



Modul 11: IPv4-Adressierung

Material für Instruktoren

Einführung in die
Netzwerktechnik v7.0 (ITN)





Modul 11: IPv4- Adressierung

Einführung in die
Netzwerktechnik v7.0 (ITN)



Modulziele

Modultitel: IPv4-Adressierung

Modulziel: Berechnen eines IPv4-Subnetting-Schemas, um das Netzwerk effizient zu segmentieren.

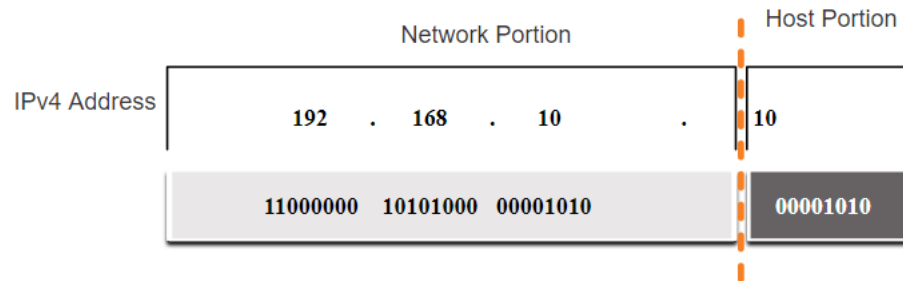
Thema	Ziel
Die Struktur der IPv4-Adresse	Beschreiben Sie die Struktur einer IPv4-Adresse, einschließlich des Netzwerkteils, des Hostteils und der Subnetzmaske.
IPv4 Unicast-, Broadcast- und Multicast-Adressen	Vergleichen Sie die Eigenschaften und Verwendungsmöglichkeiten der Unicast-, Broadcast- und Multicast-IPv4-Adressen.
Arten von IPv4-Adressen	Erläutern Sie öffentliche, private und reservierte IPv4-Adressen.
Netzwerksegmentierung	Erläutern Sie, wie Subnetting ein Netzwerk segmentiert, um eine bessere Kommunikation zu ermöglichen.
Subnetz eines IPv4-Netzwerks	Berechnung von IPv4-Subnetzen mit einer Präfixlänge von /24.

11.1 IPv4-Adressstruktur

IPv4-Adressstruktur

Netzwerk- und Host-Teile

- Eine IPv4-Adresse ist eine hierarchische 32-Bit-Adresse, die sich aus einem Netzwerkteil und einem Host-Teil zusammensetzt.
- Zur Unterscheidung des Netzwerkteils vom Hostteil müssen Sie sich den 32-Bit-Stream betrachten.
- Eine Subnetzmaske wird verwendet, um den Netzwerk- und Hostteil zu ermitteln.



IPv4-Adressstruktur

Die Subnetzmaske

- Um die Netzwerk- und Host-Teile einer IPv4-Adresse zu identifizieren, wird die Subnetzmaske von links nach rechts bitweise mit der IPv4-Adresse verglichen.
- Der eigentliche Prozess zum Identifizieren von Netzwerk- und Host-Teil wird als ANDing (UND-Verknüpfung) bezeichnet.

	Network Portion				Host Portion
IPv4 Address	192	.	168	.	10
	11000000	10101000	00001010		00001010
Subnet Mask	255	.	255	.	0
	11111111	11111111	11111111		00000000

IPv4-Adressstruktur

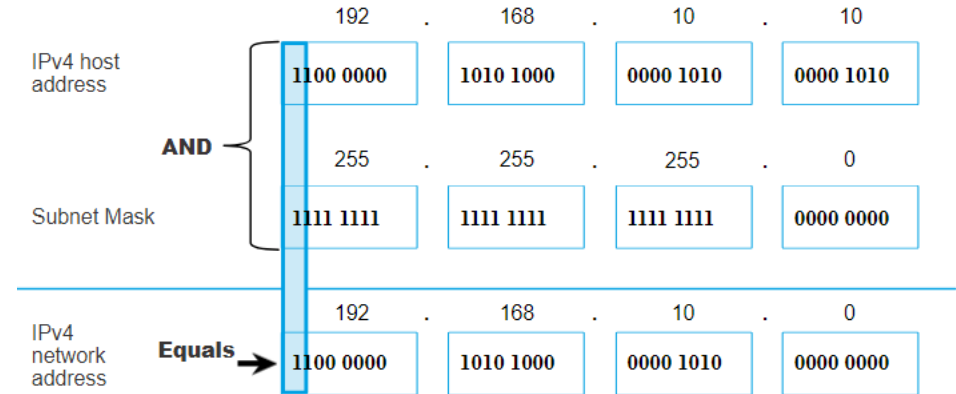
Die Präfixlänge

- Eine Präfixlänge ist eine einfachere Methode zur Identifizierung einer Subnetzmaskenadresse.
- Die Präfixlänge ist die Anzahl der Bits, die in der Subnetzmaske auf 1 gesetzt sind.
- Sie wird in "Schrägstrich-Notation" geschrieben, zählen Sie also die Anzahl der Bits in der Subnetzmaske und stellen Sie diesem Wert einen Schrägstrich voran.

Subnetzmaske	32-Bit-Adresse	Präfix Länge
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

Bestimmen des Netzwerks: Logisch UND

- Bei der Bestimmung der Netzwerkadresse wird eine logische UND boolesche Operation verwendet.
- Logisches UND ist der Vergleich von zwei Bits, wobei eine 1 UND 1 nur eine 1 und jede andere Kombination eine 0 ergibt.
- $1 \text{ UND } 1 = 1$, $0 \text{ UND } 1 = 0$, $1 \text{ UND } 0 = 0$, $0 \text{ UND } 0 = 0$
- $1 = \text{True}$ und $0 = \text{Falsch}$
- Um die Netzwerkadresse eines IPv4-Hosts zu ermitteln, wird die IPv4-Host-Adresse bitweise mithilfe eines logischen UND mit der Subnetzmaske verknüpft, um die Netzwerkadresse zu ermitteln.



Video - Netzwerk-, Host- und Broadcast-Adressen

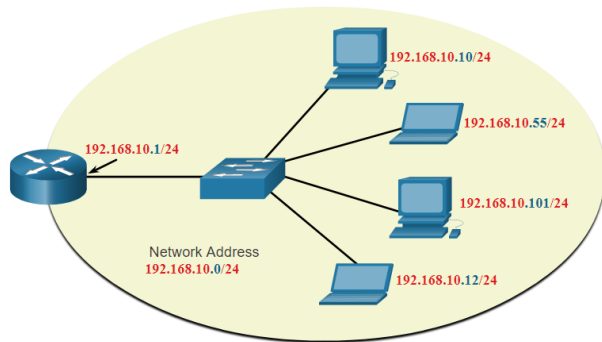
In diesem Video werden folgende Themen behandelt:

- Netzwerkadresse
- Broadcast-Adresse
- Erste nutzbare Host-Adresse
- Letzte nutzbare Host-Adresse

IPv4-Adressstruktur

Netzwerk-, Host- und Broadcast-Adressen

- Innerhalb eines jeden Netzwerks gibt es drei Arten von IP-Adressen:
 - Netzwerkadresse
 - Host-Adressen
 - Broadcast-Adresse



