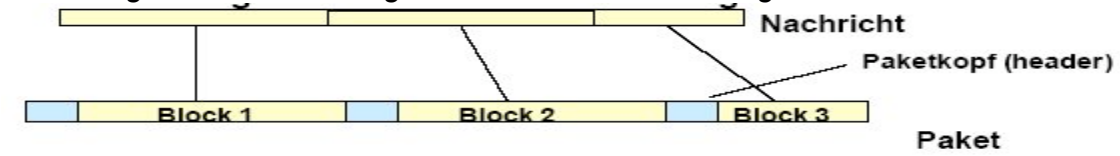
Fragenkatalog RN2 SS2004

1.) Was verstehen Sie unter „Best Effort“-Dienst?

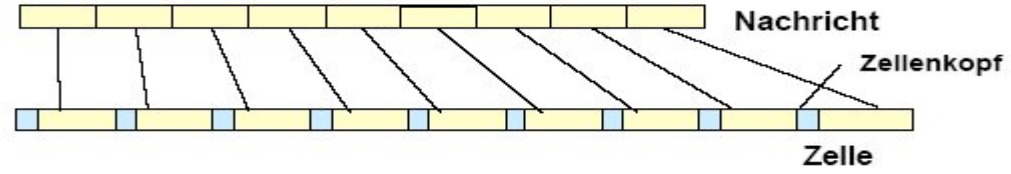
Bietet das Internet derzeit dh. einen Dienst ohne Zugangskontrollfunktion, ohne Bandbreitenreservierung und ohne Garantie von Quality of Service
Also keine Garantie für:
→ Auslieferung eines Pakets
→ Korrekte Reihenfolge
→ Praktisch keine Echtzeit

2.) Worin unterscheidet sich die Aufteilung der Gesamtinformation in Zellen bzw. Pakete?

Aufteilung in Paketen: erfolgt in unterschiedlicher Länge



Aufteilung in Zellen: erfolgt in konstanter Länge



3.) Nennen Sie Beispiele für drahtgebundene LANs.

- Ethernet
- Fast Ethernet
- Gigabit Ethernet
- Token Ring
- Token Bus
- FDDI

4.) Welche Ethernet Varianten kennen Sie (inkl. Logischer und physischer Topologie, z.B. 10Base2, 10Base5, …)?

Ethernet-Varianten (1)
• Bustopologie
– Broadcast der Nachrichten
– Einer sendet, alle empfangen
– Nur ein Teilnehmer pro Zeitpunkt kann senden
• Mit Hub
– Physisch Sterntopologie, logisch Bustopologie
– Einer Sendet zum Hub, Hub sendet an alle andere
– Hub = Multiport-Repeater
• Mit Switch
– Sterntopologie logisch und physisch
– Kein shared medium!!

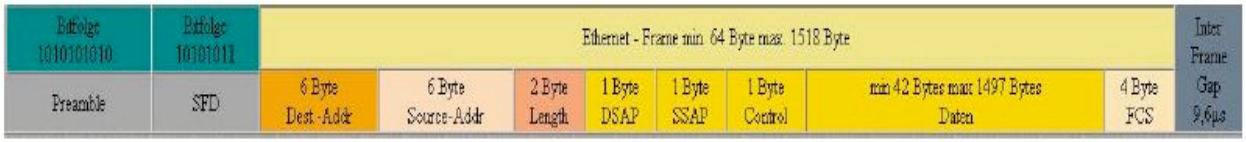
– Jeder Teilnehmer hat sein eigenen Anschluss (dedicated medium)
– Für die Dauer der Kommunikation, direkte Verbindung von A nach B mittels Switch

– 10BASE5 = Basisband-Übertragung mit 10 Mbit/s und 500 m Segmentlänge
– 10BASE-T = Basisband-Übertragung mit 10 Mbit/s über verdrillte Zweidrahtleitung
– 10BROAD36 = Breitband-Übertragung mit 10 Mbit/s über 3600 m

5.) Nennen Sie einige Felder, die im Ethernet Rahmenformat enthalten sind.

Preamble	7 bytes
Start-of-frame delimiter (SFD)	1 byte
Destination MAC address	2 oder 6 bytes
Source MAC address	2 oder 6 bytes
Lenght indicator	2 bytes
Data Padding (optional)	Bis 1550 bytes
Frame check sequence (FCS)	4 bytes

6.) Skizzieren Sie einen Ethernet (oder 802.3) –Rahmen?
siehe folie 69



7.) Vergleichen Sie IPv4 mit IPv6, MAC und IPX Adressen.

IPv4: Adresslänge = 32 bit dh 2^32 IP Adressen
IPv6: Adresslänge = 128 bit 2^128 IP Adressen
MAC: Adresslänge = 48 bit 2^48 Mac Adressen
IPX: Adresslänge = 80 bit 2^80 IP Adressen

8.) Welche IPv4 Adressklassen kennen Sie?

- Klasse A: Netze mit einer riesigen Anzahl an Hosts Erkennung: 1-126
- Klasse B: Netze mit einer großen Anzahl an Hosts
- Klasse C: Netze mit einer kleinen Anzahl an Hosts
- Klasse D: Multicast Gruppen
- Klasse E: Reserviert

9.) Was ist eine Late-Collision?

Falls die maximale Ausdehnung des Netzes zu groß ist oder über Repeater/Hubs zu viele Netzsegmente gekoppelt wurden, kann es zu einer nicht erkannten Kollision

kommen. Solche Kollisionen nennt man Late Collisions, diese können nur von höheren Protokollebenen (z.B. Schicht 4 eines verbindungsorientierten Protokolls) erkannt und korrigiert werden.

10.) Aus welchen Teilen besteht eine IPv4-Adresse?

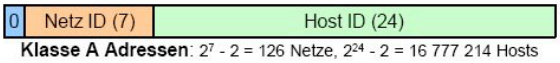
- **Vers** (Version): Kennzeichen der Protokoll-Version; stellt sicher, dass gleiche Protokollversionen zusammenarbeiten
- **IHL** (Internet Header Length): gibt die gesamte Länge des IP-Headers an Die Normallänge ohne IP-Optionen ist 5*32 Bit.
- **Servicetyp** (TOS)
- **Gesamtlänge**
- **Identifikation**
- **Flags**

11.) In welcher Weise hängt die Aufspaltung der IPv4 Adressen in Netz- und Host-Anteil mit der jeweiligen Adressklasse zusammen?

