin unterscheiden sich diese beiden Modi und wie kann man erkennen, in welchem Modus eine VPN arbeitet, ohne dass man auf das VPN zugreifen muss?
- 
- 27 Wozu benötigt man das «Diffie-Hellman»-Protokoll und was stellt dieses Protokoll sicher?
-

## **Teil D Anhang**

---

## Gesamtzusammenfassung

---

### 1 Netzwerkmanagement nach FCAPS

---

Für einen möglichst reibungslosen Betrieb eines Computernetzwerks muss dieses überwacht und betreut werden. Die dazugehörigen Aufgaben werden unter dem Begriff **Netzwerkmanagement** zusammengefasst. Das **FCAPS Management Framework** beschreibt die Funktionsbereiche, Ziele und Aufgaben für ein möglichst effizientes und effektives Netzwerkmanagement im Unternehmen. FCAPS umfasst folgende Funktionsbereiche, denen jeweils spezifische Ziele und Aufgaben zugeordnet sind:

- Fault Management
- Configuration Management
- Accounting Management
- Performance Management
- Security Management

Die **Netzwerkdokumentation** ist ein wichtiges Hilfsmittel für das operative Netzwerkmanagement und sollte deshalb folgende Elemente enthalten:

- **Netzwerkdiagramm**, das grafisch die Struktur und die Komponenten der Netzwerkinfrastruktur aufzeigt
- **Verkabelungsplan**, aus dem die vorhandenen Netzwerkanschlüsse und deren Belegung / Verfügbarkeit in Erfahrung gebracht werden können

### 2 Configuration Management

---

Beim **Network Configuration Management (NCM)** werden aktive Netzwerkgeräte wie z. B. Router, Switch, Firewalls und Access Points entsprechend den unternehmerischen Anforderungen konfiguriert und die Konfigurationseinstellungen systematisch und zentral verwaltet. Ziel des NCM ist es, Konfigurationsänderungen problemlos nachvollziehen und im Fall einer Netzwerk- oder Systemstörung rasch wieder rückgängig machen zu können.

Ein NCM lässt sich relativ einfach implementieren und betreiben:

- Für **kleine bis mittlere Netzwerke** reicht i. d. R. ein manuell betriebenes NCM aus.
- Für **mittlere bis grosse Netzwerke** sind professionelle Lösungen erhältlich, deren Funktionen sich meist automatisieren lassen. Neben proprietären und kommerziellen Lösungen gibt es auch Open-Source-Lösungen, die z. T. gratis zur Verfügung stehen.

### 3 Fault Management

---

Das **Fault Management** befasst sich hauptsächlich mit plötzlich auftretenden Störungen. Dabei kommt ein zentraler **Syslog-Server** zum Einsatz, der alle Meldungen analysiert, die von **verwalteten (managed) Netzwerkgeräten** generiert und übermittelt werden. Beim Auftreten bestimmter Ereignisse benachrichtigt dieser Server den Netzwerkadministrator via Mail oder über einen anderen Informationskanal. Mithilfe einer solch automatischen Benachrichtigung können bei einem Störfall Fehler rasch entdeckt und behoben werden, am besten noch, bevor die Benutzer etwas vom Fehler bemerken.

Für die Auswertung von Systemmeldungen und die Erkennung von Netzwerkstörungen kommen sogenannte **Network-Monitoring-Tools** oder **System-Monitore** zum Einsatz. Diese verschicken in regelmässigen Zeitabständen Anfragen an ein Netzwerkgerät, um zu prüfen, ob dieses Gerät noch antwortet. Dabei ist es möglich, für verschiedene Netzwerkdienste spezifische Anfragen zu senden. Antwortet ein Netzwerkgerät nicht innerhalb des definierten Zeitraums, wird der Netzwerkadministrator via E-Mail oder über einen anderen Informationskanal davon in Kenntnis gesetzt.

Neben technischen Hilfsmitteln sind auch **organisatorische Massnahmen** erforderlich, um Netzwerkstörungen möglichst rasch zu beheben. Dazu gehören etwa:

- Eindeutige Verantwortlichkeiten und Kompetenzen des Netzwerkadministrators.
- Klärung der Unterstützung bei grösseren Problemen oder im Notfall: Wer muss informiert werden und wie bzw. von wem kann Unterstützung angefordert werden? Eventuell muss ein Wartungsvertrag abgeschlossen werden.
- Anschaffung von Ersatzgeräten und -materialien: Wichtige, aber anfällige oder schwer zu beschaffende Komponenten sollten vorkonfiguriert bereithalten werden.

Die **Eingrenzung und Behebung von Netzwerkfehlern** hängt von diesen Faktoren ab:

- **Klare Vorgehensstrategie**
  - Mittels gezielter Fragen den Untersuchungsbereich ein- bzw. abgrenzen
  - Fehlersymptome mögliche Fehlerursachen gegenüberstellen
  - Naheliegende Lösungsschritte zuerst durchführen
- **Einsatz geeigneter Tools**
  - Einsatz einfacher, leicht bedienbarer Tools, z. B. die «Bordmittel» eines Systems
  - Kenntnis über die Wirkung der eingesetzten Tools, sprich Erfahrung in der Fehlerbehebung

## 4 Performance Management

---

Damit ein **Performance Management** betrieben werden kann, muss bekannt sein, welche Leistung bzw. Performance das Netzwerk überhaupt haben muss. Ist dieser Punkt geklärt, kann man damit beginnen, Leistungsdaten zu sammeln und auszuwerten.

Mithilfe von **SNMP** können auf einfache Weise die auf «managed» Netzwerkgeräten erhobenen Leistungsdaten abgerufen werden. Die Konfiguration eines SNMP-Agent auf einem Netzwerkgerät gestaltet sich recht einfach, doch hinsichtlich der Sicherung von vertraulichen Daten verfügt SNMP über einige Lücken. Nur SNMPv3 kann minimale Anforderungen an die Sicherheit erfüllen.

Neben SNMP etablieren sich immer mehr **NetFlow** und **sFlow** als eine zeitgemässere Art, Leistungsdaten auszuwerten. Daten basierend auf NetFlow und sFlow beinhalten neben dem bisher «reinen» Ressourcenverbrauch auch Angaben, wann und von wem diese Ressourcen verbraucht worden sind. Anhand dieser mehrstufigen Informationen lässt sich das Netzwerkperformancemanagement viel effizienter durchführen. Die gesammelten Leistungsdaten lassen sich meist durch deren grafische Darstellung einfacher analysieren. Hier muss darauf geachtet werden, dass eine geeignete **Darstellungsmethode** gewählt wird. Bei der grafischen Darstellung von Zeitreihen, das sind Daten über einen längeren Zeitraum, werden i. d. R. Histogramme dazu verwendet.