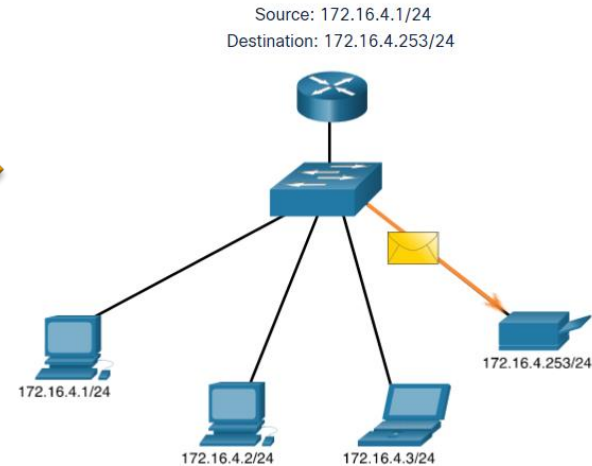
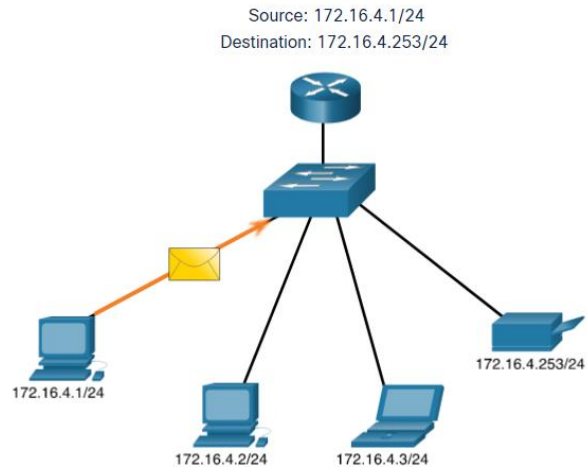
	Netzwerkteil	Host-Teil	Host Bits
Subnetzmaske 255.255.255.0 oder /24	255 255 255 11111111 11111111 11111111	0 00000000	
Netzwerkadresse 192.168.10.0 oder /24	192 168 10 11000000 10100000 00001010	0 00000000	Alles 0
Erste Adresse 192.168.10.1 oder /24	192 168 10 11000000 10100000 00001010	1 00000001	Alles 0 und eine 1
Letzte Adresse 192.168.10.254 or /24	192 168 10 11000000 10100000 00001010	254 11111110	Alles 1 und eine 0
Broadcast-Adresse 192.168.10.255 oder /24	192 168 10 11000000 10100000 00001010	255 11111111	Alle 1

11.2 IPv4-Unicast, Broadcast und Multicast

IPv4-Unicast, Broadcast und Multicast

Unicast

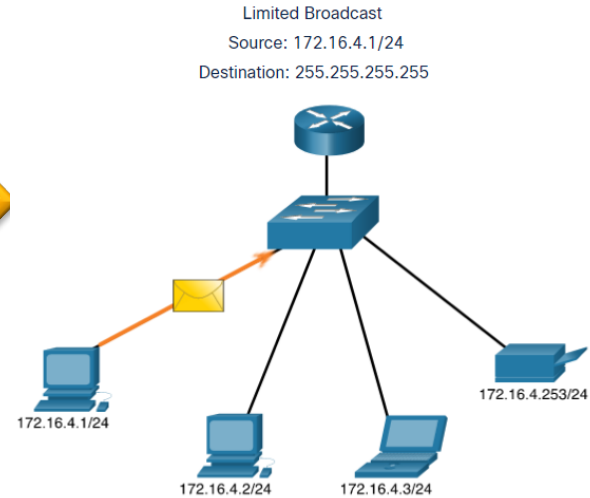
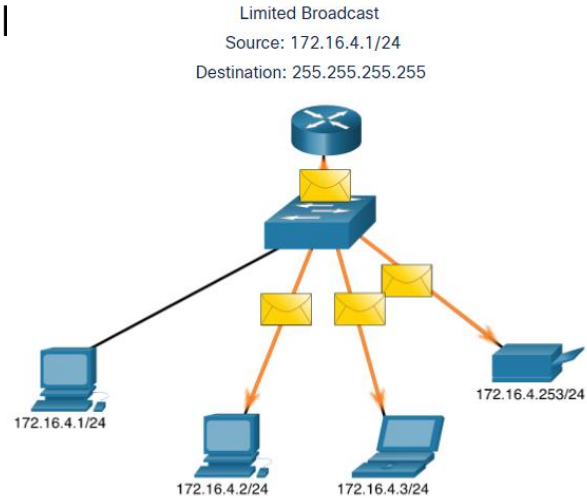
- Bei der Unicast-Übertragung wird ein Paket an eine Ziel-IP-Adresse gesendet.
- So sendet beispielsweise der PC unter 172.16.4.1 ein Unicast-Paket an den Drucker unter 172.16.4.253.



IPv4-Unicast, Broadcast und Multicast

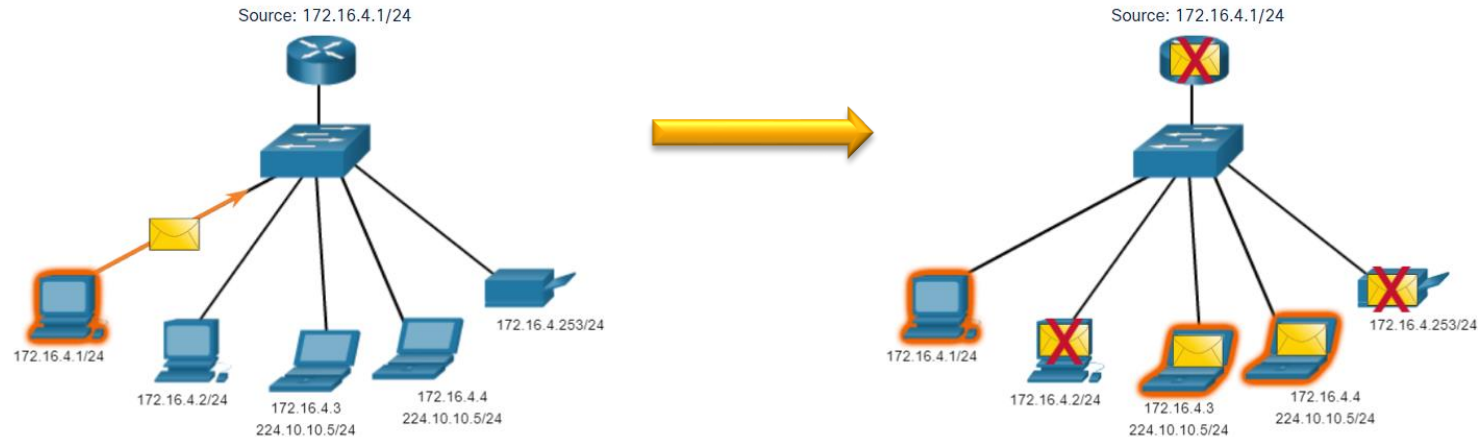
Broadcast

- Bei der Broadcast-Übertragung wird ein Paket an alle anderen Ziel-IP-Adressen gesendet.
- Beispielsweise sendet der PC unter 172.16.4.1 ein Broadcast-Paket an alle IPv4-



IPv4-Unicast, Broadcast und Multicast

- Unter Multicast wird das Senden eines Pakets an eine Multicast-Adressgruppe verstanden.
- So sendet beispielsweise der PC unter 172.16.4.1 ein Multicast-Paket an die Multicast-Gruppenadresse 224.10.10.5.



