Übersicht

Subnetting

1. Subnetting ist der Prozess, große Netzwerke in kleinere, logisch zusammengehörige Subnetze zu unterteilen.

2. Ziel ist es, die IP-Adressierung effizienter zu nutzen und Broadcast-Domänen zu begrenzen.

3. Beim IPv4 wird dies durch Subnetzmasken realisiert, die angeben, welcher Teil der Adresse das Subnetz identifiziert.

4. Eine Standard-Netzmaske gehört oft zu Klassenbasierter Adressierung, doch CIDR ermöglicht flexible Blockgrößen.

5. Die Subnetzmaske besteht aus Summe von 1-Bits und 0-Bits, z. B. 255.255.255.0 oder /24.

6. Die Netzadresse wird durch UND-Verknüpfung der IP-Adresse mit der Subnetzmaske gebildet.

7. Die Hostanteil-Bits ergeben sich aus den Bits, die in der Maske auf 0 stehen.

8. Broadcast-Adresse des Subnetzes ergibt sich, wenn alle Host-Bits auf 1 gesetzt werden.

9. Gateway- oder Router-Interface muss im Subnetz liegen, damit Traffic weitergeleitet werden kann.

10. VLSM (Variable Length Subnet Mask) erlaubt unterschiedliche Subnetzgrößen innerhalb desselben Netzwerks.

11. Subnetting erhöht Sicherheit, indem Broadcast-Domänen getrennt und Spanning-Tree-B underminimiert werden.

12. Es hilft auch bei der Skalierbarkeit großer Netzwerke und reduziert unnötigen IP-Verbrauch.

13. Bei IPv4 ist eine sorgfältige Planung der Subnetze wichtig, um Adressknappheit zu vermeiden.

14. Fehlerquellen sind falsche Masken, Überschneidungen von Subnetzen und falsche Routen.

15. Für IPv6 erfolgt Subnetting auf andere Weise, da Adressraum größer ist und Subnetze durch Präfixlänge definiert werden.

16. In vielen Netzwerken werden Subnetze durch Router-Interfaces, Switches und Firewall-Richtlinien benutzt.

17. Tools zur Planung helfen bei der Visualisierung von Subnetzen, Adressverteilungsplänen und Reservierungen.

18. Kurz gesagt: Subnetting optimiert Nutzung, reduziert Broadcast-Verkehr und erleichtert Netzwerkmanagement.

Routing

1. Routing ist der Prozess der Bestimmung des besten Pfades für Netzwerknachrichten zwischen Hosts.

2. Router sind spezialisierte Geräte, die am Rand oder im Kern eines Netzwerks stehen.

3. Im Routing trennt man Control Plane (Entscheidungen) von Data Plane (Paketweiterleitung).

4. Statisches Routing basiert auf fest konfigurierten Routen ohne dynamische Anpassung.

5. Dynamische Routing-Protokolle öğren ermöglichen automatische Pfadfindung und Anpassung.

6. Metriken wie Hop-Count, Kosten, Bandbreite, Latenz und Zuverlässigkeit beeinflussen Routenwahl.

7. Routing-Tabellen speichern Ziele, nächste Hoppunkte, Schnittstelle, Metrik und Administratieve Distance.

8. Greatest- or Longest-Prefix-Match-Prinzip wird genutzt, um die genaue Route zu finden.

9. Konvergenz ist der Zustand, in dem alle Router konsistente, aktuelle Routing-Informationen haben.

10. Routing-Schleifen können auftreten, wenn Protokolle nicht richtig konfiguriert sind.

11. Beliebte Routing-Protokolle sind RIP, OSPF, EIGRP und BGP, jeweils mit eigenen Eigenschaften.

12. RIP ist einfach, aber langsam und begrenzt in großen Netzen.

13. OSPF teilt Netze in Bereiche (Areas) und nutzt Link-State-Informationen für genauere Topologien.

14. BGP ist das Kernprotokoll des Internets und verbindet verschiedene autonome Systeme (AS).

15. Sicherheitsaspekte im Routing umfassen Authentifizierung, Filterung und Redundanz-Planung.

16. Routing-Updates können regelmäßig oder auf Ereignisse basieren, je nach Protokoll.

17. Failover-Strategien erhöhen Ausfallsicherheit, indem alternative Pfade vorgehalten werden.

18. Insgesamt ermöglicht Routing die effiziente, skalierbare und resiliente Weiterleitung von Datenpaketen.

Routing Tabellen

1. Routing-Tabellen speichern die relevanten Informationen zur Weiterleitung von Paketen.

2. Jede Zeile repräsentiert eine Route zu einem Zielnetzwerk oder -host.

3. Felder in einer Routing-Tabelle umfassen Destination, Subnetzmaske, Next Hop, Interface und Metrik.

4. Destination und Maske definieren das Zielnetzwerk mittels Longest Prefix Match.

5. Der Next Hop gibt an, welcher Router oder welches Interface als nächstes benutzt wird.

6. Die Interface-Spalte spezifiziert, über welche physische oder virtuelle Verbindung geroutet wird.

7. Die Metrik ist eine Kennzahl, die die Vorzuglichkeit der Route gegenüber Alternativen ausdrückt.

8. Die Administrative Distance priorisiert Routen inkompatibler Protokolle, die in der Tabelle erscheinen.

9. Default-Routen bieten einen Ausweg für Ziele, die nicht explizit in der Tabelle stehen.

10. Redistribution verbindet verschiedene Routing-Protokolle, um eine konsistente Sicht zu schaffen.

11. Routing-Tabellen werden regelmäßig aktualisiert, wenn sich Topologien ändern.

12. Longest-Prefix-Match-Prinzip sorgt dafür, dass die spezifischste Route verwendet wird.

13. Aggressive Freeze- oder Guard-Routings können Stabilität bei Flap-Situationen bieten.

14. In IPv6 sind Routing-Tabellen ähnlich strukturiert, nutzen jedoch Präfixe statt Masken.

15. Sicherheitsmaßnahmen schützen Routing-Tabellen vor manipulierten Updates oder Spoofing.

16. Netzwerk-Administratoren prüfen Routing-Tabellen auf Konsistenz und Redundanz.

17. Eine gute Dokumentation der Routing-Tabellen erleichtert Troubleshooting.

18. Insgesamt sind Routing-Tabellen das operative Herzstück der Weiterleitung in Netzen.