Zusammenfassung: Jahr 2

Inhaltsverzeichnis

1 Lernfeld 7 - Vernetzte IT-Systeme / PUKR

1.1 Was ist das Internet?

Das Internet ist ein Netzwerk von Netzwerken. Das Internet besteht aus der Vernetzung von sogenannten Autonomen Systemen (AS). Jedes AS hat eine mit IP vergleichbare Adresse, die AS Number (ASN).

1.2 DNS - Domain Name System

1.3 IPv4 - Internet Protocol

1.3.1 Classful Subnetting

Beim classful subnetting gibt es grundsätzlich drei Netzklassen: A, B und C. Diese zeichnen sich durch ihre Subnetzmasken aus, 255.0.0.0, 255.255.0.0 und 255.255.255.0. Beim classful subnetting wird zwischen der Host-ID und der Net-ID unterschieden. Die beiden IDs lassen sich durch die Subnetzmaske aus der IP herleiten.

```
IP             192.168.23.42    1100 0000  1010 1000  0001 0111  0010 1010
Subnetzmaske   255.255.255.0    1111 1111  1111 1111  1111 1111  0000 0000
Net-ID         192.168.23.0     1100 0000  1010 1000  0001 0111  0000 0000
Host-ID        0.0.0.42         0000 0000  0000 0000  0000 0000  0010 1010
```

Listing 1: Beispiel zu Classful Networking

1.3.2 Classless Inter-Domain Routing

Im Gegensatz zum classful subnetting zeichnet sich CIDR (Classless Inter-Domain Routing) dadurch aus, dass statt drei Netzklassen, wird die Subnetzmaske in Form eines Suffix */XX* dargestellt. Das Suffix gibt dabei an, wie viele der Bits von links beginnend auf 1 gesetzt sind. Sobald die Subnetzmaske bekannt ist, lassen sich dadurch Host- und Net-ID ermitteln.

```
IP             192.168.23.42/24
Subnetzmaske   1111 1111  1111 1111  1111 1111  0000 0000
               |       |  |       |  |       |
               +-- 8 --+  +-- 8 --+  +-- 8 --+
                 255        255        255
```

Listing 2: Beispiel zu CIDR

1.4 IPv6

1.5 Transportschicht

1.6 Router und Routingprotokolle

Routingprotokolle werden dazu verwendet, um Routing-Entscheidung zu automatisieren

1.6.1 RIP und OSPF

Route Information Protocol (RIP) und Open Shortest Path First (OSPF) ermitteln beide die kürzesten Wege innerhalb eines Netzwerkes, wobei „kürzeste“ bei RIP bedeutet, dass die Anzahl der Hops möglichst gering ist und bei OSPF weitere Metriken angesetzt werden können, um die Routing-Entscheidungen zu steuern.

1.6.2 Border Gateway Protocol - BGP

Das Border Gateway Protocol wird im Internet dazu verwendet, die IP-Adressen, die ein AS anbietet, zu announcen und entsprechend Routing-Entscheidungen anhand der Announcments zu treffen.

1.7 Algorithmen

1.8 Anwendungsschicht

1.9 Netzwerksicherheit und Firewalls

1.9.1 Firewalls: Zonen

Beim Firewalling werden generell drei Zonen unterschieden. Das Intranet bzw. die Trusted Zone, die Demilitarisierte Zone (DMZ) und das Internet, auch Untrusted Zone genannt.

Trusted Zone

DMZ

Die Demilitarisierte Zone (DMZ) wird auch als „perimeter network“ bezeichnet.

Untrusted Zone

1.9.2 Firewalls: Generationen

Aktuell werden drei Generationen von Firewalls unterschieden. Zum erst sind das die klassischen stateless firewalls, zum zweiten stateful firewalls und zu letzt die application layer firewalls.

1.9.3 Firewalls: Konzepte

Einstufige Firewall:

Zweistufige Firewall: Bei einer zweistufigen Firewall wird zwischen Intranet und DMZ sowie zwischen DMZ und Internet eine Firewall plaziert. In der Praxis werden zwei Firewalls verschiedener Hersteller verwendet, damit ein Sicherheitsproblem bei einer Firewall nicht direkt das Intranet öffnet.

Mehrstufige Firewall:

2 Lernfeld 7 - Vernetzte IT-Systeme / SEIB

2.1 Grundlagen der technischen Kommunikation

2.1.1 Gründe für die Vernetzung

Aus Gründen ...

