Annex C:
Corporate and «SoHo» access scenarios

C.1 Introduction

When connecting CPEs or "customer networks" to the NGN core network, *two* ~~2~~ aspects need to be considered:

- The network attachment, which mainly deals with IP connectivity, and
- The service attachment, which mainly deals with service registration.

Taking into account the general requirements for "customer networks" regarding IP connectivity, and taking into account already existing topologies *it* ~~one~~ can *be* conclude*d* that the following configurations need to be supported:

- *Corporate networks (Network attachment and Service attachment); and*
- *Small office and Home networks (Network attachment and Service attachment).*

C.1.1 Corporate networks

C.1.1.1 Network attachment

For Corporate networks the most likely method for network attachment (IP connectivity) is a private LAN with permanent IP connectivity to the public core network. This permanent connection uses one or more public IP address and performs NAPT. The end devices in the LAN receive a (private) IP address from a customer sited equipment (e.g. DHCP server in the corporate LAN).

It is clear that this network attachment deviates significantly of what is currently understood by network attachment via the NASS. However it is not sure that this will impact the current NASS architecture.

C.1.1.2 Service attachment

With respect to service attachment basically *two* ~~2~~ configurations are possible:

a) Each end device attaches individually to the service. This results in a direct interaction between the terminals and the NGN core network. A special case of this is sometimes referred to as hosted IP PBX or IP Centrex. In this case service attachment is not different than for an individual user.

b) The end devices attach to a customer sited intermediate (call and service control) function, which performs a service attachment proxy (it attaches to the service on behalf of the end device) This results in indirect interaction between the individual terminals and the NGN core network. The intermediate (customer sited) function is often called an IP PBX.

C.1.2 ~~Home and~~ Small office *and Home* networks

C.1.2.1 Network attachment

For ~~Home and~~ Small office *and Home* networks there are *two* ~~2~~ main methods for network attachment (IP connectivity):

- The first one is the same as for corporate networks.
- The second one is a private LAN with non-permanent IP connectivity to the public core network. This non-permanent connection uses one or more public IP address and performs NAPT. The end devices in the LAN receive a (private) IP address from a customer sited equipment (e.g. DHCP server in the SOHO LAN). ~~It is clear that~~ *This* set-up of the non-permanent connection relates to the current network attachment via the NASS. It is expected that this will not impact the current NASS architecture.

C.1.2.2 Service attachment

With respect to service attachment basically *two* ~~2~~ configurations are possible:

a) Each end device attaches individually to the service. This results in a direct interaction between the terminals and the NGN core network. A special case of this is sometimes referred to as hosted IP PBX or IP Centrex.

b) The end devices attach to a customer sited intermediate (call and service control) function, which performs a service attachment proxy (it attaches to the service on behalf of the end device) This results in indirect interaction between the individual terminals and the NGN core network. The intermediate (customer sited) function is often called an IP PBX.

C.2 Scenarios

C.2.1 Corporate networks, case 1

~~The following~~ Figure*s* 1 *and* 2 illustrate~~s~~ a possible realisation of the TISPAN NGN functional architecture, with a corporate network access permanently connected to the "public" network. Service attachment is done by each end device separately.

