

The image shows a screenshot of the Network Policy Server (NPS) console on the left and the 'Configure 802.1X' wizard on the right. The console displays a tree view with 'NPS (Local)' expanded, showing folders for 'RADIUS Clients and Servers', 'Policies', and 'Network Access Protection'. The 'Getting Started' section is active, showing a 'Standard Configuration' tab with a list of scenarios. The 'RADIUS server for 802.1X Wireless connections' scenario is selected, and a 'Configure 802.1X' button is highlighted with a red box. The wizard on the right is titled 'Select 802.1X Connections Type' and has two radio button options: 'Secure Wireless Connections' (selected and highlighted with a red box) and 'Secure Wired (Ethernet) Connections'. Below the options is a 'Name:' field with the text 'WirelessPolicy' (highlighted with a red box). At the bottom of the wizard, the 'Next' button is highlighted with a red box.

**Network Policy Server**

File Action View Help

NPS (Local)

- RADIUS Clients and Servers
  - RADIUS Clients
  - Remote RADIUS Server Groups
- Policies
  - Connection Request Policies
  - Network Policies
  - Health Policies
- Network Access Protection
- Accounting

**Getting Started**

Network Policy Server (NPS) allows you to manage client health, connection requests, and policies.

**Standard Configuration**

Select a configuration scenario from the list.

RADIUS server for 802.1X Wireless connections

**RADIUS server for 802.1X Wireless connections**

When you configure NPS as a RADIUS server, NPS authenticates and authorizes connections made by RADIUS clients.

**Configure 802.1X**

**Advanced Configuration**

**Configure 802.1X**

**Select 802.1X Connections Type**

**Type of 802.1X connections:**

- Secure Wireless Connections
- Secure Wired (Ethernet) Connections

When you deploy 802.1X wireless access points on your network, NPS can authenticate and authorize connection requests made by wireless clients connecting through the access points.

When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethernet clients connecting through the switches.

**Name:**

This default text is used as part of the name for each of the policies created with this wizard. You can use the default text or modify it.

WirelessPolicy

Previous **Next** Finish Cancel

Step through the Wizard again to add your wireless client.

The image shows the Network Policy Server (NPS) console on the left and the 'Configure 802.1X' dialog box on the right. The console displays a tree view with 'RADIUS Clients and Servers' expanded, and a 'Getting Started' section with a 'Configure 802.1X' button. The dialog box is titled 'Specify 802.1X Switches' and contains a list of RADIUS clients. One client, 'Aironet 1200', is selected, and its properties are shown in a sub-dialog. The 'Add...' button in the client list and the 'OK' button at the bottom of the main dialog are highlighted with red boxes.

**Network Policy Server Console:**

- File Action View Help
- NPS (Local)
  - RADIUS Clients and Servers
    - RADIUS Clients
    - Remote RADIUS Server Groups
  - Policies
    - Connection Request Policies
    - Network Policies
    - Health Policies
  - Network Access Protection
    - Accounting

**Getting Started**

Network Policy Server (NPS) allows you to configure NPS for client health, connection request, and network access protection.

**Standard Configuration**

Select a configuration scenario from the list below.

**RADIUS server for 802.1X Wireless LAN**

When you configure NPS as a RADIUS server, you must configure NPS to authenticate and authorize client computers called RADIUS clients.

[Configure 802.1X](#)

**Advanced Configuration**

**Configure 802.1X Dialog:**

**Specify 802.1X Switches**

Please specify 802.1X switches or Wireless Access Points (RADIUS Clients).

RADIUS clients are network access servers, such as authenticating switches and wireless access point. RADIUS clients are not client computers.

To specify a RADIUS client, click Add.

**RADIUS clients:**

Name	Address
SRW2008P	

**Aironet 1200 Properties**

**Name and Address**

Friendly name: Aironet 1200

Address (IP or DNS): 192.168.0.4

**Shared Secret**

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

Manual  Generate

Shared secret: .....

Confirm shared secret: .....

**Buttons:** Add..., Edit..., Remove, OK, Cancel

The image shows a screenshot of the Windows Network Policy Server (NPS) console and a configuration wizard. The console window on the left displays the 'Getting Started' section with a 'Standard Configuration' pane. The 'Standard Configuration' pane contains a list of configuration scenarios, with 'RADIUS server for 802.1X Wireless' selected. Below this list is a 'Configure 802.1X' button. The 'Advanced Configuration' section is also visible but empty.

The 'Configure 802.1X' wizard window is open on the right. It has a title bar 'Configure 802.1X' and a close button. The main content area is titled 'Specify 802.1X Switches' and includes the instruction: 'Please specify 802.1X switches or Wireless Access Points (RADIUS Clients)'. Below this, there is explanatory text: 'RADIUS clients are network access servers, such as authenticating switches and wireless access point. RADIUS clients are not client computers. To specify a RADIUS client, click Add.' A list box labeled 'RADIUS clients:' contains two entries: 'SRW2008P' and 'Aironet 1200'. To the right of the list box are three buttons: 'Add...', 'Edit...', and 'Remove'. At the bottom of the wizard window, there are four buttons: 'Previous', 'Next', 'Finish', and 'Cancel'. The 'Next' button is highlighted with a red rectangle.

**Step through the Wizard to select the required protocol and click "Finish" when you are done.**

The image shows a screenshot of the Network Policy Server (NPS) console and a 'Configure 802.1X' wizard window. The NPS console on the left has a tree view with 'NPS (Local)' expanded to show 'RADIUS Clients and Servers', 'Policies', and 'Network Access Protection'. The 'Getting Started' pane shows 'Standard Configuration' selected, with a list of scenarios including 'RADIUS server for 802.1X Wireless'. A 'Configure 802.1X' button is visible. The wizard window on the right is titled 'Configure 802.1X' and has a sub-header 'Completing New IEEE 802.1X Secure Wired and Wireless Connections and RADIUS clients'. It contains a summary of created policies and a 'Finish' button highlighted with a red box.

**Network Policy Server**

File Action View Help

NPS (Local)

- RADIUS Clients and Servers
  - RADIUS Clients
  - Remote RADIUS Server Groups
- Policies
  - Connection Request Policies
  - Network Policies
  - Health Policies
- Network Access Protection
  - Accounting

**Getting Started**

Network Policy Server (NPS) allows you to configure NPS for client health, connection request, and network access protection.

**Standard Configuration**

Select a configuration scenario from the list below.

- RADIUS server for 802.1X Wireless connections

**RADIUS server for 802.1X Wireless connections**

When you configure NPS as a RADIUS server, NPS authenticates and authorizes wireless clients (called RADIUS clients).

[Configure 802.1X](#)

**Advanced Configuration**

**Configure 802.1X**

**Completing New IEEE 802.1X Secure Wired and Wireless Connections and RADIUS clients**

You have successfully created the following policies and configured the following RADIUS clients.

- To view the configuration details in your default browser, click [Configuration Details](#).
- To change the configuration, click [Previous](#).
- To save the configuration and close this wizard, click [Finish](#).

