

File Transfer Protocol (FTP)

Prof. Dr. Norbert Pohlmann

Fachbereich Informatik

Verteilte Systeme und Informationssicherheit



Inhalt

- **Ziele und Einordnung**
- **Übersicht**
- **Datenformate und Datentypen**
- **Datenübertragung**
- **FTP-Kommandos**
- **Protokollmitschnitt**
- **Zusammenfassung**

■ Ziele und Einordnung

- Übersicht
- Datenformate und Datentypen
- Datenübertragung
- FTP-Kommandos
- Protokollmitschnitt
- Zusammenfassung

FTP - File Transfer Protocol

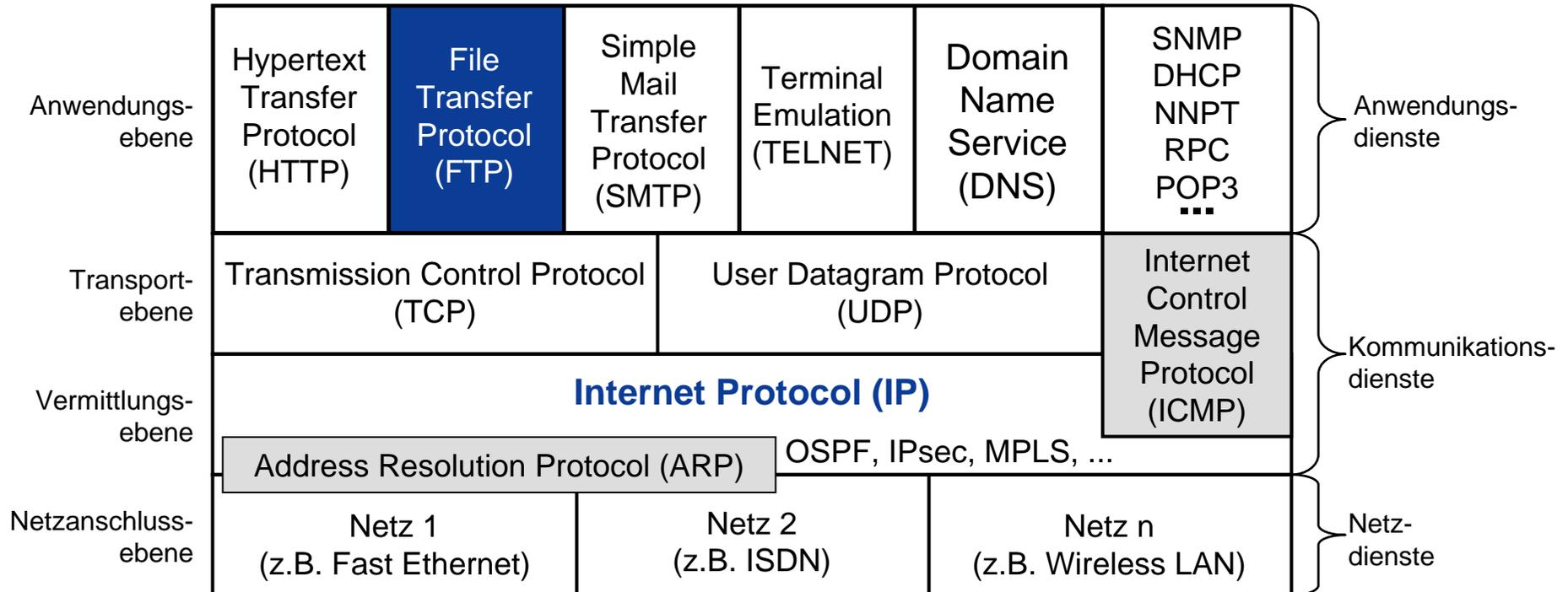
→ Ziele

- Gutes Verständnis für das File Transfer Protocol
- Erlangen der Kenntnisse über die Aufgaben, Prinzipien und Mechanismen des File Transfer Protocols
- Gewinnen von praktischen Erfahrungen über das File Transfer Protocol mit Hilfe von Protokollanalysen und Statistiken (IAS)

Die Anwendungsebene

→ File Transfer Protocol (FTP) - Einordnung

Internet-Protokollstack



Inhalt

- Ziele und Einordnung

■ Übersicht

- Datenformate und Datentypen
- Datenübertragung
- FTP-Kommandos
- Protokollmitschnitt
- Zusammenfassung

FTP - File Transfer Protocol

→ Standards und Literatur

RFC 959 - File Transfer Protocol 1985

RFC 2228 - FTP Security Extension 1997

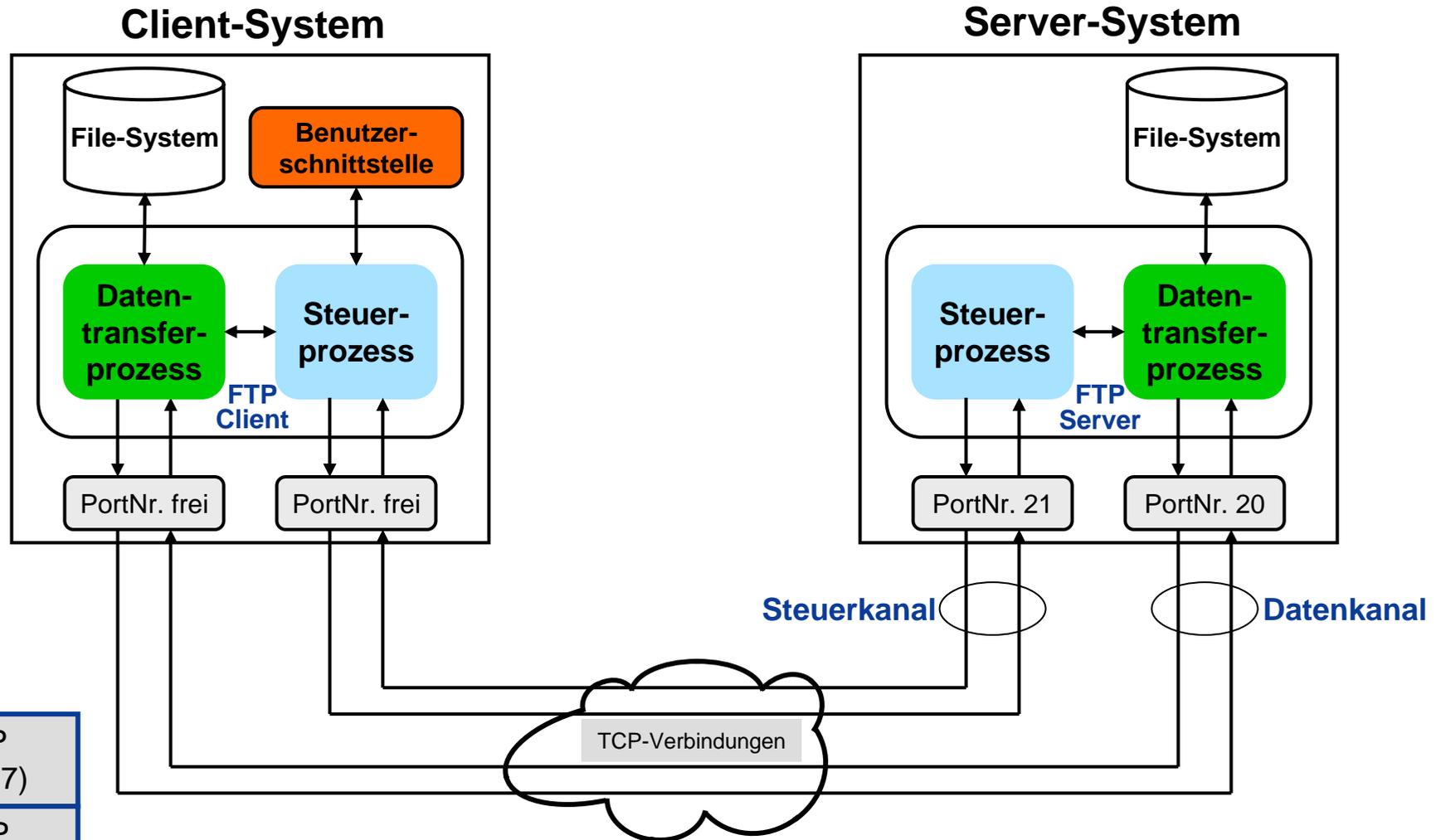
File Transfer Protocol (FTP)

→ Übersicht (1/4)

- Das File Transfer Protocol dient zum Transferieren von Dateien zwischen einem FTP-Client und einem FTP-Server.
- Eine umfangreiche Remote-Funktionalität erlaubt das Fernbedienen des Servers.
- Die **Übertragungsmechanismen von FTP** nehmen es dem Anwender ab, sich mit den Details der Betriebssystemumgebung und dem Dateisystem des FTP-Servers auseinanderzusetzen.
- Der Entwurf des Protokolls ist so ausgelegt, dass z.B. in UNIX-Umgebungen durch manuelle Eingaben vom Terminal des Anwenders aus direkt die Abwicklung von Dateiübertragungen und Remote-Sitzungen unterstützt wird.