Folie 88
Klasse A: 8 bit Netz ID, 24 bit Host ID
Klasse B: 16 bit Netz ID, 16 bit Host ID
Klasse C: 24 bit Netz ID, 8 bit Host ID

12.) Erklären Sie Klasse A Adressen (Bitmuster, etc.).

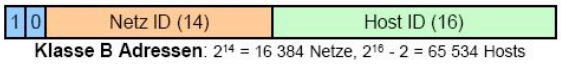
Netzadresse: 1+7 Bits (erstes Bit “0”)
Hostadresse: 24 Bits



Klasse A Adressen 2^7 - 2 = 126 Netze, 2^24 – 2 = 16 777 214 Hosts

13.) Erklären Sie Klasse B Adressen (Bitmuster, etc.).

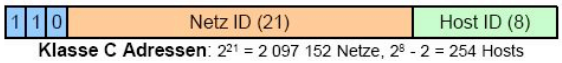
Netzadresse: 2+14 Bits (ersten Bits “10”)
Hostadresse: 16 Bits



Klasse B Adressen 2^14 = 16 384 Netze, 2^16 – 2 = 65 534 Hosts

14.) Erklären Sie Klasse C Adressen (Bitmuster, etc.).

Netzadresse: 3+21 Bits (ersten Bits “110”)
Hostadresse: 8 Bits



Klasse C Adressen 2^21 = 2 097 152 Netze, 2^8 – 2 = 254 Hosts

15.) Was ist ein Socket?

Die Kombination von IP- und Port-Nummer nennt man Socket, ein Socket identifiziert einen Kommunikationsendpunkt eindeutig. Der Socket Beispiel: "128.130.76.7:80"
Wichtige Portnummern:
13 NTP Network Time Protocol
20 FTP File Transfer Protocol -Daten

21 FTP File Transfer Protocol - Kontrolldaten
25 SMTP Simple Mail Transfer Protocol
53 DNS Domain Name Server
80 HTTP Hyper Text Transfer Protocol
119 NNTP Network News Transfer Protocol

16.) Was sind private IP-Adressen (Welche Klassen?)?
Die folgenden Bereiche sind für die private Adressierung verfügbar:
10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

17.) Was sind Loopback-Adressen?
127er IP Adressen
Noch bevor Pakete ins Netz gesendet werden, wird auf Adresse 127. ein Loopback (Schleife) erzeugt, dadurch kann man über IP auf lokale Anwendungen zugreifen

18.) Wie bestimmt man die Broadcast-IP-Adresse im Netz?
Alle bits des Hostanteils bei IP Adressen auf 1 setzen

19.) Wozu dienen Subnetze?

Netzanteil	Hostanteil

Nach außen sichtbare IP-Adressen

Netzanteil	Subnetzanteil	Hostanteil

Interne Strukturierung der IP-Adressen

Die Wahl der Subnetzmaske hängt im Prinzip von der Anzahl der gewünschten Subnetze und/oder der maximalen Anzahl pro Hosts in einer Domaine ab.
Beispiel: Klasse B Netz 129.170.x.x, Es sollen 60 Subnetze (z.B. Institute an einer Universität) errichtet werden. Welche Subnetzmaske soll gewählt werden? Wieviele Hosts können sich maximal in einem Subnet befinden?
Lösung: Subnetzmaske 255.255.252.0, 1022 Hosts pro Subnetz

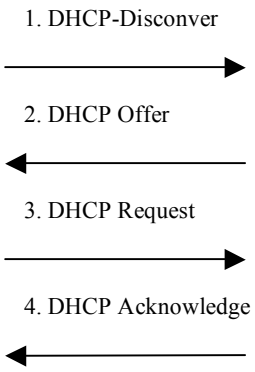
20.) Einfache Beispiele zur Bestimmung der Subnetzmaske.
wies halt kommt so kommts

21.) In welcher Weise können IP-Adressen vergeben werden?
• *Manuelle Adressvergabe:* Hier wird dem Client vom DHCP Server eine Adresse zugeteilt, welche vorher vom Netzadministrator festgelegt wurde
• *Permanente (oder auch automatische) Adressvergabe*: Hier erhält der Client eine Adresse aus einem bestimmten Bereich, diese aber für

unbegrenzte Zeit
• *Dynamische Adressvergabe:* Hier erhält der Client eine Adresse aus einem bestimmten Bereich für eine begrenzte Zeit (sg. Lease Time)

22.) Welche Möglichkeiten zur dynamischen Adressvergabe kennen Sie?
In IP basierten Netzen ist es zunehmend üblich, IP Adressen dynamisch von einem zentralen Server an Clients im Netz zu vergeben. Hierfür wurde zunächst das Protokoll BOOTP entwickelt, darauf aufsetzend wurde später das DHCP (Dynamic Host Configuration Protocol, RFC 1531) standardisiert.
Im Gegensatz zu BOOTP kann bei DHCP ein Host eine IP-Adresse schnell und dynamisch ermitteln. Für DHCP ist lediglich ein festgelegter Bereich von IP-Adressen auf einem DHCP-Server erforderlich. Sobald Hosts eine Online-Verbindung aufbauen, treten sie in Kontakt mit dem DHCP-Server und fordern eine Adresse an. Der DHCP-Server wählt eine Adresse und weist sie diesem Host zu.

23.) Was macht DHCP?
Mittels DHCP kann die gesamte Konfiguration des Computers in einer einzigen Message ermittelt werden (beispielsweise kann der Server gemeinsam mit der IP-Adresse auch eine Subnetzmaske senden). DHCP unterstützt dabei drei verschiedene



24.) Nennen Sie einige Felder im IPv4 Rahmen.
Folie 99, z.B. Nur aufzählen: IP Adressen, Time to Live, Version, Flags, Protocol

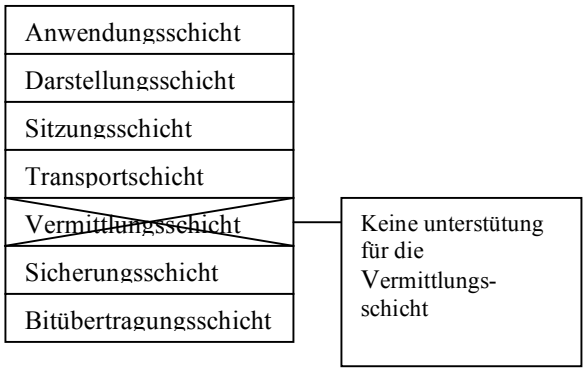
25.) Was ist das Domain Name Service?
Bei einer Domäne handelt es sich um eine Gruppe von Computern, welche nach ihrem geographischen Standort oder nach ihrem Verwendungszweck logisch zusammengefasst sind. Ein Domänenname besteht aus einer Folge von Buchstaben und/oder Ziffern, üblicherweise einem Namen oder einer Abkürzung, die anstelle der numerischen IP-Adresse einer Internet-Site verwendet wird. Durch die Verwendung von Domänen im Internet wird das Problem der Adressierung gelöst.

