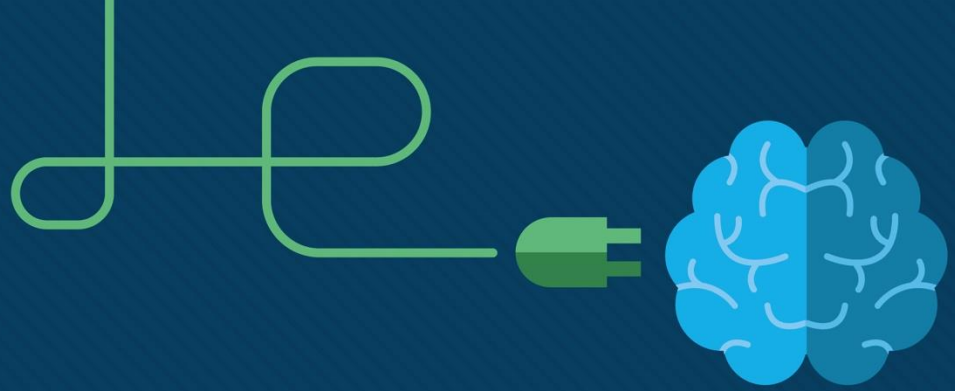
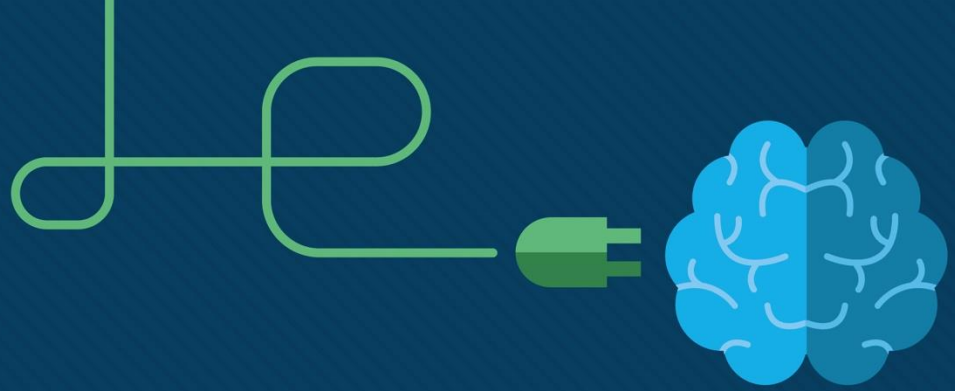


Modul 17: Einrichten eines kleinen Netzwerks

Unterlagen für Instruktoren

Einführung in Netzwerke v7.0
(ITN)



Modul 17: Einrichten eines kleinen Netzwerks

Einführung in Netzwerke v7.0
(ITN)

Modulziele

Modultitel: Aufbau eines kleinen Netzwerks

Modulziel: Implementierung eines Netzwerkdesigns für ein kleines Netzwerk, das einen Router, einen Switch und Endgeräte umfasst.

Thema	Ziel
Geräte in einem kleinen Netzwerk	Identifizieren Sie die Geräte, die in einem kleinen Netzwerk verwendet werden.
Anwendungen und Protokolle für kleine Netzwerke	Identifizieren Sie die Protokolle und Anwendungen, die in einem kleinen Netzwerk verwendet werden.
Skalieren auf größere Netzwerke	Erklären Sie, wie ein kleines Netzwerk als Grundlage für größere Netzwerke dient.
Verbindung überprüfen	Verwenden Sie die Ausgabe der Befehle ping und tracert, um die Konnektivität zu überprüfen und die relative Netzwerkleistung festzulegen.
Host- und IOS-Befehle	Verwenden Sie Host- und IOS-Befehle, um Informationen über die Geräte in einem Netzwerk zu erhalten.
Methoden der Fehlerbehebung	Beschreiben Sie gängige Methoden zur Fehlerbehebung im Netzwerk.
Fehlerbehebungsszenarien	Beheben von Problemen mit Geräten im Netzwerk.

17.1 Geräte in einem kleinen Netzwerk

Topologien kleiner Netzwerke

- Die Mehrheit der Unternehmen sind klein, deshalb sind die meisten der Unternehmensnetzwerke auch klein.
- Ein kleines Netzwerkdesign ist normalerweise einfach.
- Kleine Netzwerke verfügen in der Regel über eine einzelne WAN-Verbindung, die über DSL-, Kabel- oder Ethernet-Verbindung bereitgestellt wird.
- Für große Netzwerke ist eine IT-Abteilung erforderlich, um Netzwerkgeräte zu warten, zu sichern, um Fehler zu beheben und Organisationsdaten zu schützen. Kleine Netzwerke werden von einem lokalen IT-Techniker oder von einem beauftragten Fachmann verwaltet.

Geräteauswahl für ein kleines Netzwerk

Wie große Netzwerke erfordern auch kleine Netzwerke Planung und Design, um die Anforderungen der Benutzer zu erfüllen. Die Planung gewährleistet, dass alle Anforderungen, Kostenfaktoren und Bereitstellungsoptionen angemessen berücksichtigt werden. Eine der ersten Entwurfsüberlegungen ist die Art der zwischengeschalteten Geräte, die zur Unterstützung des Netzwerks verwendet werden sollen.

Faktoren, die bei der Auswahl von Netzwerkgeräten berücksichtigt werden müssen, sind:

- Kosten
- Geschwindigkeit und Port- /Schnittstellentypen
- Erweiterbarkeit
- Betriebssystemfunktionen und -dienste

IP-Adressierung für ein kleines Netzwerk

Erstellen Sie bei der Implementierung eines Netzwerks ein IP-Adressierungsschema und verwenden Sie es. Alle Hosts und Geräte in einem Netzwerkverbund müssen über eine eindeutige Adresse verfügen. Geräte, die in das IP-Adressierungsschema einbezogen werden, umfassen Folgendes:

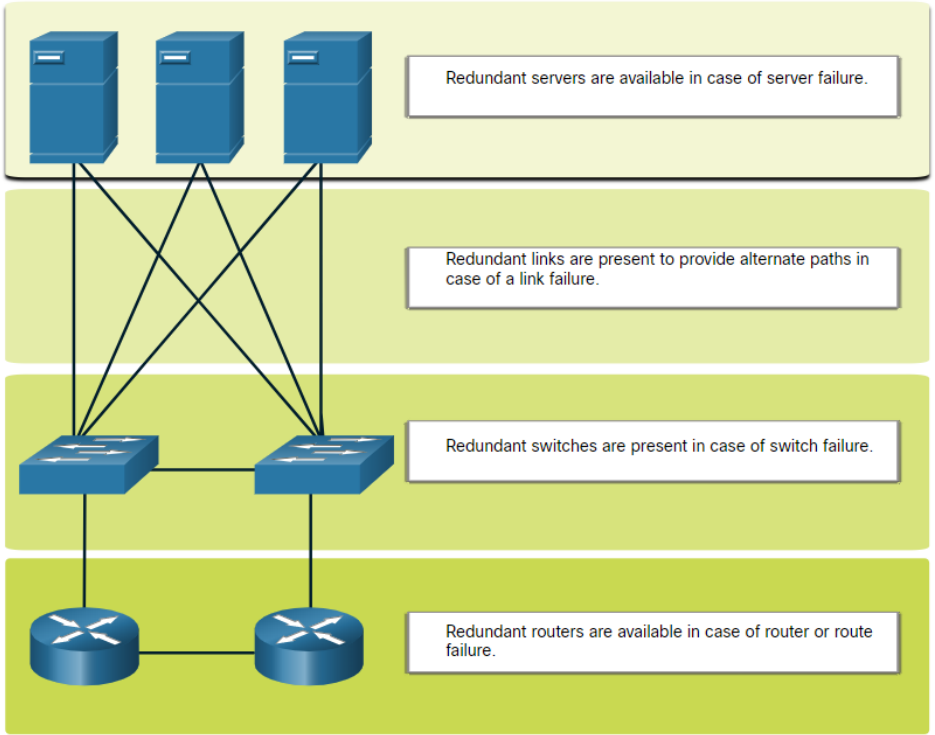
- Endbenutzer-Geräte - Anzahl und Art der Verbindungen (z. B. kabelgebunden, drahtlos, Fernzugriff)
- Server und Peripheriegeräte (z. B. Drucker und Sicherheitskameras)
- Vermittlungsgeräte einschließlich Switches und Access Points