Damit die benötigte Performance eines Netzwerks besser eingeschätzt werden kann, sollten die anfallenden Datenströme gemäss deren Anforderungen charakterisiert werden. Eine solche Charakterisierung bildet die Grundlage dafür, dass man eine Priorisierung, also eine «Bevorzugung» gewisser Daten bzw. Applikationen, beim Transport durchs Netzwerk vornehmen kann. Zur **Priorisierung der Weiterleitung von Datenströmen** stehen verschiedene standardisierte Verfahren zur Verfügung. Mit IEEE 802.1Q ist es möglich, ein Netzwerk in verschiedene **virtuelle Netzwerke (VLANs)** aufzuteilen. Dies hat den Vorteil, dass sich der Netzwerkverkehr unterschiedlicher VLANs nicht gegenseitig negativ beeinflusst. Mit IEEE 802.1p lassen sich acht verschiedene Prioritätsstufen (CoS) auf Layer 2 definieren, mit deren Hilfe ein Ethernet-Frame eines entsprechenden Datenstroms gesteuert bzw. priorisiert weitergeleitet werden kann. Die meisten Netzwerkgeräte wie Switches, Router und Access Points unterstützen diese QoS-Mechanismen.

## 5 Sicherheitsmanagement

---

Die Thematik **Netzwerksicherheit** ist ein Teilbereich innerhalb der IT-Sicherheit. Die Schutzziele der Netzwerksicherheit decken sich mehrheitlich mit denen der IT-Sicherheit. Doch bei der Netzwerksicherheit liegt der Fokus hauptsächlich auf der Erkennung und Verhinderung der Übertragung von maliziösen Daten über das Netzwerk. Dazu sind folgende Aktivitäten nötig:

- **Analysieren und Filtern der Datenströme** auf maliziöse Inhalte
- **Authentifizierung von Systemen / Benutzern** beim Netzzugang
- **Abschottung gefährdeter Netzwerkbereiche** für bestimmte Systeme und Funktionen
- **Erkennen und Stoppen** von unerlaubten Netzaktivitäten

Mit den folgenden technischen Massnahmen werden die oben aufgeführten Aktivitäten durchgeführt:

- **Firewalls** für das Filtern und Analysieren der Datenströme
- **Einsatz von 802.1X** zur Authentifizierung beim Netzzugang
- **Realisieren einer DMZ** zur Trennung von «trusted» und «untrusted» Netzwerkbereichen
- **Einsatz eines Intrusion Prevention System IPS** zum Aufspüren und Unterbinden von unerlaubten Netzaktivitäten

## 6 Funknetzwerke planen und sicher betreiben

---

Die Dynamik bei der Weiterentwicklung von Funknetzwerken hat in den letzten Jahren noch zugenommen. Daher ist es nicht immer einfach, den Überblick über Standards und Vorgaben innerhalb der **Standardgruppe 802.11** zu behalten.

Dank den verschiedenen **WLAN-Betriebsarten** kommen heutzutage Funknetzwerke in fast allen Bereichen einer Firma oder auch im privaten Umfeld zum Einsatz. Von Kleinstgruppen bis hin zu grossen Hotelkomplexen: WLANs sind aus dem Alltag kaum mehr wegzudenken. Die Effizienz und Stabilität von WLANs ist die Summe aller eingesetzten Komponenten. Bei diesen spielen vor allem die eingesetzten Antennen eine wichtige Rolle, da diese das Fundament der Datenübertragung im Funknetzwerk bedeuten.

Trotz allen Fortschritten bei der Entwicklung von WLANs der letzten Jahre darf man nicht vergessen, dass Funknetzwerke im Vergleich mit kabelbasierenden Netzen ein grösseres Angriffspotenzial haben. Damit auch WLANs die hohen Sicherheitsanforderungen an Datennetze erfüllen, müssen in WLANs folgende **Sicherheitsmassnahmen** implementiert werden:

- Verschlüsselung des Datenverkehrs innerhalb des WLANs
- Authentifizierung der WLAN-Benutzer/-Systeme
- Abgrenzung des WLANs von anderen Netzwerkbereichen
- Deaktivierung ungenutzter Dienste und Funktionen im WLAN

## 7 Lokale Netze über das Internet sicher verbinden

---

Mit dem Durchbruch des Internets sind auch die Anforderungen an die **Koppelung von Netzwerken** stark gestiegen. Als Antwort darauf werden heute häufig virtuelle private Netzwerke, sogenannte **VPNs**, verwendet. Diese kommen i. d. R. in folgenden Situationen zum Einsatz:

- **Site-to-Site-VPN:** Hier werden ganze Netzwerke miteinander verbunden.
- **End-to-Site-VPN:** Hier werden Fernzugriffe (Remote Access) auf Netzwerke möglich.
- **End-to-End-VPN:** Hier werden zwei Rechnersysteme miteinander verbunden.

VPN bietet folgende **Sicherheitsfunktionen**:

- Verschlüsselung der übertragenen Daten
- Authentisierung einer Nachricht auf dessen Echtheit bzw. Unverfälschtheit
- Authentisierung der Kommunikationspartner
- Verwaltung der verwendeten Schlüssel für die Verschlüsselung und Authentisierung

In einem VPN kommt i. d. R. das standardisierte Sicherheitsprotokoll **IPsec** zum Einsatz. Dieses bietet je nach Bedarf unterschiedliche Verschlüsselungsroutinen: Während für die Verschlüsselung der Daten der **Advanced Encryption Standard (AES)** zum Einsatz kommt, wird für den sicheren Austausch der Schlüssel zwischen zwei Kommunikationspartnern meistens das **Diffie-Hellman-Protokoll** eingesetzt. Für die Datenübertragung bietet IPsec zudem folgende Sicherheitsoptionen:

- **Authentication Header (AH)** gewährleistet die Authentizität und Integrität der Datenpakete.
- **Encapsulated Security Payload (ESP)** gewährleistet die Verschlüsselung der Datenpakete.

Die meisten VPNs laufen eingebettet auf einem Router und sind eng mit dem Hersteller und dem entsprechenden Produkt verzahnt. **OpenVPN** dagegen ist eine auf Open Source basierende Softwarelösung, die auf einem Rechner im Netzwerk betrieben werden kann.

