



# Rollen von Domänencontrollern (DC's)

---



# Multimastermodus

---



# Multimastermodus

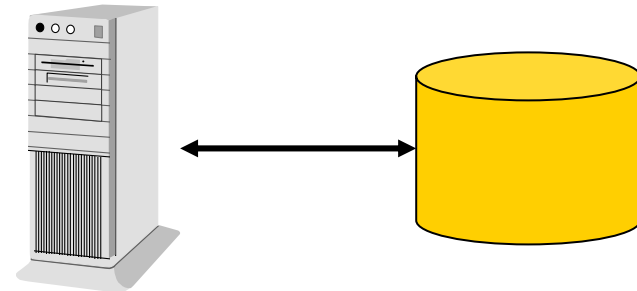
---

- Active Directory unterstützt den Multimastermodus
  - d.h. in vielen Bereichen z.B. DDNS mit Active Directory integrierten Zonen, können mehrere DC gleichberechtigt ihre Daten speichern.
- Der Multimastermodus erhöht die die Zuverlässigkeit und Stabilität eines Dienstes.
  - Der Ausfall eines DC führt nicht zwangsläufig zum Ausfall des Dienstes.

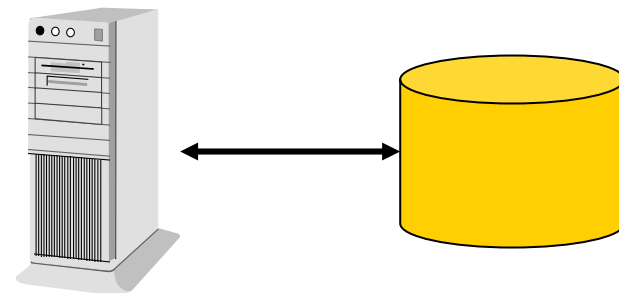
# Multimaster anhand von DDNS (1/8)



**Arbeitsplatz**

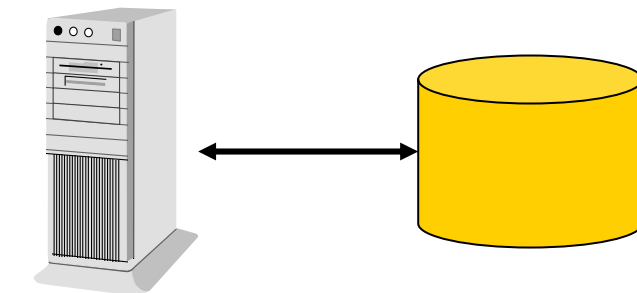
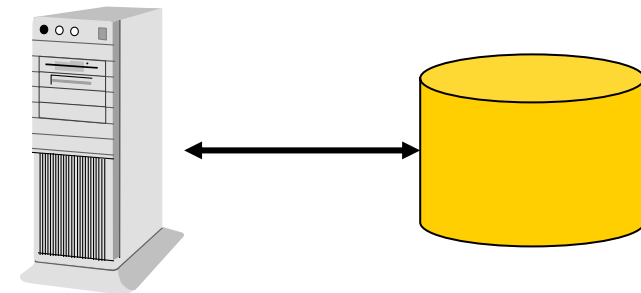
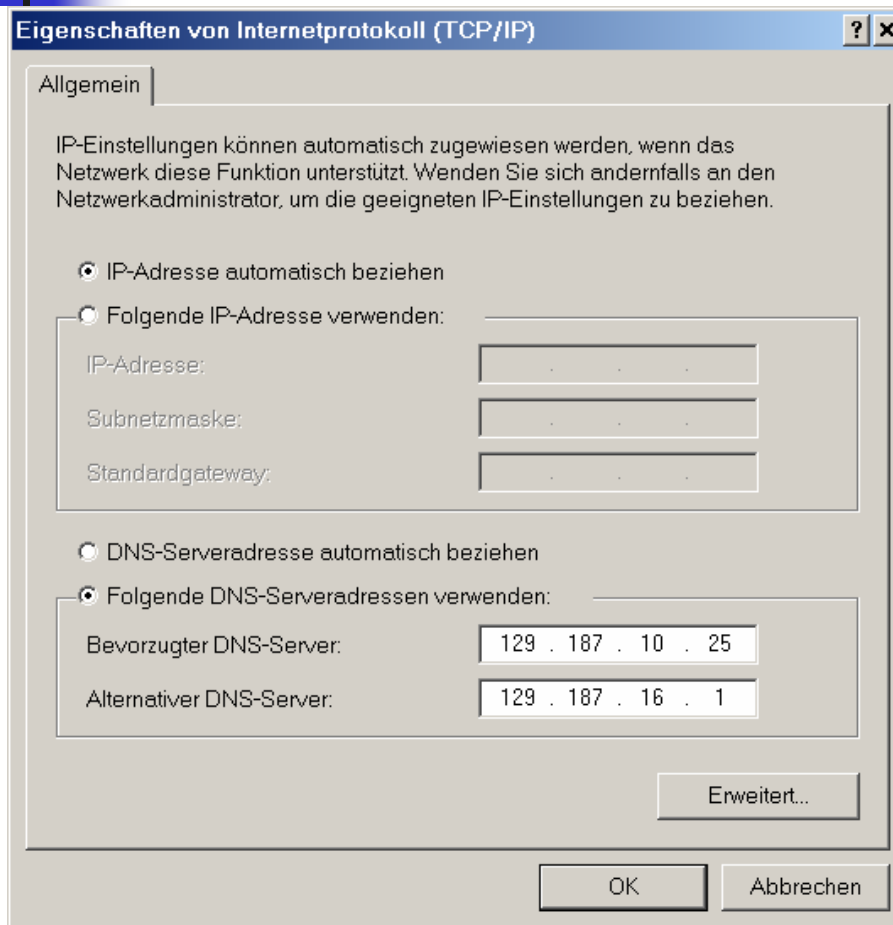


**DDNS1**



**DDNS2**

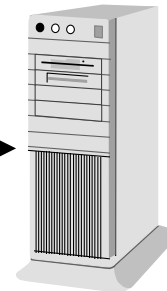
# Multimaster anhand von DDNS (2/8)



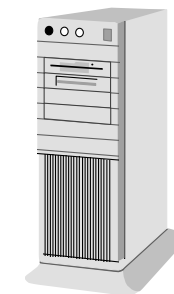
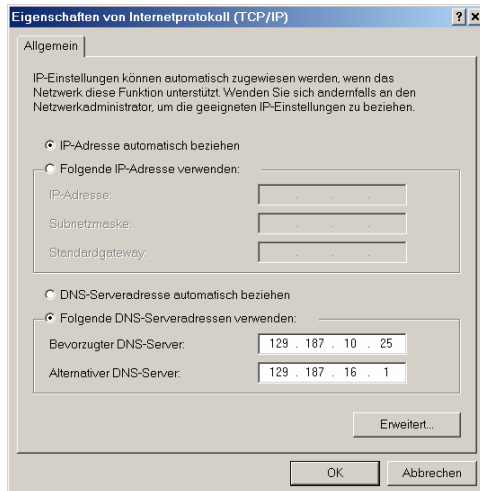
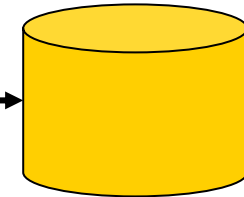
# Multimaster anhand von DDNS (3/8)



