

MEN&MICE

What's new about DNS in
Windows 2008 Server

Overview

- DNS News
 - GlobalNames Zone
 - DNS Server improvements
 - DNS Client and DNS Server IPv6 Support
 - DNS Server DNSSEC Support
 - Read Only Domain Controller
 - Link Local Multicast Name Resolution (LLMNR, mDNS)
 - Peer Name Resolution Protocol (PNRP)

DNS Server - GlobalNames Zone

- The GlobalNames Zone
 - A new function to resolve single label hostnames
 - Similar function like WINS or NetBIOS over TCP/IP (NetBT)
 - WINS and NetBT are now in the „legacy mode“ state in Windows 2008
 - The GlobalNames Zone should replace WINS and NetBT for resolving single label names
 - For static, global Names like Server and central Services
 - Not for workstations and laptops
 - This new function allows the usage of short, single label names for central services without the need to maintain a global DNS Searchlist

DNS Server – GlobalNames Zone (GNZ) - Example

- The AD Zone „ad.firma.example“ contains the Address Records (A und AAAA)
- The entry for „fileserver.ad.firma.example.“

Server Manager (WIN-2008-1) | ad.firma.example 13 record(s)

Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[58], win-2008-1.ad.firma.e...	static
(same as parent folder)	Name Server (NS)	win-2008-1.ad.firma.example.	static
(same as parent folder)	Host (A)	192.168.1.215	static
(same as parent folder)	IPv6 Host (AAAA)	fd00:0000:0000:0000:0000...	static
fileserver	Host (A)	192.168.1.100	static
win-2008-1	Host (A)	192.168.1.215	30.09.2007 14:00:00
win-2008-1	IPv6 Host (AAAA)	fd00:0000:0000:0000:0000...	30.09.2007 14:00:00

DNS Server – GlobalNames Zone (GNZ) - Example

- The „GlobalNames“ Zone contains the Aliasnames
 - The names „fs“ and „server“ for „fileserver.ad.firma.example.“

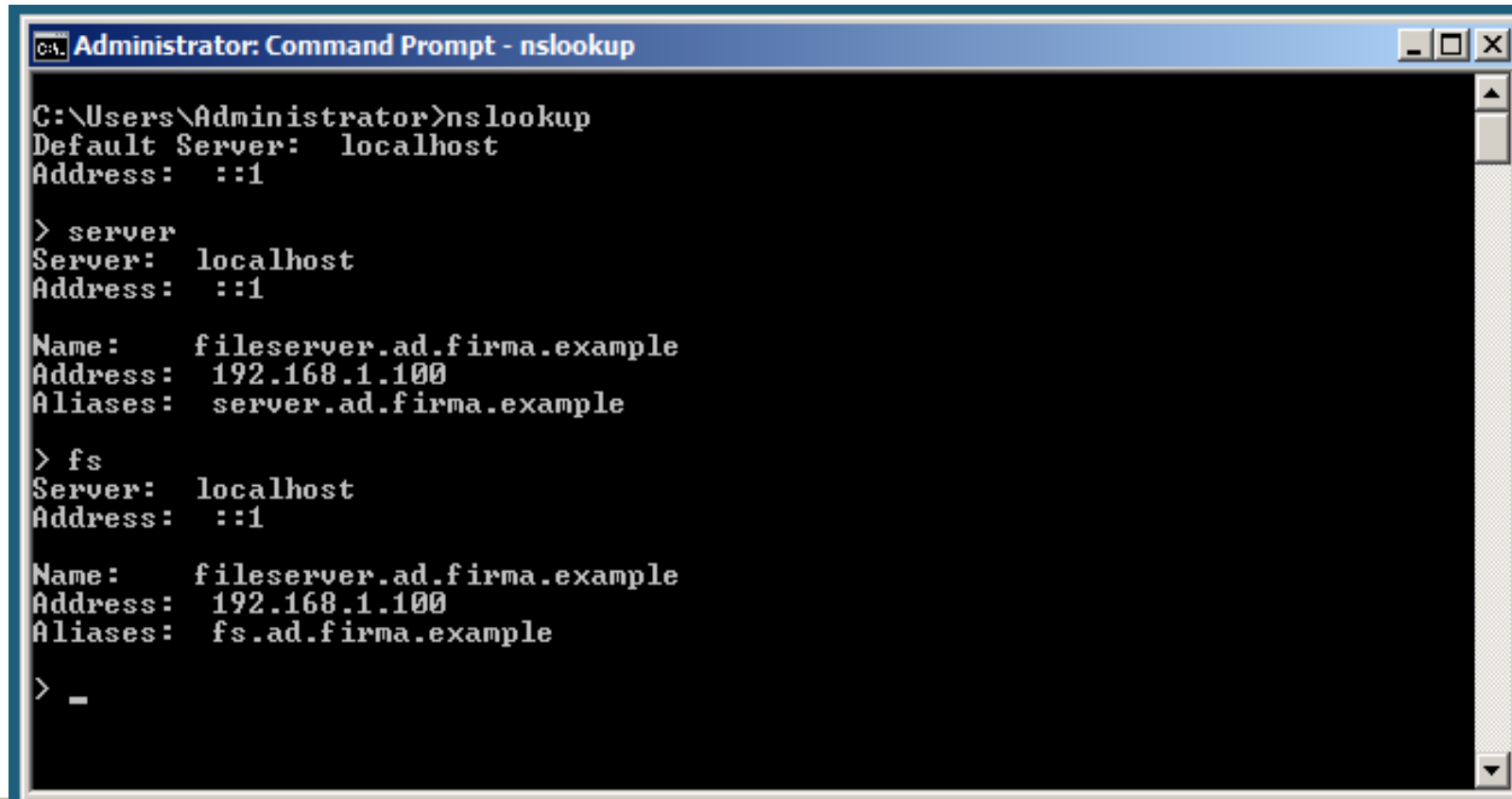
The screenshot shows the Windows Server Manager interface. The left-hand navigation pane is expanded to show the DNS server configuration for the domain 'ad.firma.example'. The 'GlobalNames' zone is selected, and the main pane displays a table of records for this zone.

