Arbeitsblatt 1 – Protokolle der Anwendungsschicht

Bilde eine Gruppe mit einem deiner Klassenkameraden. Jede Gruppe soll eine **Präsentation** zu einem der folgenden Themen vorbereiten. Jede Gruppe soll sich ebenfalls **fünf offene Fragen (keine Ja/Nein-Fragen, kein Multiple Choice)** überlegen die ein aufmerksamer Zuhörer am Ende der Präsentation beantworten können muss.

Dauer der Präsentation: 15 - 20 Minuten

Abgabetermin für die Folien und Fragen: 28.09.2025 – 23:59

Bewertung: Deine Präsentation wird zur Teilbewertung der K1-Kompetenz benutzt. Eine Evaluation mit ausgewählten Schülerfragen bildet den zweiten Teil dieser Bewertung.

Bewertungskriterien für die Präsentation:

- Inhalt
- Beachtung der Zeitvorgabe
- Qualität des Vortrags
- Qualität der gewählten Fragen

Themenübersicht

- Thema 1 – HTTP, HTTPS
- Thema 2 – FTP, NFS, Samba
- Thema 3 – Telnet, SSH
- Thema 4 – SMTP/IMAP/POP
- Thema 5 – DNS
- Thema 6 – BitTorrent und andere File Sharing Protokolle

Inhalt

Es ist dir und deiner Gruppe frei überlassen, wie ihr euren Vortrag inhaltlich gestalten werdet. Wählt die Punkte aus, die am besten zu eurem Thema passen:

- Anwendungsbeispiele (En: Use Cases)
  - Wo wird das Protokoll im Alltag / in der IT-Infrastruktur eingesetzt?
    Beispiele: HTTP bei Webseiten, SMTP bei E-Mails, FTP für Datentransfer, DNS für Namensauflösung usw.
- Headerformat samt wichtiger Informationen
  - Aufbau des Protokoll-Headers (z. B. Quelle/Ziel-Port, Flags, Sequenznummer, Befehlsfelder).
    Relevante Felder erklären (nicht jedes Bit, nur die Kerninfos).
- Nachrichtenformat und Nachrichtenaustausch
  - Ablaufdiagramm oder Sequenzdiagramm für einen typischen Austausch.
    Beispiel: 3-Way-Handshake bei TCP, HELO/EHLO im SMTP, GET/Response im HTTP.
- Konfigurationsbeispiele
  - CLI-Beispiele (Router/Switch/Linux).
    Wie richte ich einen einfachen Server/Client ein?

- Beispiele von benötigten Benutzerbefehlen zur Bearbeitung eines häufigen Anwendungsbeispiels
    - Typische Kommandos, die ein Anwender eintippt.
      z. B. ftp, ssh, telnet, nslookup, curl, ping, dig.
- Vergleich mit ähnlichen Protokollen
    - Was unterscheidet SMTP/IMAP/POP?
      HTTP vs. HTTPS, FTP vs. SFTP/NFS/Samba, Telnet vs. SSH.
- Demo in Packet Tracer
    - Umsetzung der Aufgabe praktisch zeigen.
      Mit Screenshots, CLI-Ausgaben oder einer Live-Vorführung.
- Demo mit einer VM
    - Falls eine Gruppe VMs (z. B. Ubuntu) nutzen kann: Real-Setup (Apache2, OpenSSH, Bind9, Postfix, etc.).
- Demo mit Wireshark
    - Pakete mitschneiden, Header/Handshake sichtbar machen.
      Wichtig: zeigen, welche Felder im Protokoll auftauchen.
- Datenfluss einer Kommunikation durch die verschiedenen OSI-Schichten darstellen
    - Vom Application Layer bis zum Physical Layer durchspielen.
      Z. B. DNS: Anfrage → TCP/UDP → IP → Ethernet → Kabel.
      Am besten als Schaubild.

Dateibenennungen (Vorschlag)

- T1_HTTP-HTTPS_Aufgabe.pkt
- T2_FTP_ShareSim_Aufgabe.pkt
- T3_Telnet-SSH_SecureMgmt.pkt
- T4_SMTP-POP_MailLab.pkt
- T5_DNS_SplitHorizon.pkt
- T6_P2P-Policy_Simulation.pkt

Abgabe-Hinweise

- Kurze **Readme** pro Aufgabe (IP-Plan, Passwörter, Befehlsauszüge).
- **Screenshots** der erfolgreichen Tests (Browser/FTP/Mail/CLI).
- Konfig-Snippets mit: show run | s interface, show access-lists, show ip route, ggf. show policy-map interface.