File Transfer Protocol (FTP)

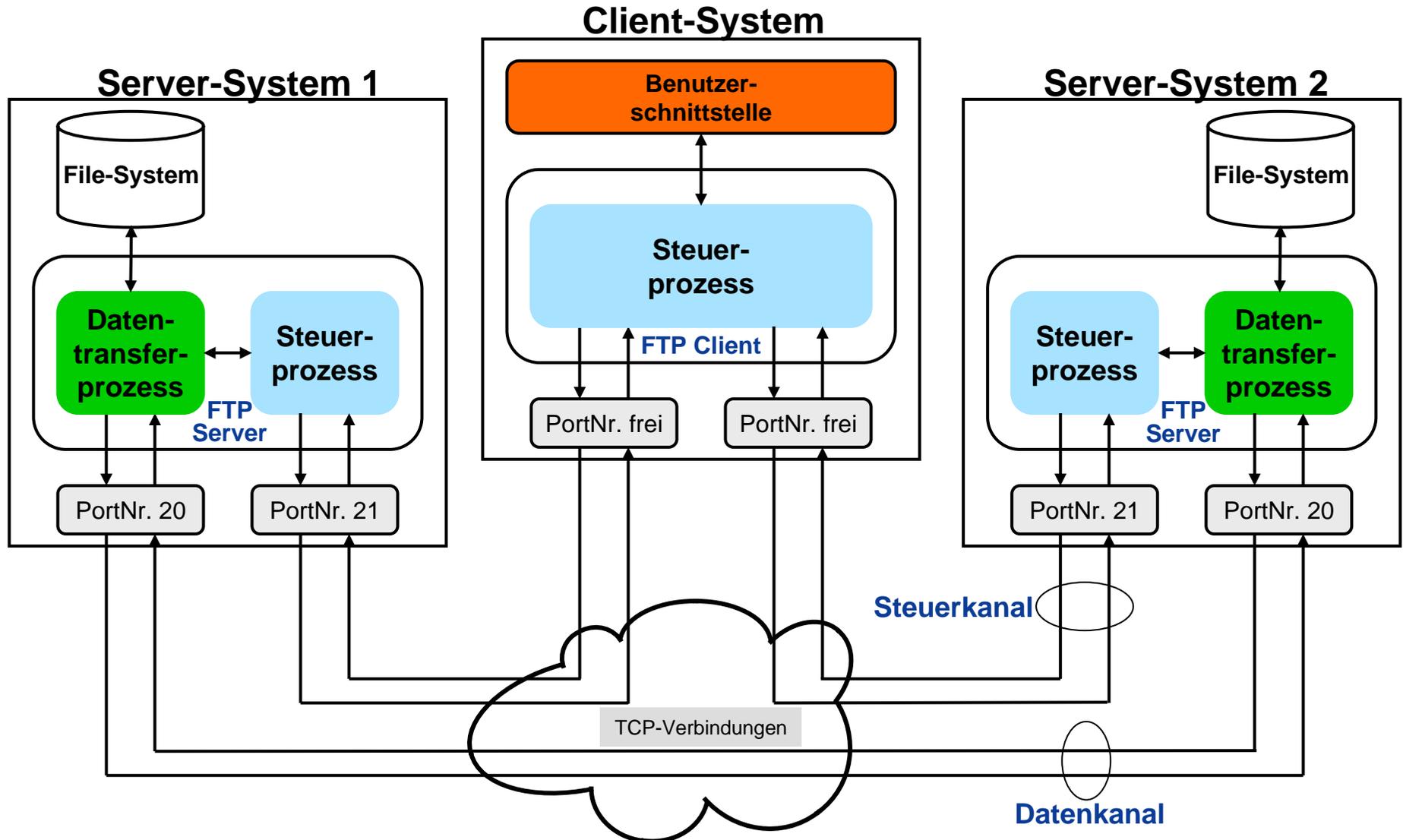
→ Übersicht (2/4) - Client-Server Beziehung



FTP (OSI 7)
TCP
IP

File Transfer Protocol (FTP)

→ Übersicht (2/4) - 1 Client- 2 Server



File Transfer Protocol (FTP)

→ Übersicht (3/4)

- Zwischen dem Remote-FTP-Server und dem FTP-Client bestehen **zwei gleichberechtigte Verbindungen**.
- Die eine dient zum Austausch von Befehlen.
- Sie stellt eine Art von **Steuerkanal** dar.
- Die andere ist der eigentliche **Datenkanal**, auf dem die Dateien in beide Richtungen übertragen werden.
- Alle Übertragungen auf dem Steuerkanal werden mit Hilfe des „Telnet-Protokolls“ abgewickelt.
- Dies kann durch ein in der server- oder anwendungsseitigen Implementation enthaltenes Protokollmodul oder mit Hilfe des vorhandenen nativen Telnet in der Betriebssystemumgebung realisiert werden.
- Weil allerdings nur relativ geringe Anteile der Telnet-Funktionalität benötigt werden, realisieren die meisten Implementationen wegen des Vorteils des kompakteren Codes ein eigenes „abgespecktes“ Telnet-Modul.

File Transfer Protocol (FTP)

→ Übersicht (4/4)

- Die Parameter für den Dateiaustausch über den Datenkanal (Port, Übertragungsmodus, Darstellungsart und Struktur) werden mit Hilfe entsprechender FTP-Befehle über den Steuerkanal an den Server übermittelt.
- Der **Datentransferprozess** auf der Anwenderseite „hört“ permanent den entsprechenden Port ab.
- Der FTP-Server stellt beim „Active Mode“ die Datenverbindung her und konfiguriert sie entsprechend den zuvor auf dem Steuerkanal übermittelten Parametern.
- Der Aufbau von FTP macht es erforderlich, dass der Steuerkanal so lange verbunden bleiben muss, wie Dateien übertragen werden (siehe PM).

Inhalt

- Ziele und Einordnung
- Übersicht
- **Datenformate und Datentypen**
 - Datenübertragung
 - FTP-Kommandos
 - Protokollmitschnitt
 - Zusammenfassung

File Transfer Protocol (FTP)

→ Unterschiedliche Datenformate und ihre Speicherung

- Unabhängig vom Dateisystem einer Rechnerplattform und der Art des Formats, in der die Daten dort auf einem Speichermedium abgelegt werden, übertragen FTP Dateien vom sendenden zum empfangenen Rechnersystem (z.B. ASCII und EBCDIC).
- In der Regel wird bei Zeichenübertragung Standard-NVT-ASCII als Datendarstellungsformat verwendet.
- Beide am Dateitransfer beteiligte Seiten müssen ihr natives Format entsprechend konvertieren.
- Ähnlich müssen verschiedene Binärformate berücksichtigt werden.
- Normalerweise verfügen die FTP-Implementierungen auf der jeweiligen Plattform über entsprechende Anpassungsoptionen.

File Transfer Protocol (FTP)

→ Datentypen

- Der für die Dateiübertragung verwendete Datentyp wird vom Anwender durch Angeben eines Datenformattyps festgelegt (TYPE).
- Der Formattyp kann implizit oder explizit festgelegt werden.
- **Datentyp ASCII (A)**
 - Der Datentyp ASCII wird für die Übertragung zwischen zwei Rechnersystemen eingesetzt, die dieses Format nutzen.
- **Datentyp EBCDIC (E)**
 - Der Datentyp EBCDIC wird für die Übertragung zwischen zwei Rechnersystemen eingesetzt, die dieses Format nutzen.
- **Datentyp IMAGE (I)**
 - Der Datentyp IMAGE wird für die Übertragung von Bilddarstellung eingesetzt. Bilder werden als aufeinanderfolgende Reihe von Bits übertragen.
 - Der Bitstrom wird dabei auf einzelne Bytes aufgeteilt.
 - Auf der Seite des empfangenen Rechnersystems müssen die Bits in entsprechender Reihenfolge auf dem Speichermedium abgelegt werden.

Inhalt

- Ziele und Einordnung
- Übersicht
- Datenformate und Datentypen
- **Datenübertragung**
- FTP-Kommandos
- Protokollmitschnitt
- Zusammenfassung

File Transfer Protocol (FTP)

→ Datenübertragung (1/4)

- Als Voraussetzung für das Übertragen von Dateien muss der Datenkanal eingerichtet und alle für den Transfer erforderlichen Parameter über den Steuerkanal festgelegt sein.
- Der Transfer von Daten über den Datenkanal kennt unterschiedliche Modi.
- Der Defaultmodus „Stream“ besitzt keine Signalisierung, wann ein übertragenes File zu Ende ist.
- Die Konsequenz ist, dass für jedes zu übertragene File (oder auch andere Daten wie Listings) der Datenkanal am Ende wieder geschlossen wird.
- D.h. für weitere Daten muss mehrfach der Datenkanal auf- und abgebaut werden (siehe PM).
- Weitere Modi sind „Block“ und „Compressed“, die auch ein Dateiende signalisieren können, so dass nicht für jede einzelne Datei ein eigener Datenkanal erforderlich ist.

File Transfer Protocol (FTP)