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[1], win-2008-1.ad.firma.ex...	static
(same as parent folder)	Name Server (NS)	win-2008-1.ad.firma.example.	static
fs	Alias (CNAME)	fileserver.ad.firma.example	
server	Alias (CNAME)	fileserver.ad.firma.example	

The right-hand pane shows the 'Actions' menu for the 'GlobalNames' zone, with 'More Actions' visible.

DNS Server – GlobalNames Zone (GNZ) - Example

- Nameresolution for short names „fs“ and „server“ does now resolve into the real IP Address and also the full name



```
Administrator: Command Prompt - nslookup
C:\Users\Administrator>nslookup
Default Server:  localhost
Address:  ::1

> server
Server:  localhost
Address:  ::1

Name:    fileserver.ad.firma.example
Address: 192.168.1.100
Aliases: server.ad.firma.example

> fs
Server:  localhost
Address:  ::1

Name:    fileserver.ad.firma.example
Address: 192.168.1.100
Aliases: fs.ad.firma.example

> _
```

DNS Server – GlobalNames Zone (GNZ)

- The GNZ function must be enabled using „dnscmd“

```
dnscmd <servername> /config /enableglobalnamesupport 1
```

- A normal „ForwardZone“ using the “special” name „GlobalNames“ must be created
 - Ideally the GlobalNames Zone will only contain CNAME Alias pointer to the real DNS entries in other zones
 - The DNS Server then synthesizes a CNAME record in the target zone. The “GlobalNames” Zone is not seen in the answer. This can be irritating while troubleshooting from the outside.

DNS Server – GlobalNames Zone (GNZ)

- Where is the GNZ useful?
 - For companies that like to switch from a mixed DNS/WINS Environment to a pure DNS name resolution
 - mixed DNS/WINS environments are hard and costly to maintain, troubleshooting in such mixed environments is hard or even impossible
 - For networks with mixed IPv4 and IPv6 Environments
 - WINS and NetBT does not work under IPv6
 - For networks that would like to use „short“ Device-Names also in heterogeneous environments
 - Contrary to WINS and NetBT, the „GlobalZone“ is a pure DNS solutions and works without additional software on the all Operating Systems, like on Unix and MacOS X.