Es wird empfohlen, ein IP-Adressierungsschema basierend auf dem Gerätetyp zu planen, zu dokumentieren und beizubehalten. Die Verwendung eines geplanten IP-Adressierungsschemas erleichtert die Identifizierung eines Gerätetyps und die Behebung von Problemen.

Netzwerkredundanz in einem kleinen Netzwerk

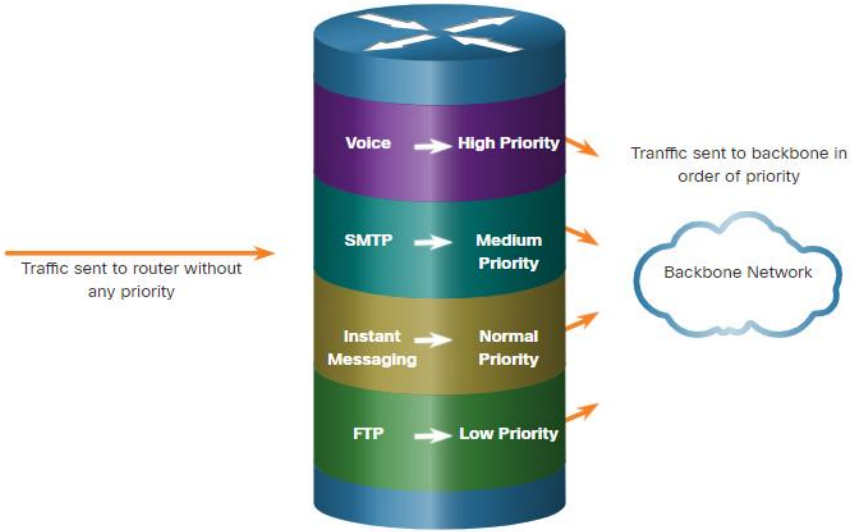
Um ein hohes Maß an Zuverlässigkeit sicherzustellen, muss *Redundanz* beim Netzwerkdesign berücksichtigt werden. Redundanz hilft dabei, Single Points of Failure zu beseitigen.

Redundanz kann durch die Installation von doppelten Geräten erreicht werden. Dies kann auch durch die Bereitstellung von mehrfachen Netzwerkverbindungen für kritische Bereiche erreicht werden.



Traffic Management

- Das Ziel eines guten Netzwerkdesigns ist es, die Produktivität der Mitarbeiter zu steigern und die Ausfallzeiten des Netzwerks zu minimieren.
- Die Router und Switches in einem kleinen Netzwerk müssen so konfiguriert werden, dass sie Echtzeitdatenverkehr wie Sprache und Video unterstützten und diesen klar vom anderen Datenverkehr trennen. Ein gutes Netzwerkdesign beinhaltet Quality of Service (QoS).
- Prioritäts-Queuing umfasst vier Warteschlangen. Die Warteschlange mit hoher Priorität wird immer zuerst abgearbeitet.



17.2 Anwendungen und Protokolle für kleine Netzwerke

Allgemeine Anwendungen

Nachdem Sie es eingerichtet haben, benötigt Ihr Netzwerk weiterhin bestimmte Arten von Anwendungen und Protokollen, um zu arbeiten. Das Netzwerk ist nur so nützlich, wie die in ihm verfügbaren Anwendungen.

Es gibt zwei Arten von Softwareprogrammen oder -prozessen, die Zugriff auf das Netzwerk bieten: Netzwerkanwendungen und Dienste der Anwendungsschicht.

- **Netzwerkanwendungen**: Anwendungen, die Protokolle der Anwendungsschicht integrieren und in der Lage sind, direkt mit den unteren Schichten des Protokollstapels zu kommunizieren.
- **Application Layer Services**: Für Anwendungen, die nicht netzwerkfähig sind, die Programme, die mit dem Netzwerk verbunden sind und die Daten für die Übertragung vorbereiten.

Gemeinsame Protokolle

Netzwerkprotokolle unterstützen die Anwendungen und Dienste, die von Mitarbeitern in einem kleinen Netzwerk verwendet werden.

- Netzwerkadministratoren benötigen häufig Zugriff auf Netzwerkgeräte und Server. Die beiden gängigsten Remote-Zugriffslösungen sind Telnet und Secure Shell (SSH).
- Hypertext Transfer Protocol (HTTP) und Hypertext Transfer Protocol Secure (HTTPS) werden zwischen Webclients und Webservern verwendet.
- Simple Mail Transfer Protocol (SMTP) wird zum Senden von E-Mails , Post Office Protocol (POP3) oder Internet Mail Access Protocol (IMAP) werden von Clients zum Abrufen von E-Mails verwendet.
- File Transfer Protocol (FTP) und Security File Transfer Protocol (SFTP) werden zum Herunterladen und Hochladen von Dateien, zwischen einem Client und einem FTP-Server, verwendet.
- DHCP (Dynamic Host Configuration Protocol) wird von Clients verwendet, um eine IP-Konfiguration von einem DHCP-Server zu erhalten.
- Der Domain Name Service (DNS) löst Domänennamen in IP-Adressen auf.

Hinweis: Ein Server kann mehrere Netzwerkdienste bereitstellen. Zum Beispiel könnte ein Server ein E-Mail-, FTP- und SSH-Server sein.

Gemeinsame Protokolle (Fortf.)

Diese Netzwerkprotokolle bilden das grundlegende Handwerkszeug eines Netzwerkprofis, und definitiert:

- Prozesse an beiden Enden einer Kommunikationssitzung.
- Arten von Nachrichten.
- Syntax der Meldungen.
- Bedeutung von Informationsfeldern.
- Wie Nachrichten gesendet werden und die erwartete Antwort.
- Interaktion mit der nächst unteren Schicht.

Viele Unternehmen haben, wo es möglich ist, Richtlinien zur Verwendung sicherer Versionen dieser Protokolle eingeführt (z.B. SSH,SRTP und HTTPS).

