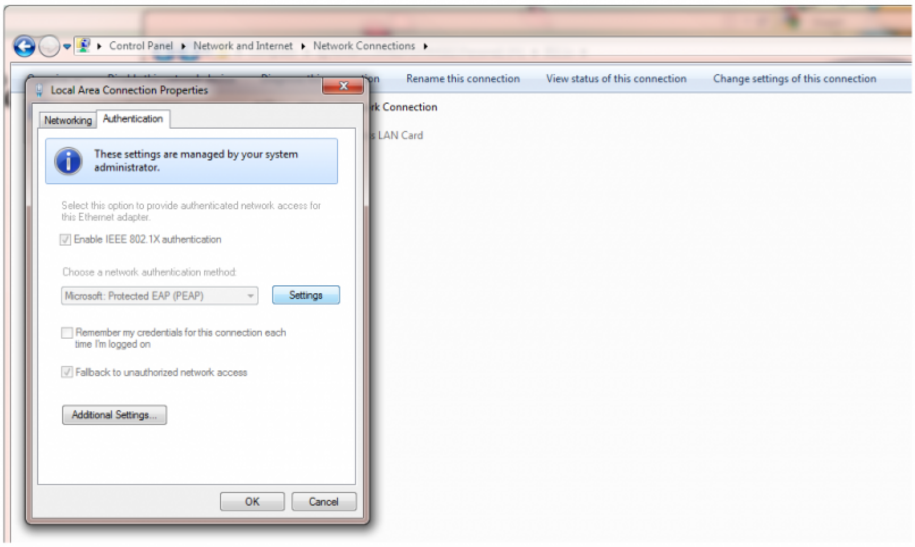
Configuring 802.1x Authentication On A Cisco Network

This document will help you configure 802.1x authentication on a Cisco Network using Microsoft Network Policy Server (NPS) to perform RADIUS authentication. You will be able to authenticate a client whether it's directly connected to an access layer device, or behind a Cisco Voice Over IP (VOIP) phone.

Windows 7 Client configuration

The first thing you're going to want to tackle is your windows clients. You need to tell them that they need to authenticate themselves, and how they need to do it. The configuration for either your wired or wireless connection is going to be identical. The only thing you need to do is apply this configuration to the appropriate interface.

In windows 7 open up the network sharing center, select "change adapter settings", then open the properties window for the interface you want to configure authentication on. Once the connection properties window opens you'll select the "Authentication" tab and under the "Choose a network authentication method:" drop down you'll select Microsoft: Protected EAP (PEAP)


Control Panel ▸ Network and Internet ▸ Network Connections ▸
Rename this connection
View status of this connection
Change settings of this connection
Local Area Connection Properties
Networking
Authentication
rk Connection
s LAN Card
Settings
Additional Settings...
OK
Cancel

These settings are managed by your system administrator.

Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

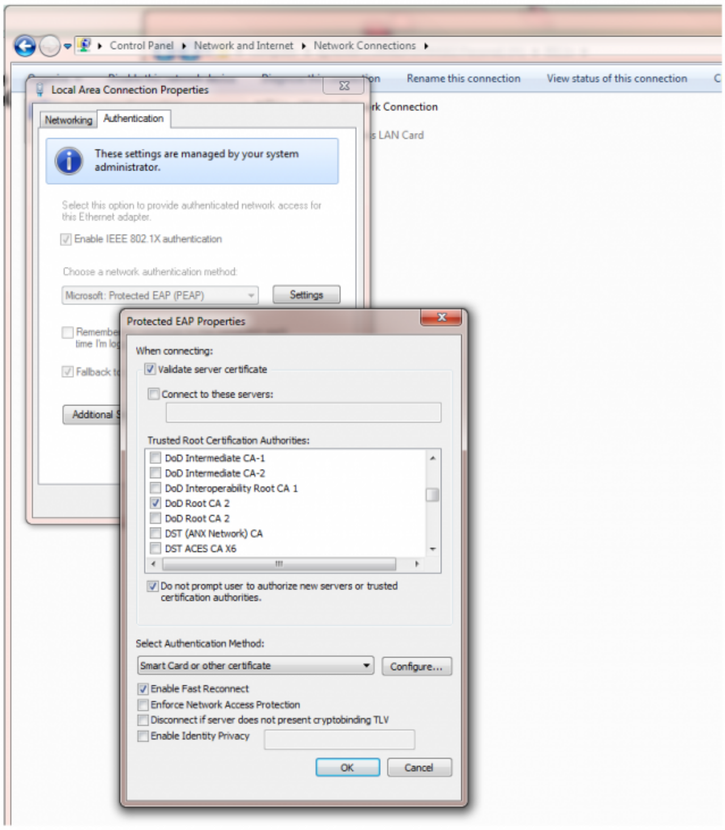
Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

□ Remember my credentials for this connection each time I'm logged on

☑ Fallback to unauthorized network access

Once you've selected PEAP click settings and begin telling the system what it's going to use in order to authenticate. For the machine we've decided that the Network Policy server is going to ensure that the client connecting has DoD Root CA 2 installed along with being a member of the domain. You'll do this in the "Trusted Root Certification Authorities" section. While you're on this window under the "Select Authentication Method" Drop down you'll select "Smart Card or other certificate" as well as, "Enable Fast Reconnect." Once this is complete, you'll select the "Configure" option to the right of "Smart Card or other certificate."



Control Panel ▸ Network and Internet ▸ Network Connections ▸
Rename this connection
View status of this connection
rk Connection
s LAN Card

Local Area Connection Properties

Networking | Authentication

These settings are managed by your system administrator.

Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

Choose a network authentication method:

Microsoft: Protected EAP (PEAP) | Settings

Protected EAP Properties

When connecting:

☑ Validate server certificate

☐ Connect to these servers:

Trusted Root Certification Authorities:

- ☐ DoD Intermediate CA-1
- ☐ DoD Intermediate CA-2
- ☐ DoD Interoperability Root CA 1
- ☑ DoD Root CA 2
- ☐ DoD Root CA 2
- ☐ DST (ANX Network) CA
- ☐ DST ACES CA X6

☑ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Smart Card or other certificate | Configure...

☑ Enable Fast Reconnect

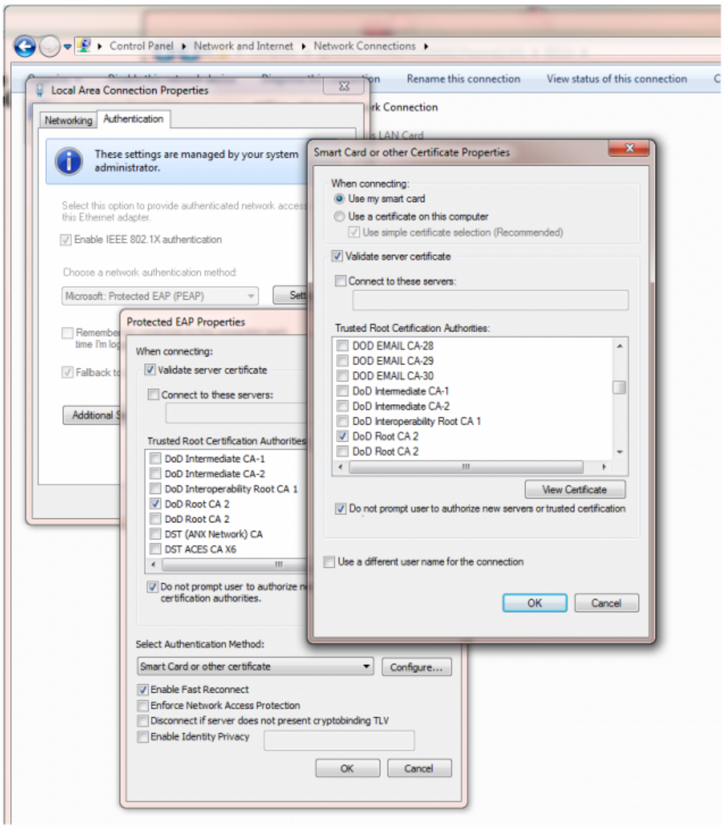
☐ Enforce Network Access Protection

☐ Disconnect if server does not present cryptobinding TLV

☐ Enable Identity Privacy

OK | Cancel

When the "Smart Card or other Certificate Properties" window opens make sure that "Smart Card" is selected under " When connecting", and the appropriate certificate is selected under "Trusted Root Certification Authorities." You're also going to want to make sure that the "Do not prompt user to authorize new servers or trusted certification" is selected. Once you're done configuring your authentication methods select Ok to exit all of the way back out to the authentication tab.



Smart Card or other Certificate Properties

When connecting:

● Use my smart card

○ Use a certificate on this computer

☑ Use simple certificate selection (Recommended)

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ DOD EMAIL CA-28
□ DOD EMAIL CA-29
□ DOD EMAIL CA-30
□ DoD Intermediate CA-1
□ DoD Intermediate CA-2
□ DoD Interoperability Root CA 1
☑ DoD Root CA 2
□ DoD Root CA 2

☑ Do not prompt user to authorize new servers or trusted certification

□ Use a different user name for the connection

Protected EAP Properties

When connecting:

☑ Validate server certificate

□ Connect to these servers:

Select Authentication Method: Smart Card or other certificate

☑ Enable Fast Reconnect

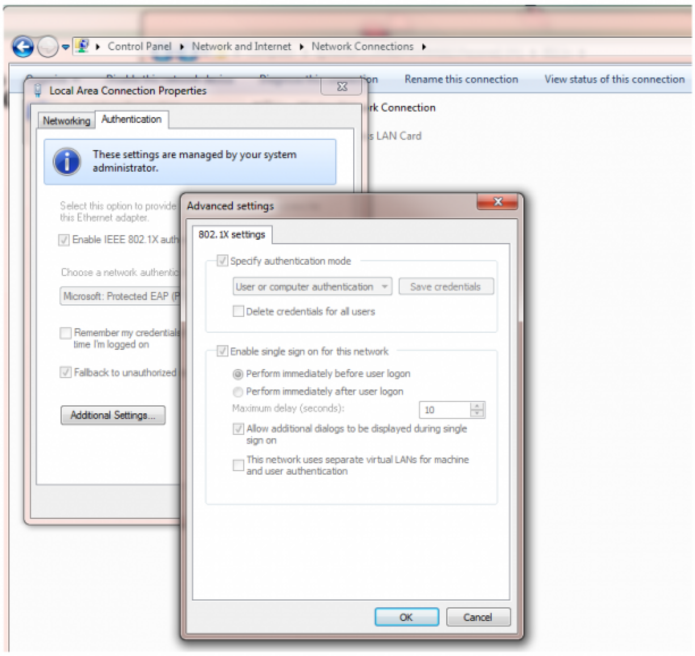
□ Enforce Network Access Protection

□ Disconnect if server does not present cryptobinding TLV

□ Enable Identity Privacy

Control Panel ▸ Network and Internet ▸ Network Connections
Rename this connection
View status of this connection
Local Area Connection Properties
Networking
Authentication
These settings are managed by your system administrator.
Enable IEEE 802.1X authentication
Microsoft: Protected EAP (PEAP)
View Certificate
Configure...
OK
Cancel

Under additional settings, you're going to select “Specify authentication mode”, and under the drop down in that section select “User or computer authentication.” Finally, select the “Enable single sign on for this network” box, “perform immediately before user log on”, and “Allow additional dialogs to be displayed during single sign on”. Save by clicking Ok and exit all of the way out of “Local Area Connection Properties”.



Advanced settings

802.1X settings

☑ Specify authentication mode: User or computer authentication

□ 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

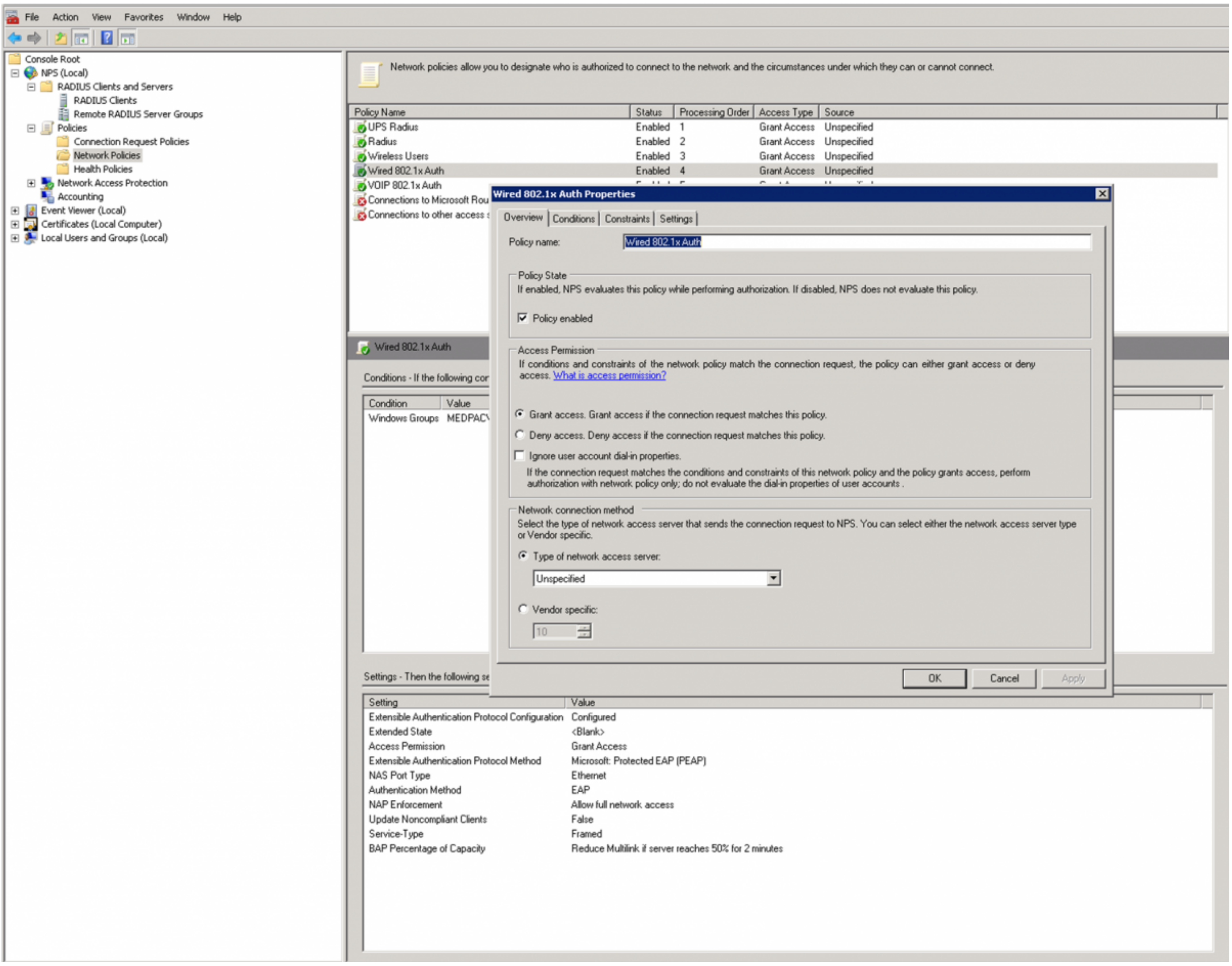
☑ Allow additional dialogs to be displayed during single sign on

□ This network uses separate virtual LANs for machine and user authentication

Control Panel ▸ Network and Internet ▸ Network Connections
Rename this connection
View status of this connection
Local Area Connection Properties
Networking
Authentication
These settings are managed by your system administrator.
Enable IEEE 802.1X authentication
Microsoft: Protected EAP (PEAP)
Remember my credentials for this connection each time I'm logged on
Fallback to unauthorized network access
Additional Settings...
Save credentials
OK
Cancel

Configuring Network Policy Server On Windows Server 2008 to permit wired or wireless 802.1x authentication

Log into the server you're going to use to perform Radius authentication and open up a Microsoft Management Console (MMC). Once this window is open go to File > Add/Remove Snap-in… > And add Network Policy Sever (NPS) for the local computer. Under NPS you're going to drill down to the Network Policies folder, right click that folder and select new. You're going to want the fields in this wizard to reflect what's in the following images.


File
Action
View
Favorites
Window
Help
Console Root
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Event Viewer (Local)
Certificates (Local Computer)
Local Users and Groups (Local)

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
UPS Radius	Enabled	1	Grant Access	Unspecified
Radius	Enabled	2	Grant Access	Unspecified
Wireless Users	Enabled	3	Grant Access	Unspecified
Wired 802.1x Auth	Enabled	4	Grant Access	Unspecified
VOIP 802.1x Auth				
Connections to Microsoft Rou				
Connections to other access s				

Wired 802.1x Auth

Conditions - If the following cor

Condition	Value
Windows Groups	MEDPAC\

Wired 802.1x Auth Properties

Policy name: Wired 802.1x Auth

Policy State

If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

☑ Policy enabled

Access Permission

If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. What is access permission?

● Grant access. Grant access if the connection request matches this policy.

○ Deny access. Deny access if the connection request matches this policy.

☐ Ignore user account dial-in properties.

If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts .

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific.

● Type of network access server:

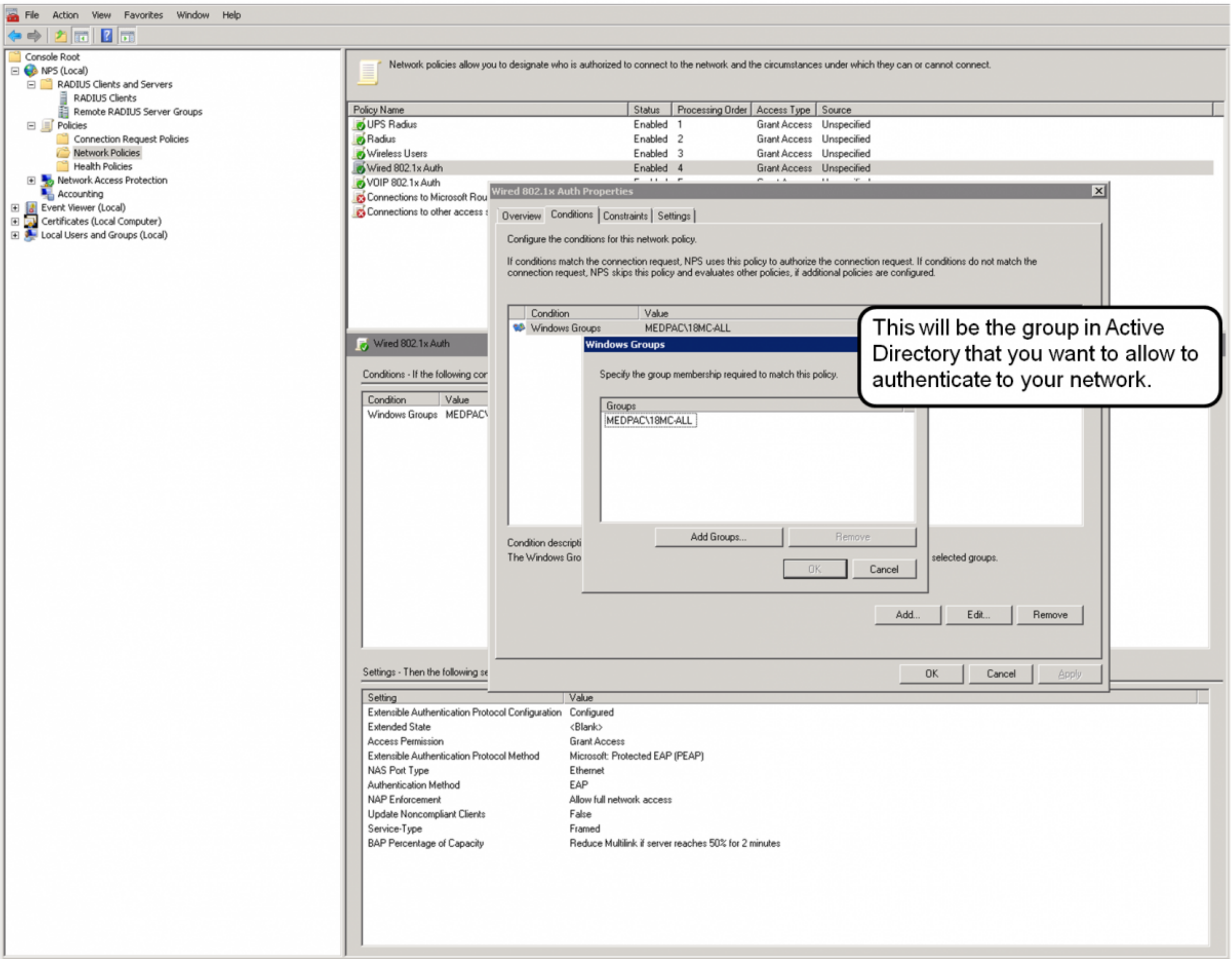
Unspecified

○ Vendor specific:

10

Settings - Then the following se

Setting	Value
Extensible Authentication Protocol Configuration	Configured
Extended State	<Blank>
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
NAS Port Type	Ethernet
Authentication Method	EAP
NAP Enforcement	Allow full network access
Update Noncompliant Clients	False
Service-Type	Framed
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes



Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
UPS Radius	Enabled	1	Grant Access	Unspecified
Radius	Enabled	2	Grant Access	Unspecified
Wireless Users	Enabled	3	Grant Access	Unspecified
Wired 802.1x Auth	Enabled	4	Grant Access	Unspecified
VOIP 802.1x Auth				
Connections to Microsoft Rou				
Connections to other access s				

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
Windows Groups	MEDPAC\18MC-ALL

Specify the group membership required to match this policy.

