

Projeto de contingência para acesso à rede Ethernet usando a rede telefônica

Fabio Montoro
10 janeiro 2013

Este projeto consiste na implantação de uma solução de Acesso Remoto a uma rede Local corporativa, por meio da Rede Pública de Telefonia Comutada (PSTN), criando uma contingência para comunicação entre as diversas filiais, localizadas em endereços diversos, e a matriz da corporação que abriga o Data Center com armazenamento e processamento de dados.

O projeto define duas zonas principais: **modems-clientes** e **servidor de acesso remoto** (RAS Remote Access Server).

Modems-clientes

Devem ser definidas algumas estações de trabalho consideradas estratégicas, para terem privilégio de acesso à rede corporativa central, de forma discada, pela rede PSTN. Esse acesso será feito em caso de quedas dos links principais do backbone de comunicação entre uma filial e a matriz, independentemente do tipo de Link que esteja operando as comunicações.

Em cada estação de trabalho deve ser configurado um discador, com o endereço de comunicação do RAS, e o usuário da respectiva máquina passa a ter “usuário” e “senha”, que o qualificará para a conexão à rede da matriz cujo acesso será liberado somente caso a autenticação seja feita com sucesso, de acordo com a política de acesso definida para cada usuário.

Os modems especificados para esta solução devem ser compatíveis com os padrões V.92, V.44, V.90, K56Flex™, V.34+ ou ISDN.

Após a autenticação, o usuário poderá realizar acesso à rede da matriz de acordo com a política de acesso atribuída a ele.

Os modems devem ser adequadamente configurados para essa função.

RAS (Remote Access Server)

O sistema é composto de dois equipamentos RAS (Remote Access Servers), um na Sala de Equipamentos (ER) do edifício, e outro no Data Center do Edifício, marca Patton, modelo 2960.

A escolha destes dois locais foi resultado da análise da localização dos servidores, que praticamente se concentram nesses dois ambientes

Os RAS (Remote Access Servers) se ligam à rede LAN usando endereço IP a ser determinado, e uma nova VLAN deve ser configurada especificamente para clientes tipo “Dial Up” (conectados via PSTN).

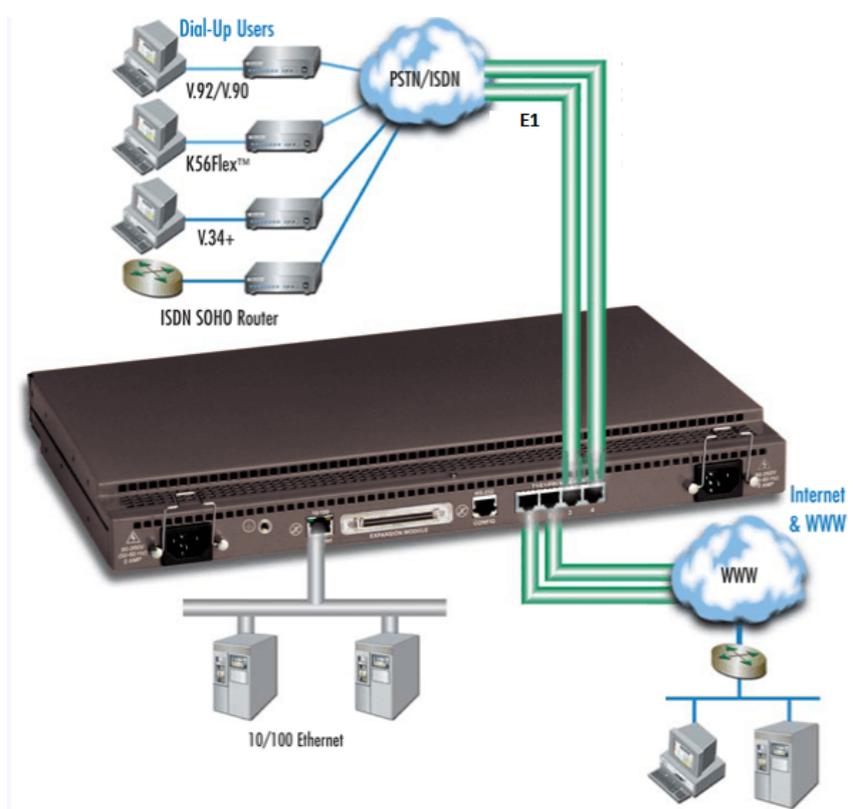


Fig. 1: diagrama básico de aplicação do servidor de acesso remoto (RAS)

A política de acesso à rede LAN deve ser definida em função das normas de segurança do proprietário. Em seguida os usuários deverão ser cadastrados e configurados como “Dial Up”, juntamente com suas respectivas permissões de acesso. Tais informações deverão seguir a política de segurança do proprietário.

Os RAS (Remote Access Servers) são configurados e conectados à Rede Pública de Telefonia Comutada (PSTN) via interface de comunicação E1, permitindo até 30 acessos simultâneos para cada concentrador RAS por link. Cada RAS suporta até 2 (duas) interface de comunicação E1, suportando assim até 60 (sessenta) acessos simultâneos via Rede Pública

de Telefonia Comutada (PSTN). Os links E1 devem estar em perfeito estado operacional, contratados diretamente pelo proprietário.

O acesso WEB, disponível nos equipamentos RAS deverão ser configurados, permitindo o gerenciamento WEB remoto dos equipamentos RAS (Remote Access Servers). Os equipamentos RAS também aceitam ser configurados por gerenciamento SNMP, usando software de gerenciamento SNMP.

É recomendável implantar um RAS de cada vez, fazendo todos os testes necessários, bem como uma fase de operação assistida com um total 150 (cento e cinquenta) horas.

A figura 2 mostra os modelos de RAS ofertados pelo fabricante, onde se constata que a escolha por dois modelos de 60 acessos foi a melhor opção para a solução desejada (alta confiabilidade, mitigação de falhas de acesso) que pedia 120 acessos simultâneos. Desta forma dois equipamentos são mutuamente redundantes e podem superar uma eventual falha em um deles



	Model 2960					Model 2996		Model 3120			
Model Number	2960/16	2960/24	2960/30	2960/48	2960/60	2996/96	2996/120	3120/48	3120/60	3120/96	3120/120
Number of Connections	16	24	30	48	60	96/120 Calls—4 T1's or 4 E1's		48	60	96	120
Power Supplies	Dual Redundant (Fixed) AC					Dual Redundant (Fixed) AC		Dual-Redundant (Hot Swap) AC or DC			
Ethernet Ports	One 10/100Base-T					One 10/100Base-T		Two 10/100Base-T			
WAN Ports	Four					Four		Four			
Modem Modulations	V.92, V.44, V.90, K56Flex™, V.34 Annex 12, V.34, V.32bis, V.32, V.23, V.22, V.22bis, V.21, Bell 212A, Bell 202, Bell 103, EIA-PN-2330, V.8, V.8bis, Sync/Async receiver/transmitter for V.14, V.42/V.42bis error correction & compression.										
PSTN Signaling	E1 Primary Rate interface (Q.931), E1 MFR2 (R2), T1 Primary Rate Interface, T1 Robbed bit with Loop/Ground Start or E&M Wink, E&M Immed, Taiwan R1 and Drop & Insert										
Management Services	HTTP, SNMP, TELNET Dial-in and Ethernet or RS-232 console port, SYSLOG client, Remote software upgrade via FTP, User configurable login prompts and banners										
Authentication	RADIUS, PAP/CHAP, Username/Password, and Static Users Database (111 Entries)										
Software Upgrades	Achieved through Flash upgrades via FTP (upgrades available from www.palton.com)										
Protocol Services	TCP/IP suite with extensive protocol statistics • ICMP/TFTP/FTP/RLOGIN/TELNET • Ethernet ARP, Proxy ARP and RARP protocols • Point-to-Point Protocol (PPP) • SLIP protocol • Van Jacobson TCP header compression PPP address and protocol compression • RADIUS authentication and accounting, with support for primary and secondary servers • RIP and RIPv2 • User configurable static routes • MultiLink PPP • Multi-chassis MultiLink • Layer 3 and Layer 4 IP Filtering • NFAS • DNIS										
Dial-out Services	Dial-out with support for multi-link PPP • Single-line call-back • Remote authentication using PAP and CHAP and session time										