DNS weist Namen IP-Nummern zu verteilte Datenbanken auf verschiedenen über Internet zugänglichen Servern hierarchisch geordneter Namensraum (Bsp. www.gte.tuwien.ac.at =maxwell.tuwien.ac.at = 128.130.76.7). Zusätzlich sind die

Domänen auch bei E-Mail-Adressen von zentraler Bedeutung. Im Internet gibt es mehr als 200 Domänen auf der obersten Ebene (sogenannte Top-Level Domains). Dazu gehören beispielsweise folgende:

- .us - USA
- .de - Deutschland
- .at – Österreich

26.) Nennen Sie Beispiele routbare bzw. nicht routbare Protokolle. Worin unterscheiden sich routbare von nicht routbaren Protokollen.



IPX/SPX, AppleTalk unterstützen die Schicht 3 und sind daher "routbar„

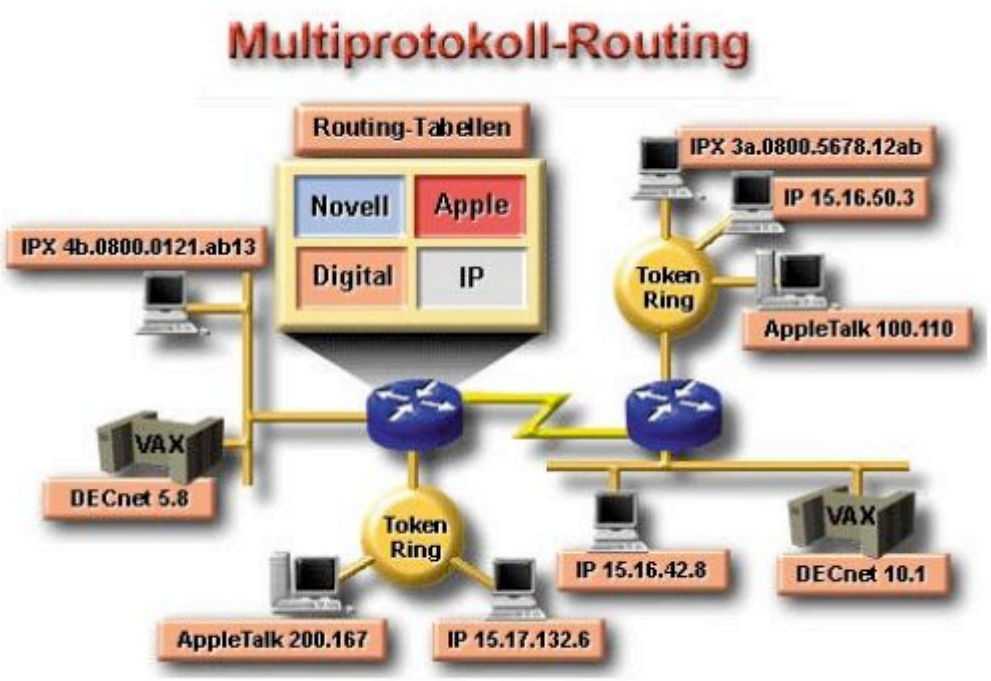
Nichtroutbare Protokolle: Protokolle, welche die Schicht 3 nicht unterstützen, z.B. NetBEUI. NetBEUI ist ein kleines, schnelles und effizientes Protokoll, das für die Anwendung auf nur einem Netzsegment gedacht ist.

Routbare Protokolle: TCP/IP,

Eigenschaften routbarer Protokolle

Damit ein Protokoll routbar ist, muss es in der Lage sein, jedem einzelnen Gerät eine Netznummer und eine Host-Nummer zuzuweisen. Für einige Protokolle, wie beispielsweise IPX, ist nur die Zuweisung einer Netznummer erforderlich. Bei anderen Protokollen, wie beispielsweise IP, ist es erforderlich, dass Sie eine vollständige Adresse und eine Subnetzmaske angeben. Die Netzadresse wird durch eine AND-Verknüpfung der Adresse mit der Subnetmaske ermittelt.

27.) Was verstehen Sie unter „Multiprotokoll-Routing“?



Router leiten den Verkehr aus allen gerouteten Protokollen über das Internetwork

28.) Was ist NetBEUI?

NetBEUI (Network Basic Extended User Interface) ist ein Protokoll der Transportschicht (Schicht 4)- Name NetBIOS Extended User Interface. Es harmoniert sehr mit alten DOS-Systemen, benötigt nur sehr wenig Speicher und ist schnell in der Ausführung. NetBEUI kann nicht geroutet werden, die Verwendung ist somit auf kleine LANs beschränkt. Der Vorteil dieses Protokolls von Microsoft ist allerdings, daß es ziemlich einfach zu konfigurieren ist und mit sehr wenig Overhead arbeitet. Jeder Computer bekommt irgend einen willkürlichen Namen, zum Beispiel „FEUTL", „ZINK" oder „ICS". Diese Namen werden intern automatisch den in den Netz-Karten fix vergebenen MAC-Adressen zugeordnet. Anhand des NetBEUINamens nicht erkennbar ist, in welchem Netz sich der Rechner befindet.
Für NetBEUI spricht allerdings ein Sicherheits-Aspekt: wird eine Internet-Verbindung hergestellt wird, könnte im Prinzip jeder irgendwo im Web befindlicher Rechner auf die Ressourcen des lokalen Netzes zugreifen, wenn dieses wie das Internet das TCP/IP-Protokoll benutzt (Ausnahme Firewall). Eine einfache und zuverlässige Lösung, dies definitiv zu verhindern, ist die Benutzung eines anderen Protokolls als TCP/IP im lokalen Netz- eben NetBEUI. Wenn in der Router- oder DFÜ-Konfiguration NetBEUI nicht ausdrücklich freigegeben ist, haben andere Rechner im Internet keine Möglichkeit, auf das lokale Netz zuzugreifen. NetBEUI ist ein Standardprotokoll zwischen PCs, das von einigen Betriebssystemen verwendet wird um Point-to-Point-LANS aufzubauen. Dieses Protokoll sollte nur verwendet werden wenn wenige PCs miteinander vernetzt werden sollen, da der administrative Aufwand erheblich ist. Denn jeder PC im Netz muss individuell konfiguriert werden bezüglich Zugriffsrechten und Diensten, die der Server zur Verfügung stellt. Domain Name Service (DNS) wie sie z.B. unter TCP/IP untestützt werden stehen nicht zur Verfügung. Windows for Workgroups, Windows9x und Windows NT verwenden NetBEUI als Protokoll. In grösseren Netzen sollte jedoch

