MEN&MICE

New DNS Technologies in the LAN

Everything you always wanted to know about mDNS, DNS-SD, LLMNR and similar technologies but were too afraid to ask.

Carsten Strotmann, Men & Mice Services

What's in it?

- Overview on DNS related technologies for Name- and Service-Resolution
  - Multicast DNS (mDNS)
  - DNS based Service Discovery (DNS-SD)
  - Link Local Multicast Name Resolution (LLMNR)
  - Peer Name Resolution Protocol (PNRP)

Motivation??

- Men & Mice is not in the Ad-Hoc Network or P2P Business....
  - ... and is not involved in the team creating these protocols
- ... but we do DNS Audits and DNS Troubleshooting
- ... we want to know how these new technologies can affect networks and DNS in “real-life”
- Phase 1: Research and Lab-Testing
- Phase 2: Real World numbers

mDNS

(Multicast DNS)

mDNS – Multicast DNS

- Multicast DNS is used to resolve DNS Records in link-local networks without a central DNS Server
- Uses port 5353
- Uses multicast addresses
  - 224.0.0.251 (IPv4)
  - FF02::FB (IPv6)
- mDNS Packet Format 99% compatible with "Plain-Old-DNS"

mDNS – Multicast DNS

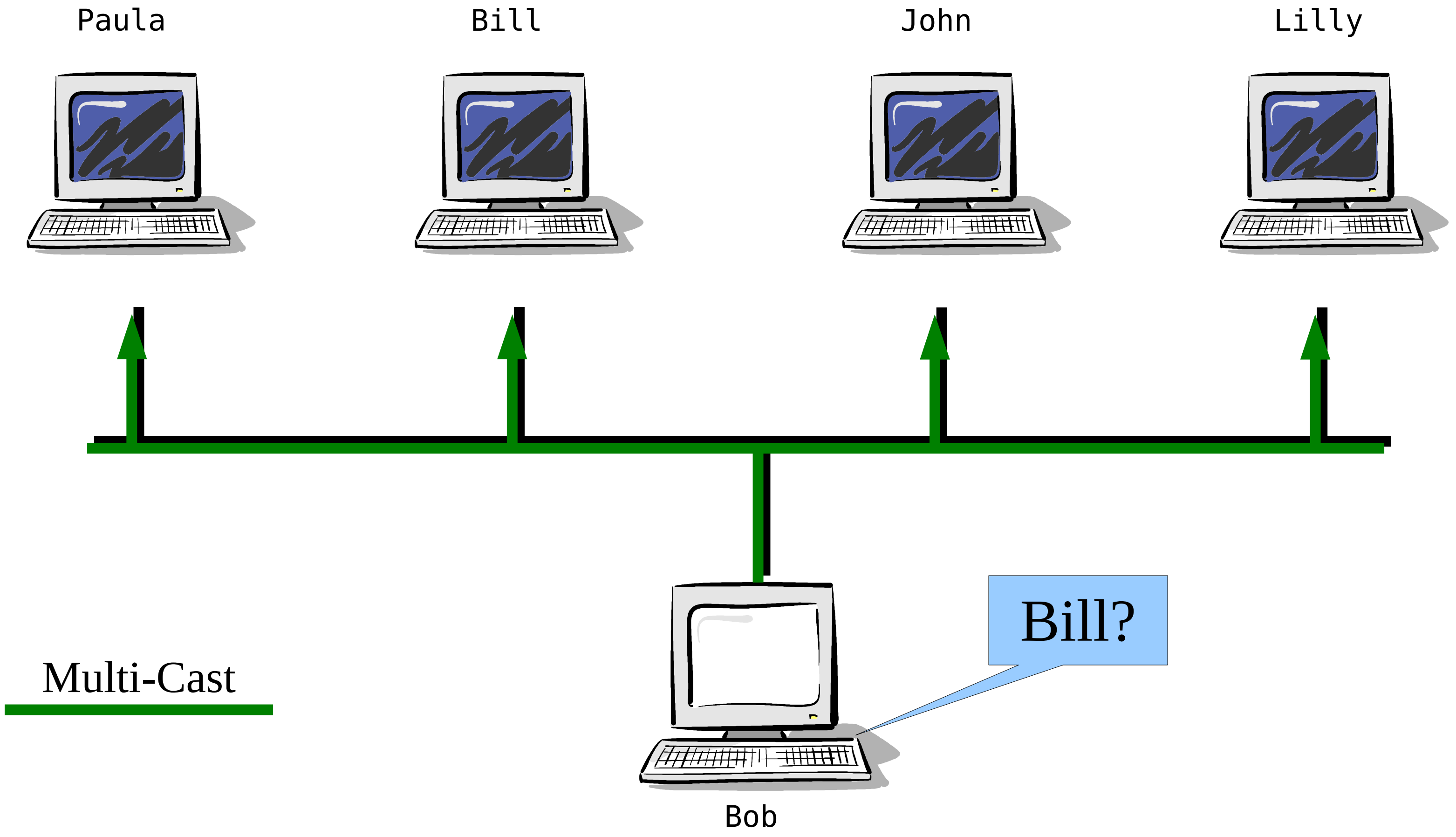
- 3 different Query behaviours
  - One-Shot queries
  - Multiple responses
  - Ongoing queries