Fig. 2: modelos disponíveis comercial do servidor de acesso remoto (RAS)

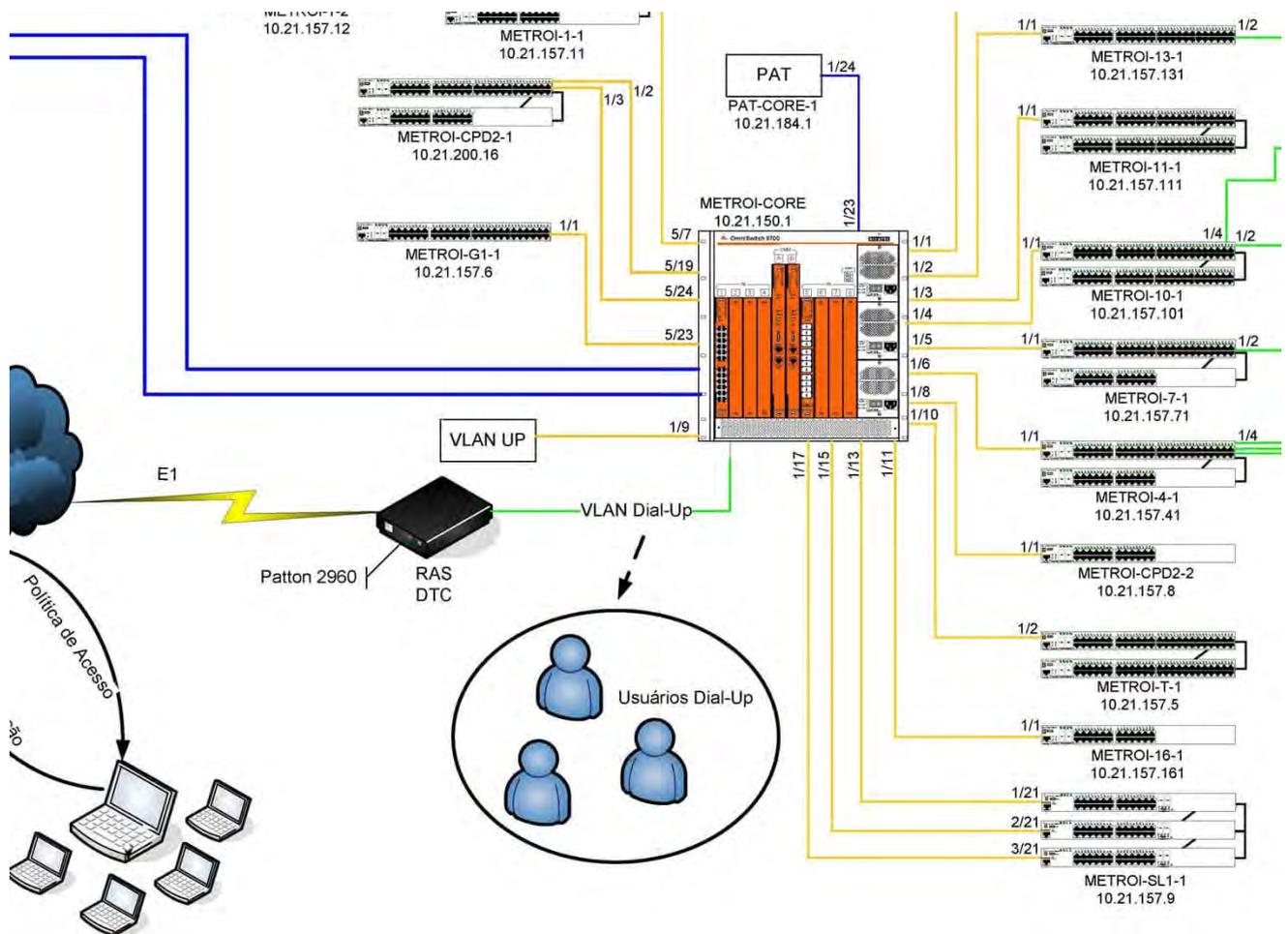