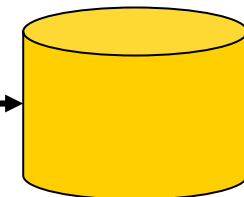
**Arbeitsplatz**



**DDNS1**



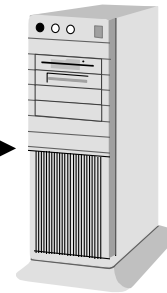
**DDNS2**



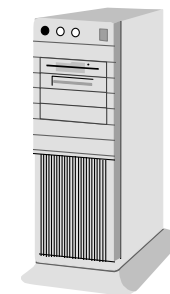
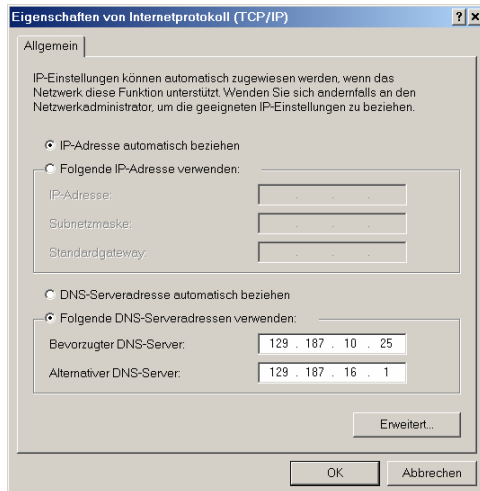
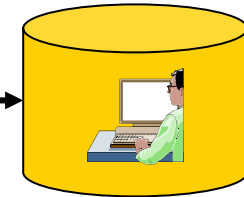
# Multimaster anhand von DDNS (4/8)



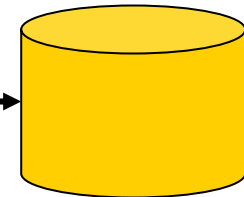
**Arbeitsplatz**



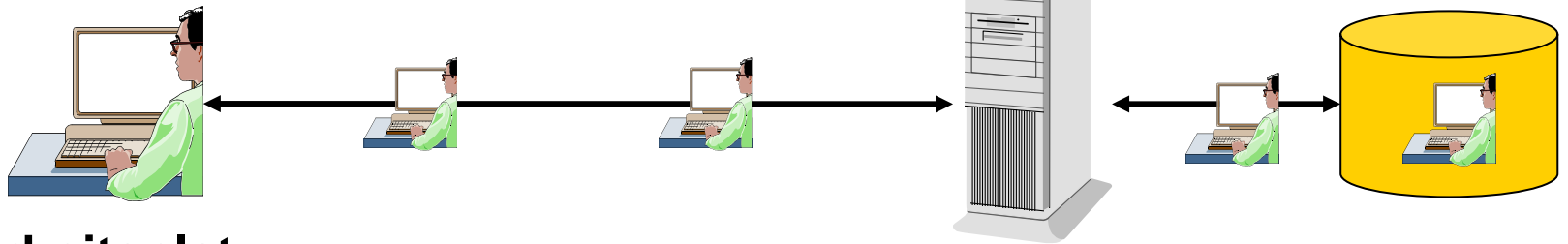
**DDNS1**



**DDNS2**

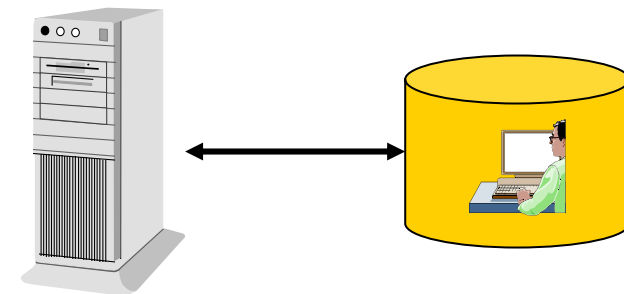
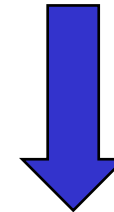


# Multimaster anhand von DDNS (5/8)

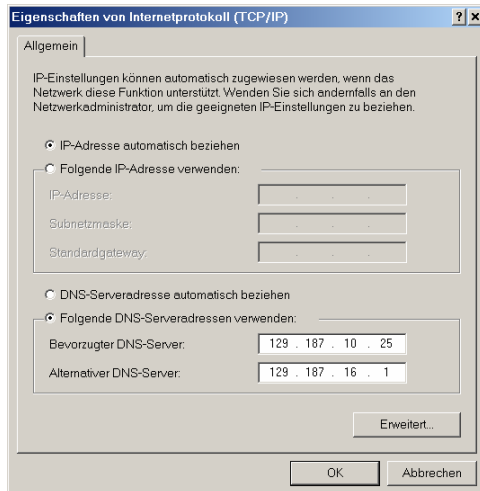


**Arbeitsplatz**

**DDNS1**



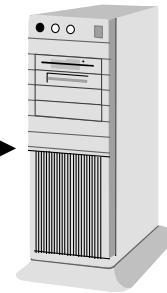
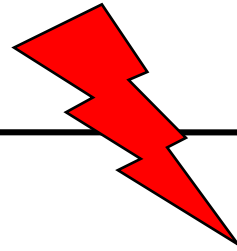
**DDNS2**



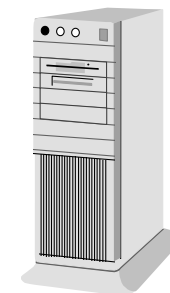
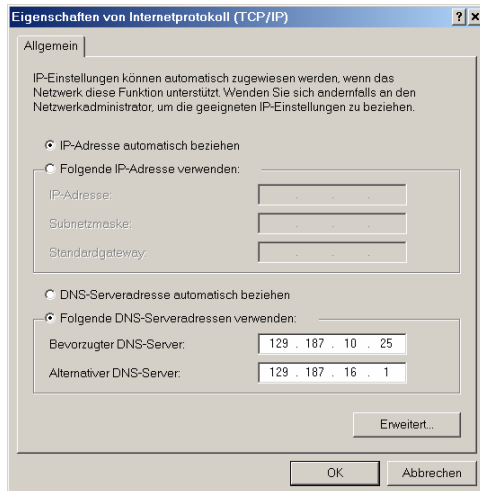
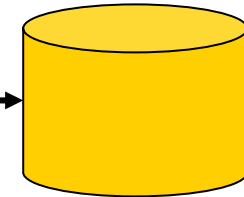
# Multimaster anhand von DDNS (6/8)