- One-Shot queries can be done with “DIG”

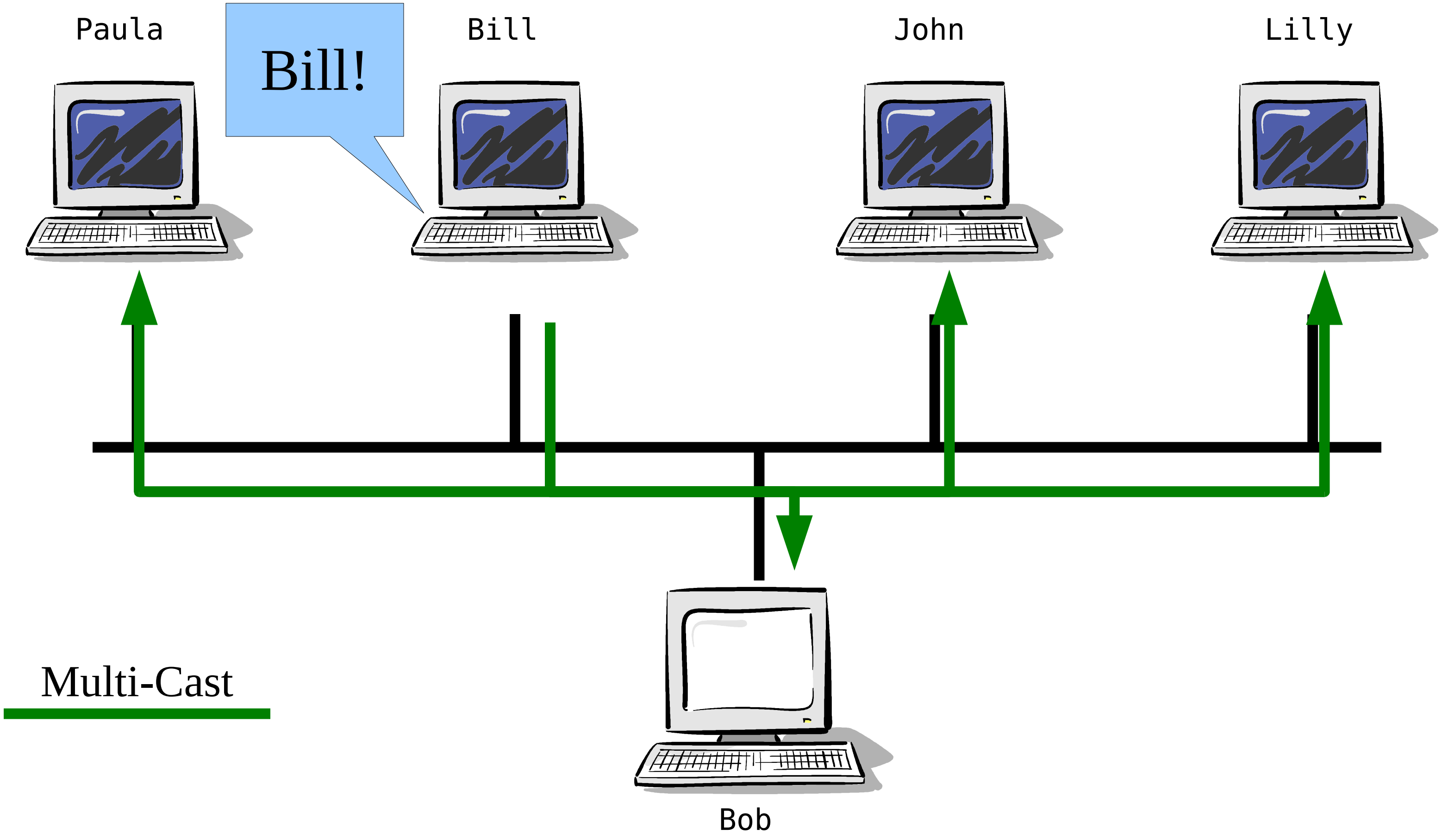
```
dig -p 5353 @224.0.0.251 _ssh._tcp.local ptr
```