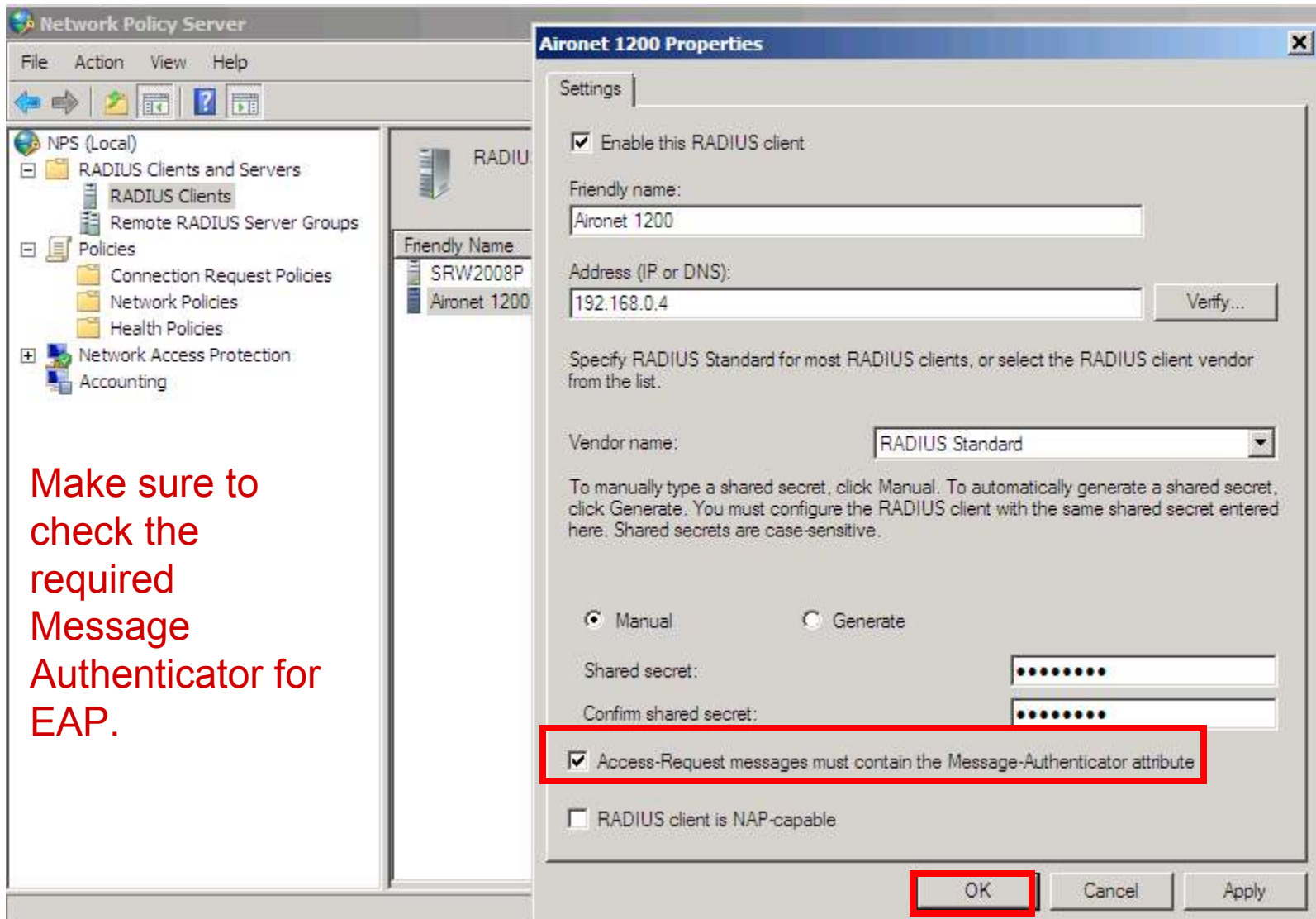
**Connection Request Policy:**  
WirelessPolicy

**Network Policies:**  
WirelessPolicy

[Configuration Details](#)

[Previous](#) [Next](#) **Finish** [Cancel](#)





The screenshot shows the Network Policy Server (NPS) console. On the left is a tree view with 'Policies' expanded to 'Connection Request Policies'. The main pane shows a table of policies:

Policy Name	Status	Processing Order	Source
WiredPolicy	Enabled	1	Unspecified
WirelessPolicy	Enabled	2	Unspecified
Use Windows authentication for all users	Enabled	3	Unspecified

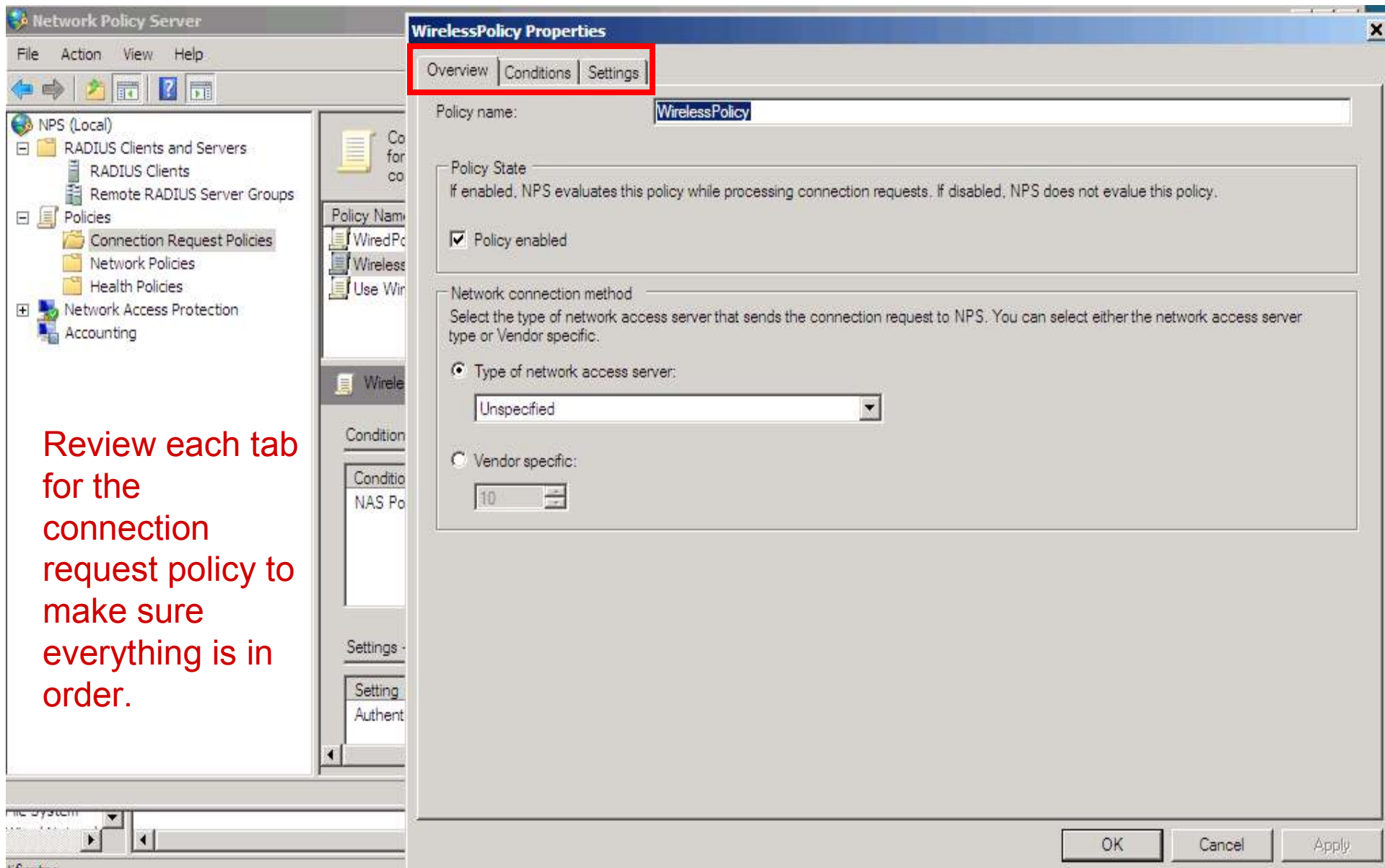
The 'WirelessPolicy' row is selected and highlighted in blue, and a red box is drawn around the entire table. Below the table, the configuration for 'WirelessPolicy' is shown, including a condition table:

Condition	Value
NAS Port Type	Wireless - Other OR Wireless - IEEE 802.11

And a settings table:

Setting	Value
Authentication Provider	Local Computer

On the right, the 'Actions' pane is open to 'WirelessPolicy', with 'Move Up' and 'Move Down' buttons highlighted in red. A red text box on the left contains the instruction: 'Make sure to "Move Up" the policies as shown'.



