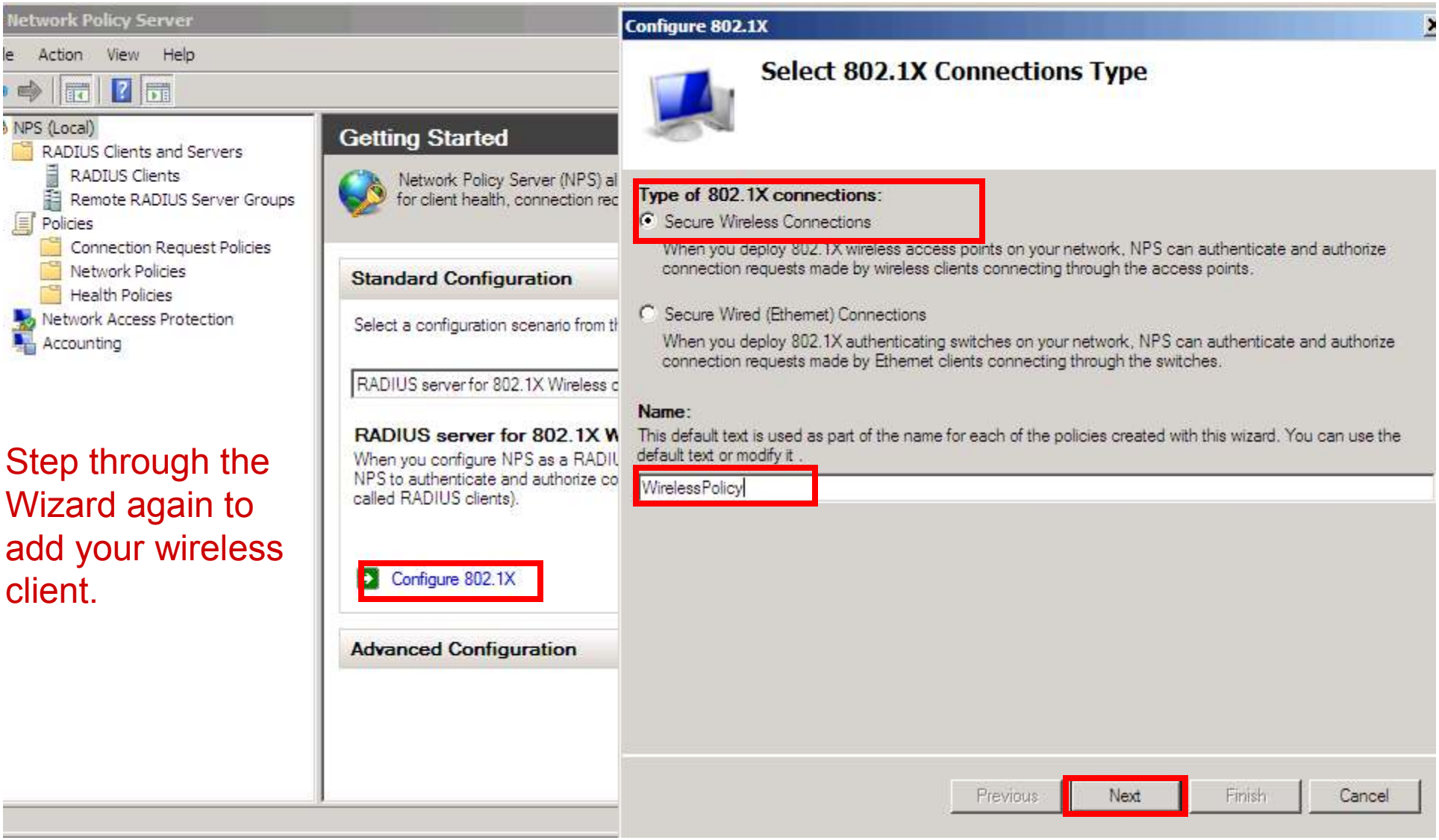
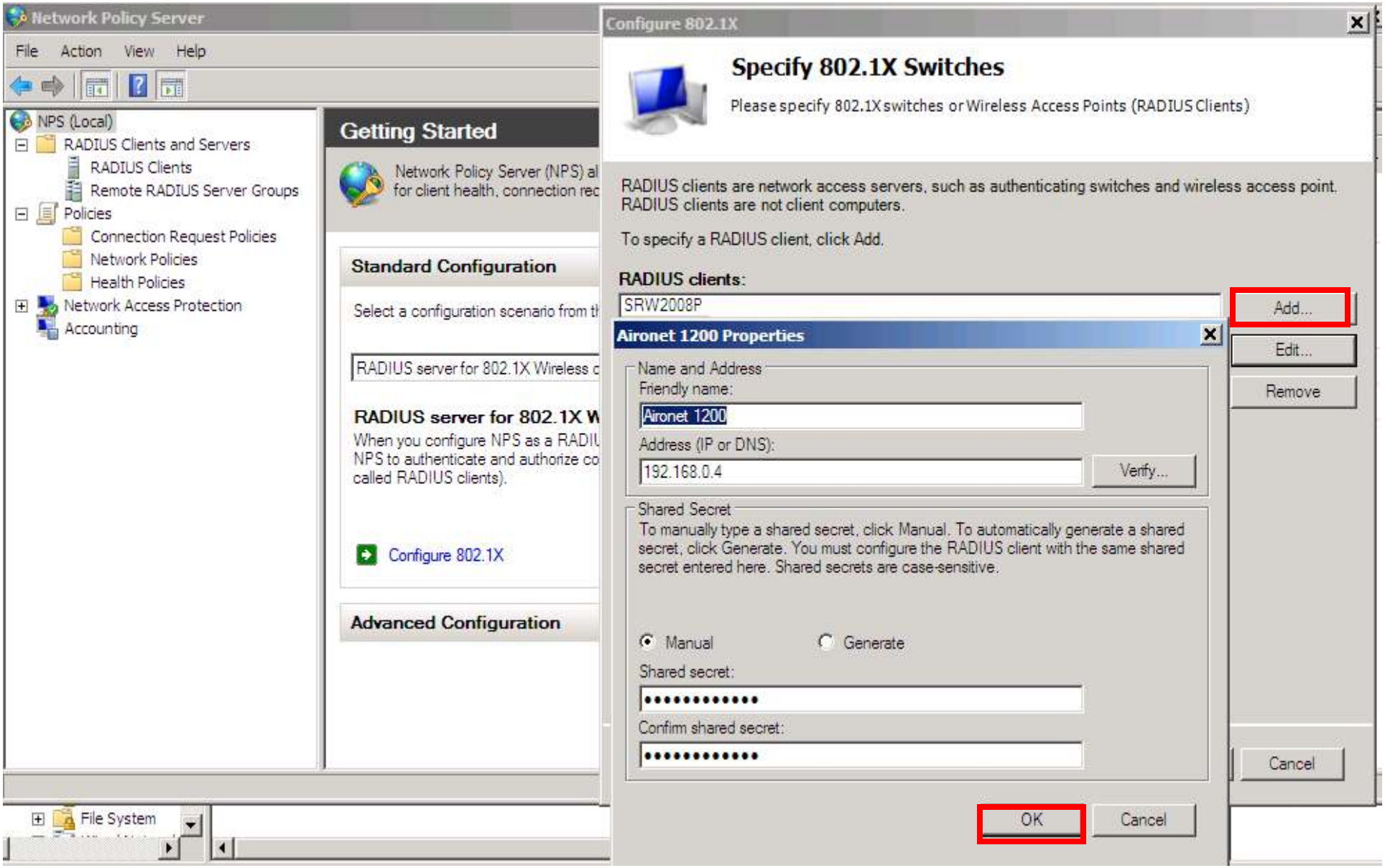
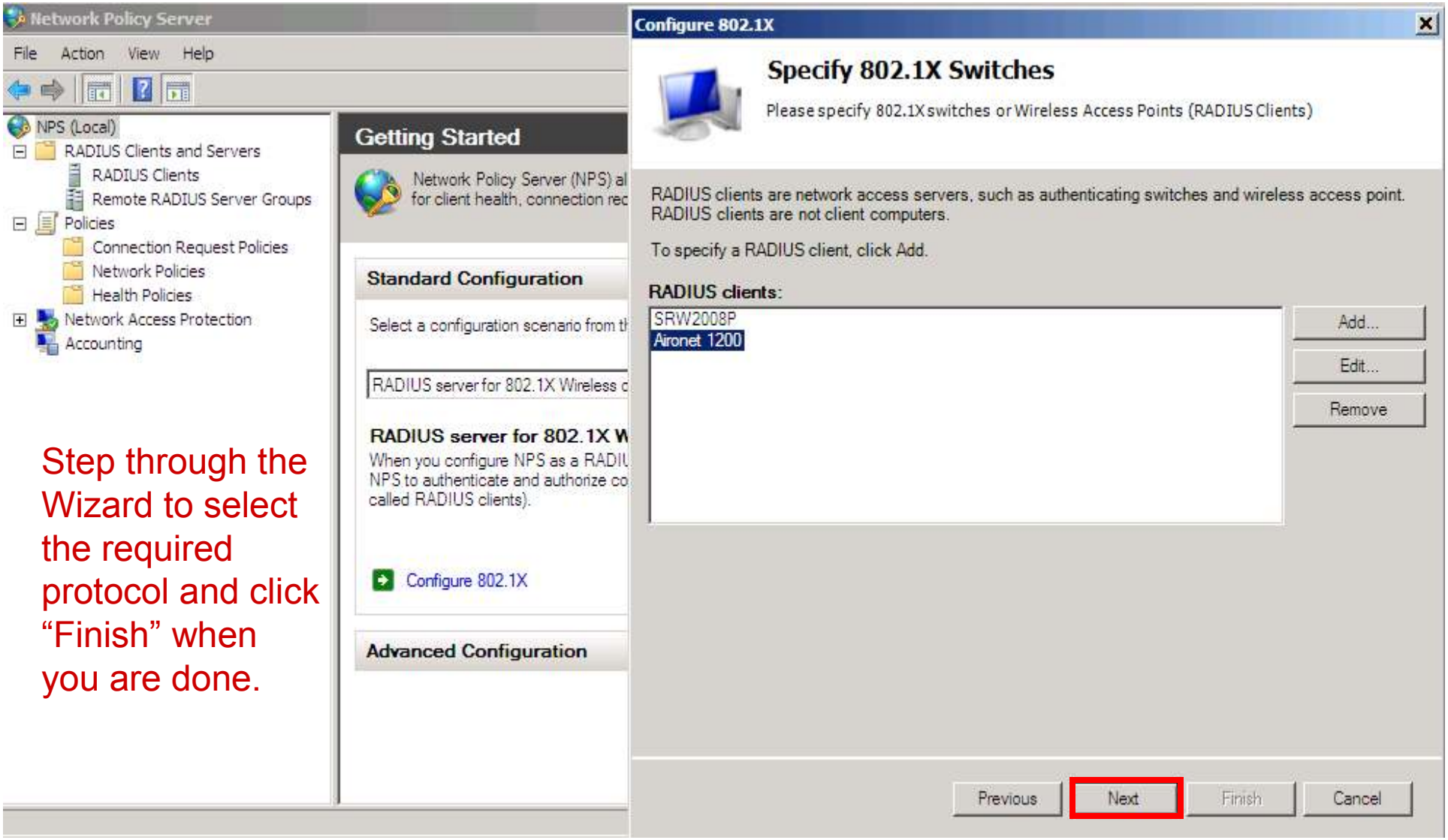


