KAPITEL 10

Ethernet-LAN-Designs analysieren

Während Ethernet die Abläufe in der Ethernet-Verbindung selbst definiert, werden die interessanteren und auch detaillierteren Prozesse an den Endpunkten dieser Leitungen ausgeführt: den Netzwerkkarten (NICs) in den Geräten und den LAN-Switches. Auf Grundlage der Erläuterungen in Kapitel 2, »Grundlagen zu Ethernet-LANs«, tauchen wir in diesem Kapitel tief in die vielfältigen Aspekte eines modernen Ethernet-LAN ein. Schwerpunktmäßig behandeln wir dabei das Gerät, mit dem solche LANs erstellt werden: den LAN-Switch.

Die Behandlung des Ethernet- und LAN-Switchings ist in diesem Kapitel in zwei große Abschnitte unterteilt. Im ersten Abschnitt beschreiben wir die von LAN-Switches bei der Weiterleitung von Ethernet-Frames verwendete Logik und die zugehörige Terminologie. Der zweite Abschnitt widmet sich Entwurfs- und Implementierungsproblemen, die beim Aufbau eines neuen Ethernet-LAN in einem Gebäude oder auf einem Campus auftreten können. Hier werden Themen wie die Verwendung von Switches für unterschiedliche Zwecke, die Auswahl zwischen verschiedenen Arten von Ethernet-Leitungen und die Nutzung des Autonegotiatings behandelt.

Fragen zur Einschätzung des Wissensstands

Beantworten Sie die Fragen (wahlweise hier oder mithilfe der PCPT-Software), um einzuschätzen, wie viel Zeit Sie für dieses Kapitel einplanen sollten. Die Antworten stehen am unteren Rand der Seite, die auf die Seite mit den Fragen folgt. Erläuterungen finden Sie im Anhang C auf der DVD sowie in der PCPT-Software.

Tabelle 10.1 Fragen zur Einschätzung des Wissensstands: Zuordnung von Grundlagenthemen und Fragen

Grundlagenthema	Fragen
Kollisions- und Broadcast-Domänen analysieren	1–2
Campus-LAN-Topologien analysieren	3–5
Standardoptionen im Physical Layer für das LAN analysieren	6

1. Welches der folgenden Geräte würde sich in derselben Kollisionsdomäne wie PC1 befinden?
   - **a.** PC2, der von PC1 durch einen Ethernet-Hub getrennt ist
   - **b.** PC3, der von PC1 durch eine transparente Bridge getrennt ist
   - **c.** PC4, der von PC1 durch einen Ethernet-Switch getrennt ist
   - **d.** PC5, der von PC1 durch einen Router getrennt ist

2. Welches der folgenden Geräte befindet sich in derselben Broadcast-Domäne wie PC1? (Wählen Sie drei Antworten aus.)

- **a.** PC2, der von PC1 durch einen Ethernet-Hub getrennt ist
- **b.** PC3, der von PC1 durch eine transparente Bridge getrennt ist
- **c.** PC4, der von PC1 durch einen Ethernet-Switch getrennt ist
- **d.** PC5, der von PC1 durch einen Router getrennt ist

3. Welche der folgenden Aussagen sind normalerweise für die Topologie eines Campus-LAN-Modells mit zwei Ebenen zutreffend? Wählen Sie zwei Antworten aus.

- **a.** Das Modell basiert auf einer Full-Mesh-Topologie zwischen Access- und Distribution-Switches.
- **b.** Das Modell basiert auf einer Partial-Mesh-Topologie zwischen Access- und Distribution-Switches.
- **c.** Das Modell basiert auf einer Partial-Mesh-Topologie zwischen Distribution- und Core-Switches.
- **d.** Die Endbenutzer- und Servergeräte sind direkt an die Access-Layer-Switches angeschlossen.

4. Welche der folgenden Aussagen sind normalerweise für die Topologie eines Campus-LAN-Modells mit drei Ebenen zutreffend? Wählen Sie zwei Antworten aus.

- **a.** Das Modell basiert auf einer Partial-Mesh-Topologie zwischen Access- und Distribution-Switches.
- **b.** Das Modell basiert auf einer Full-Mesh-Topologie zwischen Access- und Distribution-Switches.
- **c.** Das Modell basiert auf einer Partial-Mesh-Topologie zwischen Distribution- und Core-Switches.
- **d.** Die Endbenutzer- und Servergeräte sind direkt an die Distribution-Layer-Switches angeschlossen.

5. Welche der folgenden Aussagen stellt die beste Zuordnung zwischen einem Teil eines typischen 3-Ebenen-Modells und der Idee dar, die dem angegebenen allgemeinen Begriff aus dem Bereich des Topologiedesigns zugrunde liegt?

- **a.** Der Access-Layer sieht wie eine Partial-Mesh-Topologie aus.
- **b.** Der Distribution-Layer sieht wie eine Full-Mesh-Topologie aus.
- **b.** Der Distribution-Layer sieht wie ein Hybriddesign aus.
- **b.** Der Access-Layer sieht wie eine Sterntopologie aus.

6. Welche der folgenden Ethernet-Standards unterstützen eine maximale Kabellänge von mehr als 100 Metern? Wählen Sie zwei Antworten aus.

- **a.** 100BASE-T
- **b.** 1000BASE-SX
- **c.** 1000BASE-T
- **d.** 1000BASE-LX

Grundlagenthemen

Kollisions- und Broadcast-Domänen analysieren

Ethernet-Geräte und die von ihnen verwendete Logik haben erheblichen Einfluss darauf, wie moderne LANs designt werden. Für einige der Begriffe, mit denen wichtige Designmerkmale beschrieben werden, muss man in der Geschichte von Ethernet weit zurückgehen, und aufgrund ihres Alters mag der eine oder andere Begriff Ihnen nicht einleuchtend erscheinen, wenn Sie diese Technologie erst heute kennenlernen. Gleich im ersten Abschnitt des Kapitels betrachten wir zwei solche älteren Begriffe: Kollisionsdomänen und Broadcast-Domänen. Damit Sie die Benennungen begreifen und sie in modernen Ethernet-LANs korrekt einsetzen, werden wir versuchen, ihre Bedeutung vor dem Hintergrund der historischen Zusammenhänge näher zu beleuchten.

Ethernet-Kollisionsdomänen

Der Begriff *Kollisionsdomäne* reicht weit zurück in die Historie von Ethernet-LANs. Offen gestanden ist die Bezeichnung für viele Menschen, die die Ethernet-Technologie erst heute kennenlernen, durchaus verwirrend. Das liegt vor allem daran, dass Kollisionen in modernen Ethernet-LANs – sofern sie korrekt aufgebaut sind – gar nicht mehr auftreten können. Damit wir Kollisionsdomänen richtig verstehen, müssen wir zunächst einen Blick in die Geschichte von Ethernet werfen. Im folgenden Abschnitt sehen wir uns deswegen ein paar historische Ethernet-Geräte an, anhand derer wir eine Kollisionsdomäne definieren. Im Anschluss finden Sie Erläuterungen zu der Frage, wie dieser Begriff in einem modernen Ethernet-LAN mit Switches eigentlich zu verstehen ist.

10BASE-T mit Hub

Die im Jahr 1990 vorgestellte 10BASE-T-Technologie hat das Design von Ethernet-LANs grundlegend in Richtung solcher Strukturen geändert, wie wir sie aus modernen Designs kennen. Mit 10BASE-T wurde ein Verkabelungsmodell eingeführt, das modernen Ethernet-LANs ähnelt. Hierbei war jedes beteiligte Gerät über ein UTP-Kabel mit einem zentralen Gerät verbunden. Allerdings wurden in frühen 10BASE-T-Netzwerken sogenannte *Ethernet-Hubs* anstelle von LAN-Switches eingesetzt. (Das lag daran, dass die Technologie, mit der sich auch ein einfacher LAN-Switch konstruieren ließe, zu jener Zeit schlicht noch nicht zur Verfügung stand.)

Obwohl sowohl Hub als auch Switch dieselbe Sterntopologie bei der Verkabelung nutzen, leitet ein Ethernet-Hub Traffic nicht wie ein Switch weiter. Vielmehr erfolgt die Weiterleitung hier im Physical Layer. Das bedeutet, dass der Hub das eingehende elektrische Signal nicht interpretiert, Absender- und Empfänger-MAC-Adresse nicht ausliest usw. Ein Hub agiert also im Wesentlichen wie ein Repeater, nur eben mit mehreren Ports. Wenn ein Repeater ein elektrisches Signal empfängt, *leitet er dieses unverzüglich in regenerierter Form über alle Ports mit Ausnahme desjenigen weiter, über den das Signal empfangen wurde*. Physisch betrachtet versendet der Hub also einfach nur eine »bereinigte Version« des elektrischen Signals. Wir sehen das in Abbildung 10.1, wo das von Rainer kommende Signal über die beiden Ausgänge auf der rechten Seite weitergeleitet wird.

Antworten zu den Fragen zur Einschätzung des Wissensstandes:

1 A **2** A, B, C **3** B, D **4** A, C **5** D **6** B, D

Schlüssel-thema

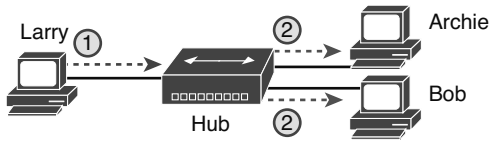


Abbildung 10.1 10BASE-T (mit Hub) Der Hub leitet Signale über alle anderen Ports weiter.

Da der Hub im Physical Layer agiert, müssen mit dem Netzwerk verbundene Geräte CSMA/CD (Carrier Sense Multiple Access with Collision Detection) verwenden, um Daten nacheinander zu versenden. Wir haben diese Technologie am Ende von Kapitel 2 bereits kennengelernt. Beachten Sie, dass der Hub selbst die CSMA/CD-Logik nicht verwendet, sondern lediglich ein elektrisches Signal, das er empfängt, regeneriert und dann über alle anderen Ports wieder versendet. Insofern sorgt die Logik des Hubs zwar dafür, dass alle Geräte eine Kopie des ursprünglichen Frames erhalten, führt aber gleichzeitig aufgrund des Fehlens von CSMA/CD zu Kollisionen. Abbildung 10.2 veranschaulicht diesen Effekt: Wenn die beiden Geräte rechts in der Abbildung gleichzeitig einen Frame versenden, versucht der Hub, die beiden Signale in elektrischer Form über den Port auf der linken Seite weiterzuleiten.

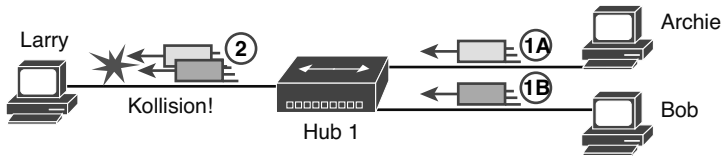


Abbildung 10.2 Kollision durch Verwendung eines Hubs

Da ein Hub nicht versucht, Kollisionen zu vermeiden, befinden sich alle an ihn angeschlossenen Geräte in derselben Kollisionsdomäne. Eine *Kollisionsdomäne* umfasst diejenigen Netzwerkkarten und Geräteanschlüsse, bei denen bei gleichzeitigem Versand eines Frames eine Kollision auftreten würde. In den Abbildungen 10.1 und 10.2 befinden sich alle drei PCs wie auch der Hub in derselben Kollisionsdomäne. Die wichtigsten Aspekte zu Hubs lassen sich wie folgt zusammenfassen:

Schlüssel-thema

- Ein Hub agiert als Multiport-Repeater, d. h., er regeneriert blindlings alle eingehenden Signale und versendet sie dann wieder über alle Ports mit Ausnahme desjenigen, über den das Signal empfangen wurde. CSMA/CD-Regeln werden dabei ignoriert.
- Senden nun zwei oder mehr Geräte gleichzeitig, dann tritt durch die vom Hub verwendeten Verfahren eine elektrische Kollision auf, durch die beide Signale beschädigt werden.
- Die verbundenen Geräte müssen das Problem mithilfe der CSMA/CD-Logik beheben. Die Geräte nutzen also die gesamte verfügbare Bandbreite gemeinsam.
- Hubs bilden eine physische Sterntopologie.