IPv6 Addresses in URLs

- The Windows Server 2008 TCP/IP Stack supports literal IPv6 Addresses in URLs according to RFC 2732 (Format for Literal IPv6 Addresses in URL's)
 - So it is possible to reach a web server with Address „FEDC:BA98:7654:3210:FEDC:BA98:7654:3210“ with the URL
`http://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:80/index.html`
 - This is not intended for “End-Users”
 - But helpful for Administrators and Troubleshooting
- Also supported in Windows Vista

IPv6 Addresses in „ipv6-literal.net“

- Many „legacy“ Applications cannot handle pure IPv6 Adresses, but they can work with DNS Names
 - IPv6 Addresses can be entered in Applications running on Vista and Windows Server 2008 as DNS names
 - To create such a IPv6 Address as DNS Name, all colons „:“ in the IPv6 Address must be replaced by dashes „-“ ...
 - ... and the 2nd Level Domain „ipv6-literal.net“ must be appended
 - The Windows Vista/2008 Server TCP/IP Stack will not send these DNS Names ending in “ipv6-literal.net” to the DNS resolver, instead it will connect directly to the derived IPv6 Address
 - Example: IPv6 Address
FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
will be converted into
FEDC-BA98-7654-3210-FEDC-BA98-7654-3210.ipv6-literal.net.

More news about the DNS Resolver

- The Windows 2008 DNS resolver now supports IDN Names according to RFC 3490 (Internationalized Domain Names)
 - IDN Domains can now also be used directly under Windows
Example: `http://www.öko.de`
- The DNS Resolver will now also register it's own IPv6 Address in DNS via dynamic DNS updates

DNS Server improvements

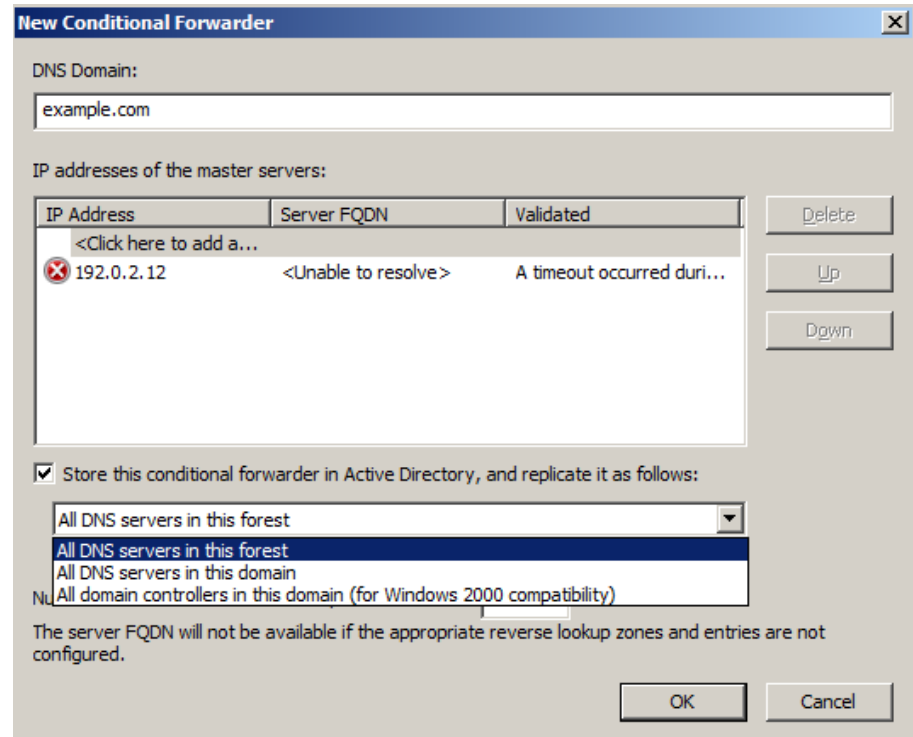
- AD-integrated zones will now be loaded in the background
 - A restart of the Windows 2000/2003 DNS Server in huge environments can take minutes up to one hour
 - The DNS Server is not available during this time
 - The Windows 2008 DNS Server load AD-Zones in the background

DNS Server improvements

- AD-Zone loading in background
 - When the Windows 2008 DNS Server starts
 - 1. it will create a list of Zones to load
 - 2. will load the „root-hints“
 - 3. will load all file based zones
 - 4. will start to answer to queries
 - 5. all remaining AD-integrated zones will be loaded in the background
 - If the DNS Server receives an query for a zone that has not been loaded, the zone will be loaded immediately and the query will be answered
 - The DNS Server will restart almost instantaneously

DNS Server improvements

- DNAME Support
 - The DNS Server in Windows 2008 now supports the DNAME RR (but only from the commandline)
- Replicating Forward Zones
 - When Active Directory is deployed, Conditional Forwarding Configurations (aka Forward Zones) can be replicated to all DNS Servers using AD replication