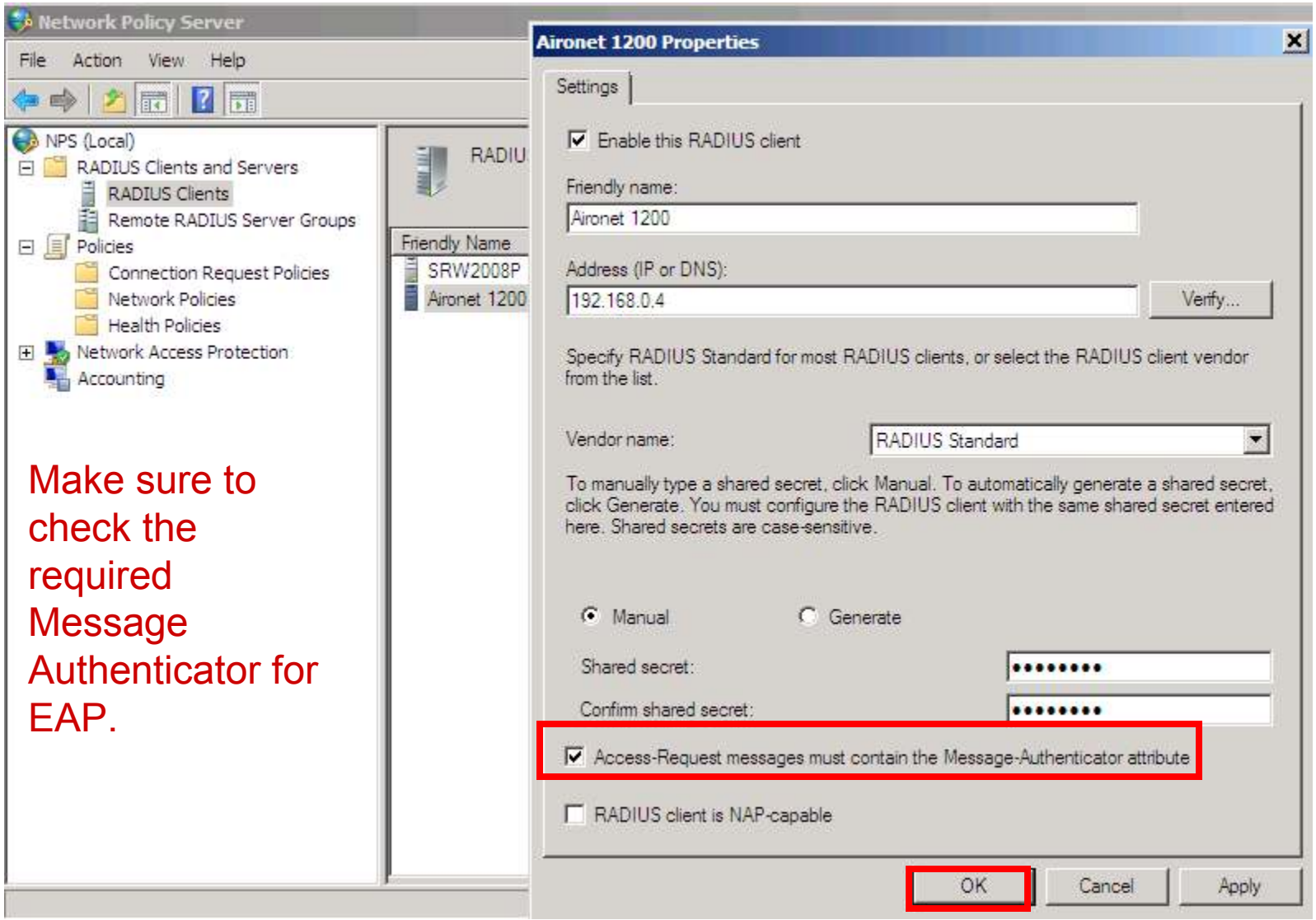
Step through the Wizard again to add your wireless client.


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) al
for client health, connection rec
Standard Configuration
Select a configuration scenario from th
RADIUS server for 802.1X Wireless c
RADIUS server for 802.1X W
When you configure NPS as a RADIU
NPS to authenticate and authorize co
called RADIUS clients).
Configure 802.1X
Advanced Configuration
File System
Configure 802.1X
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:
SRW2008P
Add...
Edit...
Remove
Aironet 1200 Properties
Name and Address
Friendly name:
Aironet 1200
Address (IP or DNS):
192.168.0.4
Verify...
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:
OK
Cancel
Cancel

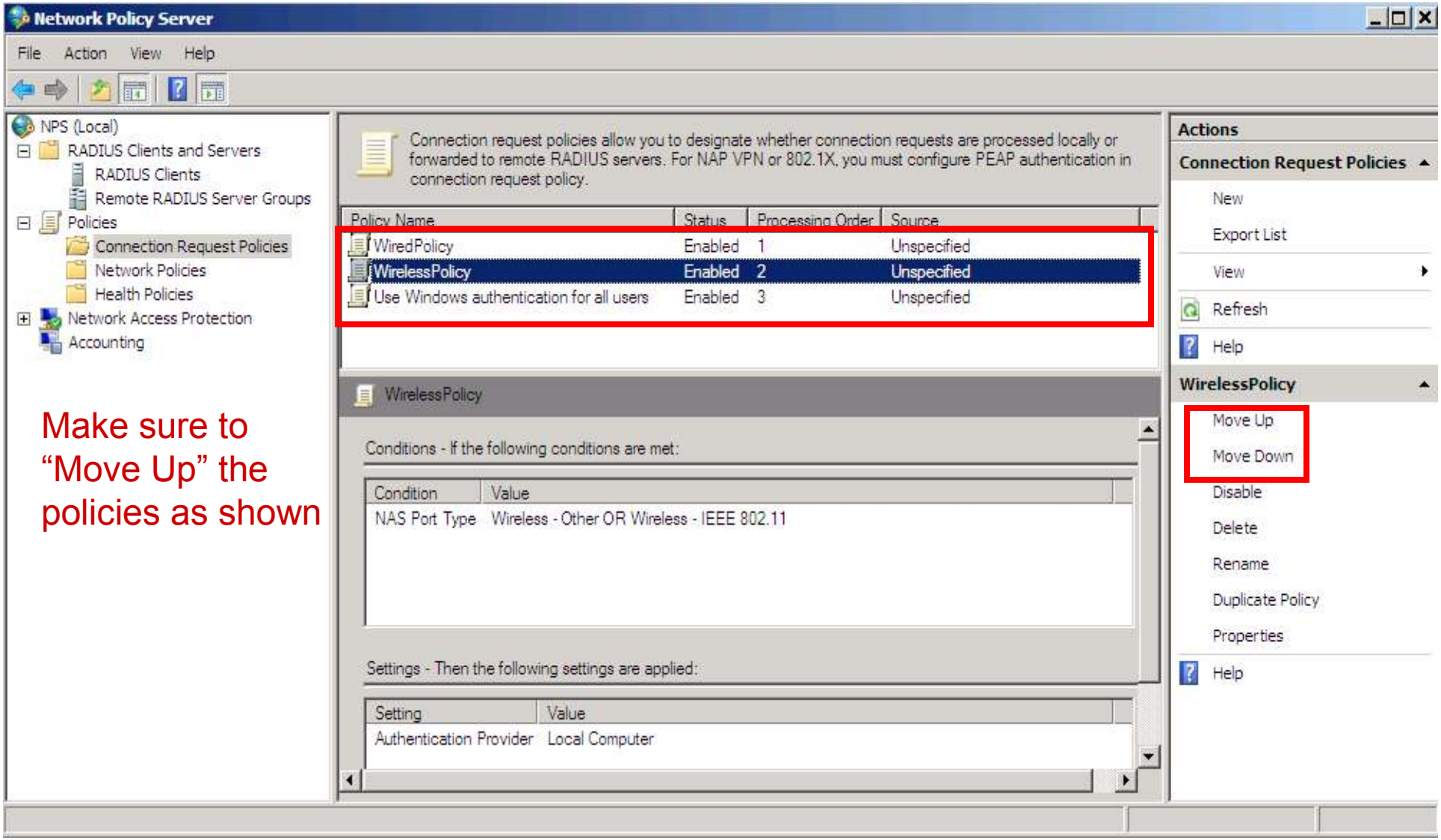


Step through the Wizard to select the required protocol and click “Finish” when you are done.

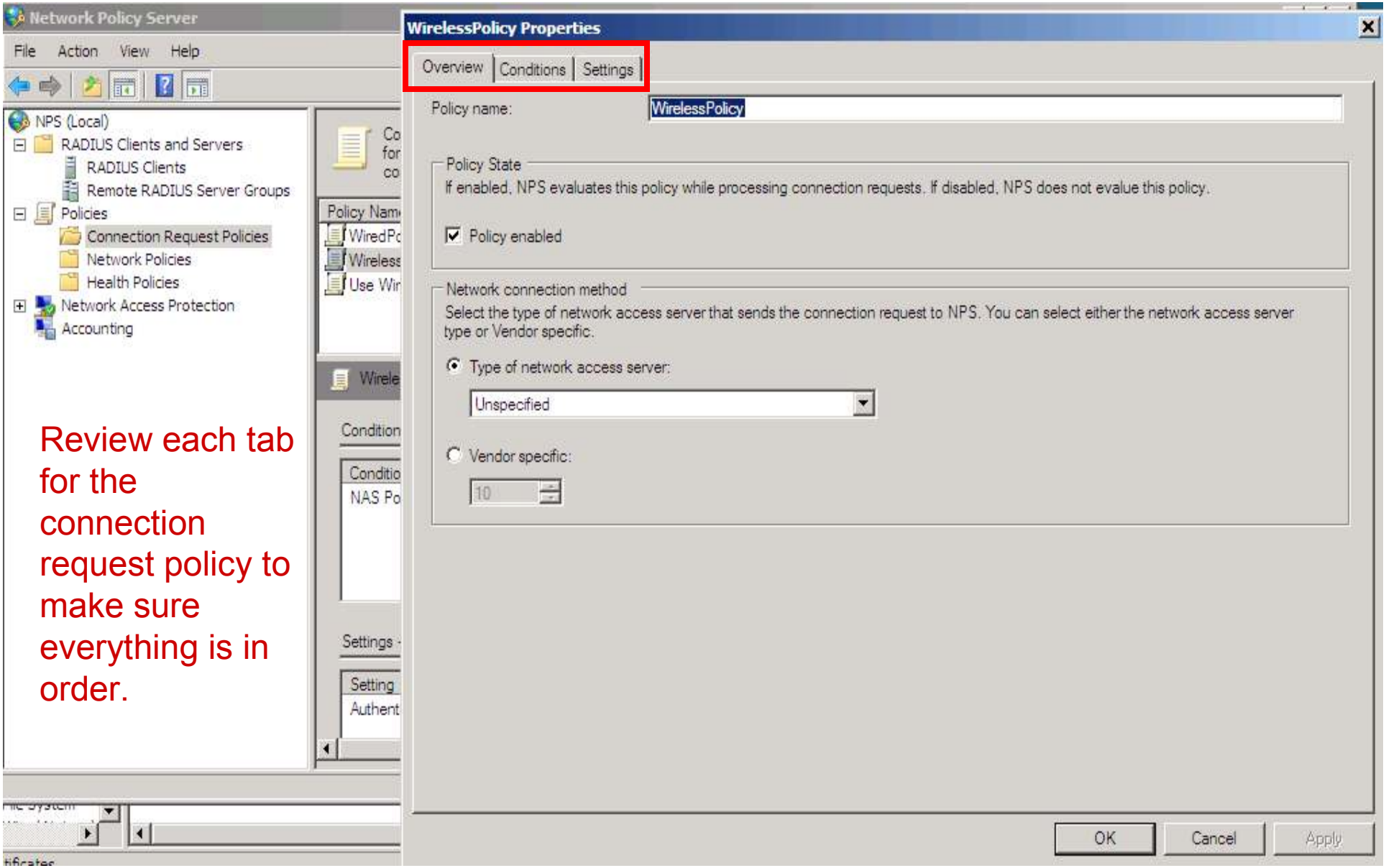

Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Getting Started
Network Policy Server (NPS) al
for client health, connection rec
Standard Configuration
Select a configuration scenario from th
RADIUS server for 802.1X Wireless c
RADIUS server for 802.1X W
When you configure NPS as a RADIU
NPS to authenticate and authorize co
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