Transparente Ethernet-Bridges

Aus der Sicht des Netzdesigners stellte die Einführung von 10BASE-T eine erhebliche Verbesserung gegenüber früheren Ethernet-Typen dar. Die neue Technologie hatte nicht nur eine Senkung der Kosten für Kabel und Kabelinstallation zur Folge, sondern führte auch zu einer erhöh-

ten Verfügbarkeit des Netzwerks. Wenn man sich allerdings aus heutiger Perspektive ein LAN vorstellt, in dem alle Geräte mehr oder weniger lang warten müssen, bis sie an der Reihe sind, dann lässt sich mutmaßen, dass eine solche Struktur die Netzwerkleistung erheblich beschränkt. Und genauso war es auch. Die Ethernet-Performance, so nahm man an, würde sich in erster Linie dadurch verbessern lassen, dass Frames gleichzeitig versendet werden könnten, ohne dass es zu Kollisionen käme.

Die erste Methode, mit der mehrere Geräte gleichzeitig senden konnten, waren transparente Ethernet-Bridges. *Transparente Ethernet-Bridges* (die meist einfach nur *Bridges* genannt wurden), brachten eine Reihe von Verbesserungen:

- Bridges wurden zwischen Hubs eingesetzt und unterteilten das Netzwerk so in mehrere *Kollisionsdomänen*.
- Bridges erhöhen die Ethernet-Gesamtkapazität, da jede Kollisionsdomäne im Wesentlichen eine separate CSMA/CD-Instanz darstellt, innerhalb derer es zu jeder Zeit immer nur einen Sender geben darf.

Abbildung 10.3 zeigt, welche Auswirkungen der Aufbau eines LAN hat, das zwei durch eine Bridge getrennte Hubs enthält. Die sich hieraus ergebenden beiden Kollisionsdomänen unterstützen jeweils Datenraten von maximal 10 Mbit/s; würde jedoch nur ein einzelner Hub verwendet, dann reduzierte sich diese Datenrate auf maximal 10 Mbit/s für das *gesamte* Netzwerk.

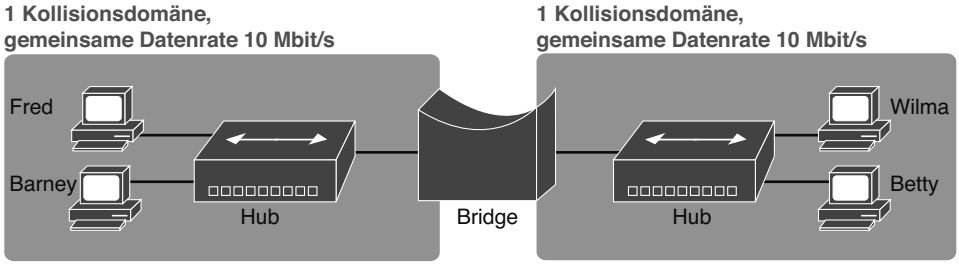


Abbildung 10.3 Erstellung zweier Kollisionsdomänen und zweier gemeinsamer Ethernet-Netzwerke mit einer Bridge

Die Entstehung mehrerer Kollisionsdomänen ist ein Nebeneffekt der Weiterleitungslogik von Bridges. Eine Bridge trifft ihre Weiterleitungsentscheidungen wie ein moderner LAN-Switch, was nicht verwundert, weil Bridges ja die Vorläufer solcher Switches waren. Wie Switches legen Bridges Ethernet-Frames im Arbeitsspeicher ab und warten dann entsprechend den Vorgaben der CSMA/CD-Regeln, bis sie mit dem Versenden über das ausgehende Interface an der Reihe sind. In anderen Fällen muss die Bridge den Frame dagegen noch nicht einmal weiterleiten. Wenn beispielsweise Fred einen Frame an die MAC-Adresse von Barney schickt, würde dieser von der Bridge keinesfalls auf die rechte Seite in der Abbildung weitergeleitet.

Ethernet-Switches und Kollisionsdomänen

Die Grundfunktionen von LAN-Switches sind dieselben wie bei Bridges, doch sind die Übertragungsraten deutlich höher und der Funktionsumfang ist wesentlich größer. Wie Bridges segmentieren Switches ein LAN in separate Kollisionsdomänen, die jeweils über eine eigene Kapazität verfügen. Und wenn das Netzwerk keinen Hub umfasst, dann ist jede einzelne

Verbindung in einem modernen LAN eine eigene Kollisionsdomäne – ungeachtet der Tatsache, dass in diesem Fall überhaupt keine Kollision auftreten kann.

Abbildung 10.4 zeigt exemplarisch ein einfaches LAN mit einem Switch und vier PCs. Der Switch erstellt vier Kollisionsdomänen, in denen in diesem Fall mit einer Bandbreite von jeweils 100 Mbit/s über jede Verbindung gesendet werden kann. Da keine Hubs vorhanden sind, kann jede Leitung im Vollduplexmodus betrieben werden, wodurch sich die Kapazität jeweils noch einmal verdoppelt.

Schlüssel-thema

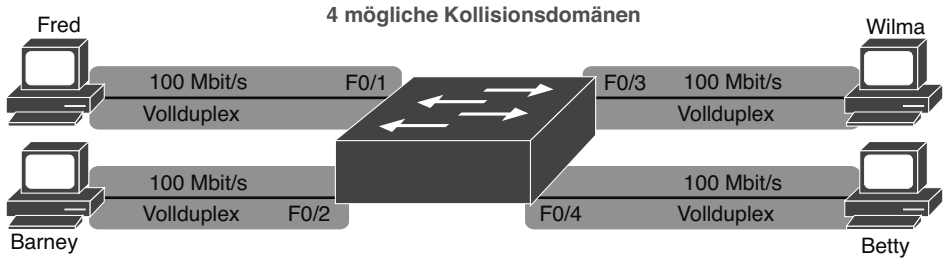


Abbildung 10.4 Erstellung von vier Kollisionsdomänen und vier Ethernet-Segmenten mit einem Switch

Nun wollen wir einmal einen Schritt zurücktreten und uns Gedanken über ein paar Aspekte moderner Ethernet-LANs machen. Heutzutage werden solche LANs nicht mehr mit Hubs oder Bridges, sondern mit Ethernet-Switches gebaut. Switches sind miteinander verbunden. Dabei ist jede einzelne derartige Verbindung eine Kollisionsdomäne.

Auch wenn es befremdlich klingen mag: In all diesen Kollisionsdomänen in modernen LANs treten womöglich niemals Kollisionen auf. Das gilt für jede Verbindung, die im Vollduplexmodus betrieben wird, d. h., bei der beide Geräte die Verbindung gleichzeitig zum Senden und Empfangen verwenden. Der Vollduplexbetrieb besagt ja im Wesentlichen Folgendes: Zwischen einem Switch und einem Endgerät können keine Kollisionen auftreten, d. h., wir können durch Verwendung des Vollduplexmodus CSMA/CD deaktivieren.

HINWEIS Die Router in einem Netzdesign bilden ebenfalls separate Kollisionsdomänen, denn Frames, die an einem LAN-Interface eines Routers empfangen oder gesendet werden, kollidieren nicht mit Frames an anderen LAN-Interfaces des Routers.

Auswirkungen von Kollisionen auf das LAN-Design

Worin also besteht der Sinn und Zweck dieser Abhandlung über Kollisionsdomänen? Vor langer Zeit waren Kollisionen in Ethernet-Netzwerken etwas völlig normales und deswegen war die Analyse eines Netzdesigns auf Kollisionsdomänen auch durchaus sinnvoll. Am anderen Ende des Spektrums steht heute ein modernes Campus-LAN, in dem ausschließlich Switches (aber keine Hubs oder transparenten Bridges) zum Einsatz kommen und in dem alle Verbindungen im Vollduplexmodus arbeiten – hier gibt es keine Kollisionen. Hat der Begriff »Kollisionsdomäne« also heute überhaupt noch eine Berechtigung? Und müssen wir uns immer noch Gedanken darüber machen?

Die kurze Antwort lautet: Ja, wir müssen. Der Begriff »Kollisionsdomäne« ist immer noch wichtig und auch Kollisionen sind immer noch wichtig – zumindest so wichtig, dass Netzwerktechniker

darauf vorbereitet sein müssen, dieses Konzept zu verstehen und bei Ausnahmen von der obigen Regel ein Troubleshooting durchzuführen. Wenn ein Port, der im Vollduplexmodus laufen sollte (was Kollisionen ausschlösse), stattdessen im Halbduplexmodus betrieben wird – etwa aufgrund einer fehlerhaften Konfiguration, infolge des Autonegotiatings oder aus irgendeinem anderen Grund –, dann kann es zu Kollisionen kommen. In solchen Fällen müssen die Techniker in der Lage sein, die Kollisionsdomäne zu erkennen.

Fassen wir die wesentlichen Punkte zu Kollisionsdomänen zusammen:

Schlüsselthema

- LAN-Switches platzieren jedes einzelne Interface in einer separaten Kollisionsdomäne.
- LAN-Bridges (die dieselbe Logik wie Switches verwenden) platzieren jedes Interface in einer separaten Kollisionsdomäne.
- Router platzieren jedes LAN-Interface in einer separaten Kollisionsdomäne. (Der Begriff »Kollisionsdomäne« gilt nicht für WAN-Interfaces.)
- LAN-Hubs platzieren nicht jedes einzelne Interface in einer separaten Kollisionsdomäne.
- In einem modernen LAN, das ausschließlich LAN-Switches und Router umfasst und für jede Verbindung den Vollduplexmodus nutzt, treten überhaupt keine Kollisionen auf.
- Auch wenn in modernen LANs mit Switches und Routern das Auftreten von Kollisionen dank Vollduplexmodus unmöglich sein sollte, sollten Sie beim Troubleshooting jede Ethernet-Leitung als separate Kollisionsdomäne betrachten.

Abbildung 10.5 zeigt ein Beispiel für ein Design mit Hubs, Bridges, Switches und Routern. Heutzutage würde man ein solches Design nicht mehr verwenden, doch es bietet genügend Informationen, um nachzuvollziehen, welche Geräte separate Kollisionsdomänen bilden.

