

# XTSeminars

## MICROSOFT WINDOWS SERVER 2008 R2 AND WINDOWS 7 DIRECTACCESS

Make the transition to IPv6 and reap the benefits

Presented by  
John Craddock

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTSeminars Ltd 2010



### **John Craddock**

Created by John Craddock, XTSeminars Ltd brings you world class IT seminars written and delivered by experts. As an infrastructure and security architect he has designed and implemented global distributed IT solutions, providing services to industry leaders including Microsoft.

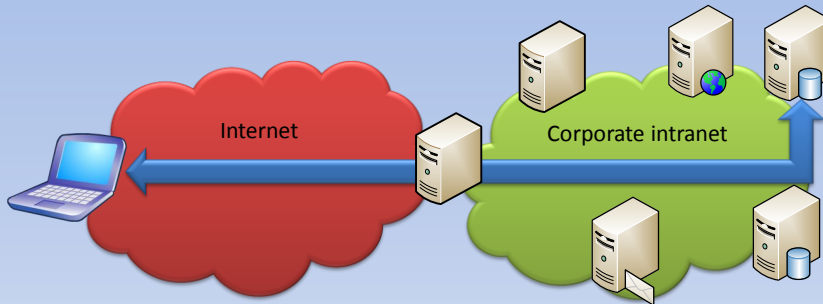
John is an international speaker, delivering technical seminars, sessions and keynotes around the world and is a featured speaker at major IT conferences such as Microsoft TechEd.

John Craddock can be engaged as a consultant by contacting him directly:  
[John.craddock@xtseminars.co.uk](mailto:John.craddock@xtseminars.co.uk)

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTSeminars Ltd 2010

**XTSeminars**

## DirectAccess – Simple?



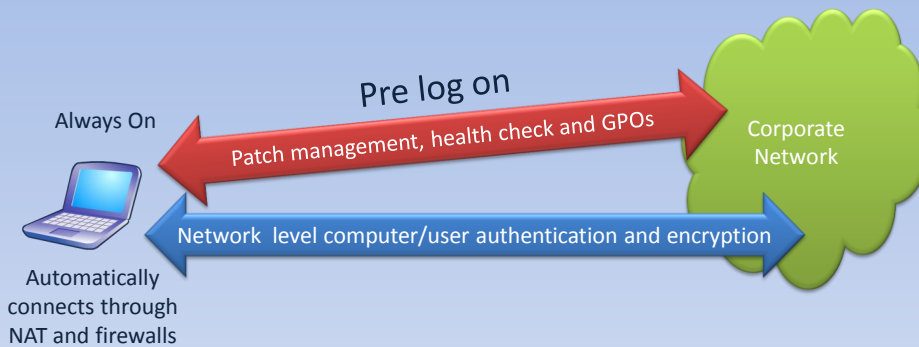
- ✘ When a DirectAccess client connects to the Internet it is automatically connected to the corporate intranet
  - No user action required

3

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## A VPN on Steroids



*VPNs connect the user to the network*  
*DirectAccess extends the network to the remote computer and user*

4

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Requirements

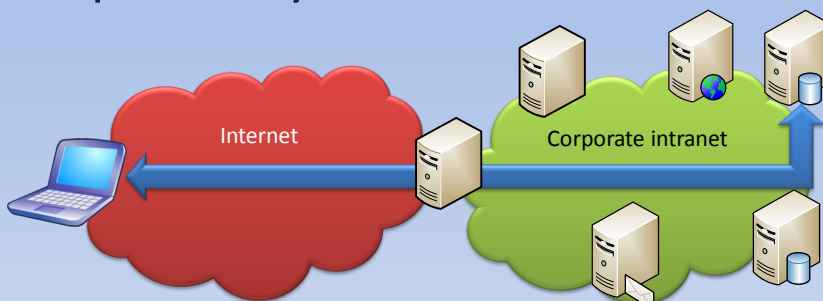
- ✘ DirectAccess Clients
  - Windows 7 Enterprise or Ultimate
  - Windows Server 2008 R2
- ✘ DA Server
  - Windows 2008 R2
  - Forefront Unified Access Gateway (UAG)
    - Running on Windows 2008 R2 Standard or Enterprise
  - Two IPv4 public addresses (more for a UAG array)
- ✘ Both the client and server must be domain joined





5

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Simple? May Be Not

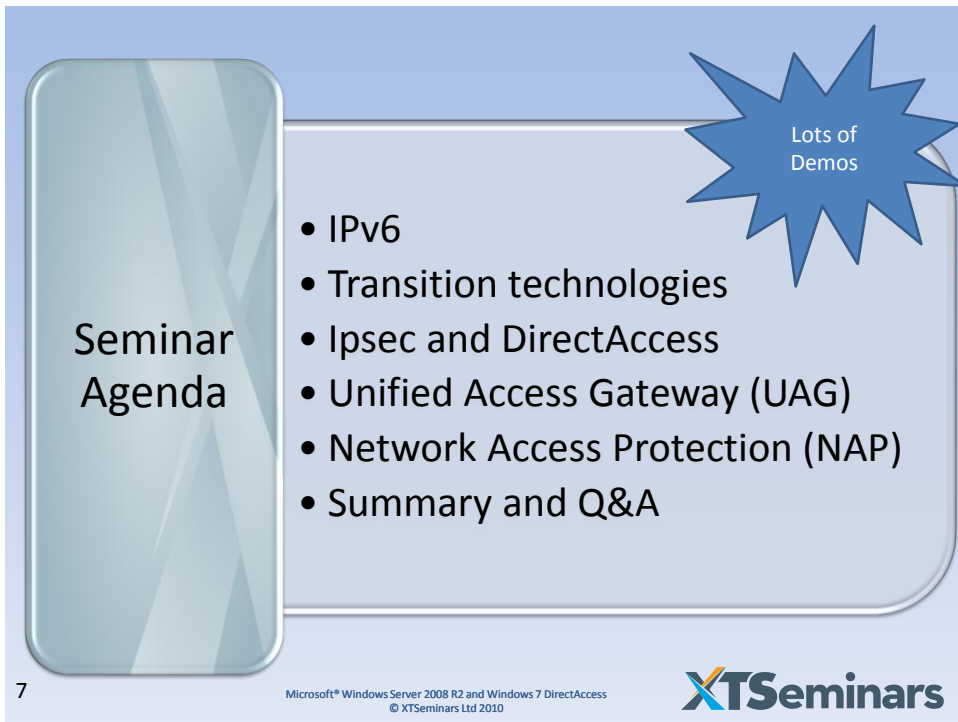


-  Tunnelling technologies for the Internet and intranet to support IPv6 over IPv4
-  Internet tunnelling selection based on client location – Internet, NAT, firewall
-  Encryption/authentication of Internet traffic (end-to-edge/end-to-end)  
PKI required
-  Client location detection: Internet or corporate intranet

6

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**



**Seminar Agenda**

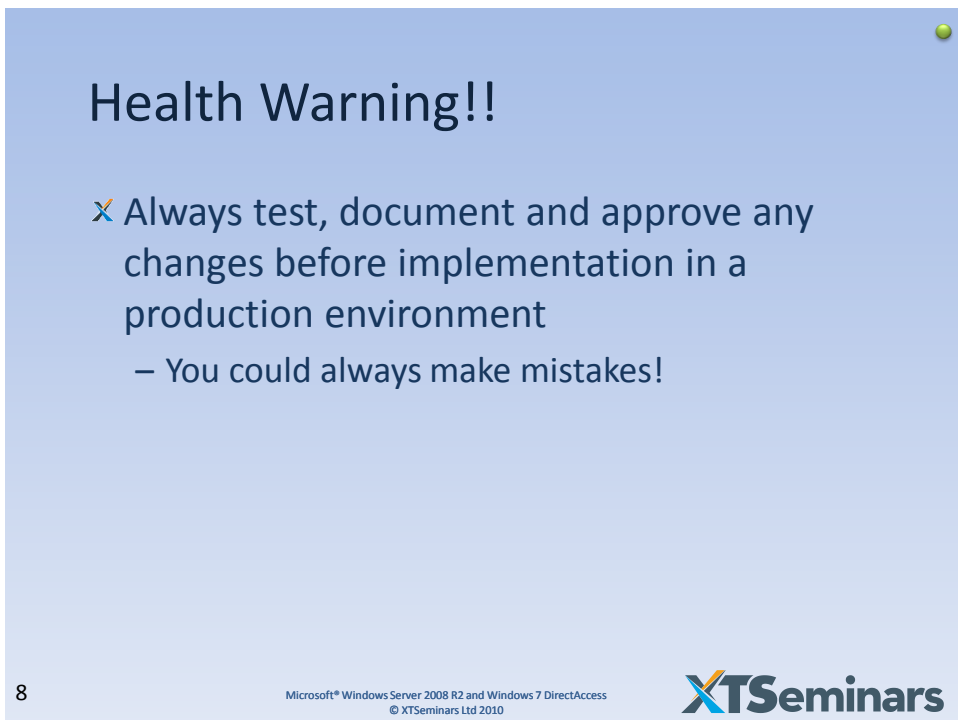
- IPv6
- Transition technologies
- Ipsec and DirectAccess
- Unified Access Gateway (UAG)
- Network Access Protection (NAP)
- Summary and Q&A

Lots of Demos

7

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**



## Health Warning!!

- ✘ Always test, document and approve any changes before implementation in a production environment
  - You could always make mistakes!

8

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Legal Stuff

Every effort has been made to make this seminar as complete and as accurate as possible but no warranty or fitness is implied. The presenters, authors, publisher and distributor assume no responsibility for errors or omissions, or for damages resulting from the use of the information contained herein.

Names identifying the directory and associated objects are fictitious and are not intended to represent any organizations or people.

We have endeavored to provide trademark information about products mentioned in the seminar materials by the appropriate use of capitals. However, we cannot guarantee the accuracy of this information. Use of a term in these materials should not be regarded as affecting the validity of any trademark or service mark.

Active Directory®, Microsoft® Windows® 2000, Microsoft® Windows® Server 2003 and Microsoft® Excel® are either registered trademarks or trademarks of Microsoft Corporation in the United States and /or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

© All materials are copyright XTseminars Ltd and may not be reproduced in any form without prior written permission

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

9

## Seminar Agenda

- IPv6
- Transition technologies
- Ipsec and DirectAccess
- Unified Access Gateway (UAG)
- Network Access Protection (NAP)
- Summary and Q&A

10

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

Ethernet adapter Local Area Connection:

```

Connection-specific DNS Suffix . . . . . : 
Description . . . . . : Microsoft Virtual Machine Bus Network Adapter
Physical Address. . . . . : 00-15-5D-0B-04-6C
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
IPv6 Address. . . . . : fd00:9999:0:2:ed99:dda3:ff0b:ec63(Preferred)
Temporary IPv6 Address. . . . . : fd00:9999:0:2:a48f:e34e:2283:9d1c(Preferred)
Link-local IPv6 Address . . . . . : fe80::ed99:dda3:ff0b:ec63%12(Preferred)
IPv4 Address. . . . . : 10.20.19.11(Preferred)
Subnet Mask . . . . . : 255.255.128.0
Default Gateway . . . . . : 
DHCPv6 IAID . . . . . : 251663709
DHCPv6 Client DUID. . . . . : 00-01-00-01-12-1D-50-16-00-15-5D-0B-04-6C
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                          fec0:0:0:ffff::2%1
                          fec0:0:0:ffff::3%1
NetBIOS over Tcpi. . . . . : Enabled
  
```

Tunnel adapter isatap.{8C8B1176-A8F8-4CB7-93B2-971C461C6F78}:


```

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . : 
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
  
```

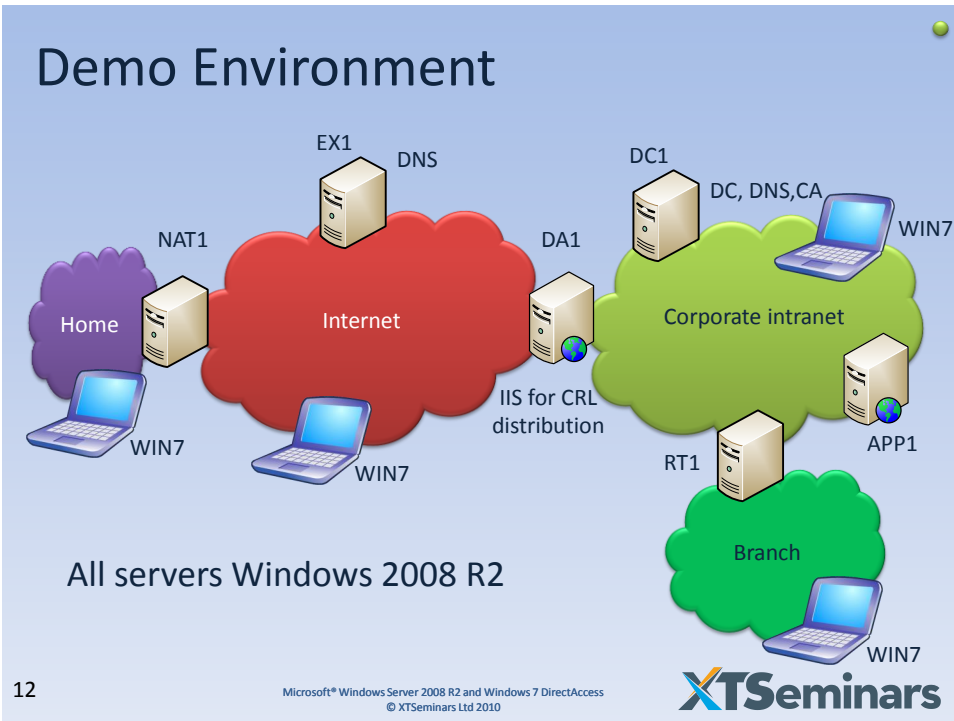
Tunnel adapter Local Area Connection\* 11:

```

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . : 
Description . . . . . : Microsoft Teredo Tunneling Adapter
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
  
```



Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## IPv6

- ✘ IPv6 natively supports many of the extensions that have been added to IPv4
  - IPSec
  - QoS
- ✘ IPv6 adds
  - An enormous address space (128-bits)
    - 340,282,366,920,938,463,463,374,607,431,768,211,456 possible addresses
  - An efficient routing hierarchy
  - Automatic configuration (DHCP may not be required)
  - New protocol for interaction with neighbouring nodes

13

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## Drawbacks

- ✘ Requires a new routing infrastructure to support native IPv6
  - IPv6 can be used across IPv4 networks using transition technologies, 6to4, ISATAP and Teredo
- ✘ Most IPv6 addresses are not easy (impossible) to memorise!
  - Will require the use of host names for all references
- ✘ Not all applications will be IPv6 compatible

14

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## Layer 2



- ✗ Layer-2 remains the same
  - No need to replace layer-2 appliances

15

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Address Notation

2009:0adb:0001:56af:0321:000d:98fe:dbfe

↑      ↑↑↑      ↑      ↑↑↑

Leading zeros can be removed

2009:adb:1:56af:321:d:98fe:dbfe

- ✗ The 128 bit number is split into eight 16-bit blocks
  - The value of each 16-bit block is written as four hex digits
  - Each block is separated by a colon
  - Referred to as colon-hexadecimal notation

16

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**



## Compressing Zeros

2009:0000:0000:0000:0321:000d:98fe:dbfe  
 2009::0321:000d:98fe:dbfe

2009:0000:0000:0321:0000:0000:0000:dbfe  
 2009::0321::dbfe ← Invalid

- ✘ Contiguous 16-bit blocks containing zeros can be compressed
  - Known as double-colon notation
  - Only one set of blocks can be compressed
    - Normally the first set of blocks from the left

17

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
 © XTseminars Ltd 2010

**XTseminars**

## IPv6 Prefix

2009:0adb:0001:56af:0321:000d:98fe:dbfe

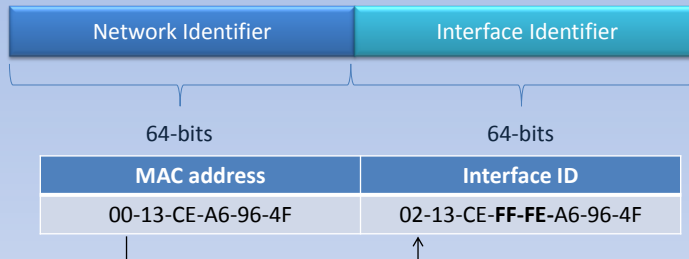
- ✘ The IPv6 prefix indicates the number of bits identifying the network
  - IPv6 does not support the IPv4 style subnet mask

18

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
 © XTseminars Ltd 2010

**XTseminars**

## IPv6 Addressing



- ✘ The Interface Identifier is the Extended Unique Identifier EUI-64 address
  - Can be assigned to the adapter
  - Or derived from the MAC address of the card
    - 48 bit MAC is padded with FFFE
    - Universal / Local administered bit inverted

19

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Randomized Identifiers

- ✘ Windows Server 2008 and Windows 7 use a permanent interface identifier that is randomly generated
  - Can be disabled via:
    - netsh interface ipv6 set global randomizeidentifiers=disabled
- ✘ With randomizeidentifiers enabled if a server is reinstalled it will have a new IP address
  - To avoid IP address changes for infrastructure servers such as DNS or DHCP
    - Disable randomization

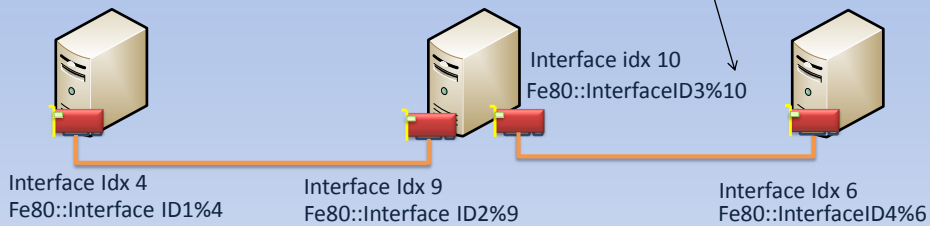
20

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Link-local Address

Zone IDs eliminate ambiguity when more than one interface is connected to a network



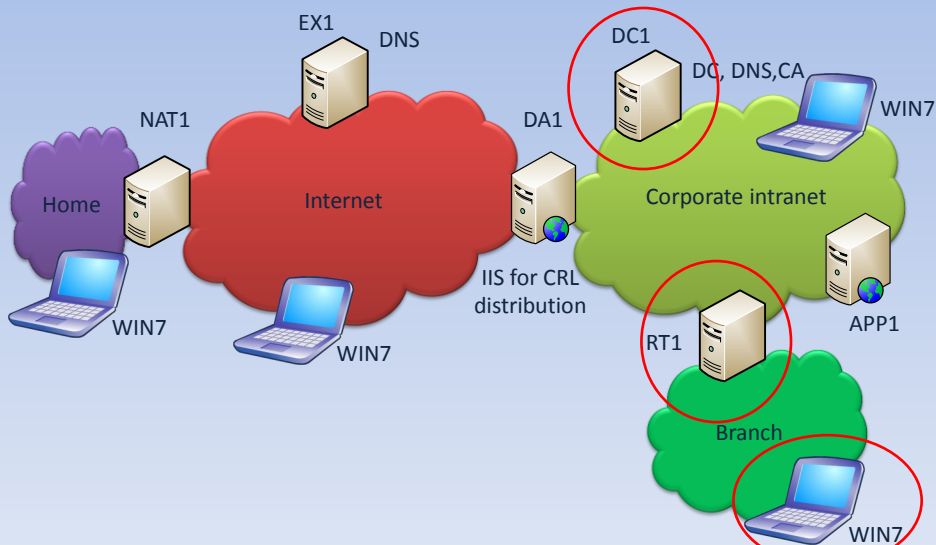
- ✘ Fe80::<InterfaceID> , automatically assigned and only accessible on local network segment
  - All hosts have a link-local address even if they have a global address
- ✘ The Interface Index (Idx) identifies the interface that the address is bound to

21

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Demo: Link-local Addresses



22

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## What No Broadcasts?

