Unterrichtseinheit 7:

Konfigurieren von Remotezugriff

Über Remotezugriff können Benutzer an einem Remotestandort eine Verbindung zu Ihrem Netzwerk herstellen.

Aufbau einer RAS-Verbindung (siehe Kapitel 7 / Seite 3)

Remotezugriffsvorgang
Der RAS-Server, ein Computer, auf dem Windows2000 Server und der Routing und RAS-Dienst ausgeführt werden, authentifiziert Benutzer und RAS-Sitzungen.
Der RAS-Server fungiert hierbei als ein Gateway, indem er Daten zwischen dem Client und dem LAN übertragt.

RAS-Verbindungsarten

- **DFÜ-Verbindungen:**
  Um über DFÜ-Remotezugriff eine Verbindung zum Netzwerk herzustellen, verwendet ein RAS-Client ein Kommunikationsnetzwerk, wie beispielsweise ein öffentlich geschaltetes Datennetzwerk (Public Switched Telephone Network PSTN) um eine physikalische Verbindung zu einen Anschluss an einem RAS-Server im privaten Netzwerk zu erstellen. Hierbei erfolgt das Einwählen beim RAS-Server normalerweise über ein Modem oder einen ISDN-Adapter (pro Verbindung).
  Es ergeben sich hierfür beträchtliche Kosten für Ferngespräche.

- **VPN-Verbindungen:**
  Sichere Remote-Verbindung über das Internet durch eine verschlüsselte virtuelle Punkt-zu-Punkt-Verbindung zu einem VPN-Gateway im privaten Netzwerk. Der Benutzer stellt die Verbindung zum Internet über einen Internetdienstanbieter (Internet Service Provider ISP) her.
  Die Kosten für Ferngespräche werden dadurch gesenkt und der Zugang ist für n Clients bereitgestellt.

Datentransportprotokoll

Routing und RAS in Windows2000 verwendet sowohl RAS- (für WAN-Verbindungen), als auch LAN-Protokolle (für Datenübertragung innerhalb des LANs), damit Clients die Verbindung zu RAS-Servern herstellen können.

Schicht 5	RAS Protokoll		PPP, SLIP		
Schicht 4 Schicht 3	Netzwerk Protokolle	Transport Vermittlung	IPX SPX	NetBEUI	TCP, UDP IP

RAS-Protokolle	LAN-Protokolle
PPP (Standard)	TCP/IP
SLIP (Serial Line Internetprotokoll) (alt, nur für Client)	NWLink
Microsoft RAS (alt)	NetBEUI
ARAP (nur Serverkomponente für Apple-Client)	AppleTalk

VPN-Protokoll

VPN-Protokolle kapseln Datenpakete in PPP-Datenpakete ein und können damit eine sichere verschlüsselte Übertragung über das Internet gewährleisten.

Der Weg der Daten kann folgendermaßen interpretiert werden:
Daten vom Sender → VPN → PPP → TCP/IP → WWW → TCP/IP → PPP → VPN → Übertragene Daten am Empfänger

VPNs verwenden entweder PPTP oder L2TP für den Verbindungsaufbau. Windows2000 aktiviert diese Protokolle automatisch, wenn während der Installation von Routing und RAS VPN-Anschlüsse erstellt werden.

PPTP (MS-spezialisiert)	L2TP (universell)
Netzwerk mus IP-basiert sein	Netzwerk kann IP-, Frame Relay-, x.25- oder ATM-basiert sein
Keine Headerkompression	Headerkompression
Keine Tunnelauthentifizierung	Tunnelauthentifizierung (dadurch werden sowohl die Kennwörter, als auch die Daten geschützt)
PPP-Verschlüsselung integriert	Verwendet IPSec-Verschlüsselung

Konfigurieren eingehender Verbindungen

Verbindungen werden folgendermaßen konfiguriert:
- In einer Domäne: Setup-Assistent für den Routing- und RAS-Server
- Bei einer Workstation oder Server ohne Domäne: mit Netzwerkverbindungsassistent

