2209 Kerberos Basics for Windows Administrators

Gary Olsen
Consultant
Americas Escalation Team
HP Services
Gary.olsen@hp.com

HP WORLD 2003
Solutions and Technology Conference & Expo

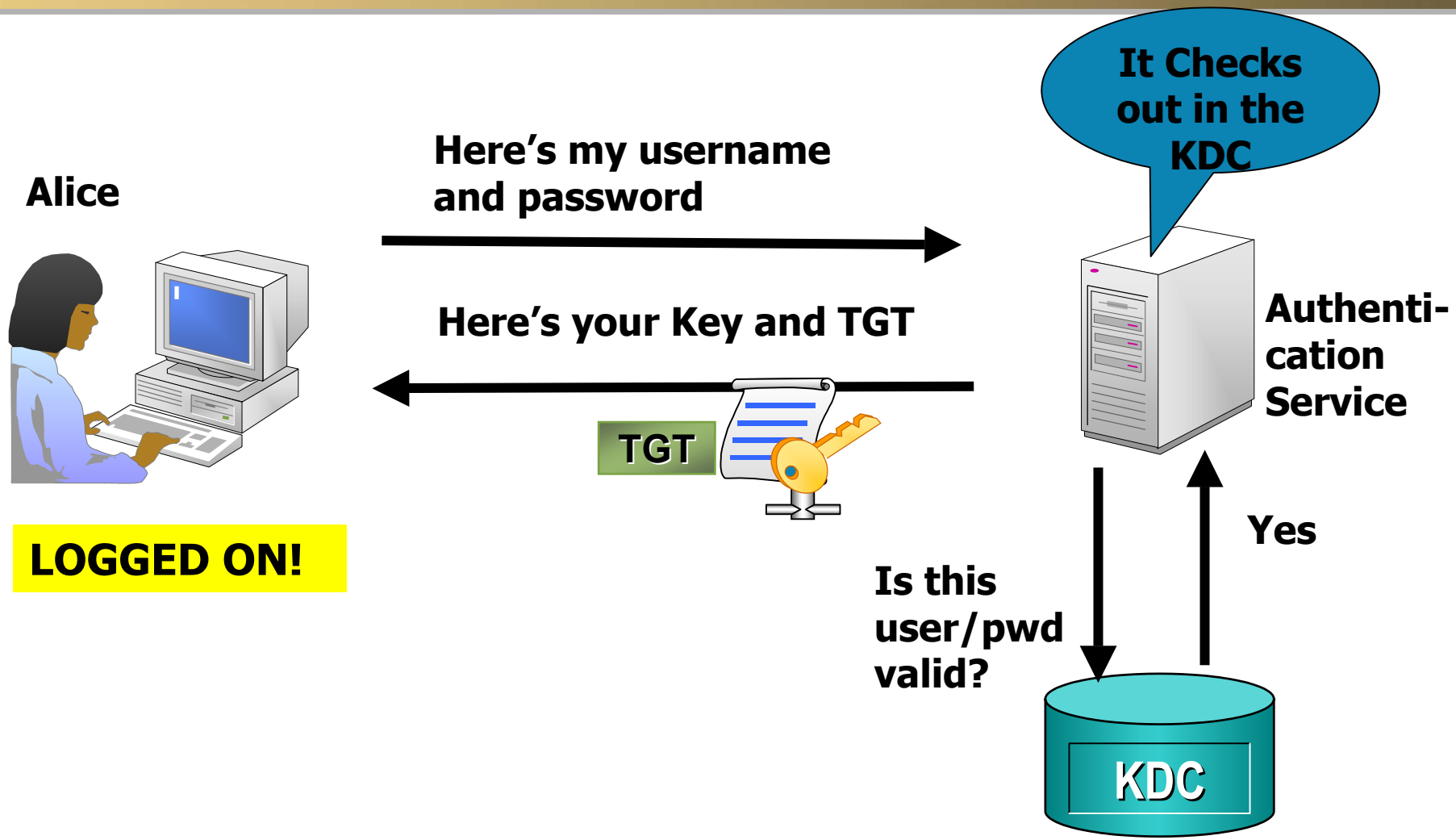
Topics

- “Native” Kerberos Authentication and Authorization
- Windows® 2000 Kerberos implementation
- Cross-platform interoperability
- Troubleshooting
- Time Services

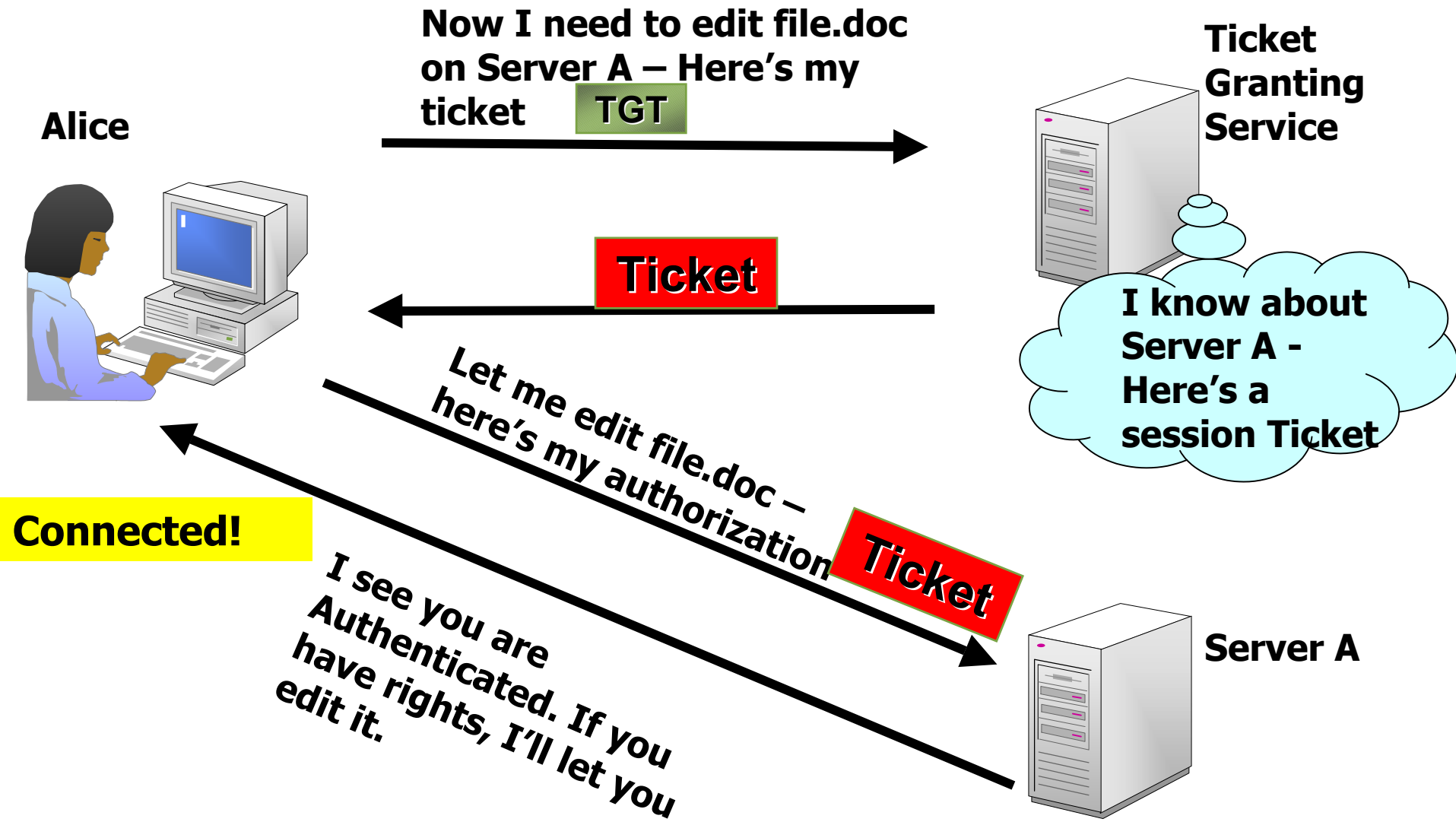
Why Kerberos?