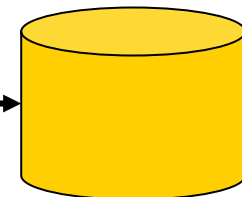
**Arbeitsplatz**



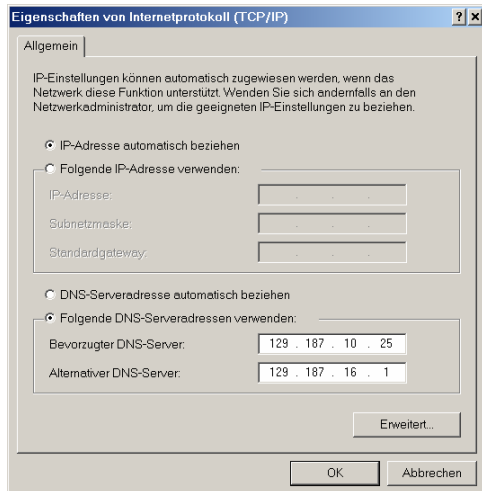
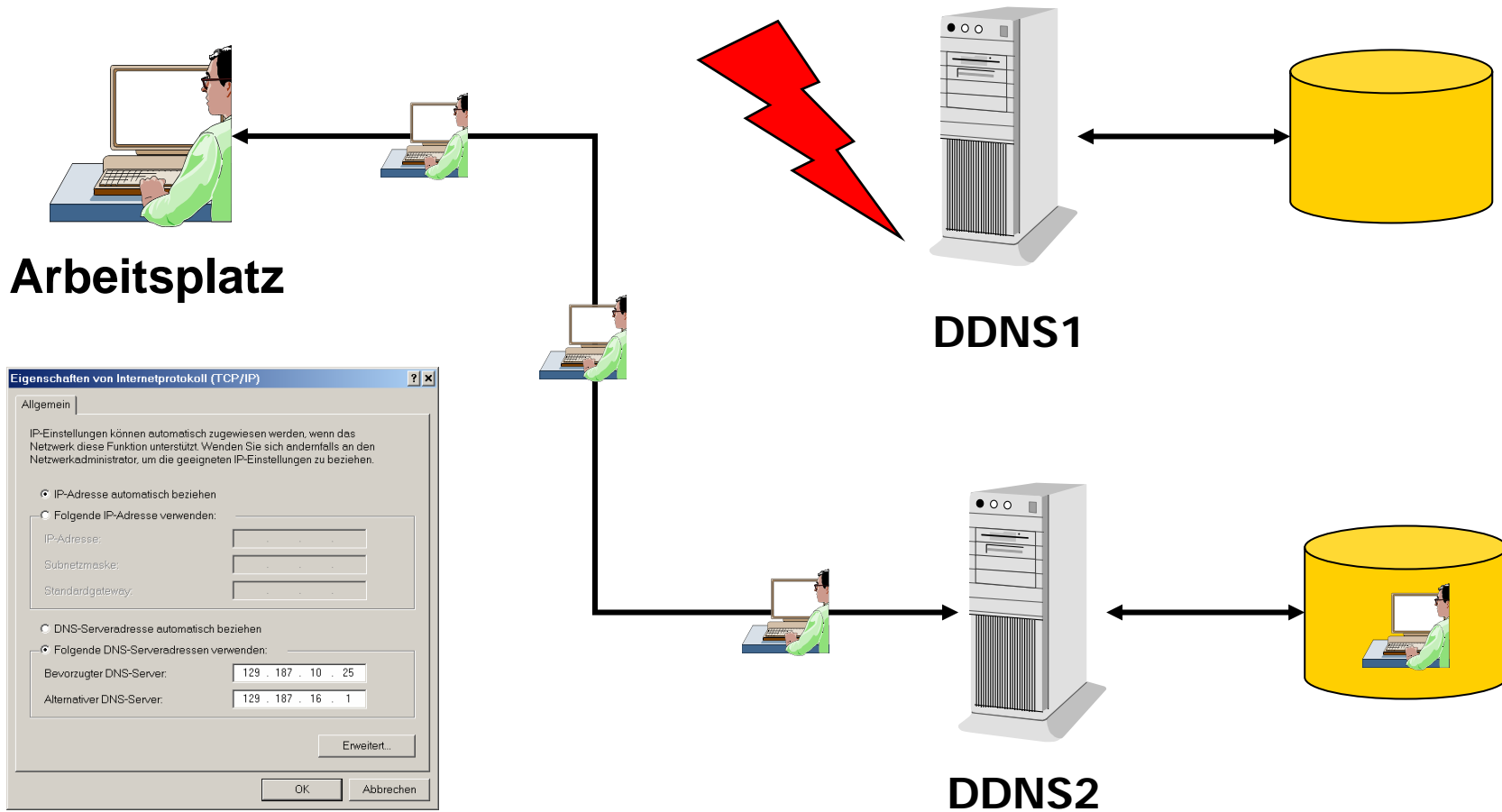
**DDNS1**



