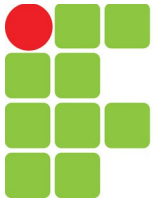

INSTITUTO FEDERAL
SANTA CATARINA

PROJETO VLAN

Florianópolis – SC

Abril de 2014

INSTITUTO FEDERAL
SANTA CATARINA

PROJETO VLAN

GRUPO DE TRABALHO – VLAN

Portaria nº 17 de 03/01/2014

Memorando nº 4887 de 26/12/2013

GRUPO DE TRABALHO – VLAN

Portaria nº 17 de 03/01/2014

Memorando nº 4887 de 26/12/2013

Período de atividade entre 02/01/2014 a 10/03/2014

Construção de modelo de rede local virtual para todos os câmpus do IFSC

INTEGRANTES DO GT-VLAN

Glaidson Menegazzo Verzeletti (Coordenador) - Câmpus Lages

Alberto Barros – Câmpus Criciúma

Daniel Schultz – PRODIN

Evandro Espíndola – Câmpus Florianópolis

Gilberto Coutinho – Câmpus Canoinhas

Renato Cesca – Câmpus Florianópolis

Ricardo Martins – Câmpus São José

Vinícius Coelho – PRODIN

PARTICIPAÇÃO

Emerson Ribeiro de Mello – Diretor de Tecnologia da Informação – DTIC

Ederson Torresini – Câmpus São José

Marcelo Maia Sobral – Câmpus São José

Comunidade T.I.C. – IFSC

Histórico de Trabalho

Data	Versão	Descrição
19/12/2013		Reunião com tic@, coordenada pelo Emerson, definindo estratégias de trabalho
20/12/2013		Encaminhamento da reunião, indicando prazos e metodologia de trabalho
03/01/2014		Publicação da portaria n. 17 oficializando os trabalhos do GT-VLAN
20/01/2014		Iniciado mapeamento de VLAN nos campus
03/02/2014		Disponibilizado formulário online para mapeamento das VLAN no IFSC
17/02/2014		Consulta vocacionada para conhecer realidades particulares de alguns campus
20/02/2014		Solicitação ao GT modelos de VLAN idealizados, segundo particularidades locais
28/02/2014		Compilação do mapeamento das VLANs
10/03/2014		Compilação de recomendações literárias quanto a particularidades sobre VLANs IDs
25/03/2014	1	Elaborado o modelo denominado “Proposta-01”
31/03/2014	2	Ajustes de acordo com análise do GT resultando na “Proposta-02”
01/04/2014		Submetida “Proposta-02” para aprovação pela comunidade T.I.C. do IFSC
11/04/2014	3	Ajustes do modelo, resultando no modelo denominado “Proposta-03”
14/04/2014		Aprovação do modelo pelo diretor de T.I.C do IFSC
15/04/2014	Oficial	Publicação do projeto final

Sumário

1. MOTIVAÇÃO.....5

2. METODOLOGIA.....6

3. PREMISSAS E PONDERAÇÕES.....7

4. MODELO FINAL.....8

ANEXO A.....14

ANEXO B.....21

ANEXO C.....22

ANEXO C.....22

ANEXO D.....23

1. MOTIVAÇÃO

O Instituto Federal de Santa Catarina contando com uma estrutura multicampi, situação esta que aliada a uma política de Tecnologia da Informação e Comunicação que prevê a implantação contínua de serviços para a comunidade acadêmica, se encontra em um momento em que as padronizações se fazem necessárias como forma de se criar um alicerce seguro para a consolidação de novas soluções.

De acordo com este pensamento, surge a necessidade de padronização da segmentação de rede, ou simplesmente VLANs (Virtual Local Area Networks), propiciando a solidez exigida para que soluções de gestão de rede mais maduras possam ser adotadas e implementadas com facilidade, como é o caso da eduroam[1].

Em janeiro de 2014 é criado o grupo de trabalho de rede virtual local, ou somente GT-VLAN, com o objetivo único de propor um modelo teórico de segmentação de rede, o qual possa ser escalável de forma a atender tanto câmpus menores (avançados) quanto câmpus maiores do IFSC.