Groups
MEDPAC\18MC-ALL

Condition descripti

The Windows Gro ... selected groups.

Wired 802.1x Auth

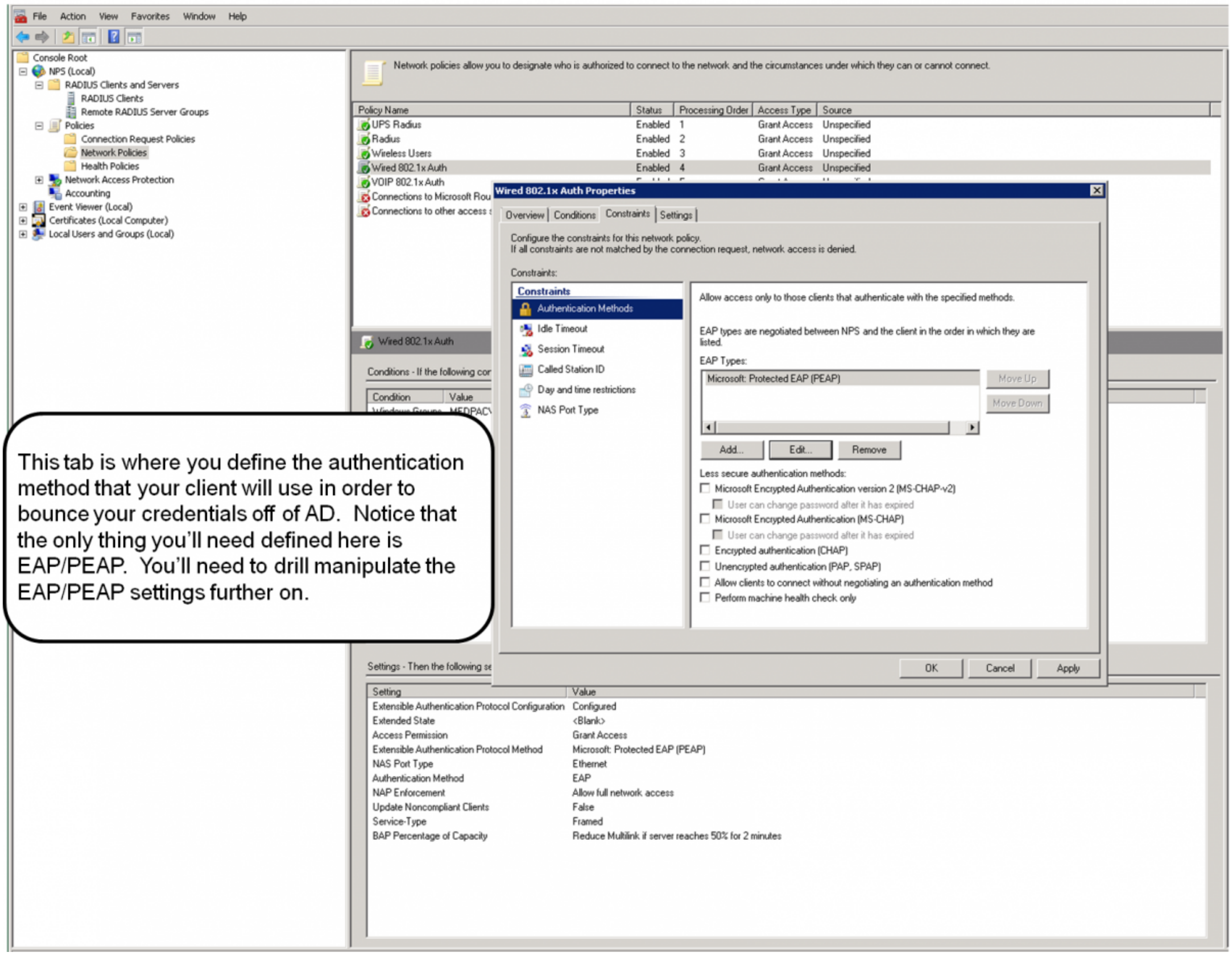
Conditions - If the following cor

Condition	Value
Windows Groups	MEDPAC\

Settings - Then the following se

Setting	Value
Extensible Authentication Protocol Configuration	Configured
Extended State	<Blank>
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
NAS Port Type	Ethernet
Authentication Method	EAP
NAP Enforcement	Allow full network access
Update Noncompliant Clients	False
Service-Type	Framed
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes

This will be the group in Active Directory that you want to allow to authenticate to your network.



Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
UPS Radius	Enabled	1	Grant Access	Unspecified
Radius	Enabled	2	Grant Access	Unspecified
Wireless Users	Enabled	3	Grant Access	Unspecified
Wired 802.1x Auth	Enabled	4	Grant Access	Unspecified
VOIP 802.1x Auth				
Connections to Microsoft Rou				
Connections to other access				

Wired 802.1x Auth Properties

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: Protected EAP (PEAP)

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

Wired 802.1x Auth

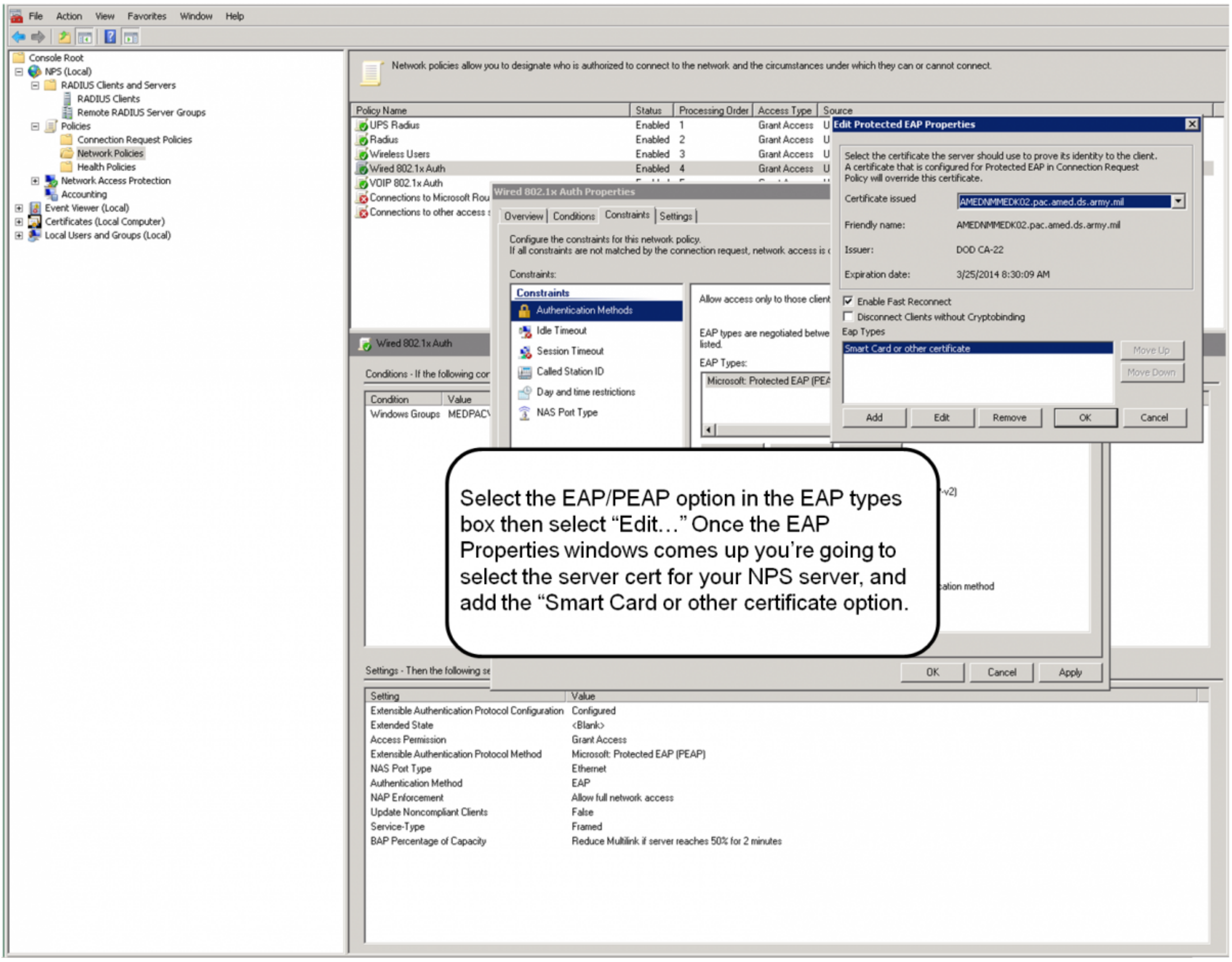
Conditions - If the following cor

Condition	Value
Windows Groups	MEDPAC\

Settings - Then the following se

Setting	Value
Extensible Authentication Protocol Configuration	Configured
Extended State	<Blank>
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
NAS Port Type	Ethernet
Authentication Method	EAP
NAP Enforcement	Allow full network access
Update Noncompliant Clients	False
Service-Type	Framed
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes

This tab is where you define the authentication method that your client will use in order to bounce your credentials off of AD. Notice that the only thing you'll need defined here is EAP/PEAP. You'll need to drill manipulate the EAP/PEAP settings further on.



Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
UPS Radius	Enabled	1	Grant Access	U
Radius	Enabled	2	Grant Access	U
Wireless Users	Enabled	3	Grant Access	U
Wired 802.1x Auth	Enabled	4	Grant Access	U
VOIP 802.1x Auth				
Connections to Microsoft Rou				
Connections to other access s				

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

Allow access only to those client

EAP types are negotiated betwe listed.

EAP Types:

Microsoft: Protected EAP (PEA

Conditions - If the following cor

Condition	Value
Windows Groups	MEDPAC\

Edit Protected EAP Properties

Select the certificate the server should use to prove its identity to the client. A certificate that is configured for Protected EAP in Connection Request Policy will override this certificate.

Certificate issued: AMEDNMMEDK02.pac.amed.ds.army.mil

Friendly name: AMEDNMMEDK02.pac.amed.ds.army.mil

Issuer: DOD CA-22

Expiration date: 3/25/2014 8:30:09 AM

☑ Enable Fast Reconnect

□ Disconnect Clients without Cryptobinding

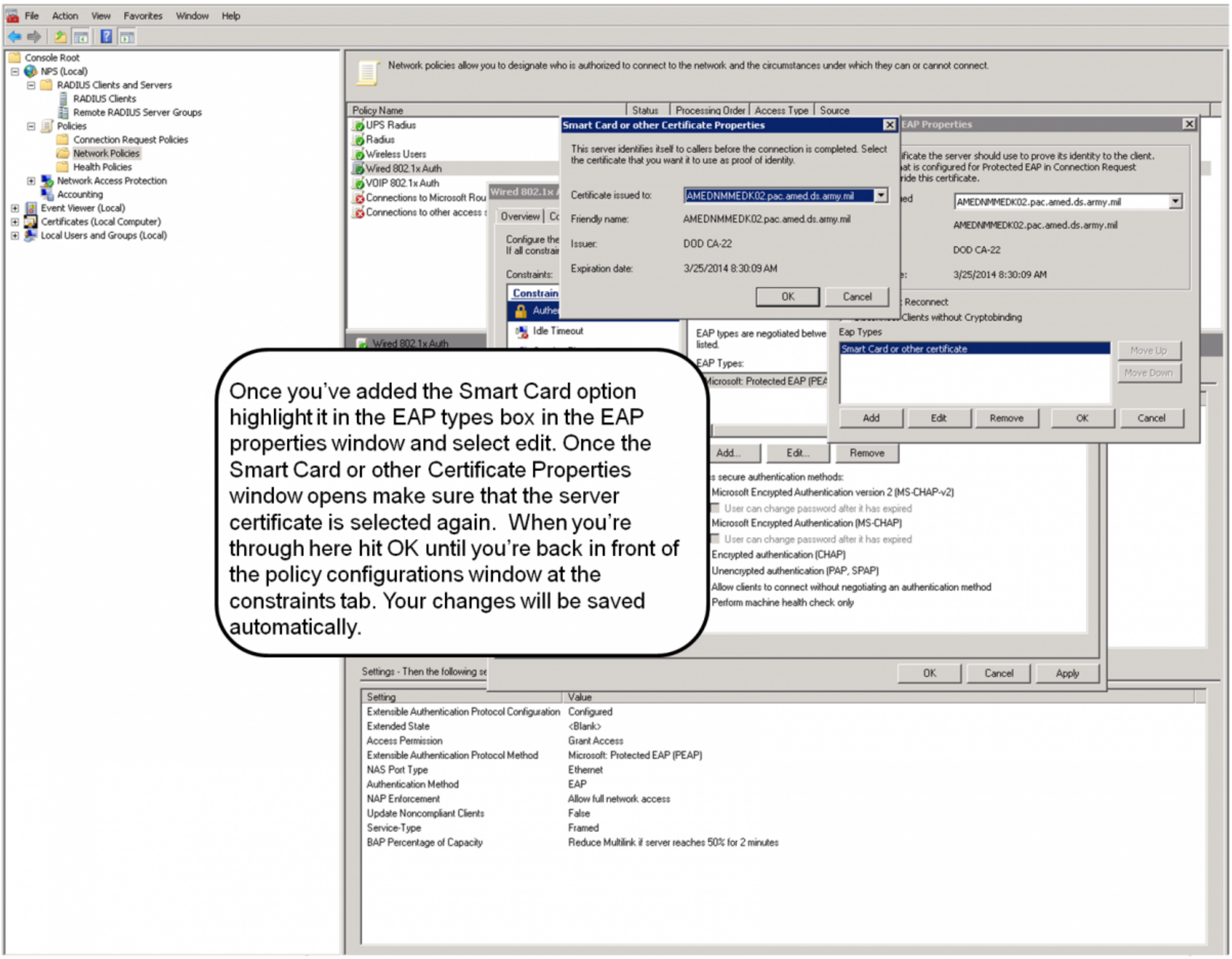
Eap Types

Smart Card or other certificate

Select the EAP/PEAP option in the EAP types box then select "Edit…" Once the EAP Properties windows comes up you're going to select the server cert for your NPS server, and add the "Smart Card or other certificate option.

Settings - Then the following se

Setting	Value
Extensible Authentication Protocol Configuration	Configured
Extended State	<Blank>
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
NAS Port Type	Ethernet
Authentication Method	EAP
NAP Enforcement	Allow full network access
Update Noncompliant Clients	False
Service-Type	Framed
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes



Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

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: AMEDNMMEDK02.pac.amed.ds.army.mil

Friendly name: AMEDNMMEDK02.pac.amed.ds.army.mil

Issuer: DOD CA-22

Expiration date: 3/25/2014 8:30:09 AM

EAP Properties

AMEDNMMEDK02.pac.amed.ds.army.mil

DOD CA-22

3/25/2014 8:30:09 AM

Eap Types

Smart Card or other certificate

EAP types are negotiated between ... listed.

EAP Types:

Microsoft: Protected EAP (PEA

...s 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)

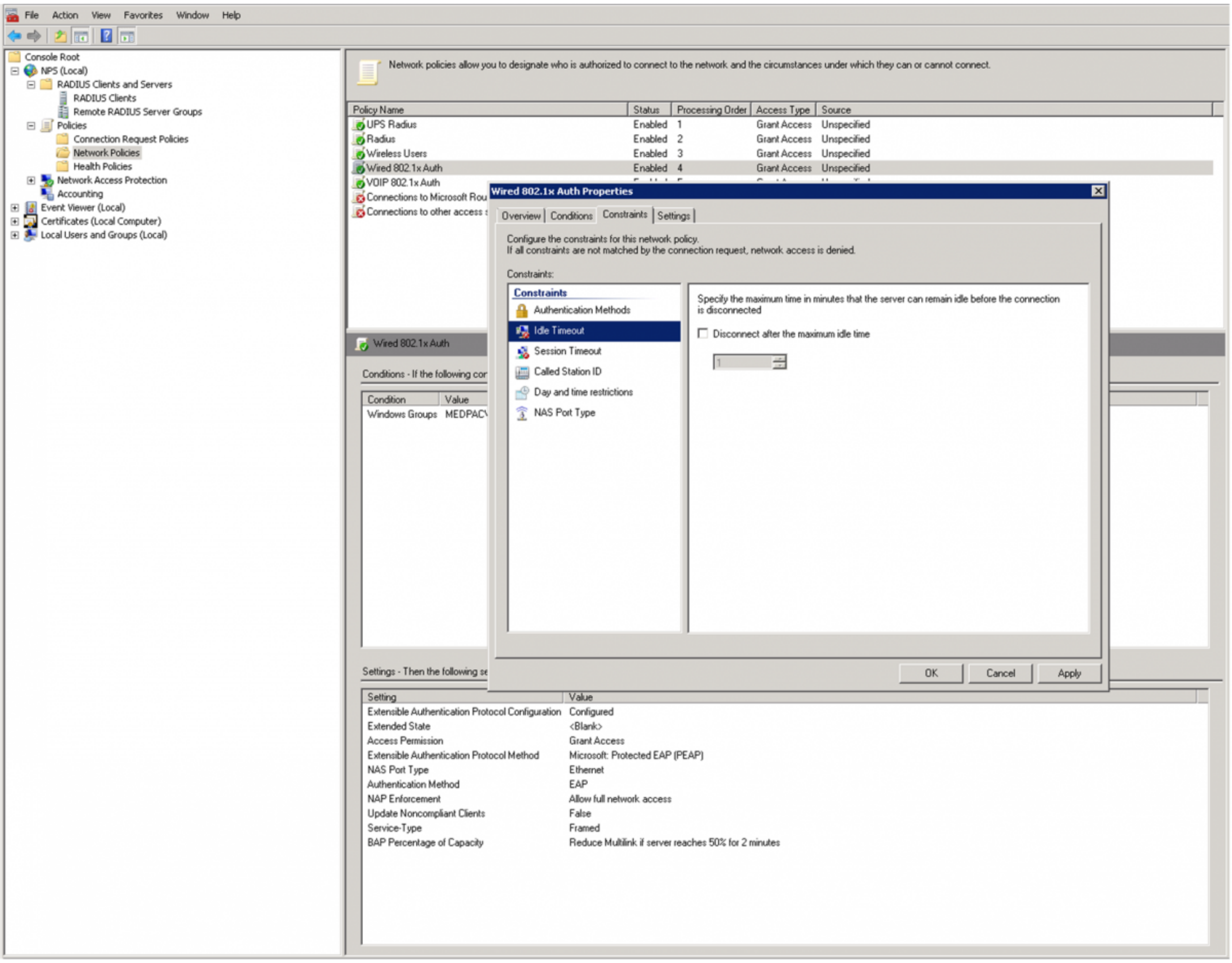
Allow clients to connect without negotiating an authentication method

Perform machine health check only

Settings - Then the following se...

Setting	Value
Extensible Authentication Protocol Configuration	Configured
Extended State	<Blank>
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
NAS Port Type	Ethernet
Authentication Method	EAP
NAP Enforcement	Allow full network access
Update Noncompliant Clients	False
Service-Type	Framed
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes

Once you’ve added the Smart Card option highlight it in the EAP types box in the EAP properties window and select edit. Once the Smart Card or other Certificate Properties window opens make sure that the server certificate is selected again. When you’re through here hit OK until you’re back in front of the policy configurations window at the constraints tab. Your changes will be saved automatically.