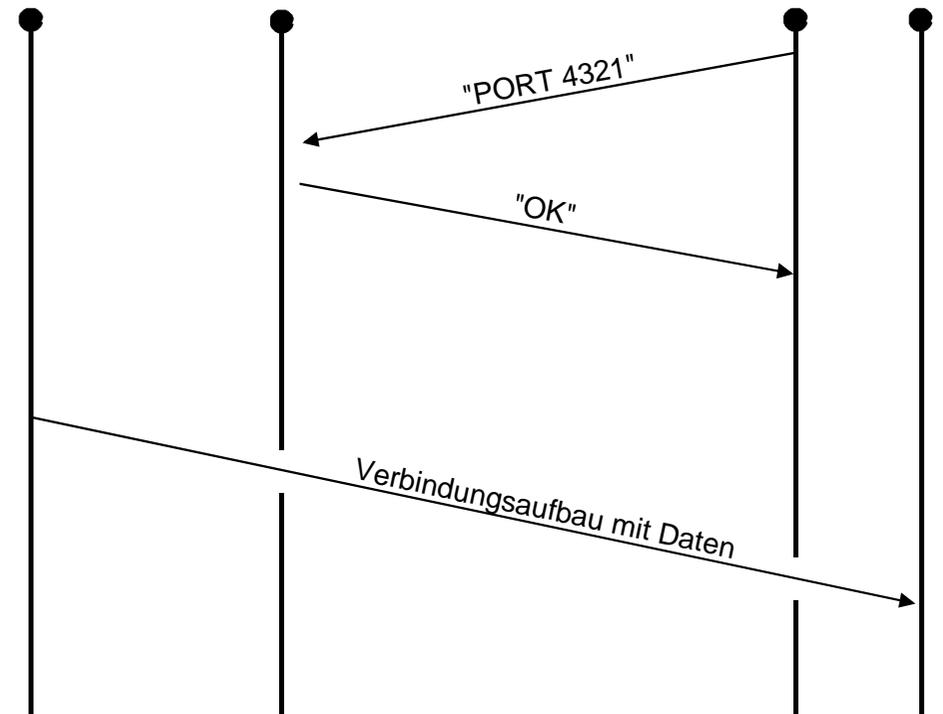
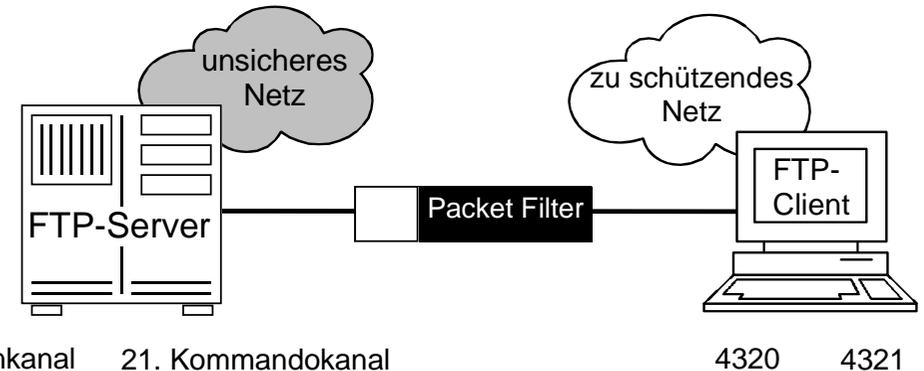
→ Datenübertragung (2/4)

- Für den Datenkanal gibt es zwei verschiedene Varianten: eine „aktive“ Verbindung und eine „passive“ Verbindung.
- Da in jedem Falle der Client zunächst die Initiative ergreift und den Steuerkanal aufbaut, bezieht sich die Unterscheidung zwischen „aktiv“ und „passiv“ auf die Herstellung des Datenkanals aus der **Sicht des Servers**.
- „Aktiv“ heißt hier, der Server stellt den Datenkanal her, „passiv“ heißt, der Server wartet auf den Verbindungsaufbau des Datenkanals durch den Client.

File Transfer Protocol (FTP)

→ Datenübertragung (3/4) - ACTIVE MODE

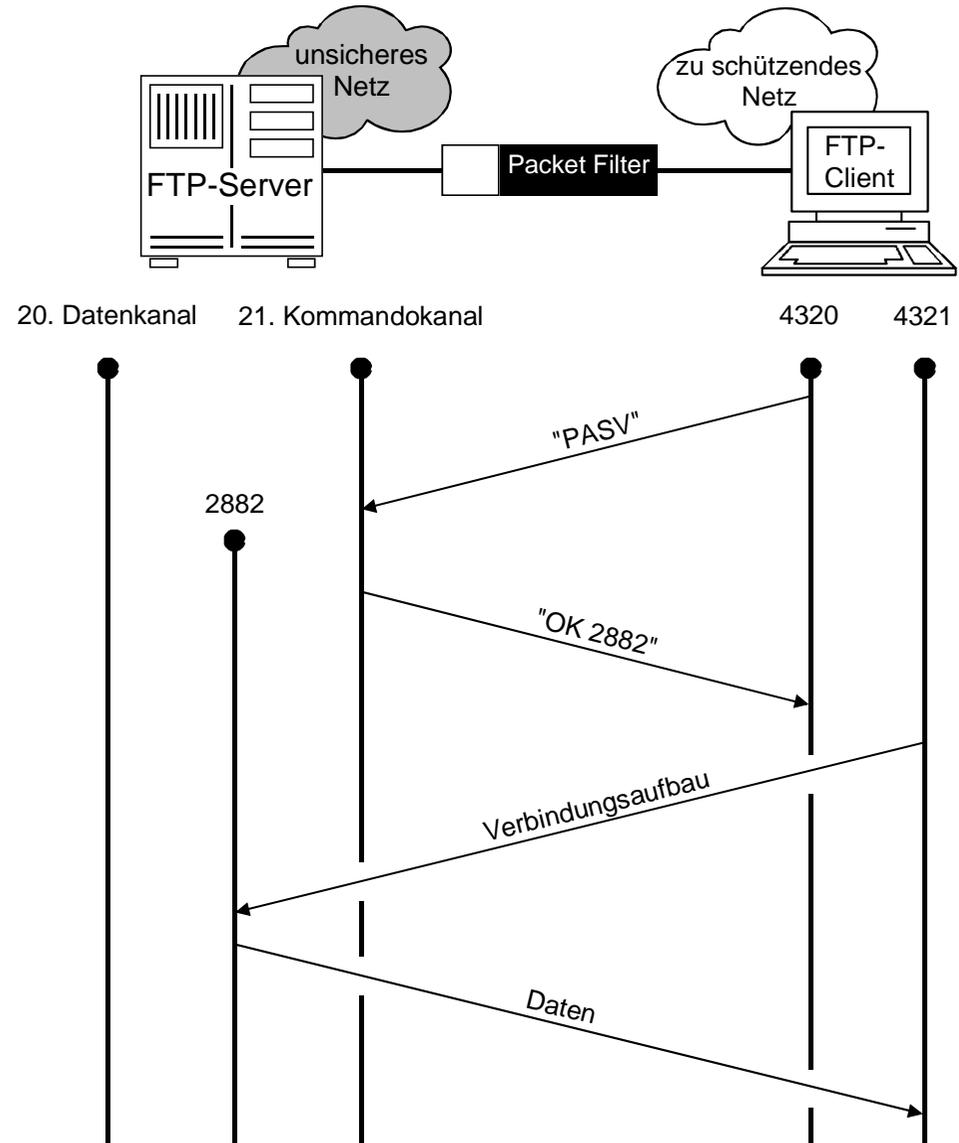
- Server-Port für den Steuerkanal ist Port 21.
- Für die Dateiübertragung einer aktiven FTP-Verbindung teilt der Client dem Server mit, welchen Port der Server verwenden soll (hier Port 4321).
- Der Server baut dann den Datenkanal zu dem angegebenen Port auf.
- Source-Port des Servers ist immer Port 20.
- **Problem bei diesem Mode:** Es muss für TCP-Verbindungen ein Verbindungsaufbau aus dem unsicheren Netz ermöglicht werden!
- Da dies sicherheitskritisch ist, wird dieser Mode von den meisten Firewalls verhindert und **kann in der Regel nicht verwendet werden!**



File Transfer Protocol (FTP)

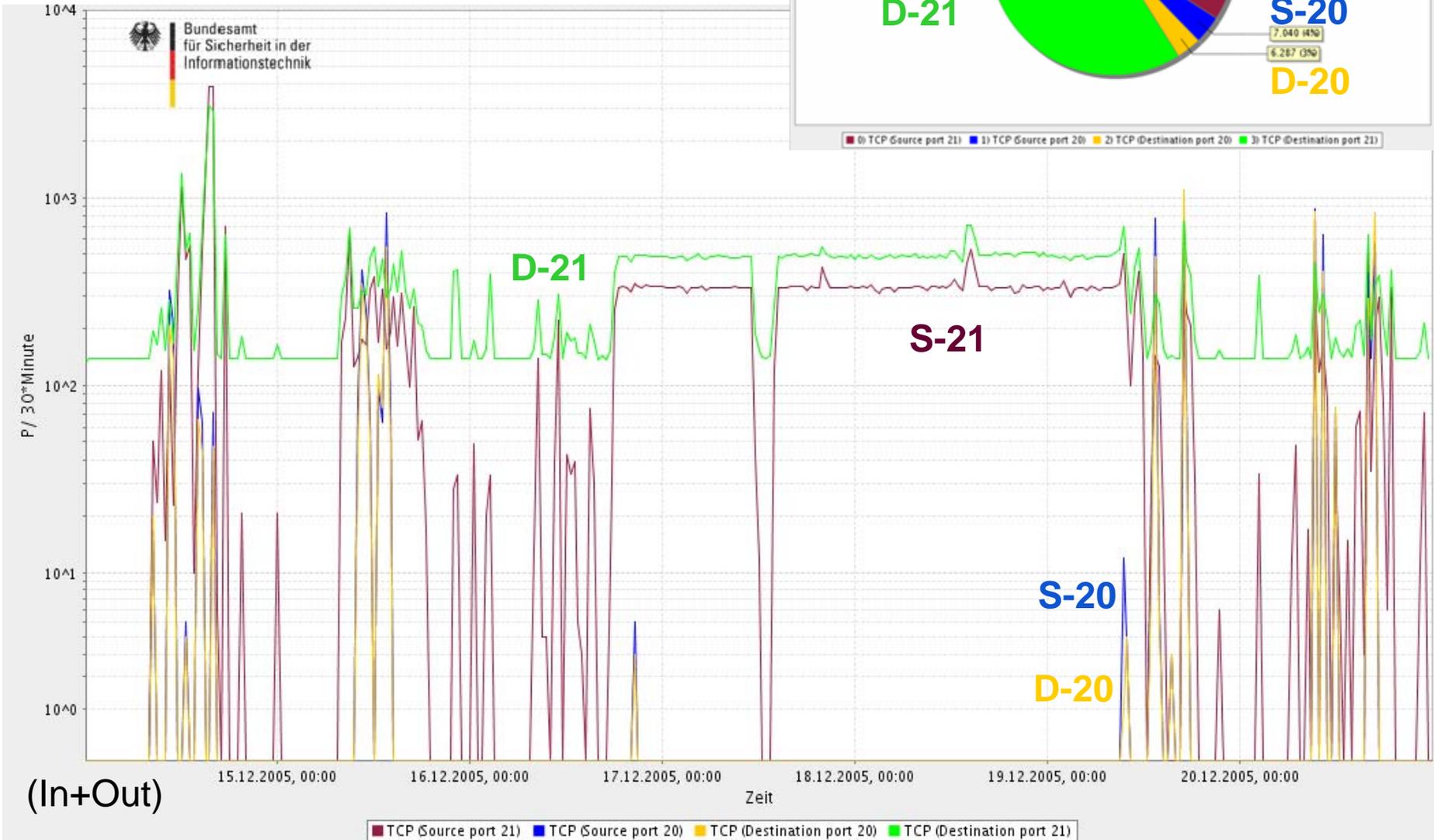
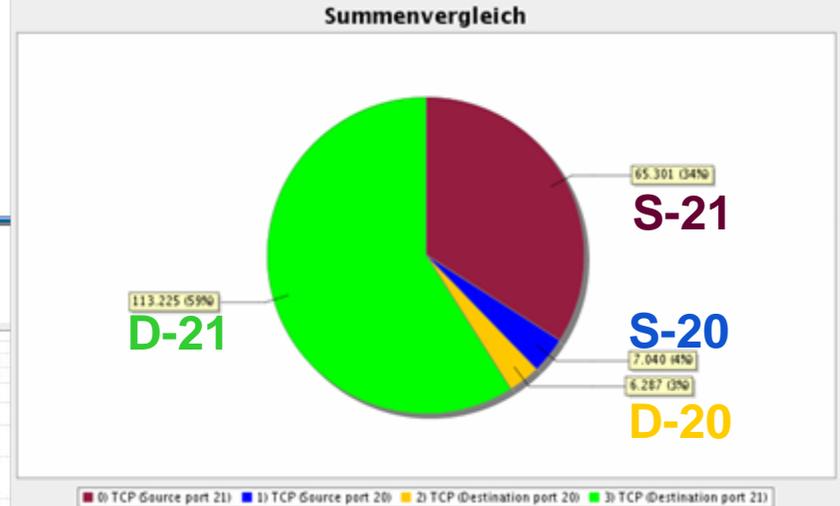
→ Datenübertragung (4/4) - PASSIVE MODE