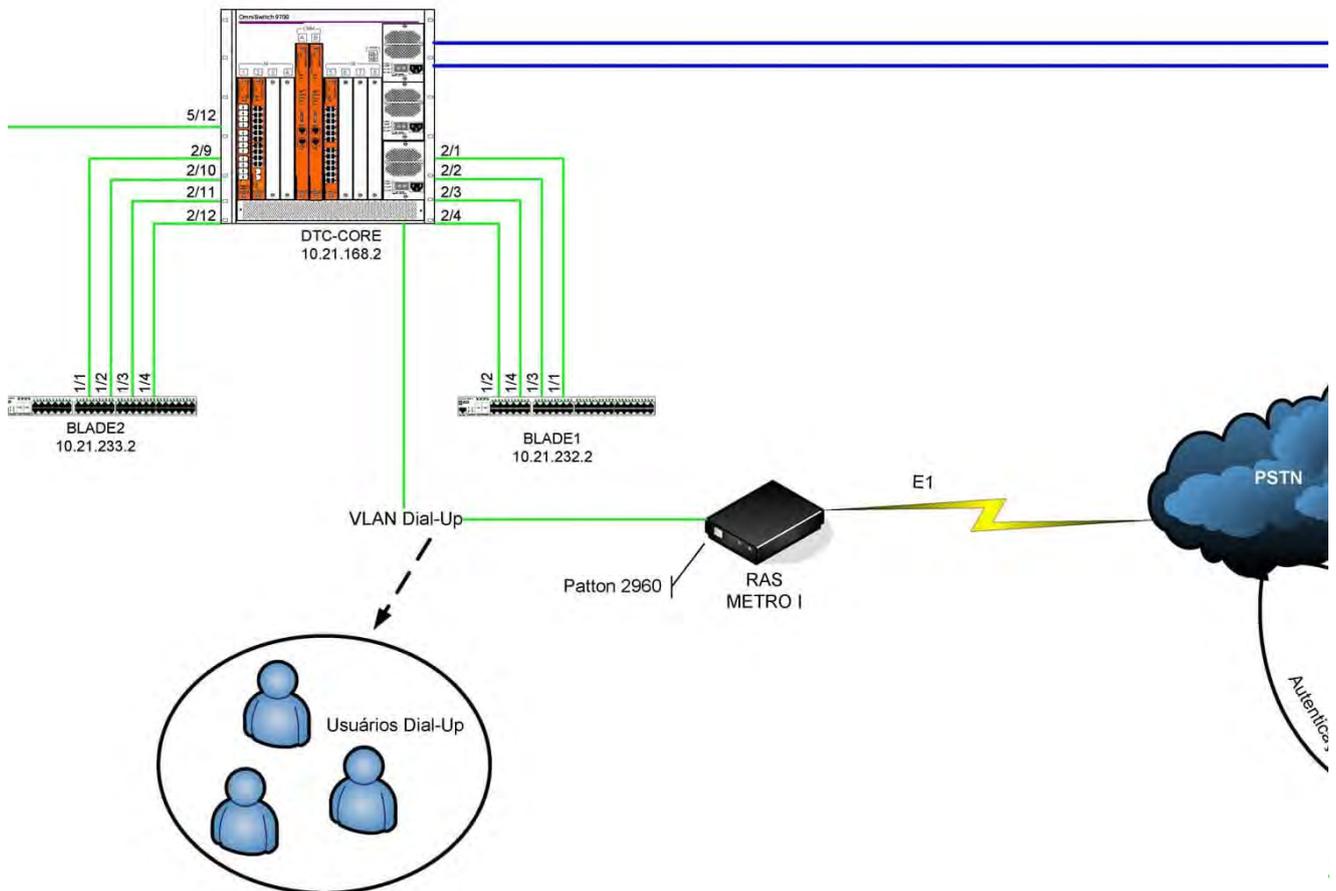
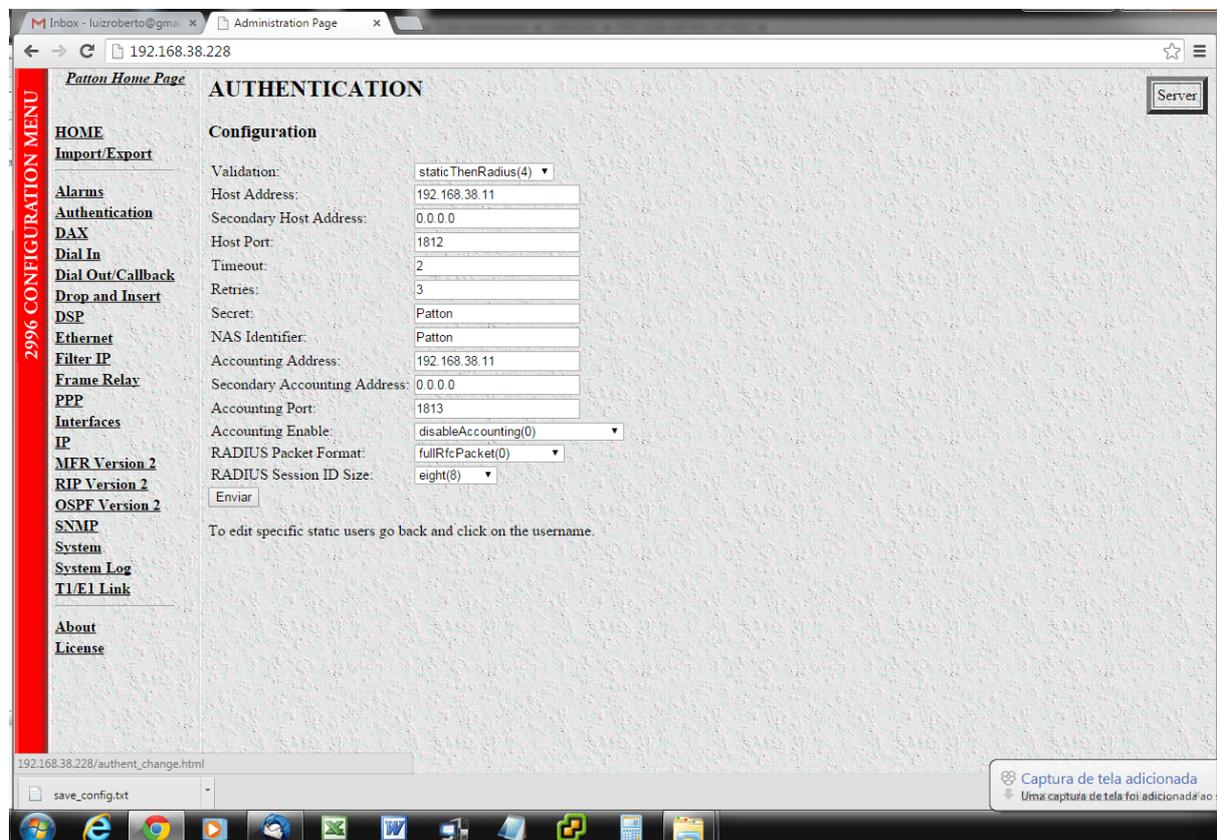
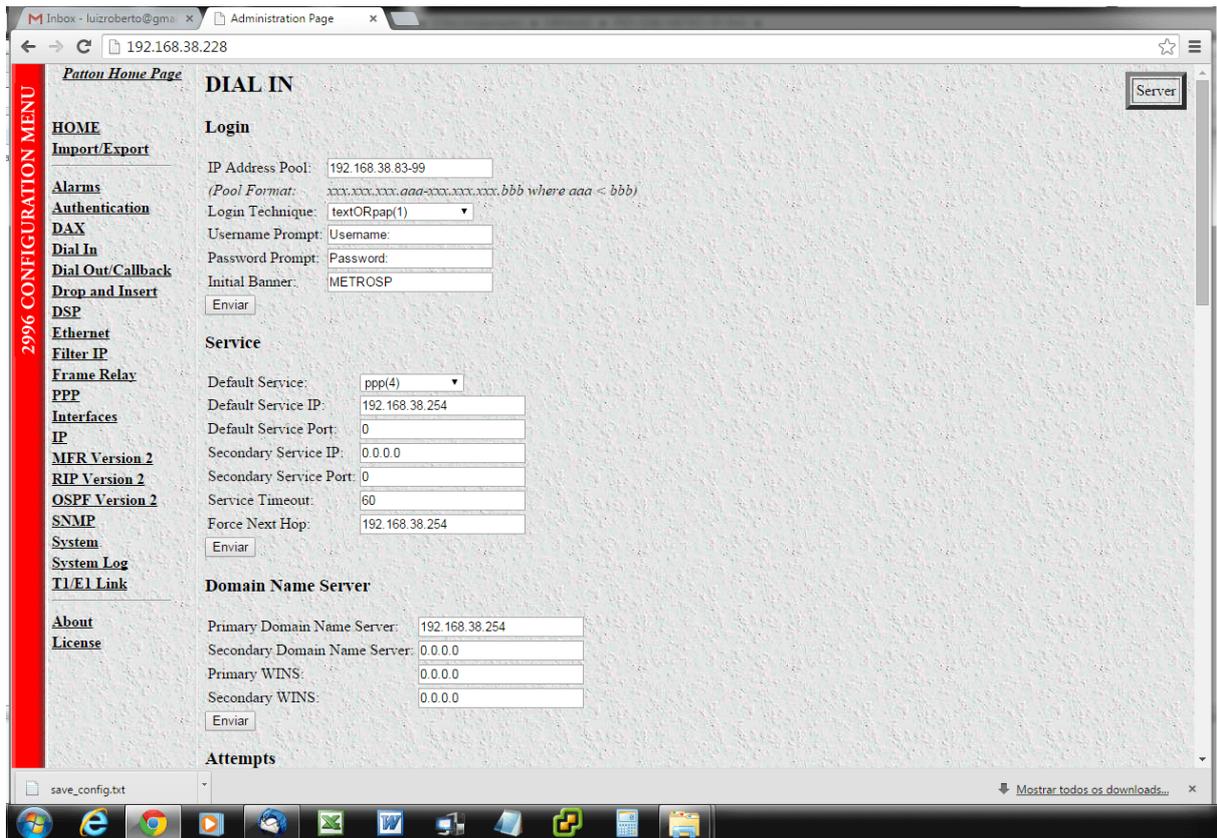