Sprach- und Videoanwendungen

- Unternehmen nutzen heutzutage zunehmend IP-Telefonie und Streaming Media, um mit Kunden und Geschäftspartnern zu kommunizieren und ihren Mitarbeitern die Möglichkeit zu geben, auch aus der Ferne zu arbeiten.
- Der Netzwerkadministrator muss sicherstellen, dass die entsprechenden Geräte im Netzwerk installiert und so konfiguriert sind, dass eine priorisierte Zustellung sichergestellt wird.
- Die Faktoren, die Netzwerkadministratoren kleiner Netzwerke bei der Unterstützung von Echtzeitanwendungen berücksichtigen müssen:
  - **Infrastruktur:** Verfügt es über die Kapazität und Fähigkeit, Echtzeitanwendungen zu unterstützen?
  - **VoIP -** VoIP ist in der Regel günstiger als IP-Telefonie, aber auf Kosten von Qualität und Funktionen.
  - **IP-Telefonie -** Dabei kommen dedizierte Server für die Anrufsteuerung und Signalisierung zum Einsatz.
  - **Echtzeitanwendungen -**Das Netzwerk muss QoS-Mechanismen (Quality of Service) unterstützen, um Latenzprobleme zu minimieren. Echtzeit-Transportprotokoll (RTP) und Echtzeit-Transportsteuerungsprotokoll (RTCP) und zwei Protokolle , die Echtzeitanwendungen unterstützen .

17.3 Skalierung auf größere Netzwerke

Geringer Netzwerkzuwachs

Wachstum ist ein natürlicher Prozess für viele kleine und mittlere Unternehmen und ihre Netzwerke müssen entsprechend mitwachsen. Idealerweise hat der Netzwerkadministrator genügend Vorlaufzeit, um intelligente Entscheidungen bezüglich der Erweiterung des Netzwerks im Einklang mit dem Unternehmenswachstum zu treffen.

Zur Skalierung eines Netzwerks ist eine Reihe von Elementen erforderlich:

- **Netzwerkdokumentation** - Physische und logische Topologie
- **Geräteinventar** – Liste der Geräte, die das Netzwerk **nutzen bzw. aus denen dieses besteht**
- **Budget** -Einzelplanung des IT-Budgets, einschließlich des Budgets für den Erwerb von Ausrüstung im Geschäftsjahr
- **Traffic-Analyse** – Protokolle, Anwendungen, Dienste und deren Datenverkehrsanforderungen; sollte dokumentiert werden

Diese Elemente fließen in die Entscheidungsfindung bezüglich der Skalierung eines kleinen Netzwerks mit ein.

Protokollanalyse

Es ist wichtig, die Art des Verkehrs, der das Netz durchquert, sowie den aktuellen Verkehrsfluss zu verstehen. Es gibt mehrere Netzwerkverwaltungstools, die für diesen Zweck verwendet werden können.

Um Verkehrsflussmuster zu bestimmen, ist es wichtig, Folgendes zu tun:

- Datenverkehr während der Stoßnutzungszeiten zu erfassen, um einen guten Überblick über die verschiedenen Arten von Datenverkehr zu erhalten.
- Führen Sie die Erfassung auf verschiedenen Netzwerksegmenten und Geräten durch, da ein Teil des Datenverkehrs lokal in einem bestimmten Segment stattfindet.
- die vom Protokollanalysator gesammelten Informationen basierend auf der Quelle und dem Ziel des Datenverkehrs sowie der Art des gesendeten Datenverkehrs zu analysieren.
- Diese Analyse kann dazu dienen, Entscheidungen über eine effizientere Verwaltung des Datenverkehrs zu treffen.

Mitarbeiternetzwerkauslastung

Viele Betriebssysteme bieten integrierte Tools, um solche Informationen zur Netzwerkauslastung anzuzeigen. Diese Tools können verwendet werden, um einen „Schnappschuss“ von Informationen wie den folgenden zu erfassen:

- Betriebssystem und Betriebssystemversion
- CPU-Auslastung
- RAM Nutzung
- Festplattennutzung
- Nicht-Netzwerkanwendungen
- Netzwerkanwendungen

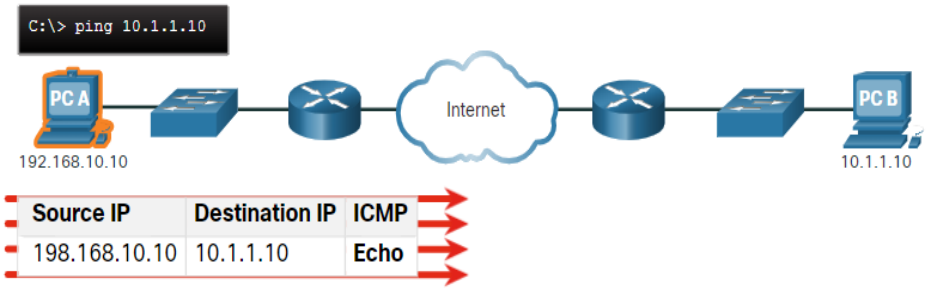
Die Dokumentation von Snapshots für Mitarbeiter in einem kleinen Netzwerk über einen bestimmten Zeitraum ist sehr nützlich, um sich entwickelnde Protokollanforderungen und zugehörige Datenverkehrsströme zu identifizieren.

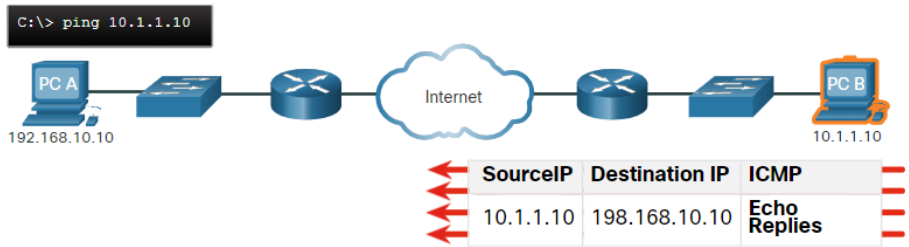
17.4 Überprüfen Sie die Konnektivität

Überprüfen der Konnektivität mit Ping

Unabhängig davon, ob Ihr Netzwerk klein und neu ist oder ob Sie ein bestehendes Netzwerk skalieren, Sie werden immer in der Lage sein wollen, zu überprüfen, ob Ihre Komponenten ordnungsgemäß miteinander und mit dem Internet verbunden sind.

- Der Befehl ping, der auf den meisten Betriebssystemen verfügbar ist, ist die effektivste Möglichkeit, die Layer-3-Konnektivität zwischen einer Quell- und Ziel-IP-Adresse schnell zu testen.
- Der Befehl ping verwendet die ICMP (Internet Control Message Protocol) echo (ICMP Type 8) und echo Antwort (ICMP Type 0) Nachrichten.





Überprüfen der Konnektivität mit Ping (Fortsetzung)

Auf einem Windows 10-Host sendet der Befehl ping vier aufeinanderfolgende ICMP-Echo-Nachrichten und erwartet vier aufeinanderfolgende ICMP-Echo-Antworten vom Ziel. Der IOS-Ping sendet fünf ICMP-Echo-Nachrichten und zeigt einen Indikator für jede empfangene ICMP-Echo-Antwort an.