- NT very inefficient
  - Part of the “Microsoft Only World”
  - Requires authorization every time you access a resource
  - Network traffic
  - Load on PDC/BDC
- Kerberos
  - Industry Standard – plays nicely with others
  - Inter-Forest Transitive Trust (2003)
  - Issues Session Tickets – no need to be re-authorized or re-authenticated.

Kerberos Basics - Logon



Kerberos Basics – Resource Access



Windows 2003 Kerberos Implementation

- Better implementation than Win2K
- Single sign on to Windows 2003 domains and Kerberos-based services *
- PK extensions for smart card logon
- Active Directory™ support for inter-forest account management *
- Cross-Forest and Forest-Realm Trusts *

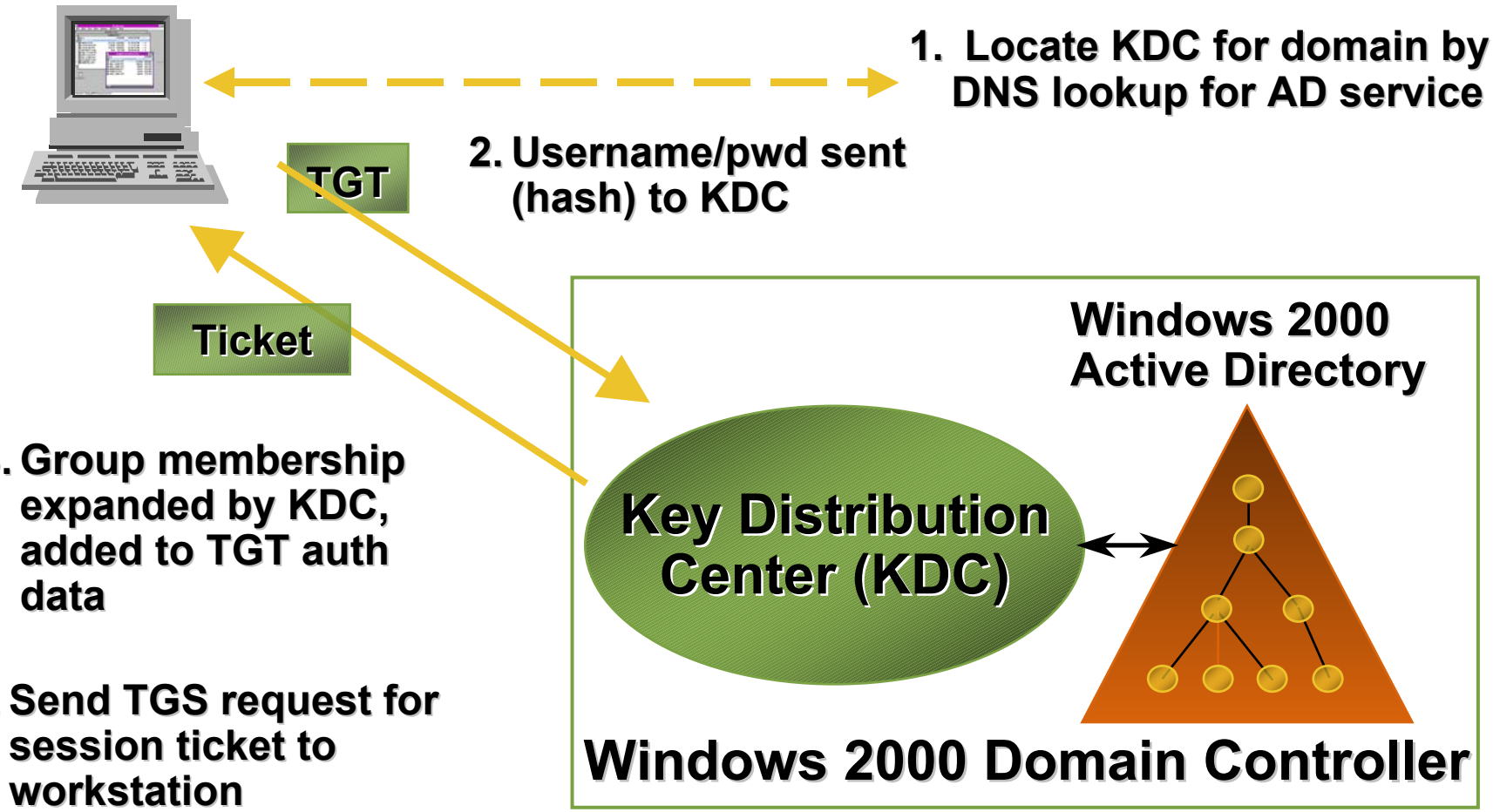
* Not available in Windows 2000

Authentication And Authorization

- Authenticate using domain credentials
  - User account defined in Active Directory (logon)
- Authorization based on group membership
  - Centralize management of access rights
  - What resources do you have access to?
- Distributed security tied to the Windows 2000 Security Model
  - Network services use impersonation
  - Object-based access control lists