2.1.2 Das ISO/OSI-Referenzmodell

2.1.3 Netzwerktopologie

Ring, Stern, Baum, Mesh, Bus

2.1.4 Übertragungsmedien

Zu den leitergebunden Übertragungsmedien gehören Kupferkabel, Koaxialkabel und Lichtwellenleiter. Leiterungebundene Übertragungsmedien basieren beispielsweise auf Funk- oder Lasertechnologien. Zu den bekannten Funktechnologien gehören unter anderem WLan und Richtfunk. Per Richtfunk lassen sich über mehrere Kilometer Übertragungsgeschwindigkeiten von 1+ GB/s erreicht werden.

Kupferkabel werden nach einem bestimmten Schema bezeichnet, das sich auf den Aufbau des Kabels bezieht. Das Schema lautet XX/YZZ, wobei XX für **U**ngeschirmt, **S**hielded, **Foiled** und **SF** stehen kann. XX bezieht sich dabei auf das gesamte Kabel. F/YZZ heißt also, dass die vier Twisted Pairs von einer Folie umgeben sind. An der Stelle von Y kann ebenfalls U, S oder F stehen. Y bezieht sich im Gegensatz zu XX auf die einzelnen Twisted Pairs, XX/FZZ bedeutet also, dass die einzelnen Paare von einer Folie umgeben sind. Schließlich kann es sich bei ZZ um Twisted Pair (TW) oder Quad Pair (QP) handeln. Bis Cat 5e wird TP verwendet. QP wird beispielsweise bei Cat 6 Kabeln verwendet. Zusammengefasst gilt folgendes:

- XX: U, F, S, FS
- Y: U, F, S
- ZZ: TP, QP

Der ganze Aufwand wird betrieben, um den Einfluss von elektromagnetischen Feldern auf die umliegenden Kabel einzudämmen. Die Verdrillung der Adernpaare hilft ebenfalls, die elektromagnetische Wirkung zu schwächen. Da elektromagnetische Felder überall dort auftreten, wo elektrische Ströme fließen, sind Kabelschätze zumeist zweigeteilt, sodass die Stromkabel physisch von den Patchkabeln getrennt sind. Dieselben Effekte können auch in Aufzugschächten dafür sorgen, dass die Internetverbindung immer dann abbricht, wenn jemand den Aufzug benutzt.

2.2 Strukturierte Verkabelung

Strukturierte Verkabelung sollte a) zukunftssicher, b) dienstneutral und c) leichterweiterbar sein. Darin sind noch keine Redundanzen enthalten. Unter Zukunftssicherheit wird ein Zeitraum von 10 bis 15 Jahren verstanden. In der strukturierten Verkabelung werden drei Bereiche unterschieden: 1. Tertiärer Bereich, 2. Sekundär Bereich und 3. Primärer Bereich. Die Topologie der drei Bereiche entspricht einem Baum mit Stern „Blättern“. Durch Querverbindungen wird aus dem Baum ein teilvermaschtes Netz mit Redundanzen, um die Ausfallsicherheit zu erhöhen. Diese Art der Verkablung garantiert eine leichte Erweiterbarkeit des Netzes. Wenn die Umstände – was in der Realität meist der Fall ist – nur den tertiären und den sekundären Bereich vorsehen, also keine Gebäude miteinander verbunden werden müssen, wird von einem *collapsed backbone* gesprochen. Bei einem collapsed backbone ist der Router an den Gebäudeverteiler angeschlossen.

Teritärer Bereich

Im Tertiärbereich sind Kupferverkabelungen mit einer maximalen Länge von 100m vorgesehen. Die Endgeräte werden an einen Etagenverteiler (EV) angeschlossen, wodurch eine Sterntopologie entsteht.

Sekundärer Bereich

Im Sekundärbereich wird ein Verkabelung mit Kupfer bzw. Lichtwellenleitern empfohlen, wobei LWL bevorzugt werden sollten. Die maximale Länge beträgt hier 500m. Die Etagenverteiler des tertitären Bereichs werden an Gebäudeverteiler (GV) angeschlossen. Der Sekundärbereich wird von Cisco auch als Distribution Layer bezeichnet.

Primärer Bereich

Im primären Bereich werden nur noch Lichtwellenleiter empfohlen. Bevor LWL verfügbar waren, wurden Koaxialkabel genutzt. Die Gebäudeverteiler werden an die Standortverteiler (SV) angeschlossen. Dadurch entsteht schließlich eine Baumtopologie.

