Modul 117 Prüfung II Zusammenfassung

Das IPERKA Modell

Vorteile der IPERKA Methode: Die Projektphasen lassen sich leicht merken, da jeder Anfangsbuchstabe für eine jeweilige Phase steht: Informieren, Planen, Entscheiden, Realisieren, Kontrollieren und Auswerten. Diese Methode fördert das methodische und strukturierte Vorgehen, da die einzelnen Tätigkeiten problemlos den entsprechenden Projektphasen zugeordnet werden können. IPERKA legt starkes Gewicht auf die Planung, erst wenn ein solides Konzept ausgearbeitet ist und man sich für die Lösungsvariante entschieden hat, sollte man mit der Realisierung beginnen. Auch die Auswertung gehört zu einer strukturierten Vorgehensweise. Am Schluss schaut man auf das Projekt zurück, wertet die Erfahrungen aus und zieht dabei Lehren für zukünftige Projekte ähnlicher Art.

Netzwerke planen:

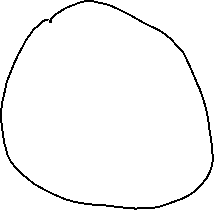
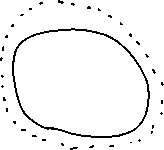
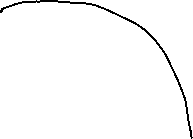
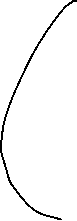
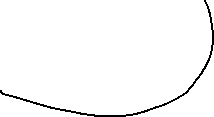
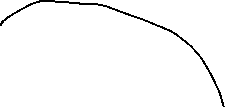
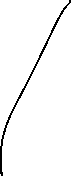
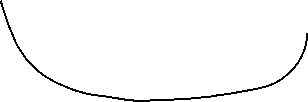
Wichtig ist es sich zuerst einen Überblick der Ausgangslage zu schaffen.

Ein Bild, das Entwurf, Text, Lineart, Zeichnung enthält.

Automatisch generierte BeschreibungSprich ein Soll und Ist Vergleich zu machen. Dies kann man beispielsweise mit einem Mindmap oder einer Tabelle machen. In dem Vergleich soll so detailliert wie möglich beschrieben sein, was aktuell vorhanden ist und was es braucht. Zudem auch andere wichtige Infos wie beispielsweise die Grösse des Raumes, wie viel Menschen in dem Raum arbeiten werden, ob ein bestimmtes Budget vorhanden ist und weitere Informationen.

Ausdehnungen der Netzwerke

Je nach Netzwerktyp gibt es unterschiedlich grosse Ausdehnungen. Gut zu merken sind diese mit folgender Darstellung.



PAN (Personal Area Network): Hat eine Ausdehnung von wenigen Metern für die Datenübertragung im unmittelbaren Umfeld einer Person. PAN ist nur für den Betrieb innerhalb eines Raums konzipiert. Anwendungsbeispiel: Verwendung von Wireless Headsets, Freisprechanlage im Auto.

LAN/WLAN (Local Area Network): Die Ausdehnung ist nur innerhalb der Grenzen (Mauern) eines Gebäudes, also <<nur>> auf die Lokalität bezogen. Grösse des Raumes spielt hierbei keine Rolle. Im LAN kommen keine öffentlichen Übertragungsdienste zum Einsatz. Anwendungsbeispiel: Vernetzen aller Arbeitsplatzrechner und Drucker mit einem zentralen Server im lokalen Gebäude.

CAN (Campus Area Network): Ausdehnung: Nur innerhalb der Grenzen eines privaten Geländes z.B. Firmengelände, Spitalkomplex… auch hier kommen nur eigene, private Kommunikationsmittel zum Einsatz. Anwendungsbeispiel: Vernetzung der verschiedenen Gebäude auf dem Firmengelände.

MAN(Metropolitan Area Network): Ein solches Netzwerk erstreckt sich über mehrere, nahe gelegene Standorte. Ausgehen vom Zentrum (Kernstadt) betrifft es Standorte, die im (direkten) Einzugsgebiet des Zentrums liegen. Für solche Netzanwendungen gibt es spezielle Übertragungsdienste. Anwendungsbeispiel: Kantonsverwaltung, Vernetzung von Filialen mit dem Hauptsitz einer regional tätigen Firma.