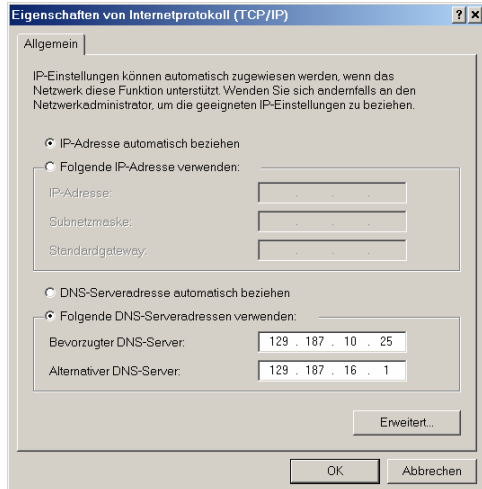
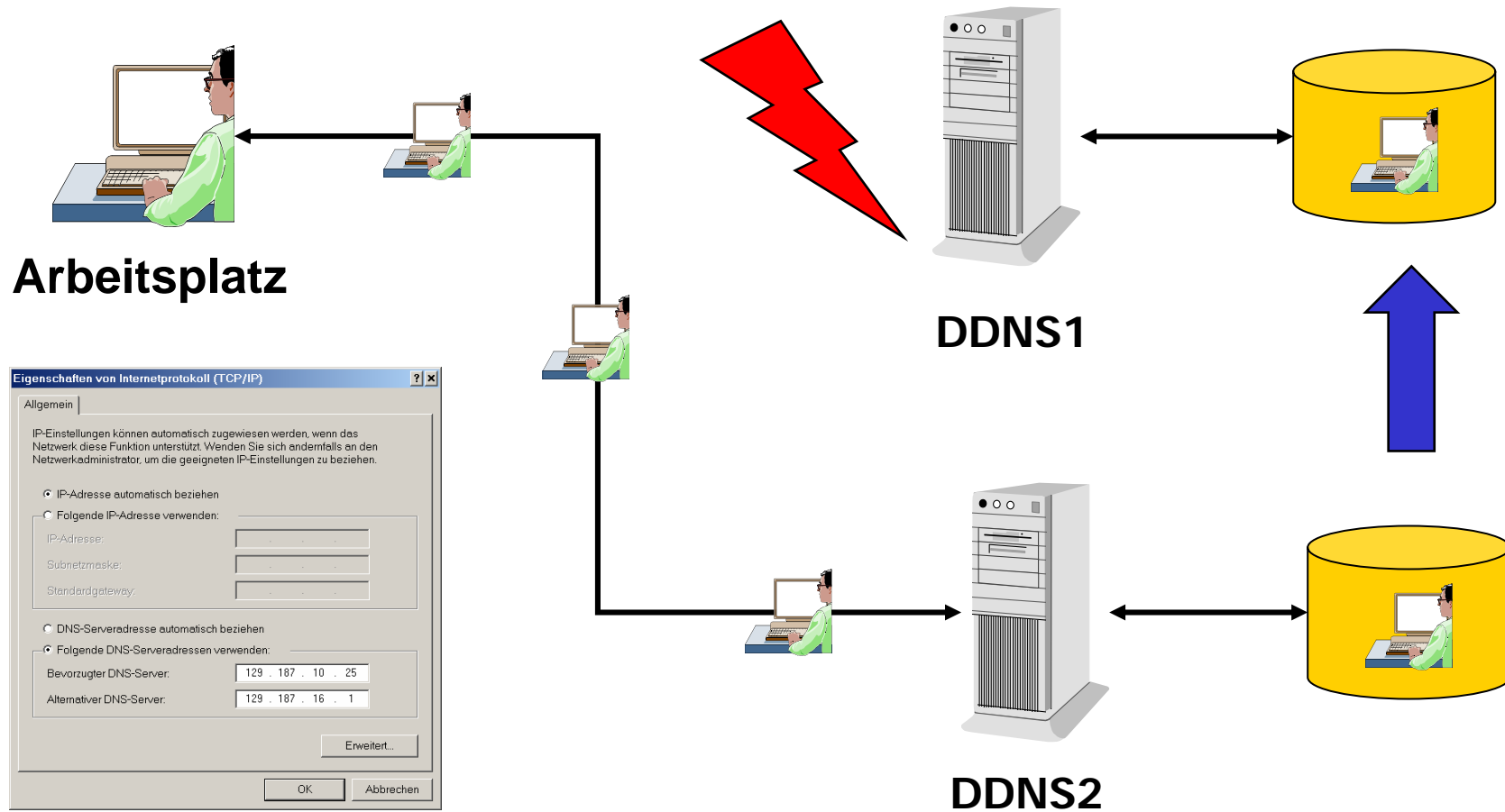
**DDNS2**



# Multimaster anhand von DDNS (7/8)



# Multimaster anhand von DDNS (8/8)





# Betriebsmasterrollen

---



# Betriebsmasterrollen

---

- Es gibt Funktionen bei denen eine Multimastermodus nicht möglich ist.
- Die Funktionen die nur einen Einzelmastermodus erlauben werden **Betriebsmasterrollen** genannt.
- Windows 2000 kennt 5 Betriebsmasterrollen.



# Betriebsmasterrollen

---

- In ***jeder Active Directory Gesamtstruktur*** müssen folgende Rollen enthalten sein:
  - Schemamaster
  - Domänennamenmaster
  
- In ***jeder Domäne*** in der Gesamtstruktur müssen folgende Rollen enthalten sein:
  - Relativer ID-Master
  - Primärer Domänencontrolleremulator (PDC)
  - Infrastrukturmater



# Schemamaster

---

- Der Schemamaster-Domänencontroller steuert alle Aktualisierungen und Änderungen in Bezug auf das Schema.
- Um das Schema zu erweitern (z.B. Exchange) müssen Sie auf den Schemamaster zugreifen können.
- Zu einem Zeitpunkt darf es nur einen Schemamaster in der Gesamtstruktur geben.



# DomänenNamenMasterRolle

---

- Der Domänencontroller der die Domänennamenmasterrolle steuert das
  - Hinzufügen oder
  - Entfernenvon Domänen in der Gesamtstruktur.
  
- Zu einen Zeitpunkt darf es nur einen DC mit der Domänennamenmasterrolle in der Gesamtstruktur geben



## Relativer ID-Master (1/2)

---

- Der RID-Master ordnet den verschiedenen DC's seiner Domäne Sequenzen relativer ID's zu.
- Wenn ein DC
  - einen Benutzer,
  - eine Gruppe oder
  - ein Computerobjekt
- erstellt, weist der DC diesem Objekt immer eine eindeutige Sicherheits-ID zu. Die SID besteht aus einer Domänen-sicherheits-ID, die bei allen in einer bestimmten Domäne erstellten SIDs übereinstimmt, sowie aus einer relativen ID, die für jede in der Domäne erstellte SID eindeutig ist.



## Relativer ID-Master (2/2)

---

- Wenn Sie ein Objekt zwischen Domänen verschieben möchten (mit MOVETREE.EXE; ADS Objektmanager) müssen Sie die Verschiebung auf dem RID-Master der Domäne initiieren in der sich das Objekt befindet.
- In einer Domäne kann immer nur ein relativer ID-Master vorhanden sein.



## PDC-Emulator (1/2)

---

- Der Domänencontroller, der in Windows NT 4.0 als primärer Domänencontroller (PDC = Primary Domain Controller) eingerichtet ist, um Netzwerkclients zu unterstützen, auf denen keine Clientsoftware für Active Directory installiert ist.
- Außerdem repliziert dieser Verzeichnisänderungen auf alle Reservedomänencontroller (BDC = Backup Domain Controller) in Windows NT in der Domäne.



## PDC-Emulator (2/2)

---

- In einer Windows 2000-Domäne im einheitlichen Modus
  - empfängt der PDC-Emulationsmaster bevorzugte Replikation von Kennwortänderungen, die von anderen Domänencontrollern in der Domäne ausgeführt werden,
  - und bearbeitet alle Anforderungen zur Kennwortauthentifizierung, die auf dem lokalen Domänencontroller fehlschlagen.
- In einer Domäne kann immer nur ein PDC-Emulator vorhanden sein.



## Infrastruktur Master

---

- Der Domänencontroller, der die Zuordnungen von Benutzern zu Gruppen aktualisiert, wenn sich eine Zugehörigkeit zu einer Gruppe geändert hat, und der die Änderungen auf alle anderen Domänencontroller in der Domäne repliziert.
- In einer Domäne kann immer nur ein Infrastrukturmater vorhanden sein.