[1] O eduroam (education roaming) é um serviço de acesso sem fio seguro, desenvolvido para a comunidade internacional de educação e pesquisa. A iniciativa permite que os estudantes, os pesquisadores e as equipes das instituições participantes obtenham conectividade à Internet, através de conexão sem fio (wi-fi), dentro de seus campi e em qualquer localidade que ofereça essa facilidade como provedora de serviço.

2. METODOLOGIA

Para atender a proposta inicial de oferecer ao IFSC um modelo teórico escalável de VLANs o GT-VLAN adotou a seguinte linha de trabalho:

1º- Fazer um levantamento da realidade de cada câmpus
2º- Formular um modelo desejável de VLANs
3º- Mesclar o modelo idealizado com a realidade de cada local
4º- Submeter este modelo à análise da comunidade T.I.C. do IFSC
5º- Coletar as sugestões da comunidade T.I.C. e adequá-las a um modelo unificado
6º- Aprovar modelo unificado junto à diretoria de T.I.C. do IFSC

Inicialmente o trabalho de mapeamento das realidades de cada campus foi feito através de um formulário on-line, onde cada profissional de T.I.C. pode opinar de forma autônoma sobre a situação atual da sua própria infraestrutura local. Levantamento este que poderá ser consultado no anexo A.

Os campus foram então agrupados em 5 (cinco) tipos, de acordo com seu tamanho e número de alunos. Para tanto foi utilizada a proposta feita durante a realização do PDI (Plano de Desenvolvimento Institucional) 2014/2018 e aprovada em reunião do CODIR de 16/09/2013. Com as informações de tipologia de campus e infraestrutura atual, foi elaborado o documento “resumo”, conforme anexo C.

O grupo de trabalho se reuniu e decidiu o que seria importante constar no modelo de VLANs e o que seria de obrigatória implementação. Este estudo foi então mesclado ao “resumo” feito anteriormente, chegando-se a um modelo denominado “Proposta-01”. Novamente o GT após uma análise criteriosa sugeriu 2 (duas) pequenas alterações, conforme consta no anexo D, chegando-se finalmente na “Proposta-02”, a qual foi submetida a apreciação da comunidade T.I.C. do IFSC.

Durante o período de análise do modelo proposto, surgiram algumas novas ideias (Anexo D), as quais foram incorporadas ao projeto, gerando a “Proposta-03”, em última instância aprovada pela diretoria de tecnologia da informação do IFSC.

3. PREMISSAS E PONDERAÇÕES

De acordo com as características de alguns equipamentos de rede presente nos câmpus do IFSC e sugestões de algumas literaturas sobre o assunto, o GT-VLAN selecionou algumas premissas básicas para nortear a confecção do modelo proposto, conforme segue:

1. CISCO ASA 5505: Aceita VLANs com IDs entre 1 e 4090
2. CISCO ASA 5505: Licença indica possibilidade de criação de 8 portas tronco (interfaces de 0 a 7), porém somente 20 VLANs (Configuration -> Licensing -> Activation Key)
3. Material da CISCO (Netacad CCNA) classifica as VLANs de ID 1 a 1005 como Intervalo Normal e IDs de 1006 a 4094 como Intervalo Estendido, onde as de modo estendido são utilizadas especialmente por operadoras e possuem menos opções que as VLANs de intervalo normal. Cita ainda que o VTP (VLAN Trunking Protocol) suporta somente VLANs de modo normal.
4. Marcos Filippetti em seu livro CCNA versão 4.1 afirma que as VLANs de número 2 a 1005 são elegíveis para implementação do processo de prunning (poda).
5. Steve McQuery, no livro Interconectando Cisco Network Devices, afirma que VLANs de ID 1, 1002, 1003, 1004 e 1005 são consideradas default, sendo as últimas reservadas para uso em topologias como Token Ring e FDDI.
6. De acordo com o levantamento feito nos campus, não haveria necessidade de utilizar as VLANs estendidas, o que seria necessário somente caso os campus viessem a ter IDs exclusivos e não padronizados. Nesta última situação faria sentido criar blocos grande com IDs de VLAN estendida de forma a identificar cada campus.