Konfigurieren eingehender DFÜ-Verbindungen (serverseitig)
Installieren und konfigurieren aller Protokolle, die von den DFÜ-Benutzer verwendet werden (TCP/IP, NWLink, NetBEUI, AppleTalk) → Programme → Verwaltung → Routing und RAS → mit rechter Maustaste auf den zu konfigurierenden Server klicken → Routing und RAS konfigurieren und aktivieren → Weiter → Allgemeine Konfigurationen → RAS-Server → Weiter → Remoteclientprotokolle → alle Transportprotokolle überprüfen → Weiter → Netzwerkauswahl → Weiter → IP-Adresszuweisung (eine Option auswählen) → Mehrere RAS-Server verwalten → Weiter → Fertig stellen

Konfiguration von VPN-Anschlüssen

Wird Routing und RAS zum ersten Mal gestartet, so erstellt Windows2000 automatisch fünf PPTP- und fünf L2TP-Anschlüsse (Ports). Die Anzahl der virtuellen Anschlüsse (kann auf eine Zahl erhöht oder verringert werden, die für die dem RAS-Server zur Verfügung stehende Bandbreite geeignet ist), die für jeden RAS-Server zur Verfügung stehen, wird nicht durch die Verfügbarkeit der Hardware beschränkt.

Anmerkung:
Wird im Setup-Assistenten für den Routing- und RAS-Server die Option VPN-Server ausgewählt, so erstellt Windows 2000 automatisch 128PPTP- und 128L2TP-Anschlüsse.

Programme → Verwaltung → Routing und RAS → Eigenschaften von Ports → Gerät auswählen → Konfigurieren → „RAS-Verbindungen (nur eingehend)" aktivieren → in den Dialogfeldern „Gerät konfigurieren" und „Eigenschaften von Ports" auf „OK" klicken

Konfigurieren von Modem- und Kabelanschlüssen

Wird Routing und RAS zum ersten Mal ausgeführt, erkennt Windows2000 automatisch alle installierten Modems und erstellt Modemanschlüsse für diese, sowie auch für alle erkannten parallelen oder seriellen Kabelverbindungen.

Programme → Verwaltung → Routing und RAS → Eigenschaften von Ports → Konfigurieren (Modem-, parallele und serielle Anschlüsse werden einzeln aufgeführt und können entweder einzeln oder gemeinsam konfiguriert werden) → Gerät konfigurieren → Kontrollkästchen „RAS-Verbindung (nur eingehend)" aktivieren → in den Dialogfeldern „Gerät konfigurieren" und „Eigenschaften von Ports" auf „OK" klicken

Konfigurieren von Benutzereinwähleinstellungen

Auf einen alleinstehenden Server werden die Einwähleinstellungen konfiguriert in:
→ Einwahl → Eigenschaften → Snap-In → Lokale Benutzer und Gruppen.
Bei Active Directory werden die Einwähleinstellungen konfiguriert in:
→ Einwahl → Eigenschaften → Active Directory-Benutzer und -Computer.

Aktivieren des Verifizierens der Anruferkennung

Wenn die Option Anruferkennung verifizieren ausgewählt ist, überprüft der Server die Rufnummer des Anrufers. Um die Verbindung herstellen zu können müssen alle Teile der Verbindung die Anruferkennung unterstützen

- ISDN-Rufnummer
- Hardware
- Netz
- Router

Konfigurieren ausgehender Verbindungen (Client)

Es gibt drei grundlegende Arten von ausgehenden Verbindungen:

- DFÜ-Verbindungen
  - Verbindungen zu einem privaten Netzwerk oder Server
  - Verbindung zu einem ISP
- Verbindungen zu einem VPN
- Direkte Verbindungen zu einem anderen Computer über Kabel

Es werden sämtliche ausgehende Verbindungen unter Windows 2000 mit Hilfe des Netzwerkverbindungs-Assistenten konfiguriert.