## Antworten zu den Repetitionsfragen

- 
- 1 Seite 126** Eine VPN-Lösung, egal ob HW- oder SW-basiert, erfüllt folgende Aufgaben:
- Verschlüsselung der zu übertragenden Daten
  - Authentisierung der Teilnehmer einer VPN-Verbindung und der ausgetauschten Datenpakete
  - Verwaltung der Schlüssel zur Datenverschlüsselung und Authentifikation
- 
- 2 Seite 49** Das Fault Management «kümmert» sich um die Beseitigung von Fehlern, die plötzlich und unerwartet eintreten. Beim Performance Management stehen hingegen Fehlersituationen im Vordergrund, die sich über einen (längeren) Zeitraum entwickeln, bevor sie zu einem Problem werden. Hier geht es also hauptsächlich um die vorsorgliche Vermeidung möglicher Probleme.
- 
- 3 Seite 29** Das NCM speichert und verwaltet «lediglich» die Konfigurationsinformationen eines Netzwerkgeräts. ITIL CM hingegen speichert alle relevanten Informationen über die Eigenschaften der HW-/SW-Ressourcen eines IT-Systems. ITIL CM konzentriert sich auf die Frage «Aus welchen Komponenten besteht ein bestimmtes IT-System?» und nicht «Wie wurde dieses IT-System konfiguriert?».
- 
- 4 Seite 20** Das Netzwerkmanagement hat das Ziel, den effizienten und anforderungsgerechten (sicher, stabil, skalierbar, performant) Betrieb der Netzwerkinfrastruktur zu gewährleisten.
- 
- 5 Seite 49** Der Adressbereich für APIPA-Adressen lautet 169.254.0.0–169.254.255.255. Hat ein Rechner eine APIPA-Adresse zugewiesen erhalten, so heisst dies i. d. R., dass der DHCP-Server nicht in Betrieb ist bzw. der Rechner den DHCP-Server nicht erreichen konnte.
- 
- 6 Seite 93** Diese unterschiedlichen Firewall-Arten sind verfügbar:
- Paketfilter
  - Paketfilter + Stateful Inspection (SPI)
  - Paketfilter + Stateful Inspection (SPI) + Application Layer Firewall (ALF)
- 
- 7 Seite 126** Im Transport-Modus wird der bestehende IP-Header um die Dienstdaten von IPsec ergänzt. Im Tunnel-Modus bleibt der bestehende IP-Header unangetastet und IPsec generiert nun einen zusätzlichen IP-Header mit seinen benötigten Dienstdaten.  
  
Wenn man die Datenpakete einer VPN mittels eines Sniffers aufzeichnet, kann man anhand der Struktur des IP-Headers erkennen, in welchem Modus die VPN zurzeit arbeitet. Der Overhead im Tunnel-Modus ist durch den zusätzlichen IP-Header um einiges höher, als dies im Transport-Modus der Fall ist.
- 
- 8 Seite 116** WLANs benutzen ein öffentlich frei zugängliches Frequenzband, das sogenannte ISM-Band (ISM, Industrial, Scientific and Medical). Damit möglichst viele Anwender dieses ISM-Band benutzen können, ist die Sendeleistung der einzelnen WLAN-Systeme stark eingeschränkt.  
  
Dank der Verwendung einer optimalen Antenne kann die begrenzte Sendeleistung durch den erzielten Antennengewinn (gemessen in dB) wettgemacht, in manchen Fällen sogar um einiges gesteigert werden.

- 
- 9 Seite 80
1. Fehlende Bandbreite: Zu wenig oder aufgebrauchte Bandbreiten sind eines der Top-Probleme, die sich negativ auf Netzwerkperformance auswirken. Dieses Problem entsteht dann, wenn mehr Daten über eine Verbindung übertragen werden sollen, als dass Bandbreite (Übertragungskapazität) auf dieser Verbindung zur Verfügung steht.
  2. Übermittlungs-/Übertragungsfehler: Solche Fehler haben auch eine negative Wirkung auf die Netzwerkperformance. Es gibt viele Ursachen, die zu einem Übertragungsfehler führen können. So kann z. B. eine hohe Latenzzeit (Verzögerung) zu Time-out-Problemen führen. In einer solchen Situation fordert der Empfänger bei bestimmten Protokollen (z. B. TCP) nach einer bestimmten Zeit den Sender dazu auf, ihm ein Datenpaket nochmals zu senden. Diesen Vorgang nimmt der Benutzer als eine langsame Verbindung bzw. eine langsame Applikation wahr.
- 
- 10 Seite 93
- Ein IPS sucht nach folgenden Bedrohungen bzw. unerlaubten Aktivitäten:
- Nach bestimmten Mustern (Patterns), anhand deren ein Angriff erkannt werden kann
  - Nach «protokollfremden» eingebetteten Programmcodes bzw. ausführbaren Befehlen innerhalb der Applikationsdaten eines Datenpakets
  - Nach unerlaubten Netzaktivitäten wie z. B. «Peer-to-Peer»-Funktionen (P2P) oder verbotenen Nachrichtendiensten (z. B. Instant Messaging wie Skype oder Twitter)
  - Nach dem Abruf von verbotenen Dateninhalten aus dem Internet wie Pornografie, Gewaltszenen etc.
- 
- 11 Seite 20
- Die verwendeten Symbole in einem Netzwerdiagramm/-schema müssen möglichst allgemein bekannt sein, damit Missverständnisse vermieden werden. Mit der Verwendung der «Cisco Networking Symbols» ist diese Anforderung weitgehend erfüllt, da diese Symbole allgemein bekannt und sehr weit verbreitet sind.
- 
- 12 Seite 93
- Eine DMZ (Demilitarisierte Zone) ist ein abgeschotteter Netzwerkbereich, in dem Systeme bzw. Dienste betrieben werden, die direkt aus dem Internet (untrusted) angesprochen werden können. Ein direkter Zugriff aus der DMZ in das interne LAN (trusted) wird i. d. R. unterbunden. Somit kann auch ein Angreifer, der es geschafft hat, ein System innerhalb der DMZ erfolgreich zu übernehmen, nicht ins interne LAN zugreifen. Somit kann in einem solchen Fall der Schaden auf einen ganz bestimmten Netzbereich beschränkt werden. Zugriffe aus dem internen LAN in die DMZ hingegen sind möglich.
- 
- 13 Seite 81
1. IEEE 802.1Q: Ermöglicht die Bildung von VLANs über mehrere Netzwerkswitches hinweg. Dadurch können Applikationen zu einem eigenständigen Netzbereich zusammengefasst werden, der isoliert von anderen Datenströmen / Applikationen betrieben werden kann.
  2. IEEE 802.1p: Ermöglicht die Bildung von 8 (0–7) sogenannten CoS-Prioritätsklassen. Dank dieser CoS-Info kann ein Frame aus einem Datenstrom priorisiert, sprich bevorzugt von einem Netzwerkswitch verarbeitet werden.
- 
- 14 Seite 81
- Die Kommunikation zwischen dem SNMP-Agent und der Managementkonsole wird nicht verschlüsselt, sondern in Klartext durchgeführt. SNMP verfügt über keine native (eigenständige) Verschlüsselung.
- Wenn immer möglich sollte man SNMPv3 einsetzen, da diese Version zumindest über eine brauchbare Authentifizierung verfügt. Mit SNMPv3 können nicht nur lokale Benutzer und Gruppen eingerichtet werden, sondern die Passwörter der Benutzer werden verschlüsselt auf dem SNMP-Agent abgelegt. Werden nun diese Passwörter über das Netzwerk übertragen, so sind zumindest diese verschlüsselt.

