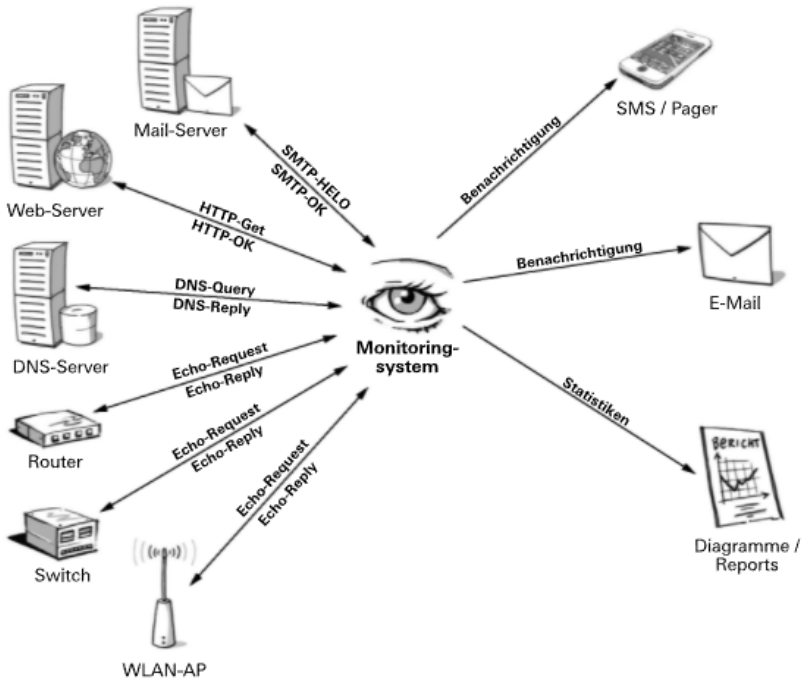
3.2.2 Network-Monitoring-Tools

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)

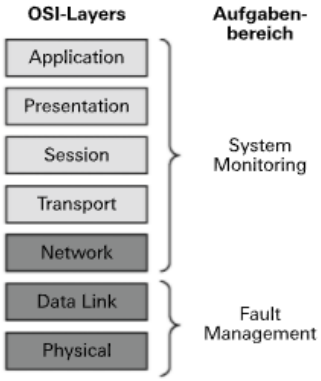
Folgende Grafik zeigt die typischen Komponenten und Informationsflüsse eines solchen Monitoring-Systems:

[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 Systemadministrators 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

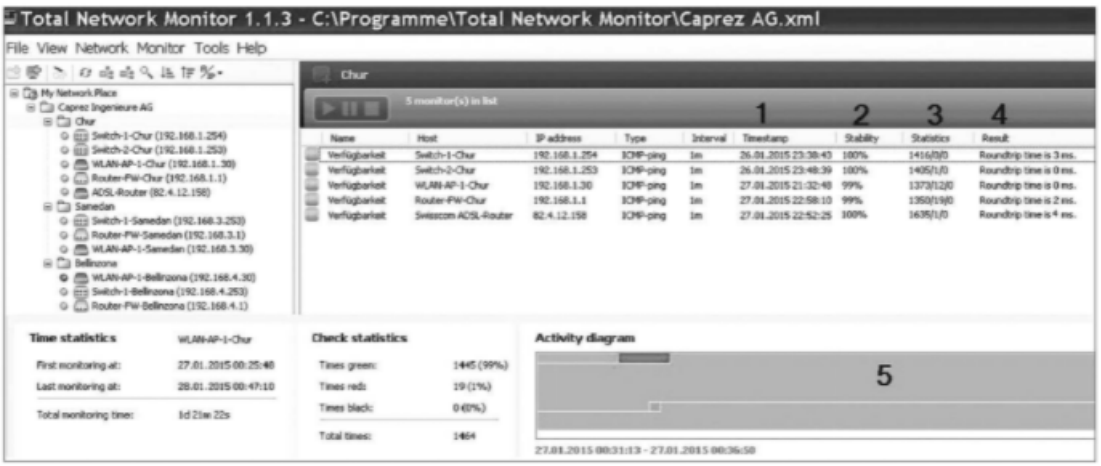


Hinweis

▷ 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/ 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:

1. **Timestamp:** letzter Zeitpunkt, zu dem sich der Verfügbarkeitsstatus eines Netzwerkgeräts geändert hat.
2. **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.
3. **Statistics:** Summen folgender Werte: Anzahl der beantworteten und unbeantworteten Anfragen, Anzahl der Zeitintervalle, zu denen der Sensor[1] deaktiviert war.
4. **Result:** durchschnittliche Übertragungsdauer einer Ping-Anfrage vom Sender zum Empfänger und wieder zurück.
5. **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[2] eine **Ping**[3]**-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 Netzwerkausfalls 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**[1]**-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.