File
Action
View
Favorites
Window
Help
Console Root
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Event Viewer (Local)
Certificates (Local Computer)
Local Users and Groups (Local)

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
UPS Radius	Enabled	1	Grant Access	Unspecified
Radius	Enabled	2	Grant Access	Unspecified
Wireless Users	Enabled	3	Grant Access	Unspecified
Wired 802.1x Auth	Enabled	4	Grant Access	Unspecified
VOIP 802.1x Auth				
Connections to Microsoft Rou				
Connections to other access s				

Wired 802.1x Auth

Conditions - If the following cor

Condition	Value
Windows Groups	MEDPAC\

Wired 802.1x Auth Properties

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

Constraints:

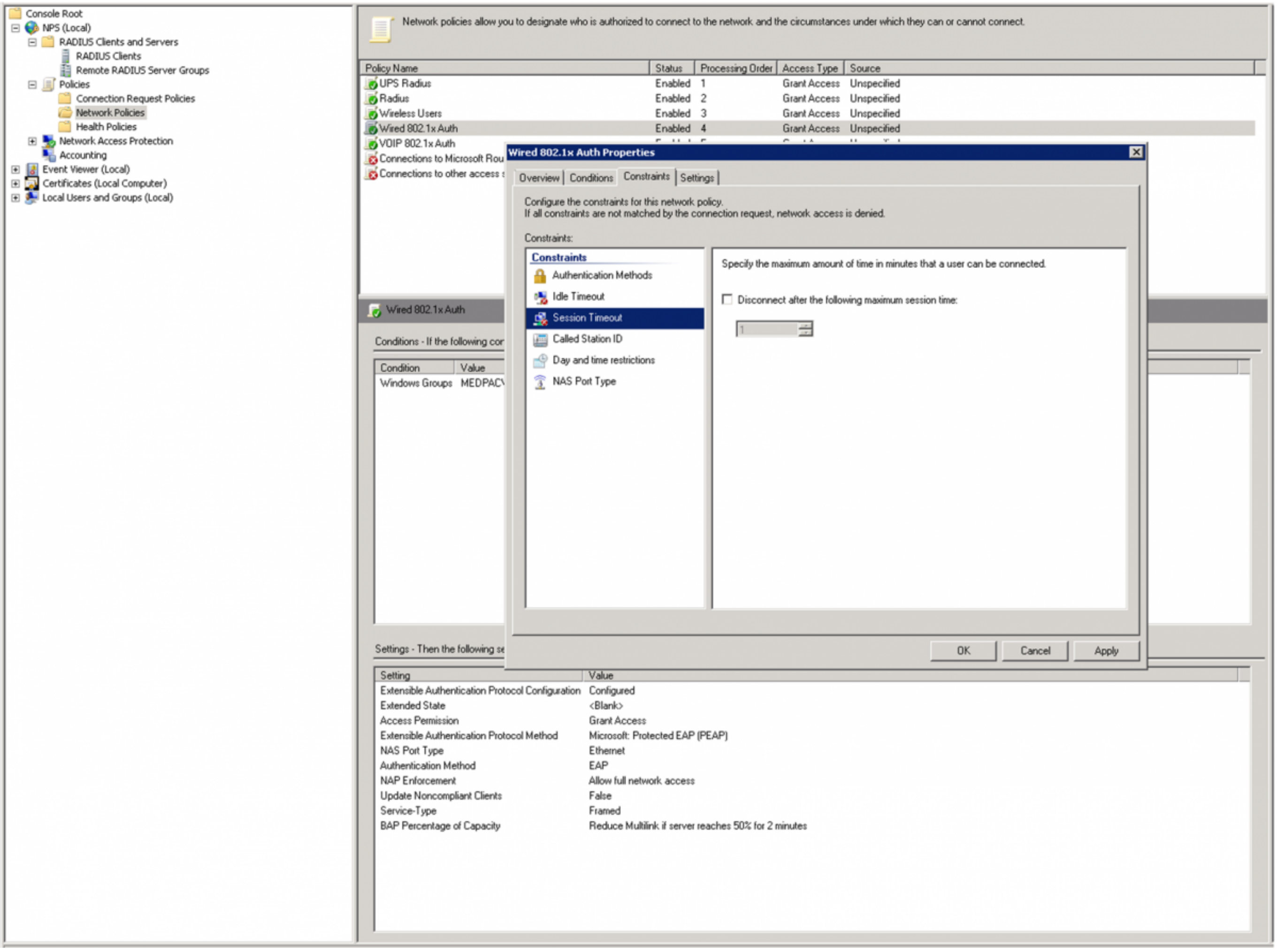
Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

□ Disconnect after the maximum idle time

1

Settings - Then the following se

Setting	Value
Extensible Authentication Protocol Configuration	Configured
Extended State	<Blank>
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
NAS Port Type	Ethernet
Authentication Method	EAP
NAP Enforcement	Allow full network access
Update Noncompliant Clients	False
Service-Type	Framed
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes


Console Root
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Event Viewer (Local)
Certificates (Local Computer)
Local Users and Groups (Local)

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
UPS Radius	Enabled	1	Grant Access	Unspecified
Radius	Enabled	2	Grant Access	Unspecified
Wireless Users	Enabled	3	Grant Access	Unspecified
Wired 802.1x Auth	Enabled	4	Grant Access	Unspecified
VOIP 802.1x Auth				
Connections to Microsoft Rou				
Connections to other access s				

Wired 802.1x Auth

Conditions - If the following cor

Condition	Value
Windows Groups	MEDPAC\

Settings - Then the following se

Setting	Value
Extensible Authentication Protocol Configuration	Configured
Extended State	<Blank>
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
NAS Port Type	Ethernet
Authentication Method	EAP
NAP Enforcement	Allow full network access
Update Noncompliant Clients	False
Service-Type	Framed
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes

Wired 802.1x Auth Properties

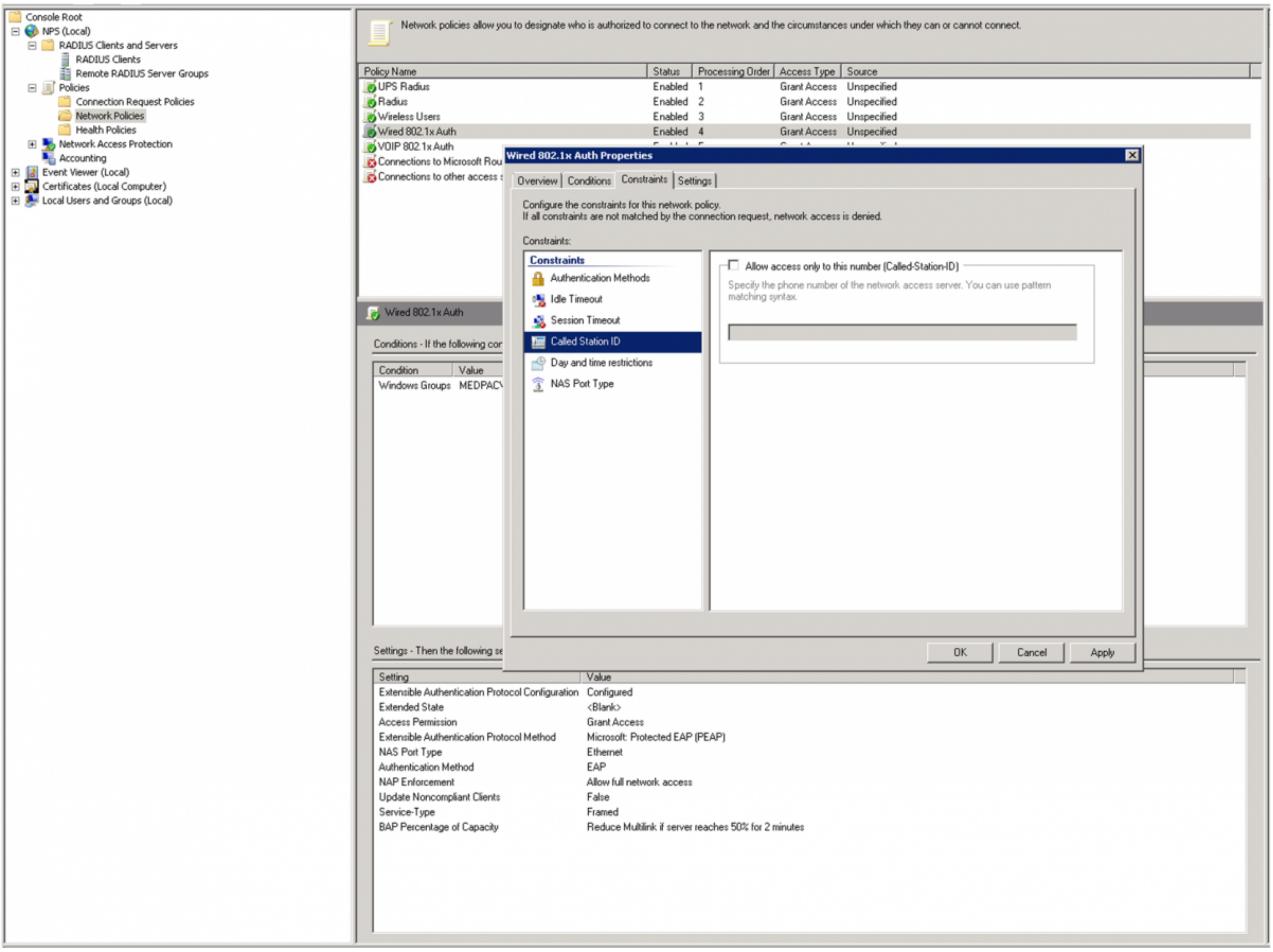
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Specify the maximum amount of time in minutes that a user can be connected.

□ Disconnect after the following maximum session time:

1


Console Root
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Event Viewer (Local)
Certificates (Local Computer)
Local Users and Groups (Local)

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
UPS Radius	Enabled	1	Grant Access	Unspecified
Radius	Enabled	2	Grant Access	Unspecified
Wireless Users	Enabled	3	Grant Access	Unspecified
Wired 802.1x Auth	Enabled	4	Grant Access	Unspecified
VOIP 802.1x Auth				
Connections to Microsoft Rou				
Connections to other access s				

Wired 802.1x Auth

Conditions - If the following cor

Condition	Value
Windows Groups	MEDPAC\

Settings - Then the following se

Setting	Value
Extensible Authentication Protocol Configuration	Configured
Extended State	<Blank>
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
NAS Port Type	Ethernet
Authentication Method	EAP
NAP Enforcement	Allow full network access
Update Noncompliant Clients	False
Service-Type	Framed
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes

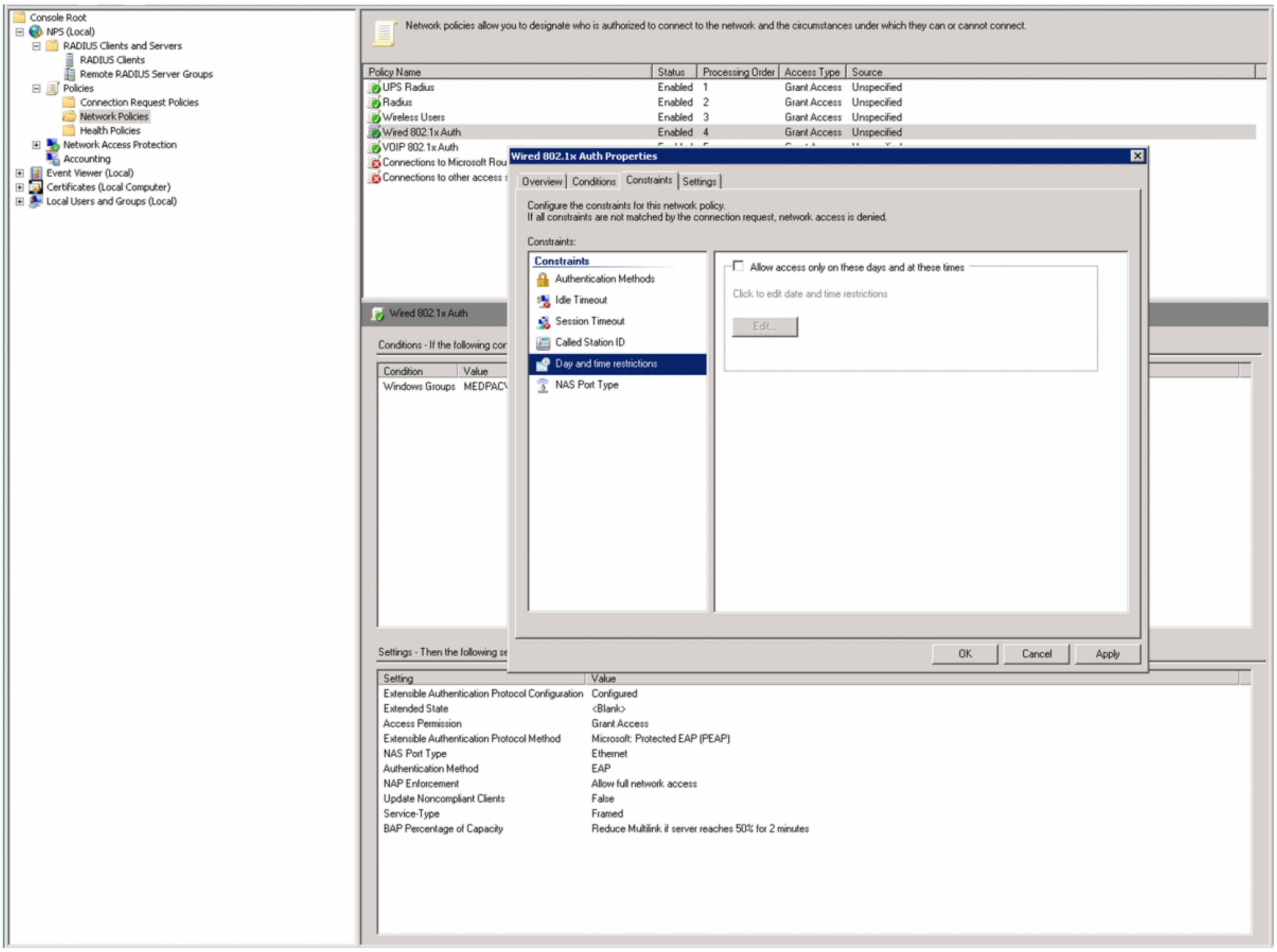
Wired 802.1x Auth Properties

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

Constraints:

☐ Allow access only to this number (Called-Station-ID)

Specify the phone number of the network access server. You can use pattern matching syntax.


Console Root
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Event Viewer (Local)
Certificates (Local Computer)
Local Users and Groups (Local)

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
UPS Radius	Enabled	1	Grant Access	Unspecified
Radius	Enabled	2	Grant Access	Unspecified
Wireless Users	Enabled	3	Grant Access	Unspecified
Wired 802.1x Auth	Enabled	4	Grant Access	Unspecified
VOIP 802.1x Auth				
Connections to Microsoft Rou				
Connections to other access s				

Wired 802.1x Auth Properties

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

Constraints:

□ Allow access only on these days and at these times

Click to edit date and time restrictions

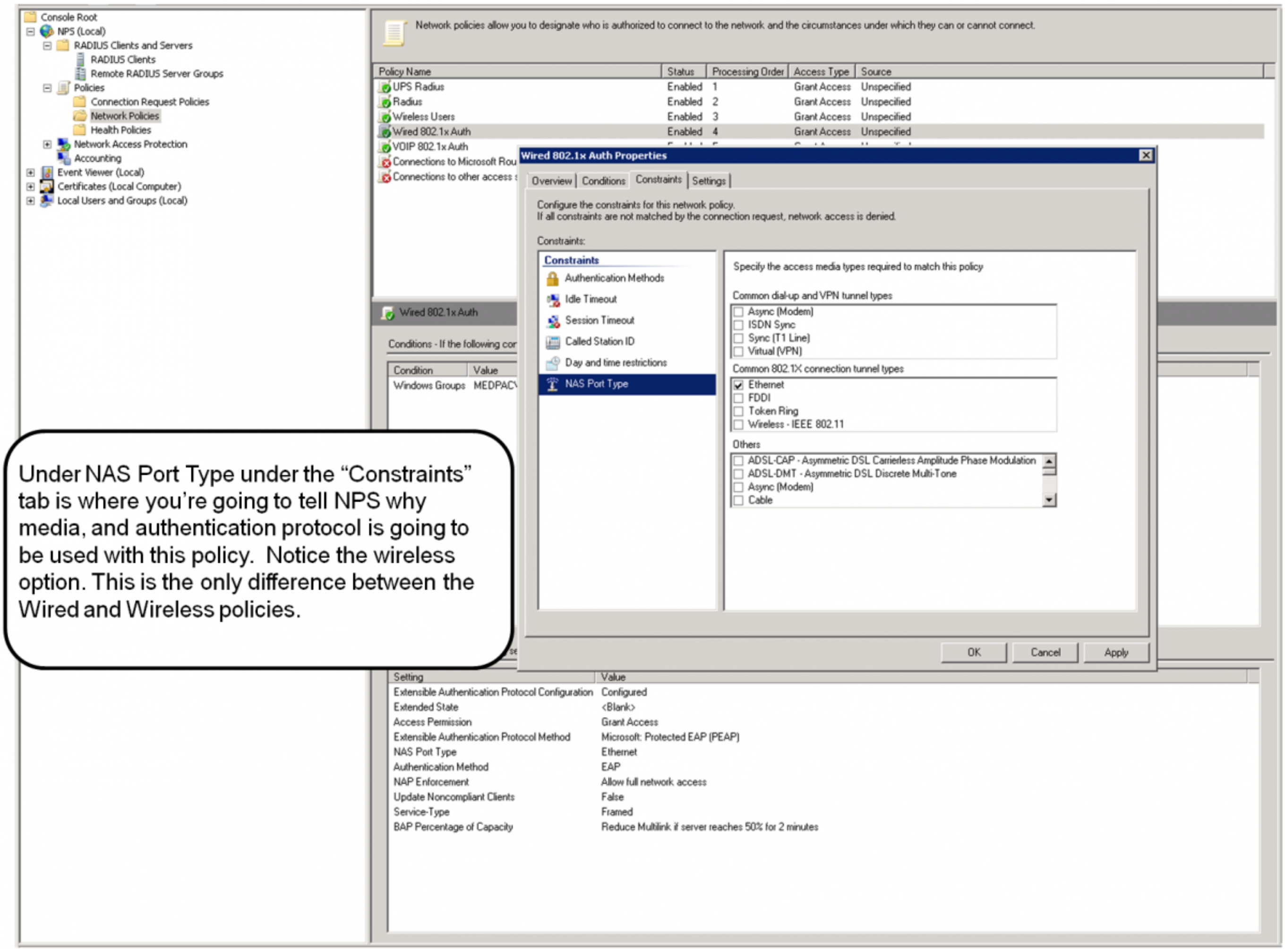
Wired 802.1x Auth

Conditions - If the following cor

Condition	Value
Windows Groups	MEDPAC\

Settings - Then the following se

Setting	Value
Extensible Authentication Protocol Configuration	Configured
Extended State	<Blank>
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
NAS Port Type	Ethernet
Authentication Method	EAP
NAP Enforcement	Allow full network access
Update Noncompliant Clients	False
Service-Type	Framed
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes



Console Root
- NPS (Local)
  - RADIUS Clients and Servers
    - RADIUS Clients
    - Remote RADIUS Server Groups
  - Policies
    - Connection Request Policies
    - Network Policies
    - Health Policies
  - Network Access Protection
  - Accounting
- Event Viewer (Local)
- Certificates (Local Computer)
- Local Users and Groups (Local)

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
UPS Radius	Enabled	1	Grant Access	Unspecified
Radius	Enabled	2	Grant Access	Unspecified
Wireless Users	Enabled	3	Grant Access	Unspecified
Wired 802.1x Auth	Enabled	4	Grant Access	Unspecified
VOIP 802.1x Auth				
Connections to Microsoft Rou				
Connections to other access s				

Wired 802.1x Auth

Conditions - If the following cor

Condition	Value
Windows Groups	MEDPAC\

Wired 802.1x Auth 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

Specify the access media types required to match this policy

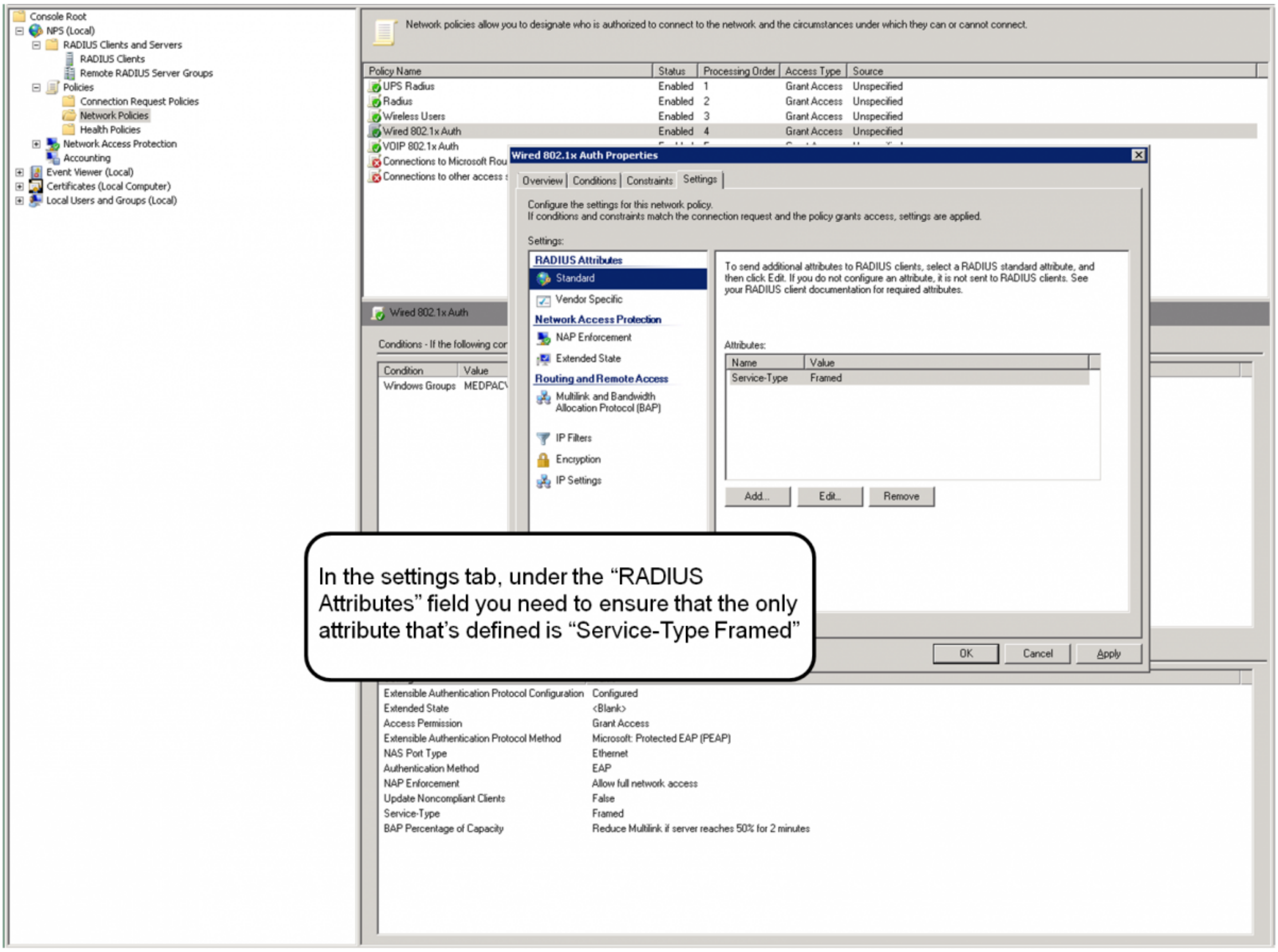
Common dial-up and VPN tunnel types
- ☐ Async (Modem)
- ☐ ISDN Sync
- ☐ Sync (T1 Line)
- ☐ Virtual (VPN)

Common 802.1X connection tunnel types
- ☑ Ethernet
- ☐ FDDI
- ☐ Token Ring
- ☐ Wireless - IEEE 802.11

Others
- ☐ ADSL-CAP - Asymmetric DSL Carrierless Amplitude Phase Modulation
- ☐ ADSL-DMT - Asymmetric DSL Discrete Multi-Tone
- ☐ Async (Modem)
- ☐ Cable

Setting	Value
Extensible Authentication Protocol Configuration	Configured
Extended State	<Blank>
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
NAS Port Type	Ethernet
Authentication Method	EAP
NAP Enforcement	Allow full network access
Update Noncompliant Clients	False
Service-Type	Framed
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes

Under NAS Port Type under the “Constraints” tab is where you’re going to tell NPS why media, and authentication protocol is going to be used with this policy. Notice the wireless option. This is the only difference between the Wired and Wireless policies.