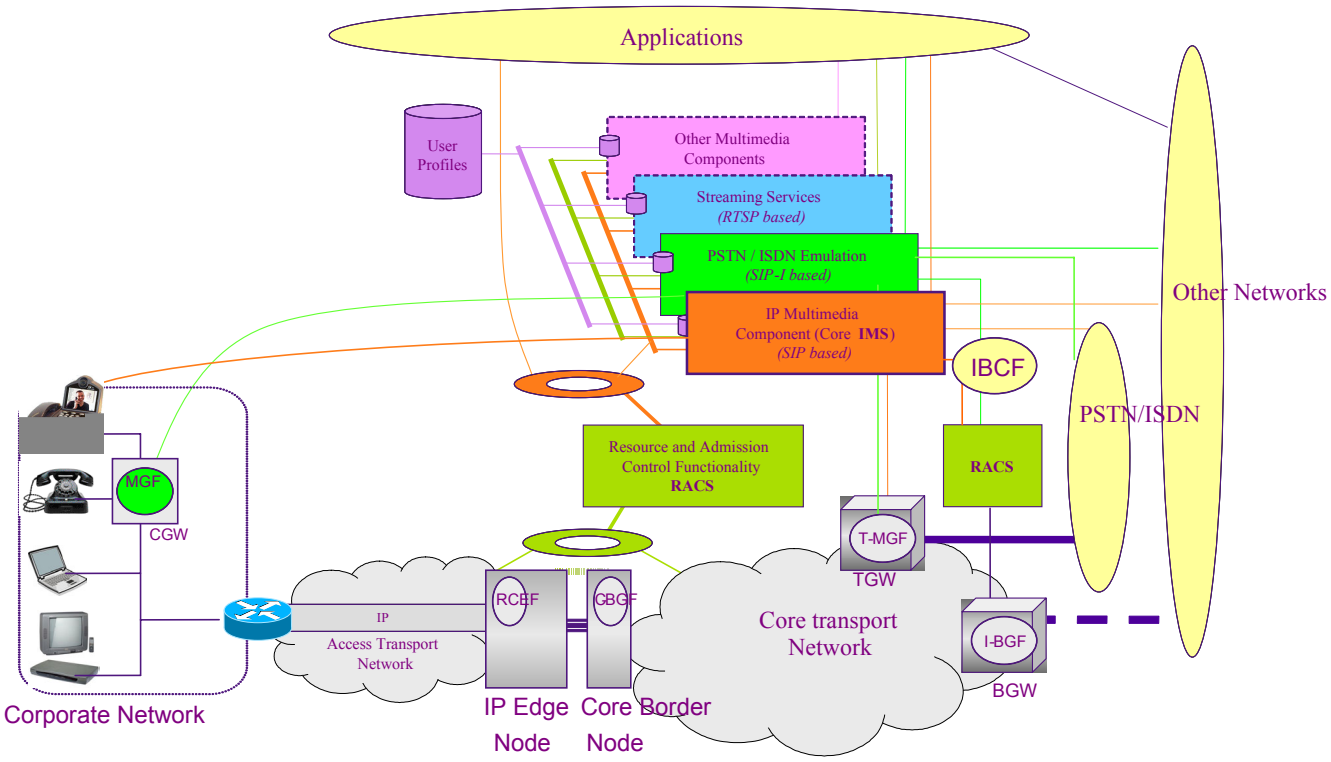

Figure 1:
Example overall architecture for Corporate network interconnect

This configuration assumes the following:

- A Border Gateway Function (C-BGF) is implemented in a Core Border Node sitting at the boundary between the corporate (access) network and a core network, at the core network side; *and*
- A Resource Control and Enforcement Function (RCEF) is implemented in an IP Edge node sitting at the boundary between the corporate network and the core network, at the access side.

Additionally the following assumptions ~~(similar to the assumptions for the xDSL case, see WI 2007)~~ are made :

- A Border Gateway Function (I-BGF) is implemented in a Border Gateway (BGW) sitting at the boundary with other IP networks;
- A Media Gateway Function (T-MGF) is implemented in a Trunking Gateway (TGW) at the boundary between the core network and the PSTN/ISDN; *and*
- A Media Gateway Function (MGF) is implemented in a Corporate Gateway (CGW) located in the customer premises.

Note: These assumptions are similar to the ones for the xDSL case, see WI 02007.