- 
- 15 Seite 49** Durch die Verwendung eines Syslog-Servers lassen sich die Systemmeldungen von verteilten Systemen an einem zentralen Ort sammeln. Dank dieser Möglichkeit ist auch die Analyse der Systemmeldungen viel effizienter durchgeführt worden.
- 16 Seite 116** Mit der Deaktivierung / Unterdrückung der SSID «verschwindet» zwar das entsprechende WLAN für einen normalen Benutzer aus seinem Sichtfeld, d. h., in der WLAN-Übersicht wird es nicht mehr angezeigt. Doch mit gängigen und frei erhältlichen WLAN-Scannern wie Kismet oder NetStumbler werden «versteckte», sprich hidden WLANs angezeigt. Da es dennoch einfach ist, «versteckte» WLANs aufzuspüren, ist das Unterdrücken der SSID nicht wirklich eine sichere / effiziente Sicherheitsmaßnahme.
- 17 Seite 80** SNMPv3 wurde um ein User Security Model erweitert. Das heißt, dass für den Zugriff auf einen SNMP-Agenten ein Log-in sowie ein Passwort eingegeben werden müssen. Diese Zugangsdaten werden auch verschlüsselt auf dem Agenten abgelegt. Doch die Übertragung der eigentlichen SNMP-Daten über das Netzwerk geschieht immer noch unverschlüsselt, was viele Möglichkeiten zur Manipulation des Agenten bzw. des Systems bietet. Ein sicheres Protokoll verschlüsselt die Daten jeweils während der Übertragung.
- 18 Seite 49** Folgende organisatorische Maßnahmen haben das Ziel, den normalen operativen Betrieb in einer Firma möglichst unterbruchsfrei zu gewährleisten bzw. im Störungsfall möglichst rasch wieder zur Verfügung zu stellen:
- Speichern der aktuellen Konfigurationseinstellungen eines Netzwerkgeräts
  - Der Abschluss eines Wartungsvertrags bei zentralen, wichtigen Netzwerkgeräten
  - Das Beschaffen von Ersatzgeräten/-material für Systeme, deren Ersatz einige Tage dauern kann
- 19 Seite 29** Mittels TFTP sollten keine Daten via Internet übermittelt werden, weil diese im Klartext übertragen werden. Entsprechend sind vertrauliche Daten in einer Konfigurationsdatei bei diesem Protokoll nicht vor unberechtigtem Zugriff bzw. vor unbefugter Einsicht geschützt.
- 20 Seite 49** A) Eine Überprüfung mittels Ping gibt nur Auskunft darüber, ob ein System via IP ansprechbar ist. Ist z. B. der Maildienst auf dem entsprechenden System abgestürzt, so erhalten wir mit hoher Wahrscheinlichkeit eine Antwort auf die Ping-Anfrage, die aussagt, dass das System «IP-mäßig» läuft. Aber den Status, sprich die Verfügbarkeit des Maildiensts, können wir daraus nicht erkennen. Dies kann u. U. zu einer Fehleinschätzung führen.  
B) Mittels des Versands einer dienstspezifischen Anfrage, bei einem Mailserver z. B. das Senden einer «HELO-Anfrage» des SMTP-Protokolls, kann genau erkannt werden, ob der Maildienst wirklich antwortet.
- 
- 21 Seite 20**
- Fault Management
  - Configuration Management
  - Accounting Management
  - Performance Management
  - Security Management

- 
- 22 Seite 126
- Authentication Header (AH): Dieses Übertragungsprotokoll dient zur Sicherstellung der Integrität und der Authentizität eines Datenpakets.
  - Encapsulated Security Payload (ESP): Dieses Übertragungsprotokoll dient zur Verschlüsselung der zu übertragenden Datenpakete.
- 
- 23 Seite 81
1. Problemanalyse durchführen: Zuerst müssen wir abklären, ob überhaupt bzw. welches Problem im Zusammenhang mit dem Internetzugang besteht.
  2. Eigenschaften des Internetzugangs abklären: Noch bevor wir uns mit Optimierungsmassnahmen beschäftigen, in unserem Fall dem Bandbreitenmanagement, müssen wir die technischen Eigenschaften des Internetanschlusses kennen.
  3. Lösungsmassnahmen definieren: Sobald die Probleme im Detail bekannt sind, können Gedanken hinsichtlich möglicher Massnahmen zur Beseitigung der Probleme gemacht werden.
  4. Lösungsmassnahmen implementieren: Die vorgeschlagenen Lösungsmassnahmen können nun umgesetzt werden.
  5. Lösungsmassnahmen überprüfen: Eine Weile der Umsetzung sollte jede Massnahme auf deren Wirksamkeit (Effizienz) überprüft werden.
- 
- 24 Seite 80
- Bei der Darstellung «Wer hat welchen Anteil an der übertragenen Datenmenge?» während einer bestimmten Zeitspanne eignet sich die Darstellung dieser Ergebnisse in Form einer «Rangliste», sprich Ranking. Innerhalb des Netzwerkmanagements spricht man auch von einer «Top Talker»-Liste.
  - Bei der Darstellung der Auslastung / Netzwerklast einer Verbindung über einen bestimmten Zeitraum, sogenannten Zeitreihen, eignet sich vor allem das Histogramm.
- 
- 25 Seite 29
- Das NCM speichert und archiviert die aktuellen Informationen über die Konfiguration eines Netzwerkgeräts, um im Fehlerfall allfällige Konfigurationsänderungen leichter zu erkennen und im Bedarfsfall die letztmals verwendete Konfiguration eines Netzwerkgeräts rasch und einfach wiederherstellen zu können.
- 
- 26 Seite 93
- Der Fokus von 802.1X liegt auf der Authentifizierung von lokalen Systemen und Benutzern, die auf das Netzwerk zugreifen möchten. Es hat sich in der Vergangenheit gezeigt, dass erfolgreiche Angriffe gegen Netze und deren Systeme nicht nur von externen Stellen durchgeführt werden, sondern auch von lokaler Seite ein gewisses Risiko ausgeht. 802.1X ist eine effiziente Methode, um auch die Risiken von lokaler Seite zu minimieren.
- 
- 27 Seite 126
- «Diffie-Hellman» ist ein Schlüsselaustauschprotokoll. Damit zwei Systeme untereinander verschlüsselte Informationen austauschen können, müssen diese Rechner die zur Verschlüsselung benötigten Schlüssel (Key) austauschen. «Diffie-Hellman» erlaubt einen sicheren Austausch dieser Schlüssel auch über eine ungesicherte Verbindung.
- 
- 28 Seite 80
- Dank NetFlow / sFlow werden nicht «nur» die reinen Verbrauchszahlen angezeigt, sondern NetFlow / sFlow rapportiert daneben auch noch z. B. den Zeitpunkt, den Absender / Empfänger und die Port-Nummer der übertragenen Daten. Dank dieser Zusatzinformationen wird die Analyse des Netzwerkverkehrs um einiges einfacher, da man sonst diese zusätzlichen Informationen aus mehreren Messungen zusammentragen muss.