TCP/IP verendet werden, das ebenfalls standardmässig von Windows unterstützt wird. Hier ist der Verwaltungsaufwand geringer, wenn Internetanwendungen (EMail, Webbrowser, etc.) eingesetzt werden sollen ist TCP/IP zwingend erforderlich.

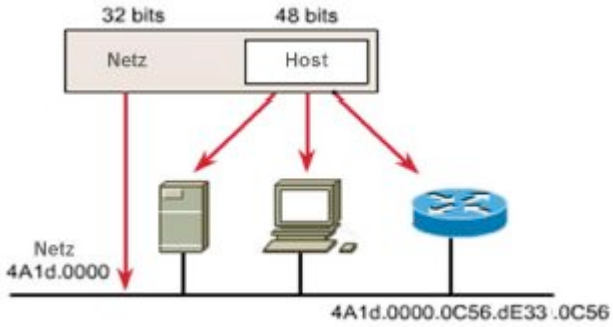
29.) Was ist NetBIOS?

NetBIOS stellt eine Standardschnittstelle für LAN-Karten bereit und ermöglicht so die Einrichtung von Peer-to-Peer- Verbindungen zwischen Rechnern. NetBIOS ist ein von IBM entwickeltes Protokoll für die Peer-to-Peer-Kommunikation zwischen PCs. Die NetBIOS-Schnittstelle ist für die meisten Betriebssysteme verfügbar. Der LAN-Manager und die Microsoft Networks-Systeme (MSNET) verwenden NetBIOS. NetBIOS ist auch für Novell NetWare verfügbar. NetBIOS kann außerdem bei vielen anderen Netzen (XNS, TCP/IP,IPX und X.25) verwendet werden.
NetBIOS ist, wie gesagt, eine Schnittstelle, die u. a. von IBM für das ursprüngliche IBM-PC-Netz entwickelt wurde. Es ermöglicht die Kommunikation zwischen Anwendungsprogrammen und den zugrundeliegenden Netzprotokollen sowie derHardware. NetBIOS kann somit als eine Schnittstelle für den Zugriff auf Ressourcen in einer LANStruktur (Hardware und Netz-Protokolle) angesehen werden, ohne deren herstellerspezifische Besonderheiten. Insofern ist es dem BIOS in der Architektur von PCs äquivalent. Eine der wichtigsten Unterschiede zwischen den Funktionen des BIOS und des NetBIOS besteht darin, daß NetBIOS-Funktionen Verbindung mit den Netzgeräten aufnehmen müssen, bevor sie Informationen von ihnen lesen oder auf sie schreiben können. NetBIOS ermöglicht das Öffnen und Schließen von Verbindungen sowie das Lesen und Schreiben von Daten.
NetBIOS kann nicht geroutet werden, da es keine Verbindungsschicht hat, auf dem ein Router aufsetzen könnte.Über NetBIOS liegt die Kommunikationssteuerungsschicht. Diese Schicht entspricht einem Netzbetriebssystem (Network Operating System, kurz NOS), sie verwaltet den Zugriff auf die Ressourcen im Netz - ebenso wie ein lokales Betriebssystem. Zwischen der Kommunikationssteuerungsschicht und Betriebssystem liegt eine weitere Schicht namens Redirektionsschicht (Redirector), die entscheidet, ob Ressourcen lokale Ressourcen oder Netzressourcen sind. Sie isoliert Anwendungen von der Netzhardware und der lokalen Hardware, sodaß die Anwendungen theoretisch nicht feststellen können, ob Daten auf einem Rechner im Netz oder auf der lokalen Festplatte gespeichert sind.
In Geräten, die gleichzeitig als Server fungieren, fängt diese Schicht Anforderungen von Remote-Client-Rechnern ab und leitet sie an die lokale Hardware um, ohne daß die lokale Anwendung des Servers davon Kenntnis erlangen würde. Dieses Konzept des virtuellen Laufwerks ermöglichte die Transparenz, die dem Arbeiten in LANs heutzutage zu eigen ist. Man kann mit einem virtuellen Laufwerk ebenso wie mit einem lokalen Laufwerk arbeiten; es befindet sich jedoch in einem Remote-Rechner und wird möglicherweise von vielen Benutzern gleichzeitig verwendet.

30.) Wie sind IPX-Adressen aufgebaut, wie werden sie angegeben?

Novell IPX ist eine eigene Paket von Protokollen, nämlich:
• Ein verbindungsloses Protokoll der Schicht 3, das keine Paketbestätigung erfordert
• Schicht 3 Adressen mit 80 Bits, die das Netz und den Host spezifiziert
• Die ersten 32 Bit beschreiben das Netz (genauso viele Möglichkeiten wie IPv4-Adressen)
• Die Host-ID entspricht der MAC-Adresse, diese sollte weltweit eindeutig sein

IPX-Adressen



31.) Welche Protokolle werden für serielle Übertragung (Analog-Modem, ISDN) verwendet?