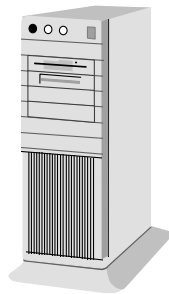
# Zusammenfassung

Rolle	Gesamtstruktur	Domäne
Schemamaster	Einmal	
Domänennamensmaster	Einmal	
RID-Master		Einmal
PDC-Emulatormaster		Einmal
Infrastrukturmaster		Einmal



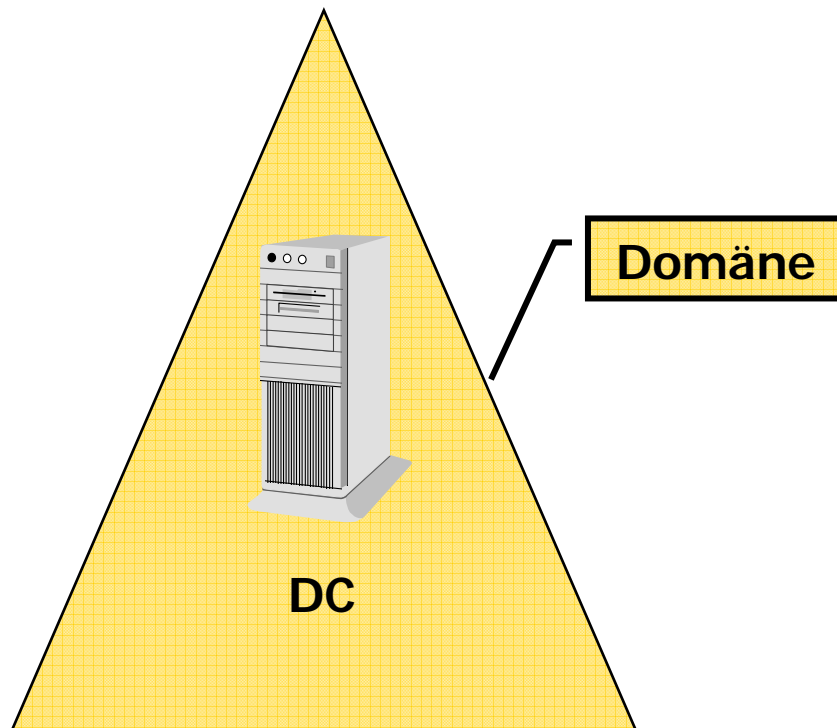
# Welche Rollen hat der erste DC ? (1/6)