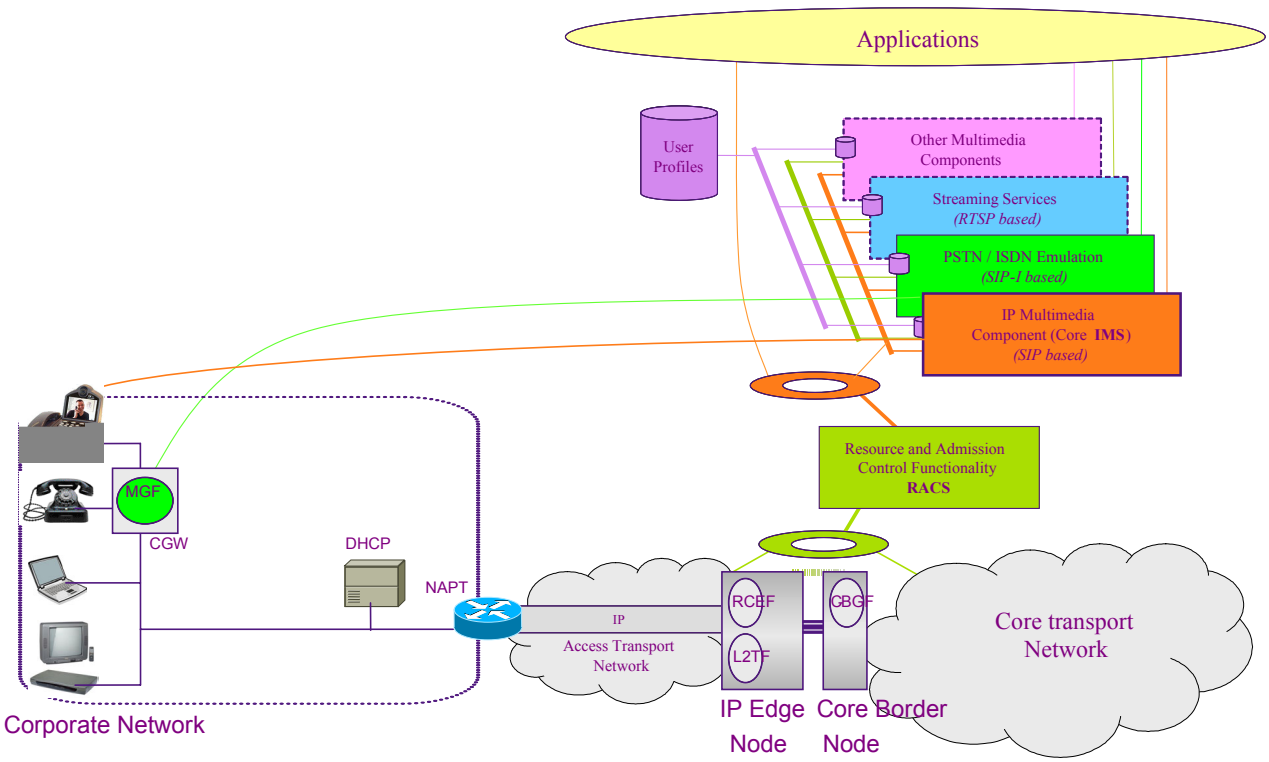

Figure 2:
Example detailed architecture for Corporate network interconnect

The network attachment of the end devices located in the corporate network "bypasses" the NASS. The following assumptions are made regarding the functions normally performed by the NASS:

- Dynamic provision of IP addresses and other terminal configuration parameters is done through dedicated equipment in the corporate network (e.g. DHCP server);
- Authentication taking place at the IP layer, prior or during the address allocation procedure is taken care of by the corporate network for what the end devices are concerned. The complete corporate network is considered to be authenticated permanently by the "public" NGN;
- Authorisation of network access based on user profiles is taken care of by the corporate network for what the end devices are concerned. The complete corporate network is considered to have permanent authorisation by the "public" NGN. Remark: as the NASS is bypassed, the public network doesn't necessarily have a user profile for each individual user. It may have a user profile for the complete corporate network;

- Access network configuration based on user profiles is a matter for the corporate network. The permanent IP connectivity between the corporate network and the "public" network is static and needs to be properly engineered. Remark: as the NASS is bypassed, the public network doesn't necessarily have a user profile for each individual user. It may have a user profile for the complete corporate network; *and*

- Location management taking place at the IP layer is a matter of the corporate network with regard to the end devices. From a "public" network point of view no (dynamic) location management is needed because of the permanent nature of the IP connectivity !

The service attachment is assumed to be done individually per end device and should not differ from the service attachment for individual users. However, the users of a corporate network will probably use a different AS (e.g. an IP centrex server).

C.2.2 Corporate networks, case 2

~~The following~~ Figure*s* 3 *and* 4 illustrate~~s~~ another possible realisation of the TISPAN NGN functional architecture, with a corporate network access. Service attachment is done by a customer sited intemediate functional entity (e.g. IP PBX).