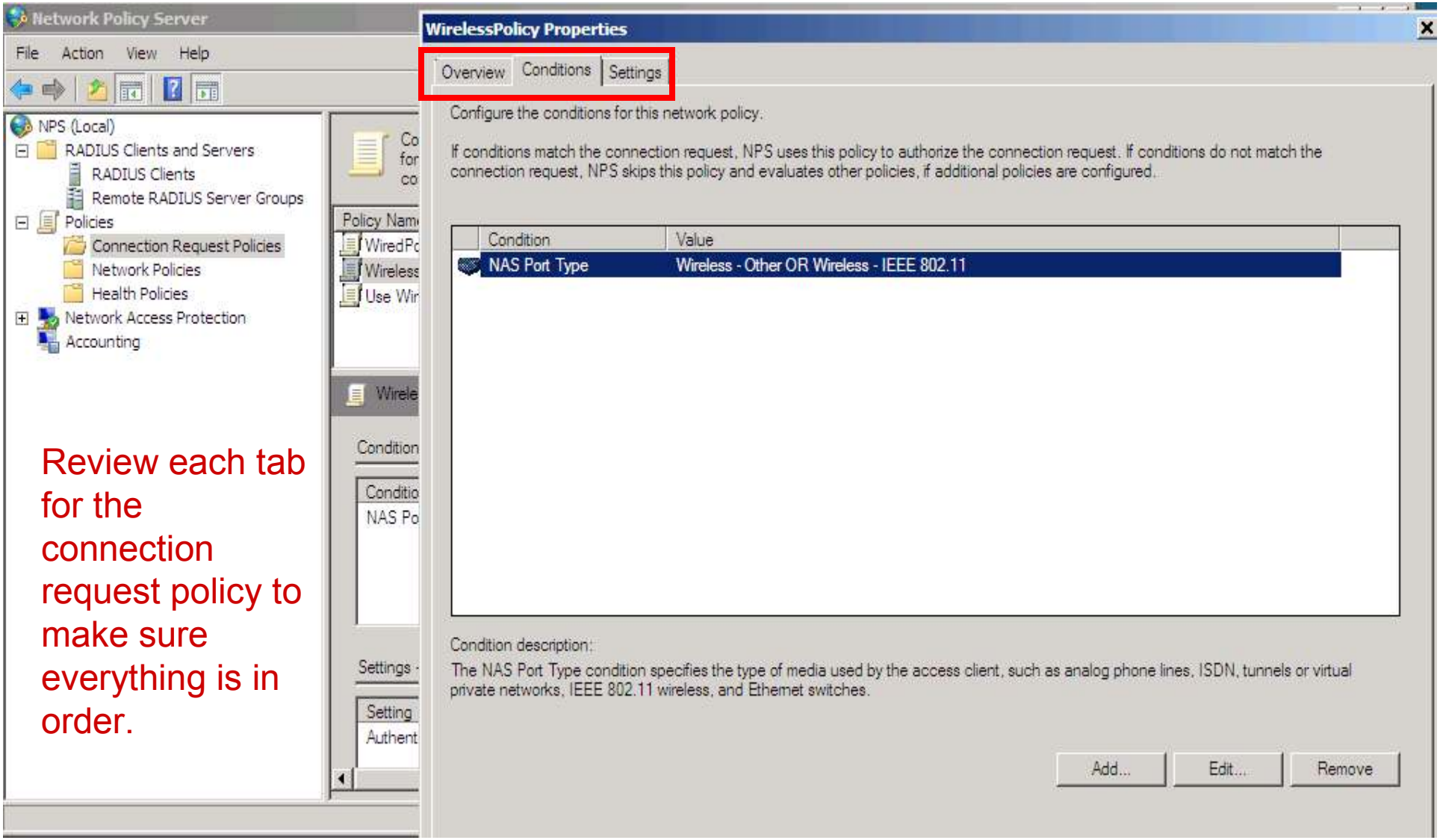
Make sure to check the required Message Authenticator for EAP.



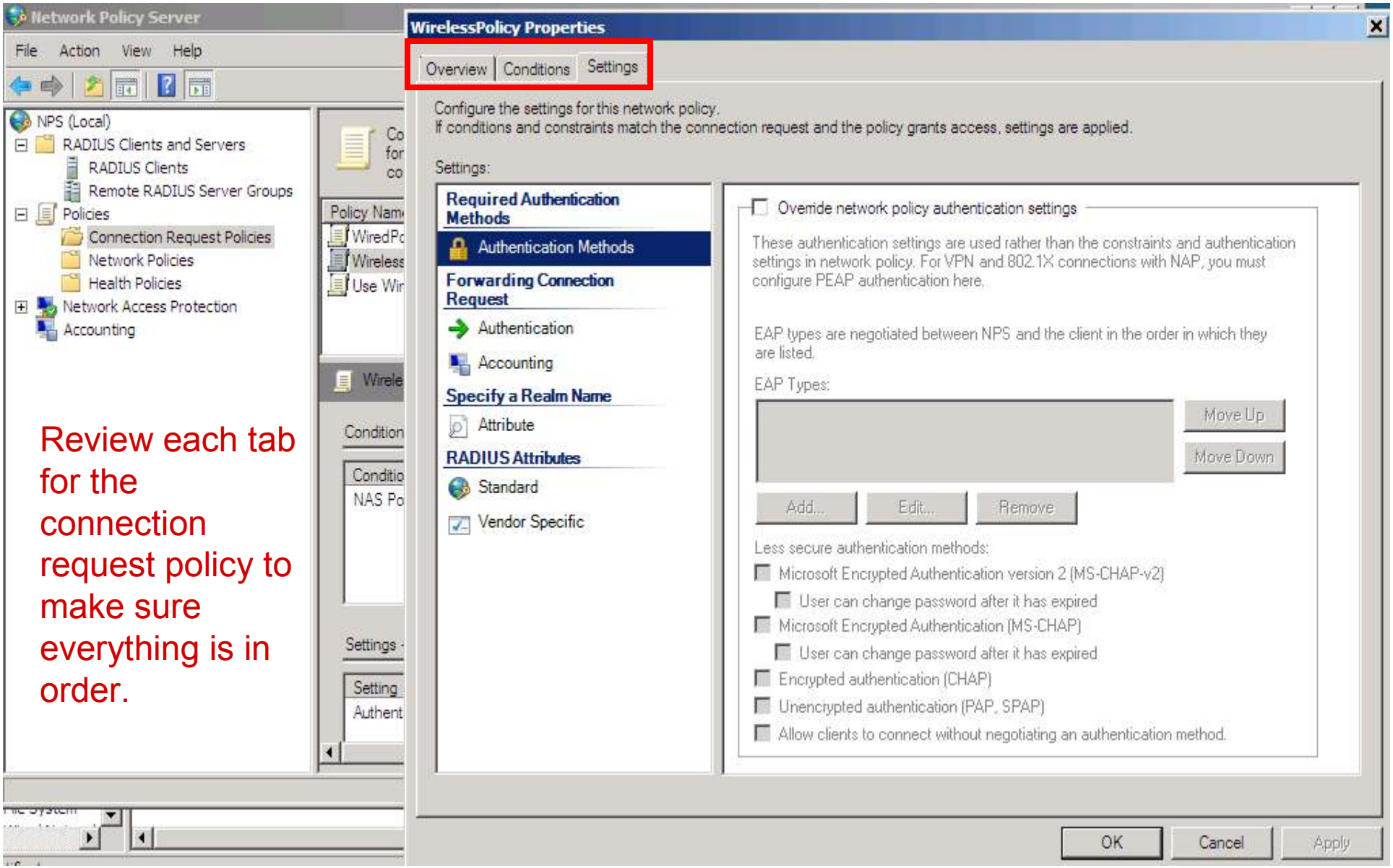
Make sure to "Move Up" the policies as shown



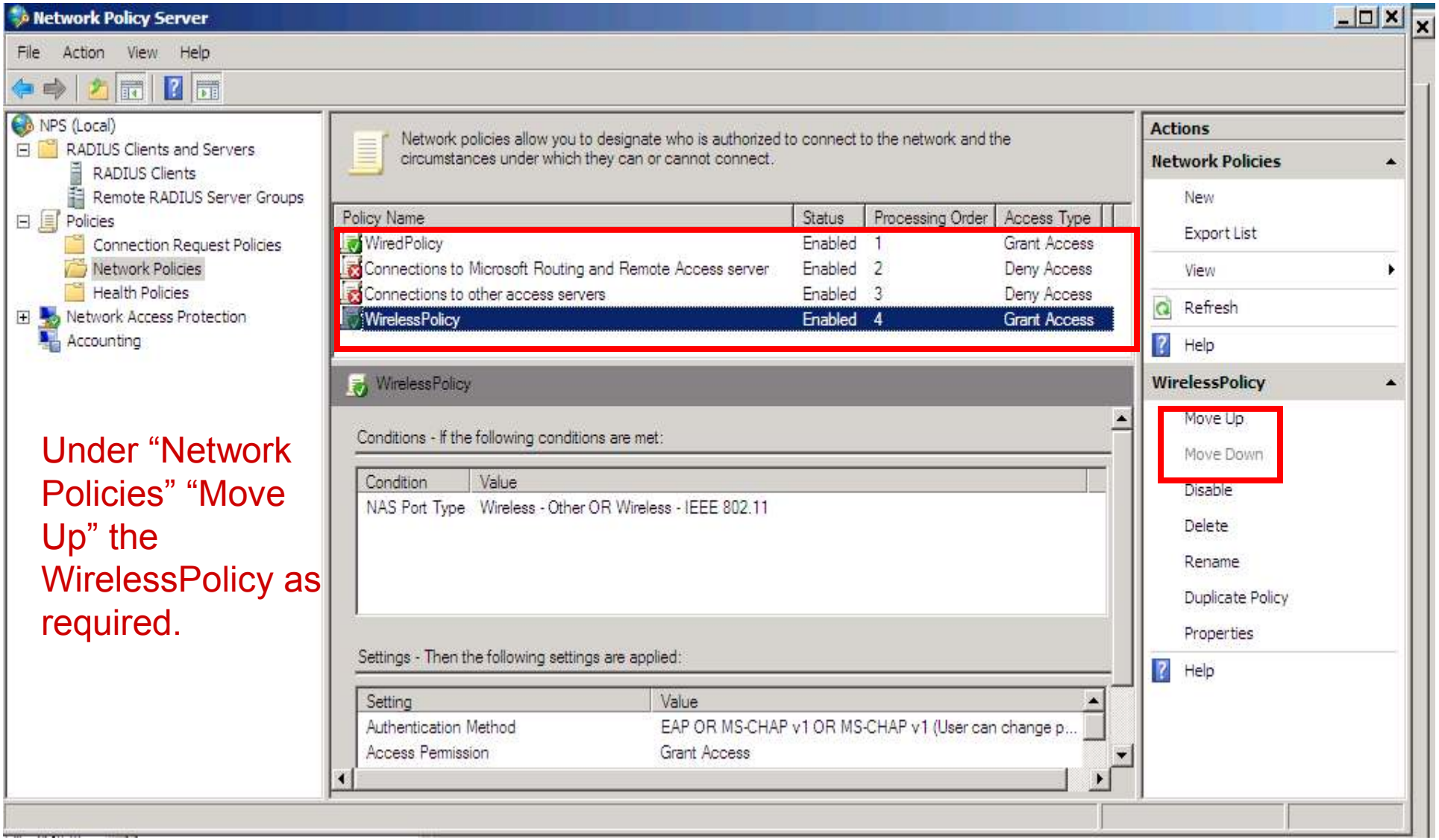
Review each tab for the connection request policy to make sure everything is in order.