Schlüsselthema

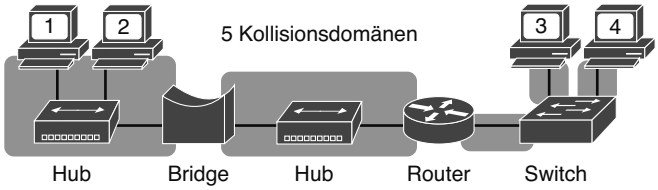


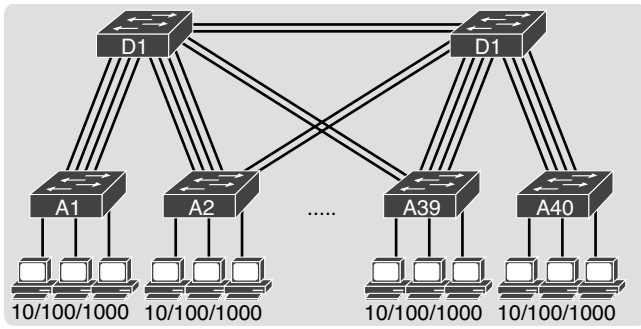
Abbildung 10.5 Beispiel eines Hubs, der keine Kollisionsdomänen bildet, während andere dies tun

10

Ethernet-Broadcast-Domänen

Stellen Sie sich vor, dass irgendein Gerät in einem beliebigen Ethernet-LAN einen Ethernet-Broadcast sendet. Eine Ethernet-*Broadcast-Domäne* umfasst alle Geräte, an die dieser Broadcast übermittelt wird.

Stellen Sie sich zunächst einmal den Weg eines Broadcast-Frames durch ein modernes LAN vor. Wir nehmen dabei an, dass alle Switches die Default-Einstellungen verwenden, d. h., alle Interfaces landen in VLAN 1. Folglich würde ein Broadcast, der von irgendeinem Gerät gesendet würde, an alle Geräte geflutet, die an irgendeinen Switch angeschlossen wären. (Ausgenommen wäre natürlich das Gerät, das den Frame ursprünglich versendet hat.) In Abbildung 10.6 etwa würde – vorausgesetzt, alle Ports gehörten zu VLAN 1 – ein Broadcast an alle in der Abbildung gezeigten Geräte übertragen.



Ein VLAN!

Abbildung 10.6 Einzelne große Broadcast-Domäne

Von allen normalen Netzwerkgeräten, die wir in diesem Buch behandeln, ist der Router das einzige, das einen LAN-Broadcast nicht weiterleitet. Hubs leiten Broadcasts natürlich weiter, da sie das elektrische Signal gar nicht erst als Ethernet-Frame betrachten. Bridges und Switches hingegen fluten LAN-Broadcasts entsprechend derselben Weiterleitungslogik. Im Gegensatz dazu leiten Router Ethernet-Broadcast-Frames nicht weiter – dies ist ein Nebeneffekt der Routing-Logik – und unterteilen ein Netzwerk auf diese Weise in getrennte Broadcast-Domänen. Abbildung 10.7 fasst all diese Gedanken in einem einzigen Beispiel zusammen.

Schlüssel-thema

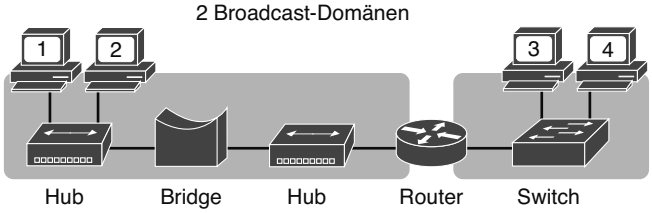


Abbildung 10.7 Durch Router getrennte Broadcast-Domänen

Definitionsgemäß werden Broadcasts, die von einem Gerät in einer Broadcast-Domäne versendet werden, nicht in andere Broadcast-Domänen weitergeleitet. Im vorliegenden Beispiel gibt es zwei Broadcast-Domänen. Der Router leitet einen LAN-Broadcast, der von einem PC auf der linken Seite in das Netzwerksegment auf der rechten übermittelt wird, nicht weiter.

VLANs

Router bilden mehrere Broadcast-Domänen – dies ist wie erwähnt ein Nebeneffekt der Funktionsweise des IP-Routings. Natürlich könnte ein Netzdesigner nun hingehen und mehr Router-Interfaces einsetzen, um eine größere Anzahl kleinerer Broadcast-Domänen zu realisieren, aber hierbei drohen die Router-Interfaces schnell aufgebraucht zu sein. Es gibt jedoch ein besseres Tool – eines, das in LAN-Switches integriert ist und keine zusätzlichen Ports benötigt: virtuelle LANs (VLANs).

VLANs sind mit Abstand das beste Werkzeug, um die passende Anzahl Broadcast-Domänen einzurichten – alle mit der passenden Größe und den vorgesehenen Geräten darin. Um einzuschätzen, wie dies mit VLANs umgesetzt wird, müssen Sie sich zunächst einmal einen wesentlichen Aspekt von LANs vergegenwärtigen:

Ein LAN umfasst alle Geräte in derselben Broadcast-Domäne.

Mit VLANs wird in einer Switch-Konfiguration jeder Port einem bestimmten VLAN zugewiesen. Die Switches bilden mehrere Broadcast-Domänen, indem sie einige Interfaces einem VLAN und andere Interfaces einem anderen VLAN zuschlagen. Die Weiterleitungslogik des Switchs übergibt keine Frames von einem Port in einem VLAN an einen Port in einem anderen VLAN, d. h., der Switch unterteilt das LAN in separate Broadcast-Domänen. Stattdessen sind Router für die Weiterleitung von Paketen zwischen VLANs zuständig und verwenden dafür Routing-Logik. Es bilden also nicht alle Ports des Switchs eine einzelne Broadcast-Domäne, sondern der Switch unterteilt sie abhängig von der Konfiguration in viele Broadcast-Domänen.

Stellen Sie sich zur Veranschaulichung einmal vor, Sie müssten zwei separate Broadcast-Domänen mit Switches konfigurieren, die mit dem VLAN-Konzept gar nicht vertraut sind. Ein Switch, der keine Ahnung von VLANs hätte, würde einen Frame, den er über einen Port empfängt, über alle seine anderen Ports fluten. Deswegen wurden, wenn das Design zwei Broadcast-Domänen vorsah, zwei Switches verwendet (nämlich einer je Broadcast-Domäne, siehe Abbildung 10.8).

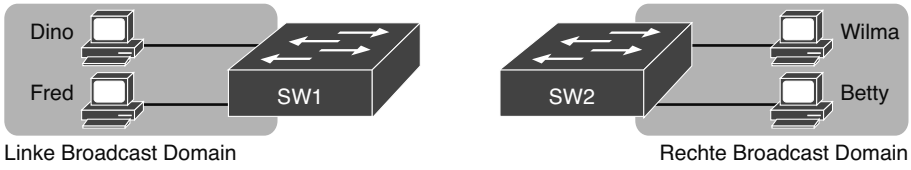


Abbildung 10.8 Beispielnetzwerk mit zwei Broadcast-Domänen ohne VLANs

Alternativ können Sie mehrere Broadcast-Domänen mit einem einzigen Switch erstellen, sofern dieser mit VLANs zurechtkommt. Sie müssen lediglich einige Ports dem einen VLAN und einige andere einem anderen VLAN zuweisen. (Der hierzu verwendete Interfacesubbefehl auf Cisco Catalyst-Switches heißt **switchport access vlan 2**, wobei in diesem Fall ein Port in VLAN 2 abgelegt wird.) Abbildung 10.9 zeigt dieselben beiden Broadcast-Domänen wie in der vorhergehenden Abbildung, nun aber als zwei separate VLANs an einem einzelnen Switch implementiert.

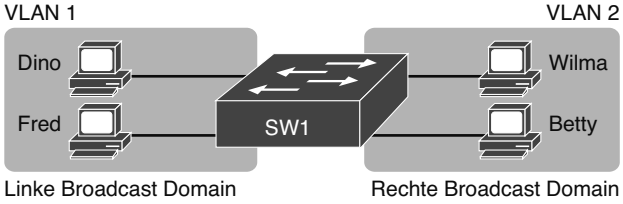


Abbildung 10.9 Beispielnetzwerk mit zwei VLANs an einem Switch

In diesem Abschnitt stellen wir das Konzept der VLANs kurz vor. Kapitel 11, »Virtuelle Ethernet-LANs implementieren«, behandelt VLANs in aller Ausführlichkeit und beschreibt auch, wie VLANs in Campus-LANs konfiguriert werden.

Auswirkungen von Broadcast-Domänen auf das LAN-Design

Moderne LAN-Designs versuchen Kollisionen zu vermeiden, weil diese die Performance beeinträchtigen. Das Auftreten von Kollisionen im Netzwerk bietet auch keinerlei Vorteile. Allerdings lassen sich Broadcasts durch ein LAN-Design nicht entfernen, weil Broadcast-Frames in vielen Protokollen eine wichtige Rolle spielen. Wenn es also um Broadcast-Domänen geht, dann eher darum, passende Kompromisse zu finden, statt sie vollständig aus dem Design zu entfernen.

Machen Sie sich einmal kurz klar, wie groß eine Broadcast-Domäne etwa ist, d. h., wie viele Geräte sich in derselben Broadcast-Domäne befinden. Bei einer kleinen Anzahl großer Broadcast-Domänen kann die Performance der Geräte in der jeweiligen Broadcast-Domäne erheblich beeinträchtigt werden. Schlagen wir jedoch den umgekehrten Weg ein und erstellen viele Broadcast-Domänen mit jeweils nur wenigen Geräten, dann entstehen andere Probleme.

Betrachten wir zunächst den Gedanken einer zu großen Broadcast-Domäne. Wenn ein Host einen Broadcast empfängt, muss er den erhaltenen Frame verarbeiten. Alle Hosts müssen den einen oder anderen Broadcast versenden, um ordnungsgemäß zu funktionieren. Wenn also ein Broadcast empfangen wird, muss die Netzwerkkarte den Prozessor des Computers unterbrechen, um ihm die eingehende Nachricht zu übergeben. Der Prozessor wiederum braucht dann immer ein ganz klein wenig Zeit, um den empfangenen Broadcast-Frame zu verarbeiten. (Beispielsweise sind Nachrichten des ARP-Protokolls, das wir in Kapitel 4, »Grundlagen zu IPv4-Adressierung und -Routing«, kennengelernt haben, LAN-Broadcasts.) Das Versenden von Broadcasts ist also nichts Schlechtes, aber für ihre Verarbeitung wird auf allen Hosts eben eine gewisse Zeit benötigt. Je mehr Geräte sich in derselben Broadcast-Domäne befinden, desto mehr unnötige Unterbrechungen müssen die Prozessoren der einzelnen Geräte erdulden.

Wir werden in diesem Abschnitt des Buchs nicht alle Abwägungen beschreiben, die beim VLAN-Design getroffen werden müssen. Sie müssen sich hier lediglich merken, dass die Größe eines VLAN zwar berücksichtigt werden sollte, dass aber auch viele andere Faktoren ins Spiel kommen können. Wie groß sind die VLANs? Wie sind die Geräte gruppiert? Erstrecken sich die VLANs über alle Switches – oder nur über ein paar? Gibt es eine auffällige Konsistenz im VLAN-Design oder wirkt alles ziemlich planlos? Indem Sie diese Fragen beantworten, finden Sie nach und nach heraus, was der Designer sich gedacht hat und welche Anforderungen an den Betrieb des Netzwerks gestellt wurden.

HINWEIS Möchten Sie genauer wissen, welche Empfehlungen Cisco dazu gibt, was in einem VLAN landen sollte und welche Auswirkungen die Größe von VLANs hat, dann lesen Sie das aktuelle Cisco-Dokument »Campus LAN Validated Design«. (Suchen Sie auf Cisco.com nach dieser Phrase.)

Fassen wir die wesentlichen Punkte zu Broadcast-Domänen zusammen:

Schlüsselthema

- Broadcasts existieren wirklich. Bereiten Sie sich deswegen darauf vor, ein Design zu analysieren und die einzelnen Broadcast-Domänen (also die Gruppen von Geräten, deren Broadcasts alle anderen Geräte in der jeweiligen Domäne erreichen) zu definieren.
- VLANs sind laut Definition Broadcast-Domänen, die durch Konfiguration entstehen.
- Router bilden separate Broadcast-Domänen an ihren einzelnen Ethernet-Interfaces, weil sie keine LAN-Broadcasts weiterleiten.