11.3 Arten von IPv4-Adressen

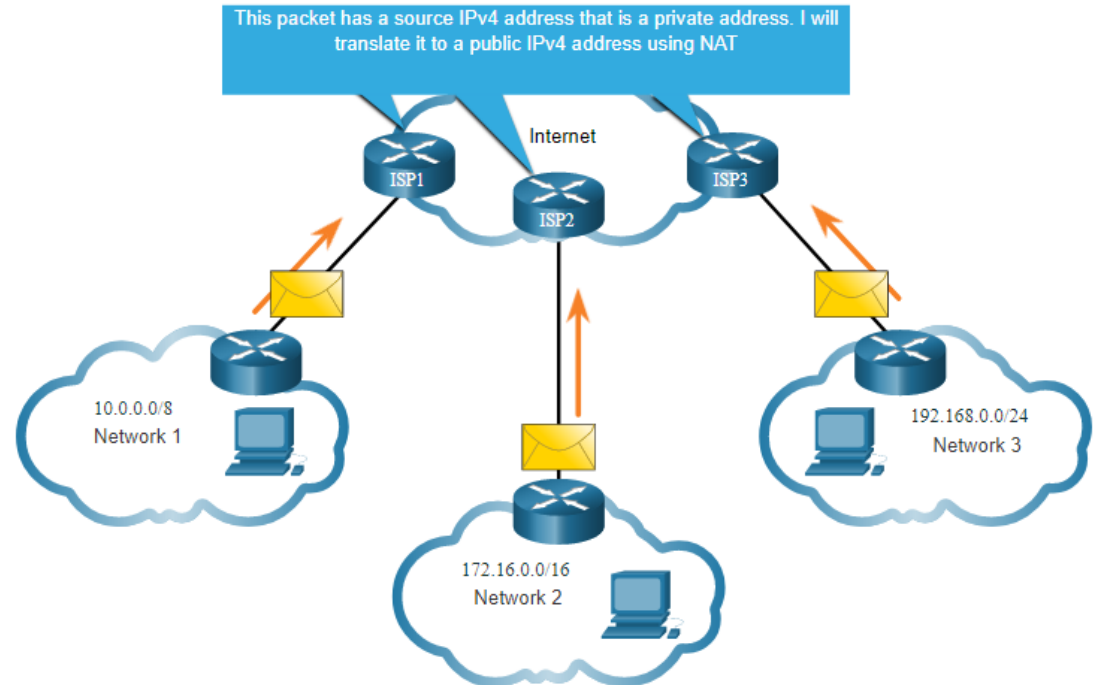
Öffentliche und private IP-Adressen

- Wie in RFC 1918 definiert, werden öffentliche IPv4-Adressen weltweit zwischen den Routern der Internet Service Provider (ISP) geroutet.
- Private Adressen sind gängige Adressblöcke, die von den meisten Organisationen benutzt werden, um internen Hosts IPv4-Adressen zuzuweisen.
- Private IPv4-Adressen sind nicht eindeutig und können intern in jedem Netzwerk verwendet werden.
- Allerdings können private Adressen nicht global geroutet werden.

Netzwerkadresse und -präfix	Privater Adressbereich in RFC 1918
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/12	172.16.0.0 - 172.31.255.255
192.168.0.0/16	192.168.0.0 - 192.168.255.255

Arten von IPv4-Adressen beim Routing im Internet

- Network Address Translation (NAT) übersetzt private IPv4-Adressen in öffentliche IPv4-Adressen.
- NAT ist in der Regel auf dem Edge-Router aktiviert, der mit dem Internet verbunden ist.
- Es übersetzt die interne private Adresse in eine öffentliche globale IP-Adresse.