Console Root
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Event Viewer (Local)
Certificates (Local Computer)
Local Users and Groups (Local)

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
UPS Radius	Enabled	1	Grant Access	Unspecified
Radius	Enabled	2	Grant Access	Unspecified
Wireless Users	Enabled	3	Grant Access	Unspecified
Wired 802.1x Auth	Enabled	4	Grant Access	Unspecified
VOIP 802.1x Auth				
Connections to Microsoft Rou				
Connections to other access s				

Wired 802.1x Auth

Conditions - If the following cor

Condition	Value
Windows Groups	MEDPAC\

Wired 802.1x Auth Properties

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

Settings:

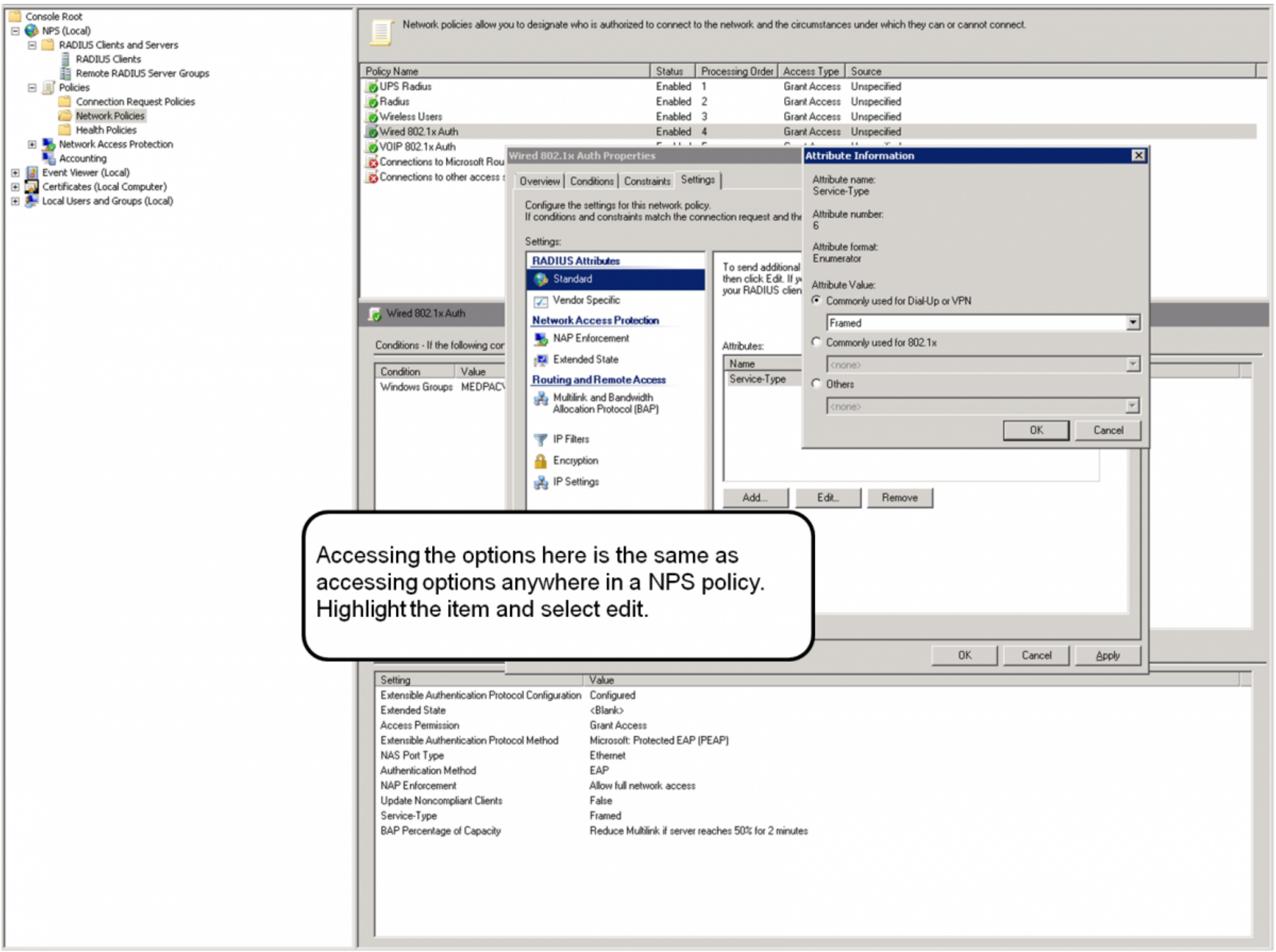
To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Service-Type	Framed

Extensible Authentication Protocol Configuration	Configured
Extended State	<Blank>
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
NAS Port Type	Ethernet
Authentication Method	EAP
NAP Enforcement	Allow full network access
Update Noncompliant Clients	False
Service-Type	Framed
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes

In the settings tab, under the "RADIUS Attributes" field you need to ensure that the only attribute that's defined is "Service-Type Framed"


Console Root
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Event Viewer (Local)
Certificates (Local Computer)
Local Users and Groups (Local)

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
UPS Radius	Enabled	1	Grant Access	Unspecified
Radius	Enabled	2	Grant Access	Unspecified
Wireless Users	Enabled	3	Grant Access	Unspecified
Wired 802.1x Auth	Enabled	4	Grant Access	Unspecified
VOIP 802.1x Auth				
Connections to Microsoft Rou				
Connections to other access s				

Wired 802.1x Auth

Conditions - If the following cor

Condition	Value
Windows Groups	MEDPAC\

Wired 802.1x Auth Properties

Configure the settings for this network policy.
If conditions and constraints match the connection request and the

Settings:

To send additional then click Edit. If y your RADIUS clien

Attributes:

Name
Service-Type

Attribute Information

Attribute name:
Service-Type

Attribute number:
6

Attribute format:
Enumerator

Attribute Value:

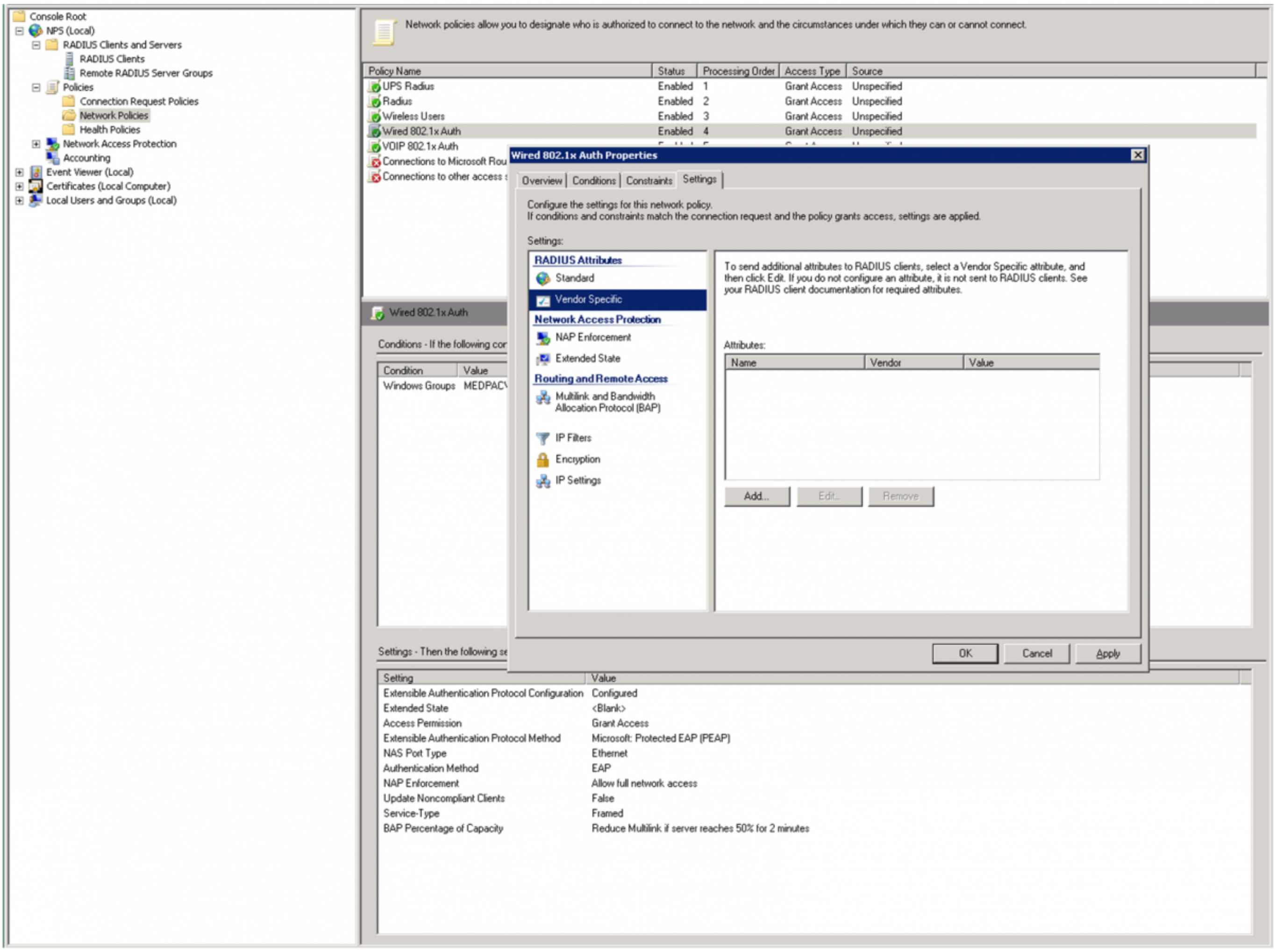
● Commonly used for Dial-Up or VPN
Framed

○ Commonly used for 802.1x
<none>

○ Others
<none>

Accessing the options here is the same as accessing options anywhere in a NPS policy. Highlight the item and select edit.

Setting	Value
Extensible Authentication Protocol Configuration	Configured
Extended State	<Blank>
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
NAS Port Type	Ethernet
Authentication Method	EAP
NAP Enforcement	Allow full network access
Update Noncompliant Clients	False
Service-Type	Framed
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes



Console Root
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Event Viewer (Local)
Certificates (Local Computer)
Local Users and Groups (Local)

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
UPS Radius	Enabled	1	Grant Access	Unspecified
Radius	Enabled	2	Grant Access	Unspecified
Wireless Users	Enabled	3	Grant Access	Unspecified
Wired 802.1x Auth	Enabled	4	Grant Access	Unspecified
VOIP 802.1x Auth				
Connections to Microsoft Rou				
Connections to other access s				

Wired 802.1x Auth

Conditions - If the following cor

Condition	Value
Windows Groups	MEDPAC\

Wired 802.1x Auth Properties

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

Settings:

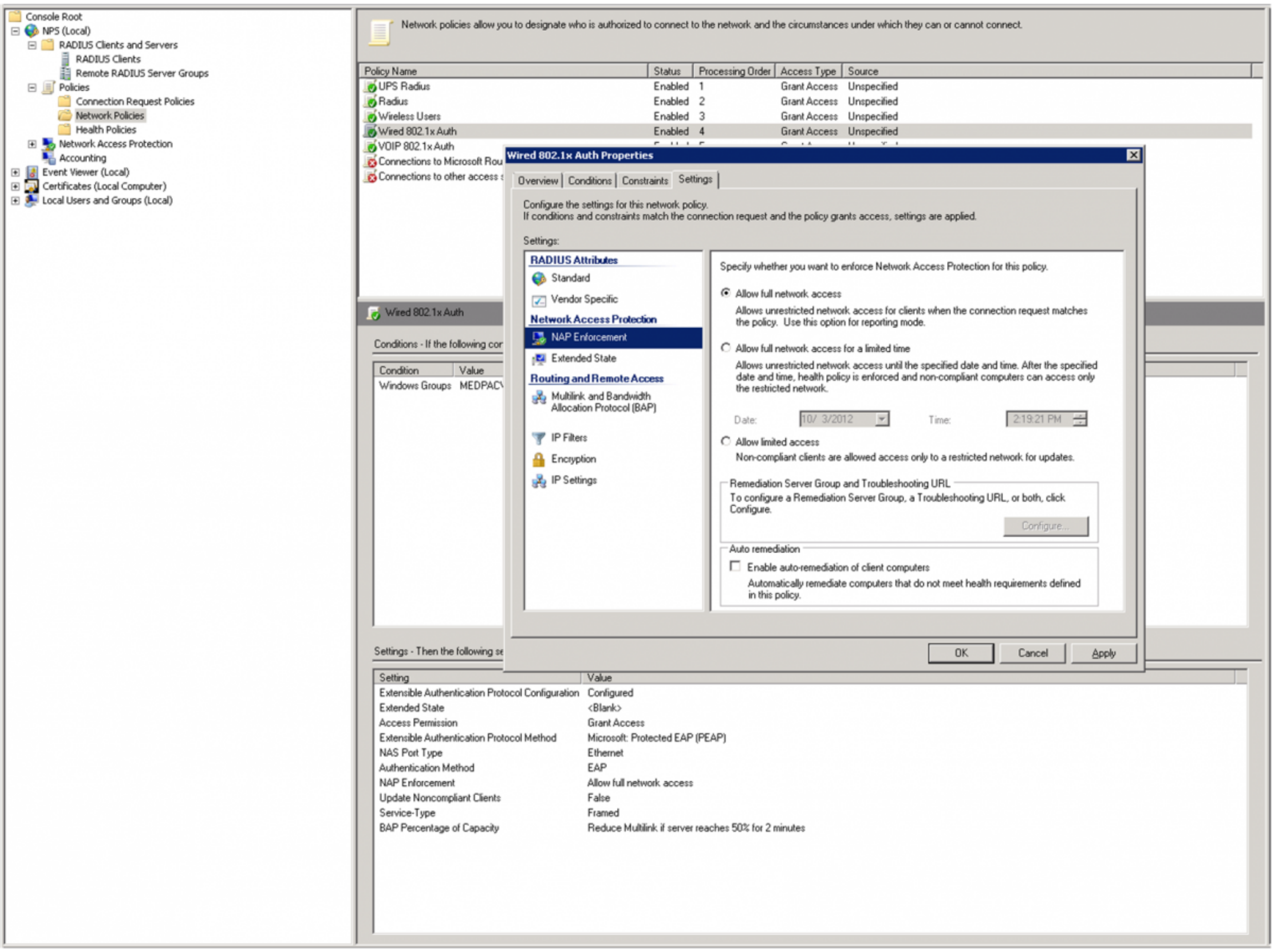
To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Vendor	Value

Settings - Then the following se

Setting	Value
Extensible Authentication Protocol Configuration	Configured
Extended State	<Blank>
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
NAS Port Type	Ethernet
Authentication Method	EAP
NAP Enforcement	Allow full network access
Update Noncompliant Clients	False
Service-Type	Framed
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes


Console Root
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Event Viewer (Local)
Certificates (Local Computer)
Local Users and Groups (Local)

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
UPS Radius	Enabled	1	Grant Access	Unspecified
Radius	Enabled	2	Grant Access	Unspecified
Wireless Users	Enabled	3	Grant Access	Unspecified
Wired 802.1x Auth	Enabled	4	Grant Access	Unspecified
VOIP 802.1x Auth				
Connections to Microsoft Rou				
Connections to other access s				

Wired 802.1x Auth

Conditions - If the following cor

Condition	Value
Windows Groups	MEDPAC\

Settings - Then the following se

Wired 802.1x Auth Properties

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

Settings:

Specify whether you want to enforce Network Access Protection for this policy.

● Allow full network access

Allows unrestricted network access for clients when the connection request matches the policy. Use this option for reporting mode.

○ Allow full network access for a limited time

Allows unrestricted network access until the specified date and time. After the specified date and time, health policy is enforced and non-compliant computers can access only the restricted network.

Date: 10/ 3/2012 Time: 2:19:21 PM

○ Allow limited access

Non-compliant clients are allowed access only to a restricted network for updates.

Remediation Server Group and Troubleshooting URL

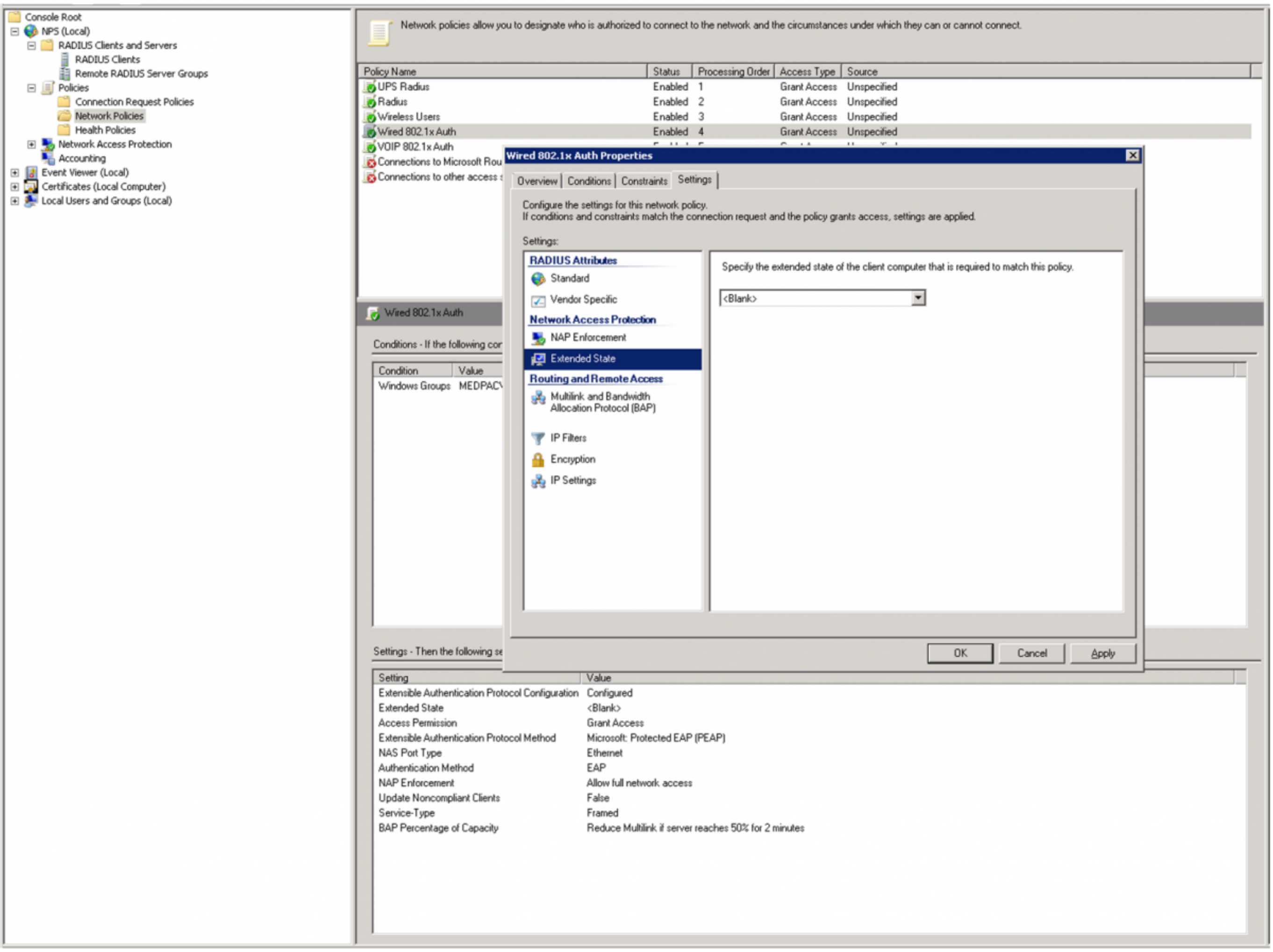
To configure a Remediation Server Group, a Troubleshooting URL, or both, click Configure.