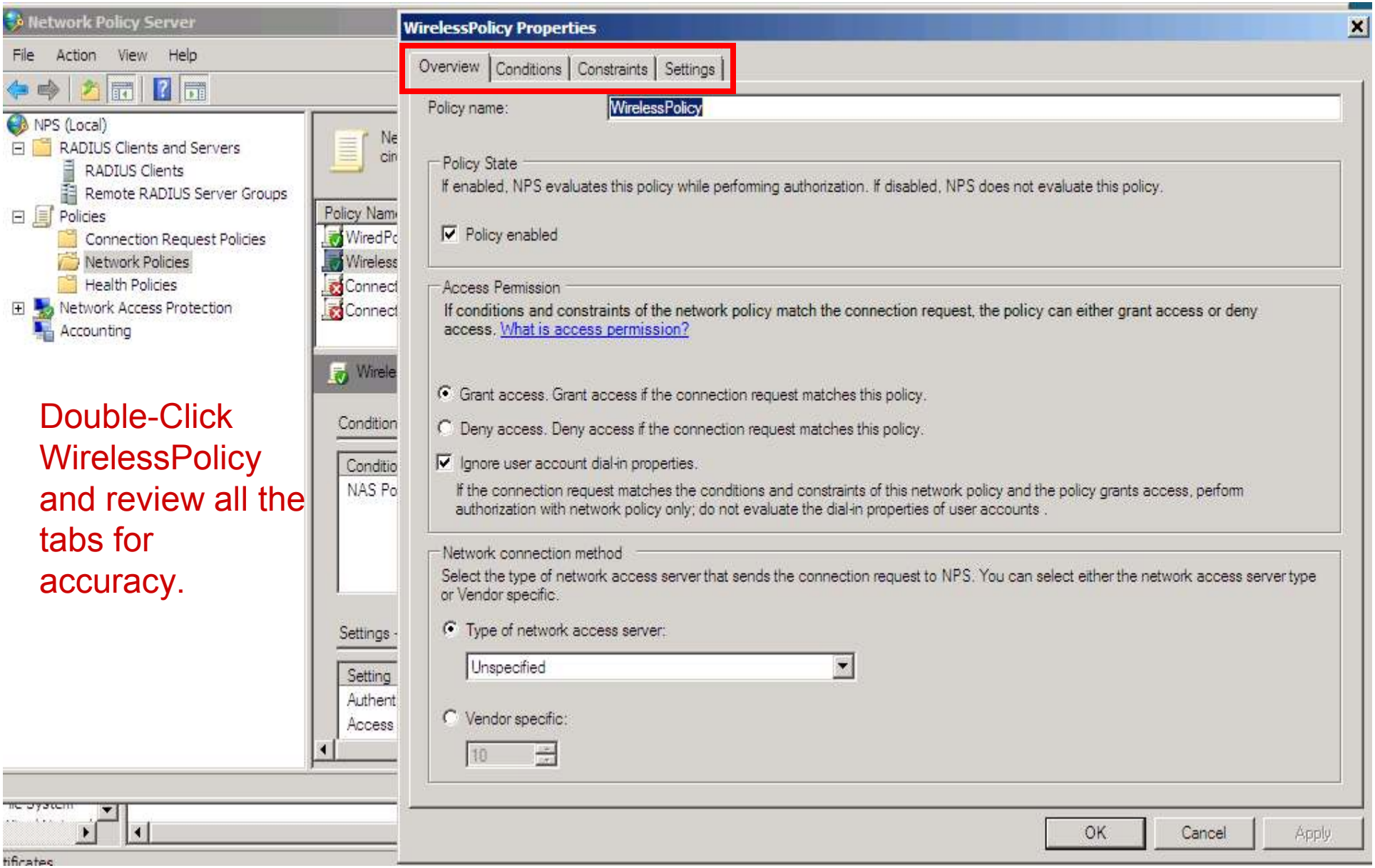
Review each tab for the connection request policy to make sure everything is in order.



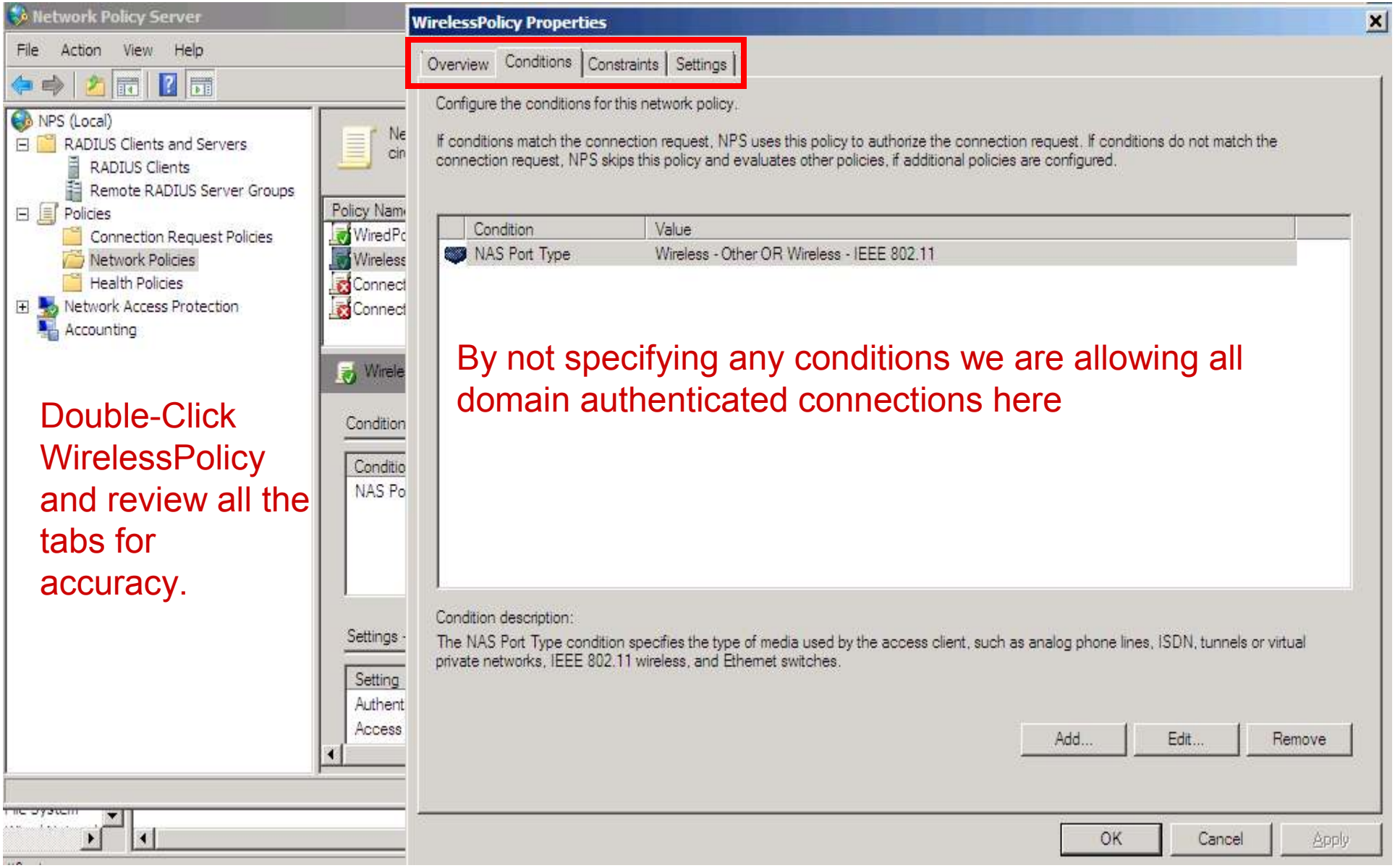
Review each tab for the connection request policy to make sure everything is in order.