Spezielle Verwendung IPv4-Adressen

Loopback-Adressen

- 127.0.0.0 /8 (127.0.0.1 to 127.255.255.254)
- Häufig als nur 127.0.0.1 identifiziert
- Wird auf einem Host verwendet, um zu testen, ob TCP/IP betriebsbereit ist.

```
C:\Users\NetAcad> ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

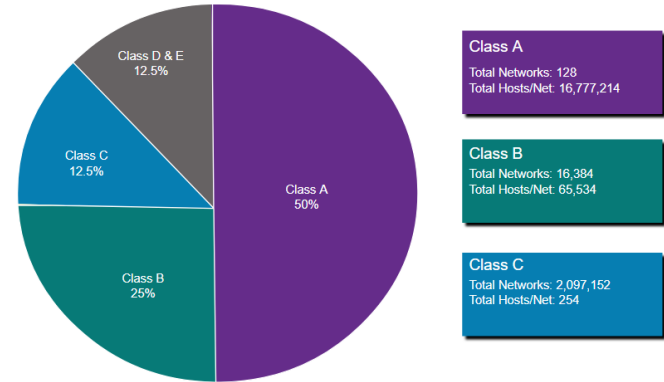
Link-Local-Adressen

- 169.254.0.0 /16 (169.254.0.1 to 169.254.255.254)
- Allgemein bekannt als APIPA-Adressen (Automatic Private IP Addressing) oder selbst zugewiesene Adressen.
- Wird von Windows-DHCP-Clients zur Selbstkonfiguration verwendet, wenn keine DHCP-Server verfügbar sind.

Legacy Classful Addressing

RFC 790 (1981) zugewiesene IPv4-Adressen in Klassen

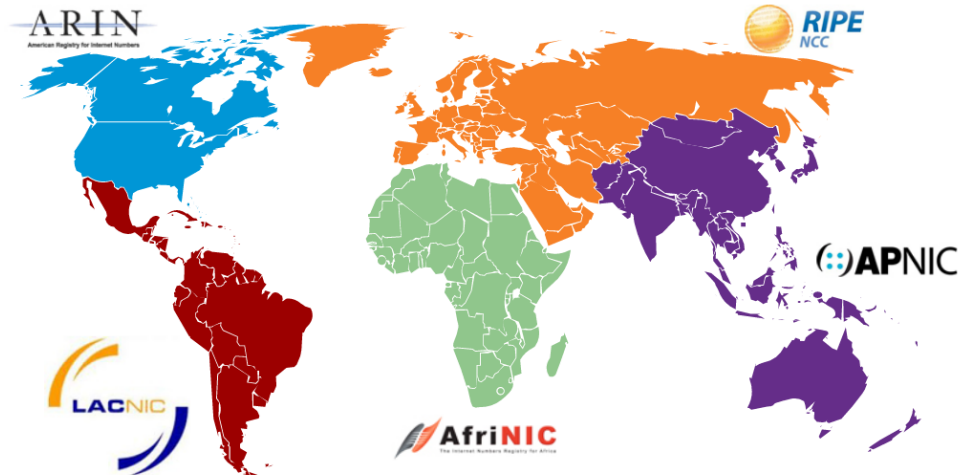
- Klasse A (0.0.0.0/8 bis 127.0.0.0/8)
 - Klasse B (128.0.0.0 /16 — 191.255.0.0 /16)
 - Klasse C (192.0.0.0 /24 — 223.255.255.0 /24)
 - Klasse D (224.0.0.0 bis 239.0.0.0)
 - Klasse E (240.0.0.0 — 255.0.0.0)
-
- Durch klassenlose Adressierung wurden viele IPv4-Adressen verschwendet.



Die klassenweise Adresszuweisung wurde durch eine klassenlose Adressierung ersetzt, die die Regeln der Klassen (A, B, C) ignoriert.

Zuweisung von IP-Adressen

- Die Internet Assigned Numbers Authority (IANA) verwaltet und vergibt Blöcke von IPv4- und IPv6-Adressen an fünf regionale Internet-Register (RIR).
- Die RIRs sind für die Zuweisung von IP-Adressen an ISPs zuständig, die kleineren ISPs und Organisationen IPv4-Adressblöcke zur Verfügung stellen.

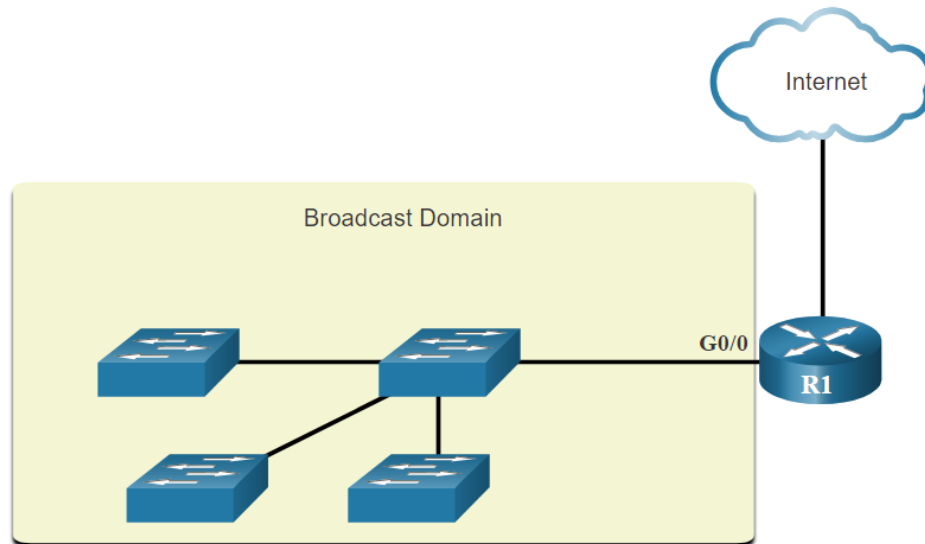


11.4 Netzwerksegmentierung

Netzwerksegmentierung

Broadcast-Domänen und Segmentierung

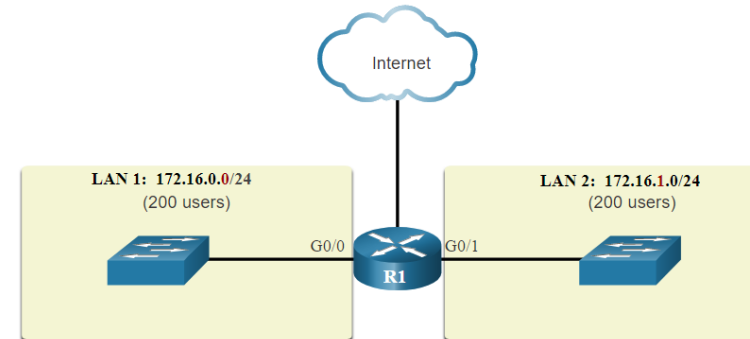
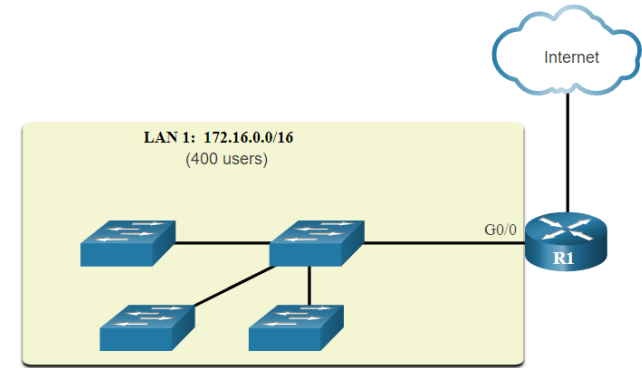
- Viele Protokolle verwenden Broadcasts oder Multicasts (z. B. verwendet ARP Broadcasts zum Auffinden anderer Geräte, Hosts senden DHCP-Discovery-Broadcasts zum Auffinden eines DHCP-Servers).
- Switches leiten Broadcasts über alle Schnittstellen weiter, mit Ausnahme der Schnittstelle, auf der der Broadcast empfangen wurde.



- Das einzige Gerät, das Broadcasts stoppt, ist ein Router.
- Router leiten keine Broadcasts weiter.
- Jede Router-Schnittstelle stellt eine Verbindung zu einer Broadcast-Domäne her und Broadcasts werden nur innerhalb dieser spezifischen Broadcast-Domäne verbreitet.

Probleme mit großen Broadcast-Domänen

- Ein Problem mit großen Broadcast-Domänen besteht darin, dass aufgrund der zahlreichen Hosts übermäßig viele Broadcasts erzeugt werden und die Netzwerkleistung damit beeinträchtigt wird.
- Wird die Größe des Netzwerks reduziert, werden auch kleinere Broadcast-Domänen gebildet. Diese Vorgehensweise wird als Subnetting (Subnetzbildung) bezeichnet.
- Die Netzwerkadresse 172.16.0.0 /16 wird in zwei Subnetze mit jeweils 200 Benutzern unterteilt: 172.16.0.0 /24 und 172.16.1.0 /24.
- Broadcasts werden nur innerhalb der kleineren Broadcast-Domänen weitergeleitet.

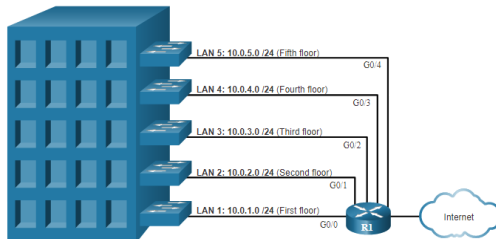


Netzwerksegmentierung

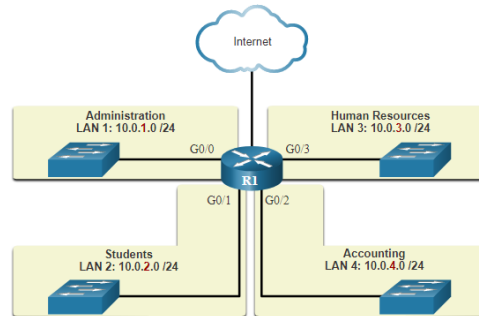
Gründe für die Segmentierung von Netzwerken

- Durch die Subnetzbildung wird der gesamte Netzwerkverkehr reduziert und die Netzwerkleistung wird verbessert.
- Sie kann zur Implementierung von Sicherheitsrichtlinien zwischen Subnetzen verwendet werden.
- Subnetting reduziert die Anzahl der Geräte, die von anormalem Broadcast-Verkehr betroffen sind.
- Subnetze werden aus einer Vielzahl von Gründen verwendet, unter anderem durch:

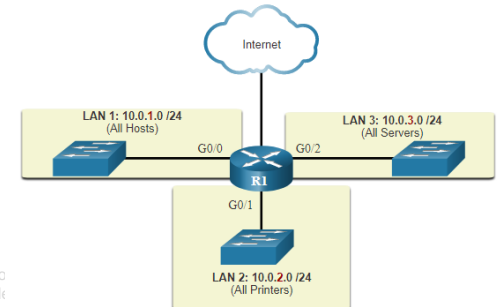
Standort



Gruppe oder Funktion



Gerätetyp



11.5 Subnetz eines IPv4-Netzwerks

Subnetz eines IPv4-Netzwerk

Subnetz in einem Oktettbereich

- Die Subnetzbildung von Netzwerken erfolgt am einfachsten im Oktettbereich /8, /16 und /24.
- Beachten Sie, dass sich die Anzahl der Hosts pro Subnetz durch die Verwendung längerer Präfixlängen verringert.

Präfixlänge	Subnetzmaske	Subnetzmaske im Binärformat (n = Netzwerk, h = Host)	Anzahl der Hosts
/8	255.0.0.0	<code>nnnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh</code> <code>11111111.00000000.00000000.00000000</code>	16.777.214