- 
- 29** Seite 116 Heutzutage solle nur noch WPA2 bzw. WPA2-PSK zur Sicherung des WLAN-Datenverkehrs eingesetzt werden. Bei WPA2 kommt mit AES eine der sichersten Verschlüsselungsroutinen zum Einsatz. Auf gar keinen Fall darf man WEP einsetzen, da WEP viele Schwachstellen besitzt und für Angreifer keinerlei Schutz bietet.
- 
- 30** Seite 20
- Diagramm des Netzwerks
  - Verkabelungsplan inklusive Patchpanel-Belegungsplan
  - Liste der Netzwerkdienste
  - Inventarlisten von Netzwerkkomponenten
- 
- 31** Seite 49
- Ein falscher Eintrag in der hosts-Datei.
  - Ein falscher Eintrag auf dem DNS-Server.
  - Ein falscher / veralteter Eintrag im DNS-Cache eines Rechners (MS Windows).
  - Der DNS-Server ist nicht erreichbar bzw. der DNS-Dienst ist deaktiviert.
  - In der IP-Konfiguration ist ein falscher DNS-Server definiert.
- 
- 32** Seite 116 Bei einer Richtfunkstrecke muss immer die Fresnel-Zone in die Planung mit einfließen. «Nur» die freie Sichtverbindung kann u. U. nicht ausreichen, da die Fresnel-Zone zwischen dem Sender und dem Empfänger auch einen bestimmten hindernisfreien Raum gegen unten haben muss. Ragt ein Hindernis in die sogenannte Fresnel-Zone hinein, kann dies die Datenübertragung stören. Das wiederum kann einen negativen Einfluss auf die Übertragungskapazität und die Übertragungsqualität haben.

## Glossar

---

### A

<b>Accounting Management</b>	Das Accounting Management dient dazu, eine aufwandorientierte Verrechnung der Benutzung von Netzwerkdienstleistungen und Ressourcen zu gewährleisten.
<b>ANSI</b>	American National Standards Institute ist die amerikanische Stelle zur Normung industrieller Verfahrensweisen. Sie ist Mitglied in der ISO (International Organization for Standardization).
<b>APIPA</b>	Automatic Private IP Addressing, automatische Zuweisung einer IP-Adresse aus dem Range 169.254.x.x.
<b>ARP</b>	Address Resolution Protocol, ermöglicht die Zuordnung einer Internetadresse (IP-Adresse) zu einer Hardwareadresse (MAC-Adresse). Gehört zur Netzwerkschicht (Layer 3) im OSI-Referenzmodell.
<b>Authentifizierung</b>	Zugriffsprüfung bzw. die Identitätsprüfung einer Person oder eines Systems anhand eines bekannten Merkmals wie z. B. Passwort, Adresse o. Ä.

---

### B

<b>Blockschaltbild</b>	Eine Darstellungsform für technische Diagramme. In dieser Darstellungsform stehen die Detailinformationen im Vordergrund, nicht das Gesamtbild.
<b>Bluetooth</b>	Kurzstrecken-Funkstandard (PAN) IEEE-802.15, selbstkonfigurierend, geeignet für PDAs, Handys, Freisprechkits etc.

---

### C

<b>Cache</b>	Ein schneller Zwischenspeicher (Buffer) mit beschränkter Kapazität zwischen zwei unterschiedlich schnellen Speichersystemen, z. B. zwischen dem Arbeitsspeicher (RAM) und der Festplatte. Der Cachespeicher versucht Leistungseinbussen, hervorgerufen durch die unterschiedlichen Zugriffsgeschwindigkeiten verschiedener Systemkomponenten, zu verhindern.
<b>CH-DSG</b>	Schweizerisches Datenschutzgesetz, gibt klare Vorgaben, welche Art von Daten bzw. Informationen per Gesetz als schutzwürdig eingestuft werden und somit als vertraulich gelten.
<b>Configuration Management</b>	Das Configuration Management dient dazu, dass sämtliche Konfigurationsdaten von Systemen einer IT-Infrastruktur vollständig, aktuell und fehlerfrei zur Verfügung stehen.
<b>CSMA / CA</b>	Carrier Sense Multiple Access / Collision Avoidance, ein spezielles Ethernetprotokoll, das darauf optimiert wurde, Kollisionen während der Datenübertragung zu verhindern.

---

### D

<b>De-facto-Standard</b>	Ein Standard, der nicht durch ein Normierungsgremium wie z. B. ISO-OSI oder IEEE verabschiedet wurde, sondern lediglich durch die grosse Verbreitung oder deren breite Anerkennung (durch die Faktenlage) zu einem «Standard» geworden ist.
<b>DIN</b>	Deutsches Institut für Normung.
<b>DNS</b>	Domain Name System, dient zur Auflösung bzw. der Ersetzung des Hostnamens zur zugehörigen IP-Adresse, da Rechnersysteme nur IP-Adressen «verstehen», aber keine Hostnamen.
<b>Downtime</b>	Als Downtime wird die Zeitspanne bezeichnet, in der ein Computersystem nicht verfügbar bzw. nicht funktionstüchtig ist. Das Gegenteil von Downtime ist Uptime.

---

**F**

<b>Fault Management</b>	Das Fault Management dient dazu, die Verfügbarkeit / Stabilität einer IT-Infrastruktur zu gewährleisten bzw. möglichst hoch zu halten.
<b>FCAPS</b>	Fault, Configuration, Accounting, Performance und Security Management. Eine andere Bezeichnung für das OSI Management Framework (OSI-MF).
<b>Fresnel</b>	Augustin Jean Fresnel, franz. Physiker und Ingenieur (1788–1827), Begründer der Wellentheorie.

---

**G**

<b>GSM</b>	Global System for Mobile Communication, das heutige globale Handynetz.
------------	--

---

**H**

<b>Hotspot</b>	Öffentlich zugänglicher Einwählpunkt/-bereich zu einem WLAN. Oft zu finden in Hotels, Flughäfen o. ä. Lagen.
----------------	--

---

**I**

<b>IEEE</b>	Institute of Electrical and Electronics Engineers, nordamerikanischer Berufsverband der El.-Ingenieure. Äußerst aktiv in der Entwicklung neuer Netzwerkstandards.
<b>IrDA</b>	Infrared Data Association, beschreibt die physischen Spezifikationen und ein Kommunikationsprotokoll für Infrarotschnittstellen. Eine typische Technologie für PANs (Personal Area Networks).
<b>ITU</b>	International Telecommunication Union, befasst sich weltweit mit den technischen Aspekten der Telekommunikation. Umfasst zurzeit 190 Mitgliedstaaten und ist eine Unterorganisation der UNO.

---

**K**

<b>Kryptografie</b>	Ist die Wissenschaft der Verschlüsselung von Informationen und damit ein Teilgebiet der Kryptologie. Kryptos stammt aus dem Griechischen und bedeutet «verborgen».
---------------------	--

---

**L**

<b>Leistungsindikator</b>	Ein (Mess)instrument, das genaue Angaben (Indikatoren) über die Leistungsfähigkeit eines technischen Systems geben kann.
---------------------------	--

---

**M**

<b>MAC-Adresse</b>	Media-Access-Control-Adresse, die HW-Adresse jeder einzelnen Netzwerkschnittstelle. Diese dient zur eindeutigen Identifikation eines Geräts in einem Netzwerk.
<b>Managementkonsole</b>	Die zentrale Station (Manager) in einer SNMP-Managementlösung, auf der die Daten der verteilten Agents zwecks Auswertung und Weiterverarbeitung gesendet werden.
<b>MIB</b>	Management Information Base, eine Art Datenbank, in der die Daten von SNMP-Agents zur Verwaltung eines Netzwerks gespeichert werden.