MEN&MICE

mDNS – Multicast DNS



mDNS – Multicast DNS



mDNS – Multicast DNS

- Prevent “chattiness”
  - Known Answer List (with TC Bit set, it can stretch multiple packets),
    - “Known Answer List” is not authoritative
- exponential backoff / no constant query rate
- use of TTL, query before record is expired/removed from cache
- multicast answers (other clients listen and fill their cache)
  - mDNS Cache is independent from DNS cache

mDNS – Multicast DNS

- Answer Suppression:
  - If a host is preparing a response and sees a response from another host with the same answer as its own, then it can suppress its own response.

mDNS – Multicast DNS

- Name collision detection:
  - choose a name, send a mDNS query(s) for Record Type "any"
  - 3 queries, 250ms waiting time (750ms total)
  - Tiebreaker algorithm for race-condition, chosen name in authority section.
    - This type of conflict is resolved in favour of the record with the lexicographically later content (Record Class, Record Type, RData)
  - if a naming collision is detected in operation, the client goes back to probing state

mDNS – Multicast DNS

- Announcing a name (or service)
  - Send a mDNS response record containing all records of this client with cache flush bit set
    - *“When a resource record appears in the answer section of the DNS Response with the "cache flush" bit set, it means, "This is an assertion that this information is the truth and the whole truth, and anything you may have heard before regarding records of this name/type/class is no longer valid"*

mDNS – Multicast DNS

- Removing a name (or service)
  - Send a response packet with TTL set to zero (“0”)

mDNS – Multicast DNS

- mDNS is using the “reserved” namespace “.local”
  - So all requests for `<something>.local` will go to mDNS instead of classic DNS
  - For some operating systems, fallback to classic DNS is possible
- mDNS packets can be up to 9000bytes/packet
- mDNS is using UTF-8 encoded names

mDNS – Multicast DNS

- Possible Operational issues:
  - Applications sending mDNS queries to classic DNS
  - Applications sending mDNS packets to classic DNS Servers
  - A classic DNS Domain ".local" is hidden
    - We see ".local" quite often in MS based enterprise networks with Active Directory deployed

DNS-SD

(DNS Service Discovery)

DNS-SD – DNS based Service Discovery

- Technology to discover Services on a network
  - Works link-local as well as globally
- Uses existing DNS Records in a “creative” way
- DNS-SD is using the service types defined for SRV records
  - Like “_http._tcp” for a webserver

DNS-SD – DNS based Service Discovery

- Discovery a service on the network
  - First the DNS-SD client sends a query for a PTR Record for the domain