Auto remediation

□ Enable auto-remediation of client computers

Automatically remediate computers that do not meet health requirements defined in this policy.

Setting	Value
Extensible Authentication Protocol Configuration	Configured
Extended State	<Blank>
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
NAS Port Type	Ethernet
Authentication Method	EAP
NAP Enforcement	Allow full network access
Update Noncompliant Clients	False
Service-Type	Framed
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes


Console Root
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Event Viewer (Local)
Certificates (Local Computer)
Local Users and Groups (Local)

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
UPS Radius	Enabled	1	Grant Access	Unspecified
Radius	Enabled	2	Grant Access	Unspecified
Wireless Users	Enabled	3	Grant Access	Unspecified
Wired 802.1x Auth	Enabled	4	Grant Access	Unspecified
VOIP 802.1x Auth				
Connections to Microsoft Rou				
Connections to other access s				

Wired 802.1x Auth Properties

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

Settings:

Specify the extended state of the client computer that is required to match this policy.

<Blank>

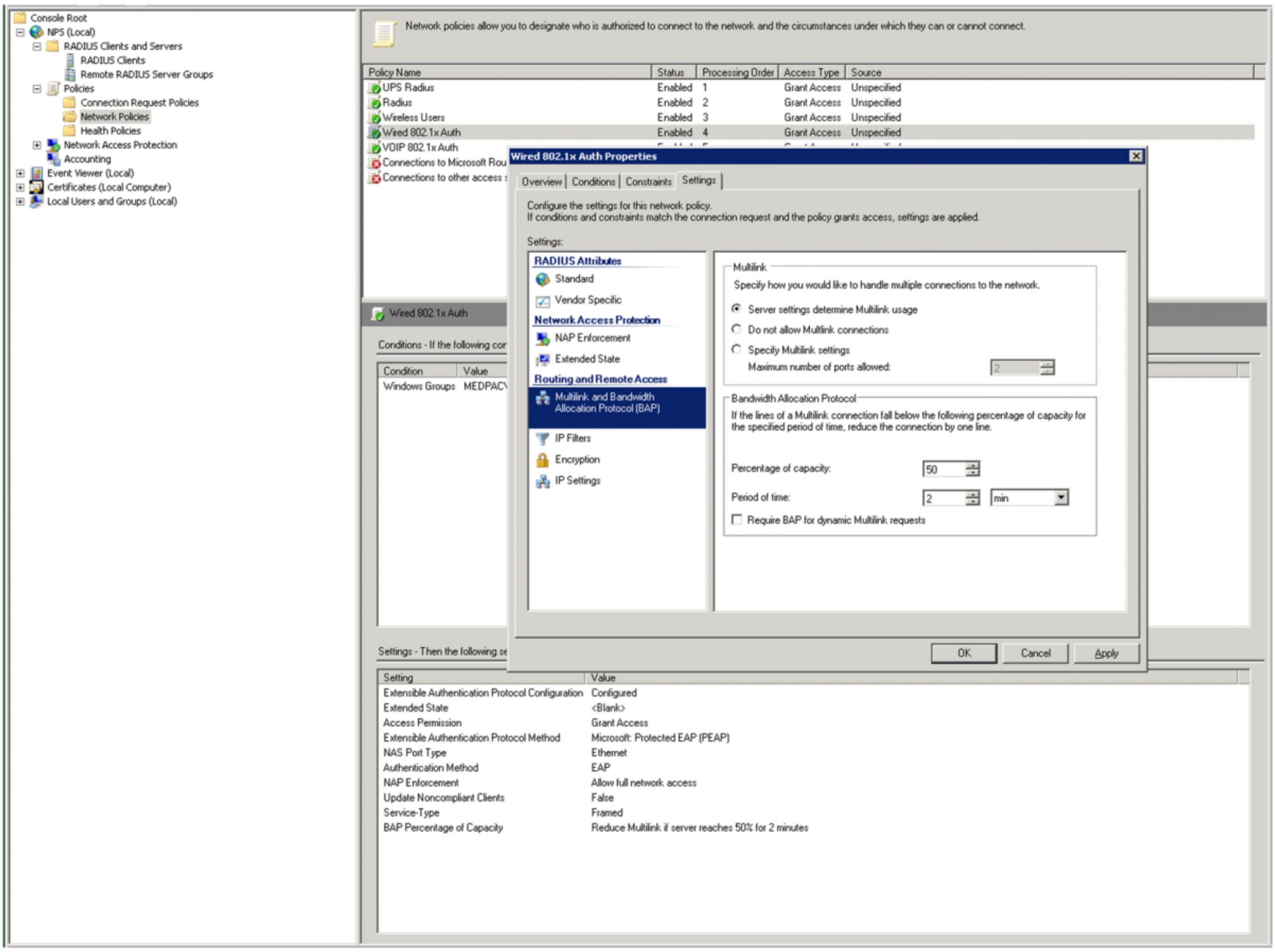
Wired 802.1x Auth

Conditions - If the following cor

Condition	Value
Windows Groups	MEDPAC\

Settings - Then the following se

Setting	Value
Extensible Authentication Protocol Configuration	Configured
Extended State	<Blank>
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
NAS Port Type	Ethernet
Authentication Method	EAP
NAP Enforcement	Allow full network access
Update Noncompliant Clients	False
Service-Type	Framed
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes



Console Root
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Event Viewer (Local)
Certificates (Local Computer)
Local Users and Groups (Local)

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
UPS Radius	Enabled	1	Grant Access	Unspecified
Radius	Enabled	2	Grant Access	Unspecified
Wireless Users	Enabled	3	Grant Access	Unspecified
Wired 802.1x Auth	Enabled	4	Grant Access	Unspecified
VOIP 802.1x Auth				
Connections to Microsoft Rou				
Connections to other access s				

Wired 802.1x Auth

Conditions - If the following cor

Condition	Value
Windows Groups	MEDPAC\

Wired 802.1x Auth Properties

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

Settings:

Multilink

Specify how you would like to handle multiple connections to the network.

● Server settings determine Multilink usage

○ Do not allow Multilink connections

○ Specify Multilink settings

Maximum number of ports allowed: 2

Bandwidth Allocation Protocol

If the lines of a Multilink connection fall below the following percentage of capacity for the specified period of time, reduce the connection by one line.

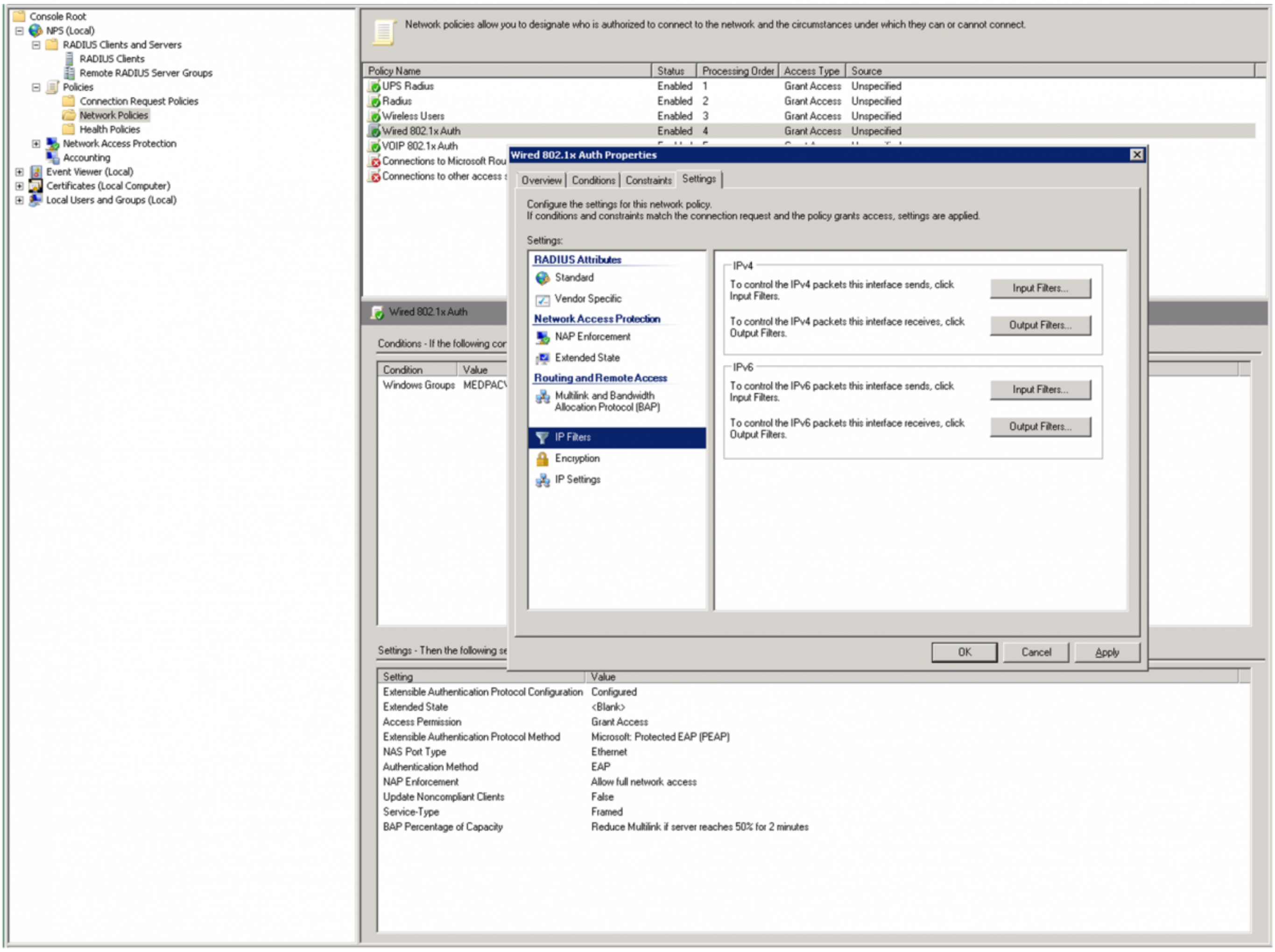
Percentage of capacity: 50

Period of time: 2 min

□ Require BAP for dynamic Multilink requests

Settings - Then the following se

Setting	Value
Extensible Authentication Protocol Configuration	Configured
Extended State	<Blank>
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
NAS Port Type	Ethernet
Authentication Method	EAP
NAP Enforcement	Allow full network access
Update Noncompliant Clients	False
Service-Type	Framed
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes


Console Root
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Event Viewer (Local)
Certificates (Local Computer)
Local Users and Groups (Local)

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
UPS Radius	Enabled	1	Grant Access	Unspecified
Radius	Enabled	2	Grant Access	Unspecified
Wireless Users	Enabled	3	Grant Access	Unspecified
Wired 802.1x Auth	Enabled	4	Grant Access	Unspecified
VOIP 802.1x Auth				
Connections to Microsoft Rou				
Connections to other access s				

Wired 802.1x Auth

Conditions - If the following cor

Condition	Value
Windows Groups	MEDPAC\

Wired 802.1x Auth Properties

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

Settings:

IPv4

To control the IPv4 packets this interface sends, click Input Filters.

To control the IPv4 packets this interface receives, click Output Filters.

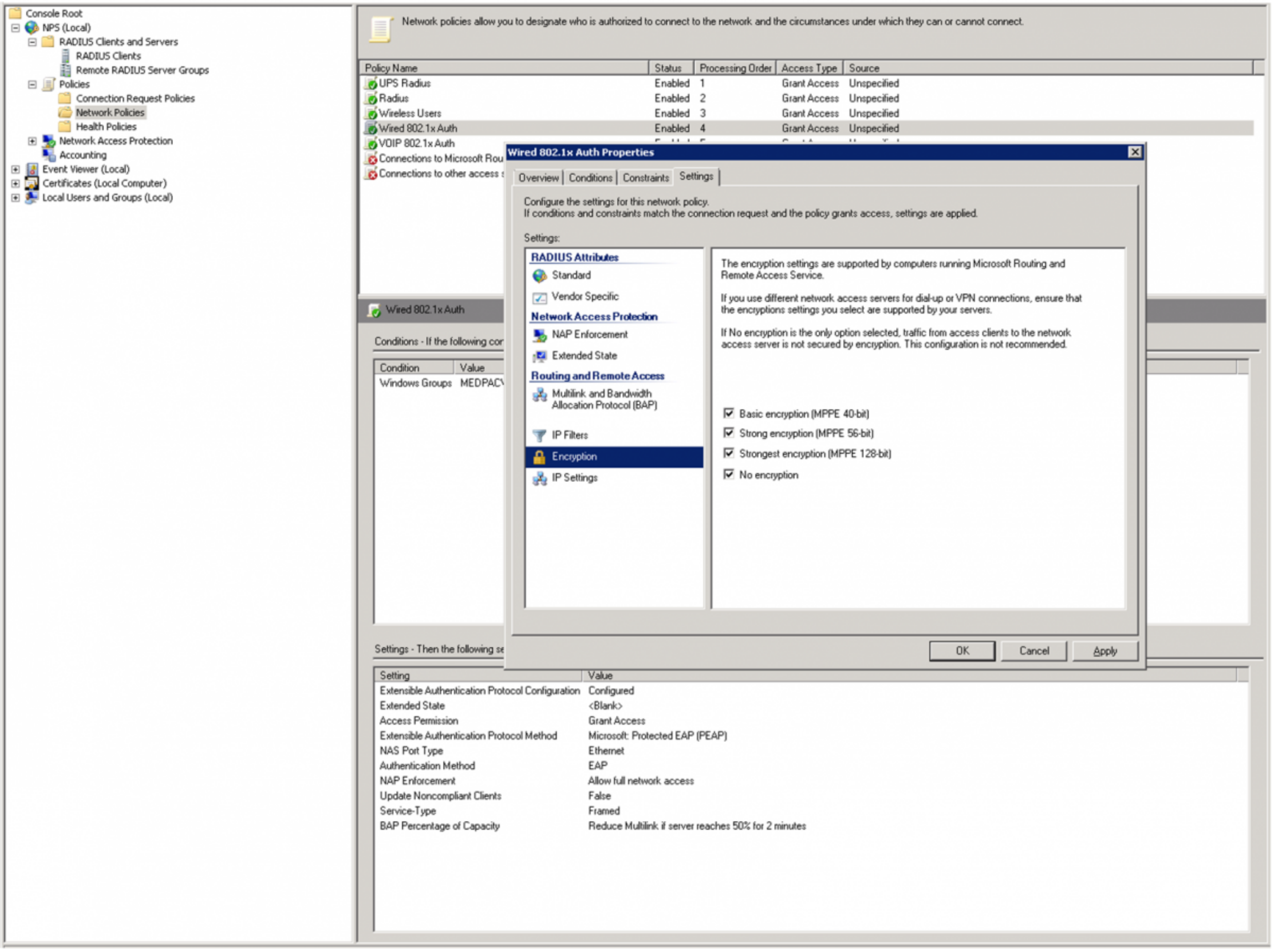
IPv6

To control the IPv6 packets this interface sends, click Input Filters.

To control the IPv6 packets this interface receives, click Output Filters.

Settings - Then the following se

Setting	Value
Extensible Authentication Protocol Configuration	Configured
Extended State	<Blank>
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
NAS Port Type	Ethernet
Authentication Method	EAP
NAP Enforcement	Allow full network access
Update Noncompliant Clients	False
Service-Type	Framed
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes


Console Root
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Event Viewer (Local)
Certificates (Local Computer)
Local Users and Groups (Local)

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
UPS Radius	Enabled	1	Grant Access	Unspecified
Radius	Enabled	2	Grant Access	Unspecified
Wireless Users	Enabled	3	Grant Access	Unspecified
Wired 802.1x Auth	Enabled	4	Grant Access	Unspecified
VOIP 802.1x Auth				
Connections to Microsoft Rou				
Connections to other access s				

Wired 802.1x Auth

Conditions - If the following cor

Condition	Value
Windows Groups	MEDPAC\

Wired 802.1x Auth Properties

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

Settings:

The encryption settings are supported by computers running Microsoft Routing and Remote Access Service.

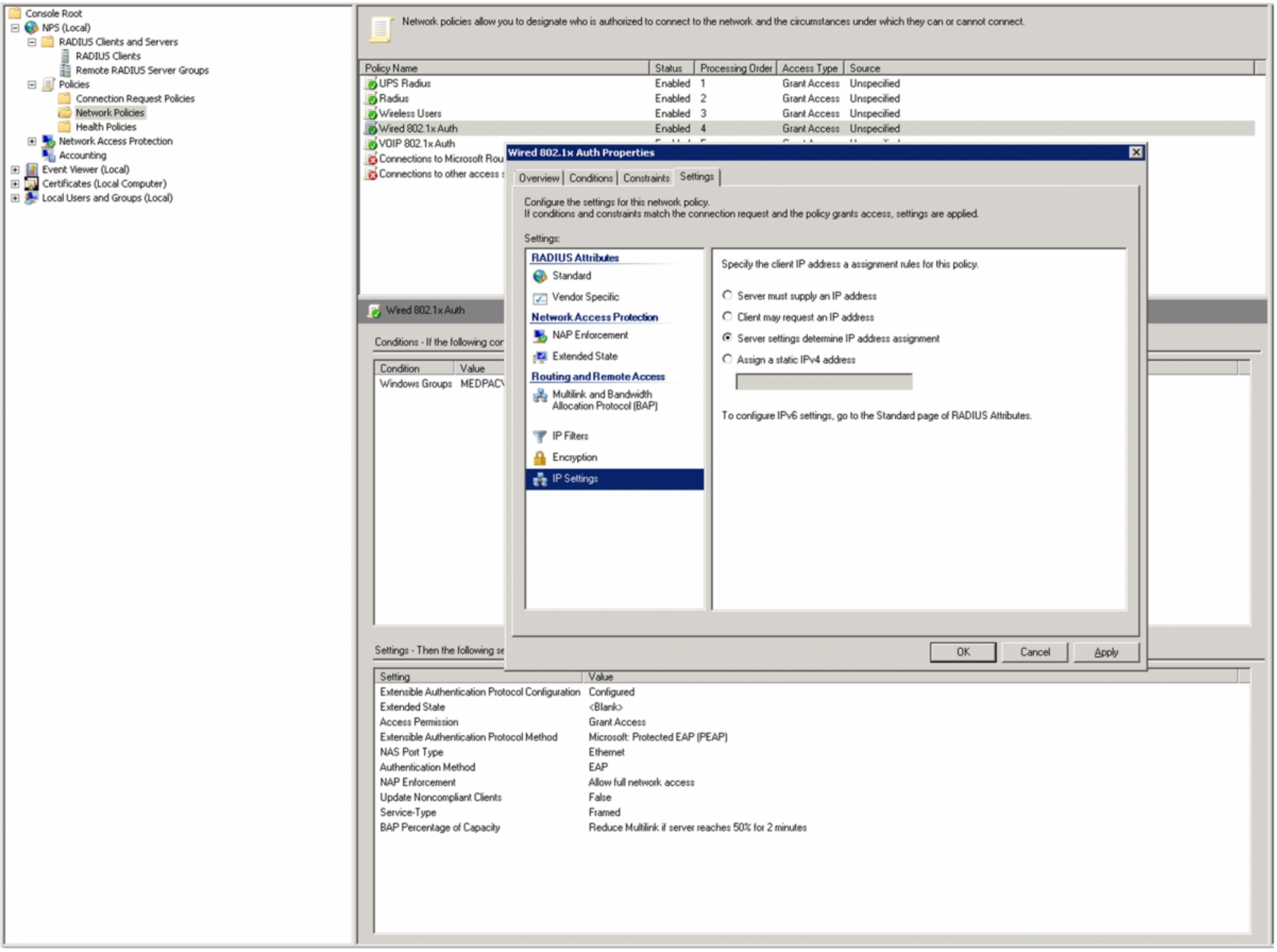
If you use different network access servers for dial-up or VPN connections, ensure that the encryptions settings you select are supported by your servers.