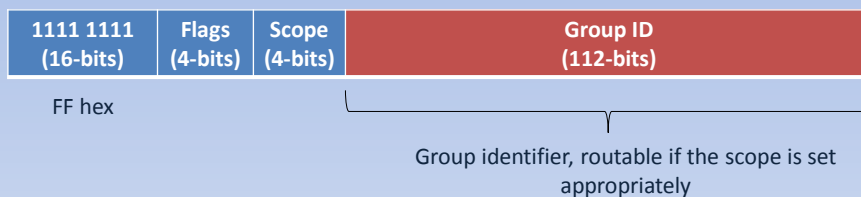
- ✘ The problem with a broadcast is that it “disturbs” every node on the link
  - The network card receives the broadcast and passes it up the stack and consumes CPU time
    - If the broadcast is not intended for the node, the stack rejects it (what a waste of CPU time!)
- ✘ With multicasts, the network card is programmed to listen for specific addresses
  - It only passes relevant traffic to the stack

23

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## IPv6 Multicast Addresses



- ✘ The flags designate if the address is permanent or temporary
  - Permanent address are well known, assigned by IANA
- ✘ The scope defines if the address is routable
  - Link-local, site-local

24

IANA = Internet Assigned Numbers Authority

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Some Well know Multicast Addresses

ff02::1/128	Link-local all-nodes multicast
ff02::2/128	Link-local all-routers multicast
ff05::2/128	Site-local all routers multicast
ff02::1:2/128	All-dhcp-agents
ff02::1:3/128	Link-local Multicast Name Resolution

- ✘ For a complete list see:
  - <http://www.iana.org/assignments/ipv6-multicast-addresses/>
- ✘ To view the multicast addresses that a host is listening on
  - Netsh interface ipv6 show join

25

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## NIC Table



MAC address 00-13-CE-A6-96-4F

Passes information up the stack for the following inbound addresses	
00-13-CE-A6-96-4F	MAC address
FF-FF-FF-FF-FF-FF	Broadcast
33-33-00-00-00-01	All nodes IPv6 multicast (ff02::1/128)
33-33-00-01-00-02	All DHCP agents IPv6 multicast (ff02::1:2/128)
33-33-FF-XX-XX-XX	Solicited-node IPv6 multicast

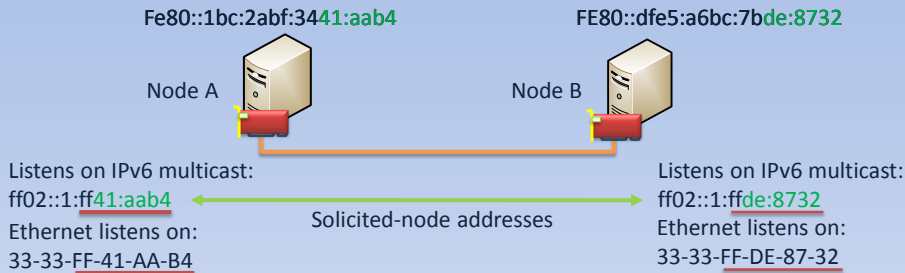
- ✘ For multicast, the Ethernet address starts 33-33
  - The remaining 32 bits are taken from the last 32 bits of the IPv6 multicast address
- ✘ The card is programmed to listen for appropriate addresses

26

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## Neighbor Discovery – Clever!



- ✗ To discover the MAC address of node B, node A sends a Neighbor Solicitation message
  - IPv6: ff02::1:ffde:8732 MAC: 33-33-FF-de-87-32
- ✗ Unlike an IPv4 ARP broadcast where all nodes are disturbed, the solicited-node multicast address behaves almost like a unicast address

27

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
 © XTseminars Ltd 2010

**XTseminars**

## Neighbor Solicitation

```

Frame Details
-----
Frame: Number = 3, Captured Frame Length = 86, MediaType = ETHERNET
Ethernet: Etype = IPv6, DestinationAddress: [33-33-FF-2C-DA-9E], SourceAddress: [00-15-5D-0B-04-6F]
IPv6: Next Protocol = ICMPv6, Payload Length = 32
  Versions: IPv6, Internet Protocol, DSCP 0
  PayloadLength: 32 (0x20)
  NextProtocol: ICMPv6, 58 (0x3a)
  HopLimit: 255 (0xFF)
  SourceAddress: FE80:0:0:0:38F7:674F:133E:38C3
  DestinationAddress: FF02:0:0:0:0:1:FF2C:DA9E
ICMPv6: Neighbor Solicitation, Target = FE80:0:0:0:30F1:F7EA:B82C:DA9E
  MessageType: Neighbor Solicitation, 135 (0x87)
  Code: 0 (0x0)
  Checksum: 38995 (0x9853)
  Reserved: 0 (0x0)
  TargetAddress: FE80:0:0:0:30F1:F7EA:B82C:DA9E
  SourceLinkLayerAddress:
    Type: Source Link-Layer Address, 1 (0x1)
    Length: 1, in unit of 8 octets
    Address: 00-15-5D-0B-04-6F
  
```

28

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
 © XTseminars Ltd 2010

**XTseminars**

## Neighbor Advertisement

```

Frame Details
-----
Frame: Number = 4, Captured Frame Length = 86, MediaType = ETHERNET
Ethernet: Etype = IPv6, DestinationAddress: [00-15-5D-0B-04-6F], SourceAddress: [00-15-5D-0B-04-68]
IPv6: Next Protocol = ICMPv6, Payload Length = 32
  Versions: IPv6, Internet Protocol, DSCP 0
  PayloadLength: 32 (0x20)
  NextProtocol: ICMPv6, 58 (0x3a)
  HopLimit: 255 (0xFF)
  SourceAddress: FE80:0:0:0:30F1:F7EA:B82C:DA9E
  DestinationAddress: FE80:0:0:0:38F7:674F:133E:38C3
ICMPv6: Neighbor Advertisement, Target = FE80:0:0:0:30F1:F7EA:B82C:DA9E
  MessageType: Neighbor Advertisement, 136 (0x88)
  Code: 0 (0x0)
  Checksum: 21761 (0x5501)
  NeighborAdvertisementFlag: 1610612736 (0x60000000)
    R: (0.....) Not router
    S: (.1.....) Solicited
    O: (...1.....) Override
    Rsv: (...00000000000000000000000000000000)
  TargetAddress: FE80:0:0:0:30F1:F7EA:B82C:DA9E
  TargetLinkLayerAddress:
    Type: Target Link-Layer Address, 2 (0x2)
    Length: 1, in unit of 8 octets
    Address: 00-15-5D-0B-04-68
  
```

29

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XT**seminars

## Viewing MAC Resolution

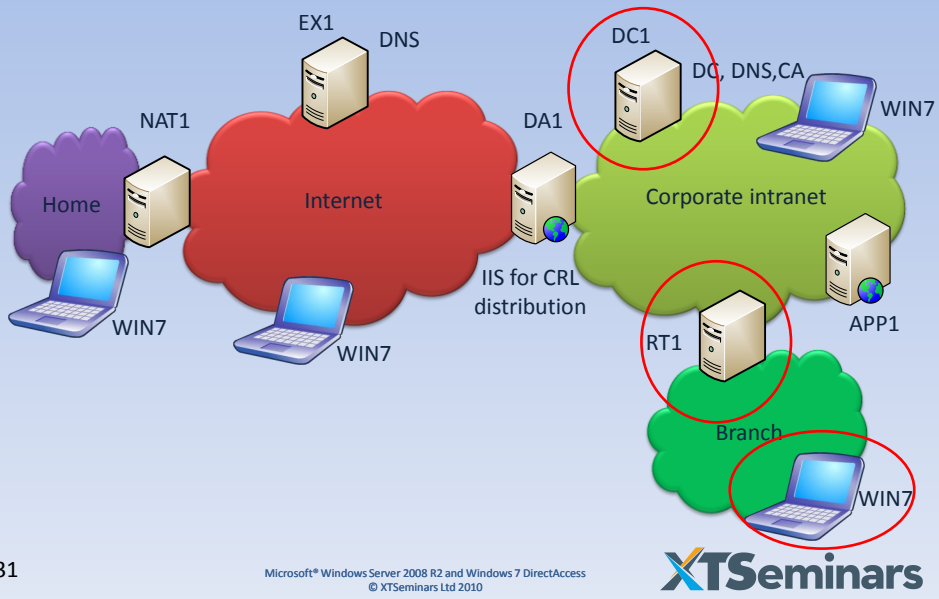
- ✗ Resolved MAC addresses stored in neighbors cache
  - Netsh interface ipv6 show neighbors
- ✗ In addition to the neighbors cache a destination cache is also maintained
  - Holds information on
    - Destination IPv6 address
    - Connected interface index
    - Maximum Transmission Unit (MTU)
    - Next Hop Address
  - Netsh interface ipv6 show destinationcache

30

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

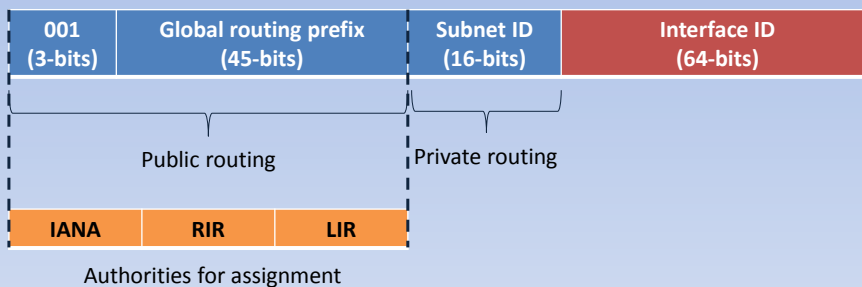
**XT**seminars

## Demo: Viewing MAC Resolution



## Global Addresses

Global address (Internet registered)



✕ Global Addresses are fully routable on the public Internet



## Assignment of Global Addresses



- ✘ Internet Assigned Numbers Authority (IANA) allocates large blocks of addresses to the five Regional Internet Registries (RIR)
- ✘ RIRs allocate blocks to Local Internet Registries (LIR) (often ISPs) and large end sites
- ✘ Smaller ISPs and end sites can obtain IPv6 address space from their upstream provider

33

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTSeminar Ltd 2010

**XTSeminar**s

## Numbers to Expect...

- ✘ As of March 2010, IANA has released addresses for allocation, starting
  - 2001:, 2002:, 2003:, 2400:, 2600:, 2610:, 2620:, 2800:, 2A00: and 2C00:
- ✘ 2002:: /16 is reserved for 6to4 deployments
- ✘ 2001:0000:: /32 global Teredo IPv6 service prefix
- ✘ 2001:0DB8:: /32 non-routable reserved for documentation purpose
- ✘ For full details see
  - <http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml>

34

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTSeminar Ltd 2010

**XTSeminar**s

# Private Unicast Addresses

(Similar to IPv4 private address ranges)

## Site-Local address

1111 1110 11 (10-bits)	Subnet ID (54-bits)	Interface ID (64-bits)
---------------------------	------------------------	---------------------------

FEC hex

Site-local address prefixed fec0::/10 was depreciated in RFC 3879

## Unique Local address

1111 1101 (8-bits)	Global ID (40-bits)	Subnet ID (16-bits)	Interface ID (64-bits)
-----------------------	------------------------	------------------------	---------------------------

FD hex

Private routing between sites

Routing between LANs within a site

35

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTSeminars Ltd 2010

# Unique Local Address

1111 1101 (8-bits)	Global ID (40-bits)	Subnet ID (16-bits)	Interface ID (64-bits)
-----------------------	------------------------	------------------------	---------------------------

Organizational prefix

- ✘ RFC 4193 states that the IPv6 addresses are created using a pseudo-randomly allocated global ID
- ✘ In our examples we use fd00:9999::/48 as the organizational prefix
  - Creating different subnets using the SubnetID

36

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTSeminars Ltd 2010

## Special Addresses & Formats

- ✘ `::1` represents the loopback address
  - IPv4 equivalent 127.0.0.1
- ✘ `::` is an unspecified address
  - IPv4 equivalent 0.0.0.0
- ✘ In URL, enclose address in square brackets
  - `https://[2009::321:d:98fe:dbfe%15]:2031`
- ✘ For UNC path, use IPv6Address.ipv6-literal.net names
  - `\\2009--321-d-98fe-dbfes15.ipv6-literal.net`

ZoneIDs in red

37

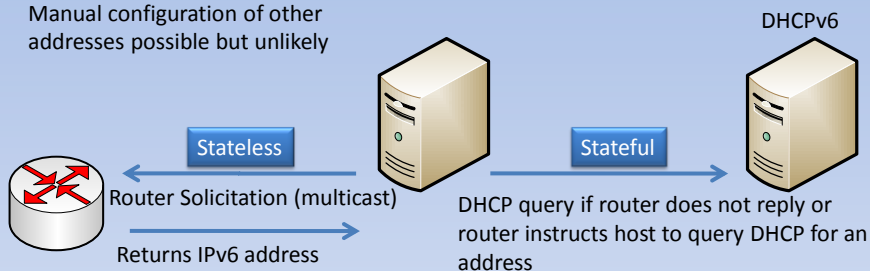
Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Host Configuration

Auto configure link-local address

Manual configuration of other addresses possible but unlikely



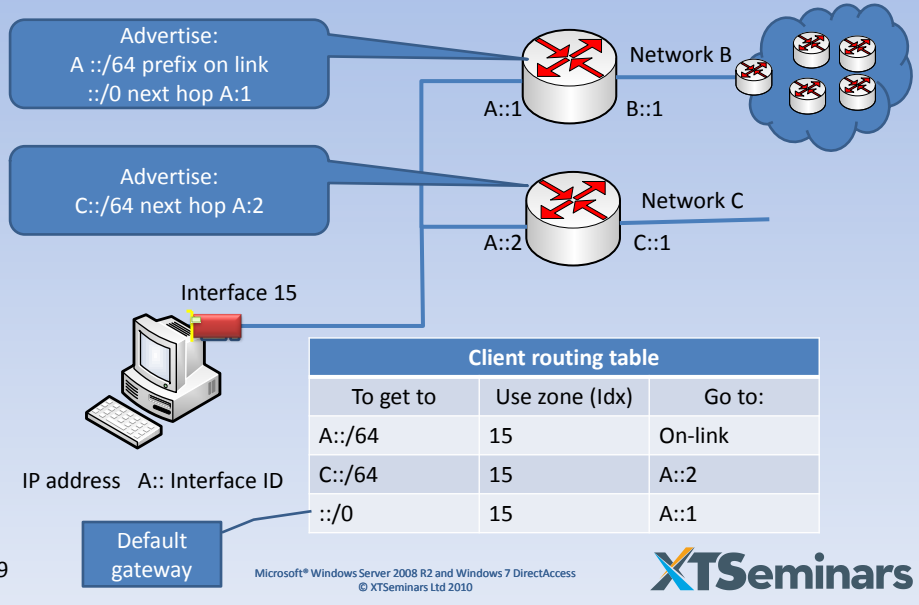
- ✘ DHCP can supply complete configuration or just additional options
  - ✘ Referred to as *DHCPv6 stateful* if address supplied otherwise *DHCPv6 stateless*

38

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

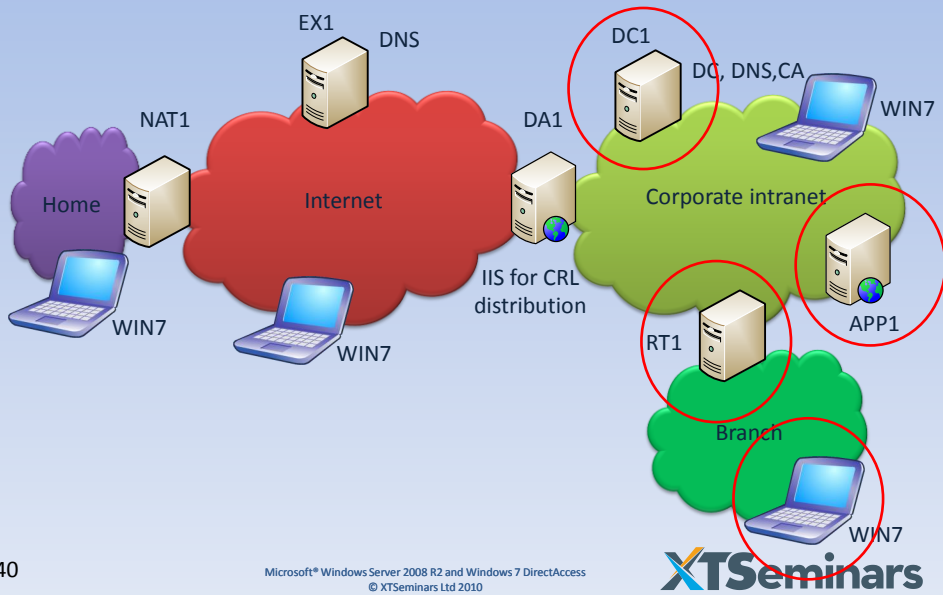
**XTseminars**

# Routing (simplified)



39

# Demo: Routing Configuration



40

## Routing Configuration (*reference*)



Host

```
:: Set DNS address
netsh interface ipv6 set dnsservers 12 static fd00:9999:0:1::10
```

```
::Set Network adapter addresses
netsh interface ipv6 set address dacorp fd00:9999:0:1::1/64
netsh interface ipv6 set address dabranch fd00:9999:0:2::1/64
```



Router

```
::Enable routing and advertising
netsh interface ipv6 set interface dacorp forwarding=enabled advertise=enabled
netsh interface ipv6 set interface dabranch forwarding=enabled advertise=enabled
```

```
::Publish network prefixes
netsh interface ipv6 set route fd00:9999:0:2::/64 dabranch publish=yes
netsh interface ipv6 set route fd00:9999:0:1::/64 dacorp publish=yes
```

## Router Advertisement

```
RouterAdvertisementFlag:
  M: (1.....) Managed address configuration
  O: (.1.....) Other stateful configuration
  A: (.0.....) Not a Mobile IP Home Agent
  RouterPreference: (...00...) Medium, 0 (0x0)
  Reserved: (.....000)
RouterLifetime: 0 (0x0)
ReachableTime: 0 (0x0)
RetransTimer: 0 (0x0)
SourceLinkLayerAddress:
MTU:
PrefixInformation:
  Type: Prefix Information, 3 (0x3)
  Length: 4, in unit of 8 octets
  PrefixLength: 64 (0x40)
  Flags: 192 (0xC0)
    L: (1.....) On-Link determination allowed
    A: (.1.....) Autonomous address-configuration
    R: (.0.....) Not router Address
    S: (...0....) Not a site prefix
    P: (...0....) Not a router prefix
    Rsv: (.....000)
  ValidLifetime: 2592000 (0x278D00)
  PreferredLifetime: 604800 (0x99A80)
  Reserved: 0 (0x0)
  Prefix: FD00:9999:0:1:0:0:0:0
```

M flag

Use DHCP for address

O flag

Use DHCP for other config

Add to prefix table

Create an address from prefix

## DHCP Stateful or Stateless

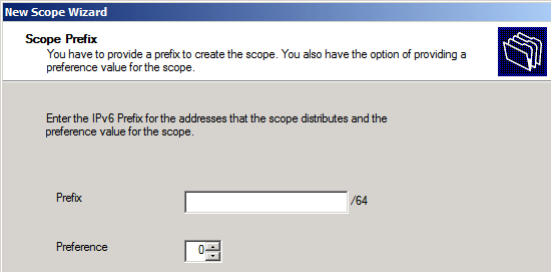
- ✘ Advertise Routing prefix
  - Netsh interface ipv6 add route  
`<ipv6prefix>::/<prefixlength> <server_interface >  
 publish=yes`
- ✘ Enable stateful / stateless
  - netsh interface ipv6 set interface  
`< server_interface > advertise=en managed=en  
 other=en`

43

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
 © XTseminars Ltd 2010



## DHCPv6



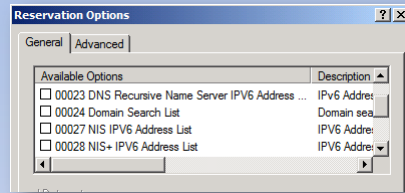
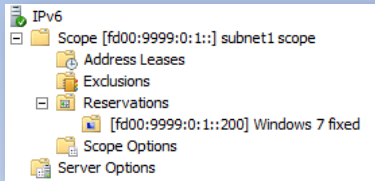
- ✘ Similar to IPv4 configuration except you only define the prefix
  - The DHCP server automatically assigns a randomized InterfaceID

44

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
 © XTseminars Ltd 2010



## Options

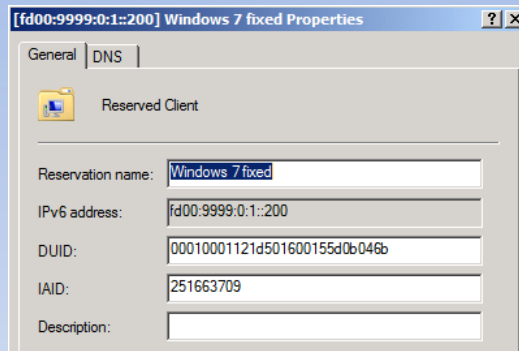


- ✗ *Server Options* assigned to all scopes
- ✗ *Scope Options* assigned for each scope
- ✗ *Reservation Options* assigned for each reservation

45

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

## Reservations



- ✗ The DHCP Unique Identifier (DUID) uniquely identifies the host
- ✗ The Identity Association Identifier (IAID) identifies the Interface

46

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

## DUID and IAID

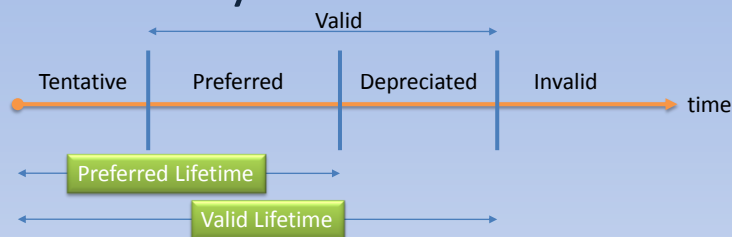
- ✘ Windows generates the DUID based on the Link-layer Address Plus Time (DUID-LLT)
  - DUID is generated only once for a machine
  - It is global across all adapters
  - It is persistent even if the adapter changes
- ✘ Identity Association (IA)
  - A collection of addresses assigned to a client
  - Each IA has an associated identifier (IAID)
    - Each interface has at least one IAID