SLIP ist eine Abkürzung für „Serial Line Internet Protocol“. Normalerweise wird das IP-Protokoll für Ethernetverbindungen verwendet. Da es vom Sinne der Leitungsausnutzung her ökonomischer ist nur während der Datenübertragung die Leitung zu belegen und sie ansonsten wieder freizugeben wurde das SLIP-Protokoll entwickelt. Nur wenn Daten übertragen werden sollen werden diese in Pakete aufgeteilt, adressiert und verschickt. Während der verbleibenden Zeit wird der Kanal nicht benutzt und kann daher quasi gleichzeitig von mehreren Benutzern verwendet werden.
Da man allerdings bei einer seriellen Leitung, z.B. einer Modemleitung oder ISDN diese nur für sich alleine besitzt, besteht nun die Möglichkeit mit dem IP-Protokoll gleichzeitig mehrere Sitzungen zu führen. Wenn man also eine SLIP-Verbindung zum Host besteht, kann man gleichzeitig mehrere Telnet-Sessions mit unterschiedlichen Rechnern aufbauen.

32.) Was verstehen Sie unter Routing? Welche Ziele sollen mit Hilfe des Routing realisiert werden?

Umfasst die Entscheidung, auf welcher Anschlussleitung bzw. zu welchem Nachbarknoten ein eintreffendes Paket an einem Vermittlungsknoten weitergeleitet werden soll, d.h. welcher Weg (Pfad) zwischen Quell- und Zielknoten zu verwenden ist.
→ Vermittlung eines Pakets von einem Eingangsport zu einem Ausgangsport.

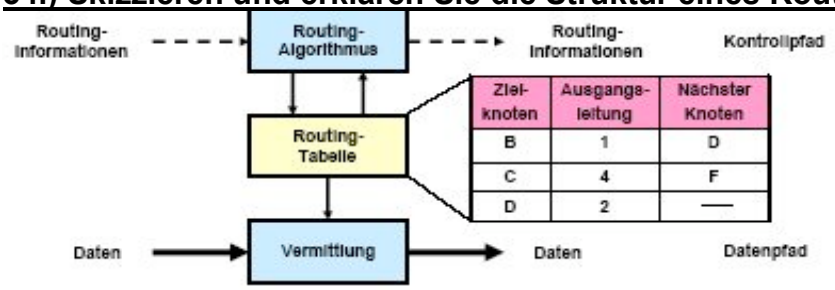
Ziele

Bereitstellung möglichst ,,kurzer‘‘ Wege zwischen Quellknoten und Zielknoten
• Gleichmäßige Netzbelastung
• Maximierung des Netzdurchsatzes
• Minimierung der Paketverzögerungen

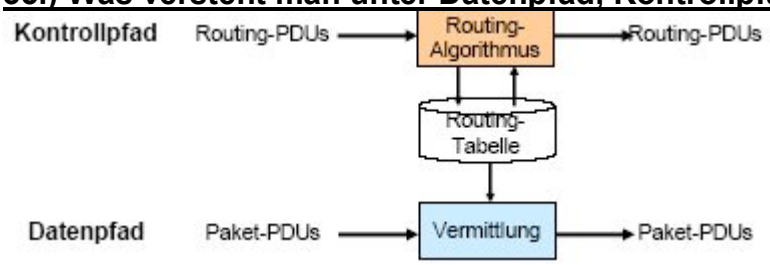
33.) Was verstehen Sie unter Routing-Algorithmus und Routing-Protokoll?

Routing-Algorithmus: umfasst den logischen Berechnungs- prozeß zur Bestimmung des Weges im Netz.
Routing-Protokoll: regelt basierend auf einem Algorithmus zur Wegeauswahl zusätzlich den Austausch bzw. die Verteilung der benötigten Routing-Informationen im Netz, und zwar:
-zwischen zentralem Knoten und übrigen Vermittlungsknoten (zentrales Routing)
-zwischen den einzelnen Vermittlungsknoten (verteiltes Routing)

34.) Skizzieren und erklären Sie die Struktur eines Routers.



35.) Was versteht man unter Datenpfad, Kontrollpfad sowie Routing-Tabelle?



Datenpfad: Vermittlung der Daten (auf der Vermittlungsschicht).
Kontrollpfad: Steuerung der Vermittlung nach Maßgabe des Routing-Algorithmus‘.
Routing-Tabelle: Enthält Routing-Informationen, die für die Vermittlung relevant sind.

Im Detail:
Kontrollpfad: Steuert das Routen der Datenpakete durch das Netz, ist aber nicht direkt im Routing-Prozess involviert. Die Routingprotokolle sind dabei oberhalb der 3. Schicht des OSI-Modells angesiedelt. Die Aktualisierung der Routingtabelle geschieht mittels eines Algorithmus, die Routingtabelle enthält Routinginformation, die das Weiterleiten der Pakete ermöglicht
Datenpfad: Wegewahl der Daten (Routing) wird anhand der Routinginformation in der Routingtabelle durchgeführt- Vermittlung der Pakete auf 3. Schicht des OSI-Modells (Vermittlungsschicht).

36.) Was ist der Unterschied zwischen gerouteten-Protokollen und Routing-Protokollen?

- Geroutete Protokolle sind Netzprotokolle, die in ihrer Vermittlungsschichtadresse genügend Informationen zum Weiterleiten eines Pakets von einem Host zu einem anderen Host auf der Basis des Adressierungsschemas bereitstellen. Das Internet-Protokoll (IP) ist ein Beispiel für ein geroutetes Protokoll.
- Routing-Protokolle unterstützen geroutete Protokolle, indem sie Mechanismen für die gemeinsame Nutzung von Routing-Informationen bereitstellen. Routing-Protokollnachrichten bewegen sich zwischen Routern. Mithilfe eines Routing-Protokolls können die Router mit anderen Routern kommunizieren, um Tabellen zu aktualisieren und zu verwalten. Zu den TCP/IP-Beispielen für Routing-Protokolle zählen:

o RIP (Routing Information Protocol)
o IGRP (Interior Gateway Routing Protocol)
o EIGRP (Enhanced Interior Gateway Routing Protocol)

o OSPF (Open Shortest Path First)

37.) Nennen Sie Qualitätsmaße des Routing.

• IT Bandbreite: Datenkapazität einer Verbindung
• Verzögerungszeit: benötigte Zeit, um ein Paket über eine Verbindung von der Quelle zum Ziel zu übertragen
• Auslastung einer Netzressource (z.B. Router oder Verbindung)
• Zuverlässigkeit: Fehlerrate einer Verbindung
• Zahl der Hops: die Anzahl der Router, die ein Paket passieren muss, bevor es sein Ziel erreicht
• Impulse (Ticks): die Verzögerung auf einer Datenverbindung aufgrund der Taktimpulse (ungefähr 55 Millisekunden)
• Kosten: ein willkürlicher Wert, der in der Regel auf der Bandbreite, finanziellen Ausgaben, etc. beruht

38.) Welche Routing-Algorithmen kennen Sie?