IOS Ping Indikatoren sind wie folgt:

Element	Beschreibung
!	•Ausrufezeichen zeigt den erfolgreichen Empfang einer Echo-Antwortnachricht an. •Es validiert eine Layer-3-Verbindung zwischen Quelle und Ziel.
.	•Ein Zeitraum bedeutet, dass die Zeit abgelaufen ist, die auf eine Echo-Antwortnachricht wartet. •Dies deutet, dass irgendwo entlang des Pfads ein Verbindungsproblem aufgetreten ist.
U	•Das großgeschriebene **U** zeigt an, dass ein Router entlang des Pfads mit einer ICMP-Nachricht geantwortet hat, dass das Ziel nicht erreichbar ist. •Mögliche Gründe sind, dass der Router die Richtung zum Zielnetzwerk nicht kennt oder der Host im Zielnetzwerk nicht gefunden werden konnte.

Hinweis: Andere mögliche Ping-Antworten sind Q, M,? oder &. Die Bedeutung dieser Antworten ist jedoch für dieses Modul nicht von Belang.

Erweiterter Ping

Das Cisco IOS bietet einen "erweiterten" Modus des **Ping** Befehls.

Der erweiterte Ping wird im privilegierten EXEC-Modus durch Eingabe von **ping** ohne Ziel-IP-Adresse aufgerufen. Sie erhalten dann mehrere Eingabeaufforderungen, um den erweiterten **Ping**anzupassen.

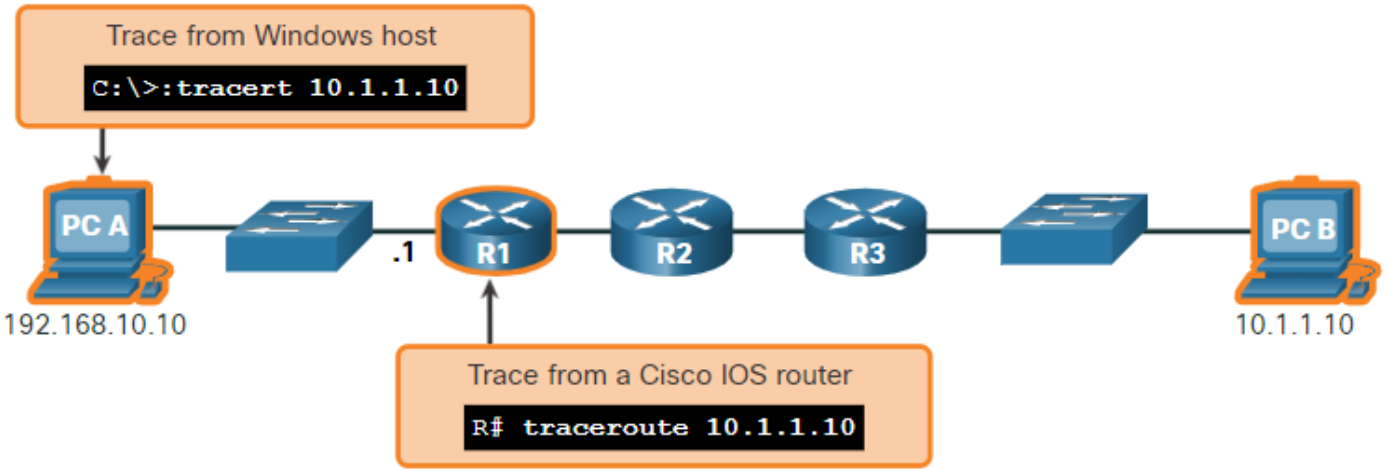
Hinweis: Durch Drücken **von Enter** werden die angegebenen Standardwerte akzeptiert. Der Befehl **ping ipv6** wird für erweiterte IPv6-Pings verwendet.

```
R1# ping
Protocol [ip]:
Target IP address: 10.1.1.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Ingress ping [n]:
Source address or interface: 192.168.10.1
DSCP Value [0]:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0x0000ABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R1#
```

Überprüfen der Konnektivität mit Traceroute

Der Befehl ping ist nützlich, um schnell festzustellen, ob ein Layer 3-Konnektivitätsproblem vorliegt. Es identifiziert jedoch nicht, wo sich das Problem entlang des Pfades befindet.

- Traceroute kann helfen, Layer 3-Problembereiche in einem Netzwerk zu finden. Der Befehl „trace“ gibt eine Liste der Hops zurück, entlang derer ein Paket durch ein Netzwerk geroutet wird.
- Die Syntax des trace-Befehls variiert zwischen den Betriebssystemen.



Überprüfen der Konnektivität mit Traceroute (Fortsetzung)

- Im Folgenden finden Sie eine Beispielausgabe des Befehls **tracert** auf einem Windows 10-Host.

  Hinweis: Verwenden Sie **Strg-C** , um ein **Tracert** in Windows zu unterbrechen.

- Die einzige erfolgreiche Antwort war vom Gateway auf R1. Die Zeitüberschreitung der Anforderungen an den nächsten Hop wurde wie durch das Sternchen (*) angegeben, was bedeutet, dass der nächste Hop-Router nicht reagiert hat oder ein Fehler im Netzwerkpfad vorliegt. In diesem Beispiel scheint ein Problem zwischen R1 und R2 zu bestehen.

```
C:\Users\PC-A> tracert 10.1.1.10
Tracing route to 10.1.10 over a maximum of 30 hops:
  1     2 ms     2 ms     2 ms  192.168.10.1
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
^C
C:\Users\PC-A>
```

Überprüfen der Konnektivität mit Traceroute (Fortsetzung)

Im Folgenden sind Beispielausgaben von traceroute Befehl von R1:

```
R1# traceroute 10.1.1.10
Type escape sequence to abort.
Tracing the route to 10.1.1.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 0 msec 1 msec
  2 209.165.200.230 1 msec 0 msec 1 msec
  3 10.1.1.10 1 msec 0 msec
R1#
```

```
R1# traceroute 10.1.1.10
Type escape sequence to abort.
Tracing the route to 10.1.1.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 0 msec 1 msec
  2 209.165.200.230 1 msec 0 msec 1 msec
  3  *  *  *
  4  *  *  *
  5  *
```

- Links bestätigte der Trace, dass er PC B erfolgreich erreichen konnte.
- Auf der rechten Seite war der 10.1.1.10-Host nicht verfügbar, und die Ausgabe zeigt Sternchen an, bei denen die Antwortzeitüberschreitung erreicht wurde. Timeouts weisen auf ein potenzielles Netzwerkproblem hin.
- Verwenden Sie **Strg-Shift-6** , um eine **Traceroute** in Cisco IOS zu unterbrechen.

Hinweis: Die Windows-Implementierung von Traceroute (tracert) sendet ICMP Echo Requests. Cisco IOS und Linux verwenden UDP mit einer ungültigen Portnummer. Das endgültige Ziel gibt eine ICMP-Port nicht erreichbar Nachricht zurück.

Erweiterte Traceroute

Wie der erweiterte **Ping** -Befehl gibt es auch einen erweiterten **traceroute** -Befehl . Es ermöglicht dem Administrator, Parameter im Zusammenhang mit der Befehlsausführung anzupassen.