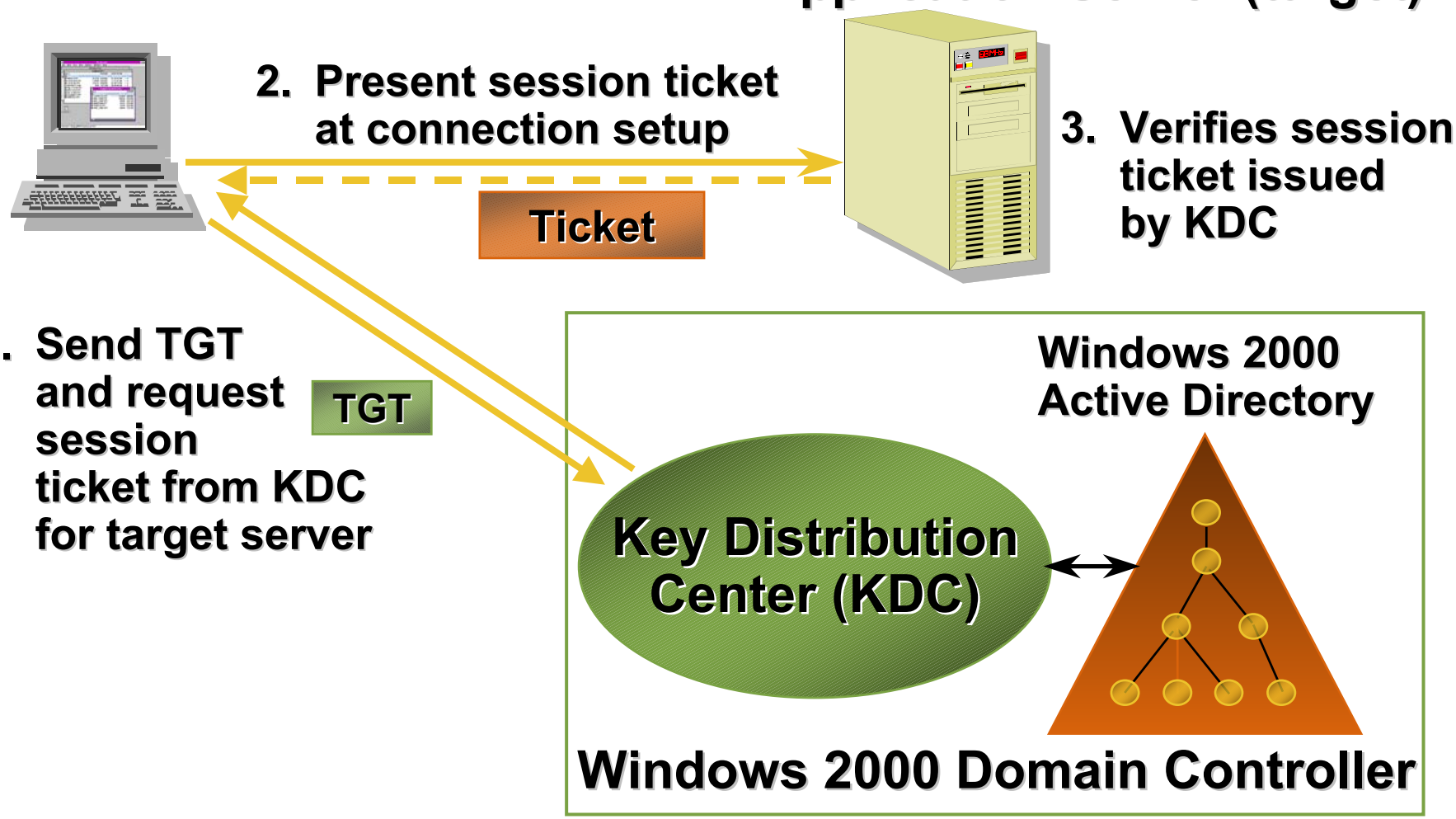
Kerberos Authentication

Interactive Domain Logon

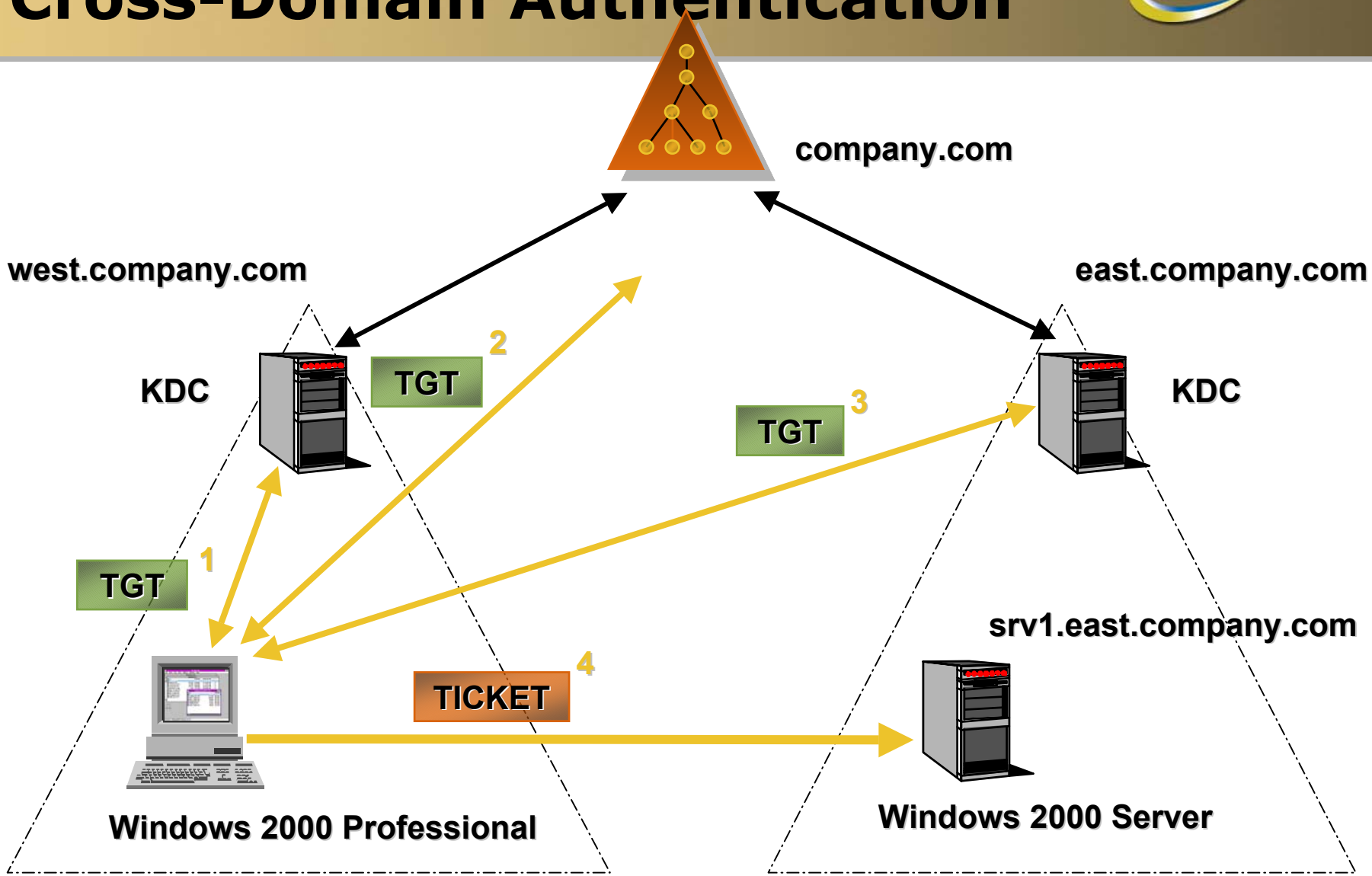


Kerberos Authorization

Network Server Connection



Cross-Domain Authentication



Cross Platform Interoperability

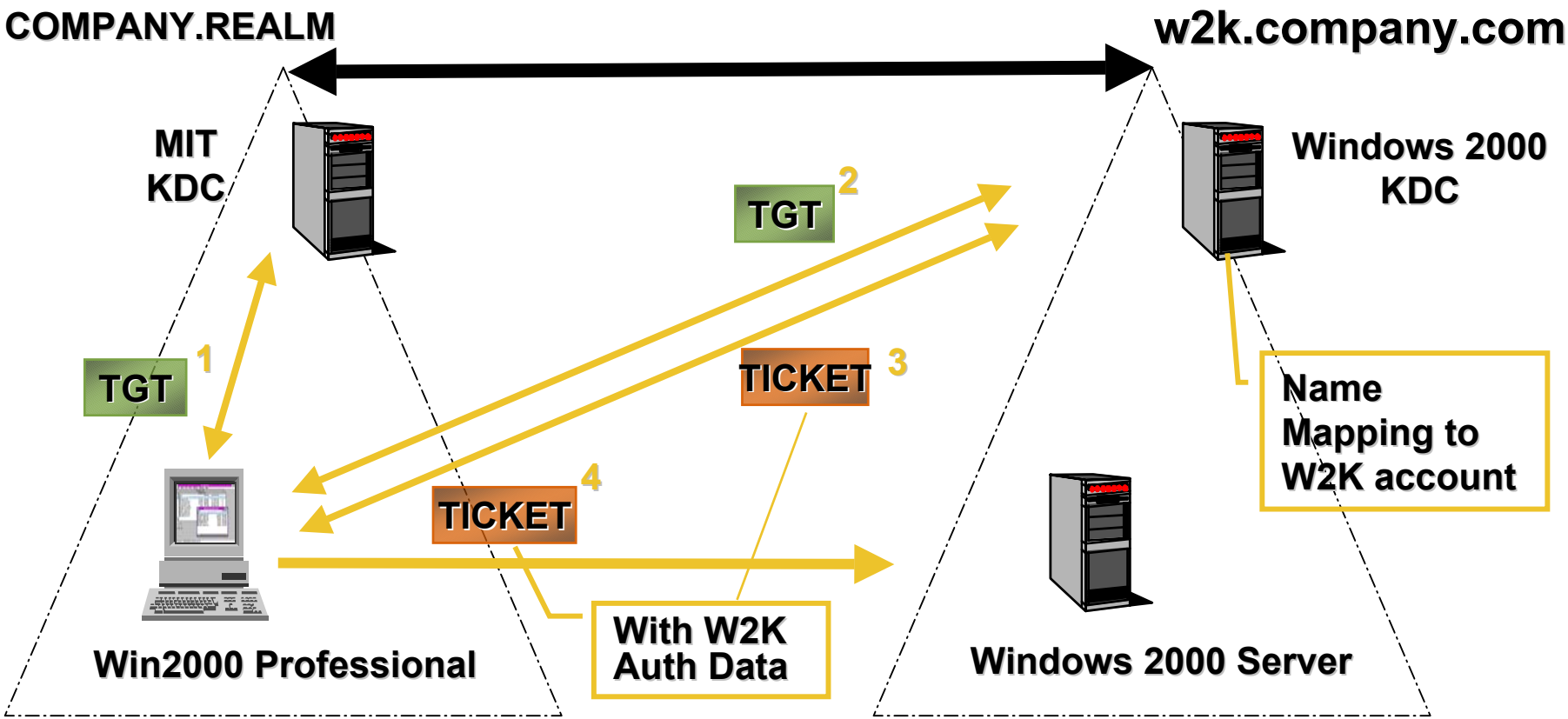
Sharing Resources between MIT Kerberos V5 Realms and Windows 2003 Forests

