

Erfahrungsbericht Cisco & Remote Access (Radius)

Compaq Computer GmbH
Jürgen Wedler
Consultant Network Services
Kieler Str. 147, D-22769 Hamburg
Tel: +49 (40) 85361 145
Fax: +49 (40) 85361 322
Mobil: +49 (175) 4352770
E-Mail: juergen.wedler@compaq.com

Juergen.Wedler@Compaq.com

History

Bis 1998 betrieb die Unilever HH einen RAS Zugang mit Conware Routern. Aufgrund technischer Probleme mit den Routern, wurde nach einer anderen Lösung gesucht und auch gefunden.

Diese Lösung basiert auf dem Cisco IOS Release 11.3 und Cisco 36X0 Routern. Alle Remote Anwender waren als Dialer Interface auf den Routern hinterlegt.

Juergen.Wedler@Compaq.com

Juergen.Wedler@Compaq.com

History

Es kristallisierte sich schnell heraus, daß diese Lösung schon kurzfristig den Anforderungen nicht gerecht werden würde.

Das Problem ist, daß zum einen die Anzahl der Dialer Interface auf ca. 250 beschränkt ist, zum anderen keine Ausfallsicherheit besteht.

Auch die Administration auf den Routern war umständlich, da die Konfigurationen auf dem Router gemacht werden mußten.

Gesucht wurde nach einer Lösung, die mehr User zuläßt, zentral administriert wird, skalierbar ist und Redundanzen zur Verfügung stellt.

Juergen.Wedler@Compaq.com

Juergen.Wedler@Compaq.com

Anforderung

Die Remote Access Lösung sollte:

- einfach skalierbar sein
- PPP Multilink unterstützen
- analog / ISDN / V.110 unterstützen
- Radius / TACACS

Außerdem sollte, damit die Kosten lokal verwaltet werden können, bei den Clients ein D-Channel Callback möglich sein.

Juergen.Wedler@Compaq.com

Juergen.Wedler@Compaq.com

Lösung:

Die Entscheidung fiel auf Cisco.

Zwei Access Server AS5300 mit jeweils 4 ISDN-PRI Ports und 60 integrierten Modems sollten den Anfang machen. Mit dem IOS 12.0 gab es ein neues Feature, das genau den Anforderungen entsprach.

Als zentrales Administrations Tool sollte ein Radius oder TACACS Server dienen.

TACACS: Terminal Access Controller Access Control System Plus
oder

Radius: Remote Authentication Dial-In User

Juergen.Wedler@Compaq.com

Juergen.Wedler@Compaq.com

Radius Server

Als Software bot sich der Cisco Secure Server an.

Er unterstützt Radius und TACACS+ sowie diverse Datenbanken.

Die Anfänge waren schnell gemacht; es stellte sich jedoch schnell heraus, daß Cisco Secure nicht die Lösung war.

Immer wieder Probleme aufgrund fehlender oder schlecht dokumentierter Features; Support von Cisco in diesem Teilbereich nicht optimal.

Von einem Provider brachte ich dann die Idee des Radiators mit.
Ein Radius Server auf Perl basierend, der auf jeder Plattform läuft.
Egal ob WIN NT, Win98/95 oder Unix.

Es war uns zwar bewußt, daß wir wieder in neue Probleme laufen würden, aber der Support durch den Hersteller fing gut an.

Juergen.Wedler@Compaq.com

Juergen.Wedler@Compaq.com

Radius Server

Die User im Radius File werden als Text File hinterlegt.

Für jeden Client müssen zwei statische Routen konfiguriert werden:

```
#####  
#                               NAS 1 IP Adresse 193.26.81.27/24
```

```
RFE027 User-Password = "cisco"
```

```
RFE027-1 User-Password="cisco",Service-Type=Outbound-User  
cisco-avpair="ip:route=193.17.152.20 255.255.255.252 193.17.152.21 name Shiva1"  
cisco-avpair="ip:route=193.17.152.21 255.255.255.255 Dialer1 200 name Shiva1"
```

Anmerkung:

Pro User nur 50 Routen möglich

Die Abfrage läuft automatisch, bis es keine User mehr gibt.

Juergen.Wedler@Compaq.com

Juergen.Wedler@Compaq.com

Radius Server

Weiterhin müssen die Einträge für Dial/In & Dial/Out definiert werden:

```
SHIVA1 User-Password = "cisco", Calling-Station-ID = „4012345678“  
Service-Type=Framed,  
Idle-Timeout = 60
```

```
Shiva1-out User-Password = "cisco",Service-Type=Outbound-User  
Service-Type=Outbound-User,  
cisco-avpair="outbound:dial-number=04012345678"
```

Juergen.Wedler@Compaq.com

Juergen.Wedler@Compaq.com

Radius Server

Wie funktioniert?