WAN(Wide Area Network): Ein solches Netzwerk verbindet weit entfernte Standorte, die sich aber noch immer auf dem **gleichen** Kontinent befinden. Auch hier werden spezielle Übertragungsdienste angeboten. Anwendungsbeispiel: Vernetzung eines europaweit tätigen Unternehmens.

GAN (Global Area Network): Ein solches, weltweites Netzwerk verbindet Standorte, die rund um den Globus auf verschiedenen Kontinenten verteilt sind. Bei der Verwendung von Satellitenverbindung muss die hohe Latenzzeit betrachtet werden. (Latenz von 300-400ms) Anwendungsbeispiel: Vernetzung mit den globalen Standorten eines international agierenden Konzerns.

Peer-to-Peer und Server-basierte Netzwerke

Die Betriebsart eines Netzwerkes bestimmt, wie das „Zusammenspiel“ zwischen den einzelnen Systemen und Benutzern abläuft. Obwohl sich ein Netzwerk grundsätzlich mit jeder Betriebsart einrichten lässt, spielen bei der Wahl der optimalen Betriebsart folgende Punkte eine wesentliche Rolle: Grösse des Netzwerks hinsichtlich Benutzer und Systeme, Anforderungen an das Netzwerk hinsichtlich Sicherheit. Zur Verfügung stehende Ressourcen wie finanzielle Mittel, Fachwissen, etc.

Peer-to-Peer Netzwerk

In einem Peer-to-Peer Netzwerk sind alle vorhanden Systeme/Computer „gleichberechtigt“. Es gibt daher also keine zentrale oder übergeordnete Instanz. Jeder Teilnehmer **regelt und steuert selbstständig** in Eigenverantwortung, wer auf die Ressourcen seines Systems zugreifen darf und was damit gemacht werden kann.

**Vorteile:** Lokale Ressourcen können rasch und einfach durch den jeweiligen Benutzer freigegeben werden. Spezielle Berechtigungen oder die Zustimmung eines Systemadministrators sind für diesen Zweck nicht notwendig.

**Nachteile:** Die ordnungsgemässe Inbetriebnahme und Steuerung von PtP-Funktionen setzt gewissen IT-Fachwissen voraus. Das unbedarfte Aktivieren von PtP-Funktionen kann zu schwerwiegenden Problemen hinsichtlich der Sicherheit führen.

Client-Server-Netzwerk

In einem Client-Server-Netzwerk werden bestimmte Services zentral auf einem Server betrieben und den Netzteilnehmern zur Verfügung gestellt. Durch die Zentralisierung von Diensten werden die Arbeitsstationen von diesen Aufgaben entlastet. Folgende Dienste werden oft auf dedizierten Server betrieben: Datei und Druckdienste, Gatewaydienste, Webserver.

**Vorteile:** Ermöglicht eine effiziente Verwaltung von Netzwerkbenutzern und Netzwerkdiensten, da all diese Arbeiten zentral auf einem Server ausgeführt werden können. Die Informationen und Dienste eines zentralen Netzwerkservers stehen auch anderen Programmen und Systemen zur Verfügung. **Nachteile:** Für die Benutzung eines Servers werden oft Programme benötigt, deren Lizenzen häufig ein Vielfaches, von dem einer normalen Clientlizenz kosten. Für die ordnungsgemässes Einrichtung und Konfiguration eines dedizierten Netzwerkservers wird spezielles Fachwissen vorausgesetzt.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Verschiedene Netzwerktopologien

**Ein Bild, das Kinderkunst, Zeichnung, Diagramm, Origami enthält.

Automatisch generierte Beschreibung**Die Topologie eines Netzwerks bestimmt, wie die einzelnen Systeme in einem Netzwerk miteinander verbunden sind. Bei der Wahl der Netzwerktopologie müssen genau wie bei der Ausdehnung die grundlegenden Anforderungen an das Netzwerk beachtet werden. Muss das Netzwerk besonders ausfallsicher sein? Können/dürfen nur möglichst wenig Kabel zum Bau des Netzwerks verwendet werden? Ausserdem muss man bei einer Topologie beachten, wo sich dessen SPOF (Single Point Of Failure) befindet. Der SPOF in einem Netzwerk beschreibt die Stelle, wo ein Defekt das ganze Netzwerk lahmlegen würde.