HP WORLD 2003
Solutions and Technology Conference & Expo

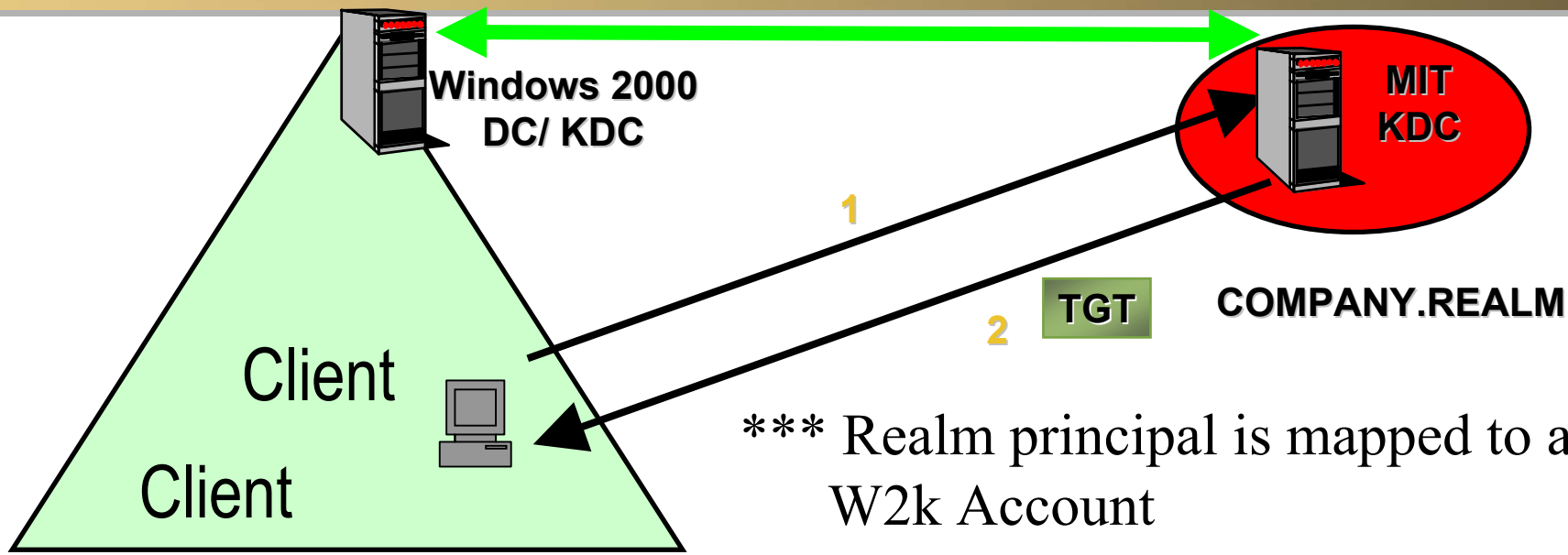
Cross-Platform Interoperability

- Based on Kerberos V5 Protocol
  - Windows 2000 not fully v5 compliant
  - Windows 2003 is
- Windows 2000 and 2003 Domain Controllers host the KDC
- Simple cross-realm authentication
  - UNIX realm to Windows 2003 forest/domain
  - Client authenticated by KDC for his/her domain