Campus-LAN-Topologien analysieren

Der Begriff *Campus-LAN* bezeichnet ein LAN, dessen Zweck in der Vernetzung eines oder auch mehrerer in unmittelbarer Nähe zueinander stehender Gebäude besteht. Eine solche Umgebung ist etwa gegeben, wenn ein Unternehmen mehrere Gebäude im selben Industriegebiet mietet. Die Netzwerktechniker können dann ein Campus-LAN einrichten, das Switches in allen Gebäuden sowie Ethernet-Verbindungen zwischen diesen Switches umfasst, wodurch ein größeres Campus-LAN entsteht.

Beim Planen und Entwerfen eines Campus-LAN müssen die Netzwerktechniker die verfügbaren Ethernet-Typen und die jeweils unterstützten Kabellängen berücksichtigen. Des Weiteren müssen die Techniker die für jedes Ethernet-Segment erforderliche Übertragungsrate festlegen. Außerdem sollte man einige Gedanken auf die Frage verwenden, welche Switches womöglich direkt mit Endbenutzergeräten verbunden und welche Switches wiederum an diese Endbenutzer-Switches angeschlossen werden sollten. Schließlich muss der Techniker bei den meisten Projekten die bereits vorhandene und installierte Hardware berücksichtigen und die Frage in Betracht ziehen, ob eine höhere Übertragungsrate in einigen Segmenten die Anschaffung neuer Geräte rechtfertigt.

In diesem zweiten der drei Hauptabschnitte dieses Kapitels behandeln wir die Topologie eines Campus-LAN-Modells. Netzdesigner schließen nicht einfach Geräte an einen x-beliebigen Port an und verbinden Switches nach Belieben miteinander, so wie Sie es vielleicht mit ein paar wenigen Geräten tun würden, die alle auf demselben Tisch in einem Lab-Umfeld stehen. Es gibt nämlich eine ganze Reihe besserer Ansätze für das Design einer Campus-LAN-Topologie und wir wollen in diesem Abschnitt einige wesentliche Aspekte und Begriffe vorstellen. Abschließend werden wir uns dann ansehen, welche Ethernet-Standards sich für die einzelnen Leitungen im Campus-LAN-Modell anbieten, und deren spezifische Vor- und Nachteile in diesem Umfeld beleuchten.

2-Ebenen-Campus-Modell (Collapsed Core)

Damit man alle Anforderungen an ein Campus-LAN formulieren und mit den Kollegen auch sinnvoll diskutieren kann, verwenden die meisten Cisco-orientierten LAN-Modelle eine allgemeine Terminologie für designerische Merkmale. Für dieses Buch müssen Sie einige wesentliche Begriffe aus der Terminologie des Campus-LAN-Modells kennen.

2-Ebenen-Campus-Modell

Abbildung 10.10 zeigt ein typisches Modell eines großen Campus-LAN einschließlich der zugehörigen Terminologie. In diesem LAN sind ca. tausend PCs an Switches angeschlossen, die jeweils etwa 25 Ports unterstützen. Die Erläuterungen zur Terminologie folgen unten.

Schlüssel-thema

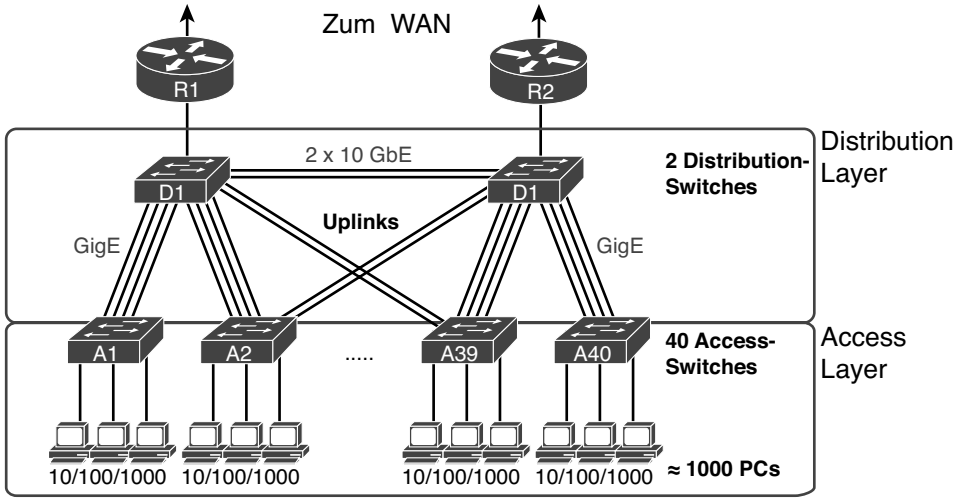


Abbildung 10.10 Campus-LAN mit designspezifischer Terminologie

Cisco verwendet zur Beschreibung der Rollen der einzelnen Switches in einem Campus-Modell die folgenden drei Begriffe: *Access*, *Distribution* und *Core*. Diese Rollen unterscheiden sich in erster Linie darin, ob der jeweilige Switch Daten von Benutzergeräten und LAN-internen Komponenten überträgt (Access-Switch) oder aber Daten zwischen anderen LAN-Switches weiterleitet (Distribution- und Core-Switches).

Access-Switches sind direkt mit Endbenutzern verbunden und stellen Benutzergeräten den LAN-Zugang bereit. Normalerweise befinden sich Access-Switches am Rand des LAN und senden Daten von und an Endbenutzergeräte, mit denen sie verbunden sind.

Distribution-Switches vermitteln einen Pfad, über den Access-Switches Daten aneinander weiterleiten können. Definitionsbedingt ist jeder Access-Switch mit mindestens einem, aus Redundanzgründen in der Regel mit zwei Distribution-Switches verbunden. Die Distribution-Switches sind dafür zuständig, Datenverkehr in andere Teile des LAN weiterzuleiten. Beachten Sie, dass die meisten Modelle aus Redundanzgründen mindestens zwei Uplinks zu zwei verschiedenen Distribution-Switches verwenden (Abbildung 10.10).

Die Abbildung zeigt ein 2-Ebenen-Modell. Die beiden Ebenen heißen Access-Layer (oder Access-Tier) und Distribution-Layer (bzw. Distribution-Tier). Mit einem derartigen 2-Ebenen-Modell lassen sich zwei wesentliche Probleme beim Netzdesign beseitigen:

- Es bietet einen Ort, an dem Endgeräte angeschlossen werden können (den Access-Layer mit den Access-Switches).
- Es verbindet die Switches mit einer sinnvoll gewählten Anzahl Kabel und Switch-Ports, indem alle 40 Access-Switches an beide Distribution-Switches angeschlossen werden.

Topologieterminologie in einem 2-Ebenen-Modell

In den Prüfungsthemen sind einige Begriffe zu den Bereichen LAN- und WAN-Topologie und Netzdesign aufgeführt. Insofern ist jetzt der richtige Zeitpunkt, kurz innezuhalten und ein wenig über diese Begriffe zu sprechen.

Betrachten wir zunächst die formalen Definitionen unserer vier Topologiebegriffe:

Schlüsselthema

Sterntopologie: ein Design, in dem mehrere Geräte jeweils mit einem zentralen Gerät verbunden sind. Würde man alle Leitungen aufzeichnen, dann sähe dieses Design wie ein Stern aus, von dem aus Licht in alle Richtungen abgestrahlt wird.

Full-Mesh-Topologie: Bei dieser auch »vollständig vermaschte Topologie« genannten Struktur gibt es zwischen allen beteiligten Knoten jeweils eine Verbindung.

Partial-Mesh-Topologie: Bei dieser auch »teilvermaschte Topologie« genannten Struktur gibt es zwischen einigen, aber nicht allen beteiligten Knoten Verbindungen. Anders gesagt: Eine vermaschte Topologie ist keine vollständig vermaschte Topologie.

Hybridtopologie: Ein Design, bei dem unterschiedliche Topologiekonzepte innerhalb eines größeren (und in der Regel komplexeren) Designs kombiniert werden.

Auf Grundlage dieser formalen Definitionen ist festzustellen, dass das 2-Ebenen-Modell eigentlich ein Hybridmodell darstellt, in dem im Access-Layer eine Stern- und im Distribution-Layer eine Partial-Mesh-Topologie zum Einsatz kommen. Warum, das sehen Sie in Abbildung 10.11. Hier wird ein typischer Access-Layer-Switch aufgegriffen, doch statt die PCs alle unterhalb des Switchs anzuordnen, sind sie um den Switch herum verteilt. Auf der rechten Seite sehen wir eine ähnliche Version derselben Skizze, die uns zeigt, warum man von einer Sterntopologie spricht: Sie sieht tatsächlich aus wie die Kinderzeichnung eines Sterns.

Schlüsselthema

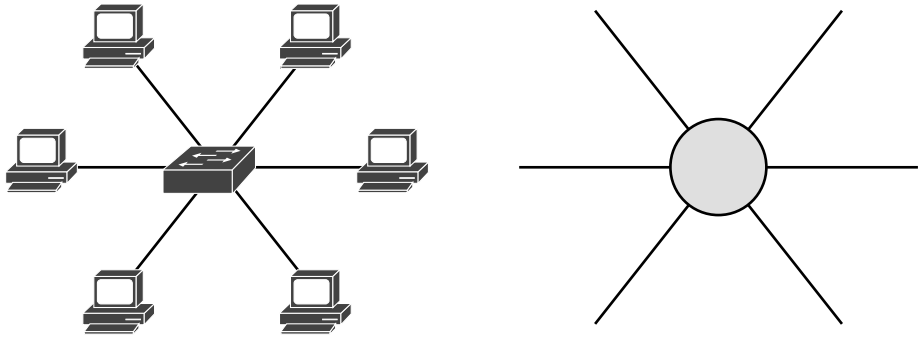


Abbildung 10.11 Konzept der Sterntopologie in der Netzwerktechnik

Der Distribution-Layer bildet eine Partial-Mesh-Topologie. Wenn Sie die Access- und Distribution-Switches als Knoten in einem Design betrachten, dann bestehen zwischen einigen Knoten Leitungsverbindungen, zwischen anderen jedoch nicht. Sehen Sie sich noch einmal Abbildung 10.10 an – Sie werden dort feststellen, dass die Access-Layer-Switches nicht miteinander verbunden sind.

Schließlich könnte ein Design auch vollständig vermascht sein. Allerdings benötigt ein Campusdesign – aus Gründen, die den Rahmen dieser Beschreibung sprengen würden – nicht die Anzahl von Leitungen und Ports, die für ein Full-Mesh-Design erforderlich wären. Trotzdem wollen wir uns der Vollständigkeit halber zunächst einmal ansehen, wie viele Verbindungen und Switch-Ports für einen einzelnen Pfad zwischen Knoten in einem Full-Mesh-Design mit sechs Knoten (Abbildung 10.12) benötigt würden.