47

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Address Lifecycle



- ✘ Duplicate Address Detection (DAD) is performed during the tentative period
  - If no duplicates are detected the address is assumed to be unique and valid
- ✘ Depreciated address can still be used
  - Avoid use for new communications

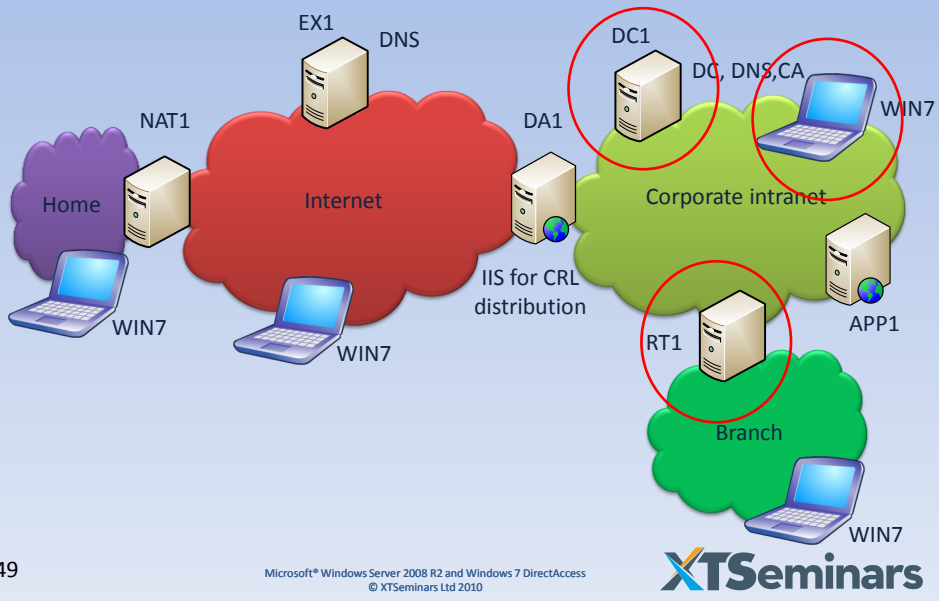
48

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**



## Demo: Configuring DHCPv6



## Command (reference)

```

::Change state or router advertisement m
& 0 flags
netsh interface ipv6 set interface dacorp
other=ena/dis man=ena/dis
::Turn of prefix publishing
netsh interface ipv6 set route
fd00:9999:0:1::/64 dacorp publish=no
::View addresses
netsh interface ipv6 show addresses
::renew & release DHCPv6
ipconfig /renew6    ipconfig /release6

```

# Name Resolution

- ✗ IPv6 supports two protocols for Name Resolution
  - DNS
  - Link-local Multicast Name Resolution (LLMNR)
- ✗ DNS for IPv6 includes the AAAA record
  - Maps host names to IPv6 addresses
  - Reverse look up is supported via the ip6.arpa domain

51

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



# DNS Records

The screenshot shows two windows from the Windows DNS console. The top window displays the DNS records for the 'example.com' zone, showing 20 records. The bottom window displays the DNS records for the '1.0.0.0.0.0.0.9.9.9.0.0.d.f.ip6.arpa' zone, showing 8 records.

Name	Type	Data
(same as parent folder)	IPv6 Host (AAAA)	fd00:9999:0000:0001:f577:56e8:24db:5dc2
(same as parent folder)	IPv6 Host (AAAA)	fd00:9999:0000:0001:0000:0000:0000:0010
APP1	Host (A)	10.20.100.11
APP1	IPv6 Host (AAAA)	fd00:9999:0000:0001:2aa6:c1c9:81c7:d82f
C1	IPv6 Host (AAAA)	fd00:9999:0000:0001:f9db:de09:09f0:99b8
C1	IPv6 Host (AAAA)	fd00:9999:0000:0001:ed99:dda3:ffb:ec63
DA1	Host (A)	10.20.100.12
DA1	IPv6 Host (AAAA)	fd00:9999:0000:0001:c7c1:760a:916a:f581
dc-1	Host (A)	10.20.100.10

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[7], dc1.example.com
(same as parent folder)	Name Server (NS)	dc1.example.com
fd00:9999:0000:0001:0000:0000:0000:0010	Pointer (PTR)	dc1.example.com
fd00:9999:0000:0001:2aa6:c1c9:81c7:d82f	Pointer (PTR)	app1.example.com
fd00:9999:0000:0001:c7c1:760a:916a:f581	Pointer (PTR)	da1.example.com
fd00:9999:0000:0001:ed99:dda3:ffb:ec63	Pointer (PTR)	c1.example.com
fd00:9999:0000:0001:f577:56e8:24db:5dc2	Pointer (PTR)	dc1.example.com
fd00:9999:0000:0001:f9db:de09:09f0:99b8	Pointer (PTR)	c1.example.com

- ✗ A client can query for both IPv6 and IPv4 records

52

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## Hardcoded DNS Addresses

- ✘ To provide stateless DNS configuration three site-local addresses reserved for DNS servers
  - fec0:000:0000:ffff::1, fec0:000:0000:ffff::2 and fec0:000:0000:ffff::3
- ✘ The site-local addresses prefixed fec0::/10 was deprecated in RFC 3879
  - The hardcoded DNS addresses remain

53

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## LLMNR

- ✘ LLMNR allows name resolution when a DNS server is not available
  - Resolves names only for the local link
- ✘ A host sends an LLMNR Name Query Request to the link-local scope multicast ff02::1:3
  - MAC 33-33-00-01-00-03
  - All nodes listen on this address
- ✘ The host that is authoritative for the name sends a unicast reply

54

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010




```

Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix . . . . . : 
    Description . . . . . : Microsoft Virtual Machine Bus Network Adapter
    Physical Address. . . . . : 00-15-5D-0B-04-6C
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . . : Yes
    IPv6 Address. . . . . : fd00:9999:0:2:ed99:dda3:ff0b:ec63(Preferred)
    Temporary IPv6 Address. . . . . : fd00:9999:0:2:a48f:e34e:2283:9d1c(Preferred)
    Link-local IPv6 Address . . . . . : fe80::ed99:dda3:ff0b:ec63%12(Preferred)
    IPv4 Address. . . . . : 10.20.19.11(Preferred)
    Subnet Mask . . . . . : 255.255.128.0
    Default Gateway . . . . . : 
    DHCPv6 IAID . . . . . : 251663709
    DHCPv6 Client DUID. . . . . : 00-01-00-01-12-1D-50-16-00-15-5D-0B-04-6C
    DNS Servers . . . . . : fec0:0:0:ffff::1%1
    . . . . . : fec0:0:0:ffff::2%1
    . . . . . : fec0:0:0:ffff::3%1
    NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.{8C8B1176-A8F8-4CB7-93B2-971C461C6F78}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . : 
    Description . . . . . : Microsoft ISATAP Adapter
    Physical Address. . . . . : 00-00-00-00-00-00-00-00-E0
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . . : Yes

Tunnel adapter Local Area Connection* 11:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . : 
    Description . . . . . : Microsoft Teredo Tunneling Adapter
    Physical Address. . . . . : 00-00-00-00-00-00-00-E0
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . . : Yes
    
```

So what about these!




Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTSeminars Ltd 2010

## Seminar Agenda

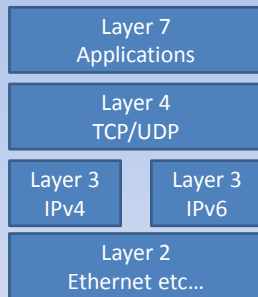
- IPv6
- Transition technologies
- Ipsec and DirectAccess
- Unified Access Gateway (UAG)
- Network Access Protection (NAP)
- Summary and Q&A

56

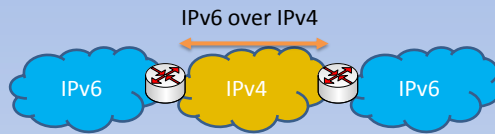
Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTSeminars Ltd 2010



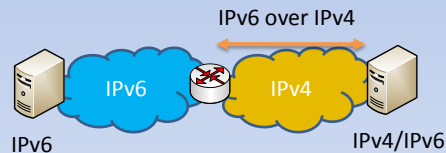
## Transition Technologies



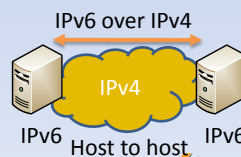
Dual IP architecture



Router to router tunnelling



Host to router , router to host



Host to host

57

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Tunnelling



- ✗ The tunnel end may be a single host or IPv6 network
- ✗ IPv6 Traffic can be tunnelled in IPv4 as
  - IP (used by 6to4 and ISATAP)
  - UDP (used by Teredo)
  - HTTPS (used by IPHTTPS)

58

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## 6to4 Network

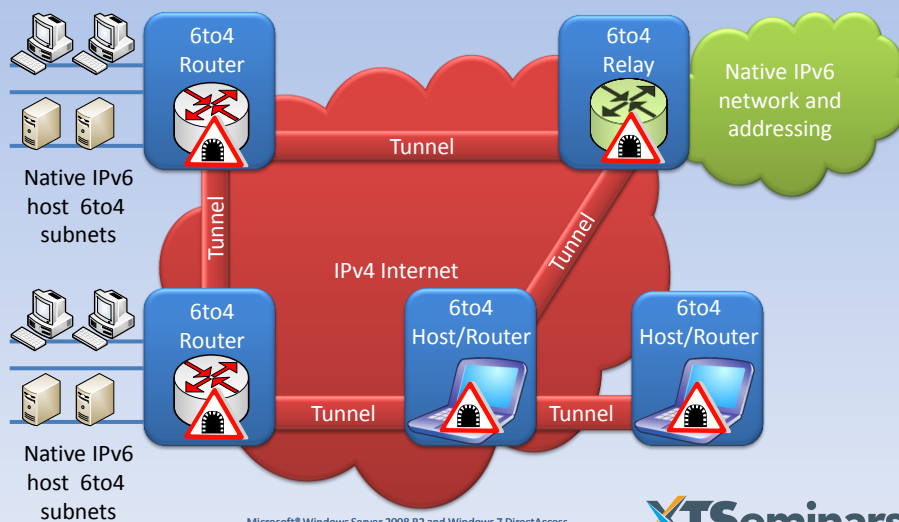
- ✗ The 6to4 Network is an Internet based public IPv6 network
  - Addresses start with the 2002::/16 prefix
- ✗ IPv6 traffic is tunnelled in IPv4 between 6to4 routers and relays

59

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## 6to4 Components



60

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## 6to4 Addressing

- ✘ Host configured with a public IPv4 address
  - 6to4 interface automatically enabled and assigned a unique global (public) IPv6 address
- ✘ Interface assigned IPv6 address: `2002:wwxx:yyzz:0:0:0:wwxx:yyzz`
  - `wwxx:yyzz` is the hexadecimal representation of the host's IPv4 address
- ✘ `144.19.200.2` translates to `9013:c802`
  - Corresponding 6to4 address
    - `2002:9013:c802:0:0:0:9013:c802`

61

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## Just a Bit of Hex

8 Binary BITS can contain a number between 0 and 255

Each BIT represents a different numerical value

128	64	32	16	8	4	2	1
-----	----	----	----	---	---	---	---

1	0	0	1	0	0	1	1
---	---	---	---	---	---	---	---

Written in decimal is  $128 + 16 + 2 + 1 = 147$

XY

Hexadecimal is a method of representing 8-bits as two hexadecimal digits

X represents the number of 16s in the 8-bit value and Y the remainder

$$\begin{array}{r} 9 \\ 16 \overline{) 147} \\ \underline{142} \\ 3 \end{array}$$

147 in decimal is 93 in hex

62

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## Letters as well!

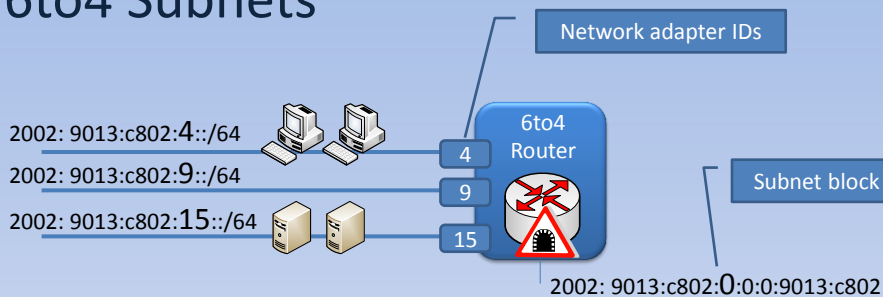
- ✗ Each hex digit must represent up to the value of 15, so alpha characters are used as well
  - 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f
- ✗ To check an address assignment such as 9013:c802, remember this represent 4 x 8-bit blocks and the 1<sup>st</sup> character in each hex pair is the number of 16s
  - $9 \times 16 + 0 = 144$ ,  $1 \times 16 + 3 = 19$ ,  $12 \times 16 + 8 = 200$
  - 144.19.200.2

63

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## 6to4 Subnets



- ✗ All traffic for 2002:wwxx:yyzz::/48 is tunnelled to 2002:wwxx:yyzz:0:0:0:wwxx:yyzz
  - The 16 bit subnet block can be used to identify subnets
- ✗ If 6to4 is enabled, ICS creates subnets based on the interface IDs of the internal networks

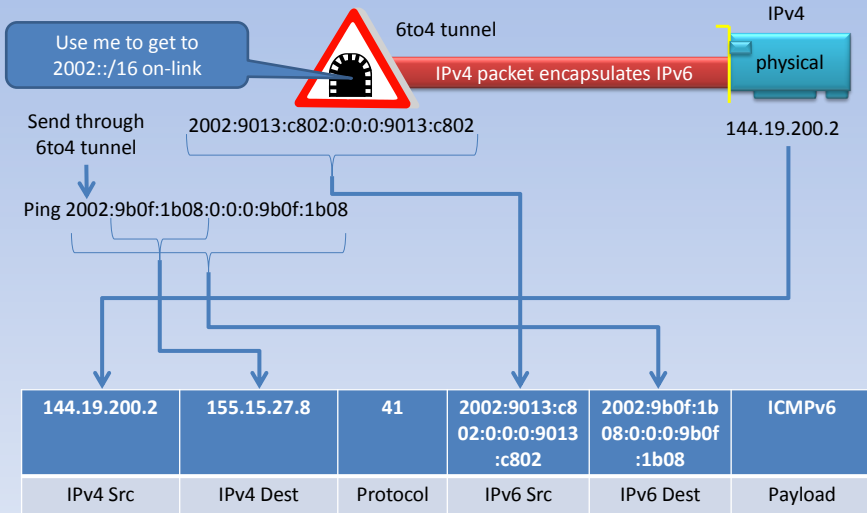
64

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**



## 6to4 Host/Router to 6to4 Host

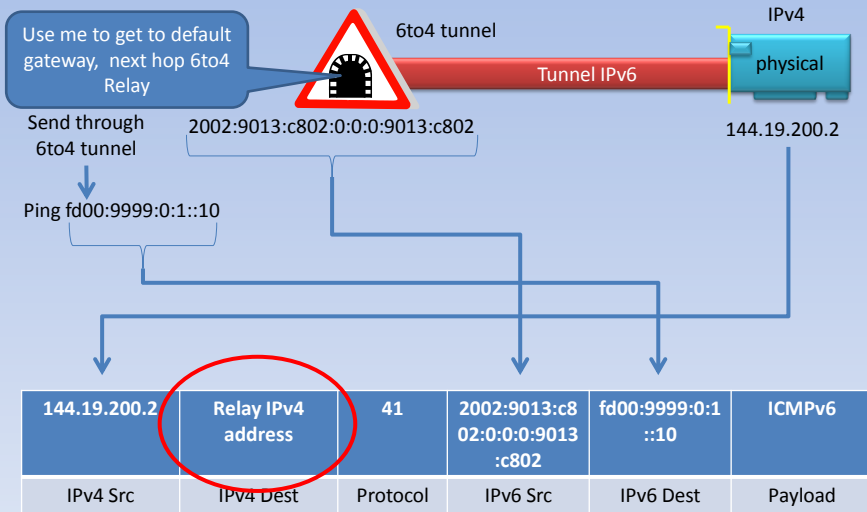


65

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## 6to4 Host/Router to Native Host

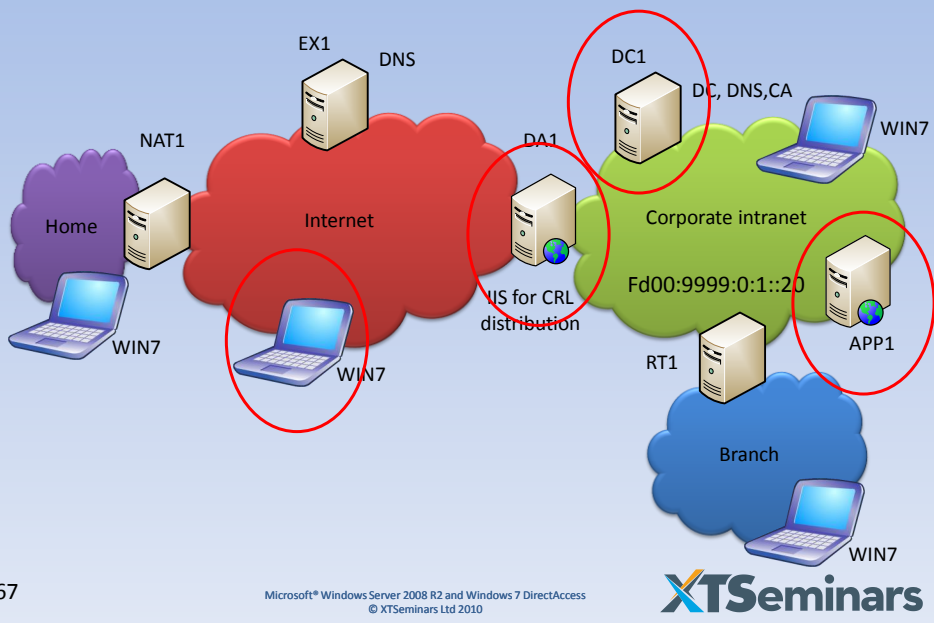


66

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## Demo: Enabling 6to4



## 6to4 Configuration (reference)



6to4  
Host/Router

```
:: Set name of 6to4 relay
netsh interface 6to4 set relay corprelay.example.com
:: host must be able to resolve FQDN
```



6to4  
Relay

```
::Enable 6to4 Interface
netsh interface 6to4 set state enabled
::Enable forwarding on 6to4 interface
netsh interface ipv6 set interface "6to4 Adapter" forwarding=enabled
::Set fixed IP for DACorp interface
netsh interface ipv6 set address dacorp fd00:9999:0:1::200/64
::Enable forwarding and advertising on DACorp interface
netsh interface ipv6 set interface DACorp forwarding=enabled advertise=enabled
::Add DNS record for relay
corprelay.example.com 144.19.0.10
```

## Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

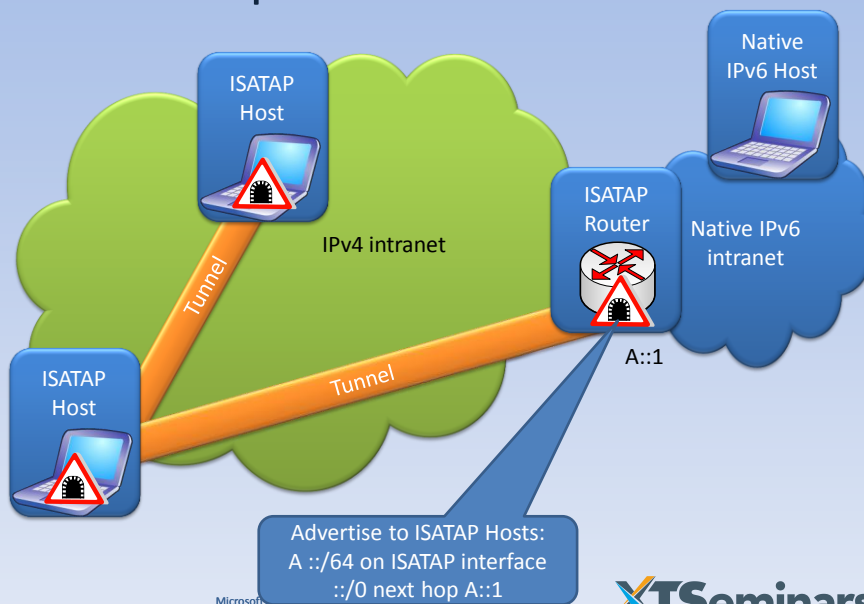
- ✘ ISATAP is similar to 6to4 as it tunnels IPv6 within an IPv4 packet
  - Protocol ID 41
- ✘ ISATAP is used for tunnelling IPv6 across IPv4 intranets