Tipp:
Der Assistent für das Microsoft Verbindungs-Manager-Verwaltungskit (Connection Manager Administration Kit, CMAK) vereinfacht den Anpassungsvorgang, da hiermit benutzerdefinierte Elemente für den Dienst angegeben werden können (z.B. DFÜ-Standort, Rufnummern, VPN-Einstellungen...). Auf dieser Basis wird anschließend ein benutzerdefiniertes Installationspaket erstellt.

Erstellen einer DFÜ-Verbindung Kap

Neue ausgehende Verbindungen werden folgendermaßen erstellt:
*Programme → Einstellungen → Netzwerk- und DFÜ-Verbindungen → Neue Verbindung erstellen → Weiter → Entweder „**In ein privates Netzwerk einwählen**“ (entweder ISP für eine Internetverbindung oder Modems eines privaten Netzwerkes) oder auf „**In das Internet einwählen**“ (Assistent für den Internetzugang) auswählen → „**für alle Benutzer verwenden**“ (Kontrollkästchen „**Gemeinsame Nutzung der Internetverbindung aktivieren**“ anklicken) oder „**nur selbst verwenden**“ auswählen → Weiter → Namen eingeben → Fertig stellen*

Herstellen einer Verbindung zu einem virtuellen privaten Netzwerk VPN

Erstellen einer Verbindung zu einem VPN (DFÜ zum ISP muss schon eingerichtet sein):
*Programme → Einstellungen → Netzwerk- und DFÜ-Verbindungen → Neue Verbindung erstellen → Verbindung mit einem privaten Netzwerk über das Internet herstellen → Weiter → Nachfolgende Schritte ausführen → Weiter → Namen und IP eingeben → Weiter → „**für alle Benutzer verwenden**“ (Kontrollkästchen „**Gemeinsame Nutzung der Internetverbindung aktivieren**“ anklicken) oder „**nur selbst verwenden**“ auswählen → Weiter → Namen eingeben → Fertig stellen*

Erstellen einer direkten Verbindung über ein Kabel:
(Ist der Computer Mitglied einer Domäne, sollte Routing und RAS verwendet werden)
*Programme → Einstellungen → Netzwerk- und DFÜ-Verbindungen → Neue Verbindung erstellen → Direkt mit anderem Computer verbinden → Weiter → Nachfolgende Schritte ausführen → Weiter → „**für alle Benutzer verwenden**“ (Kontrollkästchen „**Gemeinsame Nutzung der Internetverbindung aktivieren**“ anklicken) oder „**nur selbst verwenden**“ auswählen → Weiter → Namen eingeben → Fertig stellen*

Konfigurieren von Mehrfachverbindungen

Mehrfachverbindungen (arbeitet mit dem Protokoll PPP Multilink zusammen) versetzen den Computer in die Lage, zwei oder mehr Kommunikationsanschlüsse wie einen einzigen Anschluss mit größerer Bandbreite zu verwenden.

PPP Multilink
Das Protokoll PPP Multilink kombiniert die Bandbreite von zwei oder mehr Kommunikationsverbindungen, um eine einzige virtuelle Datenverbindung zu erstellen und so eine skalierbare Bandbreite basierend auf den Datenmengen bereitzustellen. Allerdings muss die Funktion Mehrfachverbindung sowohl auf dem Client als auch auf dem RAS-Server aktiviert sein.

BAP
Mit BAP wird die Funktion Mehrfachverbindung erweitert, indem Verbindungen bei Bedarf dynamisch hinzugefügt oder getrennt werden.

Konfigurieren von Mehrfachverbindungen und BAP auf dem RAS-Server

Durch das Aktivieren (auf der Registerkarte PPP im Dialogfeld Eigenschaften jedes RAS-Servers) von „Mehrfachverbindungen“ und „Dynamische Bandbreitensteuerung mit BAP oder BACP“ wird das Protokoll PPP Multilink, bzw. BAP aktiviert.