- Beim „PASSIVE MODE“ muss der Client dem Server mitteilen, dass er eine passive Verbindung wünscht.
- Statt des PORT-Kommandos verwendet er das Kommando **PASV**.
- Der Server teilt dem Client daraufhin einen freien Port (hier 2882) mit, zu dem der Client die Datenverbindung aufbauen kann.
- Der „Passive Mode“ ist zu bevorzugen, da hier die Verbindung aus dem sicheren Netz definiert und aufgebaut wird!
- **Damit wird ein potentielles Risiko minimiert!**



IAS: FB Informatik

→ FTP-Ports



Inhalt

- Ziele und Einordnung
- Übersicht
- Datenformate und Datentypen
- Datenübertragung
- **FTP-Kommandos**
- Protokollmitschnitt
- Zusammenfassung

File Transfer Protocol (FTP)

→ FTP-Kommandos - Requests (1/3)

- Die Kommandos, die der Steuerprozess nutzt, sind reine ASCII-Kommandos, die der Server ebenfalls mit einer ASCII-Nachricht quittiert.
- Die Kommandos unterscheiden sich nach Access (Login, Logout, Verzeichniswechsel, ...), Transferparameter (z.B. aktiv/passiv, binäre Datenkommunikation oder ASCII-Konvertierung) und den eigentlichen FTP-Diensten (Daten übertragen, aber auch Verzeichnisse anlegen, Daten löschen, usw.).
- Die folgenden Tabellen geben einen Überblick über die wichtigsten Kommandos.

File Transfer Protocol (FTP)

→ FTP-Kommandos - Requests (2/3)

Kommandos	Beschreibung
CDUP	Change to Parent Directory: In das übergeordnete Verzeichnis wechseln
CWD	Change Working Directory: In das angegebene Verzeichnis wechseln
DELE	Angegebene File auf dem Server löschen
HELP	Ausgabe aller Kommandos, die der Server versteht
LIST	Holen des aktuellen Verzeichnisses
MKD	Make Directory: Verzeichnis anlegen
NLIST	"Name List": die Ausgabe dient zur Weiterverarbeitung durch ein Programm, etwa bei einem "multiple get"
NOOP	Dieser Befehl veranlaßt den FTP-Server, als Lebenszeichen eine OK-Nachricht zu senden (ansonsten keine weitere Funktion)
PASS	Passwort des Benutzers auf dem Server
PASV	Anforderung des passiven Modus für die Datenübertragung

File Transfer Protocol (FTP)

→ FTP-Kommandos - Requests (3/3)

Kommandos	Beschreibung
PORT	Angabe des Ports für eine aktive Verbindung (Aktive Mode)
PWD	Print Working Directory: es wird das aktuelle Arbeitsverzeichnis angezeigt
QUIT	Verbindung beenden
RETR	Retrieve: Daten vom Server holen - Datei-Transfer S →C
REST	Restart: nach einem Systemabsturz
RMD	Remove Directory: Verzeichnis löschen
STOR	Store: Daten auf dem Server speichern - Datei-Transfer C →S
TYPE	Datenrepräsentation: ASCII (A), EBCDIC (E), Image (I)
USER	Angabe des Users für den Login (User-ID)

File Transfer Protocol (FTP)

→ FTP-Antworten - Response

- Dreistellige ASCII-Zahl, optionale Kommentare, <CR><LF>
 - 1yz Aktion gestartet, aber noch nicht abgeschlossen (z.B. Transfer-Kommando erhalten, aber noch nicht ausgeführt)
 - 2yz Aktion erfolgreich beendet
 - 3yz Aktion gestartet, aber zusätzliches Kommando erforderlich (z.B. nach USER ist noch PASS auszuführen)
 - 4yz Aktion nicht erfolgreich, Wiederholung möglich
 - 5yz Aktion endgültig nicht erfolgreich

 - x0z Syntaxfehler
 - x1z Information
 - x2z betrifft Steuer- oder Datenverbindung
 - x3z betrifft Authentifizierung
 - x4z nicht spezifiziert
 - x5z betrifft den Zustand des Filesystems

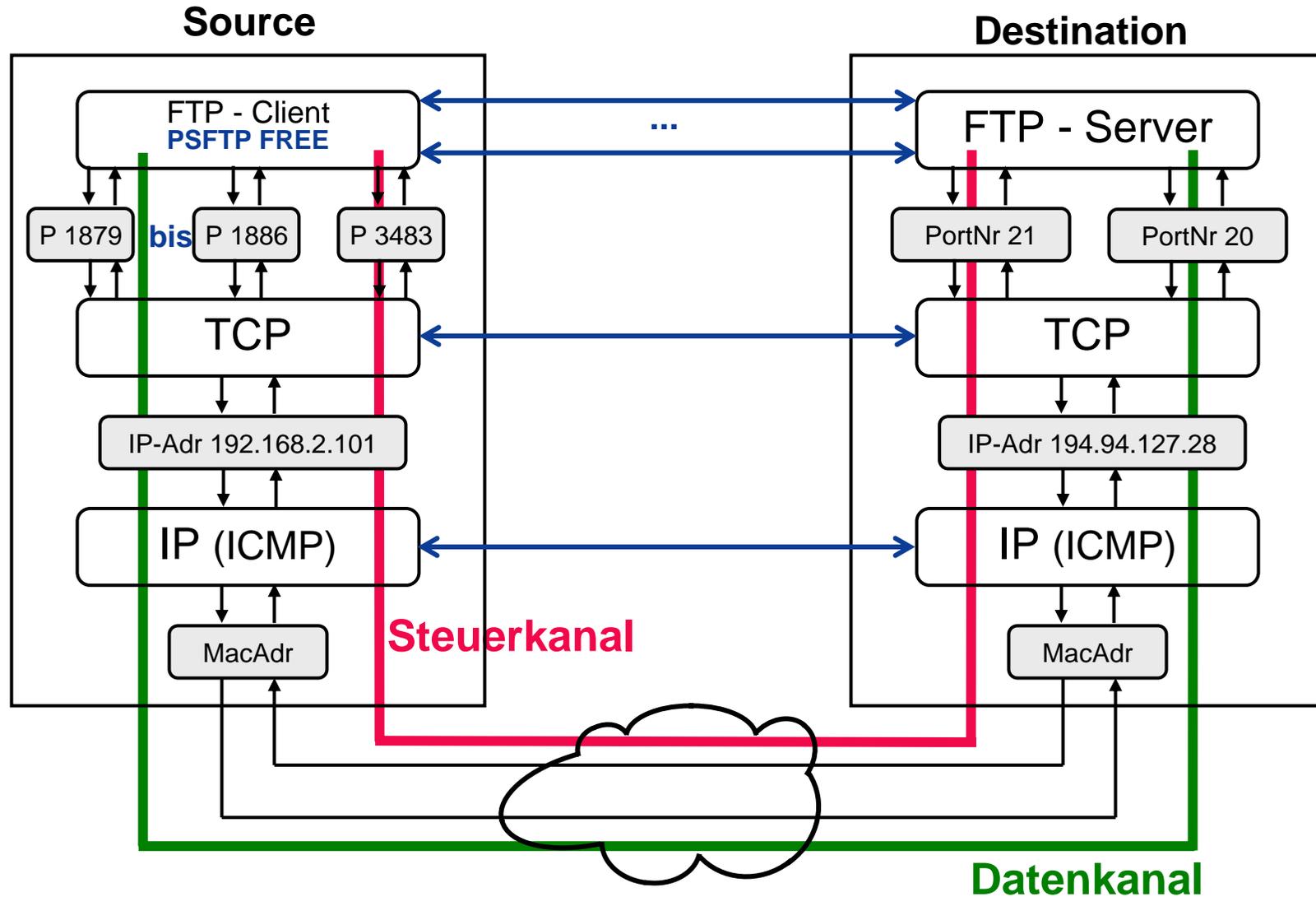
 - z zusätzliche Statuskennung
- Beispiele:
 - 226 Datenübertragung ok
 - 331 user-id ist ok, Passwort ist erfolgreich
 - 425 Datenverbindung kann nicht geöffnet werden

Inhalt

- Ziele und Einordnung
- Übersicht
- Datenformate und Datentypen
- Datenübertragung
- FTP-Kommandos
- **Protokollmitschnitt**
- Zusammenfassung

Protokollmitschnitt - FTP

→ FTP Dateiaustausch zum Skripte-Server



Protokollmitschnitt - FTP

→ Dateien auf dem Client und Server

The screenshot shows the PSFTP FREE interface. The local directory is `D:\Vorlesungen\Netzwerkmanagement\NWM_SS03\PDF\` and the remote directory is `/home/pohlmann/files/Netzwerkmanagement`. Both directories contain a list of PDF files. The file `SNMP_MRTG_22_05_03.pdf` is circled in red in both views.