/16	255.255.0.0	<code>nnnnnnnnn.nnnnnnnnn.hhhhhhhh.hhhhhhhh</code> <code>11111111.11111111.00000000.00000000</code>	65.534
/24	255.255.255.0	<code>nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.hhhhhhhh</code> <code>11111111.11111111.11111111.00000000</code>	254

Subnetz eines IPv4-Netzwerks

Subnetz in einem Oktettbereich (Fortsetzung)

- In der ersten Tabelle wird 10.0.0.0/8 mit /16 und in der zweiten Tabelle eine /24 Maske subnettiert.

Subnetzadresse (65.536 mögliche Subnetze)	Host-Bereich (65.534 mögliche Hosts pro Subnetz)	Broadcast
10.0.0.0/16	10.0.0.1 - 10.0.255.254	10.0.255.255
10.1.0.0/16	10.1.0.1 - 10.1.255.254	10.1.255.255
10.2.0.0/16	10.2.0.1 - 10.2.255.254	10.2.255.255
10.3.0.0/16	10.3.0.1 - 10.3.255.254	10.3.255.255
10.4.0.0/16	10.4.0.1 - 10.4.255.254	10.4.255.255
10.5.0.0/16	10.5.0.1 - 10.5.255.254	10.5.255.255
10.6.0.0/16	10.6.0.1 - 10.6.255.254	10.6.255.255
10.7.0.0/16	10.7.0.1 - 10.7.255.254	10.7.255.255
...
10.255.0.0/16	10.255.0.1 - 10.255.255.254	10.255.255.255

Subnetzadresse (65.536 mögliche Subnetze)	Host-Bereich (254 mögliche Hosts pro Subnetz)	Broadcast
10.0.0.0/24	10.0.0.1 - 10.0.0.254	10.0.0.255
10.0.1.0/24	10.0.1.1 - 10.0.1.254	10.0.1.255
10.0.2.0/24	10.0.2.1 - 10.0.2.254	10.0.2.255
...
10.0.255.0/24	10.0.255.1 - 10.0.255.254	10.0.255.255
10.1.0.0/24	10.1.0.1 - 10.1.0.254	10.1.0.255
10.1.1.0/24	10.1.1.1 - 10.1.1.254	10.1.1.255
10.1.2.0/24	10.1.2.1 - 10.1.2.254	10.1.2.255
...
10.100.0.0/24	10.100.0.1 - 10.100.0.254	10.100.0.255
...
10.255.255.0/24	10.255.255.1 - 10.255.255.254	10.255.255.255

Subnetz eines IPv4-Netzwerks

Subnetz in einem Oktettbereich

- In der Tabelle finden Sie sechs Möglichkeiten zum Subnetz eines /24-Netzwerks.

Präfixlänge	Subnetzmaske	Subnetzmaske im Binärformat (n = Netzwerk, h = Host)	Anzahl der Subnetze	Anzahl der Hosts
/25	255.255.255.128	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nhhhhhhhh 11111111.11111111.11111111.10000000	2	126
/26	255.255.255.192	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nnhhhhhhh 11111111.11111111.11111111.11000000	4	62
/27	255.255.255.224	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nnnhhhhhh 11111111.11111111.11111111.11100000	8	30
/28	255.255.255.240	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nnnnnhhhh 11111111.11111111.11111111.11110000	16	14
/29	255.255.255.248	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nnnnnnhhh 11111111.11111111.11111111.11111000	32	6
/30	255.255.255.252	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nnnnnnhh 11111111.11111111.11111111.11111100	64	2

Subnetz und IPv4-Netzwerk

Video — Die Subnetzmaske

- Dieses Video zeigt den Prozess des Subnetting.

Video — Subnetz mit der Magic Number

- In diesem Video wird das Subnetz mit der magischen Nummer demonstriert.

Paket Tracer — Subnetz eines IPv4-Netzwerks

In diesem Paket Tracer werden Sie Folgendes tun:

- Entwurf eines Subnetting-Schemas für ein IPv4 Netzwerk
- Konfiguration der Geräte
- Testen des Netzwerks und Fehlerbehebung

11.6 Subnetz mit /16- und /8- Präfix

Subnetz mit /16- und /8-Präfix Subnetze mit einem /16-Präfix erstellen

- Die Tabelle zeigt alle möglichen Szenarien für die Subnetzbildung mit einem /16-Präfix auf.

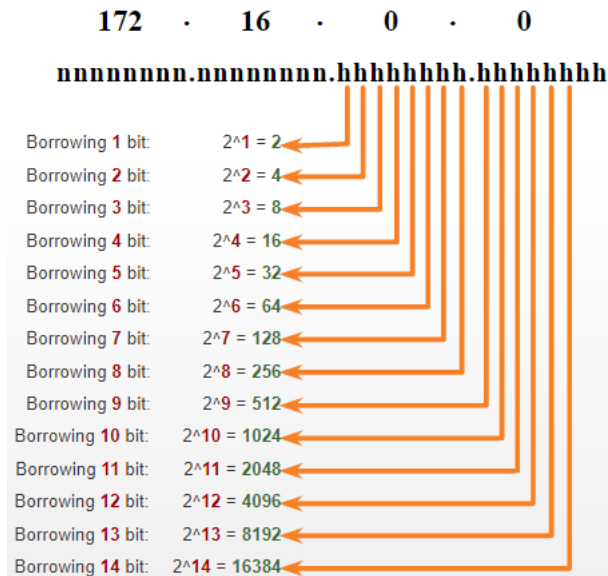
Präfixlänge	Subnetzmaske	Netzwerkadresse (n = Netzwerk, h = Host)	Anzahl der Subnetze	Anzahl der Hosts
/17	255.255.128.0	nnnnnnnn.nnnnnnnn.nh h h h h h h h h h h h h h h h h 11111111.11111111.10000000.00000000	2	32766
/18	255.255.192.0	nnnnnnnn.nnnnnnnn.nnh h h h h h h h h h h h h h h h h 11111111.11111111.11000000.00000000	4	16382
/19	255.255.224.0	nnnnnnnn.nnnnnnnn.nnn h h h h h h h h h h h h h h h h 11111111.11111111.11100000.00000000	8	8190
/20	255.255.240.0	nnnnnnnn.nnnnnnnn.nnnn h h h h h h h h h h h h h h h h 11111111.11111111.11110000.00000000	16	4094
/21	255.255.248.0	nnnnnnnn.nnnnnnnn.nnnnn h h h h h h h h h h h h h h h h 11111111.11111111.11111000.00000000	32	2046
/22	255.255.252.0	nnnnnnnn.nnnnnnnn.nnnnnn h h h h h h h h h h h h h h h h 11111111.11111111.11111100.00000000	64	1022