**Ein Bild, das Entwurf, Zeichnung, Diagramm enthält.

Automatisch generierte BeschreibungBustopologie**: Diese kommt bei der Vernetzung von Arbeitsplatzrechner heute nicht mehr zum Einsatz. Bei beispielsweise Roboterstrassen findet man diese Art von Vernetzung noch häufig.

An den Endwiderständen werden die kommenden elektrischen Signale kontrolliert abgeleitet.

**Vorteile:** Beim Ausfall einer Arbeitsstation bleibt die Kommunikation zwischen den anderen Arbeitsstationen aufrechterhalten, solange die Arbeitsstation keine Störsignale sendet. Zudem wird wenig Kabel benötigt. Die Stelle eines Busunterbruchs lässt sich relativ einfach lokalisieren. **Nachteile:** Der SPOF wirkt sich auf das gesamte Netzwerksegment (Bus) aus. Das Abhören von Nachrichten auf der Leitung ist sehr einfach. Zudem hat die Bustopologie eine schlechte Ausnützung der Übertragungsrate.

**Sterntopologie:** Die Sterntopologie ist heutzutage die häufigste Art, Rechnersysteme miteinander zu vernetzen. Der zentrale Punkt innerhalb einer Sterntopologie ist der „Hub“. Dieser Begriff wird schon lange nicht mehr verwendet, da der „Hub“ schon vor Jahren durch Switches abgelöst wurde. Ein Switch ist somit der zentrale Knoten in einer Sterntopologie. Zwischen jeder Arbeitsstation und dem Switch besteht eine Peer-to-Peer Verbindung.

**Vorteile:** Eine Arbeitsstation, die Störungen im Netz verursacht, kann vom Netz „getrennt“ werden. Die Ausnützung der Übertragungskapazität ist gut. Nachrichten anderer Arbeitsstationen werden nicht an alle Arbeitsstationen übertragen. **Nachteile:** Der SPOF wirkt sich auf das gesamte Netzwerksegment aus. Für den Bau einer Sterntopologie wird im Vergleich zur Bustopologie deutlich mehr Kabel verwendet.

Ein Bild, das Entwurf, Diagramm, Zeichnung, Design enthält.

Automatisch generierte Beschreibung

3

**Ringtopologie**: Ähnlich wie bei Bustopologie kommt die „reine“ Ringtopologie heute nicht mehr zum Einsatz. Beim Zusammenkoppeln mehrerer Netzwerke hingegen ist die Ringstruktur immer noch die 1. Wahl. Solche speziellen Verbindungen nennt man auch „Backbone“

Ein Bild, das Entwurf, Zeichnung, Kunst, Darstellung enthält.

Automatisch generierte BeschreibungEin Bild, das Diagramm, Reihe, Zeichnung, Muster enthält.

Automatisch generierte BeschreibungRingstruktur mit Backbone:

Zudem gibt es auch eine

Doppelte Ringstruktur.

Bei einem Unterbruch des

Operativen Ringes wird die

Datenübertragung automatisch

auf den zweiten, sprich redundanten Ring umgeschaltet. Dies ist jedoch nur möglich, wenn an die Station ein DAS- Adapter angebunden ist.

**Vorteile:** Mithilfe der Doppelring Struktur kann bereits auf der Kabelebene, ein fehlertolerantes Übertragungsnetz aufgebaut werden. **Nachteile**: Der SPOF bei einer „reinen“ Ringstruktur wirkt sich auf das gesamte Netzwerksegment aus:

Ein Bild, das Text, Diagramm, Kreis, Entwurf enthält.

Automatisch generierte Beschreibung

**Baumtopologie:** Baumtopologien sind ein „Relikt der Grossrechnerwelt“. Physisch werden solche Netze heute nicht mehr gebaut. Die Baumtopologie repräsentiert eine rein hierarchische Struktur. Alles wird über die höchste Instanz abgewickelt. Peer-to-Peer ist nicht möglich bzw. müsste vom Zentralrechner freigegeben sein. Vorsorgemassnahmen gegen einen eventuellen Unterbruch im Netzwerk muss bei Planung gut beachtet werden.

Ein Bild, das Entwurf, Zeichnung, Lineart, Diagramm enthält.