Name	Größe	Typ	Geändert am	Attr
alt		Dateiordner	02.04.2003 08:31	
Ausarbeitungen_NWM_07_04_03.pdf	65.298	Adobe Acrobat...	07.04.2003 17:05	a
Einfuehrung_NWM_1_04_03.pdf	209.974	Adobe Acrobat...	07.04.2003 17:05	a
Grundlagen_ASN1_07_04_03.pdf	156.142	Adobe Acrobat...	07.04.2003 17:04	a
Grundlagen_Netzkoppelelemente_07_04_03...	170.896	Adobe Acrobat...	07.04.2003 17:03	a
Grundlagen_OSI_07_04_03.pdf	133.427	Adobe Acrobat...	07.04.2003 17:04	a
IT-Sicherheitsprozess NMW_1_04_03.pdf	1.525.923	Adobe Acrobat...	07.04.2003 17:08	a
OSI-Management_22_06_03.pdf	236.749	Adobe Acrobat...	22.06.2003 19:36	a
OSI-SNMP-Vergleich_22_06_03.pdf	80.223	Adobe Acrobat...	23.06.2003 22:11	a
Sicherheitspolitik_07_04_03.pdf	147.964	Adobe Acrobat...	07.04.2003 17:07	a
SNMP_MRTG_22_05_03.pdf	55.662	Adobe Acrobat...	27.05.2003 16:37	a
SNMP_Teil1_Einfuehrung_02_05_03.pdf	258.205	Adobe Acrobat...	06.05.2003 22:10	a
SNMP_Teil2_SNMPv1_03_05_03.pdf	214.701	Adobe Acrobat...	06.05.2003 22:11	a
SNMP_Teil3_SNMPv2_28_03_03.pdf	219.985	Adobe Acrobat...	24.05.2003 21:27	a
SNMP_Teil4_SNMPv3_28_03_03.pdf	310.077	Adobe Acrobat...	24.05.2003 21:28	a
SNMP_Teil5_Agenten_14_05_03.pdf	93.275	Adobe Acrobat...	27.05.2003 16:34	a
SNMP_Teil6_RMON_19_05_03.pdf	158.507	Adobe Acrobat...	27.05.2003 16:36	a
Struktur_NWM_Vorlesung_1_04_03.pdf	91.447	Adobe Acrobat...	07.04.2003 17:06	a
TMN_23_06_03.pdf	709.987	Adobe Acrobat...	23.06.2003 22:10	a

Name	Größe
Ausarbeitungen_NWM_07_04_03.pdf	65.298
Einfuehrung.pdf	209.977
Grundlagen_ASN1_07_04_03.pdf	156.142
Grundlagen_Netzkoppelelemente_07_04_0...	170.896
Grundlagen_OSI_07_04_03.pdf	133.427
IT-Sicherheit.pdf	1.525.917
OSI-Management_22_06_03.pdf	236.749
OSI-SNMP-Vergleich_22_06_03.pdf	80.223
SNMP_MRTG_22_05_03.pdf	55.662
SNMP_Teil1_Einfuehrung_02_05_03.pdf	258.205
SNMP_Teil2_SNMPv1_03_05_03.pdf	214.701
SNMP_Teil3_SNMPv2_28_03_03.pdf	219.985
SNMP_Teil4_SNMPv3_28_03_03.pdf	310.077
SNMP_Teil5_Agenten_14_05_03.pdf	93.275
SNMP_Teil6_RMON_19_05_03.pdf	158.507
Sicherheitspolitik_07_04_03.pdf	147.964
Struktur.pdf	91.444
TMN_23_06_03.pdf	709.987

Protokollmitschnitt - FTP

→ Verbindungsaufbauprozedur

No.	Time	Source	Destination	Protocol	Info	
1	0.000000	192.168.2.101	192.168.2.1	DNS	Standard query A skripte.informatik.fh-ge.de	} DNS-Anfrage
2	0.116758	192.168.2.1	192.168.2.101	DNS	Standard query response A 194.94.127.28	
3	0.209624	192.168.2.101	194.94.127.28	TCP	3483 > ftp [SYN]	} Aufbau des Steuerkanals (Port 3483)
4	0.285685	194.94.127.28	192.168.2.101	TCP	ftp > 3483 [SYN, ACK] Seq=635574929 Ack=1054243470 Win=15466 Len=0	
5	0.285769	192.168.2.101	194.94.127.28	TCP	3483 > ftp [ACK] Seq=1054243470 Ack=635574930 Win=64676 Len=0	
10	20.662773	194.94.127.28	192.168.2.101	FTP	Response: 220 ProFTPD 1.2.2rc3 Server (FH-GE Skripte FTP Server)	
11	20.663258	192.168.2.101	194.94.127.28	FTP	Request: USER pohlmann	} Identifikation
12	20.740138	194.94.127.28	192.168.2.101	TCP	ftp > 3483 [ACK] Seq=635575027 Ack=1054243485 Win=15466 Len=0	
13	20.741923	194.94.127.28	192.168.2.101	FTP	Response: 331 Password required for pohlmann.	
14	20.742263	192.168.2.101	194.94.127.28	FTP	Request: PASS XXXXXXXX	} Authentifikation
15	20.831917	194.94.127.28	192.168.2.101	FTP	Response: 230 User pohlmann logged in.	
16	20.832681	192.168.2.101	194.94.127.28	FTP	Request: REST 100	} Restart des Servers
17	20.908872	194.94.127.28	192.168.2.101	FTP	Response: 350 Restarting at 100.	
18	20.922723	192.168.2.101	194.94.127.28	FTP	Request: REST 0	} „Orientierung“
19	21.002005	194.94.127.28	192.168.2.101	FTP	Response: 350 Restarting at 0.	
20	21.054925	192.168.2.101	194.94.127.28	FTP	Request: CWD /	} „Orientierung“
21	21.133871	194.94.127.28	192.168.2.101	FTP	Response: 250 CWD command successful.	
22	21.143322	192.168.2.101	194.94.127.28	FTP	Request: PWD	} „Orientierung“
23	21.220857	194.94.127.28	192.168.2.101	FTP	Response: 257 "/" is current directory.	
24	21.223429	192.168.2.101	194.94.127.28	FTP	Request: TYPE A	} „Orientierung“
25	21.301840	194.94.127.28	192.168.2.101	FTP	Response: 200 Type set to A.	

Problem: Passwort ist im Klartext

Protokollmitschnitt - FTP

→ Abfrage des aktuellen DIR

PortNr, die der Client nutzen soll
 $7 * 256 + 87 = 1879$

No.	Time	Source	Destination	Protocol	Info
26	21.313298	192.168.2.101	194.94.127.28	FTP	Request: PASV
27	21.394499	194.94.127.28	192.168.2.101	FTP	Response: 227 Entering Passive Mode (194,94,127,28(7,87))
28	21.435839	192.168.2.101	194.94.127.28	TCP	3484 > 1879 [SYN] Seq=1059597838 Ack=0 Win=64240 Len=0
29	21.436099	192.168.2.101	194.94.127.28	FTP	Request: LIST -a
30	21.512655	194.94.127.28	192.168.2.101	TCP	1879 > 3484 [SYN, ACK] Seq=658130059 Ack=1059597839 Win=15466 Len=0
31	21.512720	192.168.2.101	194.94.127.28	TCP	3484 > 1879 [ACK] Seq=1059597839 Ack=658130060 Win=64676 Len=0
32	21.531545	194.94.127.28	192.168.2.101	TCP	ftp > 3483 [ACK] Seq=635575359 Ack=1054243553 Win=15466 Len=0
33	21.596368	194.94.127.28	192.168.2.101	FTP	Response: 150 Opening ASCII mode data connection for file list
34	21.599500	194.94.127.28	192.168.2.101	FTP-DATA	FTP Data: 56 bytes
35	21.609533	194.94.127.28	192.168.2.101	FTP-DATA	FTP Data: 731 bytes
36	21.609615	192.168.2.101	194.94.127.28	TCP	3484 > 1879 [ACK] Seq=1059597839 Ack=658130847 Win=63889 Len=0
37	21.614405	194.94.127.28	192.168.2.101	FTP-DATA	FTP Data: 368 bytes FIN=1
38	21.614486	192.168.2.101	194.94.127.28	TCP	3484 > 1879 [ACK] Seq=1059597839 Ack=658131216 Win=63521 Len=0
39	21.615776	194.94.127.28	192.168.2.101	FTP	Response: 226 Transfer complete.
40	21.615803	192.168.2.101	194.94.127.28	TCP	3483 > ftp [ACK] Seq=1054243553 Ack=635575437 Win=64169 Len=0
41	21.625736	192.168.2.101	194.94.127.28	TCP	3484 > 1879 [FIN, ACK] Seq=1059597839 Ack=658131216 Win=63521 Len=0
42	21.704914	194.94.127.28	192.168.2.101	TCP	1879 > 3484 [ACK] Seq=658131216 Ack=1059597840 Win=15466 Len=0