4. MODELO FINAL

O modelo oficial de VLANs do IFSC, segue um padrão composto basicamente por 3 (três) dígitos, os quais se desdobram para oferecer uma estrutura escalável e ao mesmo tempo simples em termos administrativos. Abaixo é apresentado o significado de cada dígito identificador:

ID	DESCRIÇÃO
Z . .	Dígito Identificador do Grupo Principal
. x .	Dígito que identifica uma subdivisão em blocos, porém limitados ao escopo do grupo principal.
. . y	Subdivisão do bloco

Tabela 01 – Dígitos identificadores

O “Dígito Identificador Principal” define os macro-grupos utilizados para a segmentação hierarquizada do modelo oficial, conforme segue comentado logo abaixo:

ID	GRUPO PRINCIPAL	DESCRIÇÃO
0 x y	Enlaces	Links com internet, backbone interno, NAS, rede de backup, etc.
1 x y	DMZ, Servers, T.I.C.	Duas redes de servidores (DMZ e Servers) e uma para equipe de T.I.C
2 x y	Administrativo	X: Grandes Departamentos. Y: Subdivisões
3 x y	Academico	X: Grandes Áreas (pesquisa, laboratórios, etc). Y: Subdivisões
4 x y	Academico & Visitante	Bloco estendido para VLAN Aluno, com IDs 490 a 499 reservado para rede visitante cabeada
5 x y	Wireless	520 - 529: Administrativo 530 - 539: Acadêmico 540 - 549: Visitante
6 x y	CFTV	Monitoramento por câmeras IPs
7 x y	VoIP	Ramais IP
8 x y	Impressora	Impressoras com suporte à rede.
9 x y	Gerencia	Configuração e gerência dos ativos de rede.

Tabela 02 – Modelo resumido

Resumidamente, foi aprovado 12 (doze) IDs considerados obrigatórios em todos os campus do IFSC. Estes constarão em qualquer infraestrutura e servirão como base para a implantação de novos sistemas e soluções de rede.

VLAN ID	VLAN_NAME
0 1 0	Internet
1 0 0	DMZ
1 0 5	BD
1 1 0	Server
1 2 0	TIC
2 0 0	ADM
3 0 0	Aluno
5 2 0	Wifi_ADM
5 3 0	Wifi_Aluno
5 4 0	Wifi_Visitante
8 0 0	Impressora
9 0 0	Gerencia

Tabela 03 – VLAN IDs obrigatórios

Detalhando o modelo aprovado para o IFSC, segue abaixo cada grupo de VLANs devidamente comentado, onde é marcado em vermelho os IDs obrigatórios (ver tabela 03), em preto os IDs desejáveis e em cinza claro as possibilidades para expansão da infraestrutura. Os exemplos de uso demonstram a escalabilidade deste modelo, onde pode-se eventualmente chegar por exemplo a 190 IDs distintos para a VLAN Acadêmica, o que possibilita ao gestor de rede adequar o modelo de acordo com cada realidade local.

	VLAN_ID	VLAN_Name	DESCRIÇÃO
-	1	**Default**	Obrigatória, por ser considerada VLAN administrativa.

Obs.: *Não deve ser utilizada para tráfego de rede, no entanto deve ser mantida por questões de compatibilidade dos equipamentos e recomendação dos fabricantes.*

0	**0** 1 0	Internet	Link principal com a Internet
	0 1 1	Internet_01	...Exemplo para segundo enlace de Internet
	0 1 2	Internet_02	...Exemplo para terceiro enlace de Internet
	0 2 0	Backbone	Backbone da rede interna do câmpus – uso exclusivo para comunicação entre roteadores da rede local (LAN)
	0 3 0	NAS	Backbone exclusivo para comunicação do sistema de backup
	0 3 1	SAN	Backbone exclusivo para implementações de transferência de arquivos em blocos, com alta performance. Implementação utilizada por sistema de storage.