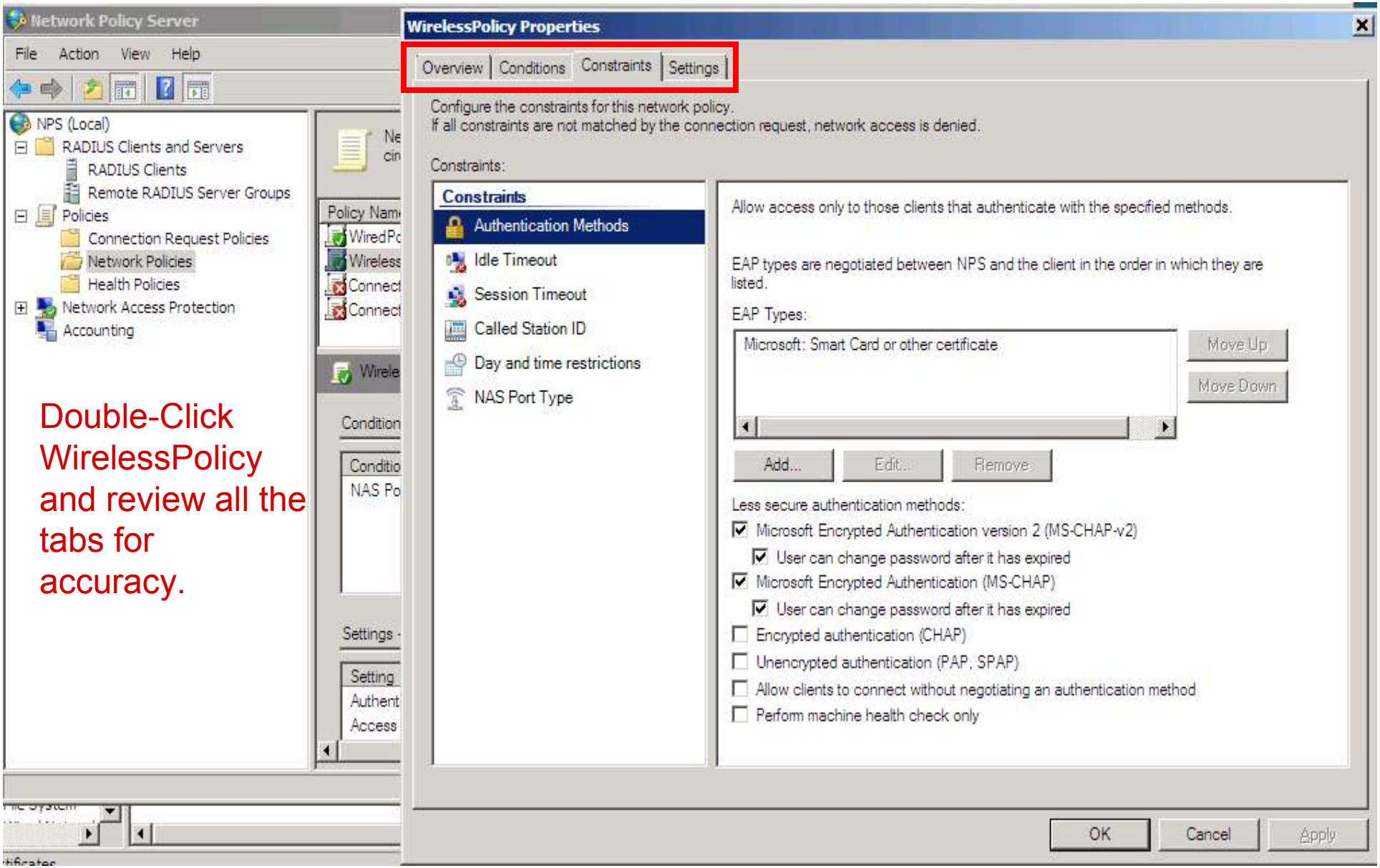


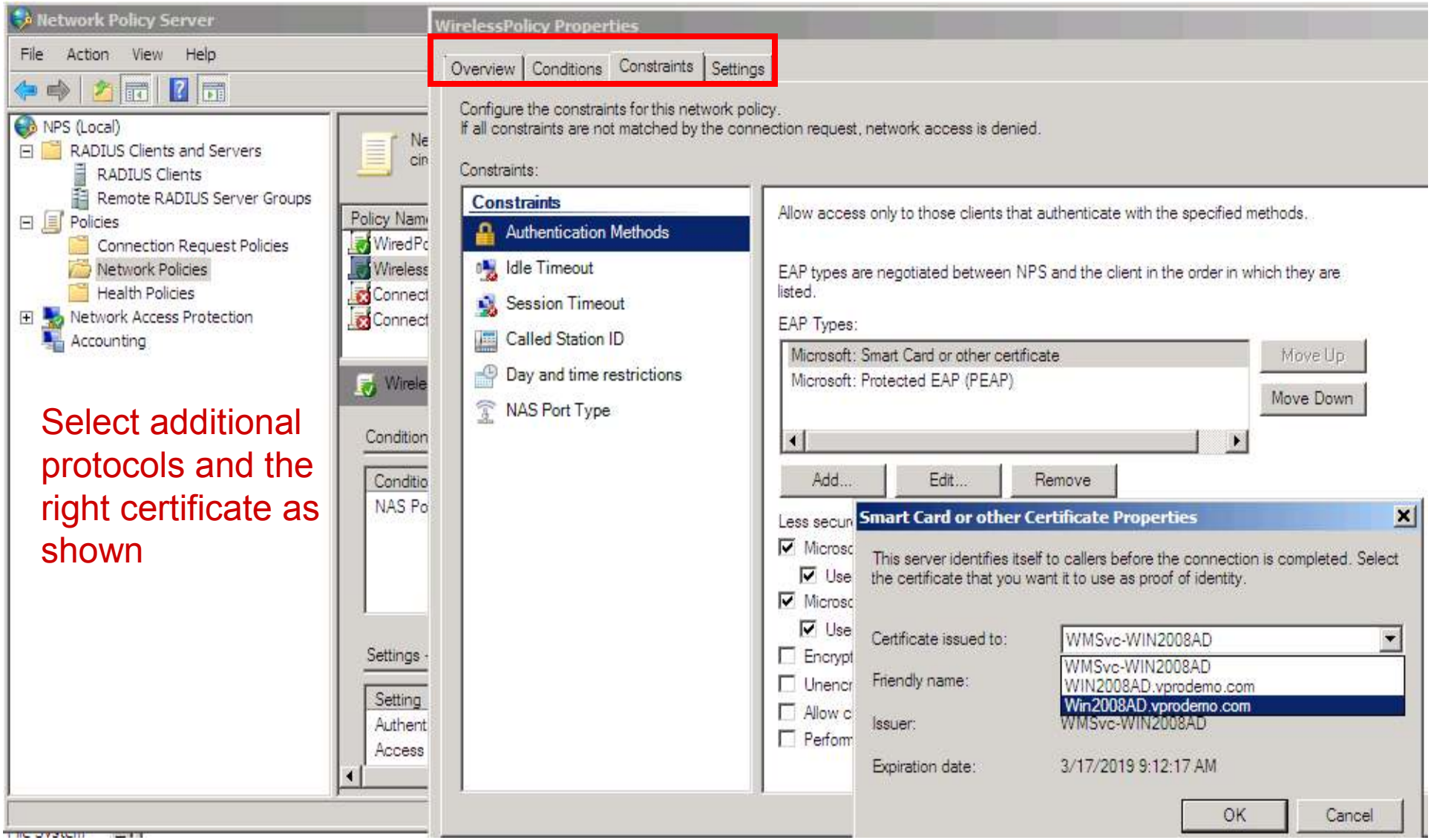
Under “Network Policies” “Move Up” the WirelessPolicy as required.



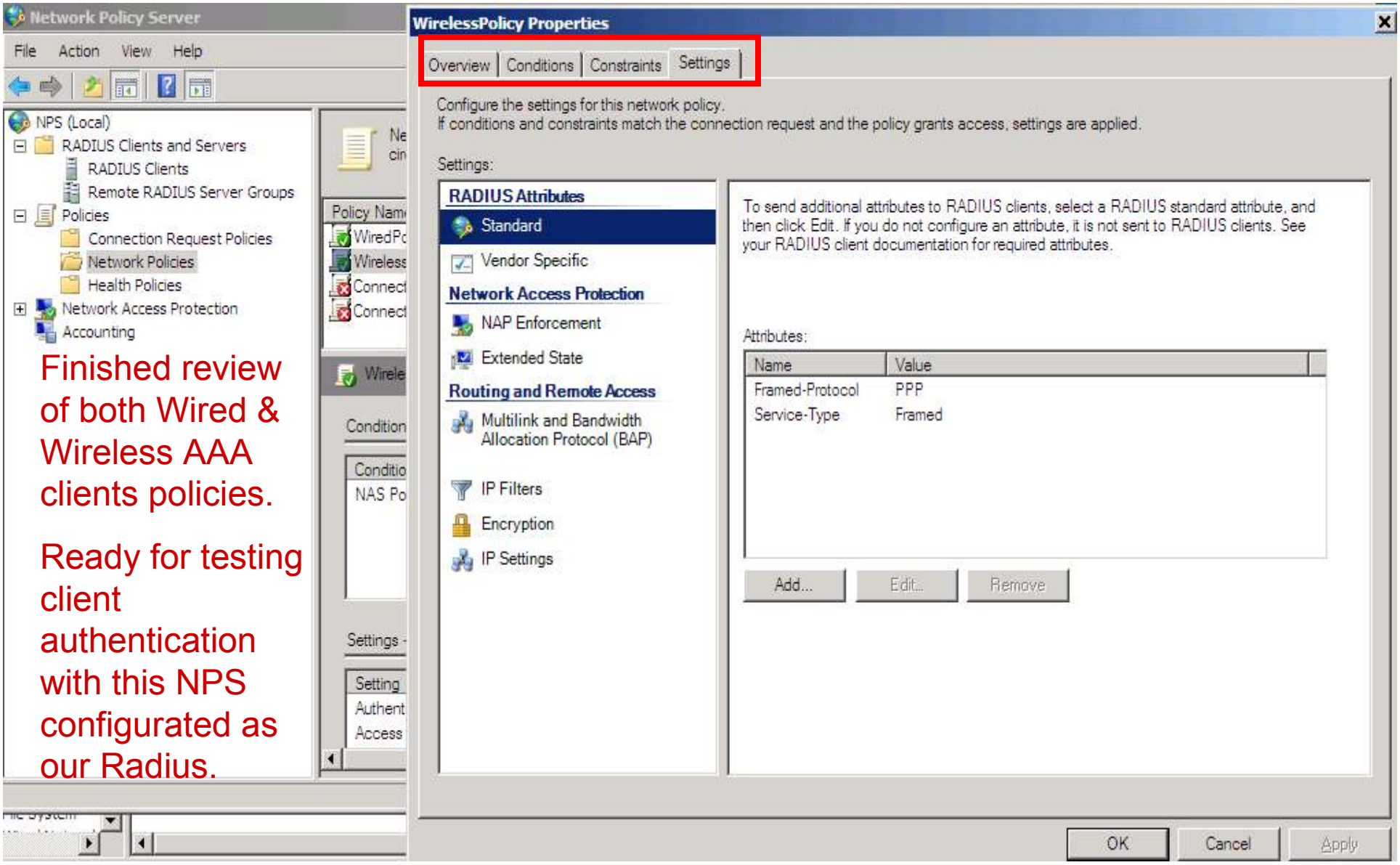
Double-Click WirelessPolicy and review all the tabs for accuracy.


Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Double-Click WirelessPolicy and review all the tabs for accuracy.
WirelessPolicy Properties
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


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
Double-Click WirelessPolicy and review all the tabs for accuracy.
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:
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
Move Up
Move Down
Add...
Edit...
Remove
Less secure authentication methods:
Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
User can change password after it has expired
Microsoft Encrypted Authentication (MS-CHAP)
User can change password after it has expired
Encrypted authentication (CHAP)
Unencrypted authentication (PAP, SPAP)
Allow clients to connect without negotiating an authentication method
Perform machine health check only
OK
Cancel
Apply



Select additional protocols and the right certificate as shown

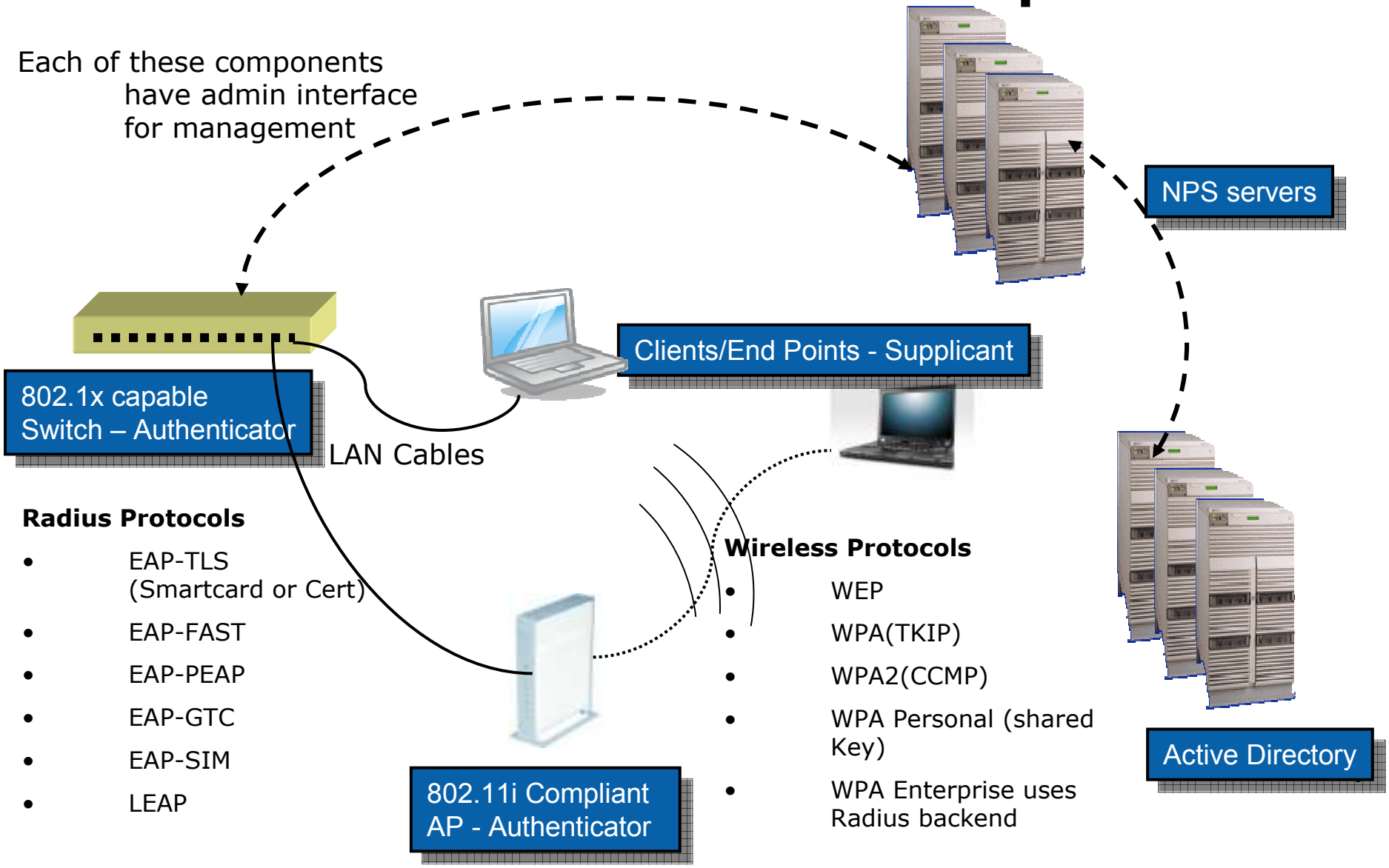


Finished review of both Wired & Wireless AAA clients policies.