Review each tab for the connection request policy to make sure everything is in order.

The screenshot shows the Network Policy Server console with the 'WirelessPolicy Properties' dialog box open. The 'Settings' tab is highlighted with a red box. The dialog box contains a table of conditions and a description of the selected condition.

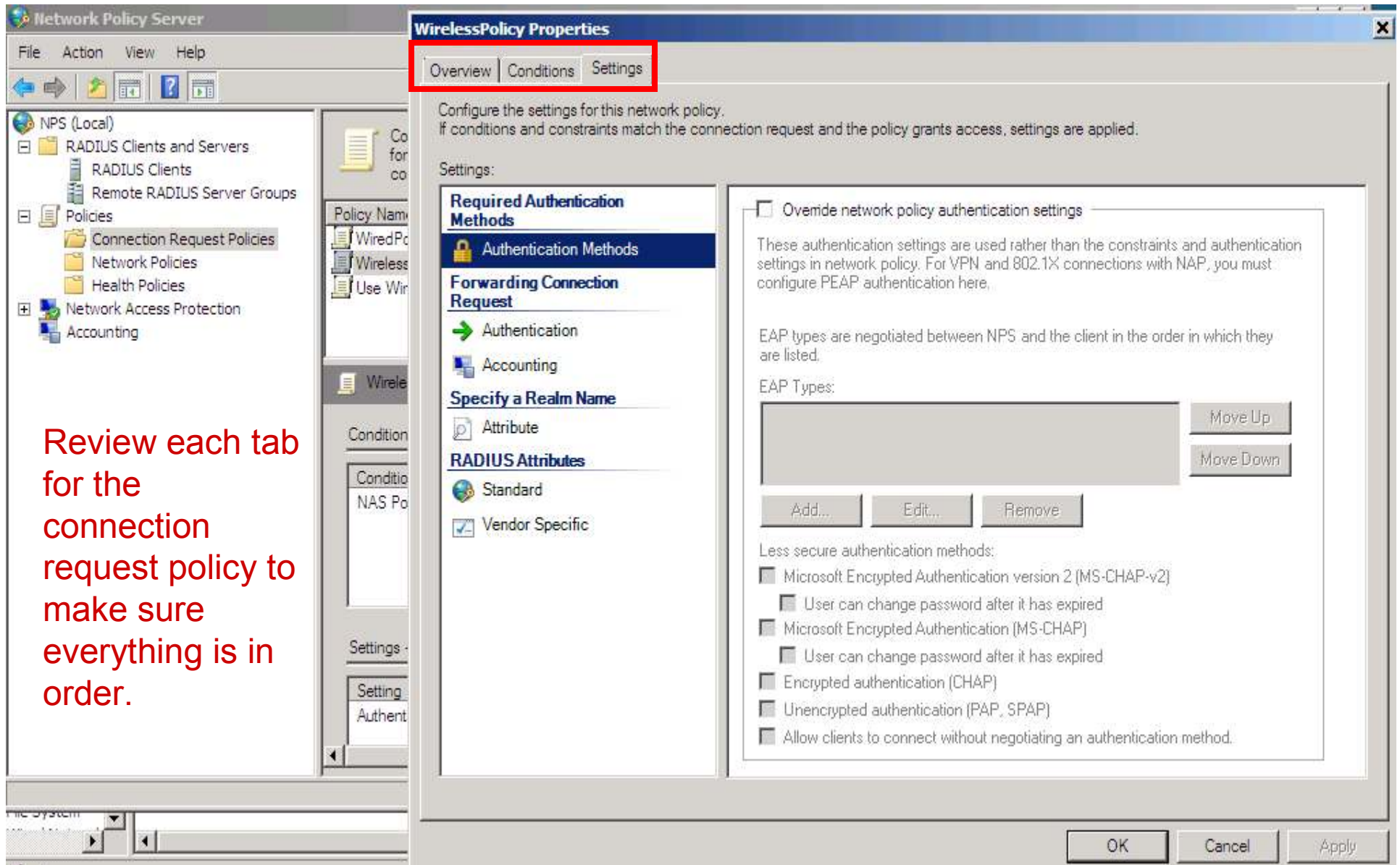
**Review each tab for the connection request policy to make sure everything is in order.**

Condition	Value
NAS Port Type	Wireless - Other OR Wireless - IEEE 802.11

Condition description:  
The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.

Buttons: Add... Edit... Remove





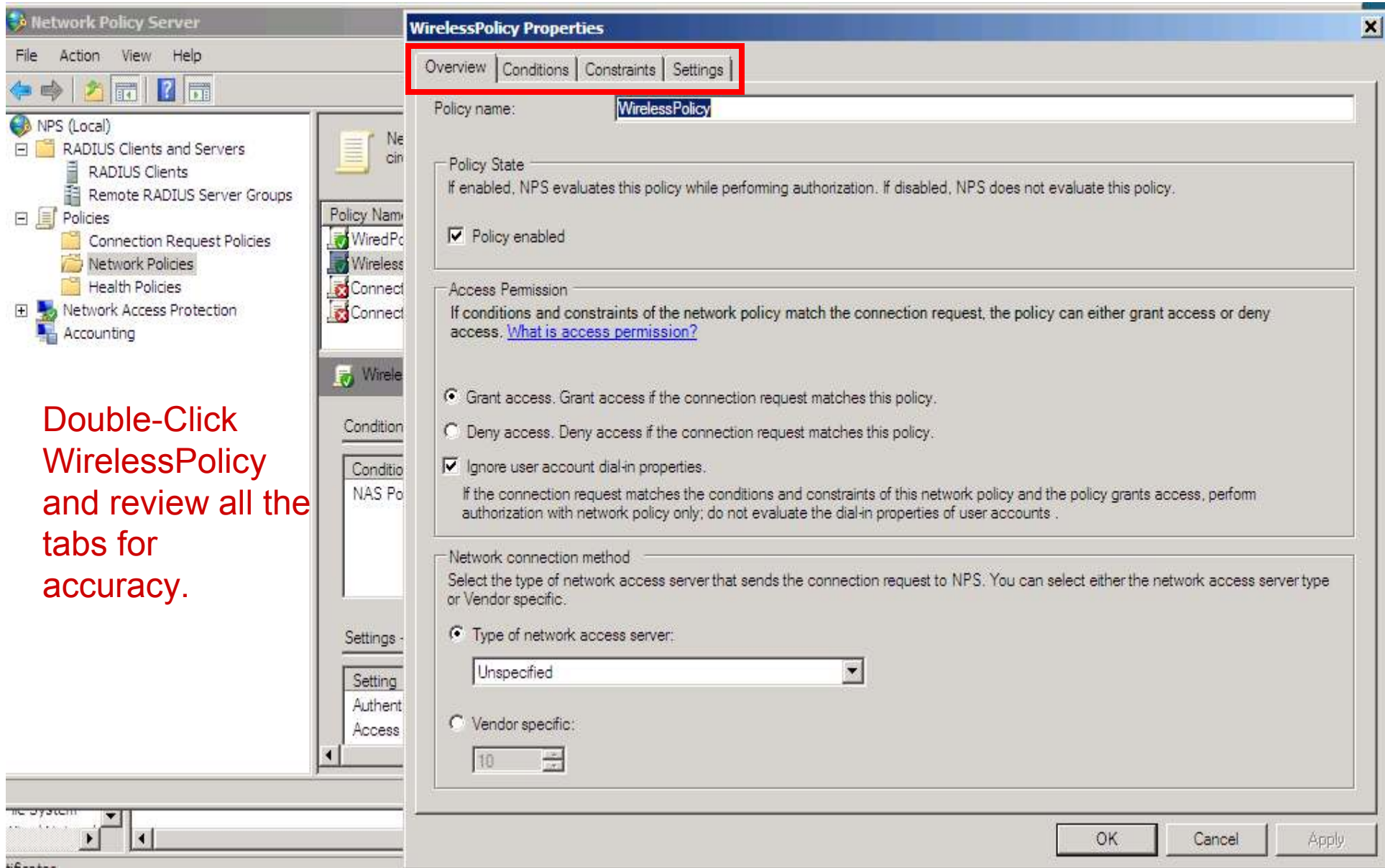
Review each tab for the connection request policy to make sure everything is in order.