    `<service>.<transport>.local.`

    or

    `<service>.<transport>.<browse-domain>`
  - This will return a list of PTR records if the service exists on the network. The PTR Records
    - (m)DNS will return 0 or more of

      `<instance>.<service>.<transport>.<domain>`

DNS-SD – DNS based Service Discovery

- Application will display the available instance names
  - Instance names are in UTF-8
    - This looks unfamiliar (cluttered) for “old-skool” DNS admins (like me ;)

```
Carsten's\032little\032Web-Server._http._tcp.example.com.
```

DNS-SD – DNS based Service Discovery

- Services can have subtypes
  - For example for a password protected version of the protocol
  - Subtypes:

```
<subtype>._sub.<service>.<transport>.<domain>
```

- Subtypes are optional

DNS-SD – DNS based Service Discovery

- When the user has selected a service instance, DNS-SD will lookup the parameters and hostname(s) for the service
  - The hostname is stored in SRV records
  - The Parameters are stored as “key=value” pairs in TXT records

DNS-SD – DNS based Service Discovery

- Some real world Zonefile examples:
  - The PTR Records:

```
_http._tcp  3600 IN PTR     \032*\032Zeroconf._http._tcp.dns-sd.org.
_http._tcp  3600 IN PTR     \032*\032Multicast\032DNS._http._tcp.dns-sd.org.
_http._tcp  3600 IN PTR     \032*\032CNN,\032World\032news._http._tcp.dns-sd.org.
_http._tcp  3600 IN PTR     \032*\032BBC,\032World\032news._http._tcp.dns-sd.org.
```

DNS-SD – DNS based Service Discovery

- Some real world Zonefile examples:
  - The SRV and TXT Records for “zeroconf.org” Website:

```
\032*\032Zeroconf._http._tcp 3600 IN SRV 0 0 80 zeroconf.org.
\032*\032Zeroconf._http._tcp 3600 IN TXT "path=/"
```

DNS-SD – DNS based Service Discovery

Some Demo

(a RIPE meeting is a nice
DNS-SD and mDNS Playground)

DNS-SD – DNS based Service Discovery

- Two protocol enhancements for DNS-SD haven't been implemented in “real-world” DNS so far (to my knowledge)
  - DNS Update Leases (DNS-UL)
  - DNS Long lived Queries (DNS-LLQ)

DNS-SD – DNS based Service Discovery

- MDNS / DNS-SD “in the wild”
  - Apple MacOS X 10.2 and up (Rendevous/Bonjour)
  - FreeUnix (Linux, xBSD, Solaris)
    - Avahi (also available for MacOS X)
    - KDE and Gnome integration
    - A number of Applications using it
  - Windows XP/Vista (Implementation from Apple)
  - Both implementations are available as OpenSource Software
  - Language bindings for all major programming languages exist

DNS-SD – DNS based Service Discovery

- Possible Operational issues:
  - DNS Admins creating wrong static DNS-SD entries
    - Creating DNS problems
  - DNS-SD clients auto-register using DDNS, causing trouble
    - "*what if I register "_ldap._tcp." in the same zone on the same BIND DNS Server via dynamic update that also MS Active Directory is using?*"
  - DNS Bandwidth, Server load?

LLMNR

(Link Local Name Resolution)

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
- Defined in RFC 4795 (informal, January 2007)
- Enabled in MS Vista and Windows Server 2008 (aka Longhorn)
- Similar functions, but not compatible with mDNS (multicast DNS) of Apple (Bonjour/Rendezvous)