69

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## ISATAP Components

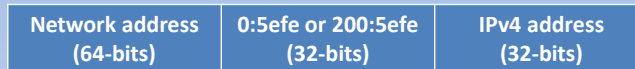


70

Microsoft  
© XTseminars Ltd 2010

**XTseminars**

## ISATAP Host Configuration



0:5efe for a private IPv4 address  
200:5efe for a public IPv4 address

- ✘ The ISATAP interface address is constructed from a combination of the IPv6 network address and the IPv4 address
  - The 32-bit IPv4 address is be written in dotted decimal notation
    - fd00:9999:0:100:0:5efe:10.40.99.120

71

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

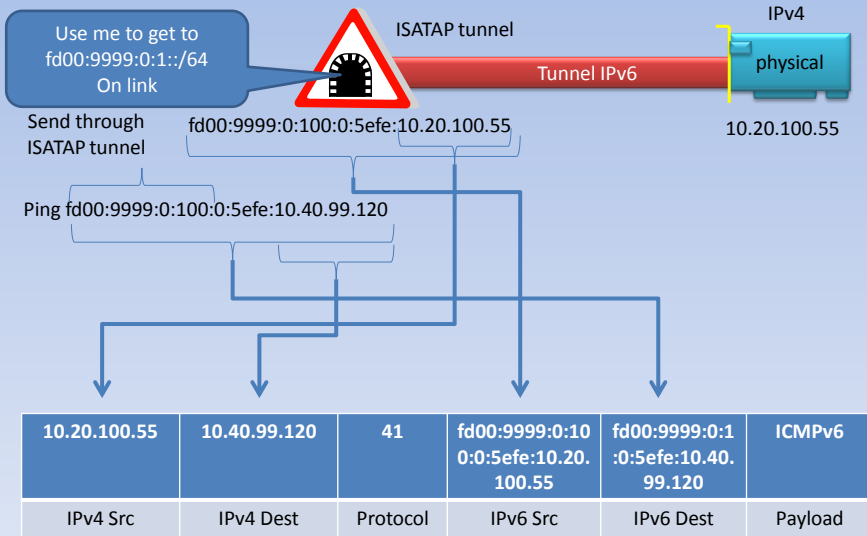
## ISATAP Host Configuration

- ✘ The host can either be configured with the address of the ISATAP router or it can resolve it via DNS
  - If the host can resolve ISATAP via DNS, it automatically configures its ISATAP tunnel interface
  - The network address of the interface is published by the ISATAP router
- ✘ The location of the ISATAP router is published in DNS with the key word ISATAP
  - For example: isatap.example.com
  - DNS blocks the name isatap via the globalqueryblocklist
    - This must be cleared

72

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

## ISATAP Host to ISATAP Host

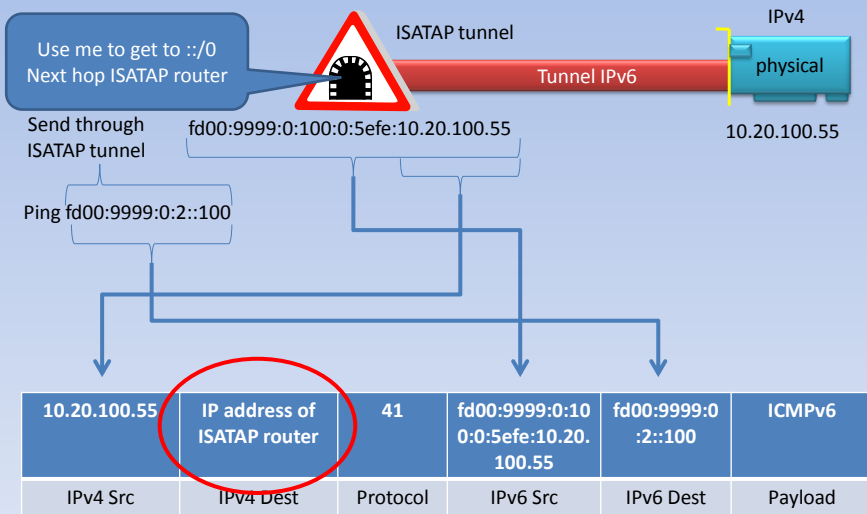


73

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## ISATAP Host to Native IPv6 Host

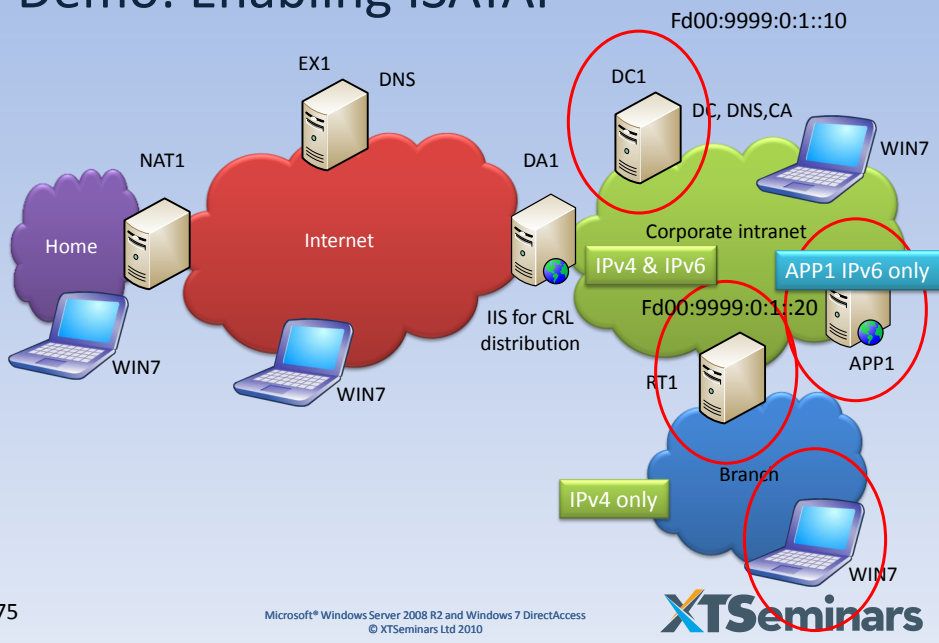


74

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## Demo: Enabling ISATAP



## ISATAP Configuration (reference)



No Client configuration, ISATAP interface automatically configured when client can resolve the name ISATAP from DNS



```

::Enable IPv4 routing
netsh interface ipv4 set interface dacorp forwarding=enabled
netsh interface ipv4 set interface dabranch forwarding=enabled
::configure IPV6 address, advertising and routing on DACorp interface
netsh interface ipv6 set address dacorp fd00:9999:0:1::1/64
netsh interface ipv6 set interface dacorp forwarding=enabled advertise=enabled
netsh interface ipv6 set route fd00:9999:0:1::/64 dacorp publish=yes

```

```

netsh interface isatap set router 10.40.100.1
netsh interface ipv6 set interface 15 forwarding=enabled advertise=enabled
netsh interface ipv6 add route fd00:9999:0:100::/64 15 publish=yes

```



DNS Server

```

Remove ISATAP block : dnscmd /config /globalqueryblocklist wpad
Publish isatap.example.com
Alternatively, don't publish in DNS and configure the host:
Netsh interface ipv6 isatap set state router xxy.example.com

```

## 2008 DNS & ISATAP

- ✘ To support the processing of DNS name queries on the ISATAP interface the DNS server must be running on
  - Windows Server 2008 R2
  - Windows Server 2008 with Q958194 installed
  - Windows Server 2008 with SP2 or later

77

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## Supporting IPv4 Only Hosts

- ✘ For connections between IPv6 hosts and hosts that only support IPv4
  - NAT-PT and DNS-ALG required
- ✘ Improved translation with NAT64 and DNS64
- ✘ Forefront Unified Access Gateway (UAG)
  - Includes support for NAT64 and DNS64

78

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## IPv4 Only Resources

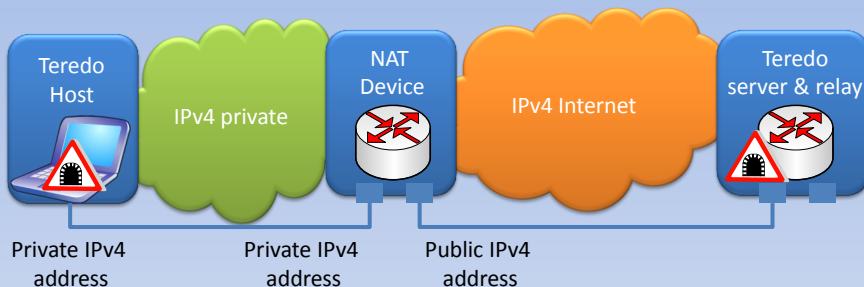
- ✘ Applications that are not IPv6 capable will need to be reached via an IPv6/IPv4 translation device such as NAT64 and DNS64
- ✘ Examples of IPv4 only resources
  - Windows 2000
  - Built-in applications and services running on Windows XP and Server 2003
- ✘ Check with the vendor for IPv6 capabilities
- ✘ Upgrade where possible

79

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Teredo



- ✘ Teredo provides connectivity when the host is behind one or more NATs
  - The NAT will probably not support tunnelling IPv6 within IPv4 (protocol 41)
  - Teredo tunnels IPv6 in UDP

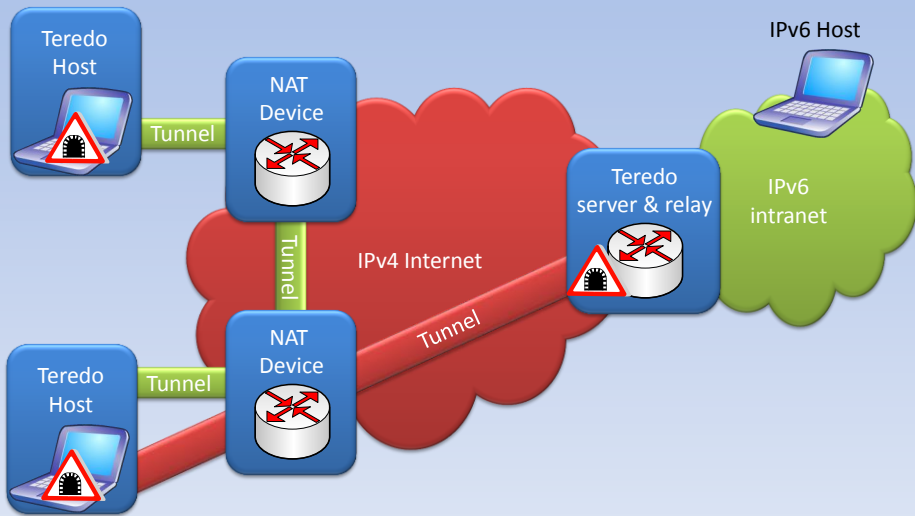
80

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**



# Teredo Components

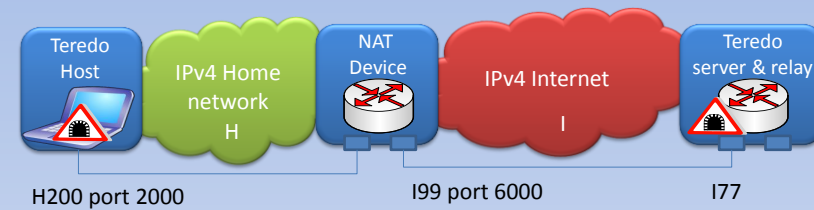


81

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



# IPv4 Outbound Packet Translation



I77	H200	UDP	3544	2000	IPv6
Dst IP	Src IP	Protocol	Dst port	Src port	Payload
↓ Translation ↓					
I77	I99	UDP	3544	6000	IPv6
Dst IP	Src IP	Protocol	Dst port	Src port	Payload

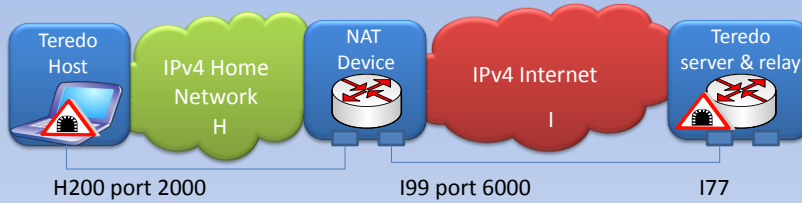
Mapping stored: H200 port 2000 ↔ I99 port 6000

82

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## Inbound traffic



I99	I77	UDP	6000	3544	IPv6
Dst IP	Src IP	Protocol	Dst port	Src port	Payload



Translation



H200	I77	UDP	2000	3544	IPv6
Dst IP	Src IP	Protocol	Dst port	Src port	Payload

Mapping in table: H200 port 2000 ↔ I99 port 6000

83

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## The Challenge

- ✗ NAT normally allows inbound traffic as a response to an outbound request
  - To allow any host to initiate communication with a Teredo host the NAT mappings will need to remain valid
- ✗ Three different types of NAT
  - Cone
    - For mapped external IP and ports, allows inbound packets from any source IP address or port
  - Restricted
    - Only allows inbound from IP and Port that matched the original outbound destination IP and Port
  - Symmetric
    - Maps the same internal IP address and port to different external IP addresses and ports depending on the outbound destination address

84

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Initial Negotiation

- ✗ The Teredo host connects to the Teredo server
- ✗ The server performs tests to determine the type of NAT that the host is behind
  - To do this the server needs to be configured with two consecutive IPv4 addresses
- ✗ The Server provides the address of the host's Teredo tunnel

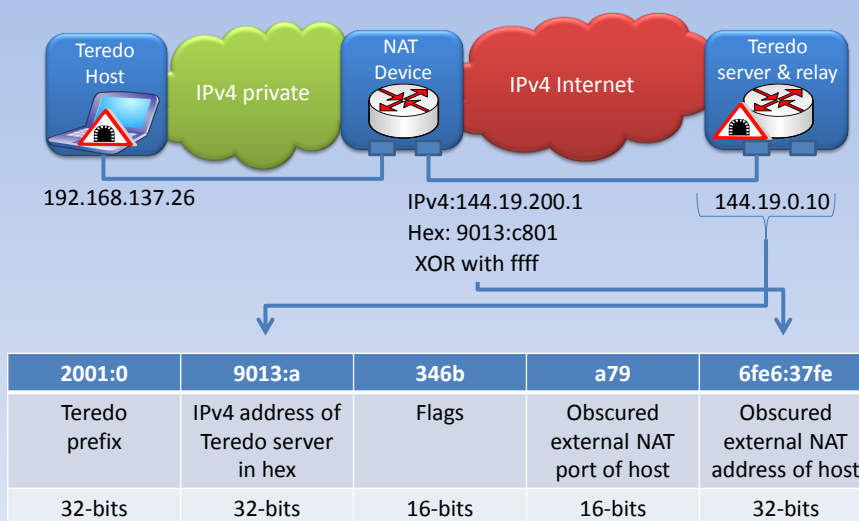
85

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Teredo Host Address

2001:0:9013:a:346b:a79:6fe6:37fe

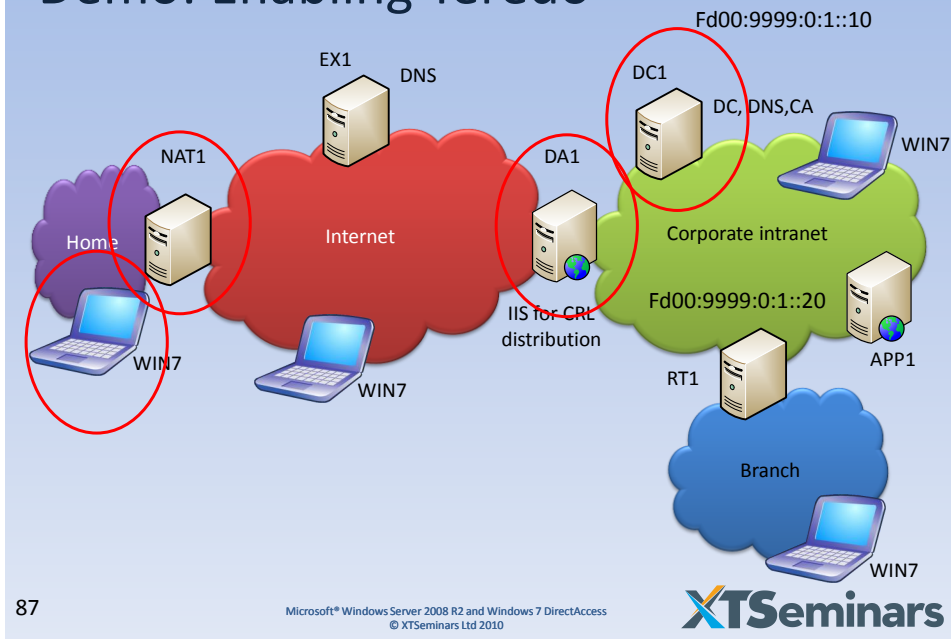


86

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Demo: Enabling Teredo



## Teredo Configuration (reference)



### Teredo Host

```

::Enable client for Teredo
netsh interface ipv6 set teredo enterpriseclient teredo.example.com
::To resolve IPv6 DNS
HKLM\CCS\Services\DNSCache\Parameters\AddrConfigControl DWORD 0

```



### Teredo server & relay

```

::Add DNS entry for Teredo server
teredo.example.com 144.19.0.10
::Add second IP address to Teredo server - used for NAT detection
netsh interface ipv4 add address dainternet 144.19.0.11/16
::enable teredo server
netsh interface teredo set state type=server teredo.example.com
servervirtualip=144.19.0.10
::Enable Teredo tunnelling interface
netsh interface ipv6 set interface 11 forwarding= enabled
netsh interface ipv6 set route 2001::/32 11 publish=yes

```

## IPHTTPS

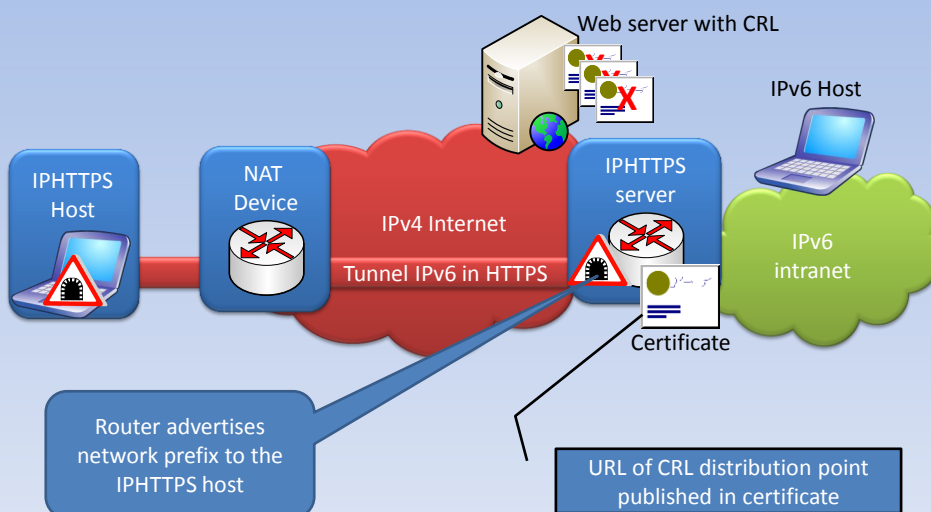
- ✗ IPHTTPS can be used if a host behind NAT cannot tunnel using Teredo
  - Firewall blocking port 3544
- ✗ IPHTTPS encapsulates IPv6 in HTTPS
  - Most firewalls will pass HTTPS
- ✗ Challenges
  - Certificates required
  - Host must have access to the CRL distribution point