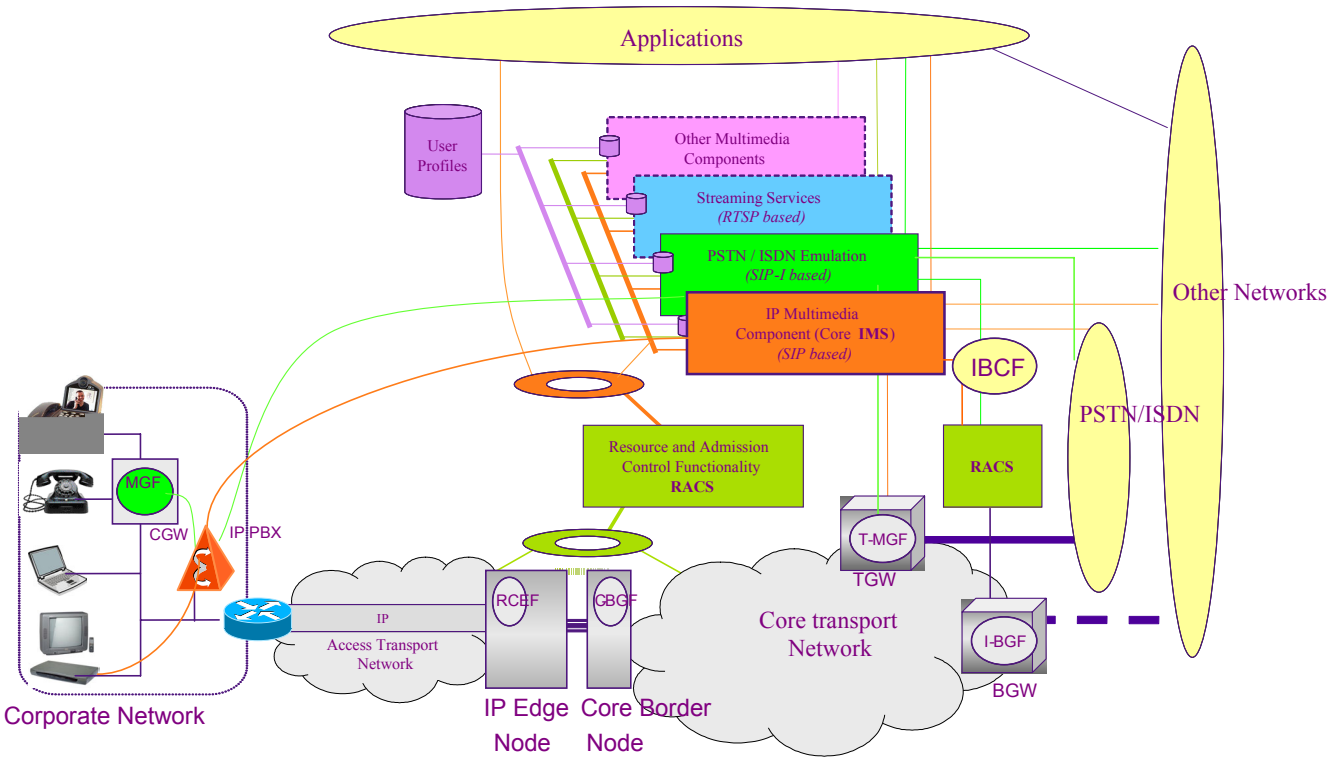

Figure 3:
Example overall architecture for Corporate network interconnect

This configuration has the same assumptions as above.

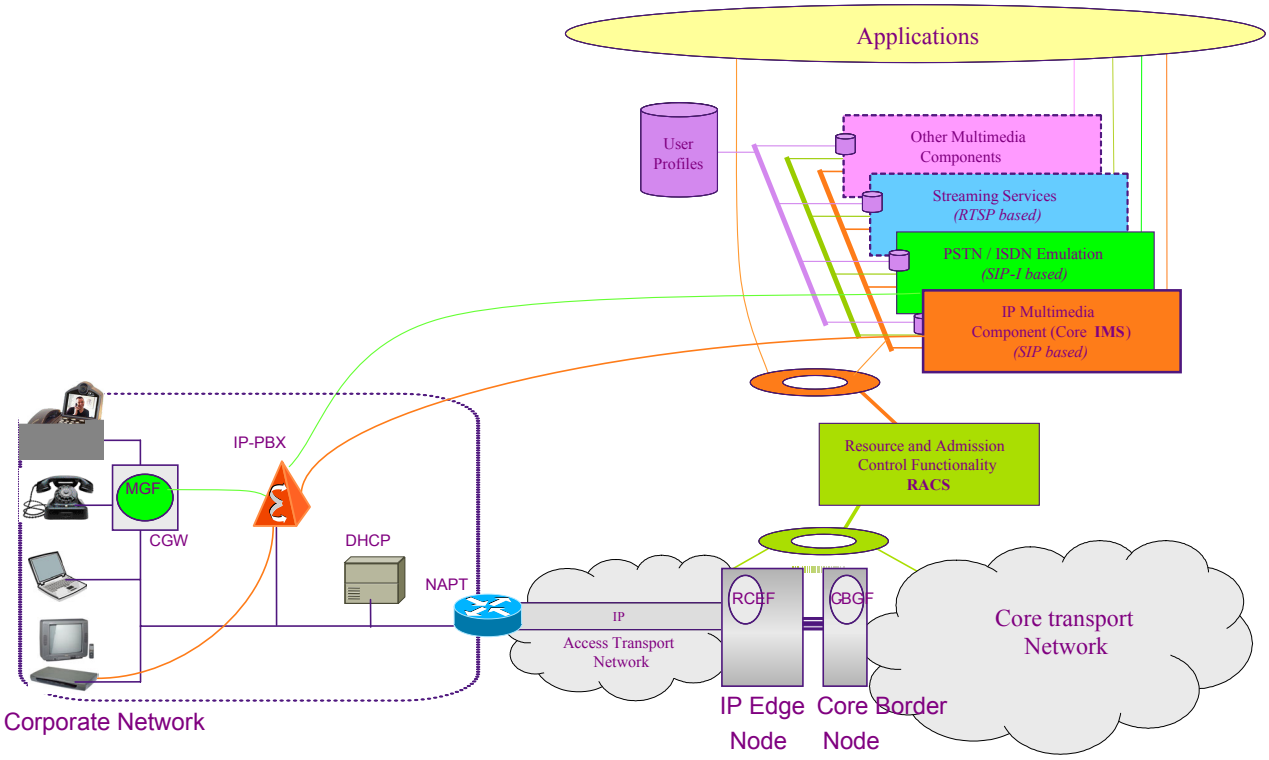

Figure 4:
Example detailed architecture for Corporate network interconnect

The network attachment of the end devices located in the corporate network "bypasses" the NASS. The same assumptions as in the case above are made regarding the functions normally performed by the NASS.