---

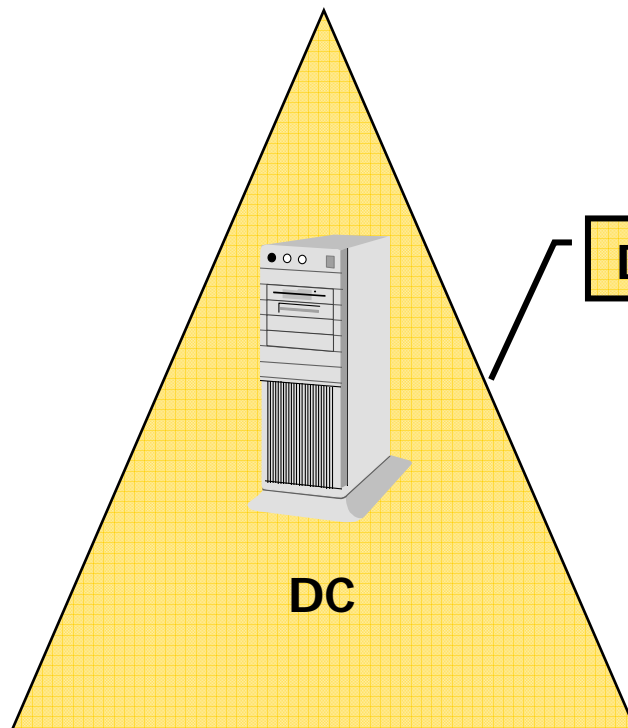


**DC**

# Welche Rollen hat der erste DC ? (2/6)

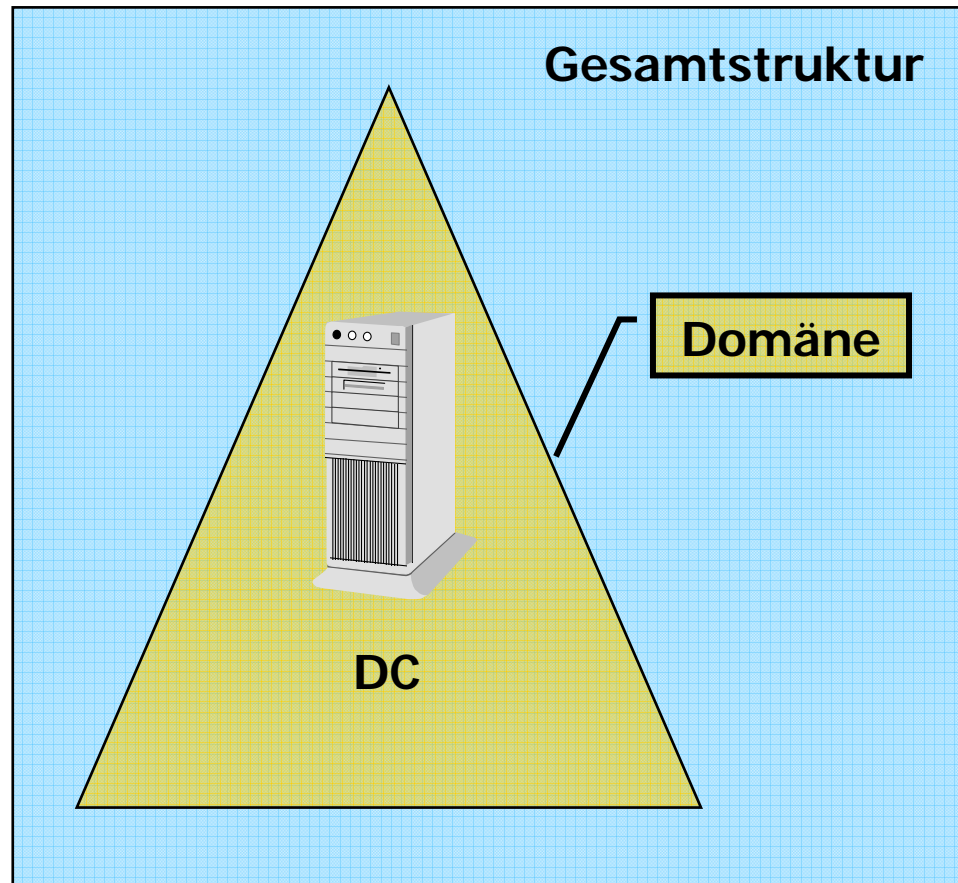


# Welche Rollen hat der erste DC ? (3/6)



- RID-Master
- PDC-Emulatormaster
- Infrastrukturmaster

# Welche Rollen hat der erste DC ? (4/6)

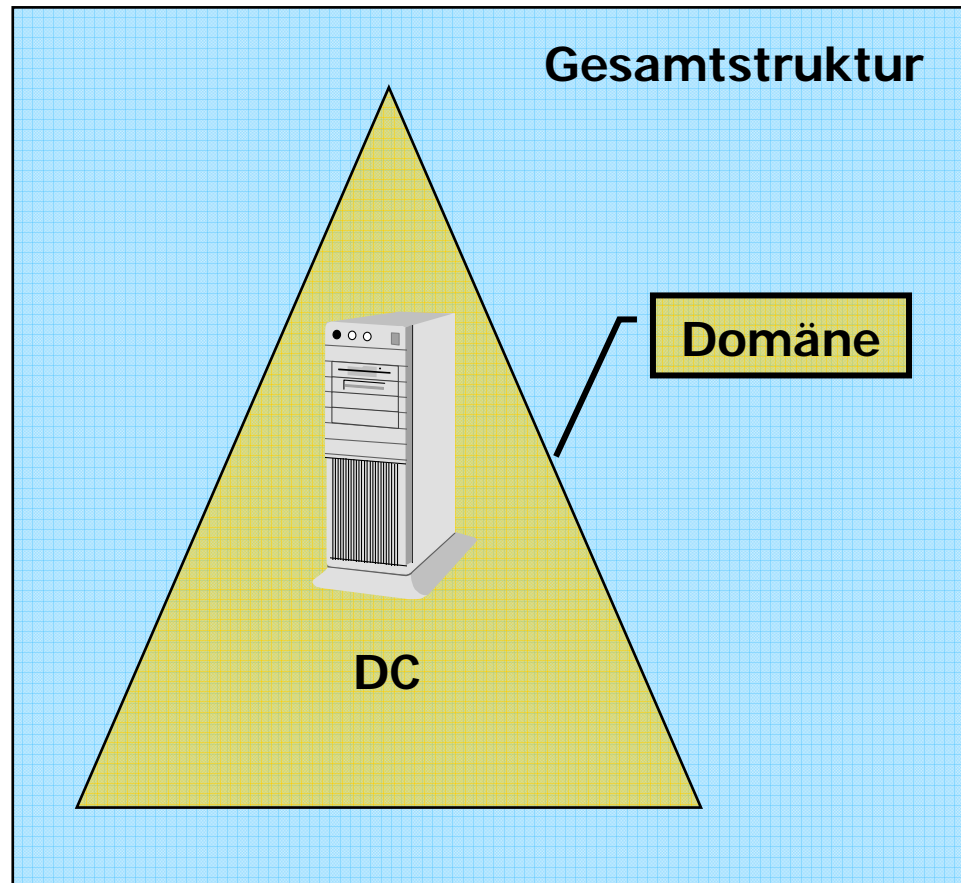


**RID-Master**

**PDC-Emulatormaster**

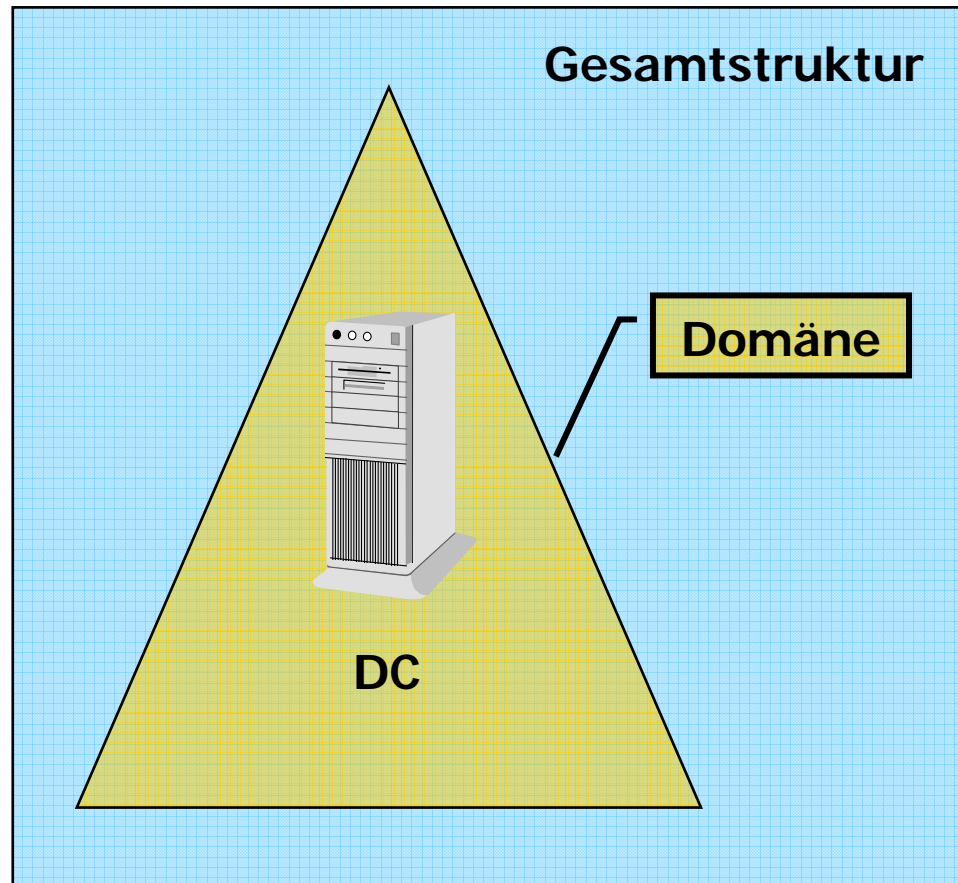
**Infrastrukturmaster**

# Welche Rollen hat der erste DC ? (5/6)



- RID-Master**
- PDC-Emulatormaster**
- Infrastrukturmaster**

# Welche Rollen hat der erste DC ? (6/6)



**Schemamaster**

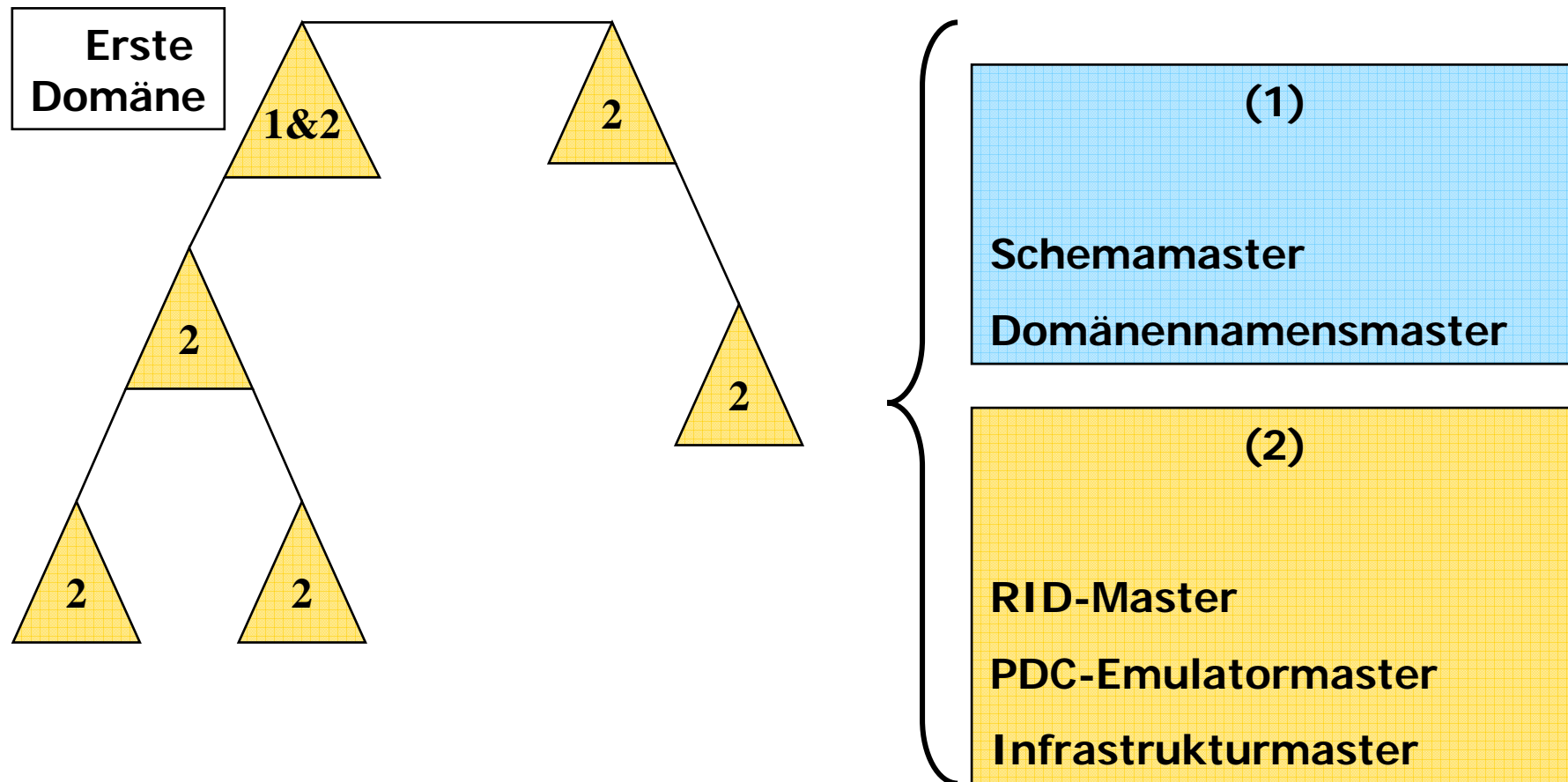
**Domänennamensmaster**

**RID-Master**

**PDC-Emulatormaster**

**Infrastrukturmaster**

# Verteilung der Rollen in einen Wald





## Planung der Rollen in einer Domäne ?

---

- Halten Sie wenn möglich die Rolle des
  - RID-Masters und
  - PDC-Emulators
- zusammen.
  
- Trennen Sie den
  - Infrastrukturmaster und den
  - Global Katalog



# Planung der Rollen in einer Gesamtstruktur ?

---

- Die Rollen
  - Schemamaster und
  - DNS-Master
- sollten auf demgleichen DC sein



# Ausfall eines Betriebsmasters

---



## Reagieren auf Betriebsmasterausfälle (1/3)

---

- Einige Funktionen des Betriebsmasters sind für den einwandfreien Betrieb des Netzwerkes unverzichtbar. Andere Funktionen wiederum können längere Zeit nicht verfügbar sein, bevor ihr Ausfall zu einem Problem wird.
- Dass der Inhaber einer Einzelmasterbetriebsfunktion nicht verfügbar ist, bemerken Sie in der Regel, wenn Sie versuchen, eine durch den betreffenden Betriebsmaster gesteuerte Funktion auszuführen.
- Wenn ein Betriebsmaster aufgrund eines Computerausfalls oder aufgrund von Netzwerkproblemen nicht verfügbar ist, können Sie die Funktion des Betriebsmasters übernehmen. Die Übernahme wird auch als erzwungene Übertragung der Betriebsmasterfunktion bezeichnet.



## Reagieren auf Betriebsmasterausfälle (2/3)

---

- Bevor die Übertragung erzwungen wird, sollten Sie
  - die Ursache und
  - die erwartete Dauer des Computer- oder Netzwerkausfalls ermitteln.
- Handelt es sich um ein Netzwerkproblem oder einen Serverausfall, das bzw. der schnell behoben ist, warten Sie, bis der Inhaber der Funktion wieder verfügbar ist.
- Ist der mit der Funktion betraute Domänencontroller ausgefallen, muss entschieden werden, ob er schnell wiederhergestellt und online geschaltet werden kann.



## Reagieren auf Betriebsmasterausfälle (3/3)

---