Der Windows **tracert** -Befehl ermöglicht die Eingabe verschiedener Parameter über Optionen in der Befehlszeile. Es wird jedoch nicht wie der erweiterte traceroute IOS-Befehl geführt. Die folgende Ausgabe zeigt die verfügbaren Optionen für den Windows-Befehl **tracert** an:

```
C:\Users\PC-A> tracert /?
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name
Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
C:\Users\PC-A>
```

Erweiterte Traceroute (Fortsetzung)

- Die erweiterte Cisco IOS **Traceroute-Option** ermöglicht es dem Benutzer, eine spezielle Art von Trace zu erstellen, indem Parameter im Zusammenhang mit der Befehlsoperation angepasst werden.
- Erweitertes Traceroute wird im privilegierten EXEC-Modus eingegeben, indem man **traceroute** ohne Ziel-IP-Adresse eingibt. IOS führt Sie durch die Befehlsoptionen, indem eine Reihe von Eingabeaufforderungen angezeigt wird, die sich auf die Einstellung der verschiedenen Parameter beziehen.

- **Hinweis**:Durch Drücken **der Eingabetaste** werden die angezeigten Standardwerte übernommen.

```
R1# traceroute
Protocol [ip]:
Target IP address: 10.1.1.10
Ingress traceroute [n]:
Source address: 192.168.10.1
DSCP Value [0]:
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 192.168.10.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 1 msec 1 msec
  2 209.165.200.230 0 msec 1 msec 0 msec
  3  *
    10.1.1.10 2 msec 2 msec
R1#
```

Netzwerk Basislinie

- Eines der wirksamsten Hilfsmittel zur Überwachung der Netzwerkleistung und zur Fehlerbehebung ist das Erstellen einer Bezugsgrundlage oder Baseline für das Netzwerk.
- Eine Methode, um mit dem Erstellen einer Baseline zu beginnen, besteht darin, die Ergebnisse eines ausgeführten ping-, trace- oder eines anderen relevanten Befehls zu kopieren und in eine Textdatei einzufügen. Diese Textdatei kann mit einem Datumsstempel versehen und für den späteren Abruf und Vergleich in einem Archiv gespeichert werden.
- Zu berücksichtigen sind dabei u. a. Fehlermeldungen und die Antwortzeiten von Host zu Host.
- Für Unternehmensnetzwerke sollten umfangreiche Baselines zur Verfügung stehen – umfangreicher, als wir sie in diesem Kurs beschreiben können. Professionelle Software-Tools stehen für die Speicherung und Verwaltung von Baseline-Informationen zur Verfügung.

Labor - Testnetzwerk-Latenzzeit mit Ping und Traceroute

In dieser Übung werden Sie die folgenden Lernziele umsetzen:

- Teil 1: Verwenden des Befehls „ping“ zum Dokumentieren der Netzwerklatenz
- Teil 2: Verwenden des Befehls „traceroute“ zum Dokumentieren der Netzwerklatenz

17.5 Host- und IOS-Befehle

IP-Konfiguration auf einem Windows-Host

In Windows 10 können Sie über das **Netzwerk- und Freigabecenter** auf die IP-Adressdetails zugreifen, um schnell die vier wichtigen Einstellungen anzuzeigen: Adresse, Subnetzmaske, Standard Gateway und DNS. Oder Sie können den Befehl **ipconfig** in der Befehlszeile eines Windows-Computers ausgeben.

- Verwenden Sie den Befehl **ipconfig /all** , um die MAC-Adresse sowie eine Reihe von Details bezüglich der Layer-3-Adressierung des Geräts anzuzeigen.
- Wenn ein Host als DHCP-Client konfiguriert ist, kann die IP-Adresskonfiguration mit den Befehlen **ipconfig /release** und **ipconfig /renew** erneuert werden.
- Der DNS-Client-Dienst auf Windows-PCs optimiert außerdem die Leistung der DNS-Namensauflösung, indem zuvor aufgelöste Namen gespeichert werden. Der Befehl **ipconfig /displaydns** zeigt alle zwischengespeicherten DNS-Einträge auf einem Windows-Computersystem an.

```
C:\Users\PC-A> ipconfig
Windows IP Configuration
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
   IPv4 Address. . . . . . . . . . . : 192.168.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1
(Output omitted)
```

IP-Konfiguration auf einem Linux-Host

- Die Überprüfung der IP-Einstellungen mit der GUI auf einem Linux-Computer unterscheidet sich je nach Linux-Distribution und Desktop-Schnittstelle.
- Verwenden Sie in der Befehlszeile den Befehl **ifconfig** , um den Status der aktuell aktiven Schnittstellen und deren IP-Konfiguration anzuzeigen.
- Der Linux- **IP-Adressenbefehl** wird verwendet, um Adressen und deren Eigenschaften anzuzeigen. Es kann auch verwendet werden, um IP-Adressen hinzuzufügen oder zu löschen.

```
[analyst@secOps ~]$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:b5:d6:cb
          inet addr: 10.0.2.15  Bcast:10.0.2.255  Mask: 255.255.255.0
          inet6 addr: fe80::57c6:ed95:b3c9:2951/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1332239 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105910 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1855455014 (1.8 GB)  TX bytes:13140139 (13.1 MB)
lo: flags=73  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Hinweis: Die angezeigte Ausgabe kann je nach Linux-Distribution variieren.

IP-Konfiguration auf einem macOS-Host

- Öffnen Sie in der Benutzeroberfläche eines Mac-Hosts **Netzwerkeinstellungen > Erweitert** , um die IP-Adressierungsinformationen abzurufen.
- Der Befehl **ifconfig** kann auch verwendet werden, um die IP-Konfiguration der Schnittstelle in der Befehlszeile zu überprüfen.
- Weitere nützliche macOS-Befehle zur Überprüfung der Host-IP-Einstellungen sind **networksetup -listallnetworkservices** und der **networksetup -getinfo <** *Netzwerkdienst* **.>**.

```
MacBook-Air:~ Admin$ networksetup -listallnetworkservices
An asterisk (*) denotes that a network service is disabled.
iPhone USB
Wi-Fi
Bluetooth PAN
Thunderbolt Bridge
MacBook-Air:~ Admin$
MacBook-Air:~ Admin$ networksetup -getinfo Wi-Fi
DHCP Configuration
IP address: 10.10.10.113
Subnet mask: 255.255.255.0
Router: 10.10.10.1
Client ID:
IPv6: Automatic
IPv6 IP address: none
IPv6 Router: none
Wi-Fi ID: c4:b3:01:a0:64:98
MacBook-Air:~ Admin$
```

Der Befehl arp

Der **arp**-Befehl wird in der Windows-, Linux- oder Mac-Eingabeaufforderung aus ausgeführt. Der Befehl listet alle Geräte auf, die sich derzeit im ARP-Cache des Hosts befinden.

- Der Befehl **arp -a** zeigt die bekannten IP-Adressen und die MAC-Adressbindungen an. Der ARP-Cache zeigt nur Informationen von Geräten an, auf die kürzlich zugegriffen wurde.
- Um sicherzustellen, dass der ARP-Cache gefüllt ist, senden Sie ein **ping** an ein Gerät, damit dieses einen Eintrag in der ARP-Tabelle erhält.
- Der Cache kann mithilfe des Befehls **arp -d** gelöscht werden, falls der Netzwerkadministrator den Cache mit aktualisierten Daten auffüllen möchte.

Hinweis: Möglicherweise benötigen Sie Administratorzugriff auf dem Host, um den Befehl **netsh interface ip delete arpcache** verwenden zu können .

Gängige Show-Befehle

Befehl	Beschreibung
show running-config	Überprüft die aktuelle Konfiguration und Einstellungen
show interfaces	Überprüft den Schnittstellenstatus und zeigt Fehlermeldungen an
show ip interface	Überprüft die Layer-3-Informationen einer Schnittstelle
show arp	Überprüft die Liste der bekannten Hosts auf den lokalen Ethernet-LANs
show ip route	Überprüft die Layer-3-Routinginformationen
show protocols	Prüft, welche Protokolle betriebsbereit sind
show version	Verifiziert den Speicher, Schnittstellen und Lizenzen des Geräts

Der Befehl show cdp neighbors

CDP liefert die folgenden Informationen zu allen CDP-Nachbargeräten:

- **Gerätekennungen** – Gibt beispielsweise den für einen Switch, Router oder andere Geräte konfigurierten Hostnamen an.
- **Adressliste** – Bis zu eine Vermittlungsschichtadresse für jedes unterstützte Protokoll.
- **Port-Kennung** – Der Name des lokalen und Remote-Ports in Form einer ASCII-Zeichenfolge, z. B. FastEthernet 0/0.
- **Liste der Funktionen** - Gibt an, ob ein bestimmtes Gerät ein Layer 2-Switch oder ein Layer 3-Switch**ist.**
- Plattform **- Die Hardwareplattform des Geräts (WS-C2960 für den Cisco 2960-Switch)**

Der Befehl **show cdp neighbors detail** gibt die IP-Adresse eines benachbarten Geräts zurück.