Thema 1 – HTTP & HTTPS

Ziel: Ein Intranet-Webserver bereitstellen, HTTP→HTTPS-Umleitung testen, und per ACL nur ein Subnetz zulassen.

Topologie:

- R1 (Router) zwischen zwei Netzen
- SW1 (Access Switch)
- PC1 (Client im Netz 192.168.10.0/24)
- PC2 (Client im Netz 192.168.20.0/24)
- Srv-WEB (Server mit HTTP & HTTPS aktiviert, im 192.168.10.0/24)

Schritte (Kurzfassung):

1. IP-Adressierung auf R1, PCs, Server konfigurieren; Default-Gateway setzen.
2. Auf **Srv-WEB** in den Dienste-Tabs **HTTP** und **HTTPS** aktivieren; eine Test-Startseite anlegen.
3. Auf R1 NAT-Overload (PAT) einrichten (optional, falls Internet-Cloud genutzt wird).
4. **ACL** auf R1: Nur 192.168.10.0/24 darf auf Srv-WEB TCP/443; HTTP (80) soll vom Server auf HTTPS umleiten (Server-Option „HTTPS only“ oder Redirect-Seite).
5. Test: Von PC1 per https://<Server-IP> erreichbar; http:// wird umgeleitet. Von PC2 ist Zugriff geblockt.

Abnahme/Checks:

- PC1: Browser → HTTPS ok, HTTP → Redirect/Block wie konfiguriert.
- PC2: Zugriff verweigert (ACL-Hit-Counter steigt).
- (Optional) Show-Befehle: show access-lists, show ip interface, show ip nat translations.

Thema 2 – FTP, NFS, Samba

Hinweis: Packet Tracer unterstützt **FTP** nativ. **NFS/SMB** (Samba) sind nicht emuliert – wir simulieren Dateifreigaben mit FTP-Ordnern und Zugriffsrechten.

Ziel: Benutzerbasierter FTP-Zugriff mit Lese/Schreib-Rechten, anonymer Read-Only-Zugang, und Zugriffsbeschränkung per ACL.

Topologie:

- R1, SW1
- Srv-FTP (FTP-Dienst aktiv, im 10.10.10.0/24)
- PC-Admin, PC-User1, PC-Guest im selben LAN

Schritte:

1. IP-Grundkonfig (Srv & PCs). Default-GW auf R1.
2. Auf **Srv-FTP**:
    - Benutzer admin (RW), user1 (RW), guest (RO/anonymous).
    - Zwei Verzeichnisse: /public (RO anonym), /projects (RW nur für angemeldete Nutzer).
3. Auf R1 (optional): erlaube FTP nur aus 10.10.10.0/24; blocke von anderem Subnetz.
4. Tests:
    - PC-Guest: Anonymer Login → /public lesbar, Upload verboten.
    - PC-User1: Auth-Login → /projects Upload/Download erlaubt.
    - PC-Admin: Kann Dateien verwalten.

Abnahme/Checks:

- FTP-Client im PT: username/password und Datei-Transfer demonstrieren (Screenshot/Beleg).
- ACL-Trefferzähler zeigt Block/Permit.

Thema 3 – Telnet & SSH

Ziel: Gerätemanagement über SSH absichern; Telnet deaktivieren; lokales User-DB & Banner; Key-Länge ≥ 1024.

Topologie:

- R1, SW1
- PC-NOC (Mgmt-Client)

Schritte:

1. Basis-IP auf R1/SW1 (SVI auf SW1, z. B. VLAN 10). Default-GW.
2. Lokale Benutzer auf R1 & SW1: admin mit Secret.
3. SSH aktivieren:
    - ip domain-name lab.local
    - crypto key generate rsa modulus 2048
    - ip ssh version 2
    - vty-Lines: transport input ssh, login local, exec-timeout, logging synchronous
    - Banner MOTD.
4. Telnet explizit deaktivieren.
5. Test: Von PC-NOC per **SSH** verbinden; Telnet scheitert.

Abnahme/Checks:

- show ip ssh, show running-config | s vty, SSH-Login erfolgreich, Telnet verweigert.

Thema 4 – SMTP / IMAP / POP

Hinweis: In PT sind **SMTP & POP3** verfügbar; **IMAP** ist je nach Version eingeschränkt. Aufgabe nutzt SMTP + POP3. (Wenn IMAP sichtbar ist, gerne zusätzlich aktivieren/testen.)

Ziel: Mailserver einrichten, zwei Domains, Benutzerpostfächer, Clients senden/empfangen; Relay-Schutz.