If No encryption is the only option selected, traffic from access clients to the network access server is not secured by encryption. This configuration is not recommended.

☑ Basic encryption (MPPE 40-bit)
☑ Strong encryption (MPPE 56-bit)
☑ Strongest encryption (MPPE 128-bit)
☑ No encryption

Settings - Then the following se

Setting	Value
Extensible Authentication Protocol Configuration	Configured
Extended State	<Blank>
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
NAS Port Type	Ethernet
Authentication Method	EAP
NAP Enforcement	Allow full network access
Update Noncompliant Clients	False
Service-Type	Framed
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes


Console Root
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Event Viewer (Local)
Certificates (Local Computer)
Local Users and Groups (Local)
Wired 802.1x Auth Properties
Overview
Conditions
Constraints
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
OK
Cancel
Apply

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
UPS Radius	Enabled	1	Grant Access	Unspecified
Radius	Enabled	2	Grant Access	Unspecified
Wireless Users	Enabled	3	Grant Access	Unspecified
Wired 802.1x Auth	Enabled	4	Grant Access	Unspecified
VOIP 802.1x Auth				
Connections to Microsoft Rou				
Connections to other access s				

Wired 802.1x Auth

Conditions - If the following cor

Condition	Value
Windows Groups	MEDPAC\

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

Settings:

Specify the client IP address a assignment rules for this policy.

○ Server must supply an IP address
○ Client may request an IP address
● Server settings determine IP address assignment
○ Assign a static IPv4 address

To configure IPv6 settings, go to the Standard page of RADIUS Attributes.

Settings - Then the following se

Setting	Value
Extensible Authentication Protocol Configuration	Configured
Extended State	<Blank>
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
NAS Port Type	Ethernet
Authentication Method	EAP
NAP Enforcement	Allow full network access
Update Noncompliant Clients	False
Service-Type	Framed
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes

Access Layer Switch Configuration

In order to have your access layer devices pass authentication to the RADIUS server you're going to configure Authentication, Authorization, and Accounting, as well as, 802.1x authentication.

aaa new-model	Enables Authentication, Authorization, and Accounting on the switch.
usename XXXXX password XXXXX	Defines a username and password in the event that AAA fails.
dot1x system-auth-control	This command prepares the switch to perform 802.1x authentication.
ip domain-name pac.amed.ds.army.mil	Defines the domain to the switch.
crypto key generate rsa	This is the command and resulting warning that you'll see after you put in the crypto key generate rsa command. I always use 2048 for the modulus, but it's up to you.
The name for the keys will be: NetworkTest.pac.amed.ds.army.mil	

Choose the size of the key modulus in the range of 360 to 2048 for your general purpose keys. Choosing a key modulus greater than 512 may take a few minutes.	
How many bits in the modulus [512]:	
aaa authentication login default group radius group radius	Log in to the switch by bouncing credentials off of the radius server
aaa authentication enable default none	This keeps us from having to enter our password when going to enable mode
aaa authentication dot1x default group radius	This tells the switch to send 802.1x authentication requests to the radius server.
aaa authorization network default group radius	When we enter commands this is the server the switch checks with to ensure our account has the appropriate privileges to execute that command.
aaa accounting exec default start-stop group radius	This assigns and address to a Radius user
aaa accounting network default start-stop group radius	This command tracks Point to Point Protocol Usage
aaa accounting system default start-stop group radius	
authentication mac-move permit	Lets you move a client around on a switch without error disabling an interface.
radius-server host (Ip address of the radius server) key (I use the switches host name)	This is where we tell the switch who the radius server is, and what credentials to use in order to authenticate.
radius-server vsa send accounting	Send vendor specific attributes in regards to accounting
radius-server vsa send authentication	Send vendor specific attributes in regards to authentication (you need this for 802.1x authentication with Cisco Phones)
vlan 802	We need to create this VLAN on your cores and access layer devices for client remediation.
name 802.1x_Un-Auth	
state active	
exit	
Interface	
interface FastEthernet1/0/21	
switchport access vlan 43	
switchport mode access	
switchport voice vlan 112	Defines the VOIP VLAN.
authentication event fail action authorize vlan 802	If you fail authentication the port moves the client to VLAN 802, our remediation VLAN.
authentication event no-response action authorize vlan 802	If the client doesn't respond to an authentication request move the client to VLAN 802.
authentication host-mode multi-domain	This command allows us to have a phone and a pc connected and authenticating off of the same interface.

authentication port-control auto	Automatically determines whether the client is authenticated and authorized on that particular interface.
dot1x pae authenticator	The port proxies authentication messages to NPS, while ignoring authentication messages from NPS to the client.
dot1x timeout quiet-period 30	
dot1x timeout supp-timeout 15	
dot1x max-req 1	
dot1x max-reauth-req 1	This tells the switch how many times to attempt to authenticate the client before it remediates it.
spanning-tree portfast	

Remediation Vlan Access Control List

By far the hardest part about this configuration is going to be writing the access control list. In the event that you place a new client onto the domain after you’ve configured 802.1x authentication you’re going to want to be able to join them to the domain. This access list limits a remediated client to only the ports, protocols, and source and destination addresses that are needed to accomplish this task. I also took into account the fact that once the client is remediated it will need to be able to receive updates from HBSS, WSUS, etc... I've created this access list outbound to our remediation vlan. So each entry in the ACL reads permit traffic from client X over port Y to the remediation subnet.

This is what I've gathered concerning what port and protocol each type of server uses during either logging into a machine on the domain, or simply logging in.

File Servers = TCP 445
Host Based Security servers = TCP 80, TCP 8443, TCP 591, TCP 8530
Wins = TCP, and UDP 137
DHCP server = UDP 67, UDP 137, TCP 445, UDP 138
Primary Domain Controller = TCP and UDP 53, UDP 389, TCP 135, TCP 25010, TCP 88, TCP 389, TCP 445, UDP 123, TCP 3268, TCP 137, TCP 25000
Hawaii Primary DNS = UDP 53, UDP 389, TCP 135, TCP 25010, TCP 88, TCP 389, TCP 445, UDP 123, TCP 3268, TCP 137, TCP 25000
Yongsan SCCM = UDP 137, TCP 445, TCP 443

Here's an example of what I've got configured here. You'll notice that I've got a few stragglers that I've yet to identify with comments, they may be windows update addresses, or things back in San Antonio that the clients check during logon. If anyone has any idea please let me know. This access list may very from site to site, so you may have to put a packet sniffer (WireShark) on a client so that you can get an idea of how you need to tailor your ACL. You'll notice that I haven't blacked the 10.80.20.0/24 subnet out. That's our 802.1x remediation VLAN here. I've got a network address translation statement configured on that VLAN interface so that it can still receive updates from Hawaii even when the client is remediated to that private subnet.

```
access-list 113 remark Ping From Admin Machine
```

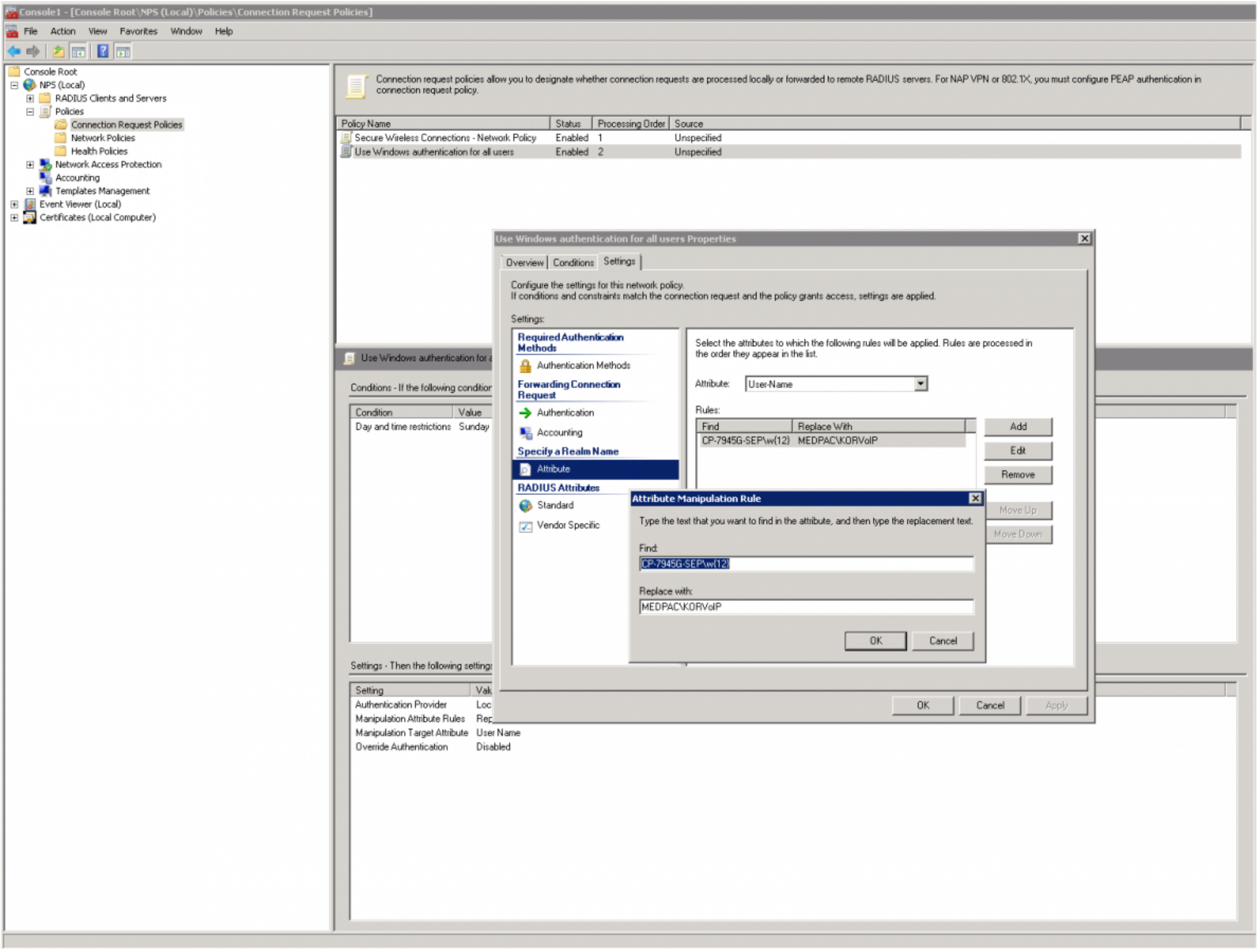
```
   access-list 113 permit icmp host XXX.XXX28.67 10.80.20.0 0.0.0.255
   access-list 113 permit udp host XXX.XXX.107.11 eq 389 10.80.20.0 0.0.0.255
   access-list 113 permit udp host XXX.XXX.107.4 eq 389 10.80.20.0 0.0.0.255
   access-list 113 permit udp host XXX.XXX.107.6 eq 389 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX.113.68 eq 443 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX.167.254 eq www 10.80.20.0
0.0.0.255
   access-list 113 permit tcp host XXX.XXX.212.198 10.80.20.0 0.0.0.255 eq
www
   access-list 113 permit tcp host XXX.XXX.212.210 eq www 10.80.20.0
0.0.0.255
   access-list 113 permit tcp host XXX.XXX.26.4 eq domain 10.80.20.0
0.0.0.255
   access-list 113 permit udp host XXX.XXX.43.15 eq domain 10.80.20.0
0.0.0.255
   access-list 113 permit udp host XXX.XXX.43.15 eq 389 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX.4.119 eq 8005 10.80.20.0 0.0.0.255
   access-list 113 remark Yongsan FS2
   access-list 113 permit tcp host XXX.XXX16.77 eq 445 10.80.20.0 0.0.0.255
   access-list 113 remark Yongsan Primary HBSS
   access-list 113 permit tcp host XXX.XXX25.35 eq www 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX25.35 eq 8443 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX25.35 eq 591 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX25.35 eq 8530 10.80.20.0 0.0.0.255
   access-list 113 remark Yongsan Secondary HBSS
   access-list 113 permit tcp host XXX.XXX25.37 eq www 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX25.37 eq 8443 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX25.37 eq 591 10.80.20.0 0.0.0.255
   access-list 113 remark Primary Wins
   access-list 113 permit udp host XXX.XXX28.10 eq netbios-ns 10.80.20.0
0.0.0.255
   access-list 113 permit tcp host XXX.XXX28.10 eq netbios-ns 10.80.20.0
0.0.0.255
   access-list 113 remark Secondary Wins
   access-list 113 permit udp host XXX.XXX28.11 eq netbios-ns 10.80.20.0
0.0.0.255
   access-list 113 permit tcp host XXX.XXX28.11 eq netbios-ns 10.80.20.0
0.0.0.255
   access-list 113 remark DHCP server
   access-list 113 permit udp host XXX.XXX28.15 eq bootps 10.80.20.0
0.0.0.255
   access-list 113 permit udp host XXX.XXX28.15 eq netbios-ns 10.80.20.0
0.0.0.255
   access-list 113 permit tcp host XXX.XXX28.16 eq 445 10.80.20.0 0.0.0.255
   access-list 113 permit udp host XXX.XXX28.180 eq netbios-dgm 10.80.20.0
0.0.0.255
   access-list 113 remark Primary Domain Controller
   access-list 113 permit tcp host XXX.XXX28.211 eq domain 10.80.20.0
0.0.0.255
   access-list 113 permit udp host XXX.XXX28.211 eq domain 10.80.20.0
0.0.0.255
```

```
   access-list 113 permit udp host XXX.XXX28.211 eq 389 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX28.211 eq 135 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX28.211 eq 25010 10.80.20.0
0.0.0.255
   access-list 113 permit tcp host XXX.XXX28.211 eq 88 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX28.211 eq 389 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX28.211 eq 445 10.80.20.0 0.0.0.255
   access-list 113 permit udp host XXX.XXX28.211 eq ntp 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX28.211 eq 3268 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX28.211 10.80.20.0 0.0.0.255 eq 137
   access-list 113 permit tcp host XXX.XXX28.211 eq 25000 10.80.20.0
0.0.0.255
   access-list 113 remark Secondary Domain Controller
   access-list 113 permit tcp host XXX.XXX28.212 eq domain 10.80.20.0
0.0.0.255
   access-list 113 permit udp host XXX.XXX28.212 eq domain 10.80.20.0
0.0.0.255
   access-list 113 permit udp host XXX.XXX28.212 eq 389 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX28.212 eq 135 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX28.212 eq 25010 10.80.20.0
0.0.0.255
   access-list 113 permit tcp host XXX.XXX28.212 eq 88 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX28.212 eq 389 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX28.212 eq 445 10.80.20.0 0.0.0.255
   access-list 113 permit udp host XXX.XXX28.212 eq ntp 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX28.212 eq 3268 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX28.212 10.80.20.0 0.0.0.255 eq 137
   access-list 113 permit tcp host XXX.XXX28.212 eq 25000 10.80.20.0
0.0.0.255
   access-list 113 remark Hawaii Primary DNS
   access-list 113 permit udp host XXX.XXX81.214 eq domain 10.80.20.0
0.0.0.255
   access-list 113 permit udp host XXX.XXX81.214 eq 389 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX81.214 eq 135 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX81.214 eq 25010 10.80.20.0
0.0.0.255
   access-list 113 permit tcp host XXX.XXX81.214 eq 88 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX81.214 eq 389 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX81.214 eq 445 10.80.20.0 0.0.0.255
   access-list 113 permit udp host XXX.XXX81.214 eq ntp 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX81.214 eq 3268 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX81.214 10.80.20.0 0.0.0.255 eq 137
   access-list 113 permit tcp host XXX.XXX81.214 eq 25000 10.80.20.0
0.0.0.255
   access-list 113 remark Hawaii Secondary DNS
   access-list 113 permit udp host XXX.XXX81.216 eq domain 10.80.20.0
0.0.0.255
   access-list 113 permit udp host XXX.XXX81.216 eq 389 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX81.216 eq 135 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX81.216 eq 25010 10.80.20.0
0.0.0.255
```

```
   access-list 113 permit tcp host XXX.XXX81.216 eq 88 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX81.216 eq 389 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX81.216 eq 445 10.80.20.0 0.0.0.255
   access-list 113 permit udp host XXX.XXX81.216 eq ntp 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX81.216 eq 3268 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX81.216 10.80.20.0 0.0.0.255 eq 137
   access-list 113 permit tcp host XXX.XXX81.216 eq 25000 10.80.20.0
0.0.0.255
   access-list 113 remark Secondary Domain Controller
   access-list 113 permit tcp host XXX.XXX28.212 eq 445 10.80.20.0 0.0.0.255
   access-list 113 remark Yongsan SCCM
   access-list 113 permit udp host XXX.XXX28.238 10.80.20.0 0.0.0.255 eq
netbios-ns
   access-list 113 permit tcp host XXX.XXX28.238 eq 445 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX28.238 eq 443 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX.227.104 eq www 10.80.20.0
0.0.0.255
   access-list 113 permit tcp host XXX.XXX.61.90 eq www 10.80.20.0 0.0.0.255
   access-list 113 permit tcp host XXX.XXX.119.90 eq www 10.80.20.0 0.0.0.255
```

Configuring NPS so that you can authenticate behind a Cisco 7945 using a Service Account to authenticate its self

Once again, you'll need to log into the NPS server open up MMC and add the NPS (Local) snap in to your console. Open your initial connection request policy and go to the “Settings” tab. Under “Settings”, go to “Attribute” under “Specify a Realm Name” next to Attribute: select “User-Name” in the drop down then select add. When you're trying to authenticate using 802.1x on a Cisco 7945 while debugging the connection you'll see that Cisco has hard coded a username into each one of there phones. The beginning of each username for the 7945 begins with “CP-7945G-SEP”. What we're trying to do with this policy is translate the Cisco configured username to the username of a service account you've created in Active Directory.


Console1 - [Console Root\NPS (Local)\Policies\Connection Request Policies]
File Action View Favorites Window Help
Console Root
NPS (Local)
RADIUS Clients and Servers
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Templates Management
Event Viewer (Local)
Certificates (Local Computer)

Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers. For NAP VPN or 802.1X, you must configure PEAP authentication in connection request policy.

Policy Name	Status	Processing Order	Source
Secure Wireless Connections - Network Policy	Enabled	1	Unspecified
Use Windows authentication for all users	Enabled	2	Unspecified

Use Windows authentication for all users Properties

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

Settings:

Select the attributes to which the following rules will be applied. Rules are processed in the order they appear in the list.

Attribute: User-Name

Rules:

Find	Replace With
CP-7945G-SEP\w{12}	MEDPAC\KORVoIP

Attribute Manipulation Rule

Type the text that you want to find in the attribute, and then type the replacement text.