**MTBF** Meantime between Failures, bezeichnet die mittlere Zeitdauer zwischen zwei Ausfällen. Der MTBF-Wert dient als Mass für die Zuverlässigkeit von Geräten und Anlagen.

---

**N**

**Netzwerkdigramm** Die grafische Darstellung eines Netzwerks oder Teile der Netzwerkinfrastruktur.

---

**O**

**OID** Object Identifier, eine eindeutige Bezeichnung eines Objekts innerhalb der MIB-Datenstruktur.

**OSI** Open Systems Interconnection, ein internationales, herstellerunabhängiges Fachgremium für eine koordinierte Entwicklung von Kommunikationstechnologien. OSI ist Mitglied des ISO-Gremiums (International Organization for Standardization), das eine Unterorganisation der UNO (United Nations Organization) ist.

**OSI Management Framework (OSI-MF)** Eine standardisierte Beschreibung (ISO/IEC 7498-4), die die Normen, Funktionen und Fachbegriffe (Terminologie) bezüglich der Verwaltung vernetzter Systemarchitekturen enthält.

---

**P**

**Performance Management** Das Performance Management dient dazu, die Leistungsfähigkeit der Netzwerkinfrastruktur gemäss den definierten Anforderungen sicherzustellen.

**Prinzipschema** Eine Darstellungsform zum Visualisieren vom Zusammenwirken von Systemen, Prozessen o. Ä. In dieser Darstellungsform steht das Gesamtbild im Vordergrund und nicht einzelne Details oder Komponenten.

**Proprietär** Als proprietär bezeichnet man in der IT Hard- und Softwarekomponenten, die auf nicht öffentlichen bzw. geheim gehaltenen Methoden und Techniken basieren. Der Anwender solcher Komponenten hat keine Möglichkeit, eigene Anpassungen daran vorzunehmen, bzw. es ist ihm ausdrücklich untersagt. Das Gegenteil von proprietärer Software sind Open-Source-Programme.

**PPTP** Point to Point Tunneling Protocol.

---

**Q**

**QoS** Quality of Service, Begriff für die Güte (Qualität) einer Datenverbindung.

---

**R**

**RAS** Remote Access Service.

**RFC** Request for Comment, technische Dokumente zum Thema Netzwerk / Internet, z.B. Protokolle, spezielle Funktionen etc., die von der IETF (Engineering Task Force) betreut und veröffentlicht werden. Alle interessierten Kreise können RFCs verfassen und diese beim IETF zwecks Standardisierung einreichen.

**RMON** Remote Monitoring ist eine Erweiterung des SNMP-Standards, um bei netzwerkfähigen Geräten statistische Daten zu erheben, diese von entfernter Stelle abzufragen.

**Roaming** Automatisches Wechseln / Anmelden in ein anderes, benachbartes Funknetz bzw. Funkzelle.

**S**

**Security Management** Das Security Management dient dazu, dass alle notwendigen Massnahmen koordiniert zum Einsatz kommen, damit die Benutzung des Netzwerks und der Transport der Daten die vorgegebenen Sicherheitsrichtlinien erfüllen.

**Skalierbarkeit** Bezeichnet die Eigenschaft eines technischen Systems, sich in Bezug auf Anforderungen (meist Leistungsanforderungen) anzupassen. Beispiel: Bei steigenden Anforderungen an Speicherplatz und Rechenleistung kann das System mit zusätzlichen Festplatten und weiteren Prozessoren (nach)ausgerüstet werden.

**SNMP** Simple Network Management Protocol, auf Deutsch ein einfaches Netzwerkverwaltungsprotokoll. Dieses Protokoll ermöglicht die Verwaltung von Netzwerkkomponenten wie z. B. Router, Switches, Server etc. von unterschiedlichen Herstellern.

**SNMP-Agent** Ein kleines Programm, das auf einer (Netzwerk)komponente läuft und laufend Daten über den Zustand des lokalen Systems sammelt und diese in der lokalen MIB abspeichert.

**SPOF** Single Point of Failure, beschreibt einen Teil / Teile eines Systems, die durch ihren Ausfall oder durch einen Fehler den Ausfall des Gesamtsystems verursachen können. Wenn immer möglich sollten SPOFs vermieden werden.

**Spoofing** Sich unerlaubt Zugriff / Zutritt verschaffen durch Angabe einer falschen Identität.

**T**

**Transaktion** Eine Folge von Verarbeitungsschritten (Operationen), die nur gemeinsam / vollständig oder gar nicht durchgeführt werden dürfen.

**Tunneling** Tunneling bezeichnet das Verfahren einer verschlüsselten, also sicheren Datenübertragung über unsichere Netze. Ein «virtueller», sicherer Tunnel wird durch das unsichere Gelände «gelegt». VPN ist ein typisches Tunnelingverfahren.

**U**

**UMTS** Universal Mobile Telecommunications System, gilt als Nachfolgetechnologie von GSM.

**V**

**Verkabelungsliste** Enthält die Informationen über die tatsächliche Verkabelung des Netzwerks. Neben den bestehenden Netzwerkanschlüssen (z. B. Dosen) innerhalb eines Gebäudes sind auch die Verbindungen im Schaltschrank des Netzwerks (Patchpanel) in dieser Liste dokumentiert.

**Vertraulichkeit** Vertraulichkeit in der IT bedeutet, dass sichergestellt ist, dass nur berechtigte Personen oder Systeme Zugriff auf vertraulich eingestufte Informationen wie z. B. Krankengeschichten oder Bankauszüge haben.

**VoIP** Voice over IP, Übertragung von Gesprächsdaten über ein IP-basierendes Netzwerk, i. d. R. das Internet.

---

## W

- WEP** Wired Equivalent Protocol, ein Verschlüsselungsverfahren für WLANs, gilt als unsicher!
- WPA** Wi-Fi Protected Access. Ein weiteres Verschlüsselungsverfahren für WLANs, wesentlich sicherer als WEP.
- WPA2** Ablösung von WPA. WPA2 ist durch IEEE 802.11i reglementiert und verwendet verbesserte Verschlüsselungsverfahren.