Obs.: *O ID 0 (zero) é utilizado apenas para fins didáticos, não sendo necessário adicioná-lo em uma implementação prática. Neste grupo são elencados todos os enlaces dedicados, tanto para Internet quanto para rede interna, chegando a abranger backbone com dedicação exclusiva a sistemas de backup ou storage.*

1	**1** 0 0	DMZ	Servidores com acesso público. Por exemplo, site do campus.
	1 0 5	BD	Servidores de banco de dados, como MySQL, PostgreSQL, LDAP, etc.
	1 1 0	Server	Servidores de rede acessíveis somente no âmbito da rede interna, como por exemplo o servidor de arquivos.
	1 1 5	Server_Aluno	Servidores de uso acadêmico em caráter temporário
	1 2 0	TIC	Rede exclusiva para profissionais de T.I.C.

VLAN DMZ: *Deverão ficar neste segmento servidores e serviços com publicação externa (Internet).*

VLAN BD: *Servidores utilizados normalmente pela DMZ ou rede Server, porém sem a necessidade de ficarem expostos diretamente aos clientes. Portanto recomenda-se fortemente a aplicação de filtros de acesso a este segmento de rede.*

VLAN Server: *Nome em inglês apenas para evitar relação com servidores (pessoas).*

VLAN Server_Aluno: *Neste segmento ficarão os servidores de rede em uso pelos projetos de pesquisa, ativos somente durante o período que durar a pesquisa ou a necessidade. O acesso a estes serviços será controlado de forma a evitar falhas na segurança, sendo a publicação externa (visível no âmbito da Internet) dependente de autorização.*

VLAN TIC: *Opcionalmente, pode-se fazer outras divisões subdivisão para desenvolvimento, suporte, estagiários, etc, com IDs 120,121,122, [...], 129, garantindo níveis diferenciados de acesso. A ideia principal é garantir a este segmento um nível de acesso à rede de gerência e ao mesmo tempo aos servidores e serviços, no que se refere à manutenção dos sistemas.*

2	2 0 0	ADM	Rede administrativa (TAE e Docentes)
	2 1 0	ADM_210	...Exemplo de segundo segmento administrativo
	2 2 0	ADM_220	...Exemplo para terceiro segmento administrativo
	2 3 0	ADM_230	...Exemplo para quarto segmento administrativo
	2 3 1	ADM_231	.....Exemplo para sub-divisão do quarto segmento administrativo
	2 3 2	ADM_232	.....Exemplo para sub-divisão do quarto segmento administrativo

Obs.: *Opcionalmente pode-se subdividir esta VLAN 200 em outros segmentos, por blocos, andares, coordenações, entre outros, a fim de diminuir o domínio de broadcast e melhorar o monitoramento e segurança na comunicação entre as sub-redes.*

3	3 0 0	Aluno	Rede de alunos, utilizada para laboratórios, salas de aula, ambientes de pesquisa, etc.
	3 1 0	Aluno_310	...Exemplo para rede de alunos
	3 2 0	Aluno_320	...Exemplo para rede de alunos
	3 2 1	Aluno_321	.....Exemplo para subdivisão da rede de alunos acima

Obs.: *Mesmo caso acima para a rede ADM, manter preferencialmente um segmento por laboratório ou área de pesquisa. Pode-se criar blocos para identificar áreas com coordenações diferentes como laboratório de informática, laboratórios de automação, entre outros, contando inclusive com subdivisões para indicar o número do laboratório.*

4	4 0 0	Aluno_400	...Exemplo para rede de alunos
	4 1 0	Aluno_410	...Exemplo para rede de alunos
	4 9 0	Visitante	Segmento utilizado como contingência para eventos externos que necessitem de infraestrutura cabeada temporária.
	4 9 1	Visitante_491	...Exemplo para rede de visitantes

Obs.: *RESERVA DOS IDS 490 a 499 PARA A REDE VISITANTES CABEADA.*

5	5 2 0	Wifi_ADM	Destinada para uso administrativo, segmento com privilégios de acesso diferenciado a sistemas. Segundo dígito (2) utilizado propositalmente como elo com a rede administrativa
	5 3 0	Wifi_Aluno	Mesmo caso anterior, segundo dígito (3) utilizado como referência ao segmento discente.
	5 4 0	Wifi_Visitante	Acesso em eventos, terceirizados e visitantes EduRoam de outras instituições.

