

ITS Klassenarbeit 03.05.2023

STP

F: Was ist STP und wofür wird es verwendet?

A: STP steht für Spanning Tree Protocol und wird verwendet, um Schleifen in einem Netzwerk zu vermeiden. Es ist ein Protokoll, das in Switches verwendet wird, um sicherzustellen, dass jeder Switch im Netzwerk nur eine einzige Verbindung zum Rest des Netzwerks hat.

F: Wie funktioniert STP, um Schleifen (Loops) im Netzwerk zu vermeiden?

A: STP wählt einen Switch im Netzwerk als Root-Bridge aus und erstellt dann einen Baum von Verbindungen, die den kürzesten Pfad von jedem Switch zur Root-Bridge bilden. Durch das Blockieren von gleichen Verbindungen im Netzwerk kann STP Schleifen vermeiden.

F: Wie wird die Root-Bridge bei STP bestimmt?

A: STP verwendet den Bridge ID, um den Root-Bridge im Netzwerk zu bestimmen. Der Bridge ID besteht aus einer Priorität und einer MAC-Adresse. Der Switch mit der niedrigsten Bridge-ID wird als Root-Bridge ausgewählt. Wenn zwei Switches die gleiche Priorität haben, wird der Switch mit der niedrigsten MAC-Adresse ausgewählt.

VLAN

F: Was ist ein VLAN und wofür wird es verwendet?

A: Ein VLAN ist ein logisches Netzwerk, das auf einem physischen Netzwerk basiert. Es wird verwendet, um Gruppen von Geräten in einem Netzwerk zu isolieren und zu segmentieren.

F: Wie unterscheiden sich VLANs von normalen Netzwerken?

A: In einem normalen Netzwerk werden alle Geräte im selben Netzwerksegment platziert, während in einem VLAN Geräte aus verschiedenen Segmenten zusammengefasst werden können, um ein virtuelles Netzwerk zu erstellen. VLANs funktionieren auf Layer 2 des OSI-Schichtenmodells

F: Wie können VLANs verwendet werden, um die Sicherheit im Netzwerk zu verbessern?

A: VLANs können verwendet werden, um den Datenverkehr zwischen verschiedenen Netzwerksegmenten zu trennen und zu kontrollieren, wer auf welche Netzwerkressourcen zugreifen kann. Dadurch kann die Sicherheit im Netzwerk erhöht werden.

F: Wie können VLANs die Netzwerkperformance in großen Netzwerken verbessern?

A: Global- und Unicast-Traffic wird auf einzelne VLANs beschränkt.

F: Wie viel Bit beträgt die Länge eines VLAN-Tags und hinter welcher Angabe steht er im Ethernet Frame?

A Ein VLAN-Tag ist 32 Bit lang und wird im Ethernet-Frame direkt nach der Absender-MAC-Adresse eingefügt.

F: Wie kann man auf Geräte aus einem anderen VLAN zugreifen.

A:

- Router: Ein Router kann verwendet werden, um den Datenverkehr zwischen verschiedenen VLANs weiterzuleiten. Der Router muss in der Lage sein, den Datenverkehr zwischen den VLANs zu routen und somit eine Verbindung zwischen den Netzwerken herzustellen.
 - Layer 3 Switch: Ein Layer 3 Switch ist in der Lage, den Datenverkehr zwischen verschiedenen VLANs zu routen.
-

F: Was passiert, wenn zwei unterschiedliche VLANs an einem Switch mit einem Ethernet-Kabel verbunden werden?

A: Die beiden VLAN-Segmente werden zu einem. Der Datenverkehr der beiden VLANs ist nicht mehr getrennt.

F: Nenne zwei Möglichkeiten, VLANs über mehrere Switches zu verbinden? Stellen Sie beide Möglichkeiten grafisch dar. A:

Von jedem VLAN werden jeweils ein Port von jedem Switch miteinander verbunden.



Auf jedem Switch wird ein Interface als Trunk (Tagged) konfiguriert und über VLAN Tags auf dem jeweiligen Empfänger Switch wieder an die Untagged Ports verteilt.



RIP

F: Nach welchem Kriterium priorisiert das RIP-Protokoll die Verbindungen zwischen Routern in einem Netzwerk?

A: Das RIP-Protokoll priorisiert die Verbindungen basierend auf der Anzahl der Hops, die ein Paket passieren muss, um ein Ziel ausgehend vom aktuellen Router zu erreichen. Wenn mehrere Pfade zur Verfügung stehen, wählt RIP den Pfad mit der geringsten Anzahl von Hops aus.

F: Warum ist das RIP-Protokoll nur bedingt geeignet für komplexere Netzwerke.

A: Da die Kostenmetrik nur auf der Anzahl der Hops basiert. Es ist somit nicht möglich weitere Faktoren, wie z.B Bandbreite oder Kosten der Verbindung in die Berechnung einfließen zu lassen.

NAT

F: Welche drei Varianten von NAT gibt es?

A: Statisches NAT, Dynamisches NAT, Port Address Translation (PAT)

F: Nenne **einen** Vor- und Nachteil zu **einer** der drei Varianten von NAT:

- statisch:
 - Vorteil: Die internen Geräte sind von außen erreichbar.
 - Nachteil: Für jedes Endgerät mit einer privaten Adresse wird eine öffentliche Adresse benötigt
- dynamisch:
 - Vorteil: Mehrere private Adressen können sich eine geringere Anzahl an öffentlichen IP-Adressen teilen.
 - Nachteil: Wenn der IP-Adresspool leer ist, können keine weiteren Endgeräte mit dem externen Netz kommunizieren
- PAT:
 - Vorteil: Mit einer öffentlichen IP-Adresse können theoretisch bis zu 2^{16} Endgeräte mit privaten Adressen gleichzeitig ins Internet kommunizieren.
 - Nachteil: Die internen Geräte sind von außen nicht erreichbar.

From:

<https://wiki.mqnet.de/> - mqnet - Wiki

Permanent link:

https://wiki.mqnet.de/schule/its/klassenarbeit_2023-05-03

Last update: **17.10.2025 14:18**