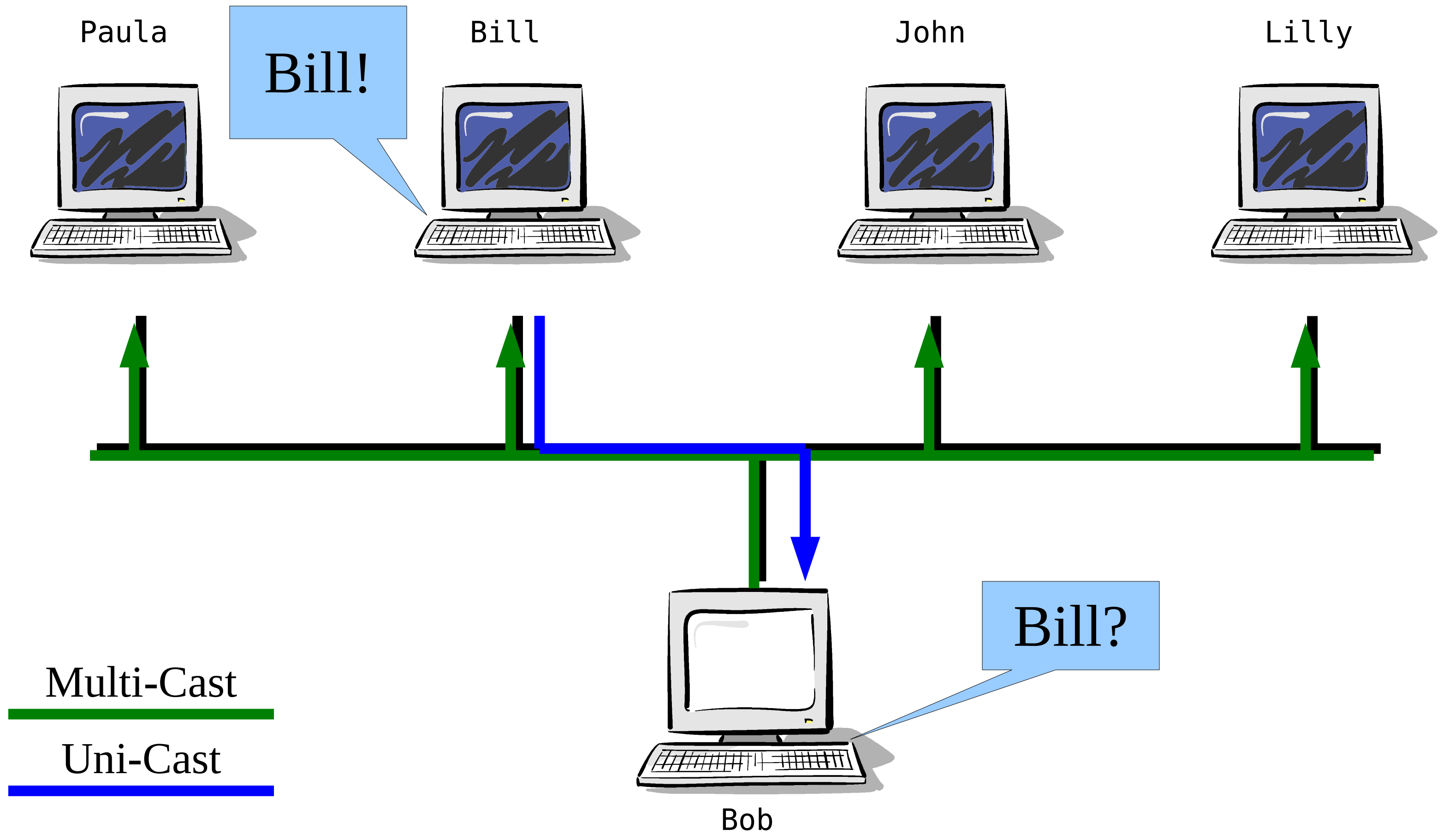
Link Local Multicast Name Resolution (LLMNR)

- LLMNR, how does it work
  - Request will be send to the multicast addresses „FF02::1:3“ (IPV6) or „224.0.0.252“ (IPv4)
    - Packets are similar, but not identical to classic DNS Packets
    - Existing tools cannot be used
  - Devices in the same network segment owning the requested hostname send an answer per Unicast

Link Local Multicast Name Resolution (LLMNR)

- LLMNR, how does it work
  - 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
  - Name queries for „hostname.local“ will be automatically resolved using a LLMNR for „hostname“. The (unicast) DNS TLD „.local“ is hidden.