Der Router lädt sich alle 24 Stunden automatisch die Routen zu den Usern vom Radius Server herunter. In den Routen ist das Netz der Clients sowie der Name hinterlegt.

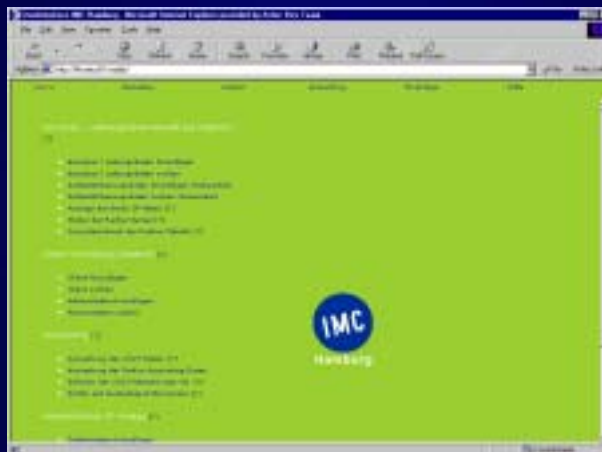
Dial In: Der Router ruft in die Zentrale,
CLID, Username & Passwort werden geprüft

Dial Out: Anhand der IP Adresse kennt der Router den Namen des Clients. Er holt sich vom Radius Server die Configurationsdaten und baut sich ein virtuelles Interface auf.

Juergen.Wedler@Compaq.com

Juergen.Wedler@Compaq.com

Web Interface und SQL Datenbank



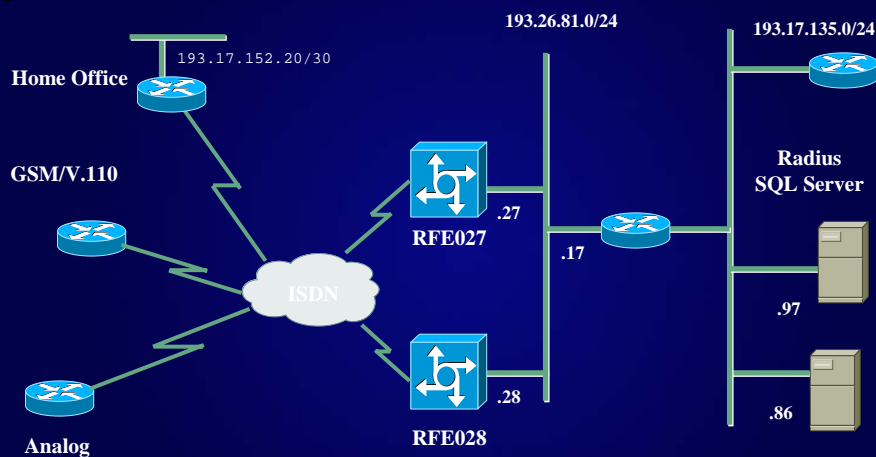
Juergen.Wedler@Compaq.com

Web Interface und SQL Datenbank



Juergen.Wedler@Compaq.com

Layout



Juergen.Wedler@Compaq.com

Juergen.Wedler@Compaq.com

Client Definition

Home Office: Die Router haben feste Adressen, die PC's bekommen per DHCP die IP Adresse vom Server. Rufnummernüberprüfung ist auf beiden Seiten eingeschaltet. Idle Timeout wird Client bezogen gesetzt.

Mowis: Die Clients wählen sich per Handy ein und erhalten vom DHCP Server eine Adresse zugewiesen.
Problem: DHCP forwarding muß auf dem virtuellen Interface per User konfiguriert sein.

Analog: Clients können sich per Modem einwählen.

Juergen.Wedler@Compaq.com

Juergen.Wedler@Compaq.com

Config

```
aaa new-model
aaa authentication login default group radius local
aaa authentication ppp default group radius local
aaa authorization network default group radius
aaa authorization configuration default group radius
aaa accounting network default stop-only group radius
aaa route download 720
```

Juergen.Wedler@Compaq.com

Juergen.Wedler@Compaq.com

Config cont.