The service attachment of the individual end devices is done towards the customer sited IP PBX. This IP PBX "performs" service attachment on behalf of it's end devices to the "public" network. Whether this is done using signalling, or through configuration in the "public" network remains an open issue. In the latter case the service attachment has a rather permanent character, the "public" network is not aware of the presence of a particular user.

Note: ~~Remark:~~ *The method* how network attachment and service attachment work in cases of a corporate network user "roaming" outside the corporate network is *not detailed in this Annex* ~~for further study~~.

C.2.3 ~~Home and~~ Small office *and Home* networks, case 1

The cases described above for corporate networks also apply for "~~Home and~~ Small office *and Home* networks" having a permanent IP connectivity to the "public network". In the case of non-permanent IP connectivity the cases 1 and 2 apply.

~~The following~~ Figure*s* 5 *and* 6 illustrate~~s~~ a possible realisation of the TISPAN NGN functional architecture, with a "~~Home and~~ Small office *and Home*" network access, not permanently connected to the "public" network. Service attachment is done by each end device separately.

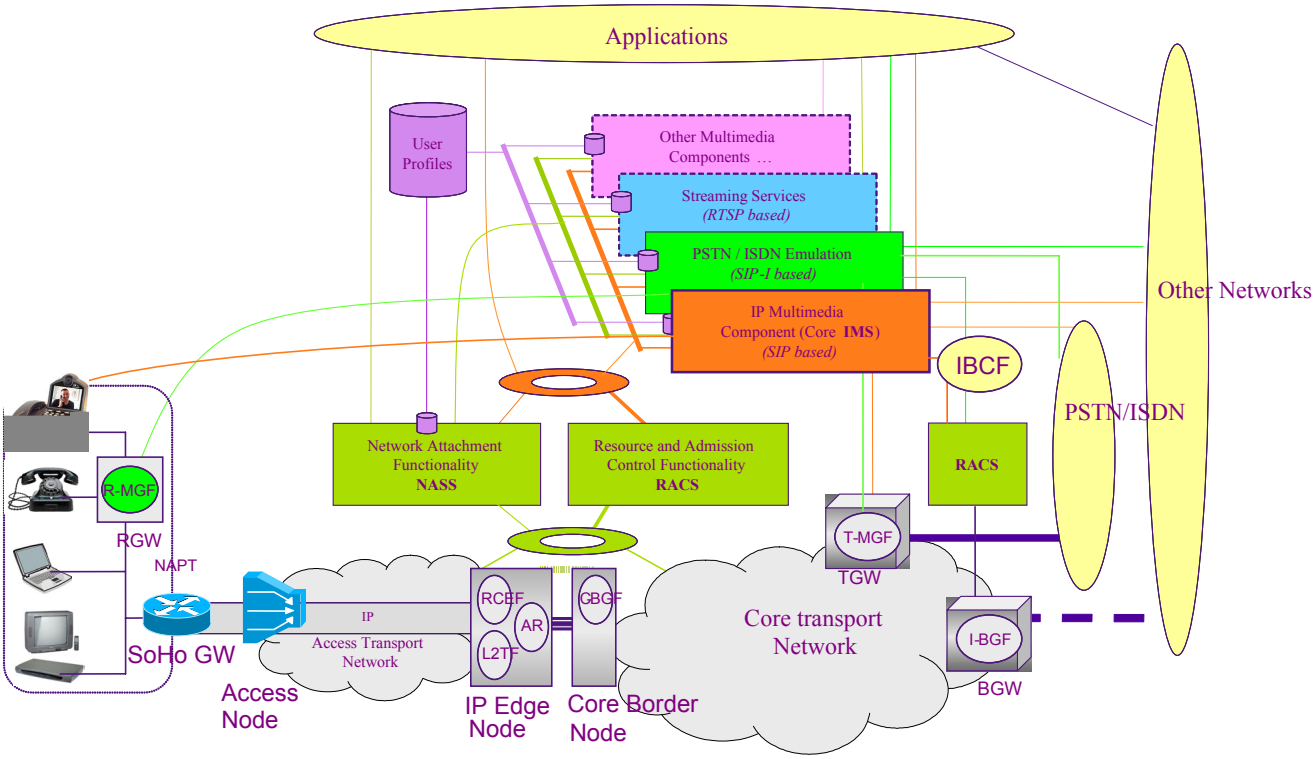

Figure 5:
Example overall architecture for ~~Home and~~ Small office *and Home* network interconnect

This configuration assumes the following (same as for the xDSL case, see WI 2007):

- A Border Gateway Function (C-BGF) is implemented in a Core Border Node sitting at the boundary between the ~~home and~~ small office *and home* (access) network and a core network, at the core network side;
- A Resource Control and Enforcement Function (RCEF) is implemented in an IP Edge node sitting at the boundary between the ~~home and~~ small office *and home* network and the core network, at the access side. This node also implements the L2TF and ARF functional entities;
- A Border Gateway Function (I-BGF) is implemented in a Border Gateway (BGW) sitting at the boundary with other IP networks;
- A Media Gateway Function (T-MGF) is implemented in a Trunking Gateway (TGW) at the boundary between the core network and the PSTN/ISDN; *and*
- A Media Gateway Function (MGF) is implemented in a Residential Gateway (RGW) located in the customer premises.