- Die Übernahme einer Betriebsmasterfunktion ist generell ein **drastischer** Schritt, der nur in Betracht gezogen werden sollte, wenn ein neuerlicher Betrieb des aktuellen Betriebsmasters **vollständig ausgeschlossen** wird.
- Diese Entscheidung richtet sich nach der jeweiligen Funktion und danach, wie lange der Inhaber der Funktion nicht verfügbar sein wird.



# Ausfall des Schemamasters

---

- Netzwerkbenutzer werden den vorübergehenden Ausfall des Schemabetriebsmasters nicht bemerken. Der Ausfall ist auch für Netzwerkadministratoren nicht transparent, sofern nicht versucht wird, das Schema zu ändern oder eine Anwendung zu installieren, durch die das Schema während der Installation geändert wird.
- Die Übernahme dieser Funktion ist jedoch ein drastischer Schritt, der erst in Betracht gezogen werden sollte, wenn der Schemamaster dauerhaft ausfällt.
- *Ein Domänencontroller, dessen Schemamasterfunktion übernommen wurde, darf nie wieder online geschaltet werden.*



# Ausfall des DNS-Masters

---

- Netzwerkbenutzer werden den vorübergehenden Ausfall des DNS-Masters nicht bemerken. Der Ausfall ist auch für Netzwerkadministratoren nicht transparent, sofern nicht versucht wird, der Gesamtstruktur eine Domäne hinzuzufügen bzw. eine Domäne daraus zu entfernen.
- Die Übernahme dieser Funktion ist jedoch ein drastischer Schritt, der erst in Betracht gezogen werden sollte, wenn der DNS-Master dauerhaft ausfällt.
- *Ein Domänencontroller, dessen DNS-Masterfunktion übernommen wurde, darf nie wieder online geschaltet werden.*



## Ausfall des RID-Masters

---

- Netzwerkbenutzer werden den vorübergehenden Ausfall des RID-Masters nicht bemerken.
- Der Ausfall ist auch für Netzwerkadministratoren nicht transparent, es sei denn, es werden Objekte in einer Domäne erstellt, und in der betreffenden Domäne sind keine relativen Bezeichner mehr verfügbar.
- *Ein Domänencontroller, dessen RID-Masterfunktion übernommen wurde, darf nie wieder online geschaltet werden.*



# Ausfall der PDC-Emulation

---

- Der Ausfall der PDC-Emulation hat direkte Auswirkungen auf die Netzwerkbenutzer. Ist die PDC-Emulation nicht verfügbar, muss die Funktion u. U. sofort übernommen werden.
- Wenn der aktuelle PDC-Emulationsmaster über einen unangemessen langen Zeitraum nicht verfügbar ist und in seiner Domäne Clients ohne Windows 2000-Clientsoftware oder Windows NT-Reservedomänencontroller enthalten sind, lassen Sie die Funktion des PDC-Emulationsmasters vom Standby-Betriebsmaster übernehmen.
- Sobald der ursprüngliche PDC-Emulationsmaster den Betrieb wieder aufnimmt, kann die Funktion wieder auf den ursprünglichen Domänencontroller übertragen werden.