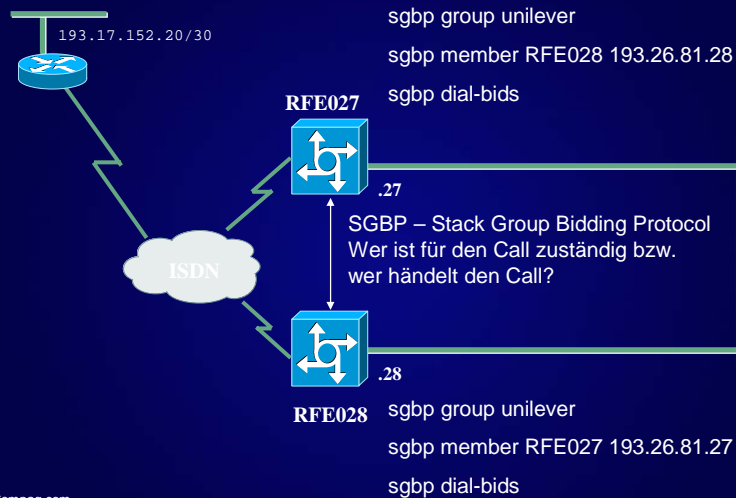
```

router eigrp 100
 redistribute connected
 redistribute static
 network 193.26.81.0
!
dialer-list 1 protocol ip permit
ip local pool dialin-pool 193.26.87.10 193.26.87.120
ip classless
ip route 0.0.0.0 0.0.0.0 193.26.81.17
!
radius-server host 193.17.135.86 auth-port 1645 acct-port 1646
radius-server host 193.26.94.38 auth-port 1645 acct-port 1646
radius-server retransmit 3
    
```

Juergen.Wedler@Compaq.com

Juergen.Wedler@Compaq.com

SGBP



Juergen.Wedler@Compaq.com

Juergen.Wedler@Compaq.com

Routing

```
cisco-avpair="ip:route=193.17.152.20 255.255.255.252 193.17.152.21 name Shiva1"  
cisco-avpair="ip:route=193.17.152.21 255.255.255.255 Dialer1 200 name Shiva1"
```

```
RFE027#sh ip route static download  
Connectivity: A - Active, I - Inactive
```

```
A 193.17.151.4 255.255.255.252 193.17.151.5 name pfrank_r  
A 193.17.151.5 255.255.255.255 Dialer1 200 name pfrank_r  
A 193.17.151.8 255.255.255.252 193.17.151.9 name tsitti_r  
A 193.17.151.9 255.255.255.255 Dialer1 200 name tsitti_r
```

Juergen.Wedler@Compaq.com

Juergen.Wedler@Compaq.com

Routing

Verbindung läuft über RFE028

```
RFE027#sh ip rout 193.26.89.221  
Routing entry for 193.26.89.221/32  
Known via "eigrp 100", distance 170, metric 42562560, type external  
Redistributing via eigrp 100  
Advertised by eigrp 100 (self originated)  
Last update from 193.26.81.28 on FastEthernet0, 00:30:26 ago  
Routing Descriptor Blocks:  
* 193.26.81.28, from 193.26.81.28, 00:30:26 ago, via FastEthernet0  
Route metric is 42562560, traffic share count is 1  
Total delay is 100100 microseconds, minimum bandwidth is 64 Kbit  
Reliability 255/255, minimum MTU 1500 bytes  
Loading 1/255, Hops 1
```

Juergen.Wedler@Compaq.com

Juergen.Wedler@Compaq.com

Accounting

Mon Dec 11 00:00:10 2000

NAS-IP-Address = 193.26.81.27
NAS-Port = 20326
NAS-Port-Type = ISDN-Sync
User-Name = „testme_r“
Called-Station-Id = "12345678"
Calling-Station-Id = "0987654321"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Framed
Acct-Session-Id = "00008ACB"
Framed-Protocol = PPP
Framed-IP-Address = 193.26.89.117
Acct-Terminate-Cause = User-Request
Acct-Input-Octets = 514
Acct-Output-Octets = 554
Acct-Input-Packets = 35
Acct-Output-Packets = 36
Acct-Session-Time = 90
Juergen.Wedler@Compaq.com
Acct-Delay-Time = 0
Timestamp = 976489210

Juergen.Wedler@Compaq.com

Debug ...

Debug ISDN q931

Debug aaa authentication
Debug aaa authorization
Debug Radius

Debug vtemplate
Debug vprofile

Juergen.Wedler@Compaq.com

Juergen.Wedler@Compaq.com

Debug Radius

Apr 10 13:23:56.332: RADIUS: Initial Transmit Serial0:9 id 248 193.17.135.86:1645,
Access-Request, len 117

Apr 10 13:23:56.332:	Attribute 4 6 C11A511B	NAS IP Address
Apr 10 13:23:56.332:	Attribute 5 6 00004E29	NAS Port
Apr 10 13:23:56.332:	Attribute 26 17 00000009020B5365	Vendor Specific
Apr 10 13:23:56.332:	Attribute 61 6 00000002	NAS Port Type
Apr 10 13:23:56.332:	Attribute 1 10 6D6D6573	Username
Apr 10 13:23:56.332:	Attribute 30 9 33353734	Called Station ID
Apr 10 13:23:56.332:	Attribute 31 12 32343236	Calling Station ID
Apr 10 13:23:56.332:	Attribute 3 19 FCDE0710	CHAP Password
Apr 10 13:23:56.332:	Attribute 6 6 00000002	Service Type
Apr 10 13:23:56.332:	Attribute 7 6 00000001	Framed Protocol

Juergen.Wedler@Compaq.com

Juergen.Wedler@Compaq.com

Show ...