Link Local Multicast Name Resolution (LLMNR)



Link Local Multicast Name Resolution (LLMNR)

- Possible Operational issues:
  - Applications sending LLMNR queries to classic DNS
  - A classic DNS Domain “.local” is hidden
    - We see “.local” quite often in MS based enterprise networks with Active Directory deployed

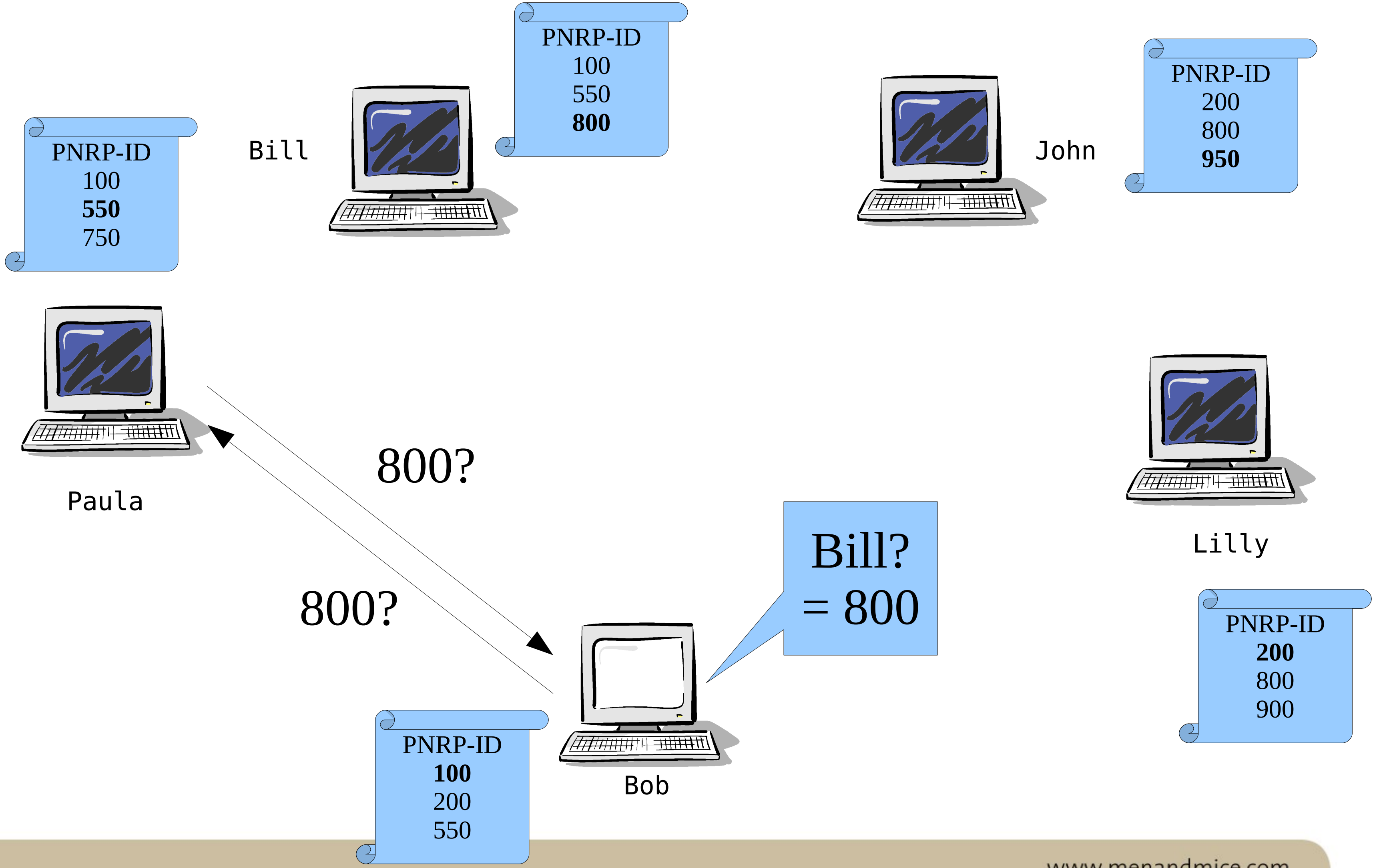
PNRP

(Peer Name Resolution Protocol)