# Ausfall des Infrastrukturmasters

---

- Netzwerkbenutzer werden den vorübergehenden Ausfall eines Infrastrukturmasters nicht bemerken. Der Ausfall ist auch für Netzwerkadministratoren nicht transparent, es sei denn, kürzlich wurde eine große Anzahl Konten verschoben oder umbenannt.
- Ist der Infrastrukturmater für einen unangemessen langen Zeitraum nicht verfügbar, kann die Funktion von einem Domänencontroller übernommen werden, der zwar nicht als globaler Katalog konfiguriert ist, jedoch über gute Verbindungen zu einem globalen Katalog (einer beliebigen Domäne) verfügt und sich idealerweise an demselben Standort wie der aktuelle globale Katalog befindet.
- Sobald der ursprüngliche Infrastrukturmater den Betrieb wieder aufnimmt, kann die Funktion wieder auf den ursprünglichen Domänencontroller übertragen werden.



# Zusammenfassung

---

- Ein Domänencontroller, dessen
  - Schemamaster
  - DNS-Master
  - RID-Master
- übernommen wurde,  
*darf nie wieder online geschaltet werden !!*
- Ein Domänencontroller, dessen
  - PDC-Emulatormaster
  - Infrastrukturmater
- Übernommen wurde, kann diese wieder zurück erhalten.



# So übernehmen Sie die Funktion des Schemamasters

---

- Klicken Sie auf Start und dann auf Ausführen, und geben Sie **cmd** ein.
- Geben Sie **ntdsutil** ein.
- Geben Sie an der Eingabeaufforderung **ntdsutil** den Befehl **roles** ein.
- Geben Sie an der Eingabeaufforderung **fsmo maintenance** den Befehl **connections** ein.
- Geben Sie an der Eingabeaufforderung Serververbindungen den Befehl **connect to server**, gefolgt von einem vollqualifizierten Domänennamen ein.
- Geben Sie an der Eingabeaufforderung Serververbindungen den Befehl **quit** ein.
- Geben Sie an der Eingabeaufforderung **fsmo maintenance** den Befehl **seize schema master** ein.
- Geben Sie an der Eingabeaufforderung **fsmo maintenance** den Befehl **quit** ein.
- Geben Sie an der Eingabeaufforderung **ntdsutil** den Befehl **quit** ein.



# So übernehmen Sie die Funktion des DNS-Masterfunktion

---

- Klicken Sie auf Start und dann auf Ausführen, und geben Sie `cmd` ein.
- Geben Sie `ntdsutil` ein.
- Geben Sie an der Eingabeaufforderung `ntdsutil` den Befehl `roles` ein.
- Geben Sie an der Eingabeaufforderung `fsmo maintenance` den Befehl `connections` ein.
- Geben Sie an der Eingabeaufforderung Serververbindungen den Befehl `connect to server`, gefolgt von einem vollqualifizierten Domänennamen ein.
- Geben Sie an der Eingabeaufforderung Serververbindungen den Befehl `quit` ein.
- Geben Sie an der Eingabeaufforderung `fsmo maintenance` den Befehl `seize domain naming master` ein.
- Geben Sie an der Eingabeaufforderung `fsmo maintenance` den Befehl `quit` ein.
- Geben Sie an der Eingabeaufforderung `ntdsutil` den Befehl `quit` ein.



# So übernehmen Sie die Funktion des RID-Masterfunktion

---

- Klicken Sie auf Start und dann auf Ausführen, und geben Sie **cmd** ein.
- Geben Sie **ntdsutil** ein.
- Geben Sie an der Eingabeaufforderung **ntdsutil** den Befehl **roles** ein.
- Geben Sie an der Eingabeaufforderung **fsmo maintenance** den Befehl **connections** ein.
- Geben Sie an der Eingabeaufforderung Serververbindungen den Befehl **connect to server**, gefolgt von einem vollqualifizierten Domänennamen ein.
- Geben Sie an der Eingabeaufforderung Serververbindungen den Befehl **quit** ein.
- Geben Sie an der Eingabeaufforderung **fsmo maintenance** den Befehl **seize RID master** ein.
- Geben Sie an der Eingabeaufforderung **fsmo maintenance** den Befehl **quit** ein.
- Geben Sie an der Eingabeaufforderung **ntdsutil** den Befehl **quit** ein.



# So übernehmen Sie die Funktion des PDC-Emulationsfunktion

---

- Klicken Sie auf Start und dann auf Ausführen, und geben Sie `cmd` ein.
- Geben Sie `ntdsutil` ein.
- Geben Sie an der Eingabeaufforderung `ntdsutil` den Befehl `roles` ein.
- Geben Sie an der Eingabeaufforderung `fsmo maintenance` den Befehl `connections` ein.
- Geben Sie an der Eingabeaufforderung Serververbindungen den Befehl `connect to server`, gefolgt von einem vollqualifizierten Domänennamen ein.
- Geben Sie an der Eingabeaufforderung Serververbindungen den Befehl `quit` ein.
- Geben Sie an der Eingabeaufforderung `fsmo maintenance` den Befehl `seize PDC` ein.
- Geben Sie an der Eingabeaufforderung `fsmo maintenance` den Befehl `quit` ein.
- Geben Sie an der Eingabeaufforderung `ntdsutil` den Befehl `quit` ein.



# So übernehmen Sie die Funktion des Infrastrukturmasters

---

- Klicken Sie auf Start und dann auf Ausführen, und geben Sie `cmd` ein.
- Geben Sie `ntdsutil` ein.
- Geben Sie an der Eingabeaufforderung `ntdsutil` den Befehl `roles` ein.
- Geben Sie an der Eingabeaufforderung `fsmo maintenance` den Befehl `connections` ein.
- Geben Sie an der Eingabeaufforderung Serververbindungen den Befehl `connect to server`, gefolgt von einem vollqualifizierten Domänennamen ein.
- Geben Sie an der Eingabeaufforderung Serververbindungen den Befehl `quit` ein.
- Geben Sie an der Eingabeaufforderung `fsmo maintenance` den Befehl `seize infrastructure master` ein.
- Geben Sie an der Eingabeaufforderung `fsmo maintenance` den Befehl `quit` ein.
- Geben Sie an der Eingabeaufforderung `ntdsutil` den Befehl `quit` ein.



# Fragen ?

---