Find: CP-7945G-SEP\w{12}

Replace with: MEDPAC\KORVoIP

Use Windows authentication for a

Conditions - If the following condition

Condition	Value
Day and time restrictions	Sunday

Settings - Then the following settings

Setting	Val
Authentication Provider	Loc
Manipulation Attribute Rules	Rep
Manipulation Target Attribute	User Name
Override Authentication	Disabled

In order to find out what the username is for your particular phone just debug the interface you're performing authentication on with the “debug radius authentication” command. You'll see that the phone offers up its log in name under the “User-Name” field.

```
   Jul  7 23:22:37.609: %LINK-5-CHANGED: Interface FastEthernet1/0/21,
changed state to administratively down
   Jul  7 23:22:38.616: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet1/0/21, changed state to down
   Jul  7 23:22:41.736: %ILPOWER-7-DETECT: Interface Fa1/0/21: Power Device
detected: IEEE PD
   Jul  7 23:22:41.745: %ILPOWER-5-POWER_GRANTED: Interface Fa1/0/21: Power
granted
   Jul  7 23:22:43.355: %LINK-3-UPDOWN: Interface FastEthernet1/0/21, changed
state to down
   Jul  7 23:22:49.051: %AUTHMGR-5-START: Starting 'dot1x' for client
(24b6.57b0.9982) on Interface Fa1/0/21 AuditSessionID
0A0B10FC000000AE1D9CAF68
   Jul  7 23:22:49.060: %LINK-3-UPDOWN: Interface FastEthernet1/0/21, changed
state to up
   Jul  7 23:22:49.135: RADIUS/ENCODE(000000CF):Orig. component type = DOT1X
   Jul  7 23:22:49.135: RADIUS(000000CF): Config NAS IP: 0.0.0.0
   Jul  7 23:22:49.135: RADIUS/ENCODE(000000CF): acct_session_id: 207
   Jul  7 23:22:49.135: RADIUS(000000CF): sending
   Jul  7 23:22:49.135: RADIUS/ENCODE: Best Local IP-Address 10.11.16.252 for
```

```
Radius-Server 204.208.28.26
   Jul  7 23:22:49.135: RADIUS(000000CF): Send Access-Request to
204.208.28.26:1645 id 1645/20, len 234
   Jul  7 23:22:49.135: RADIUS:  authenticator 80 98 5A AE 58 8D CF 3E - D6
4B E4 28 82 72 6B 19
   Jul  7 23:22:49.135: RADIUS:  User-Name           [1]   26
"CP-7945G-SEP24B657B09982"
   Jul  7 23:22:49.135: RADIUS:  Service-Type        [6]   6   Framed
[2]
   Jul  7 23:22:49.135: RADIUS:  Framed-MTU          [12]  6   1500
   Jul  7 23:22:49.135: RADIUS:  Called-Station-Id   [30]  19
"EC-30-91-BE-58-97"
   Jul  7 23:22:49.135: RADIUS:  Calling-Station-Id  [31]  19
"24-B6-57-B0-99-82"
   Jul  7 23:22:49.135: RADIUS:  EAP-Message         [79]  31
   Jul  7 23:22:49.144: RADIUS:   02 01 00 1D 01 43 50 2D 37 39 34 35 47 2D
53 45 50 32 34 42 36  [CP-7945G-SEP24B6]
   Jul  7 23:22:49.144: RADIUS:   35 37 42 30 39 39 38 32          [ 57B09982]
   Jul  7 23:22:49.144: RADIUS:  Message-Authenticato[80]  18
   Jul  7 23:22:49.144: RADIUS:   5E 92 42 6F 2F 31 C1 18 57 FD 1F B8 5F B1
2B 7D         [ ^Bo/1W_+}]
   Jul  7 23:22:49.144: RADIUS:  EAP-Key-Name        [102] 2   *
   Jul  7 23:22:49.144: RADIUS:  Vendor, Cisco       [26]  49
   Jul  7 23:22:49.144: RADIUS:   Cisco AVpair       [1]   43
"audit-session-id=0A0B10FC000000AE1D9CAF68"
   Jul  7 23:22:49.144: RADIUS:  NAS-Port-Type       [61]  6   Ethernet
[15]
   Jul  7 23:22:49.144: RADIUS:  NAS-Port            [5]   6   50121
   Jul  7 23:22:49.144: RADIUS:  NAS-Port-Id         [87]  20
"FastEthernet1/0/21"
   Jul  7 23:22:49.144: RADIUS:  NAS-IP-Address      [4]   6   10.11.16.252
   Jul  7 23:22:49.144: RADIUS(000000CF): Started 5 sec timeout
   Jul  7 23:22:49.152: RADIUS: Received from id 1645/20 204.208.28.26:1645,
Access-Challenge, len 118
   Jul  7 23:22:49.152: RADIUS:  authenticator B0 B2 A6 75 7C A6 A1 9C - 30
7C CB 50 17 78 6F 3B
   Jul  7 23:22:49.152: RADIUS:  Session-Timeout     [27]  6   60
   Jul  7 23:22:49.152: RADIUS:  EAP-Message         [79]  36
   Jul  7 23:22:49.152: RADIUS:   01 02 00 22 04 10 C4 E4 9E 71 C6 69 67 F3
58 11 5A 57 F2 69 CD 01 41 4D 45 44 4E 4D 4D 45  ["qigXZWiAMEDNMME]
   Jul  7 23:22:49.152: RADIUS:   44 4B 30 32              [ DK02]
   Jul  7 23:22:49.152: RADIUS:  State               [24]  38
```

Configuring NPS and the Cisco 7945 so that

the phone can Perform 802.1x Authentication

Once you're in front of the phone, you'll click the settings button then go to “Security Configuration” > “802.1X Authentication”. Once you're in the 802.1X Authentication screen you're going to select the “Device Authentication” option select “Enable” then exit. Then go to the “EAP-MD5” option and configure the “Shared Secret”, which is going to be the password for your service account. This configuration won't prevent the phone from associating its self on a non-802.1x capable port. If the interface is configured with the voice VLAN the phone will still associate its self to the controller. The only thing that this configuration does is once the phone is connected to a 802.1x capable port it will provide credentials to authenticate with.

You're also going to need to configure NPS to authenticate the phone. In server 2008 they removed the EAP-MD5 option so we have to go into the registry and re-enable it. So log into your NPS machine and open up “regedit.” Once the window opens you're going to go to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\EAP folder and create a folder called 4. Do that by right clicking the EAP folder and select “New”, then “Key”. Once that folder's created you're going to want to create the following options…

Value name: RolesSupported
Value type: REG_DWORD
Value data: 0000000a

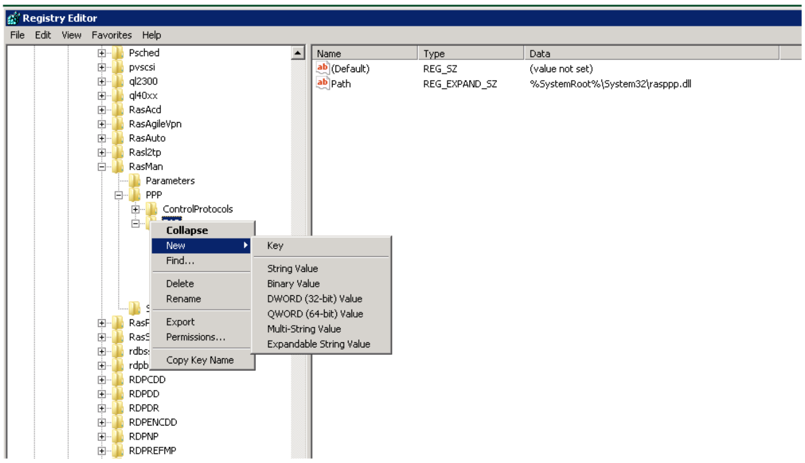
Value name: FriendlyName
Value type: REG_SZ
Value data: MD5-Challenge

Value name: Path
Value type: REG_EXPAND_SZ
Value data: %SystemRoot%\System32\Raschap.dll

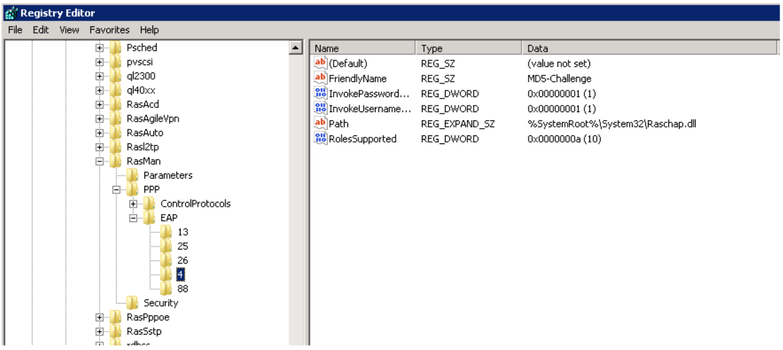
Value name: InvokeUsernameDialog
Value type: REG_DWORD
Value data: 00000001

Value name: InvokePasswordDialog
Value type: REG_DWORD
Value data: 00000001

Here's what you're going to see as you're creating the folder called 4 and the resulting registry settings…

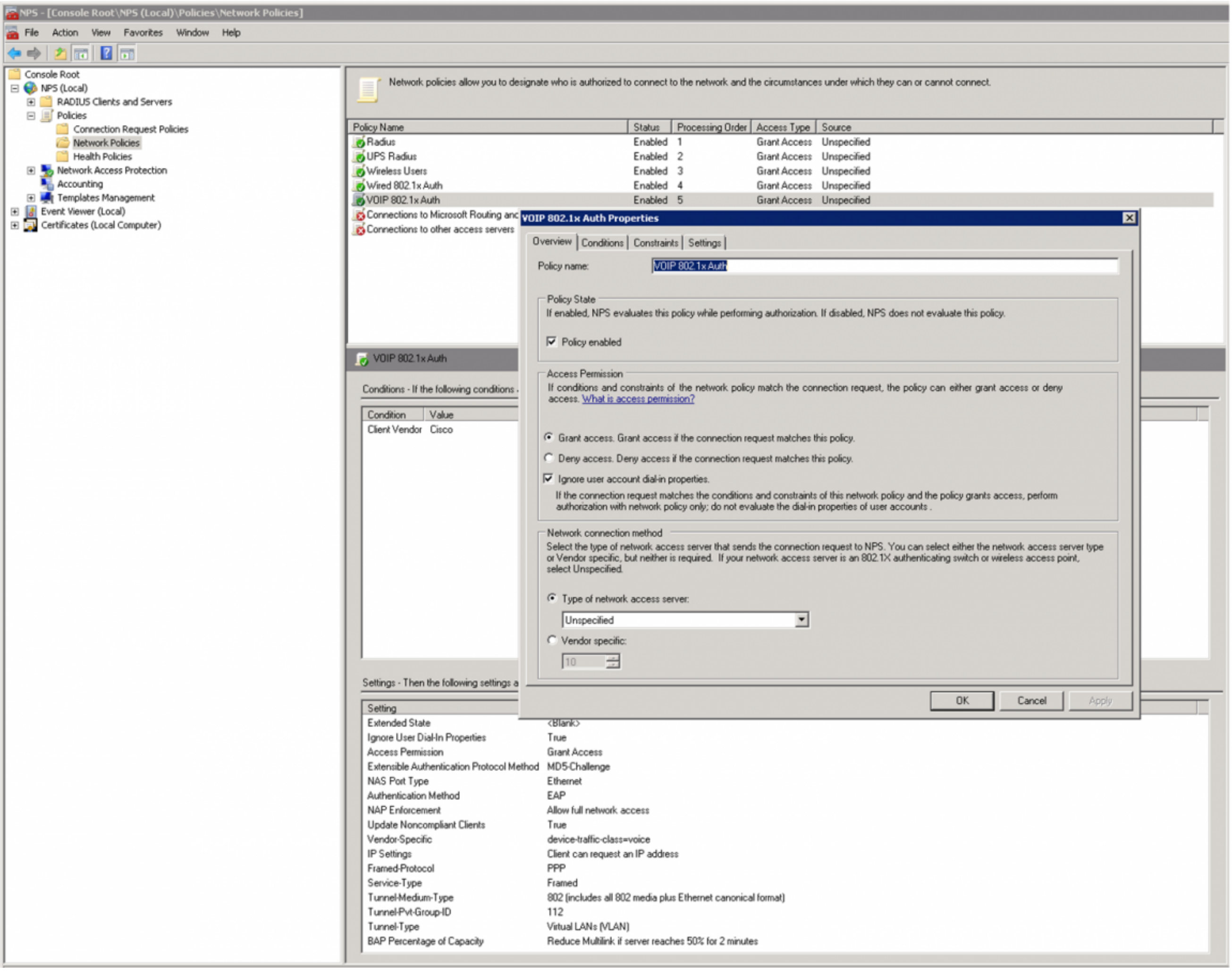


Name	Type	Data
(Default)	REG_SZ	(value not set)
Path	REG_EXPAND_SZ	%SystemRoot%\System32\rasppp.dll



Name	Type	Data
(Default)	REG_SZ	(value not set)
FriendlyName	REG_SZ	MD5-Challenge
InvokePassword...	REG_DWORD	0x00000001 (1)
InvokeUsername...	REG_DWORD	0x00000001 (1)
Path	REG_EXPAND_SZ	%SystemRoot%\System32\Raschap.dll
RolesSupported	REG_DWORD	0x0000000a (10)

Now you're going to create the network policy that your phone is going to authenticate against. Any of the slides that I haven't taken screen shots of are going to be the same as the policy you created earlier in order to authenticate the PC.



NPS - [Console Root\NPS (Local)\Policies\Network Policies]
File
Action
View
Favorites
Window
Help
Console Root
NPS (Local)
RADIUS Clients and Servers
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Templates Management
Event Viewer (Local)
Certificates (Local Computer)

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
Radius	Enabled	1	Grant Access	Unspecified
UPS Radius	Enabled	2	Grant Access	Unspecified
Wireless Users	Enabled	3	Grant Access	Unspecified
Wired 802.1x Auth	Enabled	4	Grant Access	Unspecified
VOIP 802.1x Auth	Enabled	5	Grant Access	Unspecified
Connections to Microsoft Routing anc				
Connections to other access servers				

VOIP 802.1x Auth

Conditions - If the following conditions

Condition	Value
Client Vendor	Cisco

Settings - Then the following settings a

Setting	
Extended State	<Blank>
Ignore User Dial-In Properties	True
Access Permission	Grant Access
Extensible Authentication Protocol Method	MD5-Challenge
NAS Port Type	Ethernet
Authentication Method	EAP
NAP Enforcement	Allow full network access
Update Noncompliant Clients	True
Vendor-Specific	device-traffic-class=voice
IP Settings	Client can request an IP address
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID	112
Tunnel-Type	Virtual LANs (VLAN)
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes

VOIP 802.1x Auth Properties

Policy name: VOIP 802.1x Auth

Policy State

If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

☑ Policy enabled

Access Permission

If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. What is access permission?

● Grant access. Grant access if the connection request matches this policy.

○ Deny access. Deny access if the connection request matches this policy.

☑ Ignore user account dial-in properties.

If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts .

Network connection method

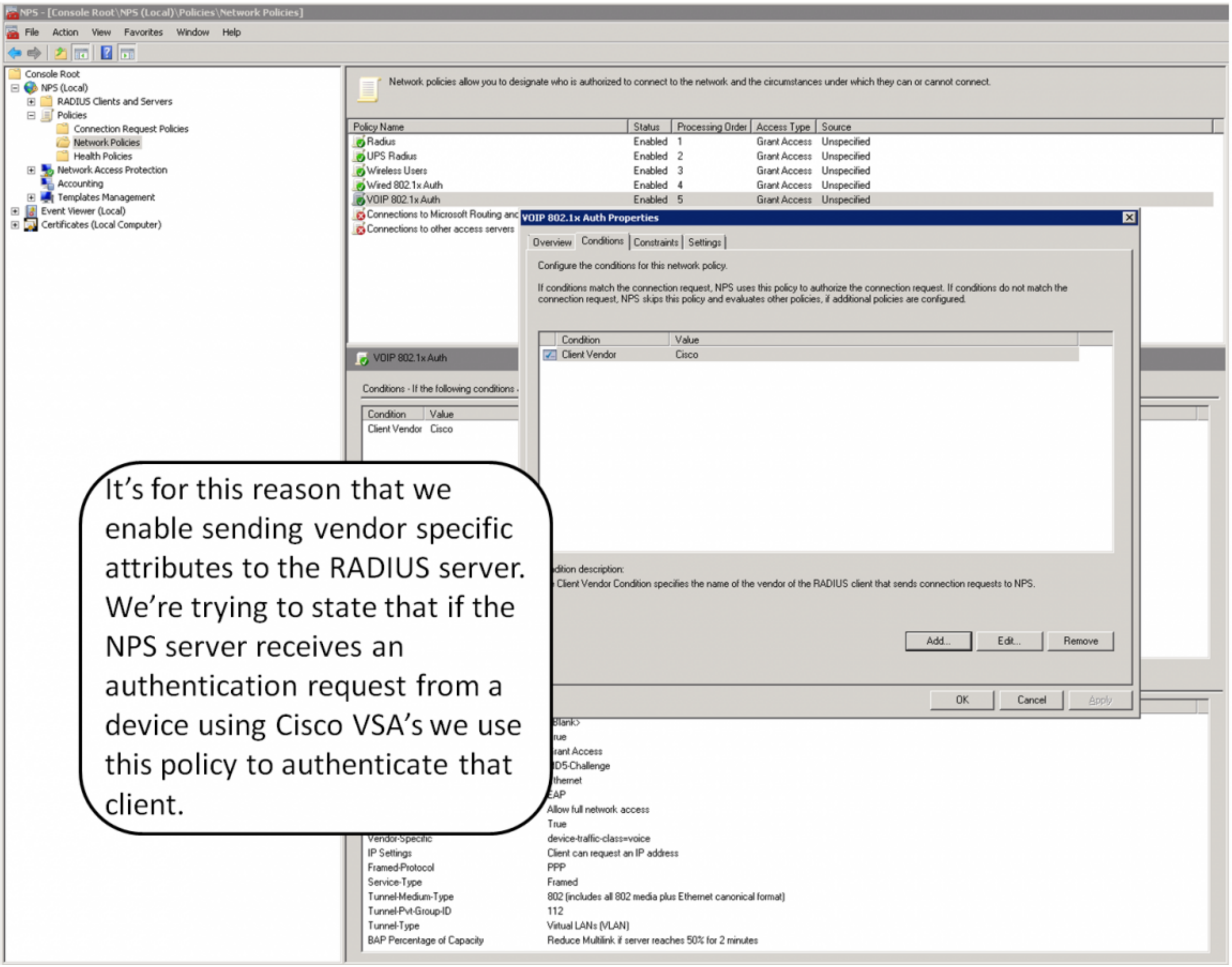
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

● Type of network access server:

Unspecified

○ Vendor specific:

10


NPS - [Console Root\NPS (Local)\Policies\Network Policies]
File
Action
View
Favorites
Window
Help
Console Root
NPS (Local)
RADIUS Clients and Servers
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Templates Management
Event Viewer (Local)
Certificates (Local Computer)

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
Radius	Enabled	1	Grant Access	Unspecified
UPS Radius	Enabled	2	Grant Access	Unspecified
Wireless Users	Enabled	3	Grant Access	Unspecified
Wired 802.1x Auth	Enabled	4	Grant Access	Unspecified
VOIP 802.1x Auth	Enabled	5	Grant Access	Unspecified
Connections to Microsoft Routing anc				
Connections to other access servers				

VOIP 802.1x Auth

Conditions - If the following conditions

Condition	Value
Client Vendor	Cisco

	Blank>
	rue
	rant Access
	D5-Challenge
	thernet
	EAP
	Allow full network access
	True
Vendor-Specific	device-traffic-class=voice
IP Settings	Client can request an IP address
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID	112
Tunnel-Type	Virtual LANs (VLAN)
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes

VOIP 802.1x Auth Properties

Configure the conditions for this network policy.

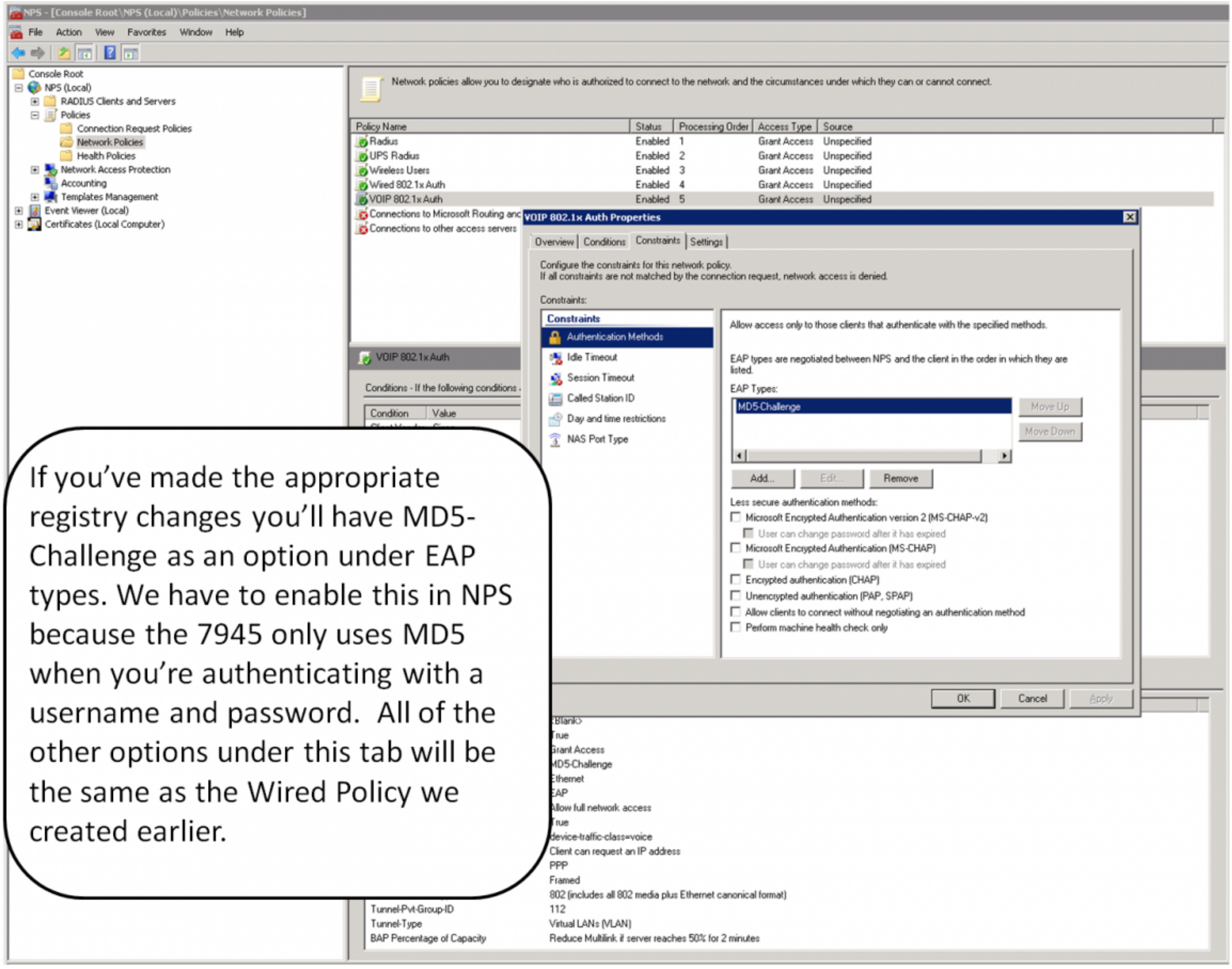
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

	Condition	Value
☑	Client Vendor	Cisco

dition description:

Client Vendor Condition specifies the name of the vendor of the RADIUS client that sends connection requests to NPS.