89

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## IPHTTPS Components

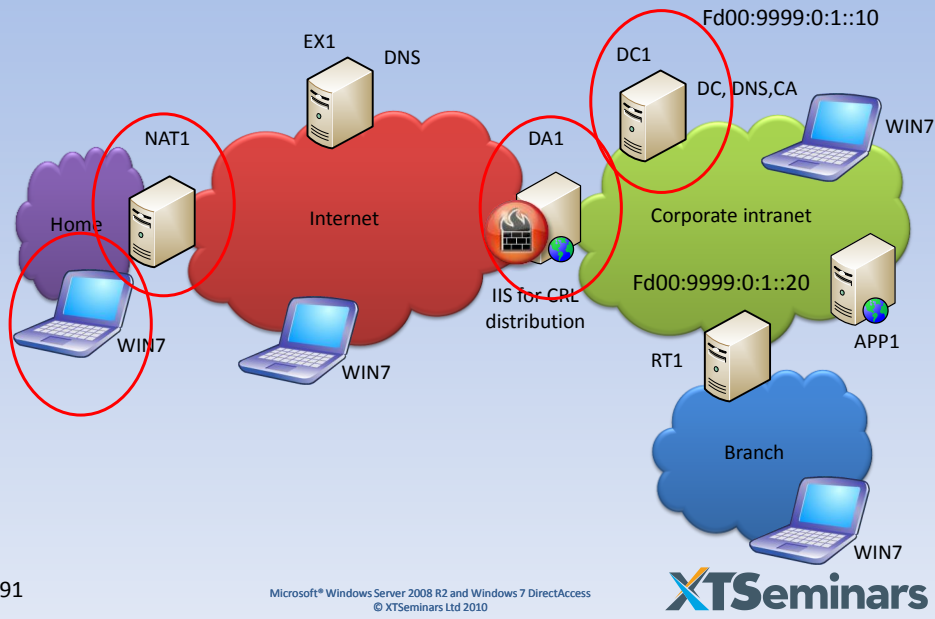


90

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Demo: Enabling IPHTTPS



## IPHTTPS Configuration (reference)

**IPHTTPS Host**

```
netsh interface httpstunnel add interface client
https://DA1.example.com:443/IPHTTPS enabled
```

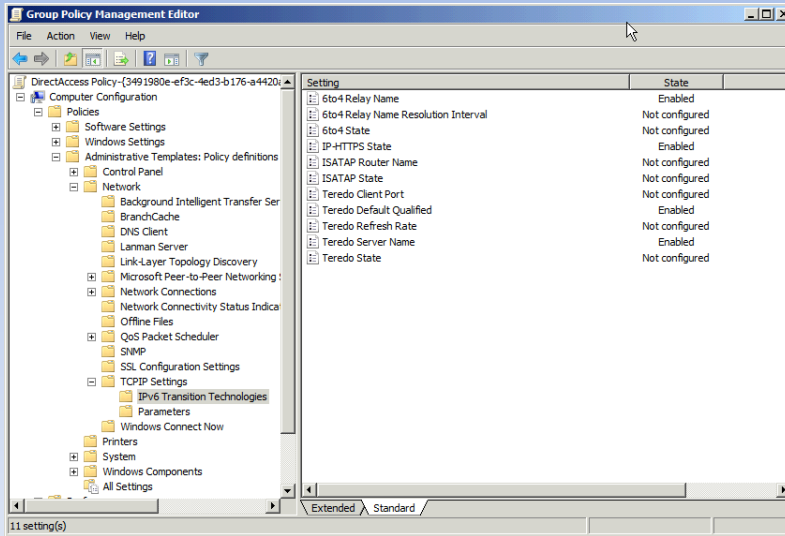
Client must be able to resolve URL and have access to the CRL distribution point

**IPHTTPS server**

```
:: Create IP-HTTPS tunnel interface and bind to DA\Internet IP
netsh interface httpstunnel add interface url=
"https://DA1.example.com:443/IPHTTPS" type=server state=default
::Enable IP-HTTPS interface to forward and advertise
netsh interface ipv6 set interface iphttpsInterface forwarding=enabled
advertise=enabled
::Advertise prefix on IP-HTTPS interface
netsh interface ipv6 add route 2001:feff::/64 iphttpsinterface publish=yes
::Bind certificate to listening port
netsh http add sslcert ipport=144.19.0.10:443 certhash=
c4d1c97ee770f033dab9091fa7304a6946db4ca6 appid=
{00112233-4455-6677-8899-AABBCCDDEEFF}
```

**Certificate**

# Don't Like Netsh?

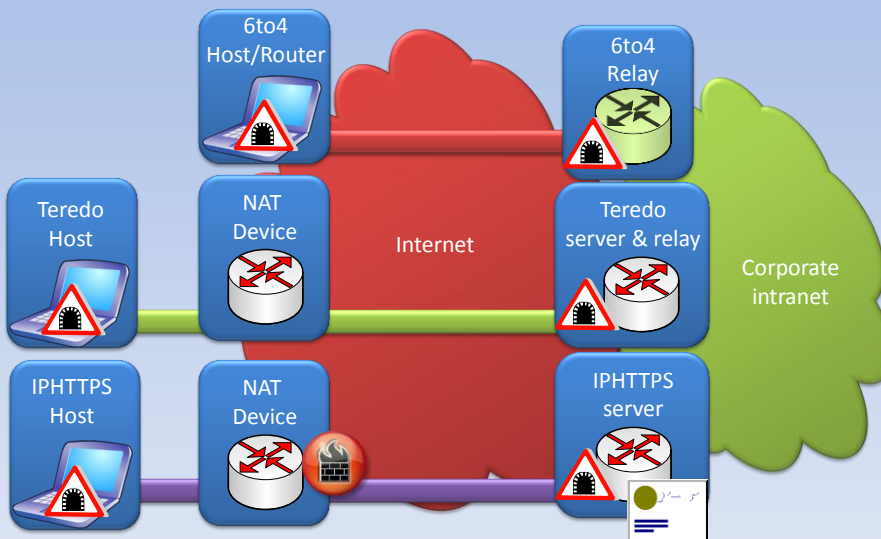


93

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



# Summary: Internet to Intranet

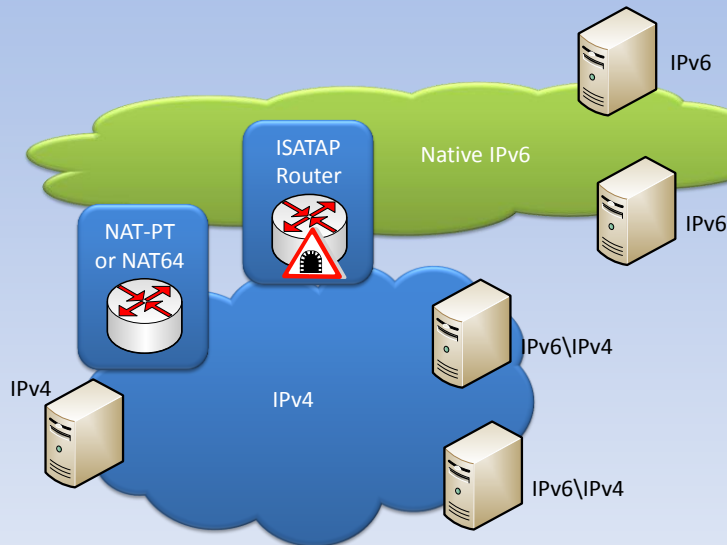


94

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## Summary: IPv6/IPv4 Intranet



95

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

### Ethernet adapter Local Area Connection:

```

Connection-specific DNS Suffix . . . . . : 
Description . . . . . : Microsoft Virtual Machine Bus Network Adapter
Physical Address. . . . . : 00-15-5D-0B-04-6C
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
IPv6 Address. . . . . : fd00:9999:0:2:ed99:dda3:ff0b:ec63(Preferred)
Temporary IPv6 Address. . . . . : fd00:9999:0:2:a48f:e34e:2283:9d1c(Preferred)
Link-local IPv6 Address . . . . . : fe80::ed99:dda3:ff0b:ec63%12(Preferred)
IPv4 Address. . . . . : 10.20.19.11(Preferred)
Subnet Mask . . . . . : 255.255.128.0
Default Gateway . . . . . : 
DHCPv6 IAID . . . . . : 251663709
DHCPv6 Client DUID. . . . . : 00-01-00-01-12-1d-50-16-00-15-5D-0B-04-6C
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                   : fec0:0:0:ffff::2%1
                   : fec0:0:0:ffff::3%1
NetBIOS over Tcpi. . . . . : Enabled
  
```

### Tunnel adapter isatap.{8C8B1176-A8F8-4CB7-93B2-971C461C6F78}:

```

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . : 
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
  
```

### Tunnel adapter Local Area Connection\* 11:

```

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . : 
Description . . . . . : Microsoft Teredo Tunneling Adapter
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
  
```



Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## Seminar Agenda

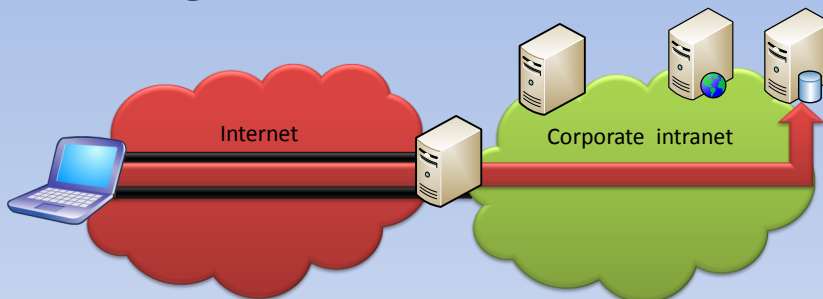
- IPv6
- Transition technologies
- Ipsec and DirectAccess
- Unified Access Gateway (UAG)
- Network Access Protection (NAP)
- Summary and Q&A

97

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Securing the Tunnel



- ✘ DirectAccess uses IPsec to secure network traffic
  - Traffic over the Internet is encrypted and authenticated
  - Access via IPHTTPs is double encrypted
    - Encrypted IPv6 within HTTPS

98

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## IPsec to the Rescue

- ✘ IPsec is managed through Windows Firewall with Advanced Security
  - Best deployed through group policy
- ✘ Connection rules create:
  - IPsec tunnels (authenticated and encrypted)
  - Authenticated connects (computer and user authentication)
- ✘ Inbound / outbound rules set requirements for encryption

99

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## Traffic Profile

Traffic profile:

<Protocol> <source IP> <destination IP> <source port> <destination port>

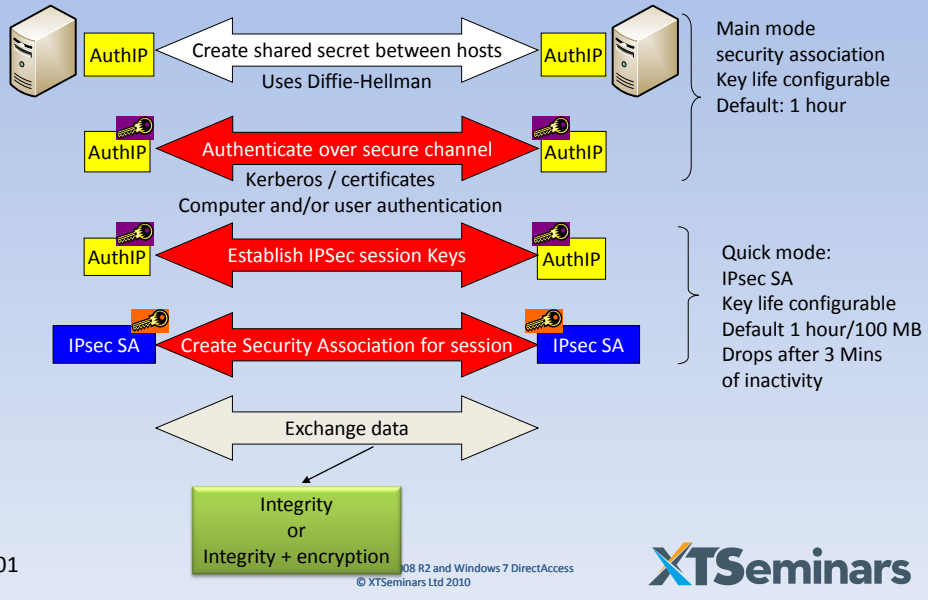
- ✘ Rules are based on a traffic profile
  - Connection Security Rule
    - Authenticate all TCP traffic between A & B on ports W & X
  - Inbound/Outbound Rule
    - Encrypt authenticated TCP traffic between A & B on ports W & X

100

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



# IPsec Primer



# Main Mode Association

Local Address	Remote Address	1st Authentication Method	2nd Authentication Method	Encryption	Integrity
2001:0:9013:a:10ce:a37:6fec:37fe	2002:9013:a:9013:b	Computer certificate	User (NTLMv2)	AES-CBC...	SHA-256
2001:0:9013:a:10ce:a37:6fec:37fe	2002:9013:b:9013:b	Computer certificate	User (Kerberos V5)	AES-CBC...	SHA-256

**2001:0:9013:a:10ce:a37:6fec:37fe Properties**

General

Local IP address: 2001:0:9013:a:10ce:a37:6fec:37fe  
Remote IP address: 2002:9013:b:9013:b

First authentication: Computer certificate  
First authentication Local ID: None  
First authentication Remote ID: None  
Second authentication: User (Kerberos V5)  
Second authentication Local ID: CORP\Administrator  
Second authentication Remote ID: host/da-da1.corp.example.com  
Encryption: AES-CBC 128  
Integrity: SHA-256  
Key exchange: None

[Learn more about these settings](#)

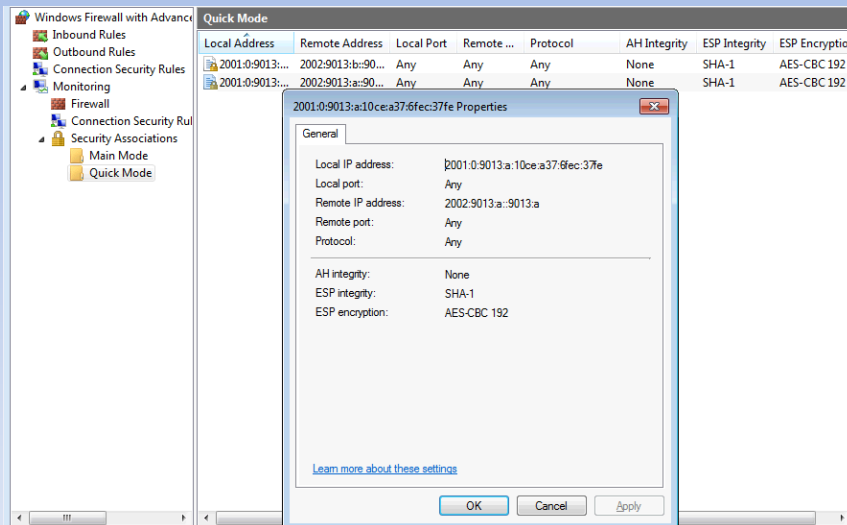
OK Cancel Apply

102

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## Quick Mode Association



103

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

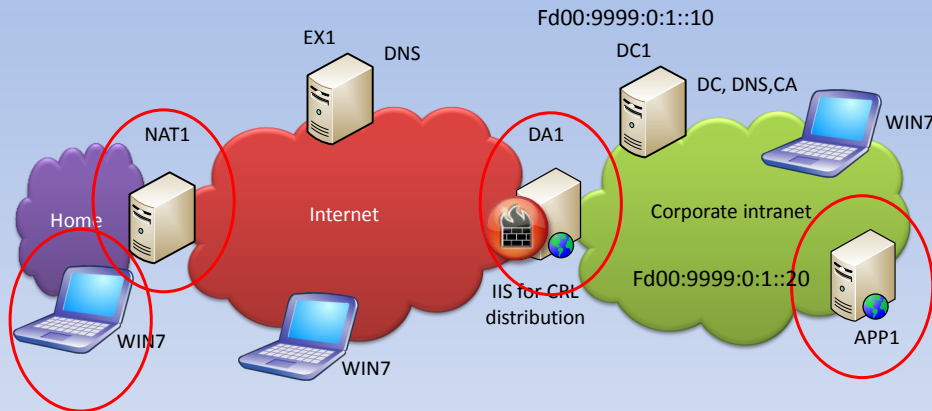
## Negotiated Security Options

- ✘ Request inbound and outbound
  - A host responds to both IPsec and unauthenticated (non-IPsec) requests
  - It initiates communications with IPsec, and if that fails, falls back to unauthenticated communications
- ✘ Require inbound and request outbound
  - A host responds to inbound traffic secured by IPsec, and ignores unauthenticated requests
  - It initiates communications with IPsec, and if that fails, falls back to unauthenticated communications
- ✘ Require inbound and require outbound
  - A host requires IPsec-secured communications for both inbound and outgoing requests

104

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

## Demo: IPsec

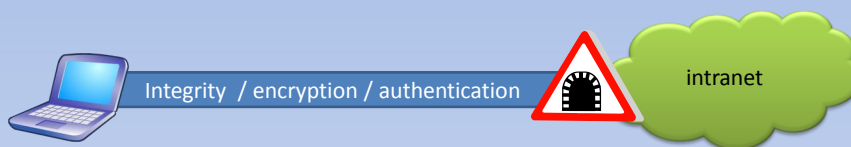


105

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## IPsec Tunnel



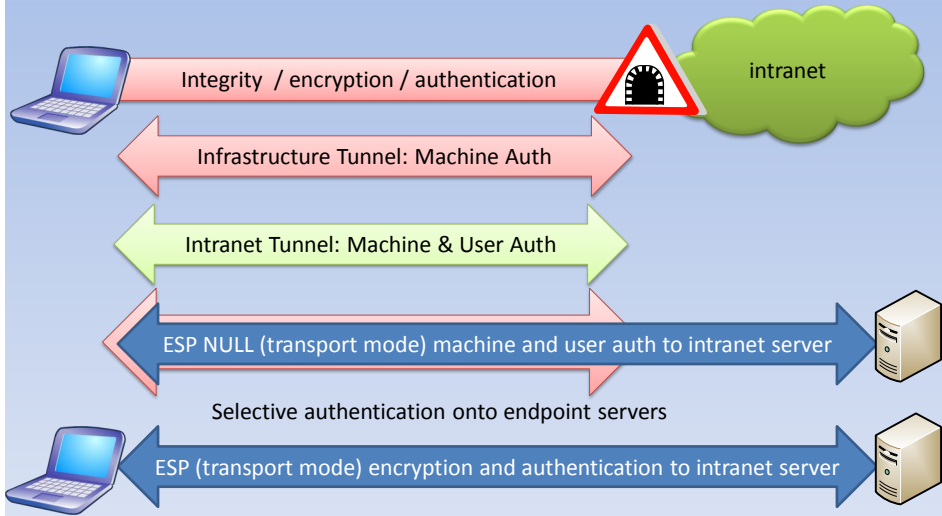
- ✘ End points can be single host or act as a gateway
  - The gateway acts as the end-point for integrity encryption and authentication
    - Traffic on the intranet is not protected by IPsec
- ✘ IPsec Gateway includes IPsec DoS Prevention
  - Reduces DoS attacks from key management protocols IKE & AuthIP

106

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

# IPsec Access Options

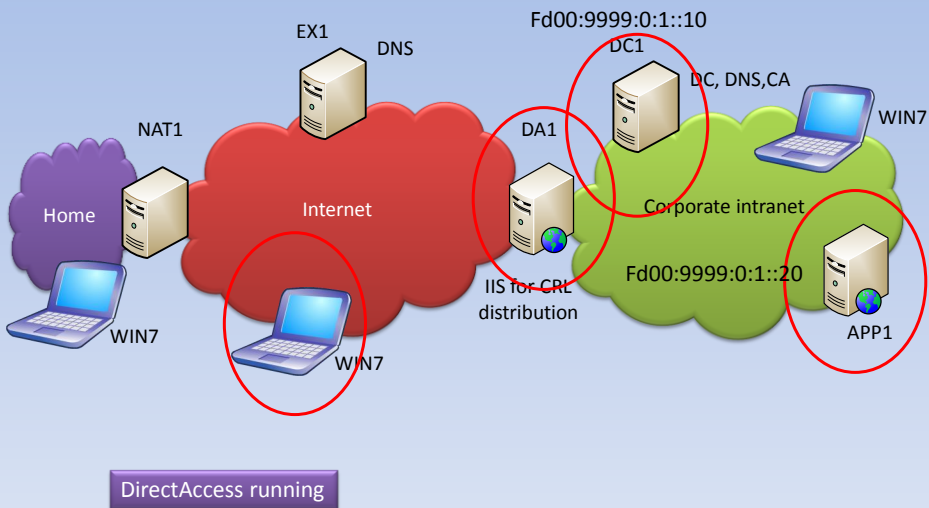


107

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



# Demo: DirectAccess Tunnels

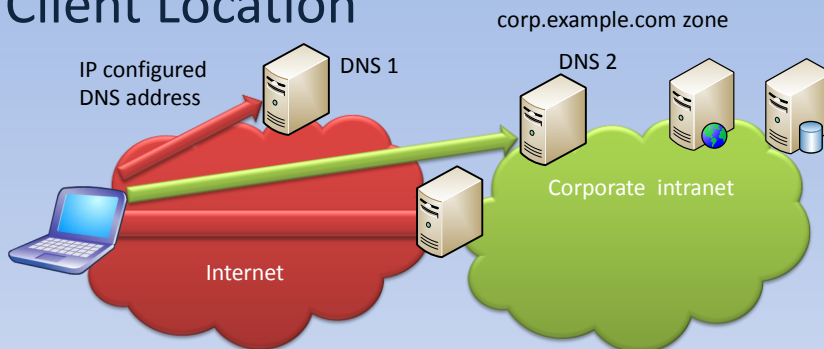


108

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## Client Location



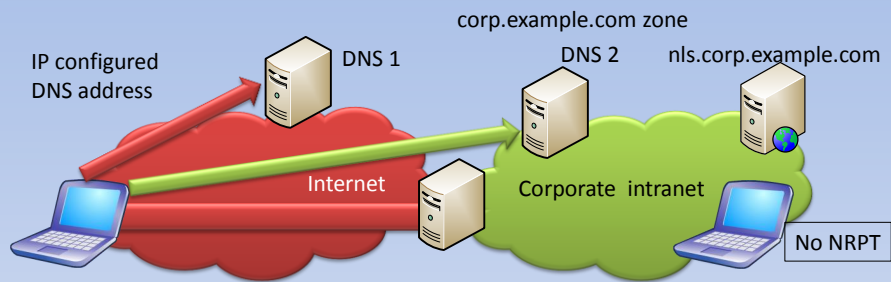
- ✘ To resolve names on the Internet
  - DirectAccess host queries DNS 1
- ✘ To resolve names on the intranet
  - DirectAccess host queries DNS 2