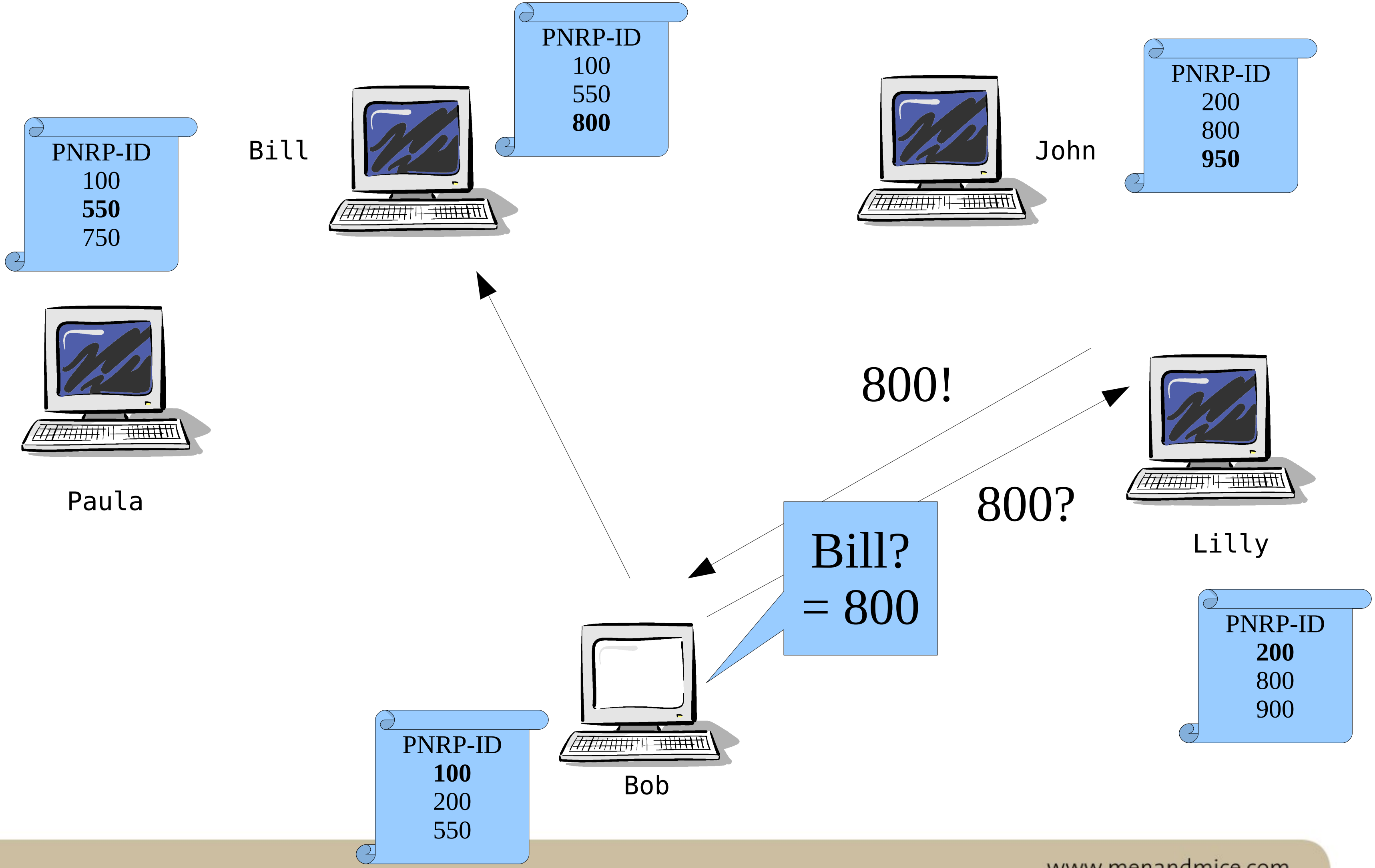
PNRP – Peer Name Resolution Protocol

- 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 is not specified for 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 using a distributed hashing algorithm.