Using Unix KDCs With Windows 2000 Authorization



Interactive Logon Process

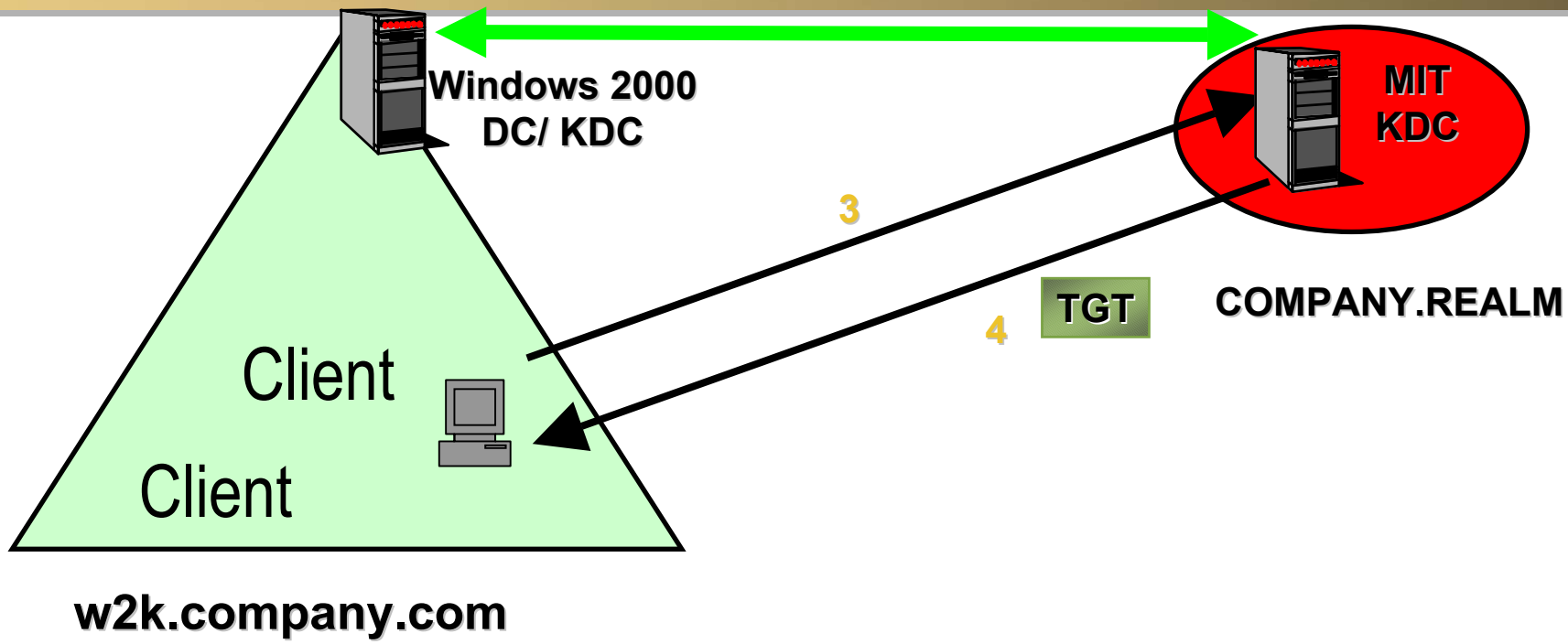


*** Realm principal is mapped to a W2k Account

Realm User logs on to Win2k client

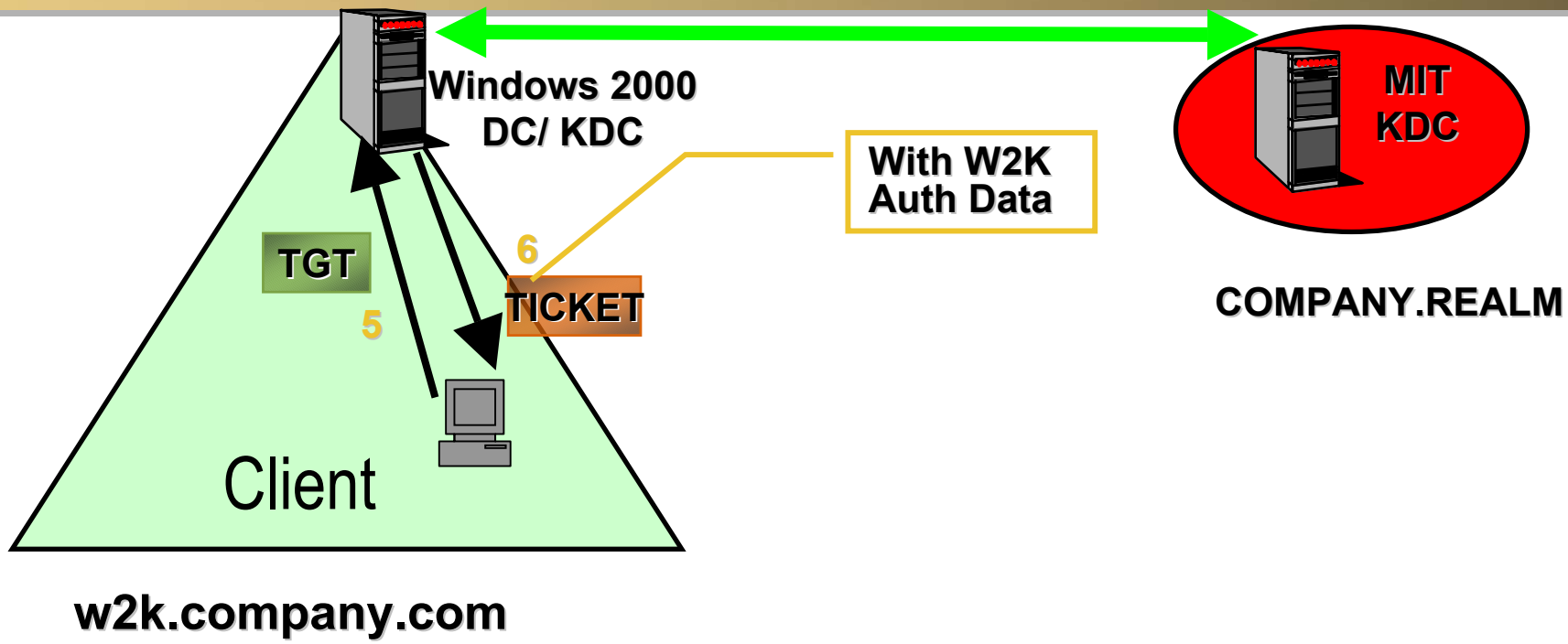
1. **User requests TGT from Realm KDC for authorization**
2. **Realm KDC returns TGT to client with Win2k DC info**

Interactive Logon Process



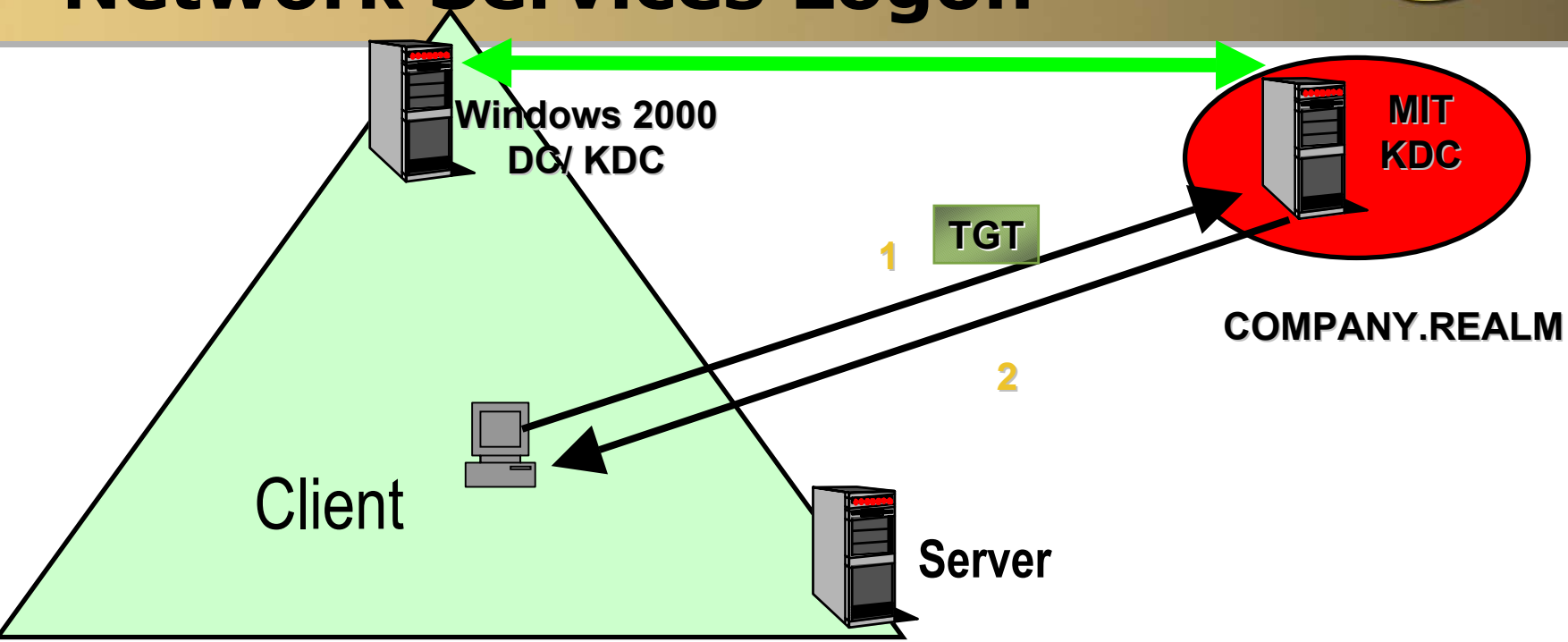
3. User requests ticket to Workstation
4. TGT for DC Returned. Contains DC and Authorization info.