→ Random Routing
→ Fluten (Flooding)
→ Hot Potato Routing
→ Shortest Path Routing (SPR, Kürzester Pfad)

39.) Erklären Sie Random Routing.

Jeder Netzknoten schickt ein ankommendes und nicht für diesen Knoten bestimmtes Paket an einen zufällig ausgewählten Nachbarknoten **Ausnahme**: Nachbarknoten, von dem das Paket gekommen ist.
• Einfacher, eher ,,akademischer“ Algorithmus.
• Inhärente Gefahr von Endlosschleifen.

40.) Erklären Sie Fluten

Jeder Netzknoten schickt ankommende und nicht für diesen Knoten bestimmtes Pakete an alle Nachbarknoten. Ausnahme: Nachbarknoten, von dem das Paket gekommen ist.
⇒ der ,,kürzeste“ Weg zwischen Knoten A und B wird stets gefunden (Vorteil)
⇒ ,,Flut“ an Paketduplikaten wird erzeugt (Nachteil), Endlosschleifen möglich
• Paket-Flut kann durch die Einführung von Zählern (in Paketen) und Schwellwerten (an Vermittlungsknoten) ,,eingedämmt“ werden.

41.) Erklären Sie „Hot-Potato“ Routing.

• Jeder Netzknoten versucht ein ankommendes Paket so schnell wie möglich weiterzuleiten. (auch Deflection Routing genannt)
⇒ Paketverluste werden weitgehend vermieden (Vorteil)
⇒ der ,,kürzeste“ Weg zwischen Knoten A und B wird nicht berücksichtigt (Nachteil)
⇒ Paket-Reihenfolge Vertauschungen und endloses Herumkreisen der Pakete möglich (Nachteil)
• Verschiedene Varianten (z.B. Weiterleitung an die Anschlußleitung mit der kürzesten Warteschlange oder Hybridlösungen) vorhanden.

42.) Erklären Sie „Shortest-Path“ Routing.

Bestimmung der ,,kürzesten Wege“ zwischen Quellknoten und Zielknoten.
• Kürzeste Wege nach folgenden Kriterien:
– geographische Entfernung
– Leitungskapazität
– Leitungsbelastung
– Paketverzögerungen
– Warteschlangen-Länge der Vermittlungsknoten
– Blockierungswahrscheinlichkeiten
Prinzipielle Probleme bei ,,Shortest Path Routing“:
– Mehrere kürzeste Wege möglich.
– Änderungen des Netzzustands (z.B. Ausfall von Netzkomponenten).
– Gefahr der Oszillationen (fluktuierende Routenänderungen).
– Nicht jeder mögliche Weg im Netz kann aus Rechenzeitgründen durchsucht werden (kombinatorische Explosion).

43.) Wie können Routingverfahren klassifiziert werden?

Zentrales Routing
– Wegeauswahl wird von einem zentralen Knoten (Routing Control Center, RCC) durchgeführt.
• Verteiltes Routing
– Wegeauswahl wird von den einzelnen Vermittlungsknoten individuell und verteilt durchgeführt.
• Statisches (nichtadaptives) Routing (siehe nächste Folie)
– Wegeauswahl wird unabhängig vom Verkehr und von der Topologie durchgeführt (,,offline‘‘).
• Dynamisches (adaptives) Routing (siehe nächste Folie)
– Wegeauswahl wird in Abhängigkeit vom Verkehr und von der Topologie durchgeführt (,,online‘‘).

44.) Was versteht man unter Konvergenzzeit beim Routing?

Der Routing-Algorithmus bildet die Grundlage des dynamischen Routings. Wenn sich die Topologie des Netzes aufgrund von Wachstum, Neukonfiguration oder Ausfall ändert, muss auch die Datenbank mit den Netzinformationen geändert werden. Die Informationen müssen eine genaue, konsistente Ansicht der neuen Topologie liefern. Diese Ansicht wird als Konvergenz bezeichnet. Wenn alle Router mit denselben Informationen arbeiten, wird das Netz als konvergiert bezeichnet. Die schnelle Konvergenz ist eine wünschenswerte Eigenschaft für ein Netz, weil sie die Zeitspanne reduziert, in der Router weiter falsche/unproduktive Routing-Entscheidungen treffen.

45.) Wie können Routingschleifen entstehen?

Routing-Schleifen können auftreten, wenn durch die langsame Konvergenz bei einer neuen Konfiguration inkonsistente Routing-Einträge erzeugt werden.

• Kurz vor dem Ausfall von Netz 1 verfügen alle Router über konsistente Informationen und korrekte Routing-Tabellen. Nun nimmt man an, dass der bevorzugte Pfad von Router C zum Netz1 über Router B führt. Die Entfernung von Router C zum Netz1 sei 3.

• Nun falle das Netz 1 aus, Router E sende ein Update an Router A. Router A unterbricht das Routing von Paketen zum Netz 1. Die Router B, C und D setzen jedoch das Routing fort, da sie noch nicht über den Ausfall informiert wurden. Wenn Router A sein Update sendet, beenden die Router B und D das Routing zum Netz 1, Router C hat jedoch kein Update erhalten. Router C geht immer noch davon aus, dass das Netz 1 über Router B erreichbar ist.

• Jetzt sendet Router C ein periodisches Update an Router D, in dem ein Pfad zum Netz 1 über Router B angegeben wird. Router D ändert seine Routing-Tabelle, um diese gute, aber falsche Information widerzuspiegeln, und gibt die Information an Router A weiter. Router A gibt die Information an die Router B und E weiter usw. Alle für Netz 1 bestimmten Pakete kreisen jetzt in einer Schleife von Router C zu B zu A zu D und wieder zurück zu C. à sehr schlecht!!

46.) Was ist ein autonomes System?