```
R3# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S3               Gig 0/0/1         122              S I   WS-C2960+ Fas 0/5
Total cdp entries displayed : 1
R3#
```

Der Befehl show ip interface brief

Einer der am häufigsten verwendeten Befehle ist **show ip interface brief** . Dieser Befehl gibt eine kürzere Ausgabe als der Befehl **show ip interface** zurück. Er liefert eine Zusammenfassung der wichtigsten Informationen für alle Netzwerkschnittstellen auf einem Router.

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   209.165.200.225 YES manual up                    up
GigabitEthernet0/0/1   192.168.10.1    YES manual up                    up
Serial0/1/0            unassigned      NO  unset  down                  down
Serial0/1/1            unassigned      NO  unset  down                  down
GigabitEthernet0       unassigned      YES unset  administratively down down
R1#
```

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.254.250 YES manual up                    up
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  up                    up
FastEthernet0/3        unassigned      YES unset  up                    up
```

Video — Der Befehl show version

In diesem Video wird die Verwendung des Befehls show version veranschaulicht, um Informationen über den Router anzuzeigen.

Packet Tracer — Interpretieren der Show Befehlsausgabe

Diese Aktivität dient dazu, die Verwendung von **show**-Befehlen des Routers zu üben. Sie müssen nichts konfigurieren, sondern untersuchen vielmehr die Ausgabe mehrerer show-Befehle.

17.6 Methoden zur Fehlerbehebung

Fehlerbehebungsmethoden

Grundlegende Ansätze zur Fehlerbehebung

Schritt	Beschreibung
Schritt 1: Identifizieren des Problems	•Dieses ist der erste Schritt des Fehlerbehebungsprozesses. •Obwohl in diesem Schritt Werkzeuge verwendet werden können, ist ein Gespräch mit dem Benutzer oft sehr hilfreich.
Schritt 2: Aufstellen einer Theorie über die wahrscheinlichen Ursachen	•Nachdem das Problem identifiziert wurde, versuchen Sie, eine Theorie der wahrscheinlichen Ursachen aufzustellen. •Bei diesem Schritt ergeben sich oftmals mehrere mögliche Problemursachen.
Schritt 3: Testen der Theorie zur Ermittlung der Ursache	•Testen Sie Ihre Theorien auf Basis der wahrscheinlichen Ursachen, um festzustellen, welche die tatsächliche Ursache des Problems ist. •Ein Techniker wendet häufig ein Schnelltestverfahren an, um zu testen und zu prüfen, ob das Problem dadurch behoben wird. •Wenn ein Schnellverfahren das Problem nicht behebt, müssen Sie weitersuchen, um die genaue Ursache zu ermitteln.
Schritt 4: Erstellen eines Aktionsplans zur Fehlerbehebung und Implementierung der Lösung	Nachdem Sie die genaue Ursache des Problems ermittelt haben, erstellen Sie einen Aktionsplan, um den Fehler zu beheben und die Lösung zu implementieren.
Schritt 5: Verifizierung der Lösung und Implementieren von Präventivmaßnahmen	•Nachdem Sie das Problem behoben haben, überprüfen Sie die volle Funktionalität. •Falls möglich, wenden Sie präventive Maßnahmen an.
Schritt 6: Dokumentieren von Erkenntnissen, Maßnahmen und Ergebnissen	•Im letzten Schritt des Fehlerbehebungsverfahrens sollten Sie Ihre Erkenntnisse, Maßnahmen und Ergebnisse dokumentieren. •Dies ist als zukünftige Referenz sehr wichtig.

Auflösen oder eskalieren?

- In manchen Fällen ist es eventuell nicht möglich, das Problem sofort zu beheben. Ein Problem sollte eskaliert werden, wenn die Entscheidung eines Managers, spezielles Fachwissen oder eine Netzwerkzugriffsstufe benötigt wird, über die der Fehlerbehebungstechniker nicht verfügt.
- Aus den Richtlinien eines Unternehmens sollte klar hervorgehen, wann und wie ein Techniker ein Problem eskalieren muss.

Der debug Befehl

- Der IOS **debug** -Befehl ermöglicht es dem Administrator, OS-Prozess-, Protokoll-, Mechanismus- und Ereignisnachrichten in Echtzeit zur Analyse anzuzeigen.
- Alle **debug** -Befehle werden im privilegierten EXEC-Modus eingegeben. In Cisco IOS kann die Ausgabe von **debug** so eingeschränkt werden, dass nur die relevante Funktion oder Teilfunktion eingeschlossen wird. Verwenden Sie den Befehl **debug** deshalb nur, um spezifische Probleme zu beheben.
  - Um eine kurze Beschreibung aller Optionen des debug-Befehls aufzulisten, geben Sie im privilegierten EXEC-Modus in der Befehlszeile den Befehl **debug ?** ein.
  - Um eine bestimmte Debugging-Funktion zu deaktivieren, fügen Sie das Schlüsselwort **no** vor dem Befehl **debug** hinzu:
  - Alternativ können Sie die Befehlsvariante **undebug** im privilegierten EXEC-Modus eingeben:
  - Um alle aktiven debug-Befehle gleichzeitig zu deaktivieren, verwenden Sie den Befehl **undebug all** :
- Seien Sie vorsichtig bei der Verwendung von einigen **debug** -Befehlen, da diese eine beträchtliche Menge an Output erzeugen und einen großen Teil der Systemressourcen in Anspruch nehmen können. Der Router wäre in diesem Fall durch die Anzeige von **Debug** -Meldungen überlastet und hätte nicht mehr genügend Verarbeitungsleistung zur Ausführung von Netzwerkfunktionen bzw. könnte nicht mehr auf Befehle zum Deaktivieren des Debugging-Vorgangs reagieren.

Der terminal monitor Befehl

- **debug** und bestimmte andere IOS-Nachrichtenausgaben werden nicht automatisch auf Remote-Verbindungen angezeigt. Dies liegt daran, dass Protokollmeldungen nicht in vty-Zeilen angezeigt werden.
- Um Protokollmeldungen auf einem Terminal (virtuelle Konsole) anzuzeigen, verwenden Sie den privilegierten EXEC-Befehl **terminal monitor** . Um das Protokollieren von Meldungen auf einem Terminal zu stoppen, verwenden Sie den privilegierten EXEC-Befehl **terminal no monitor** .