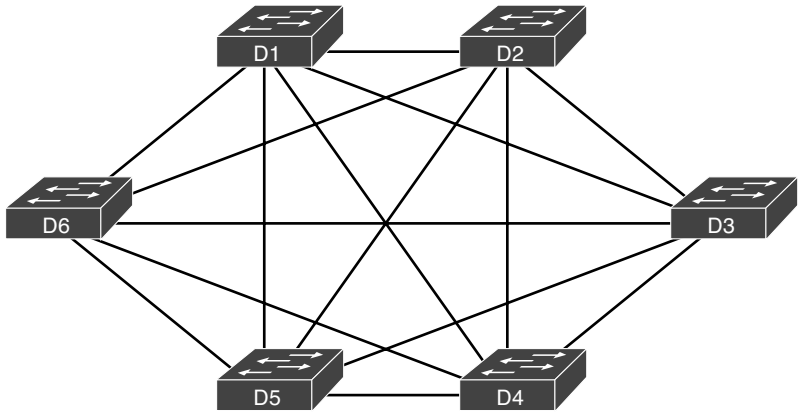


Abbildung 10.12 Verwenden einer Full-Mesh-Topologie auf dem Distribution-Layer bei sechs Switches und 15 Leitungen

Schon mit nur sechs Switches umfasst eine Full-Mesh-Topologie 15 Leitungen (und 30 Switch-Ports – zwei je Leitung).

Und nun stellen Sie sich eine vollständige Vermaschung auf dem Distribution-Layer für ein Design wie das in Abbildung 10.10 gezeigte vor – mit 40 Access-Switches und zwei Distribution-Switches! Statt dieses Design zu zeichnen und die Verbindungen zu zählen, lässt sich ihre Anzahl auch mit der guten alten Mathematik berechnen, wie wir sie noch von der Schule kennen: $n(n - 1) \div 2$, d. h. im vorliegenden Fall $42 \cdot 41 \div 2 = 861$ Verbindungen und 1722 Switch-Ports, die insgesamt benötigt werden.

Im Vergleich dazu benötigt das Partial-Mesh-Design in Abbildung 10.10, in dem nur jeweils ein Leitungspaar von jedem Access-Switch zu jedem Distribution-Switch führt, in der Summe nur 160 Leitungen und insgesamt 320 Switch-Ports.

3-Ebenen-Campus-Modell (Core-Modell)

Das in Abbildung 10.10 gezeigte 2-Ebenen-Modell mit Teilvermaschung auf dem Distribution-Layer ist das wohl gängigste Campus-LAN-Modell. Es ist unter zwei Bezeichnungen bekannt: als »2-Ebenen-Modell« (aus naheliegenden Gründen) und – nicht ganz so offensichtlich – als »Collapsed Core«. Der Begriff *Collapsed Core* bezieht sich auf die Tatsache, dass im 2-Ebenen-Modell die dritte Ebene – die Core-Ebene – fehlt. Wir werden uns der Vollständigkeit halber im nächsten Abschnitt ein 3-Ebenen-Modell mit Core ansehen.

Stellen Sie sich vor, Ihr Campus umfasst lediglich zwei oder drei Gebäude. In jedem Gebäude ist ein 2-Ebenen-Modell implementiert, d. h., es gibt pro Gebäude ein Paar Distribution-Switches und Access-Switches sind nach Bedarf im Gebäude verteilt. Wie würden Sie die LANs in den verschiedenen Gebäuden miteinander verbinden? Bei nur wenigen Gebäuden ist es durchaus sinnvoll, einfach die Distribution-Switches zu verkabeln (Abbildung 10.13).

Schlüssel-thema

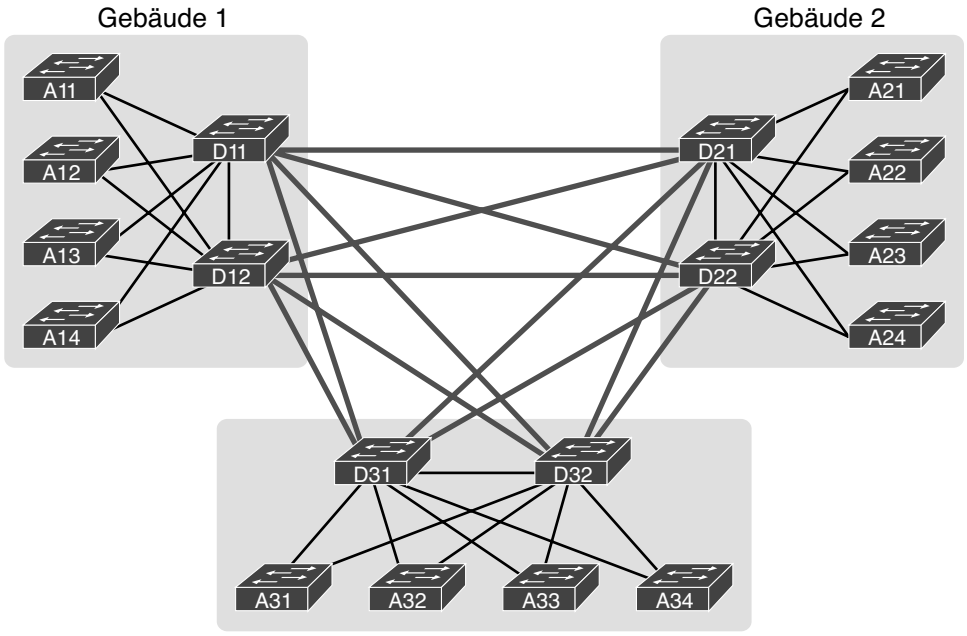


Abbildung 10.13 2-Ebenen-Modell ohne Core für drei Gebäude

Das in Abbildung 10.13 gezeigte Design hat sich bewährt und wird von vielen Unternehmen eingesetzt. Manchmal wird im Zentrum des Netzwerks eine Full-Mesh-, manchmal auch eine Partial-Mesh-Topologie eingesetzt. Dies hängt von der Verkabelungssituation zwischen den Gebäuden ab.

In umfangreicheren Modellen jedoch lassen sich mit einer dritten Ebene – dem Core-Layer – Switch-Ports und Kabel einsparen. Beachten Sie außerdem, dass für die Verbindungen zwischen den Gebäuden – also den Kabeln, die nach außen führen – häufig teurere Glasfaser mit ebenfalls teureren Switch-Ports eingesetzt werden. Das bedeutet, dass sich durch Reduzierung der gebäudeübergreifenden Verkabelung in erheblichem Maße Kosten verringern lassen.

Naheliegenderweise werden bei einem 3-Ebenen-Modell einige weitere Switches – die Core-Switches – benötigt, deren Aufgabe in der gegenseitigen Verbindung der Distribution-Switches besteht. Abbildung 10.14 zeigt die Migration des Collapsed-Core-Modells aus Abbildung 10.13 in ein 3-Ebenen-Modell.

Schlüssel-thema

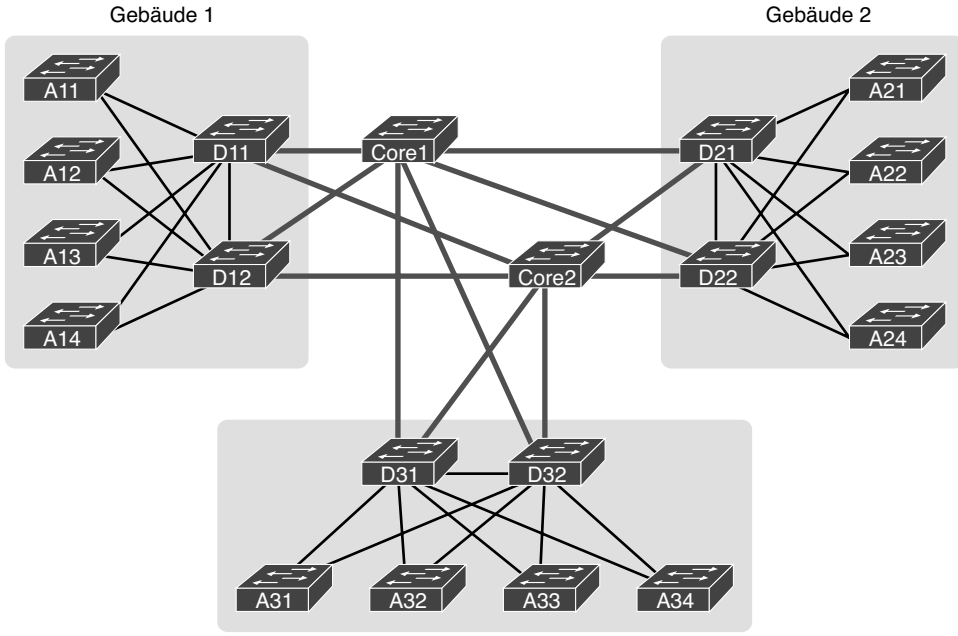


Abbildung 10.14 3-Ebenen-Modell (Core-Modell) für drei Gebäude

HINWEIS Die Core-Switches sind in der Mitte der Abbildung gezeigt. In der Realität befinden sie sich hingegen häufig im selben Raum wie einer der Distribution-Switches und nicht an einem speziell hierfür vorgesehenen Ort in der Mitte des Campus. Die Abbildung stellt jedoch die Topologie in den Mittelpunkt, nicht die physische Anordnung.

Wenn Sie ein Core-Modell mit Teilvermaschung der Core-Verbindungen einsetzen, bieten Sie zwar weiterhin Konnektivität für alle Teile des LAN und für die Router, die die Pakete über das WAN versenden, benötigen aber weniger Leitungen zwischen den Gebäuden.

In der folgenden Liste sind die Begriffe zusammengefasst, die die Rollen der Campus-Switches beschreiben:

- **Access-Switch:** Stellt einen Zugangspunkt für Endbenutzergeräte bereit. Frames werden unter normalen Umständen nicht zwischen zwei Access-Switches weitergeleitet.
- **Distribution-Switch:** Ein solcher Switch stellt einen Anbindungspunkt für Access-Switches bereit, der den übrigen Geräten im LAN Konnektivität vermittelt und über den Frames Switch-übergreifend weitergeleitet werden. Ein Anschluss von Endbenutzergeräten ist nicht vorgesehen.
- **Core-Switch:** Hiermit lassen sich Distribution-Switches in sehr großen Campus-LANs anbinden. Dies ermöglicht aufgrund der reinen Größe des Netzwerks sehr viel höhere Datenraten für die Weiterleitung.

Terminologie beim Topologiedesign

In den Themen der ICND1- und CCNA-Prüfungen sind verschiedene Begriffe zum Netzdesign aufgeführt, die mit der Topologie im Zusammenhang stehen. Im folgenden Abschnitt werden diese Schlüsselbegriffe zusammengefasst und mit den zugehörigen Konzepten verknüpft.

Betrachten Sie zunächst Abbildung 10.15, in der bereits einige dieser Termini aufgeführt sind. Auf der linken Seite der Abbildungen sind häufig Access-Switches mit einer Anzahl parallel angeordneter Kabel gezeigt. Allerdings werden ein Access-Switch und seine Zugangsleitungen häufig als *Sterntopologie* bezeichnet. Warum dies? Sehen Sie sich die zweite Darstellung des Access-Switchs in der Mitte der Abbildung an, von dem aus die Kabel sternförmig abgehen. Das sieht nicht wie ein echter Stern aus, wohl aber so, wie ein kleines Kind einen Stern zeichnen würde – daher die Benennung.