The screenshot shows the Network Policy Server console. In the left-hand tree view, the 'Network Policies' folder is expanded. The 'WirelessPolicy' is selected in the main pane. A table below the title bar lists the policies:

Policy Name	Status	Processing Order	Access Type
WiredPolicy	Enabled	1	Grant Access
Connections to Microsoft Routing and Remote Access server	Enabled	2	Deny Access
Connections to other access servers	Enabled	3	Deny Access
WirelessPolicy	Enabled	4	Grant Access

The 'WirelessPolicy' row is highlighted in blue. Below the table, the 'WirelessPolicy' details are shown, including conditions and settings. The 'Conditions' section shows a single condition: 'NAS Port Type' with the value 'Wireless - Other OR Wireless - IEEE 802.11'. The 'Settings' section shows 'Authentication Method' as 'EAP OR MS-CHAP v1 OR MS-CHAP v1 (User can change p...)' and 'Access Permission' as 'Grant Access'. On the right-hand side, the 'Actions' pane is open, and the 'Move Up' and 'Move Down' options are highlighted with a red box.

Under “Network Policies” “Move Up” the WirelessPolicy as required.



Double-Click  
WirelessPolicy  
and review all the  
tabs for  
accuracy.

Network Policy Server

File Action View Help

Overview Conditions Constraints Settings

Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

Condition	Value
NAS Port Type	Wireless - Other OR Wireless - IEEE 802.11

**By not specifying any conditions we are allowing all domain authenticated connections here**

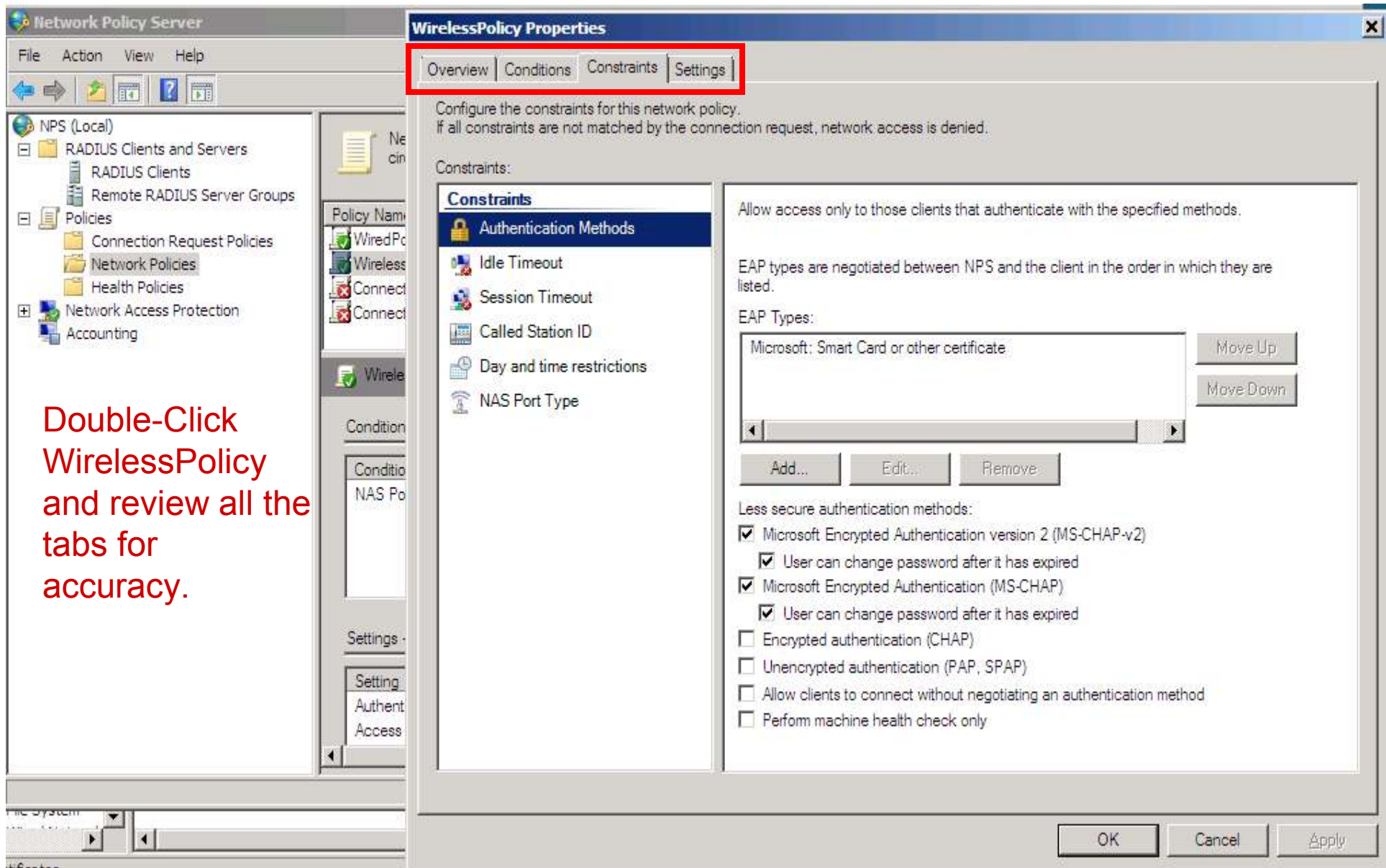
Condition description:  
The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.

Add... Edit... Remove

OK Cancel Apply

Double-Click  
WirelessPolicy  
and review all the  
tabs for  
accuracy.





Double-Click  
WirelessPolicy  
and review all the  
tabs for  
accuracy.

**Select additional protocols and the right certificate as shown**

**WirelessPolicy Properties**

Overview | Conditions | **Constraints** | Settings

Configure the constraints for this network policy.  
If all constraints are not matched by the connection request, network access is denied.

Constraints:

- Authentication Methods
  - Idle Timeout
  - Session Timeout
  - Called Station ID
  - Day and time restrictions
  - NAS Port Type

Allow access only to those clients that authenticate with the specified methods.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

- Microsoft: Smart Card or other certificate
- Microsoft: Protected EAP (PEAP)

Buttons: Move Up, Move Down, Add..., Edit..., Remove

**Smart Card or other Certificate Properties**

This server identifies itself to callers before the connection is completed. Select the certificate that you want it to use as proof of identity.

Certificate issued to: WMSvc-WIN2008AD

Friendly name: WMSvc-WIN2008AD  
WIN2008AD.vprodemo.com  
**Win2008AD.vprodemo.com**

Issuer: WMSvc-WIN2008AD

Expiration date: 3/17/2019 9:12:17 AM

Buttons: OK, Cancel

Network Policy Server

File Action View Help

Overview | Conditions | Constraints | **Settings**

Configure the settings for this network policy.  
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

**RADIUS Attributes**

- Standard
- Vendor Specific

**Network Access Protection**

- NAP Enforcement
- Extended State

**Routing and Remote Access**

- Multilink and Bandwidth Allocation Protocol (BAP)
- IP Filters
- Encryption
- IP Settings