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

Review 802.1x Architectural Components

Each of these components have admin interface for management



Radius Protocols

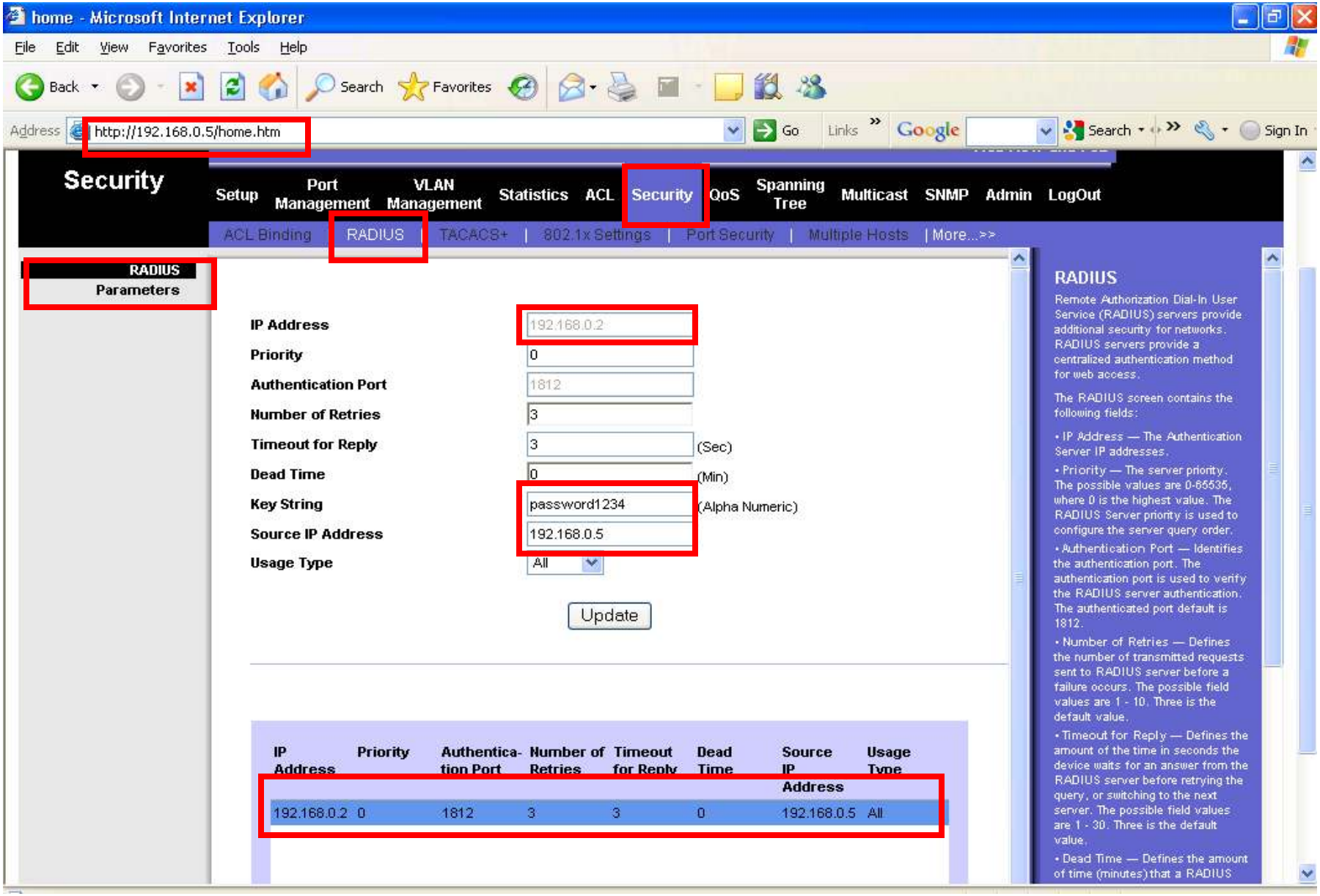
- EAP-TLS (Smartcard or Cert)
- EAP-FAST
- EAP-PEAP
- EAP-GTC
- EAP-SIM
- LEAP

Wireless Protocols

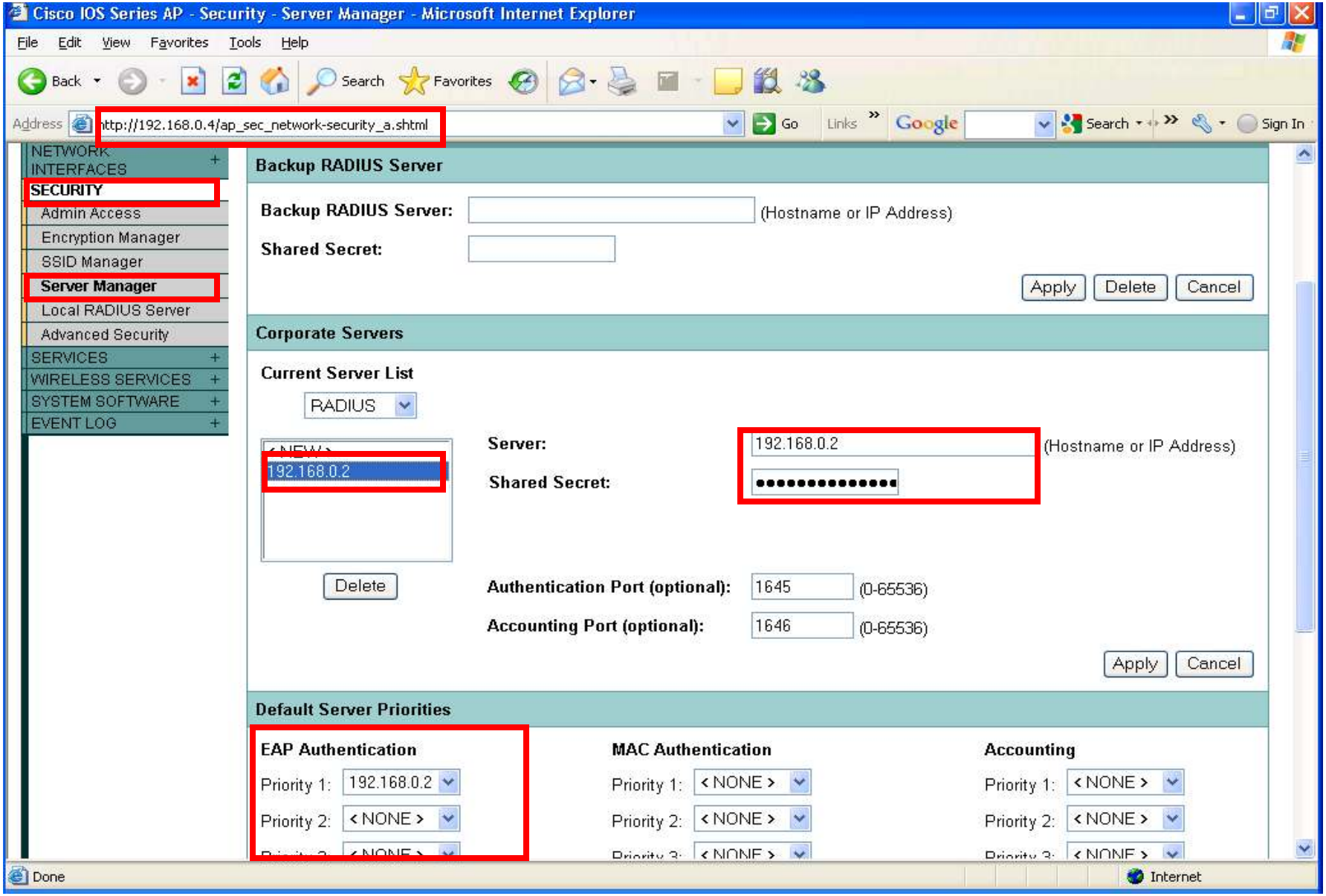
- WEP
- WPA(TKIP)
- WPA2(CCMP)
- WPA Personal (shared Key)
- WPA Enterprise uses Radius backend

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.



Wired AAA Client 192.168.0.5 web interface for configuring Radius Secret



Wireless AAA Client 192.168.0.4 web interface for configuring Radius Secret

Client Configuration

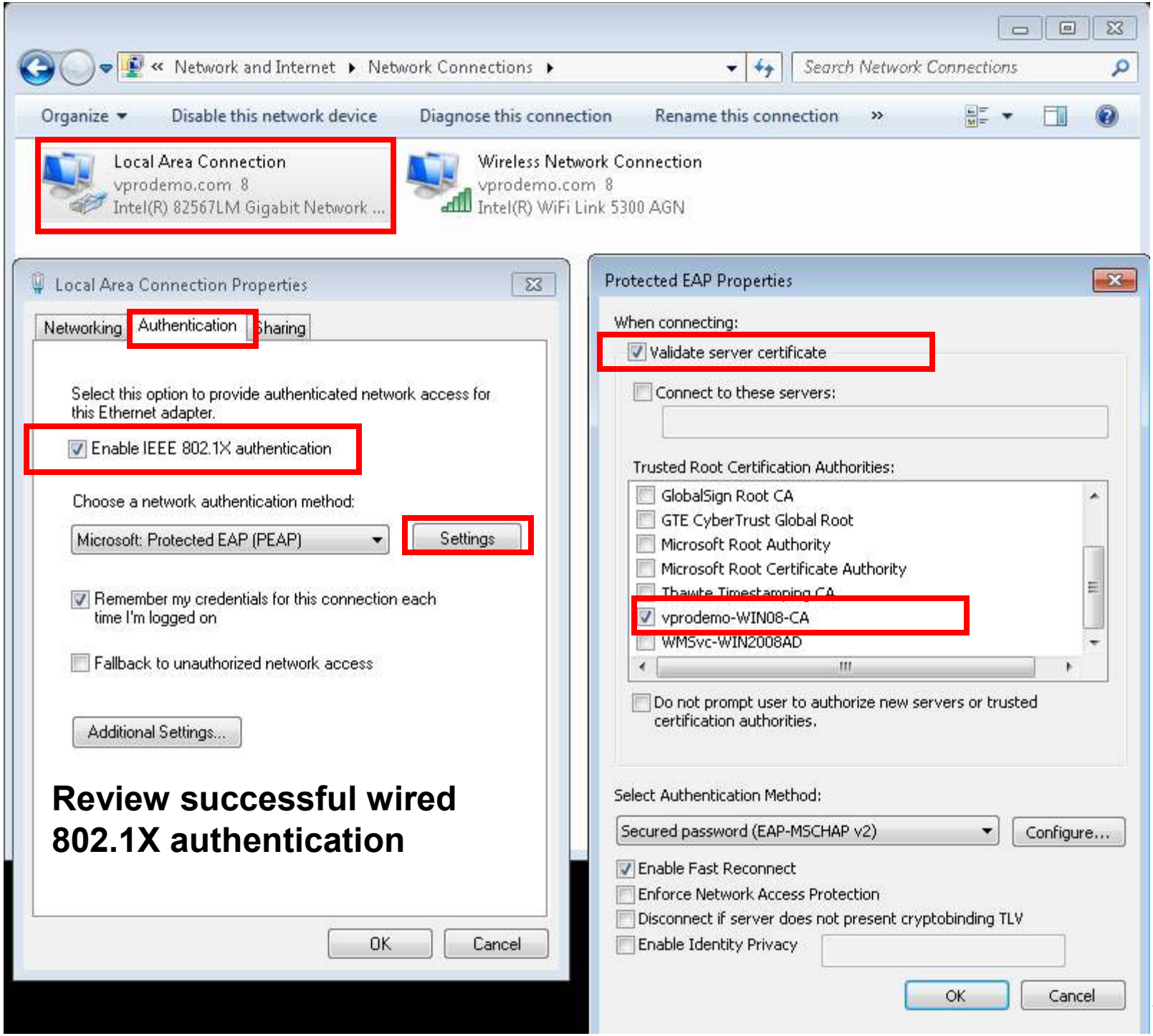
Right Click on Local Area Connection Adapter properties, click on Authentication tab. (see next slide)