Topologie:

- R1
- Srv-MAIL (SMTP + POP3, optional IMAP), 192.168.50.2/24
- PC-Alice (alice@contoso.local), PC-Bob (bob@fabrikam.local)

Schritte:

1. IP-Konfig & DNS-Einträge auf **Srv-DNS** (optional) für mail.contoso.local, mail.fabrikam.local; oder Clients mit direkter Server-IP.
2. **Srv-MAIL**:
    - Domains anlegen: contoso.local, fabrikam.local
    - Benutzer: alice, bob (Passwörter setzen)
    - SMTP aktiv; POP3 aktiv; (IMAP falls vorhanden)
    - „Relay only for local users/auth“ aktivieren (falls Option vorhanden; sonst per Design notieren).
3. Mail-Clients auf PCs konfigurieren (SMTP-Server, POP3-Server, Accounts).
4. Tests: Alice → Bob Mail senden; Bob abholen; Antwort zurück.

Abnahme/Checks:

- Gesendete/empfangene Mails im Client sichtbar (Screenshots).
- (Optional) Versuch zu relayn ohne Auth scheitert.

Thema 5 – DNS

Ziel: Autoritativer DNS-Server für eine Zone, Forwarder, A/CNAME/MX/E-inträge, und Split-Horizon (intern vs. extern).

Topologie:

- R1
- Srv-DNS-INT (interner DNS für zone corp.local)
- Srv-DNS-EXT (externer DNS für corp.example)
- PC-INT (im LAN), PC-EXT (anderes Netz)

Schritte:

1. IP-Konfig für beide Zonen. R1 routet zwischen Netzen.
2. **Srv-DNS-INT:** Zone corp.local
    - www → 10.0.0.10 (interner Web)
    - CNAME intranet → www
    - MX für corp.local → mail.corp.local
    - Forwarder auf externen Resolver (oder Srv-DNS-EXT).
3. **Srv-DNS-EXT:** Zone corp.example
    - www → 203.0.113.10 (simulierter externer Web)
4. **Split-Horizon:**
    - PC-INT nutzt Srv-DNS-INT (sieht interne IPs).
    - PC-EXT nutzt Srv-DNS-EXT (sieht externe IPs).
5. Tests: nslookup intranet.corp.local von PC-INT → interne IP. Von PC-EXT unbekannt. www.corp.example löst extern auf.

Abnahme/Checks:

- nslookup/dig (PT hat nslookup) Belege; Zugriff passt zum Standort.

Thema 6 – BitTorrent & andere File-Sharing-Protokolle (Simulation)

Hinweis: BitTorrent/Peers sind in PT **nicht nativ**. Wir simulieren P2P-Muster mit mehreren Clients/„Seedern“ via **FTP/HTTP** und erzwingen/überwachen Policies mit **ACLs** & **QoS-Marking** (falls Version unterstützt).

Ziel: P2P-ähnlichen Datenverkehr modellieren (viele Peers, viele gleichzeitige Streams), Traffic-Kontrolle umsetzen:

- Blockiere bekannte P2P-Ports (z. B. TCP/UDP 6881–6889) am WAN-Edge.
- Erlaube „legitime“ Dateiübertragung (FTP/HTTPS).
- Rate-Limit oder Priorisierung für Business-Dienste (HTTP(S) Priorität > FTP).

Topologie:

- R-EDGE (WAN-Router)
- SW-LAN
- Srv-DL1/Srv-DL2 (Download-Server mit HTTP/FTP)
- PC-PeerA/B/C/D (Clients)

Schritte:

1. IP-Adressierung & Routing.
2. Auf Srv-DL1/DL2 HTTP & FTP aktivieren; Dateien bereitstellen.
3. Auf R-EDGE **Extended ACL**:
    - Deny TCP/UDP 6881–6889 (P2P-typische Ports) inbound vom LAN ins WAN.
    - Permit HTTP/HTTPS/FTP.
    - Standard-Deny am Ende.
4. Tests:
    - Versuche, von PCs „P2P-Ports“ mit generiertem PDU (oder manuell) zu erreichen → sollte droppen (ACL-Counter).
    - Gleichzeitige Downloads via HTTP (schneller) vs. FTP (gedrosselt/prioritätsniedriger, wenn QoS aktiv).
    - Nachweis per show access-lists, show policy-map interface.

Abnahme/Checks:

- ACL blockt die P2P-Portbereiche; legitime Dienste funktionieren.
- (Wenn QoS genutzt) Policy-Counters steigen; sichtbarer Unterschied bei parallelen Transfers.