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

Add... Edit... Remove

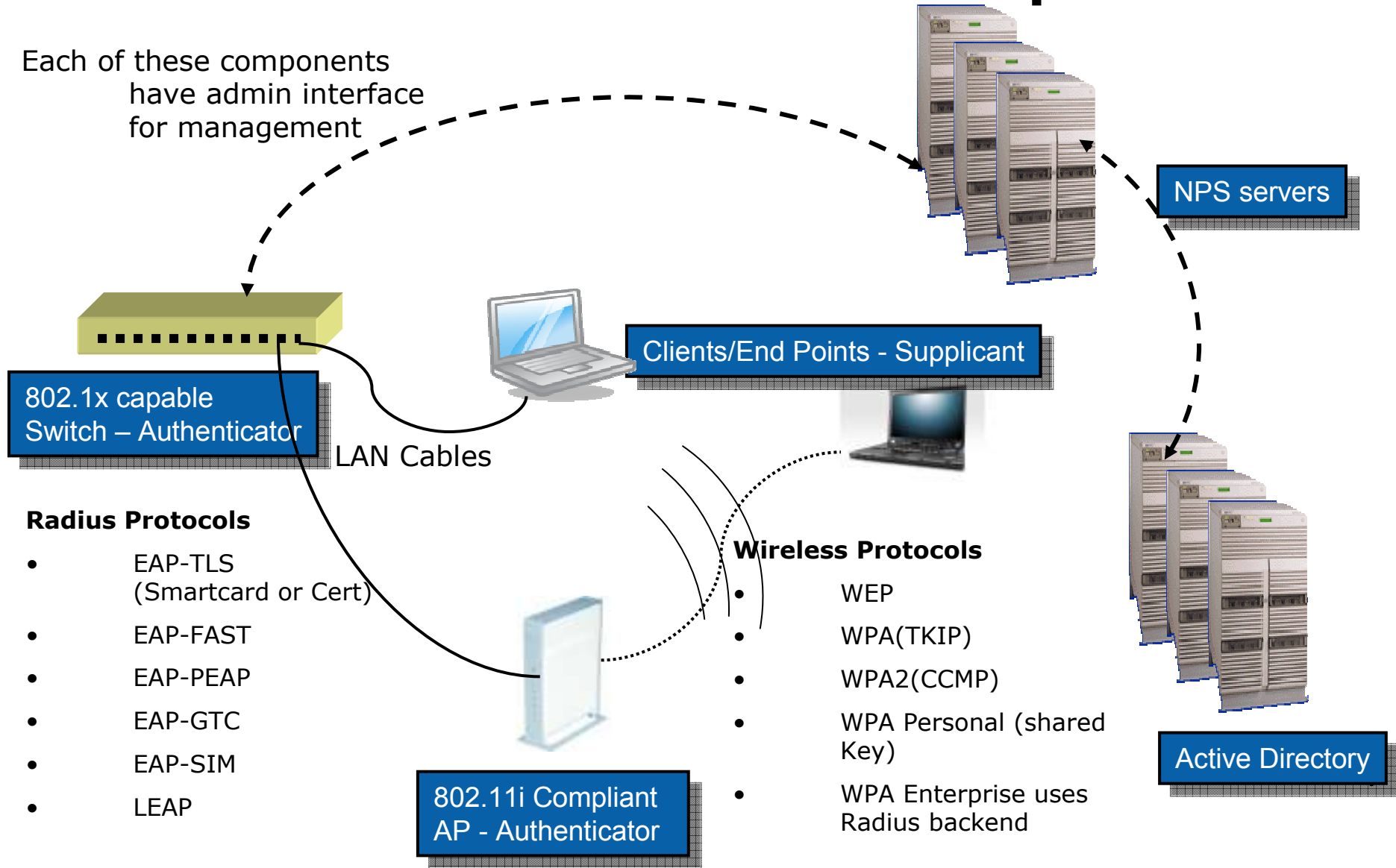
OK Cancel Apply

Finished review of both Wired & Wireless AAA clients policies.

Ready for testing client authentication with this NPS configured as our Radius.

# Review 802.1x Architectural Components

Each of these components have admin interface for management





# 802.1x Architectural Components

- Before Proceeding Remember to use the web interface for your wired & wireless AAA clients and correspondingly bind them with the NPS Radius with the same shared secret.
  - We used “password1234” without quotes for this document.
- Choose a windows client for testing. We chose a Win 7 client for our testing.
- Make sure your wired switch is configured with some “Open” ports and some “Secure” ports although it is not necessary.
  - Having this way you can validate connectivity on an open port if you experience problems with 802.1x configuration.

home - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://192.168.0.5/home.htm> Go Links Google Search Sign In

**Security** Setup Port Management VLAN Management Statistics ACL **Security** QoS Spanning Tree Multicast SNMP Admin LogOut

ACL Binding **RADIUS** TACACS+ 802.1x Settings Port Security Multiple Hosts More...>>

**RADIUS Parameters**

IP Address: 192.168.0.2

Priority: 0

Authentication Port: 1812

Number of Retries: 3

Timeout for Reply: 3 (Sec)

Dead Time: 0 (Min)

Key String: password1234 (Alpha Numeric)

Source IP Address: 192.168.0.5

Usage Type: All

Update

IP Address	Priority	Authentic- ation Port	Number of Retries	Timeout for Reply	Dead Time	Source IP Address	Usage Type
192.168.0.2	0	1812	3	3	0	192.168.0.5	All

**RADIUS**

Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks. RADIUS servers provide a centralized authentication method for web access.

The RADIUS screen contains the following fields:

- IP Address — The Authentication Server IP addresses.
- Priority — The server priority. The possible values are 0-65535, where 0 is the highest value. The RADIUS Server priority is used to configure the server query order.
- Authentication Port — Identifies the authentication port. The authentication port is used to verify the RADIUS server authentication. The authenticated port default is 1812.
- Number of Retries — Defines the number of transmitted requests sent to RADIUS server before a failure occurs. The possible field values are 1 - 10. Three is the default value.
- Timeout for Reply — Defines the amount of the time in seconds the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server. The possible field values are 1 - 30. Three is the default value.
- Dead Time — Defines the amount of time (minutes) that a RADIUS

Wired AAA Client 192.168.0.5 web interface for configuring Radius Secret

The screenshot displays the Cisco IOS Series AP Security Server Manager web interface. The browser window title is "Cisco IOS Series AP - Security - Server Manager - Microsoft Internet Explorer". The address bar shows the URL "http://192.168.0.4/ap\_sec\_network-security\_a.shtml". The left sidebar contains a navigation menu with "SECURITY" and "Server Manager" highlighted. The main content area is divided into several sections:

- Backup RADIUS Server:** Contains fields for "Backup RADIUS Server:" (Hostname or IP Address) and "Shared Secret:". Buttons for "Apply", "Delete", and "Cancel" are present.
- Corporate Servers:** Contains a "Current Server List" section with a dropdown menu set to "RADIUS". A list of servers is shown, with "192.168.0.2" selected. A "Delete" button is below the list. To the right of the list are fields for "Server:" (192.168.0.2), "Shared Secret:" (masked with dots), "Authentication Port (optional):" (1645), and "Accounting Port (optional):" (1646). Buttons for "Apply" and "Cancel" are at the bottom right.
- Default Server Priorities:** Contains three columns: "EAP Authentication", "MAC Authentication", and "Accounting". The "EAP Authentication" column has Priority 1 set to "192.168.0.2", Priority 2 set to "< NONE >", and Priority 3 set to "< NONE >". The "MAC Authentication" and "Accounting" columns have Priority 1, 2, and 3 all set to "< NONE >".