Konfigurieren von Mehrfachverbindungen und BAP auf dem RAS-Client

Programme → Einstellungen → Netzwerk- und DFÜ-Verbindungen → mit rechter Maustaste auf die zu aktivierende Verbindung klicken → Eigenschaften → Allgemein → Kontrollkästchen, die in Frage kommen auswählen → Optionen → Mehrere Geräte → Nachfolgende Schritte auswählen → Konfigurieren → OK

Konfigurieren von Authentifizierungsprotokollen

RAS-Server arbeiten mit Authentifizierung, um die Identität der Benutzer zu bestimmen.

Standardmäßige Authentifizierungsprotokolle

PAP (Password Authentication Protocol)	Niedrig	Verwendet unverschlüsselte Kennwörter
SPAP (Hardware) (Shiva Password Authentication Protocol)	Mittel	Bidirektional reversibler Verschlüsselungsmechanismus (Kennwortdaten werden verschlüsselt)
CHAP (auch MD5) (Challenge Authentication Protocol)	Mittel	Unidirektionales Verschlüsselungsschema MD5, um die Antwort zu verschlüsseln
MS-CHAP (auch MPPE) (Microsoft Challenge Handshake Authentication Protocol)	Hoch	Unidirektional verschlüsseltes Kennwort (auf einem Windows2000 RAS-Server ist dieses Protokoll standardmäßig aktiviert) (ab Win98/WinNT)
MS-CHAP v2 (neue Version von MS-CHAP) (Microsoft Challenge Handshake Authentication Protocol)	Hoch	Bidirektionale Authentifizierung, leistungsfähigere Schlüssel für die Verschlüsselung (nur für VPN bei Win98/WinNT)

Extensible Authentication-Protokoll (flexibel) EAP

EAP ermöglicht für RAS-Server die benutzerdefinierte Authentifizierung. Hierbei verhandeln Client und RAS-Server die exakte Authentifizierungsmethode, die verwendet werden soll.

EAP unterstützt folgende Protokolle:

- MD5-CHAP
- Transport Layer Security (TLS)
- Weitere Authentifizierungsmethoden von Drittanbietern

Unter Verwendung der EAP-Anwendungsprogrammierungsschnittstellen (Application Programming Interfaces, APIs) für Techniken wie beispielsweise Tokencards, Smartcards, biometrische Hardware (z.B.: Netzhaut- oder Fingerabdruckscanner) sowie für Authentifizierungstechniken entwickeln, die heute noch nicht bereitgestellt werden.

Konfigurieren von Verschlüsselungsprotokollen (für die Daten)

Die Datenverschlüsselung bietet Sicherheit durch das Verschlüsseln oder Codieren der Daten, die zwischen einem RAS-Client und einem RAS-Server übertragen werden. Die Verschlüsselungsprotokolle werden auf der Registerkarte **Verschlüsselung** im Dialogfeld **Einwählprofil bearbeiten** der RAS-Richtlinie aktiviert.

Wichtig:
Die Datenverschlüsselung steht nur zur Verfügung, wenn als Authentifizierungsprotokoll MS-CHAP (v1 oder v2) oder TLS (ein EAP-Protokoll) verwendet wird!

Es gibt zwei Methoden zum Verschlüsseln der Daten: MPPE und IPSec.