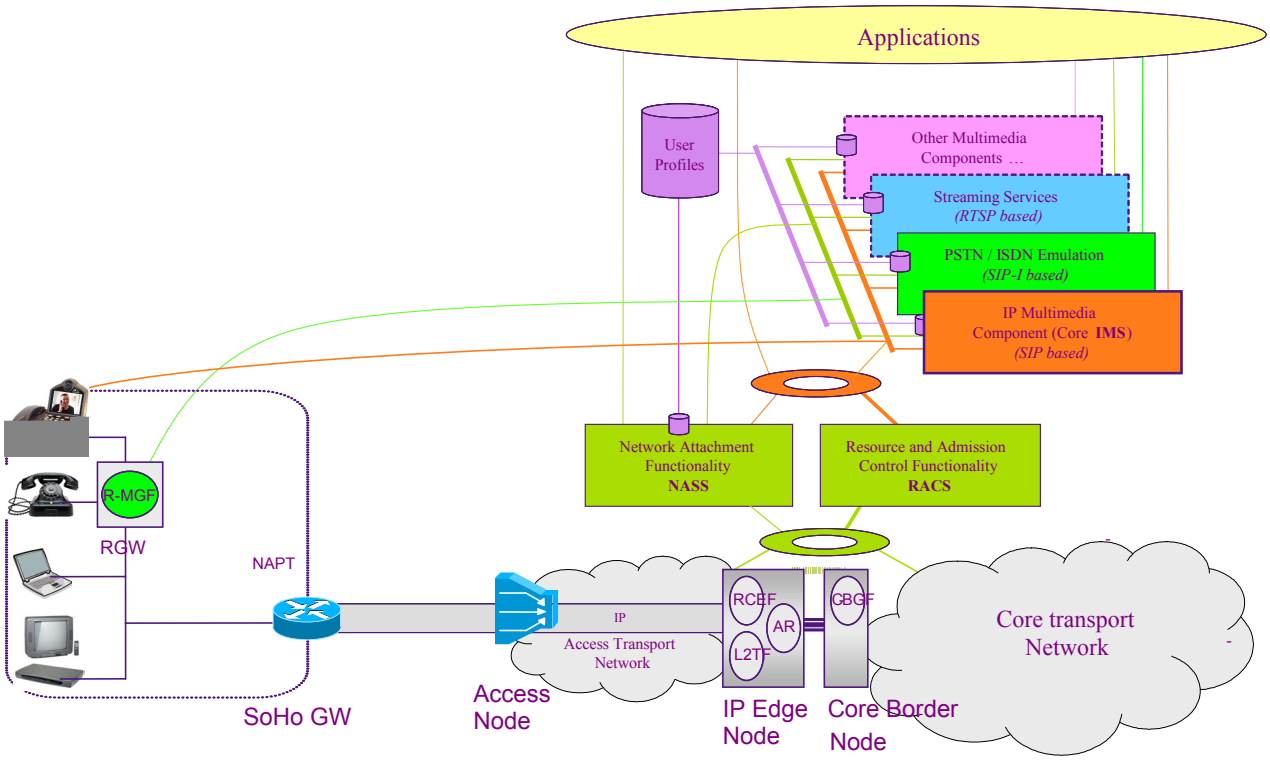

Figure 6:
Example detailed architecture for Corporate network interconnect

The network attachment of the end devices located in the ~~home and~~ small office *and home* network "bypasses" the NASS. However, the SoHo GW uses the NASS to attach the whole "~~Home and~~ Small office network *and Home*" to the core network. The following assumptions are made regarding the functions normally performed by the NASS :

- Dynamic provision of IP addresses and other terminal configuration parameters: The SoHo GW receives an IP address and other configuration parameters from the NASS at his public network side. It provides (private) IP address and configuration parameters to the end devices at its ~~home and~~ small office *and home* network side;
- Authentication taking place at the IP layer, prior or during the address allocation procedure: the Home GW is authenticated by the NASS. Whether the end devices authenticate towards the Home GW is a ~~Home and~~ Small office *and Home* matter;
- Authorisation of network access based on user profiles: The NASS performs this function for all traffic coming from the Home GW;
- Access network configuration based on user profiles: is performed by the NASS as currently described. However, individual users are not known by the NASS, only the SoHo user (group account) is known; *and*
- Location management taking place at the IP layer~~:~~ is performed by the NASS as currently described.