```
R2# telnet 209.165.200.225
Trying 209.165.200.225 ... Open
 Authorized access only!
User Access Verification
Password:
R1> enable
Password:
R1# debug ip icmp
ICMP packet debugging is on
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
```

```
R1#  terminal monitor
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
*Aug 20 16:03:49.735: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.737: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.738: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.740: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.741: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
R1# no debug ip icmp
ICMP packet debugging is off
R1#
```

17.7 Fehlersuche Szenarien

Duplexbetrieb und Mismatch-Probleme

- Miteinander verbundene Ethernet-Schnittstellen müssen im gleichen Duplexmodus betrieben werden, um eine optimale Kommunikationsleistung zu erzielen und Ineffizienz und Latenz auf der Verbindung zu vermeiden .
- Die Ethernet-Autonegotiationsfunktion erleichtert die Konfiguration, minimiert Probleme und maximiert die Verbindungsleistung zwischen zwei miteinander verbundenen Ethernet-Anschlüssen. Die verbundenen Geräte kündigen zuerst die unterstützten Funktionen an und wählen dann den Modus mit der höchsten Leistung aus, der von beiden Seiten unterstützt wird.
- Wenn eines der beiden verbundenen Geräte im Vollduplex- und das andere im Halbduplex-Modus arbeitet, tritt eine Duplex-Diskrepanz auf. Zwar findet die Datenkommunikation bei einer Duplex-Diskrepanz immer noch statt, jedoch bei sehr schlechter Verbindungsleistung.
- Duplexfehler werden in der Regel durch eine falsch konfigurierte Schnittstelle oder in seltenen Fällen durch eine fehlgeschlagene Autonegotiation verursacht. Duplex-Diskrepanzen lassen sich möglicherweise nur schwer beheben, da die Kommunikation zwischen den Geräten weiterhin stattfindet.

IP-Adressierungsprobleme auf IOS-Geräten

- Zwei häufige Ursachen für eine falsche IPv4-Zuweisung sind Fehler bei der manuellen Zuweisung oder Probleme im Zusammenhang mit DHCP.
- Netzwerkadministratoren müssen IP-Adressen häufig manuell Geräten wie Server und Routern zuweisen. Wenn bei der Zuweisung ein Fehler gemacht wird, sind Kommunikationsprobleme mit dem Gerät sehr wahrscheinlich.
- Verwenden Sie auf einem IOS-Gerät den Befehl **show ip interface** oder **show ip interface brief** , um zu überprüfen, welche IPv4-Adressen den Netzwerkschnittstellen zugewiesen sind. Beispielsweise würde die Ausgabe des **show ip interface brief** Befehls wie gezeigt den Schnittstellenstatus auf R1 validieren.

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   209.165.200.225 YES manual up                    up
GigabitEthernet0/0/1   192.168.10.1    YES manual up                    up
Serial0/1/0            unassigned      NO  unset  down                  down
Serial0/1/1            unassigned      NO  unset  down                  down
GigabitEthernet0       unassigned      YES unset  administratively down down
R1#
```

IP-Adressierungsprobleme auf Endgeräten

- Wenn bei Windows-basierten Systemen das Gerät keinen DHCP-Server kontaktieren kann, weist Windows automatisch eine Adresse aus dem Bereich 169.254.0.0/16 zu. Diese Funktion wird als Automatic Private IP Addressing (APIPA) bezeichnet.
- Ein Computer mit einer APIPA-Adresse kann nicht mit anderen Geräten im Netzwerk kommunizieren, da diese Geräte höchstwahrscheinlich nicht zum Netzwerk 169.254.0.0/16 gehören.

  Hinweis: Andere Betriebssysteme, wie Linux und OS X, verwenden keine APIPA.
- Wenn das Gerät nicht mit dem DHCP-Server kommunizieren kann, kann der Server keine IPv4-Adresse für das spezifische Netzwerk zuweisen und das Gerät kann nicht kommunizieren.
- Um die einem Windows-basierten Computer zugewiesenen IP-Adressen zu überprüfen, verwenden Sie den Befehl **ipconfig** , wie in der Abbildung gezeigt.

Standard-Gateway-Probleme

- Das Standardgateway für ein Endgerät ist das nächstgelegene Netzwerkgerät , das zu dem selben Netzwerk wie das -Endgerät gehört, und Datenverkehr an andere Netzwerke weiterleiten kann. Wenn ein Gerät eine falsche oder eine nicht vorhandene Standardgateway-Adresse hat, kann es nicht mit Geräten in Remote-Netzwerken kommunizieren.
- Ähnlich wie IPv4-Adressierungsprobleme können auch Probleme mit dem Standardgateway auf eine falsche Konfiguration (bei manueller Zuweisung) oder auf DHCP-Probleme (bei automatischer Zuweisung) zurückzuführen sein.
- Um das Standardgateway auf Windows-basierten Computern zu überprüfen, verwenden Sie den Befehl **ipconfig**.
- Verwenden Sie auf einem Router den Befehl **show ip route**, um die Routing-Tabelle anzuzeigen und zu überprüfen, ob das Standardgateway festgelegt wurde. Diese Route wird verwendet, wenn die Zieladresse des Pakets mit keiner anderen Route in der Routing-Tabelle übereinstimmt.

Problembehandlung bei DNS-Problemen

- Es ist üblich, dass Benutzer fälschlicherweise den Betrieb eines Internetlinks mit der Verfügbarkeit des DNSin Beziehung setzen.
- DNS-Serveradressen können manuell oder automatisch über DHCP zugewiesen werden.
- Obwohl Unternehmen und Organisationen üblicherweise ihre eigenen DNS-Server verwalten, kann jeder erreichbare DNS-Server zum Auflösen von Namen verwendet werden.
- Cisco bietet OpenDNS, welches einen sicheren DNS-Dienst bietet, indem Phishing und einige Malware-Websites gefiltert werden. OpenDNS-Adressen sind 208.67.222.222 und 208.67.220.220. Erweiterte Funktionen wie Webinhaltsfilterung und Sicherheit stehen Heim- und Unternehmensnetzwerken zur Verfügung.
- Verwenden Sie den Befehl **ipconfig /all**, wie gezeigt, um zu überprüfen, welcher DNS-Server vom Windows-Computer verwendet wird.
- Der Befehl **nslookup** ist ein weiteres nützliches DNS-Fehlerbehebungs-Tool für PCs. Mit **nslookup** kann ein Benutzer DNS-Abfragen manuell tätigen und die DNS-Antwort analysieren.

Laborübung — Beheben von Verbindungsproblemen

In dieser Übung werden Sie die folgenden Lernziele umsetzen:

- Identifizieren des Problems
- Implementieren von Netzwerkänderungen
- Überprüfen der vollständigen Funktionalität
- Dokumentieren von Erkenntnisse und Konfigurationsänderungen

Packet Tracer – Fehlersuche bei Verbindungsproblemen

Ziel dieser Packet Tracer-Aktivität ist es, die Ursache von Verbindungsproblemen zu ermitteln und ggf. zu beheben. Wenn dies nicht möglich ist, sollten die Probleme eindeutig dokumentiert werden, sodass sie eskaliert werden können.