Fig. 2: modelos disponíveis comercial do servidor de acesso remoto (RAS)

A figura 3 mostra o diagrama do sistema e seu funcionamento.

As figuras a seguir mostram as telas de configuração



Administration Page x 192.168.38.228

Patton Home Page

ETHERNET A Server

State: linkIndication100Duplex(6)

PrimaryIpAddress: 192.168.38.228

PrimaryIpMask: 255.255.255.0

PrimaryIpFilters:

SecondaryIpAddress: 192.168.50.228

SecondaryIpMask: 255.255.255.0

SecondaryIpFilters:

Technique: static(1)

Technique: auto(0)

2996 CONFIGURATION MENU

- HOME
- Import/Export
- Alarms
- Authentication
- DAX
- Dial In
- Dial Out/Callback
- Drop and Insert
- DSP
- Ethernet
- Filter IP
- Frame Relay
- PPP
- Interfaces
- IP
- MFR Version 2
- RIP Version 2
- OSPF Version 2
- SNMP
- System
- System Log
- T1/E1 Link
- About
- License

save_config.txt

Captura de tela adicionada
Uma captura de tela foi adicionada ao se

192.168.38.11 - Conexão de Área de Trabalho Remota

Network Policy Server

File Action View Help

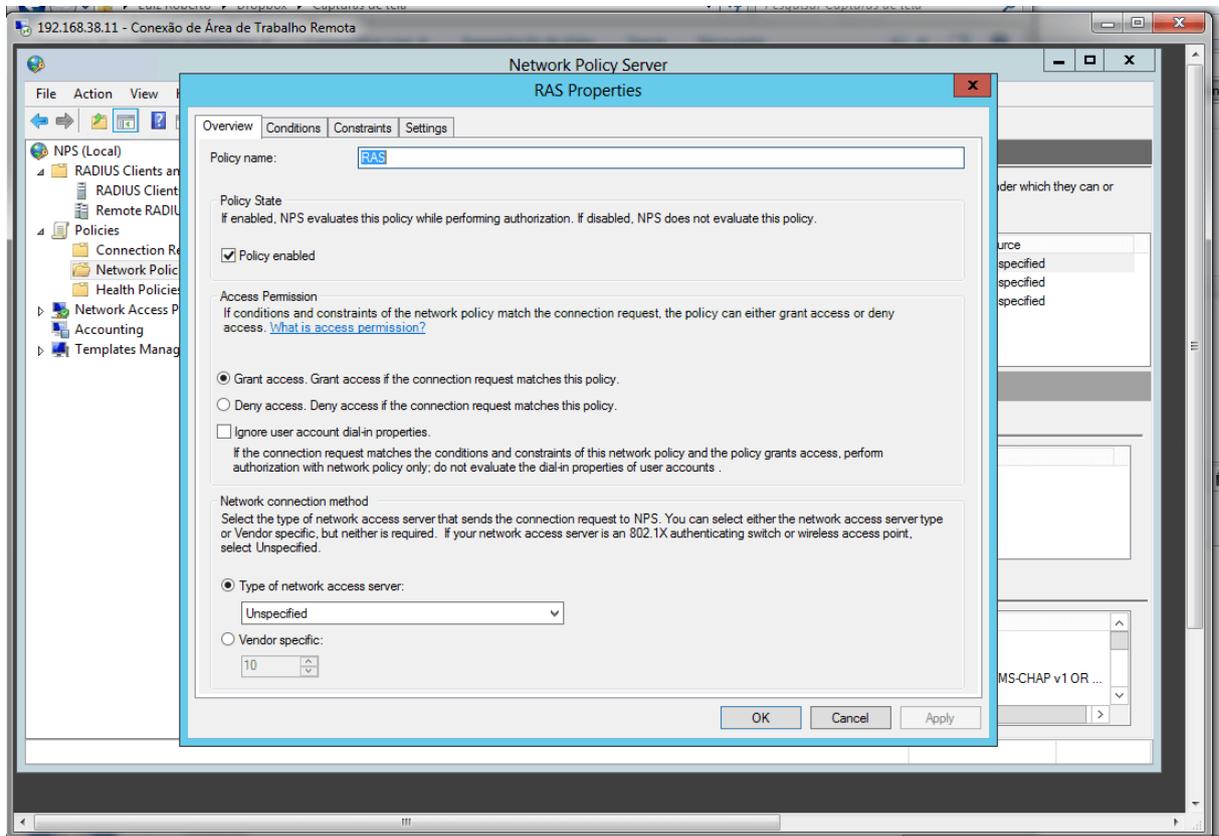
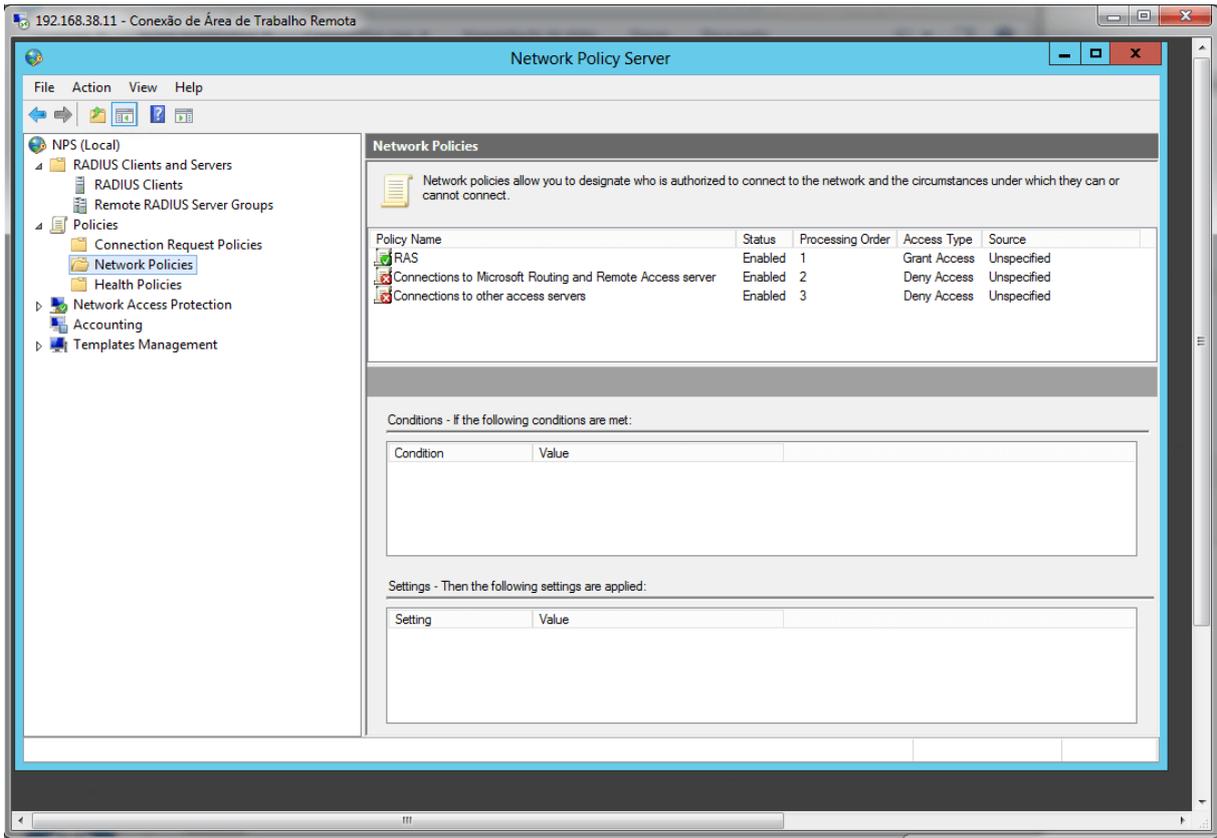
NPS (Local)