Passive Mode

Aufbau eines Datenkanals (Port 1879)

Datenübertragung - LIST

Abbau des Datenkanals (Port 1879) durch den Server

Abbau des Datenkanals (Port 1879) durch den Client

Kumulative Besträtigung

Protokollmitschnitt - FTP

→ Wechsel zu und Abfrage von DIR „/home“

No.	Time	Source	Destination	Protocol	Info	
43	26.512832	192.168.2.101	194.94.127.28	FTP	Request: CWD /home	} Verzeichniswechsel zu „/home“
44	26.592959	194.94.127.28	192.168.2.101	FTP	Response: 250 CWD command successful.	
45	26.601794	192.168.2.101	194.94.127.28	FTP	Request: PWD	} Abfrage vom aktuellen DIR
46	26.680955	194.94.127.28	192.168.2.101	FTP	Response: 257 "/home" is current directory.	
47	26.691503	192.168.2.101	194.94.127.28	FTP	Request: TYPE A	} Passive Mode
48	26.769927	194.94.127.28	192.168.2.101	FTP	Response: 200 Type set to A.	
49	26.781166	192.168.2.101	194.94.127.28	FTP	Request: PASV	
50	26.861529	194.94.127.28	192.168.2.101	FTP	Response: 227 Entering Passive Mode (194,94,127,28,7,88).	
51	26.875115	192.168.2.101	194.94.127.28	TCP	3485 > 1880 [SYN] Seq=1060984727 Ack=0 Win=64240 Len=0	} Aufbau eines Datenkanals (Port 1880)
52	26.875385	192.168.2.101	194.94.127.28	FTP	Request: LIST -a	
53	26.951347	194.94.127.28	192.168.2.101	TCP	1880 > 3485 [SYN, ACK] Seq=670041108 Ack=1060984728 Win=15466 Len=0	
54	26.951437	192.168.2.101	194.94.127.28	TCP	3485 > 1880 [ACK] Seq=1060984728 Ack=670041109 Win=64676 Len=0	
55	26.971585	194.94.127.28	192.168.2.101	TCP	ftp > 3483 [ACK] Seq=635575570 Ack=1054243592 Win=15466 Len=0	} Datenübertragung - LIST
56	27.035507	194.94.127.28	192.168.2.101	FTP	Response: 150 Opening ASCII mode data connection for file list	
57	27.126381	194.94.127.28	192.168.2.101	FTP-DATA	FTP Data: 56 bytes	
58	27.136410	194.94.127.28	192.168.2.101	FTP-DATA	FTP Data: 752 bytes	
59	27.136497	192.168.2.101	194.94.127.28	TCP	3485 > 1880 [ACK] Seq=1060984728 Ack=670041917 Win=63868 Len=0	
60	27.138065	194.94.127.28	192.168.2.101	FTP-DATA	FTP Data: 66 bytes FIN=1	
61	27.138106	192.168.2.101	194.94.127.28	TCP	3485 > 1880 [ACK] Seq=1060984728 Ack=670041984 Win=63802 Len=0	
62	27.139855	194.94.127.28	192.168.2.101	FTP	Response: 226 Transfer complete.	} Abbau des Datenkanals (Port 1880) durch den Server
63	27.139879	192.168.2.101	194.94.127.28	TCP	3483 > ftp [ACK] Seq=1054243592 Ack=635575648 Win=63958 Len=0	
64	27.143519	192.168.2.101	194.94.127.28	TCP	3485 > 1880 [FIN, ACK] Seq=1060984728 Ack=670041984 Win=63802 Len=0	} Abbau des Datenkanals (Port 1880) durch den Client
65	27.225464	194.94.127.28	192.168.2.101	TCP	1880 > 3485 [ACK] Seq=670041984 Ack=1060984729 Win=15466 Len=0	

Protokollmitschnitt - FTP

→ Wechsel zu und Abfrage von DIR „/home/pohlmann“

No.	Time	Source	Destination	Protocol	Info
66	28.665565	192.168.2.101	194.94.127.28	FTP	Request: CWD /home/pohlmann
67	28.748598	194.94.127.28	192.168.2.101	FTP	Response: 250 CWD command successful.
68	28.754188	192.168.2.101	194.94.127.28	FTP	Request: PWD
69	28.831141	194.94.127.28	192.168.2.101	FTP	Response: 257 "/home/pohlmann" is current directory.
70	28.834367	192.168.2.101	194.94.127.28	FTP	Request: TYPE A
71	28.913019	194.94.127.28	192.168.2.101	FTP	Response: 200 Type set to A.
72	28.924225	192.168.2.101	194.94.127.28	FTP	Request: PASV
73	29.000922	194.94.127.28	192.168.2.101	FTP	Response: 227 Entering Passive Mode (194,94,127,28,7,89).
74	29.008198	192.168.2.101	194.94.127.28	TCP	3486 > 1881 [SYN] Seq=1061544661 Ack=0 Win=64240 Len=0
75	29.008461	192.168.2.101	194.94.127.28	FTP	Request: LIST -a
76	29.094887	194.94.127.28	192.168.2.101	TCP	1881 > 3486 [SYN, ACK] Seq=674648287 Ack=1061544662 Win=15466 Len=0
77	29.094944	192.168.2.101	194.94.127.28	TCP	3486 > 1881 [ACK] Seq=1061544662 Ack=674648288 Win=64676 Len=0
78	29.102431	194.94.127.28	192.168.2.101	TCP	ftp > 3483 [ACK] Seq=635575790 Ack=1054243640 Win=15466 Len=0
79	29.178934	194.94.127.28	192.168.2.101	FTP	Response: 150 Opening ASCII mode data connection for file list
80	29.216288	194.94.127.28	192.168.2.101	FTP-DATA	FTP Data: 56 bytes
81	29.221735	194.94.127.28	192.168.2.101	FTP-DATA	FTP Data: 446 bytes
82	29.221797	192.168.2.101	194.94.127.28	TCP	3486 > 1881 [ACK] Seq=1061544662 Ack=674648791 Win=64174 Len=0
83	29.223508	194.94.127.28	192.168.2.101	FTP	Response: 226 Transfer complete.
84	29.223532	192.168.2.101	194.94.127.28	TCP	3483 > ftp [ACK] Seq=1054243640 Ack=635575868 Win=63738 Len=0
85	29.226549	192.168.2.101	194.94.127.28	TCP	3486 > 1881 [FIN, ACK] Seq=1061544662 Ack=674648791 Win=64174 Len=0
86	29.307715	194.94.127.28	192.168.2.101	TCP	1881 > 3486 [ACK] Seq=674648791 Ack=1061544663 Win=15466 Len=0

Protokollmitschnitt - FTP

→ Wechsel zu und Abfrage von DIR „/home/pohlmann/files“

No.	Time	Source	Destination	Protocol	Info
87	31.384111	192.168.2.101	194.94.127.28	FTP	Request: CWD /home/pohlmann/files
88	31.462144	194.94.127.28	192.168.2.101	FTP	Response: 250 CWD command successful.
89	31.468059	192.168.2.101	194.94.127.28	FTP	Request: PWD
90	31.543283	194.94.127.28	192.168.2.101	FTP	Response: 257 "/home/pohlmann/files" is current directory.
91	31.548290	192.168.2.101	194.94.127.28	FTP	Request: TYPE A
92	31.626119	194.94.127.28	192.168.2.101	FTP	Response: 200 Type set to A.
93	31.638155	192.168.2.101	194.94.127.28	FTP	Request: PASV
94	31.718017	194.94.127.28	192.168.2.101	FTP	Response: 227 Entering Passive Mode (194,94,127,28,7,90).
95	31.722188	192.168.2.101	194.94.127.28	TCP	3487 > 1882 [SYN] Seq=1062308907 Ack=0 Win=64240 Len=0
96	31.722443	192.168.2.101	194.94.127.28	FTP	Request: LIST -a
97	31.798373	194.94.127.28	192.168.2.101	TCP	1882 > 3487 [SYN, ACK] Seq=666009867 Ack=1062308908 Win=15466 Len=0
98	31.798446	192.168.2.101	194.94.127.28	TCP	3487 > 1882 [ACK] Seq=1062308908 Ack=666009868 Win=64676 Len=0
99	31.822221	194.94.127.28	192.168.2.101	TCP	ftp > 3483 [ACK] Seq=635576016 Ack=1054243694 Win=15466 Len=0
100	31.885240	194.94.127.28	192.168.2.101	FTP	Response: 150 Opening ASCII mode data connection for file list
101	31.912678	194.94.127.28	192.168.2.101	FTP-DATA	FTP Data: 56 bytes
102	31.917058	194.94.127.28	192.168.2.101	FTP-DATA	FTP Data: 286 bytes
103	31.917120	192.168.2.101	194.94.127.28	TCP	3487 > 1882 [ACK] Seq=1062308908 Ack=666010211 Win=64334 Len=0
104	31.918505	194.94.127.28	192.168.2.101	FTP	Response: 226 Transfer complete.
105	31.918544	192.168.2.101	194.94.127.28	TCP	3483 > ftp [ACK] Seq=1054243694 Ack=635576094 Win=63512 Len=0
106	31.920561	192.168.2.101	194.94.127.28	TCP	3487 > 1882 [FIN, ACK] Seq=1062308908 Ack=666010211 Win=64334 Len=0
107	32.004112	194.94.127.28	192.168.2.101	TCP	1882 > 3487 [ACK] Seq=666010211 Ack=1062308909 Win=15466 Len=0