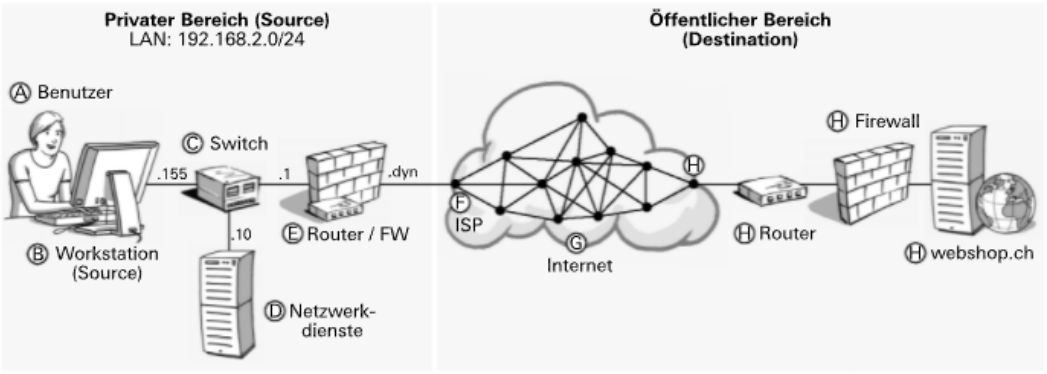
3.3 Fehlersuche und -analyse

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
Abklärungen beim Benutzer	• Seit wann genau funktioniert die Verbindung nicht mehr? • Wurde eine Fehlermeldung ausgegeben? • Kann Ihr Arbeitskollege auf die gewünschte Webpage zugreifen?	• Informationen über die Störung • Informationen über die aktuelle Situation • Informationen über die Situation vor der Störung
Visuelle bzw. physische Kontrolle	• Ist das Netzwerkkabel korrekt angeschlossen? • Ist das Gerät eingeschaltet? • Leuchtet eine bestimmte LED?	• Informationen darüber, ob überhaupt ein Fehler vorliegt • Informationen darüber, welche Art von Fehler wahrscheinlich vorliegt (Verbindungs-, Hardware-, Softwarefehler)

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**[1] 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`	`(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)

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 Fehlersuche 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 Webpage 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.

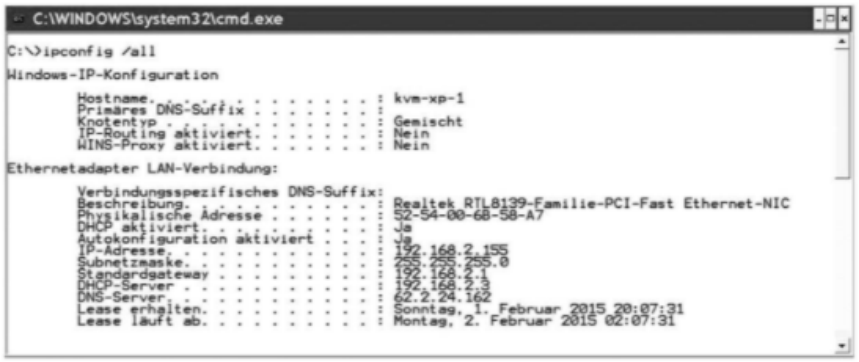
3. Netzwerkkonfiguration des Benutzerrechners überprüfen (B)

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)



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**[1]**-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)

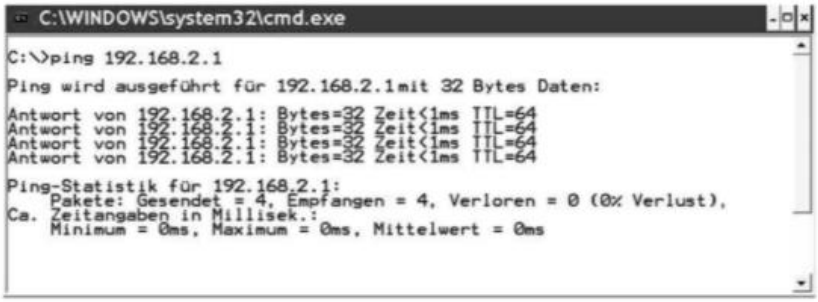
Vorliegende Information(en): aktuelle IP-Adresskonfiguration vom DHCP-Server erhalten

- 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)

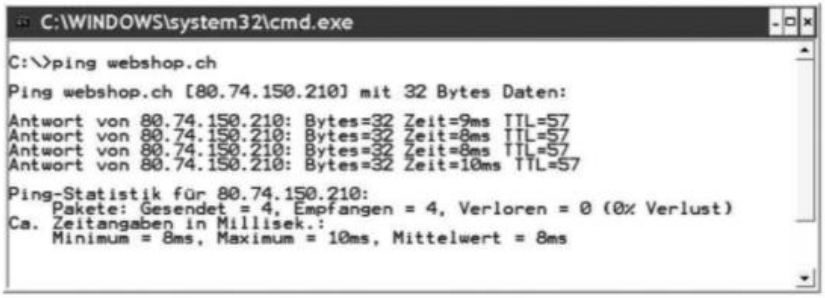


Hinweis

▷ 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)



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.