2.3 Hochverfügbarkeit

Hochverfügbarkeit wird über die Verfügbarkeit eines Dienstes definiert und nicht über Komponenten. Die Verfügbarkeit wird in Prozent angegeben und beträgt in der Regel 99%. Ein Beitrag zur Hochverfügbarkeit eines Dienstes ist die redundante Auslegung der Netzwerkkomponenten. Dabei ist zu beachten, dass redundant angeschlossene Komponenten zu Broadcast-Stürmen neigen, weil ARP-Request an alle aktiven Anschlüsse geschickt werden. Im Prinzip wird zur Herstellung von Redundanz ein Loop gesteckt. Dadurch, dass ARP-Requests auf mehreren Interfaces reinkommen, ist der Switching Address Table (SAT) der Switche nicht konsistent und ändert sich ständig.

2.3.1 Spanning Tree Protocol

Spanning Tree Protocol (STP) wird verwendet, um die Schleifenfreiheit von Topologien sicherzustellen. Die Wurzel des Baums ist die sogenannte Root Bridge. Welcher Switch eines redundanten Setups die aktuelle Root Bridge ist, wird durch eine Wahl festgelegt. Dies geschieht, indem alle Switches bzw. Bridges ihre Bridge-ID (kurz: BID; jede Bridge wird über eine eigene BID identifiziert) an eine bestimmte Multicast-Gruppe mitteilen. Die Bridge-ID ist 8 Byte lang (2 Byte Bridge Priority, 6 Byte MAC-Adresse). Die Bridge mit der „niedrigsten“ Priorität wird zur Root Bridge. Sollte die Bridge Priority identisch sein, wird als ergänzendes Kriterium die MAC-Adresse der Komponenten benutzt (auch hier gewinnt wieder die Bridge mit der niedrigeren Zahl).

STP wird unter anderem dazu genutzt, um Broadcast-Stürme, inkonsistente Switching Address Tables (SAT) und multiple Frames zu vermeiden. Im Gegensatz zu IP-Packeten besitzen Ethernet-Frames keine time to live, sodass Frames in einem Loop unendlich oft geswitcht werden.

Ähnlich wie bei OSPF wird bei STP über Pfadkosten ermittelt, über welchen Port er die Root Bridge erreichen kann. Der Unterschied zu OSPF besteht in erster Linie darin, dass es sich bei STP um ein Layer 2 Protokoll handelt und die Implementierung sich entsprechend unterscheidet.

STP unterscheidet zwischen Root-Ports und Designated-Ports. Dabei kann es immer nur einen Root-Port geben. Das ist der Port, der vom Switch zur Root-Bridge führt. Ein Switch kann mehrere Designated-Ports haben, bspw. sind alle Ports der Root-Bridge, die zu anderen Switchen führen, Designated-Ports.

Gibt es zwei Pfade zur Root-Bridge wird anhand von Priorität und MAC der günstigste Pfad gewählt. Der Pfad über den nicht gewählten Weg wird blockiert. Der entsprechende Pfad wird als Non-Designated-Port bezeichnet und befindet sich im Blocking State, um Loops zu verhindern.

Alternativen zu STP: Es wurden einige Alternativen zum STP vorgeschlagen und standardisiert. Dazu gehören unter anderem:

- Rapid Spanning Tree Protocol (RSTP): Die Idee von RSTP besteht darin, bei einer Änderung der Topologie nicht sofort die gesamte Netzstuktur zu löschen, sondern erst einmal wie gehabt weiter zu arbeiten und Alternativpfade berechnet werden. Erst danach wird ein neuer Baum zusammengesetzt. Die Ausfallzeit lässt sich so von 30s auf $<$1s reduzieren. Die aktuelle Spezifikation wird durch IEEE 802.1D-2004 festgelegt.
- Multiple Spanning Tree Protocol (MSTP): MSTP ist eine Erweiterung zu RSTP und ermöglicht im Zusammenhang mit VLANs verschiedene Instanzen des Spannbaums. Für VLANs können also unabhängige STP-Instanzen gebildet werden.
- Per VLAN Spanning Tree Protocol (PVSTP): PVSTP ist im Prinzip dasselbe wie MSTP, jedoch Cisco proprietär.
- Shortest Path Bridging (SPB): Um die Begrenzungen von STP zu überwinden, wurde mit IEEE 802.1aq SPB standardisiert.

Schrittweiser Aufbau des Baumes

1.
2.
3.
4.
5.
6.
7.