DNSSEC Support

- Unfortunately, there seems to be no additional support for DNSSEC in Windows 2008 Server
 - Same status as in Windows 2003

Read-Only Domain Controller

- Windows 2008 supports a special form of DC, the „Read-Only“ Domain Controller
 - The RODC contains a copy of the AD data, but this data cannot be changed
 - The RODC can be deployed in areas where the physical security of the server cannot be guaranteed
 - A RODC can be used for AD-integrated DNS Server in DMZ or similar areas
 - The RODC can be used for a DNS Server if AD replication of DNS Data is needed

Generic, non DNS specific improvements

- Windows 2008 Server Core Installation
 - A “low-fat” server installation without the bloat (no Desktop, IE, Media Player, .NET Framework etc.)
 - Ideal for DNS or DHCP Server deployments
 - Admin needs to master the commandline and it's tools!
- Almost all configuration can now be done from the commandline, many can be done from the GUI
- Build-in virtual machine technology (Hyper-V)
 - Can run non-Windows OS (like Linux)
 - Needs 64Bit CPU

Prediction of adoption

- Windows 2008 server brings some substantial value for most customers
 - Will see quick(er) adoption in the field (compared to Vista)
 - Probably most migrations will be in 2009

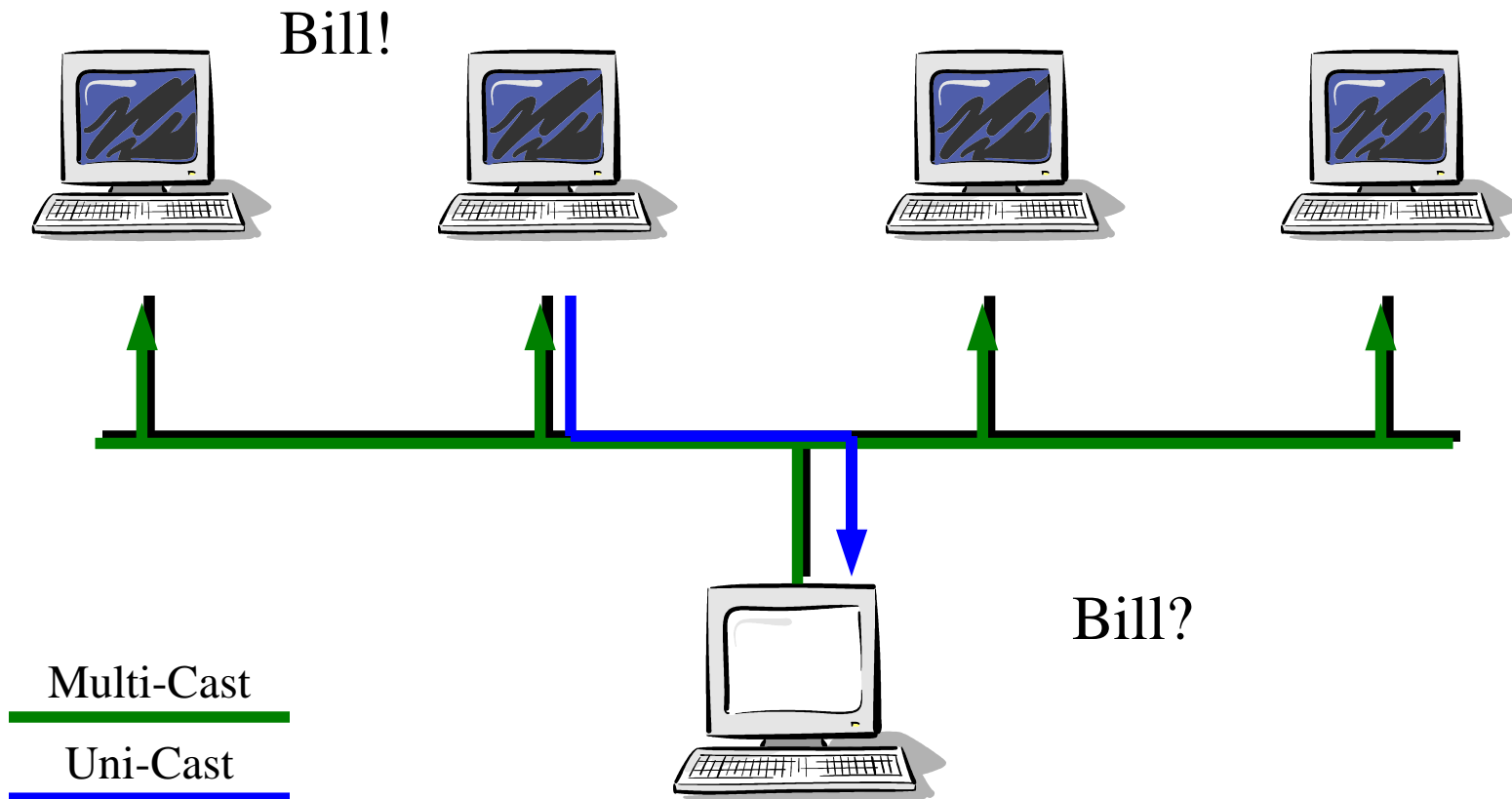
Link Local Multicast Name Resolution (LLMNR)