Automatisch generierte Beschreibung**Vorteile:** Mittels Baum-bzw. hierarchischer Struktur sehr standardisierte Netz -und/ oder Systemstruktur realisieren. Solche Systeme lassen sich kostengünstiger betreiben und überwachen beispielsweise als Client-Server-System. **Nachteile:** Der SPOF wirkt sich auf den gesamten Baum aus, wenn der Fehler direkt die Anbindung zum Zentralrechner betrifft. Bei Defekt eines Concentrator kommt es nur zum partiellen Ausfall des Baums bzw. eines „Zweigs“

**Maschentopologie:** In einer Maschentopologie können eine oder mehrere Verbindungen ausfallen, ohne dass die Verbindung abbricht. Bei dieser Architektur ist also kein SPOF verbinden! Es gibt eine einfache und eine vollvermaschte Struktur. Vorteile: Eine solche Struktur besitzt keinen SPOF. Es können mehrere Verbindungen zwischen den Routern ausfallen ohne, dass die Datenübertragung vollständig abbricht.

Nachteile: Die Bestimmung des Übertragungswegs bzw. einer Route benötigt eine gewisse Zeit sowie Rechnerleistung. Aufgrund der Komplexität des Netzes ist die Fehlersuche aufwendiger und komplizierter als bei anderen Topologien.

Ein Bild, das Entwurf, Zeichnung, Diagramm, technische Zeichnung enthält.

Automatisch generierte Beschreibung

IP-Adressen

Datennetze arbeiten nach dem Prinzip der Paketvermittlung, das heisst jedes Datenpaket muss über Adressinformationen verfügen, damit es zum gewünschten Empfänger gesendet werden kann. Dabei gibt es die MAC Adresse also die physische Adresse und die IP Adresse ist die sogenannte logische Adresse. Die MAC Adresse besteht aus 6 Byte. Die ersten drei Byte kennzeichnen den Hersteller und die letzten 3 Byte die einzelne Karte.

Ein Bild, das Text, Screenshot, Schrift, Reihe enthält.

Automatisch generierte Beschreibung

**Aufbau und Struktur:** Bei jeder IP-Adresse werden zwei Bestandteile unterschieden:

Der Netzwerkanteil, auch Net-ID genannt, Der Rechneranteil, auch Host-ID genannt. Man kann die Net-ID und Host ID mit einer Telefonnummer vergleichen, die Net-ID ist an der Netzmaske erkennbar. Man unterscheidet zudem zwischen IPv4 und IPv6 Adressen. IPv6 Adressen ist der neuere Standard, er bietet mehr Anzahl Möglichkeiten von IP-Adressen. IPv6 wurde gemacht, da es global immer mehr Geräte gibt. IPv4 besteht aus 32 Bit (4,29 Milliarden Adressen) IPv6 hingegen besteht aus 128 Bit

**Subnetze:** Wenn man das Netz in mehrere kleineren Netze aufteilt, wird dies, Subnetting genannt. Vorteile des Subnetting sind, dass sie Datenpakete direkt miteinander ausgetauscht werden, was die Netzlast reduziert. Der Systemadministrator behält zudem einen guten Überblick über die einzelnen Hosts und die Sicherheit ist erhöht sich, da die Netze voneinander getrennt sind. **Die Subnetzmaske** zeigt uns zudem die Grenze zwischen dem Netzwerkanteil und dem Rechneranteil. Der Name kommt daher, da die Subnetz Maske einen teil maskiert, abdeckt. Sie deckt nämlich den Teil ab, welcher den Netzwerkanteil (Net-ID) darstellt. Mit Hilfe der Subnetzmaske kann ein Rechner feststellen, ob sich die IP-Adresse des Zielrechners im eigenen Subnetz befindet oder, ob sich das Zielsystem in einem anderen, fremden Netzwerk befindet.

**ARP Protokoll**: Das ARP-Protokoll (Address Resolution Protocol)

verbindet die MAC und die IP-Adresse.

ARP ist die „Übersetzung“ von IP in MAC-Adresse. ARP funktioniert über ARP Request und ARP Replay.

Port dient zur Erkennung der Anwendung.