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

## How Does It Do that?

- ✘ Name Resolution Policy Table (NRPT) to the rescue
- ✘ NRPT allows the definitions of which DNS servers to query based on the namespace to be resolved
  - The NRPT can point DNS queries for corp.example.com to the intranet DNS server
  - All other DNS queries are sent to the DNS server address configured in the client IP settings

# NRPT



## NRPT:

corp.example.com: query DNS 2

All other name spaces query DNS server configured in client IP settings

There is a special entry in the table to direct DNS queries for an internal HTTPS website to the DNS servers configured in the client IP settings  
For example: queries for nls.corp.example.com always go to IP configured DNS address and this is not resolvable on the internet

111

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

# Viewing the NRPT

```
Administrator: Command Prompt

Settings for .corp.example.com
-----
Certification authority           : DC=com, DC=example, DC=corp, CN=corp-D
A-DCL-CA                         : disabled
DNSSEC (Validation)              : disabled
IPsec settings                   : disabled
DirectAccess (DNS Servers)       : 2002:9013:a:1:0:5efe:10.20.100.10
DirectAccess (Proxy Settings)    : Bypass proxy

Settings for nls.corp.example.com
-----
Certification authority           : DC=com, DC=example, DC=corp, CN=corp-D
A-DCL-CA                         : disabled
DNSSEC (Validation)              : disabled
IPsec settings                   : disabled
DirectAccess (DNS Servers)       :
DirectAccess (Proxy Settings)    : Bypass proxy

C:\windows\system32>
```

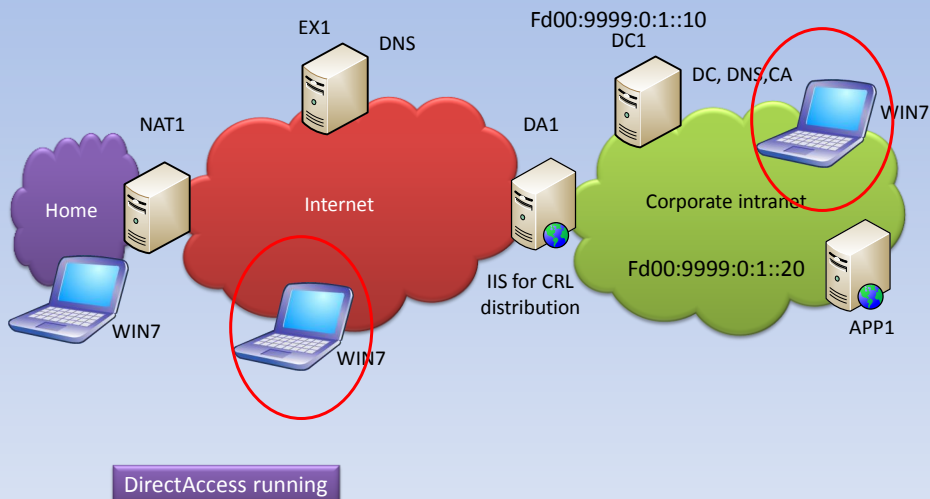
112

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**



## Demo: NRPT in Action



113

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## NRPT Inside/Outside

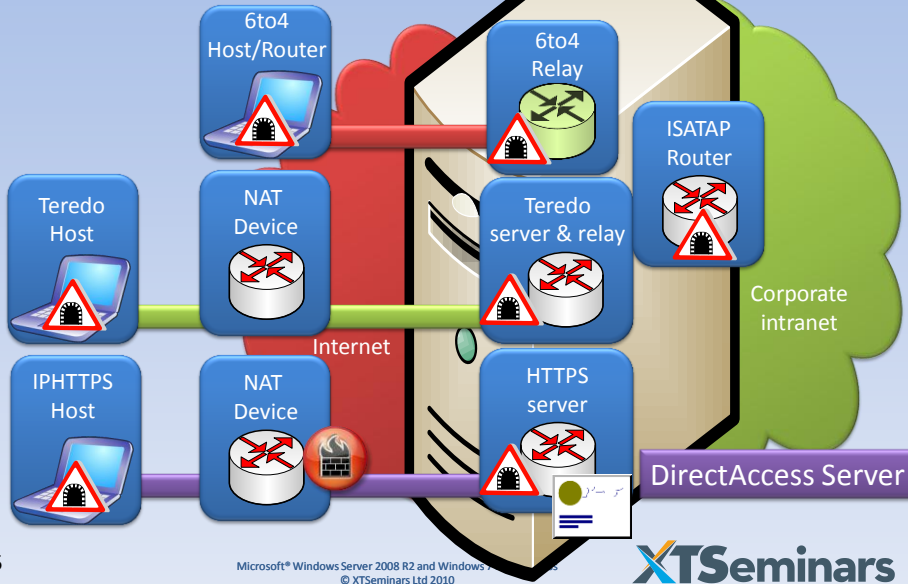
- ✘ NRPT enabled by default
- ✘ If the client can access an internal HTTPS website (<https://nls.corp.example.com>)
  - Considered to be on the intranet
  - NRPT disabled
- ✘ No access to secure website
  - Considered to be on the Internet
  - NRPT remains enabled

114

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

# Putting it All Together



115

Microsoft® Windows Server 2008 R2 and Windows 7  
© XTseminars Ltd 2010

**XTseminars**

# DirectAccess Management Console

**DirectAccess Setup**  
DirectAccess allows remote client computers to securely and seamlessly access the internal network.

Setup is complete. Click Finish to review a configuration summary.

**Step 1**

Remote Clients

Identify the client computers that will be enabled for DirectAccess.

Edit...

Internet

**Step 2**

DirectAccess Server

Define connectivity and security policies for controlling the DirectAccess server.

Edit...

**Step 3**

Infrastructure Servers

Identify the Infrastructure Servers (DNS, DC, Management) required by DirectAccess clients.

Edit...

**Step 4**

Application Servers

Identify the application servers that accept secure connections from clients.

Edit...

Internal Network

116

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Before Running Setup

- ✘ DNS server requires isatap block to be removed
- ✘ Set connection specific DNS suffix on the internal adapter
- ✘ Computer certificates must be issued to computers
- ✘ Server certificates must be issued to
  - DA server with external DNS name in certificate
  - NLS web server with nls url address in certificate
- ✘ CRL distribution should be configured in certificate
  - CRL distribution location must be available on both the Internet and intranet

117

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## Authentication to Servers

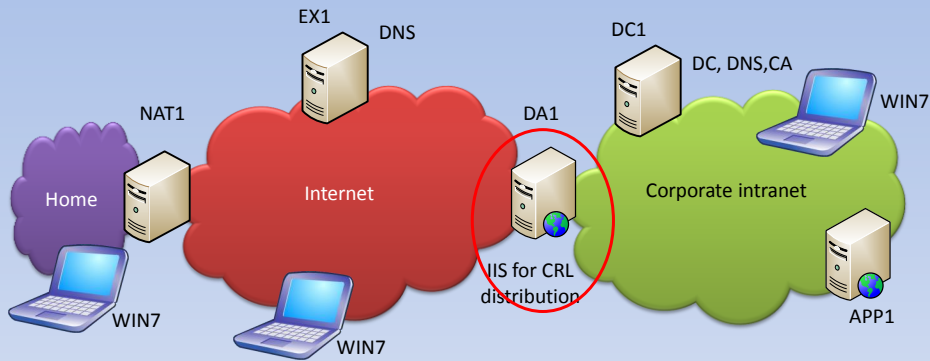
- ✘ IPsec ESP NULL can be used for authentication to end-point servers
  - Provides another layer of protection
  - Can control which servers are available from DA host
  - Requires 2008 end-point servers
    - IPSEC does not work over IPv6 for Windows 2003
- ✘ Two factor authentication can be enabled for end-to-end authentication
  - Requires 2008 domain functional level

118

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## Demo: DirectAccess Wizard



119

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## DirectAccess Setup

- ✘ Configures on DA server
  - 6to4 relay
  - Teredo server and relay
  - IPHTTPS server
  - ISATAP
- ✘ Creates group policy for IPsec rules for
  - DA server IPsec Tunnel
  - DA client IPsec Tunnel
  - DA clients and servers requiring end point authentication

120

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## DirectAccess Setup (continued)

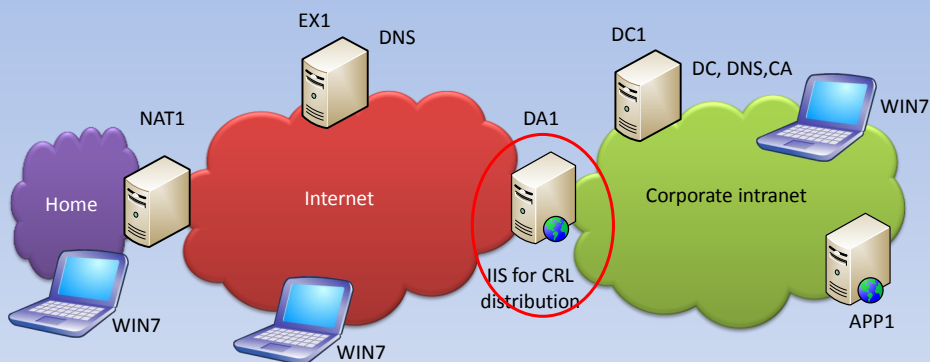
- ✘ Creates group policy for client configuration
  - Enable and supply addresses for
    - 6to4 relay
    - Teredo server and relay
    - IPHTTPS server
  - Enable and configure NRPT
  - Enable inside/outside probe
- ✘ DA server and DA clients must be members of the domain

121

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Demo: DA Configuration



122

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Windows DirectAccess

- ✘ The DA server represents a single point of failure
  - Functionality can be split across multiple servers for performance
- ✘ For HA, run DA server as VM in a Hyper-v cluster
  - Does not guarantee DA service availability
  - Live Migration available in Windows 2008 R2
- ✘ Load balancing option available with UAG

123

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



### Seminar Agenda

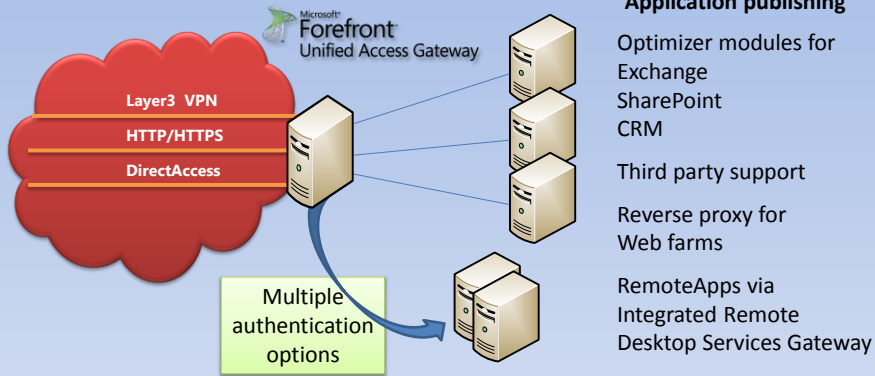
- IPv6
- Transition technologies
- Ipsec and DirectAccess
- Unified Access Gateway (UAG)
- Network Access Protection (NAP)
- Summary and Q&A

124

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



# Forefront Unified Access Gateway



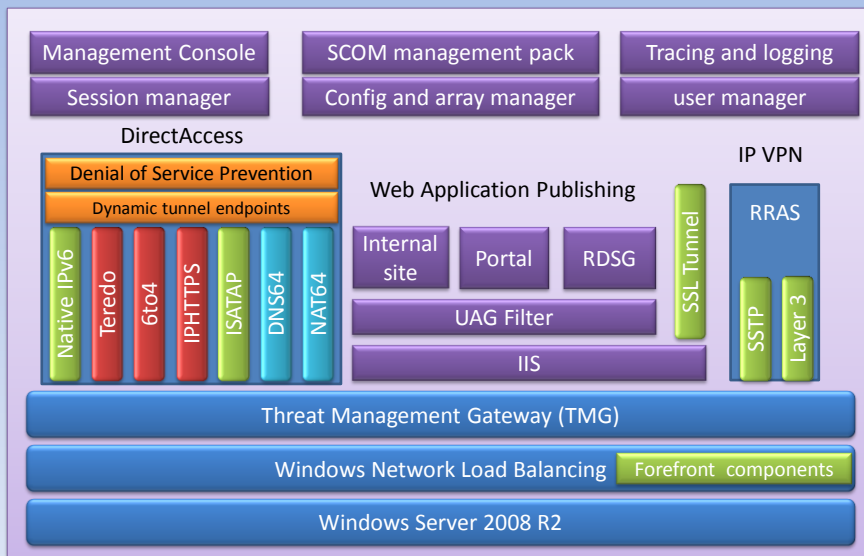
- ✕ Single entry-point for all remote access
  - Extends Windows DirectAccess capabilities to IPv4 only servers

125

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess © XTseminars Ltd 2010



# UAG Architecture

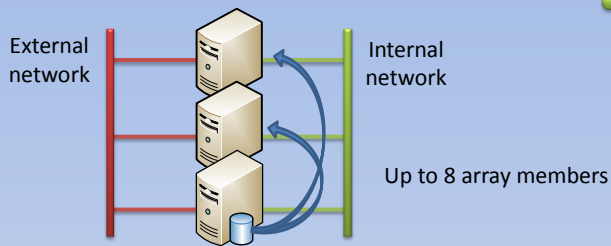


126

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess © XTseminars Ltd 2010



## UAG Array



- ✘ Array with Network Load Balancing (NLB) for increased scalability and availability
- ✘ One server acts as the Array Manager Server (AMS)
  - Configuration automatically propagated to all other array members
  - Configuration stored in AD LDS

127

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## UAG and DirectAccess

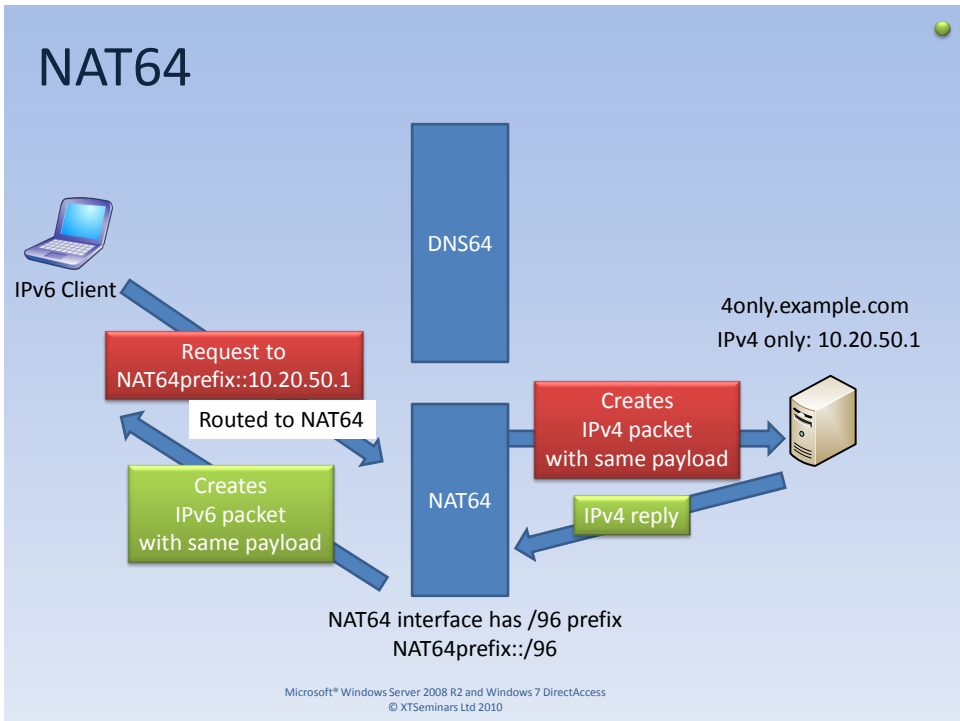
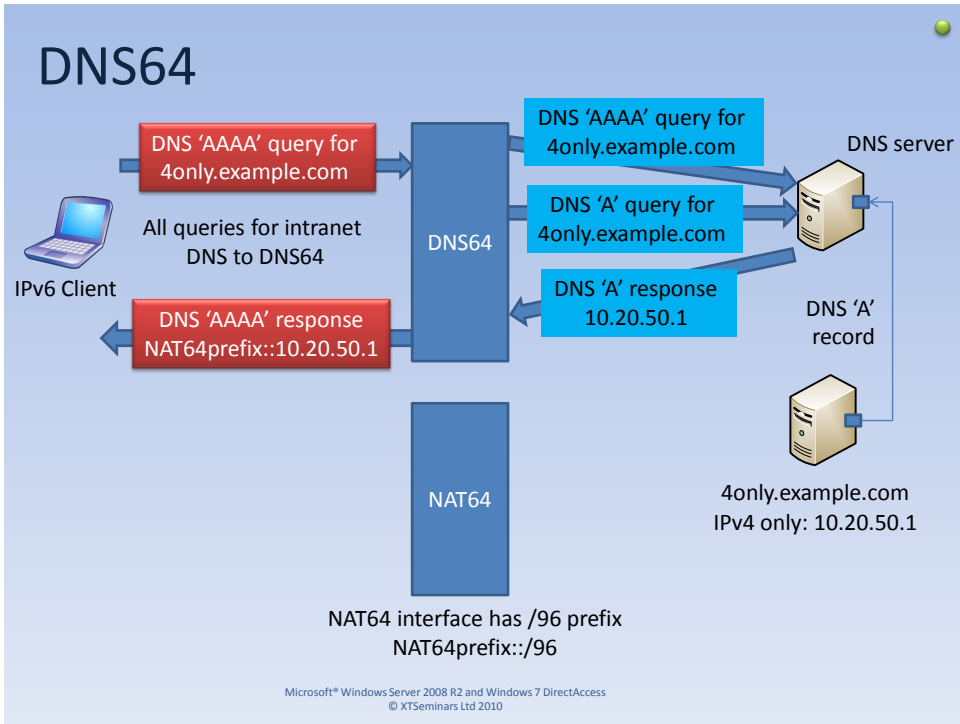
- ✘ The UAG wizard for DirectAccess provides many more configuration options
- ✘ DNS64 and NAT64 combine to allow access to IPv4 only servers

128

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**





# Connecting to http://da-app1

Frame Number	Time Offset	P	Source	Destination	Protocol Name	Description
53	14.453125		10.10.100.13	DA-APP1	TCP	TCP:Flags=...S, SrcPort=51631, DstPort=HTTP(80), Payload...
54	14.453125		10.10.100.13	DA-APP1	TCP	TCP:Flags=...A.S, SrcPort=HTTP(80), DstPort=51631, Payload...
55	14.453125		10.10.100.13	DA-APP1	TCP	TCP:Flags=...A.S, SrcPort=51631, DstPort=HTTP(80), Payload...
56	14.453125		10.10.100.13	DA-APP1	HTTP	HTTP:Request, GET /
57	14.453125		10.10.100.13	DA-APP1	HTTP	HTTP:Response, HTTP/1.1 Status Code = 304, URL: /
58	14.656250		10.10.100.13	DA-APP1	TCP	TCP:Flags=...A.S, SrcPort=51631, DstPort=HTTP(80), Payload...
59	14.453125		2002:9013:C8...	2002:9013:C8...	TCP	TCP:[Syn]Retransmit #53]Flags=...S, SrcPort=51631, DstPort=...
60	14.453125		2002:9013:C8...	2002:9013:C8...	TCP	TCP:Flags=...A.S, SrcPort=HTTP(80), DstPort=51631, Payload...
61	14.453125		2002:9013:C8...	2002:9013:2...	TCP	TCP:[Dup Ack #55]Flags=...A.S, SrcPort=51631, DstPort=HTT...

Frame Number	Time Offset	P	Source	Destination	Protocol Name	Description
59	29.516250		2002:9013:2...	2002:9013:C8...	TCP	TCP:Flags=...R., SrcPort=HTTP(80), DstPort=51638, Payload...
60	30.375000		FE80:0:0:0B8...	FF02:0:0:0:0...	DHCPV6	DHCPV6:MessageType = SOLICIT
61	46.375000		FE80:0:0:0B8...	FF02:0:0:0:0...	DHCPV6	DHCPV6:MessageType = SOLICIT
62	51.781250		10.10.100.13	DA-APP1	TCP	TCP:Flags=...S, SrcPort=19539, DstPort=HTTP(80), Payload...
63	51.781250		10.10.100.13	DA-APP1	TCP	TCP:Flags=...A.S, SrcPort=HTTP(80), DstPort=19539, Payload...
64	51.781250		10.10.100.13	DA-APP1	TCP	TCP:Flags=...A.S, SrcPort=19539, DstPort=HTTP(80), Payload...
65	51.808125		10.10.100.13	DA-APP1	HTTP	HTTP:Request, GET /
66	51.843750		10.10.100.13	DA-APP1	HTTP	HTTP:Response, HTTP/1.1 Status Code = 304, URL: /
67	52.046875		10.10.100.13	DA-APP1	TCP	TCP:Flags=...A.S, SrcPort=19539, DstPort=HTTP(80), Payload...