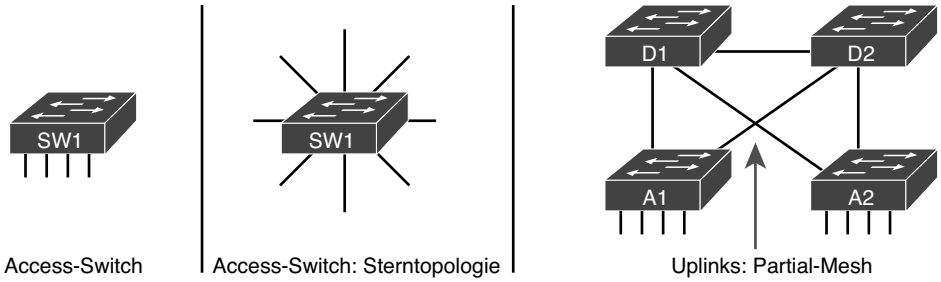


Abbildung 10.15 Terminologie des LAN-Designs

Auf der rechten Seite der Abbildung sehen wir erneut ein 2-Ebenen-Modell, wobei hier der Schwerpunkt auf der Darstellung der Leitungsvermaschung zwischen Access- und Distribution-Switches liegt. Jede Gruppe von Knoten, die über mehr Leitungen verbunden sind, wird normalerweise als *Mesh* (dt. *Geflecht*) bezeichnet. In diesem Fall handelt es sich um ein *Partial Mesh*, also ein teilvermaschtes Geflecht, denn nicht alle Knoten verfügen über eine Direktverbindung zueinander. Ein Design, in dem alle Knoten mit einer Leitung verbunden sind, wäre ein *Full Mesh*.

Diese Topologiekonzepte werden auch in der Realität eingesetzt, doch noch häufiger werden beide miteinander kombiniert. So finden wir auf der rechten Seite von Abbildung 10.14 eine Kombination aus der Sterntopologie des Access-Layers mit dem Partial Mesh des Distribution-Layers. Derartige Strukturen, die Konzepte in kombinierter Form einsetzen, heißen oft auch *Hybriddesigns*.

Standardoptionen im Physical Layer für das LAN analysieren

Wenn Sie das Design eines Netzwerks analysieren, das nicht von Ihnen selbst entworfen wurde, dann können Sie hierzu die verschiedenen Arten der Verkabelung und der verwendeten Switch-Ports wie auch der eingesetzten Ethernet-Standards betrachten. Sie fragen sich dann vielleicht, warum für die Verbindungen im Netzwerk der jeweilige Ethernet-Leitungstyp ausgewählt wurde. Die Antwort auf diese Frage gibt viel preis über den Aufbau des physischen Campus-LAN.

Das IEEE hat bei der Entwicklung der Ethernet-Standards hervorragende Arbeit geleistet, denn den Netzdesignern werden zahlreiche Optionen an die Hand gegeben. Es sind insbesondere zwei Aspekte, die das langfristige Wachstum von Ethernet garantieren konnten:

Schlüsselthema

- Das IEEE hat viele zusätzliche 802.3-Standards für verschiedene Kabeltypen und -längen sowie für unterschiedliche Datenraten entworfen.
- Alle physischen Standards greifen auf dieselben Data-Link-Layer-Eigenschaften zurück und nutzen dieselben Frame-Standardformate. Das bedeutet, dass im selben Ethernet-LAN unterschiedliche Verbindungen im Physical Layer vorhanden sein können – je nach Entfernung, Budget und Verkabelungsbedarf.

Denken Sie beispielsweise einmal an den Access-Layer auf Diagrammen mit generischen Designs, aber in Bezug auf Verkabelung und Ethernet-Standards. In der Praxis befinden sich die Access-Layer-Switches in einem verschlossenen Schaltschrank irgendwo auf dem gleichen Stockwerk wie die Endbenutzergeräte. Die Elektrotechniker verlegen das für den Access-Layer verwendete UTP-Kabel von diesem Schaltschrank bis zu den Wandanschlussdosen in den verschiedenen Büros oder überall dorthin, wo ein LAN-Anschluss für ein Ethernet-Gerät sinnvoll erscheinen mag. Typ und Qualität der zwischen Schaltschrank und Ethernet-Anschlussdosen verwendeten Kabel geben die unterstützten Ethernet-Standards vor. Auf jeden Fall hat derjenige, der das LAN-Design zum Zeitpunkt der Kabelverlegung entworfen hat, sich Gedanken darüber gemacht, welche Kabeltypen benötigt werden, um diejenigen Ethernet-Standards für den Physical Layer zu unterstützen, die im betreffenden LAN zum Einsatz kommen sollten.

Ethernet-Standards

Im Laufe der Zeit hat das IEEE Ethernet immer weiterentwickelt und neue Standards verabschiedet, die höhere Datenraten und neue Kabeltypen und -längen unterstützen. Abbildung 10.16 zeigt, wie sich die Datenrate bei Ethernet im Laufe der Zeit gesteigert hat. Die frühesten Standards nutzten bis in die 1990er-Jahre hinein 10 Mbit/s, während Verkabelung und Topologie immer stärker optimiert wurden. Mit der Einführung von Fast Ethernet (100 Mbit/s) im Jahr 1995 begann dann auch die kontinuierliche Geschwindigkeitssteigerung, die bis zum heutigen Tag anhält.

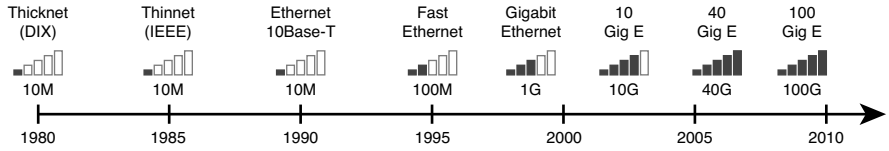


Abbildung 10.16 Ethernet-Standards im zeitlichen Verlauf

HINWEIS Häufig hat das IEEE die Unterstützung höherer Geschwindigkeiten zunächst für Glasfaserkabel eingeführt und – teils erst mehrere Jahre – später die Entwicklung der Standards abgeschlossen, die dieselbe Datenrate auch über UTP-Kabel unterstützen. Abbildung 10.16 zeigt die jeweils ersten Standards für die jeweilige Datenrate unabhängig vom verwendeten Kabeltyp.

Wann immer das IEEE Unterstützung für einen neuen Kabeltyp oder eine höhere Datenrate einführt, wird gleichzeitig ein neuer Teilstandard für den 802.3-Standard verabschiedet. Diese Teilstandards unterscheiden sich durch den oder die Buchstaben, die auf den Standardnamen folgen. Wenn also von Standards die Rede ist, müssen Sie manchmal den Standardnamen (einschließlich des betreffenden Buchstabens) nennen. Als etwa die Gigabit-Ethernet-Unterstützung über kostengünstige UTP-Kabel vorgestellt wurde, resultierte dies im Standard 802.3ab. Die Netzwerktechniker hingegen bezeichnen denselben Standard eher als »1000BASE-T« – oder eben einfach als »Gigabit Ethernet«. Tabelle 10.2 listet einige der IEEE 802.3-Standards für den Physical Layer und die zugehörigen Namen auf.

Tabelle 10.2 Merkmale des IEEE-Physical Layer

Offizieller IEEE-Standardname	Kurzname	Informelle Bezeichnungen	Übertragungsrate	Kabeltyp (typ.)
802.3i	10BASE-T	Ethernet	10 Mbit/s	UTP
802.3u	100BASE-T	Fast Ethernet	100 Mbit/s	UTP
802.3z	1000BASE-X	Gigabit Ethernet, GigE	1000 Mbit/s (1 Gbit/s)	Glasfaser
802.3ab	1000BASE-T	Gigabit Ethernet, GigE	1000 Mbit/s (1 Gbit/s)	UTP
802.3ae	10GBASE-X	10 GigE	10 Gbit/s	Glasfaser
802.3an	10GBASE-T	10 GigE	10 Gbit/s	UTP
802.3ba	40GBASE-X	40 GigE	40 Gbit/s	Glasfaser
802.3ba	100GBASE-X	100 GigE	100 Gbit/s	Glasfaser

Auswahl des passenden Ethernet-Standards für eine Leitung

Beim Entwerfen eines Ethernet-LAN können und sollten Sie sich ein paar Gedanken zur Topologie machen – mit Access-, Distribution- und möglicherweise auch Core-Layer. Allerdings können Sie aus der Topologie noch nicht ersehen, welche Standards Sie für die einzelnen Verbindungen auswählen sollten. Letztendlich müssen Sie sich entscheiden, welchen Ethernet-Standard welche Leitung nutzen soll. Diese Entscheidung wird anhand der folgenden Tatsachen zu den einzelnen Standards des Physical Layer getroffen:

- Datenrate
- Zulässige Maximalentfernung zwischen den Geräten bei Verwendung eines Standards oder Kabels
- Kosten für Verkabelung und Switch-Hardware
- Typ bereits vor Ort verlegter Verkabelung

Für die drei derzeit gängigsten Ethernet-Typen (10BASE-T, 100BASE-T und 1000BASE-T) gilt jeweils eine maximale Kabellänge von 100 Metern und alle verwenden UTP-Kabel. Leider sind UTP-Kabel häufig von unterschiedlicher Qualität und es ist nicht verwunderlich, dass die Kabelqualität umso höher sein muss, je höher die Datenrate des gewählten Standards ist.

Infolgedessen bieten manche Gebäude vielleicht bessere Kabel, die Datenraten bis hin zu Gigabit Ethernet unterstützen, während die Verkabelung in anderen Gebäuden unter Umständen »nur« Fast Ethernet bewältigt.

Die amerikanische Telecommunications Industry Association (TIA) definiert die Qualitätsstandards für Ethernet-Kabel. In jedem Ethernet-Standard, bei dem UTP-Kabel zum Einsatz kommt, ist eine TIA-Kabelqualität – eine sogenannte *Kategorie* – als Mindestanforderung angegeben. So benötigt 10BASE-T etwa Kabel der Kategorie 3 (CAT3) oder besser, während 100BASE-T die höherwertige CAT5-Verkabelung vorsieht und 1000BASE-T noch bessere CAT5e- oder CAT6-Kabel erfordert. (Bei den TIA-Standards gilt, dass die Kabelqualität umso höher ist, je höher auch die Kategorienummer ist.) Wenn in einem Gebäude beispielsweise nur die ältere CAT5-Verkabelung zwischen den Schaltschränken und den Büros installiert ist, müssen die Netzwerktechniker einen Austausch der Kabel in Betracht ziehen, sofern etwa Gigabit Ethernet unterstützt werden soll. Tabelle 10.3 führt die gängigsten Ethernet-Typen, die zugehörigen Kabelsorten und die Längenbeschränkungen auf.

Tabelle 10.3 Ethernet-Typen, Medien und Segmentlänge (nach IEEE-Definition)

Ethernet-Typ	Medium	Zulässige Segmentlänge
10BASE-T	mind. TIA CAT3, zweipaarig	100 m
100BASE-T	mind. TIA CAT5-UTP, zweipaarig	100 m
1000BASE-T	mind. TIA CAT5e-UTP, vierpaarig	100 m
10GBASE-T	mind. TIA CAT5e-UTP, vierpaarig	100 m
10GBASE-T[1]	mind. TIA CAT6-UTP, vierpaarig	38–55 m
1000BASE-SX	Multimode-Glasfaser	550 m
1000BASE-LX	Multimode-Glasfaser	550 m
1000BASE-LX	9-µm-Singlemode-Glasfaser	5 km

[1] Die Auswahl von 10GBASE-T mit der geringfügig schlechteren CAT6-Verkabelung bei kurzen Übertragungsstrecken stellt einen Versuch dar, 10 Gigabit Ethernet für bestimmte Installationen mit installiertem CAT6 zu unterstützen.