Interactive Logon Process



5. User Presents TGT to DC for WS Ticket
6. DC Returns ticket to Workstation
7. User Logged on

Network Services Logon

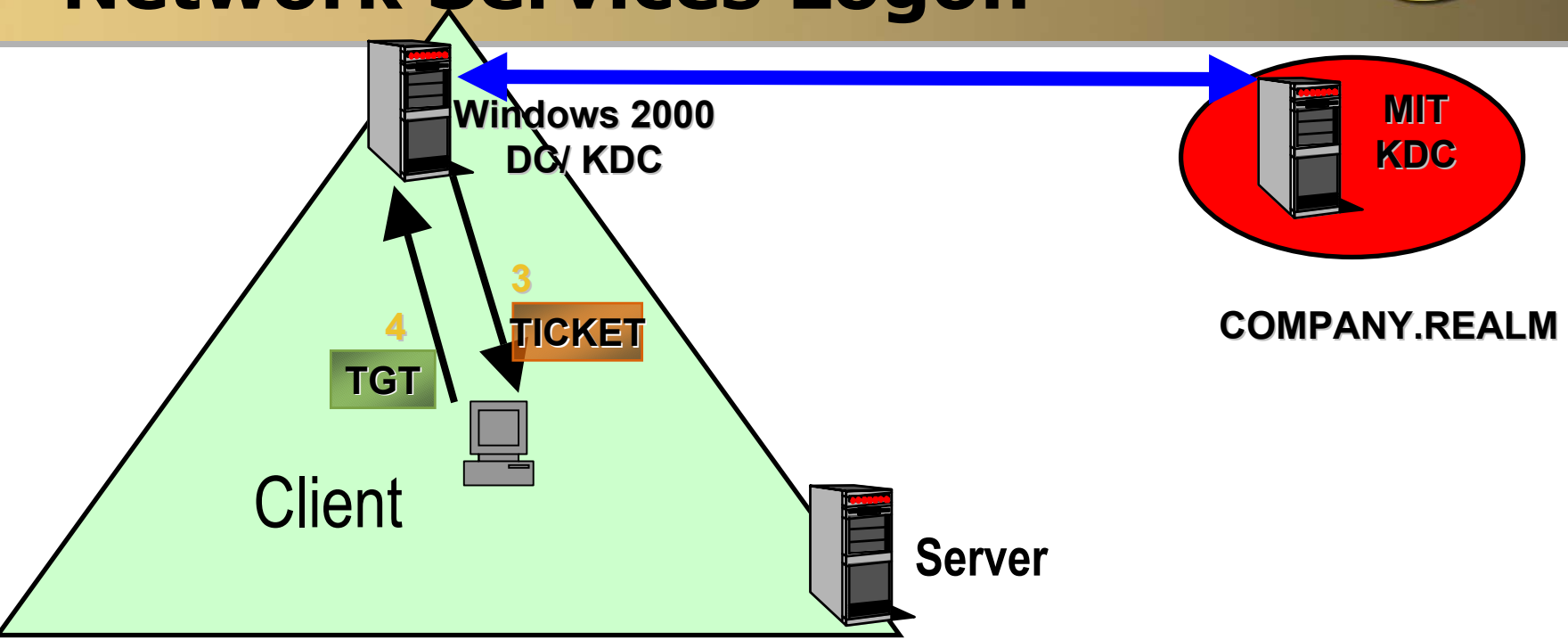


w2k.company.com

1. User Presents Authenticated TGT to DC, requests Ticket for W2K server (svc or app)

2. KDC Returns authorization data and refers to the W2K DC

Network Services Logon

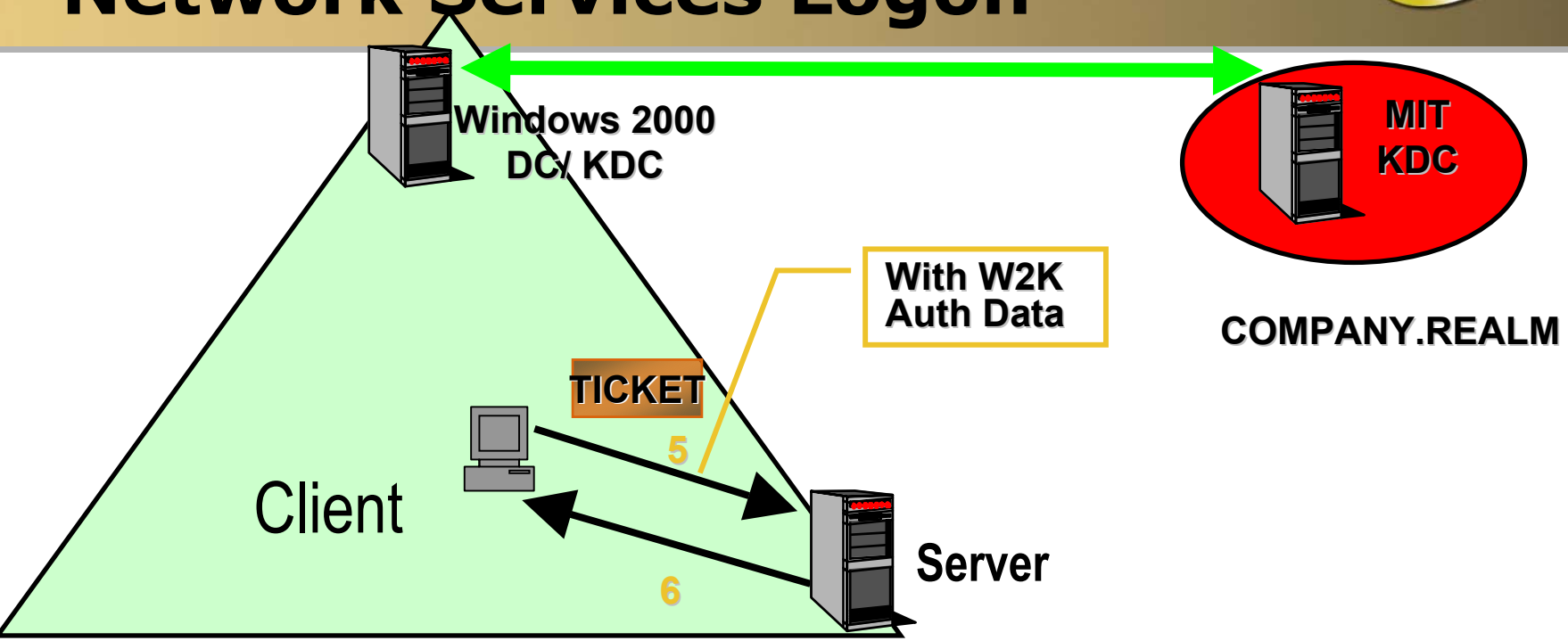


w2k.company.com

3. Client presents new TGT to DC & requests Ticket for Server

4. DC gets Authorization info (groups, SIDS) & returns Service ticket for the Server to the client

Network Services Logon



w2k.company.com

5. Client presents service ticket to Server

6. Network authorization complete

Troubleshooting

- kerbtray.exe –Reskit utility displays client Tickets
- Time between DCs and clients must be within 5 minutes by default
  - Moving machines between time zones
  - Time Service not configured
- Session tickets good for 10 hours
  - Changing group membership, etc. need new ticket.
  - Revoke/renew with Kerbtray.exe