Wireless AAA Client 192.168.0.4 web interface for configuring Radius Secret

# Client Configuration

Right Click on Local Area Connection Adapter properties, click on Authentication tab. (see next slide)

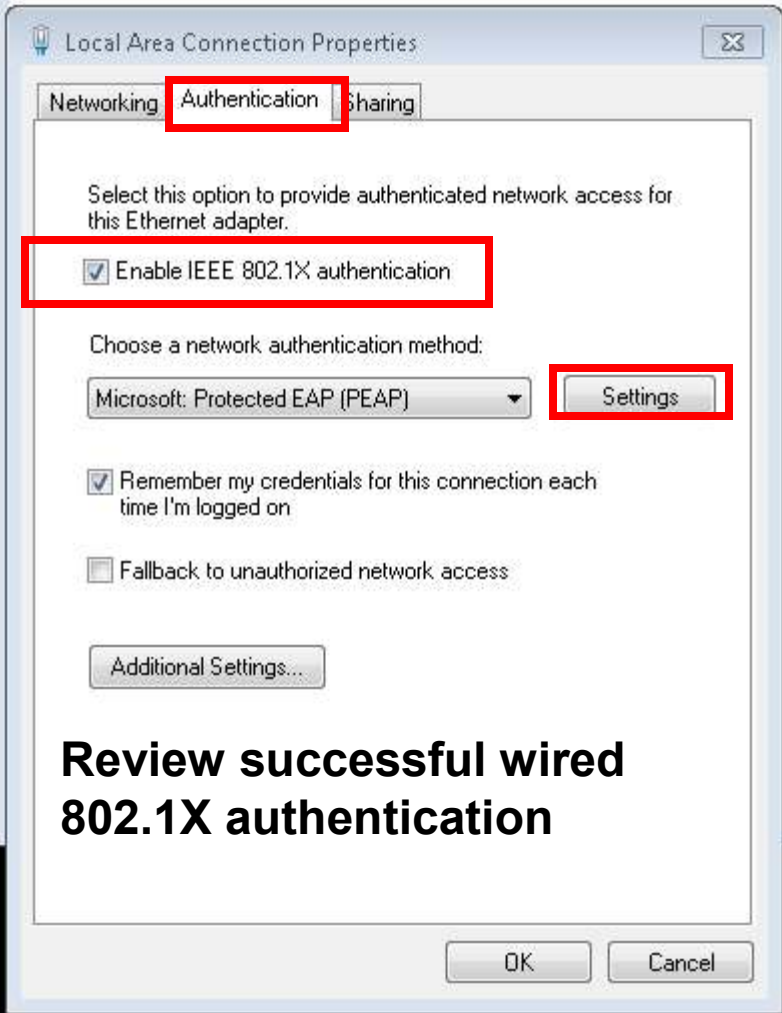
Make sure “wired autoconfig” or “wireless autoconfig” service is running if this tab is not visible.

Check “Enable IEEE 802.1X authentication”.

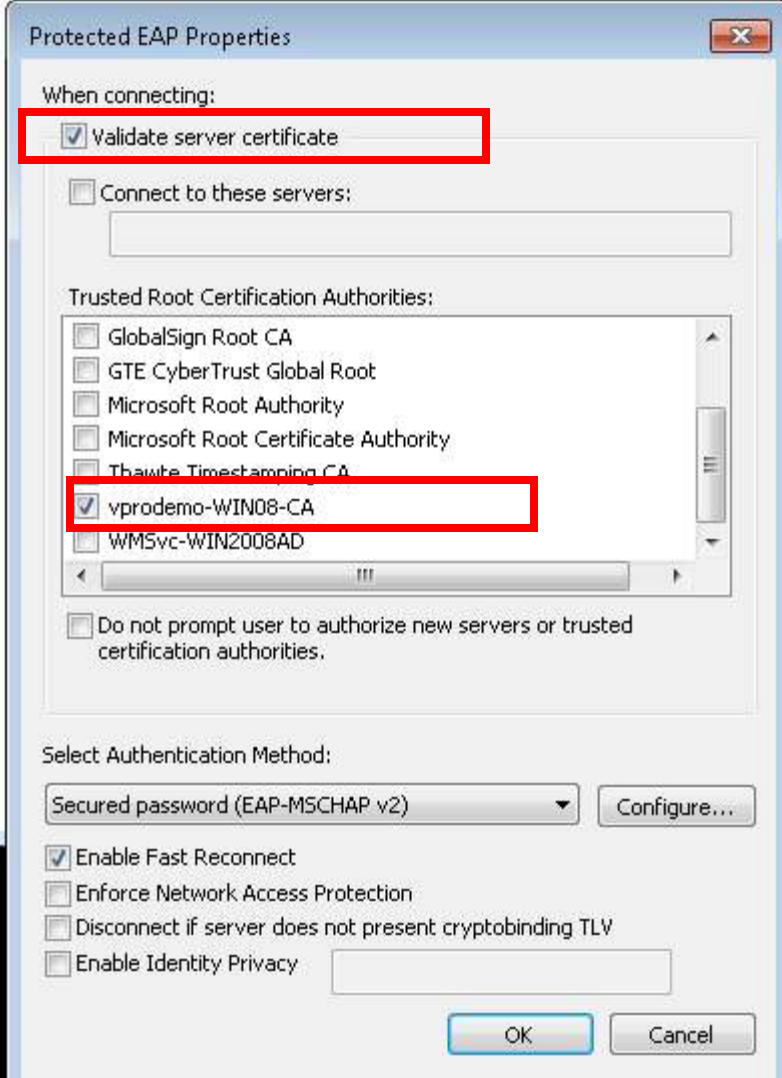
Click OK.

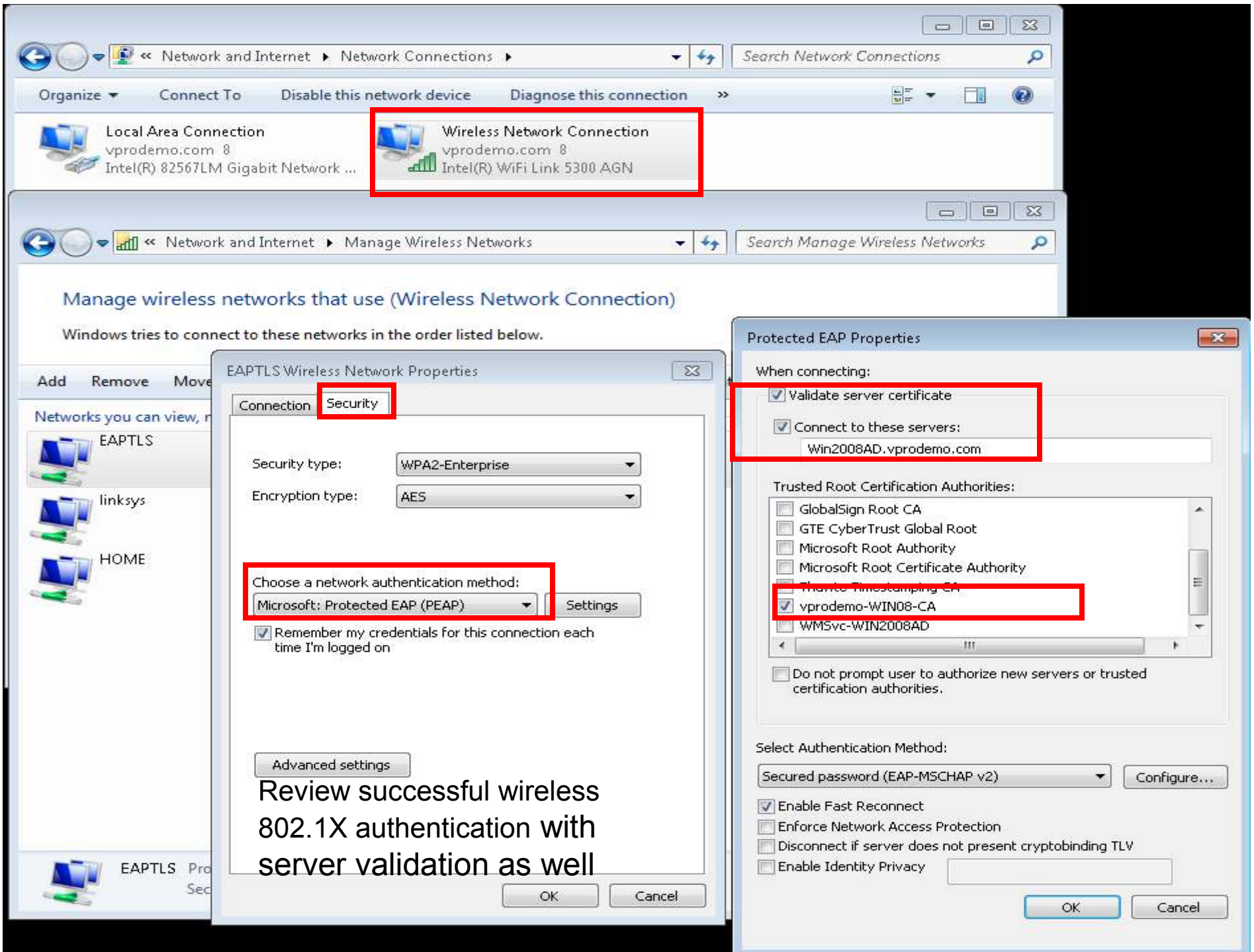
Disconnect the client from an “Open” port on your wired 802.1X enabled switch and connect to “Secure” port on the same switch.