Obs.: *Para as redes Wifi foi deixado um intervalo de identificação relativamente grande entre elas, justamente para garantir no futuro uma possível fragmentação. É recomendação dos grandes fabricantes a segmentação da rede wireless em vários grupos de broadcast pela própria característica de tráfego deste sinal de rádio. Portanto, para cada rede é possível fazer uma segmentação em até 10 grupos. Quem determinará este ajuste, a priori, serão os mecanismos de monitoramento de performance da rede wireless.*

6	6 0 0	CFTV	Segmento destinado às câmeras de vigilância IP.

Obs.: *A separação dos dispositivos de segurança, como as câmeras IPs para vigilância monitorada, requerem um controle de acesso exclusivo. A separação destes equipamentos em um segmento isolado facilita a aplicação de ACLs específicas, dessa forma evitando o acesso por pessoas não autorizadas.*

7	7 0 0	VoIP	Ramais e gateway IP

Obs.: *Foi determinado a segmentação destes dispositivos devido à característica sensível de necessidade quanto à qualidade de serviço (QoS). Sub-redes adicionais podem ser criadas neste grupo 7 para atender demandas muito específicas, como transmissões multimídia, câmeras compartilhadas, entre outras aplicações que exigem um controle mais refinado de gestão de tráfego.*

8	8 0 0	Impressora	

Obs.: *A segmentação da rede de impressão, garante um melhor nível de segurança para estes dispositivos que normalmente não acompanham uma camada de segurança muito vasta, ou que na maioria dos casos permite que qualquer pessoa possa fazer impressão diretamente.*

O acesso aos dispositivos pode ser limitado somente ao próprio servidor de impressão, o que garante que todo documento passe por um sistema de controle de filas antes de ser impresso.

Eventualmente pode-se liberar o acesso a dispositivos de digitalização (scanners) através de regras específicas de ACLs.

9	9 0 0	Gerencia	Rede exclusiva para configuração de ativos de rede.

Obs.: *Para este segmento se entende o uso por ativos de rede que compõem normalmente o alicerce de rede cabeada ou wireless, como os switchs e APs (access points).*

ANEXO A

Consulta pública sobre Infraestrutura de VLANs

(INFORMAÇÕES RETIRADAS PARA FINS DE DIVULGAÇÃO PÚBLICA)

CAMPUS

ID	Nome	Sub-rede	Observações

Servidor:
Data Envio:
TIPO CAMPUS*

ANEXO B

TIPOLOGIA DOS CÂMPUS

REITORIA	TIPO I	TIPO II	TIPO III	TIPO IV	TIPO V
	FLN	SJE	ARU	CDR	GPB
			CCO	CAN	URP
			CTE	CRI	XXE
			JAR	GAS	
			JLE	ITJ	
				JGW	
				LGS	
				PHB	
				SMO	

Ps: *A tipologia de campus é um dos temas abordados na elaboração do PDI 2014/2018 e pode ser consultado em "Estrutura Organizacional", no tópico "das diretrizes para o planejamento estratégico".*

ANEXO C

Compilação realizada a partir da consulta pública sobre a Infraestrutura de VLANs