- LLMNR offers DNS-like name resolution without a DNS Server ...
 - ... but only in the local network segment (therefore „Link-Local“)
 - ... works independent from the DNS Client
 - own Cache
 - Works on Port 5355 (not 53 like DNS)
- Application area
 - Small networks without DNS Server (meeting room, small office etc)
 - Home-User
 - Ad-Hoc Wireless Networks
- Defined in RFC 4795 (informal, January 2007)
- Similar functions, but not compatible with mDNS (multicast DNS) of Apple (Bonjour/Bonjourvous)

Link Local Multicast Name Resolution (LLMNR)

- LLMNR, how does it work
 - Request will be send to the multicast addresses „FF02::1:3“ (IPV6) or „224.0.0.252“ (IPv4)
 - Devices in the same network segment owning the requested hostname send an answer per Unicast
- The TCP/IP stack checks on startup if the own hostname is unique in the local network, using LLMNR
 - If the hostname is not unique, the TCP/IP stack will not send LLMNR answers but will check every 15 minutes for uniqueness of its own hostname
- Namequeries for „hostname.local“ will be automaticlly resolved using a LLMNR fro „hostname“. The DNS TLD „.local“ can therefore not be fully used (needs further investigation).

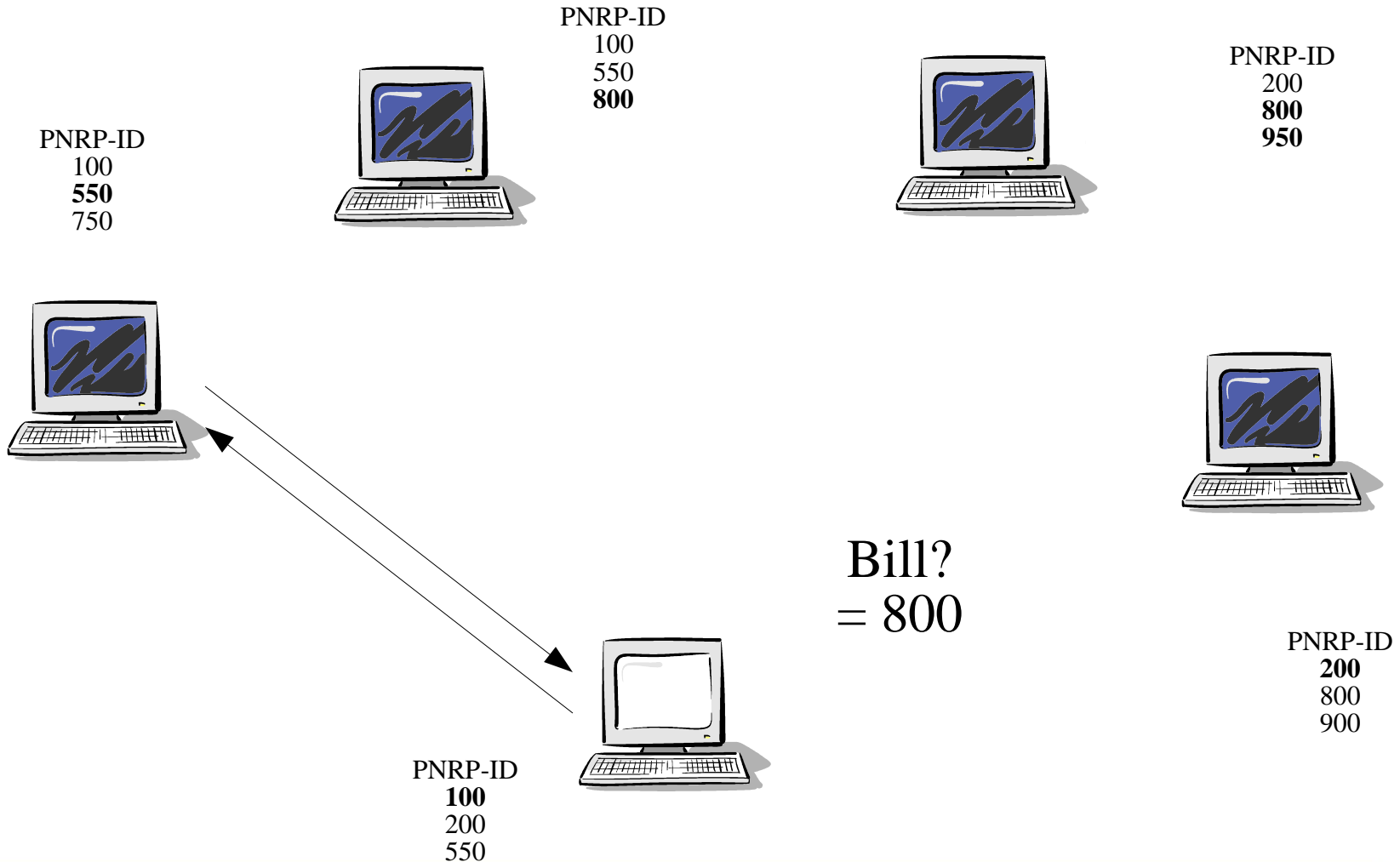
Link Local Multicast Name Resolution (LLMNR)