## Stichwortverzeichnis

### Numerics

13 Funkkanäle	98
2.4-GHz-Frequenzband	98
5-GHz-Frequenzband	99

### A

Abwehrfunktion	111
Access Mode	57
Access Point (AP)	100, 102
Accounting Management	13
Activity Diagram	37
Ad-hoc-Modus	99
AES	108
Aggressive Mode	121
Aktivitäten	40
Anforderungen	12
Ansprechpersonen/-stellen	54
APIPA-Adresse	42
ARP-Nachrichten	91
ARP-Tabelle	91
Art der Datenfilterung	84
Asset Management	22
Authentication Header (AH)	119
Authentication-System	88
Authenticator	88
Authentifizierung der Benutzer und Systeme	87
Authentifizierung mittels 802.1X	109
Authentifizierung mittels lokaler Benutzerkonten	109
Authentifizierung mittels MAC-Filter	109
Authentifizierung mittels Pre-Shared Key	110
Authentifizierung nach IEEE 802.1X	87
Authentifizierungsmethode	87
Authentisierung	119

### B

Bad-Block-Events	31
Balkendiagramm	61
Bandbreite einer LAN-Verbindung	66
Bandbreite einer Übertragungsstrecke	65

Bandbreiten-Management	67
------------------------	----

Basic Service Set (BSS)	100
-------------------------	-----

Basic Service Set Identifier (BSSID)	100
--------------------------------------	-----

Beacon-Frame-Format	114
---------------------	-----

Bedarfsgerechter Internetanschluss	78
------------------------------------	----

Beispielvorgehen für die Fehlersuche und -analyse	40
---	----

Belastungstest	66
----------------	----

Belegungsliste des Patchpanels	17
--------------------------------	----

Benachrichtigung	34
------------------	----

Betriebsarten	99
---------------	----

Betriebszeit des WLANs	115
------------------------	-----

Bordmittel	40
------------	----

Bruttodatendurchsatz	98
----------------------	----

### C

Cacti	64
Calligra Suite	20
Caprez Ingenieure AG	15
CCMP	108
CLI-Befehl	26
Community Name / String	57
Configuration Management	13
Configuration Management nach ITIL	22
Content Filtering	85
CoS-Bits	74

### D

Darstellungsarten von Messwerten	61
Datendurchsatz	55
Datenpakete	32
Datenströme in einem Netzwerk	63
Datenübertragungsrate	97, 98
Datenverschlüsselung	119
Default-CoS/ToS	76
Demilitarisierte Zone (DMZ)	88
DHCP	113
Dienstanfragen	38
Dienstdaten	69, 119
DNS-Cache	48
DNS-Server	38

Dokumentierung wichtiger Betriebsinformationen	15
DoS-Attacke	84
Dynamic Host Configuration Protocol	113
<b>E</b>	
EAP	108
Einflussgrößen	14
Einstellungen eines aktiven Netzwerkgeräts	21
End-to-End	118
End-to-Site	118
End-to-Site-VPN	124
Enterprise Mode	108
Erhöhung der Bandbreite	67
Ersatzmaterial	39
Erweiterte Möglichkeiten	84
ESP	120
Expiration Time	111
Extended Service Set (ESS)	100
<b>F</b>	
Facility	33
Fault Management	13, 30
FCAPS Configuration Management	22
FCAPS Management Framework (FCAPS-MF)	13, 14
FCAPS-Rahmen	13
Fehler im LAN	39
Fehlersuche	40
Fernzugriff	24, 125
FIFO-Prinzip	55
Filtereinstellungen	33
Firewall	83
Firewall-Konzept	89
Firewall-Regeln	83
Firewall-Typen	84
Forward-Queue	83
Frequenzbereich	98
Friendly AP	111
Funkantenne	104
Funkbereich	12
Funkkanäle	98
Funkstörungen	106

Funktionen	31
Funkzelle	99
<b>G</b>	
Gesicherte Verbindung	120
Grundoperationen	84
Gruppenrechte	59
<b>H</b>	
Hand over	100
Hardening	112
Hauptaufgaben	102
Header-Erweiterung	119
Hindernisse und Entfernungen	98
Histogramm	61
Hosts	48
<b>I</b>	
Icons von Cisco	16
IEEE-Standards der Reihe 802.11	97
IEEE-Standards für WLANs	97
IKE-Protokoll	120
Independent Basic Service Set (IBSS)	99
Infrastruktur-Modus	100
Input-Queue	83
Interferenzen	106
Internetanschluss analysieren	78
Internetbrowser	125
Internetprotokoll (IP)	119
Intrusion Detection System (IDS)	90
Intrusion Prevention System (IPS)	90
Inventarliste	22
Iperf	66
IPsec	119
<b>J</b>	
Jitter	55
<b>K</b>	
Kabel- und Steckverbindungen	105
Kanalauflistung	98
Kann-Informationen	16

Kommunikationskanäle	34
Komponenten	12
Konfiguration des SNMP-Agent	57
Konfiguration eines Syslog-Servers	32
Konfigurationsdatei	22
Konfigurationseinstellungen	22
Konfigurationsinformationen	21
Kuchendiagramm	61

**L**

Latenz	91
Latenzzeit	55
Layer 1	36
Layer 2	36
Leistung	98
Leistungsfähigkeit	12
Logische Trennung	69
Lösungsvariante implementieren	78
Lösungszeiten im Störungsfall	54

**M**

Mailserver	38
Main Mode	121
Maliziöse Inhalte	83
Management Information Base (MIB)	56
Man-in-the-middle-Attacke	91, 110
Manuelle Sicherung der Konfigurationsdateien	24
Massnahmen evaluieren	78
MIC	108
Mietleitungen	117
MIMO-Antenne	99
MIMO-Technik	105
Monitoring	37
MS Visio 2013	19
Muss-Informationen	16

**N**

Namensauflösung	48
NetFlow	63
NetFlow / sFlow Collector	64
NetFlow / sFlow Exporter	64
NetFlow-Messung	64

Nettodatendurchsatz	98
Network Configuration Management (NCM)	21
Network-Monitoring-Tools	35
Netzwerkdiagramm	15
Netzwerkdienste	12, 112
Netzwerkdokumentation	14
Netzwerkgeräte	12
Netzwerkinfrastruktur	12
Netzwerkkarte (NIC)	70, 77, 103
Netzwerkmanagement	12
Netzwerkschnittstelle	70
Netzwerksicherheit	82
Netzwerkstruktur	69
Netzwerksymbole	16
Netzwerkverbindungen	36
Netzwerkverkabelung	12
Netzwerkzugang	88
ntop	64
NTP-Dienst	32
Nutzdaten	68
Nutzdaten (Payload)	85

**O**

Öffentliche Übertragungsdienste	12
Öffentlicher Bereich	39
OID (Object Identifier)	56
Online-Speedtest	66
Open-Source-Programme	64
OpenVPN	124
OpenVPN-Client	124
OpenVPN-Client SW	125
OpenVPN-Server	124, 125
Operatives Performance Management	54
Ordnungsgemässer Systembetrieb	36
Organisatorische Massnahmen	38
Output-Queue	83