The service attachment is assumed to be done individually per end device and should not differ from the service attachment for individual users. However, the users of a ~~Home and~~ Small office *and Home* network will probably use a different AS (e.g. an IP centrex server).

Note: ~~Remark:~~ *The method* how network attachment and service attachment work~~s~~ in cases of a ~~home and~~ small office *and home* network user "roaming" outside the ~~home and~~ small office *and home* network is *not detailed in this Annex* ~~for further study~~.

C.2.4 ~~Home and~~ Small office *and Home* networks, case 2

The ~~following~~ Figure*s* 7 *and* 8 illustrate~~s~~ a possible realisation of the TISPAN NGN functional architecture, with a "~~Home and~~ Small office *and Home*" network access, not permanently connected to the "public" network.

Service attachment is done by a customer sited intemediate functional entity (e.g. IP PBX).

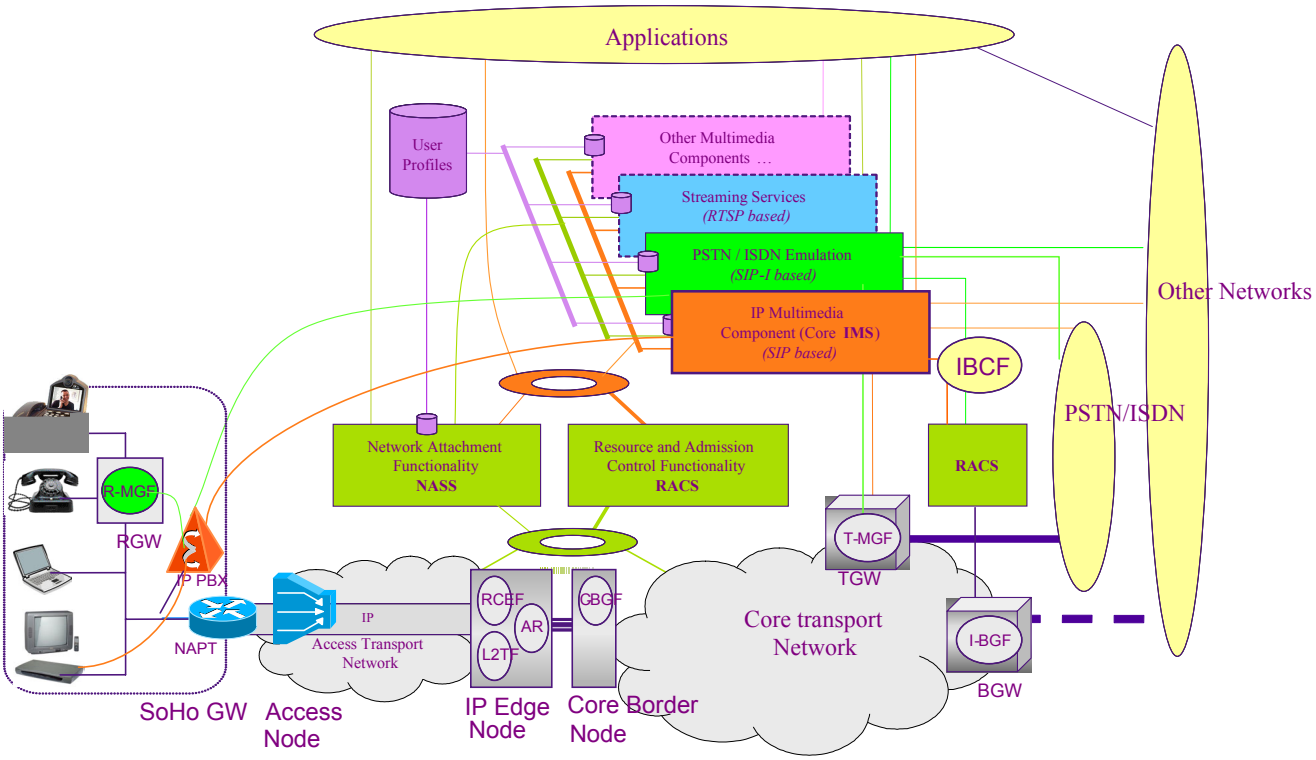

Figure 7:
Example overall architecture for ~~Home and~~ Small office *and Home* network interconnect

This configuration assumes the following ~~(same as for the xDSL case, see WI 2007)~~:

- A Border Gateway Function (C-BGF) is implemented in a Core Border Node sitting at the boundary between the ~~home and~~ small office *and home* (access) network and a core network, at the core network side.
- A Resource Control and Enforcement Function (RCEF) is implemented in an IP Edge node sitting at the boundary between the ~~home and~~ small office *and home* network and the core network, at the access side. This node also implements the L2TF and ARF functional entities.
- A Border Gateway Function (I-BGF) is implemented in a Border Gateway (BGW) sitting at the boundary with other IP networks.
- A Media Gateway Function (T-MGF) is implemented in a Trunking Gateway (TGW) at the boundary between the core network and the PSTN/ISDN.
- A Media Gateway Function (MGF) is implemented in a Residential Gateway (RGW) located in the customer premises.