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

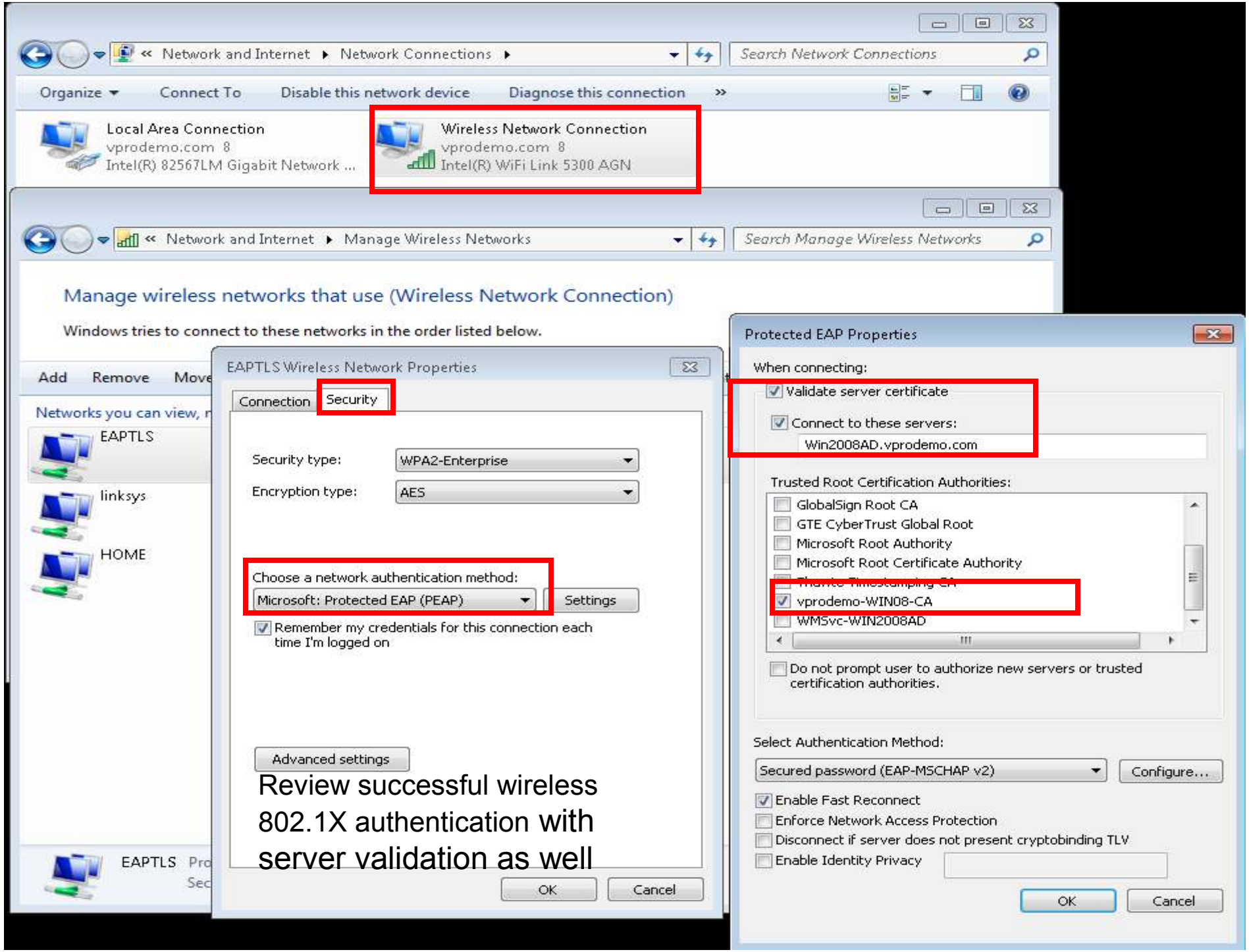
Check “Enable IEEE 802.1X authentication”.

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.

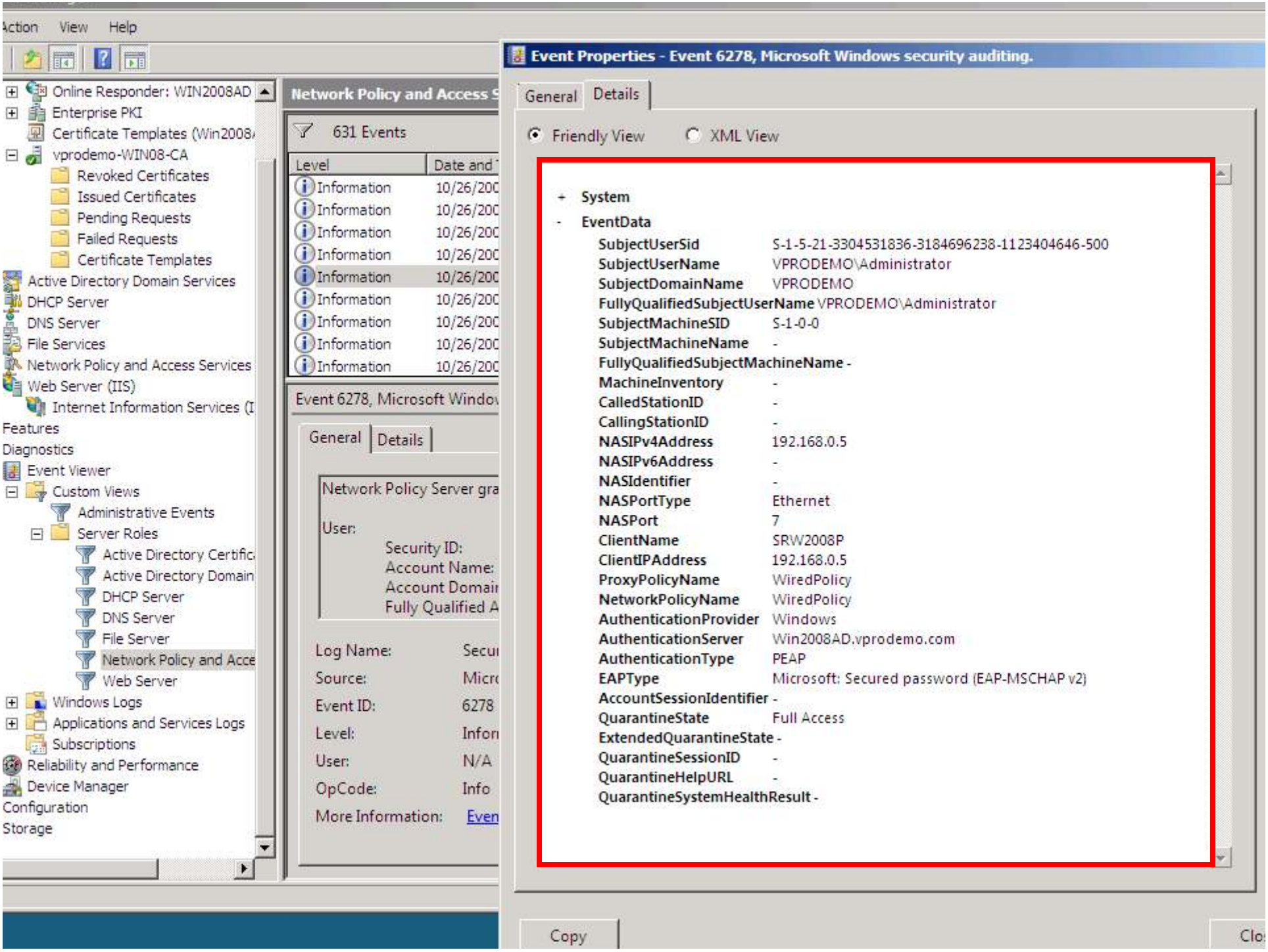


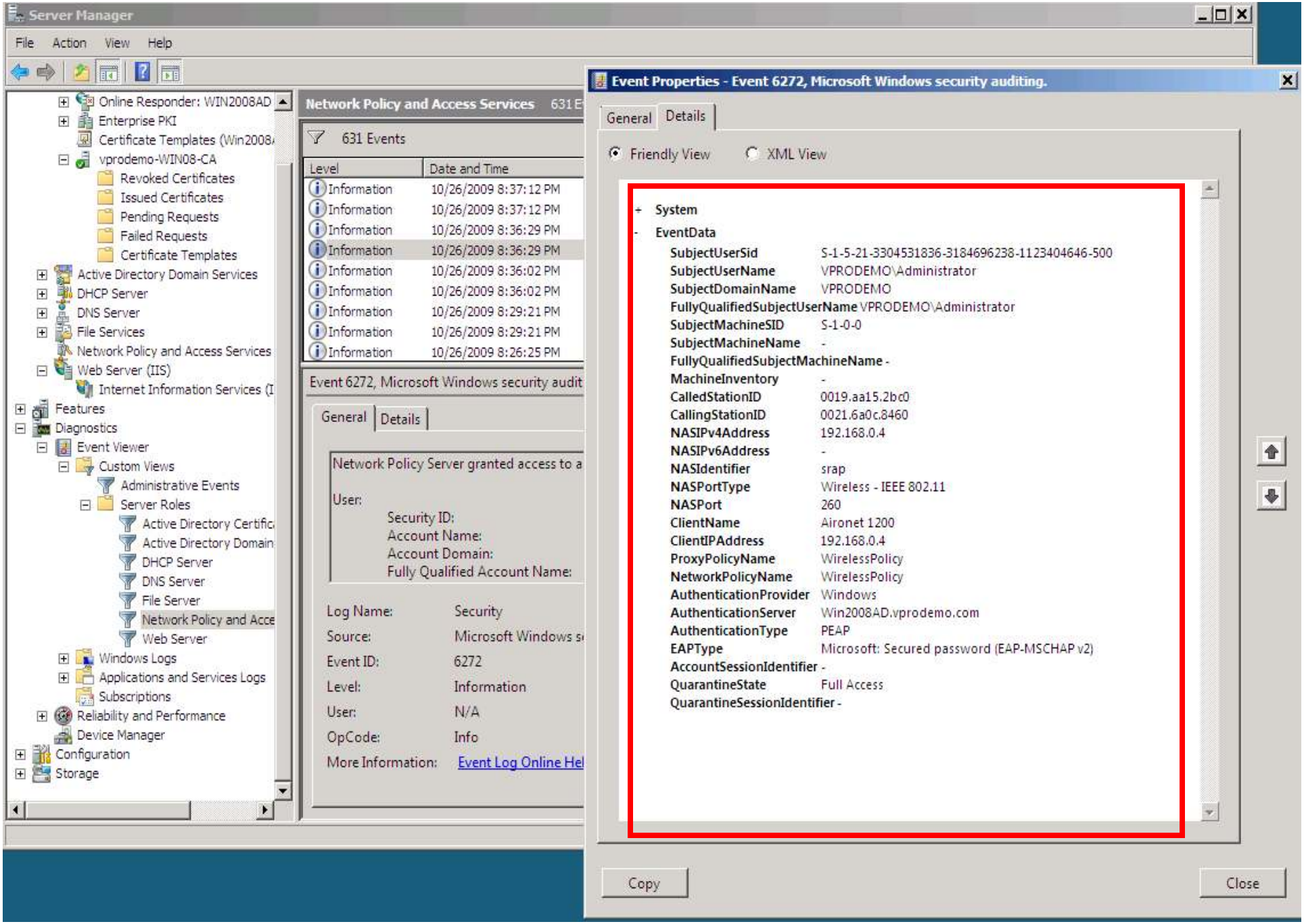
Review successful wired 802.1X authentication


Network and Internet ▸ Network Connections ▸
Search Network Connections
Organize
Connect To
Disable this network device
Diagnose this connection
Local Area Connection
vprodemo.com 8
Intel(R) 82567LM Gigabit Network ...
Wireless Network Connection
vprodemo.com 8
Intel(R) WiFi Link 5300 AGN
Network and Internet ▸ Manage Wireless Networks
Search Manage Wireless Networks
Manage wireless networks that use (Wireless Network Connection)
Windows tries to connect to these networks in the order listed below.
Add
Remove
Move
Networks you can view,
EAPTLS
linksys
HOME
EAPTLS Wireless Network Properties
Connection
Security
Security type:
WPA2-Enterprise
Encryption type:
AES
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
Advanced settings
OK
Cancel
Protected EAP Properties
When connecting:
Validate server certificate
Connect to these servers:
Win2008AD.vprodemo.com
Trusted Root Certification Authorities:
GlobalSign Root CA
GTE CyberTrust Global Root
Microsoft Root Authority
Microsoft Root Certificate Authority
vprodemo-WIN08-CA
WMSvc-WIN2008AD
Do not prompt user to authorize new servers or trusted certification authorities.
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Configure...
Enable Fast Reconnect
Enforce Network Access Protection
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK
Cancel
Review successful wireless 802.1X authentication with server validation as well

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).