Ethernet definiert auch Standards für die Nutzung von Glasfaserkabel. Glasfaserkabel verwenden extrem dünne Fasern aus Glas, die Lichtimpulse weiterleiten. Zur Übermittlung von Bits wechseln die Switches die Lichtstärke: Starkes Licht im Kabel steht für binäre Nullen, schwächeres Licht für Einsen.

Beim allgemeinen Vergleich zwischen den Ethernet-Standards für Glasfaser- und UTP-Kabel fallen zwei Dinge auf. Erstens gestatten optische Verbindungen wesentlich längere Kabelstrecken, wobei jedoch die Kosten für Kabel und Switch-Hardware deutlich höher sind. Zudem sind Glasfaserkabel im Vergleich zu Kupferkabel wesentlich weniger anfällig gegenüber Störungen von außen, was größere Übertragungsstrecken zulässt.

Für optische Ethernet-Verbindungen gibt es zahlreiche Standards, die allerdings alle in eine von zwei allgemeinen Kategorien fallen. Beim Vergleich dieser beiden Kategorien unterstützen die kostengünstigeren Optionen in der Regel Übertragungsstrecken von mehreren hundert Metern

und verwenden preiswerte LEDs (Leuchtdioden) für die Datenübertragung. Andere optische Standards ermöglichen wesentlich längere Strecken bis hin zu vielen Kilometern, doch sind die Kabel teurer und zur Übertragung werden Laser eingesetzt. Die Abwägung ist relativ unkompliziert: Stellen Sie einfach fest, wie lang die für eine gegebene Verbindung zu verlegenden Kabel sein müssen, welche Standards die entsprechende Streckenlänge unterstützen und wie sich die Strecke möglichst preiswert realisieren lässt.

In der Praxis kennen die meisten Techniker nur die allgemeinen Tatsachen aus Tabellen wie Tabelle 10.3: 100 Meter bei UTP, ca. 500 Meter bei Multimode-Glasfaser und etwa 5000 Meter bei bestimmten Ethernet-Standards für Singlemode-Glasfaser. Sobald es aber bei der Leitungsplanung ans Eingemachte geht, muss sich jeder Netzwerktechniker mit den Details auseinandersetzen, die Länge der jeweiligen Kabelstrecke entsprechend ihres Verlaufs durch das Gebäude bestimmen usw.

WLANs und kabelgestütztes Ethernet in Kombination

Moderne Campus-LANs umfassen eine Vielzahl kabelloser Geräte, die mit dem Access-Layer des LAN verbunden sind. Bei Cisco gibt es für WLANs einen eigenen Zertifizierungsverlauf mit CCNA, CCNP und CCIE Wireless, weswegen der CCNA R&S-Pfad sich traditionell nur sehr eingeschränkt den WLANs widmet. Das gilt auch für die aktuellen Prüfungsversionen – erwähnt werden WLANs nur bei einem einzigen CCNA R&S-Prüfungsthema:

> Auswirkungen von Infrastrukturkomponenten in einem Unternehmensnetzwerk beschreiben: Access-Points und Wireless-Controller

Aus dieser Tatsache sollten Sie jedoch nicht ableiten, dass Wireless-Technologien weniger wichtig sind als Ethernet. Im Gegenteil: Mittlerweile gibt es auf den Access-Layern moderner Unternehmensnetzwerke möglicherweise bereits mehr kabellos angebundene Geräte als verkabelte. Beide Bereiche sind wichtig, nur hält Cisco die Zertifizierungspfade – und damit auch die Lehrmaterialien – getrennt voneinander.

Im letzten Abschnitt dieses Kapitels werden wir uns diesem einen Thema widmen, das zwei Wireless-spezifische Begriffe umfasst.

WLANs im Home-Office

Zunächst einmal werden sowohl Ethernet-LANs als auch WLANs vom IEEE definiert. Falls das noch nicht klar war: Alle Ethernet-Standards nutzen Kabel, d. h., Ethernet definiert kabelgestützte LANs. Die IEEE 802.11-Arbeitsgruppe definiert WLANs. Diese sind übrigens auch unter der Bezeichnung »Wi-Fi« bekannt – nach einem geschützten Begriff der Wi-Fi Alliance, einem Zusammenschluss von Unternehmen, der die kommerzielle WLAN-Entwicklung vorantreiben soll.

Die meisten von Ihnen werden WLAN bereits verwendet haben und viele tun das täglich. Vielleicht haben Sie schon zuhause ein kleines WLAN eingerichtet, wie es in Abbildung 10.17 angezeigt ist. Dabei haben Sie ggf. auch ein Endgerät verwendet, das als *WLAN-Router* bezeichnet wird. Auf der einen Seite dieses Geräts ist das Internet angeschlossen, auf der anderen die WLAN-fähigen Geräte im Haushalt. In einem solchen Umfeld können Geräte wahlweise per WLAN oder über ein Ethernet-Kabel angebunden werden.

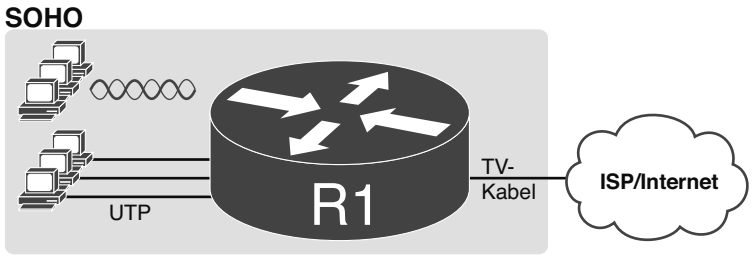


Abbildung 10.17 Konventionelles Heimnetzwerk mit kabelgestütztem Ethernet und WLAN

Zwar zeigt die Abbildung die Hardware nur in Form eines einzelnen Router-Symbols an, intern jedoch agiert dieser WLAN-Router wie drei separate Geräte, die immer auf einem Unternehmenscampus zu finden sind:

- ein Ethernet-Switch für die kabelgebundenen Ethernet-Verbindungen
- ein WLAN-Access-Point zur Kommunikation mit den kabellosen Geräten im Netzwerk und zur Weiterleitung von Frames von und an das kabelgebundene Netzwerk
- ein Router zur Weiterleitung von IP-Paketen von und an die LAN- und WAN-Interfaces (Internet)

Abbildung 10.18 greift die vorherige Abbildung wieder auf, unterteilt diese internen Komponenten jedoch so, als ob es sich um getrennte Geräte handelte. Hiermit soll lediglich verdeutlicht werden, dass ein einzelner WLAN-Router für Endkunden die Funktionen mehrerer verschiedener Geräte erfüllt.

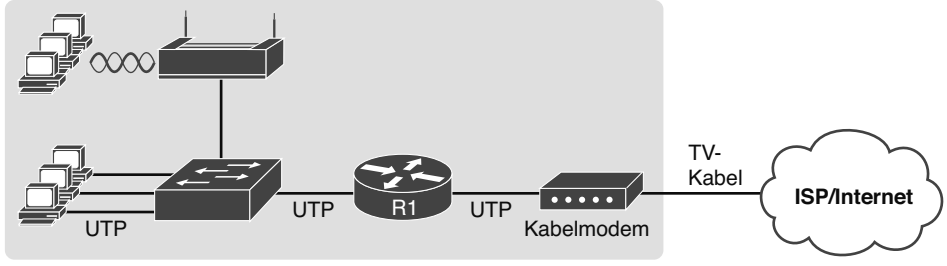


Abbildung 10.18 Darstellung der Funktionen in einem WLAN-Router für Endkunden

In einem SOHO-WLAN funktioniert der WLAN-Access-Point autonom und implementiert dabei alle Funktionen, die zum Erstellen und Steuern des WLAN benötigt werden. (Im Gegensatz dazu funktioniert der AP in den meisten Unternehmens-WLANs gerade nicht autonom.) Anders formuliert, kommuniziert der autonome AP mit den verschiedenen WLAN-Geräten per Funkwellen und unter Verwendung der 802.11-Protokolle. Für kabelgebundene Geräte werden dagegen Ethernet-Protokolle benutzt. Der Access-Point führt vor der Weiterleitung Konvertierungen zwischen den unterschiedlichen Header-Formaten von 802.11- und 802.3.-Frames durch.

Neben solchen einfachen Weiterleitungen muss der autonome AP auch eine Reihe von Steuer- und Managementfunktionen bieten. Der AP authentifiziert neue Geräte, definiert den Namen des WLAN (die sogenannte »Service Set ID«, kurz SSID) und regelt weitere Details.

Unternehmens-WLANs und WLAN-Controller

Wenn Sie über Ihr Tablet, Smartphone oder Laptop im Heimnetzwerk eine WLAN-Verbindung herstellen und dann mit dem Gerät das Haus verlassen, wird diese Wireless-Verbindung wahrscheinlich früher oder später abreißen. Sie werden wohl kaum davon ausgehen, automatisch mit dem WLAN Ihres Nachbarn verbunden zu werden (vor allem dann nicht, wenn dieser Nachbar alles richtig gemacht, d. h. die Sicherheitsfunktionen seines Access-Point so konfiguriert hat, dass Dritte nicht auf sein Netzwerk zugreifen können). In einem Wohngebiet entsteht nämlich nicht ein einzelnes WLAN, auf das alle Geräte in allen Haushalten Zugriff haben, sondern vielmehr eine Vielzahl autonomer WLANs mit eingeschränkter Reichweite.

In Unternehmen allerdings wird das genaue Gegenteil benötigt: Die Mitarbeiter sollen sich auf dem Unternehmensgelände frei bewegen können und trotzdem jederzeit mit dem WLAN verbunden bleiben. Hierzu sind viele APs erforderlich, die miteinander kooperieren, statt autark zu arbeiten, und auf diese Weise ein großes WLAN bilden.

Machen wir uns zunächst einmal Gedanken über die Anzahl der APs, die ein Unternehmen benötigt. Jeder AP kann nur einen bestimmten räumlichen Bereich abdecken. Wie groß dieser ist, hängt von zahlreichen Bedingungen und vom verwendeten WLAN-Standard ab. (Wir reden dabei von Regelreichweiten zwischen 30 und 60 Metern.) Gleichzeitig könnte aber auch das umgekehrte Problem auftreten: dass Sie nämlich eine große Zahl APs in einem relativ kleinen räumlichen Bereich aufstellen müssen, um genügend WLAN-Kapazität zu bieten. In der Designphase für ein WLAN wird häufig viel Zeit damit verbracht zu entscheiden, wie viele APs welchen Typs wo aufgestellt werden müssen, um den anfallenden Traffic zu bewältigen.

HINWEIS Falls es Ihnen nicht bereits aufgefallen sein sollte, werfen Sie doch in Neubauten oder Einkaufsläden gelegentlich mal einen Blick an die Decke – Sie werden dort in der Regel WLAN-APs sehen.

Jeder AP muss dann mit dem kabelgebundenen LAN verbunden werden, weil die meisten Empfängergeräte, mit denen WLAN-Benutzer kommunizieren müssen, sich im kabelgebundenen Teil des Netzwerks befinden. Tatsächlich sind die APs aus naheliegenden Gründen normalerweise in räumlicher Nähe zu den Benutzern angeordnet, d. h., sie sind mit denselben Access-Switches wie die Endbenutzer verbunden (Abbildung 10.19).

Stellen Sie sich nun vor, Sie befänden sich am unteren Rand der Abbildung. Ihr Smartphone bietet WLAN-Unterstützung, d. h., sobald Sie Ihre Arbeitsstelle betreten, stellt es automatisch eine Verbindung mit dem Unternehmens-WLAN her. Sie sind dann den ganzen Tag lang auf dem Firmengelände unterwegs, besuchen Meetings, gehen zu Tisch usw. Dabei bleiben Sie ständig mit dem Unternehmens-WLAN verbunden, Ihr Smartphone jedoch stellt Verbindungen zu vielen unterschiedlichen APs her und nutzt diese.