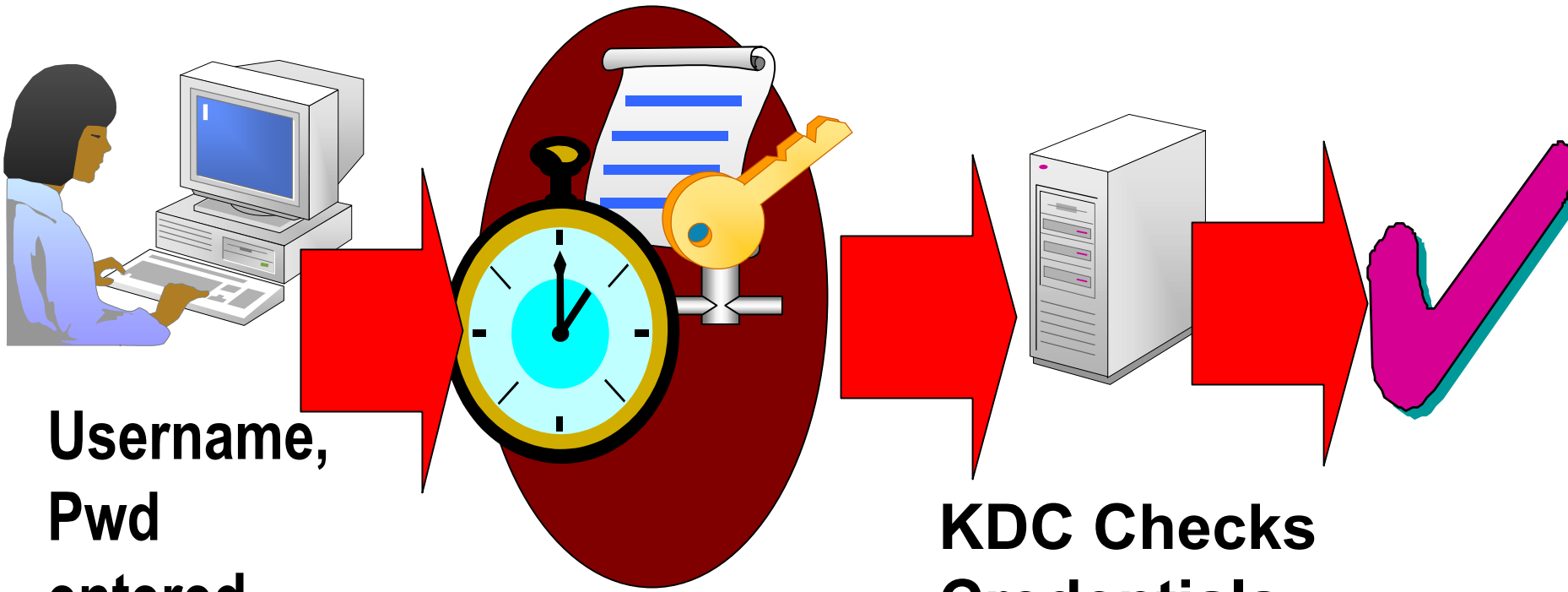
Windows 2003 Time Services

HP WORLD 2003
Solutions and Technology Conference & Expo

Topics

- The role of time in Authentication
- Windows Time Service
- Troubleshooting

The Role of Time in Authentication



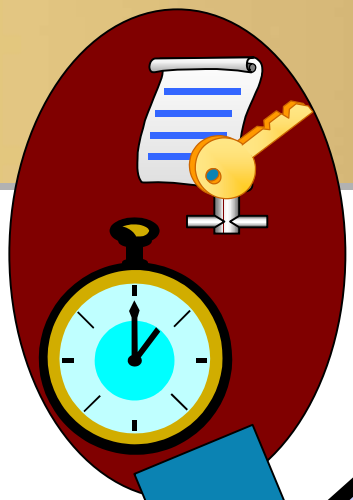
Username, Pwd entered

Authenticator Created: Time stamp, public key, Certificate

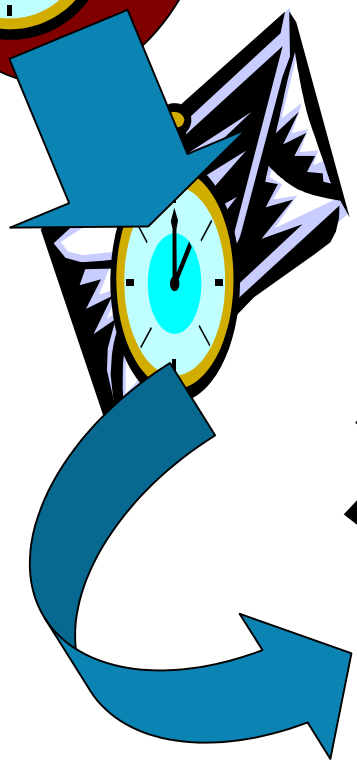
KDC Checks Credentials – validates.

User Logs in

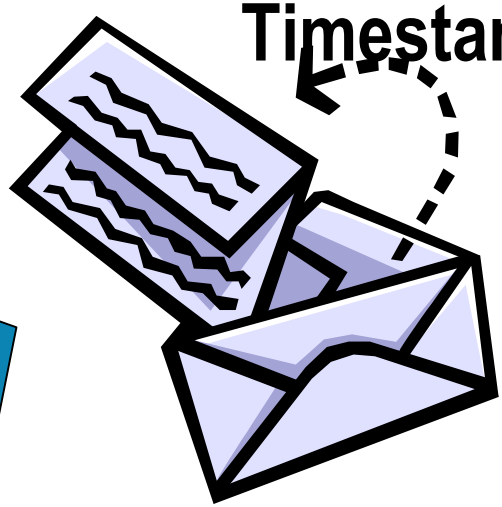
Time and Authorization



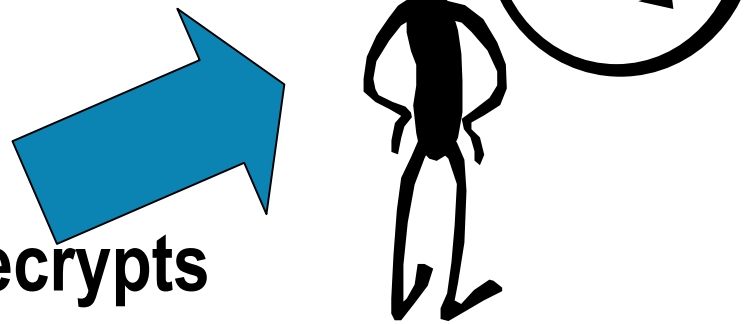
Authenticator



Server Decrypts Timestamp



Compare to Server's Time



Within defined Time Skew?

Time earlier or same as previous authenticator

Time and Authorization

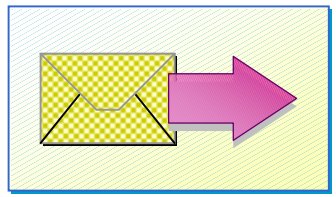
Server returns it's public key and corrects client time if needed

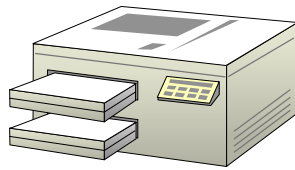
User gets session ticket

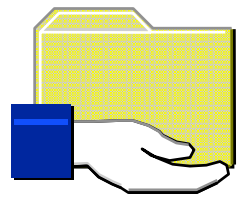
Ticket

Time and Authorization

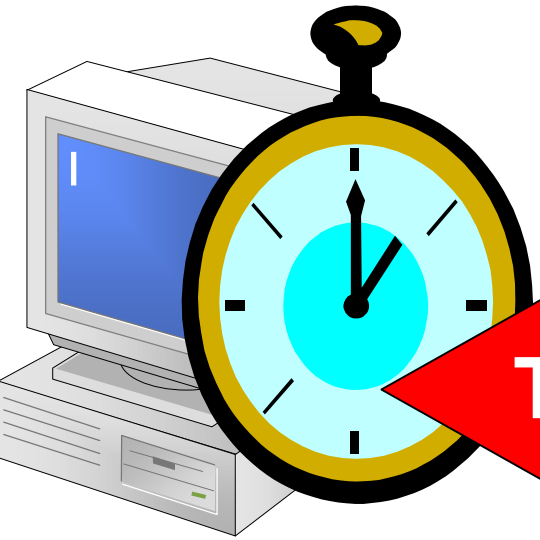
User can access resources on Server for Ticket Lifetime (10 hrs)







Dealing with Time Skew



Request for Services

TIME SKEW ERROR

CLIENT ADJUSTS FOR SKEW IF WITHIN TICKET LIFETIME

Session Key

Dealing with Time Skew

- Client can retry Authentication up to 4 times with Time Skew
- Kerberos then forces client to synch with server clock
- Can force this manually:
- Default skew is 5 minutes – can configure but larger skew is less secure

Windows Time Service

- Provides network clock synchronization
  - Windows 2000, Windows XP, Windows 2003
  - Implemented in w32time.dll
- Originally developed for Windows 2000
  - Kerberos requires clients be in sync
  - Windows 2003 provides increased accuracy and flexibility