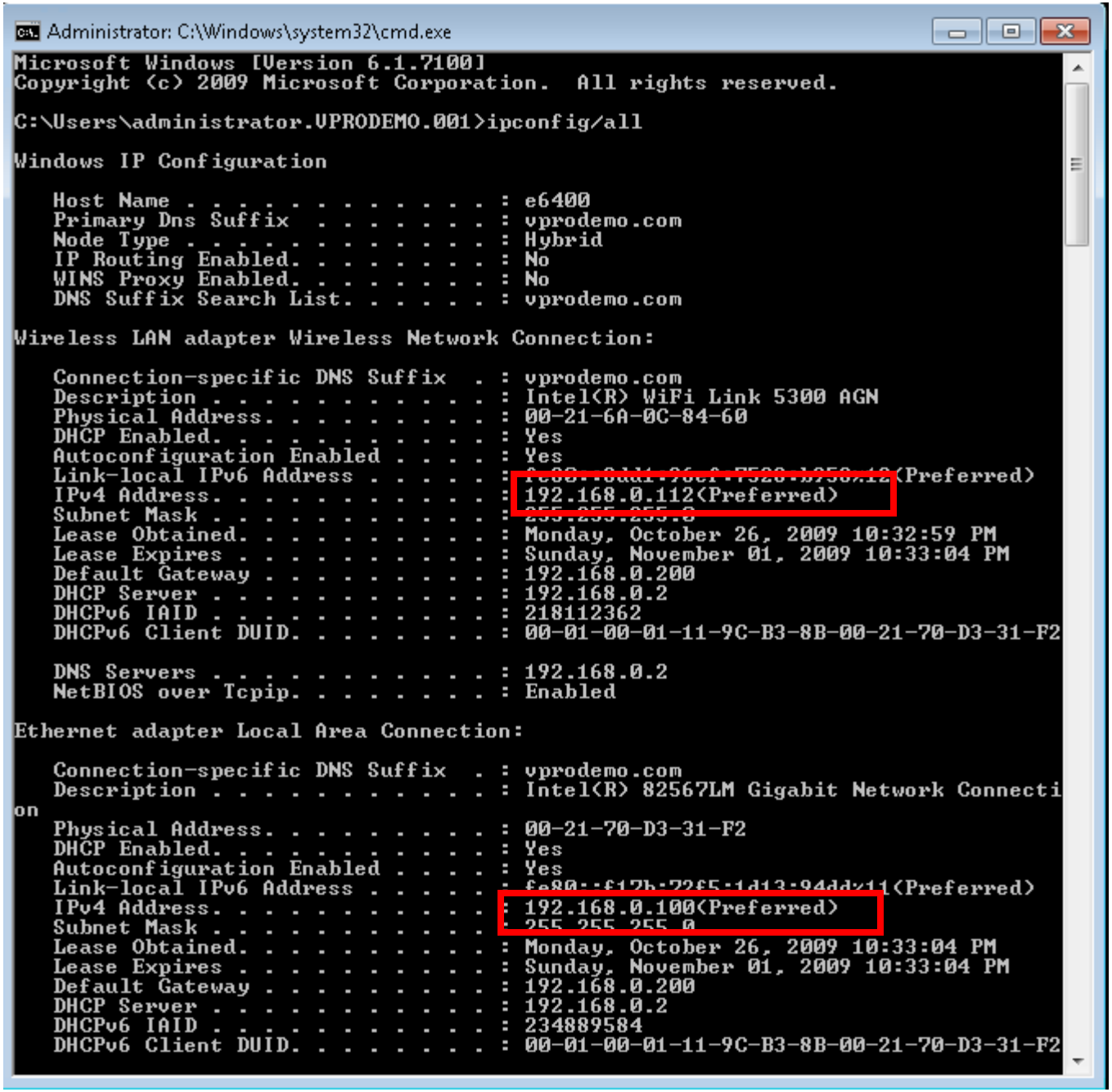

Action View Help
Online Responder: WIN2008AD
Enterprise PKI
Certificate Templates (Win2008
vprodemo-WIN08-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Active Directory Domain Services
DHCP Server
DNS Server
File Services
Network Policy and Access Services
Web Server (IIS)
Internet Information Services (I
Features
Diagnostics
Event Viewer
Custom Views
Administrative Events
Server Roles
Active Directory Certific
Active Directory Domain
DHCP Server
DNS Server
File Server
Network Policy and Acce
Web Server
Windows Logs
Applications and Services Logs
Subscriptions
Reliability and Performance
Device Manager
Configuration
Storage
Network Policy and Access S
631 Events
Level
Date and
Information 10/26/200
Information 10/26/200
Information 10/26/200
Information 10/26/200
Information 10/26/200
Information 10/26/200
Information 10/26/200
Information 10/26/200
Information 10/26/200
Event 6278, Microsoft Windo
General
Details
Network Policy Server gra
User:
Security ID:
Account Name:
Account Domai
Fully Qualified A
Log Name: Secu
Source: Micr
Event ID: 6278
Level: Infor
User: N/A
OpCode: Info
More Information: Even
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
Clo


Server Manager
File 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 (I
Features
Diagnostics
Event Viewer
Custom Views
Administrative Events
Server Roles
Active Directory Certific
Active Directory Domain
DHCP Server
DNS Server
File Server
Network Policy and Acce
Web Server
Windows Logs
Applications and Services Logs
Subscriptions
Reliability and Performance
Device Manager
Configuration
Storage
Network Policy and Access Services 631 E
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 srap
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



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.

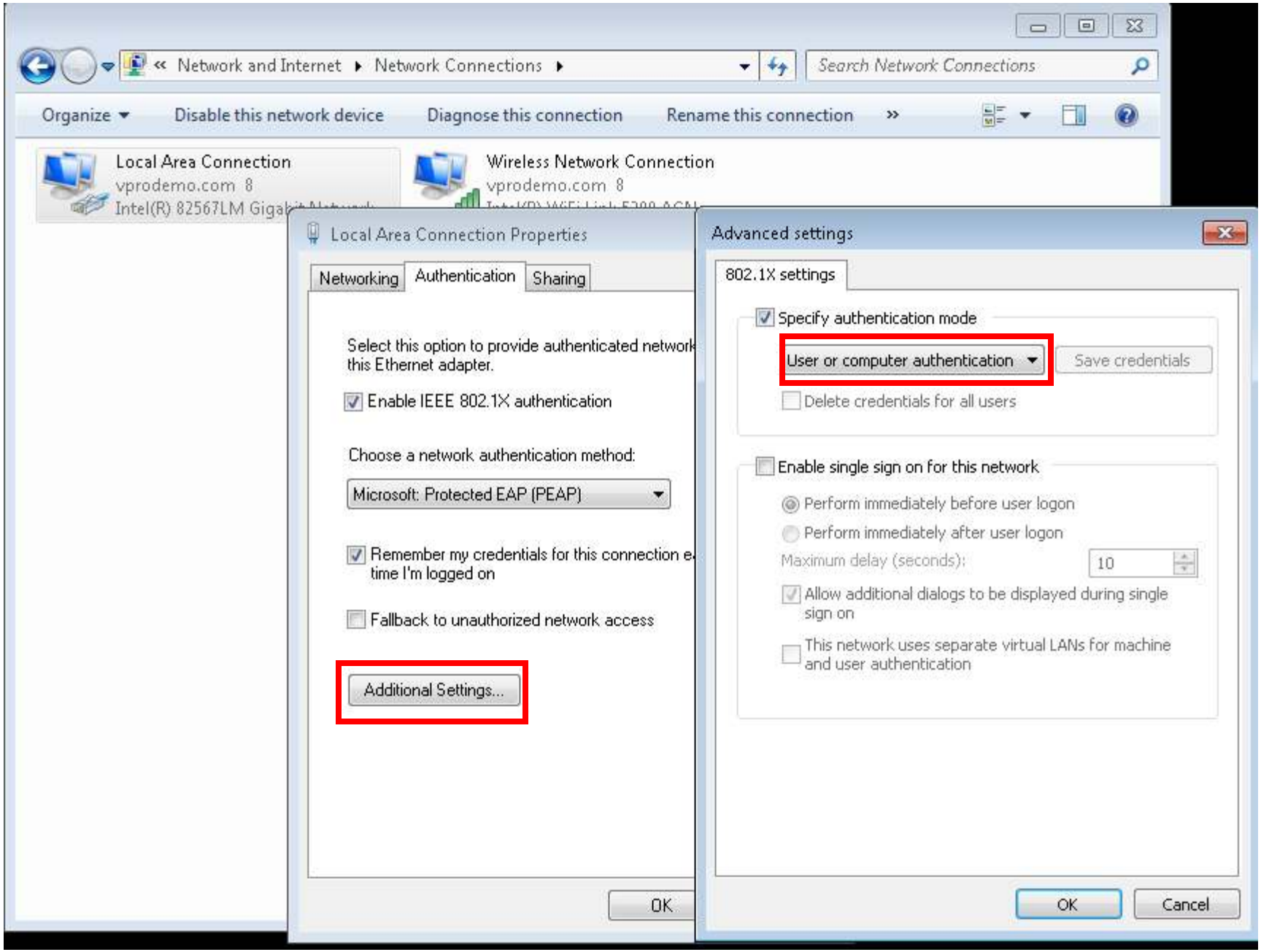
We already saw these settings on the NPS by allowing “Domain Users” as well as “Domain Computers” under the Network Policy.

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<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
```


« Network and Internet ▸ Network Connections ▸
Search Network Connections
Organize
Disable this network device
Diagnose this connection
Rename this connection
»
Local Area Connection
vprodemo.com 8
Wireless Network Connection
vprodemo.com 8
Local Area Connection Properties
Networking
Authentication
Sharing
Select this option to provide authenticated network
this Ethernet adapter.
Enable IEEE 802.1X authentication
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Remember my credentials for this connection e
time I'm logged on
Fallback to unauthorized network access
Additional Settings...
OK
Advanced settings
802.1X settings
Specify authentication mode
User or computer authentication
Save credentials
Delete credentials for all users
Enable single sign on for this network
Perform immediately before user logon
Perform immediately after user logon
Maximum delay (seconds):
10
Allow additional dialogs to be displayed during single sign on
This network uses separate virtual LANs for machine and user authentication
OK
Cancel

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.