17.8 Modul Praxis und Quiz

Lab — Design und Aufbau eines kleinen Unternehmensnetzwerks

In diesem Labor entwerfen und bauen Sie ein Netzwerk. Sie werden erklären, wie ein kleines Netzwerk aus direkt verbundenen Segmenten erstellt, konfiguriert und verifiziert wird.

Packet Tracer – Überprüfen der Kenntnisse

In dieser Packet Tracer Aktivität werden Sie alle Fähigkeiten nutzen, die Sie in diesem Kurs erworben haben.

Szenario:

Der Router Central, der ISP-Cluster und der Webserver sind vollständig konfiguriert. Sie müssen ein neues IPv4-Adressierungsschema erstellen, das 4 Subnetze mit dem 192.168.0.0/24-Netzwerkaufnehmen kann. Die IT-Abteilung benötigt 25 Hosts. Die Vertriebsabteilung benötigt 50 Hosts. Das Subnetz für den Rest des Personals benötigt 100 Hosts. Ein Gast-Subnetz für 25 Hosts wird später hinzugefügt. Außerdem müssen Sie die grundlegenden Sicherheitseinstellungen und Schnittstellenkonfigurationen auf R1 abschließen. Anschließend konfigurieren Sie die SVI-Schnittstelle und die grundlegenden Sicherheitseinstellungen auf den Switches S1, S2 und S3.

Packet Tracer - Herausforderung der Fehlerbehebung

In dieser Paket Tracer Aktivität werden Sie in einem vorhandenen LAN eine Reihe von Problemen, mit Fehlersuche und -behebung beseitigen.

Was habe ich in diesem Modul gelernt?

- Faktoren, die bei der Auswahl von Netzwerkgeräten für ein kleines Netzwerk berücksichtigt werden müssen, sind Kosten, Geschwindigkeit und Arten von Ports/Interfaces, Erweiterbarkeit sowie Betriebssystemfunktionen und -dienste.
- Erstellen Sie bei der Implementierung eines Netzwerks ein IP-Adressierungsschema und verwenden Sie es auf Endgeräten, Servern und Peripheriegeräten sowie zwischengeschalteten Geräten.
- Redundanz kann durch die Installation doppelter Geräte erreicht werden, kann aber auch durch Bereitstellung eines doppelten Netzwerks erreicht werden. Links für kritische Bereiche .
- Die Router und Switches in einem kleinen Netzwerk müssen so konfiguriert werden, dass sie Echtzeitdatenverkehr wie Sprache und Video unterstützten und diesen klar vom anderen Datenverkehr trennen.
- Es gibt zwei Arten von Softwareprogrammen oder -prozessen, die Zugriff auf das Netzwerk bieten: Netzwerkanwendungen und Dienste der Anwendungsschicht.
- Um ein Netzwerk zu skalieren, sind mehrere Elemente erforderlich: Netzwerkdokumentation, Geräteinventar, Budget und Datenverkehrsanalyse.
- Der Befehl ping ist der effektivste Weg, um die Layer-3-Konnektivität zwischen einer Quell- und Ziel-IP-Adresse schnell zu testen.
- Das Cisco IOS bietet einen „erweiterten“ Modus des Ping-Befehls, mit dem der Benutzer spezielle Arten von Pings erstellen kann, indem Parameter im Zusammenhang mit der Befehlsoperation angepasst werden.

Was habe ich in diesem Modul gelernt (Fortsetzung)?

- Der Befehl „trace“ gibt eine Liste der Hops zurück, entlang derer ein Paket durch ein Netzwerk geroutet wird.
- Es gibt auch einen erweiterten traceroute-Befehl. Es ermöglicht dem Administrator, Parameter im Zusammenhang mit der Befehlsausführung anzupassen.
- Netzwerkadministratoren zeigen die IP-Adressierungsinformationen (Adresse, Subnetzmaske, Standard Gatewayadresse und DNS) auf einem Windows-Host an, indem Sie den Befehl ipconfig ausgeben. Weitere notwendige Befehle sind **ipconfig /all**, **ipconfig /release**und **ipconfig /renew**und **ipconfig /displaydns**.
- Das Überprüfen von IP-Einstellungen mithilfe der GUI auf einem Linux-Computer unterscheidet sich je nach Linux-Distribution (Distribution) und Desktop-Schnittstelle. Notwendige Befehle sind ifconfig und ip address.
- Öffnen Sie in der Benutzeroberfläche eines Mac-Hosts die Netzwerkeinstellungen > Erweitert, um die IP-Adressierungsinformationen abzurufen. Andere IP-Adressierungsbefehle für Mac sind ifconfig und networksetup -listallnetworkservices und networksetup -getinfo <network service>.
- Der **arp**-Befehl wird in der Windows-, Linux- oder Mac-Eingabeaufforderung aus ausgeführt. Der Befehl listet alle Geräte auf, die sich derzeit im ARP-Cache des Hosts befinden, einschließlich IPv4 Adresse, physische Adresse und die Art der Adressierung(statisch/dynamisch) für jedes Gerät.
- Der Befehl **arp -a** zeigt die bekannten IP-Adressen und die MAC-Adressbindungen an.

Was habe ich in diesem Modul gelernt (Fortsetzung)?

- Häufige Show-Befehle sind **show running-config**, **show interfaces, show ip address, show arp, showip route**, show protocol and **show version**. Der Befehl **show cdp neighbor** enthält die folgenden Informationen zu jedem CDP-Nachbargerät: Bezeichner, Adressliste, Portkennung, Capabilities-Liste und Plattform.
- Mithilfe des Befehls **show cdp neighbors detail** kann festgestellt werden, ob bei einem der CDP-Nachbargeräte ein IP-Konfigurationsfehler vorliegt.
- Die Ausgabe des Befehls **show ip interface brief** zeigt alle Schnittstellen auf dem Router an, die den einzelnen Schnittstellen zugewiesene IP-Adresse, falls vorhanden, sowie den Betriebsstatus der Schnittstelle.
- Die sechs grundlegenden Schritte zur Fehlerbehebung Schritt 1. Identifizieren des Problems Schritt 2. Theorie über die wahrscheinliche Ursache erstellen. Schritt 3: Testen der Theorie zur Ermittlung der Ursache Schritt 4: Erstellen eines Aktionsplans zur Fehlerbehebung und Implementierung der Lösung Schritt 5: Überprüfen Sie die Lösung und implementieren Sie vorbeugende Maßnahmen. Schritt 6: Dokumentieren der Erkenntnisse, Maßnahmen und Ergebnisse
- Ein Problem sollte eskaliert werden, wenn die Entscheidung eines Managers, spezielles Fachwissen oder eine Netzwerkzugriffsstufe benötigt wird, über die der Fehlerbehebungstechniker nicht verfügt.
- IOS-Prozesse, -Protokolle, -Mechanismen und -Ereignisse generieren Meldungen, um ihren Status mitzuteilen. Mit dem IOS-Befehl debug kann der Administrator diese Meldungen in Echtzeit zu Analysezwecken anzeigen.
- Um Protokollmeldungen auf einem Terminal (virtuelle Konsole) anzuzeigen, verwenden Sie den privilegierten EXEC-Befehl terminal monitor.


CISCO