	VLAN (Descrição)	REI	ARU	CAN	CCO	CDR	CRI	CTE	FLN*	GAS	JAR	JLE	LGB	SJE	URP	XXE	TOTAL	%
1	**DMZ 01**			x	x	x		x	x	x	x	x	x	x	x		11	73
2	**DMZ 02**													x			1	7
3	**Enlace Outsite 01**			x		x		x	x		x	x	x	x	x	x	10	67
4	**Enlace Outside 02**			x		x					x	x			x	x	6	40
5	**Enlace Outside 03**															x	1	7
6	**Enlace Inside 01**												x			x	2	13
7	**Enlace Inside 02**															x	1	7
8	**Enlace Inside 02**															x	1	7
9	**Servidores**	x							x				x	x		x	5	33
10	**T.I.C.**								x			x	x				3	20
11	**ADM cabeada 01**	x	x	x		x	x	x	x	x	x	x	x	x	x	x	14	93
12	**ADM cabeada 02**	x	x						x				x			x	5	33
13	**ADM cabeada 03**								x				x				2	13
14	**ADM cabeada 04**								x								1	7
15	**ADM cabeada 05**								x								1	7
16	**ADM cabeada 06**								x								1	7
17	**ADM cabeada 07**								x								1	7
18	**ADM cabeada 08**								x								1	7
19	**WIFI_ADM**	x	x			x			x			x	x			x	7	47
20	**Alunos Cabeada**		x	x		x	x	x	x	x			x				8	53
21	**Lab 1**		x			x			x				x	x	x	x	7	47
22	**Lab 2**		x			x			x				x	x	x	x	7	47
23	**Lab 3**		x						x				x				3	20
24	**Lab 4**		x						x				x				3	20
25	**Lab 5**								x				x				2	13
26	**Lab 6**								x				x				2	13
27	**WIFI_Aluno**		x			x			x			x	x				5	33
28	**Visitante**												x				1	7
29	**WIFI_Visitante**	x	x						x				x				4	27
30	**CFTV**								x				x				2	13
31	**VoIP**												x				1	7
32	**Impressora**								x			x	x				3	20
33	**Gerencia**								x			x	x				3	20

LEGENDA

Reitoria	
Campus Tipo I	FLN*: VLANs de acordo com projeto idealizado
Campus Tipo II	
Campus Tipo III	
Campus Tipo IV	GPB, ITJ, JGW, PHB e SMO não responderam a consulta pública
Campus Tipo V	
30%	Mais de 30% dos campus implementaram esta VLAN

ANEXO D

Histórico de Adequações dos modelos propostos

Proposta 01 -> 02

31/03/2014	Alterado bloco 4 para servir como segmento estendido à "VLAN Aluno", mantendo reserva de IDs 440 a 449 para a rede Visitante Cabeada. Na proposta-01 o bloco 4 contemplava apenas o segmento VISITANTES.
31/03/2014	Alterado nome das VLANs de forma que nomenclatura das subdivisões tenham relação com o próprio ID (número), de forma a ficar mais clara a relação entre o nome e o ID.

Proposta 02 -> 03

11/04/2014	Mudado bloco da VLAN cabeada para "visitantes", para o intervalo entre 490 a 499.
11/04/2014	Incluída a VLAN com ID 105 como obrigatória, como forma de serem inclusos serviços de banco de dados, como LDAP, SQL, etc
11/04/2014	Incluída a VLAN com ID 115 como opcional, para que servidores de rede utilizados em projetos de pesquisa pelos professores e alunos pudessem ser contemplados.
11/04/2014	Mudada descrição da VLAN com ID 900, de forma que entenda se tratar de um segmento utilizado exclusivamente por ativos que compõem os pilares da rede cabeada e sem fio.
11/04/2014	Incluída a VLAN com ID 031 (SAN) de forma a diferenciar uma rede de backbone com fim de exclusividade para serviços de backup (normalmente topologia NAS) de uma rede de backbone de alta performance utilizada por serviços de armazenamento em bloco, como sistemas de storage.
15/04/2014	VLAN de impressoras marcada como obrigatória. Mantida separação deste segmento em virtude do tráfego diferenciado (alto volume de dados e baixa prioridade).
15/04/2014	Alterada nomenclatura do nome da VLAN "Enlace" para "Internet"
15/04/2014	Alterada nomenclatura do nome da VLAN "Adm" para "ADM": somente alterada para caixa alta.