W32Time in Security

- W32Time ensures that all client clocks are within allowable time skew
- Non-synchronized clocks are vulnerable to attack
  - Expired Ticket Acceptance attacks
  - Replay attacks

W32Time Time Protocols

- Simple Network Time Protocol (SNTP)
- Network Time Protocol (NTP)
- Network Protocol Interoperability

Simple Network Time Protocol

- Simplified protocol that does not provide the same accuracy as NTP
- Used in Windows 2000
- Uses the same packet format as NTP
- Primary difference from NTP is the lack of complex data grooming algorithms
- Maintained for backwards compatibility

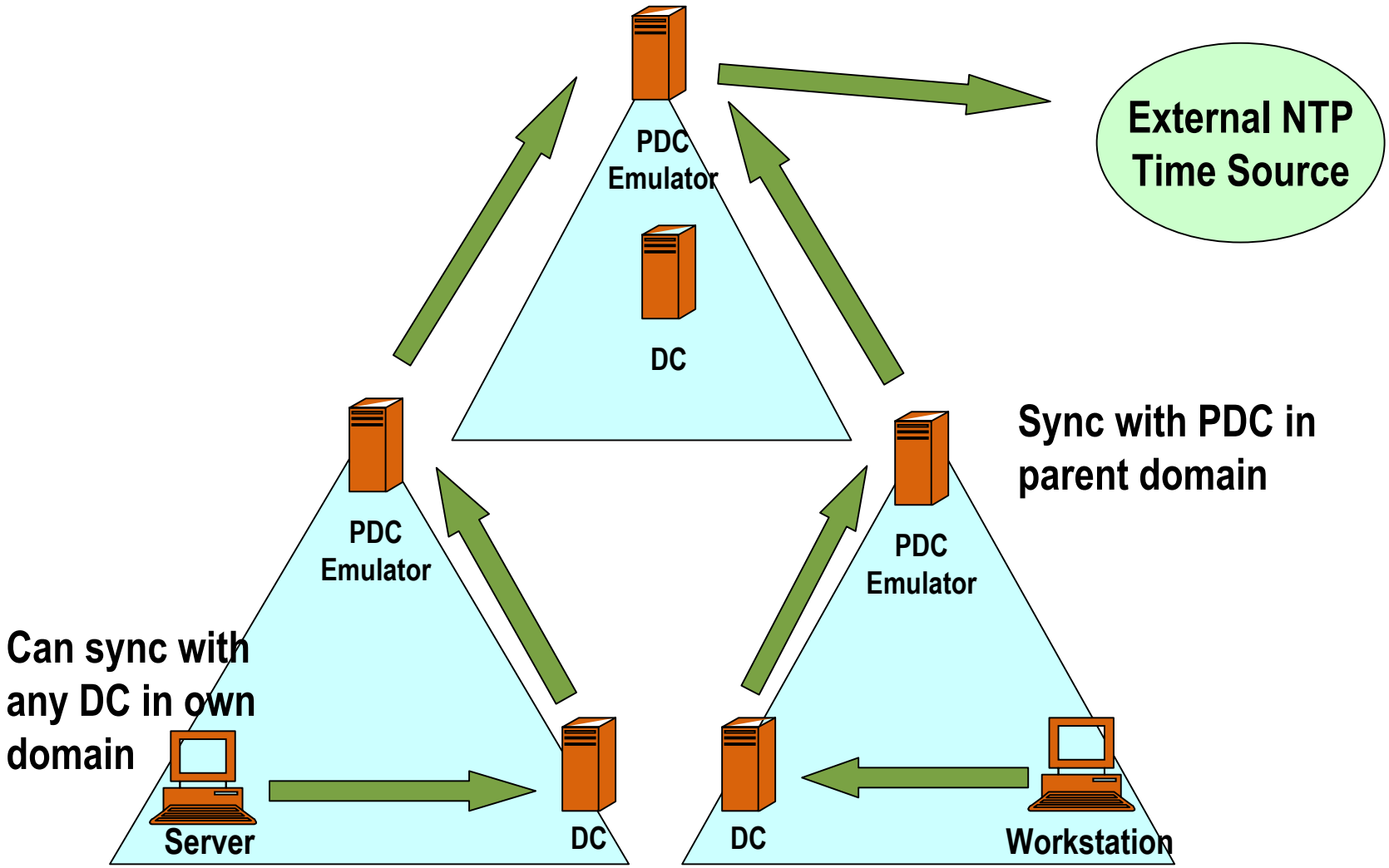
Network Time Protocol

- Supports SNTP
- RFC 1769 Port 123
- Default time sync protocol
  - Better error management
  - Support for multiple time sources
  - Increased stability
  - Synchronizes time within milliseconds
- Synchronizes time only, does not determine true time
  - Relies on a reference clock

NTP Security

- Domain case
  - Domain security used to enforce the authentication of time data
  - Shared-key authentication
  - Kerberos session key used to sign packets
  - Session key is obtained from Netlogon service
- Standalone
  - No authentication takes place
- No authentication available for time servers in trusted forests
- Cross Forest Time Synchronization
  - Will work but not secure

Configuring Domain Hierarchy–based Synchronization



Automatic Domain Time Configuration

- Machines check their time against their in-bound time partner
  - At Boot
  - 3 Intervals of 45 minutes
  - then every 8 hrs
  - At 8 hr interval if time must be adjusted by > 2 seconds, will halve the time to the next interval check.
    - Repeated until

      Synch. time is within 2 seconds

      OR – Interval frequency is 45 minutes
    - When local time is more reliable, interval changes back to 8 hrs.

Troubleshooting W32Time

- Tools
  - W32tm (Windows 2000)
    - -Source (-s)
    - -adj
    - -once
  - W32tm (Windows 2003)
    - /config – force reconfiguration of time service hierarchy
    - /stripchart
    - /resync

      Options to resync time with domain hierarchy or standalone

Errors Caused by Advancing System Time

- File Replication Service
  - Premature deletion of tombstones
  - Delayed change orders
- Active Directory
  - Incorrect conflict resolution
  - Restoration of backup might fail
  - Link value replication affected
  - Kerberos authentication might fail

Computer Is Unable to Synchronize

- Computer Is Unable to Synchronize
  - W32Time won't sync if time is off by more than 15 hours
  - Usually result of user misconfiguration
  - Time is generally off by whole days.
  - Flagged by W32tm events
  - Can cause authentication failure, Replication failure, etc.

Member Server Cannot Synchronize from the Domain Hierarchy

- System Log Events 38, 47, 29k, 36 are common when time is out of sync
- Solution:
  - On Broken machine…

    C:>w32tm /dumpreg /subkey:parameters

    Output will include:

    Type REG_SZ NT5DS

    If it is “NTP” then it was manually configurerd
  - Try to resynch:
    - W32tm /resync /rediscover (Win2003)
    - W32tm –once (Win2000)
  - Otherwise (Windows 2003 only):
    - Go to HKLM\system\system\ccs\services\w32time\parameters
    - Remove the NTP Server Registry key
    - W32tm /config /syncfromflags:domhier\

Summary

- Uses Network Time Protocol (NTP)
  - Keeps clocks synced within milliseconds
- Non-domain computers sync with time.microsoft.com if connected to the Internet
- Forest members follow Active Directory hierarchy to sync
- No Human Intervention Necessary!
- Occasionally, computers will get out of sync
  - Use w32tm /resync or /config
- Time must be synchronized between forests for Cross Forest Trust to be established (and work)
- Time synch across forests is not secure

HP WORLD 2003
Solutions and Technology Conference & Expo

Interex, Encompass and HP bring you a powerful new HP World.

interex
shared knowledge • shared power

encompass
AN HP USER GROUP

hp
invent