Adressierungen: Physikalische Adressierungen sind die Adressinformationen

Fest mit einer Netzwerkschnittstelle verknüpft und ist in allen Netzen einzigartig. In der Praxis bedeutet dies, dass jede Netzwerkkarte oder sonstige Netzwerkschnittstelle eine eindeutige, physikalische Adresse besitzt, die sogenannte **MAC-Adresse.** Diese muss nicht vom Administrator vergeben werden. Logische Adressierung: Der Unterschied gegenüber der physikalischen Adressierung ist, dass die logische Adresse einer Netzwerkschnittstelle vom Administrator vergeben wird und diese Adresse nicht zwingend einzigartig in allen Netzen sein muss. Die gebräuchlichste logische Adressierung ist die **IP-Adresse.**

TCP/IP Protokoll:

TCP/IP ist ein Datenübertragungsprotokoll, das im Internet verwendet wird, damit Computer und andere Geräte Daten senden und empfangen können. TCP/IP steht für „Transmission Control Protocol/Internet Protocol“ und ermöglicht es mit dem Internet verbundenen Geräten, über Netzwerke miteinander zu kommunizieren.

Der Netzwerkanteil, auch Net-ID genannt, Der Rechneranteil, auch Host-ID genannt. Man kann die Net-ID und Host ID mit einer Telefonnummer vergleichen, die Net-ID ist an der Netzmaske erkennbar. Man unterscheidet zudem zwischen IPv4 und IPv6 Adressen. IPv6 Adressen ist der neuere Standard, er bietet mehr Anzahl Möglichkeiten von IP-Adressen. IPv6 wurde gemacht, da es global immer mehr Geräte gibt. IPv4 besteht aus 32 Bit (4,29 Milliarden Adressen) IPv6 hingegen besteht aus 128 Bit

**Subnetze:** Wenn man das Netz in mehrere kleineren Netze aufteilt, wird dies, Subnetting genannt. Vorteile des Subnetting sind, dass sie Datenpakete direkt miteinander ausgetauscht werden, was die Netzlast reduziert. Der Systemadministrator behält zudem einen guten Überblick über die einzelnen Hosts und die Sicherheit ist erhöht sich, da die Netze voneinander getrennt sind. **Die Subnetzmaske** zeigt uns zudem die Grenze zwischen dem Netzwerkanteil und dem Rechneranteil. Der Name kommt daher, da die Subnetz Maske einen Teil maskiert, abdeckt. Sie deckt nämlich den Teil ab, welcher den Netzwerkanteil (Net-ID) darstellt. Mit Hilfe der Subnetzmaske kann ein Rechner feststellen, ob sich die IP-Adresse des Zielrechners im eigenen Subnetz befindet oder, ob sich das Zielsystem in einem anderen, fremden Netzwerk befindet.

IP-Adressbereiche

1994 wurden die privaten Adressbereiche eingeführt, mittels privater IP-Adressen will man verhindern, dass Privatpersonen oder Firmen für ihre privaten Netzwerke sogenannte öffentliche Netzwerke benutzen. Vor der Einführung der privaten IP-Adressen waren alle vorhandenen IP-Adressen öffentlicher Natur. Eine öffentliche IP-Adresse darf weltweit nur 1-mal vergeben werden, private IP-Adressen dürfen mehrfach vorhanden sein, da diese Adressen nur in einem privaten Netzwerk verwendet werden können. Jeder darf so viele private IP-Adressen verwenden, wie er will, da dieser „private Adressraum“ im Grunde unerschöpflich ist. Dies Aufgrund der Tatsache, dass ein Router zwischen einem privaten und öffentlichen Netzwerk alle Datenpakete mit privaten IP-Adressen in Richtung öffentliches Netz blockiert.

Ein Bild, das Text, Screenshot, Schrift, Zahl enthält.

Automatisch generierte Beschreibung

Aufbau und Unterschiede verschiedener Kabeltypen

Ein Bild, das Text, Diagramm, Werkzeug, Screenshot enthält.

Automatisch generierte Beschreibung

Der mit Abstand meistverwendete Kabeltyp für LAN ist Twistd Pair. Bei diesem Kabeltyp gibt es die beiden Varianten shielded oder unshielded.

Ein Bild, das Text, Screenshot, Diagramm, Schrift enthält.

Automatisch generierte BeschreibungSteckverbinder:

Zugriffsverfahren CSMA/CD

Ein Bild, das Text, Schrift, Screenshot, Dokument enthält.

Automatisch generierte Beschreibung

OSI-Schichtmodell

Kommunikation zwischen Computern weltweit funktioniert untereinander dank OSI-Schichtmodell

Ein Bild, das Text, Schrift, Quittung, Handschrift enthält.

Automatisch generierte Beschreibung