/23	255.255.254.0	nnnnnnnn.nnnnnnnn.nnnnnnn h h h h h h h h h h h h h h h h 11111111.11111111.11111110.00000000	128	510
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn h h h h h h h h h h h h h h h h 11111111.11111111.11111111.00000000	256	254
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nh h h h h h h h h h h h h h h h h 11111111.11111111.11111111.10000000	512	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnh h h h h h h h h h h h h h h h h 11111111.11111111.11111111.11000000	1024	62
/27	255.255.255.ca. 224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnn h h h h h h h h h h h h h h h h 11111111.11111111.11111111.11100000	2048	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnn h h h h h h h h h h h h h h h h 11111111.11111111.11111111.11110000	4096	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnn h h h h h h h h h h h h h h h h 11111111.11111111.11111111.11111000	8192	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnnn h h h h h h h h h h h h h h h h 11111111.11111111.11111111.11111100	16384	2

100 Subnetze mit /16-Prefix erstellen

Nehmen Sie als Beispiel ein großes Unternehmen, das mindestens 100 Subnetze benötigt und die private Adresse 172.16.0.0/16 als interne Netzwerkadresse festgelegt hat.

- Die Abbildung zeigt die Anzahl der Subnetze an, die beim Entleihen von Bits aus dem dritten Oktett und dem vierten Oktett erzeugt werden können.
- Beachten Sie, dass es jetzt bis zu 22 Host-Bits gibt, die ausgeliehen werden können (d.h. die letzten beiden Bits können nicht ausgeliehen werden).

Um die Anforderung von 100 Subnetzen für das Unternehmen zu erfüllen, müssten ⁷ Bits (d.h. $2^7 = 128$ Subnetze) ausgeliehen werden (für insgesamt 128 Subnetze).

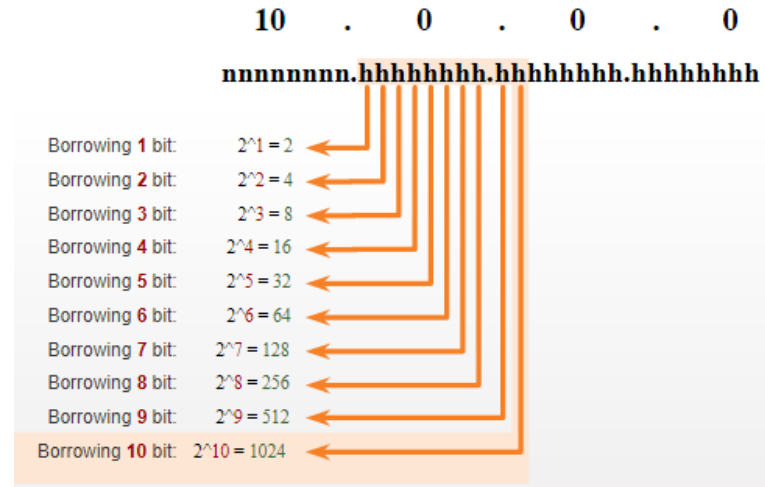


1.000 Subnetze mit /8-Prefix erstellen

Stellen Sie sich einen kleinen ISP vor, der 1.000 Subnetze für seine Kunden benötigt, die die Netzwerkadresse 10.0.0.0/8 verwenden, was bedeutet, dass 8 Bits im Netzwerkteil und 24 Hostbits zur Verfügung stehen, die für das Subnetting ausgeliehen werden können.

- Die Abbildung zeigt die Anzahl der Subnetze, die beim Ausleihen von Bits aus dem zweiten und dritten erstellt werden können.
- Beachten Sie, dass es jetzt bis zu 22 Host-Bits gibt, die ausgeliehen werden können (d.h. die letzten beiden Bits können nicht ausgeliehen werden).

Um die Anforderung von 1000 Subnetzen für das Unternehmen zu erfüllen, müssten 10 Bits (d.h. $2^{10}=1024$ Subnetze) ausgeliehen werden (für insgesamt 128 Subnetze).



Video — Subnetz über mehrere Oktette

Dieses Video zeigt das Erstellen von Subnetzen über mehrere Oktette hinweg.

Übung — Berechnen von IPv4-Subnetzen

In dieser Übung werden Sie die folgenden Lernziele umsetzen:

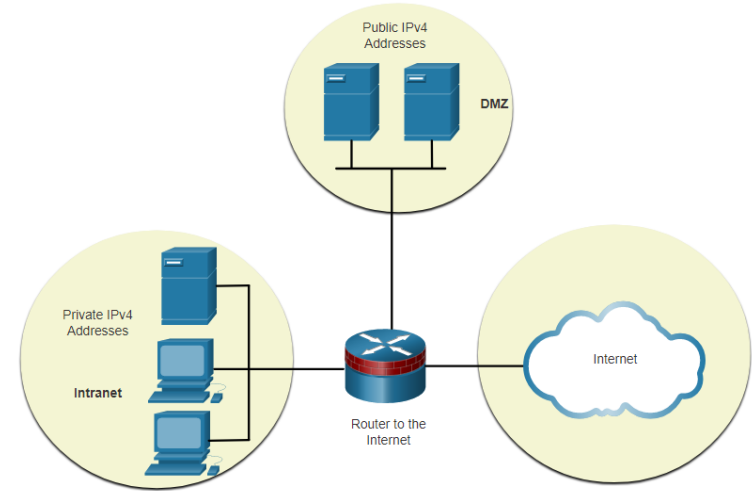
- Teil 1: Bestimmen des Subnetzes einer IPv4-Adresse
- Teil 2: Berechnen von Subnetz-Informationen für eine IPv4-Adresse

11.7 Subnetz zur Erfüllung der Anforderungen

Vergleich des Subnetzes aus dem privaten und dem öffentlichen IPv4-Adressraum

Unternehmensnetzwerke benötigen:

- Intranet - Im internen Netzwerk eines Unternehmens werden normalerweise private IPv4-Adressen verwendet.
- DMZ — Ein Unternehmen mit Servern ins Internet. Geräte in der DMZ verwenden öffentliche IPv4-Adressen.
- Ein Unternehmen könnte 10.0.0.0/8 und das Subnetz im Netzwerkbereich /16 oder /24 verwenden.
- Die DMZ-Geräte müssten mit öffentlichen IP-Adressen konfiguriert werden.



Subnetz zur Erfüllung der Anforderungen

Minimieren Sie nicht verwendete Host-IPv4-Adressen und maximieren Sie Subnetze

Beim Planen von Subnetzen müssen zwei Faktoren berücksichtigt werden:

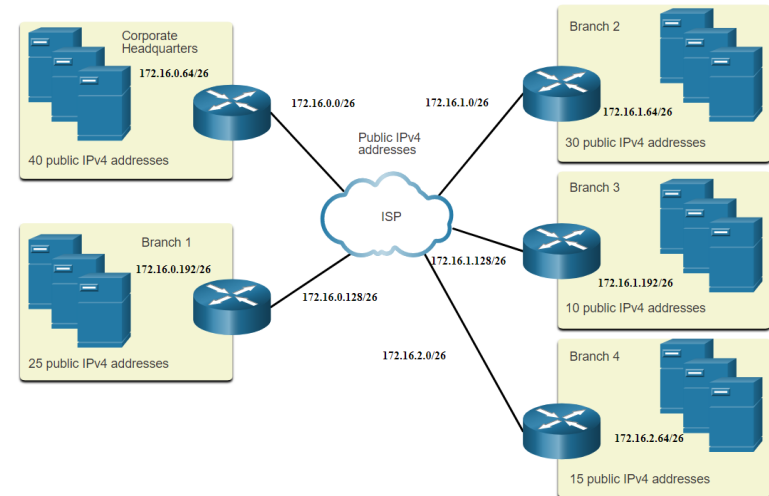
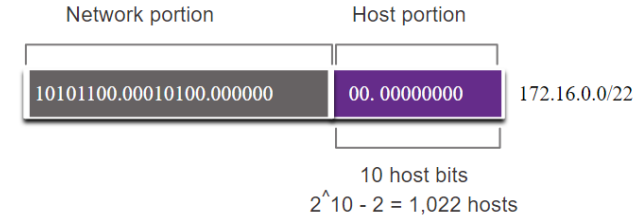
- die Anzahl der für jedes Netzwerk benötigten Host-Adressen
- die erforderliche Anzahl einzelner Subnetze

Präfixlänge	Subnetzmaske	Subnetzmaske im Binärformat (n = Netzwerk, h = Host)	Anzahl der Subnetze	Anzahl der Hosts
/25	255.255.255.128	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nhhhhhhhh 11111111.11111111.11111111.10000000	2	126
/26	255.255.255.192	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nnhhhhhhh 11111111.11111111.11111111.11000000	4	62