## Review successful wired 802.1X authentication





# Review NPS Logs

- Review wired and wireless authentication logs for your client using EAP-PEAP protocol with vprodemo\administrator username and password in the next two slides.
- We will note down the IP numbers for both wired and wireless and logoff to make sure the computer account can successfully log into the 802.1X network as well.
- Note that all these client side settings can be pushed through GPOs (out of scope here).

Event Properties - Event 6278, Microsoft Windows security auditing.

General Details

Friendly View  XML View

```

+ System
- EventData
  SubjectUserSid      S-1-5-21-3304531836-3184696238-1123404646-500
  SubjectUserName     VPRODEMO\Administrator
  SubjectDomainName   VPRODEMO
  FullyQualifiedSubjectUserName VPRODEMO\Administrator
  SubjectMachineSID   S-1-0-0
  SubjectMachineName  -
  FullyQualifiedSubjectMachineName -
  MachineInventory    -
  CalledStationID     -
  CallingStationID    -
  NASIPv4Address       192.168.0.5
  NASIPv6Address       -
  NASIdentifier        -
  NASPortType         Ethernet
  NASPort              7
  ClientName           SRW2008P
  ClientIPAddress      192.168.0.5
  ProxyPolicyName      WiredPolicy
  NetworkPolicyName    WiredPolicy
  AuthenticationProvider Windows
  AuthenticationServer Win2008AD.vprodemo.com
  AuthenticationType   PEAP
  EAPType              Microsoft: Secured password (EAP-MSCHAP v2)
  AccountSessionIdentifier -
  QuarantineState      Full Access
  ExtendedQuarantineState -
  QuarantineSessionID  -
  QuarantineHelpURL    -
  QuarantineSystemHealthResult -

```

Copy Close

Action View Help

Online Responder: WIN2008AD

Enterprise PKI

Certificate Templates (Win2008)

vprodemo-WIN08-CA

- Revoked Certificates
- Issued Certificates
- Pending Requests
- Failed Requests
- Certificate Templates

Active Directory Domain Services

DHCP Server

DNS Server

File Services

Network Policy and Access Services

Web Server (IIS)

Internet Information Services (IIS)

Features

Diagnostics

Event Viewer

- Custom Views
- Administrative Events
  - Server Roles
    - Active Directory Certificate Services
    - Active Directory Domain Services
    - DHCP Server
    - DNS Server
    - File Server
    - Network Policy and Access Services
    - Web Server

Windows Logs

Applications and Services Logs

Subscriptions

Reliability and Performance

Device Manager

Configuration

Storage

Network Policy and Access Services

631 Events

Level	Date and Time
Information	10/26/2008
Information	10/26/2008
Information	10/26/2008
Information	10/26/2008
Information	10/26/2008
Information	10/26/2008
Information	10/26/2008
Information	10/26/2008
Information	10/26/2008
Information	10/26/2008

Event 6278, Microsoft Windows security auditing.

General Details

Network Policy Server group

User:

Security ID:

Account Name:

Account Domain:

Fully Qualified Account Name:

Log Name: Security

Source: Microsoft Windows

Event ID: 6278

Level: Information

User: N/A

OpCode: Info

More Information: [Event Viewer](#)



Server Manager

File Action View Help

Network Policy and Access Services 631 Events

631 Events

Level	Date and Time
Information	10/26/2009 8:37:12 PM
Information	10/26/2009 8:37:12 PM
Information	10/26/2009 8:36:29 PM
Information	10/26/2009 8:36:29 PM
Information	10/26/2009 8:36:02 PM
Information	10/26/2009 8:36:02 PM
Information	10/26/2009 8:29:21 PM
Information	10/26/2009 8:29:21 PM
Information	10/26/2009 8:26:25 PM

Event 6272, Microsoft Windows security audit

General Details

Network Policy Server granted access to a

User:

Security ID:  
Account Name:  
Account Domain:  
Fully Qualified Account Name:

Log Name: Security  
Source: Microsoft Windows s  
Event ID: 6272  
Level: Information  
User: N/A  
OpCode: Info  
More Information: [Event Log Online Hel](#)

Event Properties - Event 6272, Microsoft Windows security auditing.

General Details

Friendly View XML View

System

EventData

SubjectUserSid S-1-5-21-3304531836-3184696238-1123404646-500  
SubjectUserName VPRODEMO\Administrator  
SubjectDomainName VPRODEMO  
FullyQualifiedSubjectUserName VPRODEMO\Administrator  
SubjectMachineSID S-1-0-0  
SubjectMachineName -  
FullyQualifiedSubjectMachineName -  
MachineInventory -  
CalledStationID 0019.aa15.2bc0  
CallingStationID 0021.6a0c.8460  
NASIPv4Address 192.168.0.4  
NASIPv6Address -  
NASIdentifier sraps  
NASPortType Wireless - IEEE 802.11  
NASPort 260  
ClientName Aironet 1200  
ClientIPAddress 192.168.0.4  
ProxyPolicyName WirelessPolicy  
NetworkPolicyName WirelessPolicy  
AuthenticationProvider Windows  
AuthenticationServer Win2008AD.vprodemo.com  
AuthenticationType PEAP  
EAPType Microsoft: Secured password (EAP-MSCHAP v2)  
AccountSessionIdentifier -  
QuarantineState Full Access  
QuarantineSessionIdentifier -

Copy Close

Notice the IP address of the wired and wireless configuration here.

Ping/t from your server.

Cold boot and watch if the 802.1X secure connection with the computer account is authenticated instead of domain user account

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7100]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\administrator.UPRODEMO.001>ipconfig/all

Windows IP Configuration

Host Name . . . . . : e6400
Primary Dns Suffix . . . . . : vprodemo.com
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : vprodemo.com

Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix . : vprodemo.com
Description . . . . . : Intel(R) WiFi Link 5300 AGN
Physical Address. . . . . : 00-21-6A-0C-84-60
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::8dd1-76e1-7528-b950%12 (Preferred)
IPv4 Address. . . . . : 192.168.0.112 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, October 26, 2009 10:32:59 PM
Lease Expires . . . . . : Sunday, November 01, 2009 10:33:04 PM
Default Gateway . . . . . : 192.168.0.200
DHCP Server . . . . . : 192.168.0.2
DHCPv6 IAID . . . . . : 218112362
DHCPv6 Client DUID. . . . . : 00-01-00-01-11-9C-B3-8B-00-21-70-D3-31-F2