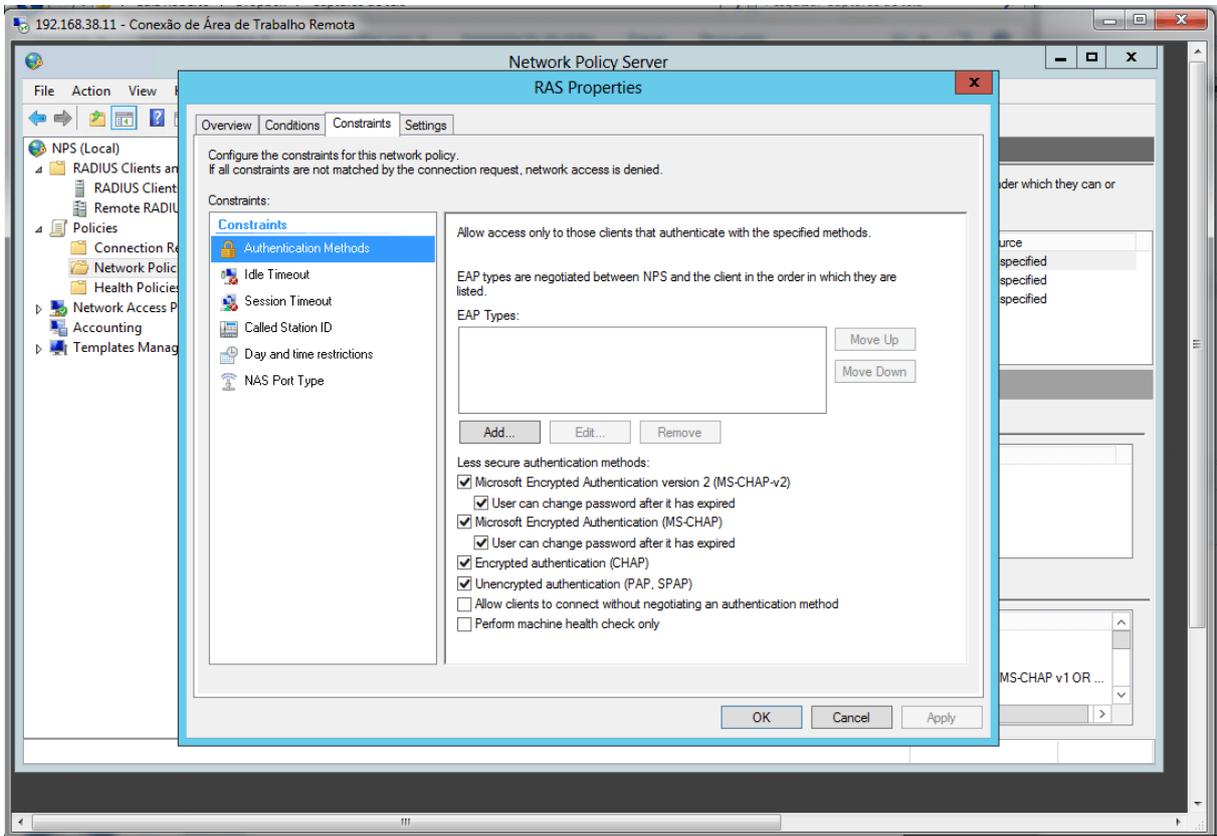
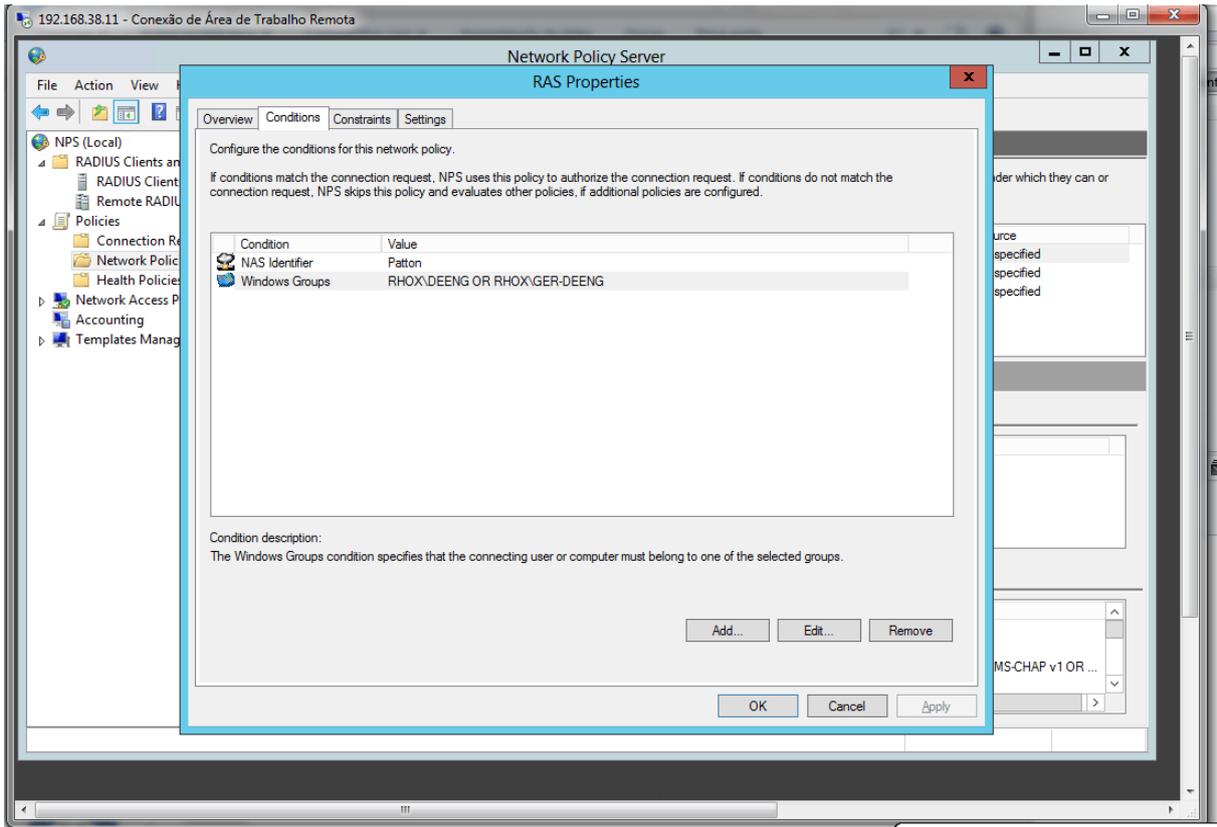
- RADIUS Clients and Servers
 - RADIUS Clients
 - Remote RADIUS Server Groups
- Policies
- Network Access Protection
- Accounting
- Templates Management