/27	255.255.255.224	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nnnhhhhhh 11111111.11111111.11111111.11100000	8	30
/28	255.255.255.240	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nnnnnhhhh 11111111.11111111.11111111.11110000	16	14
/29	255.255.255.248	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nnnnnnhhh 11111111.11111111.11111111.11111000	32	6
/30	255.255.255.252	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nnnnnnhh 11111111.11111111.11111111.11111100	64	2

Subnetz zur Erfüllung der Anforderungen

Beispiel: Effizientes IPv4-Subnetting

- In diesem Beispiel wurde der Firmenzentrale von ihrem ISP, der 1.022 Host-Adressen bereitstellt, die öffentliche Netzwerkadresse 172.16.0.0/22 (10 Host-Bits) zugewiesen.
- Es gibt fünf Standorte und somit fünf Internetverbindungen, was bedeutet, dass die Organisation 10 Subnetze benötigt, wobei das größte Subnetz 40 Adressen benötigt.
- Es wurden 10 Subnetze mit einer /26 (d.h. 255.255.255.255.192) Subnetzmaske zugewiesen.



Subnetz zur Erfüllung der Anforderungen

Packet Tracer — Subnetting Szenario

In dieser Paket Tracer-Übung werden Sie Folgendes tun:

- Entwerfen eines IP-Adressierungsschemas
- Zuweisen von IP-Adressen zu Netzwerkgeräten und Überprüfen der Netzwerkverbindungen

11.8 VLSM

VLSM

Video — VLSM Grundlagen

- In diesem Video werden die Grundlagen von VLSM erläutert.

VLSM

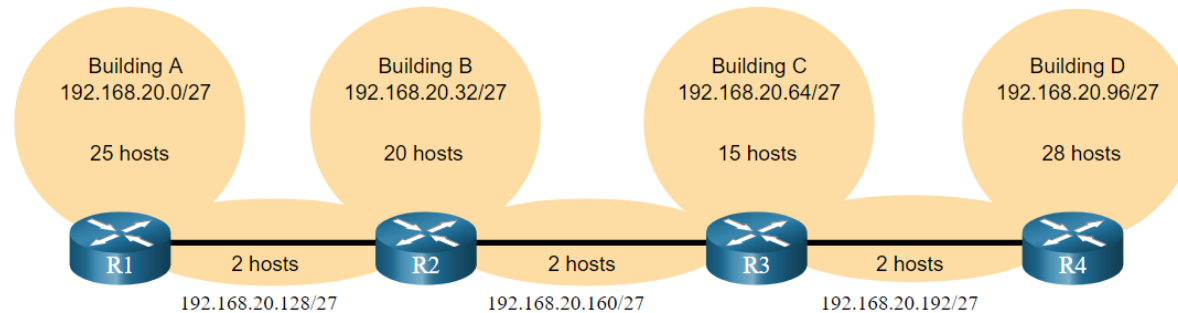
Video – VLSM-Beispiel

- Dieses Video demonstriert die Einrichtung von Subnetzen, die speziell auf die Anforderungen des Netzwerks zugeschnitten sind.

VLSM IPv4-Adresse erhalten

Aufgrund der Topologie sind 7 Subnetze erforderlich (d.h. vier LANs und drei WAN-Verbindungen). Im Gebäude D befinden sich die meisten Hosts, insgesamt 28.

- Eine /27-Maske würde 8 Subnetze mit 30 Host-IP-Adressen bereitstellen und daher diese Topologie unterstützen.



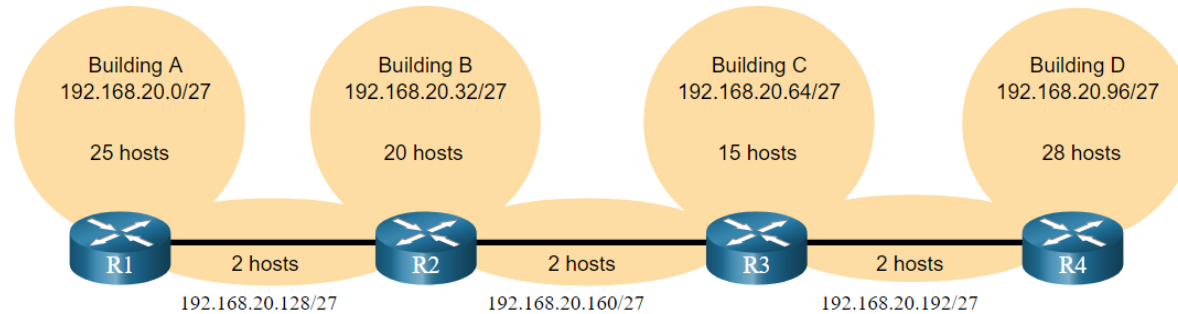
IPv4-Adresse erhalten (Fortsetzung)

Die Punkt-zu-Punkt-WAN-Verbindungen benötigen jedoch nur zwei Adressen und verschwenden daher jeweils 28 Adressen bei insgesamt 84 ungenutzten Adressen.

Host portion
 $2^5 - 2 = 30$ host IP addresses per subnet

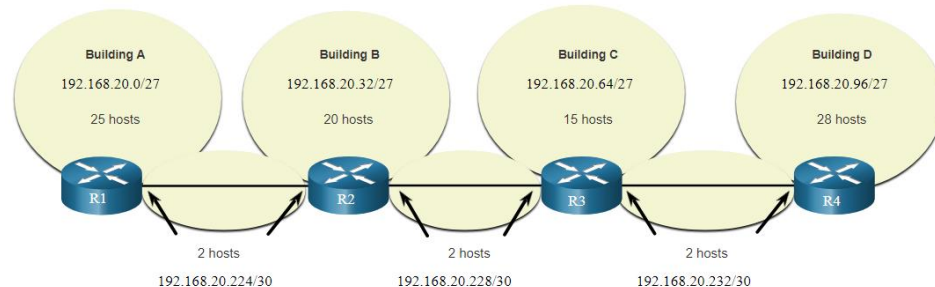
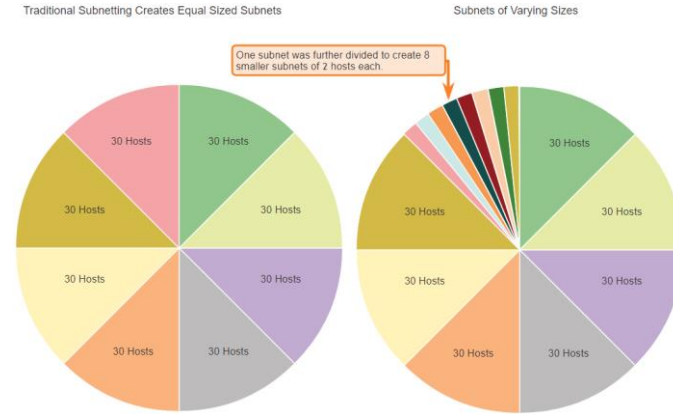
 $30 - 2 = 28$
Each WAN subnet wastes 28 addresses

 $28 \times 3 = 84$
84 addresses are unused



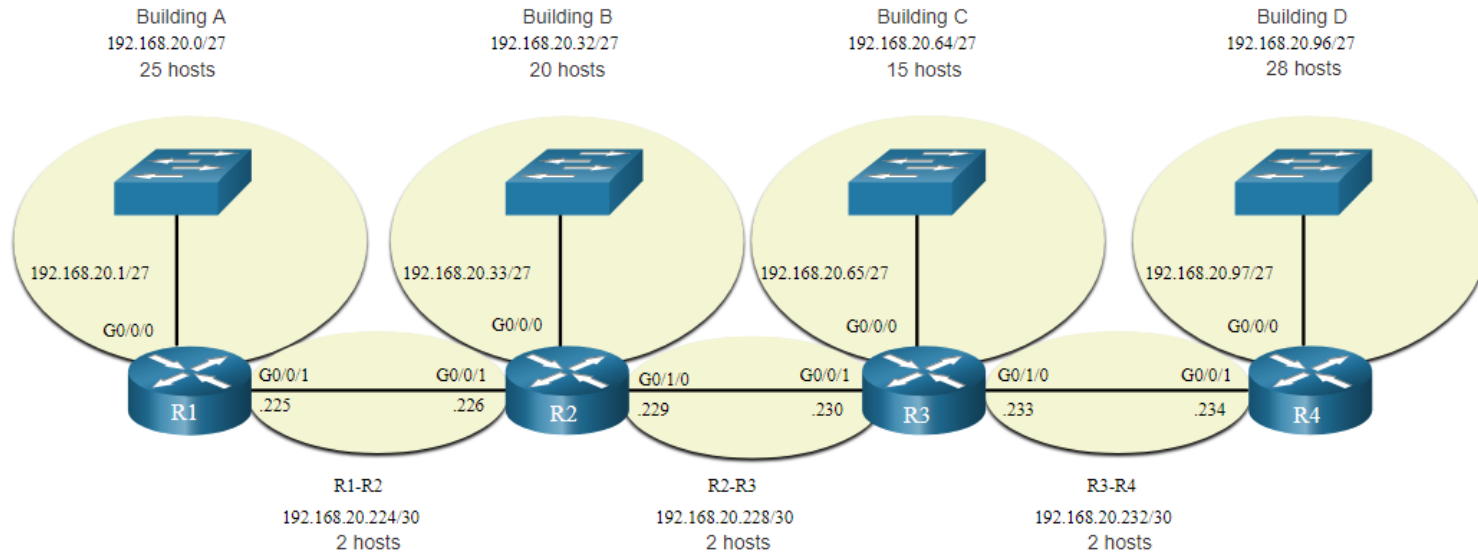
- Bei diesem Szenario ist die herkömmliche Herangehensweise bei der Subnetzbildung nicht sehr effizient und führt zu Verschwendung.
- VLSM wurde entwickelt, um die Verschwendung von Adressen zu vermeiden, indem es uns ermöglicht, ein Subnetz zu unterteilen.

- Die linke Seite zeigt das traditionelle Subnetz-Schema (d.h. dieselbe Subnetzmaske), während die rechte Seite veranschaulicht, wie VLSM verwendet werden kann, um ein Subnetz zu unterteilen und das letzte Subnetz in acht /30 Subnetze aufzuteilen.
- Wenn Sie VLSM verwenden, beginnen Sie immer damit, die Host-Anforderungen des größten Subnetzes zu erfüllen und fahren dann mit dem Subnetting fort, bis die Host-Anforderungen des kleinsten Subnetzes erfüllt sind.
- Die sich daraus ergebende Topologie mit angewandtem VLSM.



VLSM-Topologie Adresszuweisung

- Mit Hilfe von VLSM-Subnetzen können die LAN- und Inter-Router-Netzwerke ohne unnötigen Verlust angesprochen werden, wie in der Diagramm-Abbildung der logischen Topologie dargestellt.



11.9 Strukturiertes Design

Strukturiertes Design

IPv4-Netzwerk-Adresseplanung

Die IP-Netzwerkplanung ist entscheidend für die Entwicklung einer skalierbaren Lösung für ein Unternehmensnetzwerk.

- Um ein IPv4-Adressierungsschema für das gesamte Netzwerk zu entwickeln, müssen Sie wissen, wie viele Subnetze benötigt werden, wie viele Hosts ein bestimmtes Subnetz benötigt, welche Geräte Teil des Subnetzes sind, welche Teile Ihres Netzwerks private und welche öffentliche Adressen verwenden und viele weitere entscheidende Faktoren.

Untersuchen Sie die Bedürfnisse der Nutzung des Netzwerks einer Organisation und wie die Subnetze strukturiert werden sollen.