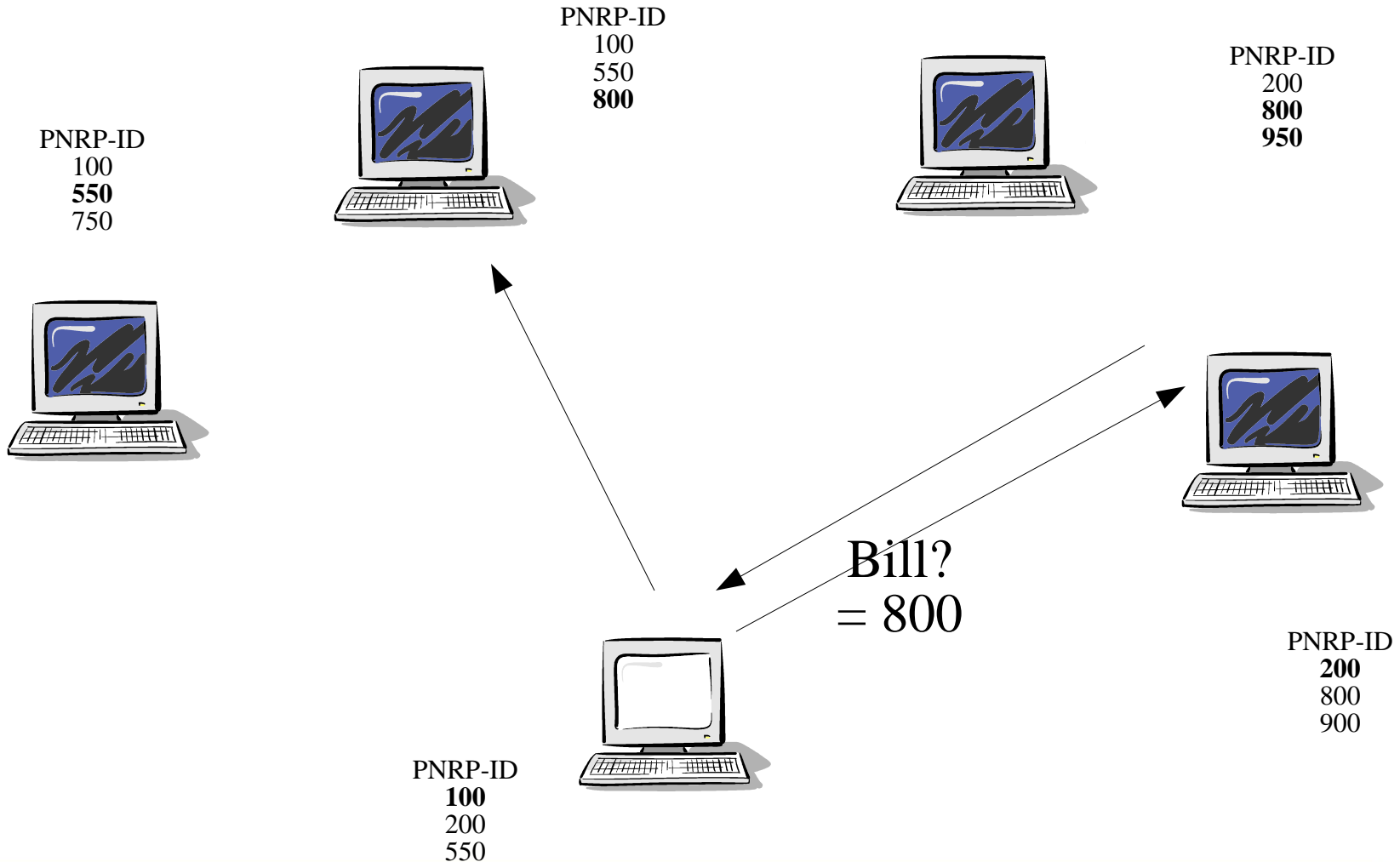
PNRP – Peer Name Resolution Protocol

- The Peer Name Resolution Protocol is another technique to resolve names without central DNS Server
 - PNRP can resolve also “Services” besides “hosts”
 - PNRP works exclusively over IPv6, it cannot be used in IPv4 networks
 - PNRP name resolution is using a 256bit PNRP-ID, created from an optional security key and the name of the endpoint or service
 - The destination host or service is located using iterative name resolution among peer system. The difference in the PNRP-ID is used to contact neighbouring peer nodes about the name or service searched. A small difference in the PNRP-ID is seen as P2P-related proximity inside the PNRP-cloud (but not geographical or network-proximity).

PNRP – Peer Name Resolution Protocol



PNRP – Peer Name Resolution Protocol



PNRP – Peer Name Resolution Protocol

– Technical information

- The PNRP Service is using Port 3540 (UDP and TCP) for communication
- PNRP Names can be resolved by existing applications by using the reserved DNS Zone „pnrp.net“. The Domain „pnrp.net“ is reserved in Windows Vista/2008 Server for PNRP Nameresolution
 - Example: `ping <servicenamne>.pnrp.net.`
- The PNRP v2-Protocol is not compatible with PNRP-Protocol (Version 1) used in Windows XP

PNRP – Peer Name Resolution Protocol

- Rating of the PNRP Function:
 - The success of PNRP will be bound to popular applications
 - PNRP is desirable for Network-Administrators, because it cannot be controlled centrally