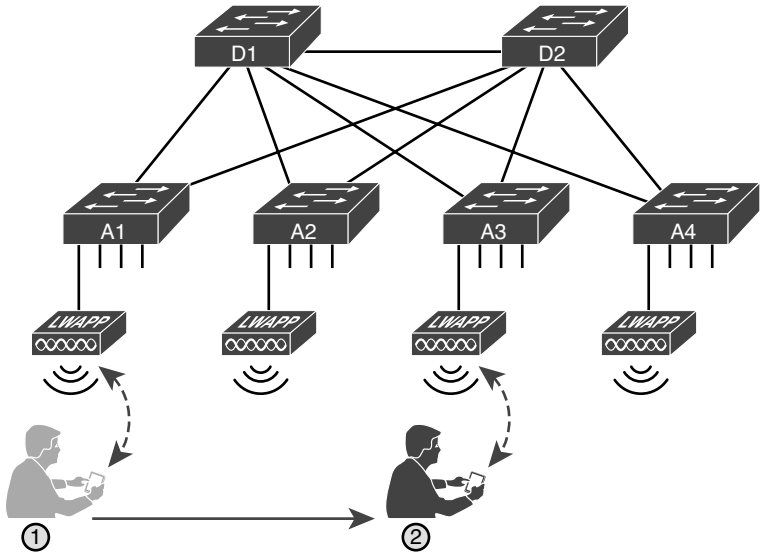


Abbildung 10.19 Campus-LAN mit mehreren Lightweight-APs und Roaming

Die Unterstützung von Roaming und anderen unternehmensspezifischen WLAN-Funktionen mithilfe autonomer APs ist bestenfalls kompliziert. Wenn Sie pro Stockwerk vielleicht ein Dutzend APs implementiert haben, dann werden dies campusweit schnell mehrere Hundert, und sie alle müssen über den Zustand ihres übergeordneten WLAN Bescheid wissen.

Die Lösung besteht darin, alle Steuer- und Managementfunktionen aus den APs in ein zentralisiertes Gerät auszulagern. Ein solches Gerät wird als »Wireless Controller« oder »WLAN-Controller« (kurz »WLC«) bezeichnet. Die APs handeln nun nicht mehr autark, sondern fungieren als sogenannte LWAPs (Lightweight APs), die lediglich Daten zwischen dem WLAN und dem WLC weiterleiten. Die gesamte Logik für das Roaming, die Definition von WLANs (SSIDs), Authentifizierung usw. werden vollständig auf dem WLC umgesetzt. Wir fassen zusammen:

- **WLC:** Steuert und verwaltet alle AP-Funktion (z. B. Roaming, WLAN-Definition, Authentifizierung)
- **LWAP (Lightweight AP):** Leitet Daten zwischen kabelgebundenem und Wireless-LAN weiter. Die Weiterleitung erfolgt vorzugsweise über den WLC. Hierbei kommt das CAPWAP-Protokoll (Control And Provisioning of Wireless Access Points) zum Einsatz.

Mit einem Design, in dem ein WLC und LWAPs eingesetzt werden, lässt sich ein sehr großes WLAN bilden und so die Erstellung vieler kleiner und unverbundener WLANs unnötig machen. Der Schlüssel besteht darin, dafür zu sorgen, dass der gesamte Wireless-Traffic über den WLC übertragen wird. Abbildung 10.20 zeigt dies. (Übrigens verwenden die LWAPs meistens ein Protokoll namens CAPWAP.)

Schlüssel-thema

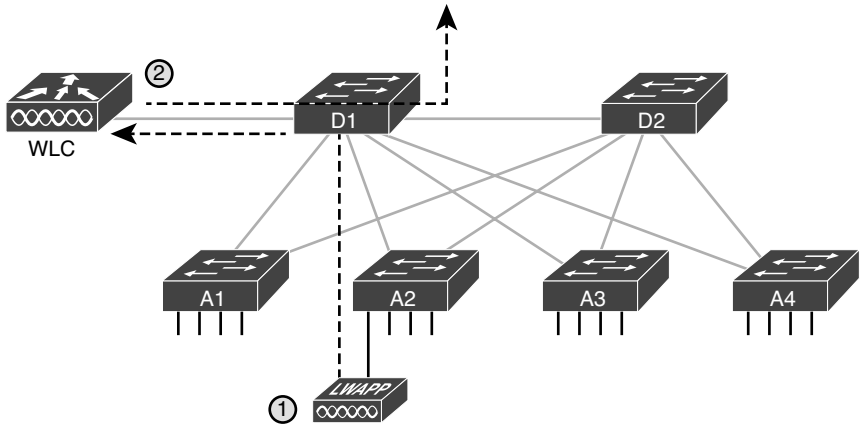


Abbildung 10.20 Campus-LAN mit mehreren Lightweight-APs und Roaming

Weil der gesamte Datenverkehr über den WLC weitergeleitet wird, kann dieser Entscheidungen treffen, die unternehmensweit am sinnvollsten sind. So möchten Sie vielleicht für die verschiedenen Abteilungen – Fertigung, Marketing usw. – separate WLANs erstellen und alle APs müssen diese unterschiedlichen WLANs kennen und unterstützen. In diesem Fall sollten etwa Benutzer, die eine Verbindung mit dem Fertigungs-WLAN herstellen möchten, dies unabhängig vom konkret verwendeten AP tun können – und genau dies macht der WLC möglich. Oder denken Sie mal an das Roaming. Angenommen, Ihr Smartphone ist mit AP1 verbunden und empfängt ein Paket, beim Empfang des nächsten Pakets ist das Smartphone aber bereits mit AP4 verbunden: Wie kann dieses Paket über das Netzwerk zugestellt werden? Nun, da alles über den WLC läuft und dieser ständig mit den APs in Kontakt ist, erkennt er, dass Ihr Gerät jetzt mit einem anderen Access-Point verbunden ist, und weiß deswegen auch, wie das Paket geroutet werden muss.

Lernzielkontrolle

Der Abschnitt »Ihr Studienplan«, den Sie in diesem Buch vor Kapitel 1 finden, beschreibt geeignete Vorgehensweisen zum Erlernen und Üben der Inhalte und Fertigkeiten aus diesem Kapitel. Dort werden die Tools und Elemente vorgestellt, die Sie am Ende jedes Kapitels verwenden. Falls Sie den Abschnitt noch nicht gelesen haben, nehmen Sie sich nun ein paar Minuten Zeit, um das nachzuholen. Kehren Sie danach zu dieser Stelle zurück und wiederholen Sie das Kapitel wie dort beschrieben, um das Gelesene in Ihrem Gedächtnis zu verankern.

Wiederholen Sie den Stoff aus diesem Kapitel unter Verwendung der Werkzeuge aus dem Buch oder von der DVD oder nutzen Sie die interaktiven Tools auf der Begleitwebsite zum Buch. Tabelle 10.4 fasst die wichtigsten Elemente zur Wiederholung zusammen und zeigt auch, wo Sie diese finden können. Damit Sie Ihre Lernfortschritte besser im Blick behalten, sollten Sie in der zweiten Spalte vermerken, wann Sie diese Aktivitäten bearbeitet haben.

Tabelle 10.4 Erfassung der Lernzielkontrollen

Element	Datum der Wiederholung	Verwendete Ressource
Schlüsselthemen wiederholen		Buch, App
Schlüsselbegriffe wiederholen		Buch, App
Fragen zur Einschätzung des Wissensstands beantworten		Buch, PCPT
Gedächtnistabellen wiederholen		Buch, App

Alle Schlüsselthemen wiederholen

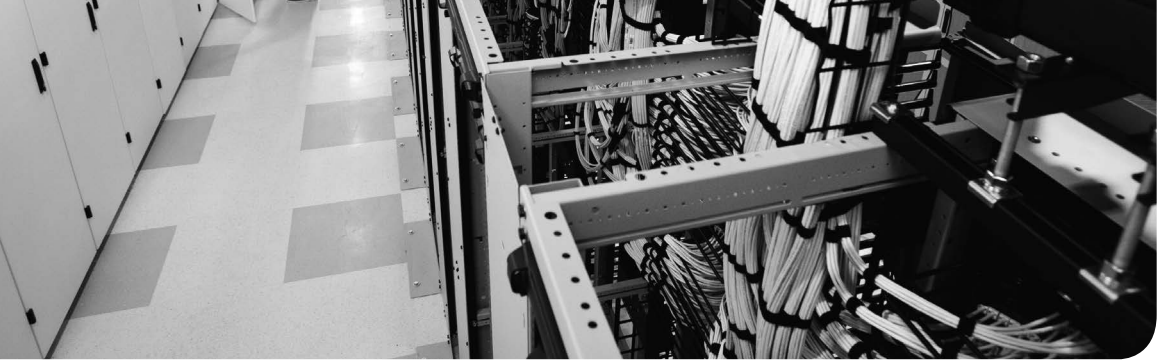
Tabelle 10.5 Schlüsselthemen in Kapitel 10

Element	Beschreibung	Seite
Abbildung 10.1	Funktionsweise eines LAN-Hubs, der elektrische Signale wiederholt	258
Liste	Wichtige Fakten zu Hubs	258
Abbildung 10.4	Switches bilden separate Kollisionsdomänen	260
Liste	Zusammenfassung der wesentlichen Aspekte von Kollisionsdomänen	261
Abbildung 10.5	Beispiel für Kollisionsdomänen	261
Abbildung 10.7	Beispiel für Broadcast-Domänen	262
Liste	Zusammenfassung der wesentlichen Aspekte von Broadcast-Domänen	264
Abbildung 10.10	Terminologie beim Campus-LAN-Modell	266
Liste	Terminologie vermaschter Topologien	267
Abbildung 10.11	Sterntopologie	267
Abbildung 10.13	2-Ebenen-LAN-Topologie (Collapsed Core)	269
Abbildung 10.14	3-Ebenen-LAN-Topologie (Core)	270
Liste	Zwei wichtige Vergleiche zur Ethernet-Technologie	272
Abbildung 10.20	WLC- und LWAP-Terminologie im Kontext eines Netzdiagramms	279

Schlüssel-thema

Schlüsselbegriffe, die Sie kennen sollten

Access-Layer, Access-Point, Autonegotiating, Broadcast-Domäne, Broadcast-Frame, Collapsed-Core-Modell, Core-Modell, Core-Layer, Distribution-Layer, Flooding, Full-Mesh-Topologie, Hub, Kollisionsdomäne, Partial-Mesh-Topologie, Sterntopologie, transparente Bridge, VLAN, WLC



In diesem Kapitel werden folgende Prüfungsthemen behandelt:

2.0 LAN-Switching-Technologien

2.1 Switching-Konzepte beschreiben und überprüfen

- 2.1.a Erlernen und Alterung von MAC-Adressen
- 2.1.b Frame-Switching
- 2.1.c Frame-Flooding
- 2.1.d MAC-Adresstabelle

2.4 Switch-übergreifende VLANs (normaler Bereich) konfigurieren und überprüfen und Troubleshooting durchführen

- 2.4.a Access-Ports (Daten und Voice)
- 2.4.b Default-VLAN

2.5 Konnektivität zwischen Switches konfigurieren und überprüfen und Troubleshooting durchführen

- 2.5.a Trunk-Ports
- 2.5.b 802.1Q
- 2.5.c Natives VLAN