Show isdn active

Call Type	Calling Number	Called Number	Remote Name	Seconds Used	Seconds Left	Seconds Idle	Charges Units/Currency
In	9876543	1234567	ruehl_r	43869			
In	8765432	2345678	alist_r	43830	-	-	
In	7654321	3456789	hleder_r	23649	-	-	

RFE027#sh us

Line	User	Host(s)	Idle	Location
* 62 vty 0	tele	idle	00:00:00	193.26.90.155
Vi1	wspard_r	Virtual PPP (VDP)	01:27:17	
Vi3	alist_r	Virtual PPP (VDP)	01:51:13	
Vi5	cschmi_r	Virtual PPP (VDP)	00:27:27	
Vi6	gvonte_r	Virtual PPP (VDP)	00:20:21	

Juergen.Wedler@Compaq.com

Juergen.Wedler@Compaq.com

Probleme

Die meisten Problem hatten wir dadurch, daß die Einzellösungen, wie sie bei Cisco beschrieben wurden, zwar immer gut liefen, aber durch die Gesamtheit unüberschaubar waren.

So hat es gedauert, bis klar war, daß die Übergabe von Username & Passwort für's Dial Out im Radius Standard nicht vorgesehen ist.

Also mußte darüber nachgedacht werden, wie man nur noch Dial In – User hat.

Die meisten Zusammenhänge mußten selbst erarbeitet werden.

Es kam der Punkt, an dem es keinen Sinn mehr machte bei Cisco einen Case zu öffnen:

Bis man dem Techniker alle Zusammenhänge erklärt hatte, war einem selbst ein Work Around eingefallen. :o))

Provider, für die die meisten Access Lösungen designed sind, benötigen nur reines Dial In. Ein User mit einem default Username & Passwort wählt sich ein, bekommt eine IP Adresse Und kann surfen.

Bei Unilever bekommt jeder User eine eindeutige IP Adresse, ist von der Zentrale aus erreichbar, Die Rufnummer wird überprüft, und die Access Server laufen im SGB-Protokoll redundant nebeneinander.

Juergen.Wedler@Compaq.com

Juergen.Wedler@Compaq.com

Probleme cont.

Cisco 803 als Client:

D-Channel Callback läuft nicht

Telefonieren geht nicht – es klingelt nur 1x
aktuelles IOS: c800-sy6-mw.122-0.5g.bin

spätestens bei Remote Capi erwarten wir die nächsten Probleme

Juergen.Wedler@Compaq.com

Juergen.Wedler@Compaq.com

Stand heute

Es stellte sich schnell heraus, daß es eine Lösung in dieser kompakten Art noch nicht gab.

Die Lösung beinhaltet:

- skalierbar, Router lassen sich in einer Standardkonfiguration einfach hinzu fügen.
- Radius Authentisierung mit Chap, Secure ID (LDAP in Vorbereitung)
- Caller ID Überprüfung mit Radius
- Stack Group Bidding Protocol
- E-IGRP
- Dial In über ISDN, Analog, V.110-GSM
- Multilink
- Stack Compression
- Accounting zum abrechnen mit den Kostenstellen.
Die Accounting Daten werden in die SQL Datenbank zurück geschrieben.

Wir haben heute etwa 3000 User, die per Dial In auf das Netz der Unilever zugreifen.

Juergen.Wedler@Compaq.com

Juergen.Wedler@Compaq.com

Zukunft

Wir sind dabei,

- das Flatfile in eine SQL Datenbank umzusetzen
- das Routing zu minimieren; wir sind dabei Super Netting einzusetzen, damit die Routing Updates minimiert werden.
Pro Dial In wird eine statische Route 2 mal ins E-IGRP redistributiert.
D.h. wir haben überm Tag gesehen einige Tausend Routing Updates, was zur Folge hat, daß der EIGRP Prozess durch booten etwa alle 6 Wochen neu gestartet werden muß.
Es treten dann undefinierte Zustände in den Routing Tabellen auf.
- neue Hardware ist geordert: 8-fach PRI inkl. 120 analoge Ports
- Wir werden im Sommer 2002 etwa 2000 User über diese Lösung angebunden haben.

Juergen.Wedler@Compaq.com

Juergen.Wedler@Compaq.com

COMPAQ

Stichwörter zu Thema bei Cisco

Stichwörter bei Cisco:

- LSA Large Scale Dialout
- Radius Attributes
- SGBP

Juergen.Wedler@Compaq.com

Juergen.Wedler@Compaq.com

COMPAQ