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

- Possible Operational issues:
  - Applications sending PNRP queries to classic DNS
    - PNRP.NET Domain returns “SERVFAIL”, will not be cached

Closing time

- You know that you have mDNS, DNS-SD, PNRP or LLMNR running in your network, if ...
  - ... you see requests for (Apple mDNS)

    ```
    1.0.0.127.dnsbugtest.1.0.0.127.in-addr.arpa.
    ```

  - ... you see requests for DNS-SD browsing

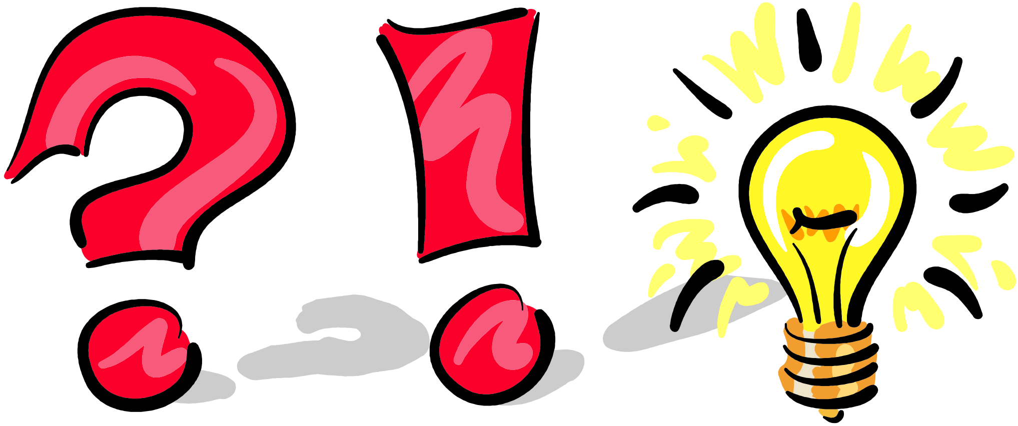
    ```
    b._dns-sd._udp.<your-local-domain>
    lb._dns-sd._udp.<your-local-domain>
    ```

  - ... you see requests for “.local” when you do not have a “.local” DNS Domain (LLMNR or mDNS)

What's next

- Men & Mice DNS Performance Monitor for mDNS, PNRP and LLMNR
- Actively looking for mDNS, DNS-SD, LLMNR and PNRP in live networks
- Update Report in about 12 month (next RIPE Meeting in Amsterdam)

The END



Requests, information and inquiries welcome.
Please contact me at
carsten@menandmice.com

Links

- Zeroconf / Bonjour / DNS-SD / mDNS
  - Zeroconf Websites
    - http://zeroconf.org
    - http://dns-sd.org
    - http://multicastdns.org
  - Zeroconf Book
    - Zero Configuration Networking: The Definitive Guide
      - By Stuart Cheshire, Daniel H. Steinberg
      - http://www.oreilly.com/catalog/bonjour/index.html
  - Avahi - http://avahi.org
  - Bonjour from Apple - http://apple.com/bonjour
    - For Windows - http://www.apple.com/support/downloads/bonjourforwindows.html

Links

- LLMNR
  - The Cable Guy - November 2006 - Link-Local Multicast Name Resolution
    - http://www.microsoft.com/technet/community/columns/cableguy/cg1106.mspx
  - Link-local Multicast Name Resolution (LLMNR)
    - http://www.faqs.org/rfcs/rfc4795.html
  - Wikipedia Zeroconf
    - http://en.wikipedia.org/wiki/Zeroconf

MEN&MICE

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