Note: This is the same as for the xDSL case, see WI 02007.

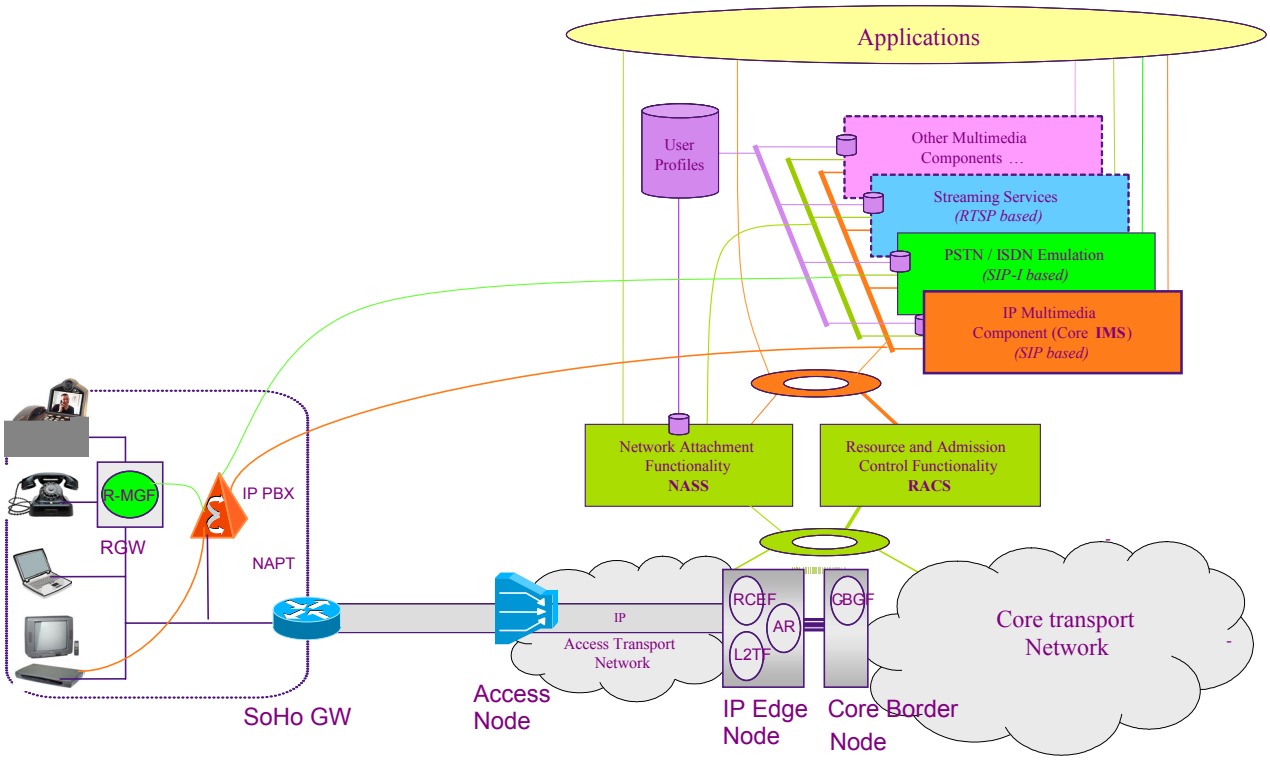

Figure 8:
Example detailed architecture for SoHo network interconnect

The network attachment of the end devices located in the ~~home and~~ small office *and home* network "bypasses" the NASS. However, the SoHo GW uses the NASS to attach the whole "~~Home and~~ Small office *and Home* network" to the core network. The same assumptions as above, regarding the functions normally performed by the NASS, are made.

The service attachment of the individual end devices is done towards the customer sited IP PBX. This IP PBX "performs" service attachment on behalf of it's end devices to the "public" network. Whether this is done using signalling, or through configuration in the "public" network remains an open issue. In the latter case the service attachment has a rather permanent character, the "public" network is not aware of the presence of a particular user.

Note: ~~Remark:~~ *The method* how network attachment and service attachment work in cases of a SoHo network user "roaming" outside the SoHo network is *not detailed in this Annex* ~~for further study~~.

~~C.3 Conclusion~~

~~The above scenarios show examples of how corporate and home and small office networks can be connected to the TISPAN NGN.~~

~~It is proposed to :~~

~~1) capture these scenarios in the appropriate document, probably as an informative annex~~

~~2) further analyse the impact of the network attachment "bypassing" the NASS~~

~~3) further analyse the impact of the service attachment performed by an customer sited intermediate functional entity.~~

~~Although not a TISPAN NGN Release 1 capability, possible roaming scenarios from a corporate or home and small office network to the "public" network should be taken into account.~~