**P**

Paketverlustrate	55
Passwort	59
Performance	12

Performance Management	13
Period	111
Personal Mode	108
Ping-Anfrage	37
Portbasiert	71
Portscan	114
Portstatistik eines Netzwerkswitches	60
Priorisierung der Datentransporte	73
Priorisierung nach 802.1p	77
Priorisierungsoptionen	73
Privat	117
Privater Bereich	39
Problem analysieren	78
PRTG-Monitoring-Lösung	33
PSK	108, 110
<b>Q</b>	
QoS-Funktion	77
QoS-Parameter	54
Queue 1	73
Queue 2	73
Queue 3	73
Queues	73
<b>R</b>	
RADIUS-Server	87
RANCID	28
Remote Access	118
Repeater	101, 104
Result	37
Roaming-Netz	100
Rogue Access Point	110
Rogue AP	111
Route zum Webserver	47
Router	38
Rundstrahl-Antenne	105
<b>S</b>	
Scan-Tools	114
Schlüsselverwaltung	119
Schutzziele der IT-Sicherheit	82
Secure Shell	113
Secured Client IP Address	113
Security Management	14
Security Mode	109
Security through obscurity	113
Segmentierung	68
Sendeleistung	104
Server Access	113
Server Ports	113
Service Provider	117
Service Set Identifier (SSID)	100
Servicequalität	54
Severity	32
sFlow	63
Sichere LAN-Koppelung	117
Sicherheit bei Funknetzwerken	107
Sicherheitsaufgaben	82
Sicherheitseinstellungen	57
Sicherheitsfunktionen	119
Sicherheitsmaßnahmen	82, 107
Sicherheitsrisiken	82, 107
Simple Network Management	56
Simple Network Management Protocol	113
Site-to-Site	118
Site-to-Site-VPN	122
Skalierbarkeit	12
SLA	54
SmartDraw Standard	19
SNMP	56, 113
SNMP-Agent	55
SNMP-Manager	55
SPOF-Risiko	38
SSH	113
SSID-Broadcasts	114
SSL	125
SSL-VPNs	125
Stabilität	12
Stability	37
Standortvernetzung	118
Statistics	37
Status einer Netzwerkschnittstelle	45
Steuerung der Datenflüsse	78

Struktur der MIB	56
Supplicant	88
Switches	38
Switching-Kapazität	73
Switchport	70
Syslog-Server	31
System Log Settings	32
Systemlog	31
Systemmeldungen eines Switches	32

**T**

Tagged	70
Tagging	70
TAP-Device	124
Telnet	113
TFTP	113
TFTP-Serverdienst	23
Timestamp	37
TKIP	108
TLS	125
Top-Talker-Liste	62
ToS-Bits	74
Total Network Monitor	36
Transport-Modus	119
Trivial File Transfer Protocol	113
Trusted LAN	108
Trusted Network	83
Tunnel-Modus	119

**U**

Überlappungsfreie Kanäle	99
Übertragungsart	119
Übertragungsprobleme	68
UDP	32
Umlegen der Defaultports	113
Universelle Gebäudeverkabelung	17
Untagged	70
Untrusted Internet	108
Untrusted Network	83
Up- und Downloaden von Konfigurationsdateien	24

**V**

Verantwortlichkeiten	38
Verarbeitungslinien	83
Verbindung (Session)	85
Verfügbarkeit	12, 37
Verfügbarkeit des Netzwerks	54
Verkabelungsplan	17
Vertraulichkeit	13
Verwaltungs- oder Dienstdaten	68
Verzeichnisstruktur	24
Virtuelles Netzwerk	117
Visualisierung der aktuellen Netzwerkstruktur	15
VLANs	112
VPN	117
VPN-Betreiber	117
VPN-Client	124

**W**

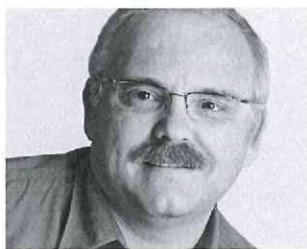
Wartungsverträge	38
WDS-Repeating-Modus	101
Webbrowser	24
Webserver	38
Wechselwirkungen	14
Weg der Datenpakete	47
Weiterleitungskapazität des Switches	73
Whois-Angaben	44
WiFi Protected Access (WPA)	108
Wired Equivalent Privacy (WEP)	108
Wirksamkeit der Lösung überprüfen	78
WLAN	112
WLAN-AP	102
WLAN-Komponenten	102
WLAN-Netzwerkkarte (WLAN-NIC)	103
WLAN-Roaming-Modus	100
WLAN-Standards	98
World Wide Web	113
WPA	108
WPA2	108
WRR-Mechanismus	73
WWW	113

---

## Z

Zeichenprogramme	19
Zentraler Ablageort der Konfigurationsdateien	23
Ziele	15, 85
Zugriffsberechtigungen	59
Zustand (State)	85



**Attila Mathé, IT Service Engineer HF,****Erwachsenenbildner FA**

Selbstständiger Netzwerkspezialist. Unterstützt verschiedene Firmen und Organisationen bei der Konzeption, Umsetzung und Optimierung von Netzwerken sowie verteilten Rechner- und Speichersystemen. Langjährige Erfahrung in der Evaluation und Implementierung von Open-Source-Lösungen. Unterrichtet an diversen Lehrinstitutionen Themen in den Bereichen Netzwerktechnologien, Netzwerk- und Systemmanagement.

**Johannes Scheuring, dipl. Ver.wiss.**

Redaktor, Studium der Verwaltungswissenschaften, verfügt über mehrjährige Berufserfahrung als Fachredaktor für internationale Soft- und Hardwarehersteller (Projektleiter, Teamleiter Dokumentation, Marketing Support für den Fachhandel). Seit 2002 bei Compendio Bildungsmedien für die Entwicklung und Herausgabe von Lehrmitteln in den Bereichen Informatik, Wirtschaftsinformatik und Betriebswirtschaft verantwortlich.

Dieses Lehrmittel vermittelt grundlegende Kenntnisse, um ein lokales Netzwerk (LAN) sicher zu administrieren und auszubauen. Anhand eines Best-Practice-Vorgehens und eines Beispielprojekts wird aufgezeigt, wie das LAN eines mittelständischen Unternehmens zielgerichtet effizient gewartet, an die betrieblichen Leistungs- und Sicherheitsbedürfnisse angepasst und optimiert werden kann. Voraussetzung dafür ist ein angemessenes Netzwerk-Monitoring sowie eine systematische Fehlersuche und -analyse. Das Lehrbuch zeigt weiter auf, was bei der Planung und beim Betrieb eines Funknetzwerks (WLAN) zu beachten ist und wie sich verschiedene LANs sicher über das Internet verbinden lassen.

**Weitere Informatik-Lehrmittel bei Compendio:**

Compendio bietet rund 50 Lehrmittel für die Grund- und Weiterbildung in der Informatik an. Die Details dazu sind auf unserer Website [www.compendio.ch](http://www.compendio.ch) abrufbar.

[www.compendio.ch](http://www.compendio.ch)

ISBN 978-3-7155-7066-2



9 783715 570662

Dieses Lehrmittel orientiert sich an den handlungsnotwendigen Kenntnissen des Moduls 145 «Netzwerk betreiben und erweitern» der ICT-Berufsbildung.

Es richtet sich in erster Linie an Auszubildende der Informatik-Erstausbildung und eignet sich sowohl für den handlungsorientierten Unterricht als auch für das Selbststudium sowie für Schulungen, die handlungsbezogene Kenntnisse im Kompetenzfeld «Network Management» vermitteln.