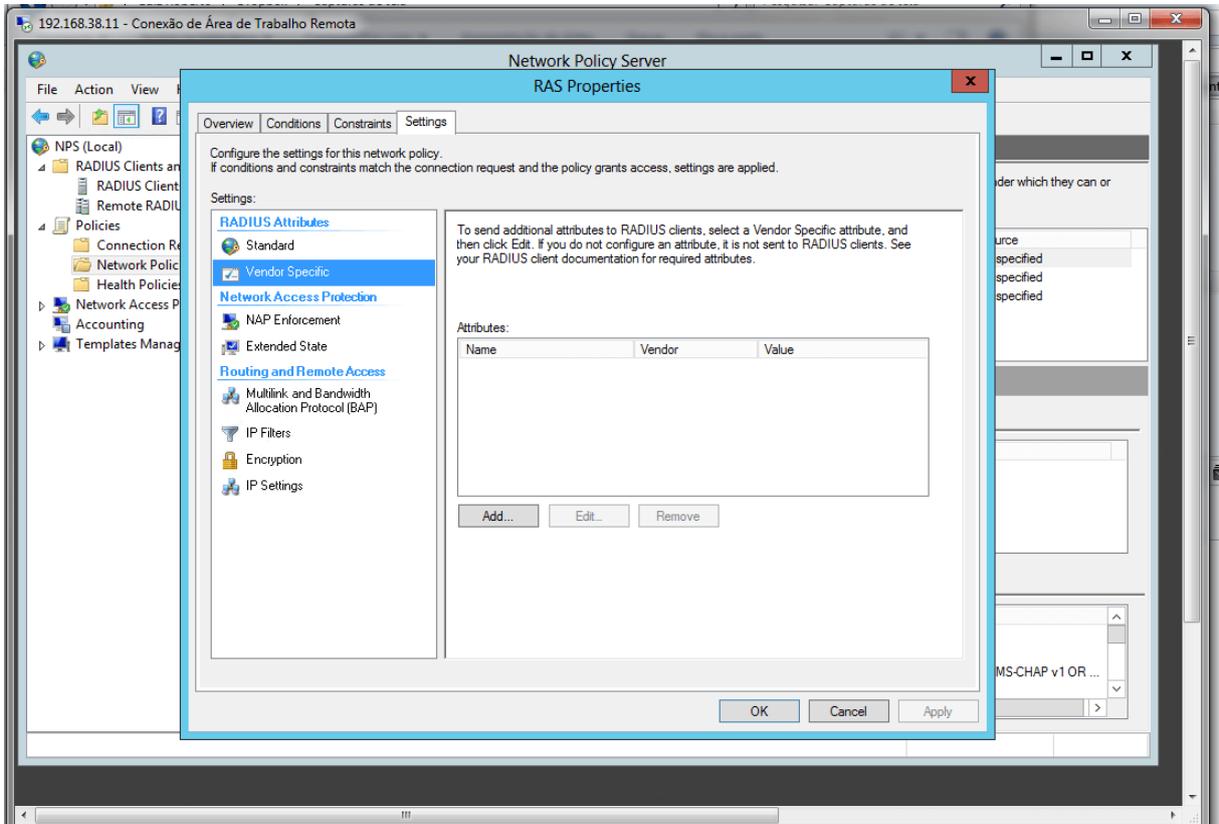
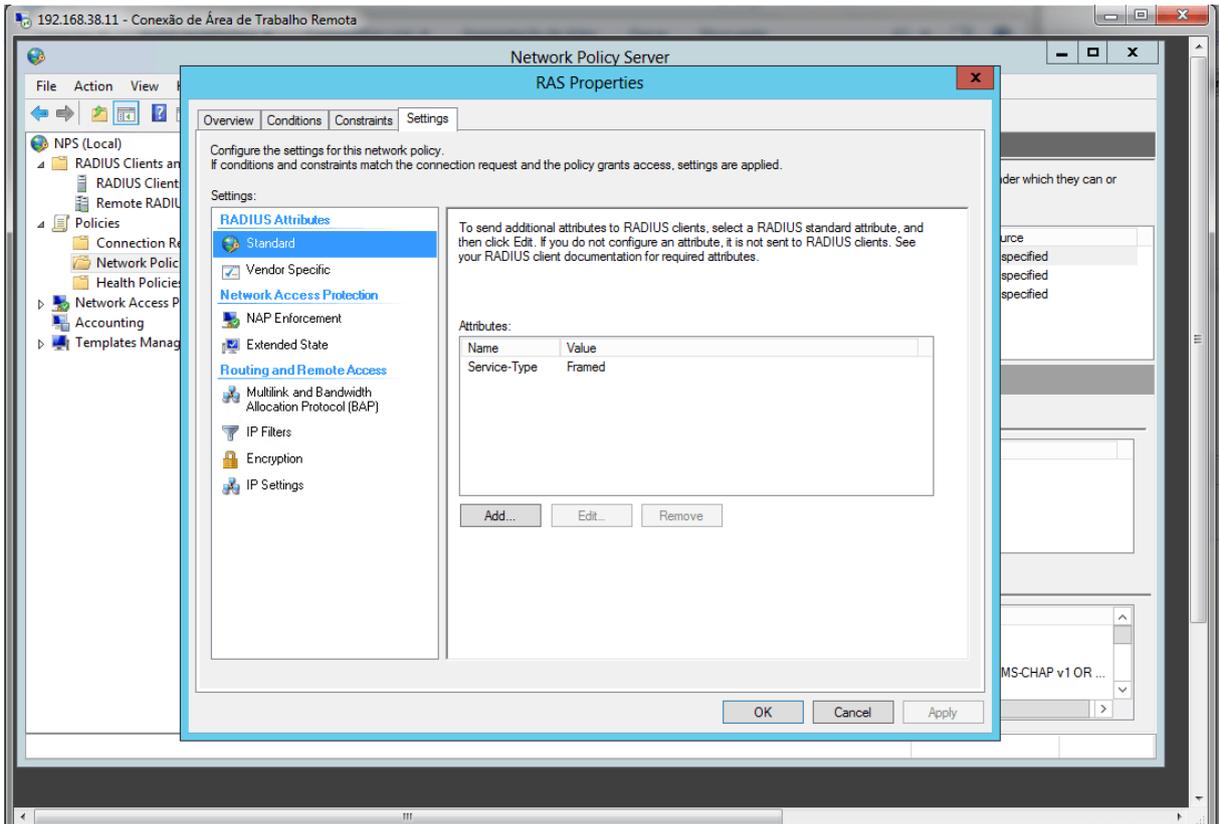
RADIUS Clients