ISATAP enabled on DA-APP1

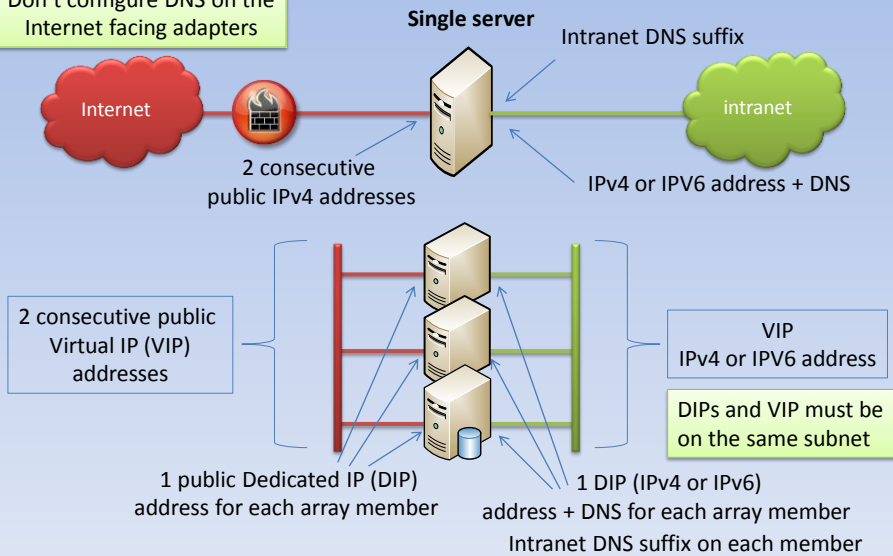
IPV4 only on DA-APP1

NAT64 in use

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess © XTseminars Ltd 2010

# Network Requirements for DA

Don't configure DNS on the Internet facing adapters



Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess © XTseminars Ltd 2010

## Preparing to install UAG for DA

- ✘ UAG is installed onto Windows Server 2008 R2
  - Accept the license and you're done
  - Check for latest updates
- ✘ The server must be domain joined for DA
- ✘ Requires certificates for IPHTTPS and Computer
  - Once UAG is installed RPC is blocked so either
    - Install certificates before installing UAG
    - Manual request and install the certificates
      - Can be requested via Certificates MMC

133

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## Getting Started Wizard

**Getting Started Wizard**

Welcome to Microsoft Forefront Unified Access Gateway 2010  
This wizard helps you configure your network settings.

- ✓ **Configure Network Settings**  
Specify how Forefront UAG is connected to your network. → Define internal and external networks
- ✓ **Define Server Topology**  
Optionally join this Forefront UAG server to an array. → Options:  
Single server  
Create array  
Join an array
- ✓ **Join Microsoft Update**  
Optionally join Microsoft Update to receive updates for Forefront UAG.

Close

134

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## DirectAccess Wizard

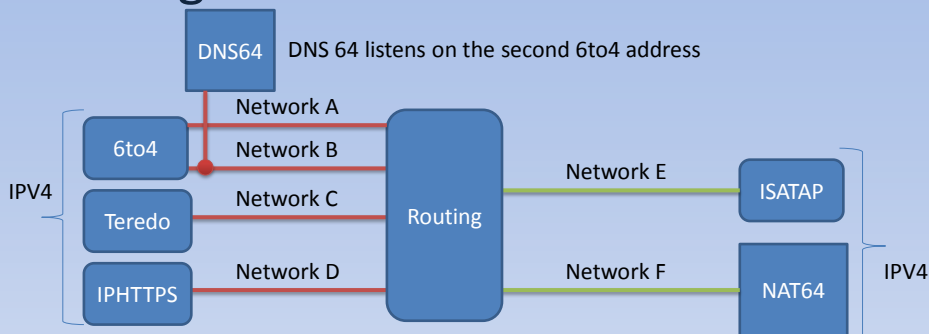
- ✘ The DirectAccess wizard is similar to the Windows Server 2008 R2 version
  - If the Internal address is IPv4
    - Automatically selects address ranges
    - Enables DNS64 & NAT64
    - Configures all transition technologies including an ISATAP router
  - If the internal address is IPv6
    - Address prefixes can be configured through the UI

135

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Routing Traffic



- ✘ Traffic entering/leaving through the Internet facing tunnels must either be routed to/from the
  - ISATAP tunnel
  - NAT64 translator

136

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Routing Continued

- ✘ To be able to route traffic each network must have a different identity
- ✘ Teredo has a predefined network prefix of 2001::/32
- ✘ For the remaining networks the DirectAccess wizard generates different networks based on the 1<sup>st</sup> 6to4 address of the Internet facing address
  - Remember the 6to4 address is globally unique as it is based on the public IPv4 address
    - 144.19.0.2 translates to 2002:9013:c802::9013:c802

137

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## Calculating the Networks

2002:9013:c802::9013:c802  2002:9013:c802:0000::/64

Subnets created  
To identify other  
networks

Network	Prefix
Network A: 6to4 (144.19.0.2)	2002:9013:c802:0000::/64
Network B: 6to4 (144.19.0.3)	2002:9013:c803:0000::/64
Network C: Teredo	2001:0::/32
Network D: IPHTTPS	2002:9013:c802:8100::/56
Network E: ISATAP	2002:9013:c802:8000::/64
Network F: NAT64	2002:9013:c802:8001:0000:0000::/96

The organizational prefix (this organization's network) is set to: 2002:9013:c802:8000::/49

138

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## Tunnel End Points

```

Rule Name: UAG DirectAccess Gateway - Clients Access
Enabling Tunnel - All
-----
Enabled: Yes
Profiles: Private,Public
Type: Dynamic
Mode: Tunnel
LocalTunnelEndpoint: 2002:9013:3::9013:3
  
```

- ✘ The Dynamic Tunnel End Points (DTE) for the infrastructure and intranet tunnels terminate on the two 6to4 addresses of the DA server
  - One DTE on each address
- ✘ View the endpoints with
  - netsh advfirewall consec show rule name=all type=dynamic

139

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## Infrastructure Tunnel

- ✘ The infrastructure tunnel Ipsec rules are applied to any traffic destined to the:
  - 6to4 address of DNS64
  - ISATAP addresses of the infrastructure servers
    - DC, DNS, NAP remediation, client management
  - NAT64 addresses of the infrastructure servers
- ✘ IPsec rule requires certificate and user (computer account) authentication
  - ICMP is exempt

140

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## Intranet Tunnel

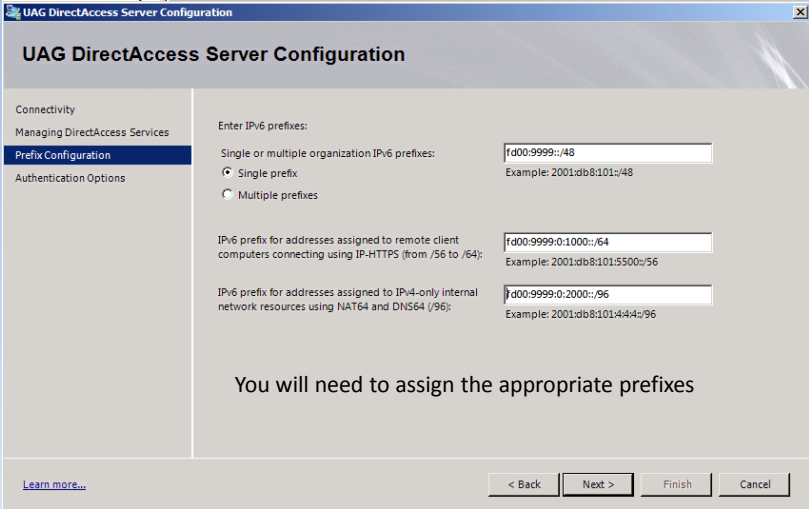
- ✘ The intranet tunnel IPsec rules are applied to any traffic destined to the:
  - Organizational prefix
    - In our example 2002:9013:c802:8000::/49
- ✘ IPsec rule requiring certificate and user (user account) authentication
  - ICMP is exempt

141

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## IPv6 on UAG Internal Network



**UAG DirectAccess Server Configuration**

Connectivity  
Managing DirectAccess Services  
**Prefix Configuration**  
Authentication Options

Enter IPv6 prefixes:

Single or multiple organization IPv6 prefixes:   
Example: 2001:db8:101::48

Single prefix  
 Multiple prefixes

IPv6 prefix for addresses assigned to remote client computers connecting using IP-HTTPS (from /56 to /64):   
Example: 2001:db8:101:5500::56

IPv6 prefix for addresses assigned to IPv4-only internal network resources using NAT64 and DNS64 (/96):   
Example: 2001:db8:101:4:44::96

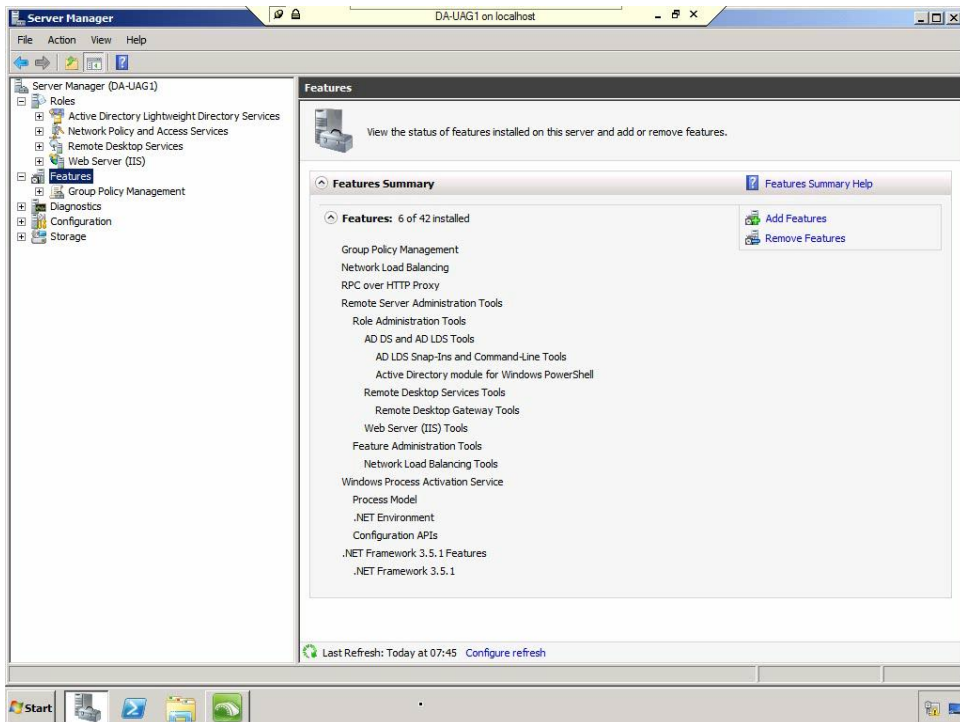
You will need to assign the appropriate prefixes

[Learn more...](#)

142

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010





## DirectAccess Connectivity Assistant

DirectAccess Connectivity Assistant GP.adml	ADML File
DirectAccess Connectivity Assistant GP.ADMX	ADMX File
Microsoft_DirectAccess_Connectivity_Assistant_DeploymentGuide	Office Open XML ...
Microsoft_DirectAccess_Connectivity_Assistant_Release_Notes.en	HTML Document
Microsoft_DirectAccess_Connectivity_Assistant_x64	Windows Installer ...
Microsoft_DirectAccess_Connectivity_Assistant_x86	Windows Installer ...

- ✗ Download from Microsoft
- ✗ Install the MSI on the Direct Access client
- ✗ Copy the .admx file to
  - %systemroot%\PolicyDefinitions.
- ✗ Copy the .adml file to
  - %systemroot%\PolicyDefinitions\



## Group Policy for DCA

Setting	State	Comment
PortalName	Not configured	No
Support Email	Not configured	No
Corporate Portal Site	Not configured	No
DTEs	Not configured	No
LocalNamesOn	Not configured	No
Corporate Resources	Not configured	No
Admin Script	Not configured	No

### ✘ To get DCA functioning

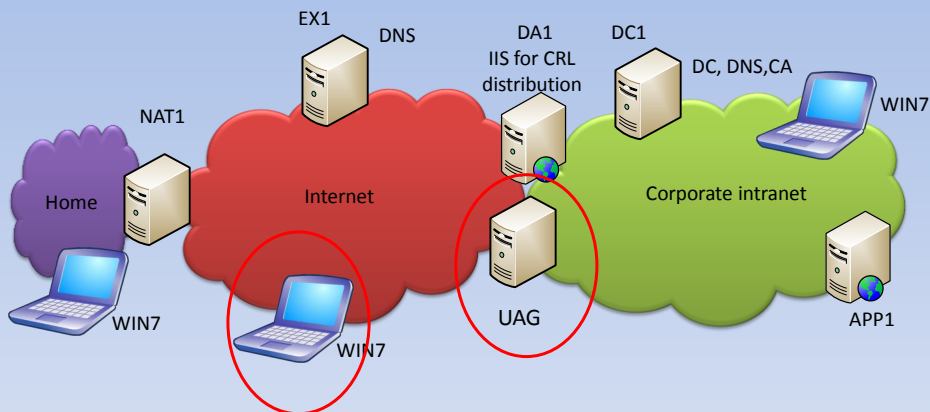
- Add settings for the Dynamic Tunnel End points
- Identify CorporateResources to test
  - PING:da-app1.corp.example.com
  - HTTP:http://da-app1.corp.example.com
  - FILE:\\da-app1.corm.example.com\data\test.txt

145

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Demo: Configuring DCA



146

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Seminar Agenda

- IPv6
- Transition technologies
- Ipsec and DirectAccess
- Unified Access Gateway (UAG)
- Network Access Protection (NAP)
- Summary and Q&A

147

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## What is Network Access Protection?



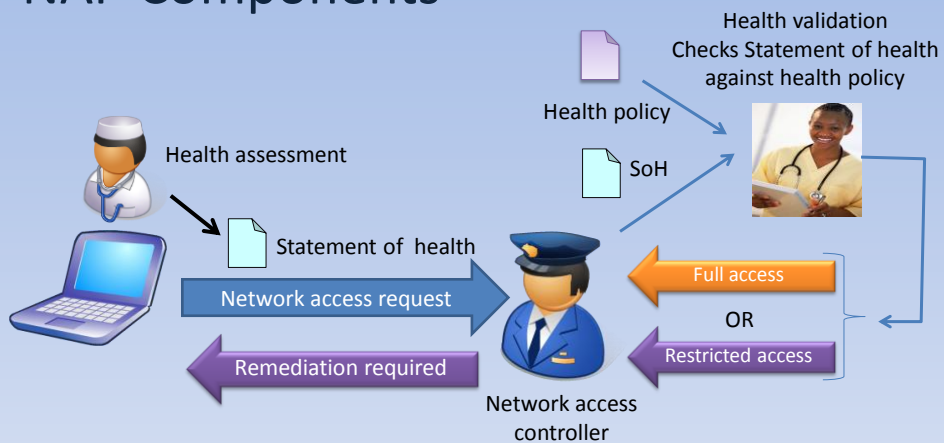
- ✘ A set of technologies that allows or restricts a computer's network access based on its health
  - Automatic remediation is possible for restricted systems

148

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## NAP Components



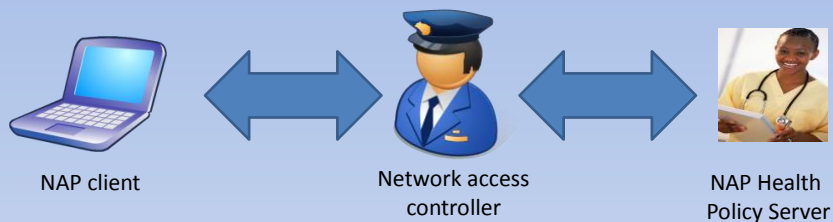
- ✘ While access is restricted, clients can gain access to remediation servers and automatically update their compliance

149

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Three Key Components



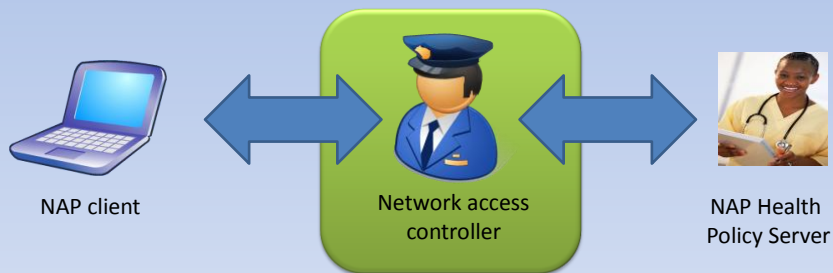
- ✘ The network access controller is the man in the middle!
  - Relays the client health to the health policy server
  - Instructed by the health policy server to allow or restrict the client's network access

150

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Three Key Components



151

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

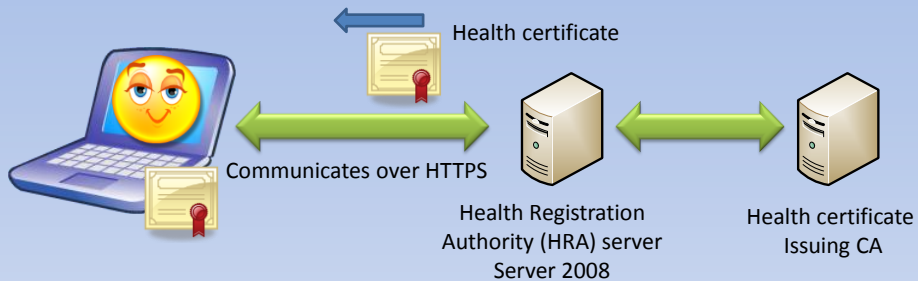
## Network Access Control

- ✗ The NAP component that controls access to the network is called the NAP Enforcement Point (NAP EP)
- ✗ Included in Windows Server 2008 are NAP EPs for
  - DHCP server
  - VPN server
  - Network access device that supports 802.1x authentication
  - Health Registration Authority (HRA) issues certificates to compliant hosts
    - IPsec restricts network access for non compliant hosts
  - Terminal Server Gateway
    - Drops connection if not compliant

152

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

## DirectAccess & IPsec Enforcement



The Health Certificate is used to authenticate to the DirectAccess tunnel end point

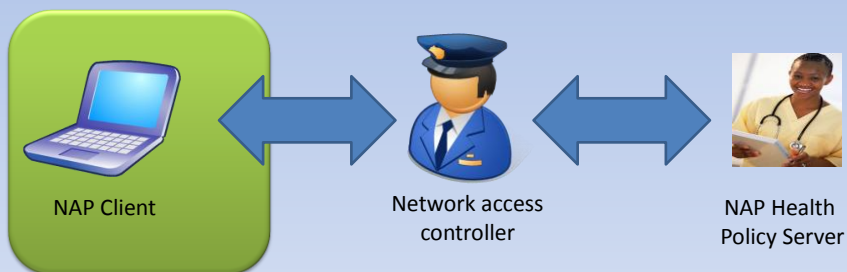
**No Health Certificate = No Access**

153

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Three Key Components

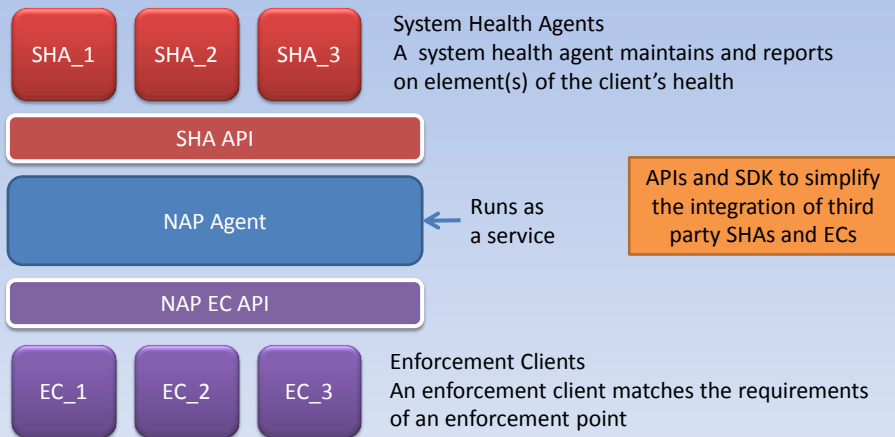


154

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Client Architecture



155

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## System Health Agent

Health Checks	Results
Firewall on?	
Antivirus application on?	
Virus signature	
Antispyware application on?	