Grund der Netzaufteilung in autonome Systeme:
Anzahl der Einträge in der Routingtabelle und Menge der ausgetauschten Routinginformation sind sonst gigantisch. Die Router haben in einem autonomen System normalerweise nur Routing- Informationen über dieses autonome System. In jedem autonomen System gibt es zumindest ein ausgezeichnetes Zwischensystem, welches als Schnittstelle zu anderen autonomen Systemen dient.
Vorteile:
• Skalierbarkeit
• Größe der Routingtabellen ist abhängig von der Größe des autonomen Systems.
• Änderungen von Einträgen in den Routingtabellen werden nur innerhalb eines autonomen Systems weitergegeben.
• Autonomie, Internet = Netz von Netzen
• Routing kann im eigenen Netz kontrolliert werden
• Routingprotokolle der autonomen Systeme müssen nicht identisch sein

47.) Welche Routing-Protokolle kennen Sie?

Routing-Protokolle legen den Weg fest, über welchen die Pakete ihr Ziel erreichen. Zu den Routing-Protokollen gehören:
• Routing Information Protocol (RIP)
• Interior Gateway Routing Protocol (IGRP)
• Enhanced Interior Gateway Routing Protocol (EIGRP)
• Open Shortest Path First (OSPF)
Über Routing-Protokolle können Router, die über ein Netz verbunden sind, eine interne "Landkarte" anderer Router im Netz erstellen. Dadurch wird das Routing ermöglicht, das Wählen des optimalen Pfades. Diese Karten werden in die Routing-Tabelle jedes einzelnen Routers übernommen.

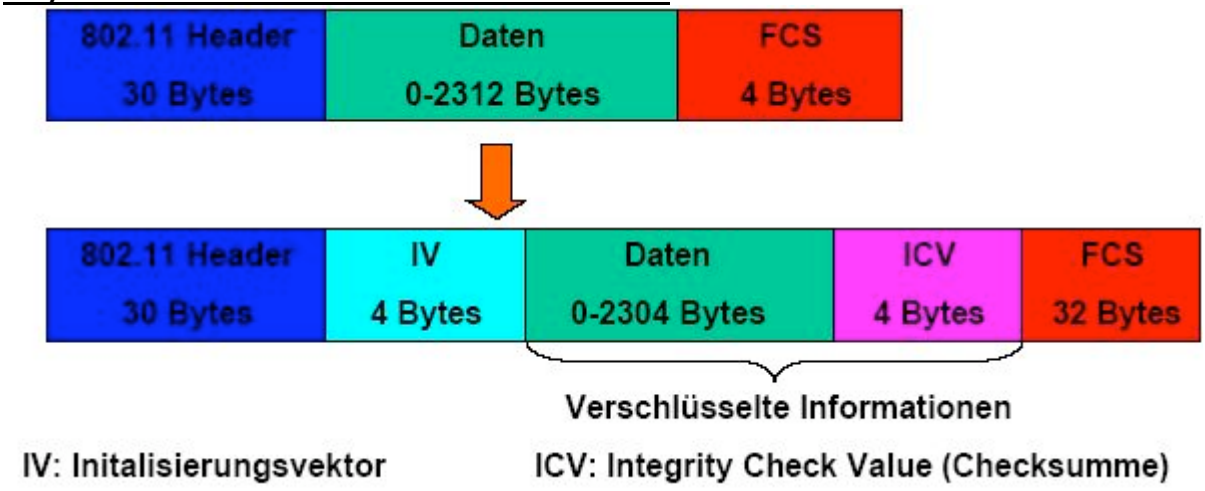
48.) Worin unterscheiden sich Distanz-Vektor-Algorithmen von Link-State-Algorithmen?

Im praktischen Einsatz sind meist verteilte adaptive Routingalgorithmen. Es werden dabei zwei grundlegende Algorithmen unterschieden, nämlich:

- **Distanz-Vektor-Algorithmen** (Beim Distanzvektor-Routing- Verfahren wird die Richtung/ Vektor und die Entfernung/Distanz zu einer Verbindung im Netz bestimmt.)
- **Link-State-Algorithmen** (Beim Link-State-Verfahren- auch Shortest Path First genannt- wird die genaue Topologie des gesamten Netzes- oder zumindest des Abschnitts, in dem sich der Router befindet- nachgebildet.)

Distanzvektor	Link-State
Betrachtet Netzwerktopologie aus der Sicht benachbarter Router	Allgemeine Ansicht der gesamten Netzwerktopolgie
Fügt Distanzvektoren von Router zu Router hinzu	Berechnet den kürzesten Weg zu anderen Routern
Häufige, periodische Updates: langsame Konvergenz	Ereignisgesteuerte Updates: schnellere Konvergenz
Gibt Kopien der Routing-Tabellen an benachbarte Router weiter	Gibt Link-State-Routing-Updates an andere Router weiter

49.) Skizzieren Sie den WLAN MAC-Rahmen



50.) Welche Sicherheitsmaßnahmen gibt's bei WLAN?

„WEP" bedeutet **W**ired **E**quivalent **P**rivacy

• Es stellt einen Schutzmechanismus auf peer-to-peer Ebene (zw. Client und AP) dar.
• Als Verschlüsselungsalgorithmus wird RC-4 verwendet.
• Zur Authentifizierung werden i.d.R. Open-System oder Shared-Key-Methoden benutzt.

WEP soll etwa das Sicherheitsniveau eines Kabel- Ethernet erreichen. Die Realisierung hat mehrere Elemente, nämlich:

• Verschlüsselung mit Stream Cipher RC4
• den Partnern ist ein geheimer Schlüssel bekannt (shared secret key)

• Integrity Check (IC) CRC-32 zur Integritätsprüfung
• 24 Bit Initialisierungs Vektor (IV)- soll identische verschlüsselte Daten bei identischem Klartext verhindern

Folgende Alternativen bieten sich an:
• Authentifizierung über private PGP/Kerberos-Schlüssel
• Benutzung einer MAC-Firewall, IP-Kontrollen
• Auch Firmen, wie Lucent bieten interessante Konzepte (so eine Art „Wireless-ID“)

51.) Wie kann grundsätzlich der Zugang zu einem WLAN mit WEP geknackt werden?