- Führen Sie eine Untersuchung der Netzwerkanforderungen durch, indem Sie das gesamte Netzwerk betrachten, um festzustellen, wie jeder Bereich segmentiert werden soll.
- Ermitteln Sie, wie viele Subnetze benötigt werden und wie viele Hosts pro Subnetz.
- Definieren Sie DHCP-Adresspools und Layer-2-VLAN-Pools.

Strukturiertes Design

Zuweisung von Geräteadressen

Innerhalb eines Netzwerks gibt es verschiedene Arten von Geräten, die Adressen erforderlich machen:

- **Endbenutzer-Clients** – Die überwiegende Mehrheit verwendet DHCP, um Fehler und die Belastung des Netzwerkbetreuungspersonals zu reduzieren. IPv6-Clients können Adressinformationen über DHCPv6 oder SLAAC abrufen.
- **Server und Peripheriegeräte – Diese sollten eine eindeutige statische IP-Adresse erhalten.**
- **Server, die über das Internet erreichbar sind**– Server müssen eine öffentliche IPv4-Adresse erhalten, auf die meist über NAT zugegriffen wird.
- **Aktive Netzwerkkomponenten** – Den Geräten werden Adressen für Netzwerkmanagement, Überwachung und Sicherheit zugewiesen.
- **Gateway** — Router und Firewall-Geräte sind das Gateway für die Hosts in diesem Netzwerk.

Bei der Entwicklung eines IP-Adressenschemas wird im allgemeinen empfohlen, dass es ein festes Muster für die Zuweisung von Adressen für jede Gerätart gibt.

Packet Tracer - VLSM Entwurfs- und Implementierungspraxis

In dieser Paket Tracer-Übung werden Sie Folgendes tun:

- Prüfen der Netzwerkanforderungen
- Entwerfen Sie das VSLM-Adressierungsschema
- Zuweisen von IP-Adressen an Netzwerkgeräte und Überprüfen der Konnektivität

11.10 Modul Praxis und Quiz

Strukturiertes Design

Packet Tracer - Entwurf und Implementierung eines VLSM-Adressierungsschemas

In dieser Paket Tracer-Übung werden Sie Folgendes tun:

- Entwerfen eines VLSM-IP-Adressierungsschemas unter Berücksichtigung der Anforderungen
- Adresskonfiguration auf Netzwerkgeräten und Hosts
- Überprüfen der IP-Konnektivität
- Beheben Sie bei Bedarf Konnektivitätsprobleme.

Strukturiertes Design

Übung - Packet Tracer - Entwurf und Implementierung eines VLSM-Adressierungsschemas

Diese Übung beinhaltet folgende Lernziele:

- Prüfen der Netzwerkanforderungen
- Entwurf des VSLM-Adresssschemas
- Verkabelung und Konfiguration des IPv4-Netzwerks

Was habe ich in diesem Modul gelernt?

- Die IP-Adressstruktur besteht aus einer hierarchischen 32-Bit-Netzwerkadresse, die einen Netz- und einen Host-Teil ausweist. Netzwerkgeräte verwenden einen Prozess namens UND-Verknüpfung unter Verwendung der IP-Adresse und der zugehörigen Subnetzmaske, um den Netzwerk- und Host-Teil zu identifizieren.
- IPv4-Zielpakete können Unicast, Broadcast und Multicast sein.
- Es gibt global routbare IP-Adressen, wie sie von der IANA vergeben werden und es gibt drei Bereiche von privaten IP-Netzwerkadressen, die nicht global geroutet, aber in allen internen privaten Netzwerken verwendet werden können.
- Reduzieren Sie große Broadcast-Domänen durch die Verwendung von Subnetzen zur Realisierung kleinerer Broadcast-Domänen, reduzieren Sie den gesamten Netzwerkverkehr und verbessern Sie die Netzwerkleistung.
- Erstellen Sie IPv4-Subnetze, indem Sie ein oder mehrere der Host-Bits als Netzwerkbits verwenden. Am leichtesten lassen sich Netzwerke jedoch in den Oktett-Bereichen /8, /16 und /24 unterteilen.
- Größere Netzwerke können in den Bereichen /8 oder /16 subnettiert werden.
- Verwenden Sie VLSM, um die Anzahl der nicht verwendeten Hostadressen pro Subnetz zu reduzieren.

Was habe ich in diesem Modul gelernt? (Forts.)

- Mit VLSM kann ein Netzwerkraum in ungleiche Teile aufgeteilt werden. Beginnen Sie immer mit der Erfüllung der Host-Anforderungen des größten Subnetzes. Fahren Sie mit der Subnetzbildung fort, bis die Host-Anforderungen des kleinsten Subnetzes erfüllt sind.
- Berücksichtigen Sie beim Entwurf eines Netzwerk-Adressierungsschemas interne, DMZ- und externe Anforderungen. Verwenden Sie ein konsistentes internes IP-Adressierungsschema mit einem festgelegten Muster, wie die Adressen den einzelnen Gerätetypen zugewiesen werden.