DNS Servers . . . . . : 192.168.0.2
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : vprodemo.com
Description . . . . . : Intel(R) 82567LM Gigabit Network Connection
Physical Address. . . . . : 00-21-70-D3-31-F2
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::e17b-72e5-1d13-94dd%11 (Preferred)
IPv4 Address. . . . . : 192.168.0.100 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, October 26, 2009 10:33:04 PM
Lease Expires . . . . . : Sunday, November 01, 2009 10:33:04 PM
Default Gateway . . . . . : 192.168.0.200
DHCP Server . . . . . : 192.168.0.2
DHCPv6 IAID . . . . . : 234889584
DHCPv6 Client DUID. . . . . : 00-01-00-01-11-9C-B3-8B-00-21-70-D3-31-F2
```

Notice both the IPs would ping even if the computer comes from cold boot.

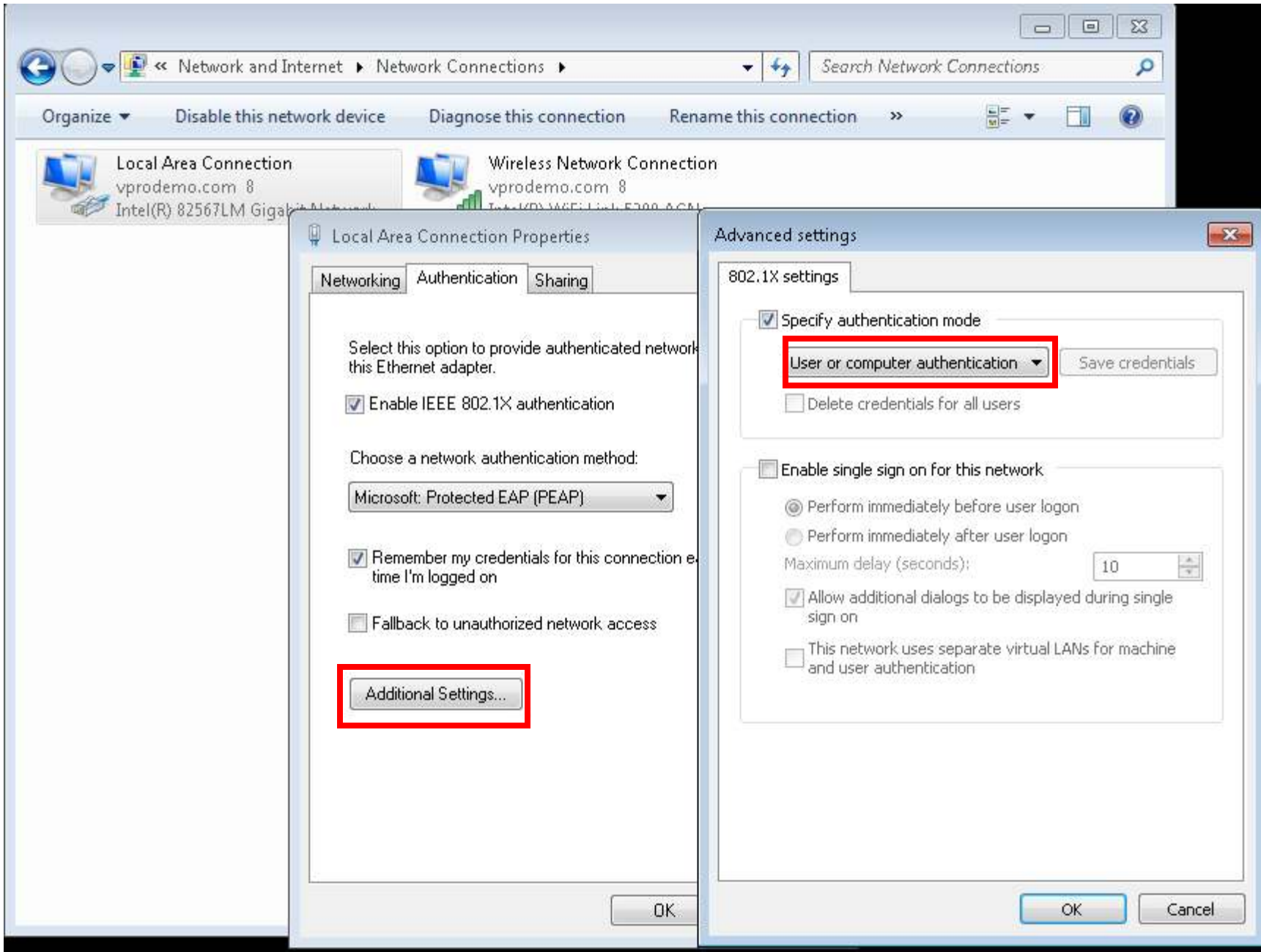
We will review the client side settings responsible for the “computer/machine” authentication.

We already saw these settings on the NPS by allowing “Domain Users” as well as “Domain Computers” under the Network Policy.

```
Administrator: C:\Windows\system32\cmd.exe - ping /t 192.168.0.112
Reply from 192.168.0.100: bytes=32 time<1ms TTL=128
Reply from 192.168.0.100: bytes=32 time<1ms TTL=128
Reply from 192.168.0.100: bytes=32 time<1ms TTL=128
Reply from 192.168.0.100: bytes=32 time<1ms TTL=128
Reply from 192.168.0.100: bytes=32 time<1ms TTL=128
Reply from 192.168.0.100: bytes=32 time=1ms TTL=128
Reply from 192.168.0.100: bytes=32 time<1ms TTL=128
Reply from 192.168.0.100: bytes=32 time<1ms TTL=128
Reply from 192.168.0.100: bytes=32 time<1ms TTL=128
Reply from 192.168.0.100: bytes=32 time<1ms TTL=128
Reply from 192.168.0.100: bytes=32 time<1ms TTL=128
Reply from 192.168.0.100: bytes=32 time<1ms TTL=128
Reply from 192.168.0.100: bytes=32 time=86ms TTL=128
Reply from 192.168.0.100: bytes=32 time<1ms TTL=128
Reply from 192.168.0.100: bytes=32 time<1ms TTL=128
Reply from 192.168.0.100: bytes=32 time<1ms TTL=128
Reply from 192.168.0.100: bytes=32 time<1ms TTL=128
Reply from 192.168.0.100: bytes=32 time<1ms TTL=128
Reply from 192.168.0.100: bytes=32 time<1ms TTL=128
Reply from 192.168.0.100: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.100:
    Packets: Sent = 64, Received = 64, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 86ms, Average = 1ms
Control-C
^C
C:\Users\Administrator>ping/t 192.168.0.112

Pinging 192.168.0.112 with 32 bytes of data:
Reply from 192.168.0.112: bytes=32 time=4ms TTL=128
Reply from 192.168.0.112: bytes=32 time=1ms TTL=128
Reply from 192.168.0.112: bytes=32 time=1ms TTL=128
Reply from 192.168.0.112: bytes=32 time=1ms TTL=128
Reply from 192.168.0.112: bytes=32 time=1ms TTL=128
Reply from 192.168.0.112: bytes=32 time=1ms TTL=128
Reply from 192.168.0.112: bytes=32 time=1ms TTL=128
Reply from 192.168.0.112: bytes=32 time=1ms TTL=128
Reply from 192.168.0.112: bytes=32 time=1ms TTL=128
Reply from 192.168.0.112: bytes=32 time=1ms TTL=128
Reply from 192.168.0.112: bytes=32 time=1ms TTL=128
Reply from 192.168.0.112: bytes=32 time=1ms TTL=128
Reply from 192.168.0.112: bytes=32 time=1ms TTL=128
Reply from 192.168.0.112: bytes=32 time=1ms TTL=128
Reply from 192.168.0.112: bytes=32 time=1ms TTL=128
```





# Summary

- We installed and configured NPS as a Radius for using a wired as well as wireless AAA clients.
- We tested the configuration with Win 7 client with both computer authentication as well as user authentication.
- Your vPro client can now be provisioned with a wired & wireless 802.1X profile and you can maintain secure network connectivity even when the client is completely shutdown.
- By having computer authentication you can wake up vPro client even wireless using AMT secure power-on command and patch the system without any user sign-on.
- For details on how to do this with Configuration Manger SP2 review my document
  - <http://communities.intel.com/docs/DOC-4206>
  - Although CISCO ACS server is detailed here this would work for NPS as well
- For details on how to do this with Configuration Manger SP1 review my document
  - <http://communities.intel.com/docs/DOC-3867>
  - Although IAS is described in detail here this would work with NPS as well with Intel Genscript used to push wireless scripts.