It's for this reason that we enable sending vendor specific attributes to the RADIUS server. We're trying to state that if the NPS server receives an authentication request from a device using Cisco VSA's we use this policy to authenticate that client.



Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
Radius	Enabled	1	Grant Access	Unspecified
UPS Radius	Enabled	2	Grant Access	Unspecified
Wireless Users	Enabled	3	Grant Access	Unspecified
Wired 802.1x Auth	Enabled	4	Grant Access	Unspecified
VOIP 802.1x Auth	Enabled	5	Grant Access	Unspecified
Connections to Microsoft Routing anc				
Connections to other access servers				

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

Constraints:

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:
MD5-Challenge

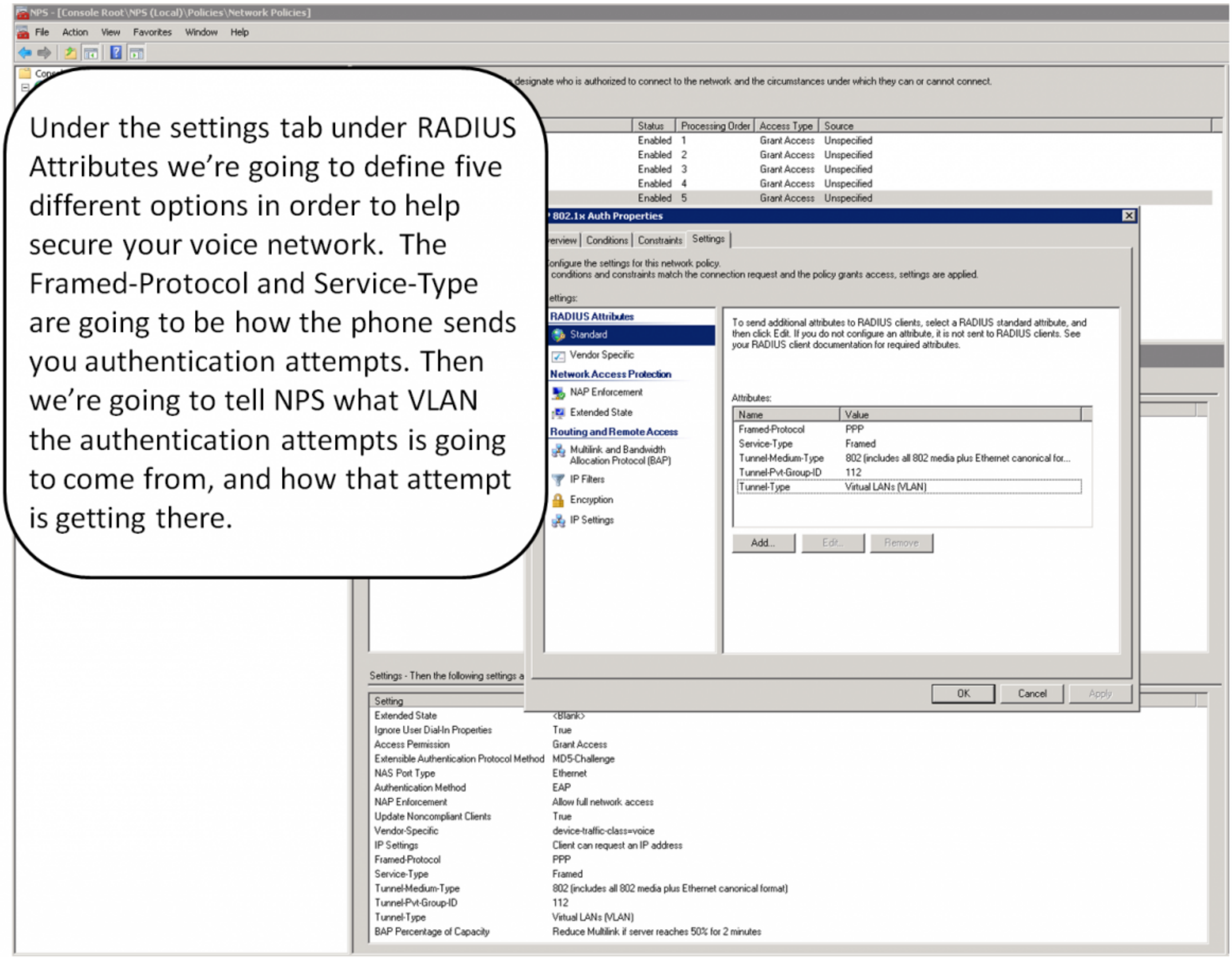
Less secure authentication methods:
- □ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
  - □ User can change password after it has expired
- □ Microsoft Encrypted Authentication (MS-CHAP)
  - □ User can change password after it has expired
- □ Encrypted authentication (CHAP)
- □ Unencrypted authentication (PAP, SPAP)
- □ Allow clients to connect without negotiating an authentication method
- □ Perform machine health check only

Conditions - If the following conditions

<Blank>
True
Grant Access
MD5-Challenge
Ethernet
EAP
Allow full network access
True
device-traffic-class=voice
Client can request an IP address
PPP
Framed
802 (includes all 802 media plus Ethernet canonical format)

Tunnel-Pvt-Group-ID	112
Tunnel-Type	Virtual LANs (VLAN)
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes

If you've made the appropriate registry changes you'll have MD5-Challenge as an option under EAP types. We have to enable this in NPS because the 7945 only uses MD5 when you're authenticating with a username and password. All of the other options under this tab will be the same as the Wired Policy we created earlier.



Under the settings tab under RADIUS Attributes we’re going to define five different options in order to help secure your voice network. The Framed-Protocol and Service-Type are going to be how the phone sends you authentication attempts. Then we’re going to tell NPS what VLAN the authentication attempts is going to come from, and how that attempt is getting there.

designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Status	Processing Order	Access Type	Source
Enabled	1	Grant Access	Unspecified
Enabled	2	Grant Access	Unspecified
Enabled	3	Grant Access	Unspecified
Enabled	4	Grant Access	Unspecified
Enabled	5	Grant Access	Unspecified

802.1x Auth Properties

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

ettings:

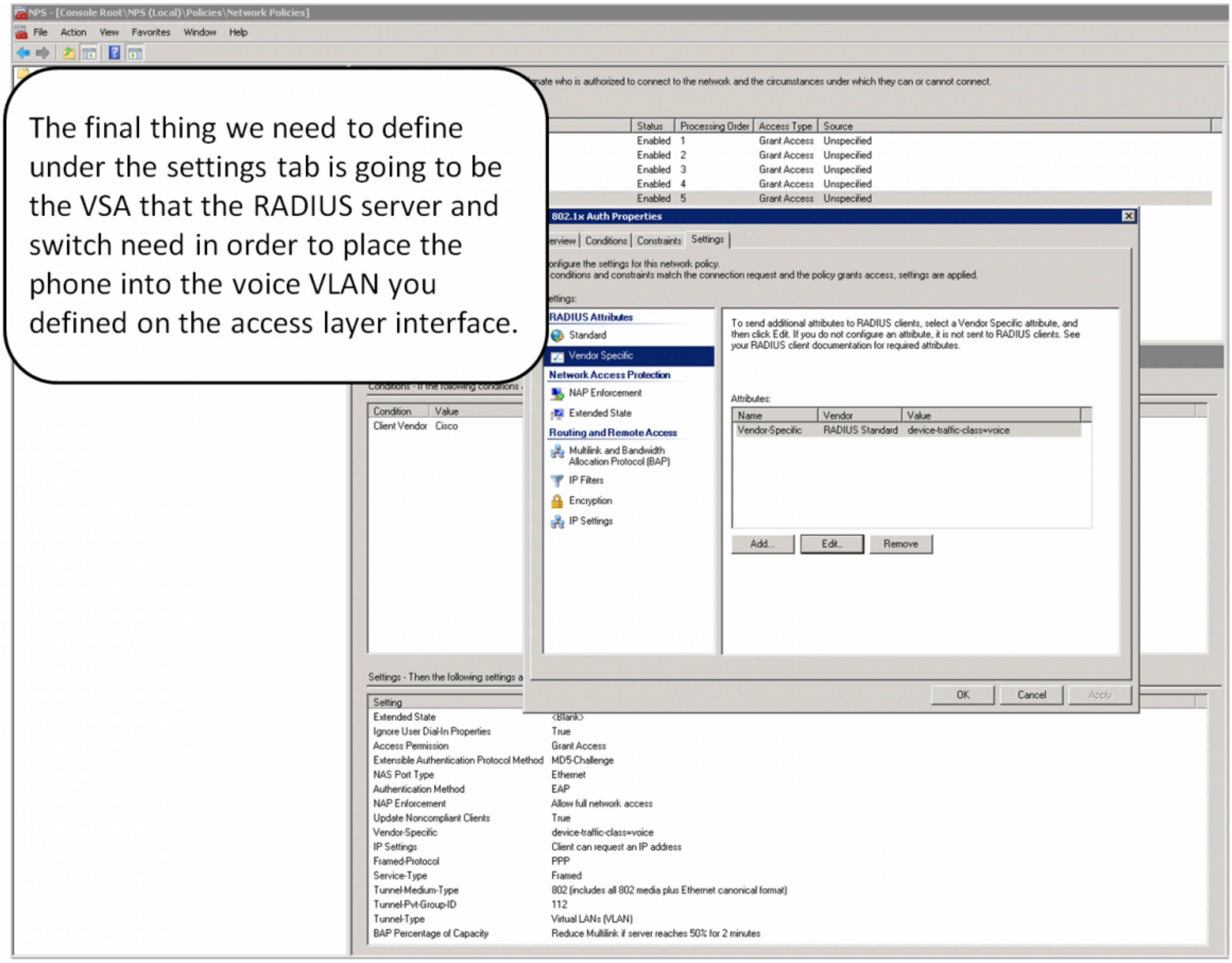
To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID	112
Tunnel-Type	Virtual LANs (VLAN)

Settings - Then the following settings a

Setting	
Extended State	<Blank>
Ignore User Dial-In Properties	True
Access Permission	Grant Access
Extensible Authentication Protocol Method	MD5-Challenge
NAS Port Type	Ethernet
Authentication Method	EAP
NAP Enforcement	Allow full network access
Update Noncompliant Clients	True
Vendor-Specific	device-traffic-class=voice
IP Settings	Client can request an IP address
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID	112
Tunnel-Type	Virtual LANs (VLAN)
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes



NPS - [Console Root\NPS (Local)\Policies\Network Policies]
File Action View Favorites Window Help
802.1x Auth Properties
erview | Conditions | Constraints | 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
Add... Edit... Remove
OK Cancel Apply

The final thing we need to define under the settings tab is going to be the VSA that the RADIUS server and switch need in order to place the phone into the voice VLAN you defined on the access layer interface.

ate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Status	Processing Order	Access Type	Source
Enabled	1	Grant Access	Unspecified
Enabled	2	Grant Access	Unspecified
Enabled	3	Grant Access	Unspecified
Enabled	4	Grant Access	Unspecified
Enabled	5	Grant Access	Unspecified

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

ettings:

To send additional attributes to RADIUS clients, select a Vendor Specific 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	Vendor	Value
Vendor-Specific	RADIUS Standard	device-traffic-class=voice

Conditions - If the following conditions

Condition	Value
Client Vendor	Cisco

Settings - Then the following settings a

Setting	
Extended State	<Blank>
Ignore User Dial-In Properties	True
Access Permission	Grant Access
Extensible Authentication Protocol Method	MD5-Challenge
NAS Port Type	Ethernet
Authentication Method	EAP
NAP Enforcement	Allow full network access
Update Noncompliant Clients	True
Vendor-Specific	device-traffic-class=voice
IP Settings	Client can request an IP address
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID	112
Tunnel-Type	Virtual LANs (VLAN)
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes

Implementation and Troubleshooting

During initial configuration you're going to want to ensure that you can log on with with client before you do anything. The best source for information regarding what's going on in the client is the “debug radius authentication” command on the switch. If you're not seeing anything in your debug your client isn't configured correctly. Another helpful command is going to be “show authentication session interface (interface #)” command. As you can see, my computer is in the “DATA” domain which is the VLAN I assigned that interface to. You can also see that my phone is in the “VOICE” domain and it sits in the voice VLAN I defined during the interface configuration. If the interface isn't assigning the switch or the phone to the appropriate VLAN chances are you've missed one of the AAA commands or you've misconfigured the VOIP policy in NPS.

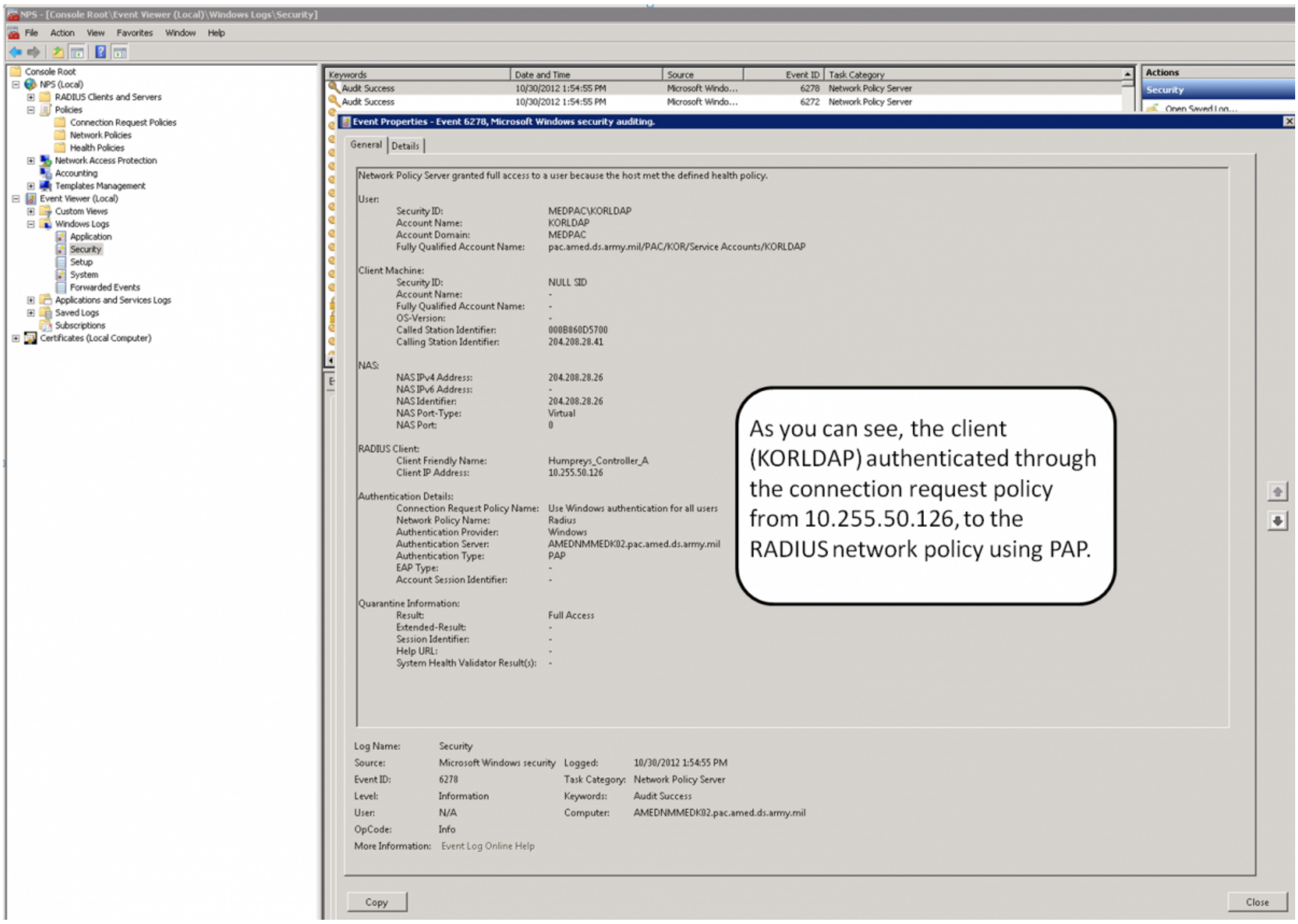
```
YONG-5259-SWX1-MBYV#sh authentication sessions int g 1/0/15
            Interface:  GigabitEthernet1/0/15
          MAC Address:  0021.9b4a.bc3c
           IP Address:  Unknown
            User-Name:  1242356183@mil
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
```

```
          Oper host mode:  multi-domain
        Oper control dir:  both
           Authorized By:  Authentication Server
              Vlan Group:  N/A
         Session timeout:  N/A
            Idle timeout:  N/A
       Common Session ID:  0A0B10640000009343E76955
         Acct Session ID:  0x000001F1
                  Handle:  0x8E000093
   Runnable methods list:
          Method   State
          dot1x    Authc Success
   ----------------------------------------
               Interface:  GigabitEthernet1/0/15
             MAC Address:  9caf.ca85.4dce
              IP Address:  Unknown
               User-Name:  CP-7945G-SEP9CAFCA854DCE
                  Status:  Authz Success
                  Domain:  VOICE
         Security Policy:  Should Secure
         Security Status:  Unsecure
          Oper host mode:  multi-domain
        Oper control dir:  both
           Authorized By:  Authentication Server
             Vlan Policy:  112
         Session timeout:  N/A
            Idle timeout:  N/A
       Common Session ID:  0A0B106400000015000F177A
         Acct Session ID:  0x00000018
                  Handle:  0x62000015
   Runnable methods list:
          Method   State
          dot1x    Authc Success
```

Afterwards you're going to want to look at the security logs in NPS. To have the authentication attempt logs sent to security logs in either the client or the NPS server open up a command prompt as an administrator and run the following command....

```
   Enable auditing: auditpol /set /subcategory:"Network Policy Server"
/success:enable /failure:enable
```

This is incredibly helpful when you're trying to see why a particular authentication attempt has failed. This log will give you an idea of where authentication is failing, and what's causing authentication to fail.


NPS - [Console Root\Event Viewer (Local)\Windows Logs\Security]
File Action View Favorites Window Help
Console Root
NPS (Local)
RADIUS Clients and Servers
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Templates Management
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Logs
Saved Logs
Subscriptions
Certificates (Local Computer)
Actions
Security
Open Saved Log...
Event Properties - Event 6278, Microsoft Windows security auditing.
General
Details
Copy
Close

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	10/30/2012 1:54:55 PM	Microsoft Windo...	6278	Network Policy Server
Audit Success	10/30/2012 1:54:55 PM	Microsoft Windo...	6272	Network Policy Server

```
Network Policy Server granted full access to a user because the host met the defined health policy.

User:
        Security ID:                        MEDPAC\KORLDAP
        Account Name:                       KORLDAP
        Account Domain:                     MEDPAC
        Fully Qualified Account Name:       pac.amed.ds.army.mil/PAC/KOR/Service Accounts/KORLDAP

Client Machine:
        Security ID:                        NULL SID
        Account Name:                       -
        Fully Qualified Account Name:       -
        OS-Version:                         -
        Called Station Identifier:          000B860D5700
        Calling Station Identifier:         204.208.28.41

NAS:
        NAS IPv4 Address:                   204.208.28.26
        NAS IPv6 Address:                   -
        NAS Identifier:                     204.208.28.26
        NAS Port-Type:                      Virtual
        NAS Port:                           0

RADIUS Client:
        Client Friendly Name:               Humpreys_Controller_A
        Client IP Address:                  10.255.50.126

Authentication Details:
        Connection Request Policy Name:     Use Windows authentication for all users
        Network Policy Name:                Radius
        Authentication Provider:            Windows
        Authentication Server:              AMEDNMMEDK02.pac.amed.ds.army.mil
        Authentication Type:                PAP
        EAP Type:                           -
        Account Session Identifier:         -

Quarantine Information:
        Result:                             Full Access
        Extended-Result:                    -
        Session Identifier:                 -
        Help URL:                           -
        System Health Validator Result(s):  -

Log Name:          Security
Source:            Microsoft Windows security   Logged:         10/30/2012 1:54:55 PM
Event ID:          6278                         Task Category:  Network Policy Server
Level:             Information                  Keywords:       Audit Success
User:              N/A                          Computer:       AMEDNMMEDK02.pac.amed.ds.army.mil
OpCode:            Info
More Information:  Event Log Online Help
```

As you can see, the client (KORLDAP) authenticated through the connection request policy from 10.255.50.126, to the RADIUS network policy using PAP.

From:
https://28-40.18mc.amedd.army.mil/kb/ - **NE&S Knowledgebase**

Permanent link:
https://28-40.18mc.amedd.army.mil/kb/doku.php?id=technologies:802.1x:802.1x_on_a_cisco_architecture

Last update: **2012/10/30 14:11**