Protokollmitschnitt - FTP

→ Wechsel zu und Abfrage von DIR „/home/pohlmann/files/Netzwerkmanagement“

No.	Time	Source	Destination	Protocol	Info
108	35.831355	192.168.2.101	194.94.127.28	FTP	Request: CWD /home/pohlmann/files/Netzwerkmanagement
109	35.912404	194.94.127.28	192.168.2.101	FTP	Response: 250 CWD command successful.
110	35.914516	192.168.2.101	194.94.127.28	FTP	Request: PWD
111	35.993501	194.94.127.28	192.168.2.101	FTP	Response: 257 "/home/pohlmann/files/Netzwerkmanagement" is current d
112	35.994720	192.168.2.101	194.94.127.28	FTP	Request: TYPE A
113	36.073372	194.94.127.28	192.168.2.101	FTP	Response: 200 Type set to A.
114	36.105318	192.168.2.101	194.94.127.28	FTP	Request: PASV
115	36.186686	194.94.127.28	192.168.2.101	FTP	Response: 227 Entering Passive Mode (194,94,127,28,7,91).
116	36.198405	192.168.2.101	194.94.127.28	TCP	3488 > 1883 [SYN] Seq=1063468483 Ack=0 Win=64240 Len=0
117	36.198663	192.168.2.101	194.94.127.28	FTP	Request: LIST -a
118	36.275155	194.94.127.28	192.168.2.101	TCP	1883 > 3488 [SYN, ACK] Seq=682589230 Ack=1063468484 Win=15466 Len=0
119	36.275241	192.168.2.101	194.94.127.28	TCP	3488 > 1883 [ACK] Seq=1063468484 Ack=682589231 Win=64676 Len=0
120	36.292225	194.94.127.28	192.168.2.101	TCP	ftp > 3483 [ACK] Seq=635576261 Ack=1054243767 Win=15466 Len=0
121	36.359724	194.94.127.28	192.168.2.101	FTP	Response: 150 Opening ASCII mode data connection for file list
122	36.365156	194.94.127.28	192.168.2.101	FTP-DATA	FTP Data: 56 bytes
123	36.374235	194.94.127.28	192.168.2.101	FTP-DATA	FTP Data: 733 bytes
124	36.374273	192.168.2.101	194.94.127.28	TCP	3488 > 1883 [ACK] Seq=1063468484 Ack=682590020 Win=63887 Len=0
125	36.375511	194.94.127.28	192.168.2.101	FTP	Response: 226 Transfer complete.
126	36.375586	192.168.2.101	194.94.127.28	TCP	3483 > ftp [ACK] Seq=1054243767 Ack=635576339 Win=64676 Len=0
127	36.462438	194.94.127.28	192.168.2.101	FTP-DATA	FTP Data: 837 bytes
128	36.462538	192.168.2.101	194.94.127.28	TCP	3488 > 1883 [ACK] Seq=1063468484 Ack=682590858 Win=64676 Len=0
129	36.466982	192.168.2.101	194.94.127.28	TCP	3488 > 1883 [FIN, ACK] Seq=1063468484 Ack=682590858 Win=64676 Len=0
130	36.544303	194.94.127.28	192.168.2.101	TCP	1883 > 3488 [ACK] Seq=682590858 Ack=1063468485 Win=15466 Len=0

Protokollmitschnitt - FTP

→ Löschen einer Datei und Abfrage des aktuellen DIR

No.	Time	Source	Destination	Protocol	Info
131	51.887371	192.168.2.101	194.94.127.28	FTP	Request: NOOP
132	51.967210	194.94.127.28	192.168.2.101	FTP	Response: 200 NOOP command successful.
133	52.147505	192.168.2.101	194.94.127.28	TCP	3483 > ftp [ACK] Seq=1054243773 Ack=635576369 Win=64646 Len=0
135	64.340826	192.168.2.101	194.94.127.28	FTP	Request: DELE SNMP_MRTG_22_05_03.pdf
136	64.433651	194.94.127.28	192.168.2.101	TCP	ftp > 3483 [ACK] Seq=635576369 Ack=1054243802 Win=15466 Len=0
137	64.442653	194.94.127.28	192.168.2.101	FTP	Response: 250 DELE command successful.
138	64.443136	192.168.2.101	194.94.127.28	FTP	Request: CWD /home/pohlmann/files/Netzwerkmanagement
139	64.524986	194.94.127.28	192.168.2.101	FTP	Response: 250 CWD command successful.
141	64.606888	194.94.127.28	192.168.2.101	FTP	Response: 257 "/home/pohlmann/files/Netzwerkmanagement" is current d
142	64.615883	192.168.2.101	194.94.127.28	FTP	Request: TYPE A
143	64.694610	194.94.127.28	192.168.2.101	FTP	Response: 200 Type set to A.
144	64.705696	192.168.2.101	194.94.127.28	FTP	Request: PASV
145	64.785212	194.94.127.28	192.168.2.101	FTP	Response: 227 Entering Passive Mode (194,94,127,28,7,92).
146	64.789566	192.168.2.101	194.94.127.28	TCP	3489 > 1884 [SYN] Seq=1070679364 Ack=0 Win=64240 Len=0
147	64.789820	192.168.2.101	194.94.127.28	FTP	Request: LIST -a
148	64.866012	194.94.127.28	192.168.2.101	TCP	1884 > 3489 [SYN, ACK] Seq=707013412 Ack=1070679365 Win=15466 Len=0
149	64.866093	192.168.2.101	194.94.127.28	TCP	3489 > 1884 [ACK] Seq=1070679365 Ack=707013413 Win=64676 Len=0
150	64.883151	194.94.127.28	192.168.2.101	TCP	ftp > 3483 [ACK] Seq=635576566 Ack=1054243875 Win=15466 Len=0
151	64.950192	194.94.127.28	192.168.2.101	FTP	Response: 150 Opening ASCII mode data connection for file list
152	64.953386	194.94.127.28	192.168.2.101	FTP-DATA	FTP Data: 56 bytes
153	64.962424	194.94.127.28	192.168.2.101	FTP-DATA	FTP Data: 733 bytes
154	64.962496	192.168.2.101	194.94.127.28	TCP	3489 > 1884 [ACK] Seq=1070679365 Ack=707014202 Win=63887 Len=0
155	64.964597	194.94.127.28	192.168.2.101	FTP	Response: 226 Transfer complete.
156	64.964622	192.168.2.101	194.94.127.28	TCP	3483 > ftp [ACK] Seq=1054243875 Ack=635576644 Win=64371 Len=0
157	65.051509	194.94.127.28	192.168.2.101	FTP-DATA	FTP Data: 758 bytes
158	65.051615	192.168.2.101	194.94.127.28	TCP	3489 > 1884 [ACK] Seq=1070679365 Ack=707014961 Win=64676 Len=0
159	65.057978	192.168.2.101	194.94.127.28	TCP	3489 > 1884 [FIN, ACK] Seq=1070679365 Ack=707014961 Win=64676 Len=0
160	65.146712	194.94.127.28	192.168.2.101	TCP	1884 > 3489 [ACK] Seq=707014961 Ack=1070679366 Win=15466 Len=0

Abfrage, ob Server noch arbeitet

Löschen der Datei „SNMP_MRTG_22_05_03.pdf“

Protokollmitschnitt - FTP

→ Übertragung einer Datei vom Client zum Server

No.	Time	Source	Destination	Protocol	Info
161	76.627677	192.168.2.101	194.94.127.28	FTP	Request: TYPE I
162	76.705590	194.94.127.28	192.168.2.101	FTP	Response: 200 Type set to I.
163	76.724403	192.168.2.101	194.94.127.28	FTP	Request: PASV
164	76.804915	194.94.127.28	192.168.2.101	FTP	Response: 227 Entering Passive Mode (194,94,127,28,7,93).
165	76.850636	192.168.2.101	194.94.127.28	TCP	3490 > 1885 [SYN] Seq=1073714353 Ack=0 Win=64240 Len=0
166	76.929386	194.94.127.28	192.168.2.101	TCP	1885 > 3490 [SYN, ACK] Seq=708235639 Ack=1073714354 Win=15466 Len=0
167	76.929474	192.168.2.101	194.94.127.28	TCP	3490 > 1885 [ACK] Seq=1073714354 Ack=708235640 Win=64676 Len=0
168	76.929857	192.168.2.101	194.94.127.28	FTP	Request: STOR SNMP_MRTG_22_05_03.pdf
169	77.022998	194.94.127.28	192.168.2.101	FTP	Response: 150 Opening BINARY mode data connection for SNMP_MRTG_22_0
170	77.023963	192.168.2.101	194.94.127.28	FTP-DATA	FTP Data: 1406 bytes
171	77.024001	192.168.2.101	194.94.127.28	FTP-DATA	FTP Data: 54 bytes
172	77.167857	194.94.127.28	192.168.2.101	TCP	1885 > 3490 [ACK] Seq=708235640 Ack=1073715760 Win=15466 Len=0
173	77.167928	192.168.2.101	194.94.127.28	FTP-DATA	FTP Data: 1406 bytes
174	77.167950	192.168.2.101	194.94.127.28	FTP-DATA	FTP Data: 1406 bytes
175	77.174142	194.94.127.28	192.168.2.101	TCP	1885 > 3490 [ACK] Seq=708235640 Ack=1073715814 Win=15466 Len=0
176	77.174199	192.168.2.101	194.94.127.28	FTP-DATA	FTP Data: 1406 bytes
177	77.174216	192.168.2.101	194.94.127.28	FTP-DATA	FTP Data: 1406 bytes
178	77.183488	192.168.2.101	194.94.127.28	TCP	3483 > ftp [ACK] Seq=1054243918 Ack=635576781 Win=64234 Len=0
179	77.382012	194.94.127.28	192.168.2.101	TCP	1885 > 3490 [ACK] Seq=708235640 Ack=1073718626 Win=15466 Len=0
180	77.382114	192.168.2.101	194.94.127.28	FTP-DATA	FTP Data: 1406 bytes
181	77.382135	192.168.2.101	194.94.127.28	FTP-DATA	FTP Data: 1406 bytes
...					
286	81.879903	194.94.127.28	192.168.2.101	TCP	1885 > 3490 [FIN, ACK] Seq=708235640 Ack=1073770017 Win=15466 Len=0
287	81.879939	192.168.2.101	194.94.127.28	TCP	3490 > 1885 [ACK] Seq=1073770017 Ack=708235641 Win=64676 Len=0
288	81.881715	194.94.127.28	192.168.2.101	FTP	Response: 226 Transfer complete.