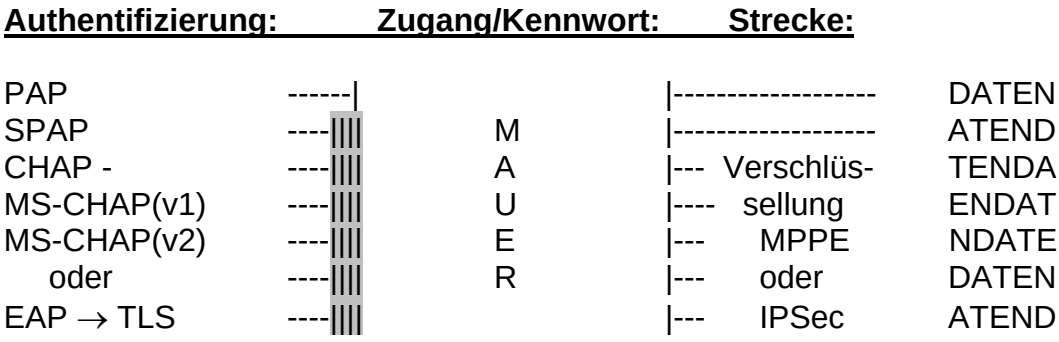
Verschlüsseln von Daten mit Hilfe von MPPE (Microsoftspezifische Lösung)

Mit MPPE werden Daten verschlüsselt, die zwischen einer PPTP-Verbindung und dem VPN-Server übertragen werden. Hierbei stehen drei Verschlüsselungsebenen zur Verfügung:

- stärkste Verschlüsselung (128 Bit)
- starke Verschlüsselung (56 Bit)
- Basisverschlüsselung (40 Bit)

Verschlüsseln von Daten mit Hilfe von IPSec (universelle Lösung)

IPSec bietet einen Rahmen für offene Standards, mit denen eine sichere private Kommunikation über IP-Netzwerke mit Hilfe von Verschlüsselung sichergestellt wird. Clients verhandeln eine Sicherheitszuordnung, die als privater Schlüssel zum Verschlüsseln des Datenflusses dient. Zum Konfigurieren der IPSec-Sicherheitsdienste (Schutz für die meisten Arten des Netzwerkverkehrs) werden IPSec-Richtlinien verwendet.

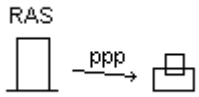


Konfiguration von Routing und RAS für die DHCP-Integration

Clients können vom RAS-Server auf drei verschiedene Arten ihre IP-Adresse erhalten:

1. Statische IP-Adresse

Die IP-Adresse wird auf dem Clientcomputer konfiguriert. (Nicht für DFÜ-Netzwerk geeignet)

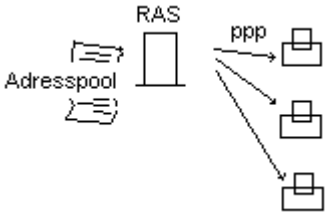


2. Aus einem Bereich von IP-Adressen

Ein RAS-Server kann eine IP-Adresse aus einem konfigurierten Adressbereich zuweisen. Es muss allerdings sichergestellt werden, dass er über eine ausreichende Anzahl von IP-Adressen verfügt, die ihm exklusiv für die Zuweisung zu Clientcomputern zugeordnet sind.

Positiv: Sicherheit durch getrennte Adressbereiche

Negativ: doppelte Verwaltung

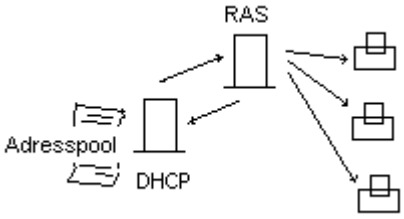


3. Vom DHCP-Server

Ein RAS-Server kann IP-Adressen von einem DHCP-Server (im 10er-Pack) erhalten und diese dann Clients zuweisen. Ein RAS-Server benötigt nur so viele IP-Adressen, wie gleichzeitig verbundene Clients vorhanden sind.

Positiv: gemeinsame Verwaltung

Negativ: Sicherheitslücke bei Ausfall des DHCP-Servers



Der RAS-Server wird zum Erhalt von IP-Adressen von einem DHCP-Server folgendermaßen konfiguriert :

Programme → Einstellungen → Systemsteuerung → Verwaltung → Routing und RAS → mit rechter Maustaste auf den entsprechenden Server klicken → Eigenschaften → IP - DHCP → Adapter → OK