 - commercial P2P applications like Skype already have working solutions for the P2P Service location problem, it remains to be seen if they make use of PNRP
 - PNRP must prove that it is scalable and secure

Links

- New Networkfeatures in Windows Server 2008 and Windows Vista
 - http://www.microsoft.com/germany/technet/itsolutions/network/evaluate/new_network.msp
- Windows 2008 DNS Server as Server Core Install and Hardening
 - <http://technet.microsoft.com/en-us/library/cc264469.aspx>
- LLMNR
 - The Cable Guy - November 2006 - Link-Local Multicast Name Resolution
 - <http://www.microsoft.com/technet/community/columns/cableguy/cg1106.msp>
 - Link-local Multicast Name Resolution (LLMNR)
 - <http://www.faqs.org/rfcs/rfc4795.html>
 - Wikipedia Zeroconf
 - <http://en.wikipedia.org/wiki/Zeroconf>

Links

– PNRP

– Windows Peer-to-Peer Networking

– <http://technet.microsoft.com/en-us/network/bb545868.aspx>

– Microsoft P2P Blogs

– <http://blogs.msdn.com/p2p/>

– Peer Name Resolution Protocol

– <http://technet.microsoft.com/en-us/library/bb726971.aspx>

– Understanding PNRP Clouds

– <http://blogs.msdn.com/p2p/archive/2007/06/12/understanding-pnrp-clouds.aspx>

– IPv6

– IPv6 Literal Addresses - Format for Literal IPv6 Addresses in URL's

– <http://www.faqs.org/rfcs/rfc2732.html>

– The Cable Guy - October 2005 - Changes to IPv6 in Windows Vista and Windows Server 2008

– <http://www.microsoft.com/technet/community/columns/cableguy/cg1005.mspx>