- ✘ The SHA gathers information about the health of the NAP client
  - SHAs can be created to check different aspects of the computer's health
    - Think of the SHA as filling in a predefined check list
  - The completed checklist is a Statement of Health (SoH)

156

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Remediation



- ✘ A SHA can be instructed by the health policy server to remediate a client's non-compliance
  - For example
    - Turn on the firewall
    - Update antivirus signatures from a remediation server

157

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Client Configuration

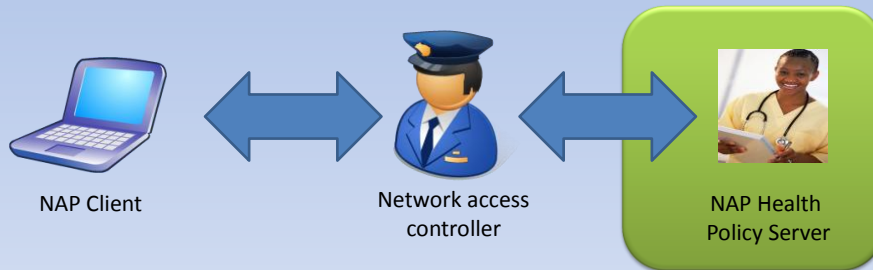
- ✘ The Network Access Protection service must be enabled and running
- ✘ The client can be configured through
  - NAP Client Configuration console
    - Napclcfg.msc
    - Only available for 2008/Vista/Windows 7
  - Group policy
    - If enabled overrides all local settings
  - Netsh

158

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Three Key Components



159

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Network Policy Server

- ✘ Installed as part of Network Policies and Access Services Role
  - Network Policy Server (NPS)
    - RADIUS Server
    - Replaces Internet Authentication Server (IAS)
      - Windows Server 2003's implementation of RADIUS

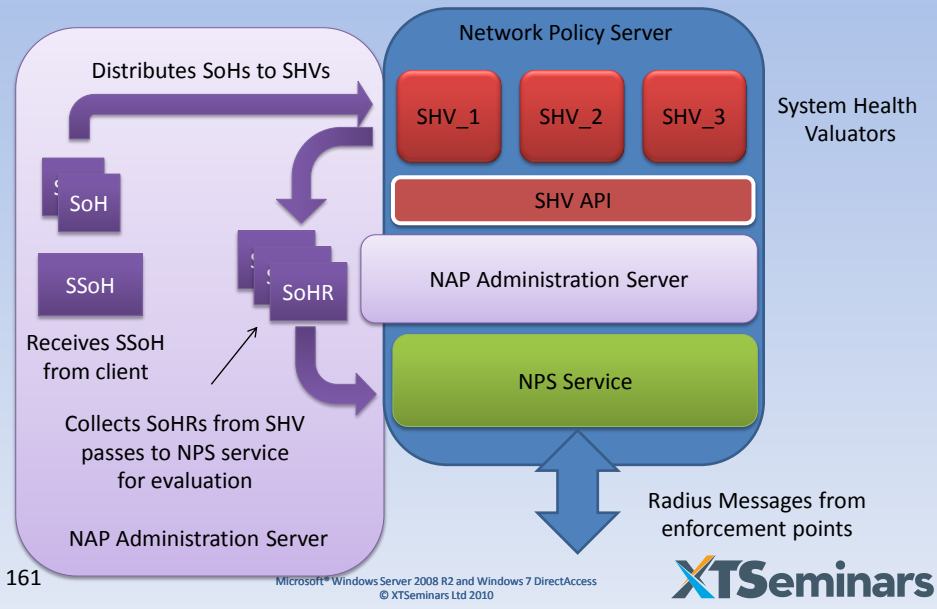
160

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

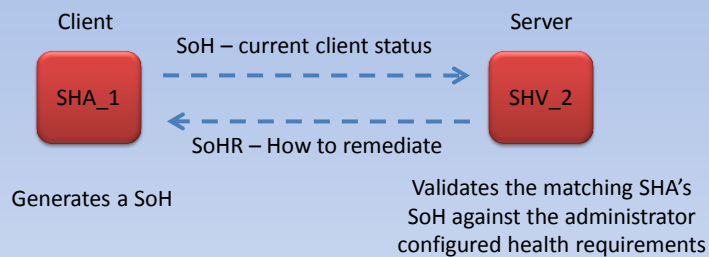
**XTseminars**



## NPS Architecture



## SHAs and SHVs



### ✕ SHAs and SHVs are matched

- Installing a third party SHA on a client will also require the server SHV to be installed

## NPS Policies

### Connection Request Policies

Specifies if a particular connection request should be processed locally or remotely

### Network Policies

Specifies how a particular connection request should be processed  
Can specify NAP enforcement based on health policy

### Health Policies

Create definitions for compliant / noncompliant systems based on SHV results

163

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## Deployment

### ✘ Reporting mode

- Network access is unrestricted and users are unaware that compliance is being checked

### ✘ Deferred enforcement

- Unrestricted access until a predefined date
  - At which point noncompliant computers will have their access restricted

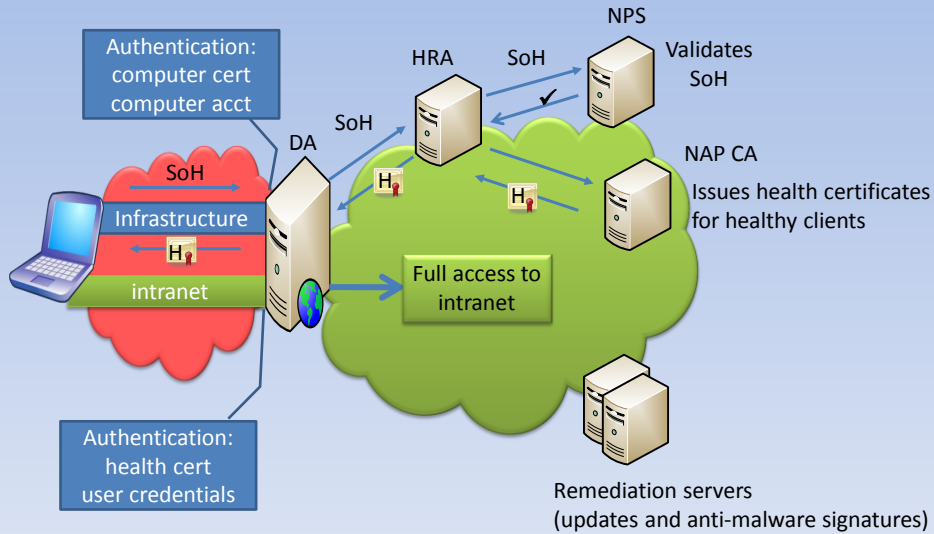
### ✘ Enforcement mode

164

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



## DirectAccess and NAP (Healthy)

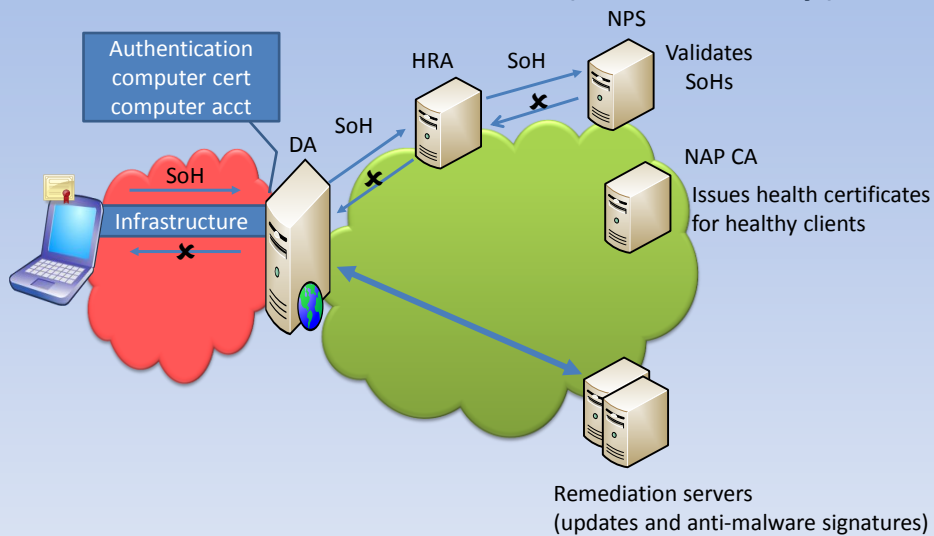


165

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## DirectAccess and NAP (Unhealthy)



166

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Integration Points

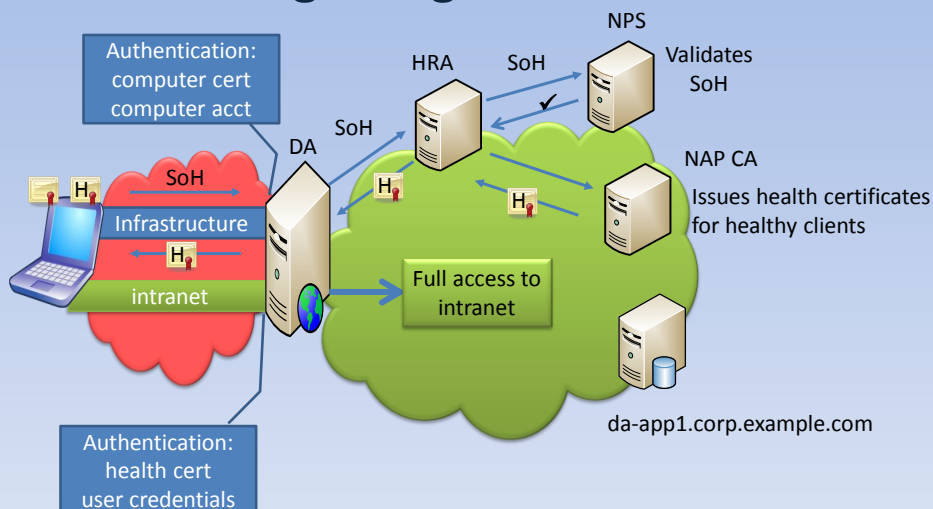
- ✘ HRA and remediation servers must be added to the list of infrastructure/management servers
  - HRA authentication must be set to NTLM
- ✘ Intranet tunnel connection security rules changed to use Health Certificate as first authentication mechanism
- ✘ An alternate design can be created by implementing an external HRA server

167

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Demo: Integrating NAP




168

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**


## Seminar Agenda

- IPv6
- Transition technologies
- Ipsec and DirectAccess
- Unified Access Gateway (UAG)
- Network Access Protection (NAP)
- Summary and Q&A

169
Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010


## A VPN on Steroids

Always On

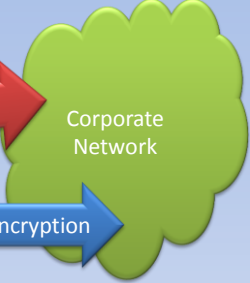


Automatically  
connects through  
NAT and firewalls

Pre log on

Patch management, health check and GPOs


Network level computer/user authentication and encryption



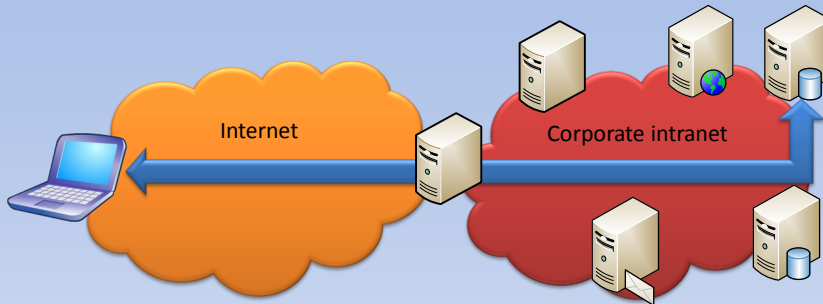
Corporate  
Network





*VPNs connect the user to the network*

*DirectAccess extends the network to the remote computer and user*

170
Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010


# The Challenges



-  Tunnelling technologies for the Internet and intranet to support IPv6 over IPv4
-  Internet tunnelling selection based on client location – Internet, NAT, firewall
-  Encryption/authentication of Internet traffic (end-to-edge/end-to-end)  
PKI required
-  Client location detection: Internet or corporate intranet

171

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Ethernet adapter Local Area Connection:

```

Connection-specific DNS Suffix . . . . . : 
Description . . . . . : Microsoft Virtual Machine Bus Network Adapter
Physical Address. . . . . : 00-15-5D-0B-04-6C
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
IPv6 Address. . . . . : fd00:9999:0:2:ed99:dda3:ff0b:ec63(Preferred)
Temporary IPv6 Address. . . . . : fd00:9999:0:2:a48f:e34e:2283:9d1c(Preferred)
Link-local IPv6 Address . . . . . : fe80::ed99:dda3:ff0b:ec63%12(Preferred)
IPv4 Address. . . . . : 10.20.19.11(Preferred)
Subnet Mask . . . . . : 255.255.128.0
Default Gateway . . . . . : 
DHCPv6 IAID . . . . . : 251663709
DHCPv6 Client DUID. . . . . : 00-01-00-01-12-1d-50-16-00-15-5d-0b-04-6c
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                          fec0:0:0:ffff::2%1
                          fec0:0:0:ffff::3%1
NetBIOS over Tcpi. . . . . : Enabled
  
```

## Tunnel adapter isatap.{8c8b1176-a8f8-4cb7-93b2-971c461c6f78}:

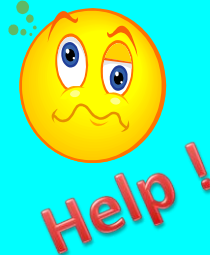
```

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . : 
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
  
```

## Tunnel adapter Local Area Connection\* 11:

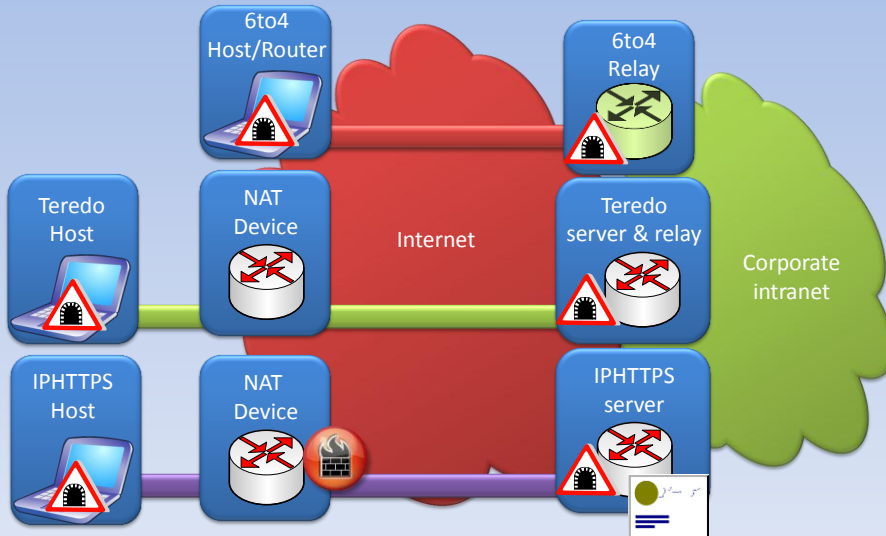
```

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . : 
Description . . . . . : Microsoft Teredo Tunneling Adapter
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
  
```



Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

## Summary: Internet to Intranet

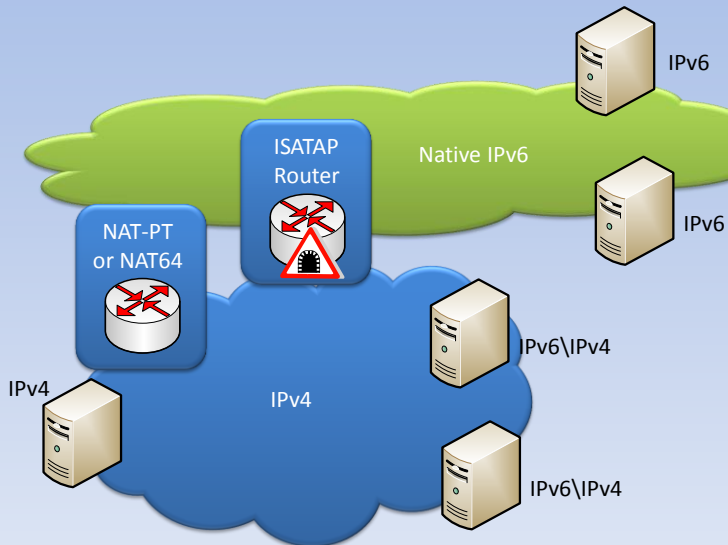


173

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

## Summary: IPv6/IPv4 Intranet

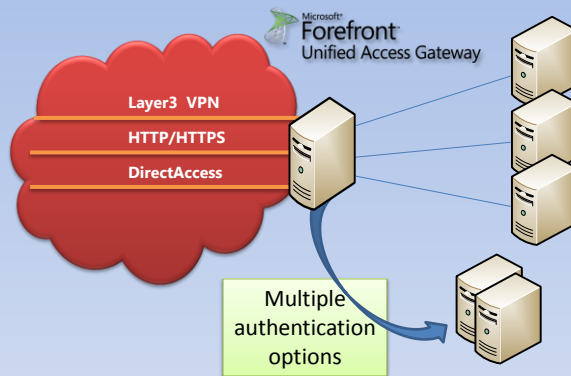


174

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

**XTseminars**

# Forefront Unified Access Gateway



## Application publishing

- Optimizer modules for Exchange SharePoint CRM
- Third party support
- Reverse proxy for Web farms
- RemoteApps via Integrated Remote Desktop Services Gateway

## Single entry-point for all remote access

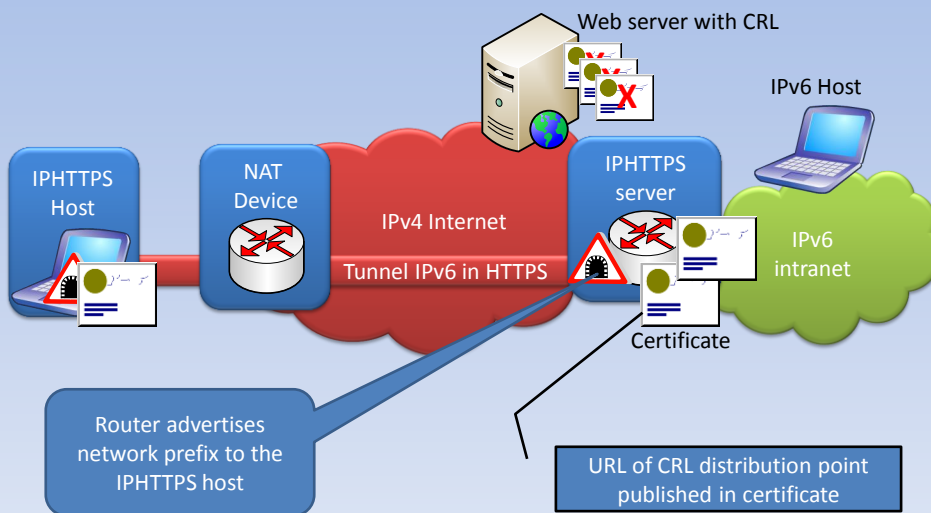
- Extends Windows DirectAccess capabilities to IPv4 only servers

175

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess © XTseminars Ltd 2010



# IPHTTPS Components



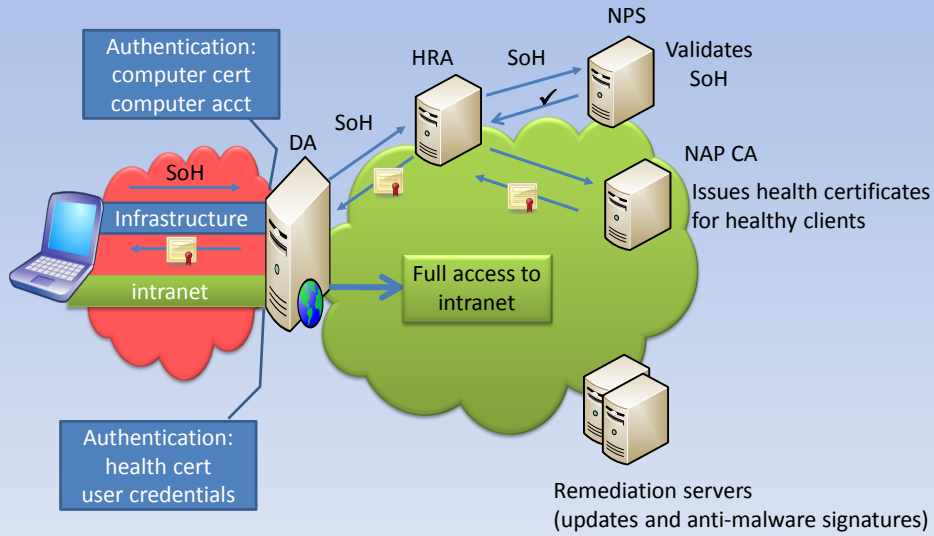
176

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess © XTseminars Ltd 2010





# DirectAccess and NAP



177

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



# Any questions



178

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010



# XTSeminars

And so we reach the end!

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTSeminars Ltd 2010

XTSeminars

## Any Questions

✕ Please email technical queries to:

[johncra@xtseminars.co.uk](mailto:johncra@xtseminars.co.uk)

✕ Consultancy services also available

Thanks for coming to the seminar  
Hope to see you again

A handwritten signature in white ink, appearing to read 'John', is centered on the slide.

Microsoft® Windows Server 2008 R2 and Windows 7 DirectAccess  
© XTseminars Ltd 2010

The logo for XTseminars, featuring the letters 'XT' in a stylized blue and orange font followed by the word 'seminars' in a black sans-serif font.