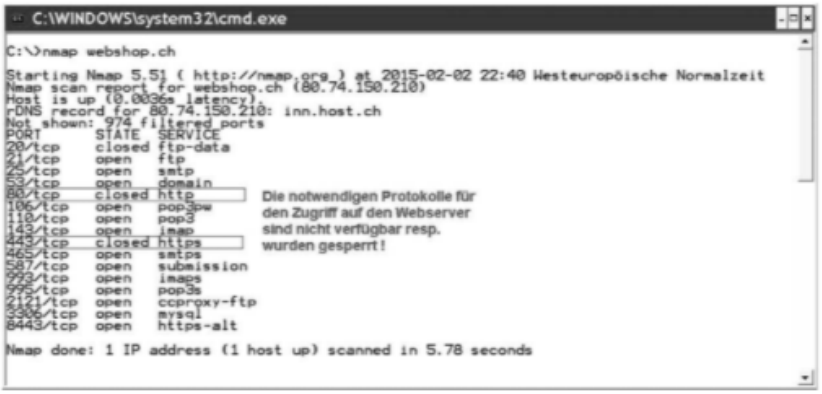
5. Dienste des entfernten Webserver überprüfen (H)

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.[1]
- 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 infrage. 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)



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 infrage:

- 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

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.

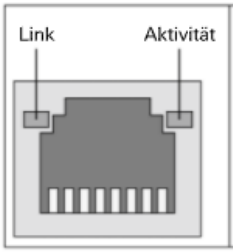
Verbindung zwischen Rechner und Switch überprüfen (B und C)

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**[1]**-Lämpchen,** die Auskunft über den Portstatus geben.

[3-20] Visuelle Kontrolle der Verbindung



Link On: Verbindung zwischen Rechner und Switch aktiv

Link Off: Verbindung zwischen Rechner und Switch nicht aktiv

Aktivität: 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 Netzwerkkabel 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)

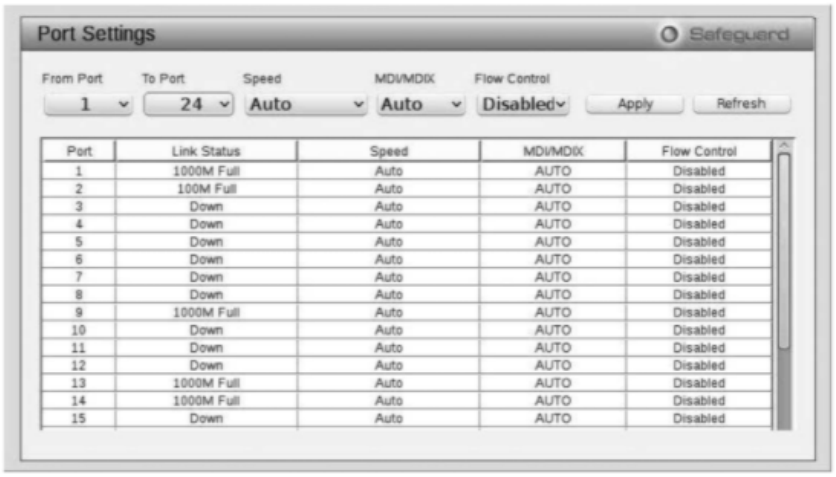
```
Switch#show interfaces status

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)

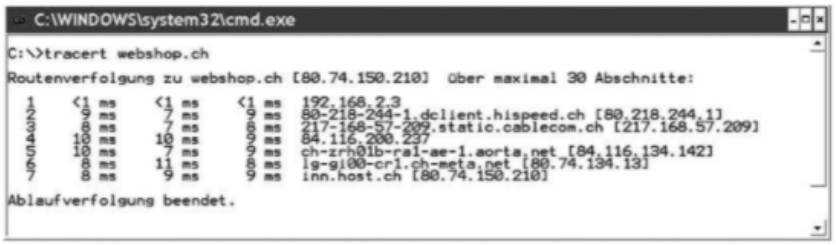


Port	Link Status	Speed	MDI/MDIX	Flow Control
1	1000M Full	Auto	AUTO	Disabled
2	100M Full	Auto	AUTO	Disabled
3	Down	Auto	AUTO	Disabled
4	Down	Auto	AUTO	Disabled
5	Down	Auto	AUTO	Disabled
6	Down	Auto	AUTO	Disabled
7	Down	Auto	AUTO	Disabled
8	Down	Auto	AUTO	Disabled
9	1000M Full	Auto	AUTO	Disabled
10	Down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



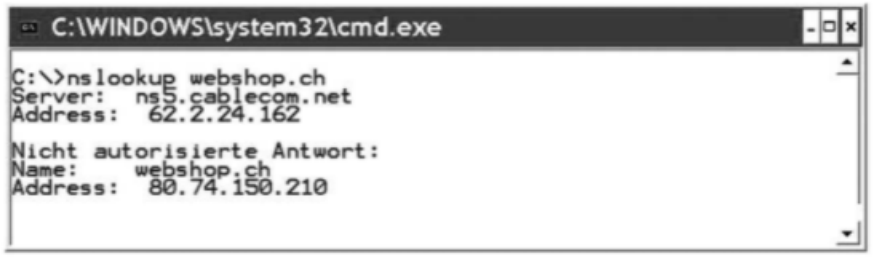
Hinweis

▷ 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»



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
  - Fehlersymptomen 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