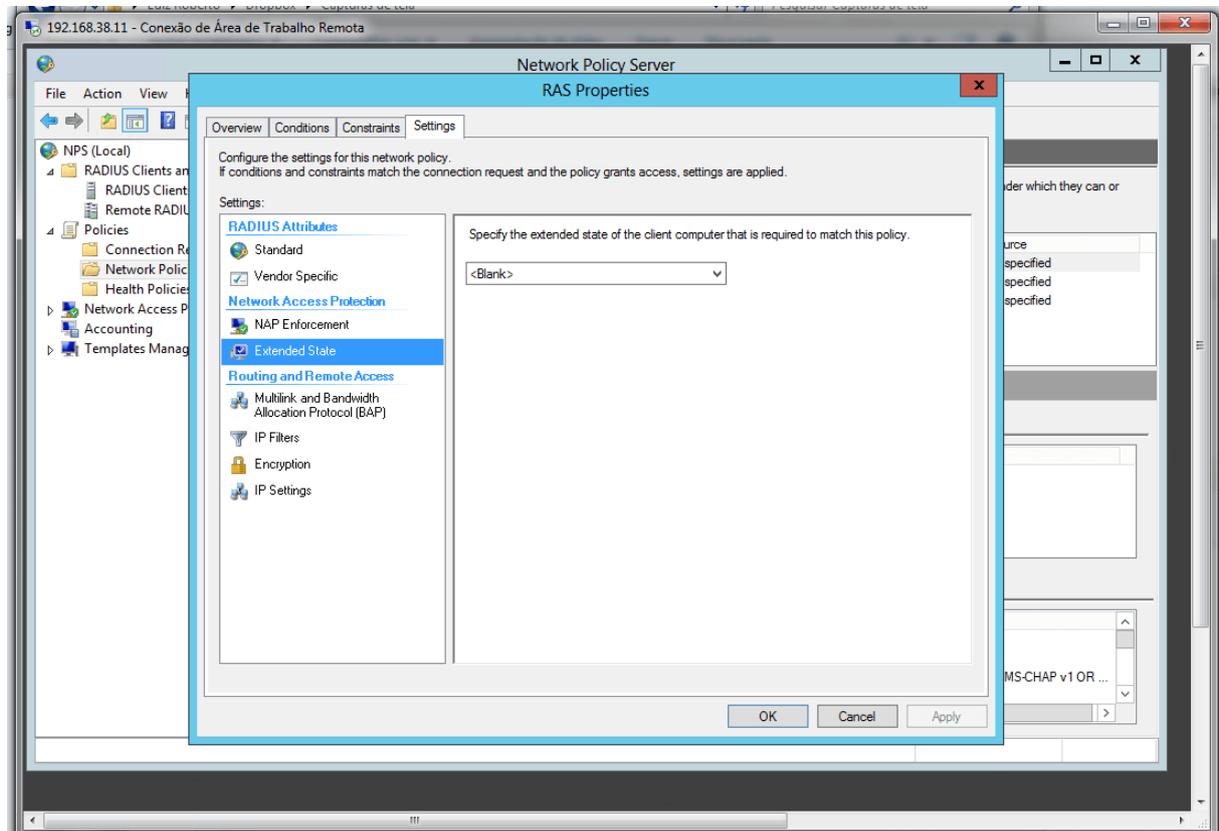
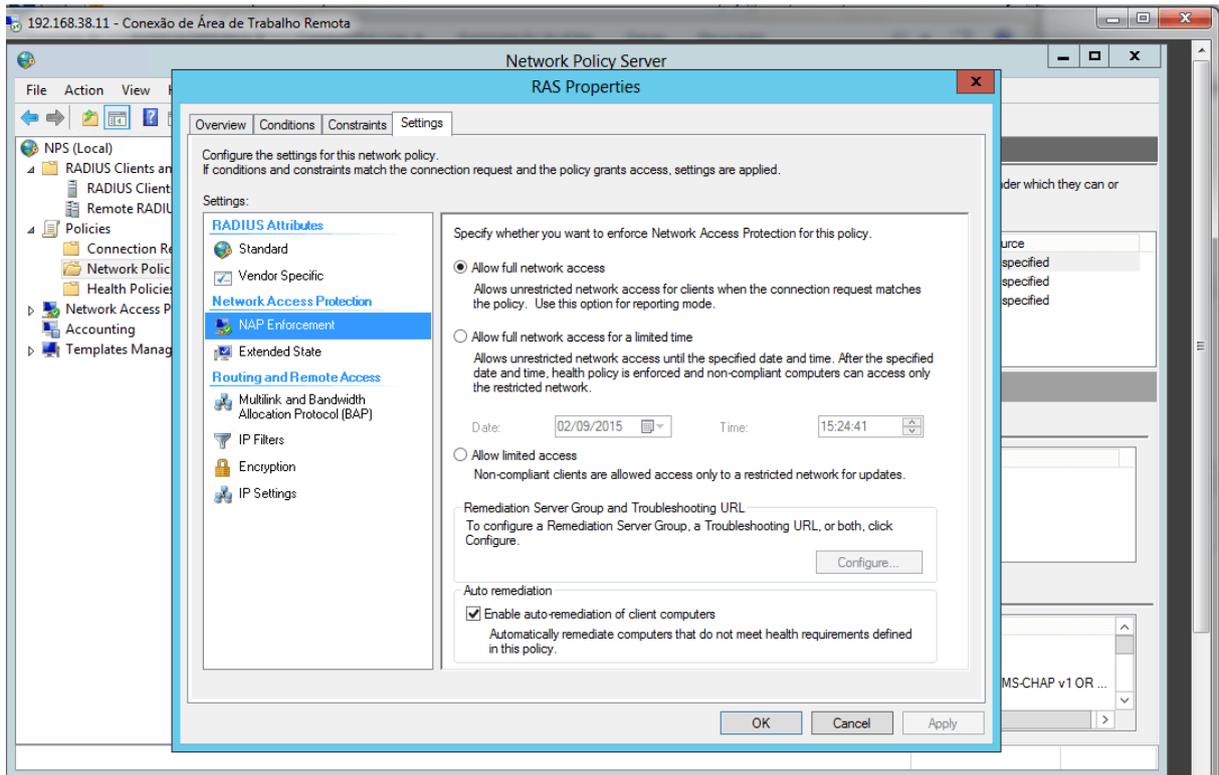
RADIUS clients allow you to specify the network access servers, that provide access to your network.