Aktivierung des „Image“-Modes

set to I.

Passive Mode

Passive Mode (194,94,127,28,7,93).

Aufbau eines Datenkanals (Port 1885)

Datenübertragung - STOR

„SNMP_MRTG_22_05_03.pdf“

Abbau des Datenkanals (Port 1885)

durch den Client

Protokollmitschnitt - FTP

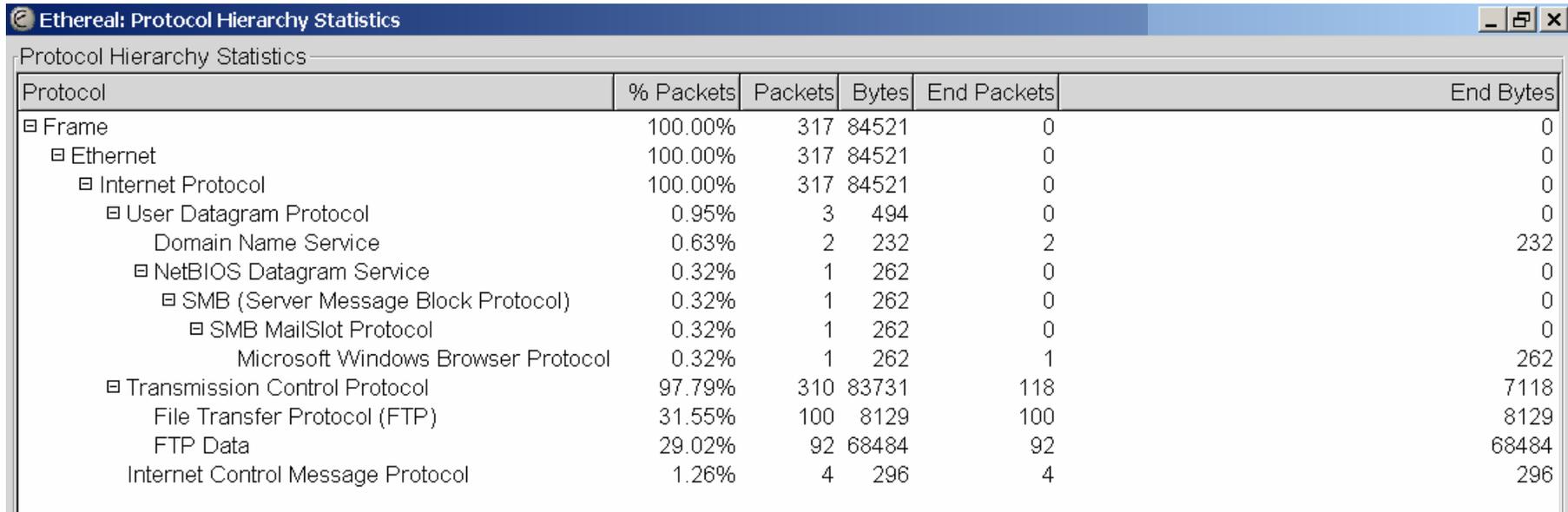
→ Abfrage des aktuellen DIR und Abbau des Steuerkanals

No.	Time	Source	Destination	Protocol	Info
289	81.882639	192.168.2.101	194.94.127.28	FTP	Request: CWD /home/pohlmann/files/Netzwerkmanagement
290	81.963175	194.94.127.28	192.168.2.101	FTP	Response: 250 CWD command successful.
291	81.967225	192.168.2.101	194.94.127.28	FTP	Request: PWD
292	82.045507	194.94.127.28	192.168.2.101	FTP	Response: 257 "/home/pohlmann/files/Netzwerkmanagement" is current d
293	82.050951	192.168.2.101	194.94.127.28	FTP	Request: TYPE A
294	82.128752	194.94.127.28	192.168.2.101	FTP	Response: 200 Type set to A.
295	82.140841	192.168.2.101	194.94.127.28	FTP	Request: PASV
296	82.218853	194.94.127.28	192.168.2.101	FTP	Response: 227 Entering Passive Mode (194,94,127,28,7,94).
297	82.224920	192.168.2.101	194.94.127.28	TCP	3491 > 1886 [SYN] Seq=1075117101 Ack=0 Win=64240 Len=0
298	82.225185	192.168.2.101	194.94.127.28	FTP	Request: LIST -a
299	82.299691	194.94.127.28	192.168.2.101	TCP	1886 > 3491 [SYN, ACK] Seq=728375425 Ack=1075117102 Win=15466 Len=0
300	82.299789	192.168.2.101	194.94.127.28	TCP	3491 > 1886 [ACK] Seq=1075117102 Ack=728375426 Win=64676 Len=0
301	82.324439	194.94.127.28	192.168.2.101	TCP	ftp > 3483 [ACK] Seq=635576972 Ack=1054243991 Win=15466 Len=0
302	82.386092	194.94.127.28	192.168.2.101	FTP	Response: 150 Opening ASCII mode data connection for file list
303	82.389224	194.94.127.28	192.168.2.101	FTP-DATA	FTP Data: 56 bytes
304	82.398805	194.94.127.28	192.168.2.101	FTP-DATA	FTP Data: 733 bytes
305	82.398889	192.168.2.101	194.94.127.28	TCP	3491 > 1886 [ACK] Seq=1075117102 Ack=728376215 Win=63887 Len=0
306	82.400062	194.94.127.28	192.168.2.101	FTP	Response: 226 Transfer complete.
307	82.400086	192.168.2.101	194.94.127.28	TCP	3483 > ftp [ACK] Seq=1054243991 Ack=635577050 Win=63965 Len=0
308	82.488342	194.94.127.28	192.168.2.101	FTP-DATA	FTP Data: 837 bytes
309	82.488448	192.168.2.101	194.94.127.28	TCP	3491 > 1886 [ACK] Seq=1075117102 Ack=728377053 Win=64676 Len=0
310	82.493220	192.168.2.101	194.94.127.28	TCP	3491 > 1886 [FIN, ACK] Seq=1075117102 Ack=728377053 Win=64676 Len=0
311	82.571555	194.94.127.28	192.168.2.101	TCP	1886 > 3491 [ACK] Seq=728377053 Ack=1075117103 Win=15466 Len=0
312	86.990925	192.168.2.101	194.94.127.28	FTP	Request: QUIT
313	87.068856	194.94.127.28	192.168.2.101	FTP	Response: 221 Goodbye.
314	87.068918	194.94.127.28	192.168.2.101	TCP	ftp > 3483 [FIN, ACK] Seq=635577064 Ack=1054243997 Win=15466 Len=0
315	87.068970	192.168.2.101	194.94.127.28	TCP	3483 > ftp [ACK] Seq=1054243997 Ack=635577065 Win=63951 Len=0
316	87.077973	192.168.2.101	194.94.127.28	TCP	3483 > ftp [FIN, ACK] Seq=1054243997 Ack=635577065 Win=63951 Len=0
317	87.155842	194.94.127.28	192.168.2.101	TCP	ftp > 3483 [ACK] Seq=635577065 Ack=1054243998 Win=15466 Len=0

Abbau des Steuerkanals (Port 3483)

Protokollmitschnitt - FTP

→ Statistik



Ethernet: Protocol Hierarchy Statistics

Protocol	% Packets	Packets	Bytes	End Packets	End Bytes
Frame	100.00%	317	84521	0	0
Ethernet	100.00%	317	84521	0	0
Internet Protocol	100.00%	317	84521	0	0
User Datagram Protocol	0.95%	3	494	0	0
Domain Name Service	0.63%	2	232	2	232
NetBIOS Datagram Service	0.32%	1	262	0	0
SMB (Server Message Block Protocol)	0.32%	1	262	0	0
SMB MailSlot Protocol	0.32%	1	262	0	0
Microsoft Windows Browser Protocol	0.32%	1	262	1	262
Transmission Control Protocol	97.79%	310	83731	118	7118
File Transfer Protocol (FTP)	31.55%	100	8129	100	8129
FTP Data	29.02%	92	68484	92	68484
Internet Control Message Protocol	1.26%	4	296	4	296

- Summe der TCP-Verbindungen = 9
 - Steuerkanal (Port 3483)
 - Datenkanal (Port 1879 bis 1886)
- Der Server sendet das letzte Datenpaket mit FIN=1.
- Die Kommandos REST und NOOP deuten auf Synchronisationsprobleme hin.

Inhalt

- Ziele und Einordnung
- Übersicht
- Datenformate und Datentypen
- Datenübertragung
- FTP-Kommandos
- Protokollmitschnitt
- **Zusammenfassung**

File Transfer Protocol (FTP)

→ Zusammenfassung

- **FTP ist das Basisprotokoll für den Dateiaustausch** - auch zwischen völlig unterschiedlichen Rechnerplattformen und Betriebssystemen.
- FTP besteht im Gegensatz zu anderen TCP-basierten Protokollen nicht aus einer einzigen TCP-Verbindung, sondern aus zwei parallelen Verbindungen, dem **Steuerkanal**, der die Signalisierung (Verbindungsauf- und -abbau, was übertragen werden soll, usw.) vornimmt, und dem **Datenkanal**, über den die eigentlichen Daten übertragen werden.

File Transfer Protocol (FTP)

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

norbert.pohlmann@informatik.fh-gelsenkirchen.de