Grundsätzlich ist es möglich den Verkehr im WLAN zu belauschen. Hat man etwa 4 bis 6 Millionen solcher Pakete (entspricht etwa 1.9 bis 15 GB) „gesnifft“ so kann mit Hilfe eines Algorithmus der WEP-Schlüssel geknackt werden. Mit moderner Hardware lässt sich daraus der WEP-Key in etwa 20 (WEP64) bis 50 Minuten (WEP128).
Für das Knacken des WEP-Schlüssels gibt es mehrere Tools:
• Netstumbler-Windows (http://www.netstumbler.com)
• Ethereal (http://www.ethereal.com, http://winpcap.polito.it)
• WepCrack http://sourceforge.net/projects/wepcrack, Perlhttp://www.activestate.com)
• Airsnort (Linux, Knoppix ab V3.2, auch für Windows, http://airsnort.shmoo.com, siehe auch http://www.wireless-bern.ch)
• Kismet (Linux, http://www.kismetwireless.net)
• Lycos WLAN Sniffer

52.) In welcher Weise können switches klassifiziert werden?

Schicht-2 Switches: Sämtliche Layer-2 Switches arbeiten auf Basis von MAC-Adressen. Bei dem Layer 2-Switch gibt es drei verschiedene Funktionsarten: Cut-Trough Switching, Store-and-Forward Switching und Modified-Cut-Through Switching.
• **Schicht-2/3 Switches:** Es gibt hier verschiedene Prinzipien, nach denen diese Switches funktionieren können. Beispielsweise kann immer geswitcht, wenn es möglich ist und nur dann geroutet, wenn es nötig ist. Es kann auch das erste Paket geroutet werden, alle anderen werden geswitcht.

Detail:
Cut Through Switches- On The Fly: Der Ethernet Switch wartet nicht, bis er das vollständige Paket gelesen hat, sondern er überträgt das ankommende Paket nach Empfang der 6-Byte-Destination-Adresse. Da nicht das gesamte Paket bearbeitet werden muss, tritt eine Zeitverzögerung von nur etwa 40µs auf. Sollte das Zielsegment bei der Übertragung gerade belegt sein, speichert der Ethernet Switch das Paket. Bei den Switches werden fehlerhafte Pakete auch auf das andere Segment übertragen. Solange der Anteil der fehlerhaften Paketen im Netz gering ist, entstehen keine Probleme. Sobald aber (z.B.: bei Verkabelungs- und Hardwarefehler oder hoher Netzlast) der Anteil der Kollisionen steigt, kann es dazu führen, dass die Leistung des Gesamtnetzes deutlich sinkt. Cut-Through-Switching bietet nur dann einen Vorteil, wenn man sehr geringe Verzögerungen bei der Übertragung zwischen einzelnen Knoten benötigt. Diese Technologie sollte nur eingesetzt werden, wenn es darum geht, in relativ kleinen Netzen eine große Anzahl Daten zwischen wenigen Knoten zu übertragen

Store and Forward: Die Switches dieser Kategorie untersuchen im Gegensatz zu den vorher erwähnten die gesamten Datenpaket. Dazu werden die Pakete kurz zwischengespeichert, auf ihre Korrektheit und Gültigkeit überprüft, ggf. Steuerinformationen interpretiert und anschließend weitergeleitet bzw. verworfen. Einerseits hat dies den Nachteil der größeren Verzögerungszeit beim Weiterschicken des Pakets, andererseits werden keinerlei fehlerhafte Pakete auf das andere Segment übertragen. Diese Lösung ist bei größeren Netzen mit vielen Knoten und Kommunikationsbeziehungen besser, weil nicht einzelne fehlerhafte Segmente durch Kollisionen das ganze Netz belasten. Bei diesen Anwendungen ist die Gesamttransferrate entscheidend, die Verzögerung wirkt sich hier kaum aus. Store and Forward-Switching ist immer dann notwendig, wenn ein Sicherheitscheck durchgeführt werden soll, oder unterschiedliche Geschwindigkeiten (z.B. 10 MBit/s zu 100 MBit/s) angeglichen werden müssen.

Modified-Cut-Through: Wie schon erwähnt kann es beim Cut-Through Switching dazu kommen, dass fehlerhafte Pakete weitergeleitet werden, was schließlich zu einer Verminderung der Performance führt. Die Fehlerbehandlung erfolgt durch Protokolle. Werden sehr viele Fehler gemeldet, dann wird der Switch in den Store-and-Forward-Modus umgeschaltet.

53.) Was ist ein VLAN?

VLANs (virtuelle lokale Netze) trennen physische (hardwaremäßige Netzstruktur) und logische Netzstruktur (organisatorischen Zugehörigkeit der Hosts), d.h. Arbeitsgruppenbildungen sind völlig unabhängig vom Standort. Trotz dieser Trennung können diese Arbeitsgruppen uneingeschränkt kommunizieren, als ob sie zum selben LAN gehören würden. Ein VLAN ist somit eine Gruppe von Netzknoten, die zusammengefasst werden.

54.) In welcher Weise können VLAN's klassifiziert werden?

Die Möglichkeit, in welcher Weise ein Client einem VLAN zugeordnet werden kann, sind:

- Schicht 1 (Physikalischer Anschluß)
- Schicht 2 (MAC-Adresse)
- Schicht 3 (Protokoll-Adressen)
- Schicht 4 – 7 (Applikation)

Lindner (Cisco Fragen)

1) In welchem Mode befinden sie sich wenn sie sich in den Ciscorouter einloggen? Welches Userinterface finden sie vor? Wie konfigurieren sie einen Useraccount?

2) Wie erfolgt der Wechesl in den Privileged Mode? Wie konfigurieren sie den Schutz dafür?

3) Wie erfolgt der Wechsel in den Konfiguration-Mode? Ab wann werden Eingaben in diesem Mode wirksam? Wie kehren sie aus dem Konfmode wieder zurück?

4) Welche Konfigurationsfiles unterscheidet der Cisco Router ? Wie werden diese verwaltet (anschauen, überschreiben, hinzufügen und sichern) ?

5) Über welche Arten lässt sich der Router konfigurieren? Welche Art ist nur möglich wenn Router noch keine Konfiguration aufweist?

6) Wo ist das IOS gespeichert? Wo befinden sich die Konfigurationsfiles? Wozu dient das ROM?

7) Mit welchem Kommando überprüfen sie die Ip Routingtabelle? Welche elemente befinden sich in der Cisco IP Routing Tabelle im Falle von RIP?

8) Wie konf. Sie IP Adressen am Router?

9) Wie konf. Sie RIPv1 am Router?

10) Wie konf. Sie RIPv1 am Router?