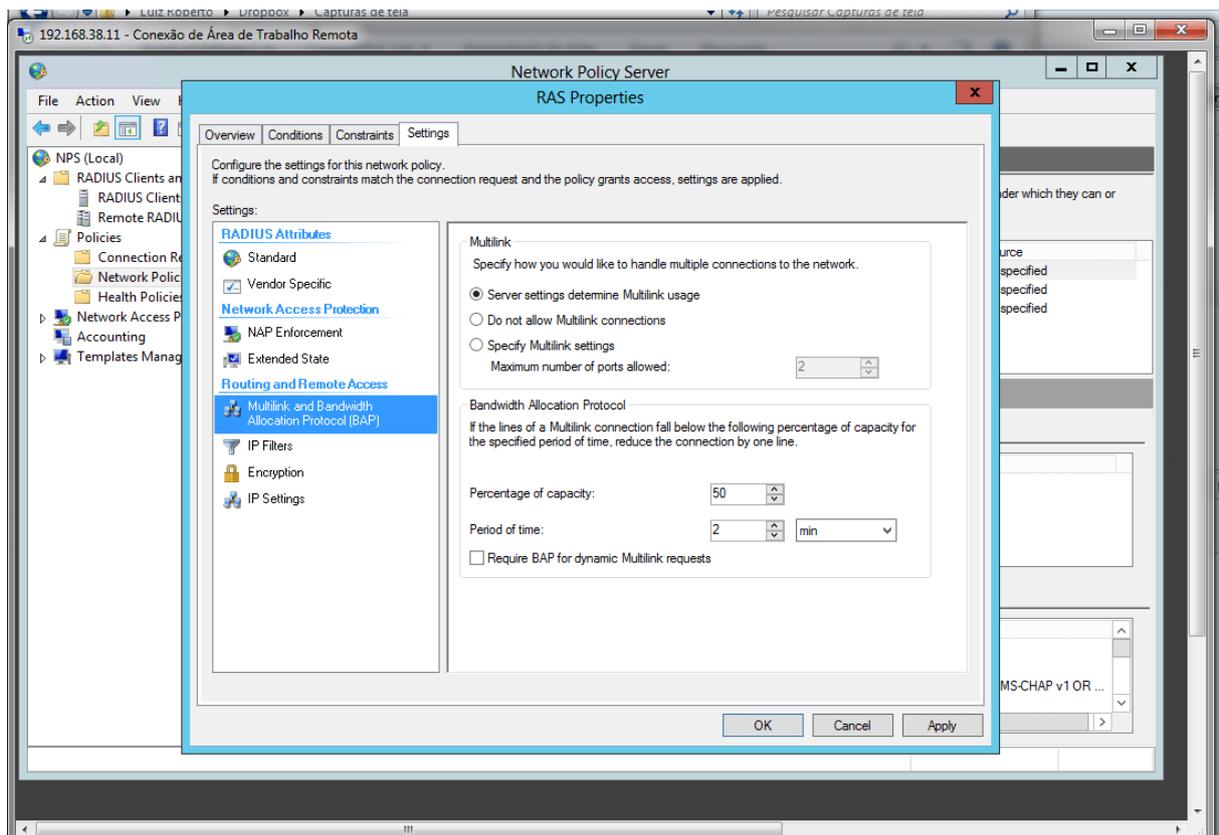
Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status
SwitchCentral	192.168.38.250	RADIUS Standard	No	Enabled
SwitchBorda	192.168.38.251	RADIUS Standard	No	Enabled
Ras	192.168.38.228	RADIUS Standard	No	Enabled



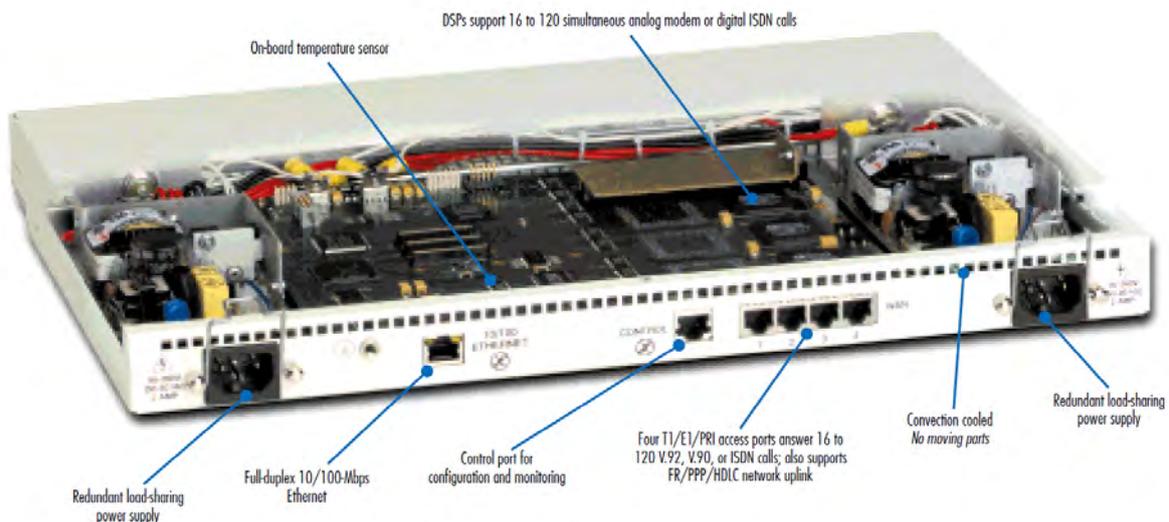








Resumo das características do RAS modelo 2960



- Baseado no processador RISC Intel modelo i80960VH operando a 100 MHz
- 4 Mbytes de memória FLASH
- 32 Mbytes de memória DRAM
- CPU com capacidade de 100 Mips
- 60 modems multinorma V34+, V90, V92 internos
- 4 interfaces WAN selecionáveis entre E1 (2.048 Mbps), T1 (1.544 Mbps) ou PRI

- Porta Ethernet LAN 10/100-Mbps
 - 100Base-TX half-/full-duplex operation (100 + 100)
 - 10Base-T half-/full-duplex operation (10 + 10)
- 1 U de altura
- Fonte de alimentação redundante

Epílogo

A solução RAS atualmente é super importante como recurso de contingência para serviços que não podem para sob pena de alto prejuízo financeiro. O presente projeto foi implantado e funcionou perfeitamente, garantindo a disponibilidade de acesso desejada pelo proprietário. Mas, é preciso dizer, que estudos recentes sugerem que as VPNs (Virtual Private Networks) substituirão em um futuro talvez próximo, os equipamentos RAS. O fabricante Patton não acredita nisso, mas eu cá tenho minhas dúvidas. Porquê? Apesar dos estudos sobre VPN temos outra questão: as linhas telefônicas analógicas chegaram ao seu limite de transmissão de dados. A tendência será a digitalização da última milha com modems digitais e, mais na frente, fibra óptica, levando os dados digitais cada vez mais pra dentro das redes públicas. Ainda temos muito tempo antes que isso ocorra e muitas corporações não podem esperar, é claro. Precisam de alta disponibilidade, alto MTBF.

- o - o - o -